# ZARYS PIERWSZYCH ZASAD TEORYI LICZB CAŁKOWITYCH

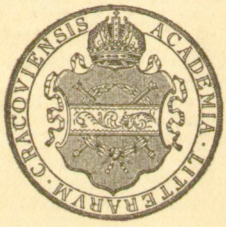
# ZARYS PIERWSZYCH ZASAD TEORYI LICZB CAŁKOWITYCH

NAPISAŁ

S. ZAREMBA

PROFESOR UNIWERSYTETU JAGIELL.






GABINET MATEMATYCZNY
Towarzystwa Naukowego Warszawskiego

W KRAKOWIE
NAKŁADEM AKADEMII UMIEJĘTNOŚCI
SKŁAD GŁÓWNY W KSIĘGARNI SPÓŁKI WYDAWNICZEJ POLSKIEJ
1907

# SPIS RZECZY.

# PRZEDMOWA.

Przedmiotem dziełka tego jest najelementarniejszy dział arytmetyki teoretycznej. Nie należałoby jednak wywnioskować z tego, że podręcznik ten ma służyć do pierwszego obeznania się z początkami arytmetyki. Dziełko to przeznaczone jest, w pierwszym rzędzie, dla przyszłych nauczycieli matematyki i cel jego polega na wyłożeniu zasad teoryi liczb całkowitych w tak ściśle naukowej postaci, aby teorya ta mogła zadość uczynić wymaganiom zawodowego matematyka.

Mojem zdaniem ściśle naukowa postać wspomnianej teoryi, jak i każdej innej teoryi matematycznej, wykracza częściowo ponad poziom, do którego można wznieść się przy nauczaniu w zakładach średnich. Z tej przyczyny omawiam w ostatnim rozdziale te zmiany, które należałoby wprowadzić do teoryi wyłożonej w rozdziałach poprzedzających, ażeby uzyskać teoryę przystępną dla uczniów najwyższych klas gimnazyalnych.

Czytelnik, który pragnąłby bliżej obeznać się z nowoczesnemi badaniami z zakresu podstaw analizy, do których oczywiście należą zasady teoryi liczb całkowitych, znajdzie odnośne wskazówki bibliograficzne w dziele następującem: Stolz u. Gmeiner, Theoretische Arithmetik, Leipzig, 1900.

Spełniam miły obowiązek, składając wyrazy wdzięczności Akademii Umiejętności w Krakowie za wydanie tego dziełka.

Winienem także wyrazić uprzejme podziękowanie p. Józefowi Rydlowi za cenną pomoc udzieloną mi przy prowadzeniu korekty.

*S. Zaremba.*

*Kraków 21 listopada 1907.*

## I. Podstawy teoryi liczb całkowitych.

§ 1. Nazwa gałęzi wiedzy, którą zamierzamy wyłożyć, wskazuje na to, że badamy w niej przedmioty zwane liczbami całkowitemi. Winniśmy dodać, że teorya liczb jest nauką dedukcyjną i jako taka nie opiera się na żadnych doświadczeniach albo spostrzeżeniach, lecz wyłącznie na pewnych pojęciach, powstałych po za jej ramami, oraz na pewnych orzeczeniach, tak zwanych aksyomatach, najzupełniej pewnych, ale przyjętych bez dowodu. Treść teoryi liczb, zarówno jak treść każdej innej nauki dedukcyjnej, polega na tworzeniu szeregu pojęć drogą definicyi i na uzasadnieniu drogą rozumowania pewnych prawd, zwanych twierdzeniami albo wnioskami; wyrazu „wniosek“ używamy zamiast wyrazu „twierdzenie“ w przypadkach, kiedy pragniemy położyć nacisk na tę okoliczność, że rozważane orzeczenie w bardzo blizkim znajduje się związku z ostatniem twierdzeniem uzasadnionem poprzednio. Bliższe określenie teoryi liczb nie jest na razie ani możebne ani pożądane.

Jedna z najważniejszych cech poprawnego wykładu nauki dedukcyjnej polega na wyraźnem uwidocznieniu jej podstaw a więc pojęć, zaczerpniętych po za jej ramami, i aksyomatów jej właściwych, czyli nie należących do układu pojęć i aksyomatów, stanowiących kompleks ogólnych warunków poprawnego myślenia. Błędem byłoby jednak myśleć, że pojęcia i aksyomaty, właściwe mającej być wyłożonej nauce, winne być podane w postaci wykazu na czele wykładu. Urzeczywistnienie tego byłoby najczęściej niepodobieństwem, albowiem samo wysłowienie aksyomatów wymaga zwykle pojęć i wyrażeń, które tylko stopniowo mogą być wprowadzane.

Po tych wyjaśnieniach nie wyda się dziwną czytelnikowi ta okoliczność, że rozdział obecny zawierać będzie, prócz właściwych podstaw teoryi liczb całkowitych, szereg definicyi i twierdzeń.

§ 2. Czem jest liczba całkowita? Pojęcie liczby całkowitej nie należy do pojęć konstruowanych drogą definicyi, lecz jest samo jednem z elementów zasadniczych, z których wytwarzamy inne pojęcia. Zapewne możemy zastanawiać się nad genezą pojęcia liczby całkowitej, ale badania tego rodzaju, które zresztą należą do teoryi poznania a nie do teoryi liczb, nie stanowią bynajmniej konstrukcyi omawianego pojęcia. Oczywiście można także, przez stworzenie stosownych warunków, ułatwić dziecku nabycie pojęcia liczby całkowitej, ale na tem polega nie konstrukcya pojęcia liczby, lecz jedno z zadań pierwszego okresu wychowania. Ponieważ zaś dziełko to przeznaczamy dla osób, które już wyszły z tego pierwszego okresu wychowania, przeto pojęcie liczby całkowitej uważać będziemy za już nabyte.

Skoro przedmiotem badań naszych mają być liczby całkowite (dla skrócenia używać będziemy niekiedy wyraz „liczba“ w znaczeniu „liczba całkowita“), winniśmy oczywiście zastanowić się nad sprawą nazywania i oznaczania liczb całkowitych.

Jeżeli pomyślana liczba uważaną jest za coś oznaczonego, nie ze względu na jej wartość, ale ze względu na związki, w których ona znajduje się z innymi jakiemikolwiek elementami, to oznaczamy ją przez dowolnie przyjęty symbol, najczęściej przez jakąś literę, nadmieniając jednocześnie wyraźnie, że taki to symbol ma oznaczać taką to liczbę. Jeżeli na przykład chcemy oznaczyć liczbę mieszkańców pewnego miasta, to możemy oświadczyć, że taki to symbol, powiedzmy litera $a$, oznaczać będzie w naszych rozważaniach wspomnianą liczbę. Należy jednak podnieść, że omówiona postać sprawy oznaczania liczb nie należy do właściwej teoryi oznaczania liczb, lecz raczej do ogólnej teoryi wysłowiania się, albowiem wymieniony sposób załatwienia tej sprawy wynika z tej ogólnej zasady, iż

każdy pomyślany przedmiot możemy oznaczyć przez dowolnie przyjęty symbol. Zadanie właściwej teoryi oznaczania liczb, czyli teoryi numeracyi, polega na ustawieniu takiego układu definicyi, z którego nazwa i symbol każdej, pod względem wartości oznaczonej liczby, wynikałyby już bez wprowadzenia żadnej nowej definicyi. Żeby odróżnić rzeczone nazwy i symbole liczb od innych nazw i symbolów tych elementów, nazw i symbolów przypadkowy charakter mających, nadajemy omawianym nazwom i symbolom miano nazw i symbolów specyficznych [1]). Wyrażenie „numeracya“ oznacza układ definicyi, określający nazwy i symbole specyficzne liczb całkowitych.

Załatwienie sprawy numeracyi wymaga pewnego obeznania się z teoryą liczb. Zdawałoby się więc, że znajdujemy się wobec koła błędnego. Tak jednak nie jest, albowiem każdą pomyślaną liczbę całkowitą możemy zrozumiale oznaczyć, określając taki układ jakichkolwiek przedmiotów, który zawierałby ich tyle, ile wynosi pomyślana liczba. Przechodzimy więc natychmiast do ustawienia podstaw teoryi liczb całkowitych, odkładając sprawę numeracyi na później.

§ 3. Zakładamy, że liczbę, której nazwą specyficzną jest wyraz „jeden“, poznaliśmy już po za ramami teoryi liczb całkowitych.

**Def. I.** Symbol następujący:

*1*

zwany jedynką, przyjmujemy za symbol specyficzny liczby jeden.

**Def. II.** Orzeczenie, iż liczba przedmiotów sprawdzających pewne warunki, jest liczbą, której nazwą specyficzną jest „zero“, uważamy jako wyrażające to samo, co orzeczenie następujące: nie istnieje żaden przedmiot sprawdzający rozważane

[1]) Na przykład, wedle zwykłej terminologii wyraz „pięć“ i symbol 5 stanowią nazwę i symbol specyficzne na normalną liczbę palców u ręki ludzkiej.

warunki; za symbol specyficzny liczby zero przyjmujemy symbol następujący:

$$0.$$

Na podstawie ogólnych zasad wysławiania się wyraz „zbiór“ oznacza ogół przedmiotów sprawdzających pewien układ warunków; ten układ warunków stanowi określenie zbioru. Ponieważ orzeczenie kształtu następującego: „liczbą przedmiotów należących do pewnego zbioru ($z$) jest pewna liczba $a$“, wyraża w rzeczywistości pewną własność określenia zbioru ($z$), a nie pewną własność przedmiotów do zbioru ($z$) należących, przeto orzeczenie takie nie jest pozbawione treści nawet w razie, kiedy liczbą $a$ jest liczba zero; w tym przypadku szczególnym, na podstawie def. III, rozważane orzeczenie opiewa, że nie istnieje żaden przedmiot sprowadzający warunki stanowiące określenie zbioru.

**Def. III.** Wynikiem dodania jedności do oznaczonej liczby całkowitej $a$ nazywamy liczbę przedmiotów, którą zawierałby zbiór, uzyskany przez dołączenie jednego nowego przedmiotu do zbioru, zawierającego już tyle przedmiotów, ile wynosi liczba $a$.

**Def. IV.** Wynik dodania jedności do liczby całkowitej, oznaczonej przez jakikolwiek symbol $a$, przedstawiamy przez symbol

$$a+1,$$

który czytamy: $a$ więcej jeden.

**Aks. I.** Każdej liczbie całkowitej odpowiada jedna i tylko jedna liczba, stanowiąca wynik dodania jedności do pierwszej.

**Aks. II.** Wynikiem dodania jedności do zera jest liczba jeden.

**Def. V.** Ciągiem nazywamy wszelki zbiór przedmiotów następujących po sobie w oznaczonym porządku. Przedmioty, z których ciąg składa się, zowią się jego elementami. Numerem porządkowym oznaczonego elementu $E$ oznaczonego ciągu ($C$) nazywamy wynik dodania jedności do liczby elementów,

poprzedzających w tym ciągu element $E$. Jeżeli w pewnym ciągu $(C)$ pewien element $E$ następuje bezpośrednio po pewnym innym elemencie $E'$, albo poprzedza bezpośrednio ten element, to elementy $E$ i $E'$ zowią się elementami sąsiednimi w ciągu $(C)$.

Uwaga. Na podstawie definicyi poprzedzającej i Aks. II numerem porządkowym pierwszego elementu jakiegokolwiek ciągu jest liczba jeden.

**Aks. III.** Zbiór liczb całkowitych możemy pomyśleć w postaci ciągu, którego pierwszym elementem jest liczba zero, a każdym dalszym, wynik dodania jedności do liczby stanowiącej element poprzeprzedzający bezpośrednio element rozważany.

**Def. VI.** Ciąg rozważany w aksyomacie poprzedzającym zwie się ciągiem naturalnym liczb całkowitych.

**Aks. IV.** Każda liczba całkowita, uważana jako element ciągu naturalnego liczb całkowitych, jest liczbą odmienną od każdej liczby całkowitej, stanowiącej inny element tego ciągu. W innych wyrazach: w ciągu naturalnym liczb całkowitych żadna liczba nie powtarza się.

§ 4. **Def. VII.** Jeżeli istnieje jedna tylko liczba całkowita, sprawdzająca pewien warunek albo pewien układ warunków $(A)$, jeżeli ta sama okoliczność zachodzi co do pewnego innego warunku albo układu warunków $(B)$, jeżeli nadto ta sama liczba całkowita sprawdza warunki $(A)$ i $(B)$, to fakt ten wyrażamy orzekając, że liczby sprawdzające warunki $(A)$ i $(B)$ są sobie równe. Symbolicznem wyrażeniem równości pewnych liczb $a$ i $b$ jest każdy z następujących układów symbolów:

$$a = b \text{ i } b = a.$$

Każdy z takich układów symbolów zwie się równością.

**Aks. V.** Jeżeli pewne orzeczenie o liczbach całkowitych, należących do pewnego zbioru $(z)$ jest słuszne, to słuszne jest także każde orzeczenie, wynikające z orzeczenia rozważanego przez zastąpienie którychkolwiek z liczb zbioru $(z)$ odpowiednio przez liczby tym liczbom równe.

**Tw. I.** Jeżeli oznaczymy przez $a$, $b$ i $c$ liczby sprawdzające równości następujące:

$(A)$ $\qquad b = c,$

i

$(B)$ $\qquad c = a,$

to liczby $a$ i $c$ sprawdzać będą równość:

$(C)$ $\qquad b = a.$

Dowód. Równość $(C)$ jest orzeczeniem, w które przechodzi orzeczenie, stanowiące równość $(B)$ przez zastąpienie w niej liczby $c$ przez równą jej, na podstawie równości $(A)$, liczbę $b$. Wnosimy stąd, na podstawie aks. poprzedzającego, że równości $(A)$ i $(B)$ pociągają za sobą równość $(C)$, co było do okazania.

**Def. VIII.** Jeżeli, w ciągu naturalnym liczb całkowitych pewna liczba $a$ poprzedza pośrednio lub bezpośrednio pewną liczbę $b$, to okoliczność tę wysławiamy którymkolwiek z orzeczeń następujących: „liczba $a$ mniejsza jest od liczby $b$“ albo „liczba $b$ większa jest od liczby $a$“.

Orzeczenia te wyrażamy symbolicznie odpowiednio w sposób następujący:

$$a < b \text{ i } b > a.$$

Takie układy symbolów zwą się nierównościami.

**Tw. II.** Jeżeli pewna liczba $a$ i pewna inna liczba $b$ nie są sobie równe, to jedna z nich zawsze mniejszą jest od drugiej.

Dowód. Istotnie każda z liczb $a$ i $b$ (aks. III, def. VI i aks. IV) stanowić będzie pewien jeden i tylko jeden z elementów ciągu naturalnego liczb całkowitych. Ponieważ zaś liczby te nie są sobie równe, przeto będą one stanowić pewne odmienne od siebie elementy ciągu naturalnego liczb całkowitych. Zatem pewna jedna z tych liczb poprzedzać będzie drugą i, z tej przyczyny, będzie od niej mniejsza, co było do okazania.

**Tw. III.** Jeżeli liczby całkowite $a$, $b$ i $c$ sprawdzają nierówności:

$$a < b$$

i

$$b < c,$$

to liczby $a$ i $c$ sprawdzają nierówność następującą:

$$a < c.$$

Dowód. W ciągu naturalnym liczb całkowitych liczba $a$, jako poprzedzająca (def. VIII) liczbę $b$, która znowu poprzedza liczbę $c$, poprzedzać będzie liczbę $c$. Zatem (def. VIII) mamy

$$a < c,$$

co było do okazania.

**Tw. IV.** Jeżeli liczby całkowite $a$, $b$ i $c$ sprawdzają związki następujące:

$(A)$ $$a = b$$

$(B)$ $$b < c$$

to liczby $a$ i $c$ sprawdzają związek następujący:

$(C)$ $$a < c.$$

Dowód. Wszelka nierówność jest symboliczną formą pewnego zdania. Z drugiej strony nierówność $(C)$ wynika z nierówności $(B)$, zastępując w tej ostatniej liczbę $b$ przez liczbę $a$, równą jej na mocy równości $(A)$. Ponieważ nierówność $(B)$ zachodzi istotnie, przeto (aks. V) nierówność $(C)$ także niezawodnie zachodzi. Co było do okazania.

**Tw. V.** Jeżeli liczby całkowite $a$, $b$ i $c$ sprawdzają związki następujące:

$$a < b$$

$$b = c$$

to liczby $a$ i $c$ sprawdzają związek następujący:

$$a < c.$$

Dowód twierdzenia tego jest całkiem analogiczny do dowodu twierdzenia poprzedzającego.

**Def. IX.** Jeżeli oznaczymy przez $a$ i $b$ pewne liczby całkowite, to każdy z następujących dwóch układów symbolów:

$$a \leqq b \text{ i } b \geqq a$$

uważamy za symboliczne wyrażenie następujących, równoważnych sobie orzeczeń: „liczba $a$ nie jest większą od liczby $b$“ i „liczba $b$ nie jest mniejszą od liczby $a$“.

W braku lepszego terminu, nazywamy powyższe układy symbolów nierównościami.

**Tw. VI.** Jeżeli liczby $a$, $b$ i $c$ sprawdzają nierówności następujące:

$$a \leqq b$$

i

$$b \leqq c,$$

to liczby $a$ i $c$ sprawdzają nierówność następującą:

$$a \leqq c.$$

Twierdzenie to wynika natychmiast z tw. I, III, IV i V.

§ 5. Istnieje obszerna klasa twierdzeń typu następującego: „pewna okoliczność ($\Omega$), dotycząca pewnej rzeczy ($z$), zawsze zachodzi, byleby pewna liczba całkowita $n$, znajdująca się w pewnym związku z rzeczą ($z$), nie była mniejszą od pewnej zupełnie oznaczonej liczby $k$“ [1]).

Z reguły dowód takiego twierdzenia prowadzimy wedle szematu następującego:

*A*) Uzasadniamy twierdzenie bezpośrednio w przypadku kiedy mamy

$$n = k.$$

*B*) Oznaczając następnie przez $p$ liczbę całkowitą od liczby $k$ nie mniejszą, okazujemy że, gdyby pewnem było, że twierdzenie zachodzi w razie kiedy mamy

$$n = p$$

---

[1]) Przykład na twierdzenie takiego typu znajdzie już czytelnik w paragrafie następującym.

to pewnem byłoby także, że twierdzenie zachodzi w przypadku kiedy mamy

$$n = p + 1$$

*C*) Z wyników uzyskanych pod *A*) i pod *B*) wnosimy bezpośrednio, że twierdzenie w podanem brzmieniu jest całkiem uzasadnione.

Żeby ułatwić czytelnikowi poznanie właściwej treści dowodu powyższego typu przedstawiamy część (*C*) rozważanego dowodu jeszcze w postaci następującej:
na podstawie wyniku uzasadnionego pod *A*) mamy pewność, że twierdzenie zachodzi w razie kiedy mamy:

$$n = k.$$

Zatem, na podstawie wyniku uzasadnionego pod *B*), mamy także pewność, że twierdzenie zachodzi w razie kiedy mamy

$$n = k'$$

przyjmując

$$k' = k + 1.$$

Stąd wnosimy dalej, opierając się znowu na wyniku uzyskanym pod *B*), że twierdzenie zachodzi jeszcze w przypadku, kiedy mamy

$$n = k'',$$

przyjmując

$$k'' = k' + 1.$$

Z tego zaś wypływa, znowu na podstawie wyniku uzyskanego pod *B*), że twierdzenie zachodzi też w przypadku kiedy mamy

$$n = k'''$$

przyjmując

$$k''' = k'' + 1$$

i tak dalej. Zatem twierdzenie zachodzi przy każdej, od liczby $k$ nie mniejszej, wartości liczby $n$.

