

Человек

ТЕОРИЯ

равнелин

Б. М.

ТЕОРИЯ СРАВНЕНИЯ

ОБЩЕСТВЕННЫЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИСТИНА И СВОБОДА

1997

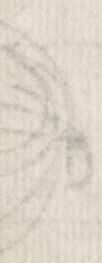
И. П. Тейтман

Академия наук Республики Беларусь, Институт математики

ОБЩЕСТВЕННЫЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
ИСТИНА И СВОБОДА

БИБЛИОТЕКА
ИСТИНА И СВОБОДА

5261



am

Kert

ТЕОРІЯ СРАВНЕНІЙ.

GABINET MATEMATYCZNY
Towarzystwa Naukowego Warszawskiego

СОЧИНЕНІЕ

L. inv. 1097

П. Чебышева,

адъюнкта ИМПЕРАТОРСКАГО С. ПЕТЕРБУРГСКАГО УНИВЕРСИТЕТА.

GABINET MATEMATYCZNY
Towarzystwa Naukowego Warszawskiego

BIBLIOTEKA
JULIANA BAYERA

А. Крайневъ

САНКТПЕТЕРБУРГЪ.

Въ типографіи Императорской Академіи Наукъ.

1849.

opis nr: 45591

ТЕОРИЯ СРАВНЕНИЯ

1848

ПЕЧАТАТЬ ПОЗВОЛЯЕТСЯ

съ тѣмъ, чтобы по отпечатаніи было доставлено въ Ценсурный Комитетъ
законенное число экземпляровъ. С. Петербургъ 12 Октября 1848 года.

Ценсоръ И. Срезневскій.

КАБИНЕТЪ ИМПЕРАТОРСКОГО
УЧЕБНАГО ЗАВѢДѢНІЯ

ИМПЕРАТОРСКОЕ
УЧЕБНОЕ ЗАВѢДѢНІЕ



5097

Въ типографіи Императорской Академіи Наукъ.

1848.

ПРЕДИСЛОВІЕ.

Не слѣдуя вполне въ изложеніи Теоріи сравненій сочиненіямъ Лежандра: *Théorie des nombres* и Гаусса: *Disquisitiones arithmeticae*, я считаю необходимымъ объяснить причины, заставившія меня сдѣлать отступленія отъ этихъ превосходныхъ сочиненій двухъ великихъ Геометровъ. Для этого я войду въ нѣкоторыя подробности объ этихъ сочиненіяхъ и о современномъ имъ состояніи Теоріи чиселъ.

Ейлеромъ положено начало всѣхъ изысканій, составляющихъ общую часть Теоріи чиселъ. Въ этихъ изысканіяхъ Эйлеру предшествовалъ Ферматъ; онъ первый началъ заниматься изслѣдованіемъ свойствъ чиселъ въ отношеніи ихъ способности удовлетворять неопредѣленнымъ уравненіямъ того или другаго вида, и результатомъ его изысканій было открытіе многихъ общихъ теоремъ Теоріи чиселъ. Но изысканія этого Геометра не имѣли непосредственнаго вліянія на развитіе науки: его предложенія остались безъ доказательствъ и безъ приложений. Въ этомъ состояніи открытія Фермата служили только вызывомъ Геометровъ на изысканія въ Теоріи чиселъ. Но не смотря на весь интересъ этихъ изысканій, до Ейлера на нихъ никто не вызывался. И это понятно: эти изысканія требовали не новыхъ приложений приемовъ уже извѣстныхъ и не новыхъ развитій при-

мовъ, прежде употреблявшихся; эти изысканія требовали созданія новыхъ пріемовъ, открытія новыхъ началъ, однимъ словомъ, основанія новой науки. Это сдѣлано было Ейлеромъ.

Между многими изысканіями Ейлера въ Теоріи чиселъ наиболѣе имѣли вліянія на успѣхъ этой науки изысканія его по слѣдующимъ двумъ предметамъ: 1) о степеняхъ чиселъ въ отношеніи остатковъ, получаемыхъ при дѣленіи ихъ на данное число и 2) о числахъ, представляющихъ сумму двухъ чиселъ, изъ которыхъ одно есть квадратъ, а другое произведеніе квадрата на данное число. Первыя положили основаніе теоріи указателей, сравненій двучленныхъ вообще и въ особенности теоріи квадратичныхъ вычетовъ; вторыя были началомъ теоріи квадратичныхъ формъ.

Основаніе теоріи указателей Эйлеръ положилъ мемуаромъ своимъ: *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia*, напечатаннымъ въ запискахъ нашей Академіи за 1773 годъ. Въ этомъ мемуарѣ онъ раскрылъ свойства указателей и первообразныхъ корней, показалъ высшій предѣлъ числа рѣшеній, допускаемыхъ сравненіями двучленными съ простымъ модулемъ и приложеніе теоріи указателей къ теоріи квадратичныхъ вычетовъ и квадратичныхъ формъ. Для совершенства теоріи указателей оставалось найти способъ опредѣленія первообразныхъ корней, не испытывая различныхъ чиселъ. Всѣ старанія Ейлера въ изысканіи этого были тщетны; онъ говоритъ: «*Via quidem adhuc non patet, tales radices primitivas pro quocvis divisore primo inveniendi, neque etiam demonstratio, qua tales radices primitivas semper dari evici, methodum eas inveniendi declarat.*» (*) Но при всемъ успѣхѣ Теоріи чиселъ, мы

(*) Op. min. col. томъ 1, стр. 523.

III

до сихъ поръ находимъ первообразные корни, испытывая различные числа, и теоремы, изложенныя мною во второмъ прибавленіи, едва ли не первый опытъ находить первообразные корни безъ предварительныхъ испытаній.

Исслѣдованія Ейлера о дѣлителяхъ чиселъ вида $a^n \pm b^n$ положили начало теоріи сравненій двучленныхъ. Эти исслѣдованія мы находимъ во многихъ мемуарахъ Ейлера; изъ нихъ особеннаго вниманія заслуживаетъ мемуаръ: *Theoremata circa divisores numerorum*. Здѣсь онъ показываетъ, что возможность удовлетворить сравненію $x^n - a \equiv 0 \pmod{mn + 1}$, при $mn + 1$ простомъ числѣ, предполагаетъ дѣлимость $a^m - 1$ на это число, и доказываетъ обратное, предполагая m и n простыми между собою. За исключеніемъ лишняго ограниченія m и n простыми между собою, эти теоремы суть основанія современной теоріи сравненій двучленныхъ вообще и въ особенности теоріи квадратичныхъ вычетовъ. Впрочемъ разсматривая у Ейлера доказательство послѣдней теоремы, легко замѣтить распространеніе ея на случай m и n какихъ нибудь. Въ мемуарѣ: *De quibusdam eximіis proprietatibus circa divisores potestatum occurrentibus* онъ особенно доказываетъ это для случая $m = 2$, не дѣлая никакихъ ограниченій относительно n , и показываетъ, что дѣлимость $a^n - 1$ на $2n + 1$ есть необходимое и достаточное условіе того, чтобы a было квадратичнымъ вычетовъ числа $2n + 1$. Кромѣ того Эйлеръ, въ другихъ мемуарахъ, много занимался квадратичными вычетами, и въ *Observationes circa divisionem quadratorum per numeros primos*, разсматривая остатки, получаемые при дѣленіи квадратовъ на простые числа, онъ вывелъ такое заключеніе:

IV

Existente s numero quocunque primo, dividantur tantum quadrata imparia 1, 9, 25, 49, etc. per divisorem $4s$, notenturque residua, quae omnia erunt formae $4q + 1$, quorum quodvis littera α indicetur, reliquorum autem numerorum, formae $4q + 1$, qui inter residua non occurrunt, quilibet littera \mathcal{A} indicetur, quo facto si fuerit

divisor numerus

primus formae

$4ns + \alpha$

$4ns - \alpha$

$4ns + \mathcal{A}$

$4ns - \mathcal{A}$

tum est

$+ s$ residuum et $- s$ residuum

$+ s$ residuum et $- s$ non-residuum

$+ s$ non-residuum et $- s$ non-residuum

$+ s$ non-residuum et $- s$ residuum.

Это открытіе мы находимъ у Ейлера въ 1-мъ томѣ *Opera Analytica*, 1772 года. Не трудно въ немъ узнать законъ взаимности двухъ простыхъ чиселъ, обнаруженный Лежандромъ въ 1785 годѣ и положенный имъ въ основаніе теоріи квадратичныхъ вычетовъ.

Въ теоріи квадратичныхъ формъ Эйлеръ началъ свои изысканія съ суммы двухъ квадратовъ, и въ мемуарѣ: *De numeris, qui sunt aggregata duorum quadratorum* доказалъ, что дѣлители суммы двухъ квадратовъ простыхъ между собою должны представлять подобную сумму, и вывелъ линейную форму этихъ дѣлителей. Такимъ образомъ онъ дошелъ до знаменитой теоремы Фермата о разложеніи простыхъ чиселъ вида $4m + 1$ на два квадрата. Подобнымъ образомъ Эйлеръ нашелъ квадратичныхъ и линейныхъ дѣлителей для квадрата, сложенного съ удвоеннымъ или утроеннымъ квадратомъ, и предложилъ безъ доказательства линейныя формы дѣлителей многихъ квадратич-

ныхъ формъ. Такъ положилъ Эйлеръ основаніе теоріи дѣлителей квадратичныхъ формъ. Геніальныя открытія, сдѣланныя Лагранжемъ въ этой части Теоріи чиселъ, открыли путь Эйлеру къ новымъ изысканіямъ. Слѣдствіемъ ихъ было новое развитіе теоріи квадратичныхъ формъ со многими приложениями ея къ изслѣдованію, что данное число простое или нѣтъ, и какъ можно найти простыя числа чрезвычайно большія.

Эйлеръ не ограничивался въ изысканіяхъ своихъ одними конечными формулами; онъ показалъ также, какимъ образомъ употребленіемъ рядовъ можно дойти до различныхъ предложеній Теоріи чиселъ. Сюда относятся изысканія его *de partitione numerorum* и о суммахъ дѣлителей различныхъ чиселъ.

Имѣя въ виду развитіе общей части Теоріи чиселъ, мы не будемъ останавливаться на изысканіяхъ Эйлера въ Анализѣ Диофанта, результатомъ которыхъ было рѣшеніе уравненій второй степени съ двумя неизвѣстными, изслѣдованіе уравненій вида $ax^2 + by^2 = cz^2$, доказательство невозможности нѣкоторыхъ уравненій съ двумя и тремя неизвѣстными и рѣшеніе многихъ неопредѣленныхъ уравненій весьма сложныхъ, и перейдемъ къ изысканіямъ Лагранжа, которымъ сдѣланы весьма важныя развитія въ общихъ началахъ Теоріи чиселъ. Сюда относятся изысканія его о числѣ рѣшеній, допускаемыхъ сравненіями съ простымъ модулемъ, и изслѣдованія свойствъ квадратичныхъ формъ. Мы видѣли, что Эйлеромъ найденъ высшій предѣлъ числа рѣшеній двучленныхъ сравненій; Лагранжъ доказалъ, что этотъ же предѣлъ будетъ при всякомъ числѣ членовъ. Этимъ открытіемъ Лагранжъ далъ возможность доказать многія предложенія Теоріи чиселъ, которыхъ доказательства прежде представляли непреодолимые затрудненія. Къ числу такихъ предложеній должно отнести существованіе первообразныхъ корней для

всѣхъ простыхъ чиселъ; доказательство, предложенное на это Эйлеромъ, основывается на свойствахъ двучленныхъ сравненій, которое могло быть строго доказано только послѣ открытія Лагранжа. Но изъ всѣхъ трудовъ Лагранжа въ Теоріи чиселъ наиболѣе имѣли вліянія на успѣхъ этой науки его изысканія о квадратичныхъ формахъ. Онъ далъ общія начала для тѣхъ изысканій, которыя сдѣланы были Эйлеромъ для не многихъ простѣйшихъ формъ, и эти начала, развиты Лежандромъ, составили полную теорію дѣлителей квадратичныхъ формъ, одну изъ самыхъ главныхъ въ Теоріи чиселъ и особенно важную по своимъ приложеніямъ къ опредѣленію дѣлителей даннаго числа.

Развитіе теоріи квадратичныхъ формъ, сдѣланное Лежандромъ, было слѣдствіемъ открытіи его въ теоріи квадратичныхъ вычетовъ. Заключение, приведенное нами выше изъ сочиненія Ейлера: *Observationes circa divisionem quadratorum per numeros primos* содержитъ ту теорему, которая нынѣ извѣстна подъ именемъ закона взаимности двухъ простыхъ чиселъ и которой обязана своимъ успѣхомъ теорія квадратичныхъ вычетовъ. Въ запискахъ Парижской Академіи наукъ за 1785 годъ Лежандръ доказалъ ее на основаніи признаковъ возможности уравненія $ax^2 + by^2 = cz^2$, имъ же открытыхъ, и показалъ приложенія ея къ изслѣдованію сравненій второй степени и опредѣленію дѣлителей квадратичныхъ формъ.

Въ такомъ состояніи находились различныя части Теоріи чиселъ, когда Лежандръ написалъ сочиненіе свое: *Essai sur la Théorie des nombres*, изданное послѣ со многими прибавленіями, но безъ существенныхъ измѣненій въ системѣ изложенія главныхъ частей, подъ названіемъ *Théorie des nombres*. При всемъ развитіи отдѣльныхъ частей Теоріи чиселъ, систематическое изложеніе этой науки представляло непреодолимыя трудности.

Мы видѣли, что законъ взаимности двухъ простыхъ чиселъ, служащій основаніемъ теоріи квадратичныхъ вычетовъ и вслѣдствіе того необходимый для теоріи квадратичныхъ формъ, выведенъ былъ Лежандромъ изъ свойствъ уравненій второй степени. Поэтому теорія квадратичныхъ вычетовъ и формъ могла быть изложена только послѣ предварительнаго изложенія теоріи неопредѣленныхъ уравненій второй степени, теоріи по предмету своему гораздо высшей и съ своей стороны представляющей приложеніе теоріи квадратичныхъ вычетовъ. Вслѣдствіе этого въ сочиненіи своемъ Лежандръ, послѣ предварительнаго изложенія различныхъ предложеній относительно чиселъ, начинаетъ съ рѣшенія неопредѣленныхъ уравненій, и только по изложеніи полной теоріи уравненій второй степени онъ приступаетъ къ *общимъ свойствамъ чиселъ*, гдѣ находимъ у него главныя предложенія Теоріи сравненій и полную теорію квадратичныхъ вычетовъ и квадратичныхъ формъ. Такой порядокъ въ изложеніи главныхъ частей Теоріи чиселъ, лишившій ее системы, оставался необходимымъ только до тѣхъ поръ, пока Гауссъ не показалъ, какимъ образомъ законъ взаимности двухъ простыхъ чиселъ можетъ быть выведенъ непосредственно изъ разсматриванія сравненій. Такъ открылась возможность, не нарушая естественнаго порядка въ главныхъ частяхъ Теоріи чиселъ, изложить сравненія второй степени вмѣстѣ съ другими сравненіями прежде уравненій второй степени, и потому на основаніи результатовъ Теоріи сравненій упростить изслѣдованіе уравненій высшихъ степеней.

Обращаемся теперь къ сочиненію Гаусса. Мы видѣли, какія развитія сдѣланы были въ различныхъ частяхъ Теоріи чиселъ трудами Ейлера, Лагранжа и Лежандра. Но Гауссъ въ сочиненіи своемъ: *Disquisitiones arithmeticae* не пользовался изысканіями

ми этих Геометровъ. Онъ независимо отъ нихъ развилъ главныя части Теоріи чиселъ, обогативъ ее новыми приемами, многими открытіями и весьма важными приложениями къ рѣшенію двучленныхъ уравненій. Но при всемъ достоинствѣ сочиненія Гаусса мы не можемъ не признать, что большая часть его выводовъ лишена той простоты, которою отличаются приемы Ейлера, Лагранжа и Лежандра. Въ этомъ отношеніи его изложеніе отдѣльныхъ частей Теоріи чиселъ, за исключеніемъ нѣкоторыхъ, нельзя предпочесть изложенію Лежандра.

Изъ этого видно, что ни сочиненіе Лежандра, ни сочиненіе Гаусса не представляютъ Теоріи чиселъ въ томъ совершенномъ видѣ, въ которомъ она можетъ быть изложена послѣ развитіи, сдѣланныхъ въ ней трудами этихъ Геометровъ, а тѣмъ болѣе послѣ изысканій Геометровъ позднѣйшихъ. Поэтому въ изложеніи Теоріи сравненій я долженъ былъ руководствоваться не однимъ Лежандромъ и не однимъ Гауссомъ, но вмѣстѣ и Лежандромъ и Гауссомъ и многими другими, занимавшимися этою частью Теоріи чиселъ. Но чтобы привести въ систему изысканія Геометровъ, употреблявшихъ приемы весьма разнообразныя, я долженъ былъ измѣнить большую часть ихъ выводовъ. Кромѣ того для полноты системы я нашелъ необходимымъ развить нѣкоторыя статьи. Такъ въ теоріи сравненій 1-й степени я рассматриваю отдѣльно три случая, когда это сравненіе имѣетъ одно рѣшеніе, нѣсколько и не имѣетъ ни одного. Излагая свойства сравненій высшихъ степеней, предлагаю относительно ихъ нѣсколько общихъ теоремъ, кромѣ теоремы Лагранжа. Въ теоріи квадратичныхъ формъ показываю средство узнавать, когда двѣ квадратичныя формы дѣлителей приводятся къ однимъ линейнымъ формамъ. Кромѣ того въ сочиненіи моемъ находится три прибавленія. Въ первомъ я излагаю распростра-

IX

пеніе знакоположенія Лежандра, сдѣланное Якоби, и показываю приложение этого къ изслѣдованію квадратичныхъ вычетовъ; во второмъ я доказываю теоремы, опредѣляющія первообразный корень нѣкоторыхъ чиселъ по ихъ виду; въ третьемъ я предлагаю результаты своихъ изысканій относительно свойствъ функціи, опредѣляющей сколько простыхъ чиселъ не превосходятъ данной величины.



ОГЛАВЛЕНИЕ.

ПРЕДВАРИТЕЛЬНЫЯ ПОНЯТІЯ.

§§.	Стран.
1. Предметъ Теоріи чиселъ и Теоріи сравненій.....	1
2. О числахъ абсолютно простыхъ.....	2
3. О числахъ относительно простыхъ.....	3
4. Свойства чиселъ относительно простыхъ.....	—
5. О разложеніи чиселъ на простые множители.....	5
6. Теоремы на этомъ основанныя.....	7
7. О числахъ, составляющихъ арифметическую прогрессию.....	12

ГЛАВА I.

О сравненіи вообще.

8. Понятіе о сравненіи.....	18
9. О свойствахъ сравненія чиселъ между собою.....	19
10. О рѣшеніи сравненій.....	23
11. О наименьшихъ вычетахъ.....	24
12. О числѣ рѣшеній сравненія.....	27

ГЛАВА II.

О сравненіи первой степени.

13. Рѣшеніе этихъ сравненій при модуль простомъ съ коэффициентомъ неизвѣстнаго.....	30
14. Теоремы Фермата и Ейлера.....	31
15. Приложение этихъ теоремъ къ рѣшенію сравненій 1-й степени.....	35
16. О сравненіяхъ, въ которыхъ модуль и коэффициентъ неизвѣстнаго имѣютъ общаго дѣлителя.....	37

II

ГЛАВА III.

О сравненіяхъ высшихъ степеней вообще.

§§	страни.
17. Освобожденіе отъ коэффициента высшей степени неизвѣстнаго.....	40
18. Высшей предѣлъ числа рѣшеній.....	42
19. Приложеніе этого къ доказательству теоремы Вильсона и другихъ свойствъ чиселъ.....	45
20. Приведеніе сравненій къ виду, въ которомъ степень его меньше модуля.....	49
21. Признакъ, по которому узнаемъ, что сравненіе имѣеть столько рѣшеній, сколько единицъ въ показателѣ его.....	50

ГЛАВА IV.

О сравненіяхъ второй степени.

22. Приведеніе полныхъ сравненій второй степени къ сравненію вида $z^2 \equiv q \pmod{p}$	54
23. О числѣ рѣшеній сравненія $z^2 \equiv q \pmod{p}$	58
24. О символѣ $\left(\frac{q}{p}\right)$	59
25. Свойства этого символа.....	61
26. Выраженія его опредѣляющія; слѣдствія ихъ: 1) значеніе $\left(\frac{2}{p}\right)$, 2) законъ взаимности двухъ простыхъ чиселъ.....	66
27. Способъ находить значеніе $\left(\frac{q}{p}\right)$	78
28. Рѣшеніе уравненій: $\left(\frac{x}{p}\right) = 1$, $\left(\frac{x}{p}\right) = -1$	81
29. Рѣшенія сравненія $z^2 \equiv q \pmod{p}$, при p простомъ вида $4n + 3$..	85
30. О сравненіи $z^2 \equiv q \pmod{p}$ при p составномъ	86

ГЛАВА V.

О сравненіяхъ двучленныхъ.

31. О сравненіи $x^m - A \equiv 0 \pmod{p}$, при p простомъ.....	91
32. О сравненіи $x^m - A \equiv 0 \pmod{p}$ при p простомъ.....	96
33. О сравненіи $x^m - A \equiv 0 \pmod{p}$ при p составномъ	102

III

ГЛАВА VI.

О сравненіяхъ вида $a^x \equiv A \pmod{p}$.

§§.	Стран.
34. О сравненіи $a^x \equiv A \pmod{p}$ вообще и въ особенности о сравненіи $a^x \equiv 1 \pmod{p}$	106
35. О рѣшеніяхъ сравненія $a^x \equiv A \pmod{p}$	110
36. Объ указателяхъ	112
37. О рѣшеніи двучленныхъ сравненій помощью таблицъ указателей..	116
38. Теоремы для опредѣленія первообразныхъ корней	122
39. Опредѣленіе первообразныхъ корней.....	124
40. Другой способъ опредѣленія первообразныхъ корней.....	125
41. О числѣ первообразныхъ корней.....	130

ГЛАВА VII.

О сравненіяхъ второй степени съ двумя неизвѣстными.

42. О сравненіи $x^2 + Ay^2 + B \equiv 0 \pmod{p}$	134
43. О дѣлителяхъ $x^2 \pm Ay^2$	135
44. Опредѣленіе дѣлителей $x^2 \pm Ay^2$ при A простомъ.....	143
45. О свойствахъ квадратичныхъ формъ.....	152
46. О выраженіи ими дѣлителей $x^2 \pm ay^2$	157
47. Опредѣленіе линейныхъ дѣлителей помощью квадратичныхъ формъ.	164

ГЛАВА VIII.

Приложеніе Теоріи сравненій къ разложенію чиселъ на простые множители.

48. Разложеніе чиселъ на простые множители приводится къ опредѣленію дѣлителей.....	177
49. Опредѣленіе дѣлителей чиселъ вида $a^m \pm 1$	178
50. Опредѣленіе дѣлителей чиселъ на основаніи теоріи дѣлителей $x^2 \pm ay^2$	183

ПРИБАВЛЕНІЯ.

I. О квадратичныхъ вычетахъ.....	193
II. Объ опредѣленіи первообразныхъ корней	203
III. Объ опредѣленіи числа простыхъ чиселъ, не превосходящихъ данной величины	209
Таблицы: 1) Простыхъ чиселъ до 6000.....	231
2) Указателей и первообразныхъ корней для простыхъ модулей, не превосходящихъ 200	235
3) Линейныхъ дѣлителей $x^2 + ay^2$ отъ $a = 1$ до $a = 101$	265
4) Линейныхъ дѣлителей $x^2 - ay^2$ отъ $a = 1$ до $a = 101$	273



[The page contains several paragraphs of text that are extremely faint and illegible due to fading and bleed-through from the reverse side. The text appears to be organized into sections, possibly numbered or lettered, but the specific content cannot be discerned.]

ПРЕДВАРИТЕЛЬНЫЯ ПОНЯТІЯ.

=

§ 1. Теорія чиселъ, иначе называемая Трансцендентною Арифметикою, есть наука о рѣшеніи неопредѣленныхъ уравненій въ числахъ цѣлыхъ. Заимствуя понятія о числахъ изъ Арифметики и объ уравненіяхъ изъ Алгебры и Трансцендентнаго Анализа, она въ тоже время существенно отлична отъ этихъ наукъ. Она отличается отъ Арифметики тѣмъ, что разсматриваетъ числа только въ отношеніи ихъ способности удовлетворять неопредѣленнымъ уравненіямъ того или другаго вида, и слѣд. остается независимою отъ системы нумераціи, на которой основываются дѣйствія Арифметики. Она отличается отъ Алгебры и другихъ частей опредѣленнаго анализа тѣмъ, что, разсматривая уравненія, она ограничивается только цѣлыми значеніями неизвѣстныхъ.

Разсматривая такимъ образомъ и числа и уравненія съ особенной точки зрѣнія, Теорія чиселъ доходитъ до результатовъ совершенно новыхъ и весьма важныхъ для Арифметики и Теоріи опредѣленныхъ уравненій. Первой она облегчаетъ выкладки, по огромности своей невыполнимыя безъ ея помощи; второй она открываетъ путь къ рѣшенію вопросовъ, безъ помощи ея не разрѣшимыхъ.

Всякое уравненіе, заключающее нѣсколько переменныхъ, подлежитъ изслѣдованію Теоріи чиселъ. Но не все они одинаково доступны изслѣдованію и не все они имѣютъ одинаковую важность по приложениямъ своимъ. Теорія чиселъ до сихъ поръ ограничивается только разсмотрѣніемъ уравненій наиболѣе простыхъ и въ тоже время имѣющихъ наиболѣе важныя приложения. Изъ этихъ уравненій особеннаго вниманія заслуживаютъ тѣ, которыя заключаютъ одно изъ неизвѣстныхъ въ первой степени; они замѣчательны какъ по свойствамъ своимъ, такъ и по приложениямъ къ упрощенію дѣйствій Ариметики и рѣшенію вопросовъ, касающихся опредѣленнаго анализа. Эти то уравненія составляютъ предметъ изслѣдованія Теоріи сравненій.

§ 2. Прежде чѣмъ приступимъ къ изслѣдованію этихъ уравненій, мы остановимся на свойствахъ чиселъ, извѣстныхъ намъ частію изъ Ариметики и изложимъ ихъ съ надлежащею подробностію.

Все числа раздѣляются на два рода: простые и составныя. Простымъ называется такое число, которое можетъ дѣлиться только на 1 и самого себя. Составнымъ называется такое число, которое можетъ дѣлиться на другое число, большее 1. Такъ 2, 3, 5, 7, 11 и проч. суть числа простые, а 4, 6, 8, 9, 10 и проч. суть числа составныя.

Не трудно убѣдиться въ томъ, что простыхъ чиселъ безконечное множество. Въ самомъ дѣлѣ, допустивши противное и называя черезъ N наибольшее изъ простыхъ чиселъ, мы должны допустить, что все числа большія N суть составныя и слѣд. происходятъ отъ перемноженія 2, 3, 5, 7, 11, . . . N , взятыхъ въ нѣкоторыхъ степеняхъ. Но несправедливость этого обнаруживается числомъ $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \dots \cdot (N-1) \cdot N + 1$, которое, очевидно, не дѣлится на числа 2, 3, 5, 7, 11 . . . N и слѣд. перемноженіемъ ихъ степеней не можетъ быть составлено. И такъ нельзя допустить, чтобы простыхъ чиселъ было не безконечное множество.

Для опредѣленія всехъ простыхъ чиселъ, меньшихъ данна-

го предѣла N , способъ самый простой состоитъ въ томъ, чтобы въ рядѣ

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, ..., $N - 1$, N
выкидывать послѣдовательно числа кратныя 2, 3, 5, 7,
и т. д. А это, очевидно, можетъ быть выполнено зачеркиваніемъ въ рядѣ

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, $N - 1$, N
чиселъ чрезъ 1, считая отъ 2, черезъ 2 считая отъ 3, ^{черезъ 3 считая отъ 4} чрезъ 4 считая отъ 5, и вообще черезъ $n - 1$ чиселъ считая отъ числа n . Такимъ образомъ въ этомъ рядѣ исключатся все числа составныя и останутся однѣ лишь простыя числа.

§ 3. Два или нѣсколько чиселъ называются относительно простыми, если они не имѣютъ общаго множителя. Такъ числа 10 и 21 суть относительно простыя. Изъ сказаннаго нами о числахъ относительно простыхъ слѣдуетъ, какъ частный случай, что если A , будучи само по себѣ простымъ числомъ, не дѣлится B , то A и B , суть числа относительно другъ друга простыя. Въ самомъ дѣлѣ, въ этомъ случаѣ числа A и B не могутъ имѣть общимъ дѣлителемъ 1-е) ни числа отличнаго отъ A ; ибо A будучи простымъ числомъ не можетъ дѣлиться на другое число, 2-е) ни самого A ; ибо B по положенію на A не дѣлится. Замѣчая, что если B меньше A , то B на A дѣлится не можетъ, мы по предыдущему заключаемъ, что при B меньшемъ A и A простымъ числа B и A будутъ относительно другъ друга простыя. Это свойство чиселъ можетъ быть выражено такъ: «всякое число, меньшее даннаго простаго числа, есть относительно его простое число.» Такъ 2, 3, 4, 5, 6, 7, 8, 9, 10, суть простыя относительно 11.

Отсюда не трудно вывести такое заключеніе:

Два числа не равныя между собою и само по себѣ простыя суть относительно другъ друга простыя.

§ 4. Мы теперь займемся изложеніемъ свойствъ чиселъ относительно простыхъ.

*

1. ТЕОРЕМА.

Если A и B суть числа простые относительно S ; то и произведение их AB есть число простое относительно S .

Доказательство. Для доказательства этой теоремы ищем общего наибольшего дѣлителя чиселъ A и S . Для этого, какъ извѣстно изъ Арифметики, должны A дѣлить на S , полученнымъ при этомъ остаткомъ должны дѣлить S , новымъ остаткомъ дѣлить первый остатокъ и т. д. Последнйй остатокъ будетъ 1; ибо A и S , какъ числа относительно простые, общего дѣлителя имѣть не могутъ. Если же мы изобразимъ черезъ q, q_1, q_2, \dots, q_n частныя, получаемыя при этихъ дѣленяхъ, а черезъ $r, r_1, r_2, \dots, r_{n-2}, r_{n-1}, r_n$ остатки; то приравнивая дѣлимое произведенію дѣлителя на частное, сложенному съ остаткомъ и замѣчая, что послѣднйй остатокъ r_n равенъ 1, получаемъ такія уравненія.

$$A = Sq + r, S = rq_1 + r_1, r = r_1 q_2 + r_2 \dots \dots \dots r_{n-2} = r_{n-1} q_n + 1,$$
 которыя по умноженіи на B дадутъ

$$(1) \dots AB = BSq + Br, BS = Brq_1 + Br_1, Br = Br_1 q_2 + Br_2, \dots \dots \dots Br_{n-2} = Br_{n-1} q_n + B.$$

Первое изъ этихъ уравненій показываетъ, что общій дѣлитель AB и S будетъ дѣлить Br , второе, что этотъ дѣлитель будетъ дѣлить Br_1 , третье, что онъ будетъ дѣлить Br_2 , и т. д., наконецъ послѣднее, что общій дѣлитель AB и S будетъ дѣлить B . Но B и S , по положенію, не имѣютъ общаго дѣлителя; слѣд. не имѣютъ его AB и S , что и слѣдовало доказать.

Распространяя эту теорему на нѣсколько простыхъ чиселъ относительно S_0, S_1, S_2, \dots , мы убѣждаемся, что числа $ABCD \dots$ и $S_0 S_1 S_2 \dots$ суть относительно другъ друга простые, если A, B, C, D, \dots всё суть числа простые относительно каждаго изъ чиселъ S_0, S_1, S_2, \dots

2. Т Е О Р Е М А.

Если S , будучи простымъ числомъ относительно A , дѣлитъ произведеніе AB ; то оно дѣлитъ и B .

Доказательство. Для доказательства этой теоремы мы выводимъ уравненія (1) и изъ этихъ уравненій замѣчаемъ, что дѣлимость AB на S предполагаетъ дѣлимость на S чиселъ $B\gamma$, $B\gamma_1$, $B\gamma_2, \dots$ и наконецъ дѣлимость B , что и слѣдовало доказать.

3. Т Е О Р Е М А.

Если изъ двухъ чиселъ A и B , простыхъ между собою, каждое дѣлитъ S ; то и произведеніе ихъ AB дѣлитъ S .

Доказательство. Называя черезъ L частное отъ дѣленія S на A , мы для опредѣленія величины S будемъ имѣть

$$S = AL;$$

откуда слѣдуетъ дѣлимость AL на B ; пбо по положенію S дѣлится на B . Но по предыдущей теоремѣ дѣлимость AL на B , гдѣ B число простое съ A , предполагаетъ дѣлимость L на B . Называя же черезъ M число, получаемое при этомъ дѣленіи, мы будемъ имѣть

$$L = BM;$$

вслѣдствіе чего предыдущее уравненіе дастъ

$$S = ABM;$$

откуда ясно видна дѣлимость S на AB , что и слѣдовало доказать.

Распространяя эту теорему на нѣсколько чиселъ, мы заключаемъ, что S дѣлится на $ABCD \dots$, если оно дѣлится на каждое изъ чиселъ A, B, C, D, \dots и числа A, B, C, D, \dots простыя между собою.

§ 5. Мы приступимъ теперь къ разсмотрѣнію свойствъ чиселъ, обнаруживающихся при ихъ разложеніи на простые множители.

Извѣстно изъ Арифметики, что всякое число можетъ быть разложено на произведеніе простыхъ чиселъ. Означая черезъ $\alpha, \beta, \gamma, \dots$ различныя простые числа, входящія въ составъ N и черезъ m, n, p, \dots степени ихъ, мы будемъ имѣть

$$N = \alpha^m \beta^n \gamma^p \dots$$

Изъ этого уравненія, на основаніи 1-й теоремы мы заключаемъ, что N есть простое число относительно всѣхъ чиселъ простыхъ само по себѣ и отличныхъ отъ $\alpha, \beta, \gamma, \dots$. Въ самомъ дѣлѣ, по § 3 всякое простое число, отличное отъ $\alpha, \beta, \gamma, \dots$ будетъ также простымъ относительно $\alpha, \beta, \gamma, \dots$ и слѣд. относительно его будетъ простымъ числомъ произведеніе $\alpha^m \beta^n \gamma^p \dots$. Отсюда мы можемъ заключить вообще, что всякое число не можетъ дѣлиться на простое число, въ составъ его не входящее. Что же касается до дѣлимости N , которое мы предположили равнымъ $\alpha^m \beta^n \gamma^p \dots$, на степени чиселъ $\alpha, \beta, \gamma, \dots$ въ составъ его входящихъ, то также не трудно убѣдиться, что оно не можетъ дѣлиться на $\alpha^{m'}$ при $m' > m$, на $\beta^{n'}$ при $n' > n$ и т. д. Въ самомъ дѣлѣ, такъ какъ $N = \alpha^m \beta^n \gamma^p \dots$; то частное отъ дѣленія N на $\alpha^{m'}$ представится дробью

$$\frac{\alpha^m \beta^n \gamma^p \dots}{\alpha^{m'}}, \text{ или } \frac{\beta^n \gamma^p \dots}{\alpha^{m'-m}},$$

что при $m' > m$ не можетъ быть числомъ цѣлымъ; ибо α , будучи числомъ простымъ отличнымъ отъ β, γ, \dots , по замѣченному нами, дѣлится $\beta^n \gamma^p \dots$ не можетъ. Итакъ N можетъ дѣлиться только на степени $\alpha, \beta, \gamma, \dots$, не превосходящія m, n, p , и слѣд. число N можетъ дѣлиться только на числа, въ составъ которыхъ входятъ однѣ простые числа $\alpha, \beta, \gamma, \dots$ и въ степеняхъ не превосходящихъ m, n, p, \dots . Такимъ образомъ доходимъ мы до слѣдующей теоремы:

4. ТЕОРЕМА.

Число N можетъ дѣлиться на число P только въ томъ случаѣ, когда всѣ простые множители числа P входятъ въ составъ N и въ N степени ихъ не ниже чѣмъ въ P

На основаніи этой теоремы не трудно доказать слѣдующую:

5. Т Е О Р Е М А.

Для числа N возможно одно только разложениіе на простые множители.

Доказательство. Въ самомъ дѣлѣ, если мы допустимъ для числа N два разложениія на простые множители, такъ:

$$N = \alpha^m \beta^n \gamma^p \dots, \quad N = \alpha_1^{m'} \beta_1^{n'} \gamma_1^{p'} \dots;$$

то, дѣля эти уравненія одно на другое, найдемъ

$$\frac{\alpha^m \beta^n \gamma^p \dots}{\alpha_1^{m'} \beta_1^{n'} \gamma_1^{p'} \dots} = 1, \quad \frac{\alpha_1^{m'} \beta_1^{n'} \gamma_1^{p'} \dots}{\alpha^m \beta^n \gamma^p \dots} = 1.$$

Первое изъ этихъ уравненій по предыдущей теоремѣ предполагаетъ, что всѣ числа $\alpha_1, \beta_1, \gamma_1, \dots$ находятся въ рядѣ чиселъ $\alpha, \beta, \gamma, \dots$, а второе обратно, что всѣ числа $\alpha, \beta, \gamma, \dots$ находятся въ рядѣ $\alpha_1, \beta_1, \gamma_1, \dots$; откуда слѣдуетъ, что числа $\alpha, \beta, \gamma, \dots$ и $\alpha_1, \beta_1, \gamma_1, \dots$ суть однѣ и тѣ-же. Принимая же $\alpha = \alpha_1, \beta = \beta_1, \gamma = \gamma_1, \dots$, мы по предыдущей теоремѣ изъ уравненія

$$\frac{\alpha^m \beta^n \gamma^p \dots}{\alpha^{m'} \beta_1^{n'} \gamma_1^{p'} \dots} = 1$$

имѣемъ

$$m' \text{ не } > m, \quad n' \text{ не } > n, \quad p' \text{ не } > p, \dots;$$

Подобнымъ образомъ уравненіе

$$\frac{\alpha_1^{m'} \beta_1^{n'} \gamma_1^{p'} \dots}{\alpha^m \beta^n \gamma^p \dots} = 1$$

предполагаетъ $m \text{ не } > m', \quad n \text{ не } > n', \quad p \text{ не } > p', \dots$

Изъ соединенія же этихъ неравенствъ съ предыдущими находимъ

$$m = m', \quad n = n', \quad p = p', \dots$$

И такъ разсматриваемыя нами два разложениія числа N не разнятся между собою ни простыми числами ни степенями ихъ; откуда и слѣдуетъ предложенная нами теорема.

§ 6. Разложениемъ чиселъ на простые множители легко доказать слѣдующія теоремы:

6. ТЕОРЕМА.

Если N дѣлитъ квадратъ числа M и не можетъ дѣлиться на квадратъ какого-либо числа; то N дѣлитъ также M .

Доказательство. Разложениемъ числа N на простые множители мы находимъ

$$N = \alpha^m \beta^n \gamma^p \dots$$

Но такъ какъ N по положенію не можетъ дѣлиться на квадратъ какого либо числа, то здѣсь показатели m, n, p, \dots не могутъ превосходить 1; пбо въ противномъ случаѣ при m не < 2 число N , очевидно, дѣлилось бы на α^2 , при n не < 2 оно дѣлилось бы на β^2 , и т. д. Слѣд. въ предыдущемъ уравненіи всѣ показатели m, n, p, \dots равны 1; а потому

$$N = \alpha \beta \gamma \dots$$

гдѣ $\alpha, \beta, \gamma, \dots$ простые числа, различныя между собою. Убѣдясь въ этомъ, разлагаемъ M на простые множители; это даетъ намъ

$$M = \alpha_1^{m'} \beta_1^{n'} \gamma_1^{p'} \dots \quad (2)$$

гдѣ $\alpha_1, \beta_1, \gamma_1, \dots$ различныя простые числа. Изъ этого уравненія мы выводимъ

$$M^2 = \alpha_1^{2m'} \beta_1^{2n'} \gamma_1^{2p'} \dots$$

и замѣчая, что по положенію, M^2 дѣлится на N , гдѣ $N = \alpha \beta \gamma \dots$, мы по теоремѣ 4-й заключаемъ, что въ рядѣ $\alpha_1, \beta_1, \gamma_1, \dots$ заключаются всѣ числа $\alpha, \beta, \gamma, \dots$ и что степени ихъ въ составѣ M^2 не суть 0. Слѣд. всѣ числа $\alpha, \beta, \gamma, \dots$ входятъ въ составъ M и слѣд. M дѣлится на $\alpha, \beta, \gamma, \dots$ и вмѣстѣ съ тѣмъ (см. теорему 3) дѣлится и на произведеніе ихъ, равное N , что и слѣдовало доказать.

Такъ замѣчая, что 15 не можетъ дѣлиться на квадратъ какого либо числа и что оно дѣлится 45^2 , равное 2025, мы заключаемъ, что 15 будетъ также дѣлится 45.

7. ТЕОРЕМА.

Корень h -й степени числа N только въ томъ случаѣ есть число цѣлое, когда степени простыхъ множителей его суть числа кратныя h .

Доказательство. Разложениемъ числа N и корня его h -й степени на простые множители находимъ

$$N = \alpha^m \beta^n \gamma^p \dots, \sqrt[h]{N} = \alpha_1^{m'} \beta_1^{n'} \gamma_1^{p'} \dots$$

Первое изъ этихъ уравненій и второе по возведеніи его въ степень h даютъ слѣдующія два разложенія числа N на простые множители:

$$N = \alpha^m \beta^n \gamma^p \dots, N = \alpha_1^{hm'} \beta_1^{hn'} \gamma_1^{hp'} \dots$$

Но по теоремѣ 5-й эти разложенія должны быть тождественны. А потому числа $\alpha, \beta, \gamma, \dots$ должны быть равны числамъ $\alpha_1, \beta_1, \gamma_1, \dots$ и числа m, n, p, \dots должны имѣть равныхъ въ рядѣ hm', hn', hp', \dots ; последнее ясно обнаруживаетъ, что m, n, p, \dots суть числа кратныя h , въ чемъ и заключается предложенная теорема.

Такъ находя число 576 равнымъ $2^6 3^2$ и замѣчая, что здѣсь показатели 6 и 2 имѣютъ общимъ дѣлителемъ только 2, мы заключаемъ, что изъ всѣхъ корней числа 576 только корень квадратный имѣетъ значеніе цѣлое.

8. ТЕОРЕМА.

Если N разложениемъ на простые множители приводится къ $\alpha^m \beta^n \gamma^p \dots$; то сумма различныхъ дѣлителей N есть $\frac{\alpha^{m+1} - 1}{\alpha - 1} \cdot \frac{\beta^{n+1} - 1}{\beta - 1} \cdot \frac{\gamma^{p+1} - 1}{\gamma - 1} \dots$, а число ихъ есть $(m + 1)(n + 1)(p + 1) \dots$

Доказательство. По 4-й теоремѣ число N , какъ равное $\alpha^m \beta^n \gamma^p \dots$, можетъ дѣлиться только на числа равныя $\alpha^{m'} \beta^{n'} \gamma^{p'} \dots$, гдѣ $m' \leq m, n' \leq n, p' \leq p, \dots$. Поэтому всѣ

дѣлители числа N опредѣляются значеніями $\alpha^{m'} \beta^{n'} \gamma^{p'} \dots\dots$,
соотвѣтствующими

$$\begin{aligned} m' &= 0, 1, 2, \dots\dots m-1, m, \\ n' &= 0, 1, 2, \dots\dots n-1, n, \\ p' &= 0, 1, 2, \dots\dots p-1, p, \end{aligned}$$

и слѣд. найдутся въ рядѣ членовъ, получаемыхъ перемноженіемъ
выраженій

$$\begin{aligned} &\alpha^0 + \alpha + \alpha^2 + \dots\dots + \alpha^{m-1} + \alpha^m, \\ &\beta^0 + \beta + \beta^2 + \dots\dots + \beta^{n-1} + \beta^n, \\ &\gamma^0 + \gamma + \gamma^2 + \dots\dots + \gamma^{p-1} + \gamma^p, \\ &\dots\dots\dots \\ &\dots\dots\dots \end{aligned}$$

А поэтому сумма дѣлителей числа N опредѣлится произведеніемъ
 $(\alpha^0 + \alpha + \alpha^2 + \dots + \alpha^{m-1} + \alpha^m) (\beta^0 + \beta + \beta^2 + \dots + \beta^{n-1} + \beta^n)$
 $(\gamma^0 + \gamma + \gamma^2 + \dots + \gamma^{p-1} + \gamma^p) \dots\dots\dots$,
которое равно

$$\frac{\alpha^{m+1} - 1}{\alpha - 1} \cdot \frac{\beta^{n+1} - 1}{\beta - 1} \cdot \frac{\gamma^{p+1} - 1}{\gamma - 1} \dots\dots;$$

пбо

$$\begin{aligned} \alpha^0 + \alpha + \alpha^2 + \dots\dots + \alpha^{m-1} + \alpha^m &= \frac{\alpha^{m+1} - 1}{\alpha - 1}, \\ \beta^0 + \beta + \beta^2 + \dots\dots + \beta^{n-1} + \beta^n &= \frac{\beta^{n+1} - 1}{\beta - 1}, \\ \gamma^0 + \gamma + \gamma^2 + \dots\dots + \gamma^{p-1} + \gamma^p &= \frac{\gamma^{p+1} - 1}{\gamma - 1}, \\ &\dots\dots\dots \\ &\dots\dots\dots \end{aligned}$$

Число же дѣлителей N опредѣлится числомъ членовъ про-
изведенія

$$(\alpha^0 + \alpha + \alpha^2 + \dots + \alpha^{m-1} + \alpha^m) (\beta^0 + \beta + \beta^2 + \dots + \beta^{n-1} + \beta^n)$$
$$(\gamma^0 + \gamma + \gamma^2 + \dots + \gamma^{p-1} + \gamma^p) \dots\dots\dots,$$

или, что одно и тоже, значеніемъ этого выраженія при $\alpha = 1$,
 $\beta = 1$, $\gamma = 1, \dots\dots$ Слѣд. число дѣлителей N есть

$$(m + 1) (n + 1) (p + 1) \dots\dots$$

Такъ для числа 72, равнаго $2^3 \cdot 3^2$, сумма дѣлителей опредѣлится выраженіемъ $\frac{2^4 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1}$, что равняется 195, а число дѣлителей 72 будетъ $(3 + 1) \times (2 + 1)$, или 12. Въ справедливости этихъ заключеній мы убѣждаемся, замѣтивъ, что дѣлители 72 суть

1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72,

которыхъ сумма равна 195, а число ихъ 12.

9. ТЕОРЕМА.

Если N разложеніемъ на простые множители приводится къ $\alpha^m \beta^n \gamma^p \dots$, гдѣ по крайней мѣрѣ одно изъ чиселъ m, n, p, \dots есть нечетное; то для числа N возможно $\frac{1}{2} (m + 1) (n + 1) (p + 1) \dots$ различныхъ разложеній на два множителя.

Если же все показатели m, n, p, \dots числа четныя; то для N возможно $\frac{1}{2} (m + 1) (n + 1) (p + 1) \dots + \frac{1}{2}$ такихъ разложеній.

Доказательство. Въ первомъ случаѣ по 7-й теоремѣ нѣтъ числа, котораго бы квадратъ равнялся N , а потому число N не можетъ разлагаться на произведеніе двухъ множителей равныхъ между собою и слѣд. всякое разложеніе числа N на два множителя опредѣлитъ два дѣлителя его. Откуда ясно, что число разложеній N на два множителя равно половинѣ числа его дѣлителей и слѣд. по предыдущей теоремѣ оно равно

$$\frac{1}{2} (m + 1) (n + 1) (p + 1) \dots$$

Во второмъ случаѣ, — въ случаѣ m, n, p, \dots четныхъ, въ числѣ разложеній N на два множителя будетъ между прочимъ такое, въ которомъ оба множителя равны и которымъ слѣдовательно опредѣлится одинъ дѣлитель числа N ; затѣмъ все остальные разложенія, какъ и въ первомъ случаѣ, дадутъ по два дѣлителя. Итакъ, называя черезъ K искомое число раз-

ложений N на два множителя, мы найдемъ $1 + 2(K - 1)$ для числа дѣлителей N . Но по предыдущей теоремѣ число дѣлителей N есть $(m + 1)(n + 1)(p + 1) \dots$. Слѣдовательно

$$1 + 2(K - 1) = (m + 1)(n + 1)(p + 1) \dots;$$

откуда для величины K находимъ

$$K = \frac{1}{2}(m + 1)(n + 1)(p + 1) \dots + \frac{1}{2},$$

что и слѣдовало доказать.

Такъ для числа 72, равнаго $2^3 \cdot 3^2$, число разложений на два множителя должно быть $\frac{1}{2}(3 + 1)(2 + 1)$, или 6. Дѣйствительно находимъ мы, что для 72 возможны только слѣдующія 6 разложений на два множителя

$$1 \cdot 72, 2 \cdot 36, 3 \cdot 24, 4 \cdot 18, 6 \cdot 12, 8 \cdot 9.$$

Для числа же 36, равнаго $2^2 \cdot 3^2$, число различныхъ разложений на два множителя будетъ $\frac{1}{2}(2 + 1) \times (2 + 1) + \frac{1}{2}$, или 5. Дѣйствительно для 36 возможны только слѣдующія разложения на два множителя

$$1 \cdot 36, 2 \cdot 18, 3 \cdot 12, 4 \cdot 9, 6 \cdot 6.$$

§ 7. Прежде чѣмъ пойдемъ далѣе, мы докажемъ относительно дѣлмости чиселъ, составляющихъ арифметическую прогрессию, слѣдующую теорему, которая намъ будетъ нужна теперь и впоследствии.

10. ТЕОРЕМА.

Если разность прогрессіи есть число простое съ p , а число членовъ равно mp ; то въ такой прогрессіи число членовъ дѣлящихся на p есть t .

Доказательство. Пусть будетъ разсматриваемая прогрессія $a, a + d, a + 2d, \dots, a + (mp - 2)d, a + (mp - 1)d$, гдѣ d число простое съ p . Этотъ родъ членовъ разбивается на t слѣдующихъ:

$$\left. \begin{aligned} a, a+d, a+2d, \dots a+(p-1)d, \\ a+pd, a+pd+d, a+pd+2d, \dots a+pd+(p-1)d, \\ \dots \dots \dots \\ a+npd, a+npd+d, a+npd+2d, \dots a+npd+(p-1)d, \\ \dots \dots \dots \\ a+(m-1)pd, a+(m-1)pd+d, a+(m-1)pd+2d, \dots a+(mp-1)d \end{aligned} \right\} (3)$$

и не трудно убѣдиться, что каждый изъ этихъ рядовъ заключаетъ одинъ членъ дѣлящійся на p . Для обнаруженія этого разсмотримъ рядъ

$$a + npd, a + npd + d, a + npd + 2d, \dots a + npd + (p-1)d.$$

Въ немъ не можетъ быть двухъ членовъ, которые бы при дѣленіи на p дали остатки равные; ибо разность такихъ двухъ членовъ дѣлалась бы на p , а въ невозможности этого мы убѣждаемся, замѣтивъ, что разность какихъ-либо двухъ членовъ этого ряда приводится къ произведенію d , числа простаго съ p , на число $< p$, что по 2-й теоремѣ на p дѣлится не можетъ. Но если остатки отъ дѣленія

$$a + npd, a + npd + d, a + npd + 2d, \dots a + npd + (p-1)d$$

на p всѣ различны между собою и слѣд. въ числѣ ихъ не можетъ быть болѣе одного равнаго нулю; то съ другой стороны одинъ изъ нихъ не обходимо будетъ нулемъ; ибо предполагая противное и замѣчая, что кромѣ нуля относительно остатковъ отъ дѣленія чиселъ на p можно сдѣлать только $p-1$ предположеній

$$1, 2, 3, \dots p-1,$$

мы должны бы были допустить, что въ числѣ p остатковъ отъ дѣленія

$$a + npd, a + npd + d, a + npd + 2d, \dots a + npd + (p-1)d$$

есть два по крайней мѣрѣ равные, что по доказанному нами невозможно.

Убѣдясь такимъ образомъ, что въ рядѣ

$$a + npd, a + npd + d, a + npd + 2d, \dots a + npd + (n-1)d$$

и слѣд. въ каждомъ изъ (3) число членовъ дѣлящихся на p

есть 1, мы заключаемъ, что во всѣхъ m рядахъ (3) число членовъ дѣлящихся на p есть m . Но совокупность всѣхъ этихъ рядовъ, какъ видѣли, составляетъ разсматриваемую нами прогрессию

$$a, a + d, a + 2d, \dots, a + (mp - 2)d, a + (mp - 1)d;$$

откуда и слѣдуетъ предложенная нами теорема.

Изъ этой теоремы не трудно вывести слѣдующую:

11. ТЕОРЕМА.

Если a число простое само по себѣ и A простое съ a , то въ рядѣ $1, 2, 3, \dots, aAN - 1, aAN$ число членовъ простыхъ съ A къ числу членовъ простыхъ съ A и a относится какъ a къ $a - 1$.

Доказательство. Въ Арифметикѣ доказано, что общій наибольшій дѣлитель чиселъ X и A есть также общій наибольшій дѣлитель числа A и остатка отъ дѣленія X на A . Отсюда слѣдуетъ, что если X и A неимѣютъ общаго дѣлителя, то и остатокъ отъ дѣленія X на A будетъ число простое съ A и обратно, если остатокъ отъ дѣленія X на A есть число простое съ A , то X также число простое съ A . Но такъ какъ остатокъ отъ дѣленія на A будетъ всегда менѣе A , то при X простомъ съ A остатокъ отъ дѣленія X на A будетъ всегда одно изъ чиселъ меньшихъ съ A и простыхъ съ A . Пусть же

$$a', a'', a''', \dots, a^{(n)}$$

будутъ числа простыя съ A и меньшія A ; нетрудно опредѣлить видъ числа X , для котораго остатокъ отъ дѣленія на A былъ бы равенъ одному изъ чиселъ $a', a'', a''' \dots a^{(n)}$. Такъ, чтобы найти X , которое при дѣленіи на A даетъ остатокъ a' , пусть будетъ m' частное отъ дѣленія X на A ; приравнявая дѣлимое произведенію дѣлителя на частное сложенному съ остаткомъ, мы находимъ для выраженія X слѣдующую формулу:

$$X = a' + m'A.$$

Также находимъ слѣдующія формулы для чиселъ, которыхъ остатки отъ дѣленія на A суть $\alpha'', \alpha''', \dots, \alpha^{(n)}$:

$$X = \alpha' + m'A; X = \alpha'' + m''A, \dots X = \alpha^{(n)} + m^{(n)}A.$$

Итакъ все числа, которыя при дѣленіи на A даютъ остатки равные $\alpha', \alpha'', \alpha''' \dots, \alpha^{(n)}$ и слѣд. по замѣченному нами, суть числа простыя съ A , выразятся такимъ образомъ

$$X = \alpha' + m'A, X = \alpha'' + m''A, X = \alpha''' + m'''A, \dots X = \alpha^{(n)} + m^{(n)}A.$$

Такъ выражаются все числа простыя съ A . На основаніи этихъ формулъ легко доказать предложенную нами теорему.

Съ этою цѣлію мы опредѣляемъ по этимъ формуламъ все числа простыя съ A и меньшія aAN , давая въ нихъ буквамъ $m', m'', m''', \dots, m^{(n)}$ значенія $0, 1, 2, 3$, и т. д. до тѣхъ поръ, пока числа, опредѣляемые этими формулами, не будутъ болѣе aAN .

Такъ находимъ, что все числа простыя съ A и меньшія aAN суть

$$\begin{aligned} \alpha', \alpha' + A, \alpha' + 2A, \dots, \alpha' + (aN - 1)A, \\ \alpha'', \alpha'' + A, \alpha'' + 2A, \dots, \alpha'' + (aN - 1)A, \\ \alpha''', \alpha''' + A, \alpha''' + 2A, \dots, \alpha''' + (aN - 1)A, \\ \dots, \\ \alpha^{(n)}, \alpha^{(n)} + A, \alpha^{(n)} + 2A, \dots, \alpha^{(n)} + (aN - 1)A. \end{aligned}$$

и всехъ ихъ, какъ не трудно замѣтить, счетомъ есть aNn .

Теперь не трудно показать число простыхъ чиселъ съ A и a и въ тоже время меньшихъ aAN . Для этого стоитъ только въ найденныхъ нами числахъ, простыхъ съ A , выкинуть числа кратныя a ; ибо a число само по себѣ простое и слѣд. по § 3 все числа, не дѣлящіяся на него, будутъ простыя съ нимъ. Но по предыдущей теоремѣ въ рядѣ

$$\alpha', \alpha' + A, \alpha' + 2A, \alpha' + 3A, \dots, \alpha' + (aN - 1)A$$

число членовъ дѣлящихся на a есть N ; слѣд. простыхъ съ a здѣсь $aN - N$, или $(a - 1)N$. Тоже замѣчаемъ о прочихъ рядахъ

$$\begin{aligned} \alpha'', \alpha'' + A, \alpha'' + 2A, \dots \alpha'' + (aN - 1)A, \\ \alpha''', \alpha''' + A, \alpha''' + 2A, \dots \alpha''' + (aN - 1)A, \\ \dots \\ \alpha^{(n)}, \alpha^{(n)} + A, \alpha^{(n)} + 2A, \dots \alpha^{(n)} + (aN - 1)A. \end{aligned}$$

Откуда слѣдуетъ, что чиселъ меньшихъ aAN и простыхъ съ A и a будетъ $(a - 1)Nn$. Но это число къ числу всѣхъ чиселъ меньшихъ aAN и простыхъ съ aAN , которое, какъ видно, есть aNn , относится какъ $a - 1$ къ a , что и слѣдовало доказать.

На основаніи теоремъ изложенныхъ нами не трудно будетъ доказать слѣдующую теорему:

12. ТЕОРЕМА.

Если N разложеніемъ на простые множители приводится къ $\alpha^m \beta^n \gamma^p \dots \pi^r$; то число простыхъ чиселъ съ N и меньшихъ N есть $\alpha^m \beta^n \gamma^p \dots \pi^r \cdot \frac{\alpha - 1}{\alpha} \cdot \frac{\beta - 1}{\beta} \cdot \frac{\gamma - 1}{\gamma} \dots \frac{\pi - 1}{\pi}$.

Доказательство. На основаніи предыдущихъ теоремъ не трудно показать сколько чиселъ простыхъ съ $\alpha, \beta, \gamma \dots \pi$ въ рядѣ

$$1, 2, 3, \dots \alpha^m \beta^n \gamma^p \dots \pi^r.$$

Для этого мы пишемъ этотъ рядъ въ видѣ арифметической прогрессіи съ разностию равною 1 такимъ образомъ :

$$1, 1 + 1, 1 + 2 \cdot 1, \dots 1 + (\alpha \cdot \alpha^{m-1} \beta^n \gamma^p \dots \pi^r - 1).$$

На основаніи 10-й теоремы мы заключаемъ, что здѣсь членовъ дѣлящихся на α есть $\alpha^{m-1} \beta^n \gamma^p \dots \pi^r$; затѣмъ остальные, числомъ $\alpha^m \beta^n \gamma^p \dots \pi^r - \alpha^{m-1} \beta^n \gamma^p \dots \pi^r$, или $\alpha^m \beta^n \gamma^p \dots \pi^r \cdot \frac{\alpha - 1}{\alpha}$, будутъ простыя съ α (см. § 3). Итакъ въ рядѣ

$$1, 2, 3, \dots \alpha^m \beta^n \gamma^p \dots \pi^r$$

число членовъ простыхъ съ α есть $\alpha^m \beta^n \gamma^p \dots \pi^r \cdot \frac{\alpha - 1}{\alpha}$.

Отсюда по 11-й теоремѣ мы заключаемъ, что число членовъ простыхъ съ α и β , ип, что одно и тоже, простыхъ съ про-

пзведеиёмъ $\alpha\beta$ есть $\alpha^m \beta^n \gamma^p \dots \pi^r \cdot \frac{\alpha-1}{\alpha} \cdot \frac{\beta-1}{\beta}$; далѣе по той же теоремѣ, зная, что число членовъ въ рядѣ

$$1, 2, 3, \dots \alpha^m \beta^n \gamma^p \dots \pi^r$$

простыхъ съ $\alpha\beta$ есть $\alpha^m \beta^n \gamma^p \dots \pi^r \cdot \frac{\alpha-1}{\alpha} \cdot \frac{\beta-1}{\beta}$, мы находимъ, что здѣсь число членовъ простыхъ съ $\alpha\beta\gamma$ есть

$$\alpha^m \beta^n \gamma^p \dots \pi^r \frac{\alpha-1}{\alpha} \cdot \frac{\beta-1}{\beta} \cdot \frac{\gamma-1}{\gamma}, \text{ п т. д.}$$

Наконецъ найдемъ такимъ образомъ, что число членовъ простыхъ съ $\alpha\beta\gamma \dots \pi$ есть

$$\alpha^m \beta^n \gamma^p \dots \pi^r \frac{\alpha-1}{\alpha} \cdot \frac{\beta-1}{\beta} \cdot \frac{\gamma-1}{\gamma} \dots \frac{\pi-1}{\pi}.$$

Такъ опредѣляется число простыхъ чиселъ съ $\alpha\beta\gamma \dots \pi$ и меньшихъ $\alpha^m \beta^n \gamma^p \dots \pi^r$. Но это все равно, какъ бы мы разсматривали числа простыя съ N , или $\alpha^m \beta^n \gamma^p \dots \pi^r$; ибо все простыя числа относительно $\alpha^m \beta^n \gamma^p \dots \pi^r$ суть простыя относительно $\alpha\beta\gamma \dots \pi$ и обратно. Въ этомъ мы убѣждаемся тѣмъ, что относительно $\alpha^m \beta^n \gamma^p \dots \pi^r$, также какъ относительно $\alpha\beta\gamma \dots \pi$, всякое число будетъ простое, если въ составѣ его нѣтъ $\alpha, \beta, \gamma, \dots, \pi$; въ противномъ же случаѣ оно не будетъ простымъ ни относительно $\alpha^m \beta^n \gamma^p \dots \pi^r$, ни относительно $\alpha\beta\gamma \dots \pi$.

Итакъ $\alpha^m \beta^n \gamma^p \dots \pi^r \cdot \frac{\alpha-1}{\alpha} \cdot \frac{\beta-1}{\beta} \cdot \frac{\gamma-1}{\gamma} \dots \frac{\pi-1}{\pi}$ есть число членовъ въ рядѣ

$$1, 2, 3, \dots \alpha^m \beta^n \gamma^p \dots \pi^r$$

простыхъ съ $\alpha^m \beta^n \gamma^p \dots \pi^r$, что и слѣдовало доказать.

Такъ для опредѣленія сколько чиселъ простыхъ съ 36 и меньшихъ 36, мы разлагаемъ 36 на простые множители. Находя, что 36 равно $2^2 \cdot 3^2$, мы по доказанной нами теоремѣ заключаемъ, что всѣхъ чиселъ простыхъ съ 36 и меньшихъ 36 есть $2^2 \cdot 3^2 \frac{2-1}{2} \cdot \frac{3-1}{3}$, или 12. Дѣйствительно между всѣми числами отъ 1 до 36 мы находимъ 12 чиселъ

1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35
 простыхъ съ 36; всѣ же прочія
 2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18,
 20, 21, 22, 24, 26, 27, 28, 30, 32, 33, 34
 суть составныя.

Этимъ мы окончиваемъ изложеніе свойствъ чиселъ, необходимыхъ намъ въ послѣдствіи и переходимъ къ изслѣдованію сравненій.

ГЛАВА I.

О СРАВНЕНІЯХЪ ВООБЩЕ.

§ 8. Теорія сравненій имѣетъ предметомъ изслѣдованіе неопредѣленныхъ уравненій, въ которыя одна изъ неизвѣстныхъ входитъ въ первой степени. Общій видъ этихъ уравненій есть

$$F(x, y, z, \dots) = Au + B,$$

гдѣ F данная функція, A и B извѣстныя числа. Такъ какъ эти уравненія очень часто употребляются, то для нихъ введено особенное знаменіе. Не трудно замѣтить, что при неопредѣленномъ значеніи числа u уравненіе

$$F(x, y, z, \dots) = Au + B,$$

приводясь къ равенству

$$\frac{F(x, y, z, \dots) - B}{A} = u,$$

есть ни что иное, какъ выраженіе дѣлимости разности $F(x, y, z, \dots) - B$ на A . А потому мы можемъ представить это уравненіе такъ

$$F(x, y, z, \dots) \equiv B \pmod{A},$$

означая вообще знакомъ \equiv , поставленнымъ между двумя числами, дѣлимость разности ихъ на третье число, которое съ словомъ *mod.* поставляемъ въ скобкахъ.

Такъ для означенія, что разность $17 - 5$ дѣлится на 3 будемъ писать

$$17 \equiv 5 \text{ (mod. 3).}$$

Выраженія вида

$$M \equiv N \text{ (mod. } A)$$

извѣстны подъ названіемъ сравненій, числа M и N сравнимыми по модулю A , число A модулемъ сравненія. Сравниваемыя числа M , N могутъ имѣть значенія и положительныя и отрицательныя; во всякомъ случаѣ выраженіе

$$M \equiv N \text{ (mod. } A)$$

будетъ означать дѣлимость алгебраической разности $M - N$ на A . Число же A , модуль сравненія, мы будемъ всегда предполагать числомъ положительнымъ.

Замѣтимъ, что по сказанному нами знакоположенію будетъ всегда

$$M \equiv r \text{ (mod. } A),$$

если r есть остатокъ отъ дѣленія M на A ; ибо называя черезъ q частное при дѣленіи M на A и приравнивая дѣлимое произведенію дѣлителя на частное, сложенному съ остаткомъ, найдемъ

$$M = Aq + r,$$

откуда ясно, что разность M и r дѣлится на A .

Не трудно также убѣдиться въ обратномъ, что если при M и r положительныхъ число r меньше A и сравнимо съ M по модулю A ; то r есть остатокъ отъ дѣленія M на A ; ибо изъ сравненія $M \equiv r \text{ (mod. } A)$ выходитъ $\frac{M-r}{A} = q$; откуда $M = Aq + r$, а это уравненіе при $r < A$ и $r = > 0$ обнаруживаетъ въ r остатокъ отъ дѣленія M на A .

Изъ того, что дѣлимое сравнимо съ остаткомъ, если дѣлитель принять за модуль, какъ частный случай, мы выводимъ, что если M дѣлится на A безъ остатка; то

$$M \equiv 0 \text{ (mod. } A).$$

На основаніи этого мы будемъ говорить часто, что число сравнимо съ 0 по модулю A , вмѣсто того, чтобы говорить, что оно дѣлится на A .

§ 9. Изъ понятія, составленнаго нами о сравненіяхъ, не трудно обнаружить въ нихъ слѣдующія свойства:

*

1) Два числа, сравнимыя съ однимъ и тѣмъ же числомъ по какому либо модулю, сравнимы и между собою по тому же модулю. Въ самомъ дѣлѣ, если $M \equiv N \pmod{A}$, $M' \equiv N \pmod{A}$; то и $M \equiv M' \pmod{A}$; ибо сравненія $M \equiv N \pmod{A}$, предполагаютъ, что A дѣлитъ разности $M - N$, $M' - N$ и слѣд. дѣлитъ разность этихъ разностей. Но эта послѣдняя разность есть $M - M'$ и дѣлимость ея на A выражается сравненіемъ $M \equiv M' \pmod{A}$.

2) Въ сравненіяхъ, подобно уравненіямъ, члены могутъ быть переносимы изъ одной части въ другую. Такъ если $M + M' \equiv N \pmod{A}$; то $M \equiv N - M' \pmod{A}$. Въ самомъ дѣлѣ, сравненіе $M + M' \equiv N \pmod{A}$ выражаетъ дѣлимость $M + M' - N$ на A ; но $M + M' - N$ равно $M - (N - M')$; дѣлимость же этого на A выражается сравненіемъ $M \equiv N - M' \pmod{A}$.

3) Два или нѣсколько сравненій съ однимъ и тѣмъ же модулемъ могутъ быть почленно складываемы и вычитаемы. Такъ если $M \equiv N \pmod{A}$, $M' \equiv N' \pmod{A}$; то $M \pm M' \equiv N \pm N' \pmod{A}$. Въ этомъ не трудно убѣдиться, замѣтивъ, что сравненія $M \equiv N \pmod{A}$, $M' \equiv N' \pmod{A}$ предполагаютъ дѣлимость разностей $M - N$, $M' - N'$ на A . Откуда слѣдуетъ дѣлимость на A числа равнаго $M - N \pm (M' - N')$, или $M \pm M' - (N \pm N')$; а это выражается сравненіемъ $M \pm M' \equiv (N \pm N') \pmod{A}$, что и слѣдовало доказать. Отъ соединенія двухъ сравненій не трудно перейти къ соединенію трехъ, четырехъ и т. д.

4) Члены сравненія могутъ быть умножены на одно число.

Такъ, если $M \equiv N \pmod{A}$; то $kM \equiv kN \pmod{A}$. Въ самомъ дѣлѣ, по предыдущему свойству, сложивши почленно k одинаковыхъ сравненій $M \equiv N \pmod{A}$, найдемъ $kM \equiv kN \pmod{A}$. Такъ докажется возможность умножать члены сравненія на всякое цѣлое, положительное число. Что же касается до умноженія на число отрицательное, то мы замѣчаемъ, что если $kM \equiv kN \pmod{A}$; то также $-kM \equiv -kN \pmod{A}$; ибо первое сравненіе предполагаетъ дѣлимость числа $kM - kN$ на

A , а это число съ знакомъ — будетъ $-kM + kN$ и дѣлимость его на A выражается сравненіемъ $-kM \equiv -kN \pmod{A}$.

5) Два или нѣсколько сравненій съ однимъ и тѣмъ же модулемъ могутъ быть почленно перемножены.

Не трудно убѣдиться, что если $M \equiv N \pmod{A}$ и $M' \equiv N' \pmod{A}$; то $MM' \equiv NN' \pmod{A}$. Въ самомъ дѣлѣ, сравненія $M \equiv N, M' \equiv N' \pmod{A}$ выражаютъ дѣлимость чиселъ $M - N, M' - N'$ на A . Называя же черезъ q, q' частныя получаемыя при этихъ дѣленіяхъ находимъ

$$\frac{M - N}{A} = q, \frac{M' - N'}{A} = q',$$

откуда выходитъ

$$M = Aq + N, M' = Aq' + N'.$$

Эти уравненія по перемноженіи даютъ

$$MM' = A^2qq' + A(qN' + q'N) + NN',$$

что обнаруживаетъ дѣлимость $MM' - NN'$ на A , и слѣд. сравненіе $MM' \equiv NN' \pmod{A}$.

Если мы перемножимъ такимъ образомъ сравненія $M \equiv N, M' \equiv N' \pmod{A}$ между собою, произведевіе ихъ перемножимъ съ $M \equiv N'' \pmod{A}$ и т. д.; то мы дойдемъ до сравненія $MM'M'' \dots \equiv NN'N'' \dots \pmod{A}$. Предполагая же здѣсь $M = M' = M'' = \dots, N = N' = N'' \dots$ и называя черезъ k число равныхъ чиселъ $M, M', M'', \dots, N, N', N'' \dots$ найдемъ $M^k \equiv N^k \pmod{A}$. На основаніи этого легко доказать слѣдующее предложеніе:

6) Значенія цѣлой функціи съ цѣлыми коэффиціентами отъ двухъ чиселъ сравнимыхъ по какому нибудь модулю сравнимы потому же модулю.

Такъ, если $M \equiv N \pmod{A}$, $f(x) = ax^m + bx^{m-1} + cx^{m-2} + \dots$, гдѣ a, b, c, \dots числа цѣлыя; то $f(M) \equiv f(N) \pmod{A}$. Въ самомъ дѣлѣ, изъ сравненія $M \equiv N \pmod{A}$ по доказанному нами сейчасъ выходитъ

$$M^m \equiv N^m, M^{m-1} \equiv N^{m-1}, M^{m-2} \equiv N^{m-2}, \dots \pmod{A};$$

умножая эти сравненія на a, b, c, \dots , выводимъ

$aM^m \equiv aN^m, bM^{m-1} \equiv bN^{m-1}, cM^{m-2} \equiv cN^{m-2} \dots (\text{мод. } A)$.

Эти же сравненія, будучи сложены почленно, даютъ $aM^m + bM^{m-1} + cM^{m-2} + \dots \equiv aN^m + bN^{m-1} + cN^{m-2} + \dots (\text{мод. } A)$, гдѣ замѣняя $aM^m + bM^{m-1} + cM^{m-2} + \dots, aN^m + bN^{m-1} + cN^{m-2} + \dots$ черезъ $f(M), f(N)$, имѣемъ $f(M) \equiv f(N) (\text{мод. } A)$, что и слѣдовало доказать.

7) Члены сравненія могутъ быть сокращены на ихъ общаго множителя, если этотъ множитель число простое съ модулемъ.

Такъ, если $kM \equiv kN (\text{мод. } A)$, гдѣ k число простое съ A ; то $M \equiv N (\text{мод. } A)$. Въ самомъ дѣлѣ, сравненіе $kM \equiv kN (\text{мод. } A)$ предполагаетъ дѣлимость $kM - kN$, или $k(M - N)$ на A . Но при k простомъ съ A по 2-й теоремѣ это предполагаетъ дѣлимость $M - N$ на A , а это выражается сравненіемъ $M \equiv N (\text{мод. } A)$.

8) Если одна часть сравненія и модуль дѣлятся на какое нибудь число; то на то же число должна дѣлиться и другая часть сравненія; иначе сравненіе не возможно.

Такъ, если $M \equiv kN (\text{мод. } kA)$, то M дѣлится на k . Въ самомъ дѣлѣ, это сравненіе предполагаетъ, что разность $M - kN$ дѣлится на kA . Называя же черезъ q частное отъ этого дѣленія, имѣемъ $\frac{M - kN}{kA} = q$. Откуда выходитъ $M = k(N + Aq)$, что обнаруживаетъ дѣлимость M на k .

9) Общій множитель членовъ сравненія и модуля можетъ быть сокращенъ. Такъ если $kM \equiv kN (\text{мод. } kA)$; то $M \equiv N (\text{мод. } A)$. Въ самомъ дѣлѣ, сравненіе $kM \equiv kN (\text{мод. } kA)$ предполагаетъ дѣлимость $kM - kN$ на kA ; но $\frac{kM - kN}{kA}$ приводится къ $\frac{M - N}{A}$; дѣлимость же $M - N$ на A выражается сравненіемъ $M \equiv N (\text{мод. } A)$.

10) Два числа, сравнимыя по двумъ или нѣсколькимъ модулямъ простымъ между собою, сравнимы и по произведенію ихъ. Такъ, если $M \equiv N (\text{мод. } A), M \equiv N (\text{мод. } A')$, гдѣ A, A' числа простые между собою; то $M \equiv N (\text{мод. } AA')$. Въ

самомъ дѣлѣ, сравненія $M \equiv N \pmod{A}$, $M \equiv N \pmod{A}$ предполагаютъ дѣлимость $M - N$ на A и A' . Но при A и A' простыхъ между собою эта дѣлимость (теор. 3) предполагаетъ дѣлимость $M - N$ на произведение AA' , что выражается сравненіемъ $M \equiv N \pmod{AA'}$. На основаніи этого, имѣя нѣсколько сравненій $M \equiv N \pmod{A}$, $M \equiv N \pmod{A'}$, $M \equiv N \pmod{A''}$..., гдѣ всѣ числа A, A', A'', \dots суть простые относительно другъ друга, мы изъ соединенія двухъ первыхъ находимъ $M \equiv N \pmod{AA'}$; соединяя же это сравненіе съ $M \equiv N \pmod{A''}$, получаемъ $M \equiv N \pmod{AA'A''}$ и такъ даже, въ чемъ и заключается предложенная намъ теорема.

11) *Не нарушая сравненія модуль можетъ быть замѣненъ числомъ, на которое онъ дѣлится.* Такъ, если $M \equiv N \pmod{AA'}$; то $M \equiv N \pmod{A}$. Въ самомъ дѣлѣ, умножая члены этого сравненія на A' , найдемъ $A'M \equiv A'N \pmod{AA'}$. Но по замѣченному намъ свойству сравненій (см. н^о 9) общій множитель членовъ сравненія и модуля можетъ быть сокращенъ. Сокращая же въ сравненіи $A'M \equiv A'N \pmod{AA'}$ множитель A' , находимъ $M \equiv N \pmod{A}$, что и слѣдовало доказать.

Вотъ главные свойства сравненій двухъ чиселъ между собою; эти свойства послужатъ намъ для рѣшенія сравненій, заключающихъ одно или нѣсколько неизвѣстныхъ. Къ этому мы теперь и приступимъ.

§ 10. Мы видѣли, что въ сравненіи члены могутъ быть переносимы изъ одной части въ другую. Предполагая же всѣ члены перенесенными въ одну часть сравненія, мы приведемъ его къ виду

$$f(x, y, z, \dots) \equiv 0 \pmod{p},$$

гдѣ f какая нибудь функція, p данное число, принимаемое за модуль, x, y, z, \dots числа неизвѣстныя.

Исслѣдованія наши мы начнемъ съ простѣйшихъ сравненій, съ сравненій, заключающихъ одно неизвѣстное и сначала рассмотримъ тотъ случай, когда функція, входящая въ сравненіе, есть цѣлая съ цѣлыми коэффициентами.

Ограничиваясь сравненіями этого вида, мы докажемъ для нихъ слѣдующую теорему:

13. Т Е О Р Е М А.

Если сравненію $fx \equiv 0 \pmod{p}$ удовлетворяетъ $x = a$; то ему удовлетворяютъ и все числа сравнимыя съ a по модулю p *).

Доказательство. Въ самомъ дѣлѣ по свойствамъ сравненій, замѣченныхъ нами въ предыдущемъ параграфѣ (см. тамъ $n^{\circ}6$), изъ сравненія $X \equiv a \pmod{p}$ выходитъ $fX \equiv fa \pmod{p}$. Но a по положенію удовлетворяетъ сравненію $fx \equiv 0 \pmod{p}$, слѣд. $fa \equiv 0 \pmod{p}$, а въ этомъ случаѣ по $n^{\circ}1$ предыдущаго параграфа изъ сравненія $fX \equiv fa \pmod{p}$ выходитъ $fX \equiv 0 \pmod{p}$, что и слѣдовало доказать.

§ 11. Мы видѣли, что если a есть число удовлетворяющее сравненію $fx \equiv 0 \pmod{p}$; то ему удовлетворяютъ и все числа сравнимыя съ a по модулю p . Посмотримъ теперь какія же числа будутъ сравнимы съ a по модулю p . Для этого мы припомнимъ, что числа, сравнимыя между собою по модулю p , суть тѣ, которыхъ разность дѣлится на p безъ остатка; поэтому X будетъ числомъ сравнимымъ съ a по модулю p , если разность ихъ дѣлится на p . Называя же частное отъ дѣленія $a - X$ на p черезъ N , мы найдемъ $\frac{a - X}{p} = N$; откуда $X = a - pN$. Вотъ общая формула всехъ чиселъ сравнимыхъ съ a по модулю p . Давая здѣсь числу N различныя величины какъ положительныя, такъ и отрицательныя, мы найдемъ безконечное множество чиселъ, сравнимыхъ съ a по модулю p . Но изъ всехъ чиселъ сравнимыхъ съ a по модулю p особеннаго вниманія заслуживаютъ два числа: 1-е) число положительное наименьшее изъ всехъ чиселъ сравнимыхъ съ a по модулю p ; оно извѣстно подъ названіемъ *наименьшаго по-*

(*) Здѣсь и вездѣ въ послѣдствіи подъ знаками fx, Fx, ffx, \dots мы будемъ разумѣть цѣлыя функціи съ цѣлыми коэффициентами.

ложительного вычета числа a по модулю p ; 2-е) число отрицательное, котораго численная величина менѣе численной величины всѣхъ отрицательныхъ чиселъ, сравнимыхъ съ a по модулю p ; такое число извѣстно подъ названіемъ *наименьшаго отрицательнаго вычета числа a по модулю p* . Кроме того мы будемъ отличать особеннымъ именемъ *обсолютно малаго вычета числа a по модулю p* тотъ изъ наименьшихъ вычетовъ положительный или отрицательный, который имѣетъ наименьшую численную величину. Въ случаѣ равенства численныхъ величинъ наименьшаго положительнаго вычета числа a по модулю p и наименьшаго отрицательнаго вычета его мы за абсолютно малый вычетъ числа a по модулю p можемъ безъ различія принимать тотъ или другой изъ наименьшихъ вычетовъ и мы будемъ говорить, что въ этомъ случаѣ абсолютно малый вычетъ числа a по модулю p имѣетъ двѣ величины.

По формулѣ $X = a - Np$, опредѣляющей всѣ числа сравнимыя съ a по модулю p , не трудно найти и наименьшій положительный вычетъ a по модулю p и наименьшій отрицательный вычетъ его. Для этого мы уравненіе $X = a - Np$ пишемъ такъ $X = p \left(\frac{a}{p} - N \right)$; откуда видно, что наименьшая численная величина X соотвѣтствуетъ значеніямъ N наиблизе подходящимъ къ $\frac{a}{p}$; притомъ видно также, что X будетъ имѣть значеніе положительное или отрицательное, смотря потому будетъ ли N менѣе или болѣе чѣмъ $\frac{a}{p}$.

Итакъ наименьшій положительный вычетъ числа a по модулю p опредѣлится по формулѣ $a - Np$, когда за N мы возьмемъ число наиблизе подходящее къ $\frac{a}{p}$, но не превосходящее $\frac{a}{p}$; такое число, очевидно, при a положительномъ мы найдемъ въ частномъ, дѣля a на p и пренебрегая остаткомъ. Откуда ясно, что наименьшій положительный вычетъ по модулю p числа положительнаго мы найдемъ въ остаткѣ отъ дѣленія его на p . Такъ для опредѣленія наименьшаго положительнаго вычета 23

по модулю 7, мы будем имѣть формулу $23 - 7N$, гдѣ за N должны будемъ взять цѣлое число, получаемое при дѣленіи 23 на 7. Выполняя это дѣленіе находимъ, что здѣсь $N = 3$. Дѣлая $N = 3$ въ формулѣ $23 - 7N$, находимъ, что 2 есть наименьшій положительный вычетъ 23 по модулю 7.

Также для наименьшаго положительнаго вычета -2 по модулю 5 находимъ формулу $-2 - 5N$, гдѣ за N должны взять число ближе подходящее къ $-\frac{2}{5}$, но не превосходящее $-\frac{2}{5}$. Такое число есть -1 ; слѣд. искомый вычетъ есть $-2 + 5 = 3$.

Не трудно убѣдиться, что всегда малый положительный вычетъ a по модулю p меньше p . Это слѣдуетъ изъ сказаннаго нами объ опредѣленіи его. Мы видѣли, что онъ опредѣляется формулою $a - pN$, гдѣ N есть цѣлое число ближе подходящее къ $\frac{a}{p}$; а потому $\frac{a}{p} - N < 1$ и слѣд.

$$a - pN = p \left(\frac{a}{p} - N \right) < p.$$

Для опредѣленія наименьшаго отрицательнаго вычета числа a по модулю p , мы должны въ формулѣ $a - pN$, или $p \left(\frac{a}{p} - N \right)$ принять за N число, которое бы было больше $\frac{a}{p}$ и ближе подходило къ $\frac{a}{p}$; такое число при a положительномъ, очевидно, мы получимъ, если, дѣля a на p , дробь частнаго замѣнимъ единицею. Такъ наименьшій отрицательный вычетъ числа 23 по модулю 7 опредѣлится формулою $23 - 7N$, гдѣ за N должны взять частное $\frac{23}{7} = 3 + \frac{2}{7}$, замѣнивъ единицею дробь $\frac{2}{7}$; это дастъ намъ $N = 4$ и по формулѣ $23 - 7N$ находимъ, что наименьшій отрицательный вычетъ числа 23 по модулю 7 есть $23 - 7 \cdot 4$, или -5 .