Powyższa metoda dowodzenia znaną jest pod nazwą indukcyi matematycznej. Metoda ta oczywiście rdzennie jest

odmienną od metod indukcyjnych spostrzegawczych lub eksperymentalnych. Metoda indukcyi matematycznej oczywiście opiera się na aksyomacie następującym:

**Aks. VI.** Jeżeli pewne orzeczenie ($\Omega$) obejmujące pewną liczbę całkowitą $n$ sprawdza warunki następujące:

*A*) Uważane orzeczenie jest słusznem w przypadku szczególnym, kiedy liczba $n$ równa się pewnej oznaczonej liczbie całkowitej $k$.

*B*) Gdyby pewnem było, że orzeczenie ($\Omega$) słusznem jest w razie kiedy mamy

$$n = p,$$

oznaczając przez $p$ dowolnie przyjętą, od liczby $k$ nie mniejszą liczbę całkowitą, to orzeczenie to słusznem byłoby także w przypadku kiedy mamy

$$n = p + 1;$$

to wówczas orzeczenie ($\Omega$) słusznem jest, byleby liczba całkowita $n$ nie była mniejszą od liczby $k$.

Aksyomat ten nazwiemy „zasadą indukcyi matematycznej".

Poincaré upatruje[1]), niezawodnie całkiem słusznie, w zasadzie indukcyi matematycznej główne źródło płodności rozważań matematycznych.

§ 6. **Tw. VII.** Jeżeli oznaczymy przez $a$ ostatnią liczbę takiego, od liczby *jeden* rozpoczynającego się ciągu liczb całkowitych, w którym każda dalsza liczba jest wynikiem dodania jedności do liczby, która ją poprzedza bezpośrednio, to liczba $a$ będzie liczbą elementów rozważanego ciągu.

Dowód. Twierdzenie jest oczywiście słuszne (def. III) w przypadku, gdy w rozważanym ciągu liczba jeden poprzedza bezpośrednio liczbę $a$. Gdyby zaś twierdzenie było słuszne i w razie kiedy liczba $a$ byłaby pewną liczbą $b$, to (def. III) twierdzenie byłoby także słuszne w przypadku, w którymby liczba $a$ była wynikiem dodania jedności do

[1]) Poincarè, La science a l'hypothese.

liczby $b$. Przeto (aks. VI) twierdzenie jest słuszne w każdym razie, co było do okazania.

**Def. X.** Zbiorem skończonym nazywamy wszelki zbiór, któremu odpowiada oznaczona liczba całkowita, będąca liczbą przedmiotów, do tego zbioru należących.

**Def. XI.** Jeżeli pewien zbiór ma tę własność, że możemy wyłączyć z niego tyle przedmiotów, ile wynosi każda dowolnie przyjęta liczba całkowita, to zbiór ten nazywamy zbiorem nieskończonym.

**Tw. VIII.** Zbiór wszystkich liczb całkowitych jest zbiorem nieskończonym.

Dowód. Istotnie, uważajmy ciąg naturalny $(C)$ liczb całkowitych oraz dowolnie przyjętą liczbę $a$. Jeżeli z ciągu $(C)$ usuniemy liczbę *zero* i liczby od liczby $a$ większe, to otrzymamy zbiór, zawierający tyle liczb ile wynosi liczba $a$; okoliczność tę sprawdzamy bezpośrednio w przypadkach, kiedy liczba $a$ jest zerem albo jednością; przy każdej zaś innej wartości liczby $a$ rzeczona okoliczność zachodzi na podstawie twierdzenia VII. Wnosimy stąd natychmiast, że twierdzenie o które chodziło, zachodzi istotnie.

Uwaga. Żeby dowieść, iż pewien zbiór $(z)$ jest nieskończony, można poprzestać na okazaniu, że ze zbioru $(z)$ możemy wyłączyć tyle przedmiotów, ile wynosi każda liczba całkowita większa od pewnej oznaczonej liczby całkowitej $k$; jeżeli bowiem możemy wyłączyć ze zbioru $(z)$ pewną liczbę $(m > k)$ przedmiotów, to oczywiście możemy tem bardziej wyłączyć ze zbioru tego tyle liczb, ile wynosi każda liczba od liczby $k$ nie większa.

**Aks. VII.** Żaden zbiór nie może być jednocześnie skończonym i nieskończonym, ale każdy — jest albo skończonym, albo nieskończonym.

**Tw. IX.** Jeżeli do jakiegokolwiek zbioru nieskończonego $(A)$ dołączymy jakikolwiek inny zbiór $(B)$, to uzyskany zbiór $(C)$ będzie także zbiorem nieskończonym.

Dowód. Oznaczmy przez $n$ dowolnie przyjętą liczbę całkowitą. Ze zbioru $(A)$ wyłączam tyle przedmiotów, ile wynosi

liczba $n$ i oznaczam przez $(z)$ zbiór tych przedmiotów. Zbiór $(z)$ zawsze będziemy mogli utworzyć, albowiem zbiór $(A)$ jest nieskończony (def. XI). Ponieważ każdy przedmiot zbioru $(z)$ oczywiście należy do zbioru $(C)$, przeto zbiór $(z)$ uważany być może za wynik wyłączenia ze zbioru $(C)$ tylu pewnych przedmiotów, ile wynosi liczba $n$. Zatem zbiór $(C)$ jest nieskończony, co było do okazania.

Żeby na pytanie następujące: ile wynosi liczba przedmiotów należących do pewnego zbioru? zawsze można było dać odpowiedź typu następującego: liczba, o którą chodzi jest takato, wprowadzamy wyrażenie „liczba nieskończoność“, określając to wyrażenie definicyą następującą:

**Def. XII.** Orzeczenie następujące: liczba przedmiotów, należących do pewnego zbioru, jest liczbą nieskończoność, wyraża to samo co orzeczenie — : rzeczony zbiór jest nieskończony. Oczywiście liczba nieskończoność ma tę wspólną cechę z każdą liczbą całkowitą, że, podobnie do liczby całkowitej, stanowi własność, którą może mieć zbiór, niezależnie od natury przedmiotów do zbioru należących.

Możnaby może rozszerzyć znaczenie wyrażenia „liczba całkowita“ w ten sposób, żeby liczba nieskończoność za liczbę całkowitą uważaną być mogła. Ze względu na to, że takie rozszerzenie wyrażenia „liczba całkowita“ naturalnem wydawać się może, używamy niekiedy, celem usunięcia wszelkiego nieporozumienia, wyrażenia „liczba całkowita skończona“ zamiast wyrażenia „liczba całkowita“. Winniśmy jednak dodać, że w rzeczywistości wspomniane rozszerzenie znaczenia wyrażenia „liczba całkowita“ do nauki, jako niedogodne, nie weszło.

Żeby zrozumieć przyczynę tego, należy tylko zwrócić się do tw. IX. Z twierdzenia tego wnosimy, że liczba nieskończoność nie jest czemś tak całkiem określonem jak każda liczba całkowita skończona. Dla tego też, gdybyśmy liczbę nieskończoność zaliczyli do liczb całkowitych, to, przy wysłowieniu przeważnej części twierdzeń, zmuszeni bylibyśmy

zastrzegać, że, w stosunku do nich, liczba nieskończoność stanowi wyjątek.

§ 7. **Tw. X.** Oznaczmy przez $a$ i $c$ pierwszą i ostatnią liczbę takiego ciągu $(C)$ liczb całkowitych, w którym każda po liczbie $a$ bezpośrednio lub pośrednio następująca liczba jest większa od liczby, która poprzedza ją bezpośrednio. W takim razie liczby $a$ i $c$ sprawdzać będą nierówność następującą:

$$a < c.$$

Dowód. Oznaczmy przez $n$ liczbę liczb położonych w ciągu $(C)$ między liczbami $a$ i $c$. Jeżeli mamy

$$n = o$$

to twierdzenie, jako prosta toutologia, niezawodnie jest słuszne.

Załóżmy chwilowo, że twierdzenie zachodzi w razie kiedy mamy

$$n = k$$

i rozważajmy przypadek, kiedy liczba $n$ ma wartość określoną równością następującą:

$$n = k + 1.$$

Oznaczając tedy przez $b$ liczbę poprzedzającą bezpośrednio w ciągu $(C)$ liczbę $c$, mamy

$$a < b \text{ oraz } b < c$$

przeto na podstawie tw. III, mieć będziemy

$$a < c.$$

Opierając się na zasadzie indukcyi matematycznej wnosimy z poprzedniego, że twierdzenie w podanem brzmieniu jest słuszne.

Wniosek. Jeżeli oznaczymy przez $a'$ i $c'$ takie do ciągu $(C)$, rozważanego w twierdzeniu poprzedzającem, należące liczby, z których pierwsza poprzedza tamtą, to będziemy mieli

$$a' < c'.$$

Istotnie liczby $a'$ i $c'$ oczywiście uważane być mogą za pierwszy i ostatni element ciągu tego samego rodzaju, co ciąg $(C)$ i dlatego muszę rzeczywiście sprawdzać wysłowioną nierówność.

**Tw. XI.** Zachowując oznaczenia wprowadzone przy wysłowieniu twierdzenia poprzedzającego, uważajmy pewną liczbę całkowitą $l$ nie mniejszą od liczby $a$ i nie większą od liczby $c$. Jeżeli tedy liczba $l$ nie równa się żadnej liczbie należącej do ciągu $(C)$, to liczba ta sprawdzać będzie nierówności następujące

$$l > \alpha$$
$$l < \beta$$

gdzie $\alpha$ i $\beta$ oznaczają pewne liczby bezpośrednio po sobie następujące w ciągu $(C)$.

Dowód. Oznaczając, jak przy tw. X, przez $n$ liczbę liczb położonych w ciągu $(C)$ między liczbami $a$ i $c$, stwierdzamy, że w przypadku, kiedy mamy

$$n = o$$

twierdzenie zachodzi niezawodnie, albowiem redukuje się ono tedy do prostej toutologii. Załóżmy chwilowo, że twierdzenie zachodzi w razie, kiedy mamy

$$n = k$$

i rozważajmy przypadek, w którym jest

$$n = k + 1.$$

Oznaczmy tedy przez $b$ liczbę poprzedzającą bezpośrednio w ciągu $(C)$ liczbę $c$. Jeżeli liczba $l$ nierówna się żadnej liczbie należącej do ciągu $(C)$, to oczywiście mogą tylko zachodzić przypadki następujące:

$A$) Liczba $l$ sprawdza nierówności następujące:

$$l > b$$
$$l < c.$$

W takim razie liczba $l$ sprawdzałaby wysłowione twierdzenie.

*B*) Liczba $l$ sprawdza nierówność

$$l < b$$

Jeżeli tedy oznaczymy przez $(C')$ ciąg, w który przechodzi ciąg $(C)$ przez usunięcie ostatniego elementu $c$, to, opierając się na chwilowo przyjętem założeniu, stwierdzimy natychmiast, że w ciągu $(C')$, a więc i w ciągu $(C)$, istnieć będą takie bezpośrednio po sobie następujące liczby $\alpha$ i $\beta$, które sprawdzać będą nierówności następujące:

$$l > \alpha \text{ i } l < \beta.$$

Ostatecznie przekonaliśmy się, że, gdyby twierdzenie, o które chodzi, zachodziło w przypadku, kiedy mamy

$$n = k,$$

to twierdzenie to zachodziłoby jeszcze w przypadku, w którym mielibyśmy

$$n = k + 1.$$

Ponieważ zaś stwierdziliśmy wyżej, że twierdzenie zachodzi istotnie w razie kiedy liczba $n$ równa się liczbie zeru, przeto wnosimy, że twierdzenie, które pragnęliśmy udowodnić, zachodzi rzeczywiście w podanem brzmieniu.

**Tw. XII.** W każdym układzie $(U)$, zawierającym skończoną liczbę $p$ $(p > 1)$ odmiennych od siebie liczb całkowitych istnieje liczba najmniejsza i liczba największa.

Dowód. Twierdzenie to nie różni się od tw. II w razie, kiedy mamy

$$p = 1 + 1$$

Załóżmy, że rozważane twierdzenie zachodziłoby gdybyśmy mieli

$$p = k$$

i przyjmijmy:

$$p = k + 1.$$

Oznaczmy przez $a$ jedną z liczb układu $(U)$, a przez $(U')$ układ, w który przechodzi układ $(U)$ po usunięciu liczby $a$. Układ $(U')$ zawierać będzie $k$ nierównych sobie liczb. Zatem

na mocy chwilowo przyjętego założenia, znajdzie się w układzie tym pewna liczba najmniejsza $b$ i pewna liczba największa $c$. Oczywiście zachodzić musi jeden z układów nierówności następujących:

$$a < b < c$$

albo

$$b < a < c$$

albo

$$b < c < a.$$

W każdym razie twierdzenie, o które chodzi, byłoby sprawdzone. Zatem na podstawie zasady indukcyi matematycznej rozważane twierdzenie zachodzi istotnie w każdym razie.

Wniosek. W każdym zbiorze liczb całkowitych, zawierającym skończoną, przynajmniej jedności równą liczbę liczb, znajduje się zawsze jedna przynajmniej liczba nie większa od żadnej innej liczby zbioru i przynajmniej jedna liczba nie mniejsza od żadnej z nich.

Rozszerzając nieco znaczenie wyrazów „najmniejsza“ i „największa“, wysławiamy wniosek poprzedzający w sposób następujący: w każdym zbiorze liczb całkowitych, zawierającym skończoną, przynajmniej jedności równą liczbę liczb, istnieje przynajmniej jedna liczba najmniejsza i przynajmniej jedna liczba największa.

Jeżeli liczba najmniejszych liczb, pewnego zbioru, od jedności jest większą, to te najmniejsze liczby oczywiście są sobie równe; ten sam związek zachodzi oczywiście pomiędzy liczbami największemi, jeżeli ich liczba jest większa od jedności. Równie oczywistą jest ta okoliczność, że najmniejszą i największą liczbą zbioru, zawierającego jedną tylko liczbę, jest jednocześnie jedyna liczba do zbioru należąca.

§ 8. Nie jesteśmy jeszcze przygotowani do ostatecznego załatwienia sprawy numeracyi, której poświęcimy jeden z przyszłych rozdziałów, sądzimy jednak, że w interesie jasności stosownem będzie wprowadzić numeracyę prowizoryczną. W tym celu przyjmujemy, tytułem prowizorycznym, umowę następującą: oznaczając przez $a$ jakąkolwiek liczbę całkowitą

od jedności większą a przez $b$ liczbę, która w ciągu naturalnym liczb całkowitych poprzedza bezpośrednio liczbę $a$, przyjmiemy za symbol specyficzny liczby $a$ symbol wynikający z symbolu

$$b+1$$

przez postawienie, na miejscu litery $b$, symbolu specyficznego liczby, którą litera ta oznacza; za nazwę specyficzną liczby $a$ przyjmiemy wyrażenie, polegające na wymówieniu, po nazwie specyficznej liczby $b$, wyrazów: więcej jeden. Jeżeli uwzględnimy tę okoliczność, iż symbole i nazwy specyficzne liczb zero i jeden przyjęliśmy niezależnie od umowy poprzedzającej, to, posługując się metodą indukcyi matematycznej, łatwo okażemy, że wspomniana umowa określa w zupełności pewną numeracyę.

Przykład. Łatwo stwierdzimy, że symbolem specyficznej normalnej liczby palców u ręki ludzkiej będzie symbol

$$1+1+1+1+1,$$

a nazwą specyficzną liczby tej będzie wyrażenie: jeden więcej jeden więcej jeden więcej jeden więcej jeden. Powyższą numeracyę podaliśmy tytułem prowizorycznem, albowiem odnośna symbolistyka i terminologia oczywiście bardzo są niepraktyczne.

Uwaga. Ponieważ zwyczajne nazwy i symbole liczb całkowitych są niewątpliwie czytelnikowi znane, przeto, celem uproszczenia mowy i pisma, będziemy już w dalszym ciągu posługiwali się zwykłą terminologią i symbolistyką, nie krępując się tą okolicznością, że później dopiero zamierzamy ją wprowadzić. Postępując w ten sposób bynajmniej nie chybimy naszego celu, który polega na ściśle naukowem wyłożeniu naszego przedmiotu. Istotnie cel nasz zostanie osiągniętym, byleby dla czytelnika było całkiem jasną ta okoliczność, że mielibyśmy możność, w sprawie oznaczania i nazywania liczb całkowitych, wyłącznie poprzestać na wyżej uzyskanych wynikach aż do chwili wprowadzenia zwyczajnej terminologii i symbolistyki. Ponieważ więc wszelkie niepero-

zumienie będzie wykluczonem, przeto omówiony sposób postępowania należy uważać za całkiem usprawiedliwiony.

§ 9. Celem zapobieżenia pewnemu nieporozumieniu poświęcamy obecny paragraf następującej uwadze, krytyczny charakter mającej.

Przy elementarnem nauczaniu teoryi liczb wprowadza się, prawie powszechnie, podział liczb na dwa rodzaje, mianowicie odróżniają liczby oderwane od liczb mianowanych. Na podstawie takiego podziału liczb wyraz „pięć“ oznaczałby pewną liczbę oderwaną, a wyrażenie „pięć jabłek“ oznaczałoby liczbę mianowaną. W osnowie takiego traktowania rzeczy leży kapitalny błąd, albowiem to co nazywają liczbą mianowaną wcale żadną liczbą nie jest. Każdy zbiór przedmiotów ma pewną własność, którą oznaczamy liczbą, ale żaden zbiór liczbą nie jest. Są to stosunki zupełnie analogiczne do tych, które zachodzą n. p. pomiędzy pojęciem koloru a przedmiotami kolorowymi. Pięć jabłek nie stanowi liczby zarówno jak zielone sukno nie stanowi zielonego koloru. Jednem słowem krytykowany przez nas podział liczb na liczby oderwane i mianowane polega na bałamutnem nieodróżnieniu jednej z cech pewnej rzeczy od samej tej rzeczy.

Uwagę tę uważaliśmy za konieczną, ażeby czytelnik poznał z jakiej przyczyny omówionego podziału liczb nie wprowadzamy.

§ 10. Zakończyliśmy w ustępach poprzedzających sprawę wyłożenia podstaw teoryi liczb całkowitych i poświęcamy paragraf obecny krytycznemu przeglądowi uzyskanych wyników.

Czy podstawy teoryi liczb zostały wyczerpująco przedstawione w ustępach poprzedzających? Odpowiedź na to pytanie oczywiście mogłaby być daną dopiero po przestudyowaniu wszystkich dalszych rozdziałów, w każdym jednak razie, treść odpowiedzi zależeć będzie w pewnej mierze od osobistego uznania. Istotnie, zaznaczyliśmy zaraz na wstępie, że traktując o podstawach teoryi liczb pominęliśmy wszystko to, co razem wzięte stanowi ogólne warunki logicznego myślenia. Otóż odróżnienie właściwych podstaw teoryi liczb całkowitych

od ogólnych warunków logicznego myślenia oczywiście nie może być przeprowadzone w sposób całkiem ścisły i z konieczności musi nosić w pewnej mierze piętno umysłowości indywidualnej autora.

Drugie pytanie, które samo przez się nasuwa się, jest następujące: Czy podane aksyomaty są od siebie niezależne? W innych wyrazach: Czy jeden lub kilka z tych aksyomatów nie są logicznemi konsekwencyami aksyomatów pozostałych? Oczywiście bowiem, gdyby jedno z orzeczeń podanych pod rubrykę aksyomatów było logiczną konsekwencyą innych orzeczeń z tej samej rubryki, to omawiane orzeczenie należałoby podać nie jako aksyomat lecz jako twierdzenie, poparte stosownym dowodem. Nie sądzimy, żeby można było dać, na roztrząsane pytanie, odpowiedź całkiem zadowalniającą. Winniśmy jednak dodać, że sprawa niezależności aksyomatów jest niezawodnie drugorzędnej wagi. Istotnie uwidocznienie podstaw jakiejś gałęzi wiedzy ważnem jest tylko z tego względu, że ono umożliwia badanie stopnia pewności twierdzeń tej nauki. Otóż, z tego stanowiska, przypadek, w którym podane aksyomaty nie byłyby całkiem od siebie niezależnymi, nie mógłby być źródłem poważniejszej trudności.

Z poprzedniego wynika, że sprawa ustawienia podstaw teoryi liczb nie może być uważaną za załatwioną w sposób ostateczny we wszystkich szczegółach. Ta sama okoliczność ma jeszcze inną przyczynę: kompleks podstaw oznaczonej nauki dedukcyjnej może być, bez żadnego błędu, ustawiony w rozmaitych postaciach, albowiem pomiędzy orzeczeniami, wchodzącemi w skład rozważanej nauki można różnemi sposobami wybrać taki ich układ, który stanowić mógłby układ aksyomatów. Zatem, zależnie od sposobu załatwienia tej kwestyi pewne orzeczenie może przyjąć postać aksyomatu albo twierdzenia.

Na zakończenie winniśmy podnieść, że ta okoliczność, iż sprawa ustawienia podstaw teoryi liczb, dziś przynajmniej, nie może być uważaną za załatwioną w sposób ostateczny we wszystkich szczegółach, bynajmniej nie pociąga za sobą

tej konsekwencyi, iżby to samo można było powiedzieć o dalszych częściach tej teoryi. Zapewne zachodzą i tu także pewne różnice w sposobie traktowania przedmiotu zależnie od osobistego uznania poszczególnych autorów, jednakże wszyscy opierają się wyraźnie i wyłącznie na orzeczeniach, wyłożonych w paragrafach poprzedzających, posługując się przy tem powszechnie przyjętemi formami dowodów.

## II. Dodawanie.

§ 11. Wynikiem dodania do jakiejkolwiek liczby całkowitej $a$ jakiejkolwiek, od jedności większej, liczby całkowitej $b$, a więc liczby, która sama uważaną być może za wynik dodania jedności do pewnej, od jedności nie mniejszej liczby $k$, nazywamy wynik dodania jedności do wyniku dodania liczby $k$ do liczby $a$.

Ze względu na zasadę indukcyi matematycznej (§ 5, aks. VI) i na definicyę III (§ 3), oraz na podstawie aks. I (§ 3), winniśmy uważać wynik dodania do jakiejkolwiek liczby całkowitej $a$ każdej liczby całkowitej $b$ od jedności nie mniejszej za rzecz określoną w zupełności przez powyższą definicyę.

Żeby usunąć zastrzeżenie co do wartości liczby $b$ umawiamy się uważać za wynik dodania zera do jakiejkolwiek liczby tę samą liczbę.

Wynik dodania pewnej jakiejkolwiek liczby $b$ do pewnej jakiejkolwiek liczby $a$ oznaczamy przez symbol następujący:

$$a + b,$$

który czytamy $a$ więcej $b$.

§ 12. W interesie prostoty i przejżystości dalszych rozważań przerywamy wykład teoryi dodawania, żeby zupełnie ogólnie określić używanie nawiasu w teoryi liczb, żeby zapoznać czytelnika z pewnemi wyrażeniami technicznemi i żeby uzasadnić pewne ogólne twierdzenie.

Działaniem arytmetycznem nazywamy wszelką czynność polegającą na wyprowadzeniu z jednej liczby lub z kilku

liczb nowej liczby, zwanej wynikiem działania, w sposób określony odpowiednią definicyą.

Wzorem nazywamy wszelki symbol tak utworzony z symbolów, oznaczających pewne liczby, ażeby symbol ten przedstawiał wynik jednego działania, albo wynik pewnego układu działań wykonanych nad uważanemi liczbami.

Podając definicyę pewnego działania określamy jednocześnie zawsze wzór na wynik działania w założeniu, że każda z liczb podlegających działaniu oznaczoną jest przez pojedynczy symbol, t. j. przez symbol nie będący sam wzorem. Tak właśnie uczyniliśmy przed chwilą przy definicyi dodawania. Na pierwszy rzut oka zdawałoby się, że mając definicyę określającą sposób napisania wzoru na wynik pewnego działania ($D$) w tym przypadku, kiedy liczby, działaniu podlegające, oznaczone są przez pojedyncze symbole, możemy napisać wzór na wynik działania ($D$), jakiekolwiek byłyby symbole, oznaczające liczby podlegające działaniu, pisząc zamiast symbolów pojedynczych owe symbole. Tak jednak nie jest, albowiem wymieniony sposób postępowania mógłby doprowadzić do wzoru o znaczeniu wątpliwem. Jeżeli naprzykład, postępując omawianym sposobem, zechcemy napisać wzór na wynik dodania do pewnej liczby $a$ wyniku dodania pewnej liczby $y$ do pewnej liczby $x$, to otrzymamy wzór następujący:

$$a + x + y.$$

Otóż znaczenie wzoru tego jest wątpliwem, albowiem wzór ten mógłby zarówno uważanym być za wzór na wynik dodania liczby $y$ do wyniku dodania liczby $x$ do liczby $a$ i za wzór przedstawiający ten element, o którego przedstawienie nam chodzi. Żeby tego rodzaju wątpliwości usunąć, postępujemy w sposób następujący: jeżeli liczba, podlegająca pewnemu działaniu oznaczoną jest nie przez pojedynczy symbol, lecz przez jakikolwiek inny symbol, jeżeli przy tem nie chcemy wprowadzić osobnego pojedynczego symbolu do oznaczenia rozważanej liczby, to piszemy, zamiast takiego poje-

dynczego symbolu, zamknięty w nawiasie symbol rozważanej liczby. Na tej zasadzie wzór na wynik dodania do pewnej liczby $a$ wyniku dodania liczby $y$ do liczby $x$ będzie następujący:

$$a + (x + y).$$

W przypadkach, kiedy usunięcie nawiasu nie może spowodować żadnego nieporozumienia, oczywiście usuwamy go.

**Tw. I.** Jeżeli pewien jakikolwiek wzór $W$ określa w zupełności pewną liczbę całkowitą $a$, jeżeli dalej pewien wzór $W'$ uważany być może za wynik zastąpienia jakiejkolwiek liczby liczb wchodzących do wzoru $W$ i przedstawionych przez symbole pojedyncze, albo przez wzory je określające w zupełności, przez liczby rozważanym liczbom odpowiednio równe i przedstawione w postaci pojedynczych symbolów albo wzorów, określających je w zupełności, to wzór $W'$ przedstawia liczbę oznaczoną w zupełności, równą tej liczbie $a$, którą przedstawia wzór $W$. W innych wyrazach: przy przyjętych założeniach, mamy

$$W = W'.$$

Dowód. Równość

(1) $$W' = a$$

jest orzeczeniem wynikającem z orzeczenia

(2) $$W = a$$

przez zastąpienie w tem ostatniem pewne liczby przez liczby tym liczbom równe. Ponieważ zakładamy, ze równość (2) zachodzi istotnie, przeto (aks. V) równość (1) zachodzi niezawodnie. Z równości zaś (1) i (2) wynika (Tw. I § 4), że mamy

$$W = W''$$

co było do okazania.

§ 13. **Tw. II.** Jakiekolwiek liczby całkowite oznaczylibyśmy przez litery $a$, $b$ i $c$, mamy

$$a + (b + c) = (a + b) + c. \qquad (1)$$

Dowód. $A$) Twierdzenie jest słusznem w przypadku, kiedy mamy

$$c = 1.$$

W innych wyrazach: mamy

$$a + (b + 1) = (a + b) + 1. \tag{2}$$

Istotnie: jeżeli liczba $b$ od jedności mniejszą nie jest, to związek (2) zachodzi, albowiem w takim razie związek ten jest tylko symboliczną postacią definicyi podanej w § 11; jeżeli zaś liczba $b$ jest od jedności mniejszą, jeżeli więc liczba ta równa się zeru, to, na podstawie równości (aks. II) następującej

$$0 + 1 = 1$$

i tw. I, mamy

$$a + (0 + 1) = a + 1 \tag{3}$$

Ponieważ zaś (§ 11) mamy

$$a + 0 = a$$

przeto (tw. I)

$$(a + 0) + 1 = a + 1 \tag{4}$$

z równości (3) i (4) (tw. I § 5) wynika równość:

$$a + (0 + 1) = (a + 0) + 1.$$

Dowiedliśmy więc, że równość (2) zachodzi w każdym razie.

*B*) Zakładamy chwilowo, że, oznaczając przez $k$ pewną liczbę od jedności nie mniejszą, mamy

$$a + (b + k) = (a + b) + k \tag{5}$$

Ponieważ (patrz pod *A*) mamy

$$b + (k + 1) = (b + k) + 1,$$

przeto (tw. I)

$$a + \{b + (k + 1)\} = a + \{(b + k) + 1\}.$$

Opierając się powtórnie na wyniku uzyskanym pod *A*) oraz na tw. I, mamy

$$a + \{(b + k) + 1\} = \{a + (b + k)\} + 1$$

zatem (tw. I. § 4):

(6) $$a + \{b + (k + 1)\} = \{a + (b + k)\} + 1.$$

Na podstawie równości (5) i tw. I, mamy:

(7) $$\{a + (b + k)\} + 1 = \{(a + b) + k\} + 1.$$

Nareszcie mamy jeszcze (patrz pod *A*)):

(8) $$\{(a + b) + k\} + 1 = (a + b) + (k + 1).$$

Równości (6), (7) i (8) pociągają za sobą równość następującą:

(9) $$a + \{b + (k + 1)\} = (a + b) + (k + 1)$$

Dowiedliśmy więc co następuje: gdyby równość (5) zachodziła, to zachodziłaby także równość (9). W innych wyrazach: gdyby równość (1) zachodziła w razie kiedy mamy

$$c = k,$$

oznaczając przez $k$ liczbę całkowitą od jedności nie mniejszą, to, równość rozważana zachodziłaby także w razie kiedy mamy

$$c = k + 1.$$

*C*) Na podstawie wyników uzyskanych pod *A*) i pod *B*) i ze względu na zasadę indukcyi matematycznej związek (1) zachodzi niezawodnie, jeżeli tylko liczba $c$ nie jest od jedności mniejszą.

*D*) Opierając się na definicyi podanej w § 11 oraz na tw. I. stwierdzimy łatwo, że związek (1) zachodzi także w razie kiedy mamy

$$c = o$$

*E*) Z wyników uzyskanych pod *C*) i pod *D*) wnosimy natychmiast, że twierdzenie słuszne jest w podanem brzmieniu.

**Tw. III.** Jakiekolwiek liczby całkowite oznaczałyby litery $a$ i $b$ mamy

$$a + b = b + a \qquad (1)$$

Dowód.

*A*) Twierdzenie jest oczywiście słuszne w przypadku, gdy mamy

$$a = b = 0$$

*B*) Załóżmy chwilowo, że równość (1) zachodzi w razie, kiedy liczba $a$ równa się zeru a liczba $b$ — pewnej liczbie $k$. Będziemy tedy mieli:

$$0 + k = k + 0 \tag{2}$$

Mamy (Tw. II.)

$$0 + (k + 1) = (0 + k) + 1.$$

Ze względu zaś na (2) i na tw. I. mamy:

$$(0 + k) + 1 = (k + 0) + 1$$

Zatem

$$0 + (k + 1) = (k + 0) + 1 \tag{3}$$

Ponieważ (§ 11)

$$k + 0 = k,$$

przeto

$$(k + 0) + 1 = k + 1 \tag{4}$$

Z równości (3) i (4) wnosimy, że

$$0 + (k + 1) = k + 1$$

A ponieważ

$$(k + 1) + 0 = k + 1,$$

przeto

$$0 + (k + 1) = (k + 1) + 0. \tag{5}$$

Dowiedliśmy więc, że, gdyby związek (2) zachodził, to związek (5) zachodziłby także.

*C*) Posługując się zasadą indukcyi matematycznej oraz wynikami uzyskanemi pod *A*) i pod *B*) dochodzimy do wniosku następującego: jakakolwiek byłaby liczba $b$, mamy

$$0 + b = b + 0.$$

*D*) Załóżmy chwilowo, że dla pewnej liczby $k$ mamy

(6) $$1 + k = k + 1$$

Mamy (Tw. II):

$$1+(k+1)=(1+k)+1.$$

A ponieważ, ze względu na równość (6), mamy:

$$(1+k)+1=(k+1)+1,$$

przeto

(7) $$1+(k+1)=(k+1)+1.$$

Zatem, gdyby równość (6) zachodziła istotnie, to zachodziłaby także równość (7). Ponieważ zaś równość (6) zachodzi rzeczywiście (patrz pod *C*)) w razie kiedy litera $k$ oznącza liczbę zero, przeto, na mocy zasady indukcyi matematycznej, mamy:

$$1+b=b+1$$

jakąkolwiek liczbę ornaczałaby litera $b$.

*E*) Załóżmy chwilowo że, dla pewnej liczby $k$ mamy

(8) $$k+b=b+k$$

jakąkolwiek liczbę oznaczałaby litera $b$.

Mamy (Tw. II):

$$b+(k+1)=(b+k)+1$$

Ponieważ zaś, ze względu na (8) i w tw. I., mamy

$$(b+k)+1=(k+b)+1,$$

Przeto

$$b+(k+1)=(k+b)+1$$

Ponieważ dalej (Tw. II)

$$(k+b)+1=k+(b+1)$$

Przeto

$$b+(k+1)=k+(b+1)$$

Ponieważ zaś, na podstawie wyniku uzyskanego pod *D*), mamy

$$k+(b+1)=k+(1+b),$$

przeto

$$b + (k + 1) = k + (1 + b)$$

Zważywszy teraz (Tw. II.), że mamy

$$k + (1 + b) = (k + 1) + b$$

znajdziemy:

$$b + (k + 1) = (k + 1) + b. \tag{9}$$

Dowiedliśmy więc, że, gdyby zachodził związek (8) to zachodziłby także związek (9). A ponieważ, na podstawie wyniku uzyskanego pod *D*), związek (8) zachodzi istotnie w razie kiedy mamy

$$k = 1,$$

przeto, na podstawie zasady indukcyi matematycznej, związek (1) zachodzi pod jedynym warunkiem, że liczba $a$ nie jest mniejsze od jedności. Ponieważ jednak dowiedliśmy pod *C*), że związek (1) zachodzi w razie, kiedy mamy $a = 0$, przeto dochodzimy ostatecznie do wniosku, iż związek (1) zachodzi jakiekolwiek byłyby liczby $a$ i $b$. Co było do okazania.

§ 14. Skończony zbiór przedmiotów pomyślanych w oznaczonym porządku stanowi to, co nazywamy p e r m u t a c y ą tych przedmiotów. Zatem wyraz „permutacya“ oznacza to samo, co wyrażenie „ciąg składający się ze skończonej liczby przedmiotów“ czyli „ciąg skończony“. Przedmioty, z których składa się pewna permutacya, zowią się elementami tej permutacyi. Numerem porządkowym elementu permutacyi jest liczba, oznaczająca numer porządkowy uważanego elementu w tym ciągu, który stanowi rozważaną permutacyę. Elementami sąsiednimi pewnej permutacyi nazywamy każde takie dwa jej elementy, z których jeden poprzedza bezpośrednio drugi. Jeżeli w pewnej permutacyi $P$ pewnych przedmiotów przemienimy numery porządkowe pewnych dwóch elementów $E$ i $E'$, pozostawiając bez zmiany numery porządkowe wszystkich innych elementów, to uzyskamy nową permutacyę $P'$

tych samych przedmiotów; stosunek wzajemny permutacyj $P$ i $P'$ wyrażamy, orzekając, że te permutacye wynikają jedna z drugiej drogą transpozycyi elementów $E$ i $E'$.

**Tw. IV.** (przygotowawcze). Jeżeli w pewnej permutacyi $P$, przedmiotów stanowiących pewien zbiór $(z)$, pewien element $A$ nie jest ostatnim elementem, to możemy zawsze z permutacyj przedmiotów zbioru $(z)$ ułożyć ciąg $(C)$, sprawdzający warunki następujące:

1) Pierwszym elementem ciągu $(C)$ jest permutacya $P$.

2) Każda dalsza permutacya ciągu tego jest wynikiem transpozycyi pewnych dwóch elementów sąsiednich w permutacyi poprzedzającej.

3) Ostatnim elementem ciągu $(C)$ jest taka permutacya, w której element $A$ jest elementem ostatnim. Twierdzenie to wysławiamy krótko w sposób następujący: dany element danej permutacyi możemy zawsze przenieść na ostatnie miejsce przez wykonanie pewnej skończonej liczby transpozycyj elementów sąsiednich.

Dowód. Twierdzenie to jest oczywiste w razie, kiedy element $A$ jest przedostatnim elementem uważanej permutacyi $P$, albowiem ciąg $(C)$ utworzyć możemy tedy z permutacyi $P$ i z permutacyi, w którą przejdzie permutacya $P$ po wykonaniu transpozycyi elementu $A$ i elementu ostatniego. Załóżmy chwilowo, że twierdzenie zachodzi w razie, kiedy liczba $m$ elementów następujących w permutacyi $P$ po elemencie $A$ równa się pewnej liczbie całkowitej $k$ i zwróćmy się do przypadku, w którym mamy

$$m = k + 1.$$

Oznaczmy przez $P'$ permutacyę uzyskaną drogą transpozycyi, w permutacyi $P$, elementu $A$ z elementem następującym bezpośrednio po tym elemencie. Na podstawie chwilowo przyjętego założenia permutacya $P'$ uważaną być może za pierwszy element pewnego ciągu $(C')$, w którym każdym dalszym elementem będzie permutacya wynikająca z permutacyi, stanowiącej element poprzedzający, drogą transpozycyi dwóch

elementów sąsiednich i którego ostatnim elementem będzie taka permutacya, w której element $A$ będzie elementem ostatnim. Jeżeli do ciągu $(C')$ dołączymy permutacyę $P$ w taki sposób, żeby w nowym ciągu permutacya ta stanowiła element pierwszy, to uzyskamy oczywiście ciąg sprawdzający warunki twierdzenia. Wnosimy stąd, opierając się na zasadzie indukcyi matematycznej, że twierdzenie, które pragnęliśmy uzasadnić, istotnie zachodzi.