Опредѣливши наименьшій положительный вычетъ и наименьшій отрицательный, мы легко узнаемъ тотъ изъ нихъ, который долженъ быть принятъ за абсолютно малый вычетъ. Но его также можно опредѣлить непосредственно на основаніи формулы $a - pN$, или $p \left(\frac{a}{p} - N \right)$. Для этого стоитъ только выбрать

значение N такъ, чтобы $\frac{a}{p} - N$ имѣло наименьшую численную величину; такое значение N мы, очевидно, найдемъ, опредѣляя частное $\frac{a}{p}$ и откидывая въ немъ дробную часть, когда она меньше $\frac{1}{2}$ или замѣняя ее единицею, если она болѣе $\frac{1}{2}$. Если же дробная часть $\frac{a}{p}$ не болѣе $\frac{1}{2}$ и не меньше $\frac{1}{2}$; то мы ее по произволу можемъ или откинуть или замѣнить единицею; въ томъ и другомъ случаѣ численная величина $\frac{a}{p} - N$ будетъ равна $\frac{1}{2}$. Такъ для опредѣленія абсолютнаго малаго вычета 23 по модулю 7, мы должны въ формулѣ $23 - 7 \cdot N$ принять за N частное $\frac{23}{7} = 3 + \frac{2}{7}$, откинувши дробь $\frac{2}{7}$. Это даетъ намъ $N = 3$ и слѣдовательно искомый абсолютно малый вычетъ будетъ $23 - 7 \cdot 3 = 2$.

Напротивъ при опредѣленіи абсолютнаго малаго вычета 25 по модулю 7, мы возьмемъ въ формулѣ $23 - 7 \cdot N$ за N частное $\frac{25}{7} = 3 + \frac{4}{7}$, замѣнивъ единицею дробь $\frac{4}{7}$. Это дастъ намъ $N = 4$ и для величины искомаго вычета найдемъ $25 - 7 \cdot 4 = -3$.

Изъ сказаннаго нами слѣдуетъ, что при опредѣленіи абсолютно малаго вычета по формулѣ $a - Np$, мы за N принимаемъ число, котораго разность съ $\frac{a}{p}$ будетъ имѣть численную величину не болѣе $\frac{1}{2}$. А потому абсолютно малый вычетъ числа a по модулю p , опредѣляясь формулою $a - Np$, или $p \left(\frac{a}{p} - N \right)$ будетъ имѣть численную величину не превосходящую $\frac{p}{2}$.

§ 12. Рассмотрѣвши числа, сравнимыя съ a по модулю p , обращаемся къ рѣшенію сравненія $fx \equiv 0 \pmod{p}$.

Мы видѣли, что если этому сравненію удовлетворяетъ a , то ему удовлетворяетъ и всякое число X , для котораго имѣетъ мѣсто сравненіе $X \equiv a \pmod{p}$. Этихъ чиселъ безконечное множество; но всѣ они, сравнимыя съ однимъ и тѣмъ же числомъ a и слѣдоват. между собою по модулю p , принимаются за одно рѣшеніе сравненія $fx \equiv 0 \pmod{p}$. По этому мы будемъ говорить, что сравненіе $fx \equiv 0 \pmod{p}$ имѣетъ одно только рѣшеніе, если ему удов-

летворяют только числа, для которых $x \equiv a \pmod{p}$; мы будем говорить, что сравнение $fx \equiv 0 \pmod{p}$ имѣетъ два рѣшенія, если ему кромѣ чиселъ, опредѣляемыхъ сравненіемъ

$$x \equiv a \pmod{p},$$

удовлетворяютъ другія, получаемыя изъ сравненія

$$x \equiv a_1 \pmod{p},$$

гдѣ a не $\equiv a_1 \pmod{p}$. П вообще мы будемъ говорить, что сравнение $fx \equiv 0 \pmod{p}$ имѣетъ n рѣшеній; если ему удовлетворяютъ только числа, опредѣляемыя сравненіями

$$x \equiv a, x \equiv a_1, x \equiv a_2, \dots, x \equiv a_{n-1} \pmod{p},$$

гдѣ $a, a_1, a_2, \dots, a_{n-1}$ суть числа не сравнимыя между собою по модулю p . На основаніи этого мы докажемъ слѣдующую теорему:

14. ТЕОРЕМА.

Сравненіе $fx \equiv 0 \pmod{p}$ имѣетъ столько рѣшеній, сколько чиселъ въ рядѣ $0, 1, 2, \dots, p-1$ ему удовлетворяетъ и если эти числа суть $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n$; то $x \equiv \alpha_1, x \equiv \alpha_2, x \equiv \alpha_3, \dots, x \equiv \alpha_n \pmod{p}$ суть рѣшенія сравненія $fx \equiv 0 \pmod{p}$.

Доказательство. Въ § 10 видѣли, что если $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n$ удовлетворяютъ сравненію $fx \equiv 0 \pmod{p}$; то ему удовлетворяютъ и всѣ числа, опредѣляемыя сравненіями

$$x \equiv \alpha_1, x \equiv \alpha_2, x \equiv \alpha_3, \dots, x \equiv \alpha_n \pmod{p}.$$

Но не трудно доказать съ одной стороны, что кромѣ этихъ чиселъ нѣтъ ни одного удовлетворяющаго сравненію $fx \equiv 0 \pmod{p}$, а съ другой, что числа $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n$ не сравнимы между собою по модулю p ; откуда по сказанному нами о числѣ рѣшеній сравненія $fx \equiv 0 \pmod{p}$ и будетъ слѣдовать предложенная теорема.

Для доказательства перваго предположимъ, что какое либо число A удовлетворяетъ сравненію $fx \equiv 0 \pmod{p}$, не удовлетворяя ни одному изъ слѣдующихъ:

$$x \equiv \alpha_1, x \equiv \alpha_2, x \equiv \alpha_3, \dots, x \equiv \alpha_n \pmod{p}.$$

Если A удовлетворяетъ сравненію $fx \equiv 0 \pmod{p}$; то по § 10 будетъ удовлетворять ему и всякое число, сравнимое съ

нимъ по модулю p и слѣд. наименьшій положительный вычетъ его. Называя этотъ вычетъ черезъ α , мы будемъ имѣть

$$A \equiv \alpha, f(\alpha) \equiv 0 \pmod{p} \dots \dots \dots (4)$$

и α , какъ наименьшій положительный вычетъ A по модулю p , будетъ заключаться въ рядѣ $0, 1, 2, \dots, p-1$. Но если α заключается въ этомъ рядѣ и удовлетворяетъ сравненію $f(x) \equiv 0 \pmod{p}$; то α есть одно изъ чиселъ $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n$; пбо по положенію $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n$ суть единственные числа ряда $0, 1, 2, \dots, p-1$ удовлетворяющія сравненію $f(x) \equiv 0 \pmod{p}$. Но это невозможно; пбо по (4) A удовлетворяетъ сравненію $x \equiv \alpha \pmod{p}$, между тѣмъ какъ по положенію оно не удовлетворяетъ ни одному изъ сравненій

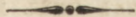
$$x \equiv \alpha_1, x \equiv \alpha_2, \dots, x \equiv \alpha_n \pmod{p}.$$

Переходимъ теперь къ доказательству, что числа $\alpha_1, \alpha_2, \dots, \alpha_n$ не сравнимы между собою по модулю p . Для этого допустимъ противное; пусть будетъ $\alpha_1 \equiv \alpha_2 \pmod{p}$. Изъ этого сравненія слѣдуетъ дѣлимость $\alpha_1 - \alpha_2$ на p , что не возможно; пбо α_1, α_2 числа положительные и каждое изъ нихъ меньше p , вслѣдствіе чего разность ихъ будетъ имѣть численную величину меньше p и слѣдовательно не дѣлимую на p .

Такъ убѣждаемся мы въ справедливости теоремы, нами предложенной.

Чтобы показать приложеніе этой теоремы возьмемъ сравненіе $x^5 - x - 1 \equiv 0 \pmod{5}$. Внося сюда вмѣсто x числа $0, 1, 2, 3, 4$, мы убѣждаемся, что только 2 удовлетворяетъ разсматриваемому сравненію. Откуда заключается, что это сравненіе имѣетъ одно рѣшеніе $x \equiv 2 \pmod{5}$.

Такимъ же образомъ для сравненія $x^2 - 3 \equiv 0 \pmod{11}$ находимъ два рѣшенія $x \equiv 5, x \equiv 6 \pmod{11}$; разсматривая же сравненіе $x^2 - 11 \equiv 0 \pmod{3}$ убѣждаемся, что оно не имѣетъ ни одного рѣшенія.



ГЛАВА II.

О СРАВНЕНИИ ПЕРВОЙ СТЕПЕНИ.

§ 13. Общій видъ сравненій первой степени есть

$$ax - b \equiv 0 \pmod{p},$$

гдѣ a , b какія нибудь числа положительныя или отрицательныя; p число положительное. Сравненія этого вида представляютъ два случая существенно отличныя одинъ отъ другаго; ихъ мы рассмотримъ отдѣльно. Первый случай это когда a и p числа относительно другъ друга простыя; второй, когда они имѣютъ общаго множителя. Мы начнемъ съ перваго случая a и p простыхъ между собою и докажемъ слѣдующую теорему:

15. ТЕОРЕМА.

Сравненіе $ax - b \equiv 0 \pmod{p}$ при a простомъ съ p имѣетъ всегда одно рѣшеніе.

Доказательство. Изъ доказаннаго нами въ параграфѣ 12 о числѣ рѣшеній сравненія $fx \equiv 0 \pmod{p}$ слѣдуетъ, что сравненіе $ax - b \equiv 0 \pmod{p}$ имѣетъ столько рѣшеній, сколько находится въ рядѣ $0, 1, 2, \dots, p-1$ чиселъ, ему удовлетворяющихъ, или, что одно и тоже, сколько въ рядѣ $a \cdot 0 - b, a \cdot 1 - b, a \cdot 2 - b, \dots, a(p-1) - b$ чиселъ дѣлящихся на p . Но какъ эти числа составляютъ арифметическую прогрессию, которой разность есть a , число простое съ p по положенію, число же членовъ равно p ; то по 10-й теоремѣ здѣсь будетъ одинъ членъ дѣлящійся на p . Слѣд. въ сдѣланномъ нами предположеніи сравненіе $ax - b \equiv 0 \pmod{p}$ имѣетъ одно рѣшеніе, что и слѣдовало доказать.

Убѣдившись такимъ образомъ, что въ рассматриваемомъ нами случаѣ сравненіе $ax - b \equiv 0 \pmod{p}$ имѣетъ одно рѣшеніе, мы покажемъ теперь, какъ найдется оно. Въ настоящее время извѣстно нѣсколько способовъ рѣшать сравненіе $ax - b \equiv 0 \pmod{p}$; замѣчательнѣйшіе изъ нихъ мы предложимъ въ послѣдствіи, говоря о свойствахъ чиселъ, на которыхъ они основаны.

ваются. Здѣсь же замѣтимъ, что сравненіе $ax - b \equiv 0 \pmod{p}$ можетъ быть рѣшено по способу предполагаемому въ Алгебрѣ для рѣшенія неопредѣленнаго уравненія $ax - pz = b$, отъ котораго сравненіе $ax - b \equiv 0 \pmod{p}$ отличается только знакомъ положеніемъ. Дѣйствительно, сравненіе $ax - b \equiv 0 \pmod{p}$ есть ничто иное, какъ выраженіе дѣлимости $ax - b$ на p , что можетъ быть представлено уравненіемъ $\frac{ax - b}{p} = z$, предполагая z произвольнымъ цѣлымъ числомъ. Откуда для опредѣленія x и z получаемъ уравненіе $ax - pz = b$.

И такъ рѣшеніемъ уравненія $ax - pz = b$ опредѣляются значенія x , удовлетворяющія сравненію $ax - b \equiv 0 \pmod{p}$. Эти значенія x , какъ извѣстно, выражаются такъ: $x = \alpha + np$, гдѣ α одна изъ величинъ x , способная удовлетворить уравненію $ax - pz = b$, n число произвольное. По принятому нами знакомъ положенію мы вмѣсто того, чтобы писать $x = \alpha + np$, предполагая n произвольнымъ числомъ, можемъ написать $x \equiv \alpha \pmod{p}$ и въ этомъ видѣ мы будемъ всегда представлять рѣшеніе сравненія $ax - b \equiv 0 \pmod{p}$.

Напримѣръ, имѣя для рѣшенія сравненіе $7x - 3 \equiv 0 \pmod{10}$, мы возьмемъ уравненіе $7x - 10z = 3$. Рѣшая это уравненіе, мы найдемъ для значенія x и z такія выраженія $x = 9 + 10n$, $z = 6 + 7n$; откуда для рѣшенія сравненія $7x - 3 \equiv 0 \pmod{10}$ получаемъ

$$x \equiv 9 \pmod{10}.$$

§ 14. На основаніи доказанныхъ нами теоремъ относительно сравненій вообще и въ особенности относительно сравненій вида $ax - b \equiv 0 \pmod{p}$ могутъ быть доказаны двѣ любопытныя теоремы относительно чиселъ, которыя послужатъ намъ также для рѣшенія сравненій первой степени. Этими-то свойствами чиселъ мы теперь и займемся.

16. ТЕОРЕМА.

Если p число простое и не дѣлитъ a ; то $a^{p-1} \equiv 1 \pmod{p}$.

Доказательство. Пусть будутъ $r_1, r_2, r_3, \dots, r_{p-1}$ наимень-

шіе положительныя вычеты чиселъ $1a, 2a, 3a, \dots, (p-1)a$ по модулю p ; они будутъ удовлетворять сравненіямъ

$$1a \equiv r_1, 2a \equiv r_2, 3a \equiv r_3, \dots, (p-1)a \equiv r_{p-1} \pmod{p} \dots (5)$$

Перемножая эти сравненія между собою, мы найдемъ

$$1 \cdot 2 \cdot 3 \dots (p-1) a^{p-1} \equiv r_1 r_2 r_3 \dots r_{p-1} \pmod{p} \dots (6)$$

Но нетрудно убѣдиться, что произведенія

$$1 \cdot 2 \cdot 3 \dots (p-1), r_1 r_2 r_3 \dots r_{p-1}$$

равны между собою.

Для этого мы замѣчаемъ, что $r_1, r_2, r_3, \dots, r_{p-1}$, какъ наименьшіе положительныя вычеты чиселъ $1a, 2a, 3a, \dots, (p-1)a$ по модулю p , могутъ имѣть только значенія

$$0, 1, 2, \dots, p-1.$$

Притомъ ни одно изъ нихъ не можетъ быть нулемъ; ибо въ противномъ случаѣ сравненіе (6) предполагало бы дѣлимость

$$1 \cdot 2 \cdot 3 \dots (p-1) a^{p-1}$$

на p , между тѣмъ какъ $1, 2, 3, \dots, p-1$ и a числа простыя съ p .

И такъ числа $r_1, r_2, r_3, \dots, r_{p-1}$ могутъ имѣть только значенія

$$1, 2, 3, \dots, p-1.$$

Но между числами $r_1, r_2, r_3, \dots, r_{p-1}$ не можетъ быть двухъ имѣющихъ одну и ту-же величину; ибо предпологая $r_m = r_\mu = b$, мы по (5) имѣли бы

$$ma \equiv b, \mu a \equiv b \pmod{p},$$

гдѣ m и μ два числа изъ ряда $1, 2, 3, \dots, p-1$, и слѣд. для сравненія $ax \equiv b \pmod{p}$ нашли бы два рѣшенія

$$x \equiv m, x \equiv \mu \pmod{p},$$

что не возможно.

Отсюда слѣдуетъ, что въ составъ ряда

$$r_1, r_2, r_3, \dots, r_{p-1}$$

могутъ входить только числа

$$1, 2, 3, \dots, p-1$$

и каждое только по одному разу.

Но такъ какъ въ рядахъ

$$r_1, r_2, r_3, \dots, r_{p-1},$$

$$1, 2, 3, \dots, p-1$$

одинакое число членовъ; то въ первый должны входить всѣ вторые, слѣд. эти ряды составлены изъ однихъ и тѣхъ-же чиселъ и притомъ взятыхъ по одному разу; а потому произведение членовъ перваго ряда равно произведению членовъ втораго. Убѣдясь въ этомъ, мы можемъ въ (6) замѣнить произведение $r_1 r_2 r_3 \dots r_{p-1}$ произведениемъ $1 \cdot 2 \cdot 3 \dots (p-1)$.

Такимъ образомъ находимъ

$$1 \cdot 2 \cdot 3 \dots (p-1) a^{p-1} \equiv 1 \cdot 2 \cdot 3 \dots (p-1) \pmod{p}.$$

Но члены этого сравненія могутъ быть сокращены на 2, 3, . . . $p-1$; пбо всѣ эти числа, будучи меньше p , будутъ относительно его простыя. Выполнивъ же эти сокращенія, найдемъ

$$a^{p-1} \equiv 1 \pmod{p},$$

что и слѣдовало доказать.

Такъ для $p = 7$, $a = 2$ будетъ $2^{7-1} \equiv 1 \pmod{7}$, въ справедливости чего мы убѣждаемся, замѣтивъ, что 2^6 равно 64 и $64 \equiv 1 \pmod{7}$.

Эта теорема есть одна изъ замѣчательнѣйшихъ въ Теоріи чиселъ и имѣетъ весьма важныя приложения. Она открыта Ферматомъ; но предложена имъ была безъ доказательства. Первый, успѣвшій ее доказать, былъ Эйлеръ; онъ же далъ слѣдующую теорему болѣе общую.

17. ТЕОРЕМА.

Если n означаетъ сколько чиселъ простыхъ съ N и меньшихъ N и a число простое съ N ; то $a^n \equiv 1 \pmod{N}$.

Доказательство. Называя черезъ N_1, N_2, \dots, N_n числа простыя съ N и меньшія N , чрезъ r_1, r_2, \dots, r_n наименьшіе положительные вычеты чиселъ aN_1, aN_2, \dots, aN_n по модулю N , имѣемъ

$$aN_1 \equiv r_1, aN_2 \equiv r_2, \dots, aN_n \equiv r_n \pmod{N}, \dots \dots \dots (7)$$

что по перемноженіи даетъ

$$N_1 N_2 \dots N_n a^n \equiv r_1 r_2 r_3 \dots r_n \pmod{N} \dots \dots \dots (8)$$

Но не трудно убѣдиться, что произведенія $N_1 N_2 \dots N_n$, $r_1 r_2 \dots r_n$ равны.

Такъ какъ r_1, r_2, \dots, r_n суть наименьшіе положительныя вычеты чиселъ aN_1, aN_2, \dots, aN_n по модулю N ; то они могутъ имѣть только значенія

$$0, 1, 2, \dots, N - 1$$

и изъ этихъ значеній для $r_1, r_2, r_3, \dots, r_n$ возможны только тѣ, которыя не имѣютъ общаго множителя съ N ; ибо сравненіе (8), котораго первая часть состоитъ изъ произведенія простыхъ чиселъ съ N , предполагаетъ, что N и $r_1, r_2, r_3, \dots, r_n$ не имѣютъ общаго дѣлителя.

Отсюда слѣдуетъ, что для $r_1, r_2, r_3, \dots, r_n$ возможны только значенія

$$N_1, N_2, \dots, N_n.$$

Притомъ между числами $r_1, r_2, r_3, \dots, r_n$ не можетъ быть двухъ равныхъ между собою; ибо при равенствѣ $r_m = r_\mu = b$ мы по (7) имѣли бы

$$a\mu \equiv b, a\mu \equiv b \pmod{N},$$

гдѣ m, μ два какія нибудь числа изъ ряда $1, 2, \dots, N - 1$ и слѣд. для сравненія $ax \equiv b \pmod{N}$ мы нашли бы два рѣшенія, что не возможно.

Отсюда слѣдуетъ, что въ составъ ряда

$$r_1, r_2, r_3, \dots, r_n$$

входятъ однѣ лишь числа

$$N_1, N_2, \dots, N_n$$

и каждое только по одному разу. Но какъ въ этихъ рядахъ одинакое число членовъ; то въ первый должны взойти всѣ числа втораго и слѣд. эти ряды составлены изъ однихъ и тѣхъ же чиселъ, притомъ взятыхъ по одному разу, а потому произведеніе чиселъ перваго ряда равно произведенію чиселъ втораго.

Убѣдясь въ этомъ, мы можемъ въ (8) произведеніе $r_1 r_2 \dots r_n$ замѣнить произведеніемъ $N_1 N_2 \dots N_n$. Такимъ образомъ находимъ

$$N_1 N_2 \dots N_n a^n \equiv N_1 N_2 \dots N_n \pmod{N}.$$

Но здѣсь члены сравненія могутъ быть сокращены на общихъ множителей N_1, N_2, \dots, N_n ; ибо числа эти суть простые съ N . Выполнивъ же эти сокращенія найдемъ

$$a'' \equiv 1 \pmod{N},$$

что и слѣдовало доказать.

Такъ если $N = 20$, $a = 3$; то по 12-й теоремѣ для величины n , означающаго сколько простыхъ чиселъ съ 20 и меньшихъ 20, находимъ 8 и по доказанной нами теоремѣ будетъ $3^8 \equiv 1 \pmod{20}$. Въ справедливости этого сравненія мы убѣждаемся, находя, что $3^8 = 6561$ и $6561 \equiv 1 \pmod{20}$.

§ 15. На основаніи этихъ теоремъ не трудно найти рѣшеніе сравненія $ax - b \equiv 0 \pmod{p}$, гдѣ a по прежнему предполагаемъ простымъ съ p .

Начнемъ съ частнаго случая p простаго. Такъ какъ a по положенію число простое съ p и p само по себѣ простое; то a не дѣлится на p (§ 3) и по теоремѣ 16-й, которую вездѣ впоследствии будемъ употреблять подъ именемъ теоремы Ферматовой, будетъ имѣть мѣсто сравненіе $a^{p-1} \equiv 1 \pmod{p}$, что по умноженіи на b можетъ быть такъ представлено

$$a \cdot ba^{p-2} - b \equiv 0 \pmod{p}.$$

Сличая же это сравненіе съ даннымъ для рѣшенія $ax - b \equiv 0 \pmod{p}$, мы замѣчаемъ, что послѣднему удовлетворяетъ $x = ba^{p-2}$; а потому рѣшеніе его представится формулою

$$x \equiv ba^{p-2} \pmod{p}.$$

Такъ опредѣляются рѣшенія сравненія

$$ax - b \equiv 0 \pmod{p}$$

при p простомъ и недѣлящемъ a .

На примѣръ для рѣшенія сравненія $3x - 8 \equiv 0 \pmod{5}$ найдемъ

$$x \equiv 8 \cdot 3^{5-2} \pmod{5},$$

или

$$x \equiv 216 \pmod{5}.$$

Это рѣшеніе сравненія $3x - 8 \equiv 0 \pmod{5}$ мы можемъ

*

представить проще, замѣняя 216 его наименьшимъ положительнымъ вычетомъ по модулю 5. Такъ находимъ

$$x \equiv 1 \pmod{5}$$

для рѣшенія сравненія $3x - 8 \equiv 0 \pmod{5}$.

Переходимъ теперь къ рѣшеніямъ сравненій, которыхъ модуль число составное. Пусть дано будетъ сравненіе $ax - b \equiv 0 \pmod{N}$, гдѣ N какое нибудь число, число же a , какъ предполагали, простое съ N . По теоремѣ Ейлера (теорема 17) мы будемъ имѣть

$$a^n \equiv 1 \pmod{N},$$

означая черезъ n сколько чиселъ меньшихъ N и простыхъ съ N .

Это сравненіе по умноженіи на b можетъ быть такъ представлено

$$a \cdot b a^{n-1} - b \equiv 0 \pmod{N}.$$

Случая это сравненіе съ даннымъ для рѣшенія $ax - b \equiv 0 \pmod{N}$, находимъ, что ему удовлетворяетъ

$$x \equiv ba^{n-1} \pmod{N}.$$

Что касается до значенія n , опредѣляющаго сколько чиселъ простыхъ съ N и меньшихъ N , то по 12-й теоремѣ мы его легко найдемъ. На основаніи этой теоремы мы находимъ, что n равно

$$\alpha^m \beta^{n'} \gamma^p \dots \frac{\alpha-1}{\alpha} \cdot \frac{\beta-1}{\beta} \cdot \frac{\gamma-1}{\gamma} \dots,$$

если N разложеніемъ на простые множители приводится къ $\alpha^m \beta^{n'} \gamma^p \dots$. Такимъ образомъ мы убѣждаемся, что вообще рѣшеніе сравненія

$$ax - b \equiv 0 \pmod{\alpha^m \beta^{n'} \gamma^p \dots},$$

гдѣ $\alpha, \beta, \gamma, \dots$ различныя простые числа, опредѣляется слѣдующею формулою

$$x \equiv ba^{\alpha^m \beta^{n'} \gamma^p \dots} \frac{\alpha-1}{\alpha} \cdot \frac{\beta-1}{\beta} \cdot \frac{\gamma-1}{\gamma} \dots - 1 \pmod{\alpha^m \beta^{n'} \gamma^p \dots}$$

Такъ для рѣшенія сравненія $2x - 7 \equiv 0 \pmod{15}$, гдѣ $15 = 3 \cdot 5$, находимъ

$$x \equiv 7 \cdot 2^{3 \cdot 5} \cdot \frac{3-1}{3} \cdot \frac{5-1}{5} - 1 \pmod{15},$$

или

$$x \equiv 896 \pmod{15}.$$

Замѣняя же здѣсь 896 его наименьшимъ положительнымъ вычетомъ по модулю 15, мы это сравненіе представимъ такъ

$$x \equiv 11 \pmod{15}.$$

Этимъ мы окончиваемъ изслѣдованія сравненій первой степени, въ которыхъ модуль и коэффициентъ неизвѣстнаго суть числа относительно другъ друга простые и переходимъ къ тому случаю, когда эти числа имѣютъ общаго множителя.

§ 16. По свойству сравненій, показанному нами въ § 10, сравненіе $ax \equiv b \pmod{p}$ не возможно, если a и p имѣютъ общаго множителя, который не дѣлитъ b . Откуда слѣдуетъ такая теорема:

18. ТЕОРЕМА.

Сравненіе $ax - b \equiv 0 \pmod{p}$ не имѣетъ рѣшенія, если общій множитель a и p не дѣлитъ b .

Такъ убѣждаемся, что сравненія $20x - 7 \equiv 0 \pmod{15}$, $6x - 5 \equiv 0 \pmod{9}$ не имѣютъ рѣшенія.

Обращаемся теперь къ сравненіямъ вида $ax - b \equiv 0 \pmod{p}$, когда общіе множители a и p дѣлятъ b . Для этихъ сравненій докажется слѣдующая теорема:

19. ТЕОРЕМА.

Если a и p имѣютъ общимъ наибольшимъ дѣлителемъ d и d дѣлитъ b то сравненіе $ax - b \equiv 0 \pmod{p}$ имѣетъ d рѣшеній, которыя могутъ быть такъ представлены: $x \equiv \alpha$, $x \equiv \alpha + \frac{p}{d}$, $x \equiv \alpha + \frac{2p}{d}$, ..., $x \equiv \alpha + \frac{(d-1)p}{d} \pmod{p}$, гдѣ α есть число $< \frac{p}{d}$ и не < 0 , удовлетворяющее сравненію $\frac{a}{d}x - \frac{b}{d} \equiv 0 \pmod{\frac{p}{d}}$.

Доказательство. Если d есть общій наибольшій дѣлитель чиселъ a и p и на него дѣлится b ; то сравненіе

$$ax - b \equiv 0 \pmod{p}$$

по сокращеніи его членовъ и модуля на d будетъ

$$\frac{a}{d}x - \frac{b}{d} \equiv 0 \pmod{\frac{p}{d}},$$

гдѣ $\frac{a}{d}$, $\frac{p}{d}$, $\frac{b}{d}$ числа цѣлыя; притомъ, какъ нетрудно убѣдиться, числа $\frac{a}{d}$, $\frac{p}{d}$ будутъ простыя относительно другъ друга; ибо въ противномъ случаѣ d не было бы общимъ наибольшимъ дѣлителемъ a и p . Но при $\frac{a}{d}$, $\frac{p}{d}$ простыхъ между собою, какъ видѣли, сравненіе

$$\frac{a}{d}x - \frac{b}{d} \equiv 0 \pmod{\frac{p}{d}}$$

имѣетъ всегда рѣшеніе, которое по приемамъ, показаннымъ нами, легко найдется. Пусть же будетъ α число, заключающееся въ рядѣ $0, 1, 2, \dots, \frac{p}{d} - 1$ и удовлетворяющее сравненію

$$\frac{a}{d}x - \frac{b}{d} \equiv 0 \pmod{\frac{p}{d}};$$

всѣ числа удовлетворяющія этому сравненію найдутся изъ слѣдующаго

$$x \equiv \alpha \pmod{\frac{p}{d}}.$$

Эти же числа будутъ удовлетворять и сравненію

$$ax - b \equiv 0 \pmod{p},$$

которое отъ

$$\frac{a}{d}x - \frac{b}{d} \equiv 0 \pmod{\frac{p}{d}}$$

отличается только множителемъ d , общимъ модулю и членамъ сравненія.

И такъ всѣ числа, удовлетворяющія сравненію

$$ax - b \equiv 0 \pmod{p},$$

опредѣляются такъ

$$x \equiv \alpha \pmod{\frac{p}{d}}.$$

На основаніи этого не трудно показать сколько въ рядѣ

$$0, 1, 2, \dots, p - 1$$

чисель, удовлетворяющихъ сравненію $ax - b \equiv 0 \pmod{p}$, чѣмъ и опредѣлится число рѣшеній этого сравненія. Для этого мы находимъ общую формулу чисель, удовлетворяющихъ сравненію

$$x \equiv a \pmod{\frac{p}{d}}.$$

По сказанному нами въ § 11 находимъ, что формула, опредѣляющая эти числа, есть

$$x = a - N \frac{p}{d}.$$

Но эта формула, гдѣ, какъ видѣли, a не < 0 и $< \frac{p}{d}$, даетъ для x значенія не выходящія изъ предѣловъ 0 и $p - 1$ только при $N = 0, -1, -2, \dots, -(d-2), -(d-1)$, поэтому въ рядѣ 0, 1, 2, $p - 1$ числа удовлетворяющія сравненію $x \equiv a \pmod{\frac{p}{d}}$ и слѣд. сравненію $ax - b \equiv 0 \pmod{p}$ суть

$$a, a + \frac{p}{d}, a + \frac{2p}{d}, a + \frac{3p}{d}, \dots, a + \frac{(d-1)p}{d}.$$

А такъ какъ ихъ числомъ d ; то по 14-й теоремѣ сравненіе $ax - b \equiv 0 \pmod{p}$ имѣетъ d рѣшеній, которыя суть

$$x \equiv a, x \equiv a + \frac{p}{d}, x \equiv a + \frac{2p}{d}, \dots, x \equiv a + \frac{(d-1)p}{d} \pmod{p},$$

откуда и слѣдуетъ предложенная теорема.

Такъ сравненіе $15x - 9 \equiv 0 \pmod{12}$, въ которомъ коэффициентъ x и модуль имѣютъ общимъ наибольшимъ дѣлителемъ 3 и членъ не содержащій x дѣлится на 3, имѣетъ три рѣшенія. Чтобы найти ихъ, мы сокращаемъ въ данномъ сравненіи члены и модуль на 3; такимъ образомъ получаемъ сравненіе

$$5x - 3 \equiv 0 \pmod{4}.$$

На основаніи сказаннаго нами въ предыдущемъ параграфѣ мы находимъ, что рѣшеніе его есть

$$x \equiv 3 \cdot 5 \cdot 2^2 \cdot \frac{2-1}{2} - 1 \pmod{4},$$

или

$$x \equiv 15 \pmod{4}.$$

Замѣняя здѣсь 15 его наименьшимъ положительнымъ вычетомъ по модулю 4, находимъ

$$x \equiv 3 \pmod{4}.$$

Отсюда для рѣшенія предложеннаго сравненія получаемъ

$$x \equiv 3, x \equiv 7, x \equiv 11 \pmod{12}.$$

Г Л А В А Ш.

О СРАВНЕНИЯХЪ ВЫСШИХЪ СТЕПЕНЕЙ ВООБЩЕ.

§ 17. Въ этой статьѣ мы ограничимся разсмотрѣнiемъ сравненій съ простыми модулями. По этому общій видъ сравненiй, которыми будемъ заниматься, представится такъ

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Nx + S \equiv 0 \pmod{p},$$

гдѣ p простое число, A, B, C, \dots, N, S какія нибудь числа. Прежде чѣмъ приступимъ къ изслѣдованiю ихъ рѣшенiй, замѣтимъ, что въ нихъ коэффициентъ высшей степени x можетъ быть сдѣланъ единицею. Въ самомъ дѣлѣ, въ сравненiи

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Nx + S \equiv 0 \pmod{p}$$

можетъ быть откинуть всякiй членъ, котораго коэффициентъ дѣлится на p . Такъ если C дѣлится на p ; то по нашему законоположенiю будетъ

$$C \equiv 0 \pmod{p},$$

что по умноженiи на x^{m-2} даетъ

$$Cx^{m-2} \equiv 0 \pmod{p}.$$

Вычитая же это сравненiе изъ

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Nx + S \equiv 0 \pmod{p},$$

мы освободимъ послѣднее отъ члена Cx^{m-2} . Тоже можетъ быть сдѣлано со всякимъ другимъ членомъ, если коэффициентъ его дѣлится на p . Предположимъ теперь, что сравненiе

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Nx + S \equiv 0 \pmod{p}$$

освобождено отъ членовъ, которыхъ коэффициенты дѣлятся на p и Ax^m есть членъ съ высшею степенью x . Въ этомъ слу-

чаѣ A , не будучи кратнымъ p , будетъ простое относительно его; а потому найдется число α , для котораго будетъ

$$A\alpha - 1 \equiv 0 \pmod{p}.$$

Умножая это сравненіе послѣдовательно на

$$Vx^{m-1}, Cx^{m-2}, \dots Hx, S, \text{ найдемъ}$$

$$AB\alpha x^{m-1} - Vx^{m-1} \equiv 0 \pmod{p}.$$

$$AC\alpha x^{m-2} - Cx^{m-2} \equiv 0,$$

.....

$$AH\alpha x - Hx \equiv 0,$$

$$AS\alpha - S \equiv 0.$$

Эти сравненія по сложеніи съ разсматриваемымъ нами

$$Ax^m + Vx^{m-1} + Cx^{m-2} + \dots + Hx + S \equiv 0 \pmod{p}$$

даютъ

$$Ax^m + AB\alpha x^{m-1} + AC\alpha x^{m-2} + \dots + AH\alpha x + AS\alpha \equiv 0 \pmod{p}.$$

Но такъ какъ A число простое съ p ; то это сравненіе можетъ быть сокращено на A ; въ слѣдствіе чего оно приведется къ слѣдующему

$$x^m + V\alpha x^{m-1} + C\alpha x^{m-2} + \dots + H\alpha x + S\alpha \equiv 0 \pmod{p},$$

гдѣ коэффициентъ высшей степени x есть 1, что и слѣдовало сдѣлать.

Такъ для преобразованія сравненія $2x^3 + 3x + 7 \equiv 0 \pmod{11}$ въ другое, въ которомъ бы коэффициентъ высшей степени x былъ равенъ единицѣ, мы должны найти число α , для котораго $2\alpha - 1 \equiv 0 \pmod{11}$. Такое число есть 6. Послѣ того мы къ данному сравненію должны приложить слѣдующія:

$$2.3.6x - 3x \equiv 0 \pmod{11},$$

$$2.7.6 - 7 \equiv 0.$$

Сложивши эти сравненія съ $2x^3 + 3x + 7 \equiv 0 \pmod{11}$ и сдѣлавъ приведеніе, находимъ

$$2x^3 + 2.3.6x + 2.6.7 \equiv 0 \pmod{11};$$

откуда по сокращеніи на 2 получаемъ сравненіе

$$x^3 + 18x + 42 \equiv 0 \pmod{11},$$

гдѣ коэффициентъ высшей степени x есть 1.

§ 18. Относительно сравнений высших степеней докажется следующая теорема:

20. Т Е О Р Е М А.

При p простомъ сравненіе

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + S \equiv 0 \pmod{p}$$

не можетъ имѣть болѣе m рѣшеній.

Доказательство. Для доказательства этой теоремы мы замѣчаемъ, что по § 13-му она справедлива для $m = 1$ т. е. для сравненій первой степени. Чтобы доказать справедливость ея для всякой другой степени, докажемъ, что она должна быть справедлива для сравненій степени m , если справедлива она для сравненій степени $m - 1$.

Чтобы убѣдиться въ этомъ мы допустимъ противное; допустимъ, что сравненіе

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + S \equiv 0 \pmod{p}$$

имѣетъ болѣе m рѣшеній, между тѣмъ какъ сравненія такого же вида степени $m - 1$ болѣе $m - 1$ рѣшеній имѣть не можетъ и докажемъ несообразность этого.

Мы видѣли, что число рѣшеній всякаго сравненія съ модулемъ p опредѣляется числомъ чиселъ въ рядѣ

$$0, 1, 2, \dots, p - 1$$

удовлетворяющихъ сравненію. Поэтому сравненіе

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + S \equiv 0 \pmod{p}$$

можетъ имѣть болѣе m рѣшеній только въ томъ случаѣ, когда ему удовлетворяетъ $m + 1$ чиселъ изъ ряда

$$0, 1, 2, \dots, p - 1.$$

Пусть эти числа будутъ

$$a, a_1, a_2, \dots, a_m.$$

Возьмемъ одно изъ нихъ, напримѣръ a , и разностию $x - a$ будемъ дѣлить

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + S;$$

частное, очевидно, будетъ вида

$$x^{m-1} + B_1 x^{m-2} + C_1 x^{m-3} + \dots + H_1 x + S_1;$$

въ остаткѣ будетъ нѣкоторое число R . Приравнивая дѣлимое произведенію дѣлителя на частное, сложенному съ остаткомъ, найдемъ

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + S = (x - a)(x^{m-1} + B_1 x^{m-2} + C_1 x^{m-3} + \dots + H_1 x + S_1) + R.$$

Въ слѣдствіе чего сравненіе

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + S \equiv 0 \pmod{p}$$

представится такъ

$$(x - a)(x^{m-1} + B_1 x^{m-2} + C_1 x^{m-3} + \dots + H_1 x + S_1) + R \equiv 0 \pmod{p}.$$

Дѣлая здѣсь $x = a$, гдѣ a , по положенію, есть одно изъ чиселъ, удовлетворяющихъ разсматриваемому нами сравненію, найдемъ

$$R \equiv 0 \pmod{p};$$

вычитая же это сравненіе изъ предыдущаго, получаемъ

$$(x - a)(x^{m-1} + B_1 x^{m-2} + C_1 x^{m-3} + \dots + H_1 x + S_1) \equiv 0 \pmod{p} \dots (9)$$

Вотъ къ какому виду приводится разсматриваемое нами сравненіе.

Посмотримъ теперь могутъ ли ему удовлетворять всѣ $m - 1$ чиселъ

$$a, a_1, a_2, \dots, a_m.$$

если сравненіе

$$x^{m-1} + B_1 x^{m-2} + C_1 x^{m-3} + \dots + H_1 x + S_1 \equiv 0 \pmod{p},$$

степени $m - 1$, не имѣетъ болѣе $m - 1$ рѣшеній. Если это сравненіе не имѣетъ болѣе $m - 1$ рѣшеній; то всѣ m чиселъ

$$a_1, a_2, \dots, a_m,$$

взятая нами изъ ряда $0, 1, 2, \dots, p - 1$, не могутъ ему удовлетворять. Пусть будетъ a_1 то число, которое ему не удовлетворяетъ; въ этомъ случаѣ

$$a_1^{m-1} + B_1 a_1^{m-2} + C_1 a_1^{m-3} + \dots + H_1 a_1 + S,$$

не будучи сравнимо съ нулемъ по модулю p , представить число недѣляющееся на p и слѣд. простое съ p ; ибо p число само по себѣ простое. То-же имѣетъ мѣсто относительно разности $a_1 - a$; ибо числа a_1 и a , будучи не болѣе $p - 1$ и не менѣе 0 ,

въ разности не могутъ дать число, дѣлящееся на p . Итакъ числа

$a_1 - a, a_1^{m-1} + B_1 a_1^{m-2} + H_1 a_1^{m-3} + \dots + S_1 a_1 + H_1$
простыя относительно p ; слѣд. простое число относительно p
и произведение ихъ

$(a_1 - a)(a_1^{m-1} + B_1 a_1^{m-2} + H_1 a_1^{m-3} + \dots + S_1 a_1 + H_1)$;
откуда въ противность допущеннаго нами слѣдуетъ, что $x = a_1$
не удовлетворяетъ сравненію (9). Слѣд. сдѣланное нами допущеніе
невозможно, что и слѣдовало доказать.

На основаніи этой теоремы можно доказать слѣдующую бо-
лѣе общую:

21. ТЕОРЕМА.

Если въ сравненіи

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + S \equiv 0 \pmod{p}$$

*не всѣ коэффициенты дѣлятся на p ; то оно болѣе m рѣше-
ній имѣть не можетъ.*

Доказательство. Мы видѣли въ § 17, что въ сравненіи

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + S \equiv 0 \pmod{p}$$

могутъ быть опущены всѣ члены, которыхъ коэффициенты дѣ-
лятся на p . Такимъ опущеніемъ членовъ сравненіе

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + S \equiv 0 \pmod{p}$$

приведется къ тождеству

$$0 \equiv 0 \pmod{p},$$

если всѣ коэффициенты A, B, C, \dots, H, S суть кратные p . Въ
противномъ случаѣ сравненіе

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx \equiv 0 \pmod{p}$$

приведется къ другому, котораго коэффициенты не будутъ дѣ-
литься на p . Дѣлая въ этомъ сравненіи по § 17 коэффициентъ
вышей степени равнымъ единицѣ, мы по предыдущей тео-
ремѣ заключимъ, что оно не имѣетъ болѣе рѣшеній, чѣмъ на-
ходится единицъ въ показателѣ его степени; и слѣд. не имѣ-
етъ болѣе m рѣшеній; ибо, очевидно, сравненіе, получаемое изъ

$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Nx + S \equiv 0 \pmod{p}$
 опушеніемъ какихъ бы то нибыло членовъ, не можетъ быть
 степени болѣе m ; откуда и слѣдуетъ предложенная нами тео-
 рема.

§ 19. На основаніи этой теоремы могутъ быть доказаны
 многія любопытныя свойства чисель.

Такъ можно доказать слѣдующую теорему:

22. ТЕОРЕМА.

Кoeffициенты всѣхъ степеней x въ разложеніи выраженія

$$(x-1)(x-2)(x-3)\dots(x-\overline{p-1}) - x^{p-1} + 1$$

дѣлится на p , если p число простое.

Доказательство. Выраженіе

$$(x-1)(x-2)(x-3)\dots(x-\overline{p-1})$$

обращается въ нуль при $x = 1, 2, 3, \dots, p-1$. Слѣд. всѣ эти
 величины x удовлетворяютъ сравненію

$$(x-1)(x-2)(x-3)\dots(x-\overline{p-1}) \equiv 0 \pmod{p}.$$

По теоремѣ же Фермата эти числа удовлетворяютъ сравненію

$$x^{p-1} - 1 \equiv 0 \pmod{p}.$$

Вычитая это сравненіе изъ предыдущаго, мы находимъ та-
 кое сравненіе

$$(x-1)(x-2)(x-3)\dots(x-\overline{p-1}) - x^{p-1} + 1 \equiv 0 \pmod{p},$$

которому также будутъ удовлетворять числа $1, 2, 3, \dots, p-1$;
 ибо оно получено изъ сравненій, которымъ числа $1, 2, 3, \dots, p-1$
 удовлетворяютъ. Если же сравненію

$$(x-1)(x-2)(x-3)\dots(x-\overline{p-1}) - x^{p-1} + 1 \equiv 0 \pmod{p};$$

удовлетворяютъ числа $1, 2, 3, \dots, p-1$; то оно имѣетъ $p-1$
 рѣшеній

$$x \equiv 1, x \equiv 2, x \equiv 3, \dots, x \equiv p-1 \pmod{p}.$$

А это по предыдущей теоремѣ не иначе можетъ имѣть мѣ-
 сто какъ при дѣлимости на p всѣхъ коэффиціентовъ въ срав-
 неніи

$$(x-1)(x-2)(x-3)\dots(x-\overline{p-1}) - x^{p-1} + 1 \equiv 0 \pmod{p};$$

ибо это сравнение, какъ не трудно замѣтить, степени $p - 2$; откуда и слѣдуетъ предложенная нами теорема.

Посмотримъ теперь къ какимъ сравненіямъ приводитъ насъ эта теорема. Для этого мы замѣчаемъ, что выраженіе

$(x - 1)(x - 2)(x - 3) \dots (x - p - 1) - x^{p-1} + 1$
по выполненіи умноженій и приведеніи членовъ будетъ
 $-(1 + 2 + 3 + \dots + p - 1)x^{p-2} + (1.2 + 1.3 + 2.3 + \dots)x^{p-3} -$
 $(1.2.3 + 2.3.4 + \dots)x^{p-4} + \dots + (-1)^{p-1} 1.2.3 \dots (p-1) + 1$;
слѣдов. по доказанной нами теоремѣ числа

$$\begin{aligned} & 1 + 2 + \dots + p - 1, \\ & 1.2 + 1.3 + 2.3 + \dots, \\ & 1.2.3 + 2.3.4 + \dots, \\ & \dots \\ & (-1)^{p-1} 1.2.3 \dots (p-1) + 1 \end{aligned}$$

будутъ кратныя p , что по нашему знакоположенію представится такими сравненіями

$$\begin{aligned} & 1 + 2 + 3 + \dots + p - 1 \equiv 0, \text{ (mod. } p) \\ & 1.2 + 1.3 + 2.3 + \dots \equiv 0, \\ & 1.2.3 + 2.3.4 + \dots \equiv 0, \\ & \dots \\ & (-1)^{p-1} 1.2.3 \dots (p-1) + 1 \equiv 0. \end{aligned}$$

Вотъ сравненія, которыя будутъ имѣть мѣсто для всякаго простаго числа p . Такъ для $p = 5$ будетъ

$$\begin{aligned} & 1 + 2 + 3 + 4 \equiv 0 \text{ (mod. } 5), \\ & 1.2 + 1.3 + 1.4 + 2.3 + 2.4 + 3.4 \equiv 0, \\ & 1.2.3 + 2.3.4 + 1.2.4 + 1.3.4 \equiv 0, \\ & 1.2.3.4 + 1 \equiv 0. \end{aligned}$$

Особенно замѣчательно здѣсь сравненіе

$$(-1)^{p-1} 1.2.3 \dots (p-1) + 1 \equiv 0 \text{ (mod. } p),$$

которое приводитъ насъ къ слѣдующей теоремѣ, извѣстной подъ названіемъ теоремы Вильсона.

9. ТЕОРЕМА.

Если p число простое; то $1.2.3 \dots (p-1) + 1 \equiv 0 \text{ (mod. } p)$.

Доказательство. Число p можетъ быть или 2 или болѣе 2; въ послѣднемъ случаѣ оно, какъ простое, будетъ всегда не четное. Но сравненіе

$$(-1)^{p-1} 1.2.3 \dots (p-1) + 1 \equiv 0 \pmod{p},$$

справедливое для всякаго простаго числа p , при p не четномъ даетъ

$$1.2.3 \dots (p-1) + 1 \equiv 0 \pmod{p}.$$

Это же сравненіе имѣетъ мѣсто и при $p = 2$; ибо для этой величины p оно приводится къ слѣдующему:

$$- 1 + 1 \equiv 0 \pmod{2},$$

что справедливо. Такъ убѣждаемся въ предложенной нами теоремѣ.

Не трудно доказать, что вообще если m чиселъ $a_1, a_2, a_3, \dots, a_m$, которыя мѣньше p и не менѣе 0, удовлетворяютъ сравненію

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv 0 \pmod{p};$$

то

$$- A(a_1 + a_2 + a_3 + \dots + a_m) \equiv B \pmod{p}$$

$$A(a_1 a_2 + a_1 a_3 + a_2 a_3 + \dots) \equiv C,$$

.....

$$(-1)^{m-1} A(a_1 a_2 \dots a_{m-1} + a_2 a_3 \dots a_m + \dots) \equiv L,$$

$$(-1)^m A a_1 a_2 a_3 \dots a_m \equiv M.$$

Въ самомъ дѣлѣ, числа $a_1, a_2, a_3, \dots, a_m$ обращаютъ въ нуль выраженіе

$$A(x - a_1)(x - a_2)(x - a_3) \dots (x - a_m).$$

Слѣд. эти числа удовлетворяютъ сравненію

$$A(x - a_1)(x - a_2) \dots (x - a_m) \equiv 0 \pmod{p}.$$

Но тѣ же числа по положенію удовлетворяютъ сравненію

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv 0 \pmod{p},$$

а потому удовлетворяютъ они и сравненію

$$A(x - a_1)(x - a_2)(x - a_3) \dots (x - a_m)$$

$$- Ax^m - Bx^{m-1} - Cx^{m-2} - \dots - Lx - M \equiv 0 \pmod{p},$$

получаемому въ разности предыдущихъ сравненій. Но если этоу сравненію удовлетворяютъ m чиселъ $a_1, a_2, a_3, \dots, a_m$, взя-



тыхъ нами изъ ряда $0, 1, 2, 3, \dots, p-1$; то оно имѣетъ m рѣшеній; степень же его меньше m ; ибо въ выраженіи

$$A(x - a_1)(x - a_2)(x - a_3)\dots(x - a_m) \\ - Ax^m - Bx^{m-1} - Cx^{m-2} - \dots - Lx - M$$

членъ съ x^m сокращается. Въ слѣдствіе этого по 21-й теоремѣ мы заключаемъ, что въ сравненіи

$$A(x - a_1)(x - a_2)(x - a_3)\dots(x - a_m) \\ - Ax^m - Bx^{m-1} - Cx^{m-2} - \dots - Lx - M \equiv 0 \pmod{p}$$

коэффициенты всѣхъ степеней x дѣлятся на p . Но въ этомъ сравненіи коэффициенты $x^{m-1}, x^{m-2}, \dots, x, x^0$ суть

$$-A(a_1 + a_2 + a_3 + \dots + a_m) - B,$$

$$A(a_1a_2 + a_1a_3 + a_2a_3 + \dots) - C,$$

$$\dots$$

$$(-1)^{m-1}A(a_1a_2\dots a_{m-1} + a_2a_3\dots a_m + \dots) - L$$

$$(-1)^m Aa_1a_2a_3\dots a_m - M.$$

Слѣд. по принятому нами знаковоложенію будетъ

$$-A(a_1 + a_2 + a_3 + \dots + a_m) - B \equiv 0 \pmod{p},$$

$$A(a_1a_2 + a_1a_3 + a_2a_3 + \dots) - C \equiv 0,$$

$$\dots$$

$$(-1)^{m-1}A(a_1a_2\dots a_{m-1} + a_2a_3\dots a_m + \dots) - L \equiv 0,$$

$$(-1)^m Aa_1a_2a_3\dots a_m - M \equiv 0;$$

откуда и выходятъ сравненія

$$-A(a_1 + a_2 + a_3 + \dots + a_m) \equiv B \pmod{p},$$

$$A(a_1a_2 + a_1a_3 + a_2a_3 + \dots) \equiv C,$$

$$\dots$$

$$(-1)^{m-1}A(a_1a_2\dots a_{m-1} + a_2a_3\dots a_m + \dots) \equiv L,$$

$$(-1)^m Aa_1a_2a_3\dots a_m \equiv M,$$

которыя имѣли въ виду доказать.

Такъ изъ сравненія

$$x^3 + 2x^2 + x - 4 \equiv 0 \pmod{11},$$

которому удовлетворяютъ числа 1, 3, 5, мы найдемъ

$$-(1 + 3 + 5) \equiv 2 \pmod{11},$$

$$1 \cdot 3 + 1 \cdot 5 + 3 \cdot 5 \equiv 1,$$

$$-1 \cdot 3 \cdot 5 \equiv -4.$$

§ 20. Мы доказали, что сравненіе

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + J \equiv 0 \pmod{p}$$

не можетъ имѣть болѣе m рѣшеній. Теперь посмотримъ при какихъ условіяхъ это сравненіе имѣетъ не менѣе m рѣшеній.

При этомъ мы будемъ всегда предполагать m не болѣе $p-1$.

Покажемъ же предварительно, что сравненіе

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv 0 \pmod{p}$$

можетъ быть всегда приведено къ этому виду.

24. ТЕОРЕМА.

Если p число простое; то сравненіе

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv 0 \pmod{p}$$

можетъ быть замѣнено сравненіемъ степени $p-1$

$$A_1x^{p-1} + B_1x^{p-2} + C_1x^{p-3} + \dots + L_1x + M_1 \equiv 0 \pmod{p},$$

идь полиномъ $A_1x^{p-1} + B_1x^{p-2} + C_1x^{p-3} + \dots + L_1x + M_1$ есть остатокъ отъ дѣленія

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + S$$

на $x^p - x$.

Доказательство. Дѣлимъ полиномъ

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + S$$

на $x^p - x$; частное и остатокъ будутъ функціи цѣлыя съ цѣлыми коэффициентами; притомъ степень остатка будетъ меньше степени дѣлителя $x^p - x$; слѣд. не болѣе $p-1$. Пусть же частное этого дѣленія будетъ Φx и

$$A_1x^{p-1} + B_1x^{p-2} + C_1x^{p-3} + \dots + L_1x +$$

остатокъ; приравнивая дѣлимое произведенію дѣлителя на частное сложенному съ остаткомъ, найдемъ

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M =$$

$$\Phi x(x^p - x) + A_1x^{p-1} + B_1x^{p-2} + C_1x^{p-3} + \dots + L_1x + M_1 \dots (10)$$

На основаніи этого уравненія не трудно убѣдиться, что сравненіе

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv 0 \pmod{p}$$

тождественно сравненію

$$A_1x^{p-1} + B_1x^{p-2} + C_1x^{p-3} + \dots + L_1x + M_1 \equiv 0 \pmod{p},$$

Въ самомъ дѣлѣ, выраженіе $x^p - x$ при всѣхъ значеніяхъ x будетъ сравнимо съ 0 по модулю p ; ибо оно очевидно дѣлится на p при x краткомъ p , а при x недѣлящемся на p будетъ $x^{p-1} - 1 \equiv 0 \pmod{p}$ и слѣд. $x^p - x \equiv 0 \pmod{p}$ по теоремѣ Фермата. Изъ этого видно, что при всѣхъ значеніяхъ x будетъ сравнимо съ нулемъ произведеніе $\Phi x(x^p - x)$.

По этому не измѣняя сравненія

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv \pmod{p},$$

мы можемъ вычесть изъ первой части его $\Phi x(x^p - x)$, вслѣдствіе чего оно представится такъ

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M - \Phi x(x^p - x) \equiv 0 \pmod{p},$$

а это по (10) приводится къ слѣдующему

$$A_1 x^{p-1} + B_1 x^{p-2} + C_1 x^{p-3} + \dots + L_1 x + M_1 \equiv 0 \pmod{p},$$

что и требовалось доказать.

На этомъ основаніи мы заключаемъ, что степень сравненія съ модулемъ 2 можетъ быть понижена до 1, съ модулемъ 3 до 2, съ модулемъ 5 до 4, и т. д.

Такъ имѣя сравненіе $x^5 + x^2 - 1 \equiv 0 \pmod{3}$, мы степень его можемъ понизить до 2-хъ. Для этого ищемъ остатокъ отъ дѣленія $x^5 + x^2 - 1$ на $x^3 - x$. Такъ какъ этотъ остатокъ есть $x^2 + x - 1$; то рассматриваемое нами сравненіе замѣнится такимъ

$$x^2 + x - 1 \equiv 0 \pmod{3}.$$

§ 21. Показавши какимъ образомъ степень сравненія съ модулемъ p можетъ быть понижена до $p - 1$, приступимъ теперь къ опредѣленію условій, подъ которыми сравненіе

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv 0 \pmod{p}$$

имѣетъ m рѣшеній, гдѣ m не болѣе $p - 1$. Мы здѣсь предполагаемъ коэффициентъ высшей степени x равнымъ единицею; ибо видѣли, что это можетъ быть сдѣлано во всякомъ сравненіи.

Вотъ теоремы, по которымъ мы всегда узнаемъ имѣетъ ли данное сравненіе столько рѣшеній, сколько въ показателѣ его степени находится единицъ или нѣтъ.

25. Т Е О Р Е М А.

Если сравненіе

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv 0 \pmod{p}$$

имѣетъ m рѣшеній; то въ остаткѣ отъ дѣленія $x^p - x$ на $x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M$ все коэффициенты дѣлятся на p .

Доказательство. Пусть будетъ Fx частное отъ дѣленія $x^p - x$ на $x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M$ и Φx остатокъ отъ этого дѣленія. Приравнивая дѣлимое произведенію дѣлителя на частное, сложенному съ остаткомъ, найдемъ, $x^p - x = Fx(x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M) + \Phi x$; откуда выходитъ

$$x^p - x - Fx(x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M) = \Phi x \dots (11)$$

Возьмемъ теперь сравненіе

$$x^p - x - Fx(x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M) \equiv 0 \pmod{p}$$

и докажемъ, что въ сдѣланныхъ нами предположеніяхъ это сравненіе имѣетъ не менѣе m рѣшеній. Это слѣдуетъ изъ того, что при всѣхъ величинахъ x выраженіе $x^p - x$, какъ видѣли, въ § 20, сравнимо съ 0 по модулю p ; выраженіе же

$$Fx(x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M)$$

становится сравнимымъ съ 0 по модулю p при всѣхъ числахъ, удовлетворяющихъ сравненію

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv 0 \pmod{p};$$

это же сравненіе имѣетъ m рѣшеній по положенію.

И такъ сравненіе

$$x^p - x - Fx(x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M) \equiv 0$$

имѣетъ по крайней мѣрѣ m рѣшеній. Но оно по (11) приводится къ

$$\Phi x \equiv 0 \pmod{p},$$

котораго степень меньше m ; ибо Φx означаетъ у насъ остатокъ отъ дѣленія $x^p - x$ на

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M.$$

*

Убѣдясь такимъ образомъ съ одной стороны, что сравненіе $\Phi x \equiv 0 \pmod{p}$ имѣемъ покрайней мѣрѣ m рѣшеній, а съ другой, что оно степени ниже m , мы по теоремѣ 21-ой заключаемъ, что въ Φx всѣ коэффициенты суть числа кратныя p , въ чемъ и заключается предложенная нами теорема.

Докажемъ теперь обратную этой теоремѣ.

26. Т Е О Р Е М А.

Если остатокъ отъ дѣленія $x^p - x$ на $x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M$ имѣетъ всѣ коэффициенты кратныя p ; то сравненіе

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv 0 \pmod{p}$$

имѣетъ m рѣшеній.

Доказательство. Пусть будутъ Fx и Φx частное и остатокъ отъ дѣленія $x^p - x$ на

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M;$$

остатокъ Φx , по положенію, будетъ имѣть всѣ коэффициенты кратныя p ; поэтому для всякой величины x будетъ

$$\Phi x \equiv 0 \pmod{p}; \dots \dots \dots (12)$$

частное же Fx будетъ цѣлая функція такого вида

$$x^{p-m} + B_1 x^{p-m-1} + \dots \dots \dots$$

Приравнивая дѣлимое произведенію дѣлителя на частное, сложенному съ остаткомъ, найдемъ

$$x^p - x = Fx(x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M) + \Phi x;$$

откуда

$$x^p - x - \Phi x = Fx(x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M).$$

Но такъ какъ по (12) и по сказанному нами выше относительно $x^p - x$ выраженіе $x^p - x - \Phi x$ сравнимо съ нулемъ по модулю p для всѣхъ чиселъ $0, 1, 2, \dots, p-1$; то всѣ эти числа будутъ удовлетворять сравненію

$$Fx(x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M) \equiv 0 \pmod{p};$$

ибо первая часть его по выведенному нами сейчасъ уравненію тождественна разности $x^p - x - \Phi x$.

И такъ всѣ числа $0, 1, 2, \dots, p-1$ удовлетворяютъ сравненію

$$Fx(x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M) \equiv 0 \pmod{p}.$$

Но этому сравненію никакое число не можетъ удовлетворять, не удовлетворяя ни одному изъ сравненій

$$Fx \equiv 0, \quad x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv 0 \pmod{p}.$$

Въ самомъ дѣлѣ, если эти сравненія не удовлетворяются при $x = \alpha$, то $F\alpha$ и $\alpha^m + B\alpha^{m-1} + C\alpha^{m-2} + \dots + L\alpha + M$ суть числа не дѣлящіяся на p , а потому и простыя съ p ; ибо p число само простое. Но если $F\alpha$ и

$$\alpha^m + B\alpha^{m-1} + C\alpha^{m-2} + \dots + L\alpha + M$$

суть числа простыя съ p ; то и произведеніе ихъ

$$F\alpha(\alpha^m + B\alpha^{m-1} + C\alpha^{m-2} + \dots + L\alpha + M)$$

число простое съ p и слѣд. сравненіе

$$Fx(x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M) \equiv 0 \pmod{p}$$

при $x = \alpha$ не удовлетворяется.

И такъ каждое изъ p чиселъ $0, 1, 2, \dots, p-1$ будетъ удовлетворять по крайней мѣрѣ одному изъ сравненій

$$Fx \equiv 0, \quad x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv 0 \pmod{p},$$

а потому если назовемъ черезъ n и n' сколько чиселъ въ рядѣ $0, 1, 2, \dots, p-1$ удовлетворяетъ сравненію $Fx \equiv 0 \pmod{p}$ и

$$x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv 0 \pmod{p};$$

то сумма $n + n'$ будетъ не менѣе p . Притомъ числа n, n' , означая сколько чиселъ въ рядѣ $0, 1, 2, \dots, p-1$ удовлетворяетъ сравненіямъ

$$Fx \equiv 0, \quad x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv 0 \pmod{p},$$

будутъ равны числу рѣшеній этихъ сравненій; слѣд. по теоремѣ 20-й число n' не болѣе m , а n не болѣе $p-m$; ибо, видѣли, Fx есть функція такого вида $x^{p-m} + B_1x^{p-m-1} + \dots$

И такъ числа n, n' , опредѣляющія число рѣшеній сравненій

$$Fx \equiv 0, \quad x^m + Bx^{m-1} + Cx^{m-2} + \dots + Lx + M \equiv 0 \pmod{p},$$

будутъ удовлетворять условіямъ

$$n + n' = > p, \quad n = < p - m, \quad n' = < m.$$

Первыя два условія по исключеніи n даютъ $n' = > m$, а

это въ совокупности съ условіемъ $n' = < m$ обнаруживаетъ равенство $n' = m$. Откуда и слѣдуетъ предположенная теорема.

На основаніи послѣднихъ двухъ теоремъ мы узнаемъ всегда имѣеть ли данное сравненіе столько рѣшеній, сколько въ показателѣ его степени содержится единицъ. Для этого мы, слѣлавъ предварительно коэффициентъ высшей степени x въ данномъ сравненіи равнымъ единицѣ по способу, показанному въ § 17, и называя черезъ p модуль его, дѣлимъ $x^p - x$ на первую часть сравненія. Если остатокъ, получаемый при этомъ дѣленіи, имѣеть всѣ коэффициенты кратные p ; то по послѣдней теоремѣ мы заключимъ, что данное сравненіе имѣеть столько рѣшеній, сколько въ показателѣ его степени содержится единицъ. Въ противномъ же случаѣ по теоремѣ предпослѣдней мы заключимъ, что сравненіе не имѣеть столько рѣшеній.

Напр. чтобы узнать имѣеть ли сравненіе

$$x^5 - x^2 - 2x \equiv 0 \pmod{5}$$

три рѣшенія или нѣтъ, мы дѣлимъ $x^5 - x$ на $x^5 - x^2 - 2x$. Такъ какъ остатокъ этого дѣленія есть $5x^2 - 5x$, гдѣ оба коэффициента дѣлятся на 5, то мы заключаемъ, что рассматриваемое нами сравненіе имѣеть три рѣшенія.

Напротивъ для $x^5 - x$ на $x^5 + x^2 - 2$ и находя въ остаткѣ $x^2 - 3x + 2$, гдѣ коэффициенты не дѣлятся на 5, заключаемъ, что сравненіе

$$x^5 + x^2 - 2 \equiv 0 \pmod{5}$$

имѣеть менѣе трехъ рѣшеній.

ГЛАВА IV.

О СРАВНЕНІЯХЪ ВТОРОЙ СТЕПЕНИ.

§ 22. Общій видъ сравненій второй степени есть

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

Это сравненіе приводится къ сравненіямъ первой степени въ

двухъ случаяхъ. Во первыхъ когда $p = 2$. Въ этомъ случаѣ по 24-й теоремѣ, степень сравненія

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

можетъ быть понижена до 1. Во вторыхъ сравненіе

$$ax + bx + c \equiv 0 \pmod{p}$$

приводится къ первой степени, когда a дѣлится на p ; ибо въ этомъ случаѣ будемъ имѣть

$$a \equiv 0 \pmod{p},$$

что по умноженіи на x^2 дастъ

$$ax^2 \equiv 0 \pmod{p},$$

вычитая же это сравненіе изъ $ax^2 + bx + c \equiv 0 \pmod{p}$, найдемъ $bx + c \equiv 0 \pmod{p}$.

И такъ въ случаѣ $p = 2$ или a кратнаго p сравненіе $ax^2 + bx + c \equiv 0 \pmod{p}$ приводится къ сравненію первой степени, которое рѣшить мы умѣемъ. Обращаемся теперь къ случаю $p \neq 2$ и a не дѣлящаго на p и для упрощенія нашихъ изысканій ограничимся сначала случаемъ p простаго. Мы теперь покажемъ къ чему приводится въ этомъ случаѣ рѣшеніе сравненія

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

Такъ какъ p предполагаемъ числомъ простымъ отличнымъ отъ 2 и a не дѣлящимся на p ; то $4a$ будетъ число простое съ p ; а потому, какъ не трудно убѣдиться, сравненіе $ax^2 + bx + c \equiv 0 \pmod{p}$ будетъ тождественно такому $4a(ax + bx + c) \equiv 0 \pmod{p}$. Въ самомъ дѣлѣ, первое сравненіе предполагаетъ второе; ибо не нарушая сравненія мы можемъ члены его умножить на всякое число; обратно, второе предполагаетъ первое; ибо оно получается изъ втораго сокращеніемъ общаго множителя $4a$, сокращеніемъ позволительнымъ, потому что $4a$ число простое съ p . Но сравненіе $4a(ax^2 + bx + c) \equiv 0 \pmod{p}$ можетъ быть такъ написано

$$(2ax + b)^2 - b^2 + 4ac \equiv 0 \pmod{p}.$$

Откуда выводимъ

$$z^2 \equiv b^2 - 4ac \pmod{p},$$

предполагая

$$z = 2ax + b.$$

Изъ этого мы видимъ, что рѣшеніе сравненія

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

приводится къ рѣшенію сравненія

$$z^2 \equiv b^2 - 4ac \pmod{p}$$

и опредѣленію x по уравненію

$$2ax + b = z.$$

Но что касается до опредѣленія x по уравненію $2ax + b = z$, когда рѣшеніемъ сравненія $z^2 \equiv b^2 - 4ac \pmod{p}$ найдено z ; то оно сводится на рѣшеніе сравненія первой степени. Въ самомъ дѣлѣ, рѣшеніе сравненія $z^2 \equiv b^2 - 4ac \pmod{p}$, по замѣченному нами вообще о рѣшеніи сравненій $fx \equiv 0 \pmod{p}$, гдѣ fx цѣлая функція x съ цѣлыми коэффициентами, представится однимъ или нѣсколькими сравненіями вида

$$z \equiv a \pmod{p}.$$

Въ слѣдствіе чего для опредѣленія неизвѣстнаго x , связаннаго съ z уравненіемъ $2ax + b = z$, будемъ имѣть

$$2ax + b \equiv a \pmod{p}.$$

Это сравненіе, какъ первой степени, мы рѣшать умѣемъ; замѣтимъ также, что оно, въ сдѣланныхъ нами предположеніяхъ, будетъ всегда имѣть одно рѣшеніе; ибо здѣсь $2a$ и p будутъ числа относительно другъ друга простыя.

Итакъ вся трудность рѣшенія сравненія

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

заключается въ рѣшеніи сравненія

$$z^2 \equiv b^2 - 4ac \pmod{p};$$

этимъ сравненіемъ мы теперь и займемся. Мы его будемъ писать такъ

$$z^2 \equiv q \pmod{p},$$

пологая для сокращенія $b^2 - 4ac \equiv q$.

Разсматривая сравненіе

$$z^2 \equiv q \pmod{p},$$

мы замѣчаемъ, что оно при $q \equiv 0 \pmod{p}$ будетъ удовлетво-
ряться предположеніемъ $z \equiv 0 \pmod{p}$. Не трудно также убѣ-
диться, что въ этомъ случаѣ $z \equiv 0 \pmod{p}$ есть единственное
рѣшеніе сравненія $z^2 \equiv q \pmod{p}$. Въ самомъ дѣлѣ, если q срав-
нимо съ нулемъ по модулю p ; то сравненіе $z^2 \equiv q \pmod{p}$ вы-
ражаетъ дѣлимость z^2 на p . Но p , будучи числомъ простымъ,
не можетъ дѣлиться на квадратъ какого либо числа; слѣд. по
6-ой теоремѣ дѣлимость z^2 на p предполагаетъ дѣлимость z
на p , а это выражается сравненіемъ

$$z \equiv 0 \pmod{p}.$$

Итакъ если q сравнимо съ нулемъ по модулю p ; то срав-
неніе $z^2 \equiv q \pmod{p}$ имѣетъ одно только рѣшеніе $z \equiv 0 \pmod{p}$.

Переходимъ теперѣ къ случаю q несравнимаго съ нулемъ
по модулю p ; въ этомъ случаѣ относительно рѣшеній сравне-
нія $z^2 \equiv q \pmod{p}$ будетъ имѣть мѣсто слѣдующая теорема:

27. ТЕОРЕМА.

*Если q не сравнимо съ нулемъ по модулю p ; то сравне-
ніе $z^2 \equiv q \pmod{p}$ или не имѣетъ рѣшенія или имѣетъ два
рѣшенія.*

Доказательство. Мы видѣли, что вообще сравненіе $fx \equiv 0$
 \pmod{p} имѣетъ столько рѣшеній, сколько чиселъ въ рядѣ
 $0, 1, 2, \dots, p-1$ ему удовлетворяетъ. На основаніи этого не
трудно доказать, что сравненіе $z^2 \equiv q \pmod{p}$ при $q \not\equiv 0$
 \pmod{p} не можетъ имѣть одно только рѣшеніе. Въ самомъ дѣлѣ,
пусть будетъ α то число, которое въ рядѣ $0, 1, 2, \dots, p-1$
удовлетворяетъ сравненію $z^2 \equiv q \pmod{p}$. Число α не можетъ
быть нулемъ; ибо, дѣлая въ сравненіи $z^2 \equiv q \pmod{p}$ число z
равнымъ нулю, находимъ $0 \equiv q \pmod{p}$, что противно положе-
нію. Итакъ α будетъ однимъ изъ чиселъ $1, 2, \dots, p-1$.

Но не трудно убѣдиться, что если α удовлетворяетъ срав-
ненію $z^2 \equiv q \pmod{p}$; то $p - \alpha$ будетъ также удовлетворять
ему; ибо $(p - \alpha)^2$, какъ равное $p^2 - 2\alpha p + \alpha^2$, сравнимо съ α^2
по модулю p . Слѣдовательно $p - \alpha$ будетъ опредѣлять второе

рѣшеніе сравненія $z^2 \equiv q \pmod{p}$, если число $p - a$ заключается въ рядѣ

$$0, 1, 2, \dots, p - 1$$

и отлично отъ a . Но первое слѣдуетъ изъ того, что a не болѣе p и не менѣе 1; второе же необходимо должно имѣть мѣсто, потому что въ противномъ случаѣ было бы $p - a = a$, и слѣд. $2a = p$, что не возможно; ибо p число простое отличное отъ 2, а потому четнымъ быть не можетъ.

Итакъ если въ рядѣ найдется одно число удовлетворяющее сравненію $z^2 \equiv q \pmod{p}$; то найдется и другое ему удовлетворяющее. Слѣд. это сравненіе не можетъ имѣть одно только рѣшеніе. Но это сравненіе, будучи второй степени, не можетъ имѣть также болѣе двухъ рѣшеній; слѣдовательно оно должно имѣть или два рѣшенія или не одного, что и слѣдовало доказать.

§ 23. Мы займемся теперь изслѣдованіемъ признаковъ, по которымъ можно узнать, что сравненіе $z^2 \equiv q \pmod{p}$, гдѣ предполагаемъ $q \not\equiv 0 \pmod{p}$, имѣетъ ли два рѣшенія или нѣтъ.

На основаніи теоремъ, доказанныхъ нами въ § 21, не трудно узнать имѣетъ ли данное сравненіе $z^2 \equiv q \pmod{p}$ два рѣшенія или нѣтъ. Для этого мы должны найти остатокъ, получаемый при дѣленіи $z^p - z$ на $z^2 - q$. Чтобы найти этотъ остатокъ мы дѣлимое $z^p - z$ представляемъ такъ

$$z \left[(z^2)^{\frac{p-1}{2}} - q^{\frac{p-1}{2}} \right] + z \left[q^{\frac{p-1}{2}} - 1 \right]$$

и замѣчаемъ, что $(z^2)^{\frac{p-1}{2}} - q^{\frac{p-1}{2}}$ дѣлится на $z^2 - q$. Слѣд. при дѣленіи этого выраженія на $z^2 - q$ остатокъ будетъ

$$z \left[q^{\frac{p-1}{2}} - 1 \right].$$

Отсюда по теоремѣ 26-й мы заключаемъ, что сравненіе $z^2 \equiv q$

\pmod{p} имѣетъ два рѣшенія, если $q^{\frac{p-1}{2}} - 1$ дѣлится на p , или, что одно и то же по нашему законоположенію, если имѣетъ мѣсто сравненіе

$$q^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Если же это сравнение не удовлетворяется и слѣд. $q^{\frac{p-1}{2}} - 1$ не дѣлится на p ; то по теоремѣ 25-й заключимъ, что сравненіе $z^2 \equiv q \pmod{p}$ не имѣетъ двухъ рѣшеній, а потому оно не можетъ имѣть и не одного рѣшенія; ибо по теоремѣ 27-й это сравненіе или имѣетъ два рѣшенія или не имѣетъ не одного.

Итакъ сравненіе $z^2 \equiv q \pmod{p}$ имѣетъ два рѣшенія или не имѣетъ не одного, смотря по тому будетъ ли

$$q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

или это сравненіе не будетъ имѣть мѣста. Въ первомъ случаѣ мы будемъ говорить, что сравненіе $z^2 \equiv q \pmod{p}$ возможно; во второмъ, что оно невозможно.

Припомнимъ здѣсь, что все это выведено нами въ предположеніяхъ, что p число простое, отличное отъ 2, а q какое нибудь число положительное или отрицательное, не дѣлящееся на p .

Такъ, чтобы узнать имѣетъ ли сравненіе $z^2 \equiv 3 \pmod{5}$ рѣшенія или нѣтъ, мы возводимъ 3 въ степень $\frac{5-1}{2}$, или 2. Находя, что 3^2 не сравнимо съ 1 по модулю 5, мы заключаемъ, что сравненіе $z^2 \equiv 3 \pmod{5}$ не имѣетъ рѣшенія, другими словами, это сравненіе невозможно.

Напротивъ мы убѣждаемся, что сравненіе $z^2 \equiv 2 \pmod{7}$ имѣетъ рѣшенія, находя, что $2^{\frac{7-1}{2}} \equiv 8$ и 8 сравнимо съ 1 по модулю 7.

§. 24. Если p и q не велики, то не трудно узнать удовлетворяется ли сравненіе $q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ или нѣтъ. Но это становится весьма труднымъ, когда p и q большія числа. Мы покажемъ теперь какимъ образомъ, не вычисляя значенія $q^{\frac{p-1}{2}}$, можно рѣшить удовлетворяется ли сравненіе $q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

или нѣтъ и чрезъ то узнать имѣтъ ли рѣшенія сравненіе $z^2 \equiv q \pmod{p}$ или нѣтъ. Съ этою цѣлію мы докажемъ теперь, что если q не дѣлится p и p число простое, отличное отъ 2, какъ мы и предполагали, то число $q^{\frac{p-1}{2}}$ удовлетворяетъ всегда одному изъ двухъ сравненій

$$q^{\frac{p-1}{2}} \equiv 1, \quad q^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Въ самомъ дѣлѣ, если ни одно изъ этихъ сравненій не удовлетворяется; то ни число $q^{\frac{p-1}{2}} - 1$ ни число $q^{\frac{p-1}{2}} + 1$ не дѣлится на p ; и слѣд. оба они простыя съ p ; ибо p само по себѣ простое число. Но если оба числа $q^{\frac{p-1}{2}} - 1, q^{\frac{p-1}{2}} + 1$ суть простыя съ p , то и произведеніе ихъ $(q^{\frac{p-1}{2}} - 1)(q^{\frac{p-1}{2}} + 1)$, или $q^{p-1} - 1$ число простое съ p ; а это не справедливо; ибо по теоремѣ Фермата разность $q^{p-1} - 1$ дѣлится на p . Итакъ одно изъ двухъ сравненій

$$q^{\frac{p-1}{2}} \equiv 1, \quad q^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

необходимо должно удовлетвориться. Съ другой стороны не трудно убѣдиться, что оба эти сравненія въ одно время не могутъ имѣть мѣсто; ибо допустивши ихъ, мы находимъ $1 \equiv -1 \pmod{p}$, откуда $2 \equiv 0 \pmod{p}$, что не возможно; ибо p , предполагаемое отличнымъ отъ 2, дѣлится 2 не можетъ.

Изъ сказаннаго нами слѣдуетъ, что возможность удовлетворить сравненію $z^2 \equiv q \pmod{p}$ опредѣляется знакомъ, съ которымъ сравненіе

$$q^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

удовлетворяется. Если оно удовлетворяется съ $+$; то сравненіе $z^2 \equiv q \pmod{p}$ имѣетъ рѣшенія, и въ этомъ случаѣ число q называютъ *квадратичнымъ вычетомъ* числа p ; въ противномъ случаѣ, если сравненіе $q^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ удовлетворяется съ знакомъ $-$, сравненіе $z^2 \equiv q \pmod{p}$ не имѣетъ рѣшенія и число q называютъ *неквадратичнымъ вычетомъ* числа p . Кромѣ того для

сокращенія письма вмѣсто того, чтобы писать p и q удовлетворяютъ сравненію $q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, [что, какъ видѣли, есть признакъ возможности сравненія $z^2 \equiv q \pmod{p}$] согласились писать

$$\left(\frac{q}{p}\right) = 1,$$

въ противномъ же случаѣ, если $q^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, пишутъ

$$\left(\frac{q}{p}\right) = -1.$$

По этому знакоположенію $\left(\frac{q}{p}\right)$ будетъ означать 1 съ тѣмъ изъ двухъ знаковъ \pm , съ которымъ она удовлетворяетъ сравненію $q^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$, и слѣд. значеніе этого символа вполне будетъ определено сравненіемъ $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$ и условіемъ, что численная величина $\left(\frac{q}{p}\right)$ есть 1.

Такъ мы нашли, что сравненіе $q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ удовлетворяется при $q = 2, p = 7$. Слѣд. по нашему знакоположенію будетъ

$$\left(\frac{2}{7}\right) = 1.$$

Напротивъ мы видѣли, что $3^{\frac{5-1}{2}}$ по модулю 5 сравнимо съ -1 ; слѣд.

$$\left(\frac{3}{5}\right) = -1.$$

Такимъ образомъ изъ $\left(\frac{2}{7}\right) = 1$ мы заключаемъ объ возможности рѣшить сравненіе $z^2 \equiv 2 \pmod{7}$ и число 2 называемъ квадратичнымъ вычетомъ 7. Напротивъ изъ равенства $\left(\frac{3}{5}\right) = -1$ заключимъ, что сравненіе $x^2 \equiv 3 \pmod{5}$ не имѣетъ рѣшенія и слѣдовательно 3 будетъ неквадратичный вычетъ 5.

§ 25. Показавши значеніе символа $\left(\frac{q}{p}\right)$, мы приступимъ теперь къ раскрытію его свойствъ. Для этого мы докажемъ слѣдующія теоремы:

28. Т Е О Р Е М А.

Величина символа $\left(\frac{1}{p}\right)$ есть 1, а символа $\left(\frac{-1}{p}\right)$ есть $(-1)^{\frac{p-1}{2}}$.

Доказательство. Мы видѣли, что символъ $\left(\frac{q}{p}\right)$ удовлетворяетъ сравненію $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$.

Для я здѣсь послѣдовательно $q = 1$ и $q = -1$, находимъ

$$1 \equiv \left(\frac{1}{p}\right), \quad (-1)^{\frac{p-1}{2}} \equiv \left(\frac{-1}{p}\right) \pmod{p},$$

или $1 - \left(\frac{1}{p}\right) \equiv 0, \quad (-1)^{\frac{p-1}{2}} - \left(\frac{-1}{p}\right) \equiv 0 \pmod{p}.$

Такъ какъ численная величина значений символовъ $\left(\frac{1}{p}\right), \left(\frac{-1}{p}\right)$ есть 1; то разности $1 - \left(\frac{1}{p}\right), (-1)^{\frac{p-1}{2}} - \left(\frac{-1}{p}\right)$ при неравенствѣ

$\left(\frac{1}{p}\right)$ съ 1, $\left(\frac{-1}{p}\right)$ съ $(-1)^{\frac{p-1}{2}}$ приведутся или къ 2 или къ -2 ; но ни 2 ни -2 несравнимо съ 0 по модулю p ; ибо p отлично отъ двухъ. Слѣд. нельзя допустить неравенства

$\left(\frac{1}{p}\right)$ съ 1, $\left(\frac{-1}{p}\right)$ съ $(-1)^{\frac{p-1}{2}}$; откуда и слѣдуетъ предложенная нами теорема.

На основаніи этой теоремы мы заключаемъ, что $\left(\frac{1}{5}\right) = 1, \left(\frac{-1}{5}\right) = 1, \left(\frac{-1}{11}\right) = -1.$

29. Т Е О Р Е М А.

Если Q есть произведеніе чиселъ q_1, q_2, \dots, q_n ; то

$$\left(\frac{Q}{p}\right) = \left(\frac{q_1}{p}\right) \left(\frac{q_2}{p}\right) \dots \left(\frac{q_n}{p}\right).$$

Доказательство. Символы $\left(\frac{Q}{p}\right), \left(\frac{q_1}{p}\right), \left(\frac{q_2}{p}\right) \dots \left(\frac{q_n}{p}\right)$, какъ видѣли, удовлетворяютъ сравненіямъ

$$Q^{\frac{p-1}{2}} \equiv \left(\frac{Q}{p}\right), \quad q_1^{\frac{p-1}{2}} \equiv \left(\frac{q_1}{p}\right), \quad q_2^{\frac{p-1}{2}} \equiv \left(\frac{q_2}{p}\right), \dots, q_n^{\frac{p-1}{2}} \equiv \left(\frac{q_n}{p}\right) \pmod{p}$$

Перемножая все эти сравнения кроме первого между собою, находимъ

$$q_1^{\frac{p-1}{2}} q_2^{\frac{p-1}{2}} \dots q_n^{\frac{p-1}{2}} \equiv \left(\frac{q_1}{p}\right) \left(\frac{q_2}{p}\right) \dots \left(\frac{q_n}{p}\right) \pmod{p},$$

или, что одно и то же,

$$[q_1 q_2 \dots q_n]^{\frac{p-1}{2}} \equiv \left(\frac{q_1}{p}\right) \left(\frac{q_2}{p}\right) \dots \left(\frac{q_n}{p}\right) \pmod{p}.$$

Но по положению произведение $q_1 q_2 \dots q_n$ равно Q ; въ слѣдствіе чего предыдущее сравнение представится такъ

$$Q^{\frac{p-1}{2}} \equiv \left(\frac{q_1}{p}\right) \left(\frac{q_2}{p}\right) \dots \left(\frac{q_n}{p}\right) \pmod{p}.$$

Но мы видѣли, что $Q^{\frac{p-1}{2}} \equiv \left(\frac{Q}{p}\right) \pmod{p}$.

Это сравненіе вмѣстѣ съ предыдущимъ дастъ

$$\left(\frac{Q}{p}\right) \equiv \left(\frac{q_1}{p}\right) \left(\frac{q_2}{p}\right) \dots \left(\frac{q_n}{p}\right) \pmod{p},$$

или
$$\left(\frac{Q}{p}\right) - \left(\frac{q_1}{p}\right) \left(\frac{q_2}{p}\right) \dots \left(\frac{q_n}{p}\right) \equiv 0 \pmod{p}.$$

Но такъ какъ численная величина символовъ

$$\left(\frac{Q}{p}\right), \left(\frac{q_1}{p}\right), \left(\frac{q_2}{p}\right), \dots \left(\frac{q_n}{p}\right)$$

есть 1; то разность выражений $\left(\frac{Q}{p}\right)$ и $\left(\frac{q_1}{p}\right) \left(\frac{q_2}{p}\right) \dots \left(\frac{q_n}{p}\right)$ въ случаѣ неравенства ихъ приведется или $+2$ или -2 . Но ни въ томъ ни въ другомъ случаѣ предыдущее сравненіе не можетъ имѣть мѣста; ибо p число отличное отъ 2. Итакъ нельзя допустить неравенства величинъ $\left(\frac{Q}{p}\right), \left(\frac{q_1}{p}\right) \left(\frac{q_2}{p}\right) \dots \left(\frac{q_n}{p}\right)$; откуда и слѣдуетъ предложенная нами теорема.

На основаніи этой теоремы опредѣленіе символа $\left(\frac{Q}{p}\right)$ при Q составномъ сводится на опредѣленіе символовъ

$$\left(\frac{q_1}{p}\right), \left(\frac{q_2}{p}\right) \dots \left(\frac{q_n}{p}\right),$$

гдѣ q_1, q_2, \dots, q_n простые числа составляющія Q . Такъ желая опредѣлить $\left(\frac{15}{7}\right), \left(\frac{30}{101}\right)$, найдемъ, что

$$\left(\frac{15}{7}\right) = \left(\frac{3}{7}\right) \left(\frac{5}{7}\right), \quad \left(\frac{30}{101}\right) = \left(\frac{2}{101}\right) \left(\frac{3}{101}\right) \left(\frac{5}{101}\right).$$

На основаніи этой же теоремы мы заключаемъ о такомъ равенствѣ

$$\left(\frac{q^n}{p}\right) = \left(\frac{q}{p}\right)^n.$$

Чтобы вывести это изъ доказанной нами теоремы стоить принять числа q_1, q_2, \dots, q_n за равныя q . Въ этомъ случаѣ уравненіе

$$\left(\frac{Q}{p}\right) = \left(\frac{q_1}{p}\right) \left(\frac{q_2}{p}\right) \dots \dots \dots \left(\frac{q_n}{p}\right)$$

намъ дастъ

$$\left(\frac{Q}{p}\right) = \left(\frac{q}{p}\right)^n,$$

число же Q , равное произведенію $q_1 q_2 \dots q_n$, приведетъ къ q^n .

Такъ найдемъ, что

$$\left(\frac{27}{5}\right) = \left(\frac{3^3}{5}\right) = \left(\frac{3}{5}\right)^3, \quad \left(\frac{32}{7}\right) = \left(\frac{2^5}{7}\right) = \left(\frac{2}{7}\right)^5.$$

Въ частномъ случаѣ $n = 2$ мы изъ уравненія

$$\left(\frac{q^n}{p}\right) = \left(\frac{q}{p}\right)^n$$

выводимъ

$$\left(\frac{q^2}{p}\right) = \left(\frac{q}{p}\right)^2.$$

Но будетъ ли $\left(\frac{q}{p}\right)$ равно $+1$ или -1 , всегда квадратъ его будетъ 1 ; слѣд.

$$\left(\frac{q^2}{p}\right) = 1.$$

Это свойство символа $\left(\frac{Q}{p}\right)$ можетъ служить къ значительнымъ упрощеніямъ при опредѣленіи ихъ величинъ. По доказанной нами теоремѣ мы имѣемъ

$$\left(\frac{Nq^2}{p}\right) = \left(\frac{N}{p}\right) \left(\frac{q^2}{p}\right);$$

куда внеся значеніе $\left(\frac{q^2}{p}\right)$ изъ предыдущаго уравненія, находимъ

$$\left(\frac{Nq^2}{p}\right) = \left(\frac{N}{p}\right).$$

На основаніи этого равенства мы заключаемъ, что при опре-

дѣленіи величины символа $\left(\frac{Q}{p}\right)$ мы можемъ исключать изъ Q всякій множитель, составляющій точный квадратъ.

Такъ опредѣленіе $\left(\frac{45}{7}\right)$ сводится на опредѣленіе $\left(\frac{5}{7}\right)$; опредѣленіе $\left(\frac{8}{5}\right)$ на опредѣленіе $\left(\frac{2}{5}\right)$

Прежде чѣмъ пойдемъ далѣе замѣтимъ, что на основаніи доказанныхъ нами теоремъ относительно символа $\left(\frac{q}{p}\right)$ значеніе $\left(\frac{-q}{p}\right)$ по $\left(\frac{q}{p}\right)$ опредѣляется уравненіемъ

$$\left(\frac{-q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right).$$

Въ самомъ дѣлѣ, на основаніи послѣдней теоремы, рассматривая $-q$ какъ произведеніе -1 и q , находимъ

$$\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{q}{p}\right);$$

куда внеся значеніе $\left(\frac{-1}{p}\right)$ по 28-й теоремѣ, имѣемъ

$$\left(\frac{-q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right),$$

что и слѣдовало доказать.

Такъ находимъ $\left(\frac{-3}{5}\right) = (-1)^{\frac{5-1}{2}} \left(\frac{3}{5}\right) = \left(\frac{3}{5}\right)$;

$$\left(\frac{-2}{7}\right) = (-1)^{\frac{7-1}{2}} \left(\frac{2}{7}\right) = -\left(\frac{2}{7}\right).$$

30. ТЕОРЕМА.

Если q и q_1 сравнимы по модулю p ; то $\left(\frac{q}{p}\right) = \left(\frac{q_1}{p}\right)$.

Доказательство. По положенію числа q и q_1 сравнимы по модулю p . Но изъ сравненія

$$q \equiv q_1 \pmod{p},$$

по возведеніи обѣихъ частей его въ степень $\frac{p-1}{2}$, имѣемъ

$$q^{\frac{p-1}{2}} \equiv q_1^{\frac{p-1}{2}} \pmod{p}.$$

Символы же $\left(\frac{q}{p}\right)$, $\left(\frac{q_1}{p}\right)$ удовлетворяют сравненіямъ

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right), \quad q_1^{\frac{p-1}{2}} \equiv \left(\frac{q_1}{p}\right) \pmod{p}.$$

Въ слѣдствіе чего предыдущее сравненіе даетъ

$$\left(\frac{q}{p}\right) \equiv \left(\frac{q_1}{p}\right) \pmod{p},$$

или

$$\left(\frac{q}{p}\right) - \left(\frac{q_1}{p}\right) \equiv 0 \pmod{p}.$$

Но такъ какъ численная величина $\left(\frac{q}{p}\right)$ и $\left(\frac{q_1}{p}\right)$ есть 1; то первая часть этого сравненія, въ случаѣ неравенства значений $\left(\frac{q}{p}\right)$ и $\left(\frac{q_1}{p}\right)$, будетъ + 2 или - 2, что невозможно; ибо p от- лично отъ 2. Слѣд. оба эти символа должны имѣть одну вели- чину, что и слѣдовало доказать.

$$\text{Такъ находимъ, что } \left(\frac{23}{7}\right) = \left(\frac{23-7}{7}\right) = \left(\frac{23-2 \cdot 7}{7}\right).$$

На основаніи этой теоремы мы заключаемъ, что символъ $\left(\frac{q}{p}\right)$ равенъ $\left(\frac{r}{p}\right)$, если r есть остатокъ отъ дѣленія q на p ; ибо, какъ замѣтили въ § 8, остатокъ сравнимъ съ дѣлимимъ, когда за модуль принять дѣлитель. Такимъ образомъ замѣняя въ сим- волаѣ $\left(\frac{q}{p}\right)$ число q остаткомъ отъ дѣленія q на p , мы вмѣсто $\left(\frac{q}{p}\right)$ будемъ имѣть $\left(\frac{r}{p}\right)$, гдѣ $r < p$.

§ 26. Вотъ теоремы, которыя послужатъ намъ для того, чтобы опредѣленіе какого либо символа $\left(\frac{Q}{p}\right)$ привести къ опре- дѣленію символовъ вида $\left(\frac{q}{p}\right)$, гдѣ q число положительное, про- стое и меньше p . Что же касается до опредѣленія символа $\left(\frac{q}{p}\right)$, когда q число положительное, простое и меньше p , то оно бу- детъ основываться на слѣдующихъ теоремахъ:

31. Т Е О Р Е М А.

Если мы согласимся изображать наибольшее целое число, заключающееся в данномъ количествѣ, знакомъ E , поставленнымъ передъ нимъ; то значеніе $\left(\frac{q}{p}\right)$ опредѣлится уравненіемъ

$$\left(\frac{q}{p}\right) = (-1)^{E \frac{2q}{p} + E \frac{4q}{p} + \dots + E \frac{(p-1)q}{p}}.$$

Доказательство. Нетрудно убѣдиться, что при p нечетномъ и a положительномъ можно найти положительное число z , которое, будучи меньше $\frac{p}{2}$, удовлетворитъ условію

$$z \equiv (-1)^{E \frac{2a}{p}} a \pmod{p} \dots \dots \dots (13)$$

Въ самомъ дѣлѣ, если $E \frac{2a}{p}$ число четное; то это сравненіе принимаетъ такой видъ

$$z \equiv a \pmod{p}.$$

Но въ этомъ случаѣ $\frac{1}{2} E \frac{2a}{p}$ будетъ число цѣлое; а потому $a - \frac{1}{2} p E \frac{2a}{p}$ будетъ число цѣлое, удовлетворяющее сравненію

$$z \equiv a \pmod{p}.$$

Это же число, которое можетъ быть представлено такъ

$$\frac{p}{2} \left(\frac{2a}{p} - E \frac{2a}{p} \right),$$

будетъ количествомъ положительнымъ и меньшимъ $\frac{p}{2}$; ибо по значенію $E \frac{2a}{p}$ разность $\frac{2a}{p} - E \frac{2a}{p}$ должна быть не менѣе 0 и меньше 1.

Обращаемся теперь къ тому случаю, когда $E \frac{2a}{p}$ число нечетное. Если $E \frac{2a}{p}$ число нечетное, то сравненіе (13) принимаетъ такой видъ

$$z \equiv -a \pmod{p}.$$

Но въ этомъ случаѣ $\frac{1 + E \frac{2a}{p}}{2}$ есть число цѣлое; а потому предыдущему сравненію удовлетворимъ, полагая

*

$$z = \frac{1}{2} p \left(1 + E \frac{2a}{p} \right) - a,$$

а это число, которое иначе представится такъ

$$\frac{p}{2} \left[1 - \left(\frac{2a}{p} - E \frac{2a}{p} \right) \right],$$

очевидно, положительное и небольшое $\frac{p}{2}$; ибо, какъ замѣчали

выше, разность $\frac{2a}{p} - E \frac{2a}{p}$ не выходитъ изъ предѣловъ 0 и 1.

Убѣдившись такимъ образомъ въ возможности всегда удовлетворить условіямъ

$$z \equiv (-1)^{E \frac{2a}{p}} a \pmod{p}, \quad z \text{ не } < 0 \text{ и } < \frac{p}{2},$$

назовемъ черезъ $z_1, z_2, \dots, z_{\frac{p-1}{2}}$ числа, удовлетворяющія имъ въ

предположеніяхъ $a=q, a=2q, \dots, a=\frac{p-1}{2}q$. Эти числа будутъ удовлетворять сравненіямъ

$$z_1 \equiv (-1)^{E \frac{2q}{p}} q, z_2 \equiv (-1)^{E \frac{4q}{p}} 2q, \dots, z_{\frac{p-1}{2}} \equiv (-1)^{E \frac{(p-1)q}{p}} \frac{p-1}{2} q \pmod{p}, \dots (14)$$

которыя по перемноженіи даютъ

$$z_1 z_2 \dots z_{\frac{p-1}{2}} \equiv (-1)^{E \frac{2a}{p} + E \frac{4a}{p} + \dots + E \frac{(p-1)q}{p}} 1 \cdot 2 \dots \frac{p-1}{2} q^{\frac{p-1}{2}} \pmod{p} \dots (15).$$

Но не трудно убѣдиться, что произведеніе $z_1 z_2 \dots z_{\frac{p-1}{2}}$ равно

произведенію $1 \cdot 2 \dots \frac{p-1}{2}$. Для этого мы замѣчаемъ, что числа

$z_1, z_2, \dots, z_{\frac{p-1}{2}}$, будучи меньше $\frac{p}{2}$ и не меньше 0, могутъ имѣть

только значенія

$$0, 1, 2, \dots, \frac{p-1}{2}.$$

Потомъ мы замѣчаемъ, что ни одно изъ нихъ не можетъ быть нулемъ; ибо въ противномъ случаѣ предыдущее сравненіе

предполагало бы дѣлимость $1, 2, \dots, \frac{p-1}{2}$ на p ; между тѣмъ какъ $1, 2, \dots, \frac{p-1}{2}$ числа простые съ p . Итакъ числа $z_1, z_2, \dots, z_{\frac{p-1}{2}}$ могутъ равняться только числамъ

$$1, 2, \dots, \frac{p-1}{2}.$$

Также не трудно показать, что въ рядѣ $z_1, z_2, \dots, z_{\frac{p-1}{2}}$ нѣтъ двухъ чиселъ равныхъ. Въ самомъ дѣлѣ, если мы допустимъ, что здѣсь z_m и z_μ равны, гдѣ m и μ какія нибудь два числа, содержащіяся въ рядѣ $1, 2, \dots, \frac{p-1}{2}$; то имѣя по (14)

$$z_m \equiv (-1)^{\frac{2qm}{p}} mq, \quad z_\mu \equiv (-1)^{\frac{2q\mu}{p}} \mu q \pmod{p},$$

мы бы нашли

$$(-1)^{\frac{2qm}{p}} mq \equiv (-1)^{\frac{2q\mu}{p}} \mu q \pmod{p}.$$

Но это сравненіе по сокращеніи на q , число простое съ p , даетъ

$$(-1)^{\frac{2qm}{p}} m \equiv (-1)^{\frac{2q\mu}{p}} \mu \pmod{p},$$

что, очевидно, невозможно; ибо оно предполагаетъ дѣлимость разности

$$(-1)^{\frac{2qm}{p}} m - (-1)^{\frac{2q\mu}{p}} \mu$$

на p ; а эта разность приводится къ одному изъ четырехъ:

$$m + \mu, \quad -(m + \mu), \quad m - \mu, \quad -(m - \mu),$$

и такъ какъ числа m, μ взяты нами изъ ряда $1, 2, \dots, \frac{p-1}{2}$ и не равны между собою; то сумма ихъ меньше p , а разность не равна нулю; слѣд. ни то, ни другое не дѣлится на p .

Такъ убѣждаемся мы, что въ составъ ряда

$$z_1, z_2, \dots, z_{\frac{p-1}{2}}$$

могутъ входить только числа

$$1, 2, \dots, \frac{p-1}{2}$$

и каждое только по одному разу. Но такъ какъ эти ряды заключаютъ одинакое число членовъ; то въ составъ перваго войдутъ всѣ числа втораго. Слѣдов. ряды

$$z_1, z_2, \dots, z_{\frac{p-1}{2}},$$

$$1, 2, \dots, \frac{p-1}{2}$$

составлены изъ однихъ и тѣхъ же чиселъ и притомъ взятыхъ по одному разу; а потому произведение членовъ перваго ряда равно произведенію членовъ втораго.

Убѣдясь въ этомъ, мы можемъ замѣнить въ (15) $z_1 z_2 \dots z_{\frac{p-1}{2}}$

числомъ $1 \cdot 2 \dots \frac{p-1}{2}$; послѣ чего (15), будучи сокращено на $1, 2, \dots, \frac{p-1}{2}$, числа простыя съ p , даетъ

$$1 \equiv q^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} \left(E^{\frac{2q}{p}} + E^{\frac{4q}{p}} + \dots + E^{\frac{(p-1)q}{p}} \right) \pmod{p}.$$

Умножая же обѣ части этого сравненія на

$$(-1)^{\frac{p-1}{2}} \left(E^{\frac{2q}{p}} + E^{\frac{4q}{p}} + \dots + E^{\frac{(p-1)q}{p}} \right)$$

и замѣчая, что -1 , будучи возведена въ степень

$$2 \left[E^{\frac{2q}{p}} + E^{\frac{4q}{p}} + \dots + E^{\frac{(p-1)q}{p}} \right],$$

даетъ 1, находимъ

$$(-1)^{\frac{p-1}{2}} \left(E^{\frac{2q}{p}} + E^{\frac{4q}{p}} + \dots + E^{\frac{(p-1)q}{p}} \right) \equiv q^{\frac{p-1}{2}} \pmod{p}.$$

Но по свойству символа $\left(\frac{q}{p}\right)$ мы имѣемъ

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}.$$

Это же сравненіе вмѣстѣ съ предыдущимъ даетъ

$$\left(\frac{q}{p}\right) - (-1)^{\frac{p-1}{2}} \left(E^{\frac{2q}{p}} + E^{\frac{4q}{p}} + \dots + E^{\frac{(p-1)q}{p}} \right) \equiv 0 \pmod{p};$$

откуда мы заключаемъ о равенствѣ

$$\left(\frac{q}{p}\right) = (-1)^{E\frac{2q}{p} + E\frac{4q}{p} + \dots + E\frac{(p-1)q}{p}};$$

ибо въ противномъ случаѣ первая часть этого сравненія привелась бы къ 2 или -2 , что съ нулемъ не сравнимо по модулю p , отличному отъ 2. Такъ убѣждаемся мы въ справедливости предложенной нами теоремы.

На основаніи этой теоремы мы можемъ опредѣлить значенія $\left(\frac{q}{p}\right)$, не возводя q въ степень $\frac{p-1}{2}$. Такъ для опредѣленія величины $\left(\frac{5}{11}\right)$ находимъ

$$\left(\frac{5}{11}\right) = (-1)^{E\frac{2.5}{11} + E\frac{4.5}{11} + E\frac{6.5}{11} + E\frac{8.5}{11} + E\frac{10.5}{11}}$$

Замѣчая, что

$$\begin{aligned} E\frac{2.5}{11} &= E\frac{10}{11} = 0, & E\frac{8.5}{11} &= E\frac{40}{11} = 3, \\ E\frac{4.5}{11} &= E\frac{20}{11} = 1, & E\frac{10.5}{11} &= E\frac{50}{11} = 4, \\ E\frac{6.5}{11} &= E\frac{30}{11} = 2, & 0 + 1 + 2 + 3 + 4 &= 10, \end{aligned}$$

мы изъ предыдущаго уравненія выводимъ

$$\left(\frac{5}{11}\right) = (-1)^{10} = 1;$$

Выведенное нами уравненія для опредѣленія $\left(\frac{q}{p}\right)$ справедливо при всякомъ числѣ q . Но не трудно вывести изъ него уравненіе болѣе простое, которое будетъ служить для опредѣленія $\left(\frac{a}{p}\right)$ при a нечетномъ. Для этого въ уравненіи

$$\left(\frac{q}{p}\right) = (-1)^{E\frac{2q}{p} + E\frac{4q}{p} + \dots + E\frac{(p-1)q}{p}}$$

пологаемъ $q = \frac{1}{2}(a + p)$, гдѣ a подобно p число нечетное; это даетъ намъ

$$\left(\frac{\frac{1}{2}(a+p)}{p}\right) = (-1)^{E\frac{a+p}{p} + E\frac{2a+2p}{p} + \dots + E\frac{\frac{p-1}{2}a + \frac{p-1}{2}p}{p}}.$$

Умноживъ объ части этого уравненія на $\left(\frac{2}{p}\right)$, находимъ

$$\left(\frac{2}{p}\right)\left(\frac{\frac{1}{2}(a+p)}{p}\right) = \left(\frac{2}{p}\right)(-1) \left(E^{\frac{a+p}{p}} + E^{\frac{2a+2p}{p}} + \dots + E^{\frac{p-1}{2}a + \frac{p-1}{2}p} \right)$$

Но по теоремѣ 29-й произведеніе $\left(\frac{2}{p}\right)\left(\frac{\frac{1}{2}(a+p)}{p}\right)$ равно $\left(\frac{\frac{1}{2} \cdot 2 \cdot (a+p)}{p}\right)$, или $\left(\frac{a+p}{p}\right)$, а это по теоремѣ 30 равно $\left(\frac{a}{p}\right)$. Вслѣдствіе чего изъ предыдущаго уравненія выводимъ

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)(-1) \left(E^{\frac{a+p}{p}} + E^{\frac{2a+2p}{p}} + \dots + \frac{E^{\frac{p-1}{2}a + \frac{p-1}{2}p}}{p} \right)$$

Но

$$E^{\frac{a+p}{p}} = E\left(\frac{a}{p} + 1\right) = 1 + E\frac{a}{p},$$

$$E^{\frac{2a+2p}{p}} = E\left(\frac{2a}{p} + 2\right) = 2 + E\frac{2a}{p},$$

.....

$$E^{\frac{p-1}{2}a + \frac{p-1}{2}p} = E\left(\frac{p-1}{2}a + \frac{p-1}{2}p\right) = \frac{p-1}{2} + E\frac{p-1}{2}a$$

Слѣдовательно

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)(-1) \left(1 + 2 + \dots + \frac{p-1}{2} + E\frac{a}{p} + E\frac{2a}{p} + \dots + E\frac{p-1}{2}a \right)$$

А такъ какъ сумма прогрессіи $1 + 2 + \dots + \frac{p-1}{2}$ равна $\frac{p^2-1}{8}$; то изъ этого уравненія выходитъ

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)(-1) \left(\frac{p^2-1}{8} + E\frac{a}{p} + E\frac{2a}{p} + \dots + E\frac{p-1}{2}a \right) \dots\dots\dots(16)$$

Дѣлая въ этомъ уравненіи $a = 1$ и замѣчая, что

$$\left(\frac{1}{p}\right) = 1, \quad E\frac{1}{p} = 0, \quad E\frac{2}{p} = 0, \dots\dots\dots E\frac{p-1}{p} = 0,$$

находимъ

$$1 = \left(\frac{2}{p}\right) (-1)^{\frac{p^2-1}{8}},$$

что для опредѣленія величины $\left(\frac{2}{p}\right)$ даетъ

$$\left(\frac{2}{p}\right) = (-1)^{-\frac{p^2-1}{8}}.$$

Внося отсюда величину $\left(\frac{2}{p}\right)$ въ (16), находимъ

$$\left(\frac{a}{p}\right) = (-1)^{E\frac{a}{p} + E\frac{2a}{p} + \dots + E\frac{1}{2}(p-1)a} \dots \dots \dots (17)$$

Вотъ уравненіе, которое можетъ служить для опредѣленія $\left(\frac{a}{p}\right)$ при a нечетномъ. Оно подобно тому, которое доказали въ предыдущей теоремѣ, съ тою только разницею, что здѣсь подъ знакомъ E находятся количества въ двое меньшія.

Мы нашли также уравненіе

$$\left(\frac{2}{p}\right) = (-1)^{-\frac{p^2-1}{8}}.$$

Это уравненіе будетъ служить намъ при опредѣленіи $\left(\frac{q}{p}\right)$, когда q равно 2 или кратное 2. На основаніи этого уравненія не трудно показать, что $\left(\frac{2}{p}\right)$ есть 1, если $p = 8n \pm 1$ и -1 , если $p = 8n \pm 3$. Въ самомъ дѣлѣ, внося въ него $8n \pm 1$ и $8n \pm 3$ на мѣсто p , находимъ

$$\left(\frac{2}{8n \pm 1}\right) = (-1)^{\frac{(8n \pm 1)^2 - 1}{8}} = (-1)^{-8n^2 \pm 2n} = 1,$$

$$\left(\frac{2}{8n \pm 3}\right) = (-1)^{\frac{(8n \pm 3)^2 - 1}{8}} = (-1)^{-8n^2 \pm 6n - 1} = -1;$$

отсюда слѣдуетъ такая теорема:

32. ТЕОРЕМА.

Если p равно $8n \pm 1$; то $\left(\frac{2}{p}\right) = 1$; если же $p = 8n \pm 3$;

то $\left(\frac{2}{p}\right) = -1$.

Такъ находимъ, что $\left(\frac{2}{17}\right) = 1, \left(\frac{2}{13}\right) = -1$.

На основаніи уравненія (17) мы можемъ доказать еще теорему, относящуюся до опредѣленія величины $\left(\frac{q}{p}\right)$. Она заключается въ слѣдующемъ:

33. Т Е О Р Е М А.

Если a число нечетное и меньше p ; то $\left(\frac{a}{p}\right)$ равно

$$(-1)^{\frac{a-1}{2} \frac{p-1}{2}} = E^{\frac{p}{a}} E^{\frac{2p}{a}} \dots E^{\frac{1}{2}(a-1)p}.$$

Доказательство. Мы нашли (17) для опредѣленія $\left(\frac{a}{p}\right)$, когда q нечетное, такое уравненіе

$$\left(\frac{a}{p}\right) = (-1)^{\frac{a-1}{2} \frac{p-1}{2}} \left(E^{\frac{a}{p}} + E^{\frac{2a}{p}} + \dots + E^{\frac{1}{2}(p-1)a} \right),$$

Посмотримъ теперь какія значенія имѣютъ $E^{\frac{a}{p}}, E^{\frac{2a}{p}}, \dots, E^{\frac{1}{2}(p-1)a}$, гдѣ предполагаемъ a меньше p .

Дробь $\frac{a}{p}$ будетъ меньше 1; слѣд. $E^{\frac{a}{p}} = 0$; это наименьшій изъ членовъ $E^{\frac{a}{p}}, E^{\frac{2a}{p}}, \dots, E^{\frac{1}{2}(p-1)a}$. Наибольшій же

$E^{\frac{1}{2}(p-1)a}$ представится такъ $E\left(\frac{a}{2} - \frac{a}{2p}\right)$, или $E\left(\frac{a-1}{2} + \frac{p-a}{2p}\right)$,

а это очевидно равно $\frac{a-1}{2}$; ибо это есть цѣлое число, а

$\frac{p-a}{2p}$ дробь меньше единицы и положительная, потому что $a < p$.

И такъ въ рядѣ

$$E^{\frac{a}{p}}, E^{\frac{2a}{p}}, \dots, E^{\frac{1}{2}(p-1)a}$$

члены идутъ, возрастая отъ 0 до $\frac{a-1}{2}$. Чтобы опредѣлить

сумму ихъ мы найдемъ, сколько здѣсь членовъ равныхъ

0, 1, 2, $\frac{a-1}{2}$. Для этого мы опредѣлимъ сначала сколько

здѣсь членовъ не превосходящихъ k , гдѣ k есть одно изъ чиселъ $0, 1, 2, \dots, \frac{a-p}{2}$. Съ этою цѣлю положимъ, что въ рядѣ

$$E^{\frac{a}{p}}, E^{\frac{2a}{p}}, \dots, E^{\frac{la}{p}}, E^{\frac{(l+1)a}{p}}, \dots, E^{\frac{\frac{1}{2}(p-1)a}{p}} \dots \dots \dots (18)$$

последній членъ не превосходящій k есть $E^{\frac{la}{p}}$; это очевидно будетъ имѣть мѣсто въ томъ случаѣ, когда $\frac{la}{p} < k+1$, а $\frac{(l+1)a}{p} > k+1$ (*). Но изъ этихъ неравенствъ выходитъ

$$\frac{p^{k+1}}{a} - l > 0, \quad \frac{p^{k+1}}{a} - l < 1,$$

а это показываетъ, что $\frac{p^{k+1}}{a}$ съ цѣлымъ числомъ l разнится количествомъ положительнымъ, но меньшимъ 1. Слѣд. l есть наибольшее цѣлое число, заключающееся въ количествѣ $\frac{p^{k+1}}{a}$, а это по нашему знаменитію представится такъ

$$E^{\frac{p^{k+1}}{a}}.$$

И такъ число членовъ въ рядѣ (18), не превосходящихъ k , равно $E^{\frac{p^{k+1}}{a}}$. Такимъ же образомъ находимъ, что здѣсь число членовъ, не превосходящихъ $k-1$, есть $E^{\frac{p^k}{a}}$, а отсюда заключаемъ, что число членовъ равныхъ k есть $E^{\frac{p^{k+1}}{a}} - E^{\frac{p^k}{a}}$. На основаніи этого мы заключаемъ, что въ рядѣ (18) число членовъ

$$\text{равныхъ } 0 \text{ есть } \dots \dots \dots E^{\frac{p}{a}} - E^{\frac{0 \cdot p}{a}},$$

$$\text{равныхъ } 1 \dots \dots \dots E^{\frac{2p}{a}} - E^{\frac{p}{a}},$$

(*) Равенство здѣсь не можетъ имѣть мѣсто, потому что дроби $\frac{a}{p}, \frac{2a}{p}, \dots, \frac{\frac{1}{2}(p-1)a}{p}$, гдѣ p простое само по себѣ и не дѣлитъ a , не могутъ равняться цѣлому числу; дроби же $\frac{la}{p}, \frac{(l+1)a}{p}$ взяты изъ этого ряда.

равныхъ 2..... $E^{\frac{3p}{a}} - E^{\frac{2p}{a}}$,

.....
 равныхъ $\frac{a-1}{2} - 1$ есть..... $E^{\frac{1}{2}(a-1)p} - E^{\frac{1}{2}(a-3)p}$.

Чтоже касается до числа членовъ остальныхъ въ рядѣ (18), равныхъ $\frac{a-1}{2}$; то мы ихъ найдемъ, сложивъ предыдущія числа и вычтя ихъ сумму изъ $\frac{1}{2}(p-1)$, числа всѣхъ членовъ ряда (18). Такимъ образомъ находимъ, что здѣсь членовъ равныхъ $\frac{a-1}{2}$ содержится $\frac{p-1}{2} - E^{\frac{1}{2}(a-1)p}$.

На основаніи этихъ данныхъ находимъ, что сумма всѣхъ членовъ ряда (18) составляетъ

$$0. \left(E^{\frac{p}{a}} - E^{\frac{0 \cdot p}{a}} \right) +$$

$$1. \left(E^{\frac{2p}{a}} - E^{\frac{p}{a}} \right) +$$

$$2. \left(E^{\frac{3p}{a}} - E^{\frac{2p}{a}} \right) +$$

.....

$$\left(\frac{a-1}{2} - 1 \right) \left(E^{\frac{1}{2}(a-1)p} - E^{\frac{1}{2}(a-3)p} \right) +$$

$$\frac{a-1}{2} \left(\frac{p-1}{2} - E^{\frac{1}{2}(a-1)p} \right),$$

а это приводится къ слѣдующему

$$\frac{a-1}{2} \cdot \frac{p-1}{2} - E^{\frac{p}{a}} - E^{\frac{2p}{a}} - \dots - E^{\frac{1}{2}(a-1)p}.$$

И такъ сумма

$$E^{\frac{a}{p}} + E^{\frac{2a}{p}} + \dots + E^{\frac{1}{2}(p-1)a}$$

равна

$$\frac{a-1}{2} \cdot \frac{p-1}{2} - E^{\frac{p}{a}} - E^{\frac{2p}{a}} - \dots - E^{\frac{1}{2}(a-1)p}.$$

Въ слѣдствіе этого уравненіе

$$\left(\frac{a}{p} \right) = (-1) E^{\frac{a}{p}} + E^{\frac{2a}{p}} + \dots + E^{\frac{1}{2}(p-1)a}$$

дастъ

$$\left(\frac{a}{p}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{p-1}{2}} - E^{\frac{p}{a}} - E^{\frac{2p}{a}} - \dots - E^{\frac{\frac{1}{2}(a-1)p}{a}},$$

что и слѣдовало доказать.

Эта теорема также можетъ быть употреблена для опредѣленія значенія $\left(\frac{a}{p}\right)$, если a число нечетное и меньше p . Она весьма удобна въ приложеніи, если a число небольшое. Такъ для величины $\left(\frac{7}{101}\right)$ она даетъ

$$\left(\frac{7}{101}\right) = (-1)^{\frac{7-1}{2} \cdot \frac{101-1}{2}} - E^{\frac{101}{7}} - E^{\frac{2 \cdot 101}{7}} - E^{\frac{3 \cdot 101}{7}};$$

откуда выходитъ $\left(\frac{7}{101}\right) = (-1)^{3 \cdot 50 - 14 - 28 - 43} = -1$. Но эта теорема особенно замѣчательна тѣмъ, что изъ нея очень просто выводится теорема, извѣстная подъ названіемъ закона взаимности двухъ простыхъ чиселъ.

Эта теорема заключается въ слѣдующемъ:

34. ТЕОРЕМА.

Если v и s суть числа простые нечетныя и неравныя между собою; то $\left(\frac{v}{s}\right) = \left(\frac{s}{v}\right) (-1)^{\frac{v-1}{2} \cdot \frac{s-1}{2}}$.

Доказательство. Пусть будетъ v наименьшее изъ двухъ чиселъ v, s ; по доказанной нами теоремѣ при $v < s$ значеніе $\left(\frac{v}{s}\right)$ опредѣлится уравненіемъ

$$\left(\frac{v}{s}\right) = (-1)^{\frac{v-1}{2} \cdot \frac{s-1}{2}} - E^{\frac{s}{v}} - E^{\frac{2s}{v}} - \dots - E^{\frac{\frac{1}{2}(v-1)s}{v}}$$

Дѣлая же въ уравненіи (17) $a = s, p = v$, найдемъ

$$\left(\frac{s}{v}\right) = (-1)^{\frac{s}{v} + E^{\frac{2s}{v}} + \dots + E^{\frac{\frac{1}{2}(v-1)s}{v}}}$$

Эти два уравненія по перемноженіи ихъ членовъ даютъ

$$\left(\frac{v}{s}\right)\left(\frac{s}{v}\right) = (-1)^{\frac{v-1}{2} \cdot \frac{s-1}{2}}.$$

Умножая же обѣ части этого уравненія на $\left(\frac{s}{v}\right)$ и замѣчая, что $\left(\frac{s}{v}\right)^2$ есть 1, находимъ

$$\left(\frac{v}{s}\right) = \left(\frac{s}{v}\right) (-1)^{\frac{v-1}{2} \cdot \frac{s-1}{2}},$$

что и слѣдовало доказать.

Такъ мы будемъ имѣть

$$\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) (-1)^{\frac{7-1}{2} \cdot \frac{5-1}{2}} = \left(\frac{7}{5}\right) (-1)^{3 \cdot 2} = \left(\frac{7}{5}\right),$$

$$\left(\frac{11}{19}\right) = \left(\frac{19}{11}\right) (-1)^{\frac{11-1}{2} \cdot \frac{19-1}{2}} = \left(\frac{19}{11}\right) (-1)^{5 \cdot 3} = -\left(\frac{19}{11}\right).$$

§ 27. На основаніи доказанныхъ нами теоремъ относительно символа $\left(\frac{q}{p}\right)$ легко найти его величину, какъ-бы q и p ни были велики. Вотъ какъ слѣдуетъ поступать при опредѣленіи $\left(\frac{q}{p}\right)$. — Если q больше p , мы по теоремѣ 30 замѣняемъ въ $\left(\frac{q}{p}\right)$ число q остаткомъ отъ дѣленія q на p или наименьшимъ отрицательнымъ вычетомъ q по модулю p , если онъ гораздо меньше этого остатка.

Такимъ образомъ опредѣленіе $\left(\frac{q}{p}\right)$ сведется на опредѣленіе $\left(\frac{\pm R}{p}\right)$, гдѣ R будетъ меньше p . Что касается до знака — при R ; то по теоремѣ 29 мы $\left(\frac{-R}{p}\right)$ можемъ выразить черезъ $\left(\frac{R}{p}\right)$. Потомъ для опредѣленія $\left(\frac{R}{p}\right)$ разлагаемъ R на произведеніе простыхъ чиселъ, исключая при этомъ множителей, составляющихъ точные квадраты. Разложивши R на произведеніе простыхъ чиселъ, мы по теоремѣ 29 разлагаемъ $\left(\frac{R}{p}\right)$ на произведеніе нѣсколькихъ множителей вида $\left(\frac{r}{p}\right)$, гдѣ r число простое. Послѣ

того ищемъ значеніе каждаго изъ этихъ символовъ, поступая такимъ образомъ: если $r = 2$, то $\left(\frac{r}{p}\right)$ опредѣляемъ по теоремѣ 32; если же r нечетное, то по закону взаимности чиселъ выражаемъ $\left(\frac{r}{p}\right)$ черезъ $\left(\frac{p}{r}\right)$ и съ этимъ символомъ поступаемъ также какъ съ $\left(\frac{q}{p}\right)$, сводя опредѣленіе его на символы вида $\left(\frac{r'}{r}\right)$, гдѣ $r' < r$.

Продолжая эти дѣйствія, мы будемъ получать символы все съ мѣньшими и меньшими числами; по этому необходимо дойдемъ окончательно или до $\left(\frac{1}{r''}\right)$ или до $\left(\frac{2}{r''}\right)$, которыхъ величину легко найдемъ, а чрезъ нихъ опредѣлится и искомый $\left(\frac{q}{p}\right)$.

Объяснимъ это примѣрами. Пусть будетъ дано найти значеніе $\left(\frac{1013}{601}\right)$.

Для 1013 на 601 находимъ въ остаткѣ 412; откуда слѣдуетъ, что

$$\left(\frac{1013}{601}\right) = \left(\frac{412}{601}\right).$$

По исключеніи изъ 412 квадрата 2, мы находимъ число простое 103 и $\left(\frac{412}{601}\right)$ приводятся къ $\left(\frac{103}{601}\right)$; по закону же взаимности чиселъ выводимъ

$$\left(\frac{103}{601}\right) = \left(\frac{601}{103}\right) (-1)^{\frac{601-1}{2} \cdot \frac{103-1}{2}} = \left(\frac{601}{103}\right).$$

Потомъ дѣлимъ 601 на 103 и замѣчая, что остатокъ будетъ 86, между тѣмъ какъ наименьшій отрицательный вычетъ 601 по модулю 103 есть -17 , находимъ выгоднѣе его ввести. Это даетъ намъ

$$\left(\frac{601}{103}\right) = \left(\frac{-17}{103}\right).$$

Но $\left(\frac{-17}{103}\right) = \left(\frac{-1}{103}\right) \left(\frac{17}{103}\right)$, гдѣ $\left(\frac{-1}{103}\right) = (-1)^{\frac{103-1}{2}} = -1$.

Слѣд.

$$\left(\frac{-17}{103}\right) = -\left(\frac{17}{103}\right).$$

Такъ какъ 17 число простое, то выводимъ

$$\left(\frac{17}{103}\right) = \left(\frac{103}{17}\right) (-1)^{\frac{17-1}{2} \cdot \frac{103-1}{2}} = \left(\frac{103}{17}\right).$$

Замѣняя въ $\left(\frac{103}{17}\right)$ число 103 остаткомъ отъ дѣленія 103 на 17, имѣемъ

$$\left(\frac{103}{17}\right) = \left(\frac{1}{17}\right) = 1.$$

Соединяя всѣ эти уравненія, находимъ

$$\left(\frac{1013}{601}\right) = \left(\frac{412}{601}\right) = \left(\frac{601}{103}\right) = \left(\frac{-17}{103}\right) = -\left(\frac{17}{103}\right) = -\left(\frac{103}{17}\right) = -\left(\frac{1}{17}\right) = -1.$$

Итакъ искомая величина $\left(\frac{1013}{601}\right)$ есть -1 .

Для другаго примѣра беремъ $\left(\frac{20470}{1847}\right)$.

Повторяя надъ символомъ $\left(\frac{20470}{1847}\right)$ тѣ же дѣйствія, находимъ

$$\left(\frac{20470}{1847}\right) = \left(\frac{153}{1847}\right) = \left(\frac{3^2 \cdot 17}{1847}\right) = \left(\frac{17}{1847}\right);$$

$$\left(\frac{17}{1847}\right) = \left(\frac{1847}{17}\right) (-1)^{\frac{17-1}{2} \cdot \frac{1847-1}{2}} = \left(\frac{1847}{17}\right) = \left(\frac{11}{17}\right),$$

$$\left(\frac{11}{17}\right) = \left(\frac{17}{11}\right) (-1)^{\frac{17-1}{2} \cdot \frac{11-1}{2}} = \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right);$$

$$\left(\frac{6}{11}\right) = \left(\frac{2}{11}\right) \left(\frac{3}{11}\right); \quad \left(\frac{2}{11}\right) = -1;$$

$$\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) (-1)^{\frac{3-1}{2} \cdot \frac{11-1}{2}} = -\left(\frac{11}{3}\right) = -\left(\frac{-1}{3}\right) = 1.$$

Изъ соединенія этихъ уравненій получаемъ

$$\left(\frac{20470}{1847}\right) = -1.$$

Также опредѣляя величину символа $\left(\frac{2108}{2003}\right)$, находимъ

$$\left(\frac{2108}{2003}\right) = \left(\frac{105}{2003}\right) = \left(\frac{3}{2003}\right) \left(\frac{5}{2003}\right) \left(\frac{7}{2003}\right);$$

$$\left(\frac{3}{2003}\right) = \left(\frac{2003}{3}\right) (-1)^{\frac{3-1}{2} \cdot \frac{2003-1}{2}} = -\left(\frac{2003}{3}\right) = -\left(\frac{2}{3}\right) = 1,$$

$$\left(\frac{5}{2003}\right) = \left(\frac{2003}{5}\right) (-1)^{\frac{5-1}{2} \cdot \frac{2003-1}{2}} = \left(\frac{2003}{5}\right) = \left(\frac{3}{5}\right);$$

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) (-1)^{\frac{5-1}{2} \cdot \frac{3-1}{2}} = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

$$\left(\frac{7}{2003}\right) = \left(\frac{2003}{7}\right) (-1)^{\frac{7-1}{2} \cdot \frac{2003-1}{2}} = -\left(\frac{2003}{7}\right) = -\left(\frac{1}{7}\right) = -1;$$

откуда выходитъ

$$\left(\frac{2108}{2003}\right) = 1.$$

§ 28. Мы показали, какъ по даннымъ числамъ p и q найти величину символа $\left(\frac{q}{p}\right)$, чѣмъ опредѣляется имѣеть ли сравненіе $z^2 \equiv q \pmod{p}$ рѣшенія или нѣтъ. Теперь переходимъ къ рѣшенію обратнаго вопроса: по данной величинѣ $\left(\frac{x}{p}\right)$ найти значенія x , иначе, рѣшить уравненія $\left(\frac{x}{p}\right) = 1, \left(\frac{x}{p}\right) = -1$.

Начнемъ съ перваго $\left(\frac{x}{p}\right) = 1$. Мы видѣли, что уравненіе

$\left(\frac{x}{p}\right) = 1$ символически выражаетъ, что сравненіе $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ удовлетворяется. Не трудно узнать, что это сравненіе имѣеть

$\frac{p-1}{2}$ рѣшеній; для этого по сказанному въ § 21 дѣлимъ $x^p - x$ на $x^{\frac{p-1}{2}} - 1$ и замѣчая, что $x^p - x$, какъ равное $x(x^{\frac{p-1}{2} + 1} - 1)(x^{\frac{p-1}{2}} - 1)$,

дѣлится на $x^{\frac{p-1}{2}} - 1$ безъ остатка, по теоремѣ 26-ой заключаемъ,

что сравненіе $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ имѣеть $\frac{p-1}{2}$ рѣшеній.

Но эти рѣшенія (§ 12) должны представиться такъ

$$x \equiv a_1, x \equiv a_2, \dots, x \equiv a_{\frac{p-1}{2}} \pmod{p},$$

гдѣ $a_1, a_2, \dots, a_{\frac{p-1}{2}}$ суть числа въ рядѣ $0, 1, 2, \dots, p-1$, удовлетворяющія

сравненію $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Притомъ ясно, что ни одно изъ

этихъ чиселъ не будетъ равно нулю, ибо нуль не удовлетворяетъ

сравненію $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Итакъ въ рядѣ 1, 2, ..., $p-1$ на-

ходится $\frac{p-1}{2}$ чиселъ удовлетворяющихъ сравненію $x^{\frac{p-1}{2}} \equiv 1$

\pmod{p} , или уравненію $\left(\frac{x}{p}\right) = 1$, другими словами, въ рядѣ

1, 2, ..., $p-1$ находится $\frac{p-1}{2}$ квадратичныхъ вычетовъ по мо-

дулю p . За тѣмъ всѣ остальные въ рядѣ 1, 2, ..., $p-1$, ихъ

будетъ также $\frac{p-1}{2}$, удовлетворятъ уравненію $\left(\frac{x}{p}\right) = -1$: это

будутъ неквадратичные вычеты по модулю p .

Изъ сказаннаго намъ слѣдуетъ, что всѣ числа, удовлетво-

ряющія сравненію $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, или, что одно и то же,

уравненію $\left(\frac{x}{p}\right) = 1$, опредѣляются сравненіями

$$x \equiv a_1, x \equiv a_2, \dots, x \equiv a_{\frac{p-1}{2}} \pmod{p},$$

гдѣ $a_1, a_2, \dots, a_{\frac{p-1}{2}}$ числа положительныя, меньшія p и удов-

летворяющія сравненію $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Эти числа мы могли

бы найти, рѣшая сравненіе $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Но это чрезвы-

чайно затруднительно, если число p велико; поэтому мы пред-

ложимъ способъ ихъ находить независимо отъ рѣшенія срав-

ненія $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Для этого мы замѣчаемъ, что сравне-

ніе $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ есть условіе возможности удовлетворить

сравненію $z^2 \equiv a \pmod{p}$. Притомъ мы видѣли, что это срав-

неніе въ случаѣ возможности удовлетворяется двумя числами (§ 22), заключающимися въ рядѣ 1, 2, ..., $p-1$; такъ что если одно изъ этихъ чиселъ есть α , то другое $p-\alpha$. Но одно изъ

этихъ чиселъ необходимо меньше $\frac{p}{2}$ и слѣд. не болѣе $\frac{p-1}{2}$; ибо сумма ихъ есть p , а они неравны между собою. Поэтому для

числа a , при которомъ сравненіе $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ удовлетворяется, всегда найдется въ рядѣ $1, 2, \dots, \frac{p-1}{2}$ число z , удовлетворяющее сравненію $z^2 \equiv a \pmod{p}$, другими словами, для такого число a будетъ имѣть мѣсто одно изъ сравненій

$$1^2 \equiv a, \quad 2^2 \equiv a, \dots, \left(\frac{p-1}{2}\right)^2 \equiv a \pmod{p}.$$

Слѣд. число a по модулю p будетъ сравнимо съ однимъ изъ

$$1^2, \quad 2^2, \dots, \left(\frac{p-1}{2}\right)^2,$$

и такъ какъ оно меньше p ; то оно найдется между остатками отъ дѣленія этихъ чиселъ на p .

Итакъ каждое изъ чиселъ $a_1, a_2, \dots, a_{\frac{p-1}{2}}$ меньшихъ p и

удовлетворяющихъ сравненію $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ мы найдемъ въ рядѣ остатковъ, получаемыхъ при дѣленіи $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ на p . Послѣ сего значенія x , удовлетворяющія уравненію $\left(\frac{x}{p}\right) = 1$, мы опредѣлимъ сравненіями

$$x \equiv a_1, \quad x \equiv a_2, \dots, x \equiv a_{\frac{p-1}{2}} \pmod{p};$$

откуда для выраженія x , удовлетворяющаго уравненію $\left(\frac{x}{p}\right) = 1$, по § 11 найдемъ (*)

$$x = np + a_1, \quad x = np + a_2, \dots, x = np + a_{\frac{p-1}{2}}.$$

Для примѣра рѣшимъ уравненіе $\left(\frac{x}{11}\right) = 1$. По сказанному намъ это уравненіе будетъ имѣть $\frac{11-1}{2} = 5$ рѣшеній, которыя опредѣлятся сравненіями

(*) Это получаемъ мы, замѣняя въ формулахъ § 11 число N числомъ $-n$.

$$x \equiv a_1, x \equiv a_2, x \equiv a_3, x \equiv a_4, x \equiv a_5 \pmod{11},$$

гдѣ a_1, a_2, a_3, a_4, a_5 суть остатки отъ дѣленія $1^2, 2^2, 3^2, 4^2, 5^2$ на 11. Но такъ какъ эти остатки суть 1, 4, 9, 5, 3; то уравненію

$$\left(\frac{x}{11}\right) = 1$$

будутъ удовлетворять числа, опредѣляемыя сравненіями

$$x \equiv 1, x \equiv 3, x \equiv 4, x \equiv 5, x \equiv 9 \pmod{11},$$

или, что одно и то же, уравненіями

$$x = 11n + 1, x = 11n + 3, x = 11n + 4, x = 11n + 5, x = 11n + 9.$$

Зная рѣшенія уравненія $\left(\frac{x}{p}\right) = 1$, нетрудно найти рѣшенія уравненія $\left(\frac{x}{p}\right) = -1$. Для этого мы замѣчаемъ во первыхъ, что по значенію символа $\left(\frac{x}{p}\right)$ число x предполагается недѣлящимся на p и во вторыхъ, что числа, неудовлетворяющія уравненію $\left(\frac{x}{p}\right) = 1$, удовлетворяютъ уравненію $\left(\frac{x}{p}\right) = -1$. Отсюда слѣдуетъ, что мы найдемъ всѣ числа, для которыхъ $\left(\frac{x}{p}\right) = -1$, если выкинемъ изъ чиселъ, недѣлящихся на p , числа удовлетворяющія уравненію $\left(\frac{x}{p}\right) = 1$. Но всѣ числа могутъ быть представлены формулами

$$nr, nr + 1, nr + 2, \dots, nr + p - 1.$$

Откинувъ здѣсь первую формулу, которая даетъ числа кратныя p , мы находимъ для рѣшенія уравненій $\left(\frac{x}{p}\right) = 1$ и $\left(\frac{x}{p}\right) = -1$ такія формулы

$$nr + 1, nr + 2, \dots, nr + p - 1.$$

Отброся же здѣсь числа, удовлетворяющія уравненію $\left(\frac{x}{p}\right) = 1$, которыя опредѣляются формулами

$$nr + a_1, nr + a_2, \dots, nr + \frac{a_{p-1}}{2},$$

мы найдемъ всѣ числа, удовлетворяющія уравненію $\left(\frac{x}{p}\right) = -1$.

Изъ этого слѣдуетъ, что числа, удовлетворяющія уравненію $\left(\frac{x}{p}\right) = -1$, представляются формулами

$$np + b_1, np + b_2, \dots, np + b_{\frac{p-1}{2}},$$

гдѣ $b_1, b_2, \dots, b_{\frac{p-1}{2}}$ суть числа ряда $1, 2, \dots, p-1$, отличныя отъ $a_1, a_2, a_{\frac{p-1}{2}}$, остатковъ, получаемыхъ при дѣленіи $1^2, 2^2, \dots$

$\left(\frac{p-1}{2}\right)^2$ на p .

Для примѣра найдемъ рѣшенія уравненія $\left(\frac{x}{11}\right) = -1$. По сказанному нами числа, удовлетворяющія этому уравненію, представляются формулами

$$11n + b_1, 11n + b_2, 11n + b_3, 11n + b_4, 11n + b_5,$$

гдѣ b_1, b_2, b_3, b_4, b_5 найдемъ, выкинувъ изъ ряда $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ числа равныя остаткамъ, получаемымъ при дѣленіи $1^2, 2^2, 3^2, 4^2, 5^2$ на 11 . По эти остатки суть $1, 4, 9, 5, 3$. Выкинувъ ихъ изъ ряда $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$, находимъ $2, 6, 7, 8, 10$ для величинъ b_1, b_2, b_3, b_4, b_5 . Откуда заключаемъ, что числа, удовлетворяющія уравненію $\left(\frac{x}{11}\right) = -1$, опредѣляются формулами

$$11n + 2, 11n + 6, 11n + 7, 11n + 8, 11n + 10.$$

Такъ рѣшается вопросъ объ опредѣленіи значеній x по данной величинѣ $\left(\frac{x}{p}\right)$, или, что одно и то же, объ опредѣленіи квадратичныхъ и неквадратичныхъ вычетовъ даннаго числа.

§ 29. Въ предыдущихъ параграфахъ мы занимались изслѣдованіемъ, когда сравненіе $z^2 \equiv q \pmod{p}$ имѣетъ рѣшенія и когда нѣтъ. Теперь остается показать, какъ найдутся рѣшенія сравненія $z^2 \equiv q \pmod{p}$, когда оно возможно. Говоря о сравненіяхъ вида $a^x \equiv A \pmod{p}$, мы покажемъ общій и весьма простой способъ рѣшать сравненіе $z^2 \equiv q \pmod{p}$. Здѣсь же ограничимся однимъ частнымъ случаемъ, въ которомъ это рѣшеніе

можно легко найти. Случай, которымъ мы теперь ограничимся, есть тотъ, когда p вида $4n + 3$.

Возможность рѣшенія сравненія $z^2 \equiv q \pmod{p}$, какъ видѣли, предполагаетъ, что $q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Дѣлая здѣсь $p = 4n + 3$, находимъ $q^{\frac{4n+3-1}{2}} \equiv 1 \pmod{p}$, или $q^{2n+1} \equiv 1 \pmod{p}$, что по умноженіи на q будетъ $q^{2n+2} \equiv q \pmod{p}$. Сличая это сравненіе съ $z^2 \equiv q \pmod{p}$, замѣчаемъ, что послѣднему удовлетворяетъ $z = q^{n+1}$. Зная одно число удовлетворяющее сравненію $z^2 \equiv q \pmod{p}$, мы найдемъ подобныхъ чиселъ безконечное множество изъ сравненія $z \equiv q^{n+1} \pmod{p}$. Но мы видѣли, что одно изъ этихъ чиселъ будетъ положительное и меньше p ; это остатокъ отъ дѣленія q^{n+1} на p . Называя его черезъ α , мы одно изъ рѣшеній сравненія $z^2 \equiv q \pmod{p}$ представимъ такъ $z \equiv \alpha \pmod{p}$. Что касается до другаго рѣшенія этого сравненія; то по сказанному въ § 22 оно будетъ $z \equiv p - \alpha \pmod{p}$. Такъ найдутся оба рѣшенія сравненія $z^2 \equiv q \pmod{p}$ при $p = 4n + 3$.

Для примѣра найдемъ рѣшенія сравненія $z^2 \equiv 3 \pmod{11}$. Оно имѣетъ рѣшенія; ибо

$$\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) (-1)^{\frac{11-1}{2} \cdot \frac{3-1}{2}} = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1,$$

а такъ какъ $11 = 4 \cdot 2 + 3$; то рѣшенія его суть $z \equiv \alpha$, $z \equiv 11 - \alpha \pmod{11}$, гдѣ α есть остатокъ отъ дѣленія 3^{2+1} на 11. Но этотъ остатокъ есть 5; слѣд. $\alpha = 5$ и рѣшенія сравненія $z^2 \equiv 3 \pmod{11}$ суть

$$z \equiv 5, z \equiv 6 \pmod{11}.$$

§ 30. До сихъ поръ мы занимались сравненіями второй степени, предполагая модуль ихъ числомъ простымъ. Что же касается до сравненій съ модулемъ составнымъ; то мы ограничимся только доказательствомъ, что сравненіе $z^2 \equiv q \pmod{p}$ имѣетъ рѣшеніе, если p число нечетное, простое съ q и въ составъ его входятъ простыя числа $\alpha, \beta, \gamma, \dots$, для которыхъ

$$\left(\frac{q}{\alpha}\right) = 1, \left(\frac{q}{\beta}\right) = 1, \left(\frac{q}{\gamma}\right) = 1, \dots\dots\dots$$

Начнемъ съ частнаго случая $p = \alpha^m$ и покажемъ, какъ найдутся рѣшенія сравненія $z^2 \equiv q \pmod{\alpha^m}$, когда знаемъ рѣшенія сравненія $z^2 \equiv q \pmod{\alpha}$, котораго возможность, какъ видѣли, условливается равенствомъ $\left(\frac{q}{\alpha}\right) = 1$.

Предположимъ, что a есть число удовлетворяющее сравненію $z^2 \equiv q \pmod{\alpha}$, и P, Q суть числа, опредѣляемые уравненіями

$$P = \frac{(a + \sqrt{q})^m + (a - \sqrt{q})^m}{2},$$

$$Q = \frac{(a + \sqrt{q})^m - (a - \sqrt{q})^m}{2\sqrt{q}};$$

числа P, Q будутъ цѣлыя; въ этомъ легко убѣдиться разложениемъ $(a + \sqrt{q})^m, (a - \sqrt{q})^m$ по биному Ньютона. Докажемъ теперь во 1) что P и Q удовлетворяютъ сравненію $P^2 - Q^2 q \equiv 0 \pmod{\alpha^m}$ и во 2) что Q число простое съ α .

Въ первомъ мы легко убѣждаемся, замѣтивъ изъ предыдущихъ уравненій, что

$$P + Q\sqrt{q} = (a + \sqrt{q})^m, P - Q\sqrt{q} = (a - \sqrt{q})^m.$$

Перемножая же эти уравненія между собою, находимъ

$$P^2 - Q^2 q = (a^2 - q)^m.$$

Но по положенію a удовлетворяетъ сравненію $z^2 \equiv q \pmod{\alpha}$, слѣдов. $a^2 \equiv q \pmod{\alpha}$, что предполагаетъ дѣлимость $a^2 - q$ на α . Если же $a^2 - q$ имѣетъ дѣлителемъ α ; то $P^2 - Q^2 q$, равное $(a^2 - q)^m$, должно дѣлиться на α^m , а потому

$$P^2 - Q^2 q \equiv 0 \pmod{\alpha^m}.$$

Доказавши первое, переходимъ ко второму, къ доказательству, что Q число простое съ α . Для этого мы замѣчаемъ, что по уравненію

$$Q = \frac{(a + \sqrt{q})^m - (a - \sqrt{q})^m}{2\sqrt{q}}$$

дѣлимость Q на α предполагаетъ сравненіе

GABINET MATEMATYCZNY
Towarzystwa Naukowego Warszawskiego

$$\frac{(a + \sqrt{q})^m - (a - \sqrt{q})^m}{2\sqrt{q}} \equiv 0 \pmod{\alpha}.$$

Но это сравненіе, какъ не трудно убѣдиться разложеніемъ степеней $(a + \sqrt{q})^m$, $(a - \sqrt{q})^m$, содержитъ q въ цѣлыхъ степеняхъ и съ цѣлыми коэффициентами; по этому оно останется справедливымъ (§ 10), если въ немъ q замѣнимъ числомъ a^2 , сравнимымъ съ q по модуль α . Слѣд. предыдущее сравненіе предполагаетъ

$$\frac{(\alpha + \sqrt{a^2})^m - (\alpha - \sqrt{a^2})^m}{2\sqrt{a^2}} \equiv 0 \pmod{\alpha},$$

а это приводится къ

$$2^{m-1} a^{m-1} \equiv 0 \pmod{\alpha},$$

сравненію невозможному; ибо α число простое нечетное и a простое съ α .

Убѣдясь такимъ образомъ, что P и Q удовлетворяютъ сравненію

$$P^2 - Q^2q \equiv 0 \pmod{\alpha^m}$$

и Q число простое съ α , не трудно доказать, что сравненіе $Qx \equiv P \pmod{\alpha^m}$ имѣетъ рѣшеніе и это рѣшеніе удовлетворяетъ сравненію $x^2 \equiv q \pmod{\alpha^m}$. Первое слѣдуетъ изъ того, что Q , будучи числомъ простымъ съ α , будетъ простымъ также съ α^m ; въ этомъ же случаѣ сравненіе $Qx \equiv P \pmod{\alpha^m}$ имѣетъ всегда одно рѣшеніе. Намъ остается теперь показать, что числа x , опредѣляемые сравненіемъ $Qx \equiv P \pmod{\alpha^m}$, удовлетворяютъ сравненію $z^2 \equiv q \pmod{\alpha^m}$. Для этого мы, возведя обѣ части сравненія $Qx \equiv P \pmod{\alpha^m}$ въ квадратъ, выведемъ

$$Q^2x^2 \equiv P^2 \pmod{\alpha^m}.$$

Но по доказанію нап. относительно чиселъ P и Q имѣемъ

$$P^2 - Q^2q \equiv 0 \pmod{\alpha^m}.$$

Это же сравненіе вмѣстѣ съ предыдущимъ даетъ

$$Q^2x^2 \equiv Q^2q \pmod{\alpha^m},$$

а такъ какъ Q число простое съ α и слѣд. съ α^m ; то въ

этомъ сравненіи обѣ части могутъ быть сокращены на Q^2 ; вслѣдствіе чего оно приводится къ

$$x^2 \equiv q \pmod{p},$$

что и слѣдовало доказать.

И такъ мы получимъ рѣшеніе сравненія $z^2 \equiv q \pmod{\alpha^m}$ изъ сравненія

$$Qz \equiv P \pmod{\alpha^m},$$

гдѣ P и Q найдутся изъ уравненій

$$P = \frac{(a + \sqrt{q})^m + (a - \sqrt{q})^m}{2}, \quad Q = \frac{(a + \sqrt{q})^m - (a - \sqrt{q})^m}{2\sqrt{q}}$$

по a , числу удовлетворяющему сравненію

$$a^2 \equiv q \pmod{\alpha}.$$

Для примѣра возьмемъ сравненіе $z^2 \equiv -2 \pmod{3^5}$. По сказанному нами числу, удовлетворяющее ему, найдется изъ сравненія

$$Qz \equiv P \pmod{3^5},$$

гдѣ

$$P = \frac{(a + \sqrt{-2})^3 + (a - \sqrt{-2})^3}{2}, \quad Q = \frac{(a + \sqrt{-2})^3 - (a - \sqrt{-2})^3}{2\sqrt{-1}}$$

и a есть число, удовлетворяющее сравненію $a^2 \equiv -2 \pmod{3}$.

Последнее сравненіе относится къ числу тѣхъ, которыя рѣшаются по способу показанному въ § 29; рѣшая его по этому способу, мы находимъ, что ему удовлетворяетъ 1. Дѣлая $a = 1$ въ уравненіяхъ, опредѣляющихъ P и Q , имѣемъ

$$P = \frac{(1 + \sqrt{-2})^3 + (1 - \sqrt{-2})^3}{2} = -5,$$

$$Q = \frac{(1 + \sqrt{-2})^3 - (1 - \sqrt{-2})^3}{2\sqrt{-2}} = 1.$$

Отсюда для опредѣленія z , числа удовлетворяющаго сравненію $z^2 \equiv -2 \pmod{3^5}$, выходитъ

$$z \equiv -5 \pmod{3^5}.$$

Показавши какимъ образомъ рѣшается сравненіе $z^2 \equiv q \pmod{\alpha^m}$, гдѣ α какое нибудь простое нечетное число, переходимъ къ рѣшенію сравненія $z^2 \equiv q \pmod{\alpha^m \beta^n \gamma^r \dots}$.

Если $\left(\frac{q}{\alpha}\right) = 1, \left(\frac{q}{\beta}\right) = 1, \left(\frac{q}{\gamma}\right) = 1, \dots$; то по сказанному нами найдутся числа u, v, ω, \dots , удовлетворяющія сравненіямъ $u^2 \equiv q \pmod{\alpha^m}, v^2 \equiv q \pmod{\beta^n}, \omega^2 \equiv q \pmod{\gamma^r}, \dots$

Эти числа опредѣляются такими сравненіями $u \equiv A \pmod{\alpha^m}, v \equiv B \pmod{\beta^n}, \omega \equiv C \pmod{\gamma^r}, \dots$

Но не трудно убѣдиться, что между числами, опредѣляемыми каждымъ изъ этихъ сравненій, найдется число

$$A(\beta^n \gamma^r \dots)^{\alpha^{m-1}(\alpha-1)} + B(\alpha^m \gamma^r \dots)^{\beta^{n-1}(\beta-1)} + C(\alpha^m \beta^n \dots)^{\gamma^{r-1}(\gamma-1)} + \dots$$

Въ самомъ дѣлѣ, это число по модулю α^m сравнимо съ $A(\beta^n \gamma^r \dots)^{\alpha^{m-1}(\alpha-1)}$, гдѣ $(\beta^n \gamma^r \dots)^{\alpha^{m-1}(\alpha-1)}$ по теоремѣ 17 сравнимо съ 1 по тому же модулю α^m , и слѣд. $A(\beta^n \gamma^r \dots)^{\alpha^{m-1}(\alpha-1)}$ сравнимо съ A . Также докажется, что это число сравнимо съ B по модулю β^n , съ C по модулю γ^r и т. д.... А потому это число будетъ удовлетворять каждому изъ сравненій

$$u^2 \equiv q \pmod{\alpha^m}, v^2 \equiv q \pmod{\beta^n}, \omega^2 \equiv q \pmod{\gamma^r}, \dots$$

и слѣд., называя его черезъ x , будемъ имѣть

$$x^2 \equiv q \pmod{\alpha^m}, x^2 \equiv q \pmod{\beta^n}, x^2 \equiv q \pmod{\gamma^r}, \dots$$

Но такъ какъ въ этихъ сравненіяхъ модули $\alpha^m, \beta^n, \gamma^r, \dots$ числа относительно другъ друга простыя; ибо $\alpha, \beta, \gamma, \dots$ суть различныя простыя числа; то по § 9 эти сравненія предполагаютъ

$$x^2 \equiv q \pmod{\alpha^m \beta^n \gamma^r \dots}.$$

Такъ опредѣлится x , удовлетворяющій сравненію

$$x^2 \equiv q \pmod{p},$$

гдѣ q число простое съ p , а p число нечетное, состоящее изъ произведенія простыхъ чиселъ $\alpha, \beta, \gamma, \dots$, для которыхъ

$$\left(\frac{q}{\alpha}\right) = 1, \left(\frac{q}{\beta}\right) = 1, \left(\frac{q}{\gamma}\right) = 1, \dots$$

Этимъ мы окончиваемъ теорію сравненій второй степени.

ГЛАВА V.

О СРАВНЕНИЯХЪ ДВУЧЛЕННЫХЪ.

§ 31. Подъ именемъ сравненій двучленныхъ разумѣютъ сравненія такого вида

$$x^n - A \equiv 0 \pmod{p},$$

гдѣ n , A , p какія нибудь числа. Мы начнемъ съ простѣйшаго случая: $A = 1$, p число простое. Мы будемъ предполагать p отличнымъ отъ 2; ибо по § 20 при $p = 2$ сравненіе $x^n - A \equiv 0 \pmod{p}$ приводится къ 1-й степени.

Относительно сравненій вида $x^n - 1 \equiv 0 \pmod{p}$ мы докажемъ слѣдующую теорему:

34. Т Е О Р Е М А.

Если одно и тоже число удовлетворяетъ сравненіямъ $x^m - 1 \equiv 0$, $x^n - 1 \equiv 0 \pmod{p}$; то оно удовлетворяетъ также сравненію $x^\omega - 1 \equiv 0 \pmod{p}$, гдѣ ω одицій наибольшей дѣлитель чиселъ m и n .

Доказательство. Пусть будетъ a то число, которое удовлетворяетъ и сравненію $x^m - 1 \equiv 0 \pmod{p}$ и сравненію $x^n - 1 \equiv 0 \pmod{p}$; мы будемъ имѣть

$$a^m \equiv 1, a^n \equiv 1 \pmod{p},$$

и a будетъ число простое съ p ; ибо иначе было бы $a^m \equiv 0 \pmod{p}$.

По положенію ω будучи общимъ наибольшимъ дѣлителемъ чиселъ m и n , въ частныхъ $\frac{m}{\omega}$, $\frac{n}{\omega}$ дасть числа простыя между собою. Но при $\frac{m}{\omega}$, $\frac{n}{\omega}$ простыхъ между собою найдется z , удовлетворяющее сравненію $\frac{m}{\omega} z - 1 \equiv 0 \pmod{\frac{n}{\omega}}$, что предполагаетъ дѣлимость $\frac{m}{\omega} z - 1$ на $\frac{n}{\omega}$. Означая частное отъ этого дѣленія чрезъ y , найдемъ

$$\frac{m}{\omega} z - 1 \equiv \frac{n}{\omega} y;$$

откуда выходитъ

$$mz - ny = \omega \dots \dots \dots (19)$$

По изъ сравненій

$$a^m \equiv 1, a^n \equiv 1 \pmod{p},$$

возводя первое въ степень z , второе въ степень y , выводимъ

$$a^{mz} \equiv a^{ny} \pmod{p},$$

что по сокращеніи на a^{ny} (число простое съ p ; ибо, видѣли, a простое съ p) даетъ

$$a^{mz-ny} \equiv 1 \pmod{p},$$

гдѣ замѣняя $mz - ny$ черезъ ω по (19), имѣемъ

$$a^\omega \equiv 1 \pmod{p},$$

что и слѣдовало доказать.

На основаніи этой теоремы не трудно доказать слѣдующую:

35. ТЕОРЕМА.

Сравненіе $x^m - 1 \equiv 0 \pmod{p}$ имѣетъ ω рѣшеній, если ω есть общій наибольшій дѣлитель чиселъ m и $p - 1$, и эти рѣшенія найдутся изъ сравненія $x^\omega - 1 \equiv 0 \pmod{p}$.

Доказательство. Сравненію $x^m - 1 \equiv 0 \pmod{p}$ могутъ удовлетворять только числа недѣляющіяся на p ; ибо для x кратнаго p будетъ $x^m \equiv 0 \pmod{p}$. Но по теоремѣ Фермата для x не дѣляющагося на p будетъ

$$x^{p-1} - 1 \equiv 0 \pmod{p}.$$

Итакъ всѣ числа, удовлетворяющія сравненію $x^m - 1 \equiv 0 \pmod{p}$, будутъ также удовлетворять сравненію $x^{p-1} - 1 \equiv 0 \pmod{p}$; откуда слѣдуетъ по доказанной нами теоремѣ, что эти числа будутъ удовлетворять сравненію

$$x^\omega - 1 \equiv 0 \pmod{p},$$

гдѣ ω общій наибольшій дѣлитель чиселъ $p - 1$ и m .

Также не трудно убѣдиться въ обратномъ, что всѣ числа, удовлетворяющія этому сравненію, будутъ удовлетворять и сравненію $x^m - 1 \equiv 0 \pmod{p}$.

Въ самомъ дѣлѣ, изъ сравненія $x^\omega - 1 \equiv 0 \pmod{p}$ выходитъ $x^\omega \equiv 1 \pmod{p}$, а это по возведеніи въ степень $\frac{m}{\omega}$ (число $\frac{m}{\omega}$ есть цѣлое; ибо ω есть дѣлитель m), даетъ $x^m \equiv 1 \pmod{p}$, или $x^m - 1 \equiv 0 \pmod{p}$.

Итакъ сравненіямъ $x^m - 1 \equiv 0$, $x^\omega - 1 \equiv 0 \pmod{p}$ будутъ удовлетворять однѣ и тѣ же числа. Намъ остается теперь показать, что эти сравненія имѣютъ ω рѣшеній; это легко сдѣлать надъ сравненіемъ $x^\omega - 1 \equiv 0 \pmod{p}$. Такъ какъ ω есть дѣлитель $p - 1$; то $\frac{p-1}{\omega}$ есть число цѣлое; называя его его черезъ n , найдемъ $p - 1 = \omega n$. Вслѣдствіе чего $x^p - x$ представится такъ $x(x^{\omega n} - 1)$, или $x[(x^\omega)^n - 1^n]$, а это дѣлится на $x^\omega - 1$; ибо разность степеней дѣлится на разность корней. Но если $x^p - x$ дѣлится на $x^\omega - 1$ безъ остатка; то по 26-ой теоремѣ сравненіе $x^\omega - 1 \equiv 0 \pmod{p}$ имѣетъ ω рѣшеній. А такъ какъ это сравненіе удовлетворяется однимъ числомъ съ $x^m - 1 \equiv 0 \pmod{p}$; то и это сравненіе имѣетъ ω рѣшеній; откуда и слѣдуетъ предложенная намъ теорема.

Такъ сравненіе $x^{10} - 1 \equiv 0 \pmod{17}$, гдѣ общій наибольшій дѣлитель чиселъ 10 и 17—1 есть 2, будетъ имѣть только два рѣшенія, которыя найдутся изъ сравненія $x^2 \equiv 1 \pmod{17}$. Замѣчая, что этому сравненію удовлетворяютъ 1 и 17—1=16, вслѣдствіе чего рѣшенія его суть

$$x \equiv 1, x \equiv 16 \pmod{17},$$

мы заключаемъ, что рѣшенія сравненія $x^{10} - 1 \equiv 0 \pmod{17}$ суть

$$x \equiv 1, x \equiv 16 \pmod{17}.$$

На основаніи этой теоремы рѣшеніе сравненія $x^m - 1 \equiv 0 \pmod{p}$ сводится на рѣшеніе сравненія $x^\omega - 1 \equiv 0 \pmod{p}$, гдѣ ω дѣлитъ $p - 1$; этимъ-то сравненіемъ мы теперь и займемся. Относительно его мы докажемъ слѣдующую теорему:

36. Т Е О Р Е М А.

Сравненію $x^\omega - 1 \equiv 0 \pmod{p}$, гдѣ ω дѣлитъ $p - 1$, удовлетворяетъ число $\alpha = n^{\frac{p-1}{\omega}}$, если n простое съ p .

Доказательство. Въ самомъ дѣлѣ, полагая $\alpha = n^{\frac{p-1}{\omega}}$, находимъ

$$\alpha^\omega - 1 = n^{p-1} - 1.$$

Но по теоремѣ Фермата при n простомъ съ p будетъ

$$n^{p-1} - 1 \equiv 0 \pmod{p},$$

слѣдовательно также

$$a^\omega - 1 \equiv 0 \pmod{p},$$

что и слѣдовало доказать.

Такъ $2^{\frac{11-1}{5}}$, $3^{\frac{11-1}{5}}$, $4^{\frac{11-1}{5}}$, будутъ удовлетворять сравненію $x^5 - 1 \equiv 0 \pmod{11}$.

Такимъ образомъ мы можемъ найти нѣсколько рѣшеній сравненія $x^\omega - 1 \equiv 0 \pmod{p}$. Что же касается до опредѣленія всѣхъ его рѣшеній, то относительно ихъ докажется слѣдующая теорема:

37. Т Е О Р Е М А.

Если число θ удовлетворяетъ сравненію $x^\omega - 1 \equiv 0 \pmod{p}$ и не удовлетворяетъ сравненіямъ $x^\alpha - 1 \equiv 0$, $x^\beta \equiv 1$, $x^5 - 1 \equiv 0 \pmod{p}$, гдѣ $\alpha, \beta, \dots, \epsilon$ суть дѣлители ω (включая сюда и 1); то всѣ ω рѣшеній сравненія $x^\omega - 1 \equiv 0 \pmod{p}$ опредѣлятся такъ

$$x \equiv \theta, x \equiv \theta^2, \dots, x \equiv \theta^\omega \pmod{p}.$$

Доказательство. Не трудно убѣдиться, что если θ удовлетворяетъ сравненію $x^\omega - 1 \equiv 0 \pmod{p}$; то ему удовлетворяетъ и θ^n , какое бы ни было число n . Въ самомъ дѣлѣ, если θ удовлетворяетъ сравненію $x^\omega - 1 \equiv 0 \pmod{p}$; то $\theta^\omega - 1 \equiv 0 \pmod{p}$, или $\theta^\omega \equiv 1 \pmod{p}$. Но возведя обѣ части этого сравненія въ степень n , находимъ $\theta^{n\omega} \equiv 1 \pmod{p}$, или $\theta^{n\omega} - 1 \equiv 0 \pmod{p}$ а это показываетъ, что θ^n удовлетворяетъ сравненію $x^\omega - 1 \equiv 0 \pmod{p}$. На основаніи этого, мы заключаемъ, что

$$\theta, \theta^2, \dots, \theta^\omega$$

будутъ удовлетворять сравненію

$$x^\omega - 1 \equiv 0 \pmod{p},$$

и слѣд. будутъ удовлетворять ему всѣ числа, опредѣляемыя сравненіями

$$x \equiv \theta, x \equiv \theta^2, \dots, x \equiv \theta^\omega \pmod{p} \dots \dots \dots (20)$$

Докажемъ же теперь, что въ этомъ рядѣ сравненій нѣтъ двухъ сравненій тождественныхъ между собою. Для этого допустимъ противное, допустимъ, что здѣсь какія нибудь два сравненія

$$x \equiv \theta^m, x \equiv \theta^n \pmod{p}$$

тождественны между собою; числа m и n , какъ показатели θ въ сравненіяхъ (20), будутъ болѣе 0 и не болѣе ω и пусть m будетъ болѣе n .

Допустивши, что сравненія

$$x \equiv \theta^m, x \equiv \theta^n \pmod{p}$$

удовлетворяются однимъ и тѣмъ же числомъ x , мы находимъ

$$\theta^m \equiv \theta^n \pmod{p},$$

что по сокращеніи на θ^n даетъ

$$\theta^{m-n} - 1 \equiv 0 \pmod{p}.$$

Это сравненіе вмѣстѣ съ сравненіемъ $\theta^\omega \equiv 1 \pmod{p}$, которому θ удовлетворяетъ по положенію, предполагаетъ

$$\theta^{\omega'} - 1 \equiv 0 \pmod{p},$$

гдѣ ω' общій наибольшій дѣлитель $m - n$ и ω (смотри теорему 34). Но ω' не можетъ быть равнымъ ω ; ибо ω' есть дѣлитель $m - n$, гдѣ m и n болѣе 0 и не болѣе ω , а потому $m - n < \omega$. Но если число ω' меньше ω , то, дѣля ω , оно должно быть однимъ изъ дѣлителей его: $\alpha, \beta, \dots, \zeta$; вслѣдствіе чего предыдущее сравненіе должно быть однимъ изъ сравненій

$$\theta^\alpha - 1 \equiv 0, \theta^\beta - 1 \equiv 0, \dots, \theta^\zeta - 1 \equiv 0 \pmod{p}.$$

Эти же сравненія, по положенію, не могутъ имѣть мѣста.

Итакъ между сравненіями

$$x \equiv \theta, x \equiv \theta^2, \dots, x \equiv \theta^\omega \pmod{p}$$

не можетъ быть двухъ тождественныхъ между собою, слѣд. въ нихъ заключаются всѣ ω рѣшеній сравненія

$$x^\omega - 1 \equiv 0 \pmod{p},$$

что и слѣдовало доказать.

Такъ чтобы пайти всѣ рѣшенія сравненія $x^\omega - 1 \equiv 0 \pmod{p}$ (13)

мы должны найти число, которое бы удовлетворяло ему, не удовлетворяя сравнениямъ

$$x - 1 \equiv 0, x^2 - 1 \equiv 0, x^5 - 1 \equiv 0 \pmod{13}.$$

Замѣчая, что такое свойство принадлежитъ числу 4, мы заключаемъ, что рѣшенія сравненія

$$x^6 - 1 \equiv 0 \pmod{13}$$

суть

$$x \equiv 4, x \equiv 4^2, x \equiv 4^3, x \equiv 4^4, x \equiv 4^5, x \equiv 4^6 \pmod{13},$$

или

$$x \equiv 4, x \equiv 3, x \equiv 12, x \equiv 9, x \equiv 10, x \equiv 1 \pmod{13}.$$

§ 32. Переходимъ теперь къ сравненіямъ $x^m - A \equiv 0 \pmod{p}$, гдѣ A какое нибудь число недѣлящееся на p , а p число простое, которое мы опять предполагаемъ отличнымъ отъ 2.

Относительно сравненій этого вида мы докажемъ слѣдующую теорему.

38. Т Е О Р Е М А.

Сравненіе $x^m - A \equiv 0 \pmod{p}$ возможно только въ томъ случаѣ, когда $A^{\frac{p-1}{\omega}} \equiv 1 \pmod{p}$, гдѣ ω общій наибольшій дѣлитель чиселъ $p - 1$ и m . Когда же это сравненіе возможно, оно имѣетъ ω рѣшеній, которыя найдутся изъ сравненія $x^\omega - A^\pi \equiv 0 \pmod{p}$, гдѣ π есть число, удовлетворяющее условию $\frac{m}{\omega} \pi \equiv 1 \pmod{\frac{p-1}{\omega}}$.

Доказательство. Мы предполагаемъ A недѣлящимся на p ; по этому числу x , удовлетворяющее сравненію $x^m - A \equiv 0 \pmod{p}$, или $x^m \equiv A \pmod{p}$, не можетъ быть кратнымъ p ; ибо въ этомъ случаѣ было бы $x^m \equiv 0 \pmod{p}$ и сравненіе $x^m \equiv A \pmod{p}$ дало бы $A \equiv 0 \pmod{p}$. Но если x не дѣлится на p ; то по теоремѣ Фермата будетъ

$$x^{p-1} \equiv 1 \pmod{p}.$$

Возводя обѣ части этого сравненія въ степень $\frac{m}{\omega}$, а члены сравненія

$$x^m \equiv A \pmod{p}$$

въ степень $\frac{p-1}{\omega}$ (числа $\frac{m}{\omega}$, $\frac{p-1}{\omega}$ будутъ цѣлыя; ибо ω есть общій дѣлитель m и $p-1$), находимъ

$$x^{\frac{(p-1)m}{\omega}} \equiv 1, \quad x^{\frac{m(p-1)}{\omega}} \equiv A^{\frac{p-1}{\omega}} \pmod{p};$$

откуда слѣдуетъ

$$A^{\frac{p-1}{\omega}} \equiv 1 \pmod{p}.$$

И такъ для возможности сравненія

$$x^m - A \equiv 0 \pmod{p}$$

необходимо, чтобы A удовлетворяло сравненію

$$A^{\frac{p-1}{\omega}} \equiv 1 \pmod{p} \dots\dots\dots (21)$$

Предположимъ теперь, что это условіе выполняется и докажемъ, что въ такомъ случаѣ всѣ числа, удовлетворяющія сравненію

$$x^m \equiv A \pmod{p},$$

удовлетворяютъ также сравненію

$$x^\omega \equiv A^\pi \pmod{p},$$

гдѣ π число, опредѣляемое сравненіемъ

$$\frac{m}{\omega} \pi \equiv 1 \pmod{\frac{p-1}{\omega}}.$$

Число ω , будучи общимъ наибольшимъ дѣлителемъ чиселъ m и $p-1$, въ частныхъ $\frac{m}{\omega}$, $\frac{p-1}{\omega}$ даетъ числа простыя между собою. Но при $\frac{m}{\omega}$, $\frac{p-1}{\omega}$ простыхъ между собою найдется число π , удовлетворяющее сравненію $\frac{m}{\omega} \pi \equiv 1 \pmod{\frac{p-1}{\omega}}$ и для такого числа π разность $\frac{m}{\omega} \pi - 1$ будетъ дѣлиться на $\frac{p-1}{\omega}$.