**Tw. V.** Jeżeli oznaczymy przez $P$ i $P'$ dwie jakiekolwiek nie identyczne permutacye tych samych $n$ elementów, to permutacye te zawsze uważać możemy za skrajne elementy takiego ciągu $(C)$ permutacyj, z których każda wynika z permutacyi sąsiedniej drogą transpozycyi dwóch elementów sąsiednich. Krócej: każdą permutacyę oznaczonych przedmiotów możemy przemienić w każdą inną permutacyę tychże przedmiotów przez wykonanie stosownego ciągu transpozycyj elementów sąsiednich.

Dowód. W razie kiedy liczba $n$ równa się dwom, możemy oczywiście przyjąć za pierwszy element ciągu $(C)$ permutacyę $P$ a za element drugi i ostatni permutacyę $P'$. Zatem, w tym razie twierdzenie zachodzi niezawodnie. Zakładam chwilowo, że twierdzenie zachodzi w przypadku kiedy mamy

$$n = k;\ (k \geqq 2)$$

i przyjmuję

$$n = k + 1.$$

Dwa przypadki nadarzyć się mogą:

1° Ostatni element $A$ permutacyi $P'$ jest także ostatnim elementem permutacyi $P$. Jeżeli tedy usuniemy element $A$ z każdej z permutacyj $P$ i $P'$, to uzyskamy oczywiście dwie permutacye $Q$ i $Q'$ pewnych tych samych $k$ przedmiotów.

Na podstawie chwilowo przyjętego założenia możemy uważać permutacye $Q$ i $Q'$ za skrajne elementy pewnego ciągu $(C')$, sprawdzającego warunki, które czytelnik łatwo wysłowi. Do każdej permutacyi ciągu $(C')$ dołączam element $A$ w taki sposób, żeby w każdej z uzyskanych permutacyi element A był ele-

mentem ostatnim. W takim razie ciąg $(C')$ przemieni się w pewien ciąg $(C)$, który oczywiście sprawdzać będzie warunki twierdzenia.

2° Ostatni element $A$ permutacyi $P'$ nie jest ostatnim elementem permutacyi $P$. Na podstawie twierdzenia poprzedzającego możemy uważać permutacyę $P$ za pierwszy element ciągu $(C_1)$, sprawdzającego warunki wspomnianego twierdzenia. Ostatnim elementem ciągu $(C_1)$ będzie pewna permutacya $P_1$, której ostatnim elementem będzie element $A$. Zatem, ze względu na wynik uzyskany przy omawianiu przypadku pierwszego, możemy ciąg $(C_1)$ w taki sposób uzupełnić, żeby uzyskać ciąg $(C)$ sprawdzający warunki twierdzenia obecnego.

Łącząc wyniki uzyskane przy badaniu dwóch przypadków poprzedzających, dochodzimy do wniosku następującego: gdyby twierdzenie zachodziło w razie, kiedy mamy

$$n = k,$$

to twierdzenie zachodziłoby także w przypadku, w którym mielibyśmy

$$n = k + 1.$$

Ponieważ stwierdziliśmy wyżej, że twierdzenie zachodzi istotnie w razie, kiedy mamy

$$n = 2,$$

przeto, na podstawie zasady indukcyi matematycznej, twierdzenie zachodzi w każdym razie, co było do okazania.

**Tw. VI.** Jeżeli, na mocy pewnej umowy, każdej permutacyi pewnych $n$ przedmiotów odpowiada oznaczona liczba, jeżeli nadto liczby odpowiadające dwom permutacyom, z których każda może być przemieniona w drugą drogą transpozycyi dwóch elementów sąsiednich, zawsze są sobie równe, to dwie liczby odpowiadające dwom jakimkolwiek permutacyom rozważanych przedmiotów zawsze są sobie równe.

D o w ó d. Oznaczmy przez $z$ i $z'$ liczby odpowiadające dwom jakimkolwiek permutacyom $P$ i $P'$ rozważanych przedmiotów.

Na podstawie twierdzenia poprzedzającego liczby $z$ i $z'$ mogą oczywiście być uważane za skrajne wyrazy takiego ciągu następujących po sobie liczb, w którym dwie liczby sąsiednie są sobie równe. Ponieważ zaś, opierając się na tw. I (§ 4) łatwo możemy dowieść, drogą indukcyi matematycznej, że we wspomnianym ciągu liczb każde dwie liczby są sobie równe, przeto wnosimy, że równość:

$$z = z'$$

o uzasadnienie której chodzi, istotnie zachodzić będzie.

§ 15. Uważajmy tyle danych liczb, ile wynosi pewna liczba całkowita $n$ od jedności większa i, po ustawieniu tych liczb w pewnym dowolnie obranym porządku, oznaczmy ogólnie przez $a_i$ tę z nich, której numerem porządkowym jest liczba $i$. Przyjmijmy następnie

$$s_1 = a_1$$

i ogólnie,

$$s_{i+1} = s_i + a_{i+1}.$$

W takim razie, na podstawie zasady indukcyi matematycznej, symbol $s_n$ oczywiście oznaczać będzie pewną określoną liczbę. Liczba $s_n$ zwie się sumą danych $n$ liczb, a same te liczby zowią się składnikami rozważanej sumy.

W interesie zwięzłości umawiamy się rozumieć pod wyrażeniem „suma liczb należących do pewnego zbioru $(z)$“, w razie gdyby zbiór $(z)$ zawierał jedną tylko liczbę, — samą tę liczbę; a w przypadku, w którymby nie istniała żadna liczba do zbioru $(z)$ należąca — liczbę zero.

Opierając się na podanym w § 12 określeniu użycia nawiasu, możemy oczywiście napisać bezpośrednio wzór na sumę kilku danych składników, rozważanych w jakimkolwiek przypisanym z góry porządku, nie wprowadzając żadnej nowej definicyi. Na przykład, wzorem na sumę składników $a$, $b$, $c$ i $d$, rozważanych w porządku, w którym je wymieniliśmy, będzie oczywiście wzór następujący:

$$((a + b) + c) + d.$$

**Tw. VII.** Wartość sumy kilku oznaczonych składników od przyjętego dla nich porządkn nie zależy.

Dowód. Ze względu na tw. VI, twierdzenie obecne uzasadnimy w zupełności, jeżeli tylko okażemy, że przemiana numerów porządkowych dwóch składników sąsiednich na wartość sumy nie wpływa. Załóżmy chwilowo, że okoliczność ta zachodzi istotnie w razie, kiedy liczba składników sumy nie przekracza pewnej liczby $k$ ($k \geqq 2$) i oznaczmy przez $s$ jakąkolwiek sumę o $k+1$ składnikach. Oznaczmy przez $c$ składnik, następujący w sumie $s$, bezpośrednio po pewnym składniku $b$, a przez $s'$ sumę, w którą przeszłaby suma $s$, gdybyśmy przemienili w niej numery porządkowe składników $b$ i $c$. Załóżmy najpierw, że składnik $c$ nie jest ostatnim składnikiem sumy $s$. W takim razie ostatnie składniki sum $s$ i $s'$ równać się będą pewnej tej samej liczbie $d$ i wtedy na sumy $s$ i $s'$ będziemy mieli wzory następujące

$$(1) \qquad \begin{cases} s = \sigma + d \\ s' = \sigma' + d \end{cases}$$

oznaczając przez $\sigma$ i $\sigma'$ dwie sumy pewnych tych samych $k$ składników. Pewne dwa sąsiednie składniki sumy $\sigma$ równać się będą odpowiednio liczbom $b$ i $c$, a suma $\sigma'$ będzie sumą, w którą przejdzie suma $\sigma$ jeżeli tylko przemienimy w niej numery sąsiednich składników $b$ i $c$. Przeto, na podstawie przyjętego chwilowo założenia mieć będziemy:

$$\sigma = \sigma'.$$

Zatem, na podstawie tw. I, wnosimy z równości (1) że mamy:

$$s = s'.$$

Pozostaje do zbadania przypadek, w którym składnik $c$ jest ostatnim składnikiem sumy $s$. Oznaczając tedy przez $a$ sumę tych składników sumy $s$, które poprzedzają składniki $b$ i $c$, mamy:

$$(2) \qquad s = (a + b) + c.$$

Na sumę $s'$ będziemy tedy mieli wzór następujący:

$$s' = (a + c) + b. \tag{3}$$

Ze wzorów (2) i (3) wnosimy na podstawie tw. II, że mamy

$$s = a + (b + c)$$
$$s' = a + (c + b).$$

A ponieważ (tw. III) mamy

$$b + c = c + b$$

przeto, oznaczając przez $f$ wspólną wartość sum

$$b + c \text{ i } c + b$$

znajdujemy, iż

$$s = a + f$$
$$s' = a + f$$

skąd

$$s = s'$$

Dowiedliśmy zatem co następuje: gdyby w sumie zawierającej $k$ składników przemiana numerów dwóch składników sąsiednich nie miała wpływu na wartość sumy, to ta sama okoliczność zachodziłaby także co do sumy, zawierającej $k + 1$ składników. Ponieważ zaś rozważana okoliczność zachodzi istotnie w przypadku, kiedy suma zawiera dwa składniki (tw. III), przeto przemiana numerów dwóch składników sąsiednich w jakiejkolwiek sumie pozostaje bez wpływu na jej wartość. Ze względu na uwagę uczynioną na początku dowodu uzasadniliśmy tem samem twierdzenie, o które chodziło.

**Tw. VIII.** Suma, w którą przemieni się jakakolwiek dana suma przez to, że zastąpimy w niej kilka którychkolwiek składników przez składnik równy ich sumie, równa się sumie danej.

Dowód. Oznaczmy przez $s$ sumę daną a przez $(A)$ zbiór $k$ którykolwiek jej składników. Uporządkujmy składniki sumy danej w taki sposób, żeby zbiór $k$ pierwszych składników sta-

nowił właśnie zbiór $(A)$. Oznaczmy następnie ogólnie przez $a_i$ składnik rzędu $i$ — i przyjmijmy:

$$s_1 = a_1$$

oraz ogólnie

$$s_{i+1} = s_i + a_i.$$

Będziemy tedy mieli

$$s = s_n \tag{1}$$

na podstawie definicyi sumy i twierdzenia poprzedzającego Z drugiej strony, z definicyi liczby $s_n$ wynika bezpośrednio, że liczba ta równa się sumie, której jeden składnik jest liczbą $s_k$ a inne składniki są tymi składnikami sumy $s$, które, w przyjętym dla nich porządku, następują po składniku $a_k$. Zatem, na podstawie równości (1) suma $s$ równa się także sumie liczby $s_k$ i tych składników sumy $s_n$, które następują po składniku $a_k$. A ponieważ liczba $s_k$ przedstawia sumę, zbiór $(A)$ stanowiących składników sumy $s$, przeto suma $s$ równa się sumie sumy składników tworzących zbiór (A) i składników pozostałych, co było do okazania.

**Tw. IX.** Suma, w którą przejdzie jakakolwiek dana suma $s$ przez to, że zastąpimy w niej jeden którykolwiek składnik $a$ przez kilka składników, których suma równa się liczbie $a$, równa się sumie $s$.

Dla dowodu należy tylko podnieść, że twierdzenie obecne wyraża w nowych wyrazach, to samo co twierdzenie poprzedzające.

Uwaga. Na podstawie twierdzeń VII, VIII i IX możemy we wzorze na jakąkolwiek kombinacyę kilku liczb drogą dodawania opuścić nawiasy bez obawy, żeby stąd mogłą wyniknąć jakakolwiek wątpliwość co do wartości liczby, którą przedstawiałby tedy rozważany wzór.

§ 16. **Tw. X.** Oznaczmy przez $a$ jakąkolwiek liczbę całkowitą a przez $b$ liczbę całkowitą od zera odmienną, ale pozatem jakąkolwiek. Uważajmy następnie, w ciągu naturalnym

liczb całkowitych $b$ pierwsze liczby następujące po liczbie $a$ i niech $c$ oznacza ostatnią z tych liczb. Powiadam, że mamy:

$$c = a + b.$$

Dowód. Twierdzenie zachodzi isotnie w przypadku, kiedy mamy

$$b = 1,$$

na podstawie def. VI (§ 3).

Zakładamy chwilowo, że twierdzenie zachodzi w razie, kiedy liczba $b$ ma pewną wartość $b'$ i oznaczamy przez $c'$ odnośną wartość liczby $c$. Mamy tedy

$$c' = a + b'. \tag{1}$$

Przyjmijmy

$$b = b' + 1. \tag{2}$$

W takim razie liczba $c$ będzie liczbą następującą bezpośrednio w ciągu naturalnym liczb całkowitych po liczbie $c'$. Mamy więc

$$c = c' + 1.$$

Skąd:

$$c = (a + b') + 1 \tag{3}$$

na podstawie związku (1).

Opierając się na def. z § 11 wyprowadzamy z równości (3) równość:

$$c = a + (b' + 1)$$

skąd

$$c = a + b$$

na postawie równości (2). Dowiedliśmy więc, że, gdyby twierdzenie zachodziło wtedy, kiedy liczba $b$ ma pewną wartość $b'$, to twierdzenie to zachodziłoby jeszcze i w tym razie, kiedy mielibyśmy:

$$b = b' + 1.$$

Ponieważ zaś stwierdzilibyśmy, że twierdzenie zachodzi istotnie w przypadku, kiedy mamy

$$b = 1,$$

przeto, na podstawie zasady indukcyi matematycznej wnosimy, że twierdzenie zachodzi w podanem brzmieniu.

Wniosek. Jeżeli oznaczymy przez $b$ jakąkolwiek liczbę całkowitą sprawdzającą nierówność

$$b > 0,$$

to, jakąkolwiek liczbę całkowitą oznaczylibyśmy przez $a$, mieć będziemy

$$a + b > a.$$

Istotnie, że względu na twierdzenie poprzedzające, liczba $a + b$ nastąpi w ciągu naturalnym liczb całkowitych, bezpośrednio lub pośrednio po liczbie $a$. Zatem (def. VIII, § 4) liczba

$$a + b$$

będzie rzeczywiście w każdym razie większą od liczby $a$.

**Tw. XI.** Suma dwóch liczb całkowitych $a$ i $b$ równa się liczbie przedmiotów zawartych w zbiorze $(C)$, będącym wynikiem złączenia dwóch zbiorów $(A)$ i $(B)$, zawierających odpowiednio tyle przedmiotów ile wynoszą liczby $a$ i $b$.

Dowód. Jeżeli jedna z liczb $a$ i $b$, powiedzmy $b$, równa się zeru, to twierdzenie zachodzi. Istonie, w rozważanym przypadku zbiór $(C)$ oczywiście nie różni się od zbioru $(A)$ i dla tego zawiera $a$ przedmiotów. Z drugiej strony, ponieważ

$$b = 0,$$

przeto

$$a + b = a.$$

Czyli liczba przedmiotów zawartych w zbiorze $(C)$ równa się rzeczywiście sumie liczb $a$ i $b$. Pozostaje więc do zbadania przypadek, kiedy żadna z liczb $a$ i $b$ nie równa się zeru.

Ponieważ, w stosunku do twierdzenia, o które chodzi, natura przedmiotów należących do zbiorów $(A)$ i $(B)$ jest obojętną, przeto, żeby twierdzenie uzasadnić, możemy, bez szkody dla ogólności, wyszczególnić wedle upodobania przedmioty, mające należeć do powyższych zbiorów. Korzystając z tej uwagi określimy zbiory $(A)$ i $(B)$ w sposób następujący. Uwa-

żajmy w ciągu naturalnym liczb całkowitych wszystkie liczby od jedności aż do $a$ włącznie. Na podstawie tw. VII (§ 6) liczba tych liczb równać się będzie liczbie $a$. Zbiór tych liczb przyjmujemy za zbiór $(A)$. Żeby określić zbiór $(B)$ uważajmy, w ciągu naturalnym liczb całkowitych, $b$ pierwsze liczby następujące po liczbie $a$ i oznaczmy ostatnią z nich przez $c$. Za zbiór $(B)$ przyjmijmy zbiór wspomnianych $b$ liczb. W takim razie zbiór $(C)$ stanowić będą liczby całkowite ciągu naturalnego liczb całkowitych od jedności aż do liczby $c$ włącznie. Na podstawie tw. VII (§ 6) liczba liczb stanowiących zbiór $(C)$ równać się będzie liczbie $c$. Z drugiej strony, na podstawie twierdzenia poprzedzającego mamy

$$c = a + b.$$

Równość ta opiewa, że liczba przedmiotów stanowiących zbiór $(C)$ równa się sumie liczb $a$ i $b$, co było do okazania.

Wniosek. Suma kilku liczb całkowitych równa się liczbie przedmiotów zawartych w zbiorze, będącym wynikiem złączenia zbiorów zawierających odpowiednio tyle przedmiotów, ile wynoszą składniki rozważonej sumy. Wniosek ten czytelnik łatwo uzasadni drogą indukcyi matematycznej.

## III. Odejmowanie.

§ 17. Odejmowaniem nazywamy działanie, polegające na wyznaczeniu takiej liczby $r$, żeby wynik dodania liczby tej do pewnej danej liczby $b$ równał się pewnej innej danej liczbie $a$. Liczby $a$, $b$ i $r$ nazywamy odpowiednio: odjemną, odjemnikiem i resztą albo różnicą. Na różnicę odjemnej $a$ i odjemnika $b$ przyjmujemy wzór następujący:

$$a - b,$$

który czytamy: $a$ mniej $b$. Mamy zatem

$$r = a - o \tag{1}$$

oznaczając, jak wyżej, przez $r$ różnicę.

Na podstawie tw. III (rozd. II) podana przed chwilą definicya odejmowania oczywiście równoważną jest definicyi następującej: odejmowaniem nazywamy czynność polegającą na wyznaczeniu jednego ze składników sumy dwóch składników przy danych: wartości jednego z nich i wartości sumy.

Jeżeli z dwóch równości żadna nie może zachodzić bez tego, żeby zachodziła także druga z nich, to uważane równości nazywamy równoważnemi.

Z definicyi różnicy wynika bezpośrednio, iż równość (1) równoważną jest równości następującej:

$$b + r = a$$

czyli

$$b + (a - b) = a.$$

Określiwszy działanie odejmowania winniśmy wyprowadzić warunki wykonalności tego działania i upewnić się, kiedy warunki te są spełnione, czy wartość wyniku określoną jest w zupełności w zależności od wartości elementów danych t. j. odjemnej i odjemnika.

§ 18. Odpowiedź na pytania poprzedzające stanowi twierdzenie następujące:

**Tw. I.** Żeby odejmowanie było wykonalne, koniecznem jest i wystarcza żeby odjemnik nie był większym od odjemnej. Kiedy warunek ten jest spełniony, reszta jest określoną w zupełności w zależności od odjemnika i od odjemnej, mianowicie: jeżeli odjemnik równa się odjemnej to reszta jest zerem, jeżeli zaś odjemnik $b$ mniejszym jest od odjemnej $a$, to reszta równa się liczbie liczb następujacych w ciągu naturalnym liczb całkowitych po liczbie $b$ do liczby $a$ włącznie i jest zatem większą od zera.

Dowód. *A*) Podany warunek wykonalności działania jest konieczny. Oznaczając przez $a$, $b$ i $r$ odjemną, odjemnik i resztę, mamy:

(1) $$b + r = a$$

na podstawie definicyi odejmowania. Jeżeli mamy

(2) $$r = 0$$

to z równości (1) wynika równość

$$b = a. \tag{3}$$

Jeżeli zaś jest

$$r > 0,$$

to

$$b < a \tag{4}$$

na podstawie wniosku z tw. X (§ 16). Przeto, związek:

$$b \leqq a \tag{5}$$

jest istotnie koniecznym warunkiem wykonalności działania.