Называя ζ частное отъ этого дѣленія, будемъ имѣть

$$\frac{m}{\omega} \pi - 1 = \zeta \frac{p-1}{\omega},$$

или

$$m\pi - \zeta(p-1) = \omega \dots\dots\dots (22)$$

На основаніи этого уравненія мы покажемъ, что сравненіе

$$x^m \equiv A \pmod{p}$$

предполагаетъ

$$x^\omega \equiv A^\pi \pmod{p}.$$

Въ самомъ дѣлѣ, возводя обѣ части сравненія

$$x^m \equiv A \pmod{p}$$

въ степень π , находимъ

$$x^{m\pi} \equiv A^\pi \pmod{p};$$

по теоремѣ же Фермата имѣемъ

$$x^{p-1} \equiv 1 \pmod{p},$$

гдѣ возводя обѣ части въ степень ζ , получаемъ

$$x^{\zeta(p-1)} \equiv 1, \text{ или } 1 \equiv x^{\zeta(p-1)} \pmod{p}.$$

Но изъ сравненій

$$x^{m\pi} \equiv A^\pi, \quad 1 \equiv x^{\zeta(p-1)} \pmod{p},$$

перемножая ихъ почленно, выводимъ

$$x^{m\pi} \equiv A^\pi x^{\zeta(p-1)} \pmod{p},$$

что по сокращеніи на $x^{\zeta(p-1)}$ будетъ

$$x^{m\pi - \zeta(p-1)} \equiv A^\pi \pmod{p}.$$

Замѣняя же здѣсь $m\pi - \zeta(p-1)$ числомъ ω по (22), найдемъ

$$x^\omega \equiv A^\pi \pmod{p},$$

что и слѣдовало доказать.

Изъ этого видно, что сравненіе

$$x^m \equiv A \pmod{p}$$

не можетъ имѣть рѣшеній отличныхъ отъ рѣшеній $x^\omega \equiv A^\pi \pmod{p}$.

Убѣдившись въ этомъ, мы докажемъ остальную часть предложенной нами теоремы. Для этого мы докажемъ, что сравненіе $x^\omega \equiv A^\pi \pmod{p}$ имѣетъ ω рѣшеній и что всѣ они удовлетворяютъ сравненію $x^m \equiv A \pmod{p}$.

Чтобы увѣриться въ первомъ, мы по § 21 ищемъ остатокъ, получаемый при дѣленіи $x^p - x$ на $x^\omega - A^\pi$. Этотъ остатокъ мы легко находимъ, замѣчая, что $x^p - x$ можетъ быть такъ представлено.

$$[(x^\omega)^{\frac{p-1}{\omega}} - (A^\pi)^{\frac{p-1}{\omega}}]x + (A^{\frac{\pi(p-1)}{\omega}} - 1)x,$$

гдѣ $[(x^\omega)^{\frac{p-1}{\omega}} - (A^\pi)^{\frac{p-1}{\omega}}]x$, очевидно, дѣлится на $x^\omega - A^\pi$. Откуда слѣдуетъ, что искомый остатокъ есть

$$[A^{\frac{\pi(p-1)}{\omega}} - 1]x.$$

Но здѣсь коэффициентъ $A^{\frac{\pi(p-1)}{\omega}} - 1$ дѣлится на p ; ибо по (21) имѣемъ

$$A^{\frac{p-1}{\omega}} \equiv 1 \pmod{p},$$

что по возведеніи въ степень π даетъ

$$A^{\frac{\pi(p-1)}{\omega}} \equiv 1 \pmod{p};$$

слѣд. по теоремѣ 26 сравненіе $x^\omega \equiv A^\pi \pmod{p}$ имѣетъ ω рѣшеній.

Намъ остается теперь доказать, что всѣ рѣшенія сравненія $x^\omega \equiv A^\pi \pmod{p}$ удовлетворяютъ сравненію $x^m - A \equiv 0 \pmod{p}$. Для этого мы замѣтимъ, что сравненіе $x^\omega \equiv A^\pi \pmod{p}$ по возведеніи его частей въ степень $\frac{m}{\omega}$ даетъ

$$x^m \equiv A^{\frac{\pi m}{\omega}} \pmod{p}.$$

Вычитая же A изъ обѣихъ частей этого сравненія, найдемъ

$$x^m - A \equiv A^{\frac{\pi m}{\omega}} - A \pmod{p},$$

или

$$x^m - A \equiv A (A^{\frac{\pi m - \omega}{\omega}} - 1) \pmod{p}.$$

Внося сюда величину πm изъ (22), получаемъ

$$x^m - A \equiv A (A^{\frac{\varepsilon(p-1)}{\omega}} - 1) \pmod{p} \dots \dots \dots (23)$$

Но по (21) A удовлетворяетъ сравненію

$$A^{\frac{p-1}{\omega}} \equiv 1 \pmod{p},$$

которое по возведеніи его частей въ степень ε будетъ

*

$$A^{\frac{\zeta(p-1)}{\omega}} \equiv 1 \pmod{p},$$

или

$$A^{\frac{(p-1)}{\omega}} - 1 \equiv 0 \pmod{p}.$$

Въ слѣдствіе же этого сравненіе (23) приводится къ такому

$$x^m - A \equiv 0 \pmod{p},$$

что и оставалось намъ доказать.

Для примѣра возьмемъ сравненіе

$$x^8 - 3 \equiv 0 \pmod{11}.$$

Общій наибольшій дѣлитель 8 и 11 — 1 есть 2. Слѣд. для возможности этого сравненія необходимо быть

$$3^{\frac{11-1}{2}} \equiv 1 \pmod{11}.$$

Это условіе выполняется; ибо $3^{\frac{11-1}{2}} = 3^5 = 243$, что сравнимо съ 1 по модулю 11. Рѣшенія же этого сравненія найдутся изъ сравненія $x^2 - 3^\pi \equiv 0 \pmod{11}$, гдѣ π опредѣляется условіемъ

$$\frac{6}{2}\pi \equiv 1 \pmod{\frac{11-1}{2}},$$

или

$$4\pi \equiv 1 \pmod{5}.$$

Рѣшая это сравненіе по способу, показанному въ § 15, находимъ

$$\pi \equiv 4^{5-2} \equiv 64 \pmod{5}.$$

Откуда видимъ, что за π можно взять 4. Вслѣдствіе этого сравненіе

$$x^2 - 3^\pi \equiv 0 \pmod{11}$$

дастъ

$$x^2 - 81 \equiv 0 \pmod{11}.$$

Но этому сравненію удовлетворяетъ $x=9$ и $x=11-9=2$. Слѣд. рѣшенія сравненія

$$x^8 - 3 \equiv 0 \pmod{11}$$

суть

$$x \equiv 2, x \equiv 9 \pmod{11}.$$

Изъ доказанной нами теоремы относительно сравненій вида $x^m - A \equiv 0 \pmod{p}$ выводимъ слѣдующую:

39. Т Е О Р Е М А.

Сравненіе $x^m + 1 \equiv 0 \pmod{p}$ не имѣетъ рѣшенія, если $p - 1$ по освобожденіи отъ общихъ множителей съ m приводится къ числу нечетному. Въ противномъ случаѣ это сравненіе имѣетъ ω рѣшеній, если $p - 1$ и m имѣютъ общимъ наибольшимъ дѣлителемъ ω и эти рѣшенія найдутся изъ сравненія $x^\omega + 1 \equiv 0 \pmod{p}$.

Доказательство. По теоремѣ 38 для возможности сравненія

$$x^m + 1 \equiv 0 \pmod{p}$$

необходимо, чтобы удовлетворялось сравненіе

$$(-1)^{\frac{p-1}{\omega}} \equiv 1 \pmod{p};$$

а это не можетъ имѣть мѣста, если $\frac{p-1}{\omega}$ число нечетное; слѣд. частное отъ дѣленія $p - 1$ на ω , общій наибольшій дѣлитель чиселъ m и $p - 1$, должно быть числомъ четнымъ. Если же $\frac{p-1}{\omega}$ число четное; то условіе

$$(-1)^{\frac{p-1}{\omega}} \equiv 1 \pmod{p}$$

выполняется, а въ этомъ случаѣ по доказанной нами теоремѣ сравненіе

$$x^m + 1 \equiv 0 \pmod{p}$$

имѣетъ ω рѣшеній и эти рѣшенія найдутся изъ сравненія

$$x^\omega - (-1)^\pi \equiv 0 \pmod{p},$$

гдѣ π есть число, удовлетворяющее сравненію

$$\frac{m}{\omega} \pi \equiv 1 \pmod{\frac{p-1}{\omega}}.$$

Но такъ какъ въ послѣднемъ сравненіи модуль число четное, а вторая часть не дѣлится на 2; то и первая должна быть

числомъ простымъ съ 2. Откуда слѣдуетъ, что π число нечетное, а потому сравненіе

$$x^{\pi} - (-1)^{\pi} \equiv 0 \pmod{p},$$

которымъ опредѣляются рѣшенія сравненія

$$x^m + 1 \equiv 0 \pmod{p},$$

приведется къ такому

$$x^{\pi} + 1 \equiv 0 \pmod{p}.$$

Такъ убѣждаемся мы въ справедливости предложенной нами теоремы.

На основаніи этой теоремы мы заключаемъ, что сравненіе

$$x^4 + 1 \equiv 0 \pmod{13}$$

не имѣетъ рѣшенія; ибо общій наибольшій дѣлитель 4 и 13 — 1 есть 4, а частное отъ дѣленія 13 — 1 на 4 есть 3, число нечетное. Напротивъ сравненіе

$$x^9 + 1 \equiv 0 \pmod{13}$$

имѣетъ три рѣшенія; ибо общій наибольшій дѣлитель 9 и 13 — 1 есть 3, а 3, дѣля 13 — 1, даетъ въ частномъ число четное 4, и рѣшенія этого сравненія найдутся изъ сравненія

$$x^5 + 1 \equiv 0 \pmod{13}.$$

§ 33. До сихъ поръ мы говорили о сравненіи $x^m - A \equiv 0 \pmod{p}$, предполагая p числомъ простымъ. Обращаемся теперь къ тѣмъ случаямъ, когда здѣсь p число составное. Мы предположимъ p числомъ простымъ относительно m и A и докажемъ, что въ этомъ случаѣ, если можно удовлетворить сравненію $x^m - A \equiv 0$, принимая за модуль его какое либо изъ простыхъ чиселъ, входящихъ въ составъ p ; то ему можно удовлетворить и при модулѣ p .

Мы начнемъ съ частнаго случая, предположивъ, что $p = \alpha^m$, гдѣ α какое нибудь простое цѣлое, недѣляющее m и A , и покажемъ, какимъ образомъ изъ рѣшенія сравненія

$$x^m - A \equiv 0 \pmod{\alpha}$$

могутъ быть выведены рѣшенія сравненій

$$x^m - A \equiv 0 \pmod{\alpha^2}, x^m - A \equiv 0 \pmod{\alpha^5}, \text{ и т. д.}$$

Пусть будетъ a число, удовлетворяющее сравненію

$$x^m - A \equiv 0 \pmod{\alpha};$$

число a не будетъ дѣлиться на α ; ибо A по положенію не дѣлится на α . Для опредѣленія числа, удовлетворяющаго сравненію $x^m - A \equiv 0 \pmod{\alpha^2}$, положимъ $x = a + \alpha z$ и будемъ искать z подъ условіемъ

$$(a + \alpha z)^m - A \equiv 0 \pmod{\alpha^2},$$

которое приводится къ слѣдующему

$$a^m - A + ma^{m-1}\alpha z + \frac{m(m-1)}{1.2}a^{m-2}\alpha^2 z^2 + \dots + \alpha^m z^m \equiv 0 \pmod{\alpha^2}.$$

Но здѣсь α есть общій множитель членовъ сравненія и модуля; ибо a , будучи числомъ удовлетворяющимъ сравненію $x^m - A \equiv 0 \pmod{\alpha}$, въ разности $a^m - A$ даетъ число кратное α ; во всѣхъ же прочихъ членахъ сравненія и въ модуль число α входитъ множителемъ. Сокращая его, находимъ

$$\frac{a^m - A}{\alpha} + ma^{m-1}z + \frac{m(m-1)}{1.2}a^{m-2}\alpha z^2 + \dots + \alpha^{m-1}z^m \equiv 0 \pmod{\alpha}.$$

Но такъ какъ

$$\frac{m(m-1)}{1.2}a^{m-1}\alpha z^2 + \dots + \alpha^{m-1}z^m \equiv 0 \pmod{\alpha};$$

то предыдущее сравненіе приведется къ такому

$$\frac{a^m - A}{\alpha} + ma^{m-1}z \equiv 0 \pmod{\alpha}.$$

Это сравненіе, будучи первой степени относительно неизвѣстнаго z , легко рѣшается. Притомъ не трудно убѣдиться, что оно всегда имѣетъ рѣшеніе: въ немъ коэффициентъ при z , будучи составленъ изъ произведенія чиселъ m и a простыхъ съ α , будетъ число простое съ модулемъ α ; въ этомъ же случаѣ сравненіе первой степени всегда имѣетъ рѣшеніе.

Итакъ рѣшеніемъ сравненія

$$\frac{a^m - A}{\alpha} + ma^{m-1}z \equiv 0 \pmod{\alpha}$$

найдется число z , по которому число, удовлетворяющее сравненію

$$x^m - A \equiv 0 \pmod{\alpha^2},$$

выразится такъ: $x = a + \alpha z$. Покажемъ теперь, какимъ образомъ по числу b , удовлетворяющему сравненію

$$x^m - A \equiv 0 \pmod{\alpha^2},$$

найдется число x , для котораго

$$x^m - A \equiv 0 \pmod{\alpha^5}.$$

Для этого полагая въ этомъ сравненіи $x = b + \alpha^2 u$, выведемъ

$$(b + \alpha^2 u)^m - A \equiv 0 \pmod{\alpha^5}.$$

Разлагая же $(b + \alpha^2 u)^m$ по биному Ньютона, сокращая все члены сравненія и модуль на α^2 и опуская члены кратные α , какъ дѣлали выше, найдемъ для опредѣленія u сравненіе

$$\frac{b^m - A}{\alpha^2} + mb^{m-1}u \equiv 0 \pmod{\alpha}.$$

Отсюда опредѣлится u . Зная же u , мы опредѣлимъ число, удовлетворяющее сравненію

$$x^m - A \equiv 0 \pmod{\alpha^5},$$

изъ уравненія $x = b + \alpha^2 u$.

Поступая такимъ образомъ, мы будемъ находить рѣшенія сравненій $x^m - A \equiv 0$ при модуляхъ α^4 , α^5 , и т. д.

Для примѣра найдемъ рѣшеніе сравненія $x^5 - 2 \equiv 0 \pmod{3^2}$. Сначала рѣшаемъ сравненіе $x^5 - 2 \equiv 0 \pmod{3}$, которое по теоремѣ 38-й приводится къ слѣдующему

$$x - 2^\pi \equiv 0 \pmod{3},$$

гдѣ π опредѣляется условіемъ

$$5\pi \equiv 1 \pmod{2}.$$

Замѣчая, что этому условію удовлетворяетъ $\pi = 1$, мы для рѣшенія сравненія $x^5 - 2 \equiv 0 \pmod{3}$ находимъ

$$x - 2 \equiv 0 \pmod{3}.$$

Откуда заключаемъ, что 2 есть число ему удовлетворяющее, и для рѣшенія сравненія

$$x^5 - 2 \equiv 0 \pmod{3^2}$$

полагаемъ: $x = 2 + 3z$, гдѣ z опредѣляется условіемъ

$$\frac{2^5 - 2}{3} + 5 \cdot 2^{5-1}z \equiv 0 \pmod{3},$$

или

$$10 + 80z \equiv 0 \pmod{3},$$

которое по сокращеніи на 10 приводится къ слѣдующему

$$8z \equiv -1 \pmod{3}.$$

Между числами, удовлетворяющими этому сравненію, находимъ 1; принимая ее за z , мы находимъ, что $2 + 3z$ равно 5 и это будетъ число, удовлетворяющее сравненію

$$x^5 - 2 \equiv 0 \pmod{3^2}.$$

Обращаемся теперь къ сравненію $x^m - A \equiv 0 \pmod{p}$, гдѣ p какое нибудь число простое съ m и A , и докажемъ, что если p состоитъ изъ произведенія простыхъ чиселъ $\alpha, \beta, \gamma, \dots$, для которыхъ сравненія

$$x^m - A \equiv 0 \pmod{\alpha}, x^m - A \equiv 0 \pmod{\beta}, x^m - A \equiv 0 \pmod{\gamma} \dots$$

имѣютъ рѣшенія; то можно найти рѣшеніе сравненія

$$z^m - A \equiv 0 \pmod{p}.$$

Пусть будетъ $p = \alpha^\lambda \beta^\mu \gamma^\nu \dots$. По приему показанному нами мы найдемъ числа, удовлетворяющія сравненіямъ

$$x^m - A \equiv 0 \pmod{\alpha^\lambda}, x^m - A \equiv 0 \pmod{\beta^\mu}, x^m - A \equiv 0 \pmod{\gamma^\nu} \dots$$

Пусть эти числа будутъ M, N, P, \dots ; по теоремѣ 13-й всѣ числа, опредѣляемыя сравненіемъ

$$x \equiv M \pmod{\alpha^\lambda},$$

будутъ удовлетворять сравненію

$$x^m - A \equiv 0 \pmod{\alpha^\lambda};$$

числа, опредѣляемыя сравненіемъ

$$x \equiv N \pmod{\beta^\mu},$$

будутъ удовлетворять сравненію

$$x^m - A \equiv 0 \pmod{\beta^\mu},$$

и т. д. Но въ § 30 выдѣли, какимъ образомъ можно найти число, удовлетворяющее всѣмъ сравненіямъ

$$x \equiv M \pmod{\alpha^\lambda}, x \equiv N \pmod{\beta^\mu}, x \equiv P \pmod{\gamma^\nu}, \dots$$

и слѣд. всѣмъ сравненіямъ

$$x^m - A \equiv 0 \pmod{\alpha^\lambda}, x^m - A \equiv 0 \pmod{\beta^\mu}, x^m - A \equiv 0 \pmod{\gamma^\nu} \dots$$

А такъ какъ $\alpha, \beta, \gamma, \dots$ различныя простые числа; то модули этихъ сравненій $\alpha^\lambda, \beta^\mu, \gamma^\nu, \dots$ суть числа относительно

другъ друга простыя; а въ этомъ случаѣ эти сравненія по § 9 предполагаютъ

$$x^m - A \equiv 0 \pmod{\alpha^2 \beta^u \gamma^v \dots}$$

Такъ мы найдемъ число, удовлетворяющее сравненію

$$x^m - A \equiv 0 \pmod{\alpha^2 \beta^u \gamma^v \dots},$$

опредѣливши число, которое удовлетворяетъ сравненіямъ

$$x \equiv M \pmod{\alpha^2}, \quad x \equiv N \pmod{\gamma^u}, \quad x \equiv P \pmod{\beta^v}, \dots,$$

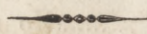
гдѣ M, N, P, \dots числа, опредѣляемыя условіями

$$M^m - A \equiv 0 \pmod{\alpha^2},$$

$$N^m - A \equiv 0 \pmod{\beta^u};$$

$$P^m - A \equiv 0 \pmod{\gamma^v};$$

.....



ГЛАВА VI.

О СРАВНЕНІЯХЪ ВИДА $a^x \equiv A \pmod{p}$.

§ 34. До сихъ поръ мы занимались изслѣдованіемъ такихъ сравненій, которыя заключаютъ въ себѣ алгебраическую цѣлую функцію неизвѣстнаго и рассмотрѣли замѣчательнѣйшія изъ этихъ сравненій: сравненія первыхъ двухъ степеней и сравненія двучленные. Теперь переходимъ къ сравненіямъ, которыя содержатъ неизвѣстное показателемъ. Изъ этихъ сравненій самое замѣчательное есть $a^x \equiv A \pmod{p}$, гдѣ p число простое, не дѣляющее a и A . Этимъ сравненіемъ мы теперь и займемся. Относительно его легко доказать слѣдующую теорему:

40. ТЕОРЕМА.

Если число a удовлетворяетъ сравненію $a^x \equiv A \pmod{p}$; то ему удовлетворяетъ и всякое число, сравнимое съ a по модулю $p - 1$.

Доказательство. Если z сравнимо съ α по модулю $p - 1$; то $z - \alpha$ дѣлится на $p - 1$. Называя ζ частное отъ дѣленія $z - \alpha$ на p , найдемъ

$$z - \alpha = (p - 1)\zeta;$$

откуда слѣдуетъ

$$a^{z-\alpha} = a^{(p-1)\zeta}.$$

Но по теоремѣ Фермата a^{p-1} и слѣд. $a^{(p-1)\zeta}$ сравнимо съ 1 по модулю p ; поэтому

$$a^{z-\alpha} \equiv 1 \pmod{p}.$$

Имѣя же по положенію

$$a^\alpha \equiv A \pmod{p},$$

мы перемноженіемъ этого сравненія съ предыдущимъ находимъ

$$a^z \equiv A \pmod{p},$$

что и слѣдовало доказать.

Изъ доказанной нами теоремѣ видно, что если сравненію $a^x \equiv A \pmod{p}$ удовлетворяетъ одно число, то ему удовлетворяетъ безконечное множество другихъ, сравнимыхъ съ первымъ по модулю $p - 1$. Но всѣ эти числа, сравнимыя между собою по модулю $p - 1$, мы принимаемъ за одно рѣшеніе сравненія $a^x \equiv A \pmod{p}$. Въ этомъ значеніи сравненіе

$$a^x \equiv A \pmod{p}$$

будетъ имѣть столько рѣшеній, сколько положительныхъ чиселъ меньшихъ $p - 1$ и слѣд. не сравнимыхъ между собою по модулю $p - 1$ ему удовлетворяетъ (*). Эти рѣшенія представляются такъ

$$x \equiv \alpha_1, x \equiv \alpha_2, \dots, x \equiv \alpha_n \pmod{p - 1},$$

гдѣ $\alpha_1, \alpha_2, \dots, \alpha_n$ суть положительные числа, меньшія $p - 1$ и удовлетворяющія сравненію

$$a^x \equiv A \pmod{p}.$$

(*) До этого мы доходимъ, повторяя о рѣшеніяхъ сравненія $a^x \equiv A \pmod{p}$ тѣже сужденія, которыя дѣлали въ § 12 при опредѣленіи числа рѣшеній сравненія $fx \equiv 0 \pmod{p}$.

Показавши какъ считаются рѣшенія сравненія $a^x \equiv A \pmod{p}$, мы приступимъ къ опредѣленію числа ихъ и начнемъ съ частнаго случая $A = 1$.

Относительно сравненія $a^x \equiv 1 \pmod{p}$ легко доказать слѣдующія теоремы:

41. ТЕОРЕМА.

Если сравненію $a^x \equiv 1 \pmod{p}$ удовлетворяетъ $x = a$; то ему удовлетворяетъ всякое число кратное a .

Доказательство. Въ самомъ дѣлѣ, если сравненію $a^x \equiv 1 \pmod{p}$ удовлетворяетъ $x = a$; то $a^a \equiv 1 \pmod{p}$. Это же сравненіе по возведеніи въ какую нибудь степень n будетъ $a^{na} \equiv 1 \pmod{p}$; откуда слѣдуетъ что na удовлетворяетъ сравненію $a^x \equiv 1 \pmod{p}$.

42. ТЕОРЕМА.

Если сравненію $a^x \equiv 1 \pmod{p}$ удовлетворяетъ число a ; то ему удовлетворяетъ и общій наибольшій дѣлитель чиселъ a и $p - 1$.

Доказательство. Эту теорему легко вывести изъ теоремы 35-й, доказанной нами для двучленного сравненія $x^m - 1 \equiv 0 \pmod{p}$, по которой число a , удовлетворяющее этому сравненію, должно также удовлетворять сравненію $x^\omega - 1 \equiv 0 \pmod{p}$, гдѣ ω общій наибольшій дѣлитель m и $p - 1$ и слѣд. сравненіе $a^m \equiv 1 \pmod{p}$ предполагаетъ сравненіе $a^\omega \equiv 1 \pmod{p}$, въ чемъ и заключается предложенная нами теорема.

43. ТЕОРЕМА.

Наименьшее число, за исключеніемъ 0, удовлетворяющее сравненію $a^x \equiv 1 \pmod{p}$, есть дѣлитель $p - 1$; прочія же числа ему удовлетворяющія суть кратныя этого дѣлителя.

Доказательство. Пусть будетъ a наименьшее число, удовлетворяющее сравненію $a^x \equiv 1 \pmod{p}$; по предыдущей теоремѣ сравненію $a^x \equiv 1 \pmod{p}$ будетъ удовлетворять общій нап-

большій дѣлитель чиселъ α и $p - 1$. Но этотъ дѣлитель чиселъ $p - 1$ и α , удовлетворяя сравненію $a^x \equiv 1 \pmod{p}$, долженъ быть равенъ α ; ибо въ противномъ случаѣ онъ бы былъ меньше α , между тѣмъ какъ по положенію α есть наименьшее число, удовлетворяющее сравненію $a^x \equiv 1 \pmod{p}$. Итакъ α должно быть дѣлителемъ числа $p - 1$.

Теперь докажемъ, что всѣ числа, удовлетворяющія сравненію $a^x \equiv 1 \pmod{p}$, суть кратныя α . Для этого мы замѣчаемъ, что по предыдущей теоремѣ сравненіе $a^x \equiv 1 \pmod{p}$ предполагаетъ $a^\omega \equiv 1 \pmod{p}$, гдѣ ω общій наибольшій дѣлитель чиселъ x и $p - 1$. Это же сравненіе вмѣстѣ съ $a^\alpha \equiv 1 \pmod{p}$ предполагаетъ (см. теор. 34) $a^{\omega'} \equiv 1 \pmod{p}$, гдѣ ω' общій наибольшій дѣлитель α и ω . Но ω' должно быть равно α ; иначе ω' , будучи общимъ наибольшимъ дѣлителемъ α и ω , было бы меньше α , и такъ какъ ω' удовлетворяетъ сравненію $a^x \equiv 1 \pmod{p}$, то мы бы нашли въ ω' число меньше α , которое удовлетворяетъ сравненію $a^x \equiv 1 \pmod{p}$, что противно положенію. Итакъ ω' равно α . Но мы видѣли, что ω' есть общій наибольшій дѣлитель x и $p - 1$; слѣд. α , равное ω' , дѣлится x , что и слѣдовало доказать.

Такъ замѣчая, что наименьшее число (послѣ 0), удовлетворяющее сравненію $2^x \equiv 1 \pmod{31}$, есть 5, мы заключаемъ, что только числа кратныя 5 будутъ удовлетворять этому сравненію.

По доказанной нами теоремѣ мы заключаемъ, что наименьшее число, удовлетворяющее сравненію $a^x \equiv 1 \pmod{p}$, есть одинъ изъ дѣлителей $p - 1$ (изъ этого числа не исключается само $p - 1$, которое по теоремѣ Фермата удовлетворяетъ сравненію $a^{p-1} \equiv 1 \pmod{p}$), и если это число есть α ; то всѣ числа, удовлетворяющія этому сравненію, начиная отъ 0, представляются такимъ рядомъ

$$0, \alpha, 2\alpha, \dots$$

откуда видно, что

$$0, \alpha, 2\alpha, \dots, \alpha \left(\frac{p-1}{\alpha} - 1 \right)$$

суть единственные числа, удовлетворяющія сравненію $a^x \equiv 1 \pmod{p}$ и меньшія $p-1$; слѣд. рѣшенія сравненія $a^x \equiv 1 \pmod{p}$ суть

$$x \equiv 0, x \equiv \alpha, x \equiv 2\alpha, \dots, x \equiv \alpha \left(\frac{p-1}{\alpha} - 1 \right) \pmod{p-1},$$

и число ихъ есть $\frac{p-1}{\alpha}$.

Такъ замѣчая, что наименьшее число, удовлетворяющее сравненію $2^x \equiv 1 \pmod{31}$, есть 5, мы заключаемъ, что это сравненіе имѣетъ $\frac{31-1}{5} = 6$ рѣшеній, которыя суть

$$x \equiv 0, x \equiv 5, x \equiv 2.5, x \equiv 3.5, x \equiv 4.5, x \equiv 5.5 \pmod{30}.$$

Мы нашли, что число рѣшеній сравненія $a^x \equiv 1 \pmod{p}$ опредѣляется отношеніемъ $p-1$ къ α , гдѣ α наименьшее число, удовлетворяющее этому сравненію. Отсюда слѣдуетъ, что это сравненіе имѣетъ одно только рѣшеніе, если наименьшее число, удовлетворяющее этому сравненію, есть $p-1$.

§ 35. Переходимъ теперь къ сравненіямъ $a^x \equiv A \pmod{p}$, гдѣ A какое нибудь число, не дѣлящееся на p , и докажемъ слѣдующую теорему:

44. ТЕОРЕМА.

Если сравненію $a^x \equiv A \pmod{p}$ удовлетворяетъ λ , а наименьшее число, удовлетворяющее сравненію $a^x \equiv 1 \pmod{p}$, есть α ; то первое сравненіе имѣетъ $\frac{p-1}{\alpha}$ рѣшеній, которыя суть

$$x \equiv \lambda, x \equiv \lambda + \alpha, x \equiv \lambda + 2\alpha, \dots, x \equiv \lambda + \left(\frac{p-1}{\alpha} - 1 \right) \alpha \pmod{p-1}.$$

Доказательство. Если λ и α удовлетворяютъ сравненіямъ

$$a^\lambda \equiv A, a^\alpha \equiv 1 \pmod{p};$$

то

$$a^\lambda \equiv A, a^\alpha \equiv 1 \pmod{p}$$

Возведя обѣ части послѣдняго сравненія въ какую нибудь степень n и перемноживъ его почленно съ $a^\lambda \equiv A \pmod{p}$, находимъ

$$a^{\lambda + n\alpha} \equiv A \pmod{p}$$

Откуда ясно, что $\lambda + n\alpha$ удовлетворяет сравненію $a^x \equiv A \pmod{p}$, какое бы ни было цѣлое число n .

Не трудно также убѣдиться, что кромѣ чиселъ вида $\lambda + n\alpha$ нѣтъ другихъ способныхъ удовлетворить сравненію $a^x \equiv A \pmod{p}$.

Въ самомъ дѣлѣ, если $a^x \equiv A \pmod{p}$; то $a^x \equiv a^{\lambda} \pmod{p}$; ибо, по положенію, λ удовлетворяетъ сравненію $a^{\lambda} \equiv A \pmod{p}$. Но сокращая сравненіе $a^x \equiv a^{\lambda} \pmod{p}$ на a^{λ} , находимъ $a^{x-\lambda} \equiv 1 \pmod{p}$, что по 43-й теоремѣ предполагаетъ дѣлимость $x - \lambda$ на α . Полагая же частное отъ дѣленія $x - \lambda$ на α равнымъ n , находимъ $x - \lambda = n\alpha$ и слѣд. $x = \lambda + n\alpha$.

Итакъ числа, удовлетворяющія сравненію $a^x \equiv A \pmod{p}$, опредѣляются формулою $x = \lambda + n\alpha$, гдѣ n какое нибудь число. Но эта формула при значеніяхъ n сравнимыхъ по модулю $\frac{p-1}{\alpha}$ даетъ числа сравнимыя между собою по модулю $p-1$; и обратно при двухъ значеніяхъ n , несравнимыхъ по модулю $\frac{p-1}{\alpha}$, значенія $\lambda + n\alpha$ будутъ также несравнимы. Въ этомъ мы убѣждаемся, замѣтивъ, что сравненіе

$$\lambda + n\alpha \equiv \lambda + n'\alpha \pmod{p-1}$$

по уничтоженіи λ и сокращеніи α въ обѣихъ частяхъ сравненія по модулю приводится къ слѣдующему

$$n \equiv n' \pmod{\frac{p-1}{\alpha}}$$

Но по модулю $\frac{p-1}{\alpha}$ всѣ числа сравнимы съ однимъ изъ слѣдующихъ

$$0, 1, 2, \dots, \frac{p-1}{\alpha} - 1,$$

которые несравнимы между собою; слѣд. всѣ числа, опредѣляемые формулою $x = \lambda + n\alpha$, будутъ сравнимы по модулю p съ однимъ изъ чиселъ

$$\lambda, \lambda + \alpha, \lambda + 2\alpha, \dots, \lambda + \alpha \left(\frac{p-1}{\alpha} - 1 \right);$$

сами же они другъ съ другомъ будутъ несравнимы. А потому

всѣ числа вида $\lambda + n\alpha$, или, что одно и тоже, удовлетворяющія сравненію $a^x \equiv A \pmod{p}$, опредѣляются сравненіями

$$x \equiv \lambda, x \equiv \lambda + \alpha, x \equiv \lambda + 2\alpha, \dots, x \equiv \lambda + \alpha \left(\frac{p-1}{\alpha} - 1 \right) \pmod{p-1},$$

и эти сравненія всѣ различны между собою; откуда и слѣдуетъ предложенная нами теорема.

Такъ замѣчая, что сравненію $2^x \equiv 13 \pmod{17}$ удовлетворяетъ $x = 6$, наименьшее же число, удовлетворяющее сравненію $2^x \equiv 1 \pmod{17}$, есть 8, мы заключаемъ, что сравненіе $2^x \equiv 13 \pmod{17}$ имѣетъ $\frac{17-1}{8}$, или 2 рѣшенія, которыя суть

$$x \equiv 6, x \equiv 6 + 8 \pmod{16}.$$

§ 36. На основаніи доказанной нами теоремы число рѣшеній сравненія $a^x \equiv A \pmod{p}$, въ случаѣ его возможности, опредѣляется числомъ рѣшеній сравненія $a^x \equiv 1 \pmod{p}$. Теперь мы рассмотримъ особенно тотъ случай, когда сравненіе $a^x \equiv 1 \pmod{p}$ имѣетъ одно рѣшеніе и слѣд. наименьшее число, удовлетворяющее сравненію $a^x \equiv 1 \pmod{p}$, есть $p - 1$. Въ этомъ случаѣ число a получаетъ названіе первообразнаго корня числа p и сравненіе $a^x \equiv A \pmod{p}$ особенно замѣчательно по своимъ приложеніямъ. Этимъ сравненіемъ мы теперь и займемся. Относительно его мы докажемъ слѣдующую теорему:

45. ТЕОРЕМА.

Если a есть первообразный корень числа p , и A не дѣлится на p ; то сравненіе $a^x \equiv A \pmod{p}$ имѣетъ одно рѣшеніе.

Доказательство. Въ самомъ дѣлѣ, по свойству первообразнаго корня a наименьшее число, удовлетворяющее сравненію $a^x \equiv 1 \pmod{p}$, есть $p - 1$. Но въ этомъ случаѣ по предыдущей теоремѣ сравненіе $a^x \equiv A \pmod{p}$ или имѣетъ одно рѣшеніе или не имѣетъ ни одного. Докажемъ же, что последнее не можетъ имѣть мѣста при A недѣлящемся на p . Для этого

допустивъ , что сравненіе $a^x \equiv A \pmod{p}$ не имѣеть рѣшенія, мы замѣчаемъ, что A , не будучи кратнымъ p , при дѣленіи на p даетъ въ остаткѣ одно изъ чиселъ

$$1, 2, \dots, p - 1,$$

и слѣд. съ однимъ изъ этихъ чиселъ будетъ сравнимо по модулю p . Пусть это число будетъ r . Имѣя $A \equiv r \pmod{p}$, мы изъ сравненія $a^x \equiv A \pmod{p}$ выведемъ $a^x \equiv r \pmod{p}$, которое не будетъ имѣть рѣшенія; ибо по положенію не имѣеть его сравненіе $a^x \equiv A \pmod{p}$. Но такъ какъ a число простое съ p ; то $a^0, a^1, a^2, \dots, a^{p-2}$ не дѣлятся на p , и слѣд. каждое изъ нихъ по модулю p сравнимо съ однимъ изъ чиселъ

$$1, 2, 3, \dots, p - 1.$$

Откуда слѣдуетъ, что все $p - 1$ чиселъ $0, 1, 2, \dots, p - 2$ удовлетворяютъ какому либо изъ $p - 1$ сравненій

$$a^x \equiv 1, a^x \equiv 2, a^x \equiv 3, \dots, a^x \equiv p - 1 \pmod{p}.$$

Но такъ какъ одно изъ нихъ есть $a^x \equiv r \pmod{p}$, которое не имѣеть рѣшенія; то все $p - 1$ чиселъ $0, 1, 2, \dots, p - 2$ должны удовлетворять остальнымъ $p - 2$ сравненіямъ, и слѣд. по крайней мѣрѣ одному изъ нихъ удовлетворяютъ два числа изъ ряда $0, 1, 2, \dots, p - 2$, что не возможно; ибо это предполагаетъ въ этомъ сравненіи два рѣшенія. Итакъ нельзя допустить, чтобы сравненіе $a^x \equiv A \pmod{p}$ при A недѣлящемся на p не имѣло рѣшенія, а это и слѣдовало доказать.

На основаніи этой теоремы мы заключаемъ, что если a есть первообразный корень числа p ; то для всякаго числа A , недѣлящагося на p , сравненіе $a^x \equiv A \pmod{p}$ будетъ имѣть одно рѣшеніе, и слѣд. будетъ удовлетворяться однимъ числомъ меньшимъ $p - 1$ и не меньшимъ нуля. Такое число называютъ *указателемъ* числа A ; первообразный же корень a получаетъ въ этомъ случаѣ названіе *основанія указателей*. Итакъ число x будетъ указателемъ числа A , по основанію a , если x , будучи меньше $p - 1$ и не меньше 0, удовлетворяетъ сравненію $a^x \equiv A \pmod{p}$, и въ этомъ случаѣ мы будемъ писать такъ

$$x = \text{Ind. } A.$$

По сказанному нами мы найдем *Ind. A*, рѣшая сравненіе $a^x \equiv A \pmod{p}$ и выбирая между числами удовлетворяющими ему то, которое меньше $p - 1$ и не меньше нуля. Такъ при однихъ и тѣхъ же модулѣ p и основаніи a мы найдемъ одну величину для указателя какого либо числа A , недѣляющагося на p . Обратно зная, что $\text{Ind. } A = x$, мы для опредѣленія числа A будемъ имѣть сравненіе $a^x \equiv A \pmod{p}$. Но этимъ не опредѣляется вполнѣ число A ; этому сравненію удовлетворяютъ все числа, сравнимыя съ A по модулю p , и слѣд. все они имѣютъ одинъ и тотъ же указатель. Итакъ зная указатель A , мы будемъ знать только число, съ которымъ A сравнимо по модулю p . Это число опредѣляется сравненіемъ $A \equiv a^x \pmod{p}$, при $x = \text{Ind. } A$. Пояснимъ это примѣромъ. Пусть будетъ $p = 7$. Такъ какъ сравненію $3^x \equiv 1 \pmod{7}$ не удовлетворяютъ числа 1, 2, 3, 4, 5; то 3 есть первообразный корень числа 7. Примемъ же его за основаніе и найдемъ указателей 1, 2, 3, 4, 5, которые будутъ также указателями всехъ чиселъ, сравнимыхъ съ 1, 2, 3, 4, 5 по модулю 7.

Чтобы найти указателя 1, мы должны рѣшить сравненіе $2^x \equiv 1 \pmod{7}$.

Но ему, очевидно, удовлетворяетъ 0; слѣд.

$$\text{Ind. } 1 = 0.$$

Не трудно убѣдиться, что и всегда указатель 1 есть 0; ибо сравненію $a^x \equiv 1 \pmod{p}$ всегда удовлетворяетъ $x = 0$.

Чтобы найти указателей 2, 3, 4, 5, 6, мы должны рѣшить сравненія

$$3^x \equiv 2, 3^x \equiv 3, 3^x \equiv 4, 3^x \equiv 5, 3^x \equiv 6 \pmod{7},$$

и между числами ему удовлетворяющими найти тѣ, которые меньше $7 - 1$ и не меньше 0; а это приводится къ тому, чтобы найти, которое изъ чиселъ

$$3^1, 3^2, 3^3, 3^4, 3^5$$

сравнимо съ 2, 3, 4, 5, 6 по модулю 7. Но такъ какъ эти числа равны

3, 9, 27, 81, 243,

и остатки отъ дѣленія ихъ на 7 суть

3, 2, 6, 4, 5;

то мы заключаемъ, что

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5 \pmod{7}.$$

Слѣд.

$$Ind. 3 = 1, \quad Ind. 2 = 2, \quad Ind. 6 = 3, \quad Ind. 4 = 4, \quad Ind. 5 = 5.$$

Отсюда для опредѣленія указателей чиселъ 1, 2, 3, 4, 5, по модулю 7 и основанію 3, выходитъ такая таблица

$$Ind. 1 = 0,$$

$$Ind. 2 = 2,$$

$$Ind. 3 = 1,$$

$$Ind. 4 = 4,$$

$$Ind. 5 = 5,$$

$$Ind. 6 = 3.$$

По этой таблицѣ мы находимъ указателей всякаго числа A , простаго съ 7, замѣчая, что такое число будетъ сравнимо по модулю 7 съ однимъ изъ чиселъ 1, 2, 3, 4, 5, 6 и слѣд. съ этимъ числомъ имѣеть одного указателя. Такъ для опредѣленія указателей 20 и -18 , мы находимъ, что по модулю 7 эти числа сравнимы съ 6 и 3. Откуда слѣдуетъ

$$Ind. 20 = Ind. 6 = 3,$$

$$Ind. -18 = Ind. 3 = 1.$$

Для опредѣленія чиселъ по данному указателю мы предыдущую таблицу расположимъ такъ :

$$0 = Ind. 1,$$

$$1 = Ind. 3,$$

$$2 = Ind. 2,$$

$$3 = Ind. 6,$$

$$4 = Ind. 4,$$

$$5 = Ind. 5.$$

По этой таблицѣ мы найдемъ, какое изъ чиселъ 1, 2, 3, 4, 5 имѣеть данный указатель. Такъ найдемъ, что указатель 3 принадлежитъ числу 6. Откуда заключаемъ, что всѣ числа, имѣющія

*

указателемъ 3 по модулю 7 и основанію 3, сравнимы съ 6 по модулю 7.

Изъ сказаннаго нами видно, что составленіе таблицъ указателей не представляетъ никакихъ затрудненій, когда найдены первообразные корни. Но какъ найти ихъ — мы покажемъ впоследствии. Теперь же мы займемся изложеніемъ свойствъ указателей, на основаніи которыхъ таблицы ихъ могутъ быть употребляемы съ чрезвычайною выгодною при рѣшеніи многихъ вопросовъ Теоріи чиселъ. Въ концѣ этой книги помѣщены таблицы указателей для модулей меньшихъ 200. Онѣ заимствованы нами изъ лекцій Алгебраическаго и Трансцендентнаго Анализа Г-на Академика Остроградскаго. Таблицы подъ буквою *I* служатъ для опредѣленія указателей по данному числу; таблицы же подъ буквою *N* по данному указателю служатъ для опредѣленія чиселъ. Въ тѣхъ и другихъ таблицахъ данное (будетъ ли это указатель или число) разбивается на десятки и единицы; единицы находятся въ верхней строкѣ, десятки въ крайней лѣвой; искомое же находится на одной вертикальной съ единицами и на одной горизонтальной съ десятками.

Такъ, чтобы найти указателя 167 по модулю 193, мы въ таблицѣ подъ буквою *I* для модуля 193 ищемъ въ верхней строкѣ 7, а въ крайней слѣва 16; число же на одной горизонтальной съ 16 и на одной вертикальной съ 7 есть 101; это и есть искомый указатель 167. Обратнo желая опредѣлить притомъ же модуль и основаніи какія числа имѣютъ указателемъ 101, мы въ таблицѣ подъ буквою *N* въ верхней строкѣ ищемъ 1, въ крайней 10; соответствующее имъ число въ таблицѣ 167. Откуда заключаемъ, что числа, имѣющія указателемъ 101, сравнимы съ 167 по модулю 193.

§ 37. Займемся теперь изслѣдованіемъ свойствъ указателей, на которыхъ основывается употребленіе ихъ таблицъ.

46. ТЕОРЕМА.

При модуль p указатель произведения нескольких чисел сравнимъ съ суммою ихъ указателей по модулю $p - 1$.

Доказательство. Пусть будетъ A, B, C, \dots данныя числа и i, i', i'', \dots ихъ указатели по модулю p и основанію a ; по свойству указателей будетъ

$$a^i \equiv A, a^{i'} \equiv B, a^{i''} \equiv C, \dots \pmod{p}.$$

Перемножая эти сравненія между собою, найдемъ

$$a^{i+i'+i''+\dots} \equiv ABC\dots \pmod{p}.$$

Но если I есть указатель $ABC\dots$; то

$$a^I \equiv ABC\dots \pmod{p}.$$

Изъ этого же сравненія и предыдущаго выходитъ

$$a^{i+i'+i''+\dots} \equiv a^I \pmod{p},$$

что по сокращеніи на a^I даетъ

$$a^{i+i'+i''+\dots-I} \equiv 1 \pmod{p}.$$

Итакъ число $i + i' + i'' + \dots - I$ удовлетворяетъ сравненію $a^x \equiv 1 \pmod{p}$, а это по теоремѣ 43-й предполагаетъ, что это число есть кратное наименьшаго числа, удовлетворяющаго сравненію $a^x \equiv 1 \pmod{p}$, которое по свойству первообразныхъ корней есть $p - 1$. Слѣд. разность $i + i' + i'' + \dots - I$ дѣлится на $p - 1$, а это выражается сравненіемъ

$$I \equiv i + i' + i'' + \dots \pmod{p - 1},$$

что и слѣдовало доказать.

Такъ по модулю 199 и основанію 127 находимъ

$$\text{Ind. } 2 = 194, \text{ Ind. } 5 = 6, \text{ Ind. } 19 = 11,$$

слѣдовательно

$$\text{Ind. } 2 \cdot 5 \cdot 19 \equiv 194 + 6 + 11 \pmod{198},$$

или

$$\text{Ind. } 190 \equiv 211 \pmod{198}.$$

Замѣчая, что число меньшее 198 и сравнимое съ 211 по модулю 198 есть 13, мы заключаемъ, что $\text{Ind. } 190 = 13$. Такъ

мы можем всегда найти указателя составнаго числа, зная указателей простыхъ чисель, входящихъ въ составъ его.

На основаніи доказанной нами теоремы мы заключаемъ, что указатель степени сравнимъ по модулю $p - 1$ съ произведе- ніемъ показателя степени на указателя корня. Въ самомъ дѣлѣ, мы нашли, что

$$\text{Ind. } ABC \dots \equiv \text{Ind. } A + \text{Ind. } B + \text{Ind. } C \dots \pmod{p - 1}.$$

Предполагая здѣсь $A = B = C = \dots$ и называя n число чисель A, B, C, \dots , мы находимъ

$$\text{Ind. } A^n \equiv n \cdot \text{Ind. } A \pmod{p - 1}.$$

Такъ при модулѣ 199 находимъ $\text{Ind. } 2^5 \equiv 3 \text{ Ind. } 2 \pmod{198}$. Но $\text{Ind. } 2$ есть 194. Слѣд. $\text{Ind. } 2^5 \equiv 3 \cdot 194 \equiv 582 \pmod{198}$.

47. ТЕОРЕМА.

Если x удовлетворяетъ сравненію $Ax^n \equiv B \pmod{p}$, гдѣ A и B числа недѣляющіяся на p и p число простое; то указатель x удовлетворяетъ сравненію $n \cdot \text{Ind. } x \equiv \text{Ind. } B - \text{Ind. } A \pmod{p - 1}$.

Доказательство. Такъ какъ два числа, сравнимыя по модулю p , имѣютъ одного указателя при томъ же модулѣ; то изъ сравненія

$$Ax^n \equiv B \pmod{p}$$

выходитъ

$$\text{Ind. } Ax^n = \text{Ind. } B.$$

Но по предыдущей теоремѣ $\text{Ind. } Ax^n$ по модулю $p - 1$ сравнимъ съ $\text{Ind. } A + \text{Ind. } x^n$, а $\text{Ind. } x^n$ сравнимъ съ $n \text{ Ind. } x$; слѣдовательно

$$\text{Ind. } A + n \text{ Ind. } x \equiv \text{Ind. } B \pmod{p - 1};$$

откуда выходитъ

$$n \cdot \text{Ind. } x \equiv \text{Ind. } B - \text{Ind. } A \pmod{p - 1},$$

что и слѣдовало доказать.

На основаніи этой теоремы легко рѣшаются всѣ сравненія вида $Ax^n \equiv B \pmod{p}$ при p простомъ, A и B недѣлящихся

на p . Сюда относятся сравненія первой степени, сравненія второй степени вида $x^2 \equiv q \pmod{p}$ и всѣ сравненія двучленные.

Начнемъ съ приложенія этой теоремы къ сравненіямъ первой степени. Если данное сравненіе есть $Ax \equiv B \pmod{p}$; то на основаніи предыдущей теоремы найдемъ

$$\text{Ind. } x \equiv \text{Ind. } B - \text{Ind. } A \pmod{p - 1}.$$

Замѣчая, что $\text{Ind. } x$ не можетъ быть менѣе 0 и болѣе $p - 2$; мы изъ этого сравненія найдемъ его величину, опредѣляя наименьшее положительное число, сравнимое съ $\text{Ind. } B - \text{Ind. } A$ по модулю $p - 1$. Найдя указателя x , мы по таблицѣ найдемъ число, съ которымъ x сравнимо по модулю p ; это и будетъ искомое рѣшеніе.

Такъ для рѣшенія сравненія

$$10x \equiv 9 \pmod{11}$$

находимъ

$$\text{Ind. } x \equiv \text{Ind. } 9 - \text{Ind. } 10 \pmod{10}.$$

Но изъ таблицъ указателей видимъ, что

$$\text{Ind. } 9 = 6, \text{ Ind. } 10 = 5;$$

откуда выходитъ

$$\text{Ind. } x \equiv 6 - 5 \equiv 1 \pmod{10},$$

и слѣдовательно $\text{Ind. } x = 1$. Но $\text{Ind. } x = 1$ соответствуетъ $x = 2$, слѣд. $x \equiv 2 \pmod{11}$.

Для рѣшенія сравненія $x^2 \equiv q \pmod{p}$, мы изъ предыдущей теоремы выводимъ

$$2 \text{ Ind. } x \equiv \text{Ind. } q \pmod{p - 1}.$$

Предполагая здѣсь p числомъ нечетнымъ, мы замѣчаемъ, что коэффициентъ искомага $\text{Ind. } x$ и модуль имѣютъ общимъ наибольшимъ дѣлителемъ 2. Изъ этого по теоремѣ 18-й мы заключаемъ, что это сравненіе и слѣд. $x^2 \equiv q \pmod{p}$ не имѣютъ рѣшенія, если $\text{Ind. } q$ не дѣлится на 2. Въ противномъ случаѣ по теоремѣ 19-й сравненіе $2 \text{ Ind. } x \equiv \text{Ind. } q \pmod{p - 1}$ будетъ имѣть два рѣшенія и слѣд. найдется два числа въ рядѣ 0, 1, 2, ..., $p - 2$ ему удовлетворяющія. Эти числа будутъ зна-

ченія $Ind. x$ и по нимъ мы найдемъ два рѣшенія сравненія $x^2 \equiv q \pmod{p}$.

Для примѣра возьмемъ сравненіе

$$x^2 \equiv 10 \pmod{101}.$$

Рѣшеніе его приведется къ сравненію

$$2 Ind. x \equiv Ind. 10 \pmod{100}.$$

Но по таблицамъ находимъ $Ind. 10 = 25$, что на 2 не дѣлится, слѣд. это сравненіе не имѣетъ рѣшенія. Дѣйствительно, опредѣляя значеніе $\left(\frac{10}{101}\right)$, находимъ

$$\left(\frac{10}{101}\right) = \left(\frac{2}{101}\right) \left(\frac{5}{101}\right) = - \left(\frac{5}{101}\right) = - \left(\frac{101}{5}\right) = - \left(\frac{1}{5}\right) = -1,$$

что обнаруживаетъ невозможность сравненія $x^2 \equiv 10 \pmod{101}$.

Для другаго примѣра возьмемъ сравненіе

$$x^2 \equiv 30 \pmod{107}.$$

Рѣшеніе этого сравненія приводится къ такому

$$2 Ind. x \equiv Ind. 30 \pmod{106}.$$

Но $Ind. 30$ есть 80, число четное. Слѣд. это сравненіе имѣетъ рѣшеніе.

Рѣшая сравненіе

$$2 Ind. x \equiv 80 \pmod{106},$$

мы находимъ, что наименьшія числа, ему удовлетворяющія, суть 40 и 93. Слѣд.

$$Ind. x = 40, Ind. x = 93.$$

Но эти показатели соотвѣтствуютъ числамъ 64 и 43. Слѣд. рѣшенія сравненія $x^2 \equiv 30 \pmod{107}$ суть

$$x \equiv 64, x \equiv 43 \pmod{107}.$$

Обращаемся теперь къ рѣшенію двучленныхъ сравненій $x^n \equiv B \pmod{p}$.

Рѣшеніе этого сравненія по предыдущей теоремѣ приводится къ слѣдующему

$$n. Ind. x \equiv Ind. B \pmod{p - 1}.$$

По теоремѣ 18-ой это сравненіе будетъ невозможно, если общій наибольшій дѣлитель чиселъ n и $p - 1$ не дѣлитъ $Ind. B$, слѣд. въ этомъ случаѣ сравненіе

$$x^n \equiv B \pmod{p}$$

не имѣеть рѣшенія. Если же общій наибольшій дѣлитель n и $p - 1$ есть ω , и ω дѣлитъ $\text{Ind. } B$; то сравненіе

$$n. \text{Ind. } x \equiv \text{Ind. } B \pmod{p - 1}$$

по теоремѣ 19-й имѣеть ω рѣшеній. Откуда выходитъ ω различныхъ значеній $\text{Ind. } x$, и слѣд. ω рѣшеній сравненія $x^n \equiv B \pmod{p}$; все это подтверждаетъ намъ 38-ю теорему, по которой сравненіе $x^n \equiv B \pmod{p}$ или не имѣеть рѣшенія или имѣеть ихъ столько, сколько единицъ въ общемъ наибольшемъ дѣлителѣ чиселъ n и $p - 1$.

Для примѣра возьмемъ сравненіе $x^{12} \equiv 17 \pmod{127}$. Для рѣшенія этого сравненія выводимъ

$$12 \text{ Ind. } x \equiv \text{Ind. } 17 \pmod{126}.$$

Находя для величины $\text{Ind. } 17$ число 118, которое не дѣлится на 6, общаго наибольшаго дѣлителя 12 и 126, мы заключаемъ, что сравненіе

$$12 \text{ Ind. } x \equiv \text{Ind. } 17 \pmod{126},$$

и слѣд. сравненіе

$$x^{12} \equiv 17 \pmod{127}$$

не имѣеть рѣшенія.

Для другаго примѣра возьмемъ сравненіе

$$x^{12} \equiv 38 \pmod{127}.$$

Изъ этого сравненія выходитъ

$$12 \text{ Ind. } x \equiv \text{Ind. } 38 \pmod{126},$$

или

$$12 \text{ Ind. } x \equiv 60 \pmod{126}.$$

Здѣсь 60 дѣлится на 6, общій наибольшій дѣлитель чиселъ 12 и 126. Слѣд. это сравненіе имѣеть 6 рѣшеній; эти рѣшенія мы найдемъ по 19-й теоремѣ, сокращая въ предыдущемъ сравненіи модуль и обѣ части на 6. Это даетъ намъ

$$2 \text{ Ind. } x \equiv 10 \pmod{21}.$$

Рѣшая это сравненіе, мы находимъ, что наименьшее число, ему удовлетворяющее, есть 5. Откуда для рѣшенія сравненія

$$12 \text{ Ind. } x \equiv 60 \pmod{126}$$

ВЫХОДИТЬ

$$\left. \begin{array}{l} \text{Ind. } x \equiv 5, \text{ Ind. } x \equiv 26, \text{ Ind. } x \equiv 47, \\ \text{Ind. } x \equiv 68, \text{ Ind. } x \equiv 89, \text{ Ind. } x \equiv 110. \end{array} \right\} \pmod{126}.$$

Изъ этихъ же сравненій слѣдуютъ такія 6 значеній $\text{Ind. } x$
5, 26, 47, 68, 89, 110.

Но этимъ указателямъ соотвѣтствуютъ числа

$$65, 30, 92, 62, 97, 35.$$

Слѣд. рѣшенія сравненія $x^{12} \equiv 17 \pmod{127}$ суть
 $x \equiv 65, x \equiv 30, x \equiv 92, x \equiv 62, x \equiv 97, x \equiv 35 \pmod{127}$.

§ 38. Переходимъ теперь къ опредѣленію первообразныхъ
корней и докажемъ, что всякое число a простое съ p и не-
удовлетворяющее сравненіямъ

$$a^{\frac{p-1}{\alpha}} \equiv 1, a^{\frac{p-1}{\beta}} \equiv 1, a^{\frac{p-1}{\gamma}} \equiv 1, \dots \pmod{p},$$

гдѣ $\alpha, \beta, \gamma, \dots$ суть простые числа, входящія въ составъ $p-1$,
есть первообразный корень числа p .

Мы видѣли, что a будетъ первообразнымъ корнемъ числа p ,
если сравненіе $a^x \equiv 1 \pmod{p}$ не удовлетворяется числомъ
мѣньшимъ $p-1$. Покажемъ же, что это будетъ имѣть мѣсто въ
сдѣланныхъ нами предположеніяхъ. Для этого мы допустимъ
противное и обнаружимъ несообразность его.

Если сравненіе $a^x \equiv 1 \pmod{p}$ удовлетворяется при $x < p-1$;
то по теоремѣ 42-й удовлетворяется сравненіе $a^{\omega} \equiv 1 \pmod{p}$,
гдѣ ω общій наибольшій дѣлитель чиселъ $p-1$ и x , и слѣд.
 ω меньше $p-1$. Поэтому дробь $\frac{p-1}{\omega}$ приведетъ къ цѣлому
числу, превосходящему 1. Но въ составъ этого числа мо-
гутъ входить только числа $\alpha, \beta, \gamma, \dots$, входящія въ составъ
 $p-1$; слѣдов. одно изъ чиселъ $\alpha, \beta, \gamma, \dots$ дѣлитъ частное
 $\frac{p-1}{\omega}$. Пусть же это будетъ β и частное отъ дѣленія $\frac{p-1}{\omega}$ на β
пусть будетъ ζ . Имѣя

$$\frac{p-1}{\omega\beta} = \zeta,$$

мы выводимъ

$$\omega_s = \frac{p-1}{\beta}.$$

На основаніи же этого уравненія, мы изъ сравненія

$$a^\omega \equiv 1 \pmod{p},$$

возводя обѣ части его въ степень s , находимъ

$$a^{\frac{p-1}{\beta}} \equiv 1 \pmod{p},$$

что противно положенію.

Итакъ сравненіе $a^x \equiv 1 \pmod{p}$ не можетъ удовлетворяться при $x < p-1$, а потому a есть первообразный корень числа p , что и слѣдовало доказать.

На основаніи этого не трудно доказать слѣдующую теорему:

48. ТЕОРЕМА.

Если для a невозможны сравненія

$$x^\alpha \equiv a, x^\beta \equiv a, x^\gamma \equiv a, \dots \pmod{p},$$

гдѣ $\alpha, \beta, \gamma, \dots$ суть простые числа, входящія въ составъ $p-1$; то a есть первообразный корень. Въ противномъ случаѣ a не есть первообразный корень.

Доказательство. По теоремѣ 38-й отсутствіе рѣшеній въ сравненіяхъ

$$x^\alpha \equiv a, x^\beta \equiv a, x^\gamma \equiv a, \dots \pmod{p},$$

гдѣ $\alpha, \beta, \gamma, \dots$ суть дѣлители $p-1$, предполагаетъ, что сравненія

$$a^{\frac{p-1}{\alpha}} \equiv 1, a^{\frac{p-1}{\beta}} \equiv 1, a^{\frac{p-1}{\gamma}} \equiv 1, \dots \pmod{p}$$

не имѣютъ рѣшенія, а въ этомъ случаѣ, какъ доказали, число a есть первообразный корень числа p .

Напротивъ того, если какое нибудь изъ сравненій

$$x^\alpha \equiv a, x^\beta \equiv a, x^\gamma \equiv a, \dots \pmod{p}$$

удовлетворяется; то имѣетъ мѣсто одно изъ сравненій

$$a^{\frac{p-1}{\alpha}} \equiv 1, a^{\frac{p-1}{\beta}} \equiv 1, a^{\frac{p-1}{\gamma}} \equiv 1, \dots \pmod{p},$$

и слѣд. число a не есть первообразный корень.

§ 39. На основаніи этой теоремы легко найти всё числа въ рядѣ 1, 2, 3, $p - 1$, которыя не суть первообразные корни. По доказанной нами теоремѣ, если a не есть первообразный корень p , то какое нибудь изъ сравненій

$$x^\alpha \equiv a, x^\beta \equiv a, x^\gamma \equiv a, \dots \pmod{p}$$

имѣеть рѣшеніе, а это мы узнаемъ потому, что одно изъ сравненій

$$\left. \begin{aligned} 1^\alpha &\equiv a, 2^\alpha \equiv a, 3^\alpha \equiv a, \dots (p-1)^\alpha \equiv a, \\ 1^\beta &\equiv a, 2^\beta \equiv a, 3^\beta \equiv a, \dots (p-1)^\beta \equiv a, \\ 1^\gamma &\equiv a, 2^\gamma \equiv a, 3^\gamma \equiv a, \dots (p-1)^\gamma \equiv a, \\ &\dots \dots \dots \dots \dots \dots \dots \dots \dots \end{aligned} \right\} \pmod{p}$$

удовлетворяется. Слѣд. число a , не будучи первообразнымъ корнемъ, будетъ сравнимо по модулю p съ однимъ изъ чиселъ

$$\begin{aligned} 1^\alpha, 2^\alpha, 3^\alpha, \dots (p-1)^\alpha, \\ 1^\beta, 2^\beta, 3^\beta, \dots (p-1)^\beta, \\ 1^\gamma, 2^\gamma, 3^\gamma, \dots (p-1)^\gamma, \end{aligned}$$

а потому между остатками отъ дѣленія этихъ чиселъ на p найдутся всё числа, которыя меньше p и не первообразные корни p . Выкинувъ же эти числа изъ ряда

$$1, 2, 3, 4, \dots p - 1,$$

мы найдемъ всё первообразные корни меньше p . Что же касается до чиселъ, которыя превосходятъ p и имѣють свойство первообразныхъ корней, они, какъ не трудно убѣдиться, будутъ сравнимы съ первыми по модулю p ; мы на нихъ не будемъ останавливаться, потому что они ничего особеннаго не представляютъ и говоря о числѣ первообразныхъ корней p , мы будемъ разумѣть только тѣ, которые меньше p .

Приложимъ сказанное нами къ опредѣленію первообразныхъ корней числа 13. Такъ какъ въ составъ $13 - 1$ входятъ 2 и 3; то въ рядѣ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 всё числа, отличныя отъ остатковъ дѣленія

$$\begin{aligned} 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, \\ 1^3, 2^3, 3^3, 4^3, 5^3, 6^3, 7^3, 8^3, 9^3, 10^3, 11^3, 12^3 \end{aligned}$$

на 13 будутъ первообразные корни.

Но дѣля

$$1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2$$

на 13, мы находимъ такой рядъ остатковъ

$$1, 4, 9, 3, 12, 10, 10, 12, 3, 9, 4, 1;$$

дѣля же

$$1^3, 2^3, 3^3, 4^3, 5^3, 6^3, 7^3, 8^3, 9^3, 10^3, 11^3, 12^3$$

находимъ остатки

$$1, 8, 1, 12, 8, 8, 5, 5, 1, 12, 5, 12.$$

Исключая изъ ряда

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$$

числа равныя этимъ остаткамъ, находимъ, что первообразные корни числа 13 суть

$$2, 6, 7, 11.$$

§ 40. Показанный нами способъ опредѣленія первообразныхъ корней, замѣчательный тѣмъ, что даетъ всѣ эти корни, становится почти не выполнимымъ, когда ищутъ первообразные корни числа довольно большаго. Въ этомъ случаѣ легче бываетъ найти одинъ изъ первообразныхъ корней (чего для насъ, какъ увидимъ, совершенно достаточно), пробуя различныя числа возводить въ степени и искать, которая изъ нихъ сравнима съ 1 по модулю p , числу котораго ищемъ первообразный корень. Если возводя a въ степени 1, 2, 3,..... мы дойдемъ до a^{p-1} , не найдя между ними числа сравнимаго съ 1 по модулю p , мы заключаемъ, что a есть первообразный корень числа p . Если же мы найдемъ, что $a^n \equiv 1 \pmod{p}$, гдѣ n меньше $p - 1$; то мы убѣдимся, что a непервообразный корень. Въ этомъ случаѣ мы будемъ искать число, котораго наименьшая степень, сравнимая съ единицею по модулю p , превосходитъ бы n и такое число мы всегда найдемъ, поступая слѣдующимъ образомъ.

Мы возьмемъ число изъ ряда

$$1, 2, 3, \dots \dots \dots p - 1,$$

отличное отъ остатковъ дѣленія

$$a^1, a^2, a^3, \dots \dots \dots a^n$$

на p и станем искать низшую степень его, сравнимую с единицею по модулю p . Пусть выбранное нами число будетъ b и низшая степень его сравнимая с единицею будетъ m . Не трудно убѣдиться, что m не будетъ ни равнымъ n , ни дѣлителемъ n ; ибо въ томъ и другомъ случаѣ число b удовлетворяло бы сравненію $b^n \equiv 1 \pmod{p}$, что не возможно по теоремѣ 37-й при b несравнимомъ съ a^1, a^2, \dots, a^{n-1} по модулю p и n наименьшемъ числѣ, удовлетворяющемъ сравненію $a^n \equiv 1 \pmod{p}$. Поэтому или m будетъ больше n и слѣд. само b будетъ числомъ, котораго низшая степень, сравнимая с единицею, превосходитъ n , или m , будучи меньше n , въ составѣ своемъ будетъ заключать множителя недѣлящаго n . Въ послѣднемъ случаѣ мы легко найдемъ по a, b, m и n число, котораго низшая степень, сравнимая с единицею, превосходитъ n . Для этого мы найдемъ общаго наибольшаго дѣлителя чиселъ m и n , и этого дѣлителя разложимъ на два множителя π и ζ такъ, чтобы $\frac{n}{\pi}$ и $\frac{m}{\zeta}$ были числа относительно другъ друга простыя (*); потомъ найдемъ значеніе $a^\pi b^\zeta$ или числа сравнимаго съ нимъ по модулю p . Такого числа низшая степень, сравнимая с единицею, будетъ всегда болѣе n . Чтобы убѣдиться въ этомъ, мы докажемъ, что если

$$c \equiv a^\pi b^\zeta, \quad c^N \equiv 1 \pmod{p};$$

то N дѣлится на $\frac{mn}{\pi\zeta}$ и слѣд. низшая степень c , сравнимая с единицею по модулю p , превосходитъ n ; ибо $\pi\zeta$, будучи общимъ дѣлителемъ m и n , гдѣ m не дѣлитъ n , будетъ меньше m .

(*) Чтобы сдѣлать такое разложеніе ω , общаго наибольшаго дѣлителя чиселъ m и n , мы разложимъ его на произведеніе простыхъ чиселъ и возьмемъ въ составъ π тѣ простые числа, которыхъ показатели въ ω не ниже показателей въ n ; въ составъ же возьмемъ тѣ простые числа, которыхъ показатели въ ω не ниже чѣмъ въ m . Что-же касается до простыхъ чиселъ, которыхъ показательъ въ m и n и слѣд. въ ω одинъ и тотъ-же, мы ихъ безъ различія можемъ взять въ составъ π или ζ .

Чтобы доказать дѣлимость N на $\frac{mn}{\pi\zeta}$, гдѣ

$$c^N \equiv 1, c \equiv a^\pi b^\zeta \pmod{p},$$

мы замѣчаемъ, что изъ этихъ сравненій по исключеніи c вы-
ходитьъ

$$a^{\pi N} b^{\zeta N} \equiv 1 \pmod{p}.$$

Возводя-же это сравненіе въ степени $\frac{n}{\pi}, \frac{m}{\zeta}$, находимъ

$$a^{nN} b^{\frac{\zeta n N}{\pi}} \equiv 1, a^{\frac{m \pi N}{\zeta}} b^{Nm} \equiv 1 \pmod{p}.$$

Но мы видѣли, что m и n удовлетворяютъ сравненіямъ

$$a^n \equiv 1, b^m \equiv 1 \pmod{p};$$

вслѣдствіе чего предыдущія сравненія приводятся къ

$$b^{\frac{n\zeta N}{\pi}} \equiv 1, a^{\frac{m\pi N}{\zeta}} \equiv 1 \pmod{p}.$$

Эти-же сравненія по теоремѣ 43 предполагаютъ, что $\frac{Nn\zeta}{\pi}$
дѣлится на m , $\frac{m\pi N}{\zeta}$ дѣлится на n ; ибо n и m суть наимень-
шія числа, удовлетворяющія сравненіямъ

$$a^x \equiv 1, b^x \equiv 1 \pmod{p}.$$

Но дѣлимость $\frac{n\zeta N}{\pi}$ на m , $\frac{m\pi N}{\zeta}$ на n предполагаетъ числа

$\frac{n\zeta N}{\pi m}, \frac{m\pi N}{\zeta n}$, или $\frac{N \frac{n}{\pi}}{\frac{m}{\zeta}}, \frac{N \frac{m}{\zeta}}{\frac{n}{\pi}}$ цѣлыми. А потому число $\frac{m}{\zeta} N$ должно

дѣлиться на $\frac{n}{\pi}$, а число $\frac{n}{\pi} N$ должно дѣлиться на $\frac{m}{\zeta}$. Но эта

дѣлимость при $\frac{m}{\zeta}$ и $\frac{n}{\pi}$ простыхъ между собою, предполагаетъ

дѣлимость N на числа $\frac{n}{\pi}$ и $\frac{m}{\zeta}$, и слѣд. на произведеніе ихъ

$\frac{mn}{\pi\zeta}$, что и имѣли въ виду доказать.

Такимъ образомъ по числу, котораго низшая степень, срав-
нимая съ единицею по модулю p , есть n , гдѣ n меньше $p - 1$,
мы всегда найдемъ число, котораго низшая степень, сравнимая
съ единицею, будетъ превосходить n ; и слѣд. повторяя эти

приемы достаточное число разъ. мы необходимо дойдемъ до числа, котораго низшая степень, сравнимая съ единицею по модулю p , будетъ не меньше $p - 1$; такое число и будетъ первообразный корень числа p .

Для примѣра опредѣлимъ по этому способу первообразный корень числа 17. Испытываемъ не есть ли 2 первообразный корень его. Для этого дѣлимъ

$$2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, \dots$$

на 17; въ остаткѣ отъ этихъ дѣлений находимъ

$$1, 2, 8, 16, 15, 13, 9, 1, \dots$$

Дойдя до остатка 1, который получаемъ при дѣленіи 2^8 на 17, мы оканчиваемъ дѣленіе и заключаемъ, что 2 не есть первообразный корень. Послѣ того беремъ другое число меньшее 17 и не заключающееся между остатками 1, 2, 8, 16, 15, 13, 9 и пробуемъ не есть-ли оно первообразный корень. Наименьшее изъ этихъ чиселъ есть 3; его мы и беремъ для испытанія.

Дѣля

$$3, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7, 3^8, 3^9, 3^{10}, 3^{11}, 3^{12}, 3^{13}, 3^{14}, 3^{15}$$

на 17 и не находя въ остаткѣ 1, мы заключаемъ, что 3 есть первообразный корень 17.

Для другаго примѣра возьмемъ число 73 и найдемъ его первообразный корень. Начнемъ испытанія съ 2, какъ числа простѣйшаго. Дѣля числа

$$2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, \dots$$

на 73, мы найдемъ въ остаткѣ

$$2, 4, 8, 16, 32, 64, 55, 37, 1, \dots$$

Откуда видимъ, что 2 удовлетворяетъ сравненію

$$2^9 \equiv 1 \pmod{73},$$

и слѣд. 2 не есть первообразный корень. Далѣе, замѣчая, что между остатками

$$2, 4, 8, 16, 32, 64, 55, 37$$

нѣтъ числа 3, мы беремъ его для испытанія. Дѣля числа

$$3, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7, 3^8, 3^9, 3^{10}, 3^{11}, 3^{12}, \dots$$

на 73, находимъ въ остаткѣ

3, 9, 27, 8, 24, 72, 70, 64, 46, 65, 49, 1.....

Слѣдовательно

$$3^{12} \equiv 1 \pmod{73}.$$

Откуда заключаемъ, что 3 также не есть первообразный корень числа 73. Но изъ 2 и 3, удовлетворяющихъ сравненіямъ

$$2^9 \equiv 1, \quad 3^{12} \equiv 1 \pmod{73},$$

мы по сказанному нами легко составимъ число, котораго низшая степень, сравнимая съ 1 по модулю 73, будетъ больше 12.

Для этого мы замѣчаемъ, что общій наибольшій дѣлитель 9 и 12 есть 3 и это число, будучи простымъ, въ составъ 12 входитъ въ первой степени, а въ составъ 9 во второй; поэтому для разложенія 3 на два множителя π и ζ такъ, чтобы $\frac{9}{\pi}$, $\frac{12}{\zeta}$ были числа простые относительно другъ друга, мы возьмемъ $\pi=1$, $\zeta=3$. Вслѣдствіе чего $2 \cdot 3^3$, или 54 будетъ число, котораго низшая степень, сравнимая съ единицею по модулю 73, превзойдетъ 12. Опредѣляя остатки отъ дѣленія

$$\begin{aligned} &54, 54^2, 54^3, 54^4, 54^5, 54^6, 54^7, 54^8, 54^9, \\ &54^{10}, 54^{11}, 54^{12}, 54^{13}, 54^{14}, 54^{15}, 54^{16}, 54^{17}, 54^{18}, \\ &54^{19}, 54^{20}, 54^{21}, 54^{22}, 54^{23}, 54^{24}, 54^{25}, 54^{26}, 54^{27}, \\ &54^{28}, 54^{29}, 54^{30}, 54^{31}, 54^{32}, 54^{33}, 54^{34}, 54^{35}, 54^{36} \end{aligned}$$

на 73, находимъ

$$\begin{aligned} &54, 69, 3, 16, 61, 9, 48, 37, 27, \\ &71, 38, 8, 67, 41, 24, 55, 50, 72, \\ &19, 4, 70, 57, 12, 64, 25, 36, 46, \\ &2, 35, 65, 6, 32, 49, 18, 23, 1. \end{aligned}$$

Откуда заключаемъ, что 36 есть наименьшее число, удовлетворяющее сравненію

$$54^{36} \equiv 1 \pmod{73}.$$

Продолжая искать первообразный корень 73, мы должны взять число, не заключающееся между найденными нами остатками отъ дѣленія степеней 54 на 73. Наименьшее изъ этихъ чиселъ есть 5; его то мы и будемъ испытывать. Возводя 54 во все степени до 72-й, мы не находимъ числа, сравнимаго съ

1 по модулю 73. Слѣдов. наименьшее число, удовлетворяющее сравненію

$$5^x \equiv 1 \pmod{73},$$

есть 72; откуда заключаемъ, что 5 есть первообразный корень 73.

Такимъ образомъ мы найдемъ одинъ изъ первообразныхъ корней всякаго простаго числа. Но когда извѣстенъ одинъ первообразный корень числа p ; то мы легко найдемъ всѣ другіе. Въ самомъ дѣлѣ, пусть будетъ a найденный нами первообразный корень числа p , и $\alpha, \beta, \gamma, \dots$ различныя простыя числа, входящія въ составъ $p - 1$. Если A есть первообразный корень, то по теоремѣ 48-й сравненія

$$x^\alpha \equiv A, x^\beta \equiv A, x^\gamma \equiv A, \dots \pmod{p}$$

не должны имѣть рѣшенія. Но изъ этихъ сравненій выходятъ

$$\alpha \text{ Ind. } x \equiv \text{Ind. } A, \beta \text{ Ind. } x \equiv \text{Ind. } A, \gamma \text{ Ind. } x \equiv \text{Ind. } A, \dots \pmod{p-1},$$

а такъ какъ $\alpha, \beta, \gamma, \dots$ суть простыя числа, входящія въ составъ $p - 1$; то условіе невозможности ихъ заключается въ недѣлимости $\text{Ind. } A$ на $\alpha, \beta, \gamma, \dots$ или, что одно и то же, невозможность ихъ условливается тѣмъ, что $\text{Ind. } A$ число простое съ $p - 1$. Но если за основаніе указателей мы предположимъ принятымъ извѣстный намъ первообразный корень a ; то

$$A \equiv a^{\text{Ind. } A} \pmod{p}.$$

Откуда слѣдуетъ, что число, которое есть первообразный корень p , будетъ сравнимо по модулю p съ a , возведеннымъ въ степень простую съ $p - 1$.

Такъ всѣ первообразные корни числа 17 по найденному нами 3 опредѣляются сравненіями

$$x \equiv 3, x \equiv 3^5, x \equiv 3^9, x \equiv 3^7, x \equiv 3^3,$$

$$x \equiv 3^{11}, x \equiv 3^{13}, x \equiv 3^{15} \pmod{17};$$

откуда слѣдуетъ, что первообразные корни 17 суть

$$3, 10, 5, 11, 14, 7, 12, 6.$$

§ 41. На основаніи сказаннаго нами мы замѣчаемъ, что въ рядѣ $1, 2, \dots, p - 1$ находится столько первообразныхъ корней p , сколько чиселъ меньшихъ $p - 1$ и простыхъ съ $p - 1$.

Не трудно также вывести это непосредственно из свойств первообразных корней, показанных нами в § 38. Чтобы найти в рядъ

$$1, 2, 3, \dots, p-1$$

все первообразные корни числа p , намъ стоитъ только выкинуть отсюда все числа, которые не могутъ быть первообразными корнями числа p . Но по § 38 это приводится къ тому, чтобы здѣсь выкинуть все числа, которые удовлетворяютъ сравненіямъ

$$x^{\frac{p-1}{\alpha}} \equiv 1, x^{\frac{p-1}{\beta}} \equiv 1, x^{\frac{p-1}{\gamma}} \equiv 1, \dots \pmod{p},$$

гдѣ $\alpha, \beta, \gamma, \dots$ простые числа, входящія въ составъ $p-1$.

На основаніи этого не трудно сосчитать сколько первообразныхъ корней между числами $1, 2, 3, \dots, p-1$. Начнемъ съ простѣйшаго случая. Предположимъ, что $p-1$ дѣлится только на простое число α , и слѣд. $p-1 = \alpha^m$. Въ этомъ случаѣ все тѣ изъ чиселъ

$$1, 2, 3, \dots, p-1,$$

которые не удовлетворяютъ сравненію $x^{\frac{p-1}{\alpha}} \equiv 1 \pmod{p}$, будутъ первообразные корни. Но по теоремѣ 35 между числами $1, 2, 3, \dots, p-1$ находится $\frac{p-1}{\alpha}$ чиселъ, удовлетворяющихъ сравненію

$x^{\frac{p-1}{\alpha}} \equiv 1 \pmod{p}$; слѣд. здѣсь все остальные $p-1 - \frac{p-1}{\alpha}$

суть первообразные корни p . Число же $p-1 - \frac{p-1}{\alpha}$ приводится къ $(p-1) \left(1 - \frac{1}{\alpha}\right)$, а это по 12 теоремѣ означаетъ сколько простыхъ чиселъ съ $p-1$ и меньшихъ $p-1$, если $p-1 = \alpha^m$.

Обращаемся теперь къ тому случаю, когда $p-1 = \alpha^m \beta^n$, гдѣ α, β различныя простые числа. Въ этомъ случаѣ мы найдемъ все первообразные корни p между $1, 2, 3, \dots, p-1$, выкинувши отсюда числа, удовлетворяющія сравненіямъ

$$x^{\frac{p-1}{\alpha}} \equiv 1, \quad x^{\frac{p-1}{\beta}} \equiv 1 \pmod{p}.$$

Но по 35 теоремѣ первому сравненію удовлетворяетъ $\frac{p-1}{\alpha}$ чиселъ меньшихъ p ; второму же удовлетворяетъ $\frac{p-1}{\beta}$ такихъ чиселъ. Притомъ между этими числами, удовлетворяющими сравненіямъ

$$x^{\frac{p-1}{\alpha}} \equiv 1, \quad x^{\frac{p-1}{\beta}} \equiv 1 \pmod{p},$$

будетъ $\frac{p-1}{\alpha\beta}$ однихъ и тѣхъ же чиселъ, удовлетворяющихъ сравненію

$$x^{\frac{p-1}{\alpha\beta}} \equiv 1 \pmod{p}.$$

Слѣд. различныхъ чиселъ, удовлетворяющихъ сравненіямъ

$$x^{\frac{p-1}{\alpha}} \equiv 1, \quad x^{\frac{p-1}{\beta}} \equiv 1 \pmod{p},$$

будетъ $\frac{p-1}{\alpha} + \frac{p-1}{\beta} - \frac{p-1}{\alpha\beta}$. За исключеніемъ ихъ всѣ числа² въ рядѣ 1, 2, 3, . . . $p-1$ будутъ первообразные корни и число ихъ будетъ $p-1 - \frac{p-1}{\alpha} - \frac{p-1}{\beta} + \frac{p-1}{\alpha\beta}$, или $(p-1)(1 - \frac{1}{\alpha})(1 - \frac{1}{\beta})$.

Но по 12 теоремѣ извѣстно, что $(p-1)(1 - \frac{1}{\alpha})(1 - \frac{1}{\beta})$ означаетъ сколько простыхъ чиселъ съ $p-1$ и меньшихъ $p-1$, если $p-1 = \alpha^m \beta^n$.

Подобнымъ образомъ, полагая $p-1 = \alpha^m \beta^n \gamma^r$, $p-1 = \alpha^m \beta^n \gamma^r \delta^s$, $p-1 = \alpha^m \beta^n \gamma^r \delta^s \zeta^t$, и т. д., докажемъ, что между числами 1, 2, 3, . . . $p-1$ столько же первообразныхъ корней, сколько чиселъ простыхъ съ $p-1$ и меньшихъ $p-1$.

Каждый изъ первообразныхъ корней p можетъ быть принять за основаніе при опредѣленіи указателей по модулю p . Выгоднѣе другихъ принимать тѣ, которые легче возводить въ степени и слѣд. опредѣлять по нимъ указателей. Впрочемъ, зная указателей по одному основанію, не трудно найти ихъ по другому. Пусть будетъ a то основаніе, по которому составлена таблица,

а b основаніе, по которому хотимъ вычислить указателя какого нибудь числа A . Называя указателя A по основанію b черезъ x , для опредѣленія x будемъ имѣть

$$A \equiv b^x \pmod{p}.$$

Изъ этого сравненія мы заключаемъ о равенствѣ указателей A и b^x по какому нибудь основанію a . Изображая этихъ указателей по принятому нами знаковомуженію черезъ $Ind. x$ и $Ind. b^x$, мы имѣемъ

$$Ind. A \equiv Ind. b^x.$$

Но по свойству указателей $Ind. b^x \equiv x Ind. b \pmod{p-1}$. Слѣдовательно

$$x Ind. b \equiv Ind. A \pmod{p-1}.$$

Рѣшеніемъ этого сравненія мы найдемъ x .

Это сравненіе будетъ имѣть одно рѣшеніе; ибо, какъ видѣли, указатель первообразнаго корня будетъ всегда число простое съ $p - 1$. Рѣшивши это сравненіе, мы легко найдемъ положительное число меньшее $p - 1$ и ему удовлетворяющее; это и будетъ искомое число x , указатель числа A при основаніи b .

Для примѣра опредѣлимъ указателя числа 25 по основанію 2 и модулю 29, зная указателей при этомъ модулѣ по основанію 10, какъ находимъ въ нашихъ таблицахъ. Называя искомый указатель черезъ x , мы для опредѣленія его выводимъ

$$x Ind. 2 \equiv Ind. 25 \pmod{28}.$$

Но $Ind. 2 = 11$, $Ind. 25 = 8$. Слѣд. x опредѣлится сравненіемъ

$$11x \equiv 8 \pmod{28}.$$

Рѣшая это сравненіе, находимъ

$$x \equiv 16 \pmod{28};$$

откуда для величины указателя 25 по основанію 2 получаемъ 16.

ГЛАВА VII.

О СРАВНЕНИЯХЪ ВТОРОЙ СТЕПЕНИ СЪ ДВУМЯ НЕИЗВѢСТНЫМИ.

§ 42. До сихъ поръ мы занимались сравненіями, въ которыхъ одна неизвѣстная; теперь мы будемъ разсматривать сравненія съ двумя неизвѣстными. Замѣчательнѣйшія изъ нихъ и имѣющія наиболѣе приложения суть сравненія второй степени вида

$$x^2 + Ay^2 + B \equiv 0 \pmod{p};$$

ими то мы и займемся теперь.

Относительно сравненій этого вида докажемъ слѣдующую теорему:

49. ТЕОРЕМА.

Если p число простое и не дѣлитъ A ; то сравненію $x^2 + Ay^2 + B \equiv 0 \pmod{p}$ можно всегда удовлетворить.

Доказательство. Эта теорема очевидна для $p = 2$; ибо тогда сравненію $x^2 + Ay^2 + B \equiv 0 \pmod{p}$ удовлетворяетъ $y = 0, x = B$. Также очевидна она, если для какого нибудь значенія y сумма $Ay^2 + B$ обращается въ число кратное p ; ибо такая величина y вмѣстѣ съ $x = 0$ удовлетворяетъ сравненію $x^2 + Ay^2 + B \equiv 0 \pmod{p}$.

Докажемъ же теперь возможность удовлетворить этому сравненію при $p > 2$ и $Ay^2 + B$ неспособномъ сдѣлаться дѣлимъ на p .

Въ этомъ случаѣ между всѣми значеніями $-Ay^2 - B$ отъ $y = 0$ до $y = p - 1$ найдется число, которое будетъ сравнимо съ x^2 по модулю p ; ибо невозможность сравненія

$$x^2 \equiv -Ay^2 - B \pmod{p}$$

при p простомъ болѣе 2 и $-Ay^2 - B$ недѣлящемся на p , какъ видѣли въ IV главѣ, предполагаетъ сравненіе

$$(-Ay^2 - B)^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p},$$

что по раскрытіи скобокъ принимаетъ такой видъ

$$\pm A^2 y^{p-1} \pm A^2 p y^{p-3} + \dots \pm B^2 + 1 \equiv 0 \pmod{p}$$

Но этому сравненію не могутъ удовлетворять всѣ p чиселъ

$$0, 1, 2, \dots, p-1;$$

ибо оно степени $p-1$ и A^2 коэффициентъ y^{p-1} , состоя изъ произведенія чиселъ простыхъ съ p , не дѣлится на p .

И такъ по крайней мѣрѣ одно изъ чиселъ

$$0, 1, 2, \dots, p-1$$

не будетъ удовлетворять этому сравненію, и такое число обратитъ $-Ay^2 - B$ въ квадратичный вычетъ p . При такомъ же значеніи $Ay^2 - B$ найдется x , удовлетворяющій сравненію

$$x^2 \equiv -Ay^2 - B \pmod{p},$$

откуда и слѣдуетъ предложенная намъ теорема.

Изъ доказанной намъ теоремы, какъ частный случай, выходитъ, что сравненіе $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ имѣетъ рѣшеніе.

§ 43. Остановимся на изслѣдованіи сравненія

$$x^2 + Ay^2 + C \equiv 0 \pmod{p}$$

при $C = 0$. Предметомъ нашихъ изслѣдованій будетъ показать, какія свойства имѣетъ число p , для котораго сравненіе

$$x^2 + Ay^2 \equiv 0 \pmod{p}$$

удовлетворяется какими нибудь числами x , y , простыми между собою. Возможность этого сравненія намъ покажетъ, что число p можетъ быть дѣлителемъ числа, выражающагося формулою $x^2 + Ay^2$, гдѣ x , y простыя между собою. Въ противномъ случаѣ мы заключимъ, что числа, выражающіяся этою формулою, недѣлимы на p . Въ первомъ случаѣ мы будемъ называть p *дѣлителемъ квадратичной формы* $x^2 + Ay^2$; во второмъ *недѣлителемъ квадратичной формы*. Мы покажемъ средства по данной формѣ $x^2 + Ay^2$ находить всѣ дѣлители ея и недѣлители. Эти числа мы будемъ представлять или формулами вида $mz + \alpha$, гдѣ z произвольное цѣлое число или формулами вида

$au^2 + 2buv + cv^2$, гдѣ u, v произвольныя цѣлыя числа, простыя между собою. Первое составляетъ изслѣдованія, извѣстныя по имени теоріи линейныхъ дѣлителей квадратичныхъ формъ; второе составляетъ теорію квадратичныхъ дѣлителей квадратичныхъ формъ.

Мы начнемъ съ теоріи линейныхъ дѣлителей и докажемъ слѣдующую теорему, которая служитъ основаніемъ ея:

50. ТЕОРЕМА.

Если сравненію $x^2 + Ay^2 \equiv 0 \pmod{p}$ удовлетворяютъ какія нибудь числа x, y , простыя между собою; то сравненіе $u^2 + A \equiv 0 \pmod{p}$ имѣетъ рѣшеніе.

Доказательство. Въ самомъ дѣлѣ, если y и x , не имѣя общаго множителя, удовлетворяютъ сравненію

$$x^2 + Ay^2 \equiv 0 \pmod{p};$$

то y простое съ p ; ибо въ противномъ случаѣ простое число, дѣлящее y и p , дѣлило бы x и слѣд. x имѣло бы общаго дѣлителя съ y . Но если y простое съ p ; то можно найти такое число u , которое будетъ удовлетворять сравненію

$$yu \equiv x \pmod{p}.$$

Это же сравненіе по возведеніи въ квадратъ обѣихъ частей будетъ

$$y^2 u^2 \equiv x^2 \pmod{p},$$

что въ совокупности съ

$$x^2 + Ay^2 \equiv 0 \pmod{p}$$

дастъ

$$y^2 u^2 + Ay^2 \equiv 0 \pmod{p}.$$

Но это сравненіе можетъ быть сокращено на y^2 ; ибо, видѣли, число y простое съ p . Такимъ образомъ находимъ

$$u^2 + A \equiv 0 \pmod{p},$$

что и слѣдовало доказать.

Итакъ возможность удовлетворить сравненію

$$x^2 + Ay^2 \equiv 0 \pmod{p}$$

числами x и y простыми между собою предполагает возможность удовлетворить сравненію

$$u^2 + A \equiv 0 \pmod{p}.$$

Обратно, когда это сравненіе удовлетворяется; то мы всегда найдемъ рѣшеніе сравненія

$$x^2 + Ay^2 \equiv 0 \pmod{p},$$

дѣлая $y = 1$, $x = u$.

На основаніи доказанной нами теоремы не трудно узнать, будетъ-ли данное число дѣлителемъ данной формы или нѣтъ.

Такъ находя -1 для величины $\left(\frac{3}{5}\right)$ по приемамъ, изложеннымъ въ IV главѣ, мы заключаемъ, что сравненіе $u^2 - 3 \equiv 0 \pmod{5}$ не имѣетъ рѣшенія. Откуда по доказанному нами слѣдуетъ, что при x и y простыхъ между собою нельзя удовлетворить сравненію

$$x^2 - 3y^2 \equiv 0 \pmod{5},$$

или, что одно и тоже, обратить $x^2 - 3y^2$ въ число кратное 5.

Также замѣчая, что $\left(\frac{-1}{p}\right)$ при p простомъ вида $4n + 3$ равно -1 , мы заключаемъ, что въ этомъ случаѣ сравненіе $u^2 + 1 \equiv 0 \pmod{p}$ не имѣетъ рѣшенія; а потому нельзя удовлетворить сравненію

$$x^2 + y^2 \equiv 0 \pmod{p}$$

числами простыми между собою.

Откуда слѣдуетъ, что никакое простое число вида $4n + 3$ не будетъ дѣлителемъ чиселъ, разлагающихся на два квадрата простые между собою.

Такъ числа

$$5 = 2^2 + 1, 10 = 3^2 + 1, 13 = 3^2 + 2^2,$$

$$17 = 4^2 + 1, 25 = 4^2 + 3^2, 26 = 5^2 + 1, \dots$$

не дѣлятся на числа 7, 11, 19, 23 вида $4n + 3$.

Напротивъ замѣчая, что $\left(\frac{-1}{p}\right)$ есть $+1$, если p простое число вида $4n + 1$, мы заключаемъ о возможности сравненія

$$u^2 + 1 \equiv 0 \pmod{p}$$

для такихъ значений p . Откуда слѣдуетъ возможность сравненія

$$x^2 + y^2 \equiv 0 \pmod{p}$$

и слѣд. дѣлимость суммы двухъ квадратовъ на p .

На основаніи доказанной нами теоремы не трудно показать видъ простаго числа p , которое можетъ быть дѣлителемъ данной формы $x^2 + Ay^2$. Мы не будемъ останавливаться на случаѣ $p = 2$; ибо 2 всегда дѣлитъ $x^2 + Ay^2$ или при $x = 1, y = 1$ или $x = 0, y = 1$. По этому мы теперь будемъ предполагать p числомъ простымъ, отличнымъ отъ 2, и въ этомъ предположеніи докажемъ слѣдующія теоремы:

51. ТЕОРЕМА.

Если A простое число вида $4n + 3$ и p нечетный дѣлитель формы $x^2 + Ay^2$; то $\left(\frac{p}{A}\right) = +1$.

Доказательство. Если p есть дѣлитель формы $x^2 + Ay^2$; то сравненіе

$$x^2 + Ay^2 \equiv 0 \pmod{p}$$

имѣетъ рѣшеніе; а это по теоремѣ 50-й предполагаетъ возможность удовлетворить сравненію

$$u^2 + A \equiv 0 \pmod{p}.$$

Разлагая здѣсь p на произведеніе простыхъ чиселъ $\alpha, \beta, \gamma, \dots$, мы по § 30 возможность этого сравненія выразимъ такъ

$$\left(\frac{-A}{\alpha}\right) = 1, \left(\frac{-A}{\beta}\right) = 1, \left(\frac{-A}{\gamma}\right) = 1, \dots$$

Изъ этихъ уравненій не трудно вывести значенія символовъ

$$\left(\frac{\alpha}{A}\right) = 1, \left(\frac{\beta}{A}\right) = 1, \left(\frac{\gamma}{A}\right) = 1, \dots$$

Такъ для опредѣленія перваго, мы выводимъ по доказаннымъ свойствамъ символа $\left(\frac{p}{q}\right)$ въ IV главѣ, что

$$\begin{aligned} \left(\frac{\alpha}{A}\right) &= \left(\frac{A}{\alpha}\right) (-1)^{\frac{\alpha-1}{2} \frac{A-1}{2}} = \left(\frac{-A}{\alpha}\right) (-1)^{\frac{\alpha-1}{2} \frac{\alpha-1}{2} \frac{A-1}{2}} \\ &= \left(\frac{-A}{\alpha}\right) (-1)^{\frac{\alpha-1}{2} \frac{A+1}{2}} \end{aligned}$$

Но такъ какъ по предыдущимъ уравненіямъ $\left(\frac{-A}{\alpha}\right)$ равно 1, а число A по положенію вида $4n + 3$; то изъ этого уравненія получаемъ

$$\left(\frac{\alpha}{A}\right) = 1.$$

Подобнымъ образомъ выводимъ

$$\left(\frac{\beta}{A}\right) = 1, \left(\frac{\gamma}{A}\right) = 1, \dots\dots$$

Перемножая же эти уравненія между собою, находимъ

$$\left(\frac{\alpha}{A}\right) \left(\frac{\beta}{A}\right) \left(\frac{\gamma}{A}\right) \dots\dots\dots = \left(\frac{\alpha\beta\gamma\dots}{A}\right) = 1;$$

откуда замѣчая, что $\alpha\beta\gamma\dots = p$, выводимъ

$$\left(\frac{p}{A}\right) = 1,$$

что и слѣдовало доказать.

52. Т Е О Р Е М А.

Если A простое число вида $4n + 1$ и p дѣлитъ $x^2 + Ay^2$; то

$$\left(\frac{p}{A}\right) = (-1)^{\frac{p-1}{2}}; \text{ т. е. } \left(\frac{p}{A}\right) = 1, \text{ если } p = 4m + 1 \text{ и } \left(\frac{p}{A}\right) = -1, \text{ если } p = 4m + 3.$$

Доказательство. Если p есть дѣлитель $x^2 + Ay^2$; то

$$x^2 + Ay^2 \equiv 0 \pmod{p},$$

и слѣд. сравненіе

$$u^2 + A \equiv 0 \pmod{p}$$

имѣетъ рѣшеніе. А это, какъ видѣли, предполагаетъ

$$\left(\frac{-A}{\alpha}\right) = 1, \left(\frac{-A}{\beta}\right) = 1, \left(\frac{-A}{\gamma}\right) = 1, \dots\dots$$

гдѣ $\alpha, \beta, \gamma, \dots\dots$ суть простые числа, входящія въ составъ p .

На основаніи свойствъ символа $\left(\frac{q}{p}\right)$ мы отсюда выведемъ значенія $\left(\frac{\alpha}{A}\right), \left(\frac{\beta}{A}\right), \left(\frac{\gamma}{A}\right), \dots\dots\dots$

Такъ для опредѣленія перваго выводимъ

$$\begin{aligned} \left(\frac{\alpha}{A}\right) &= \left(\frac{A}{\alpha}\right) (-1)^{\frac{\alpha-1}{2} \cdot \frac{A-1}{2}} = \left(\frac{-A}{\alpha}\right) (-1)^{\frac{\alpha-1}{2} + \frac{\alpha-1}{2} \cdot \frac{A-1}{2}} \\ &= \left(\frac{-A}{\alpha}\right) (-1)^{\frac{\alpha-1}{2} \cdot \frac{A+1}{2}}. \end{aligned}$$

Внося сюда величину $\left(\frac{-A}{\alpha}\right)$, которая по предыдущему есть 1, находимъ

$$\left(\frac{\alpha}{A}\right) = (-1)^{\frac{\alpha-1}{2} \cdot \frac{A+1}{2}}.$$

Но A вида $4n+1$, вслѣдствіе чего $(-1)^{\frac{\alpha-1}{2} \cdot \frac{A+1}{2}}$ равно $(-1)^{\frac{\alpha-1}{2} \cdot \frac{4n+2}{2}}$, или $(-1)^{\frac{\alpha-1}{2} (2n+1)}$, а это равно $(-1)^{\frac{\alpha-1}{2}}$; ибо $(-1)^{\frac{\alpha-1}{2} \cdot 2n}$ есть 1. По этому величина $\left(\frac{\alpha}{A}\right)$ опредѣлится такимъ уравненіемъ

$$\left(\frac{\alpha}{A}\right) = (-1)^{\frac{\alpha-1}{2}}.$$

Подобнымъ образомъ выводимъ

$$\left(\frac{\beta}{A}\right) = (-1)^{\frac{\beta-1}{2}}, \quad \left(\frac{\gamma}{A}\right) = (-1)^{\frac{\gamma-1}{2}}, \dots$$

Перемножая же всѣ эти уравненія, имѣемъ

$$\left(\frac{\alpha}{A}\right) \left(\frac{\beta}{A}\right) \left(\frac{\gamma}{A}\right) \dots = (-1)^{\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \dots},$$

или

$$\left(\frac{\alpha\beta\gamma\dots}{A}\right) = (-1)^{\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \dots},$$

гдѣ замѣнивъ $\alpha\beta\gamma\dots$ черезъ p , находимъ

$$\left(\frac{p}{A}\right) = (-1)^{\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \dots}.$$

Но не трудно убѣдиться, что $\frac{p-1}{2}$ и

$$\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \dots$$

разнятся между собою числом четнымъ. Въ самомъ дѣлѣ, мы видѣли, что $p = \alpha \beta \gamma \dots$, а потому $\frac{p-1}{2}$ равно $\frac{\alpha\beta\gamma\dots-1}{2}$, что иначе представится такъ

$$\frac{-1 + \left(1 + 2\frac{\alpha-1}{2}\right) \left(1 + 2\frac{\beta-1}{2}\right) \left(1 + 2\frac{\gamma-1}{2}\right) \dots}{2}$$

Раскрывая же здѣсь скобки и откидывая члены, имѣющіе множителемъ 2, находимъ

$$\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \dots$$

Итакъ это число съ $\frac{p-1}{2}$ разнится только числомъ четнымъ; а поэтому

$$\left(-1\right)^{\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \dots} = \left(-1\right)^{\frac{p-1}{2}};$$

вслѣдствіе чего найденное нами выраженіе $\left(\frac{p}{A}\right)$ приводится къ такому

$$\left(\frac{p}{A}\right) = \left(-1\right)^{\frac{p-1}{2}},$$

что и слѣдовало доказать.

53. Т Е О Р Е М А.

Если A простое число вида $4n + 1$ и p нечетный дѣлитель формы $x^2 - Ay^2$; то $\left(\frac{p}{A}\right) = 1$.

Доказательство. Если p дѣлитъ $x^2 - Ay^2$; то

$$x^2 - Ay^2 \equiv 0 \pmod{p}.$$

Это сравненіе предполагаетъ такое

$$u^2 - A \equiv 0 \pmod{p},$$

а отсюда выходитъ

$$\left(\frac{A}{\alpha}\right) = 1, \left(\frac{A}{\beta}\right) = 1, \left(\frac{A}{\gamma}\right) = 1, \dots$$

гдѣ $\alpha, \beta, \gamma, \dots$ простые числа, входящія въ составъ p . Опредѣляя по первому изъ этихъ уравненій значеніе $\left(\frac{\alpha}{A}\right)$, находимъ

$$\left(\frac{\alpha}{A}\right) = \left(\frac{A}{\alpha}\right) (-1)^{\frac{\alpha-1}{2} \frac{A-1}{2}} = (-1)^{\frac{\alpha-1}{2} \frac{A-1}{2}},$$

что приводится къ равенству

$$\left(\frac{\alpha}{A}\right) = 1;$$

потому что $A = 4n + 1$, и слѣд. $\frac{A-1}{2}$ равно четному числу $2n$

Подобнымъ образомъ находимъ

$$\left(\frac{\beta}{A}\right) = 1, \left(\frac{\gamma}{A}\right) = 1, \dots\dots$$

Перемножая же всѣ эти уравненія между собою, найдемъ

$$\left(\frac{\alpha\beta\gamma\dots\dots}{A}\right) = 1.$$

Но здѣсь произведеніе $\alpha\beta\gamma\dots\dots$ равно p ; слѣд.

$$\left(\frac{p}{A}\right) = 1;$$

въ чемъ и заключается предложенная теорема.

54. Т Е О Р Е М А.

Если A простое число вида $4n + 3$ и p нечетный дѣлитель формы $x^2 - Ay^2$; то $\left(\frac{p}{A}\right) = (-1)^{\frac{p-1}{2}}$, т. е. $\left(\frac{p}{A}\right) = 1$, если p вида $4t + 1$, и $\left(\frac{p}{A}\right) = -1$, если p вида $4t + 3$.

Доказательство. Дѣлимость $x^2 - Ay^2$ на p предполагаетъ сравненіе

$$x^2 - Ay^2 \equiv 0 \pmod{p},$$

а это предполагаетъ сравненіе

$$u^2 - A \equiv 0 \pmod{p},$$

и слѣд. уравненія

$$\left(\frac{A}{\alpha}\right) = 1, \left(\frac{A}{\beta}\right) = 1, \left(\frac{A}{\gamma}\right) = 1, \dots\dots$$

гдѣ $\alpha, \beta, \gamma, \dots\dots$ простые числа, входяшія въ составъ p . Опредѣляя по этимъ уравненіямъ $\left(\frac{\alpha}{A}\right)$, находимъ

$$\left(\frac{\alpha}{A}\right) = \left(\frac{A}{\alpha}\right) (-1)^{\frac{\alpha-1}{2} \frac{A-1}{2}} = (-1)^{\frac{\alpha-1}{2} \frac{A-1}{2}},$$

и слѣд.

$$\left(\frac{\alpha}{A}\right) = (-1)^{\frac{\alpha-1}{2}};$$

потому что $(-1)^{\frac{\alpha-1}{2} \frac{A-1}{2}}$ для $A = 4n + 3$ приводится къ

$$(-1)^{\frac{\alpha-1}{2} \cdot 2n + \frac{\alpha-1}{2}}, \text{ гдѣ } (-1)^{\frac{\alpha-1}{2} \cdot 2n} \text{ равно } 1.$$

Подобнымъ образомъ находимъ

$$\left(\frac{\beta}{A}\right) = (-1)^{\frac{\beta-1}{2}}, \left(\frac{\gamma}{A}\right) = (-1)^{\frac{\gamma-1}{2}}, \dots\dots$$

Перемножая же эти уравненія между собою, имѣемъ

$$\left(\frac{\alpha}{A}\right) \left(\frac{\beta}{A}\right) \left(\frac{\gamma}{A}\right) \dots\dots = (-1)^{\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \dots\dots}$$

и слѣд.

$$\left(\frac{p}{A}\right) = \left(\frac{\alpha\beta\gamma\dots\dots}{A}\right) = (-1)^{\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \dots\dots}$$

Но доказывая 52-й теорему, нашли

$$(-1)^{\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \dots\dots} = (-1)^{\frac{p-1}{2}};$$

поэтому предыдущее уравненіе даетъ

$$\left(\frac{p}{A}\right) = (-1)^{\frac{p-1}{2}},$$

что и слѣдовало доказать.

§ 44. На основаніи доказанныхъ нами теоремъ не трудно опредѣлить всѣ линейные дѣлители формъ вида $x^2 \pm Ay^2$, при A простомъ нечетномъ. Мы видѣли, что нечетные дѣлители такихъ формъ опредѣляются или уравненіемъ

$$\left(\frac{p}{A}\right) = 1$$

или уравненіемъ

$$\left(\frac{p}{A}\right) = -1,$$

смотря по тому будетъ ли въ формѣ $x^2 \mp Ay^2$ знакъ $+$ или $-$, будетъ ли A вида $4n + 3$ или $4n + 1$ и въ нѣкоторыхъ слу-

GABINET MATEMATYCZNY
Towarzystwa Naukowego Warszawskiego

чаяхъ (см. 52 и 54 теоремы) будетъ ли искомое p вида $4m + 1$ или $4m + 3$.

Но по способу, показанному нами въ § 28-мъ, мы легко найдемъ всѣ числа, удовлетворяющія уравненію $\left(\frac{p}{A}\right) = 1$ и $\left(\frac{p}{A}\right) = -1$. Рѣшенія перваго, какъ видѣли тамъ, опредѣляются уравненіями

$$p = a_1 + nA, p = a_2 + nA, \dots p = a_{\frac{A-1}{2}} + nA,$$

гдѣ n произвольное число, $a_1, a_2, \dots, a_{\frac{A-1}{2}}$ остатки отъ дѣленія $1^2, 2^2, \dots, \left(\frac{A-1}{2}\right)^2$ на A . Рѣшенія же втораго $\left(\frac{p}{A}\right) = -1$ опредѣляются уравненіями

$$p = b_1 + nA, p = b_2 + nA, \dots p = b_{\frac{A-1}{2}} + nA,$$

гдѣ $b_1, b_2, \dots, b_{\frac{A-1}{2}}$ тѣ изъ чиселъ $1, 2, \dots, A-1$, которыя неравны $a_1, a_2, \dots, a_{\frac{A-1}{2}}$.

Теперь посмотримъ, какимъ образомъ каждая изъ этихъ формулъ можетъ служить для опредѣленія чиселъ вида $4m + 1$ или $4m + 3$.

Для того чтобы число p , опредѣляемое уравненіемъ

$$p = a + nA,$$

было вида $4m + 1$, число n должно быть такого вида, чтобы сумма $a + nA$ привелась бы къ $4m + 1$, другими словами, число n должно удовлетворять сравненію

$$a + nA \equiv 1 \pmod{4},$$

или

$$nA \equiv 1 - a \pmod{4}.$$

Это сравненіе всегда будетъ имѣть одно рѣшеніе, потому что A нечетное число; рѣшая его по способу, показанному въ § 15, находимъ

$$n \equiv A(1-a) \cdot 4 \cdot \frac{2-1}{2} - 1 \pmod{4},$$

или

$$n \equiv A(1-a) \pmod{4}.$$

Этому сравненію будетъ удовлетворять одно изъ чиселъ 0, 1, 2, 3. Называя r то число, которое ему удовлетворяетъ, найдемъ

$$r \equiv A(1-a) \pmod{4}.$$

Въ слѣдствіе чего предыдущее сравненіе приводится къ такому

$$n \equiv r \pmod{4},$$

откуда для выраженія n выходитъ

$$n = 4z + r.$$

Внося же эту величину n въ сравненіе

$$r = nA + a,$$

мы находимъ

$$r = 4Az + Ar + a$$

для выраженія чиселъ вида $4m + 1$, опредѣляемыхъ уравненіемъ

$$r = nA + a.$$

Подобнымъ образомъ для чиселъ вида $4m + 3$ мы найдемъ

$$r = 4Az + Ar' + a,$$

гдѣ r' наименьшее число, сравнимое съ $A(3-a)$ по модулю 4.

Такъ изъ уравненія

$$r = nA + a,$$

опредѣляющаго одно изъ рѣшеній уравненія

$$\left(\frac{p}{A}\right) = 1,$$

выводятся уравненія, которыя даютъ одни числа вида $4m + 1$ или $4m + 3$.

Не трудно также изъ уравненія

$$r = nA + a$$

вывести другое, которое будетъ давать вмѣстѣ и числа вида

$4m + 1$ и числа вида $4m + 3$, слѣд. всѣ нечетныя числа. Для этого мы должны будемъ найти видъ числа n , для котораго сумма $nA + a$ будетъ вида $2m + 1$; или, что одно и тоже, найти рѣшеніе сравненія

$$nA + a \equiv 1 \pmod{2}.$$

Но это сравненіе приводится къ такому

$$nA \equiv 1 - a \pmod{2}.$$

Если a число нечетное, ему удовлетворить $n = 0$, слѣд. въ этомъ случаѣ его рѣшеніе будетъ

$$n \equiv 0 \pmod{2};$$

откуда для опредѣленія n выходитъ такое уравненіе

$$n = 2z.$$

Если же n нечетное; то ему удовлетворить $n = 1$ (ибо A число нечетное), и слѣд. рѣшеніе его будетъ

$$n = 2z + 1.$$

Внося эти значенія n въ уравненіе

$$p = nA + a,$$

мы находимъ для опредѣленія нечетныхъ чиселъ

$$p = 2Az + a \text{ или } p = 2Az + A + a,$$

смотря потому будетъ ли a число четное или нечетное.

Поступая такимъ образомъ съ каждымъ изъ уравненій, опредѣляющихъ рѣшенія уравненій

$$\left(\frac{p}{A}\right) = 1, \left(\frac{p}{A}\right) = -1,$$

мы найдемъ для выраженія нечетныхъ чиселъ, удовлетворяющихъ условію $\left(\frac{p}{A}\right) = 1$ или $\left(\frac{p}{A}\right) = -1$, формулы вида $2Az + a$; для выраженія же однихъ чиселъ вида $4m + 1$ или $4m + 3$, мы будемъ имѣть формулы вида $4Az + a$. Этими-то формулами на основаніи доказанныхъ нами теоремъ и опредѣляются нечетные дѣлители квадратичной формы $x^2 + Ay^2$.

Покажемъ это на примѣрахъ. Положимъ, что требуется найти видъ всѣхъ нечетныхъ дѣлителей квадратичной формы $x^2 + 19y^2$. Замѣчая, что 19 есть число простое и вида $4n + 3$, мы по

теоремъ 51 заключаемъ, что для нечетныхъ дѣлителей этой формы должно быть

$$\left(\frac{p}{19}\right) = 1.$$

Для опредѣленія чиселъ, удовлетворяющихъ этому уравненію, мы дѣлимъ

$$1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2$$

на 19; находя въ остаткѣ

$$1, 4, 9, 16, 6, 17, 11, 7, 5,$$

мы заключаемъ, что p , удовлетворяющее уравненію $\left(\frac{p}{19}\right) = 1$, должно представиться какою либо изъ формулъ

$$19n + 1, 19n + 4, 19n + 9, 19n + 16, 19n + 6, 19n + 17, \\ 19n + 11, 19n + 7, 19n + 5.$$

Но чтобы эти формулы давали одни нечетныя числа, мы по сказанному нами формулу $19n + 1$, въ которой первый членъ нечетный, замѣняемъ формулою $2 \cdot 19z + 1$, формулу $19n + 4$, которой первый членъ четный, замѣняемъ формулою

$$2 \cdot 19z + 19 + 4, \text{ и т. д.}$$

Такимъ образомъ находимъ для нечетныхъ дѣлителей $x^2 + 19y^2$ слѣдующія формулы

$$2 \cdot 19z + 1, 2 \cdot 19z + 19 + 4, 2 \cdot 19z + 9, 2 \cdot 19z + 19 + 16, \\ 2 \cdot 19z + 19 + 6, 2 \cdot 19z + 17, 2 \cdot 19z + 11, 2 \cdot 19z + 7, \\ 2 \cdot 19z + 5,$$

которыя приводятся къ такому виду

$$38z + 1, 38z + 5, 38z + 7, 38z + 9, 38z + 11, 38z + 17, \\ 38z + 23, 38z + 25, 38z + 35.$$

Такъ опредѣляются все числа, которыя могутъ дѣлится сумму $x^2 + 19y^2$ при x и y простыхъ между собою. Этимъ можно пользоваться при опредѣленіи дѣлителей данныхъ чиселъ, когда эти числа выражены формулою вида $x^2 + 19y^2$. Напр. пусть будетъ дано число 2021; такъ какъ оно равно $11^2 + 19 \cdot 10^2$; то дѣлители его, если они есть, должны представиться какими либо изъ формулъ

$38z + 1$, $38z + 5$, $38z + 7$, $38z + 9$, $38z + 11$, $38z + 17$,
 $38z + 23$, $38z + 25$, $38z + 35$.

Но если 2021 имѣть дѣлителей, то покрайней мѣрѣ одинъ изъ этихъ дѣлителей меньше $\sqrt{2021}$, и слѣд. меньше 45. Этого то дѣлителя мы и будемъ отыскивать.

Первая формула $38z + 1$ не даетъ его. Она при $z = 0$ даетъ 1, при $z = 1$ даетъ 39, что не можетъ дѣлится 2021, ибо это число не дѣлится на 3, а 39 въ составѣ своемъ содержитъ 3; при $z = 2$ и болѣе 2 формула $38z + 1$ даетъ числа превосходящія 45.

Обращаемся ко второй формулѣ $38z + 5$. При $z = 0$ она даетъ 5, число, очевидно, не дѣлящее 2021; при $z = 1$ она даетъ 43 и пробуя дѣлить этимъ числомъ 2021, находимъ, что 43 есть дѣлитель 2021.

Для другаго примѣра опредѣленія дѣлителей формъ вида $x^2 - Ay^2$ возьмемъ форму $x^2 - 7y^2$ и отыщемъ ея дѣлителей.

Такъ какъ число 7 вида $4n + 3$, то по теоремѣ 54-й дѣлители формы $x^2 - 7y^2$ вида $4m + 1$ должны удовлетворять уравненію

$$\left(\frac{p}{7}\right) = 1;$$

дѣлители же вида $4m + 3$ должны удовлетворять уравненію

$$\left(\frac{p}{7}\right) = -1.$$

Опредѣлимъ же теперь числа вида $4m + 1$, удовлетворяющія уравненію

$$\left(\frac{p}{7}\right) = 1,$$

и числа вида $4m + 3$, удовлетворяющія уравненію

$$\left(\frac{p}{7}\right) = -1.$$

Чтобы найти числа, удовлетворяющія уравненію

$$\left(\frac{p}{7}\right) = 1,$$

мы дѣлимъ $1^2, 2^2, 3^2$ на 7; находя въ остаткѣ 1, 4, 2, мы заключаемъ, что эти числа выражаются формулами

$$7n + 1, 7n + 4, 7n + 2.$$

Посмотримъ же теперь, какъ выведутся изъ нихъ формулы, опредѣляющія однѣ числа вида $4m + 1$.

По сказанному нами изъ формулы $7n + 1$ выводимъ

$$4.7z + 7r + 1,$$

гдѣ r то изъ чиселъ 0, 1, 2, 3, которое съ $7(1 - 1)$, или 0 сравнимо по модулю 4. Это число есть 0. Слѣд. формула $7n + 1$ для опредѣленія однихъ чиселъ вида $4m + 1$ даетъ $4.7z + 1$, или $28z + 1$.

Поступая также съ формулами

$$7n + 4, 7n + 2,$$

мы изъ нихъ выводимъ $4.7z + 7r + 4$, $4.7z + 7r' + 2$, гдѣ r, r' суть тѣ изъ чиселъ 0, 1, 2, 3, которыя съ $7(1 - 4)$, $7(1 - 2)$ сравнимы по модулю 4. Но такія числа суть 3, 1. Слѣд. для опредѣленія однихъ чиселъ вида $4m + 1$ формулы $7n + 4, 7n + 2$ даютъ

$$4.7z + 3.7 + 4, 4.7z + 7 + 2,$$

или

$$28z + 25, 28z + 9.$$

И такъ всѣ числа вида $4m + 1$, удовлетворяющія уравненію

$$\left(\frac{p}{7}\right) = 1,$$

и слѣд. способныя быть дѣлителями формы $x^2 - 7y^2$ опредѣляются формулами

$$28z + 1, 28z + 9, 28z + 25.$$

Переходимъ теперь къ дѣлителямъ вида $4m + 3$. Они опредѣляются уравненіемъ

$$\left(\frac{p}{7}\right) = -1.$$

Чтобы найти рѣшенія этого уравненія мы въ рядѣ 1, 2, 3, 4, 5, 6 выкидываемъ тѣ, которыя равны остаткамъ отъ дѣленія $1^2, 2^2, 3^2$ на 7. Такимъ образомъ находимъ числа 3, 5, 6, и заключаемъ, что числа, удовлетворяющія уравненію $\left(\frac{p}{7}\right) = -1$,

опредѣляются формулами $7n + 3$, $7n + 5$, $7n + 6$. Преобразовывая эти формулы въ такія, которыя даютъ одни числа вида $4m + 3$, найдемъ

$4. 7z + 7r + 3$, $4. 7z + 7r_1 + 5$, $4. 7z + 7r_2 + 6$,
гдѣ r , r_1 , r_2 тѣ изъ чиселъ 0, 1, 2, 3, которыя сравнимы съ $7(3 - 3)$, $7(3 - 5)$, $7(3 - 6)$ по модулю 4. Замѣчая, что $r = 0$, $r_1 = 2$, $r_2 = 3$, мы заключаемъ, что эти формулы суть

$4. 7z + 7. 0 + 3$, $4. 7z + 7. 2 + 5$, $4. 7z + 7. 3 + 6$,
или $28z + 3$, $28z + 19$, $28z + 27$.

Итакъ всѣ дѣлители формы $x^2 - 7y^2$ вида $4m + 1$ опредѣляются формулами

$$28z + 1, 28z + 9, 28z + 25,$$

дѣлители же вида $4m + 3$ суть

$$28z + 3, 28z + 19, 28z + 27.$$

Мы показали какъ опредѣляются дѣлители формы $x^2 \pm Ay^2$ при A простомъ, отличномъ отъ 2; покажемъ теперь такъ найдутся дѣлители этой формы, если A равно 2. Для этого мы докажемъ слѣдующую теорему:

55. ТЕОРЕМА.

Всѣ нечетные дѣлители $x^2 + 2y^2$ суть вида $8m + 1$ или $8m + 3$; всѣ нечетные дѣлители $x^2 - 2y^2$ суть вида $8m + 1$ или $8m - 1$.

Доказательство. Если p дѣлитъ $x^2 + 2y^2$; то

$$x^2 + 2y^2 \equiv 0 \pmod{p}.$$

По это сравненіе предполагаетъ возможность такого

$$u^2 + 2 \equiv 0 \pmod{p},$$

и слѣд. предполагаетъ уравненія

$$\left(\frac{-2}{\alpha}\right) = 1, \left(\frac{-2}{\beta}\right) = 1, \left(\frac{-2}{\gamma}\right) = 1, \dots$$

гдѣ α , β , γ , простыя числа, входящія въ составъ p . Посмотримъ же какого вида должны быть числа α , β , γ, \dots , чтобы удовлетворялись эти уравненія.

По свойству символовъ $\left(\frac{q}{p}\right)$ мы находимъ

$$\left(\frac{-2}{\alpha}\right) = \left(\frac{2}{\alpha}\right) (-1)^{\frac{\alpha-1}{2}}.$$

Но $\left(\frac{2}{\alpha}\right)$, какъ видѣли, опредѣляется такъ

$$\left(\frac{2}{\alpha}\right) = (-1)^{-\frac{\alpha^2-1}{8}};$$

слѣдовательно

$$\left(\frac{-2}{\alpha}\right) = (-1)^{-\frac{\alpha^2-1}{8} + \frac{\alpha-1}{2}} = (-1)^{\frac{-\alpha^2+4\alpha-3}{8}}.$$

Дѣлая въ этомъ уравненіи послѣдовательно $\alpha = 8m + 1$, $\alpha = 8m + 3$, $\alpha = 8m + 5$, $\alpha = 8m + 7$, находимъ

$$\left(\frac{-2}{8m+1}\right) = 1, \left(\frac{-2}{8m+3}\right) = 1, \left(\frac{-2}{8m+5}\right) = -1, \left(\frac{-2}{8m+7}\right) = -1.$$

Слѣд. для возможности уравненій

$$\left(\frac{-2}{\alpha}\right) = 1, \left(\frac{-2}{\beta}\right) = 1, \left(\frac{-2}{\gamma}\right) = 1, \dots\dots$$

необходимо, чтобы числа $\alpha, \beta, \gamma, \dots\dots$ были вида $8m + 1$ или $8m + 3$. А потому p , равное $\alpha\beta\gamma\dots$, должно быть произведеніемъ такого вида

$$(8m+1)(8m'+1)(8m''+1)\dots(8m_1+3)(8m_2+3)\dots(8m_\sigma+3).$$

Разлагая же здѣсь скобки и собирая въ одинъ всѣ члены, имѣющіе множителемъ 8, находимъ, что

$$p = 8P + 3^\sigma.$$

Если σ число четное; то $3^\sigma \equiv 1 \pmod{8}$; ибо $3^2 \equiv 1 \pmod{8}$.

Если же σ число нечетное; то сравненіе $3^2 \equiv 1 \pmod{8}$, по возведеніи обѣихъ частей въ степень $\frac{\sigma-1}{2}$ и умноженіи на 3 дасть $3^\sigma \equiv 3 \pmod{8}$. Итакъ 3^σ по модулю 8 сравнимо или съ 1 или съ 3. Откуда слѣдуетъ, что 3^σ или вида $8N + 1$ или $8N + 3$, а потому число p , опредѣляемое уравненіемъ

$$p = 8P + 3^\sigma,$$

будетъ или равно $8(P + N) + 1$ или $8(P + N) + 3$, въ чемъ и заключается первая часть предложенной нами теоремы. Переходимъ теперь къ доказательству второй части ея.

Если p дѣлитель формы $x^2 - 2y^2$; то

$$x^2 - 2y^2 \equiv 0 \pmod{p}.$$

Это же сравненіе предполагаетъ возможность сравненія

$$u^2 - 2 \equiv 0 \pmod{p},$$

и слѣд. уравненія

$$\left(\frac{2}{\alpha}\right) = 1, \left(\frac{2}{\beta}\right) = 1, \left(\frac{2}{\gamma}\right) = 1, \dots\dots$$

гдѣ $\alpha, \beta, \gamma, \dots$ простые числа, входящія въ составъ p . Но по теоремѣ 32 изъ этихъ уравненій слѣдуетъ, что $\alpha, \beta, \gamma, \dots$ суть числа вида $8m + 1$ или $8m - 1$, а потому произведеніе ихъ $\alpha\beta\gamma\dots$, равное p , представится такъ

$$(8m' + 1)(8m'' + 1)\dots(8m_1 - 1)(8m_2 - 1)\dots$$

Но въ разложеніи этого произведенія, кромѣ членовъ кратныхъ 8, будетъ или $+1$ или -1 . Слѣд. p должно быть вида $8m + 1$ или $8m - 1$, что и слѣдовало доказать.

Показавши, какъ опредѣляются линейные дѣлители формы $x^2 \pm Ay^2$ при A простомъ нечетномъ и $A \equiv 2$, намъ остается тоже сдѣлать для этихъ формъ при A составномъ. Но въ этомъ случаѣ линейные дѣлители $x^2 \pm Ay^2$ удобнѣе всего выводятся изъ квадратичныхъ дѣлителей, къ нимъ мы теперь и обращаемся.

§ 45. Выраженіе вида $au^2 + 2buv + cv^2$, гдѣ a, b, c опредѣленные числа, u, v неопредѣленные, мы называемъ квадратичною формою. Двѣ квадратичныя формы $au^2 + 2buv + cv^2$, $a'u^2 + 2b'uv + c'v^2$, которыя способны выражать однѣ и тѣже числа, мы будемъ называть тождественными и будемъ замѣнять одну другою. Такъ формы $au^2 + 2buv + cv^2$, $au^2 - 2buv + cv^2$, различающіяся только знакомъ коэффициента uv суть тождественныя; ибо значенія первой при $u = \alpha, v = \beta$ равны значеніямъ второй при $u = -\alpha, v = \beta$.

Изъ этого видно, что знакъ коэффициента b въ формѣ $au^2 + 2buv + cv^2$ можетъ быть всегда перемененъ и слѣд. этотъ коэффициентъ можетъ быть обращенъ въ количество положительное: такимъ мы его и будемъ всегда предполагать.

Число равное $b^2 - ac$ мы будемъ называть *опредѣлителемъ* формы $au^2 + 2buv + cv^2$. Такъ опредѣлитель формы $3u^2 + 10uv$

+ $7v^2$ будетъ $5^2 - 3.7$, или 4; опредѣлитель формы $3u^2 + 10uv - 7v^2$ будетъ $5^2 + 3.7$, или 46.

Двѣ формы, имѣющія равныхъ опредѣлителей, мы будемъ называть *подобными*. Такъ формы $3u^2 + 10uv + 7v^2$, $3u^2 + 2uv - v^2$ подобны; ибо какъ опредѣлитель первой $5^2 - 3.7$, такъ и опредѣлитель второй $1^2 + 1.3$ равны 4.

Согласившись въ этихъ названіяхъ, мы докажемъ слѣдующую теорему, весьма важную по своимъ приложеніямъ.

56. Т Е О Р Е М А.

Если въ формѣ $au^2 + 2buv + cv^2$ коэффициентъ $2b$ превосходитъ a или c ; то эта форма можетъ быть преобразована въ другую $a'u^2 + 2b'uv + c'v^2$, подобную $au^2 + 2buv + cv^2$, гдѣ $2b'$ не будетъ превосходить ни a' , ни c' . ()*

Доказательство. Для доказательства этой теоремы мы покажемъ, какимъ образомъ при $2b > a$ или $2b > c$ форма $au^2 + 2buv + cv^2$ можетъ быть преобразована въ другую $a_0u^2 + 2b_0uv + c_0v^2$, подобную первой, гдѣ численная величина b_0 меньше b . Но такъ какъ уменьшеніе численной величины коэффициента b не можетъ идти далѣе нуля; то мы необходимо дойдемъ до такой формы $a'u^2 + 2b'uv + c'v^2$, гдѣ дальнѣйшее уменьшеніе коэффициента b' не можетъ имѣть мѣста и слѣд. $2b'$ не $> a'$ и не $> c'$.

Чтобы преобразовать форму $au^2 + 2buv + cv^2$ въ другую $a_0u^2 + 2b_0uv + c_0v^2$, гдѣ бы b_0 было меньше b , пусть будетъ a наименьшее изъ двухъ чиселъ a и c (въ случаѣ равенства ихъ мы можемъ взять то или другое безъ различія) и цѣлое число, которое разнится съ $\frac{b}{a}$ не болѣе какъ $\frac{1}{2}$, пусть будетъ m : очевидно, m будетъ цѣлое число, получаемое при дѣленіи b на a , если остатокъ не превосходитъ $\frac{1}{2}a$;

(*) Здѣсь мы разумѣемъ численную величину a, b, c, a', b', c' , не обращая вниманія на знаки этихъ количествъ.

въ противномъ случаѣ m будетъ цѣлое число, получаемое при дѣленіи b на a и сложенное съ 1. Полагаемъ $u + mv = U$, и на основаніи этого уравненія исключаемъ u изъ формы $au^2 + 2buv + cv^2$. Такимъ образомъ находимъ

$$a(U - mv)^2 + 2b(U - mv)v + cv^2,$$

или

$$aU^2 + 2(b - am)Uv + (c - 2bm + am^2)v^2.$$

Не трудно убѣдиться, что эта форма подобна $au^2 + 2buv + cv^2$, и что въ ней коэффициентомъ Uv меньше $2b$. Въ самомъ дѣлѣ, опредѣлитель этой формы есть

$$(b - am)^2 - a(c - 2bm + am^2),$$

что приводится по раскрытіи скобокъ къ $b^2 - ac$, а это есть опредѣлитель формы $au^2 + 2buv + cv^2$.

Съ другой стороны, такъ какъ m выбрано нами подъ условіемъ, чтобы разность $\frac{b}{a} - m$ была числомъ не превосходящимъ $\frac{1}{2}$; то $2(b - am) = 2a\left(\frac{b}{a} - m\right)$ будетъ число, непревосходящее a и потому мѣньшее $2b$; ибо мы разсматриваемъ форму $au^2 + 2buv + cv^2$, гдѣ $2b$ превосходитъ одно изъ чиселъ a и c , притомъ a или равно c или меньше c .

Слѣд. въ полученной нами формѣ

$$aU^2 + 2(b - am)Uv + (a - 2bm + cm^2)v^2$$

коэффициентъ среднего члена меньше соответствующаго ему въ формѣ $au^2 + 2buv + cv^2$.

Если въ полученной нами формѣ этотъ коэффициентъ превосходитъ одинъ изъ коэффициентовъ крайнихъ членовъ; мы ее снова будемъ также преобразовать, какъ преобразовывали $au^2 + 2buv + cv^2$ и будемъ повторять это преобразование до тѣхъ поръ, пока получимъ форму, гдѣ такое преобразование невозможно и слѣд. средний коэффициентъ не превосходитъ ни одного изъ крайнихъ. Напр. пусть будетъ дава форма $3u^2 + 10uv + 6v^2$. Для преобразованія ея ищемъ цѣлое число, которое бы съ $\frac{5}{3}$ разнилось не болѣе какъ на $\frac{1}{2}$; и такъ какъ это число есть

2, то дѣлаемъ $u + 2v = U$. Внося отсюда величину u въ данную форму, находимъ

$$3(U - 2v)^2 + 10(U - 2v)v + 6v^2,$$

что по раскрытіи скобокъ приводится къ такой формѣ

$$3U^2 - 2Uv - 2v^2.$$

Въ этой формѣ средній коэффициентъ не превосходитъ ни одного изъ крайнихъ; въ противномъ случаѣ мы бы стали ее снова преобразовывать.

Изъ доказанной нами теоремы мы выводимъ слѣдующія:

57. ТЕОРЕМА.

Если определитель формы $au^2 + 2buv + cv^2$ есть положительное число D ; то она можетъ быть приведена къ виду $a_1u^2 + 2b_1uv - c_1v^2$, гдѣ $a_1c_1 + b_1^2 = D$, числа a_1, c_1 положительныя, которыя не меньше $2b$, и b не превосходитъ $\sqrt{\frac{D}{5}}$.

Доказательство. Въ самомъ дѣлѣ по предыдущей теоремѣ форма $au^2 + 2buv + cv^2$ преобразовывается въ форму

$$a_1u^2 + 2b_1uv + c_0v^2,$$

гдѣ $2b_1$ не превосходитъ численной величины ни a_1 , ни c_0 ; притомъ въ этой формѣ, какъ подобной $au^2 + 2buv + cv^2$, определитель будетъ имѣть ту же величину D , и слѣд. будетъ $b_1^2 - a_1c_0 = D$. Но при $D > 0$ это уравненіе предполагаетъ разность $b_1^2 - a_1c_0$ количествомъ положительнымъ, что не можетъ быть, если a_1 и c_0 имѣютъ одинакіе знаки; ибо тогда произведеніе a_1c_0 будетъ количествомъ положительнымъ, превосходящимъ b_1^2 , потому что численныя величины a_1 и c_0 не меньше $2b$. Итакъ въ формѣ $a_1u^2 + 2b_1uv + c_0v^2$ крайніе члены съ противными знаками. Положимъ же, что членъ a_1u^2 есть тотъ изъ крайнихъ, который имѣетъ знакъ $+$, а членъ c_0v^2 есть тотъ, который съ $-$. Называя черезъ c_1 численную величину c_0 , мы будемъ имѣть $c_0 = -c_1$; вслѣдствіе чего форма

$$a_1u^2 + 2b_1uv - c_0v^2$$

и уравненіе $b_1^2 - a_1c_0 = D$ измѣнятся въ такія

$$a_1u^2 + 2b_1uv - c_1v^2, \quad b_1^2 + a_1c_1 = D.$$

Но по свойству коэффициентовъ этой формы будетъ

$$a_1 \text{ не } < 2b_1, \quad c_1 \text{ не } < 2b_1;$$

вслѣдствіе чего изъ уравненія

$$b_1^2 + a_1 c_1 = D$$

выходитъ

$$D \text{ не } < b_1^2 + 2b_1 \cdot 2b_1, \quad \text{не } < 5b_1^2,$$

а потому

$$b_1 \text{ не } > \sqrt{\frac{D}{5}}.$$

Вотъ условіе, которому вмѣстѣ съ условіями

$$b_1^2 + a_1 c_1 = D, \quad a_1 \text{ не } < 2b_1, \quad c_1 \text{ не } < 2b_1$$

будутъ удовлетворять коэффициенты формы

$$a_1 u^2 + 2b_1 uv - c_1 v^2,$$

выведенной нами изъ данной

$$au^2 + 2buv + cv^2.$$

Такъ убѣждаемся въ справедливости предложенной нами теоремы.

58. ТЕОРЕМА.

Если опредѣлитель формы $au^2 + 2buv + cv^2$ есть число отрицательное — D ; то она можетъ быть приведена къ виду $a_1 u^2 + 2b_1 uv + c_1 v^2$, гдѣ $a_1 c_1 - b_1^2 = D$, количества a_1 и c_1 съ одинаковыми знаками и не меньше $2b_1$; притомъ b_1 не превосходитъ $\sqrt{\frac{D}{3}}$.

Доказательство. Мы видѣли, что форма $au^2 + 2buv + cv^2$ можетъ быть приведена къ виду $a_1 u^2 + 2b_1 uv + c_1 v^2$, гдѣ $2b_1$ не превосходитъ ни a_1 , ни c_1 ; притомъ въ этой формѣ, какъ подобной $au^2 + 2buv + cv^2$, опредѣлитель будетъ имѣть ту-же величину — D , и слѣд. $b_1^2 - a_1 c_1 = -D$.

Но это уравненіе, гдѣ D число положительное, предполагаетъ одинакіе знаки въ количествахъ a_1, c_1 . Притомъ замѣчая, что a_1 и c_1 не меньше $2b_1$, мы изъ этого уравненія выводимъ

$$2b_1 \cdot 2b_1 - b_1^2 \text{ не } > D,$$

или

$$3b_1^2 \text{ не } > D,$$

и слѣд. $b_1 \text{ не } > \sqrt{\frac{D}{3}}$.

Доказавши эту теорему, замѣтимъ, что въ разсматриваемомъ намъ случаѣ форма $a_1 u^2 + 2b_1 uv + c_1 v^2$ можетъ представлять положительныя числа только въ случаѣ a_1 положительнаго. Въ самомъ дѣлѣ, выраженіе $a_1 u^2 + 2b_1 uv + c_1 v^2$ можетъ быть такъ представлено

$$a_1 \left(u^2 + 2 \frac{b_1}{a_1} uv + \frac{c_1}{a_1} v^2 \right),$$

а это равняется

$$a_1 \left[\left(u + \frac{b_1}{a_1} v \right)^2 + \frac{a_1 c_1 - b_1^2}{a_1^2} v^2 \right],$$

и въ слѣдствіе уравненія $b_1^2 - a_1 c_1 = -D$ приводится къ

$$a_1 \left[\left(u + \frac{b_1}{a_1} v \right)^2 + \frac{D}{a_1^2} v^2 \right]$$

что въ случаѣ a_1 отрицательнаго не можетъ имѣть значенія положительнаго; ибо $D > 0$, и квадраты $\left(u + \frac{b_1}{a_1} v \right)^2, \left(\frac{v}{a_1} \right)^2$ не могутъ имѣть значенія отрицательнаго.

§ 46. Показавши свойства квадратичныхъ формъ, необходимыя намъ въ послѣдствіи, обращаемся опять къ дѣлителямъ формъ вида $x^2 \pm Ay^2$, и докажемъ слѣдующую теорему:

59. ТЕОРЕМА.

Всякій дѣлитель формы $x^2 - dy^2$ можетъ быть представленъ квадратичною формою, имѣющею опредѣлителемъ d .

Доказательство. Пусть будетъ p дѣлитель формы $x^2 - dy^2$ и P частное отъ дѣленія $x^2 - dy^2$ на P ; приравнивая дѣлимое произведенію дѣлителя на частное, имѣемъ

$$x^2 - dy^2 = pP.$$

Здѣсь y и P должны быть числа относительно другъ друга простыя; ибо по этому уравненію простое число, дѣлящее y и P , дѣлитъ x^2 и слѣд. x , что невозможно; ибо въ формѣ $x^2 - dy^2$ мы

всегда предполагаемъ x и y неимѣющими общаго дѣлителя. Но при y простомъ съ P сравненіе

$$yt \equiv x \pmod{P}$$

имѣетъ рѣшеніе, и слѣд. найдется число t , для котораго разность $yt - x$ раздѣлится на P . Полагая же частное отъ дѣленія $yt - x$ на P равнымъ u , имѣемъ

$$\frac{yt - x}{P} = u;$$

откуда выходитъ

$$x = yt - uP.$$

Внося это выраженіе x въ уравненіе

$$x^2 - dy^2 = pP,$$

найдемъ

$$(yt - uP)^2 - dy^2 = pP,$$

или

$$P^2 u^2 - 2Pytu + (t^2 - d)y^2 = pP.$$

Это уравненіе по сокращеніи на P даетъ

$$p = Pu^2 - 2ytu + \frac{t^2 - d}{P} y^2,$$

гдѣ $t^2 - d$ раздѣлится на P ; ибо это уравненіе предполагаетъ дѣлимость $(t^2 - d)y^2$ на P , а y число простое съ P . Изъ этого уравненія мы видимъ, что p выражается квадратичною формою

$$p = Pu^2 - 2ytu + \frac{t^2 - d}{P} y^2,$$

которой коэффициенты суть P , $-2t$, $\frac{t^2 - d}{P}$ и слѣд. определитель ея равенъ $t^2 - P \cdot \frac{t^2 - d}{P}$, или d , что и слѣдовало доказать.

Изъ этой теоремы въ совокупности съ показанными нами свойствами квадратичныхъ формъ легко вывести слѣдующія теоремы:

60. ТЕОРЕМА.

Дѣлитель $x^2 - Dy^2$ при $D > 0$ можетъ быть представленъ формою $au^2 + 2buv - cv^2$, гдѣ $ac + b^2 = D$, числа a и c положительныя, не меньше $2b$, и b не превосходитъ $\sqrt{\frac{D}{3}}$.

Доказательство. По предыдущей теоремѣ всякій дѣлитель формы $x^2 - Dy^2$ можетъ быть представленъ формою

$$au^2 + 2bu + cv^2,$$

въ которой опредѣлитель $b^2 - ac$ будетъ равенъ D . Но такая форма по теоремѣ 57-й можетъ быть приведена къ виду

$$au^2 + 2buv - cv^2,$$

гдѣ a, b, c удовлетворяютъ уравненію $ac + b^2 = D$, числа a, c положительныя, которыя не меньше $2b$; число b не превосходить $\sqrt{\frac{D}{3}}$; откуда и слѣдуетъ предложенная нами теорема.

61. ТЕОРЕМА.

Дѣлитель $x^2 + Dy^2$ при $D > 0$ можетъ быть представленъ формою $au^2 + 2buv + cv^2$, гдѣ $ac - b^2 = D$, числа a, c положительныя, не меньше $2b$, и b не превосходитъ $\sqrt{\frac{D}{3}}$.

Доказательство. По теоремѣ 59-й дѣлитель $x^2 + Dy^2$ представится формою

$$au^2 + 2buv + cv^2,$$

которой опредѣлитель будетъ $-D$. Но такая форма по теоремѣ 58-й приводится къ виду

$$au^2 + 2buv + cv^2,$$

гдѣ $ac - b^2 = D$, численная величина a, c не меньше $2b$, и b не превосходить $\sqrt{\frac{D}{3}}$. Притомъ a и c будутъ имѣть одинъ знакъ, который здѣсь не можетъ быть $-$; ибо видѣли въ концѣ предыдущаго параграфа, что въ этомъ случаѣ формула $au^2 + 2buv + cv^2$ не можетъ имѣть значеній положительныхъ.

Такъ убѣждаемся въ справедливости предложенной нами теоремы.

На основаніи доказанныхъ нами теоремъ можно показать какими квадратичными формами выражаются всѣ дѣлители данной формы вида $x^2 \pm Dy^2$.

Покажемъ это на примѣрахъ.

Пусть будетъ дана форма $x^2 + y^2$. По теоремѣ 61-й дѣлители ея будутъ представляться формами

$$au^2 + 2buv + cv^2,$$

гдѣ $ac - b^2 = 1$, a и c положительныя числа, не меньше $2b$, и b не превосходитъ $\sqrt{\frac{1}{3}}$. Но изъ послѣдняго слѣдуетъ, что $b = 0$; уравненіе же $ac - b^2 = 1$ при $b = 0$ даетъ $ac = 1$; откуда для значеній a и c , которыя должны быть > 0 , выходитъ

$$a = 1, c = 1.$$

Изъ этого мы заключаемъ, что всѣ дѣлители формы $x^2 + y^2$ представляются формою $u^2 + v^2$.

На основаніи этой же теоремы дѣлители $x^2 + 2y^2$ будутъ представляться формами

$$au^2 + 2buv + cv^2,$$

въ которыхъ $ac - b^2 = 2$, a и c числа положительныя, не меньше $2b$ и b не $> \sqrt{\frac{2}{3}}$.

Но изъ условія b не $> \sqrt{\frac{2}{3}}$ слѣдуетъ, что $b = 0$; послѣ того изъ уравненія $ac - b^2 = 2$ выводимъ $ac = 2$. Но такъ какъ a и c должны быть числа положительныя, то это уравненіе предполагаетъ одно изъ двухъ: или $a = 2, c = 1$ или $a = 1, c = 2$. Первому предположенію соответствуетъ форма $2u^2 + v^2$, второму $u^2 + 2v^2$.

Но эти формы тождественны между собою; слѣд. всѣ дѣлители $x^2 + 2y^2$ представятся одною формою $2u^2 + v^2$.

Подобнымъ образомъ найдемъ, что дѣлители $x^2 - y^2$ представляются формою $u^2 - v^2$, дѣлители $x^2 - 2y^2$ представляются формою $u^2 - 2v^2$ или $2u^2 - v^2$, дѣлители $x^2 - 3y^2$ представляются формами $3u^2 - v^2, u^2 - 3v^2$. Для примѣра болѣе сложныхъ формъ возьмемъ $x^2 - 21y^2$.

По теоремѣ 60-й дѣлители этой формы будутъ представляться квадратичными формами

$$au^2 + 2buv - cv^2,$$

въ которыхъ

$$b \text{ не } > \sqrt{\frac{21}{5}}, \quad ac + b^2 = 21.$$

Первое намъ опредѣляетъ всѣ возможные величины b ; изъ него мы заключаемъ, что b можетъ имѣть только значенія

$$0, 1, 2.$$

Предполагая b послѣдовательно равнымъ всѣмъ этимъ числамъ, мы изъ уравненія $ac + b^2 = 21$, обращая вниманіе на то, что a и c болѣе 0 и не менѣе $2b$, найдемъ всѣ значенія, которыя могутъ имѣть a, b, c въ формѣ $au^2 + 2buv - cv^2$, опредѣляющей дѣлителей $x^2 - 21y^2$. Такъ дѣлая $b = 0$, найдемъ $ac = 21$, что можетъ быть удовлетворено только предположеніями

$$\begin{array}{c|c|c|c} a = 1 & a = 3 & a = 7 & a = 21 \\ c = 21 & c = 7 & c = 3 & c = 1 \end{array}$$

которыя всѣ удовлетворяютъ условію: a и $c > 0$ и не $< 2b$, гдѣ $b = 0$.

Дѣлая $b = 1$, найдемъ $ac + 1 = 21$; откуда $ac = 20$, и это приводитъ насъ къ предположеніямъ

$$\begin{array}{c|c|c|c|c|c|c} a = 1 & a = 2 & a = 4 & a = 5 & a = 10 & a = 20 \\ c = 20 & c = 10 & c = 5 & c = 4 & c = 2 & c = 1 \end{array}$$

Но первое и послѣднее не удовлетворяютъ условію: a и c не $< 2b$; ибо $b = 1$.

Итакъ для $b = 1$ будетъ одно изъ четырехъ

$$\begin{array}{c|c|c|c} a = 2 & a = 4 & a = 5 & a = 10 \\ c = 10 & c = 5 & c = 4 & c = 2 \end{array}$$

Наконецъ для $b = 2$ находимъ $ac + 4 = 21$; откуда $ac = 17$, и слѣд. одно изъ двухъ

$$\begin{array}{c|c} a = 1 & a = 17 \\ c = 17 & c = 1 \end{array}$$

Но оба эти случая невозможны; ибо $2b$, будучи здѣсь равно 4, въ первомъ предположеніи превосходитъ a , во второмъ c .

Итакъ всѣ дѣлители $x^2 - 17y^2$ должны представляться формами

$$\begin{aligned} &u^2 - 21v^2, 3u^2 - 7v^2, 7u^2 - 3v^2, 21u^2 - v^2, \\ &2u^2 + 2uv - 10v^2, 4u^2 + 2uv - 5v^2, 5u^2 + 2uv - 4v^2, \\ &10u^2 + 2uv - 2v^2. \end{aligned}$$

Но формы $2u^2 + 2uv - 10v^2$, $10u^2 + 2uv - 2v^2$ даютъ однѣ числа четныя; слѣд. всѣ нечетные дѣлители $x^2 - 21y^2$ будутъ представляться формами

$$\begin{aligned} &u^2 - 21v^2, 3u^2 - 7v^2, 7u^2 - 3v^2, 21u^2 - v^2, \\ &4u^2 + 2uv - 5v^2, 5u^2 + 2uv - 4v^2. \end{aligned}$$

Для другаго примѣра возьмемъ форму $x^2 + 26y^2$. По теоремѣ 61-й дѣлители ея представятся формами

$$au^2 + 2buv + cv^2,$$

гдѣ

$$b \text{ не } > \sqrt{\frac{26}{3}}, \quad ac - b^2 = 26, \quad a \text{ и } c \text{ не } < 2b.$$

Первое неравенство предполагаетъ b однимъ изъ трехъ чиселъ

$$0, 1, 2.$$

Дѣлая $b = 0$, мы для опредѣленія a и c находимъ условія

$$ac = 26, \quad a \text{ и } c \text{ не } < 0.$$

Эти условія приводятъ насъ къ предположеніямъ

$$\begin{array}{l} a = 1 \mid a = 2 \mid a = 13 \mid a = 26 \\ c = 26 \mid c = 13 \mid c = 2 \mid c = 1. \end{array}$$

Дѣлая $b = 1$, мы находимъ

$$ac = 27, \quad a \text{ и } c \text{ не } < 2.$$

Уравненію $ac = 27$ удовлетворяютъ

$$\begin{array}{l} a = 1 \mid a = 3 \mid a = 9 \mid a = 27 \\ c = 27 \mid c = 9 \mid c = 3 \mid c = 1. \end{array}$$

Но изъ этихъ величинъ a и c условію

$$a \text{ не } < 2, \quad c \text{ не } < 2$$

удовлетворяютъ только

$$\begin{array}{l|l} a = 3 & a = 9 \\ c = 9 & c = 3. \end{array}$$

Наконецъ для $b = 2$ находимъ

$$ac = 30, \text{ а н } c \text{ не } < 4.$$

Уравненію $ac = 30$ мы удовлетворяемъ предположеніями

$$\begin{array}{l|l|l|l|l|l|l|l} a = 1 & a = 2 & a = 3 & a = 5 & a = 6 & a = 10 & a = 15 & a = 30 \\ c = 30 & c = 15 & c = 10 & c = 6 & c = 5 & c = 3 & c = 2 & c = 1. \end{array}$$

Но изъ нихъ условію

$$a \text{ не } < 4, \text{ } c \text{ не } < 4$$

удовлетворяють только

$$\begin{array}{l|l} a = 5 & a = 6 \\ c = 6 & c = 5. \end{array}$$

Отсюда для дѣлителей $x^2 + 26y^2$ выходятъ слѣдующія формы

$$\begin{aligned} & u^2 + 26v^2, 2u^2 + 13v^2, 13u^2 + 2v^2, 26u^2 + v^2, \\ & 3u^2 + 2uv + 9v^2, 9u^2 + 2uv + 3v^2, 5u^2 + 4uv + 6v^2, \\ & 6u^2 + 4uv + 5v^2. \end{aligned}$$

Замѣчая, что здѣсь $u^2 + 26v^2$ тождественно съ $26u^2 + v^2$, $2u^2 + 13v^2$ съ $13u^2 + 2v^2$, $3u^2 + 2uv + 9v^2$ съ $9u^2 + 2uv + 3v^2$, $5u^2 + 4uv + 6v^2$ съ $6u^2 + 4uv + 5v^2$, заключаемъ, что всѣ дѣлители $x^2 + 26y^2$ будутъ представляться формами

$$u^2 + 26v^2, 2u^2 + 13v^2, 3u^2 + 2uv + 9v^2, 5u^2 + 4uv + 6v^2.$$

Вотъ какимъ образомъ на основаніи доказанныхъ нами теоремъ могутъ быть выведены всѣ квадратичныя формы дѣлителей $x^2 \pm Dy^2$. Отсюда выходятъ много любопытныхъ предложеній относительно рѣшенія уравненій вида $ax^2 + 2bxy + cy^2 = N$, составляющихъ предметъ изслѣдованія Теоріи неопредѣленныхъ уравненій высшихъ степеней. Здѣсь же мы воспользуемся квадратичными формами дѣлителей $x^2 \pm Dy^2$ для опредѣленія его линейныхъ дѣлителей. Мы показали, какъ найдутся дѣлители $x^2 \pm Dy^2$, когда D число простое; теперь мы покажемъ, какъ найдутся дѣлители этой формы при всякомъ значеніи D , будетъ ли D число простое или составное. При этомъ мы бу-

*

демь предполагать D недѣлящимся на квадратъ какого нибудь числа; ибо для $D = D_1 k^2$ форма $x^2 \pm D_1 k^2 y^2$ приведется къ $x^2 \pm D_1 (ky)^2$, и слѣд. къ $x^2 \pm D_1 y_1^2$, полагая $y_1 = ky$. Итакъ разсматривая дѣлителей формы $x^2 \pm Dy^2$, мы можемъ выкинуть изъ состава D все точные квадраты; поступая такимъ образомъ, мы будемъ имѣть формы вида $x \pm Dy^2$, гдѣ D не дѣлится на квадратъ какого нибудь числа; опредѣленіемъ дѣлителей этихъ формъ мы теперь и займемся.

§ 47. Прежде чѣмъ покажемъ, какимъ образомъ изъ квадратичныхъ формъ дѣлителей могутъ быть выведены линейные дѣлители, мы докажемъ относительно формы $au^2 + 2buv + cv^2$ слѣдующія теоремы:

62. Т Е О Р Е М А.

Если опредѣлитель формы $au^2 + 2buv + cv^2$ есть d , число недѣлящееся на квадратъ; то можно найти число α , для котораго $a + 2b\alpha + c\alpha^2$ будетъ число простое съ d .

Доказательство. Въ самомъ дѣлѣ, пусть будетъ ω общій наибольшій дѣлитель c и d ; число ω не будетъ заключать въ себѣ множителемъ никакого квадрата; ибо d не дѣлится на квадратъ. Но по значенію d мы имѣемъ $b^2 - ac = d$; откуда слѣдуетъ, что ω , общій дѣлитель c и d , дѣлитъ b^2 , и слѣд. по теоремѣ 6-й дѣлитъ b . Докажемъ же теперь, во 1-хъ) что можно всегда найти число α , для котораго выраженіе $\frac{ca + b}{\omega}$ приводится къ числу простому съ $\frac{d}{\omega}$, и во 2-хъ) что такое число α обращаетъ $a + 2b\alpha + c\alpha^2$ въ число простое съ d .

Въ первомъ не трудно убѣдиться, замѣтивъ, что при дѣлимости b на ω , общій наибольшій дѣлитель c и d , по теоремѣ 19 можно найти число, удовлетворяющее сравненію

$$ca + b \equiv \omega \pmod{d},$$

что предполагаетъ дѣлимость $ca + b - \omega$ на d . Полагая же частное отъ дѣленія $ca + b - \omega$ на d равнымъ N , будемъ имѣть

$$\frac{c\alpha + b - \omega}{d} = N;$$

откуда выходитъ

$$\frac{c\alpha + b}{\omega} = 1 + N \frac{d}{\omega},$$

что обнаруживаетъ въ $\frac{c\alpha + b}{\omega}$ число простое съ $\frac{d}{\omega}$.

Чтобы убѣдиться во второмъ, мы замѣчаемъ, что выраже-
ніе $a + 2b\alpha + c\alpha^2$ можетъ быть представлено такъ

$$\frac{\omega \left(\frac{c\alpha + b}{\omega} \right)^2 - \frac{b^2 - ac}{\omega}}{\frac{c}{\omega}},$$

гдѣ замѣняя $b^2 - ac$ черезъ d , имѣемъ

$$\frac{\omega \left(\frac{c\alpha + b}{\omega} \right)^2 - \frac{d}{\omega}}{\frac{c}{\omega}}.$$

Число же d разлагается на два множителя $\frac{d}{\omega}$ и ω , ко-
торые не могутъ имѣть общаго дѣлителя; ибо d не можетъ
дѣлиться на квадратъ; притомъ $\frac{d}{\omega}$ по свойству числа α про-
стое съ $\frac{c\alpha + b}{\omega}$. Отсюда слѣдуетъ, что ни ω , ни $\frac{d}{\omega}$ не могутъ
имѣть общаго множителя съ $\omega \left(\frac{c\alpha + b}{\omega} \right)^2 - \frac{d}{\omega}$; ибо простыя
числа, входящія въ составъ ω , дѣля $\omega \left(\frac{c\alpha + b}{\omega} \right)^2$, не могутъ дѣ-
лить $\frac{d}{\omega}$; напротивъ дѣлители $\frac{d}{\omega}$ не могутъ дѣлить $\omega \left(\frac{c\alpha + b}{\omega} \right)^2$.
Итакъ $\omega \left(\frac{c\alpha + b}{\omega} \right)^2 - \frac{d}{\omega}$ и слѣд.

$$\frac{c \left(\frac{c\alpha + b}{\omega} \right)^2 - \frac{d}{\omega}}{\frac{c}{\omega}} = a + 2b\alpha + c\alpha^2$$

число простое съ ω и $\frac{d}{\omega}$, а потому и съ произведеніемъ ихъ
 d , что и слѣдовало доказать.

Для примѣра найдемъ число α , для котораго бы $3 + 2 \cdot 21\alpha + 217\alpha^2$ было число простое съ $21^2 - 3 \cdot 217 = -210$. Замѣчая, что общій наибольшій дѣлитель 217 и 210 есть 7, мы для опредѣленія α находимъ условіе, что $\frac{217\alpha + 21}{7}$, или $31\alpha + 3$ число простое съ $\frac{210}{7}$ или 30. Этому условію, какъ видѣли, можно всегда удовлетворить, рѣшая сравненіе

$$217\alpha + 21 \equiv 7 \pmod{210}.$$

Но въ этомъ случаѣ, какъ и въ большей части другихъ, мы можемъ легко найти α , пробуя различныя числа. Такъ находимъ, что $\alpha = -2$ обращаетъ $31\alpha + 3$ въ число простое съ 30. Слѣд. и выраженіе $3 + 2 \cdot 21\alpha + 217\alpha^2$ при $\alpha = -2$ будетъ число простое съ 210.

На основаніи доказанной нами теоремы для всякой формы $au^2 + 2buv + cv^2$ найдется число α , обращающее $a + 2b\alpha + c\alpha^2$ въ число простое съ опредѣлителемъ ея. Опредѣливши такое число, мы можемъ преобразовать форму $au^2 + 2buv + cv^2$ въ другую, гдѣ первый членъ будетъ имѣть коэффициентомъ число простое съ опредѣлителемъ ея d . Этому мы достигнемъ всегда, дѣлая въ этой формѣ $v - \alpha u = U$, гдѣ α есть число, обращающее $a + 2b\alpha + c\alpha^2$ въ число простое съ d . Въ самомъ дѣлѣ, изъ этого уравненія найдемъ $v = \alpha u + U$, и внося эту величину въ форму $au^2 + 2buv + cv^2$, мы ее преобразуемъ въ такую

$$au^2 + 2b(\alpha u + U)u + c(\alpha u + U)^2,$$

что по раскрытіи скобокъ даетъ

$$(a + 2b\alpha + c\alpha^2)u^2 + 2(b + \alpha c)uU + cU^2,$$

гдѣ коэффициентъ перваго члена есть $a + 2b\alpha + c\alpha^2$, число простое съ d по положенію.

Такъ чтобы сдѣлать въ формѣ $3u^2 + 2 \cdot 21uv + 217v^2$ первый коэффициентъ числомъ простымъ съ опредѣлителемъ ея, ищемъ число α , которое бы обратило $3 + 2 \cdot 21\alpha + 217\alpha^2$ въ число простое съ 210. Этому условію, какъ видѣли, удовлетворяетъ $\alpha = -2$. Поэтому для преобразованія формы

$3u^2 + 2 \cdot 21uv + 217v^2$ дѣлаемъ $v + 2u = U$, и на мѣсто v въ форму $3u^2 + 2 \cdot 21uv + 217v^2$ вносимъ $U - 2u$. Это даетъ намъ

$$3u^2 + 2 \cdot 21(U - 2u)u + 217(U - 2u)^2,$$

или

$$787u^2 - 826Uu + 217U^2.$$

Такимъ образомъ данная форма

$$3u^2 + 2 \cdot 21uv + 217v^2$$

преобразовывается въ форму

$$787u^2 - 826uU + 217U^2.$$

Последняя форма сложнѣе первой; но она имѣетъ ту выгоду, что въ ней коэффициентъ u^2 число простое съ опредѣлителемъ. Это послужитъ значительнымъ облегченіемъ при опредѣленіи линейныхъ дѣлителей, и теперь вездѣ мы будемъ предполагать квадратичныя формы преобразованными такъ, что въ нихъ первый коэффициентъ число простое съ опредѣлителемъ. Въ этомъ предположеніи мы докажемъ слѣдующія теоремы относительно квадратичныхъ формъ:

63. ТЕОРЕМА.

Если въ формѣ $au^2 + 2buv + cv^2$ число a простое съ опредѣлителемъ $b^2 - ac = d$, то можно найти число l , удовлетворяющее сравненію

$$au^2 + 2buv + cv^2 \equiv al^2 + 2bl + c \pmod{d}.$$

Доказательство. Въ самомъ дѣлѣ, при a простомъ съ d сравненіе

$$a(u^2 + 2buv + cv^2) \equiv a(al^2 + 2bl + c) \pmod{d}$$

можетъ быть сокращено на a ; вслѣдствіе чего оно приводится къ

$$u^2 + 2buv + cv^2 \equiv al^2 + 2bl + c \pmod{d},$$

которое хотимъ доказать. Но сравненіе

$$a(u^2 + 2buv + cv^2) \equiv a(al^2 + 2bl + c) \pmod{d}$$

можетъ быть такъ представлено:

$(au + bv)^2 - (b^2 - ac)v^2 \equiv (al + b)^2 - (b^2 - ac) \dots \dots (\text{mod. } d)$,
 что по равенству $b - ac^2$ съ модулем d приводится къ слѣ-
 дующему

$$(au + bv)^2 \equiv (al + b)^2 (\text{mod. } d),$$

а это удовлетворяется, если

$$al + b \equiv au + bv (\text{mod. } d).$$

Но послѣднему сравненію мы всегда можемъ удовлетворить; ибо оно первой степени и a простое съ d ; откуда и выходить пред-
 ложенная нами теорема.

На основаніи этой теоремы мы заключаемъ, что если при
 всѣхъ величинахъ l значенія $al^2 + 2bl + c$ по модулю d срав-
 нимы съ числами

$$r_1, r_2, \dots, r_n;$$

то съ ними сравнимы также и всѣ значенія $au^2 + 2buv + cv^2$,
 и слѣд. всѣ числа, опредѣляемыя этою формою будутъ одного
 изъ слѣдующихъ видовъ

$$md + r_1, md + r_2, \dots, md + r_n,$$

гдѣ m произвольное число. Чтоже касается до чиселъ r_1, r_2, \dots, r_n ,
 съ которыми сравнимы по модулю d всѣ значенія $al^2 + 2al + c$;
 то мы ихъ найдемъ, опредѣляя числа, сравнимыя съ этимъ вы-
 раженіемъ при $l = 0, 1, 2, \dots, d - 1$; ибо съ этими значеніями
 $al^2 + 2bl + c$ по модулю d будутъ сравнимы всѣ другія.

Такъ для выраженія чиселъ, опредѣляемыхъ формою

$$au^2 + 2buv + cv^2,$$

найдемъ линейныя формы

$$md + r_1, md + r_2, \dots, md + r_n.$$

Но каждая изъ этихъ формъ приводится къ четыремъ,
 смотря по виду числа m . Такъ предполагая въ первой формѣ
 m равнымъ $4z, 4z + 1, 4z + 2, 4z + 3$, мы изъ нея выве-
 демъ четыре

$$4dz + r_1, 4dz + d + r_1, 4dz + 2d + r_1, 4dz + 3d + r_1,$$

и ограничиваясь одними нечетными значеніями $au^2 + 2buv + cv^2$,
 посмотримъ, которыя изъ этихъ формъ должны быть выкинуты.

Начнемъ съ d нечетнаго. При d нечетномъ между числами $r_1, d+r_1, 2d+r_1, 3d+r_1$ будетъ два четныхъ и два нечетныхъ (см. теор. 10). Ограничиваясь одними нечетными значеніями $au^2 + 2buv + cv^2$, мы изъ четырехъ формъ

$$4dz + r_1, 4dz + d + r_1, 4dz + 2d + r_1, 4dz + 3d + r_1$$

выкинемъ двѣ, въ которыхъ члены, не содержащія z будутъ четныя. Затѣмъ для выраженія нечетныхъ значеній $au^2 + 2buv + cv^2$ останутся двѣ формы, изъ которыхъ одна будетъ давать числа вида $4m + 1$, другая вида $4m + 3$ (см. § 44).

Изъ этихъ формъ мы оставимъ или одну только или обѣ, смотря потому даетъ ли форма $au^2 + 2buv + cv^2$ однѣ числа вида $4m + 1$ или однѣ числа вида $4m + 3$ или тѣ и другія вмѣстѣ. Но это узнаемъ мы, замѣчая, что относительно u и v можно сдѣлать четыре предположенія

$$\begin{array}{l} u = 2k \quad | \quad u = 2k + 1 \quad | \quad u = 2k + 1 \quad | \quad u = 2k \\ v = 2s \quad | \quad v = 2s \quad \quad \quad | \quad v = 2s + 1 \quad | \quad v = 2s + 1. \end{array}$$

Внеся же эти значенія u и v въ форму $au^2 + 2buv + cv^2$, находимъ результаты такого вида

$$4N, 4N_1 + a, 4N_2 + a + 2b + c, 4N_3 + c,$$

гдѣ называемъ черезъ $4N, 4N_1, 4N_2, 4N_3$ совокупность членовъ, имѣющихъ множителемъ 4.

Изъ этого видно, что если ни одно изъ чиселъ $a, b, a + 2b + c$ не есть вида $4m + 1$ или $4m + 3$, то форма $au^2 + 2buv + cv^2$ не даетъ чиселъ этого вида.

Обращаемся теперь къ случаю d четнаго.

При d четномъ всѣ числа $r_1, d+r_1, 2d+r_1, 3d+r_1$ или будутъ четныя или всѣ будутъ нечетныя. Въ первомъ случаѣ мы заключимъ, что форма $au^2 + 2buv + cv^2$ не даетъ чиселъ нечетныхъ; во второмъ же по виду чиселъ $r_1, d+r_1, 2d+r_1, 3d+r_1$ мы узнаемъ какого изъ четырехъ видовъ: $8m + 1, 8m + 3, 8m + 5, 8m + 7$ числа выражаются каждою изъ линейныхъ формъ

$$4dz + r_1, 4dz + d + r_1, 4dz + 2d + r_1, 4dz + 3d + r_1,$$

и мы увидимъ, которыя изъ нихъ должны быть выкинуты, опредѣливъ, какихъ изъ четырехъ видовъ $8m + 1$, $8m + 3$, $8m + 5$, $8m + 7$ получаются числа изъ формы $au^2 + 2buv + cv^2$. Для этого мы замѣчаемъ, что относительно u и v можно сдѣлать только девять предположеній:

$$u = 2k + 1 \mid u = 2k + 1 \mid u = 2k + 1 \mid u = 4k \mid u = 4k \\ v = 2s + 1 \mid v = 4s \mid v = 4s + 2 \mid v = 2s + 1 \mid v = 4s$$

$$u = 4k \mid u = 2k + 2 \mid u = 4k + 2 \mid u = 4k + 2 \\ s = 4s + 2 \mid v = 2s + 1 \mid v = 4s + 2 \mid v = 4s$$

изъ которыхъ четыре

$$u = 4k \mid u = 4k \mid u = 4k + 2 \mid u = 4k + 2 \\ v = 4s \mid v = 4s + 2 \mid v = 4s + 2 \mid v = 4s$$

не должны имѣть мѣста; ибо въ нихъ значеніе $au^2 + 2buv + cv^2$ будетъ всегда число четное. Что же касается до остальныхъ предположеній, то дѣлая въ формѣ $au^2 + 2buv + cv^2$

$$u = 2k + 1 \mid u = 2k + 1 \mid u = 2k + 1 \mid u = 4k + 2 \mid u = 4k \\ v = 2s + 1 \mid v = 4s \mid v = 4s + 2 \mid v = 2s + 1 \mid v = 2s + 1,$$

мы находимъ результаты такого вида

$$8N + a + 2b + c, \quad 8N_1 + a, \quad 8N_2 + a + 4b + 4c \\ 8N_3 + 4a + 4b + c, \quad 8N_4 + c,$$

гдѣ $8N$, $8N_1$, $8N_2$, $8N_3$, $8N_4$ означаетъ совокупность всѣхъ членовъ, имѣющихъ множителемъ 8; сюда же относятся члены $4(k^2 + k)$, $4(s^2 + s)$, которыя на 8, очевидно, дѣлятся.