*B*) Podany warunek zapewnia wykonalność odejmowania a zapowiedziana w twierdzeniu wartość reszty sprawdza definicyę tejże. Jeżeli bowiem zachodzi równość (3), to wartość (2) na $r$ oczywiście czyni zadość równości (1). Jeżeli zaś zachodzi nierówność (4) to, na podstawie tw. X (§ 16), uczynimy zadość równości (1) oznaczając przez $r$ liczbę liczb następujących w ciągu naturalnym liczb całkowitych, po liczbie $b$ do liczby $a$ włącznie. Ponieważ wszelka wartość na $r$, czyniąca zadość równości (1), sprawdza definicyę reszty

$$a - b,$$

przeto uzasadniliśmy punkt, o który chodziło.

*C*) Reszta, o ile istnieje, określona jest w zupełności w zależności od odjemnej i od odjemnika. Istotnie załóżmy, że dwie nierówne sobie liczby sprawdzają definicyę reszty przy danych odjemnej $a$ i odjemniku $b$ i oznaczmy mniejszą z tych liczb przez $r'$, a drugą przez $r''$. Będziemy tedy mieli

$$b + r' = a \tag{6}$$

$$b + r'' = a \tag{7}$$

$$r' < r''. \tag{8}$$

Ze względu na wynik uzyskany pod *B*) możemy przyjąć:

$$r'' = r' + d$$

oznaczając przez $d$ liczbę od zera odmienną. Mamy tedy

$$b + r'' = b + (r' + d) = (b + r') + d$$

skąd

$$b + r'' > b + r' \tag{9}$$

na podstawie wniosku z tw. X. (§ 16).

Ponieważ związek (9) znajduje się w sprzeczności ze związkami (6) i (7), przeto stwierdzamy, że założenie, iż dwie nierówne sobie liczby sprawdzają definicyę reszty przy danych odjemnej i odjemniku, doprowadza do sprzeczności, a więc nigdy urzeczywistnić się nie może. Dowiedliśmy więc w zupełności twierdzenia, o które chodziło.

Wniosek I. Dwie jakiekolwiek liczby całkowite $a$ i $b$ mogą zawsze być skombinowane jedna z drugą drogą odejmowania, a wynik takiej kombinacyi, czyli różnica uważanych liczb, jest zawsze określony w zupełności w zależności od tych liczb. Istotnie, jeżeli rozważane liczby są sobie równe, to którąkolwiek z nich możemy przyjąć za odjemnik, ale różnica będzie w każdym razie równać się zeru; jeżeli zaś liczby $a$ i $b$ równe sobie nie są, to na podstawie twierdzenia poprzedzającego możemy je skombinować drogą odejmowania, ale tylko w taki sposób, żeby odjemnikiem była mniejsza z nich; zatem w tym przypadku także różnica określoną będzie w zupełności.

Wniosek. II. Jeżeli liczby całkowite $a$ i $b$ sprawdzają nierówność

$$a > b$$

to, jakąkolwiek liczbę całkowitą oznaczyliśmy przez $c$, mieć będziemy:

$$a + c > b + c.$$

Istotnie, oznaczając przez $r$ różnicę liczb $a$ i $b$ mamy

$$a = b + r$$

oraz

$$r > 0.$$

A ponieważ

$$a + c = (b + r) + c = (b + c) + r$$

przeto rzeczywiście:

$$a + c > b + c$$

na podstawie wniosku z tw. X (§ 16).

§ 19. **Tw. II.** Oznaczając przez $a$ jakąkolwiek liczbę całkowitą a przez $b$ i $c$ dwie liczby całkowite, sprawdzające warunek następujący:

$$b \geqq c, \tag{1}$$

ale pozatem jakiekolwiek, mamy w każdym razie:

$$a + (b - c) = (a + b) - c. \tag{2}$$

Nadto, jeżeli mamy

$$a \geqq b - c \tag{3}$$

to mamy

$$a - (b - c) = (a + c) - b; \tag{4}$$

jeżeli zaś zachodzi związek

$$a \leqq b - c \tag{5}$$

to mamy

$$(b - c) - a = b - (a + c). \tag{6}$$

Dowód. Podnosimy przedewszystkiem, że warunki pod którymi zapowiedzieliśmy istnienie każdej z równości (2), (4) i (6), są istotne; gdyby bowiem jeden z tych warunków spełniony nie był, to lewa strona odnośnej równości oczywiście pozbawioną byłaby sensu.

Żeby uzasadnić równość (2) przyjmujemy:

$$x = a + (b - c). \tag{7}$$

Mamy tedy:

$$x + c = \{a + (b - c)\} + c$$

skąd

$$x + c = a + \{(b - c) + c\}$$

na podstawie tw. II (§ 13).

Ponieważ

$$(b - c) + c = b$$

na podstawie definicyi odejmowania, przeto

$$x + c = a + b$$

skąd

$$x = (a + b) - c \tag{8}$$

znowu na podstawie definicyi odejmowania. Równości (7) i (8) pociągają za sobą równość (2), którą pragnęliśmy uzasadnić.

Przechodząc do dowodu równości (4) przyjmijmy:

(9) $$y = a - (b - c).$$

Mamy

$$y + b = y + \{(b - c) + c\}$$

skąd

$$y + b = \{y + (b - c)\} + c$$

na podstawie tw. II (§ 13).

Ponieważ

$$y + (b - c) = a,$$

na podstawie równości (9), przeto

$$y + b = a + c$$

skąd

(10) $$y = (a + c) - b.$$

Równości (9) i (10) pociągają za sobą równość (4), o uzasadnienie której właśnie chodziło.

Żeby nareszcie uzasadnić równość (6) przyjmijmy:

(11) $$z = (b - c) - a.$$

Mamy

$$z + (a + c) = (z + a) + c$$

na podstawie tw. II (§ 13). Ponieważ zaś

$$z + a = b - c,$$

na postawie równości (11), przeto

$$z + (a + c) = (b - c) + c$$

czyli

$$z + (a + c) = b$$

skąd

(12) $$z = b - (a + c).$$

Równości (11) i (12) pociągają za sobą równość (6). Zatem uzasadniliśmy w zupełności twierdzenie o dowód którego chodziło.

**Tw. III.** Wynik $w$ wszelkiej kombinacyi określonej liczby liczb, stanowiących pewien zbiór $(z)$, drogą skończonego ciągu działań, z których każde polega na kombinowaniu dwóch wyrażeń przez dodawanie lub odejmowanie, równa się, o ile istnieje, a więc o ile spełnione są warunki wykonalności odnośnych działań, albo sumie rozważanych liczb albo różnicy sumy pewnych z tych liczb i sumy liczb pozostałych.

Dowód. Liczba $w$ musi być wynikiem przynajmniej dwóch po sobie następujących działań, albowiem inaczej twierdzenie pozbawionem byłoby treści.

Załóżmy na początek, że liczba $w$ jest wynikiem dwóch po sobie następujących działań. W takim razie liczba $w$ będzie wynikiem kombinacyi pewnej liczby $a$ drogą jednego z dwóch rozważanych działań: albo z summą dwóch innych liczb, albo z ich różnicą. W pierwszym przypadku twierdzenie nasze byłoby prostą tautologią; zwracamy się więc natychmiast do przypadku drugiego, to jest do przypadku, w którym kombinujemy liczbę $a$ z różnicą

$$b - c$$

pewnych dwóch liczb. Dodawanie prowadzi do jednej tylko kombinacyi, mianowicie do kombinacyi

$$a + (b - c).$$

Odejmowanie zaś, zależnie od względnego położenia liczb

$$a \text{ i } (b - c)$$

w ciągu naturalnym liczb całkowitych prowadzi do jednej z kombinacyi następujących:

$$a - (b - c) \text{ albo } (b - c) - a.$$

Na podstawie twierdzenia poprzedzającego stwierdzamy, że w każdym z przypadków poprzedzających możemy przedstawić liczbę $w$ przez wzór zapowiedzianego kształtu. Zatem uzasadniliśmy twierdzenie w razie, kiedy liczba $w$ jest wynikiem dwóch po sobie następujących działań.

Załóżmy chwilowo, że twierdzenie zachodzi w razie, kiedy liczba $n$ działań, których wynikiem jest liczba $w$, nie przekracza pewnej liczby $k$ ($k \geqq 2$) i przejdźmy do przypadku, kiedy mamy

$$n = k + 1.$$

Z definicyi liczby $w$ wynika, że mamy na liczbę $w$ jeden ze wzorów następujących:

(1) $$w = w_1 + w_2$$

albo

(2) $$w = w_1 - w_2$$

gdzie każda z liczb $w_1$ i $w_2$, o ile nie jest sama jedną z liczb stanowiących zbiór $(z)$, jest albo kombinacyą, przez jedno z rozważanych działań, dwóch liczb, należących do zbioru $(z)$, albo liczbę utworzoną z liczb, należących do zbioru $(z)$, drogą wykonania najwyżej tylu działań, z których każde polega na kombinowaniu dwóch wyrażeń drogą dodawania lub odejmowania, ile wynosi liczba $k$. Na podstawie tych uwag i chwilowo przyjętego założenia, stwierdzamy, że będziemy mieli

$$w_1 = a \text{ albo } w_1 = a - b$$

oraz

$$w_2 = c \text{ albo } w_2 = c - d$$

gdzie każda z liter $a$, $b$, $c$ i $d$ oznacza summę pewnej liczby liczb do zbioru $(z)$ należących. Zwracając się obecnie do wzorów (1) i (2) wnosimy, na podstawie poprzedzającego, że na liczbę $w$ mieć będziemy jeden ze wzorów następujących:

(1) $w = a + c$
(2) $w = a + (c - d)$
(3) $w = (a - b) + c$
(4) $w = (a - b) + (c - d)$
(5) $w = a - c$
(6) $w = a - (c - d)$
(7) $w = (a - b) - c$
(8) $w = (a - b) - (c - d)$

Wzory (1) i (5) są już zapowiedzianego kształtu; wzory zaś (2), (3), (6) i (7) możemy, na podstawie twierdzenia poprzedzającego, zastąpić przez wzory żądanego kształtu. Mamy więc do zbadania tylko wzory (4) i (8). Na podstawie twierdzenia poprzedzającego i wzoru (4) mamy:

$$w = (a - b) + (c - d) = \{(a - b) + c\} - d$$

Opierając się powtórnie na twierdzeniu poprzedzającem mamy

$$(a - b) + c = (a + c) - b$$

Zatem

$$w = \{(a + c) - b\} - d$$

Skąd:

$$w = (a + c) - (b + d), \tag{9}$$

opierając się ponownie na twiedzeniu poprzedzającem.

Stwierdziliśmy więc, że wzór (4) możemy zastąpić przez wzór (9), który oczywiście jest zapowiedzianego kształtu.

Przechodząc nareszcie do wzoru (8) znajdujemy natychmiast

$$\begin{aligned} w &= \{(a - b) + d\} - c \\ &= \{(a + d) - b\} - c \\ &= (a + d) - (b + c) \end{aligned}$$

Stwierdzamy więc, że wzór (8) możemy także zastąpić przez wzór zapowiedzianej postaci.

Ostatecznie dowiedliśmy, że gdyby twierdzenie zachodziło w razie, kiedy mamy

$$n \leqq k,$$

to twierdzenie to zachodziłoby także w razie kiedy mamy

$$n = k + 1$$

a więc i w razie kiedy mamy

$$n \leqq k + 1.$$

Ponieważ zaś stwierdziliśmy wyżej, że twierdzenie zachodzi niezawodnie w przypadku, kiedy mamy

$$n = 2,$$

przeto wnosimy, na podstawie zasady indukcyi matematycznej, że twierdzenie zachodzi w podanem brzmieniu.

§ 20. **Tw. IV.** Jeżeli dwie liczby całkowite $a$ i $b$ sprawdzają nierówność

(1) $$a > b$$

to mieć będziemy:

(2) $$a - c > b - c$$

jakąkolwiek liczbę całkowitą, nie większą od $b$, oznaczylibyśmy przez $c$.

Dowód. Przyjmijmy

(3) $$a - b = r$$

Będziemy tedy mieli (tw. I)

(4) $$r > 0$$

ze względu na nierówność (1). Z równości (3) mamy:

$$a = b + r$$

Przeto

(5) $$(b - c) + r = (b + r) - c = a - c$$

na podstawie tw. II. Ze związków (4) i (5) wynika, uwzględniając wniosek z tw. X. (§ 16), nierówność (2), o dowód której właśnie chodziło.

**Tw. V.** Jeżeli dwie liczby całkowite $a$ i $b$ sprawdzają nierówność:

(1) $$a > b,$$

to mieć będziemy

(2) $$c - a < c - b,$$

oznaczając przez $c$ jakąkolwiek liczbę całkowitą, od liczby $a$ nie mniejszą.

Dowód. Ze względu na nierówność (1) możemy przyjąć

(3) $$a = b + r$$

oznaczając przez $r$ (tw. I) pewną liczbę sprawdzającą nierówność

(4) $$r > 0.$$

Na podstawie związku (3) i tw. II mamy:

$$c - a = (c - b) - r$$

skąd

$$(c - a) + r = c - b \tag{5}$$

Opierając się na wniosku z tw. X (§ 16) wnosimy natychmiast ze związków (4) i (5), że nierówność (2), o dowód której chodziło, istotnie sprawdzoną będzie.

## IV. Mnożenie.

§ 21. Iloczynem jakiejkolwiek liczby całkowitej $a$, zwanej mnożną, przez jakąkolwiek liczbę całkowitą $b$, zwaną mnożnikiem, nazywamy liczbę, na którą przyjmujemy wzór następujący

$$a \,.\, b \tag{1}$$

który czytamy $b$ razy $a$, albo $a$ pomnożone przez $b$, określając jednocześnie wartość liczby, którą ma przedstawiać wzór poprzedzający, równościami następującemi:

$$a \,.\, 0 = 0$$

oraz

$$a\,(c + 1) = (a \,.\, c) + a \tag{2}$$

jaką kolwiek liczbę całkowitą oznaczylibyśmy przez literę $c$. Czynność, polegającą na wyznaczeniu iloczynu, nazywamy mnożeniem. Nadmieniamy, że, zamiast symbolu (1), często używanym bywa na iloczyn mnożnej $a$ przez mnożnik $b$ symbol następujący:

$$a \times b.$$

Nadto, jeżeli nieporozumienie jest wykluczone, zastępujemy powyższe symbole na iloczyn liczby $a$ przez liczbę $b$, przez symbol:

$$a\ b.$$

Celem uproszczenia symbolistyki wprowadzamy umowę następującą: mając do skombinowania pewien jakikolwiek ilo-

czyn drogą dodawania lub odejmowania z jakimkolwiek innem wyrażeniem opuścimy, w odnośnym wzorze, nawias, w którym, wedle ogólnych zasad używania nawiasu (§ 12), należałoby zamknąć rozważany iloczyn. Na mocy umowy tej możemy napisać równość (2) jak następuje:

$$a \,.\, (c + 1) = a \,.\, c + a$$

Opierając się na tej okoliczności, iż działanie dodawania zawsze jest wykonalne i zawsze prowadzi do wyniku określonego w zupełności w zależności od składników, stwierdzamy natychmiast, na podstawie zasady indukcyi matematycznej, że działanie mnożenia jest wykonalne, jakiekolwiek byłyby liczby całkowite przyjęte za mnożną i mnożnik i że wynik działania określony jest w zupełności w zależności od mnożnej i mnożnika.

**Tw. I.** Jeżeli mnożnik $b$ w pewnym jakimkolwiek iloczynie

$$a \,.\, b$$

równa się jedności, to iloczyn równa się mnożnej; jeżeli zaś mnożnik jest od jedności większy, to iloczyn równa się sumie tylu składników równych mnożnej, ile wynosi mnożnik.

Dowód. Zeby uzasadnić pierwszą część twierdzenia przyjmujemy

$$b = 1.$$

Mamy

$$a \,.\, 1 = a \,.\, (0 + 1) = a \,.\, 0 + a$$

na podstawie definicyi mnożenia. Ze związków poprzedzających wynika natychmiast, że

$$a \,.\, 1 = a \tag{1}$$

co było do okazania.

Przechodząc do drugiej części przyjmujemy na początek $b = 2$. Mamy:

$$a \,.\, 2 = a\,(1 + 1) = a \,.\, 1 + a = a + a$$

na podstawie równości (1). Dowiedliśmy więc, że druga część

twierdzenia zachodzi istotnie w razie, kiedy mnożnik równa się liczbie dwa.

Zakładamy chwilowo, że twierdzenie zachodzi w razie, kiedy mamy

$$b = k \geqq 2.$$

Na podstawie definicyi mnożenia mamy:

$$a\,(k+1) = a\,.\,k + a. \qquad (2)$$

Ponieważ, wedle przyjętego chwilowo założenia, iloczyn

$$a\,.\,k$$

równa się sumie tylu składników równych liczbie $a$, ile wynosi liczba $k$, przeto, na podstawie równości (2), iloczyn

$$a\,(k+1)$$

równa się sumie tylu składników równych liczbie $a$, ile wynosi liczba

$$k+1.$$

Z uzyskanych wyników wnosimy, opierając się na zasadzie indukcyi matematycznej, że twierdzenie jest słuszne w podanem brzmieniu.

§ 22. **Tw. II.** Iloczyn sumy dwóch jakichkolwiek liczb całkowitych $a$ i $b$ przez jakąkolwiek liczbę całkowitą $m$, przyjętą za mnożnik, równa się sumie iloczynów składników sumy przez tę liczbę; czyli:

$$(a+b)\,.\,m = a\,.\,m + b\,.\,m.$$

Dowód. Twierdzenie zachodzi istotnie w przypadku szczególnym, kiedy mamy

$$m = 0$$

albowiem mamy tedy

$$(a+b)\,.\,m = 0$$
$$a\,.\,m + b\,.\,m = 0 + 0 = 0.$$

Załóżmy chwilowo, że twierdzenie zachodzi w razie, kiedy

mnożnik $m$ równa się pewnej liczbie całkowitej $k$, będziemy tedy mieli

$$(1) \qquad (a+b)\,k = a\,.\,k + b\,.\,k$$

Z drugiej strony mamy:

$$(2) \qquad (a+b)\,(k+1) = (a+b)\,k + (a+b)$$

na podstawie definicyi mnożenia. Z równości (2) wyprowadzamy, na podstawie równości (1) i twierdzeń z § 15, równość następującą:

$$(a+b)\,.\,(k+1) = (a\,.\,k + a) + (b\,.\,k + b)$$

Skąd

$$(a+b)\,(k+1) = a\,(k+1) + b\,(k+1)$$

odwołując się powtórnie do definicyi mnożenia. Z uzyskanych wyników wnosimy natychmiast, opierając się na zasadzie indukcyi matematycznej, że twierdzenie zachodzi istotnie w podanem brzmieniu.

Wniosek I. Opierając się na zasadzie indukcyi matematycznej łatwo stwierdzimy, że iloczyn jakiejkolwiek sumy przez jakikolwiek mnożnik równa się sumie iloczynów składników przez uważany mnożnik.