Отсюда слѣдуетъ, что числа, опредѣляемая формою

$$au^2 + 2buv + cv^2,$$

могутъ имѣть какой либо изъ видовъ $8m + 1$, $8m + 3$, $8m + 5$, $8m + 7$ только тогда, когда этого вида есть число между a , c , $a + 2b + c$, $4a + 4b + c$, $a + 4b + 4c$, и этимъ опредѣляется, которыя изъ четырехъ формъ

$$4dz + r_1, \quad 4dz + d + r_1, \quad 4dz + 2d + r_1, \quad 4dz + 3d + r_1$$

могутъ выражать нечетныя значенія $au^2 + 2buv + cv^2$ и которыя должны быть откинуты.

Покажемъ это на примѣрѣ.

Мы видѣли, что всѣ нечетные дѣлители $x^2 + 26y^2$ представляются формами

$$u^2 + 26v^2, 2u^2 + 13v^2, 3u^2 + 2uv + 9v^2, 5u^2 + 4uv + 6v^2.$$

Чтобы опредѣлить линейныя формы чиселъ, представляемыхъ первою, мы замѣчаемъ, что въ ней коэффициентъ u^2 не имѣетъ общаго дѣлителя съ опредѣлителемъ формы; поэтому къ ней можетъ быть приложена теорема 63. На основаніи этой теоремы мы заключаемъ, что всѣ значенія $u^2 + 26v^2$ по модулю 26 будутъ сравнимы съ тѣми же числами, съ которыми сравнимы значенія $l^2 + 26$ при $l = 0, 1, 2, \dots, 25$. Но наименьшія числа, сравнимыя съ

$$0^2 + 26, 1^2 + 26, 2^2 + 26, \dots, 25^2 + 26$$

по модулю 26, мы находимъ въ остаткѣ, получаемомъ при дѣленіи этихъ чиселъ на 26. Опредѣляя эти остатки, находимъ, что всѣ они равны

$$0, 1, 4, 9, 16, 25, 10, 23, 12, 3, 22, 17, 14, 13.$$

Откуда заключаемъ, что съ этими числами по модулю 26 сравнимы и всѣ значенія $u^2 + 26v^2$, а потому эти значенія должны представляться формами

$$\begin{aligned} &26m + 0, 26m + 1, 26m + 4, 26m + 9, 26m + 16, \\ &26m + 25, 26m + 10, 26m + 23, 26m + 12, 26m + 3, \\ &26m + 22, 26m + 17, 26m + 14, 26m + 13. \end{aligned}$$

Но изъ нихъ только формы

$$\begin{aligned} &26m + 1, 26m + 9, 26m + 25, 26m + 23 \\ &26m + 3, 26m + 17 \end{aligned}$$

даютъ числа нечетныя и простыя съ 26; ихъ мы только и оставимъ. Дѣлая здѣсь $m = 4z, 4z + 1, 4z + 2, 4z + 3$, мы выведемъ

$$\begin{aligned} &104z + 1, 104z + 27, 104z + 53, 104z + 79, \\ &104z + 9, 104z + 35, 104z + 61, 104z + 87, \\ &104z + 25, 104z + 51, 104z + 77, 104z + 103, \\ &104z + 23, 104z + 49, 104z + 75, 104z + 101, \\ &104z + 3, 104z + 29, 104z + 55, 194z + 81, \\ &104z + 17, 104z + 43, 104z + 69, 104z + 95. \end{aligned}$$

Но чтобы узнать, которые изъ этихъ формъ должно оставить и которые выкинуть, мы должны опредѣлить, какія изъ четырехъ видовъ $8m + 1$, $8m + 3$, $8m + 5$, $8m + 7$ имѣютъ числа, получаемыя изъ формы $u^2 + 26v^2$. Мы видѣли, что вообще для формы $au^2 + 2buv + cv^2$ это опредѣляется видами чиселъ

$$a, c, a + 2b + c, 4a + 4b + c, a + 4b + 4c.$$

Отсюда для формы $u^2 + 26v^2$ выходитъ

$$1, 26, 1 + 26, 4 + 26, 1 + 4 \cdot 26.$$

Но здѣсь нѣтъ чиселъ вида $8m + 5$ и $8m + 7$. Слѣд. въ найденныхъ нами въ формахъ мы должны откинуть тѣ, которыя даютъ числа этого вида.

Такъ замѣчая, что 53, 61, 77, 29, 101, 69 суть вида $8m + 5$, а числа 79, 87, 103, 55, 23, 95 вида $8m + 7$, мы откпдываемъ формы

$$104z + 53, 104z + 61, 104z + 77, 104z + 29,$$

$$104z + 101, 104z + 69, 104z + 79, 104z + 87,$$

$$104z + 103, 104z + 55, 104z + 23, 104z + 95,$$

и у насъ остаются слѣдующія:

$$104z + 1, 104z + 27, 104z + 9, 104z + 35,$$

$$104z + 25, 104z + 51, 104z + 49, 104z + 75, 104z + 3,$$

$$104z + 81, 104z + 17, 104z + 43.$$

Разкроемъ теперь линейныя формы чиселъ, опредѣляемыхъ квадратичною формою $2u^2 + 13v^2$. Но къ этой формѣ нельзя прямо приложить теорему 63; ибо въ ней коэффициентъ u^2 есть 2, число непростое съ опредѣлителемъ — 26.

По этому мы должны предварительно эту форму преобразовать по способу показанному нами выше. Для этого, замѣчая, что общій наибольшій дѣлитель 2 и 26 есть 2, мы ищемъ α , которое бы обратило $\frac{2\alpha + 0}{2}$, или α , въ число простое съ 26. Этому условію удовлетворяетъ 1, а потому для преобразованія формы $2u^2 + 13v^2$ вносимъ въ нее $U + u$ на мѣсто v , черезъ что она обращается въ слѣдующую

$$15u^2 + 26uU + 13U^2.$$

Получивъ такимъ образомъ форму, въ которой первый коэффициентъ число простое съ определителемъ — 26, мы на основаніи теоремы 63 заключаемъ, что ея значенія по модулю 26 будутъ сравнимы съ остатками, получаемыми при дѣленіи $15.0^2 + 26.0 + 13$, $15.1^2 + 26.1 + 13$, $15.2^2 + 26.2 + 13$,
 $15.25^2 + 26.25 + 13$ на 26.

Но эти остатки мы находимъ равными числамъ

13, 28, 21, 18, 19, 24, 7, 20, 11, 10, 5, 8, 15, 0;

слѣд. по модулю 26 сравнимы съ ними все значенія $15u^2 + 26$ и $U + 13U^2$, а потому они могутъ быть представлены формами

$26m + 13$, $26m + 28$, $26m + 21$, $26m + 18$,
 $26m + 19$, $26m + 24$, $26m + 7$, $26m + 20$, $26m + 11$,
 $26m + 10$, $26m + 5$, $26m + 8$, $26m + 15$, $26m + 0$.

Но изъ этихъ формъ только

$26m + 21$, $26m + 19$, $26m + 7$, $26m + 11$, $26m + 5$, $26m + 15$
 даютъ числа нечетныя и простыя съ определителемъ — 26; ихъ мы только и оставляемъ. Дѣлая здѣсь $m = 4z$, $4z + 1$, $4z + 2$, $4z + 3$, мы изъ этихъ формъ выводимъ

$104z + 21$, $104z + 47$, $104z + 73$, $104z + 99$,
 $104z + 19$, $104z + 45$, $104z + 71$, $104z + 97$,
 $104z + 7$, $104z + 33$, $104z + 59$, $104z + 85$,
 $104z + 11$, $104z + 37$, $104z + 63$, $104z + 89$,
 $104z + 5$, $104z + 31$, $104z + 57$, $104z + 83$,
 $104z + 15$, $104z + 41$, $104z + 67$, $104z + 93$.

Но такъ какъ числа, выражаемыя формою

$$15u^2 + 26uU + 13U^2,$$

не могутъ быть вида $8m + 1$ и $8m + 3$; ибо ни одно изъ чиселъ

15, 13, $15 + 26 + 13$, $4.15 + 2.26 + 13$, $15 + 2.26 + 4.13$
 не есть этого вида. Поэтому изъ найденныхъ линейныхъ формъ

мы должны выкинуть всѣ, которыя даютъ числа или вида $8m + 1$ или $8m + 3$.

Затѣмъ для выраженія чиселъ нечетныхъ и простыхъ съ опредѣлителемъ, получаемыхъ изъ формы $15u^2 + 26uU + 13U^2$, остаются

$$\begin{aligned} &104z + 21, 104z + 47, 104z + 45, 104z + 71, \\ &104z + 7, 104z + 85, 104z + 37, 104z + 63, \\ &104z + 5, 104z + 31, 104z + 15, 104z + 93. \end{aligned}$$

Чтобы найти всѣ линейные дѣлители $x^2 + 26y^2$ намъ остается найти линейныя формы для выраженія чиселъ, опредѣляемыхъ формамъ

$$3u^2 + 2uv + 9v^2, 5u^2 + 4uv + 6v^2.$$

Но при этомъ мы находимъ для формы $3u^2 + 2uv + 9v^2$ тѣ же линейныя формы какія нашли для $u^2 + 26v^2$, а для формы $5u^2 + 4uv + 6v^2$ тѣ же, какія нашли для $2u^2 + 13v^2$. И такъ всѣ нечетные дѣлители формы $x^2 + 26y^2$, простые съ 26, опредѣляются слѣдующими формамъ

$$\begin{aligned} &104z + 1, 104z + 3, 104z + 5, 104z + 7, \\ &104z + 9, 104z + 15, 104z + 17, 104z + 21, \\ &104z + 25, 104z + 27, 104z + 31, 104z + 35, \\ &104z + 37, 104z + 43, 104z + 45, 104z + 47, \\ &104z + 49, 104z + 51, 104z + 63, 104z + 71, \\ &104z + 75, 104z + 81, 104z + 85, 104z + 93. \end{aligned}$$

Такъ съ помощію квадратичныхъ формъ могутъ быть опредѣлены линейные дѣлители $x^2 \pm Dy^2$, будетъ ли D число простое или составное. Но чтобы при опредѣленіи ихъ не дѣлать лишнихъ выкладокъ, мы покажемъ теперь средство узнавать, что двѣ квадратичныя формы дѣлителей $x^2 \pm Dy^2$ приводятся къ однимъ линейнымъ формамъ, какъ въ предыдущемъ примѣрѣ

$$u^2 + 26v^2 \text{ и } 3u^2 + 2uv + 9v^2, 2u^2 + 13v^2 \text{ и } 5u^2 + 4uv + 6v^2.$$

Для этого мы докажемъ слѣдующую теорему:

64. Т Е О Р Е М А.

Если $ax^2 + 2bix + c^2$, $a_1U^2 + 2b_1UV + c_1V$ суть квадратичныя формы дѣлителей $x^2 - dy^2$, и a , a_1 числа простыя съ d ; притомъ $a_1 \equiv al^2 + 2bl + c \pmod{d}$, гдѣ l какое нибудь число; то можно найти x , удовлетворяющій сравненію

$$a_1x^2 + 2b_1x + c_1 \equiv ax^2 + 2bx + c \pmod{d}.$$

Доказательство. Въ самомъ дѣлѣ при a и a_1 простыхъ съ d сравненіе

$$a^2a_1(a_1x^2 + 2b_1x + c_1) \equiv a^2a_1(ax^2 + 2bx + c) \pmod{d}$$

можетъ быть сокращено на $a^2 \cdot a_1$ и такимъ образомъ оно приводится къ

$$a_1x^2 + 2b_1x + c_1 \equiv ax^2 + 2bx + c \pmod{d},$$

котораго возможность имѣемъ въ виду доказать. Но сравненіе

$$a^2a_1(a_1x^2 + 2b_1x + c_1) \equiv a^2a_1(ax^2 + 2bx + c) \pmod{d}$$

можетъ быть такъ представлено:

$$(aa_1x + ab_1)^2 - a^2(b_1^2 - a_1c_1) \equiv aa_1(ax + b)^2 - aa_1(b^2 - ac) \pmod{d},$$

гдѣ $b_1^2 - a_1c_1$, $b^2 - ac$ равны d ; ибо по положенію

$$a_1U^2 + 2b_1UV + c_1V^2, ax^2 + 2bix + c^2$$

суть квадратичныя формы дѣлителей $x^2 - dy^2$ (см. теор. 59).

Вслѣдствіе чего предыдущее сравненіе приводится къ такому

$$(aa_1x + ab_1)^2 \equiv aa_1(ax + b)^2 \pmod{d}.$$

Это же сравненіе удовлетворяется, если

$$aa_1x + ab_1 \equiv (ax + b)(al + b) \pmod{d}.$$

Чтобы убѣдиться въ этомъ замѣтимъ, что для этой величины $aa_1x + ab_1$ оно приводится къ

$$(ax + b)^2 (al + b)^2 \equiv aa_1(ax + b)^2 \pmod{d}.$$

Но $(al + b)^2$ сравнимо съ $a \cdot a_1$ по модулю d ; ибо по положенію

$$a_1 \equiv al^2 + 2bl + c \pmod{d};$$

откуда выходитъ

$$aa_1 \equiv a(al^2 + 2bl + c) \pmod{d},$$

или $aa_1 \equiv (al + b)^2 - (b^2 - ac) \pmod{d}$,

и слѣд. $aa_1 \equiv (al + b)^2$, потому что $b^2 - ac$ есть d .

Итакъ, чтобы удовлетворить сравненію

$$a_1x^2 + 2b_1x + c_1 \equiv ax^2 + 2bx + c \pmod{d}$$

необходимо только найти x , для котораго

$$aa_1x + ab_1 \equiv (ax + b)(al + b) \pmod{d},$$

что не представляет ни какой трудности; ибо здѣсь x въ первой степени и коэффициентъ его aa_1 число простое съ модулемъ d .

Такъ убѣждаемся въ справедливости предложенной нами теоремы.

На основаніи ея и теоремы 63-й мы заключаемъ, что если a будетъ сравнимо по модулю d съ какимъ либо значеніемъ $al^2 + 2al + c$, то числа, опредѣляемыя формами

$$au^2 + 2buv + cv^2, a_1U^2 + 2b_1UV + c_1V^2,$$

будутъ сравнимы съ одними и тѣми же числами; а потому какъ для той, такъ и для другой линейныя формы вида $md + r$ будутъ одиѣ и тѣже.

Что же касается до формъ вида $4md + r$, то мы ихъ легко выведемъ изъ формъ вида $md + r$, и на основаніи показаннаго нами способа выводять эти формы видно, что онѣ для $au^2 + 2buv + cv^2$ и $a_1U^2 + 2b_1UV + c_1V^2$ будутъ различныя или одинакія, смотря по виду чиселъ $a, c, a + 2b + c, a_1, c_1, a_1 + 2b_1 + c_1$ при d нечетномъ и по виду чиселъ $a, c, a + 2b + c, 4a + 4b + c, a + 4b + 4c, a_1, c_1, a_1 + 2b_1 + c_1, 4a + 4b_1 + c_1, a_1 + 4b_1 + 4c_1$ при d четномъ. Этимъ мы оканчиваемъ теорію дѣлителей $x^2 \pm dy^2$. Въ концѣ книги помѣщены таблицы линейныхъ дѣлителей формъ $x^2 \pm dy^2$ для всѣхъ значеній d , недѣлящихся на квадратъ, отъ $d = 1$ до $d = 101$. Эти таблицы имѣютъ весьма важныя приложенія, какъ мы увидимъ въ слѣдующей главѣ.



ГЛАВА VIII.

ПРИЛОЖЕНІЕ ТЕОРИИ СРАВНЕНІЙ КЪ РАЗЛОЖЕНІЮ ЧИСЕЛЪ НА ПРОСТЫЕ МНОЖИТЕЛИ.

§ 48. Въ заключеніе Теоріи сравненій, мы покажемъ какимъ образомъ, на основаніи ея, можетъ быть упрощено разложеніе чиселъ на простые множители.

Извѣстно, что для разложенія числа A на простые множители мы должны отыскать наименьшее простое число, которое дѣлитъ A ; если это число есть α ; то дѣлитель A на α и искать наименьшее простое число, которое дѣлитъ $\frac{A}{\alpha}$; если это число есть β ; то искать наименьшаго дѣлителя $\frac{A}{\alpha\beta}$ и продолжать это до тѣхъ поръ, пока дойдемъ до частнаго, которое не дѣлится на всѣ простыя числа, не превосходящія его квадратнаго корня. Это частное будетъ число простое, и произведеніе его на α, β, \dots будетъ искомое разложеніе числа A . Такимъ образомъ разложеніе чиселъ на простые множители приводится къ изслѣдованіямъ, что данное число имѣеть-ли дѣлителей или нѣтъ, и если имѣеть, то какой наименьшій изъ нихъ. Но эти изслѣдованія представляютъ большія трудности для чиселъ значительныхъ. Такъ на началахъ Арифметики наименьшаго дѣлителя числа N мы должны искать между всѣми простыми числами, меньшими \sqrt{N} , пробуя на нихъ дѣлитель N . Но такихъ чиселъ будетъ много, если N велико, и намъ не рѣдко придется испытать значительную часть ихъ, прежде чѣмъ попадемъ на дѣлителя N . Еще болѣе трудности встрѣчаемъ при N простомъ; въ этомъ случаѣ мы должны будемъ испытать дѣлитель N на всѣ простыя числа до \sqrt{N} . Такъ на началахъ Арифметики изслѣдованіе состава какого нибудь числа, превосходящаго 1000000, потребуетъ не рѣдко болѣе 160 дѣленій; ибо чиселъ простыхъ меньшихъ $\sqrt{1000000}$, или 1000, находить 168. На основаніи Теоріи сравненій эти изысканія зна-

чительно облегчаются; мы можем по виду данного числа опредѣлить видъ всѣхъ возможныхъ дѣлителей его, и намъ останется только испытать числа этого вида.

§ 49. Мы начнемъ съ частнаго случая, особенно замѣчательнаго, и покажемъ, какъ могутъ быть опредѣлены формы дѣлителей чиселъ вида $a^m \pm 1$, для которыхъ, на основаніи теоремъ V-й главы, не трудно доказать слѣдующее:

65. Т Е О Р Е М А.

Если p нечетное число и дѣлитъ $a^m - 1$; то p можетъ быть выражено формою $\omega z + 1$, гдѣ ω дѣлитель m (включая сюда и 1), z число простое съ $\frac{m}{\omega}$; притомъ p должно дѣлить $a^\omega - 1$.

Доказательство. Если ω есть общій наибольшій дѣлитель $p - 1$ и m ; то числа $\frac{p-1}{\omega}$, $\frac{m}{\omega}$ цѣлыя и простыя между собою. Полагая первое изъ нихъ равнымъ z , будемъ имѣть

$$\frac{p-1}{\omega} = z;$$

откуда $p = \omega z + 1$.

Намъ остается теперь доказать, что p будетъ дѣлитель $a^\omega - 1$. Для этого мы замѣчаемъ, что дѣлимость $a^m - 1$ на p выражается сравненіемъ

$$a^m - 1 \equiv 0 \pmod{p},$$

которое по теоремѣ 35-й при $p - 1$ и m имѣющихъ общимъ наибольшимъ дѣлителемъ ω предполагаетъ

$$a^\omega - 1 \equiv 0 \pmod{p},$$

и слѣд. дѣлимость $a^\omega - 1$ на p , что и слѣдовало доказать.

Изъ этой теоремы легко вывести слѣдующую:

66. Т Е О Р Е М А.

Если $2n + 1$ число простое; то простые нечетные дѣлители $a^{2n+1} - 1$ должны быть вида $2(2n + 1)z + 1$ или дѣ-

литъ $a - 1$; притомъ они должны быть дѣлителями формы $x^2 - ay^2$.

Доказательство. Если p нечетное число; то оно можетъ быть такъ представлено $2N + 1$. Но эта форма при дѣлительности N на $2n + 1$ приводится къ такой $2(2n + 1)z + 1$. Въ томъ же случаѣ, когда N не дѣлится на простое число $2n + 1$, число $2N$ будетъ простое съ $2n + 1$. Но если p дѣлится $a^{2n+1} - 1$ и выражается черезъ $2N + 1$, гдѣ $2N$ простое съ $2n + 1$; то по предыдущей теоремѣ оно должно дѣлить $a - 1$. Итакъ p должно быть вида $2(2n + 1)z + 1$ или дѣлить $a - 1$.

Докажемъ же теперь, что p должно быть дѣлителемъ формы $x^2 - ay^2$. Въ этомъ не трудно убѣдиться: p дѣлится $a^{2n+1} - 1$, и слѣд. дѣлится $a'(a^{2n+1} - 1)$, а это приводится къ $(a^{n+1})^2 - a$, выраженію вида $x^2 - ay^2$.

Замѣчая, что при $a = 2$ никакое число не дѣлится $a - 1$; дѣлители же $x^2 - ay^2$ по 55-й теоремѣ должны быть одного изъ двухъ видовъ: $8m + 1$ или $8m - 1$, мы на основаніи доказаннаго нами заключаемъ, что всѣ простые дѣлители $2^{2n+1} - 1$ при $2n + 1$ простомъ должны быть вида $2(2n + 1)z + 1$, и въ тоже время должны быть одного изъ двухъ видовъ: $8m + 1$ или $8m - 1$. Опредѣливши такимъ образомъ видъ дѣлителей числа $2^{2n+1} - 1$, не трудно найти ихъ во всякомъ частномъ случаѣ, или убѣдиться въ отсутствіи ихъ.

Для примѣра возьмемъ число $2^{23} - 1$, равное 8388607. Такъ какъ 23 число простое, то дѣлители $2^{23} - 1$ должны быть вида $46z + 1$ и въ тоже время одного изъ двухъ видовъ: $8m + 1$ или $8m - 1$. Чтобы соединить эти два свойства, мы замѣчаемъ, что z можетъ быть одного изъ четырехъ видовъ

$$4x, 4x + 1, 4x + 2, 4x + 3.$$

Для этихъ значеній z форма $46z + 1$ приводится къ такимъ четыремъ

$$184z + 1, 184z + 47, 184z + 93, 184z + 139,$$

изъ которыхъ послѣднія двѣ не даютъ чиселъ вида $8m + 1$ и

*

8m — 1. Слѣд. для дѣлителей числа 8388607 возможны только двѣ формы

$$184z + 1, 184z + 47.$$

На основаніи ихъ не трудно показать всѣ простыя числа, между которыми должно искать дѣлителей 8388607. Для этого ограничиваясь дѣлителями, не превосходящими $\sqrt{8388607}$, мы опредѣляемъ значенія

$$184x + 1, 184x + 47$$

при $x = 0, 1, 2, \dots, 15$. Между ними находимъ слѣдующія простыя числа 599, 967, 1151, 1289, 1657, 2393.

Но для на нихъ 8388607, мы замѣчаемъ, что ни одно изъ нихъ не дѣлитъ 8388607; откуда заключаемъ, что 8388607 число простое.

Такимъ же образомъ Эйлеръ нашель, что

$$2^{31} - 1 = 2147483647$$

есть число простое, и это есть самое большое простое число, доселѣ извѣстное.

Подобнымъ образомъ на основаніи доказанныхъ нами теоремъ легко изслѣдовать составъ всякаго числа, опредѣляемаго формулою $a^m - 1$.

Переходимъ теперъ къ числамъ вида $a^m + 1$, и относительно ихъ дѣлителей докажемъ слѣдующую теорему:

67. ТЕОРЕМА.

Если p простое нечетное число и дѣлитъ $a^m + 1$; то p можетъ быть такъ представлено: $2\omega z + 1$, гдѣ ω дѣлитель m (не исключая 1), который въ частномъ $\frac{m}{\omega}$ даетъ число нечетное, z число простое съ $\frac{m}{\omega}$, притомъ p должно дѣлить $a^\omega + 1$.

Доказательство. Дѣлимость $a^m + 1$ на p выражается сравненіемъ

$$a^m + 1 \equiv 0 \pmod{p},$$

которое по 39-й теоремѣ предполагаетъ

$$a^\omega + 1 \equiv 0 \pmod{p},$$

гдѣ ω общій наибольшій дѣлитель m и $p - 1$, который въ частномъ $\frac{p-1}{\omega}$ долженъ дать число четное. Полагая это частное равнымъ $2z$, найдемъ

$$\frac{p-1}{\omega} = 2z;$$

и слѣдовательно

$$p = 2\omega z + 1.$$

Но нетрудно убѣдиться, что здѣсь z число простое съ $\frac{m}{\omega}$, и частное $\frac{m}{\omega}$ число нечетное. Въ самомъ дѣлѣ, число ω , будучи общимъ наибольшимъ дѣлителемъ $p - 1$ и m , въ частныхъ $\frac{p-1}{\omega}$, $\frac{m}{\omega}$ должно дать числа простые между собою. Но первое есть $2z$, и оно не иначе можетъ быть простымъ съ $\frac{m}{\omega}$, какъ при недѣлимости $\frac{m}{\omega}$ на 2, и отсутствіи общихъ дѣлителей въ $\frac{m}{\omega}$ и z .

Намъ остается доказать, что p долженъ дѣлить $a^\omega + 1$; но это слѣдуетъ изъ сравненія

$$a^\omega + 1 \equiv 0 \pmod{p},$$

которое мы вывели выше.

Изъ этой теоремы, какъ частный случай, выходятъ такіа:

70. ТЕОРЕМА.

Простые нечетные дѣлители числа $a^{2n+1} + 1$ при $2n + 1$ простомъ должны быть вида $2(2n + 1)z + 1$ или дѣлить $a + 1$.

Доказательство. Если p нечетное число, то оно можетъ быть такъ представлено $2N + 1$. Но эта форма при дѣлимости N на $2n + 1$ приводится къ $2(2n + 1)z + 1$. Въ томъ же случаѣ, когда N не дѣлится на простое число $2n + 1$, число N простое съ $2n + 1$, и дѣлимость $a^{2n+1} + 1$ на $p = 2N + 1$, по предыдущей теоремѣ, предполагаетъ дѣлимость $a + 1$ на это, что число и слѣдовало доказать.

71. ТЕОРЕМА.

Всѣ нечетные дѣлители числа $2^{2^n} + 1$ должны быть вида $2 \cdot 2^n + 1$.

Доказательство. По теоремѣ 70-й всѣ нечетные дѣлители $2^{2^n} + 1$ могутъ быть такъ представлены

$$2 \cdot \omega z + 1,$$

гдѣ ω есть дѣлитель 2^n , который въ частномъ $\frac{2^n}{\omega}$ даетъ число нечетное. Но этому условию удовлетворяетъ только $\omega = 2^n$, слѣд. всѣ нечетные дѣлители $2^{2^n} + 1$ должны представляться такъ

$$2 \cdot 2^n z + 1,$$

что и слѣдовало доказать. На основаніи трехъ послѣднихъ теоремъ легко найти дѣлителей числа, имѣющаго видъ $a^m + 1$, или убѣдиться, что оно не имѣетъ дѣлителей.

Для примѣра возьмемъ числа 65537 и 4294967297, изъ которыхъ первое равно $2^{2^4} + 1$; второе равно $2^{2^5} + 1$.

По послѣдней изъ доказанныхъ нами теоремъ дѣлители 65537 должны быть вида $32z + 1$. Дѣлая здѣсь $z = 1, 2, 3, 4, 5, 6, 7, 8$, мы находимъ, что всѣ числа этого вида и меньшія 65537 суть

$$33, 65, 97, 129, 161, 193, 225, 257.$$

Но изъ нихъ только 97 и 193 числа простые, и такъ какъ эти числа не дѣлятъ 65537; то мы заключаемъ, что 65537 есть число простое.

По той же теоремѣ для дѣлителей числа 4294967297 имѣемъ форму $64z + 1$. Дѣлая здѣсь $z = 1, 2, \dots, 1024$, мы найдемъ всѣ числа этого вида и меньшія $\sqrt{4294967297}$. Между этими числами мы находимъ такіа простые

$$193, 257, 449, 577, 641, \dots$$

Дѣля на нихъ 4294967297, мы замѣчаемъ, что это число дѣлится на 641.

Этотъ примѣръ особенно замѣчателенъ тѣмъ, что онъ опро-

вергаетъ мнѣніе Фермата, будто бы всѣ числа вида $2^{2^n} + 1$ суть простые

§ 50. Мы видѣли, какимъ образомъ теорія двучленныхъ сравненій облегчаетъ изслѣдованія состава чиселъ, подходящихъ подъ форму $a^m \pm 1$. Теперь покажемъ, какимъ образомъ для всякаго числа A можетъ быть найдено множество формъ вида $x^2 \pm ay^2$ съ незначительными величинами a , которыя будутъ выражать или данное число A , или кратное его. Во всякомъ случаѣ, будутъ ли эти формы выражать A , или кратное A , дѣлители A будутъ дѣлителями этихъ формъ, и слѣд. видъ ихъ опредѣлится по способамъ показаннымъ въ предыдущей главѣ, или найдется изъ нашихъ таблицъ дѣлителей $x^2 \pm ay^2$, если a не превосходитъ 101.

Какое бы ни было число A , или кратное его kA , можно всегда выразить его формою вида $x^2 \pm ay^2$. Такъ принимая за x какое нибудь число, за y наибольшее число, квадратъ котораго дѣлитъ разность $A - x^2$, и полагая частное $\frac{A - x^2}{y^2}$ равнымъ a , будемъ имѣть

$$\frac{A - x^2}{y^2} = a;$$

откуда получаемъ для A такое выраженіе

$$A = x^2 + ay^2.$$

Подобнымъ образомъ могутъ быть выражены $2A, 3A, \dots$ Всѣ полученныя такимъ образомъ формы будутъ служить для опредѣленія дѣлителей A . Но изъ нихъ наиболѣе выгодны тѣ, въ которыхъ a имѣетъ незначительную величину; ибо, какъ можно было замѣтить въ теоріи дѣлителей квадратичныхъ формъ, чѣмъ меньше a , тѣмъ проще формы дѣлителей $x^2 \mp ay^2$. Поэтому изъ всѣхъ возможныхъ выраженій A , или кратнаго A формами вида $x^2 \pm ay^2$ мы должны выбрать тѣ, въ которыхъ a незначительное число. Для нѣкоторыхъ чиселъ эти формы легко могутъ быть найдены непосредственно. Такъ не трудно замѣтить, что $10001 = 100^2 + 1$, $3.3337 = 100^2 + 11$, и т. п.

Но вообще такія формы могутъ быть найдены на основаніи слѣдующей теоремы:

72. Т Е О Р Е М А .

Если d_0, d_1, d_2, \dots есть рядъ чиселъ, въ которомъ каждый членъ d_{n+1} по двумъ предыдущимъ опредѣляется уравненіемъ

$$\sqrt{A - d_{n+1}d_n} = d_n E \frac{\sqrt{A - d_n d_{n-1}} + \sqrt{A}}{d_n} - \sqrt{A - d_n d_{n-1}}; (*)$$

первые же два суть 1, $A - (E\sqrt{A})^2$; то всякая изъ формъ $x^2 - Dy$, гдѣ D равно

$$(-1)^{\alpha+\beta+\gamma+\dots} d_\alpha \cdot d_\beta \cdot d_\gamma \dots$$

способна выразить A или кратное A .

Доказательство. Прежде чѣмъ приступимъ къ этому доказательству, замѣтимъ, что ряды

$$d_0, d_1, d_2, \dots$$

$$\sqrt{A - d_1 d_0}, \sqrt{A - d_2 d_1}, \sqrt{A - d_3 d_2}, \dots$$

состоятъ изъ чиселъ цѣлыхъ. По положенію $d_0 = 1, d_1 = A - (E\sqrt{A})^2$; отсюда слѣдуетъ, что $d_0, d_1, \sqrt{A - d_1 d_0}$ суть числа цѣлыя. Но если эти количества суть числа цѣлыя; то и всѣ остальные, заключающіяся въ рядахъ

$$d_0, d_1, d_2, \dots$$

$$\sqrt{A - d_1 d_0}, \sqrt{A - d_2 d_1}, \sqrt{A - d_3 d_2}, \dots$$

не могутъ имѣть значеній дробныхъ или ирраціональных; ибо по уравненію

$$\sqrt{A - d_{n+1}d_n} = d_n E \frac{\sqrt{A - d_n d_{n-1}} + \sqrt{A}}{d_n} - \sqrt{A - d_n d_{n-1}},$$

изъ котораго выходитъ также

$$d_{n+1} = d_{n-1} + 2\sqrt{A - d_n d_{n-1}} E \frac{\sqrt{A - d_n d_{n-1}} + \sqrt{A}}{d_n} - d_n \left[E \frac{\sqrt{A - d_n d_{n-1}} + \sqrt{A}}{d_n} \right]^2,$$

(*) Знакомъ E мы означаемъ здѣсь то же, что въ § 26.

количества d_{n+1} , $\sqrt{A - d_n d_{n+1}}$ не могут имѣть значеній дробныхъ или ирраціональныхъ, если d_{n-1} , d_n , $\sqrt{A - d_n d_{n-1}}$ суть числа цѣлыя.

На основаніи этого, зная, что d_0 , d_1 , $\sqrt{A - d_0 d_1}$ числа цѣлыя, мы заключаемъ что d_2 , $\sqrt{A - d_1 d_2}$ имѣютъ значенія цѣлыя; зная, что d_1 , d_2 , $\sqrt{A - d_1 d_2}$ имѣютъ значенія цѣлыя, заключаемъ, что d_3 , $\sqrt{A - d_2 d_3}$ числа цѣлыя, и т. д.

Приступимъ теперь къ доказательству предложенной нами теоремы, и изобразимъ буквами x_0 , x_1 , x_2 , ... x_{n-2} , x_{n-1} значенія

$$\sqrt{A - d_1 d_0}, \sqrt{A - d_2 d_1}, \sqrt{A - d_3 d_2}, \dots, \sqrt{A - d_{n-1} d_{n-2}},$$

$$\sqrt{A - d_n d_{n-1}},$$

которыя, какъ видѣли, всѣ суть числа цѣлыя. Имѣя такимъ образомъ

$$\sqrt{A - d_1 d_0} = x_0,$$

$$\sqrt{A - d_2 d_1} = x_1,$$

$$\sqrt{A - d_3 d_2} = x_2,$$

.....

$$\sqrt{A - d_{n-1} d_{n-2}} = x_{n-2},$$

$$\sqrt{A - d_n d_{n-1}} = x_{n-1},$$

мы изъ этихъ уравненій выводимъ

$$x_0^2 - A = -d_1 d_0,$$

$$x_1^2 - A = -d_2 d_1,$$

$$x_2^2 - A = -d_3 d_2,$$

.....

$$x_{n-2}^2 - A = -d_{n-1} d_{n-2},$$

$$x_{n-1}^2 - A = -d_n d_{n-1},$$

которыя иначе напишутся такъ

$$(x_0 + \sqrt{A})(x_0 - \sqrt{A}) = -d_1 d_0,$$

$$(x_1 + \sqrt{A})(x_1 - \sqrt{A}) = -d_2 d_1,$$

$$(x_2 + \sqrt{A})(x_2 - \sqrt{A}) = -d_3 d_2,$$

.....

.....

$$(x_{n-2} + \sqrt{A})(x_{n-2} - \sqrt{A}) = -d_{n-1} d_{n-2},$$

$$(x_{n-1} + \sqrt{A})(x_{n-1} - \sqrt{A}) = -d_n d_{n-1}.$$

Перемножая всё эти уравнения между собою, находимъ

$$(x_0 + \sqrt{A})(x_1 + \sqrt{A})(x_2 + \sqrt{A}) \dots (x_{n-2} + \sqrt{A})(x_{n-1} + \sqrt{A}) \times \\ (x_0 - \sqrt{A})(x_1 - \sqrt{A})(x_2 - \sqrt{A}) \dots (x_{n-2} - \sqrt{A})(x_{n-1} - \sqrt{A}) = \\ (-1)^n d_0 d_1^2 d_2^2 \dots d_{n-1}^2 d_n.$$

Но перемножая между собою выражения

$x_0 \pm \sqrt{A}, x_1 \pm \sqrt{A}, x_2 \pm \sqrt{A}, \dots, x_{n-2} \pm \sqrt{A}, x_{n-1} \pm \sqrt{A}$, мы находимъ произведение такого вида $X_n \pm Y_n \sqrt{A}$, гдѣ X_n и Y_n числа цѣлыя.

Вслѣдствіе этого предыдущее уравнение приводится къ такому

$$(X_n + Y_n \sqrt{A})(X_n - Y_n \sqrt{A}) = (-1)^n d_0 d_1^2 d_2^2 \dots d_{n-1}^2 d_n.$$

Полагая же здѣсь $d_1 d_2 \dots d_{n-1} = Z_n$, и замѣчая, что $d_0 = 1$, мы находимъ

$$(X_n + Y_n \sqrt{A})(X_n - Y_n \sqrt{A}) = (-1)^n Z_n^2 d_n.$$

Такое уравненіе мы найдемъ для всякаго значенія n . Дѣлая здѣсь $n = \alpha, n = \beta, n = \gamma, \dots$, мы будемъ имѣть

$$(X_\alpha + Y_\alpha \sqrt{A})(X_\alpha - Y_\alpha \sqrt{A}) = (-1)^\alpha Z_\alpha^2 d_\alpha,$$

$$(X_\beta + Y_\beta \sqrt{A})(X_\beta - Y_\beta \sqrt{A}) = (-1)^\beta Z_\beta^2 d_\beta,$$

$$(X_\gamma + Y_\gamma \sqrt{A})(X_\gamma - Y_\gamma \sqrt{A}) = (-1)^\gamma Z_\gamma^2 d_\gamma,$$

.....

и эти уравненія по перемноженіи дадутъ

$$(X_\alpha + Y_\beta \sqrt{A})(X_\beta + Y_\beta \sqrt{A})(X_\gamma + Y_\gamma \sqrt{A}) \dots \times \\ (X_\alpha - Y_\alpha \sqrt{A})(X_\gamma + Y_\gamma \sqrt{A})(X_\gamma - Y_\gamma \sqrt{A}) \dots = \\ (-1)^{\alpha + \beta + \gamma + \dots} Z_\alpha^2 Z_\beta^2 Z_\gamma^2 \dots d_\alpha d_\beta d_\gamma \dots$$

Но перемножая между собою выражения

$$X_\alpha \pm Y_\alpha \sqrt{A}, X_\beta \pm Y_\beta \sqrt{A}, X_\gamma \pm Y_\gamma \sqrt{A}, \dots,$$

мы находимъ произведение такого вида $X \pm Y\sqrt{A}$, гдѣ X, Y числа цѣлыя. Въ слѣдствіе чего предыдущее уравненіе приводится къ такому

$$(X + Y\sqrt{A})(X - Y\sqrt{A}) = (-1)^{\alpha+\beta+\gamma+\dots} Z_\alpha^2 Z_\beta^2 Z_\gamma^2 \dots d_\alpha d_\beta d_\gamma \dots,$$

а это по разскрѣтіи скобокъ даетъ

$$X^2 - Y^2 A = (-1)^{\alpha+\beta+\gamma+\dots} Z_\alpha^2 Z_\beta^2 Z_\gamma^2 \dots d_\alpha d_\beta d_\gamma \dots,$$

$$\text{или } X^2 - (-1)^{\alpha+\beta+\gamma+\dots} d_\alpha d_\beta d_\gamma \dots (Z_\alpha Z_\beta Z_\gamma \dots)^2 = AY^2.$$

Откуда видимъ, что форма

$$x^2 - ay^2$$

при $a = (-1)^{\alpha+\beta+\gamma+\dots} d_\alpha d_\beta d_\gamma \dots$ будетъ выражать число кратное A , если x примемъ равнымъ X , и y равнымъ $Z_\alpha Z_\beta Z_\gamma \dots$, что и слѣдовало доказать.

На основаніи этой теоремы, опредѣливши числа

$$d_0, d_1, d_2, \dots$$

мы найдемъ множество формъ вида $x^2 \pm ay^2$, которыя будутъ способны выразить кратныя A .

Въ этихъ формахъ a опредѣляется произведеніемъ какихъ-либо изъ чиселъ

$$d_0, d_1, d_2, \dots,$$

и между различными сочетаніями этихъ чиселъ мы выберемъ такія, которыхъ бы произведеніе привелось къ точному квадрату съ незначительнымъ множителемъ. Принимая такія произведенія для опредѣленія a въ формѣ $x^2 \pm ay^2$, и выкидывая изъ состава a точные квадраты по § 46, мы получимъ формы съ незначительными коэффициентами, и эти то формы, на основаніи сказаннаго нами, послужатъ для опредѣленія дѣлителей A (*). Если бы мы не нашли такимъ образомъ достаточнаго числа различныхъ формъ; то мы бы стали по предыдущей теоремѣ искать формы, выражающія кратныя $2A, 3A, 4A, \dots$

(*) Въ этихъ формахъ не будетъ заключаться числа d_1, d_2, d_3, \dots , входящія въ составъ a ; но они могутъ дѣлить A , и мы ихъ должны предварительно испытать.

и между ними выбрали бы удобныя для опредѣленія дѣлителей A .

Для примѣра возьмемъ число 8520191. Не останавливаясь на формахъ, которыя могли бы быть открыты непосредственно для выраженія 8520191 или кратнаго 8520191, мы будемъ искать ихъ на основаніи предыдущей теоремы. Для этого мы опредѣлимъ числа

$$d_0, d_1, d_2, d_3, \dots$$

по уравненіямъ

$$d_0 = 1, d_1 = 8520191 - (E\sqrt{8520191})^2,$$

$$\sqrt{8520191 - d_{n+1}d_n} = d_n E \frac{\sqrt{8520191 - d_n d_{n-1}} + \sqrt{8520191}}{d_n}$$

$$\sqrt{8520191 - d_n d_{n-1}}.$$

Изъ этихъ уравненій находимъ

$d_0 = 1,$	$d_4 = 1313,$	$d_8 = 1169,$	$d_{12} = 593,$	$d_{16} = 1210.$
$d_1 = 5467,$	$d_5 = 2630,$	$d_9 = 4523,$	$d_{13} = 2854,$
$d_2 = 370,$	$d_6 = 3185,$	$d_{10} = 242,$	$d_{14} = 2965,$
$d_3 = 4319,$	$d_7 = 203,$	$d_{11} = 1855,$	$d_{15} = 371,$

Разлагая здѣсь числа на простые множители, что не представляетъ большой трудности (*), получаемъ

$d_0 = 1,$	$d_4 = 13 \cdot 101,$	$d_8 = 7 \cdot 187,$	$d_{12} = 593,$
$d_1 = 7 \cdot 11 \cdot 71,$	$d_5 = 2 \cdot 5 \cdot 263,$	$d_9 = 4523,$	$d_{13} = 2 \cdot 1427,$
$d_2 = 2 \cdot 5 \cdot 37,$	$d_6 = 5 \cdot 7^2 \cdot 13,$	$d_{10} = 2 \cdot 11^2,$	$d_{14} = 5 \cdot 593,$
$d_3 = 7 \cdot 617,$	$d_7 = 7 \cdot 29,$	$d_{11} = 5 \cdot 7 \cdot 53,$	$d_{15} = 7 \cdot 53,$
			$d_{16} = 2 \cdot 5 \cdot 11^2.$

Разсматривая составъ чиселъ $d_0, d_1, d_2, \dots, d_{16}$, мы замѣчаемъ, что числа

$d_6, d_{10}, d_{16}, d_{10} d_{16}, d_6 d_{10} d_{16}, d_2 d_{16}, d_4 d_6 d_{10} d_{16},$
по исключеніи изъ состава ихъ точныхъ квадратовъ приводятся къ незначительнымъ числамъ.

Поэтому на основаніи доказанной нами теоремы для опредѣленія дѣлителей разсматриваемаго нами числа 8520191, принимаемъ формы вида $x^2 - ay^2$, гдѣ a имѣетъ такія значенія

(*) При этомъ можно съ пользою пользоваться таблицами Вега, въ которыхъ находимъ для всѣхъ чиселъ меньшихъ 102000 разложеніе на простые множители.

$$a = (-1)^6 d_6 = 5.7^2.13,$$

$$a = (-1)^{10} d_{10} = 2.11^2,$$

$$a = (-1)^{16} d_{16} = 2.5.11^2,$$

$$a = (-1)^{10+16} d_{10} d_{16} = 2^2.5.11^2,$$

$$a = (-1)^{6+10+16} d_6 d_{10} d_{16} = 5^2.7^2.13.2^2.11^2,$$

$$a = (-1)^{2+16} d_2 d_{16} = 2^2.5^2.37.11^2,$$

$$a = (-1)^{4+6+10+16} d_4 d_6 d_{10} d_{16} = 13^2.101.5^2.7^2.2^2.11^4.$$

Исключая въ этихъ величинахъ a всѣ множители, составляющіе точные квадраты, находимъ для a слѣдующія величины
5.13, 2, 2.5, 5, 13, 37, 101.

Откуда видимъ, что дѣлители 8520191, должны имѣть видъ дѣлителей каждой изъ формъ

$$x^2 - 5.13y^2, \quad x^2 - 2y^2, \quad x^2 - 2.5y^2, \quad x^2 - 5y^2, \quad x^2 - 13y^2, \\ x^2 - 13y^2, \quad x^2 - 37y^2, \quad x^2 - 101y^2.$$

На этомъ основаніи мы и будемъ искать дѣлителей 8520191.

Для этого по таблицамъ линейныхъ дѣлителей, мы замѣчаемъ, что дѣлители $x^2 - 5.13y^2$ суть

$$260z + 1, 7, 9, 29, 33, 37, 47, 49, 51, 57, 61, 63, 67, 69, 73, \\ 79, 81, 83, 93, 97, 101, 121, 123, 129, 131, 137, 139, \\ 159, 163, 167, 177, 179, 181, 187, 191, 193, 197, 199, \\ 203, 209, 211, 213, 223, 227, 231, 251, 253, 259.$$

Но изъ нихъ дѣлителями $x^2 - 5y^2$ могутъ быть только тѣ, которые при дѣленіи на 20 даютъ остатки равные 1, 9, 11, 19; ибо для дѣлителей $x^2 - 5y^2$ находимъ

$$20z + 1, 9, 11, 19.$$

Выкидывая изъ предыдущихъ формъ всѣ, которыя не даютъ въ остаткѣ 1, 9, 11, 19, мы находимъ, что дѣлителями $x^2 - 5.13y^2$ и $x^2 - 5y^2$ вмѣстѣ могутъ быть числа вида

$$260z + 1, 9, 29, 49, 51, 61, 69, 79, 81, \\ 101, 121, 129, 131, 139, 159, 179, 181, 191, \\ 199, 209, 211, 231, 251, 259.$$

Но изъ этихъ чиселъ могутъ быть дѣлителями формы $x^2 - 2y^2$ только тѣ, которыя вида $8z + 1$ или $8z + 7$, и слѣд. при дѣленіи на 8 даютъ въ остаткѣ 1 или 7. Чтобы

вывести изъ найденныхъ нами формъ дѣлителей $x^2 - 5 \cdot 13y^2$ и $x^2 - 5y^2$ такія, которыя бы давали одни числа вида $8z + 1$ и $8z + 7$, мы преобразуемъ ихъ такъ, чтобы коэффициентъ при переменномъ z былъ кратнымъ 8. Для этого мы замѣчаемъ, что z будетъ или вида $2u$, или вида $2u + 1$. Внося эти величины въ найденныя нами формы дѣлителей $x^2 - 15y^2$ и $x^2 - 5y^2$, мы ихъ представимъ такъ

520u + 1, 9, 29, 49, 51, 61, 69, 79, 81, 101,
121, 129, 131, 139, 159, 179, 181,
191, 199, 209, 211, 231, 251, 259,
261, 269, 289, 309, 311, 321, 329,
339, 341, 361, 381, 389, 391, 399,
419, 439, 441, 451, 459, 469, 471,
491, 511, 519.

Выкидывая здѣсь тѣ формы, которыя при дѣленіи на 8 даютъ остатки, отличные отъ 1 и 7, находимъ, что общіе дѣлители формъ $x^2 - 5 \cdot 13y^2$, $x^2 - 5y^2$, $x^2 - 2y^2$ должны быть вида

520u + 1, 9, 49, 79, 81, 121, 129, 159, 191, 199,
209, 231, 289, 311, 321, 329, 361,
391, 399, 439, 441, 471, 511, 519.

У насъ остается еще для опредѣленія дѣлителей числа 8520191 четыре формы

$$x^2 - 2 \cdot 5y^2, \quad x^2 - 13y^2, \quad x^2 - 37y^2, \quad x^2 - 101y^2.$$

Изъ нихъ первыя двѣ имѣютъ дѣлителями всѣ числа, дѣлящія $x^2 - 5 \cdot 13y^2$, $x^2 - 5y^2$, $x^2 - 2y^2$, въ чемъ не трудно убѣдиться, замѣтивъ, что дѣлимость $x_1^2 - 5 \cdot 13y_1^2$, $x_2^2 - 5y_2^2$, $x_3^2 - 2y_3^2$ на p предполагаетъ

$$x_1^2 \equiv 5 \cdot 13y_1^2, \quad x_2^2 \equiv 5y_2^2, \quad x_3^2 \equiv 2y_3^2 \pmod{p};$$

откуда слѣдуетъ $x_1^2 x_2^2 \equiv 5^2 \cdot 13y_1^2 y_2^2$, $x_2^2 x_3^2 \equiv 2 \cdot 5y_2^2 y_3^2 \pmod{p}$, и слѣдов. дѣлимость формъ $x^2 - 13y^2$ и $x^2 - 2 \cdot 5y^2$ на p . Что же касается до формъ

$$x^2 - 37y^2, \quad x^2 - 101y^2;$$

то опредѣляя ихъ дѣлителей и выкидывая изъ формъ

520 и + 1, 9, 49, 79, 81, 121, 129, 159, 191, 199,
209, 231, 289, 311, 321, 329, 361, 391,
399, 439, 441, 471, 511, 519.

тѣ, которыя не согласны съ ихъ видомъ, мы ограничили бы еще болѣе числа, между которыми должны искать дѣлителей 8520191. Для этого мы найденныя формы должны преобразовать такъ, чтобы коэффициентъ при переменномъ u былъ кратнымъ 4.37 и 4.101. Послѣ чего дѣленіемъ этихъ формъ на 4.37 и 4.101 мы узнаемъ, которыя изъ нихъ подходятъ подъ формы дѣлителей $x^2 - 37y^2$, $x^2 - 101y^2$. Но при этомъ мы получимъ чрезвычайно много линейныхъ формъ для опредѣленія дѣлителей 8520131. Поэтому, не пользуясь пока формами $x^2 - 37y^2$, $x^2 - 101y^2$ для опредѣленія дѣлителей 8520191, мы остановимся на найденныхъ нами линейныхъ дѣлителяхъ общихъ формамъ $x^2 - 5 \cdot 13y^2$, $x^2 - 5y^2$, $x^2 - 2y^2$, и по нимъ опредѣлимъ всѣ простыя числа меньшія $\sqrt{8520191}$.

Эти числа суть

79	521	719	919	1231	1511	1889	2129	2521	2791.
191	569	751	991	1249	1559	1951	2161	2551	
199	599	809	1031	1361	1609	1999	2239	2591	
311	601	881	1039	1439	1759	2081	2311	2609	
439	641	911	1049	1481	1871	2089	2441	2729	

Между этими-то числами мы должны искать наименьшаго дѣлителя 8520191. Но по значительному количеству ихъ это было бы довольно продолжительно. Для этого мы предварительно исключимъ изъ нихъ тѣ, которыя не могутъ быть дѣлителями квадратичныхъ формъ $x^2 - 37y^2$, $x^2 - 101y^2$. Для этого мы замѣчаемъ изъ таблицъ, что дѣлители $x^2 - 37y^2$ при дѣленіи на 148 должны давать остатки

1, 3, 7, 9, 11, 21, 25, 27, 33,
41, 47, 49, 53, 63, 65, 67, 71,
73, 75, 77, 81, 83, 85, 95, 99,
101, 107, 115, 121, 123, 127,
137, 139, 141, 145, 147.

Но между найденными нами простыми числами этому условию удовлетворяют только только числа

521	759	1249	2081
599	881	1439	2441
601	1039	1481	2591
641	1049	1951	2729
719	1231	1999	2791.

Такимъ же образомъ находимъ, что изъ этихъ чиселъ дѣлителями $x^2 - 101y^2$ могутъ быть только

521, 601, 1231, 1249, 1999, 2441, 2729, 2791.

Пробуя дѣлить на эти числа 8520191, замѣчаемъ, что они его не дѣлятъ; откуда заключаетъ, что 8520191 число простое.

Такимъ образомъ, на основаніи теоріи дѣлителей квадратичныхъ формъ, мы можемъ изслѣдовать составъ всякаго числа, опредѣливши рядъ чиселъ

$$d_0, d_1, d_2, \dots$$

по уравненіямъ: $d_0 = 1, d_1 = A - (E\sqrt{A})^2,$

$$\sqrt{A - d_{n+1}d_n} = d_n E \frac{\sqrt{A - d_n d_{n-1}} + \sqrt{A}}{d_n} - \sqrt{A - d_n d_{n-1}}.$$

ПРИБАВЛЕНІЯ.

I.

О КВАДРАТИЧНЫХЪ ВЫЧЕТАХЪ.

Въ IV-й главѣ мы видѣли, какъ опредѣляется величина символа $\left(\frac{a}{p}\right)$, и черезъ это узнаемъ, имѣетъ ли сравненіе $x^2 \equiv a \pmod{p}$ рѣшеніе или нѣтъ. Но этотъ способъ опредѣленія величины $\left(\frac{a}{p}\right)$ можетъ быть значительно упрощенъ; можно опредѣлить значеніе $\left(\frac{a}{p}\right)$, не разлагая ни a , ни другихъ чиселъ на простые множители. Такое упрощеніе особенно важно при a большомъ; въ этомъ случаѣ разложеніе a на простые множители бываетъ очень трудно, и требуетъ гораздо болѣе времени, чѣмъ самое опредѣленіе $\left(\frac{a}{p}\right)$ по способу, который мы теперь покажемъ.

Слѣдуя Лежандру, мы изображаемъ символомъ $\left(\frac{a}{p}\right)$, при p простымъ, нечетномъ, недѣлящемъ a , единицу съ тѣмъ изъ двухъ знаковъ, съ которыми она удовлетворяетъ сравненію

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

Согласимся же теперь съ Якоби изображать произведеніе такихъ символовъ $\left(\frac{a}{p_1}\right)$, $\left(\frac{a}{p_2}\right)$, $\left(\frac{a}{p_3}\right)$; символомъ $\left(\frac{a}{p_1 p_2 p_3 \dots}\right)$.

Допустивши такое знакоположеніе, мы въ величинѣ символа $\left(\frac{a}{N}\right)$ при N нечетномъ, простомъ съ a , будемъ имѣть произведеніе символовъ $\left(\frac{a}{\alpha}\right), \left(\frac{a}{\beta}\right), \left(\frac{a}{\gamma}\right), \dots$, гдѣ $\alpha, \beta, \gamma, \dots$ суть простые множители, составляющіе N . Въ случаѣ N простаго этотъ символъ будетъ тождественъ символу Лежандра, и имъ опредѣлится возможность или невозможность сравненія $x^2 \equiv a \pmod{N}$.

Докажемъ же теперь, что символъ $\left(\frac{a}{N}\right)$ будетъ удовлетворять всѣмъ тѣмъ уравненіямъ, которыя служили намъ для опредѣленія величины символа $\left(\frac{a}{p}\right)$ при p простомъ.

Не трудно убѣдиться, что $\left(\frac{a' \cdot a'' \cdot \dots}{N}\right)$ равно $\left(\frac{a'}{N}\right) \left(\frac{a''}{N}\right) \dots$.
Въ самомъ дѣлѣ, если

$$N = \alpha \beta \gamma \dots,$$

гдѣ $\alpha, \beta, \gamma, \dots$ простые числа; то

$$\left(\frac{a' a'' \dots}{\alpha}\right) = \left(\frac{a'}{\alpha}\right) \left(\frac{a''}{\alpha}\right) \dots,$$

$$\left(\frac{a' a'' \dots}{\beta}\right) = \left(\frac{a'}{\beta}\right) \left(\frac{a''}{\beta}\right) \dots,$$

$$\left(\frac{a' a'' \dots}{\gamma}\right) = \left(\frac{a'}{\gamma}\right) \left(\frac{a''}{\gamma}\right) \dots,$$

.....

Перемножая эти уравненія, находимъ

$$\left(\frac{a' a'' \dots}{\alpha}\right) \left(\frac{a' a'' \dots}{\beta}\right) \left(\frac{a' a'' \dots}{\gamma}\right) \dots = \left(\frac{a'}{\alpha}\right) \left(\frac{a'}{\beta}\right) \left(\frac{a'}{\gamma}\right) \dots \left(\frac{a''}{\alpha}\right) \left(\frac{a''}{\beta}\right) \left(\frac{a''}{\gamma}\right) \dots,$$

что по принятому нами знакоположенію представится такъ

$$\left(\frac{a' a'' \dots}{\alpha \beta \gamma \dots}\right) = \left(\frac{a'}{\alpha \beta \gamma \dots}\right) \left(\frac{a''}{\alpha \beta \gamma \dots}\right) \dots$$

Замѣчая же, что здѣсь $\alpha \beta \gamma \dots$ равно N , найдемъ

$$\left(\frac{a' a'' \dots}{N}\right) = \left(\frac{a'}{N}\right) \left(\frac{a''}{N}\right) \dots,$$

что и хотѣли доказать. На основаніи этого мы заключаемъ, что

$$\left(\frac{a'^2}{N}\right) = 1,$$

и слѣд.

$$\left(\frac{a'^2 a''}{N}\right) = \left(\frac{a''}{N}\right).$$

На этомъ основаніи мы можемъ въ символѣ $\left(\frac{a}{N}\right)$ выкидывать изъ состава a точные квадраты.

Также не трудно доказать, что при a сравнимомъ съ a' по модулю N значеніе $\left(\frac{a}{N}\right)$ равно $\left(\frac{a'}{N}\right)$. Въ самомъ дѣлѣ, если a и a' сравнимы по модулю N и $N = \alpha\beta\gamma\dots$, то a и a' сравнимы по модулямъ $\alpha, \beta, \gamma, \dots$, и слѣд.

$$\left(\frac{a}{\alpha}\right) = \left(\frac{a'}{\alpha}\right), \left(\frac{a}{\beta}\right) = \left(\frac{a'}{\beta}\right), \left(\frac{a}{\gamma}\right) = \left(\frac{a'}{\gamma}\right).$$

Перемножая эти уравненія между собою, найдемъ

$$\left(\frac{a}{\alpha}\right) \left(\frac{a}{\beta}\right) \left(\frac{a}{\gamma}\right) \dots = \left(\frac{a'}{\alpha}\right) \left(\frac{a'}{\beta}\right) \left(\frac{a'}{\gamma}\right) \dots, \text{ или } \left(\frac{a}{\alpha\beta\gamma\dots}\right) = \left(\frac{a'}{\alpha\beta\gamma\dots}\right).$$

Но $\alpha\beta\gamma\dots = N$, слѣдовательно

$$\left(\frac{a}{N}\right) = \left(\frac{a'}{N}\right).$$

На основаніи этого мы можемъ въ символѣ $\frac{a}{N}$ число a замѣнить остаткомъ отъ дѣленія a на N , или абсолютно малымъ вычетомъ a по модулю N .

Значенія $\left(\frac{a}{N}\right)$ при $a = 1$ и $a = -1$ опредѣляются также какъ значенія $\left(\frac{a}{p}\right)$ при p простомъ уравненіями

$$\left(\frac{1}{N}\right) = 1, \left(\frac{-1}{N}\right) = (-1)^{\frac{N-1}{2}}.$$

Въ самомъ дѣлѣ, если $N = \alpha\beta\gamma\dots$, гдѣ $\alpha, \beta, \gamma, \dots$ простые числа; то

$$\left(\frac{1}{N}\right) = \left(\frac{1}{\alpha}\right) \left(\frac{1}{\beta}\right) \left(\frac{1}{\gamma}\right) \dots = 1,$$

$$\left(\frac{-1}{N}\right) = \left(\frac{-1}{\alpha}\right) \left(\frac{-1}{\beta}\right) \left(\frac{-1}{\gamma}\right) \dots = (-1)^{\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \dots}.$$

Но $\frac{N-1}{2} = \frac{\alpha\beta\gamma\dots-1}{2}$, что можетъ быть представлено такъ

*

$$\frac{(2^{\frac{\alpha-1}{2}} + 1)(2^{\frac{\beta-1}{2}} + 1)(2^{\frac{\gamma-1}{2}} + 1) \dots - 1}{2},$$

а это за исключеніем членовъ, имѣющихъ множителемъ 2, приводится къ

$$\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \dots$$

Въ слѣдствіе этого предыдущее выраженіе $\left(\frac{-1}{N}\right)$ приводится къ такому

$$\left(\frac{-1}{N}\right) = (-1)^{\frac{N-1}{2}}.$$

На основаніи этого и уравненія $\left(\frac{aa'}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{a'}{N}\right)$ значеніе $\left(\frac{-a}{N}\right)$ выразится такъ

$$\left(\frac{-a}{N}\right) = \left(\frac{a}{N}\right) (-1)^{\frac{N-1}{2}}.$$

Переходимъ теперь къ уравненію, связывающему значенія $\left(\frac{a}{N}\right)$, $\left(\frac{N}{a}\right)$. Это уравненіе подобно тому, которое мы нашли для символа $\left(\frac{a}{p}\right)$ при a , p простыхъ, и назвали законъ взаимности двухъ простыхъ чиселъ. Пусть будетъ $N = \alpha \beta \gamma \dots$, $a = \alpha' \beta' \gamma' \dots$, гдѣ α' , β' , γ' , подобно α , β , γ , простые числа. По закону взаимности простыхъ чиселъ находимъ

$$\left(\frac{\alpha'}{\alpha}\right) = \left(\frac{\alpha}{\alpha'}\right) (-1)^{\frac{\alpha-1}{2} \cdot \frac{\alpha'-1}{2}}, \quad \left(\frac{\alpha'}{\beta}\right) = \left(\frac{\beta}{\alpha'}\right) (-1)^{\frac{\beta-1}{2} \cdot \frac{\alpha'-1}{2}},$$

$$\left(\frac{\alpha'}{\gamma}\right) = \left(\frac{\gamma}{\alpha'}\right) (-1)^{\frac{\gamma-1}{2} \cdot \frac{\alpha'-1}{2}} \dots,$$

Перемножая же эти уравненія между собою, получаемъ

$$\left(\frac{-1}{N}\right) \left(\frac{\alpha'}{\beta}\right) \left(\frac{\alpha'}{\gamma}\right) \dots =$$

$$\left(\frac{\alpha}{\alpha'}\right) \left(\frac{\beta}{\alpha'}\right) \left(\frac{\gamma}{\alpha'}\right) \dots (-1)^{\frac{\alpha'-1}{2} \left(\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \dots\right)},$$

или

$$\left(\frac{\alpha'}{\alpha\beta\gamma\dots}\right) = \left(\frac{\alpha\beta\gamma\dots}{\alpha'}\right) (-1)^{\frac{\alpha'-1}{2} \left(\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \dots\right)}.$$

Но произведение $\alpha\beta\gamma\dots$ равно N ; значеніе же $\frac{\alpha-1}{2} + \frac{\beta-1}{2} + \frac{\gamma-1}{2} + \dots$, какъ замѣтили, разнится съ $\frac{N-1}{2}$ числомъ чегнымъ; вслѣдствіе этого предыдущее уравненіе приводится къ такому

$$\left(\frac{\alpha'}{N}\right) = \left(\frac{N}{\alpha'}\right) (-1)^{\frac{\alpha'-1}{2} \frac{N-1}{2}}.$$

Подобнымъ образомъ находимъ

$$\left(\frac{\beta'}{N}\right) = \left(\frac{N}{\beta'}\right) (-1)^{\frac{\beta'-1}{2} \frac{N-1}{2}},$$

$$\left(\frac{\gamma'}{N}\right) = \left(\frac{N}{\gamma'}\right) (-1)^{\frac{\gamma'-1}{2} \frac{N-1}{2}},$$

.....

Перемножая всѣ эти уравненія между собою, получаемъ

$$\left(\frac{\alpha'}{N}\right) \left(\frac{\beta'}{N}\right) \left(\frac{\gamma'}{N}\right) \dots = \left(\frac{N}{\alpha'}\right) \left(\frac{N}{\beta'}\right) \left(\frac{N}{\gamma'}\right) \dots (-1)^{\frac{N-1}{2} \left(\frac{\alpha'-1}{2} + \frac{\beta'-1}{2} + \frac{\gamma'-1}{2} + \dots\right)},$$

что подобно предыдущему приводится къ

$$\left(\frac{a}{N}\right) = \left(\frac{N}{a}\right) (-1)^{\frac{N-1}{2} \frac{a-1}{2}};$$

пбо $\alpha' \beta' \gamma' \dots = a$.

Намъ остается теперь показать уравненіе, опредѣляющее значеніе $\left(\frac{a}{N}\right)$ при $a=2$. Это уравненіе, на основаніи выведенныхъ нами, можетъ быть опредѣлено очень просто независимо отъ уравненія, выражающаго величину $\left(\frac{2}{p}\right)$ при p простымъ.

Для этого мы замѣчаемъ, что уравненіе

$$\left(\frac{a}{N}\right) = \left(\frac{N}{a}\right) (-1)^{\frac{N-1}{2} \frac{a-1}{2}}$$

при $a=2n-1$, $N=2n+1$ даетъ

$$\binom{2n-1}{2n+1} = \binom{2n+1}{2n-1} (-1)^{n(n-1)};$$

откуда слѣдуетъ

$$\binom{2n-1}{2n+1} = \binom{2n+1}{2n-1}.$$

Но по доказанному нами

$$\binom{2n-1}{2n+1} = \binom{2n-1-2n-1}{2n+1} = \binom{-2}{2n+1} = \binom{2}{2n+1} (-1)^n,$$

$$\binom{2n+1}{2n-1} = \binom{2n+1-2n+1}{2n-1} = \binom{2}{2n-1}.$$

Въ слѣдствіе этого предыдущее уравненіе даетъ

$$\binom{2}{2n+1} : \binom{2}{2n-1} = (-1)^n.$$

Дѣлая здѣсь $n = 2, 3, \dots, \frac{N-1}{2}$ и перемножая уравненія при этомъ получаемыя, находимъ

$$\binom{2}{N} = \binom{2}{3} (-1)^{2+3+\dots+\frac{N-1}{2}}.$$

Но $\binom{2}{3}$ равно -1 ; вслѣдствіе этого предыдущее уравненіе даетъ

$$\binom{2}{N} = (-1)^{1+2+3+\dots+\frac{N-1}{2}},$$

что приводится къ такому уравненію

$$\binom{2}{N} = (-1)^{\frac{N^2-1}{8}}.$$

На основаніи выведенныхъ нами уравненій, мы можемъ съ выгодою ввести символъ $\binom{a}{N}$, съ N составномъ, для опредѣленія значеній $\binom{a}{p}$ при p простомъ. Для этого мы будемъ поступать при опредѣленіи $\binom{a}{p}$ такимъ образомъ:

Если a больше p ; то символъ $\binom{a}{p}$ замѣняемъ символомъ $\binom{r}{p}$, гдѣ r остатокъ отъ дѣленія a на p (вмѣсто остатка отъ дѣленія a на p мы можемъ взять за r абсолютно малый вы-

четь a по модулю p); если r число четное; то разлагаемъ его на произведение степени 2 и числа нечетнаго; чрезъ это значеніе $\left(\frac{r}{p}\right)$ представится произведеніемъ символовъ $\left(\frac{2}{p}\right)$ и $\left(\frac{r'}{p}\right)$.

Символы $\left(\frac{2}{p}\right)$ будучи въ четномъ числѣ дадутъ произведеніе равное 1; въ противномъ случаѣ мы его найдемъ по уравненію

$\left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}$. Обращаемся къ символу $\left(\frac{r'}{p}\right)$, гдѣ $r' < p$ и r' число нечетное. По выведенному нами уравненію

$$\left(\frac{a}{N}\right) = \left(\frac{N}{a}\right) (-1)^{\frac{N-1}{2} \cdot \frac{a-1}{2}}$$

найдемъ

$$\left(\frac{r'}{p}\right) = \left(\frac{p}{r'}\right) (-1)^{\frac{r'-1}{2} \cdot \frac{p-1}{2}}.$$

Потомъ поступаемъ съ $\left(\frac{p}{r'}\right)$, какъ поступали съ $\left(\frac{a}{p}\right)$, и уменьшая такимъ образомъ послѣдовательно числа, входящія въ этотъ символъ, дойдемъ до символовъ, которыхъ значенія найдутся на основаніи уравненій

$$\left(\frac{1}{N}\right) = 1, \left(\frac{-1}{N}\right) = (-1)^{\frac{N-1}{2}}, \left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}.$$

При этомъ мы будемъ выкидывать въ символѣ $\left(\frac{a}{N}\right)$ множителей a и N , составляющихъ точные квадраты, когда такіе множители легко обнаруживаются.

Для примѣра возьмемъ символъ

$$\left(\frac{884257967}{2147483247}\right).$$

Здѣсь верхнее число меньше нижняго и притомъ нечетное; поэтому на основаніи уравненія

$$\left(\frac{a}{N}\right) = \left(\frac{N}{a}\right) (-1)^{\frac{N-1}{2} \cdot \frac{a-1}{2}}$$

выводимъ

$$\left(\frac{884257967}{2147483647}\right) = - \left(\frac{2147483647}{884257967}\right).$$

Потомъ дѣля 2147483647 на 884257967 и находя въ остаткѣ 378967713, заключаемъ, что

$$\left(\frac{2147483647}{884257967}\right) = \left(\frac{378967713}{884257967}\right).$$

Но опять на основаніи того же уравненія

$$\left(\frac{a}{N}\right) = \left(\frac{N}{a}\right) (-1)^{\frac{N-1}{2} \frac{a-1}{2}}$$

находимъ

$$\left(\frac{378967713}{884257967}\right) = \left(\frac{884257967}{378967713}\right).$$

А такъ какъ остатокъ отъ дѣленія 884257967 на 378967713 есть 126322541; то

$$\left(\frac{884257967}{378967713}\right) = \left(\frac{126322541}{378967713}\right).$$

Продолжая такимъ образомъ, выводимъ

$$\left(\frac{126322541}{378967713}\right) = \left(\frac{378967713}{126322541}\right) = \left(\frac{90}{126322541}\right);$$

$$\left(\frac{90}{126322541}\right) = \left(\frac{3}{126322541}\right)^2 \left(\frac{10}{126322541}\right) = \left(\frac{10}{126322541}\right);$$

$$\left(\frac{10}{126322541}\right) = \left(\frac{2}{126322541}\right) \left(\frac{5}{126322541}\right).$$

Но величина $\left(\frac{2}{126322541}\right)$ по уравненію $\left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}$ есть 1; слѣд.

$$\left(\frac{10}{126322541}\right) = \left(\frac{5}{126322541}\right) = \left(\frac{126322541}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Итакъ величина $\left(\frac{884257967}{2147483647}\right)$ есть -1 .

Если бы мы стали опредѣлять значеніе этого символа по способу Лежандра, изложенному намъ въ IV главѣ, мы должны бы были, приступая къ этому опредѣленію, разложить число

884257967 на простые множители, что представляет большія трудности.

Принятое нами знакоположеніе для означенія произведенія символовъ $\left(\frac{a}{p_1}\right), \left(\frac{a}{p_2}\right), \left(\frac{a}{p_3}\right), \dots$ и въ слѣдствіе того данное нами значеніе символу $\left(\frac{a}{N}\right)$ при N составномъ, можетъ быть также съ пользою употреблено въ теоріи дѣлителей квадратичной формы $x^2 \pm ay^2$. Такъ если форма $x^2 - iay^2$, гдѣ $i = \pm 1$ имѣеть дѣлителемъ число N , и N есть произведеніе простыхъ чиселъ $\alpha\beta\gamma\dots$; то $\left(\frac{ia}{\alpha}\right) = 1, \left(\frac{ia}{\beta}\right) = 1, \left(\frac{ia}{\gamma}\right) = 1, \dots$ откуда слѣдуетъ, что $\left(\frac{ia}{\alpha}\right)\left(\frac{ia}{\beta}\right)\left(\frac{ia}{\gamma}\right)\dots = 1$, и слѣд. по нашему знакоположенію

$$\left(\frac{ia}{N}\right) = 1.$$

Откуда выходитъ

$$\left(\frac{i}{N}\right)\left(\frac{a}{N}\right) = 1.$$

Умножая это уравненіе на $\left(\frac{i}{N}\right)$ и замѣчая что $\left(\frac{i}{N}\right)^2 = 1$, находимъ

$$\left(\frac{a}{N}\right) = \left(\frac{i}{N}\right).$$

Предполагая же a числомъ нечетнымъ, по доказанному нами имѣемъ

$$\left(\frac{N}{a}\right) = \left(\frac{a}{N}\right) (-1)^{\frac{a-1}{2} \cdot \frac{N-1}{2}}.$$

Это уравненіе вмѣстѣ съ предыдущимъ даетъ

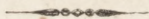
$$\left(\frac{N}{a}\right) = \left(\frac{i}{N}\right) (-1)^{\frac{a-1}{2} \cdot \frac{N-1}{2}}.$$

Отсюда для $i = 1, a = 4n + 1$ выводимъ $\left(\frac{N}{a}\right) = 1$; для $i = 1,$

$a = 4n + 3$ выводимъ $\left(\frac{N}{a}\right) = (-1)^{\frac{N-1}{2}}$; для $i = -1,$

$a = 4n + 1$ выводимъ $\left(\frac{N}{a}\right) = (-1)^{\frac{N-1}{2}}$; для $i = -1$, $a = 4n + 3$ выводимъ $\left(\frac{N}{a}\right) = 1$.

Вотъ уравненія, которымъ должны удовлетворять дѣлители формы $x^2 \pm ay^2$; въ нихъ, какъ частный случай, заключаются уравненія, которыя въ VII-й главѣ мы нашли для опредѣленія дѣлителей $x^2 \pm ay^2$ при a простомъ нечетномъ.



II.

ОБЪ ОПРЕДѢЛЕНИИ ПЕРВООБРАЗНЫХЪ КОРНЕЙ.

Въ VI-й главѣ мы показали два способа опредѣлять первообразные корни простыхъ чиселъ. Оба эти способа для чиселъ большихъ приводятся къ огромнымъ выкладкамъ. Теперь мы докажемъ нѣсколько теоремъ, на основаніи которыхъ можно для многихъ чиселъ по виду ихъ узнать ихъ первообразный корень.

ТЕОРЕМА.

Первообразный корень числа $2^{2n} + 1$ есть 3.

Доказательство. Если $p = 2^{2n} + 1$; то въ составъ $p - 1$ входитъ только простое число 2; а потому (см. 48 теорему) число a будетъ первообразный корень $2^{2n} + 1$, если сравненіе $x^2 \equiv a \pmod{2^{2n} + 1}$ не имѣетъ рѣшенія. Докажемъ же теперь, что это сравненіе не имѣетъ рѣшенія при $a = 3$. Для этого мы замѣчаемъ, что $\left(\frac{3}{2^{2n} + 1}\right)$ по закону взаимности чиселъ, равно $\left(\frac{2^{2n} + 1}{3}\right)$, а это равно $\left(\frac{-1}{3}\right)$; пбо возводя члены сравненія $4 \equiv 1 \pmod{3}$ въ степень n находимъ $4^n \equiv 1 \pmod{3}$; откуда ясно, что -1 по модулю 3 сравнимо съ $4^n + 1$, или $2^{2n} + 1$. Но $\left(\frac{-1}{3}\right) = -1$. Слѣд. $\left(\frac{3}{2^{2n} + 1}\right) = -1$; а потому сравненіе

$x^2 \equiv 3 \pmod{2^{2n} + 1}$ не имѣеть рѣшенія, и 3 есть первообразный корень числа $2^{2n} + 1$.

На основаніи этой теоремы мы заключаемъ, что 3 есть первообразный корень 5, 17, 257, 65537.

Т Е О Р Е М А.

Первообразный корень числа $2(4n + 1) + 1$ при $4n + 1$ простымъ есть 2, а числа $2(4n + 1) + 1$ при $4n + 3$ простымъ есть $2(4n + 3) - 1$.

Доказательство. Если $p = 2(4n + 1) + 1$ и $4n + 1$ число простое, большее 1; то въ составъ $p - 1$ входятъ два простыхъ числа: 2, $4n + 1$; поэтому (см. 48 теор.) число a будетъ первообразный корень числа $2(4n + 1) + 1$, если сравненія

$$x^2 \equiv a, \quad x^{4n+1} \equiv a \pmod{2(4n + 1) + 1}$$

не имѣють рѣшенія. Докажемъ же теперь, что эти сравненія не имѣють рѣшенія при $a = 2$. Невозможность перваго очевидна; оно приводится къ

$$x^2 \equiv 2 \pmod{8n + 3}$$

а по 32-й теоремѣ $\left(\frac{2}{8n+3}\right)$ есть -1 .

Что-же касается до втораго, оно будетъ

$$x^{4n+1} \equiv 2 \pmod{8n + 3};$$

откуда, возводя обѣ части сравненія въ квадратъ, находимъ

$$x^{8n+2} \equiv 4 \pmod{8n + 3}.$$

Этому сравненію не удовлетворяють числа кратныя $8n + 3$, а при x недѣлящимся на $8n + 3$ по теоремѣ Фермата будетъ

$$x^{8n+2} \equiv 1 \pmod{8n + 3}$$

Въ слѣдствіе чего предыдущее сравненіе приводится къ такому

$$1 \equiv 4 \pmod{8n + 3},$$

или

$$3 \equiv 0 \pmod{8n + 3}.$$

Это сравненіе могло бы имѣть мѣсто только при $n = 0$,

по случай $n = 0$, и слѣд. $4n + 1 = 1$ мы исключаемъ. Итакъ оба сравненія

$$x^2 \equiv a, \quad x^{4n+1} \equiv a \pmod{2(4n+1)+1}$$

при $a = 2$, $n > 0$ не имѣютъ рѣшенія, и слѣд. первообразный корень $2(4n+1)+1$ въ сдѣланныхъ нами предположеніяхъ есть 2.

Переходимъ теперь къ $p = 2(4n+3)+1$. Въ этомъ случаѣ $p - 1$ будетъ заключать простыя числа 2 и $4n+3$, и a будетъ первообразный корень $2(4n+3)+1$, если сравненія

$$x^2 \equiv a, \quad x^{4n+3} \equiv a \pmod{2(4n+3)+1}$$

не имѣютъ рѣшенія. Докажемъ же, что это случается для $a = 2(3n+3) - 1$. Первое сравненіе приводится къ

$$x^2 \equiv 8n+5 \pmod{8n+7},$$

и оно не имѣетъ рѣшеній; ибо

$$\left(\frac{8n+5}{8n+7}\right) = \left(\frac{8n+5-8n-7}{8n+7}\right) = \left(\frac{-2}{8n+7}\right) = -1.$$

Второе будетъ

$$x^{4n+1} \equiv 8n+5 \pmod{8n+7},$$

или

$$x^{4n+3} \equiv -2 \pmod{8n+7}.$$

Возводя обѣ части этого сравненія въ квадратъ и замѣчая, что по теоремѣ Фермата $x^{8n+6} \equiv 1 \pmod{8n+7}$, находимъ

$$1 \equiv 4 \pmod{8n+7}$$

что невозможно. Итакъ оба сравненія

$$x^2 \equiv a, \quad x^{4n+3} \equiv a \pmod{2(4n+3)+1}$$

при $a = 2(4n+3) - 1$ не имѣютъ рѣшенія, и слѣд. $2(4n+3) - 1$ есть первообразный корень числа $2(4n+3)+1$.

На основаніи этой теоремы мы заключаемъ, что 2 есть первообразный корень 11, 59, 83, 107, 123, а 7 имѣетъ первообразнымъ корнемъ 5; 23 имѣетъ первообразнымъ корнемъ 21; 47 имѣетъ первообразнымъ корнемъ 45 и т. д.

Т Е О Р Е М А.

Первообразный корень $4N+1$, при N простомъ и больше 2, есть 2.

Доказательство. Если $p = 4N + 1$, и N простое, большее 2; то $p - 1$ заключает два простых числа: 2 и N ; поэтому a будет первообразным корнем $4N + 1$, если сравнения

$$x^2 \equiv a, x^N \equiv a \pmod{4N + 1}$$

не имѣют рѣшенія. Докажем же, что это случается при $a = 2$. При $a = 2$ первое сравненіе будетъ

$$x^2 \equiv 2 \pmod{4N + 1}.$$

Но N нечетное число; слѣд. вида $2n + 1$, а потому $4N + 1 = 8n + 5$, въ этомъ же случаѣ по 32-й теоремѣ

$$\left(\frac{2}{4N + 1}\right) = -1,$$

и слѣд. сравненіе

$$x^2 \equiv 2 \pmod{4N + 1}$$

не имѣетъ рѣшенія. Что же касается до втораго, оно приводится къ

$$x^N \equiv 2 \pmod{4N + 1}.$$

Возведя обѣ части этого сравненія въ четвертую степень и замѣтивъ, что по теоремѣ Фермата $x^{4N} \equiv 1 \pmod{4N + 1}$, находимъ

$$1 \equiv 16 \pmod{4N + 1}.$$

или

$$3 \cdot 5 \equiv 0 \pmod{4N + 1}.$$

Но это сравненіе невозможно; ибо оно предполагаетъ 3 или 5 дѣлящимся на простое число $4N + 1$, гдѣ $N > 2$. Слѣд. оба сравненія

$$x^2 \equiv a, x^N \equiv a \pmod{4N + 1}$$

при $a = 2$ не имѣютъ рѣшенія; а потому 2 есть первообразный корень числа $4N + 1$.

Такъ числа 13, 29, 53, 149, 173, 269, 293, 317,..... будутъ имѣть первообразнымъ корнемъ 2.

ТЕОРЕМА.

Число $4 \cdot 2^m N + 1$, при N простомъ превосходящемъ $\frac{9^{2^m}}{4 \cdot 2^m}$, $m > 0$, будетъ имѣть первообразнымъ корнемъ 3.