Wniosek II. Oznaczając przez $b$ jakąkolwiek liczbę całkowitą, a przez $a$ liczbę całkowitą od liczby $b$ nie mniejszą, mamy

$$(a-b)\,.\,m = a\,.\,m - b\,m,$$

jakąkolwiek liczbę całkowitą przyjęlibyśmy za mnożnik $m$.

Istotnie, przyjmując:

$$x = (a-b)\,m,$$

mamy

$$x + b\,m = \{(a-b) + b\}\,m$$

na podstawie twierdzenia poprzedzającego. A ponieważ

$$(a-b) + b = a,$$

przeto

$$x + b\,m = a\,.\,m$$

czyli

$$x = a \,.\, m - b\, m$$

czyli jeszcze

$$(a - b)\, m = a \,.\, m - b \,.\, m,$$

co było do okazania.

**Tw. III.** Jeżeli w jakimkolwiek iloczynie mnożna równa się zeru, to iloczyn ten równa się także zeru; jeżeli zaś mnożna równa się jedności, to iloczyn równa się mnożnikowi.

Dowód. Twierdzenie zachodzi oczywiście (§ 21) w razie, kiedy mnożnik równa się zeru. Gdyby zaś twierdzenie zachodziło w razie kiedy mnożnik równałby się pewnej liczbie $k$, to twierdzenie to zachodziłoby także w przypadku, kiedy mnożnik równałby się liczbie $k + 1$; okoliczność ta wynika natychmiast z równości następujących:

$$0 \,.\, (k + 1) = 0 \,.\, k + 0.$$

$$1 \,.\, (k + 1) = 1 \,.\, k + 1.$$

Zatem twierdzenie zachodzi w każdym razie.

**Tw. IV.** Jeżeli w pewnym jakimkolwiek iloczynie zastąpimy mnożnik $b$ przez mnożną $a$, a mnożną $a$ przez mnożnik $b$, to nowy iloczyn równać się będzie iloczynowi pierwotnemu. Czyli:

$$a \,.\, b = b \,.\, a.$$

Dowód. Twierdzenie zachodzi niezawodnie w przypadku, kiedy mamy

$$a = 0$$

albowiem mamy

$$0 \,.\, b = 0$$

na podstawie twierdzenia poprzedzającego, a

$$b \,.\, 0 = 0$$

na podstawie definicyi mnożenia.

Zgodnie z zasadą metody indukcyjnej zakładamy chwilowo, że twierdzenie zachodzi w razie kiedy mamy

$$a = k.$$

Mamy tedy

(1) $$k \,.\, b = b \,.\, k.$$

Z drugiej strony, na podstawie tw. II., mamy:

$$(k + 1)\, b = k \,.\, b + 1 \,.\, b,$$

skąd:

$$(k + 1)\, b = b \,.\, k + b$$

na podstawie równości (1) i tw. III. A ponieważ

$$b \,.\, k + b = b \,.\, (k + 1)$$

na podstawie definicyi mnożenia, przeto mamy

$$(k + 1) \,.\, b = b \,.\, (k + 1).$$

Z uzyskanych wyników wnosimy natychmiast, że twierdzenie, o którego dowód chodziło, zachodzi istotnie.

Ponieważ wartość iloczynu dwóch liczb, na podstawie twierdzenia poprzedzającego, nie zależy od tego, którą z tych liczb przyjmiemy za mnożnik, przeto obejmujemy mnożną i mnożnik wspólną nazwą czynników iloczynu.

**Tw. V.** Iloczyn dwóch, od zera odmiennych liczb całkowitych, nigdy nie jest mniejszym od jednego z tych czynników i równa się jednemu z nich jedynie w razie, kiedy drugi czynnik równa się jedności.

Dowód. Oznaczmy przez $a$ ten z czynników rozważanego iloczynu $J$, który nie jest mniejszym od drugiego czynnika $b$. Na podstawie twierdzenia poprzedzającego możemy, jak też rzeczywiście uczynimy, przyjąć bez szkody dla ogólności, czynnik $b$ za mnożnik. Jeżeli jest

$$b = 1,$$

to, na podstawie tw. I., mamy

$$J = a \,.\, 1 = a.$$

Załóżmy chwilowo, że mamy

(1) $$a \,.\, k \geqq a$$

oznaczając przez $k$ pewną liczbę całkowitą nie mniejszą od jedności.

Mamy

$$a(k+1) = a \,.\, k + a \tag{2}$$

na podstawie definicyi mnożenia.

Ze związku (1) wynika, że mamy

$$a \,.\, k > 0 \tag{3}$$

albowiem liczba $a$ jest od zera odmienną. Ze związków zaś (2) i (3) wnosimy na mocy wniosku z tw. X (§ 16), że

$$a(k+1) > a \tag{4}$$

że więc iloczyn $a(k+1)$ nie jest mniejszy od liczby $a$. Na podstawie zasady indukcyi matematycznej wnosimy stąd, że mamy istotnie

$$J \geqq a.$$

Udowodniliśmy więc pierwszą część twierdzenia. Żeby udowodnić w zupełności część drugą, winniśmy tylko jeszcze okazać, że nierówność

$$b > 1 \tag{5}$$

pociąga za sobą nierówność

$$J > a \tag{6}$$

Ze względu na nierówność (5) możemy przyjąć

$$b = k + 1 \tag{7}$$

i będziemy wtedy mieli

$$k \geqq 1$$

Na podstawie tej nierówności i udowodnionej już pierwszej części twierdzenia mamy pewność, że iloczyn

$$a \,.\, k$$

sprawdzać będzie związek (1). Ponieważ związek ten pociąga za sobą związek (4), przeto, ze względu na (7), mamy

$$J = a \,.\, b > a.$$

Dowiedliśmy więc, że nierówność (5) pociąga za sobą nierówność (6) i tem samem uzasadniliśmy w zupełności twierdzenie, o które chodziło.

**Tw. VI.** Żeby iloczyn dwóch czynników równał się zeru, koniecznym jest i wystarcza, żeby jeden z nich przynajmniej równał się zeru.

Dowód. Z twierdzenia poprzedzającego wynika natychmiast, że podany warunek jest koniecznym do tego, żeby iloczyn równał się żeru. Na podstawie zaś definicyi mnożenia i tw. III stwierdzamy natychmiast, że powyższy warunek wystarcza.

**Tw. VII.** Jeżeli liczby całkowite $a$, $b$ i $c$ sprawdzają nierówności

(1) $$a > b$$

(2) $$c > 0,$$

to liczby te sprawdzają także nierówność następującą:

(3) $$a \,.\, c > b \,.\, c.$$

Dowód. Na podstawie tw. I (§ 18) mamy

(4) $$a - b > 0.$$

Jeżeli więc przyjmiemy

$$r = (a - b)c$$

to, (tw. VI) ze względu na (2), mieć będziemy:

(5) $$r > 0.$$

Z drugiej strony (wniosek II z tw. II) mamy:

$$(a - b)\, c = a \,.\, c - b \,.\, c$$

czyli

$$r = a \,.\, c - b \,.\, c,$$

skąd

(6) $$a \,.\, c = b \,.\, c + r.$$

Ze związków (5) i (6) wynika natychmiast (§ 16, wniosek z tw X), że nierówność (3), o uzasadnienie której chodziło, rzeczywiście sprawdzoną będzie.

§ 23. Uważajmy tyle danych liczb całkowitych, ile wynosi pewna liczba całkowita $n$ od jedności większa i, po ułożeniu ich w pewnym dowolnie przyjętym porządku, oznaczmy ogólnie przez $a_i$ liczbę o numerze porządkowym $i$. Przyjmijmy następnie

$$P_1 = a_1$$

i ogólnie

$$P_{i+1} = P_i \cdot a_{i+1}.$$

W takim razie, na podstawie zasady indukcyi matematycznej, symbol $P_n$ oznaczać będzie pewną określoną liczbę. W przypadku szczególnym, kiedy mamy $n = 2$, liczba $P_n$ będzie, na podstawie już wprowadzonych dyfinicyi, iloczynem danych liczb, a liczby te będą czynnikami iloczynu.

Nazwy te zachowamy jeszcze w przypadku, kiedy liczba $n$ ma jakąkolwiek wartość od liczby dwa większą. Zatem, w każdym razie, nadamy liczbie $P_n$ miano iloczynu danych liczb a samem tem liczbom nazwę czynników tego iloczynu.

Jeżeli, co się często trafia, pewna liczba $a$ znajduje się z liczbami stanowiącemi pewien zbiór $(z)$ w związku następującym: liczba $a$ równa się wogóle iloczynowi liczb zbioru $(z)$, a w przypadku szczególnym, kiedy zbiór $(z)$ zawiera jednę tylko liczbę, liczba $a$ równa się jedynej liczbie do zbioru $(z)$ należącej, to dla skrócenia, wyrażamy niekiedy rozważany związek orzekając, że liczba $a$ równa się iloczynowi liczb zbioru $(z)$.

Poprzedzająca definicya iloczynu dowolnej liczby czynników jest całkiem analogiczna do wprowadzonej w § 15 definicyi sumy dowolnej liczby składników i prowadzi do twierdzeń znajdujących się w najściślejszej analogii z twierdzeniami uzasadnionemi we wspomnianym paragrafie.

**Tw. VIII.** Wartość iloczynu kilku oznaczonych czynników nie zależy od przyjętego dla nich porządku.

Dowód. Oczywiście winniśmy tylko okazać (§ 14 tw. VI), że przemiana numerów dwóch czynników sąsiednich na wartość iloczynu nie wpływa.

Jeżeli liczba $n$, oznaczająca liczbę czynników, równa się liczbie 2, to twierdzenie obecne nie różni się od uzasadnionego wyżej tw. IV. Załóżmy więc chwilowo, zgodnie z zasadą metody indukcyi matematycznej, że przemiana numerów dwóch czynników sąsiednich na wartość iloczynu nie wpływa w razie, kiedy mamy

$$n \leqq k \tag{1}$$

oznaczając przez $k$ pewną liczbę całkowitą od liczby dwa nie mniejszą i starajmy się okazać, iż w takim razie, ta sama okoliczność zachodziłaby jeszcze gdybyśmy, mieli

$$n = k + 1. \tag{2}$$

Uważajmy więc pewien iloczyn $P$ tylu czynników, ile wynosi suma $k + 1$ i oznaczmy przez $c$ czynnik następujący bezpośrednio po pewnym czynniku $b$, a przez $P'$ iloczyn, w który przeszedłby iloczyn $P$, gdybyśmy przemienili numery porządkowe czynników $b$ i $c$.

Przypadek $A$. Czynnik $c$ nie jest ostatnim czynnikiem iloczynu $P$. W takim razie mieć będziemy

$$P = p \,.\, d$$
$$P' = p' \,.\, d$$

oznaczając: przez $d$ ostatni czynnik iloczynu $P$, przez $p$ pewien iloczyn tylu czynników, ile wynosi liczba $k$ a przez $p'$ iloczyn, w który przeszedłby iloczyn $p$, gdybyśmy w iloczynie tym przemienili numery porządkowe pewnych dwóch czynników sąsiednich (oczywiście czynników $b$ i $c$). Mamy

$$p = p'$$

na podstawie przyjętego chwilowo założenia. Przeto będziemy mieli

$$P = P'$$

o co właśnie chodziło.

Przypadek $B$. Czynnik $c$ jest ostatnim czynnikiem iloczynu $P$. Oznaczając tedy przez $a$ iloczyn czynników poprze-

dzających w iloczynie $P$ czynniki $b$ i $c$ i przyjętych w tym właśnie porządku, w którym one wchodzą do iloczynu $P$, mieć będziemy:

$$\begin{cases} P = (a \,.\, b) \,.\, c \\ P' = (a \,.\, c) \,.\, b. \end{cases} \tag{3}$$

Gdyby czynnik $c$ równał się zeru, to mielibyśmy oczywiście

$$P = (a \,.\, b) \,.\, 0 = 0$$
$$P' = (a \,.\, c) \,.\, b = 0 \,.\, b = 0$$

Zatem w tym przypadku iloczyny $P$ i $P'$ byłyby sobie równe. Zakładamy chwilowo, że mamy

$$(a \,.\, b)\, m = (a \,.\, m) \,.\, b \tag{4}$$

oznaczając przez $m$ pewną liczbę całkowitą i przyjmujemy

$$c = m + 1.$$

Mamy tedy

$$P = (a \,.\, b) \,.\, (m + 1),$$
$$P' = \{a \,.\, (m + 1)\} \,.\, b \tag{5}$$

Mamy

$$P = (a \,.\, b) \,.\, m + a \,.\, b$$

na podstawie definicyi mnożenia. Przeto

$$P = (a \,.\, m) \,.\, b + a \,.\, b$$

na podstawie równości (4). Opierając się następnie na tw. II stwierdzamy, że mamy:

$$P = (a \,.\, m + a)\, b$$

skąd

$$P = \{a \,.\, (m + 1)\}\, b \tag{6}$$

albowiem

$$a \,.\, m + a = a \,.\, (m + 1)$$

na podstawie definicyi mnożenia. Równości (5) i (6) pociągają za sobą równość

$$P = P'. \tag{7}$$

Jeżeli więc uwzględnimy wynik uzyskany przy badaniu przypadku A, to dojdziemy do rezultatu następującego: gdyby

przemiana numerów dwóch czynników sąsiednich nie wpływała na wartość iloczynu w przypadku, kiedy liczba czynników nie przekracza pewnej liczby $k$, to ta sama okoliczność zachodziłaby jeszcze w razie, kiedy liczba $n$, oznaczająca liczbę czynników, miałaby wartość określoną równością (2). Zwracając się do rozważań wyłożonych na początku dowodu wnosimy stąd natychmiast, że twierdzenie, o uzasadnienie którego chodzi, istotnie zachodzi w podanem brzmieniu.

Kierując się ścisłą, już wyżej wskazaną analogią pomiędzy teoryą sumy kilku składników a iloczynem kilku czynników, uzasadnimy z największą łatwością twierdzenia następujące:

**Tw. IX.** Iloczyn, w który przemieni się jakikolwiek dany iloczyn przez to, że zastąpimy w nim kilka którychkolwiek czynników przez ich iloczyn, równa się iloczynowi danemu.

**Tw. X.** Iloczyn, w który przejdzie jakikolwiek dany iloczyn przez to, że zastąpimy w nim jeden jakikolwiek czynnik przez iloczyn równy temu czynnikowi, równa się iloczynowi danemu.

Paragraf ten zakończymy uwagą całkiem analogiczną do uwagi wysłowionej na końcu § 15-go, mianowicie: twierdzenia VIII, IX i X pouczają nas, że we wzorze na jakąkolwiek kombinacyę kilku liczb drogą mnożenia możemy opuścić nawiasy bez obawy, żeby stąd mogła wyniknąć jakakolwiek wątpliwość co do wartości liczby, którą przedstawiałby wówczas rozważany wzór.

## V. Dzielenie.

§ 24. Całkowitą częścią ilorazu oznaczonej liczby całkowitej $a$, zwanej dzielną, przez jakąkolwiek oznaczoną liczbę całkowitą $b$, zwaną dzielnikiem, nazywamy wszelką taką liczbę całkowitą $q$, która sprawdza równość następującą:

(1) $$a = b \,.\, q + r$$

gdzie litera $r$ oznacza liczbę całkowitą, która, jeżeli jest od zera odmienną, sprawdza nierówność:

$$r < b. \tag{2}$$

Liczba $r$ zwie się resztą podziału liczby $a$ przez liczbę $b$ a działanie polegające na wyznaczeniu liczb $q$ i $r$ nazywa się dzieleniem.

**Tw. I.** Żeby liczby $q$ i $r$ sprawdzały definicye całkowitej części ilorazu i reszty przy dzieleniu jakiejkolwiek liczby $a$, przyjętej za dzielną, przez dzielnik $b$ od zera odmienny, koniecznym jest i wystarcza, żeby liczby $q$ i $r$ sprawdzały związki (1) i (2).

Dowód. Warunki te oczywiście wystarczają. Żeby przekonać się, że one są konieczne, należy tylko zważyć, że, jeżeli reszta $r$ równa się zeru, to nierówność (2) będzie sprawdzoną, ze względu na nierówność

$$b > 0;$$

jeżeli zaś reszta $r$ jest od zera odmienną, to nierówność (2) zachodzi na podstawie definicyi dzielenia. Zatem nierówność ta zachodzi w każdym razie. Co się zaś tyczy równości (1), to równość ta zawsze zachodzić musi na podstwie definicyi dzielenia. Uzasadniliśmy więc w zupełności twierdzenie, o które chodziło.

**Tw. II.** Jeżeli dzielnik przy pewnem dzieleniu równa się zeru, to dzielenie jest niewykonalne — z wyłączeniem jednak przypadku, kiedy dzielna także równa się zeru; w tym przypadku wyjątkowym całkowita część ilorazu jest całkiem nieokreślona a reszta równa się zeru.

Dowód. Zwróćmy się do równości (1) i załóżmy, że mamy

$$b = 0. \tag{3}$$

W takim razie równość (1) przyjmie kształt następujący:

$$a = r \tag{4}$$

jakąkolwiek wartość przyjęlibyśmy na liczbę $q$.

Gdybyśmy mieli

$$a = 0,$$

to, na podstawie równości (4), mielibyśmy także

$$r = 0.$$

Przeto, jeżeli dzielna i dzielnik równają się zeru, to wartość zero i tylko ta wartość na resztę oraz wszelka dowolnie przyjęta wartość na całkowitą część ilorazu sprawdzają definicye tych elementów.

Gdybyśmy zaś mieli

$$a > 0,$$

to równość (4) pociągnęłaby za sobą nierówność

$$r > 0,$$

która byłaby ze względu na równość (3) w sprzeczności z nierównością (2).

Stwierdzamy więc, że w tym przypadku nie istnieje żadnego układu wartości na $q$ i $r$, sprawdzającego definicyę całkowitej części ilorazu i reszty. W innych wyrazach: jeżeli dzielnik równa się zeru a dzielna jest od zera odmienna, to dzielenie jest niewykonalne. Udowodniliśmy więc w zupełności twierdzenie, o które chodziło.

**Tw. III.** Jeżeli dzielnik jest od zera odmienny, to dzielenie jest zawsze wykonalne, a odnośne wartości całkowitej części ilorazu i reszty są określone w zupełności, w zależności od dzielnej i dzielnika.

Dowód. Oznaczmy jak wyżej przez $a$ dzielną a przez $b$ dzielnik i, zakładając na początek, że liczba $a$ jest od zera odmienną, uważajmy część ciągu naturalnego liczb całkowitych od liczby zero do liczby $a$ włącznie. Ta część ciągu naturalnego lub liczb całkowitych stanowić będzie pewien ciąg skończony $(c)$, którego pierwszym elementem będzie liczba zero a ostatnim liczba $a$. Jeżeli zastąpimy w ciągu $(c)$ każdą do tego ciągu należącą liczbę przez iloczyn otrzymany, mnożąc przez nią liczbę $b$, to otrzymamy nowy ciąg $(c')$. Pierwszym elementem ciągu $(c')$ będzie liczba zero a każdym dalszym elementem tego ciągu będzie wynik dodania liczby $b$ do liczby stanowiącej element poprzedzający bezpośrednio element uwa-

żany. Ostatnim elementem ciągu $(c')$ będzie oczywiście iloczyn $b \,.\, a$. Ponieważ (tw. V, § 22) mamy

$$a \leqq b \,.\, a,$$

ponieważ dalej pierwszym elementem ciągu $(c')$ jest liczba zero, przeto liczba $a$ nie jest mniejszą od pierwszej liczby ciągu $(c')$, ani większą od ostatniej liczby tego ciągu. Z tego zaś wynika (tw. XI, § 7), że nadarzyć się musi jeden z dwu przypadków następujących:

*Ä*) Liczba $a$ sprawdza równość

$$a = b \,.\, m \tag{1}$$

oznaczając przez $m$ jedną z liczb należących do ciągu $(c)$.

*B*) Liczba $a$ sprawdza nierówności następujące:

$$\begin{cases} a > b \,.\, m \\ a < b \,.\, (m + 1), \end{cases} \tag{2}$$

gdzie liczby $m$ i $m + 1$ są dwiema liczbami sąsiedniemi w ciągu $(c)$.

W przypadku, kiedy zachodzi równość (1), liczba $m$ sprawdza oczywiście definicyę całkowitej części ilorazu a odnośna reszta równa się zeru. Łatwo przekonać się możemy, że w przypadku, kiedy zachodzą nierówności (2), liczba $m$ także sprawdza definicyę całkowitej części ilorazu. Istotnie przyjmijmy

$$r = a - b \,.\, m. \tag{3}$$

Będziemy tedy mieli

$$r > 0. \tag{4}$$

Ponieważ mamy

$$b = b \,.\, (m + 1) - b \,.\, m, \tag{5}$$

przeto wnosimy ze związków (3) i (5) na podstawie drugiej z nierówności (2) (tw. IV § 20), że mamy,

$$r < b \tag{6}$$

Ze związków (3) i (6) wynika natychmiast, że liczba $m$ istotnie sprawdza definicyę całkowitej części ilorazu dzielnej $a$ przez dzielnik $b$.

Dowiedliśmy więc, że, jeżeli przy dzielniku od zera od-

miennym, dzielna też jest od zera odmienną, to działanie dzielenia jest wykonalne. Ponieważ zaś w przypadku, kiedy dzielna równa się zeru, liczba zero oczywiście sprawdza definicyę całkowitej części ilorazu, przeto, byleby dzielnik był od zera odmiennym, działanie dzielenia jest niezawodnie wykonalne. Winniśmy tylko jeszcze okazać, że, jeżeli dzielnik jest od zera odmienny, to całkowita część ilorazu, a więc i reszta, są określone w zupełności w zależności od dzielnej i dzielnika.

Załóżmy, że liczby $q$ i $r$ sprawdzają definicyę całkowitej części ilorazu i reszty. Będziemy tedy mieli (tw. I)

$$a = b \cdot q + r \tag{7}$$

oraz

$$r < b. \tag{8}$$

Powiadam, że żadna liczba całkowita $x$, od liczby $q$ odmienna, nie sprawdza definicyi całkowitej części ilorazu liczby $a$ przez liczbę $b$. Dwa przypadki tylko nadarzyć się mogą, mianowicie:

$$x < q \tag{\alpha}$$

albo

$$x > q. \tag{\beta}$$

Przypadek $\alpha$. Przyjmując

$$q = x + y \tag{9}$$

będziemy mieli

$$y > 0. \tag{10}$$

Z drugiej strony wyprowadzamy z równości (7) i (9)

$$a = bx + r'$$

przyjmując

$$r' = b \cdot y + r.$$

Ze względu na nierówność (10) mamy

$$by \geqq b,$$

zatem

$$r' \geqq b.$$

Z tego zaś wynika (tw. I), uwzględniając nierówność

$$b > 0 \tag{11}$$

że liczba $x$ nie sprawdza definicyi całkowitej części ilorazu liczby $a$ przez liczbę $b$.

Przypadek $\beta$. Przyjmijmy

$$x = q + z.$$

Będziemy tedy mieli

$$bx = b \,.\, q + b \,.\, z, \tag{12}$$

a ponieważ

$$z > 0$$

przeto mamy

$$bz \geqq b,$$

zatem

$$bz > r \tag{13}$$

ze względu na nierówność (8). Ze związków (7), (12) i (13) wyprowadzamy związek (wniosek II, tw. I, § 18)

$$a < bx$$

skąd oczywiście wynika, że liczba $x$ nie sprawdza definicyi całkowitej części ilorazu liczby $a$ przez liczbę $b$.

Ostatecznie stwierdziliśmy, że żadna liczba całkowita od liczby $q$ odmienna, nie sprawdza definicyi całkowitej części ilorazu liczby $a$ przez liczbę $b$. Udowodniliśmy więc w zupełności twierdzenie, o które chodziło.

Wniosek. Z ostatniej części dowodu twierdzenia poprzedzającego wnosimy natychmiast, że, jeżeli dzielnik jest od zera odmienny, to całkowita część ilorazu równa się największej liczbie, której iloczyn przez dzielnik nie przekracza dzielnej, i jest jednocześnie mniejszą od każdej liczby, której iloczyn przez dzielnik większym jest od dzielnej.

§ 25. Oznaczmy przez $a$ i $b$ dwie jakiekolwiek liczby całkowite. Jeżeli istnieje pewna liczba całkowita $m$ sprawdzająca równość następującą:

$$a = b \,.\, m,$$

to okoliczność tę wysławiamy orzekając, iż liczba $a$ podzielną

jest przez liczbę $m$; liczba $m$ zowie się tedy ilorazem podziału liczby $a$ przez liczbę $b$, liczba $a$ — wielokrotnością liczby $b$, a liczba $b$ — podwielokrotnością liczby $a$.

Jeżeli pewna liczba $a$ podzielną jest przez pewną liczbę $b$, to odnośny iloraz przedstawiamy przez wzór następujący:

$$a : b.$$

Przy kombinowaniu wzoru tego z innemi wyrażeniami drogą dodawania albo odejmowania opuszczamy nawias, w którym, wedle ogólnych prawideł, wzór ten należałoby umieścić.

**Tw. IV.** Żeby pewna liczba $a$ podzielną była przez pewną liczbę $b$, koniecznem jest, żeby działanie dzielenia liczby $a$ przez liczbę $b$ było wykonalnem i żeby reszta podziału równała się zeru; jeżeli warunki te są spełnione, to liczba $a$ jest podzielną przez liczbę $b$ a odnośny iloraz równa się całkowitej części ilorazu podziału liczby $a$ przez liczbę $b$.

Dowód. Jeżeli liczba $a$ podzielną jest przez liczbę $b$, to odnośny iloraz i liczba zero oczywiście sprawdzają definicyę całkowitej części ilorazu i reszty podziału liczby $a$ przez liczbę $b$. Ponieważ, na podstawie tw. II i III, reszta podziału jest w każdym razie określona w zupełności w zależności od dzielnej i dzielnika, przeto stwierdzamy, że podane warunki podzielności pewnej liczby przez pewną inną liczbę są rzeczywiście konieczne; nadto, z poprzedzającego wypływa jeszcze bezpośrednio, że iloraz, o ile istnieje, równa się całkowitej części ilorazu. Ponieważ nareszcie, na podstawie definicyi podzielności, powyższe warunki podzielności jednej liczby przez drugą są oczywiście wystarczające, przeto udowodniliśmy w zupełności twierdzenie, o które chodziło.

**Tw. V.** Liczba zero podzielną jest przez każdą dowolnie przyjętą liczbę $b$; odnośny iloraz równa się zeru, jeżeli liczba $b$ jest od zera odmienną, jeżeli zaś liczba $b$ równa się zeru, to iloraz jest cakiem nieokreślony.

Twierdzenie to wynika natychmiast z przyjętych definicyi.

**Tw. VI.** Wszelka dowolnie przyjęta liczba całkowita $a$ podzielną jest przez jedność, a odnośny iloraz równa się liczbie $a$.

Dowód twierdzenia tego jest nie mniej natychmiastowy od dowodu twierdzenia poprzedzającego.

Wniosek. Każda liczba całkowita $a$ jest przez samą siebie podzielną, jeżeli uważana liczba $a$ jest od zera odmienną, to iloraz podziału liczby tej przez samą siebie równa się jedności.

**Tw. VII.** Jeżeli oznaczymy przez $b$ liczbę całkowitą od jedności odmienną, to zawsze istnieć będzie nieskończona liczba liczb całkowitych przez liczbę $b$ niepodzielnych.

Dowód. Jeżeli liczba $b$ równa się zeru, to oczywiście żadna liczba od zera odmienna przez liczbę $b$ podzielną nie będzie. Jeżeli zaś liczba $b$ jest od zera odmienną to, ponieważ jedności równać się nie może, będzie od jedności większą. Zatem istnieć będzie przynajmniej jedna liczba $r$ sprawdzająca nierówności następujące:

$$0 < r < b.$$

Jeżeli tedy przyjmiemy

$$a = b \cdot q + r$$

oznaczając przez $q$ dowolnie przyjętą liczbę całkowitą, to, na podstawie twierdzeń I i IV, liczba $a$ przez liczbę $b$ podzielną nie będzie. Udowodniliśmy więc w zupełności twierdzenie, o które chodziło.

## VI. Teorya potęg.

§ 26. Oznaczając przez $a$ i $n$ dwie liczby całkowite, nazywamy potęgą stopnia $n$ liczby $a$ taką liczbę, którą przedstawiamy przez symbol

$$a^n, \tag{1}$$

określając jednocześnie wartość liczby, którą przedstawiać ma symbol poprzedzający, równościami następującemi

$$a^1 = a \tag{2}$$

$$a^{k+1} = a^k \cdot a \tag{3}$$

jakąkolwiek liczbę całkowitą oznaczylibyśmy przez literę $k$.

Liczba $a$ zwie się podstawą potęgi, a liczba $n$ wykładnikiem tejże.

Opierając się na zasadzie indukcyi matematycznej stwierdzamy natychmiast, że równości (1) i (2) określają wartość liczby, którą ma przedstawiać symbol (1), dla każdej, od jedności nie mniejszej wartości wykładnika $n$; nadto, ponieważ, przyjmując na liczbę $k$ w równości (3) wartość zero, wyprowadzamy z niej równość

$$a = a^0 \cdot a$$

na podstawie równości (2), przeto stwierdzamy jeszcze, że definicya powyższa potęgi prowadzi do konsekwencyi następujących:

*A*) Jeżeli liczba $a$ jest od zera odmienną, to mamy

$$a^0 = 1.$$

*B*) Jeżeli liczba $a$ równa się zeru, to wartość symbolu

$$a^0$$

pozostaje całkiem nieokreśloną.

Przy kombinowaniu wzoru na potęgę z innymi wyrażeniami drogą dodawania albo odejmowania opuszczamy nawias, w którym, wedle ogólnych prawideł użycia nawiasu, należałoby zamknąć wzór na potęgę.

**Tw. I.** Jeżeli wykładnik potęgi jest od jedności większy, to potęga równa się iloczynowi tylu czynników równych podstawie, ile wynosi wykładnik.

Dowód twierdzenia tego czytelnik uskuteczni z największą łatwością metodą indukcyi matematycznej. Tą samą metodą uzasadnilibyśmy łatwo twierdzenia następujące:

**Tw. II.** Jeżeli wykładnik potęgi jest od zera odmienny, a podstawa równa się zeru, to rozważana potęga równa się zeru.

**Tw. III.** Jeżeli podstawa potęgi jest od zera odmienną, to, jakąkolwiek wartość miałby wykładnik, wartość potęgi nie jest mniejszą od jedności; w razie gdy podstawa równa się jedności, wartość potęgi równa się jedności.

§ 27. W ustępie niniejszym rozważać będziemy wyłącznie potęgi o podstawach od zera odmiennych.

**Tw. IV.** Mamy

$$a^n \cdot a^m = a^{n+m} \tag{1}$$

jakiekolwiek wartości miałyby wykładniki $n$ i $m$.

Dowód. Równość (1) zachodzi niezawodnie w przypadku, kiedy mamy

$$m = 0$$

albowiem mamy wtedy:

$$a^n \cdot a^0 = a^n \cdot 1 = a^n$$

$$a^{n+0} = a^n$$

skąd

$$a^n \cdot a^0 = a^{n+0}.$$

Zakładamy chwilowo, że, oznaczając przez $k$ pewną liczbę całkowitą, mamy

$$a^n \cdot a^k = a^{n+k}.$$

Z równości tej wynika, że mamy:

$$a^m \cdot a^k \cdot a = a^{n+k} \cdot a.$$

Ponieważ z jednej strony

$$a^{n+k}\, a = a^{n+k+1} = a^{n+(k+1)}$$

a z drugiej

$$a^n \cdot a^k \cdot a = a^n \cdot (a^k \cdot a) = a^n \cdot a^{k+1}$$

przeto, gdyby twierdzenie zachodziło dla

$$m = k$$

to ono zachodziłoby także dla

$$m = k + 1.$$

Ponieważ zaś stwierdziliśmy, że twierdzenie sprawdzonem jest w razie, kiedy

$$m = 0,$$

przeto wnosimy, że twierdzenie zachodzi w każdym razie.

**Tw. V.** Jeżeli wykładniki potęg

$$a^n \text{ i } a^m$$

sprawdzają związek

$$n \geqslant m,$$

to liczba $a^n$ podzielną jest przez liczbę $a^m$ i mamy wtedy

$$a^n : a^m = a^{n-m}.$$

Dowód. Przyjmijmy

$$x = a^{n-m}$$

Mamy wówczas (tw. IV):

$$x \,.\, a^m = a^{(n-m)+m} = a^n,$$

która to równość wyraża właśnie twierdzenie, o które chodziło.

**Tw. VI.** Mamy

$$a^n \,.\, b^n = (a \,.\, b)^n$$

jakąkolwiek wartość miałby wykładnik $n$.

Dowód. Twierdzenie zachodzi niezawodnie, jeżeli mamy

$$n = 0$$

albowiem

$$a^0 \,.\, b^0 = 1 \,.\, 1 = 1$$

$$(a \,.\, b)^0 = 1.$$

Zakładamy chwilowo, że mamy:

(1) $$a^k \,.\, b^k = (a \,.\, b)^k.$$

Z równości tej wyprowadzamy, iż

$$a^k \,.\, b^k \,.\, a \,.\, b = (a \,.\, b)^k \,.\, a \,.\, b.$$

A ponieważ mamy:

$$a^k \, b^k \,.\, a \,.\, b = (a^k \,.\, a)\,(b^k \,.\, b) = a^{k+1} \,.\, b^{k+1}$$

oraz

$$(a \,.\, b)^k \,.\, a \,.\, b = (a \,.\, b)^k \,.\, (a \,.\, b) = (a \,.\, b)^{k+1},$$

przeto stwierdzamy, że równość (1) pociąga za sobą równość:

$$a^{k+1} \,.\, b^{k+1} = (a \,.\, b)^{k+1}.$$

Z powyższych wyników wnosimy natychmiast, że twierdzenie zachodzi w podanem brzmieniu.

**Tw. VII.** Jeżeli pewna liczba $a$ podzielną jest przez pewną liczbę $b$, to, jakąkolwiek liczbę całkowitą oznaczylibyśmy przez $n$, liczb $a^n$ podzielną będzie przez liczbę $b^n$ i będziemy mieli:

$$a^n : b^n = (a : b)^n.$$

Dowód. Przyjmujemy

$$x = (a : b)^n.$$

Mamy tedy (tw. VI)

$$x \cdot b^n = \{(a : b) \cdot b\}^n = a^n.$$

Równość ta wyraża właśnie twierdzenie, o dowód którego chodziło.

**Tw. VIII.** Mamy

$$(a^n)^m = a^{n \cdot m}$$

jakiekolwiek liczby całkowite oznaczylibyśmy przez litery $n$ i $m$.

Dowód. Twierdzenie to zachodzi niezawodnie dla

$$m = 0$$

albowiem mamy wtedy:

$$(a^n)^0 = 1$$

oraz

$$a^{n \cdot 0} = a^0 = 1.$$

Załóżmy chwilowo, że mamy

$$(a^n)^k = a^{n \cdot k}. \tag{1}$$

Będziemy tedy mieli

$$(a^n)^k \cdot a^n = a^{n \cdot k} \cdot a^n.$$

Ponieważ mamy:

$$(a^n)^k \cdot a^n = (a^n)^{k+1}$$

oraz

$$a^{n \cdot k} \cdot a^n = a^{nk+n} = a^{n(k+1)},$$

przeto stwierdzamy, że równość (1) pociąga za sobą równość

$$(a^n)^{k+1} = a^{n(k+1)}$$

i wnosimy z uzyskanych wyników, że twierdzenie, o które chodzi, istotnie zachodzi w podanem brzmieniu.

§ 28. W paragrafie poprzedzającym rozważaliśmy wyłącznie potęgi o podstawach od zera odmiennych. W jakiej mierze twierdzenia uzasadnione we wspomnianym paragrafie pozostałyby w sile, gdybyśmy zastrzeżenie co do podstaw potęg znieśli?

Czytelnik łatwo uzasadni słuszność odpowiedzi następujących.

Co do tw. IV. Jeżeli mamy

$$a = 0,$$

to należy założyć, iż jeden przynajmniej z wykładników $n$ albo $m$ jest od zera odmienny. Gdyby zaś każdy z tych wykładników równał się zeru, to twierdzenie nie miałoby sensu, albowiem symbol

$$0^0$$

nie przedstawia żadnej oznaczonej liczby całkowitej.

Co do tw. V. Gdybyśmy założyli, że mamy

$$a = 0,$$

to twierdzenie pozbawionem byłoby sensu, jakiekolwiek wartości miałyby wykładniki $n$ i $m$.

Co do tw. VI. Gdyby jedna z liczb $a$ albo $b$ równała się zeru, to należałoby założyć, że mamy

$$n > 0.$$

W przeciwnym zaś razie twierdzenie nie miałoby sensu.

Co do tw. VII. Możemy przyjąć

$$a = 0$$

ale winniśmy w każdym razie zachować założenie, iż mamy

$$b > 0$$

i, co do wykładnika $n$, musimy wtedy założyć, że wykładnik ten jest od zera odmienny. W przeciwnym razie twierdzenie nie miałoby sensu.

Co do tw. VIII. Gdybyśmy przyjęli

$$a = 0,$$

to należałoby założyć, że liczby $n$ i $m$ są od zera odmienne; w przeciwnym razie twierdzenie pozbawionem byłoby sensu.

§ 29. Oznaczmy przez $n$ i $m$ dwie liczby całkowite sprawdzające warunek

$$n \leqq m$$

a przez $f(i)$ liczbę określoną w zupełności w zależności od liczby całkowitej $i$ dla wszystkich takich wartości tej liczby, które sprawdzają warunki następujące:

$$i \geqq n;\ i \leqq m.$$

Uważajmy następnie symbol następujący:

$$\sum_{i=n}^{m} f(i), \tag{1}$$

który czytamy sigma $f(i)$ od $i = n$ do $i = m$. Przez symbol poprzedzający oznaczamy liczbę, którą określamy równościami następującemi:

$$\sum_{i=n}^{n} f(i) = f(n)$$

$$\sum_{i=n}^{p+1} f(i) = \sum_{i=n}^{p} f(i) + f(p+1).$$

Opierając się na zasadzie indukcyi matematycznej stwierdzamy natychmiast, że definicya poprzedzająca określa w zupełności liczbę, którą przedstawiać ma symbol (1).

Zachowując oznaczenia poprzedzające, umawiamy się jeszcze uważać symbol:

$$\sum_{i=m}^{n} f(i)$$

za symbol przedstawiający tę samą liczbę, co symbol (1).