Доказательство. Если $p = 4 \cdot 2^m \cdot N + 1$ и N простое; то $p - 1$ заключаетъ только два простыхъ числа: 2 и N . Въ этомъ случаѣ a будетъ первообразнымъ корнемъ числа p , если сравненія

$$x^2 \equiv a, \quad x^N \equiv a \pmod{4 \cdot 2^m N + 1}$$

не имѣютъ рѣшенія. Посмотримъ же могутъ ли они имѣть рѣшеніе при $a = 3$, когда N , по положенію, число простое, болѣе $\frac{9^{2^m}}{4 \cdot 2^m}$ и слѣд. болѣе 3 и на 3 не дѣлится. Въ этомъ случаѣ N будетъ или вида $3n + 1$ или $3n - 1$. Слѣд. будетъ

$$N \equiv \pm 1 \pmod{3}.$$

Но изъ сравненія $2 \equiv -1 \pmod{3}$, возводя его въ степень $m + 2$, выводимъ

$$2^{m+2} \equiv \pm 1 \pmod{3}.$$

Откуда слѣдуетъ, что

$$2^{m+2} N \equiv \pm 1 \pmod{3}$$

а потому $4 \cdot 2^m N + 1$ будетъ сравнимо по модулю 3 или съ 0, или съ 2. Первое не можетъ имѣть мѣста; ибо оно предполагаетъ дѣлимость простаго числа $4 \cdot 2^m N + 1$ на 3; во второмъ же случаѣ $\left(\frac{4 \cdot 2^m N + 1}{3}\right)$ равно $\left(\frac{2}{3}\right) = -1$. Но по закону взаимности двухъ простыхъ чиселъ имѣемъ

$$\left(\frac{4 \cdot 2^m N + 1}{3}\right) = \left(\frac{3}{4 \cdot 2^m N + 1}\right). \text{ Слѣд. } \left(\frac{3}{4 \cdot 2^m N + 1}\right) = -1,$$

что обнаруживаетъ невозможность сравненія

$$x^2 \equiv 3 \pmod{4 \cdot 2^m N + 1}.$$

Намъ остается доказать, что сравненіе

$$x^N \equiv 3 \pmod{4 \cdot 2^m N + 1}$$

въ сдѣланныхъ нами предположеніяхъ не имѣетъ рѣшенія. Для этого мы возводимъ обѣ части его въ степень $4 \cdot 2^m$ и замѣчая, что по теоремѣ Фермата $x^{4 \cdot 2^m N} \equiv 1 \pmod{4 \cdot 2^m N + 1}$, получаемъ

$$1 \equiv 3^{4 \cdot 2^m} \pmod{4 \cdot 2^m N + 1};$$

откуда слѣдуетъ

$$(3^{2 \cdot 2^m} + 1)(3^{2 \cdot 2^m} - 1) \equiv 0 \pmod{4 \cdot 2^m N + 1},$$

что предполагаетъ дѣлимость одного изъ чиселъ $3^{2 \cdot 2^m} + 1$, $3^{2 \cdot 2^m} - 1$ на $4 \cdot 2^m N + 1$, а это невозможно; ибо N по положенію болѣе $\frac{9^{2^m}}{4 \cdot 2^m}$, и слѣд. $4 \cdot 2^m N + 1$ превосходитъ $9^{2^m} + 1$, или $3^{2 \cdot 2^m} + 1$.

Итакъ въ сдѣланныхъ нами предположеніяхъ оба сравненія

$$x^2 \equiv a, \quad x^N \equiv a \pmod{4 \cdot 2^m N + 1}$$

при $a = 3$ не имѣютъ рѣшенія; слѣд. число $4 \cdot 2^m N + 1$ имѣетъ первообразнымъ корнемъ 3.

Такъ числа 89, 173, 233, 317, 569, 809, 857 вида $8N + 1$ и 5009 вида $16N + 1$ имѣютъ первообразнымъ корнемъ 3.



III.

ОБЪ ОПРЕДѢЛЕНІИ ЧИСЛА ПРОСТЫХЪ ЧИСЕЛЪ, НЕ ПРЕВОСХОДЯЩИХЪ ДАННОЙ ВЕЛИЧИНЫ.

Мы видѣли (§ 2), какъ могутъ быть опредѣлены всѣ простыя числа отъ 1 до даннаго числа. Такимъ образомъ можно опредѣлить, сколько простыхъ чиселъ меньшихъ даннаго предѣла. Но такое опредѣленіе числа простыхъ чиселъ, меньшихъ даннаго предѣла, представляетъ большія трудности, когда за предѣлъ принимаемъ большое число. Мы займемся теперь опредѣленіемъ этого числа по приближенію, и покажемъ на основаніи этого рѣшеніе нѣкоторыхъ вопросовъ.

Во второмъ томѣ Теоріи чиселъ Лежандръ предлагаетъ формулу для приближеннаго опредѣленія числа простыхъ чиселъ, меньшихъ даннаго числа. Свою формулу Лежандръ повѣряетъ таблицею простыхъ чиселъ отъ 10000 до 1000000, и потому прилагаетъ ее къ рѣшенію нѣкоторыхъ вопросовъ Теоріи чиселъ. Не смотря на видимое согласіе формулы Лежандра съ таблицею простыхъ чиселъ, мы не можемъ не изъявить сомнѣнія на счетъ строгости ея, и вслѣдствіе того не можемъ признать вѣрными выводы, на ней основанные. Къ такому заключенію приводитъ насъ одна теорема относительно свойствъ функціи, опредѣляющей число простыхъ чиселъ, меньшихъ даннаго числа, теорема, изъ которой могутъ быть выведены многія любопытныя предложенія.

Мы займемся теперь изложением этой теоремы, а потом покажем некоторыя изъ ея приложений.

Теорема, которая будетъ предметомъ нашихъ изслѣдованій, заключается въ слѣдующемъ:

1. ТЕОРЕМА.

Если $\varphi(x)$ означаетъ число простыхъ чиселъ меньшихъ x , и какое либо число цѣлое, ρ количество > 0 ; то въ суммѣ

$$\sum_{x=2}^{x=\infty} \left[\varphi(x+1) - \varphi(x) - \frac{1}{\log x} \right] \frac{\log^n x}{x^{1+\rho}}$$

мы будемъ имѣть такую функцію, которая съ приближеніемъ ρ къ 0, приближается къ конечному предѣлу.

Доказательство. Мы докажемъ сначала, что такое свойство принадлежать функціямъ, получаемымъ черезъ дифференцирование нѣсколько разъ выраженій

$$\sum \frac{1}{m^{1+\rho}} - \frac{1}{\rho}, \quad \log \rho - \sum \log \left(1 - \frac{1}{\mu^{1+\rho}} \right),$$

$$\sum \log \left(1 - \frac{1}{\mu^{1+\rho}} \right) + \sum \frac{1}{\mu^{1+\rho}}$$

по ρ , предполагая здѣсь и вездѣ вполнѣдствіи суммирование по m разпространеннымъ на всѣ числа отъ $m=2$ до $m=\infty$, суммирование же по μ разпространеннымъ на однѣ простыя числа отъ $\mu=2$ до $\mu=\infty$.

Начнемъ съ перваго. Не трудно убѣдиться, что

$$\int_0^{\infty} \frac{e^{-x}}{e^x - 1} x^{\rho} dx = \sum \frac{1}{m^{1+\rho}} \cdot \int_0^{\infty} e^{-x} x^{\rho} dx,$$

$$\int_0^{\infty} e^{-x} x^{-1+\rho} dx = \frac{1}{\rho} \int_0^{\infty} e^{-x} x^{\rho} dx$$

а потому

$$\sum \frac{1}{m^{1+\rho}} - \frac{1}{\rho} = \frac{\int_0^{\infty} \left(\frac{1}{e^x - 1} - \frac{1}{x} \right) e^{-x} x^{\rho} dx}{\int_0^{\infty} e^{-x} x^{\rho} dx}.$$

Изъ этого уравненія видно, что производная n порядка отъ $\sum \frac{1}{m^{1+\rho}} - \frac{1}{\rho}$ по ρ будетъ выражаться дробью, у которой зна-

менателемъ будетъ $[\int_0^\infty e^{-x} x^\rho dx]^{n+1}$, а числителемъ цѣлая функция интеграловъ

$$\int_0^\infty \left(\frac{1}{e^x-1} - \frac{1}{x}\right) e^{-x} x^\rho dx, \int_0^\infty \left(\frac{1}{e^x-1} - \frac{1}{x}\right) e^{-x} x^\rho \log x dx,$$

$$\int_0^\infty \left(\frac{1}{e^x-1} - \frac{1}{x}\right) e^{-x} x^\rho \log^2 x dx, \dots\dots\dots$$

$$\dots\dots\dots \int_0^\infty \left(\frac{1}{e^x-1} - \frac{1}{x}\right) e^{-x} x^\rho \log^n x dx, \int_0^\infty e^{-x} x^\rho dx,$$

$$\int_0^\infty e^{-x} x^\rho \log x dx, \int_0^\infty e^{-x} x^\rho \log^2 x dx, \dots \int_0^\infty e^{-x} x^\rho \log^n x dx.$$

Но такая дробь, будетъ ли $n = 0$ или > 0 , приближается къ конечному предѣлу съ приближеніемъ ρ къ 0; ибо предѣлъ интеграла $\int_0^\infty e^{-x} x^\rho dx$ при $\rho = 0$ есть 1; интегралы же

$$\int_0^\infty \left(\frac{1}{e^x-1} - \frac{1}{x}\right) e^{-x} x^\rho dx, \int_0^\infty \left(\frac{1}{e^x-1} - \frac{1}{x}\right) e^{-x} x^\rho \log x dx,$$

$$\int_0^\infty \left(\frac{1}{e^x-1} - \frac{1}{x}\right) e^{-x} x^\rho \log^2 x dx, \dots \int_0^\infty \left(\frac{1}{e^x-1} - \frac{1}{x}\right) e^{-x} x^\rho \log^n x dx,$$

$$\int_0^\infty e^{-x} x^\rho \log x dx, \int_0^\infty e^{-x} x^\rho \log^2 x dx, \dots \int_0^\infty e^{-x} x^\rho \log^n x dx$$

при $\rho = 0$, очевидно, сохраняютъ конечную величину.

И такъ съ приближеніемъ ρ къ 0 всѣ производныя отъ $\sum \frac{1}{m^{1+\rho}} - \frac{1}{\rho}$, также какъ и сама $\sum \frac{1}{m^{1+\rho}} - \frac{1}{\rho}$, будутъ имѣть предѣломъ величину конечную.

Обращаемся теперь къ функции

$$\log \rho - \sum \log \left(1 - \frac{1}{\mu^{1+\rho}}\right).$$

Извѣстно, что

$$\left[\left(1 - \frac{1}{2^{1+\rho}}\right)\left(1 - \frac{1}{3^{1+\rho}}\right)\left(1 - \frac{1}{5^{1+\rho}}\right)\dots\dots\right]^{-1}$$

$$= 1 + \frac{1}{2^{1+\rho}} + \frac{1}{3^{1+\rho}} + \frac{1}{4^{1+\rho}} + \dots\dots;$$

откуда выходитъ

$$-\log \left(1 - \frac{1}{2^{1+\rho}}\right) - \log \left(1 - \frac{1}{3^{1+\rho}}\right) - \log \left(1 - \frac{1}{5^{1+\rho}}\right) \dots$$

$$= \log \left(1 + \frac{1}{2^{1+\rho}} + \frac{1}{3^{1+\rho}} + \frac{1}{4^{1+\rho}} + \dots\dots\right),$$

что по нашему законоположенію напишется такъ

$$-\sum \log \left(1 - \frac{1}{\mu^{1+\rho}} \right) = \log \left(1 + \sum \frac{1}{m^{1+\rho}} \right);$$

следовательно

$$\log \varrho - \sum \log \left(1 - \frac{1}{\mu^{1+\rho}} \right) = \log \left(1 + \sum \frac{1}{m^{1+\rho}} \right) \varrho;$$

а потому

$$\log \varrho - \sum \log \left(1 - \frac{1}{\mu^{1+\rho}} \right) = \log \left[1 + \varrho + \left(\sum \frac{1}{m^{1+\rho}} - \frac{1}{\varrho} \right) \varrho \right].$$

Изъ этого уравненія видно, что производныя

$$\log \varrho - \sum \log \left(1 - \frac{1}{\mu^{1+\rho}} \right)$$

по ϱ выразятся конечнымъ числомъ дробей, у которыхъ знаменателями будутъ цѣлыя, положительныя степени

$$1 + \varrho + \left(\sum \frac{1}{m^{1+\rho}} - \frac{1}{\varrho} \right) \varrho,$$

а числители будутъ цѣлыя функціи количества ϱ , выраженія

$\sum \frac{1}{m^{1+\rho}} - \frac{1}{\varrho}$ и производныхъ его по ϱ . Но такія дроби съ

приближеніемъ ϱ къ 0 приближаются къ конечному предѣлу;

пбо выраженіе $1 + \varrho + \left(\sum \frac{1}{m^{1+\rho}} - \frac{1}{\varrho} \right) \varrho$, составляющее знаменателей этихъ дробей, съ приближеніемъ ϱ къ 0 приближается

къ 1 (потому, что $\sum \frac{1}{m^{1+\rho}} - \frac{1}{\varrho}$, какъ доказали, при этомъ

остается конечною величиною); функція же $\sum \frac{1}{m^{1+\rho}} - \frac{1}{\varrho}$ и про-

изводныя ея, входящія въ составъ числителей этихъ дробей,

по доказанному нами, съ приближеніемъ ϱ къ 0 приближаются

къ конечному предѣлу.

Намъ остается теперь доказать это же относительно производныхъ

$$\sum \log \left(1 - \frac{1}{\mu^{1+\rho}} \right) + \sum \frac{1}{\mu^{1+\rho}}.$$

Для этого мы замѣчаемъ, что первая производная этой функціи есть

$$\sum \frac{1}{\mu^{2+2\rho}} \cdot \frac{\log \mu}{1 - \frac{1}{\mu^{1+\rho}}}.$$

По виду же этой функции не трудно замѣтить, что ея высшія производныя, выразятся конечнымъ числомъ членовъ вида

$$\sum \frac{1}{\mu^{2+2\rho}} \cdot \frac{\log^p \mu}{1 - \frac{1}{\mu^{1+\rho}}} \cdot \frac{1}{\mu^s \left(1 - \frac{1}{\mu^{1+\rho}}\right)^r},$$

гдѣ p, q, r, s , не < 0 . Но каждый изъ такихъ членовъ для $\rho = 0$ и $\rho > 0$ имѣеть конечную величину; ибо для $\rho = 0$ и $\rho > 0$ функция, состоящая подъ знакомъ Σ , относительно $\frac{1}{\mu}$ будетъ безконечно-малое порядка не ниже втораго.

Убѣдившись такимъ образомъ, что производныя отъ выражений

$$\sum \frac{1}{m^{1+\rho}} - \frac{1}{\rho}, \quad \log \rho - \sum \log \left(1 - \frac{1}{m^{1+\rho}}\right),$$

$$\sum \log \left(1 - \frac{1}{m^{1+\rho}}\right) + \sum \frac{1}{m^{1+\rho}},$$

съ приближеніемъ ρ къ 0 приближаются къ конечному предѣлу, мы заключаемъ тоже и о выраженіи

$$\frac{d^n \left[\sum \log \left(1 - \frac{1}{m^{1+\rho}}\right) + \sum \frac{1}{m^{1+\rho}} \right]}{d\rho^n} + \frac{d^n \left[\log \rho - \sum \log \left(1 - \frac{1}{m^{1+\rho}}\right) \right]}{d\rho^n}$$

$$+ \frac{d^{n-1} \left(\sum \frac{1}{m^{1+\rho}} - \frac{1}{\rho} \right)}{d\rho^{n-1}},$$

которое по выполненіи дифференцированія и сокращенія приводится къ слѣдующему

$$+ \left(\sum \frac{\log^n \mu}{m^{1+\rho}} - \sum \frac{\log^{n-1} m}{m^{1+\rho}} \right),$$

въ чемъ и заключается предложенная нами теорема; ибо, какъ не трудно замѣтить, по нашему знакоположенію выраженіе

$$\sum \frac{\log^n \mu}{m^{1+\rho}} - \sum \frac{\log^{n-1} m}{n^{1+\rho}}$$

тождественно выраженію

$$\sum_{x=2}^{x=\infty} \left[\varphi(x+1) - \varphi(x) - \frac{1}{\log x} \right] \frac{\log^n x}{x^{1+\rho}}$$

Въ самомъ дѣлѣ, послѣднее выраженіе есть разность двухъ

$$\sum_{x=2}^{x=\infty} [\varphi(x+1) - \varphi(x)] \frac{\log^n x}{x^{1+\rho}}, \quad \sum_{x=2}^{x=\infty} \frac{\log^n - 1 x}{x^{1+\rho}},$$

изъ которыхъ первое приводится къ $\sum \frac{\log^n \mu}{\mu^{1+\rho}}$ (суммѣ значений $\frac{\log^n x}{x^{1+\rho}}$, соответствующихъ простымъ числамъ); ибо $\varphi(x+1) - \varphi(x)$, означая число простыхъ чиселъ, меньшихъ $x+1$ и x , въ разности $\varphi(x+1) - \varphi(x)$ даютъ 1, когда x число простое и 0, если x число составное; второе же переменную x на m обращается въ $\sum \frac{\log^n - 1 m}{m^{1+\rho}}$.

Такъ убѣждаемся въ справедливости предложенной нами теоремы.

Изъ доказанной нами теоремы можно вывести многія любопытныя свойства функций, опредѣляющей число простыхъ чиселъ, меньшихъ даннаго предѣла. Для этого мы замѣчаемъ, что разность $\frac{1}{\log x} - \int_x^{x+1} \frac{dx}{\log x}$, при x большомъ, есть бесконечно малое относительно $\frac{1}{x}$ порядка перваго; а потому выраженіе

$$\left(\frac{1}{\log x} - \int_x^{x+1} \frac{dx}{\log x} \right) \frac{\log^n x}{x^{1+\rho}}$$

при x большомъ будетъ относительно $\frac{1}{x}$ порядка $2 + \rho$, и слѣд. при ρ не < 0 , сумма

$$\sum_{x=2}^{x=\infty} \left(\frac{1}{\log x} - \int_x^{x+1} \frac{dx}{\log x} \right) \frac{\log^n x}{x^{1+\rho}}$$

будетъ имѣть значеніе конечное. Складывая же эту сумму съ выраженіемъ

$$\sum_{x=2}^{x=\infty} \left[\varphi(x+1) - \varphi(x) - \frac{1}{\log x} \right] \frac{\log^n x}{x^{1+\rho}},$$

о которомъ сейчасъ доказали теорему 1-ю, на основаніи ея заключаемъ, что значеніе

$$\sum_{x=2}^{x=\infty} \left[\varphi(x+1) - \varphi(x) - \int_x^{x+1} \frac{dx}{\log x} \right] \frac{\log^n x}{x^{1+\rho}} dx$$

съ приближеніемъ ρ къ 0 приближается къ конечному предѣлу. А отсюда не трудно вывести слѣдующую теорему:

2. ТЕОРЕМА.

Отъ $x = 2$ до $x = \infty$ функция $\varphi(x)$, означающая число простыхъ чиселъ меньшихъ x , удовлетворяетъ безконечное число разъ и неравенству $\varphi(x) > \int_2^x \frac{dx}{\log x} - \frac{\alpha x}{\log^n x}$ и неравенству $\varphi(x) < \int_2^x \frac{dx}{\log x} + \frac{\alpha x}{\log^n x}$, какъ бы α , оставаясь количествомъ положительнымъ, ни было мало, а n ни было велико.

Доказательство. Мы ограничимся здѣсь доказательствомъ втораго неравенства, первое докажется подобнымъ образомъ. Для доказательства, что неравенству

$$\varphi(x) < \int_2^x \frac{dx}{\log c} + \frac{\alpha x}{\log^n x} \dots \dots \dots (1)$$

удовлетворять безконечное множество чиселъ, допустимъ противное, и посмотримъ къ чему приведетъ насъ это допущеніе. Допустивъ, что неравенству (1) удовлетворяетъ конечное число чиселъ, положимъ, что a есть цѣлое число, превосходящее и количество e^n и наибольшее число, удовлетворяющее неравенству (1). Въ этомъ предположеніи для $x > a$ будетъ

$$\varphi(x) \geq \int_2^x \frac{dx}{\log x} + \frac{\alpha x}{\log^n x}, \log x > n,$$

и слѣд.

$$\varphi(x) - \int_2^x \frac{dx}{\log x} \geq \frac{\alpha x}{\log^n x}, \frac{n}{\log x} < 1 \dots \dots \dots (2)$$

Но въ этомъ случаѣ, какъ сейчасъ увидимъ, въ противность доказаннаго намъ значеніе выраженія

$$\sum_{x=2}^{x=\infty} \left[\varphi(x+1) - \varphi(x) - \int_x^{x+1} \frac{dx}{\log x} \right] \frac{\log^n x}{x^{1+\rho}}$$

будетъ приближаться къ $+\infty$ съ приближеніемъ ρ къ 0. Въ самомъ дѣлѣ, это выраженіе мы можемъ разсматривать какъ предѣлъ

$$\sum_{x=2}^{x=s} \left[\varphi(x+1) - \varphi(x) - \int_x^{x+1} \frac{dx}{\log x} \right] \frac{\log^n x}{x^{1+\rho}}$$

при $s = \infty$. Предполагая же $s > a$, это выражение мы можем рассматривать как сумму

$$C + \sum_{x=a+1}^{x=s} \left[\varphi(x+1) - \varphi(x) - \int_x^{x+1} \frac{dx}{\log x} \right] \frac{\log^n x}{x^{1+\varrho}}, \dots \quad (3)$$

называя через C сумму

$$\sum_{x=2}^{x=a} \left[\varphi(x+1) - \varphi(x) - \int_x^{x+1} \frac{dx}{\log x} \right] \frac{\log^n x}{x^{1+\varrho}},$$

которая, очевидно, сохраняет конечное значение при $\varrho = 0$ и $\varrho > 0$.

Далѣ, по формулѣ

$$\sum_{a+1}^s u_x (\varrho_{x+1} - \varrho_x) = u_s \varrho_{s+1} - u_a \varrho_{a+1} - \sum_{a+1}^s \varrho_x (u_x - u_{x-1}),$$

полагая

$$\varrho_x = \varphi(x) - \int_2^x \frac{dx}{\log x}, \quad u_x = \frac{\log^n x}{x^{1+\varrho}},$$

выражение (3) преобразуемъ въ такое

$$C - \left[\varphi(a+1) - \int_2^{a+1} \frac{dx}{\log x} \right] \frac{\log^n a}{a^{1+\varrho}} + \left[\varphi(s+1) - \int_2^{s+1} \frac{dx}{\log x} \right] \frac{\log^n s}{s^{1+\varrho}} - \sum_{x=a+1}^{x=s} \left[\varphi(x) - \int_2^x \frac{dx}{\log x} \right] \left[\frac{\log^n x}{x^{1+\varrho}} - \frac{\log^n(x-1)}{(x-1)^{1+\varrho}} \right],$$

а это, называя через θ количество > 0 и < 1 , можем написать такъ

$$C - \left[\varphi(a+1) - \int_2^{a+1} \frac{dx}{\log x} \right] \frac{\log^n a}{a^{1+\varrho}} + \left[\varphi(s+1) - \int_2^{s+1} \frac{dx}{\log x} \right] \frac{\log^n s}{s^{1+\varrho}} + \sum_{x=a+1}^{x=s} \left[\varphi(x) - \int_2^x \frac{dx}{\log x} \right] \left[1 + \varrho - \frac{n}{\log(x-\theta)} \right] \frac{\log^n(x-\theta)}{(x-\theta)^{2+\varrho}}.$$

Полагая же два первые члена этого выражения равными F , и замѣчая по (2), что третій членъ > 0 , мы убѣждаемся, что все это выражение болѣе

$$F + \sum_{x=a+1}^{x=s} \left[\varphi(x) - \int_2^x \frac{dx}{\log x} \right] \left[1 + \varrho - \frac{n}{\log(x-\theta)} \right] \frac{\log^n(x-\theta)}{(x-\theta)^{2+\varrho}}$$

Изъ тѣхъ же неравенствъ (2) видно, что здѣсь подъ знакомъ суммы, въ предѣлахъ суммированія, функція сохраняетъ

знакъ +. При томъ въ предѣлахъ суммированія будетъ во 1-хъ)
 $1 + \rho - \frac{n}{\log(x-\theta)}$ болѣе $1 - \frac{n}{\log a}$; пбо $\rho > 0$, x не $< a + 1$,
 $\theta < 1$; во 2) $\varphi(x) - \int_2^x \frac{dx}{\log x}$ болѣе $\frac{\alpha(x-\theta)}{\log^n(x-\theta)}$; пбо $\varphi(x) - \int_2^x \frac{dx}{\log x}$
 не меньше $\frac{\alpha x}{\log^n x}$ по первому изъ неравенствъ (2), а по второму
 производная $\frac{\alpha x}{\log^n x}$, которая есть $\frac{\alpha}{\log^n x} \left(1 - \frac{n}{\log x}\right)$, болѣе 0, вслед-
 ствие чего $\frac{\alpha x}{\log^n x} > \frac{\alpha(x-\theta)}{\log^n(x-\theta)}$.

А потому предыдущее выраженіе болѣе

$$F + \sum_{x=a+1}^{x=s} \frac{\alpha(x-\theta)}{\log^n(x-\theta)} \left(1 - \frac{n}{\log a}\right) \frac{\log^n(x-\theta)}{(x-\theta)^{2+\rho}}.$$

Но это по сокращеніи приводится къ слѣдующему

$$F + a \left(1 - \frac{n}{\log a}\right) \sum_{x=a+1}^{x=s} \frac{1}{(x-\theta)^{1+\rho}},$$

что, очевидно, болѣе

$$F + \alpha \left(1 - \frac{n}{\log a}\right) \sum_{x=a+1}^{x=s} \frac{1}{x^{1+\rho}}.$$

А это для $s = \infty$ будетъ

$$F + \alpha \left(1 - \frac{n}{\log a}\right) \sum_{x=a+1}^{x=\infty} \frac{1}{x^{1+\rho}},$$

и съ помощію опредѣленныхъ интеграловъ напишется такъ

$$F + \alpha \left(1 - \frac{n}{\log a}\right) \frac{\int_0^{\infty} \frac{e^{-ax}}{e^x - 1} x^{\rho} dx}{\int_0^{\infty} e^{-x} x^{\rho} dx}.$$

Но это выраженіе, очевидно, съ уменьшеніемъ ρ приближается
 къ $+\infty$; пбо $\int_0^{\infty} \frac{e^{-ax}}{e^x - 1} dx = +\infty$, $\int_0^{\infty} e^{-x} dx = 1$, а α по
 положенію и $1 - \frac{n}{\log a}$ вследствие (2) суть количества положи-
 тельныя.

Убѣдившись такимъ образомъ, что въ сдѣланномъ нами
 предположеніи не только сумма

$$\sum_{x=2}^{x=\infty} \left[\varphi(x+1) - \varphi(x) - \int_2^{x+1} \frac{dx}{\log x} \right] \frac{\log^n x}{x^{1+\rho}},$$

но и количество меньше его съ приближеніемъ ρ къ 0 приближается къ $+\infty$, мы заключаемъ о несправедливости его, что и слѣдовало доказать.

На основаніи предыдущей теоремы легко доказать слѣдующую:

III. ТЕОРЕМА.

Выраженіе $\frac{x}{\varphi(x)} - \log x$ при $x = \infty$ не можетъ имѣть предѣловъ количество отличное отъ -1 .

Доказательство. Пусть будетъ L предѣлъ значенія $\frac{x}{\varphi(x)} - x$ при $x = \infty$. Въ этомъ предположеніи мы всегда найдемъ число N столь большое, что при $x > N$ значеніе $\frac{x}{\varphi(x)} - \log x$ не будетъ выходить изъ предѣловъ $L - \varepsilon$ и $L + \varepsilon$, какъ бы ε ни было мало. Слѣд. для такихъ величинъ x , при $\varepsilon > 0$, будетъ

$$\frac{x}{\varphi(x)} - \log x > L - \varepsilon, \quad \frac{x}{\varphi(x)} - \log x < L + \varepsilon \dots \dots \dots (4)$$

Но по предыдущей теоремѣ, неравенства

$$\varphi(x) > \int_2^x \frac{dx}{\log x} - \frac{\alpha x}{\log^n x}, \quad \varphi(x) < \int_2^x \frac{dx}{\log x} + \frac{\alpha x}{\log^n x}$$

удовлетворяются при безконечномъ множествѣ величинъ x и слѣд. при нѣкоторыхъ числахъ $x > N$, для которыхъ имѣютъ мѣсто неравенства (4). Но эти неравенства въ соединеніи съ послѣдними даютъ

$$\frac{x}{\int_2^x \frac{dx}{\log x} - \frac{\alpha x}{\log^n x}} - \log x > L - \varepsilon, \quad \frac{x}{\int_2^x \frac{dx}{\log x} + \frac{\alpha x}{\log^n x}} - \log x < L + \varepsilon;$$

откуда выходитъ

$$L + 1 < \frac{x - (\log x - 1) \left(\int_2^x \frac{dx}{\log x} - \frac{\alpha x}{\log^n x} \right)}{\int_2^x \frac{dx}{\log x} - \frac{\alpha x}{\log^n x}} + \varepsilon,$$

$$L + 1 > \frac{x - (\log x - 1) \left(\int_2^x \frac{dx}{\log x} + \frac{\alpha x}{\log^n x} \right)}{\int_2^x \frac{dx}{\log x} + \frac{\alpha x}{\log^n x}} - \varepsilon.$$

Изъ этихъ неравенствъ видно, что численная величина $L+1$ не превосходитъ численной величины одного изъ выражений

$$\frac{x - (\log x - 1) \left(\int_2^x \frac{dx}{\log x} + \frac{ax}{\log^n x} \right)}{\int_2^x \frac{dx}{\log x} + \frac{ax}{\log^n x}} + \varepsilon.$$

Но количество ε можетъ быть сдѣлано, какъ замѣтили, по произволу мало предположеніемъ N чрезвычайно большимъ, тоже случается при увеличиваніи x съ выраженіемъ

$$\frac{x - (\log x - 1) \left(\int_2^x \frac{dx}{\log x} + \frac{ax}{\log^n x} \right)}{\int_2^x \frac{dx}{\log x} + \frac{ax}{\log^n x}};$$

ибо въ предѣлѣ этихъ выраженій для $x = \infty$ по извѣстнымъ приемамъ дифференціального исчисления мы открываемъ 0. Убѣдивъ такимъ образомъ, что выраженіе

$$\frac{x - (\log x - 1) \left(\int_2^x \frac{dx}{\log x} + \frac{ax}{\log^n x} \right)}{\int_2^x \frac{dx}{\log x} + \frac{ax}{\log^n x}} + \varepsilon,$$

опредѣляющее высшій предѣлъ численной величины $L+1$, можетъ быть сдѣлано по произволу малымъ, мы по способу предѣловъ заключаемъ, что $L+1=0$, а потому $L=-1$, что и слѣдовало доказать.

Доказанное нами относительно предѣла значеній $\frac{x}{\varphi(x)} - \log x$ при $x = \infty$ противорѣчитъ формулѣ, предложенной Лежандромъ для приближеннаго опредѣленія числа простыхъ чиселъ меньшихъ даннаго. По его мнѣнію при x большомъ значеніе $\varphi(x)$ можетъ быть опредѣлено съ достаточною точностію уравненіемъ

$$\varphi(x) = \frac{x}{\log x - 1,08366}.$$

Но отсюда для предѣла $\frac{x}{\varphi(x)} - \log x$ при $x = \infty$ находимъ $-1,08366$, вмѣсто -1 .

На основаніи теоремы II можно показать высшій предѣлъ точности, съ которою функція $\varphi(x)$, опредѣляющая число про-

стыхъ чиселъ меньшихъ x , можетъ быть представлена какою либо данною функціею f_x . При этомъ разность $f_x - \varphi(x)$ мы будемъ сравнивать съ выраженіями

$$\frac{x}{\log x}, \frac{x}{\log^2 x}, \frac{x}{\log^3 x}, \dots$$

и для сокращенія будемъ называть A количествомъ порядка $\frac{x}{\log^n x}$, если отношеніе A къ $\frac{x}{\log^m x}$ при $x = \infty$ будетъ ∞ для $m > n$ и 0 для $m < n$. Условившись въ этомъ, мы докажемъ слѣдующую теорему:

IV. ТЕОРЕМА.

Если выраженіе

$$\frac{\log^n x}{x} \left(f_x - \int_2^x \frac{dx}{\log x} \right),$$

при $x = \infty$ имѣетъ предѣломъ количество конечное или безконечность; то f_x не можетъ представить $\varphi(x)$ вѣрно до количества порядка $\frac{x}{\log^n x}$ включительно.

Доказательство. Пусть будетъ L предѣлъ, къ которому значеніе

$$\frac{\log^n x}{x} \left(f(x) - \int_2^x \frac{dx}{\log x} \right)$$

приближается съ приближеніемъ x къ ∞ . Количество L , не будучи 0 по положенію, можетъ быть или количествомъ положительнымъ, или отрицательнымъ. Мы его предположимъ количествомъ положительнымъ; но сужденія наши безъ затрудненія приложатся и къ случаю $L < 0$.

Если значеніе

$$\frac{\log^n x}{x} \left(f(x) - \int_2^x \frac{dx}{\log x} \right)$$

съ приближеніемъ x къ ∞ имѣетъ предѣломъ L , большее 0, то мы найдемъ число N столь большое, что для $x > N$ значеніе $\frac{\log^n x}{x} \left(f(x) - \int_2^x \frac{dx}{\log x} \right)$ останется постоянно болѣе нѣ-

котораго положительнаго количества l . Слѣд. предполагая $x > N$, мы будемъ имѣть

$$\frac{\log^n x}{x} \left(f(x) - \int_2^x \frac{dx}{\log x} \right) > l \dots \dots \dots (5)$$

Но по II теоремѣ, какъ бы $\alpha = \frac{l}{2}$ ни было мало, для безконечнаго множества чиселъ будетъ имѣть мѣсто такое неравенство

$$\varphi(x) < \int_2^x \frac{dx}{\log x} + \frac{\alpha x}{\log^n x}, \dots \dots \dots (6)$$

которое даетъ

$$f(x) - \int_2^x \frac{dx}{\log x} < f(x) - \varphi(x) + \frac{\alpha x}{\log^n x},$$

что по умноженіи на $\frac{\log^n x}{x}$ и по положенію $\alpha = \frac{l}{2}$ будетъ

$$\frac{\log^n x}{x} \left[f(x) - \int_2^x \frac{dx}{\log x} \right] < \frac{\log^n x}{x} [f(x) - \varphi(x)] + \frac{l}{2},$$

а отсюда вслѣдствіе неравенства (5) выходитъ

$$\frac{\log^n x}{x} [f(x) - \varphi(x)] > \frac{l}{2}.$$

Но это неравенство, существуя вмѣстѣ съ неравенствами (5) и (6) для безконечнаго множества чиселъ, по причинѣ $\frac{l}{2} > 0$ обнаруживаетъ, что предѣлъ

$$\frac{\log^n x}{x} [f(x) - \varphi(x)]$$

при $x = \infty$ не есть нуль. Если же этотъ предѣлъ отличенъ отъ 0; то разность $f(x) - \varphi(x)$ по сдѣланному нами опредѣленію есть количество порядка $\frac{x}{\log^n x}$ или нисшаго; и слѣд. $f(x)$ разнится съ $\varphi(x)$ или количествомъ порядка $\frac{x}{\log^n x}$, или порядка нисшаго, что и слѣдовало доказать.

На основаніи этой теоремы мы узнаемъ, что формула Лежандра $\frac{x}{\log x - 1,08366}$, для которой

$$\frac{\log^2 x}{x} \left(\frac{x}{\log x - 1,08366} - \int_2^x \frac{dx}{\log x} \right),$$

при $x = \infty$ имѣетъ предѣломъ величину 0,08366, не можетъ

выражать $\varphi(x)$, число простыхъ чиселъ, меньшихъ x , вѣрно до количествъ порядка $\frac{x}{\log^2 x}$ включительно.

Также не трудно показать на основаніи этой теоремы величины постоянныхъ A и B , при которыхъ функція $\frac{x}{A \log x + B}$ могла бы выражать $\varphi(x)$ вѣрно до количествъ порядка $\frac{x}{\log^2 x}$ включительно. По предыдущей теоремѣ такія величины A и B должны удовлетворять уравненію

$$\lim. \left[\frac{\log^2 x}{x} \left(\frac{x}{A \log x + B} - \int_2^x \frac{dr}{\log r} \right) \right]_{x=\infty} = 0.$$

Но разложениемъ $\frac{x}{A \log x + B}$ въ рядъ находимъ

$$\frac{x}{A \log x + B} = \frac{1}{A} \cdot \frac{x}{\log x} - \frac{B}{A^2} \cdot \frac{x}{\log^2 x} + \frac{B^2}{A^3} \cdot \frac{x}{\log^3 x} - \dots$$

Интегрируя же $\int_2^x \frac{dx}{\log x}$ по частямъ, имѣемъ

$$\int_2^x \frac{dx}{\log x} = \frac{x}{\log x} + \frac{x}{\log^2 x} + 2 \int_2^x \frac{dx}{\log^3 x} + C.$$

Вслѣдствіе чего предыдущее уравненіе измѣняется въ слѣдующее

$$\lim. \left\{ \frac{\log^2 x}{x} \left(\frac{1}{A} \cdot \frac{x}{\log x} - \frac{B}{A^2} \cdot \frac{x}{\log^2 x} + \frac{B^2}{A^3} \cdot \frac{x}{\log^3 x} - \dots \right) \left(\dots - \frac{x}{\log x} - \frac{x}{\log^2 x} - 2 \int_2^x \frac{dx}{\log^3 x} - C \right) \right\}_{x=\infty} = 0,$$

что приводится къ такому уравненію

$$\lim. \left\{ \left(\frac{1}{A} - 1 \right) \log x - \left(\frac{B}{A^2} + 1 \right) + \frac{B^2}{A} \frac{1}{\log x} - \dots \right\}_{x=\infty} = 0.$$

Замѣчая же, что здѣсь всѣ члены, начиная съ третьяго, приближаются къ 0 съ увеличеніемъ x , мы убѣждаемся, что это уравненіе можетъ быть удовлетворено только предположеніемъ $\frac{1}{A} - 1 = 0$, $\frac{B}{A^2} + 1 = 0$. Откуда $A = 1$, $B = -1$.

И такъ изъ функцій вида $\frac{x}{A \log x + B}$ одна функція $\frac{x}{\log x - 1}$

могла бы выразить $\varphi(x)$ вѣрно до количествъ порядка $\frac{x}{\log^2 x}$ включительно.

Что же касается до выбора функціи, наиболее выражающей $\varphi(x)$, число простыхъ чиселъ, меньшихъ даннаго числа, то относительно ея можно доказать такую теорему.

V. ТЕОРЕМА.

Если функція $\varphi(x)$, определяющая число простыхъ чиселъ меньшихъ x , можетъ быть выражена вѣрно до количествъ порядка $\frac{x}{\log^n x}$ включительно алгебраически въ $x, \log x, e^x$; то такое выраженіе ея есть

$$\frac{x}{\log x} + \frac{1 \cdot x}{\log^2 x} + \frac{1 \cdot 2 \cdot x}{\log^3 x} + \dots + \frac{1 \cdot 2 \cdot 3 \dots (n-1) \cdot x}{\log^n x}.$$

Доказательство. Пусть будетъ $f(x)$ та функція, которая, заключаая алгебраически $x, \log x, e^x$, выражаетъ $\varphi(x)$ вѣрно до количествъ порядка $\frac{x}{\log^n x}$ включительно; выраженіе

$$\frac{\log^n x}{x} \left[f(x) - \frac{x}{\log x} - \frac{1 \cdot x}{\log^2 x} - \frac{1 \cdot 2 \cdot x}{\log^3 x} - \dots - \frac{1 \cdot 2 \cdot 3 \dots (n-1) \cdot x}{\log^n x} \right]$$

съ увеличеніемъ x должно приближаться къ какому либо предѣлу конечному или бесконечно великому; ибо въ противномъ случаѣ первая производная этого выраженія съ увеличеніемъ x до ∞ мѣняла бы свой знакъ бесконечное число разъ; а это, какъ легко замѣтить, не можетъ случиться съ функціею алгебраическою отъ $x, \log x, e^x$.

(*) Что алгебраическая функція отъ $x, \log x, e^x$ перестаетъ мѣнять свой знакъ при x , превосходящемъ нѣкоторый предѣлъ, въ этомъ не трудно убѣдиться. Для функціи цѣлой это ясно; знакъ такой функціи при довольно большомъ x будетъ зависетьъ отъ одного члена вида $kx^{m'}$, $\log^{m''} x \cdot e^{m'''x}$, который не мѣняетъ знака при $x < 1$. Для всякой же другой алгебраической функціи $x, \log x, e^x$, которая пусть будетъ y , это докажется такимъ образомъ. Функція y вообще будетъ корнемъ уравненія $u_0 y^m + u_1 y^{m-1} + \dots + u_m = 0$, и если v будетъ функція, получаемая черезъ исключене y изъ предыдущаго уравненія и первой производной его по x , то

И такъ для $\varphi(x)$ необходимо будетъ

$$\lim_{x \rightarrow \infty} \left\{ \frac{\log^n x}{x} \left(f(x) - \frac{x}{\log x} - \frac{1 \cdot x}{\log^2 x} - \frac{1 \cdot 2 \cdot x}{\log^3 x} - \dots \right) \right\} = L \dots (7)$$

Но съ другой стороны не трудно убѣдиться, что

$$\lim_{x \rightarrow \infty} \left[\frac{\log^n x}{x} \left(\frac{x}{\log x} + \frac{1 \cdot x}{\log^2 x} + \frac{1 \cdot 2 \cdot x}{\log^3 x} + \dots \right. \right. \\ \left. \left. + \frac{1 \cdot 2 \cdot \dots \cdot (n-1)x}{\log^n x} - \int_2^x \frac{dx}{\log x} \right) \right] = 0,$$

а это уравненіе, сложенное съ предыдущимъ, даетъ

$$\lim_{x \rightarrow \infty} \left[\frac{\log^n x}{x} \left(f(x) - \int_2^x \frac{dx}{\log x} \right) \right] = L.$$

Но такъ какъ по положенію $f(x)$ выражаетъ $\varphi(x)$ вѣрно до количества порядка $\frac{x}{\log^n x}$ включительно; а по предыдущей теоремѣ это не можетъ имѣть мѣсто, если предѣлъ значенія

$$\frac{\log^n x}{x} \left[f(x) - \int_2^x \frac{dx}{\log x} \right],$$

при $x = \infty$ не есть 0. Слѣд. $L = 0$, и уравненіе (7) даетъ

$$\lim_{x \rightarrow \infty} \left\{ \frac{\log^n x}{x} \left[f(x) - \frac{x}{\log x} - \frac{1 \cdot x}{\log^2 x} - \frac{1 \cdot 2 \cdot x}{\log^3 x} - \dots \right. \right. \\ \left. \left. \dots - \frac{1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-1)x}{\log^n x} \right] \right\} = 0,$$

а это показываетъ, что функція

$$\frac{x}{\log x} + \frac{1 \cdot x}{\log^2 x} + \frac{1 \cdot 2 \cdot x}{\log^3 x} + \dots + \frac{1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-1)x}{\log^n x}$$

не разится съ $f(x)$ количествами порядка $\frac{x}{\log^n x}$ и низшими, и слѣд. что она подобно $f(x)$ можетъ выражать $\varphi(x)$ вѣрно до количества порядка $\frac{x}{\log^n x}$ включительно, что и требовалось доказать.

Функція u_0, u_m, v , какъ цѣлая, перестанутъ мѣнять свой знакъ и обращаться въ 0 при x превосходящемъ нѣкоторый предѣлъ; а при этомъ и u будетъ сохранять свой знакъ; ибо при величинахъ x , необращающихъ v въ нуль, не можетъ имѣть уравненіе равныхъ корней; а при неравенствѣ корней знакъ одного изъ нихъ можетъ переимѣниться только съ переимѣною знака u_0 или u_m . Это свойства можетъ быть также доказано и для многихъ другихъ функцій, и на всѣ эти функціи будетъ распространяться теорема V и заключенія изъ нея вытекающія.

На основаніи доказанной нами теоремы мы заключаемъ, что если $\varphi(x)$, функція, опредѣляющая число простыхъ чиселъ меньшихъ x , можетъ быть выражена алгебраически въ x , $\log x$, e^x вѣрно до количествъ порядковъ $\frac{x}{\log x}$, $\frac{x}{\log^2 x}$, $\frac{x}{\log^3 x}$, включительно; то такое выраженіе ея есть

$$\frac{x}{\log x} + \frac{x}{\log x} + \frac{1 \cdot x}{\log^2 x} + \frac{x}{\log x} + \frac{1 \cdot x}{\log^2 x} + \frac{1 \cdot 2 \cdot x}{\log^3 x}, \dots$$

А такъ какъ эти функціи суть ни что иное, какъ значеніе интеграла $\int_2^x \frac{dx}{\log x}$ вѣрно до количествъ порядка $\frac{x}{\log x}$, $\frac{x}{\log^2 x}$, $\frac{x}{\log^3 x}$, ...;

то во всѣхъ этихъ предположеніяхъ интегралъ $\int_2^x \frac{dx}{\log x}$ будетъ выражать $\varphi(x)$ вѣрно до количествъ такого порядка, до какого она способна выразиться алгебраически въ x , $\log x$, e^x . Что

интегралъ $\int_2^x \frac{dx}{\log x}$ при x большомъ выражаетъ довольно близко число простыхъ чиселъ, меньшихъ x , въ этомъ мы легко убѣждаемся помощію таблицъ простыхъ чиселъ. Но эти таблицы, доселѣ составленныя, слишкомъ малы, чтобы видѣть изъ

нихъ превосходство формулы $\int_2^x \frac{dx}{\log x}$ предъ формулою Лежандра $\frac{x}{\log x - 1,08366}$ или подобными ей. Въ предѣлахъ этихъ таблицъ

функціи $\int_2^x \frac{dx}{\log x}$, $\frac{x}{\log x - 1,08366}$ мало разнятся; но разность ихъ

$\frac{x}{\log x - 1,08366} - \int_2^x \frac{dx}{\log x}$, имѣя *minimum* при $x = e^{\left(\frac{1,08366}{0,08366}\right)^2}$

$= 1247646$, послѣ него постоянно возрастаетъ до ∞ и при $x > 10000000$ получаетъ уже довольно большую величину. При

этихъ-то величинахъ x можно будетъ обнаружить преимущество формулы $\int_2^x \frac{dx}{\log x}$ предъ $\frac{x}{\log x - 1,08366}$. Но для этого потребна таблица простыхъ чиселъ гораздо обширнѣе тѣхъ, которыя мы до сихъ поръ имѣемъ.

Принявши для приближеннаго опредѣленія $\varphi(x)$ интегралъ $\int_2^x \frac{dx}{\log x}$, мы должны будемъ измѣнить всѣ формулы Лежандра,

выведенныя имъ въ предположеніи $\varphi(x) = \frac{x}{\log x - 1.03366}$, и формулы наши будутъ не сложнѣе его. Въ слѣдствіе же доказанныхъ нами теоремъ онѣ должны быть ближе къ истинѣ.

Для примѣра мы найдемъ здѣсь приближенныя формулы для опредѣленія значеній

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \dots + \frac{1}{X},$$

$$\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \dots \left(1 - \frac{1}{X}\right)$$

при X большомъ.

Для опредѣленія перваго мы замѣчаемъ, что по нашему зна-
коположенію будетъ

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{X} = \sum_{x=2}^{x=X} \frac{\varphi(x+1) - \varphi(x)}{x},$$

пбо $\varphi(x)$, означая число простыхъ чиселъ меньшихъ x , въ разности $\varphi(x+1) - \varphi(x)$ даетъ 0, когда x число составное и 1, когда оно простое.

Предполагая X числомъ большимъ, назовемъ λ какое нибудь число менѣе X , но еще довольно значительное, дабы въ предѣлахъ $x = \lambda$ и $x = X$, мы могли съ достаточною точностію замѣнить $\varphi(x)$ интеграломъ $\int_2^x \frac{dx}{\log x}$. Въ этомъ предположеніи предыдущее уравненіе напишется такъ

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{X} = \sum_{x=2}^{x=\lambda-1} \frac{\varphi(x+1) - \varphi(x)}{x} +$$

$$\sum_{x=\lambda}^{x=X} \frac{\varphi(x+1) - \varphi(x)}{x}.$$

Замѣняя же здѣсь во второй суммѣ $\varphi(x)$ интеграломъ $\int_2^x \frac{dx}{\log x}$, найдемъ

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{X} = \sum_{x=2}^{x=\lambda-1} \frac{\varphi(x+1) - \varphi(x)}{x} + \sum_{x=\lambda}^{x=X} \frac{\int_x^{x+1} \frac{dx}{\log x}}{x}.$$

Но вѣрно до количества порядка $\frac{1}{x}$ интеграль $\int_x^{x+1} \frac{dx}{\log x}$

можетъ быть замѣненъ выраженіемъ $\frac{1}{\log x}$, и съ такою же точ-

ностію сумма $\sum_{x=\lambda}^{x=X} \frac{1}{x \log x}$ можетъ быть замѣнена интеграломъ

$$\int_{\lambda}^X \frac{dx}{x \log x}$$

Но такую переменную предыдущее уравненіе приводится къ слѣдующему

$$\frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{X} = \sum_{x=2}^{x=\lambda-1} \frac{\varphi(x+1) - \varphi x}{x} + \int_{\lambda}^x \frac{dx}{x \log x},$$

что по выполненіи интегрированія даетъ

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{X} = \sum_{x=2}^{x=\lambda-1} \frac{\varphi(x+1) - \varphi(x)}{x} - \log \lambda + \log X,$$

или

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{X} = C + \log X, \dots \dots \dots (8)$$

полагая C равнымъ количеству $\sum_{x=2}^{x=\lambda-1} \frac{\varphi(x+1) - \varphi(x)}{x} - \log \lambda$, не зависящему отъ X .

Вотъ уравненіе, которое по опредѣленіи постояннаго C , можетъ намъ служить для приближеннаго вычисленія суммы

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{X},$$

когда X велико.

Наше выраженіе этой суммы проще выраженія ея у Лежандра, которое такого вида

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{X} = \log(\log X - 0,08366) + C.$$

Теперь переходимъ къ опредѣленію произведенія

$$\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \dots \left(1 - \frac{1}{X}\right) = P.$$

Полагая это произведеніе равнымъ P , и взявъ логарифмы отъ обѣихъ частей уравненія

$$\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \dots \left(1 - \frac{1}{X}\right) = P,$$

находимъ

$$\log P = \log \left(1 - \frac{1}{2}\right) + \log \left(1 - \frac{1}{3}\right) + \log \left(1 - \frac{1}{5}\right) + \dots \\ \dots + \log \left(1 - \frac{1}{X}\right),$$

что иначе напишется такъ

$$\log P = - \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{X}\right) + \frac{1}{2} + \log \left(1 - \frac{1}{2}\right) + \\ \frac{1}{3} + \log \left(1 - \frac{1}{3}\right) + \frac{1}{5} + \log \left(1 - \frac{1}{5}\right) + \dots + \frac{1}{X} + \log \left(1 - \frac{1}{X}\right).$$

А здѣсь вѣрно до количествъ порядка $\frac{1}{X}$ можемъ замѣнить конечный рядъ

$$\frac{1}{2} + \log \left(1 - \frac{1}{2}\right) + \frac{1}{3} + \log \left(1 - \frac{1}{3}\right) + \frac{1}{5} + \log \left(1 - \frac{1}{5}\right) + \dots \\ \dots + \frac{1}{X} + \log \left(1 - \frac{1}{X}\right)$$

рядомъ безконечнымъ

$$\frac{1}{2} + \log \left(1 - \frac{1}{2}\right) + \frac{1}{3} + \log \left(1 - \frac{1}{3}\right) + \frac{1}{5} + \log \left(1 - \frac{1}{5}\right) + \dots;$$

пбо разность этихъ рядовъ меньше

$$\frac{1}{X+1} + \log \left(1 - \frac{1}{X+1}\right) + \frac{1}{X+2} + \log \left(1 - \frac{1}{X+2}\right) + \dots,$$

а это меньше интеграла $\int_X^\infty \left[\frac{1}{x} + \log \left(1 - \frac{1}{x}\right)\right] dx$, который

равенъ $1 - (X-1) \log \left(1 - \frac{1}{X}\right)$, и котораго величина при X большомъ есть безконечно малое относительно $\frac{1}{X}$ первого порядка.

Итакъ до количества порядка $\frac{1}{X}$ въ предыдущемъ выраженіи $\log P$ мы можемъ замѣнить конечную сумму

$$\frac{1}{2} + \log \left(1 - \frac{1}{2}\right) + \frac{1}{3} + \log \left(1 - \frac{1}{3}\right) + \frac{1}{5} + \log \left(1 - \frac{1}{5}\right) + \dots \\ \dots + \frac{1}{X} + \log \left(1 - \frac{1}{X}\right)$$

безконечнымъ рядомъ

$$\frac{1}{2} + \log \left(1 - \frac{1}{2}\right) + \frac{1}{3} + \log \left(1 - \frac{1}{3}\right) + \frac{1}{5} + \log \left(1 - \frac{1}{5}\right) + \dots,$$

и называя для сокращенія величину послѣдняго черезъ C' , мы предыдущее выраженіе $\log P$ представимъ такъ

$$\log P = - \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{X} \right) + C'.$$

Внеся же сюда значеніе

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{X}$$

изъ (8), найдемъ

$$\log P = -C - \log X + C',$$

откуда выходитъ

$$P = \frac{e^{C' - C}}{\log X},$$

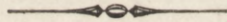
гдѣ полагая для сокращенія $e^{C' - C} = C_0$ и замѣняя P его ве-

личиною $\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \dots \left(1 - \frac{1}{X}\right)$, имѣемъ

$$\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \dots \left(1 - \frac{1}{X}\right) = \frac{C_0}{\log X}.$$

Вмѣсто этой формулы Лежандръ нашелъ такую

$$\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \dots \left(1 - \frac{1}{X}\right) = \frac{C_0}{\log X - 0,08366}.$$



функции поварят математика, во
 попредельности отсюда, что Н-во поварят,
 занимают математики, какбы. Равноденно,

(8)

$$\frac{1}{x} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots$$

$$\frac{1}{x} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots$$

$$\frac{1}{x} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots$$

$$\frac{1}{x} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots$$

ТАБЛИЦА ПРОСТЫХЪ ЧИСЕЛЪ,

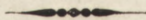
НЕ ПРЕВОСХОДЯЩИХЪ 6000.

2	127	283	467	661	877	1087
3	131	293	479	673	881	1091
5	137	307	487	677	883	1093
7	139	311	491	683	887	1097
11	149	313	499	691	907	1103
13	151	317	503	701	911	1109
17	157	331	509	709	919	1117
19	163	337	521	719	929	1123
23	167	347	523	727	937	1129
29	173	349	541	733	941	1151
31	179	353	547	739	947	1153
37	181	359	557	743	953	1163
41	191	367	563	751	967	1171
43	193	373	569	757	971	1181
47	197	379	571	761	977	1187
53	199	383	577	769	983	1193
59	211	389	587	773	991	1201
61	223	397	593	787	997	1213
67	227	401	599	797	1009	1217
71	229	409	601	809	1013	1223
73	233	419	607	811	1019	1229
79	239	421	613	821	1021	1231
83	241	431	617	823	1031	1237
89	251	433	619	827	1033	1249
97	257	439	631	829	1039	1259
101	263	443	641	839	1049	1277
103	269	449	643	853	1051	1279
107	271	457	647	857	1061	1283
109	277	461	653	859	1063	1289
113	281	463	659	863	1069	1291

1297	1523	1741	1993	2221	2437	2689
1301	1531	1747	1997	2237	2441	2693
1303	1543	1753	1999	2239	2447	2699
1307	1549	1759	2003	2243	2459	2707
1319	1553	1777	2011	2251	2467	2711
1321	1559	1783	2017	2267	2473	2713
1327	1567	1787	2027	2269	2477	2719
1361	1571	1789	2029	2273	2503	2729
1367	1579	1801	2039	2281	2521	2731
1373	1583	1811	2053	2287	2531	2741
1381	1597	1823	2063	2293	2539	2749
1399	1601	1831	2069	2297	2543	2753
1409	1607	1847	2081	2309	2549	2767
1423	1609	1861	2083	2311	2551	2777
1427	1613	1867	2087	2333	2557	2789
1429	1619	1871	2089	2339	2579	2791
1433	1621	1873	2099	2341	2591	2797
1439	1627	1877	2111	2347	2593	2801
1447	1637	1879	2113	2351	2609	2803
1451	1657	1889	2129	2357	2617	2819
1453	1663	1901	2131	2371	2621	2833
1459	1667	1907	2137	2377	2633	2837
1471	1669	1913	2141	2381	2647	2843
1481	1693	1931	2143	2383	2657	2851
1483	1697	1933	2153	2389	2659	2857
1487	1699	1949	2161	2393	2663	2861
1489	1709	1951	2179	2399	2671	2879
1493	1721	1973	2203	2411	2677	2887
1499	1723	1979	2207	2417	2683	2897
1511	1733	1987	2213	2423	2687	2903

2909	3187	3433	3659	3911	4153	4421
2917	3191	3449	3671	3917	4157	4423
2927	3203	3457	3673	3919	4159	4441
2939	3209	3461	3677	3923	4177	4447
2953	3217	3463	3691	3929	4201	4451
2957	3221	3467	3697	3931	4211	4457
2963	3229	3469	3701	3943	4217	4463
2969	3251	3491	3709	3947	4219	4481
2971	3253	3499	3719	3967	4229	4483
2999	3257	3511	3727	3989	4231	4493
3001	3259	3517	3733	4001	4241	4507
3011	3271	3527	3739	4003	4243	4513
3019	3299	3529	3761	4007	4253	4517
3023	3301	3533	3767	4013	4259	4519
3037	3307	3539	3769	4019	4261	4523
3041	3313	3541	3779	4021	4271	4547
3049	3319	3547	3793	4027	4273	4549
3061	3323	3557	3797	4049	4283	4561
3067	3329	3559	3803	4051	4289	4567
3079	3331	3571	3821	4057	4297	4583
3083	3343	3581	3823	4073	4327	4591
3089	3347	3583	3833	4079	4337	4597
3109	3359	3593	3847	4091	4339	4603
3119	3361	3607	3851	4093	4349	4621
3121	3371	3613	3853	4099	4357	4637
3137	3373	3617	3863	4111	4363	4639
3163	3389	3623	3877	4127	4373	4643
3167	3391	3631	3881	4129	4391	4649
3169	3407	3637	3889	4133	4397	4651
3181	3413	3643	3907	4139	4409	4657

4663	4943	5189	5449	5701	5953
4673	4951	5197	5471	5711	5981
4679	4957	5209	5477	5717	5987
4691	4967	5227	5479	5737	
4703	4969	5231	5483	5741	
4721	4973	5233	5501	5743	
4723	4987	5237	5503	5749	
4729	4993	5261	5507	5779	
4733	4999	5273	5519	5783	
4751	5003	5279	5521	5791	
<hr/>					
4759	5009	5281	5527	5801	
4783	5011	5297	5531	5807	
4787	5021	5303	5557	5813	
4789	5023	5309	5563	5821	
4793	5039	5323	5569	5827	
4799	5051	5333	5573	5839	
4801	5059	5347	5581	5843	
4813	5077	5351	5591	5849	
4817	5081	5381	5623	5851	
4831	5087	5387	5639	5857	
<hr/>					
4861	5099	5393	5641	5861	
4871	5101	5399	5647	5867	
4877	5107	5407	5651	5869	
4889	5113	5413	5653	5879	
4903	5119	5417	5657	5881	
4909	5147	5419	5659	5897	
4919	5153	5431	5669	5903	
4931	5167	5437	5683	5923	
4933	5171	5441	5689	5927	
4937	5179	5443	5693	5939	



ТАБЛИЦЫ

ПЕРВООБРАЗНЫХЪ КОРНЕЙ И УКАЗАТЕЛЕЙ ДЛЯ ПРОСТЫХЪ МОДУЛЕЙ, НЕ ПРЕВОСХОДЯЩИХЪ 200.

ПРОСТОЕ ЧИСЛО 2.

Первообр. корень 2. Основание 2.

I.

N.	1	2
	0	1

N.

I.	0	1
	1	2

ПРОСТОЕ ЧИСЛО 5.

Первообразные корни: 2, 3.

Основание 2.

I.

N.	1	2	3	4
	0	1	3	2

N.

I.	0	1	2	3
	1	2	4	3

ПРОСТОЕ ЧИСЛО 7.

Первообразные корни: 3, 5.

Основание 3.

I.

N.	1	2	3	4	5	6
	0	2	1	4	5	3

N.

I.	0	1	2	3	4	5
	1	3	2	6	4	5

ПРОСТОЕ ЧИСЛО 11.

Первообразные корни: 2, 6, 7, 8.

Основание 6.

I.

N.	1	2	3	4	5	6	7	8	9	10
	0	1	8	2	4	9	7	3	6	5

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	2	4	8	5	10	9	7	3	6

ПРОСТОЕ ЧИСЛО 13.

Первообразные корни: 2, 6, 7, 11.

ОСНОВАНИЕ 6.

I.

N.

N	0	1	2	3	4	5	6	7	8	9
		0	5	8	10	9	1	7	3	4
1	2	11								

I.	0	1	2	3	4	5	6	7	8	9
		1	6	10	8	9	2	12	7	3
1	4	11								

ПРОСТОЕ ЧИСЛО 17.

Первообразные корни: 3, 5, 6, 7, 10, 11, 12, 14.

ОСНОВАНИЕ 10.

I.

N.

N.	0	1	2	3	4	5	6	7	8	9
		0	10	11	4	7	5	9	14	6
1	1	13	15	12	3	2	8			

I.	0	1	2	3	4	5	6	7	8	9
		1	10	15	14	4	6	9	5	16
1	2	3	13	11	8	12				

ПРОСТОЕ ЧИСЛО 19.

Первообразные корни: 2, 3, 10, 13, 14, 15.

ОСНОВАНИЕ 10.

I.

N.

N.	0	1	2	3	4	5	6	7	8	9
		0	17	5	16	2	4	12	15	10
1	1	6	3	13	11	7	14	8	9	

I.	0	1	2	3	4	5	6	7	8	9
		1	10	5	12	6	3	11	15	17
1	9	14	7	13	16	8	4	2		

ПРОСТОЕ ЧИСЛО 23.

Первообразные корни: 5, 7, 10, 11, 14, 15, 17, 19, 20, 21.

ОСНОВАНИЕ 10.

I.

N.

N.	0	1	2	3	4	5	6	7	8	9
0		0	8	20	16	15	6	21	2	18
1	1	3	14	12	7	13	10	17	4	5
2	9	19	11							

I.	0	1	2	3	4	5	6	7	8	9
0	1	10	8	11	18	19	6	14	2	20
1	16	22	13	15	12	5	4	17	9	21
2	3	7								

ПРОСТОЕ ЧИСЛО 29.

Первообр. корни: 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27.

ОСНОВАНИЕ 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	11	27	22	18	10	20	5	26
1	1	23	21	2	3	17	16	7	9	15
2	12	19	6	24	4	8	13	25	14	

N.

I.	0	1	2	3	4	5	6	7	8	9	
		1	10	13	14	24	8	22	17	25	18
1	6	2	20	26	28	19	16	15	5	21	
2	7	12	4	11	23	27	9	3			

ПРОСТОЕ ЧИСЛО 31.

Первообразные корни: 3, 11, 12, 13, 17, 21, 22, 24.

ОСНОВАНИЕ 17.

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	12	13	24	20	25	4	6	26
1	2	29	7	23	16	3	18	1	8	22
2	14	17	11	21	19	10	5	9	28	27
3	15									

N.

I.	0	1	2	3	4	5	6	7	8	9	
	0	1	17	10	15	7	26	8	12	18	27
1	25	22	2	3	20	30	14	21	16	24	
2	5	23	19	13	4	6	9	29	28	11	

ПРОСТОЕ ЧИСЛО 37.

Первообр. корни: 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35.

ОСНОВАНИЕ 5.

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	11	34	22	1	9	28	33	32
1	12	6	20	13	3	35	8	5	7	25
2	23	26	17	21	31	2	24	30	14	15
3	10	27	19	4	16	29	18			

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	5	25	14	33	17	11	18	16	6
1	30	2	10	13	28	29	34	22	36	32
2	12	23	4	20	26	19	21	31	7	35
3	27	24	9	8	3	15				

ПРОСТОЕ ЧИСЛО 41.

Первообразные корни: 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.

ОСНОВАНИЕ 6.

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

N.

I.	0	1	2	3	4	5	6	7	8	9	
		1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34	
2	40	35	5	30	16	14	2	12	31	22	
3	9	13	37	17	20	38	23	15	8	7	

ПРОСТОЕ ЧИСЛО 43.

Первообр. корни: 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34.

ОСНОВАНИЕ 28.

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	39	17	36	5	14	7	33	34
1	2	6	11	40	4	22	30	16	31	29
2	41	24	3	20	8	10	37	9	1	25
3	19	32	27	23	13	12	28	35	26	15
4	38	18	21							

N.

I.	0	1	2	3	4	5	6	7	8	9	
		1	28	10	22	14	5	11	7	24	27
1	25	12	35	34	6	39	17	3	41	30	
2	23	42	15	33	21	29	38	32	36	19	
3	16	18	31	8	9	37	4	26	40	2	
4	13	20									

ПРОСТОЕ ЧИСЛО 47.

Первообр. корни: 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45.

ОСНОВАНИЕ 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	30	18	14	17	2	38	44	36
1	1	27	32	3	22	35	28	42	20	29
2	31	10	11	39	16	34	33	8	6	43
3	19	5	12	45	26	9	4	24	13	21
4	15	25	40	37	41	7	23			

N.

N.	0	1	2	3	4	5	6	7	8	9	
		1	10	6	13	36	31	28	45	27	35
1	21	22	32	38	4	40	24	5	3	30	
2	18	39	14	46	37	41	34	11	16	19	
3	2	20	12	26	25	15	9	43	7	23	
4	42	44	17	29	8	33					

ПРОСТОЕ ЧИСЛО 53.

Первообразные корни: 2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22;
26, 27, 31, 32, 33, 34, 35, 39, 41, 45,
48, 50, 51.

ОСНОВАНИЕ 26.

I.

N.	0	1	2	3	4	5	6	7	8	9
0		0	25	9	50	31	34	38	23	18
1	4	46	7	28	11	40	48	42	43	41
2	29	47	19	39	32	10	1	27	36	6
3	13	45	21	3	15	17	16	22	14	37
4	2	33	20	30	44	49	12	8	5	24
5	35	51	26							

N.

I.	0	1	2	3	4	5	6	7	8	9
0	1	26	40	33	10	48	29	12	47	3
1	25	14	46	30	38	34	36	35	9	22
2	42	32	37	8	49	2	52	27	13	20
3	43	5	24	41	6	50	28	39	7	23
4	15	19	17	18	44	31	11	21	16	45
5	4	51								

ПРОСТОЕ ЧИСЛО 59.

Первообразные корни: 2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30,
31, 32, 33, 34, 37, 38, 39, 40, 42, 43,
44, 47, 50, 52, 54, 55, 57.

ОСНОВАНИЕ 10.

I.

N	0	1	2	3	4	5	6	7	8	9
0		0	25	32	50	34	57	44	17	6
1	1	45	24	23	11	8	42	14	31	22
2	26	18	12	27	49	10	48	38	36	4
3	33	7	9	19	39	20	56	41	47	55
4	51	2	43	13	37	40	52	53	16	30
5	35	46	15	28	5	21	3	54	29	

N.

I.	0	1	2	3	4	5	6	7	8	9
0	1	10	41	56	29	54	9	31	15	32
1	25	14	22	43	17	52	48	8	21	33
2	35	55	19	13	12	2	20	23	53	58
3	49	18	3	30	5	50	28	44	27	34
4	45	37	16	42	7	11	51	38	26	24
5	4	40	46	47	57	39	36	6		

ПРОСТОЕ ЧИСЛО 61.

Первообр. корни: 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59.

ОСНОВАНИЕ 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	47	42	34	14	29	23	21	24
1	1	45	16	20	10	56	8	49	11	22
2	48	5	32	39	3	28	7	6	57	25
3	43	13	55	27	36	37	58	33	9	2
4	35	18	52	41	19	38	26	40	50	46
5	15	31	54	51	53	59	44	4	12	17
6	30									

N.

I.	0	1	2	3	4	5	6	7	8	9	
		1	10	39	24	57	21	27	26	16	38
1	14	18	58	31	5	50	12	59	41	44	
2	13	8	19	7	9	29	46	33	25	6	
3	60	51	22	37	4	40	34	35	45	23	
4	47	43	3	30	56	11	49	2	20	17	
5	48	53	42	54	52	32	15	28	36	55	

ПРОСТОЕ ЧИСЛО 67.

Первообр. корни: 2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63.

ОСНОВАНИЕ 12.

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	29	9	58	39	38	7	21	18
1	2	61	1	23	36	48	50	8	47	26
2	31	16	24	20	30	12	52	27	65	22
3	11	43	13	4	37	46	10	44	55	32
4	60	19	45	63	53	57	49	64	59	14
5	41	17	15	3	56	34	28	35	51	54
6	40	5	6	25	42	62	33			

N.

I.	0	1	2	3	4	5	6	7	8	9	
		1	12	10	53	33	61	62	7	17	3
1	36	30	25	32	49	52	21	51	9	41	
2	23	8	29	13	22	63	19	27	56	2	
3	24	20	39	66	55	57	14	34	6	5	
4	60	50	64	31	37	42	35	38	15	46	
5	16	58	26	44	59	38	54	45	4	48	
6	40	11	65	43	47	28					

ПРОСТОЕ ЧИСЛО 71.

Первообразные корни: 7, 11, 13, 21, 22, 28, 31, 33, 25, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69.

ОСНОВАНИЕ 62.

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	58	18	46	14	6	33	34	36
1	2	43	64	27	21	32	15	7	24	38
2	60	51	31	5	52	28	22	54	9	4
3	20	13	10	61	65	47	12	30	26	45
4	48	55	39	44	19	50	63	17	40	66
5	16	25	3	59	42	57	67	56	62	29
6	8	37	1	69	68	41	49	11	53	23
7	35									

N.

I.	0	1	2	3	4	5	6	7	8	9	
		1	62	10	52	29	23	6	17	60	28
1	32	67	36	31	5	26	50	47	3	44	
2	30	14	16	69	18	51	38	13	25	59	
3	37	22	15	7	8	70	9	61	19	42	
4	48	65	54	11	43	39	4	35	40	66	
5	45	21	24	68	27	41	57	55	2	53	
6	20	33	58	46	12	34	49	56	64	63	

ПРОСТОЕ ЧИСЛО 73.

Первообразные корни: 5, 11, 13, 14, 15, 20, 26, 28, 29, 31, 33, 34, 39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68.

ОСНОВАНИЕ 5.

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

N.

I.	0	1	2	3	4	5	6	7	8	9	
		1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62	
2	18	17	12	60	8	40	54	51	36	34	
3	24	47	16	7	35	29	72	68	48	21	
4	32	14	70	58	71	63	23	42	64	28	
5	67	43	69	53	46	11	55	56	61	13	
6	65	33	19	22	37	39	49	26	57	66	
7	38	44									

ПРОСТОЕ ЧИСЛО 79.

Первообразные корни: 3, 6, 7, 28, 29, 30, 34, 35, 37, 39, 43,
47, 48, 53, 54, 59, 60, 63, 66, 68, 70,
74, 75, 77.

ОСНОВАНИЕ 29.

I.

N	0	1	2	3	4	5	6	7	8	9
	0	50	71	22	34	43	19	72	64	
1	6	70	15	74	69	27	44	9	36	10
2	56	12	42	52	65	68	46	57	41	1
3	77	76	16	63	59	53	8	23	60	67
4	28	21	62	47	14	20	24	55	37	38
5	40	2	18	7	29	26	13	3	51	17
6	49	75	48	5	66	30	35	54	31	45
7	25	33	58	4	73	61	32	11	39	

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	29	51	57	73	63	10	53	36	17
1	19	77	21	56	44	12	32	59	52	7
2	45	41	4	37	46	70	55	15	40	54
3	65	68	76	71	5	66	18	48	49	78
4	50	28	22	6	16	69	26	43	62	60
5	2	58	23	35	67	47	20	27	72	34
6	38	75	42	33	9	24	64	39	25	14
7	11	3	8	74	13	61	31	30		

ПРОСТОЕ ЧИСЛО 83.

Первообразные корни: 2, 5, 6, 8, 13, 14, 15, 18, 19, 20,
22, 24, 32, 34, 35, 39, 42, 43, 45, 46,
47, 50, 52, 53, 54, 55, 56, 57, 58, 60,
62, 66, 67, 71, 72, 73, 74, 76, 79, 80.

ОСНОВАНИЕ 50.

I.

N.	0	1	2	3	4	5	6	7	8	9
	0	3	52	6	81	55	24	9	22	
1	2	72	58	67	27	51	12	4	25	59
2	5	76	75	16	61	8	70	74	30	36
3	54	32	15	42	7	23	28	60	62	37
4	8	38	79	49	78	21	19	69	64	48
5	1	56	73	13	77	71	33	29	39	20
6	57	34	35	46	18	66	45	53	10	68
7	26	17	31	43	63	50	65	14	40	47
8	11	44	41							

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	50	10	2	17	20	4	34	40	8
1	68	80	16	53	77	32	23	71	64	46
2	59	45	9	35	7	18	70	14	36	57
3	28	72	31	56	61	62	29	39	41	58
4	78	82	33	73	81	66	63	79	49	43
5	75	15	3	67	30	6	51	60	12	19
6	37	24	38	74	48	76	65	13	69	47
7	26	55	11	52	27	22	21	54	44	42
8	25	5								

ПРОСТОЕ ЧИСЛО 89.

Первообразные корни: 3, 6, 7, 13, 14, 15, 19, 23, 24, 26, 27, 28, 29, 30, 31, 33, 35, 38, 41, 43, 46, 48, 51, 54, 56, 58, 59, 60, 61, 62, 63, 65, 66, 70, 74, 75, 76, 82, 83, 86.

ОСНОВАНИЕ 30.

I.

N.

N.	0	1	2	3	4	5	6	7	8	9
		0	72	87	56	18	71	7	40	86
1	2	4	55	65	79	17	24	82	70	53
2	74	6	76	31	39	36	49	85	63	29
3	1	57	8	3	66	25	54	77	37	64
4	58	67	78	59	60	16	15	34	23	14
5	20	81	33	10	69	22	47	52	13	45
6	73	19	41	5	80	83	75	32	50	30
7	9	26	38	68	61	35	21	11	48	46
8	42	84	51	27	62	12	43	28	44	

I.	0	1	2	3	4	5	6	7	8	9	
		1	30	10	33	11	63	21	7	32	70
1	53	77	85	58	49	46	45	15	5	61	
2	50	76	55	48	16	35	71	83	87	29	
3	69	23	67	52	47	75	25	38	72	24	
4	8	62	80	86	88	59	79	56	78	26	
5	68	82	57	19	36	12	4	31	40	43	
6	44	74	84	28	39	13	34	41	73	54	
7	18	6	2	60	20	66	22	37	42	14	
8	64	51	17	65	81	27	9	3			

ПРОСТОЕ ЧИСЛО 97.

Первообразные корни: 5, 7, 10, 13, 14, 15, 17, 21, 23, 26, 29, 37, 38, 39, 40, 41, 56, 57, 58, 59, 60, 68, 71, 74, 76, 80, 82, 83, 84, 87, 90, 92.

ОСНОВАНИЕ 10.

I.

N.

N.	0	1	2	3	4	5	6	7	8	9
		0	86	2	76	11	88	53	66	4
1	1	82	78	83	43	13	56	19	90	27
2	87	55	72	79	68	22	73	6	33	47
3	3	26	46	84	9	64	80	41	17	85
4	77	71	45	44	62	15	69	60	58	10
5	12	21	63	14	92	93	23	29	37	65
6	89	32	16	57	36	94	74	51	95	81
7	54	25	70	20	31	24	7	39	75	42
8	67	8	61	91	35	30	34	49	52	18
9	5	40	59	28	50	38	48			

I.	0	1	2	3	4	5	6	7	8	9	
		1	10	3	30	9	90	27	76	81	34
1	49	5	50	15	53	45	62	38	89	17	
2	73	51	25	56	75	71	31	19	93	57	
3	85	74	61	28	86	84	64	58	95	77	
4	91	37	79	14	43	42	32	29	96	87	
5	94	67	88	7	70	21	16	63	48	92	
6	47	82	44	52	35	59	8	80	24	46	
7	72	41	22	26	66	78	4	40	12	23	
8	36	69	11	13	33	39	2	20	6	60	
9	18	83	54	55	65	68					

ПРОСТОЕ ЧИСЛО 101.

Первообразные корни: 2, 3, 7, 8, 11, 12, 15, 18, 26, 27, 28, 29, 34, 35, 38, 40, 42, 46, 48, 50, 51, 53, 55, 59, 61, 63, 66, 67, 72, 73, 74, 75, 83, 86, 89, 90, 93, 94, 98, 99.

ОСНОВАНИЕ 2.

I. *у доброт. по дроби. числитель.* N.

N	0	1	2	3	4	5	6	7	8	9
1	25	13	71	66	2	24	70	9	3	38
2	26	78	14	86	72	48	67	7	11	91
3	94	84	5	82	31	33	40	56	97	35
4	27	45	79	42	15	62	87	58	73	18
5	49	99	68	23	8	37	12	65	92	29
6	95	77	85	47	6	90	83	81	32	55
7	34	44	41	61	57	17	98	22	36	64
8	28	76	46	89	80	54	43	60	16	21
9	63	75	88	53	59	20	74	52	19	51
10	50									

I.	0	1	2	3	4	5	6	7	8	9
1	1	2	4	8	16	32	64	27	54	7
2	14	28	56	11	22	44	88	75	49	98
3	17	34	68	35	70	39	78	55	9	18
4	36	72	43	86	71	41	82	63	25	50
5	100	99	97	93	85	69	37	74	47	94
6	87	73	45	90	79	57	13	26	52	3
7	6	12	24	48	96	91	81	61	21	42
8	84	67	33	66	31	62	23	46	92	83
9	65	29	58	15	30	60	19	38	76	51

ПРОСТОЕ ЧИСЛО 103.

Первообразные корни: 5, 6, 11, 12, 20, 21, 35, 40, 43, 44, 45, 48, 51, 53, 54, 62, 65, 67, 70, 71, 74, 75, 77, 78, 84, 85, 86, 87, 88, 96, 99, 101.

ОСНОВАНИЕ 6.

I.

N.	0	1	2	3	4	5	6	7	8	9
1	3	29	47	66	78	14	82	50	58	28
2	49	89	75	90	93	16	10	69	22	76
3	60	99	26	86	96	91	2	81	74	21
4	95	94	33	55	19	71	34	17	37	64
5	62	5	56	11	13	88	68	85	20	70
6	4	84	43	44	72	23	30	53	40	45
7	35	77	48	9	25	73	18	61	67	42
8	39	24	38	100	79	7	101	31	65	27
9	15	98	80	54	63	87	83	52	8	41
10	6	97	51							

N.

I.	0	1	2	3	4	5	6	7	8	9
1	1	6	36	10	60	51	100	85	98	73
2	26	53	9	54	15	90	25	47	76	44
3	58	39	28	65	81	74	32	89	19	11
4	66	87	7	42	46	70	8	48	82	80
5	68	99	79	62	63	69	2	12	72	20
6	17	102	97	67	93	43	52	3	18	5
7	30	77	50	94	49	88	13	78	56	27
8	59	45	64	75	38	22	29	71	14	84
9	92	37	16	96	61	57	33	95	55	21
10	23	35	4	24	41	40	34	101	91	31
	83	86								

ПРОСТОЕ ЧИСЛО 107.

Первообразные корни: 2, 5, 6, 7, 8, 15, 17, 18, 20, 21, 22, 24, 26, 28, 31, 32, 38, 43, 45, 46, 50, 51, 54, 55, 58, 59, 60, 63, 65, 66, 67, 68, 70, 71, 72, 73, 74, 77, 78, 80, 82, 84, 88, 91, 93, 94, 95, 96, 97, 98, 103, 104.

ОСНОВАНИЕ 63.

I.

N.	0	1	2	3	4	5	6	7	8	9
1	0	76	56	78	84	13	67	57	73	50
2	2	97	29	63	45	26	47	22	35	72
3	80	21	51	48	94	70	28	6	85	30
4	86	90	18	93	54	63	49	16	34	8
5	15	77	36	64	11	89	24	68	61	87
6	69	102	10	1	40	71	37	33	83	32
7	59	81	17	41	101	104	74	27	19	88
8	75	100	79	98	7	12	82	44	43	92
9	52	9	38	99	5	3	23	55	103	20
10	4	14	66	31	25	42	53			

N.

I.	0	1	2	3	4	5	6	7	8	9
1	1	63	10	95	100	94	37	84	49	91
2	2	99	31	27	96	56	104	25	77	36
3	3	39	103	69	67	48	28	52	66	92
4	4	64	73	105	88	87	24	14	26	33
5	5	9	32	90	106	44	97	12	7	13
6	6	23	58	16	45	53	22	102	6	57
7	7	35	65	29	8	76	80	11	51	3
8	8	30	71	86	68	4	38	40	59	79
9	9	41	15	89	43	34	2	19	20	83
10	10	81	74	61	98	75	17			

ПРОСТОЕ ЧИСЛО 109.

Первообразные корни: 6, 10, 11, 13, 14, 18, 24, 30, 37, 39, 40, 42, 44, 47, 50, 51, 52, 53, 56, 57, 58, 59, 62, 65, 67, 69, 70, 72, 79, 85, 91, 95, 96, 98, 99, 103.

ОСНОВАНИЕ 10.

I.

N	0	1	2	3	4	5	6	7	8	9	
1	1	107	106	93	28	78	16	13	88	63	56
2	94	8	92	105	73	44	48	48	21	41	3
3	29	74	33	27	105	32	100	84	58	10	10
4	79	45	101	66	6	104	26	65	96	35	35
5	17	49	85	97	77	72	90	5	76	68	68
6	14	22	59	36	69	15	43	31	103	71	71
7	89	42	11	80	18	23	12	47	99	25	25
8	64	4	30	46	50	60	81	87	20	83	83
9	57	95	75	102	86	37	51	38	62	40	40
10	2	9	34	67	98	19	61	52	53	55	55
					70	24	82	39	54		

N.

I.	0	1	2	3	4	5	6	7	8	9
1	1	10	100	19	81	47	34	13	21	101
2	29	72	66	6	60	55	5	50	64	95
3	78	17	61	65	105	69	36	33	3	30
4	82	57	25	32	102	39	63	85	87	107
5	89	18	71	56	15	41	83	67	16	51
6	74	86	97	98	108	99	9	90	28	62
7	75	96	88	8	80	37	43	103	49	54
8	104	59	45	14	31	92	48	44	4	40
9	73	76	106	79	27	52	84	77	7	70
10	46	24	22	2	20	91	38	53	94	68
	26	42	93	58	35	23	12	11		

ПРОСТОЕ ЧИСЛО 113.

Первообразные корни: 3, 5, 6, 10, 12, 17, 19, 20, 21, 23, 24, 27, 29, 33, 34, 37, 38, 39, 43, 45, 46, 47, 54, 55, 58, 59, 66, 67, 68, 70, 74, 75, 76, 79, 80, 84, 86, 89, 90, 92, 93, 94, 96, 101, 103, 107, 108, 110.

ОСНОВАНИЕ 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
1	1	0	52	79	104	61	19	72	44	46
2	4	22	71	58	12	28	96	59	98	93
3	5	39	74	103	11	10	110	13	64	87
4	6	80	30	36	101	111	21	38	29	33
5	7	105	34	91	17	14	107	43	97	63
6	8	62	26	50	76	65	83	4	60	27
7	9	20	106	82	6	88	7	41	99	51
8	10	73	35	90	49	81	89	85	94	77
9	11	45	92	86	24	31	8	69	54	66
10	12	47	18	95	109	37	42	3	40	84
11	13	2	15	78	57	102	100	16	75	5
12	14	23	108	56						48

N.

I.	0	1	2	3	4	5	6	7	8	9
1	1	10	100	96	56	108	63	65	85	59
2	2	25	14	27	44	101	106	43	91	6
3	3	60	35	11	110	83	39	51	58	45
4	4	31	84	49	38	41	71	32	94	36
5	5	97	66	95	46	8	80	9	90	109
6	6	52	68	2	20	87	79	112	103	13
7	7	57	5	50	48	28	54	88	89	99
8	8	69	12	7	70	22	107	53	78	102
9	9	30	74	62	55	98	76	82	29	64
10	10	72	42	81	19	77	92	16	47	18
11	11	105	33	104	23	4	61	45	111	93
12	12	26	34							

ПРСТОЕ ЧИСЛО 127.

Первообразные корни: 3, 6, 7, 12, 14, 23, 29, 39, 43, 45, 46, 48, 53, 55, 56, 57, 58, 65, 67, 78, 83, 85, 86, 91, 92, 93, 96, 97, 101, 106, 109, 110, 112, 114, 116, 118.

I.

ОСНОВАНИЕ 109.

N.	0	1	2	3	4	5	6	7	8	9
1	3	52	59	20	47	111	41	125	54	46
2	21	22	70	11	77	96	38	69	35	79
3	26	50	90	75	10	110	82	112	60	43
4	39	76	40	121	88	31	29	120	95	124
5	114	15	56	67	87	37	53	65	97	91
6	44	30	68	45	108	5	93	107	28	34
7	2	116	100	24	4	119	78	51	61	32
8	57	92	94	25	58	103	13	102	106	123
9	49	19	47	73	12	27	113	89	16	98
10	6	101	33	14	74	7	85	84	105	1
11	55	9	71	80	83	122	115	66	109	117
12	62	104	48	99	86	81	63			

N.

I.	0	1	2	3	4	5	6	7	8	9
1	1	109	70	10	74	65	100	105	15	111
2	34	23	94	86	103	51	98	14	2	91
3	13	20	21	3	73	83	30	95	68	46
4	61	45	79	102	69	28	4	55	26	40
5	42	6	19	39	60	63	9	92	122	90
6	31	77	11	56	8	110	52	80	84	12
7	38	78	120	126	18	57	117	53	62	27
8	22	112	16	93	104	33	41	24	76	29
9	113	125	36	114	107	106	124	54	44	97
10	32	59	81	66	82	48	25	58	99	123
11	72	101	87	85	121	107	88	67	64	118
12	47	43	115	89	49	7	31	119	17	75

ПРОСТОЕ ЧИСЛО 131

Первообразные корни: 2, 6, 8, 10, 14, 17, 22, 23, 26, 29, 30, 31, 37, 40, 50, 54, 56, 57, 66, 67, 72, 76, 82, 83, 85, 87, 88, 90, 93, 95, 96, 97, 98, 103, 104, 106, 110, 111, 115, 116, 118, 119, 120, 122, 124, 126, 127, 128.

ОСНОВАНИЕ 10.

I.

N

N.	0	1	2	3	4	5	6	7	8	9
1	1	98	32	64	121	44	72	59	75	122
2	84	34	51	89	145	96	17	118	74	73
3	127	67	25	94	12	86	28	23	128	60
4	37	58	117	22	4	40	42	5	68	76
5	49	55	100	78	71	16	27	41	26	46
6	80	104	20	30	108	112	47	43	95	85
7	39	15	111	91	106	92	81	6	13	35
8	120	114	11	3	70	107	105	69	87	52
9	123	102	125	63	88	93	21	77	29	90
10	2	62	8	9	53	82	31	50	24	116
11	99	19	110	10	124	7	109	56	129	97
12	33	66	57	54	103	44	113	101	61	18
13	65									

I.	0	1	2	3	4	5	6	7	8	9
1	1	10	100	83	44	47	77	115	102	103
1	113	82	34	78	125	71	55	26	129	141
2	62	96	43	37	108	32	58	56	36	98
3	63	106	12	120	21	76	4	40	7	70
4	45	57	46	67	15	19	59	66	5	50
5	107	22	89	104	123	51	117	122	41	17
6	39	128	101	93	13	130	121	31	48	87
7	84	54	16	29	28	18	49	97	53	6
8	60	76	105	2	20	69	35	88	94	23
9	99	73	75	95	33	68	25	119	11	110
10	52	127	91	124	61	86	74	85	64	116
11	112	72	65	126	81	24	109	42	27	8
12	80	14	9	90	114	92	3	30	38	118

ПРОСТОЕ ЧИСЛО 137.

Первообразные корни: 3, 5, 6, 12, 13, 20, 21, 23, 24, 26, 27, 29, 31, 33, 35, 40, 42, 43, 45, 46, 47, 48, 51, 52, 53, 54, 55, 57, 58, 62, 66, 67, 70, 71, 75, 79, 80, 82, 83, 84, 85, 86, 89, 90, 94, 92, 94, 95, 97, 102, 104, 106, 108, 110, 111, 113, 114, 116, 117, 124, 125, 131, 132, 134.

I.

Основание 12.

N.	0	1	2	3	4	5	6	7	8	9
1	17	90	4	53	132	36	112	86	20	54
2	11	15	84	129	131	46	47	39	126	95
3	30	133	106	103	80	25	14	102	48	66
4	5	51	9	37	78	49	123	141	125	4
5	40	99	41	71	33	113	120	67	89	128
6	24	110	127	28	100	76	97	87	74	6
7	19	29	8	32	96	59	42	92	60	21
8	135	52	45	101	3	109	31	108	72	57
9	43	55	117	10	105	77	119	73	134	116
10	34	82	93	12	35	38	65	98	27	58
11	107	115	114	63	61	16	83	79	122	88
12	18	44	104	64	121	69	22	85	94	50
13	70	75	91	56	81	62	68			

N.

I.	0	1	2	3	4	5	6	7	8	9
1	93	20	103	3	36	21	115	10	120	70
2	18	79	126	5	60	35	9	108	63	71
3	30	86	73	54	100	104	15	43	105	27
4	50	52	76	90	121	82	25	26	38	45
5	129	41	81	13	19	91	133	89	109	75
6	78	114	135	113	123	106	39	57	136	125
7	130	53	88	97	68	131	65	95	44	117
8	34	134	101	116	22	127	17	67	119	58
9	11	132	77	102	128	29	74	66	107	51
10	64	83	37	33	122	94	32	110	88	85
11	61	47	16	55	112	111	99	92	8	96
12	56	124	118	46	4	48	28	62	59	23
13	2	24	14	31	98	80				

ПРОСТОЕ ЧИСЛО 139.

Первообразные корни: 2, 3, 12, 15, 17, 18, 19, 21, 22, 26, 32, 40, 50, 53, 56, 58, 61, 68, 70, 72, 73, 85, 88, 90, 92, 93, 98, 101, 102, 104, 108, 109, 110, 111, 114, 115, 119, 123, 126, 128, 130, 132, 134, 135.

ОСНОВАНИЕ 92.

I.

N.

N.	0	1	2	3	4	5	6	7	8	9
1	3	74	119	49	100	22	30	46	81	98
2	122	65	55	26	135	71	62	37	79	83
3	52	40	43	123	18	44	7	116	8	8
4	103	82	46	23	36	38	60	136	64	75
5	25	86	126	73	128	120	20	70	111	32
6	33	125	21	114	24	96	97	132	127	15
7	19	68	41	35	117	48	104	110	137	88
8	84	58	63	28	27	93	45	90	56	102
9	101	42	1	89	51	59	4	57	17	94
10	6	133	67	129	107	105	92	115	13	34
11	77	47	78	76	113	87	54	112	109	121
12	14	10	106	131	2	61	108	124	134	53
13	29	12	85	99	91	66	95	80	5	72
						31	118	50	69	

I.	0	1	2	3	4	5	6	7	8	9
1	1	92	124	10	86	128	100	26	29	27
	121	12	131	98	120	59	7	88	34	70
	46	62	5	43	64	50	13	84	83	130
	6	135	49	60	99	73	44	17	35	23
	31	72	91	32	25	76	42	111	65	3
	137	94	30	119	106	22	78	87	81	85
	36	115	16	82	38	21	125	102	71	138
	47	15	129	53	11	39	113	110	112	18
	127	8	41	19	80	132	51	105	69	93
	77	134	96	75	89	126	55	56	9	133
	4	90	79	40	66	95	122	104	116	108
	67	48	107	114	63	97	28	74	136	2
	45	109	20	33	117	61	52	58	54	103
	24	123	57	101	118	14	37	68		

ПРОСТОЕ ЧИСЛО 149.

Первообразные корни: 2, 3, 8, 10, 11, 12, 13, 14, 15, 18, 21, 23, 27, 32, 34, 38, 40, 41, 43, 48, 50, 51, 52, 55, 56, 57, 58, 59, 60, 62, 65, 66, 70, 71, 72, 74, 75, 77, 78, 79, 83, 84, 87, 89, 90, 91, 92, 93, 94, 97, 98, 99, 101, 106, 108, 09, 11, 115, 117, 122, 126, 128, 131, 134, 135, 136, 137, 138, 139, 141, 146, 147.

ОСНОВАНИЕ 10.

N.

I.

N.	0	1	2	3	4	5	6	7	8	9
1	1	10	100	106	17	21	61	14	140	59
2	143	89	145	109	47	23	81	65	54	93
3	36	62	24	91	16	11	110	57	123	38
4	82	75	5	50	53	83	85	105	7	70
5	404	146	119	147	129	98	86	115	107	27
6	521	18	31	12	120	8	80	55	103	136
7	619	41	112	77	25	101	116	117	127	78
8	735	52	73	134	148	139	49	43	132	128
9	888	135	9	90	6	60	4	40	102	126
10	968	84	95	56	113	87	125	58	133	138
11	1039	92	26	111	67	74	144	99	96	66
12	1164	44	142	79	45	3	30	2	20	51
13	1263	34	42	122	28	131	118	137	29	141
14	1369	94	46	13	130	108	37	72	124	48
15	1433	32	22	71	114	97	76	15		

N.	0	1	2	3	4	5	6	7	8	9
1	1	10	100	115	86	32	84	38	55	82
2	118	5	53	133	7	147	24	4	51	60
3	116	52	141	140	121	70	102	49	124	128
4	87	61	122	77	111	114	132	14	139	76
5	33	119	71	34	18	57	93	27	97	9
6	85	6	21	120	110	17	109	104	90	130
7	39	143	137	72	105	31	146	63	69	113
8	56	16	30	35	91	36	46	95	80	11
9	83	23	101	19	131	92	108	145	45	107
10	2	65	88	58	40	37	3	48	135	13
11	26	103	62	94	144	47	66	67	126	42
12	54	50	123	28	138	96	89	68	79	44
13	134	125	78	98	73	81	59	127	99	75
14	8	129	112	10	106	12	41	43	74	

ПРОСТОЕ ЧИСЛО 151.

Первообразные корни: 6, 7, 12, 13, 14, 15, 30, 35, 48, 54, 52, 54, 56, 64, 63, 71, 77, 82, 89, 93, 96, 102, 104, 106, 108, 109, 111, 112, 114, 115, 117, 120, 126, 129, 130, 133, 134, 140, 144, 146.

ОСНОВАНИЕ 114.

I.

N.	0	1	2	3	4	5	6	7	8	9
1	2	34	70	141	140	82	61	37	60	132
2	72	28	131	101	107	73	130	88	52	90
3	43	58	50	115	51	14	21	123	27	54
4	142	111	98	25	8	119	122	76	10	92
5	84	79	91	38	24	64	35	86	121	74
6	63	59	128	43	116	97	81	124	30	70
7	39	137	42	87	146	5	80	71	12	117
8	62	114	31	3	18	20	108	45	94	53
9	134	138	105	49	6	22	41	118	144	16
10	4	9	149	46	11	110	139	99	113	23
11	36	67	17	85	1	47	44	83	100	125
12	133	68	129	102	48	96	89	126	40	29
13	103	147	15	127	13	55	148	32	26	56
14	109	77	57	135	112	136	7	65	66	145
15	75									

N.

I.	0	1	2	3	4	5	6	7	8	9
1	1	114	10	83	100	75	94	146	34	101
2	38	104	78	134	25	132	99	112	84	63
3	85	26	95	109	44	33	138	28	21	129
4	59	82	137	65	11	46	110	7	43	70
5	128	96	72	54	116	87	103	115	124	93
6	32	24	18	89	29	135	139	142	31	61
7	8	6	80	60	45	147	148	111	121	53
8	76	57	5	15	49	150	37	141	68	51
9	19	52	39	67	88	66	125	56	42	107
10	118	13	123	130	22	92	69	14	86	140
11	105	41	144	108	81	23	55	79	97	35
12	64	48	36	27	58	119	127	133	62	122
13	16	12	9	120	90	143	145	71	91	106
14	4	3	40	30	98	149	74	131	136	102

ПРОСТОЕ ЧИСЛО 157.

Первообразные корни: 5, 6, 15, 18, 20, 21, 24, 26, 34, 38, 43, 53, 55, 60, 61, 62, 63, 66, 69, 70, 72, 73, 74, 77, 80, 83, 84, 85, 87, 88, 91, 94, 95, 96, 97, 102, 104, 114, 119, 123, 131, 133, 136, 137, 139, 142, 151, 152.

ОСНОВАНИЕ 139.

I.

N.

N.	0	1	2	3	4	5	6	7	8	9
1	2	152	104	122	138	11	113	57	129	88
2	149	23	143	81	95	22	121	54	39	116
3	124	58	111	118	119	68	70	28	107	96
4	140	75	14	151	134	99	72	76	86	114
5	13	94	112	25	45	7	30	82	6	27
6	115	155	49	145	102	141	109	12	110	47
7	59	64	61	83	19	144	98	53	87	9
8	131	20	66	97	5	139	142	137	125	32
9	90	31	63	24	67	127	77	37	105	84
10	4	108	85	123	103	34	16	91	36	8
11	154	150	21	56	73	92	153	62	18	29
12	106	148	146	41	40	33	136	46	93	117
13	132	43	100	17	3	65	101	71	38	1
14	50	42	55	126	52	26	74	80	10	51
15	135	35	89	60	44	69	78			

I.	0	1	2	3	4	5	6	7	8	9
1	1	139	10	134	100	84	58	55	109	79
2	148	5	67	50	42	29	106	133	118	74
3	81	142	25	21	93	53	145	59	37	119
4	56	91	89	125	105	151	108	97	138	28
5	124	123	141	131	154	54	127	69	14	62
6	140	149	144	77	27	142	113	7	31	70
7	153	72	117	92	71	135	82	94	35	155
8	36	137	46	114	146	41	47	96	156	18
9	147	23	57	73	99	102	48	78	9	152
10	90	107	115	128	51	24	39	83	76	45
11	132	136	64	104	12	98	120	38	101	66
12	68	32	52	6	49	60	19	129	33	34
13	16	26	3	103	30	88	143	95	17	8
14	13	80	130	15	44	150	126	87	4	85
15	40	65	86	22	75	63	122	2	121,	20
16	111	43	11	116	110	61				

ПРОСТОЕ ЧИСЛО 163.

Первообразные корни: 2, 3, 7, 11, 12, 18, 19, 20, 29, 32, 42, 44, 45, 50, 52, 63, 66, 67, 68, 70, 72, 73, 75, 76, 79, 80, 82, 89, 92, 94, 101, 103, 106, 107, 108, 109, 112, 114, 116, 117, 120, 122, 124, 128, 129, 130, 137, 139, 147, 148, 149, 153, 154, 159.

ОСНОВАНИЕ 70.

N.

I.

N.	0	1	2	3	4	5	6	7	8	9
1	2	97	23	6	142	93	114	161	51	86
2	73	42	136	153	70	136	122	159	157	127
3	45	39	31	140	68	92	66	75	36	100
4	144	20	143	106	77	17	62	44	3	160
5	95	40	37	18	38	28	50	8	54	27
6	116	30	110	85	102	150	49	155	139	34
7	1	52	137	7	146	67	107	96	9	103
8	53	40	91	134	22	90	15	26	148	65
9	88	56	133	82	115	58	74	130	69	21
10	4	29	111	35	108	135	89	131	109	119
11	99	118	121	14	79	84	125	143	98	158
12	25	32	101	63	19	117	156	147	11	149
13	59	112	120	126	64	60	48	47	105	13
14	72	87	123	134	46	76	78	41	55	151
15	138	104	16	83	5	132	80	33	12	61
16	124	152	81							

I.	0	1	2	3	4	5	6	7	8	9
1	1	70	10	48	100	154	22	73	57	78
1	81	128	158	139	113	86	152	45	53	124
2	41	99	84	12	25	120	87	59	55	101
3	61	32	121	157	69	103	38	52	54	31
4	51	147	21	3	47	30	144	137	136	66
5	56	8	71	80	58	148	91	13	95	130
6	135	159	46	123	134	89	36	75	34	98
7	14	2	140	20	96	37	145	44	146	114
8	156	162	93	153	115	63	9	141	90	106
9	85	82	35	5	24	50	77	11	148	110
10	39	122	64	79	151	138	43	76	104	108
11	62	102	131	42	6	94	60	125	111	109
12	132	112	16	142	160	116	133	19	26	27
13	97	107	155	92	83	105	15	72	150	68
14	33	28	4	117	40	29	74	127	88	129
15	65	149	161	23	143	67	126	18	119	17
16	49	7								

ПРОСТОЕ ЧИСЛО 167.

Первообразные корни: 5, 10, 13, 15, 17, 20, 23, 26, 30, 34, 35, 37, 39, 40, 44, 43, 45, 46, 51, 52, 53, 55, 59, 60, 67, 68, 69, 70, 71, 73, 74, 78, 79, 80, 82, 83, 86, 90, 91, 92, 95, 101, 102, 103, 104, 105, 106, 109, 110, 111, 113, 117, 118, 119, 120, 123, 125, 129, 131, 134, 135, 136, 138, 139, 140, 142, 143, 145, 146, 148, 149, 151, 153, 155, 156, 158, 159, 160, 161, 163, 164, 165.

N.

ОСНОВАНИЕ 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
1	1	10	100	165	147	134	4	40	66	159
2	87	35	16	160	97	135	14	140	64	139
3	54	39	56	59	89	55	49	156	57	69
4	22	53	29	123	61	109	88	45	116	158
5	77	102	48	13	130	131	144	74	172	52
6	150	164	137	34	6	60	99	155	47	136
7	24	73	62	119	21	43	96	125	81	142
8	84	5	50	166	157	67	2	20	33	163
9	127	101	8	80	132	151	7	70	32	153
10	27	103	28	113	128	111	108	78	112	118
11	11	110	98	145	114	138	44	106	58	79
12	122	51	9	90	65	149	154	37	36	26
13	93	95	115	143	144	104	38	46	126	91
14	75	82	152	17	3	30	133	161	107	68
15	12	120	31	143	94	105	48	146	124	71
16	42	86	25	83	162	117				

N.	0	1	2	3	4	5	6	7	8	9
1	1	10	100	165	147	134	4	40	66	159
2	87	35	16	160	97	135	14	140	64	139
3	54	39	56	59	89	55	49	156	57	69
4	22	53	29	123	61	109	88	45	116	158
5	77	102	48	13	130	131	144	74	172	52
6	150	164	137	34	6	60	99	155	47	136
7	24	73	62	119	21	43	96	125	81	142
8	84	5	50	166	157	67	2	20	33	163
9	127	101	8	80	132	151	7	70	32	153
10	27	103	28	113	128	111	108	78	112	118
11	11	110	98	145	114	138	44	106	58	79
12	122	51	9	90	65	149	154	37	36	26
13	93	95	115	143	144	104	38	46	126	91
14	75	82	152	17	3	30	133	161	107	68
15	12	120	31	143	94	105	48	146	124	71
16	42	86	25	83	162	117				

ПРОСТОЕ ЧИСЛО 173.

Первообр. корни: 2, 3, 5, 7, 8, 11, 12, 17, 18, 19, 20, 26, 27, 28, 30, 32, 39, 42, 44, 45, 46, 48, 50, 53, 58, 59, 61, 62, 63, 65, 66, 68, 69, 70, 71, 72, 74, 75, 76, 79, 82, 86, 87, 91, 94, 97, 98, 99, 101, 102, 103, 104, 105, 107, 108, 110, 111, 112, 114, 115, 120, 123, 125, 127, 128, 129, 131, 134, 141, 143, 145, 146, 147, 153, 154, 155, 156, 161, 162, 165, 166, 168, 170, 171.

Основание 91. N.

N	0	1	2	3	4	5	6	7	8	9
1	4	0	13	7	26	163	20	31	39	14
2	17	38	140	88	44	170	52	89	27	85
3	11	122	65	134	46	154	155	21	57	152
4	30	74	51	60	102	22	40	42	98	149
5	167	96	168	123	153	5	101	144	59	62
6	24	169	135	45	34	118	70	72	165	19
7	35	23	53	94	78	133	147	50	115	95
8	43	28	87	104	55	161	111	158	162	71
9	18	1	114	129	64	80	73	159	166	150
10	8	139	109	121	157	76	72	25	75	141
11	131	49	83	110	105	79	6	156	32	120
12	37	82	10	81	148	145	58	15	91	67
13	146	137	160	116	63	12	128	126	108	16
14	48	151	36	97	66	143	107	69	68	132
15	2	54	124	103	171	143	3	138	84	130
16	56	119	41	90	100	125	117	106	77	112
17	93	99	86							

N	1	0	1	2	3	4	5	6	7	8	9
1	1	91	150	156	10	45	116	3	100	104	
2	122	30	135	2	9	127	139	20	90	59	
3	6	27	35	71	60	97	4	18	81	105	
4	40	7	118	12	54	70	142	120	21	8	
5	36	162	37	80	44	63	24	108	140	111	
6	67	42	46	72	151	74	160	28	126	48	
7	43	107	49	134	84	32	144	129	148	147	
8	56	79	96	86	41	98	95	168	64	115	
9	85	123	121	112	158	19	172	82	23	17	
10	163	128	57	170	73	69	51	143	38	171	
11	164	46	34	153	83	114	167	146	138	102	
12	113	76	169	155	92	68	133	166	55	161	
13	119	103	31	53	152	165	137	11	136	93	
14	159	110	149	65	33	62	106	131	157	101	
15	22	99	43	145	47	125	130	66	124	39	
16	89	141	29	44	25	26	117	94	77	87	
17	132	75	78	5	109	58	88	50	52	61	
18	15	154									

ПРОСТОЕ ЧИСЛО 179.

Первообр. корни: 2, 6, 7, 8, 10, 11, 18, 21, 23, 24, 26, 28, 30, 32, 33, 34, 35, 37, 38, 40, 41, 44, 50, 53, 54, 55, 58, 62, 63, 69, 71, 72, 73, 78, 79, 84, 86, 90, 91, 92, 94, 96, 97, 98, 99, 102, 103, 104, 105, 109, 111, 112, 113, 114, 115, 118, 119, 120, 122, 123, 127, 128, 130, 131, 132, 133, 134, 136, 137, 140, 143, 148, 150, 152, 154, 157, 159, 160, 162, 163, 164, 165, 166, 167, 170, 174, 175, 176.

N.

ОСНОВАНИЕ 10.

	1	0	1	2	3	4	5	6	7	8	9
1	1	10	100	105	155	118	106	165	39	32	
2	141	157	138	127	17	170	89	174	129	37	
3	2	12	126	7	70	163	19	11	110	26	
4	3	81	94	45	92	25	71	173	119	116	86
5	4	144	8	80	84	124	166	49	132	67	133
6	5	77	54	3	30	121	136	107	175	139	137
7	6	117	96	65	113	56	23	51	152	88	164
8	7	29	111	36	2	20	21	31	131	57	33
9	8	151	78	64	103	135	97	75	34	161	178
10	9	169	79	74	24	61	73	14	140	147	38
11	10	22	41	52	162	9	90	5	50	142	167
12	11	59	53	172	109	16	160	168	69	153	98
13	12	85	134	87	154	108	6	60	63	93	35
14	13	171	99	95	55	13	130	47	112	46	102
15	14	125	176	149	58	43	4	40	40	42	62
16	15	83	114	66	123	156	128	27	91	15	150
17	16	68	143	177	159	158	148	48	122	146	28
18	17	101	115	76	44	82	104	145	18		

N.	0	1	2	3	4	5	6	7	8	9
1	1	0	73	52	146	106	125	23	41	104
2	74	27	20	134	96	158	114	44	177	26
3	53	76	9	65	93	34	29	156	169	70
4	147	101	148	144	173	32	138	19	99	8
5	107	66	102	111	51	133	64	136	166	46
6	126	94	149	127	82	62	152	78	143	110
7	24	35	145	95	92	86	172	50	81	91
8	42	30	174	150	43	120	39	122	68	16
9	105	157	33	128	31	132	61	85	119	131
10	2	170	139	83	175	3	6	56	124	113
11	28	71	137	63	151	171	38	60	5	37
12	21	54	167	153	44	140	22	13	155	18
13	135	77	47	49	124	84	55	59	42	58
14	97	10	108	161	40	176	168	98	165	142
15	159	80	67	118	123	4	154	11	164	163
16	115	88	103	25	69	7	45	109	116	90
17	15	130	112	36	17	57	141	162	89	

ПРостое число 181.

Первообразные корни: 2, 10, 18, 21, 23, 24, 28, 28, 41, 47, 50, 53, 54, 57, 58, 63, 66, 69, 76, 77, 78, 83, 84, 85, 90, 91, 96, 97, 98, 103, 104, 105, 112, 115, 118, 123, 124, 127, 128, 134, 134, 140, 153, 157, 158, 160, 163, 171, 179.

I.

Основание 10.

N.

N.	0	1	2	3	4	5	6	7	8	9
1	1	146	154	68	86	48	21	15	39	136
2	134	83	99	32	148	116	165	55	89	135
3	69	27	115	34	107	96	172	24	101	84
4	87	59	36	140	8	63	42	38	88	100
5	49	123	118	121	52	4	162	109	60	30
6	22	65	160	151	157	14	54	23	37	108
7	16	57	175	20	78	80	167	66	141	97
8	40	92	42	73	171	164	41	161	53	166
9	137	47	115	95	169	103	93	152	5	25
10	2	130	79	143	62	3	13	79	163	192
11	147	106	7	51	71	131	171	81	110	85
12	155	142	18	127	164	77	170	168	61	70
13	33	139	120	150	113	144	104	67	31	28
14	149	177	10	178	128	132	94	142	50	126
15	117	159	174	11	144	75	6	17	119	9
16	173	44	45	179	145	82	26	58	122	64
17	56	91	46	129	105	111	138	176	158	43
18	90									

N.	0	1	2	3	4	5	6	7	8	9
1	1	10	100	95	45	88	156	112	34	159
2	142	153	82	96	55	7	70	157	122	134
3	49	128	60	57	27	89	166	31	129	23
4	80	76	13	130	33	149	42	58	37	8
5	138	113	44	78	56	17	170	71	167	41
6	48	118	94	35	169	61	67	127	3	30
7	119	104	135	83	106	155	102	115	94	97
8	65	107	165	21	29	109	4	40	38	18
9	180	171	81	86	136	93	25	69	147	22
10	39	28	99	85	126	174	141	24	59	47
11	108	175	121	124	154	92	15	150	52	158
12	132	53	168	51	148	32	139	123	144	173
13	101	105	145	2	20	19	9	90	176	131
14	43	68	137	103	125	164	11	110	14	140
15	133	63	87	146	12	120	144	54	178	151
16	62	77	46	98	75	26	79	66	147	84
17	116	74	16	160	152	72	177	141	143	163

ПРОСТОЕ ЧИСЛО 191.

Первообр. корнц: 19, 21, 22, 28, 29, 33, 35, 42, 44, 47, 53, 56, 57, 58, 61, 62, 63, 71, 73, 74, 76, 77, 83, 87, 88, 89, 91, 93, 94, 95, 99, 101, 105, 106, 110, 111, 112, 113, 114, 116, 119, 123, 124, 126, 127, 131, 132, 137, 140, 141, 143, 145, 146, 148, 151, 157, 164, 165, 167, 168, 171, 173, 174, 175, 176, 178, 179, 181, 182, 183, 187, 188, 189.

N.

ОСНОВАНИЕ 157.

N.	0	1	2	3	4	5	6	7	8	9
1	0	157	10	42	100	38	45	189	68	171
2	1	107	115	101	4	55	40	168	18	152
3	2	180	81	111	46	155	78	22	16	29
4	3	169	99	72	35	147	159	133	62	184
5	4	121	88	64	116	67	14	97	140	15
6	5	150	57	163	188	102	161	65	82	77
7	6	6	178	60	61	27	37	79	179	26
8	7	69	137	117	33	24	139	49	53	108
9	8	125	143	104	93	85	166	86	132	96
10	9	5	21	50	19	118	190	34	181	149
11	10	153	146	2	123	20	84	9	76	90
12	11	136	151	23	173	39	11	8	110	80
13	12	36	113	169	175	162	31	92	119	156
14	13	32	58	129	7	144	70	103	127	75
15	14	177	94	51	176	128	41	134	28	3
16	15	30	126	109	114	135	185	13	131	130
17	16	154	112	12	165	120	122	54	74	158
18	17	52	142	138	83	43	66	48	87	98
19	18	25	105	59	95	17	186	170	141	172

N.	0	1	2	3	4	5	6	7	8	9
1	0	102	148	14	90	60	133	116	106	106
2	1	115	162	45	48	28	184	18	93	93
3	2	104	91	27	112	74	180	64	147	29
4	3	150	125	130	73	96	33	65	5	114
5	4	16	145	3	174	129	6	39	176	76
6	5	92	142	170	77	166	45	59	131	182
7	6	62	63	37	49	42	56	44	8	70
8	7	135	69	32	189	167	138	107	58	26
9	8	118	22	57	173	105	84	86	177	44
10	9	108	99	126	83	141	183	88	46	178
11	10	4	13	54	136	82	181	179	10	78
12	11	147	23	161	121	153	42	43	72	94
13	12	164	40	165	103	139	80	151	137	144
14	13	158	157	87	36	146	154	110	71	172
15	14	47	187	171	81	134	119	101	34	79
16	15	30	111	19	100	160	25	128	1	168
17	16	30	55	124	52	159	163	85	169	17
18	17	186	9	188	113	89	123	143	140	61
19	18	20	97	11	21	38	155	185	109	53

ПРОСТОЕ ЧИСЛО 193.

Первообразные корни: 5, 10, 15, 17, 19, 22, 26, 30, 34, 37, 38, 40, 44, 44, 45, 47, 51, 52, 53, 57, 58, 61, 66, 70, 73, 77, 78, 79, 80, 82, 90, 91, 102, 103, 111, 113, 114, 115, 116, 120, 123, 127, 132, 135, 136, 140, 141, 142, 146, 148, 149, 152, 153, 155, 156, 159, 163, 167, 171, 174, 176, 178, 183, 188.

I.

ОСНОВАНИЕ 10.

N.

N.	0	1	2	3	4	5	6	7	8	9
1	1	0	182	156	172	11	146	184	162	120
2	183	148	83	54	174	167	152	149	110	59
3	157	134	142	57	139	3	100	84	164	9
4	173	125	138	72	73	131	44	127	116	176
5	12	113	187	79	74	104	154	23	191	92
6	147	133	124	112	132	26	47	6	129	18
7	185	27	90	41	45	178	39	85	161	109
8	163	48	115	190	128	160	62	165	63	81
9	121	7	34	98	117	70	106	40	166	21
10	2	130	103	25	177	159	69	158	64	32
11	94	19	144	67	13	65	181	135	82	141
12	137	186	123	89	114	33	102	143	122	36
13	16	28	37	51	188	95	119	58	8	170
14	175	91	17	108	80	20	31	140	35	169
15	168	42	29	77	75	145	151	4	99	43
16	153	46	38	61	105	68	180	101	118	30
17	150	179	52	87	155	14	53	56	71	78
18	111	40	189	97	24	66	88	50	107	76
19	60	86	96							

N.	0	1	2	3	4	5	6	7	8	9
1	1	10	100	35	157	26	67	91	138	29
2	97	5	50	114	175	13	130	142	69	111
3	145	99	25	57	184	103	65	71	131	152
4	169	146	109	125	92	148	129	132	162	76
5	181	73	151	159	46	74	161	66	81	38
6	187	133	172	176	23	37	177	66	81	38
7	190	163	86	88	108	115	185	143	165	106
8	95	178	43	44	54	154	189	153	179	53
9	144	89	118	22	27	77	191	173	186	123
10	72	141	59	11	110	135	192	183	93	158
11	36	167	126	102	55	164	96	188	143	79
12	18	180	63	51	124	82	48	94	168	136
13	9	90	128	122	62	41	24	47	84	68
14	101	45	64	61	31	117	12	120	42	34
15	147	119	32	127	112	155	6	60	21	17
16	170	156	16	160	56	174	3	30	107	105
17	85	78	8	80	28	87	98	15	150	149
18	139	39	4	40	14	140	49	104	75	171
19	166	116	2	20	7	70	121	52	134	182
19	83	58								

ПРОСТОЕ ЧИСЛО 197.

Первообр. корнн: 2, 3, 5, 8, 11, 12, 13, 17, 18, 21, 27, 30, 31, 32, 35, 38, 44, 45, 46, 48, 50, 52, 56, 57, 58, 66, 67, 71, 72, 73, 74, 75, 78, 79, 80, 82, 86, 89, 91, 94, 95, 98, 99, 102, 103, 106, 108, 111, 115, 117, 118, 119, 122, 123, 124, 125, 126, 130, 131, 139, 140, 141, 145, 147, 149, 151, 152, 153, 159, 162, 165, 166, 167, 170, 176, 179, 180, 184, 185, 186, 189, 192, 194, 195.

N.

ОСНОВАНИЕ 73.

I.

N.	0	1	2	3	4	5	6	7	8	9
1	0	61	122	137	126	86	183	130	115	150
2	5	187	147	6	48	95	191	182	125	26
3	63	151	66	52	78	18	195	42	35	111
4	124	173	109	70	156	27	148	47	191	153
5	139	46	16	54	127	71	129	106	98	62
6	128	160	79	80	60	142	73	51	41	16
7	88	180	38	20	170	94	131	57	36	67
8	185	179	117	1	143	108	91	83	22	103
9	132	64	107	14	77	36	115	188	101	25
10	4	76	25	69	140	92	174	102	84	52
11	7	17	134	175	112	9	162	87	117	70
12	189	10	45	111	99	81	186	35	7	185
13	155	33	192	72	118	136	82	30	59	124
14	149	171	44	158	178	177	62	41	47	32
15	8	31	169	29	152	114	144	26	171	129
16	50	154	125	58	168	11	75	165	6	46
17	97	116	176	150	166	164	53	161	135	50
18	193	146	104	49	55	89	103	100	181	140
19	184	28	39	24	163	159	98	32	118	195
									174	152
									145	71
									127	120
									80	
									190	
									138	
									180	
									8	
									19	
									49	
									31	
									194	
									175	
									167	
									143	
									34	
									161	
									13	
									43	
									194	
									116	
									116	
									21	
									106	
									66	
									9	
									142	
									158	
									108	
									123	
									58	
									77	
									126	
									45	
									33	
									7	
									186	
									82	
									17	
									87	
									155	
									48	
									171	
									86	
									172	
									72	
									134	
									134	
									44	
									6	
									44	
									135	
									181	
									99	
									69	
									95	
									4	
									99	
									142	
									159	
									181	
									14	
									44	
									37	
									140	
									143	
									118	
									143	
									34	
									118	
									143	
									94	
									164	
									145	
									12	

ПРОСТОЕ ЧИСЛО 199.

Первообр. корн: 3, 6, 15, 22, 30, 34, 38, 39, 41, 44, 48, 54, 68, 69, 71, 73, 75, 77, 84, 87, 95, 97, 99, 105, 108, 110, 113, 118, 119, 120, 127, 129, 133, 134, 142, 143, 146, 148, 149, 150, 152, 153, 154, 163, 164, 166, 167, 168, 170, 173, 176, 179, 183, 185, 186, 189, 190, 192, 195, 197.

I. Основание 127.

N	0	1	2	3	4	5	6	7	8	9
1	0	194	155	190	6	151	32	186	112	
2	89	147	128	28	161	182	57	108	11	
3	157	76	178	143	42	124	69	24	158	
4	192	145	183	53	38	104	121	7	85	
5	8	14	120	181	148	70	98	139	64	
6	153	126	72	144	174	134	112	39	49	
7	34	71	100	44	117	167	3	23	81	
8	188	26	141	51	179	63	472	115	177	
9	144	160	66	33	94	17	135	109	60	
10	4	159	10	36	116	193	132	165	61	
11	191	78	16	73	162	80	150	42	125	
12	149	180	122	102	68	18	140	1	170	
13	130	148	138	43	35	75	45	171	27	
14	30	55	67	149	96	164	37	21	113	
15	163	40	197	169	19	82	77	84	46	
16	184	106	22	5	137	152	47	79	175	
17	59	123	168	25	111	44	173	86	88	
18	110	9	156	83	62	127	29	48	90	
19	13	87	131	52	105	91	56	95	99	

N	0	1	2	3	4	5	6	7	8	9
1	1	102	19	25	190	163	5	38	50	181
2	56	147	162	77	190	109	112	95	125	154
3	140	69	12	93	70	173	81	138	44	186
4	151	73	117	133	175	134	103	146	35	67
5	79	83	193	34	139	141	196	166	187	68
6	98	108	184	85	49	54	92	142	124	27
7	46	71	62	113	23	135	31	156	111	177
8	115	78	155	183	157	39	177	91	178	119
9	188	195	89	159	94	197	144	179	47	198
10	72	189	123	99	36	194	161	149	48	97
11	180	174	9	148	90	87	104	74	45	143
12	52	37	122	171	26	118	61	185	13	59
13	130	192	106	129	65	96	53	164	132	48
14	126	82	66	24	63	41	33	42	131	120
15	116	6	165	60	58	3	182	30	29	101
16	91	15	114	150	145	107	57	75	172	153
17	128	137	86	176	64	168	43	88	32	84
18	121	44	16	42	160	22	8	21	80	11
19	4	110	40	105	2	55	20	152		

ЛИНЕЙНЫЕ ДѢЛИТЕЛИ

КВАДРАТИЧНОЙ ФОРМЫ $x^2 + ay^2$ ДЛЯ ВСѢХЪ ВЕЛИЧИНЪ a
ОТЪ 1 ДО 101.

$x^2 + y^2$	$4z + 1$.
$x^2 + 2y^2$	$8z + 1, 3$.
$x^2 + 3y^2$	$12z + 1, 7$.
$x^2 + 5y^2$	$20z + 1, 3, 7, 9$.
$x^2 + 6y^2$	$24z + 1, 5, 7, 11$.
$x^2 + 7y^2$	$28z + 1, 9, 11, 15, 23, 25$.
$x^2 + 10y^2$	$40z + 1, 7, 9, 11, 13, 19, 23, 37$.
$x^2 + 11y^2$	$44z + 1, 3, 5, 9, 15, 23, 25, 27, 31, 37$.
$x^2 + 13y^2$	$52z + 1, 7, 9, 11, 15, 17, 19, 25, 29, 31, 47, 49$.
$x^2 + 14y^2$	$56z + 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45$.
$x^2 + 15y^2$	$60z + 1, 17, 19, 23, 31, 47, 49, 53$.
$x^2 + 17y^2$	$68z + 1, 3, 7, 9, 11, 13, 21, 23, 25, 27, 31, 33, 39, 49, 53, 63$.
$x^2 + 19y^2$	$76z + 1, 5, 7, 9, 11, 17, 23, 25, 35, 39, 43, 45, 47, 49, 55, 61, 63, 73$.
$x^2 + 21y^2$	$84z + 1, 5, 11, 17, 19, 23, 25, 31, 37, 41, 55, 71$.
$x^2 + 22y^2$	$88z + 1, 9, 13, 15, 19, 21, 23, 25, 29, 31, 35, 43, 47, 49, 51, 61, 71, 81, 83, 85$.
$x^2 + 23y^2$	$92z + 1, 3, 9, 13, 25, 27, 29, 31, 35, 39, 41, 47, 49, 55, 59, 71, 73, 75, 77, 81, 85, 87$.
$x^2 + 26y^2$	$104z + 1, 3, 5, 7, 9, 15, 17, 21, 25, 27, 31, 35, 37, 43, 45, 47, 49, 51, 63, 71, 75, 81, 85, 93$.
$x^2 + 29y^2$	$116z + 1, 3, 5, 9, 11, 13, 15, 19, 25, 27, 31, 33, 39, 43, 45, 47, 49, 53, 55, 57, 65, 75, 79, 81, 93, 95, 99, 109$.

$x^2 + 30y^2$	120z + 1, 11, 13, 17, 23, 29, 31, 37, 43, 47, 49, 59, 67, 79, 101, 113.
$x^2 + 31y^2$	124z + 1, 5, 7, 9, 19, 25, 33, 35, 39, 41, 45, 47, 49, 51, 59, 63, 67, 69, 71, 81, 87, 95, 97, 101, 103, 107, 109, 111, 113, 121.
$x^2 + 33y^3$	132z + 1, 7, 17, 19, 23, 25, 29, 37, 41, 43, 47, 49, 59, 65, 71, 79, 97, 101, 119, 127.
$x^2 + 34y^2$	136z + 1, 5, 7, 9, 19, 23, 25, 29, 31, 33, 35, 37, 39, 43, 45, 49, 59, 61, 63, 67, 71, 79, 81, 83, 89, 95, 109, 115, 121, 123, 125, 133.
$x^2 + 35y^2$	140z + 1, 3, 9, 11, 13, 17, 27, 29, 33, 39, 47, 51, 71, 73, 79, 81, 83, 87, 97, 99, 103, 109, 117, 121.
$x^2 + 37y^2$	148z + 1, 9, 15, 19, 21, 23, 25, 31, 33, 35, 39, 41, 43, 49, 51, 53, 55, 59, 65, 73, 77, 79, 81, 85, 87, 91, 101, 103, 119, 121, 131, 135, 137, 141, 143, 145.
$x^2 + 38y^2$	152z + 1, 3, 7, 9, 13, 17, 21, 23, 25, 27, 29, 37, 39, 47, 49, 51, 53, 55, 59, 63, 67, 69, 73, 75, 81, 87, 91, 107, 109, 111, 117, 119, 121, 137, 141, 147.
$x^2 + 39y^2$	156z + 1, 5, 11, 25, 41, 43, 47, 49, 55, 59, 61, 71, 79, 83, 89, 103, 119, 121, 125, 127, 133, 137, 139, 149.
$x^2 + 41y^2$	164z + 1, 3, 5, 7, 9, 11, 15, 19, 21, 25, 27, 33, 35, 37, 45, 47, 49, 55, 57, 61, 63, 67, 71, 73, 75, 77, 79, 81, 95, 99, 105, 111, 113, 121, 125, 133, 135, 141, 147, 151.
$x^2 + 42y^2$	168z + 1, 13, 17, 23, 25, 29, 31, 41, 43, 53, 55, 59, 61, 67, 71, 83, 89, 95, 103, 121, 131, 149, 159, 163.
$x^2 + 43y^2$	172z + 1, 9, 11, 13, 15, 17, 21, 23, 25, 31, 35, 41, 47, 49, 53, 57, 59, 67, 79, 81, 83, 87, 95, 97, 99, 101, 103, 107, 109, 111, 117, 121, 127, 133, 135, 139, 143, 145, 153, 165, 167, 169.
$x^2 + 46y^2$	184z + 1, 5, 9, 11, 19, 21, 25, 31, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 61, 67, 71, 73, 81, 83, 87, 91, 95, 99, 105, 107, 109, 119, 121, 125, 127, 149, 151, 155, 157, 167, 169, 171, 177, 181.
$x^2 + 47y^2$	188z + 1, 3, 7, 9, 17, 21, 25, 27, 37, 49, 51, 53, 55, 59, 61, 63, 65, 71, 75, 79, 81, 83, 89, 95, 97, 101, 103, 111, 115, 119, 121, 131, 143, 145, 147, 149, 153, 155, 157, 159, 165, 169, 173, 175, 177, 183.

$x^2 + 51y^2$	$204z + 1, 5, 11, 13, 19, 23, 25, 29, 41, 43, 49, 55, 65, 67, 71, 95, 103, 107, 113, 115, 121, 125, 127, 131, 143, 145, 151, 157, 167, 169, 173, 197.$
$x^2 + 53y^2$	$212z + 1, 3, 9, 13, 17, 19, 23, 25, 27, 29, 31, 35, 37, 39, 49, 51, 55, 57, 67, 69, 71, 75, 77, 79, 81, 83, 87, 89, 93, 97, 103, 105, 111, 113, 117, 121, 127, 139, 147, 149, 151, 153, 165, 167, 169, 171, 179, 191, 197, 201, 205, 207.$
$x^2 + 55y^2$	$220z + 1, 7, 9, 13, 17, 31, 43, 49, 57, 59, 63, 69, 71, 73, 81, 83, 87, 89, 91, 107, 111, 117, 119, 123, 127, 141, 153, 159, 167, 169, 173, 179, 181, 183, 191, 193, 197, 199, 201, 217.$
$x^2 + 57y^2$	$228z + 1, 11, 23, 25, 29, 31, 35, 41, 47, 49, 53, 61, 65, 67, 73, 79, 83, 85, 89, 91, 103, 113, 119, 121, 127, 131, 151, 157, 169, 173, 185, 191, 211, 215, 221, 223.$
$x^2 + 58y^2$	$232z + 1, 9, 15, 21, 25, 31, 33, 35, 37, 39, 47, 49, 51, 55, 57, 59, 61, 65, 67, 69, 77, 79, 81, 83, 85, 91, 95, 101, 107, 115, 119, 121, 123, 127, 129, 133, 135, 139, 143, 157, 159, 161, 169, 179, 187, 189, 191, 205, 209, 213, 215, 219, 221, 225, 227, 229.$
$x^2 + 59y^2$	$236z + 1, 3, 5, 7, 9, 15, 17, 19, 21, 25, 27, 29, 35, 41, 45, 49, 51, 53, 57, 63, 71, 75, 79, 81, 85, 87, 95, 105, 107, 119, 121, 123, 125, 127, 133, 135, 137, 139, 143, 145, 147, 153, 159, 163, 167, 169, 171, 175, 181, 189, 193, 197, 199, 203, 205, 213, 223, 225.$
$x^2 + 61y^2$	$244z + 1, 5, 7, 9, 11, 13, 23, 25, 31, 35, 41, 43, 45, 49, 51, 55, 57, 59, 63, 65, 67, 71, 73, 77, 79, 81, 87, 91, 97, 99, 109, 111, 113, 115, 117, 121, 125, 137, 139, 141, 143, 149, 151, 155, 159, 161, 169, 175, 191, 197, 205, 207, 211, 217, 223, 225, 227, 229, 241.$
$x^2 + 62y^2$	$248z + 1, 3, 7, 9, 11, 13, 21, 25, 27, 29, 33, 37, 39, 41, 43, 47, 49, 53, 61, 63, 71, 75, 77, 81, 83, 85, 87, 91, 95, 97, 99, 103, 111, 113, 115, 117, 121, 123, 129, 139, 141, 143, 147, 159, 169, 175, 179, 181, 183, 189, 191, 193, 197, 203, 213, 225, 229, 231, 233, 243.$
$x^2 + 65y^2$	$260z + 1, 3, 9, 11, 19, 23, 27, 29, 31, 33, 37, 43, 49, 57, 59, 61, 69, 71, 73, 81, 87, 93, 97, 99, 101, 103, 107, 111, 119, 121, 127, 129, 137, 147, 151, 171, 177, 181, 183, 193, 197, 207, 209, 213, 219, 239, 243, 253.$

$x^3 + 66y^2$	264z + 1, 5, 7, 13, 17, 23, 25, 35, 41, 47, 49, 53, 61, 65, 67, 77, 79, 83, 85, 91, 91, 107, 109, 115, 119, 125, 127, 131, 151, 161, 163, 169, 175, 191, 205, 221, 227, 233, 235, 245.
$x^2 + 67y^2$	268z + 1, 9, 15, 17, 19, 21, 23, 25, 29, 33, 35, 37, 39, 47, 49, 55, 59, 65, 71, 73, 77, 81, 83, 89, 91, 93, 103, 107, 121, 123, 127, 129, 131, 135, 143, 149, 151, 153, 155, 157, 159, 163, 167, 169, 171, 173, 181, 183, 189, 193, 199, 205, 207, 211, 215, 217, 223, 225, 227, 237, 241, 255, 257, 261, 263, 265.
$x^2 + 69y^2$	267z + 1, 5, 7, 13, 17, 19, 25, 35, 43, 47, 49, 53, 59, 65, 67, 71, 73, 79, 85, 89, 91, 95, 103, 113, 119, 121, 125, 131, 133, 137, 149, 167, 169, 175, 179, 193, 199, 215, 221, 235, 239, 245, 247, 265.
$x^2 + 70y^2$	280z + 1, 9, 17, 19, 33, 37, 39, 43, 47, 53, 59, 61, 67, 69, 71, 73, 79, 81, 87, 93, 97, 101, 103, 107, 121, 123, 131, 139, 143, 151, 153, 163, 167, 169, 171, 181, 191, 197, 223, 229, 233, 249, 251, 253, 257, 267, 269, 277.
$x^2 + 71y^2$	284z + 1, 3, 5, 9, 15, 19, 25, 27, 29, 37, 43, 45, 49, 57, 73, 75, 77, 79, 81, 83, 87, 89, 91, 95, 101, 103, 107, 109, 111, 119, 121, 125, 129, 131, 135, 143, 145, 147, 151, 157, 161, 167, 169, 171, 179, 185, 187, 191, 199, 215, 217, 219, 221, 223, 225, 229, 231, 233, 237, 243, 245, 249, 251, 253, 261, 263, 267, 271, 273, 277.
$x^2 + 73y^3$	292z + 1, 7, 9, 11, 15, 25, 31, 37, 39, 41, 43, 47, 49, 51, 57, 59, 61, 63, 65, 69, 77, 81, 83, 85, 87, 89, 95, 97, 99, 103, 105, 107, 109, 115, 121, 131, 135, 137, 139, 145, 149, 151, 159, 163, 165, 167, 169, 173, 175, 179, 181, 191, 199, 201, 213, 217, 221, 225, 237, 239, 247, 257, 259, 263, 265, 269, 271, 273, 275, 279, 287, 289.
$x^2 + 74y^2$	296z + 1, 3, 5, 9, 11, 13, 15, 23, 25, 27, 29, 31, 33, 39, 41, 45, 49, 55, 61, 65, 67, 69, 79, 75, 79, 81, 87, 89, 93, 99, 103, 107, 109, 115, 117, 119, 121, 123, 125, 133, 135, 137, 139, 143, 145, 147, 155, 165, 167, 169, 183, 191, 195, 199, 201, 205, 207, 211, 219, 225, 233, 237, 239, 243, 245, 249, 253, 261, 275, 277, 279, 289.

$x^2 + 77y^2$	$308z + 1, 3, 9, 13, 17, 25, 27, 31, 37, 39, 41, 43, 47, 51, 53, 59, 61, 73, 75, 79, 81, 93, 95, 101, 103, 107, 111, 113, 115, 117, 119, 123, 127, 129, 137, 141, 143, 145, 151, 153, 169, 173, 177, 183, 199, 211, 219, 221, 223, 225, 239, 241, 243, 251, 263, 279, 285, 289, 293, 297, 303.$
$x^2 + 78y^2$	$312z + 1, 19, 25, 29, 35, 37, 41, 47, 49, 53, 55, 67, 71, 77, 79, 85, 89, 101, 103, 107, 109, 115, 119, 121, 127, 131, 137, 155, 161, 163, 167, 173, 179, 187, 199, 215, 217, 229, 239, 251, 253, 269, 281, 289, 295, 301, 305, 307.$
$x^2 + 79y^2$	$316z + 1, 5, 9, 11, 13, 19, 21, 23, 25, 31, 45, 49, 51, 55, 65, 67, 73, 81, 83, 87, 89, 95, 97, 99, 101, 105, 111, 115, 117, 119, 121, 123, 125, 129, 131, 141, 143, 151, 155, 159, 163, 167, 169, 171, 173, 177, 179, 181, 183, 189, 203, 207, 209, 213, 223, 225, 231, 239, 241, 245, 247, 253, 255, 257, 259, 263, 269, 273, 275, 277, 297, 281, 283, 287, 289, 301, 309, 313.$
$x^2 + 82y^2$	$328z + 1, 7, 9, 13, 15, 25, 29, 33, 43, 47, 49, 51, 53, 55, 57, 59, 63, 69, 71, 73, 79, 81, 83, 85, 91, 93, 95, 101, 105, 107, 109, 111, 113, 115, 117, 121, 131, 135, 139, 149, 151, 155, 157, 163, 167, 169, 175, 181, 183, 185, 187, 191, 195, 199, 201, 203, 209, 225, 229, 231, 239, 241, 251, 253, 261, 263, 267, 283, 289, 291, 293, 297, 301, 305, 307, 309, 311, 317, 323, 325.$
$x^2 + 83y^2$	$332z + 1, 3, 7, 9, 11, 17, 21, 23, 25, 27, 29, 31, 33, 37, 41, 49, 51, 59, 61, 63, 65, 69, 75, 77, 81, 87, 93, 95, 99, 109, 111, 113, 119, 121, 123, 127, 131, 147, 151, 153, 161, 167, 169, 173, 175, 177, 183, 187, 189, 191, 193, 195, 197, 199, 203, 207, 215, 217, 225, 227, 229, 231, 235, 241, 243, 247, 253, 259, 261, 265, 275, 277, 279, 285, 287, 289, 293, 297, 313, 317, 319, 327.$
$x^2 + 85y^2$	$340z + 1, 9, 11, 21, 31, 37, 39, 43, 47, 49, 57, 67, 69, 71, 73, 79, 81, 83, 87, 89, 91, 97, 99, 101, 103, 113, 121, 123, 127, 131, 133, 139, 149, 159, 161, 169, 173, 177, 183, 189, 193, 197, 199, 203, 211, 223, 229, 231, 233, 247, 263, 277, 279, 281, 287, 299, 307, 311, 313, 317, 321, 327, 333, 337.$

$x^2 + 86y^2$	$344z + 1, 3, 5, 9, 15, 17, 19, 23, 25, 27, 29, 31, 37, 41, 45, 47, 49, 51, 57, 61, 69, 75, 77, 79, 81, 85, 89, 91, 93, 95, 97, 103, 111, 115, 121, 123, 125, 127, 131, 135, 141, 143, 145, 147, 149, 153, 155, 157, 163, 167, 169, 171, 179, 183, 185, 193, 205, 207, 211, 225, 227, 231, 235, 237, 239, 243, 245, 255, 261, 271, 273, 277, 279, 281, 285, 289, 291, 305, 309, 311, 323, 331, 333, 337.$
$x^2 + 87y^2$	$348z + 1, 7, 11, 13, 17, 25, 41, 47, 49, 67, 77, 89, 91, 95, 101, 103, 109, 113, 115, 119, 121, 131, 137, 139, 143, 151, 155, 169, 175, 181, 185, 187, 191, 199, 215, 221, 223, 241, 251, 263, 265, 269, 275, 277, 283, 287, 289, 293, 295, 305, 311, 313, 317, 325, 329, 343.$
$x^2 + 89y^2$	$363z + 1, 3, 5, 7, 9, 15, 17, 19, 21, 23, 25, 27, 31, 35, 43, 45, 49, 51, 53, 57, 59, 63, 69, 73, 75, 81, 83, 85, 93, 95, 97, 103, 105, 109, 115, 119, 121, 125, 127, 129, 133, 135, 143, 147, 151, 153, 155, 157, 159, 161, 163, 169, 171, 173, 175, 177, 189, 191, 207, 211, 215, 217, 219, 225, 233, 239, 243, 245, 249, 255, 257, 265, 269, 277, 279, 285, 289, 291, 295, 301, 309, 315, 317, 319, 323, 327, 343, 345.$
$x^2 + 91y^2$	$364z + 1, 5, 7, 9, 19, 23, 25, 29, 31, 33, 41, 43, 45, 47, 51, 53, 59, 73, 79, 81, 83, 89, 95, 97, 107, 111, 113, 121, 125, 127, 145, 155, 165, 167, 171, 179, 183, 187, 189, 191, 201, 205, 207, 211, 213, 215, 223, 225, 227, 229, 233, 235, 241, 255, 261, 263, 265, 271, 277, 279, 289, 293, 295, 303, 307, 309, 327, 347, 349, 353, 361.$
$x^2 + 93y^2$	$372z + 1, 17, 25, 29, 35, 43, 47, 49, 53, 55, 59, 65, 71, 77, 79, 89, 91, 95, 97, 107, 109, 115, 121, 127, 131, 133, 137, 139, 143, 151, 157, 161, 169, 185, 191, 193, 197, 199, 205, 209, 223, 227, 247, 253, 259, 269, 271, 287, 289, 299, 305, 311, 331, 335, 349, 353, 359, 361, 365, 367.$
$x^2 + 94y^2$	$376z + 1, 5, 7, 9, 11, 13, 17, 19, 25, 29, 35, 43, 45, 49, 55, 63, 65, 67, 69, 71, 77, 79, 81, 85, 89, 91, 93, 95, 97, 99, 103, 107, 109, 111, 117, 119, 121, 123, 125, 133, 139, 143, 145, 153, 159, 163, 169, 171, 175, 177, 179, 181, 183, 187, 191, 203, 209, 211, 215, 219, 221, 225, 227, 229, 239, 241, 245, 247, 249, 261, 263, 271, 275, 289, 293, 301, 303, 315, 317, 319, 323, 325, 335, 337, 339, 343, 345, 349, 353, 355, 361, 373.$

$x^2 + 95y^2$	$380z + 1, 3, 9, 11, 13, 27, 33, 37, 39, 49, 53, 61, 67, 81, 97, 99, 101, 103, 107, 111, 113, 117, 119, 121, 127, 131, 139, 143, 147, 149, 159, 161, 167, 169, 173, 183, 191, 193, 199, 201, 203, 217, 223, 227, 229, 239, 243, 251, 257, 271, 287, 289, 291, 293, 297, 301, 303, 307, 309, 311, 317, 321, 329, 333, 337, 339, 349, 351, 357, 359, 363, 373.$
$x^2 + 97y^2$	$388z + 1, 7, 9, 15, 19, 23, 25, 33, 39, 49, 51, 53, 55, 59, 61, 63, 65, 67, 71, 73, 81, 83, 85, 87, 89, 93, 101, 105, 107, 109, 111, 113, 121, 123, 127, 129, 131, 133, 135, 139, 141, 143, 145, 155, 161, 169, 171, 175, 179, 185, 187, 193, 197, 199, 205, 207, 211, 215, 221, 223, 225, 229, 231, 235, 237, 239, 241, 251, 263, 269, 271, 273, 285, 289, 293, 297, 309, 311, 313, 319, 331, 341, 343, 345, 347, 351, 353, 357, 359, 361, 367, 371, 375, 377, 383, 385.$
$x^2 + 101y^2$	$404z + 1, 3, 5, 7, 9, 11, 13, 15, 17, 21, 25, 27, 33, 35, 37, 39, 45, 49, 51, 55, 59, 63, 65, 67, 75, 77, 81, 83, 85, 91, 97, 99, 103, 105, 111, 117, 119, 121, 125, 127, 135, 137, 139, 143, 147, 151, 153, 157, 163, 165, 167, 169, 175, 177, 181, 185, 187, 189, 191, 193, 195, 197, 199, 201, 221, 225, 231, 233, 243, 245, 249, 255, 259, 263, 271, 273, 275, 287, 289, 291, 295, 297, 305, 311, 313, 315, 321, 229, 331, 335, 343, 347, 351, 357, 361, 363, 373, 375, 381, 385.$

10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

ЛИНЕЙНЫЕ ДѢЛИТЕЛИ

КВАДРАТИЧНОЙ ФОРМЫ $x^2 - ay^2$ ДЛЯ ВСѢХЪ ВЕЛИЧИНЪ a
ОТЪ 1 ДО 101.

$x^2 - 2y^2$	$8z + 1, 7.$
$x^2 - 3y^2$	$12z + 1, 11.$
$x^2 - 5y^2$	$20z + 1, 9, 11, 19.$
$x^2 - 6y^2$	$24z + 1, 5, 19, 23.$
$x^2 - 7y^2$	$28z + 1, 3, 9, 19, 25, 27.$
$x^2 - 10y^2$	$40z + 1, 3, 9, 13, 27, 31, 37, 39.$
$x^2 - 11y^2$	$44z + 1, 5, 7, 9, 19, 25, 35, 37, 39, 43.$
$x^2 - 13y^2$	$52z + 1, 3, 9, 17, 23, 25, 27, 29, 35, 43, 49, 51.$
$x^2 - 14y^2$	$56z + 1, 5, 9, 11, 13, 25, 31, 43, 45, 47, 51, 55.$
$x^2 - 15y^2$	$60z + 1, 7, 11, 17, 43, 49, 53, 59.$
$x^2 - 17y^2$	$68z + 1, 9, 13, 15, 19, 21, 25, 33, 35, 43, 47, 49, 53, 55, 59, 67.$
$x^2 - 19y^2$	$76z + 1, 3, 5, 9, 15, 17, 25, 27, 31, 45, 49, 51, 59, 61, 67, 71, 73, 75.$
$x^2 - 21y^2$	$84z + 1, 5, 17, 25, 37, 41, 43, 47, 59, 67, 79, 83.$
$x^2 - 22y^2$	$88z + 1, 3, 7, 9, 13, 21, 25, 27, 29, 39, 49, 59, 61, 63, 67, 75, 79, 81, 85, 87.$
$x^2 - 23y^2$	$92z + 1, 7, 9, 11, 13, 15, 19, 25, 29, 41, 43, 49, 51, 63, 67, 73, 77, 79, 81, 83, 85, 91.$
$x^2 - 26y^2$	$104z + 1, 5, 9, 11, 17, 19, 21, 23, 25, 37, 45, 49, 55, 59, 67, 79, 81, 83, 85, 87, 93, 95, 99, 103.$
$x^2 - 29y^2$	$116z + 1, 5, 7, 9, 13, 23, 25, 33, 35, 45, 49, 51, 53, 57, 59, 63, 65, 67, 71, 81, 83, 91, 93, 103, 107, 109, 111, 115.$
$x^2 - 30y^2$	$120z + 1, 7, 13, 17, 19, 29, 37, 49, 71, 83, 91, 101, 103, 107, 113, 119.$

$x^2 - 31y^2$	$124z + 1, 3, 5, 9, 11, 15, 23, 25, 27, 33, 41, 43, 45, 49, 55, 69, 75, 79, 81, 83, 91, 97, 99, 101, 109, 113, 115, 119, 121, 123.$
$x^2 - 33y^2$	$132z + 1, 17, 25, 29, 31, 35, 37, 41, 49, 65, 67, 83, 91, 95, 97, 101, 103, 107, 115, 131.$
$x^2 - 34y^2$	$136z + 1, 3, 5, 9, 11, 15, 25, 27, 29, 33, 37, 45, 47, 49, 55, 61, 75, 81, 87, 89, 91, 99, 103, 107, 109, 111, 121, 125, 127, 131, 133, 135.$
$x^2 - 35y^2$	$140z + 1, 9, 13, 17, 19, 23, 29, 31, 33, 43, 59, 67, 73, 81, 97, 107, 109, 111, 117, 121, 123, 127, 131, 139.$
$x^2 - 37y^2$	$148z + 1, 3, 7, 9, 11, 21, 25, 27, 33, 41, 47, 49, 53, 63, 65, 67, 71, 73, 75, 77, 81, 83, 85, 95, 99, 101, 107, 115, 121, 123, 127, 137, 139, 141, 145, 147.$
$x^2 - 38x^2$	$152z + 1, 9, 11, 13, 15, 17, 23, 25, 29, 31, 35, 37, 43, 49, 53, 69, 71, 73, 79, 81, 83, 99, 103, 109, 115, 117, 121, 123, 127, 129, 135, 137, 139, 141, 143, 151.$
$x^2 - 39y^2$	$156z + 1, 5, 7, 19, 23, 25, 31, 35, 41, 49, 61, 67, 89, 95, 107, 115, 121, 125, 131, 133, 137, 149, 151, 155.$
$x^2 - 41y^2$	$164z + 1, 5, 9, 21, 23, 25, 31, 33, 37, 39, 43, 45, 49, 51, 57, 59, 61, 73, 77, 81, 83, 87, 91, 103, 105, 107, 113, 115, 119, 121, 125, 127, 131, 133, 139, 141, 143, 155, 159, 163.$
$x^2 - 42y^2$	$168z + 1, 11, 13, 17, 19, 25, 29, 41, 47, 53, 61, 79, 89, 107, 115, 121, 127, 139, 143, 149, 151, 155, 157, 167.$
$x^2 - 43y^2$	$172z + 1, 3, 7, 9, 13, 17, 19, 21, 25, 27, 39, 41, 49, 51, 53, 55, 57, 63, 71, 75, 81, 91, 97, 101, 109, 115, 117, 119, 121, 123, 131, 133, 145, 147, 151, 153, 155, 159, 163, 165, 169, 171.$
$x^2 - 46y^2$	$184z + 1, 3, 5, 7, 9, 15, 21, 25, 27, 35, 37, 41, 45, 49, 53, 59, 61, 63, 73, 75, 79, 81, 103, 105, 109, 111, 121, 123, 125, 131, 135, 139, 143, 147, 149, 157, 159, 163, 169, 175, 177, 179, 181, 183.$
$x^2 - 47y^2$	$188z + 1, 9, 11, 15, 17, 19, 21, 23, 25, 31, 35, 37, 39, 43, 49, 53, 61, 65, 67, 81, 87, 89, 91, 97, 99, 101, 107, 121, 123, 127, 135, 139, 145, 149, 151, 153, 157, 163, 165, 167, 169, 171, 173, 177, 179, 187.$
$x^2 - 51y^2$	$204z + 1, 5, 7, 13, 25, 29, 31, 35, 41, 47, 49, 59, 65, 79, 83, 91, 113, 121, 125, 139, 145, 155, 157, 163, 169, 173, 175, 179, 191, 197, 199, 203.$

$x^2 - 53y^2$	$212z + 1, 7, 9, 11, 13, 15, 17, 25, 29, 37, 43, 47, 49, 57, 59, 63, 69, 77, 81, 89, 91, 93, 95, 97, 99, 105, 107, 113, 115, 117, 119, 121, 123, 131, 135, 143, 149, 153, 155, 163, 165, 169, 175, 183, 187, 195, 197, 199, 201, 203, 205, 211.$
$x^2 - 55y^2$	$220z + 1, 3, 9, 13, 17, 19, 23, 27, 39, 47, 49, 51, 57, 67, 69, 73, 79, 81, 89, 103, 117, 131, 139, 141, 147, 151, 153, 163, 169, 171, 173, 181, 193, 197, 201, 203, 207, 211, 217, 219.$
$x^2 - 57y^2$	$228z + 1, 7, 23, 29, 41, 43, 49, 53, 55, 59, 61, 65, 71, 73, 85, 89, 107, 113, 115, 121, 139, 143, 155, 157, 163, 167, 169, 173, 175, 179, 185, 187, 199, 203, 221, 227.$
$x^2 - 58y^2$	$232z + 1, 3, 7, 9, 11, 19, 21, 23, 25, 27, 33, 37, 43, 49, 57, 61, 63, 65, 69, 71, 75, 77, 81, 85, 99, 101, 103, 111, 121, 129, 131, 133, 147, 151, 155, 157, 161, 163, 167, 169, 171, 175, 183, 189, 195, 199, 205, 207, 209, 211, 213, 221, 223, 225, 229, 231.$
$x^2 - 59y^2$	$236z + 1, 5, 9, 11, 17, 21, 23, 25, 29, 31, 39, 41, 43, 45, 47, 49, 53, 55, 57, 67, 81, 83, 85, 91, 99, 103, 105, 111, 115, 121, 125, 131, 133, 137, 145, 151, 153, 155, 169, 179, 181, 183, 187, 189, 191, 193, 195, 197, 205, 207, 211, 213, 215, 219, 225, 227, 231, 235.$
$x^2 - 61y^2$	$244z + 1, 3, 5, 9, 13, 15, 19, 25, 27, 39, 41, 45, 47, 49, 57, 65, 73, 75, 77, 81, 83, 95, 97, 103, 107, 109, 113, 117, 119, 121, 123, 125, 127, 131, 135, 137, 141, 147, 149, 161, 163, 167, 169, 171, 179, 187, 195, 197, 199, 203, 205, 217, 219, 225, 229, 231, 235, 239, 241, 243.$
$x^2 - 62y^2$	$248z + 1, 9, 13, 15, 19, 21, 23, 25, 29, 33, 35, 37, 41, 49, 51, 53, 55, 59, 61, 67, 77, 79, 81, 85, 97, 103, 113, 117, 119, 121, 127, 129, 131, 135, 145, 151, 163, 167, 169, 171, 181, 187, 189, 193, 195, 197, 199, 207, 211, 213, 215, 219, 223, 225, 227, 229, 233, 235, 239, 247.$
$x^2 - 65y^2$	$260z + 1, 7, 9, 29, 33, 37, 47, 49, 51, 57, 61, 63, 67, 69, 73, 79, 81, 83, 93, 97, 101, 121, 123, 129, 131, 137, 139, 159, 163, 167, 177, 179, 181, 187, 191, 193, 197, 199, 203, 209, 211, 213, 223, 227, 231, 251, 253, 259.$
$x^2 - 66y^2$	$264z + 1, 5, 13, 17, 19, 25, 31, 41, 43, 49, 53, 59, 61, 65, 85, 95, 97, 103, 109, 125, 139, 155, 161, 167, 169, 179, 199, 203, 205, 211, 215, 221, 223, 233, 239, 245, 247, 251, 259, 263.$

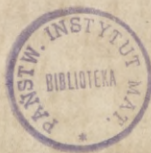
$x^2 - 67y^2$	268z + 1, 3, 7, 9, 11, 17, 21, 25, 27, 29, 31, 33, 37, 43, 49, 51, 63, 65, 73, 75, 77, 79, 81, 87, 89, 93, 95, 99, 111, 115, 119, 121, 129, 139, 147, 149, 153, 157, 169, 173, 175, 179, 181, 187, 189, 191, 193, 195, 203, 205, 217, 219, 225, 231, 235, 237, 239, 241, 243, 247, 251, 257, 259, 261, 265, 267.
$x^2 - 69y^2$	276z + 1, 5, 11, 13, 17, 25, 31, 49, 53, 55, 65, 73, 83, 85, 89, 107, 113, 121, 125, 127, 133, 137, 139, 143, 149, 151, 155, 163, 169, 187, 191, 193, 203, 211, 221, 223, 227, 245, 251, 259, 263, 265, 271, 275
$x^2 - 70y^2$	280z + 1, 3, 9, 11, 17, 23, 27, 31, 33, 37, 51, 53, 61, 69, 73, 81, 83, 93, 97, 99, 101, 111, 121, 127, 153, 159, 179, 181, 183, 187, 197, 199, 207, 211, 219, 227, 229, 243, 247, 249, 253, 257, 263, 269, 271, 277, 279.
$x^2 - 71y^3$	284z + 1, 5, 7, 9, 11, 23, 25, 29, 31, 35, 37, 39, 45, 47, 49, 51, 55, 57, 59, 63, 67, 73, 77, 81, 89, 99, 101, 109, 115, 121, 123, 125, 127, 129, 139, 145, 155, 157, 159, 161, 163, 169, 175, 183, 185, 195, 203, 207, 211, 217, 221, 225, 227, 229, 233, 235, 237, 239, 245, 247, 249, 253, 255, 259, 261, 273, 275, 277, 279, 283.
$x^2 - 73y^2$	292z + 1, 3, 9, 19, 23, 25, 27, 35, 37, 41, 49, 55, 57, 61, 65, 67, 69, 71, 75, 77, 79, 81, 85, 89, 91, 97, 105, 109, 111, 119, 121, 123, 127, 137, 143, 145, 147, 149, 155, 165, 169, 171, 173, 181, 183, 187, 195, 201, 203, 207, 211, 213, 215, 217, 221, 223, 225, 227, 231, 235, 237, 243, 251, 255, 257, 265, 267, 269, 273, 283, 289 291.
$x^2 - 74y^2$	296z + 1, 5, 7, 9, 13, 19, 25, 29, 33, 35, 41, 43, 45, 47, 49, 51, 59, 61, 63, 65, 69, 71, 73, 81, 91, 93, 95, 109, 117, 121, 125, 127, 131, 133, 137, 145, 151, 159, 163, 165, 169, 171, 175, 179, 187, 201, 203, 205, 215, 223, 225, 227, 231, 233, 235, 237, 245, 247, 249, 251, 253, 255, 261, 263, 267, 271, 277, 283, 287, 289, 291, 295.
$x^2 - 77y^2$	308z + 1, 9, 13, 15, 17, 19, 23, 25, 37, 41, 53, 61, 67, 71, 73, 81, 83, 87, 93, 101, 113, 117, 129, 131, 135, 137, 139, 141, 145, 153, 155, 163, 167, 169, 171, 173, 177, 179, 191, 195, 207, 215, 221, 225, 227, 235, 237, 241, 247, 255, 267, 271, 283, 285, 289, 291, 293, 295, 299, 307.

$x^2 - 78y^2$	$312z + 1, 7, 11, 23, 25, 29, 31, 37, 41, 43, 49, 53, 59, 77, 83, 85, 89, 95, 101, 109, 121, 137, 139, 151, 161, 173, 175, 191, 203, 211, 217, 223, 227, 229, 235, 253, 259, 263, 269, 271, 275, 281, 283, 287, 289, 301, 305, 311.$
$x^2 - 79y^2$	$316z + 1, 3, 5, 7, 9, 13, 15, 21, 25, 27, 35, 39, 43, 45, 47, 49, 59, 63, 65, 71, 73, 75, 81, 89, 91, 97, 101, 103, 105, 107, 117, 121, 125, 127, 129, 135, 139, 141, 147, 169, 175, 177, 181, 187, 189, 191, 195, 199, 209, 211, 213, 215, 219, 225, 227, 235, 241, 243, 245, 251, 253, 257, 267, 269, 271, 273, 277, 281, 289, 291, 295, 301, 303, 307, 309, 311, 313, 315.$
$x^2 - 82y^2$	$328z + 1, 3, 9, 11, 13, 19, 23, 25, 27, 29, 31, 33, 35, 39, 49, 53, 57, 67, 69, 73, 75, 81, 85, 87, 93, 99, 101, 103, 105, 109, 113, 117, 119, 121, 127, 143, 147, 149, 157, 159, 169, 171, 179, 181, 185, 201, 207, 209, 211, 215, 219, 223, 225, 227, 229, 235, 241, 243, 247, 253, 255, 259, 261, 271, 275, 279, 289, 293, 295, 297, 299, 301, 303, 305, 309, 315, 317, 319, 325, 327.$
$x^2 - 83y^2$	$332z + 1, 9, 15, 17, 19, 21, 25, 29, 33, 35, 37, 39, 41, 43, 47, 49, 55, 61, 65, 67, 69, 71, 77, 79, 81, 91, 93, 103, 107, 109, 113, 115, 121, 135, 139, 143, 153, 155, 159, 161, 163, 169, 171, 173, 177, 179, 189, 193, 197, 211, 217, 219, 223, 225, 229, 239, 241, 251, 253, 255, 261, 263, 265, 267, 271, 277, 283, 285, 289, 291, 293, 295, 297, 299, 303, 307, 311, 313, 315, 317, 323, 331,$
$x^2 - 85y^2$	$340z + 1, 3, 7, 9, 19, 21, 23, 27, 37, 49, 57, 59, 63, 69, 73, 81, 89, 97, 101, 107, 111, 113, 121, 133, 143, 147, 149, 151, 161, 163, 167, 169, 171, 173, 177, 179, 189, 191, 193, 197, 207, 219, 227, 229, 233, 239, 243, 251, 259, 267, 271, 277, 281, 283, 291, 303, 313, 317, 319, 321, 331, 333, 337, 339.$
$x^2 - 86y^2$	$344z + 1, 5, 7, 9, 11, 17, 25, 29, 35, 37, 39, 41, 45, 49, 55, 57, 59, 61, 63, 67, 69, 71, 77, 81, 83, 85, 93, 97, 99, 107, 119, 121, 125, 139, 141, 145, 149, 151, 153, 157, 159, 169, 175, 185, 187, 191, 193, 195, 199, 203, 205, 219, 223, 225, 237, 245, 247, 251, 259, 261, 263, 267, 273, 275, 277, 281, 283, 285, 287, 289, 295, 299, 303, 305, 307, 309, 315, 319, 327, 333, 335, 337, 339, 343.$

$x^2 - 87y^2$	$348z + 1, 13, 17, 19, 23, 31, 35, 41, 43, 49, 55, 59, 71, 77, 79, 83, 89, 91, 101, 107, 109, 113, 121, 127, 137, 163, 167, 169, 179, 181, 185, 211, 221, 227, 235, 239, 241, 247, 257, 259, 265, 269, 271, 277, 289, 293, 299, 305, 307, 313, 317, 325, 329, 331, 335, 347.$
$x^2 - 89y^2$	$356z + 1, 5, 9, 11, 17, 21, 25, 39, 45, 47, 49, 53, 55, 57, 67, 69, 71, 73, 79, 81, 85, 87, 91, 93, 97, 99, 105, 107, 109, 111, 121, 123, 125, 129, 131, 133, 139, 153, 157, 161, 167, 169, 173, 177, 179, 183, 187, 189, 195, 199, 203, 217, 223, 225, 227, 231, 233, 235, 245, 247, 249, 251, 257, 259, 263, 265, 269, 271, 275, 277, 283, 285, 287, 289, 299, 301, 303, 307, 309, 311, 317, 331, 335, 339, 345, 347, 351, 355.$
$x^2 - 91y^2$	$364z + 1, 3, 5, 9, 11, 15, 17, 25, 27, 29, 41, 45, 53, 63, 67, 71, 75, 81, 87, 99, 103, 113, 115, 121, 123, 125, 131, 135, 139, 143, 145, 151, 159, 163, 165, 175, 189, 199, 201, 205, 213, 219, 221, 225, 229, 233, 239, 241, 243, 245, 249, 251, 261, 265, 277, 283, 289, 291, 293, 311, 319, 323, 301, 335, 337, 339, 347, 349, 353, 355, 359, 361, 363.$
$x^2 - 93y^2$	$372z + 1, 7, 11, 17, 19, 23, 25, 29, 49, 53, 65, 67, 77, 83, 89, 97, 103, 109, 119, 121, 133, 137, 157, 161, 163, 167, 169, 175, 179, 185, 187, 193, 197, 203, 205, 209, 211, 215, 235, 239, 251, 253, 263, 269, 275, 283, 289, 295, 305, 307, 319, 323, 343, 347, 349, 353, 355, 361, 365, 371.$
$x^2 - 94y^2$	$376z + 1, 3, 5, 9, 13, 15, 17, 23, 25, 27, 29, 31, 39, 45, 49, 51, 59, 65, 69, 75, 77, 81, 83, 85, 87, 89, 93, 97, 109, 115, 117, 121, 125, 127, 131, 133, 135, 145, 147, 151, 153, 155, 167, 169, 177, 181, 195, 199, 207, 209, 221, 223, 225, 229, 231, 241, 243, 245, 249, 251, 255, 259, 261, 267, 279, 283, 287, 289, 291, 293, 295, 299, 301, 307, 311, 317, 325, 327, 331, 337, 345, 347, 349, 351, 353, 359, 361, 363, 367, 371, 373, 375.$
$x^2 - 95y^2$	$380z + 1, 7, 9, 13, 23, 29, 31, 33, 37, 43, 47, 49, 51, 53, 59, 61, 63, 71, 79, 81, 83, 87, 91, 97, 101, 113, 117, 121, 123, 149, 151, 163, 169, 173, 179, 187, 193, 201, 207, 211, 217, 229, 231, 257, 259, 263, 267, 279, 283, 289, 293, 297, 299, 301, 309, 317, 319, 321, 327, 329, 331, 333, 337, 343, 347, 349, 351, 357, 367, 371, 373, 379.$

$x^2 - 97y^2$	$388z + 1, 3, 9, 11, 25, 27, 31, 33, 35, 43, 47, 49, 53,$ $61, 65, 73, 75, 79, 81, 85, 89, 91, 93, 95, 99,$ $101, 103, 105, 109, 113, 115, 119, 121, 129,$ $133, 141, 145, 147, 151, 159, 161, 163, 167,$ $169, 183, 185, 191, 193, 195, 197, 203, 205,$ $219, 221, 225, 227, 229, 237, 241, 243, 247,$ $255, 259, 267, 269, 273, 275, 279, 283, 285,$ $287, 289, 293, 295, 297, 299, 303, 307, 309,$ $313, 315, 323, 327, 335, 339, 341, 345, 353,$ $355, 357, 361, 363, 377, 379, 385, 387.$
$x^2 - y101^2$	$404z + 1, 5, 9, 13, 17, 19, 21, 23, 25, 31, 33, 37, 43,$ $45, 47, 49, 65, 75, 77, 81, 83, 85, 91, 97, 99,$ $105, 107, 115, 117, 121, 123, 125, 131, 137, 153,$ $155, 157, 159, 165, 169, 171, 177, 179, 181,$ $183, 185, 189, 193, 197, 201, 203, 207, 211,$ $215, 219, 221, 223, 225, 227, 233, 235, 239,$ $245, 247, 249, 251, 267, 273, 279, 281, 283,$ $287, 289, 297, 299, 305, 307, 313, 319, 321,$ $323, 327, 329, 339, 355, 357, 359, 361, 367,$ $371, 373, 379, 381, 383, 385, 387, 391, 395,$ $399, 403.$

~~GABINET MATEMATYCZNY
 Towarzystwa Wiedzy i Umiejętności Warszawskiego~~



О П Е Ч А Т К И.

Страница.	Строка	Напечатано.	Вмѣсто.
6	5	C	N
—	14	косается	касается
17	6	$\frac{\gamma - 1}{\alpha}$	$\frac{\gamma - 1}{\gamma}$
21	19	$M \equiv N''$	$M'' \equiv N''$
32	3	=	\equiv
37	24	b то	b ; то
41	29	$^3 2x$	$2x^3$
44	26	$Hx \equiv$	$Hx + S \equiv$
47	20	$a \equiv M_m,$	$a_m \equiv M$
48	11	a^m	a_m
49	16 и 19	$Hx + S$	$Lx + M$
55	5 и 25	$ax + bx + c$	$ax^2 + bx + c$
		$\frac{p - 1}{2}$	$\frac{p - 1}{2}$
70	19	p	q
74	14	$E - \frac{\frac{1}{2}(p-1)a}{p}$	$E \frac{\frac{1}{2}(p-1)a}{p}$
91	28	\equiv	=
143	7	$v \equiv$	$r \equiv$
—	13	сравненіе	уравненіе
165	18	$c \left(\frac{c\alpha + b}{\omega} \right)^2 - \frac{d}{\omega}$	$\omega \left(\frac{c\alpha + b}{\omega} \right)^2 - \frac{d}{\omega}$
175	10	26 и U	26и U
192	3	759	751
205	12	$2(5n+5) - 1,$	$2(4n+5) - 1$
208	12	здѣсь числа: 173, 317 должны быть выкинуты.	
218	8	$\frac{x}{\varphi x} - x$	$\frac{x}{\varphi x} - \log x$
233	4	простое число 2	простое число 3

O R E A T I O N E M

Page	Text	Page	Text
237	proportio	1	
218	$\frac{x}{y} = \frac{z}{w}$	2	
208	proportio	3	
207	$\frac{a+b}{c} = \frac{d}{e}$	4	
197	proportio	5	
177	$\frac{a}{b} = \frac{c}{d}$	6	
167	proportio	7	
157	$\frac{a}{b} = \frac{c}{d}$	8	
147	proportio	9	
137	$\frac{a}{b} = \frac{c}{d}$	10	
127	proportio	11	
117	$\frac{a}{b} = \frac{c}{d}$	12	
107	proportio	13	
97	$\frac{a}{b} = \frac{c}{d}$	14	
87	proportio	15	
77	$\frac{a}{b} = \frac{c}{d}$	16	
67	proportio	17	
57	$\frac{a}{b} = \frac{c}{d}$	18	
47	proportio	19	
37	$\frac{a}{b} = \frac{c}{d}$	20	
27	proportio	21	
17	$\frac{a}{b} = \frac{c}{d}$	22	
7	proportio	23	