Czytelnik upewni się z łatwością, że w razie, kiedy mamy

$$m - n \geqq 1,$$

symbol (1) przedstawia sumę tych $m - n + 1$ wartości, które przyjmuje wyrażenie $f(i)$ zastępując w nim kolejno literę $i$ przez liczby całkowite ciągu naturalnego liczb całkowitych od liczby $n$ do liczby $m$ włącznie.

Opierając się na znanych twierdzeniach, czytelnik łatwo stwierdzi, że mamy:

$$a \sum_{i=n}^{m} f(i) = \sum_{i=n}^{m} a\, f(i),$$

jakąkolwiek liczbę całkowitą oznaczylibyśmy przez $a$.

**Tw. IX.** Oznaczmy przez $a$ i $b$ dwie liczby całkowite od zera odmienne, sprawdzające nierówność następującą:

$$a \geqq b,$$

a przez $n$ liczbę całkowitą od jedności nie mniejszą. Będziemy tedy mieli:

$$(1) \qquad a^n - b^n = (a - b) \sum_{i=1}^{n} a^{n-i} \cdot b^{i-1}.$$

Dowód. Jeżeli mamy

$$n = 1,$$

to twierdzenie zachodzi niezawodnie, albowiem mamy wtedy:

$$a^n - b^n = a - b$$

oraz

$$\sum_{i=1}^{n} a^{n-i} b^{i-1} = \sum_{i=1}^{1} a^{1-i} b^{i-1} = a^0 \cdot b^0 = 1.$$

Załóżmy chwilowo, że mamy:

$$(2) \qquad a^k - b^k = (a - b) \sum_{i=1}^{k} a^{k-i} \cdot b^{i-1}.$$

Będziemy tedy mieli:

$$(3) \qquad a^{k+1} - ab^k = (a - b) \sum_{i=1}^{k} a^{k+1-i} \cdot b^{i-1}.$$

Z drugiej zaś strony mamy:

$$(4) \qquad ab^k - b^{k+1} = (a - b)\, b^k = (a - b)\, b^{(k+1)-1}.$$

Z równości (3) i (4) wynika równość następująca:

$$(a^{k+1} - ab^k) + (ab^k - b^{k+1}) =$$

$$= (a - b) \sum_{i=1}^{k} a^{k+1-i} \cdot b^{i-1} + (a - b)\, b^{(k+1)-1}$$

skąd

$$5) \qquad a^{k+1} - b^{k+1} = (a - b) \sum_{i=1}^{k+1} a^{(k+1)-i} \cdot b^{i-1}.$$

Zatem równość (2) pociąga za sobą równość (5). A ponieważ równość (1), jak stwierdziliśmy wyżej, zachodzi w razie kiedy

$$n = 1,$$

przeto równość (1) zachodzi dla każdej wartości na $n$, spraw dzającej warunek

$$n \geqq 1,$$

co było do okazania.

**Tw. X.** Jeżeli oznaczymy przez $a$ i $n$ liczby całkowite od jedności większe, to liczby te sprawdzać będą nierówność następującą:

$$a^n > 1 + n(a - 1). \qquad (1)$$

Dowód. Mamy

$$a^2 = \{1 + (a - 1)\}^2 = 1 + 2(a - 1) + (a - 1)^2$$

na podstawie znanych własności mnożenia.

Ponieważ mamy

$$a > 1$$

przeto

$$a - 1 > 0$$

zatem (tw. III):

$$(a - 1)^2 \geqq 1.$$

Stwierdzamy więc, że

$$a^2 > 1 + 2(a - 1).$$

Załóżmy chwilowo, że

$$a^k > 1 + k(a - 1) \quad (k \geqq 2). \qquad (2)$$

W takim razie mielibyśmy:

$$a^{k+1} > \{1 + k(a - 1)\}(1 + (a - 1)),$$

skąd

$$a^{k+1} > 1 + (k + 1)(a - 1) + k(a - 1)^2$$

a więc tem bardziej:

$$a^{k+1} > 1 + (k + 1)(a - 1). \tag{3}$$

Dowiedliśmy więc, że nierówność (2) pociąga za sobą nierówność (3). Z uzyskanych wyników wnosimy natychmiast, że nierówność (1) zachodzi przy wysłowionych w twierdzeniu warunkach.

Wniosek. Jeżeli liczba całkowita $a$ sprawdza nierówność

$$a > 1,$$

to mamy

$$a^n > n$$

jakąkolwiek wartość miałby wykładnik całkowity $n$. Istotnie, jeżeli liczba $n$ równa się zeru albo jedności, to nierówność, o którą chodzi, stwierdzamy bezpośrednio.

Jeżeli zaś liczba $n$ jest od jedności większa, to nierówność ta wynika natychmiast z twierdzenia poprzedzającego.

**Tw. XI.** Jeżeli oznaczymy przez $a$, $b$ i $n$ liczby całkowite sprawdzające nierówności następujące:

$$a > b$$

$$n \geqq 1,$$

to liczby te sprawdzać będą nierówność:

$$a^n > b^n. \tag{1}$$

Dowód. W przypadku szczególnym kiedy mamy

$$b = 0$$

nierówność (1) wynika natychmiast z twierdzeń II i X. Jeżeli zaś mamy

$$b > 0,$$

to nierówność (1) wypływa natychmiast z tw. IX. Zatem twierdzenie obecne zachodzi istotnie w podanem brzmieniu.

**Tw. XII.** Jeżeli pewne liczby całkowite $a$, $m$ i $n$ sprawdzają nierówności następujące:

$$a > 1$$

$$m > n,$$

to liczby te sprawdzają także nierówność:

$$a^m > a^n. \tag{1}$$

Dowód. Mamy (tw. IV)

$$a^m = a^n \cdot a^{m-n} \tag{2}$$

a ponieważ

$$m - n > 0$$

przeto

$$a^{m-n} > 1 \tag{3}$$

na podstawie twierdzenia X i równości

$$a^1 = a.$$

Z nierówności (3) wnosimy (tw. VII, § 22), że

$$a^n \cdot a^{m-n} > a^n,$$

skąd, na podstawie równości (2) wynika nierówność (1) o uzasadnienie której właśnie chodziło.

Wniosek. Jeżeli liczby całkowite $a$ i $m$ sprawdzają nierówności

$$a > 1$$
$$m > 1$$

to liczby te sprawdzają także nierówność:

$$a^m > a.$$

Żeby przekonać się o tem, należy tylko zastosować twierdzenie poprzedzające do przypadku, kiedy mamy $n = 1$.

## VII. Teorya numeracyi.

§ 30. Zamierzamy obecnie zastąpić numeracyę prowizoryczną, wprowadzoną w rozdz. I, numeracyą powszechnie przyjętą, zwaną numeracyą dziesiętną.

Numeracya dziesiętna jest jedną z numeracyi, stanowiących taką klasę numeracyi, które wszystkie wypływają tą samą drogą z twierdzenia następującego.

**Tw.** Jeżeli przedstawimy przez $\varrho$ oznaczoną liczbę całkowitą, sprawdzającą nierówność

$$\varrho > 1,$$

to każdej, od liczby $\varrho$ nie mniejszej, liczbie całkowitej $a$, odpowiadać będzie skończony ciąg liczb $(C)$, określony w zupełności przez własności następujące:

1° Każda liczba ciągu tego będzie od liczby $\varrho$ mniejsza.

2° Ostatnia liczba ciągu tego będzie od zera odmienna.

3° Oznaczając ogólnie przez $c_i$ liczbę stanowiącą element rzędu (czyli numeru) $i$ w ciągu $(C)$, a przez $n$ $(n > 1)$ liczbę elementów tego ciągu, będziemy mieli

$$(1) \qquad a = \sum_{i=1}^{n} c_i \cdot \varrho^{i-1}.$$

Dowód. *A*) Istnieje jedna i tylko jedna liczba całkowita $p$, w żadnym razie od jedności nie mniejsza, sprawdzająca nierówności następujące:

$$(2) \qquad \varrho^p \leqq a < \varrho^{p+1}.$$

Istotnie uważajmy skończony ciąg liczb $(K)$, w którym element każdego jakiegokolwiek rzędu $i$ równa się

$$\varrho^i$$

i w którym liczba $\varrho^a$ stanowi element ostatni. Ponieważ mamy

$$a \geqq \varrho,$$

oraz (wniosek z tw. X, § 29)

$$a < \varrho^a$$

ponieważ (tw. XII, § 29) liczba następująca w ciągu $(K)$ po innej liczbie zawsze jest od niej większą, przeto (tw. XI, § 7) liczba $a$ albo będzie równać się pewnej liczbie ciągu $(K)$, albo też będzie liczbą pośrednią pomiędzy dwiema liczbami sąsiedniemi do tego ciągu należącemi. Zatem niezawodnie istnieć będzie przynajmniej jedna wartość na liczbę całko-

witą $p$, sprawdzająca warunki (2). Ponieważ zaś łatwo możemy stwierdzić, opierając się na tw. XII (§ 29), że dwie nierówne sobie wartości na liczbę $p$ warunków (3) jednocześnie sprawdzać nie mogą, przeto uzasadniliśmy w zupełności to, o co w niniejszym ustępie chodziło.

*B*) Jeżeli liczba $a$ przedstawialna jest przez wzór (1), to liczba ta sprawdza nierówności następujące:

$$\varrho^{n-1} \leqq a < \varrho^n. \tag{3}$$

Istotnie, ponieważ każda z liczb $c_i$ mniejszą jest od liczby $\varrho$, przeto ze wzoru (1) mamy:

$$a \leqq \sum_{i=1}^{n} (\varrho - 1)\, \varrho^{i-1}$$

skąd

$$a \leqq (\varrho - 1) \sum_{i=1}^{n} \varrho^{i-1}. \tag{4}$$

Przyjmijmy w równości wyrażającej tw. IX z § 29

$$a = \varrho \text{ a } b = 1,$$

znajdziemy tedy

$$\varrho^n - 1 = (\varrho - 1) \sum_{i=1}^{n} \sigma^{i-1}.$$

Zatem

$$a \leqq \varrho^n - 1$$

na podstawie związku (4). Mamy stąd

$$a < \varrho^n.$$

Dowiedliśmy więc, że liczba $a$ sprawdza jedną z nierówności (3). Żeby okazać, że liczba $a$ sprawdza także i drugą z tych nierówności, zważmy, że wzór (1) możemy napisać w kształcie następującym:

$$a = c_n \cdot \varrho^{n-1} + \sum_{i=1}^{n-1} c_i \varrho^{i-1}. \tag{5}$$

Ze względu na nierówność:

$$c_n \geqq 1$$

mamy (tw. V, § 22)

(6) $$c_n \cdot \varrho^{n-1} \geqq \varrho^{n-1}.$$

Ze związków (5) i (6) wynika nierówność

$$a \geqq \varrho^{n-1},$$

którą pragnęliśmy uzasadnić.

Dowiedliśmy więc, że wzór (1) pociąga za sobą nierówności (3).

*C*) Z wyników uzyskanych pod *A*) i pod *B*) wnosimy co następuje: jeżeli liczba $a$ przedstawialną jest przez wzór (1), to liczba $n$ ma wartość określoną w zupełności, mianowicie mamy:

$$n = p + 1$$

gdzie liczba $p$ określona jest nierównościami (2).

*D*) Jeżeli liczba $a$ sprawdza nierówność:

(4) $$a \geqq \varrho$$

to liczbę tę przedstawić możemy przez wzór (1). Istotnie w przypadku, kiedy

$$p = 1,$$

wzór (1) oczywiście zachodzić będzie przyjmując

$$n = 2$$

i oznaczając przez $c_2$ całkowitą część ilorazu — a przez $c_1$ resztę podziału liczby $a$ przez liczbę $\varrho$, albowiem związek (1) zachodzić będzie i będziemy mieli

$$c_1 < \varrho$$

na podstawie teoryi dzielenia; nadto będziemy też mieli

$$1 \leqq c_2 < \varrho$$

ze względu na nierówności:

$$\varrho \leqq a < \varrho^2.$$

Załóżmy chwilowo, że liczba $a$ przedstawialną byłaby przez wzór (1) gdybyśmy mieli

$$p = k$$

oznaczając przez $k$ pewną liczbę całkowitą od jedności nie mniejszą, i rozważajmy przypadek, kiedy mamy

$$p = k + 1.$$

Będziemy tedy mieli:

$$\varrho^{k+1} \leqq a < \varrho^{k+2}. \tag{5}$$

Oznaczmy przez $q$ całkowitą część ilorazu a przez $c_1$ resztę podziału liczby $a$ przez $\varrho$. Będziemy wówczas mieli:

$$a = q \cdot \varrho + c_1 \tag{6}$$

oraz

$$c_1 < \varrho. \tag{7}$$

Ponieważ związkom (5) możemy nadać kształt następujący:

$$\varrho \cdot \varrho^k \leqq a < \varrho \cdot \varrho^{k+1},$$

przeto, na podstawie wniosku z tw. III (§ 24), liczba $q$ sprawdzać będzie nierówności następujące:

$$\varrho^k \leqq q < \varrho^{k+1}.$$

Z tego wynika, na podstawie chwilowo przyjętego założenia, że możemy przyjąć:

$$q = \sum_{i=2}^{k+2} c_i \varrho^{i-2} \tag{8}$$

gdzie każda z liczb $c_i$ mniejszą będzie od $\varrho$ i gdzie liczba $c_{k+2}$ będzie od zera odmienną. Ze związków (6) i (8) wynika natychmiast na liczbę $a$ wzór następujący:

$$a = \sum_{i=1}^{k+2} c_i \varrho^{i-1}.$$

Z uzyskanych wyników wnosimy, na podstawie zasady indukcyi matematycznej, że rzeczywiście wszelka liczba całko-

wita $a$ od liczby $\varrho$ nie mniejsza przedstawialna jest przez wzór (1).

*E*) Pozostaje jeszcze do okazania, że wszystkie liczby $c_i$ wchodzące do wzoru (1) są określone w zupełności w zależności od liczby $a$. Wzór (1) napisać możemy w postaci następującej:

$$a = \varrho \sum_{i=2}^{n} c_i \varrho^{i-2} + c_1. \tag{9}$$

Jeżeli więc przyjmiemy:

$$q = \sum_{i=2}^{n} c_i \varrho^{i-2} \tag{10}$$

to liczba $q$ będzie całkowitą częścią ilorazu a $c_1$ — resztą podziału liczby $a$ przez $\varrho$. Zatem liczby $c_1$ i $q$ określone będą w zupełności. Z drugiej strony, na podstawie wyniku uzyskanego pod *C*), mamy pewność, że liczba $n$ określona będzie w zupełności w zależności od liczby $a$. Gdybyśmy mieli

$$n = 2,$$

to, ze wzoru (9), mielibyśmy

$$c_2 = q.$$

Przeto, w tym razie, twierdzenie zachodziłoby. Załóżmy chwilowo, że twierdzenie zachodzi w przypadku, kiedy mamy

$$n = k$$

i przypuśćmy, że

$$n = k + 1.$$

W takim razie, ze względu na to, ze liczba $q$ określoną jest w zupełności w zależności od liczby $a$, wszystkie te z liczb $c_i$, które wchodzą do wzoru (10) byłyby określone w zupełności w zależności od liczby $a$. Ponieważ zaś stwierdziliśmy już, że liczba $c_1$ jest określoną w zupełności w zależności od liczby $a$ w każdym razie, przeto wnosimy, że we wzorze (9), a więc i we wzorze (1), przy przyjętem chwilowo założeniu,

wszystkie liczby $c_i$ określone byłyby w zupełności w zależności od liczby $a$.

Z uzyskanych wyników wnosimy, że wszystkie liczby $c$ wchodzące do wzoru (1) będą istotnie zawsze określone w zupełności w zależności od liczby $a$. Podaliśmy zatem zupełny dowód twierdzenia, o które chodziło.

§ 31. Zamierzamy wyłożyć obecnie w jaki sposób można z każdą, od liczby jeden większą, liczbą połączyć oznaczoną numeracyę.

Oznaczmy przez $\varrho$ pewną, od jedności większą liczbę, i przyjmijmy za symbole specyficzne liczb, od liczby $\varrho$ mniejszych, jakiekolwiek symbole pojedyncze, to jest takie, z których żaden nie miałby postaci wzoru. Pozostaną tedy do określenia symbole specyficzne tylko takich liczb, które od liczby $\varrho$ nie są mniejsze. Oznaczmy przez $a$ jedną z tych liczb i zachowajmy oznaczenia wprowadzone przy wysłowieniu twierdzenia poprzedzającego. Będziemy tedy mieli:

$$a = \sum_{i=1}^{n} c_i \varrho^{i-1}. \tag{1}$$

Przyjmijmy

$$b = \sum_{i=2}^{n} c_i \varrho^{i-2}. \tag{2}$$

W takim razie będziemy mogli napisać wzór na liczbę $a$ w postaci następującej:

$$a = b \,.\, \varrho + c_1 .$$

Za symbol specyficzny liczby $a$ przyjmijmy symbol w który przemieni się symbol następujący

$$b\, c_1 \tag{3}$$

jeżeli w symbolu tym zastąpimy symbole $b$ i $c_1$ przez symbole specyficzne liczb $b$ i $c_1$.

Łatwo przekonamy się, że definicya poprzedzająca określa w zupełności symbol specyficzny liczby $a$. Istotnie, ponieważ

liczba $c_1$ jest od liczby $\varrho$ mniejszą, przeto symbol specyficzny liczby $c_1$ będzie w każdym razie określony bezpośrednio. W przypadku szczególnym, w którym mielibyśmy

$$n = 2,$$

byłoby

$$b = c_2,$$

mielibyśmy więc

$$b < \varrho$$

przeto symbol specyficzny liczby $b$ byłby także określony bezpośrednio. Stwierdzamy więc, że definicya powyższa określałaby w zupełności symbol specyficzny liczby $a$, gdybyśmy mieli

$$n = 2.$$

Załóżmy chwilowo, że rozważana definicya określałaby symbol specyficzny liczby $a$ w razie, gdy mielibyśmy

$$n = p,$$

oznaczając przez $p$ pewną liczbę całkowitą od liczby $2$ nie mniejszą, i rozważajmy przypadek, w którym byłoby

$$n = p + 1.$$

Ponieważ, na podstawie chwilowo przyjętego założenia, symbol specyficzny liczby $b$, określonej wzorem (2), byłby znany, przeto oczywiście moglibyśmy w sposób wymieniony wyprowadzić z symbolu (3) symbol specyficzny liczby $a$. Opierając się na zasadzie indukcyi matematycznej wnosimy z poprzedniego, że rozważana definicya określa rzeczywiście symbol specyficzny każdej liczby od liczby $\varrho$ nie mniejszej.

W dalszym ciągu rozumieć będziemy zawsze pod wyrazem „numeracya“ numeracyę typu poprzedzającego, prócz tylko w przypadku, kiedy wyraźnie zastrzeżemy, że chodzi o pewną numeracyę innego typu.

W stosunku do omówionej numeracyi liczba $\varrho$ zwie się podstawą a symbole specyficzne liczb od liczby $\varrho$ mniejszych — cyframi; cyfry wchodzące do symbolu specyficznego jakiejkolwiek oznaczonej liczby $a$ zowią się cyframi tej liczby;

każda liczba kształtu $\varrho^{p-1}$, gdzie $\varrho$ oznacza podstawę numeracyi, a $p$ jakąkolwiek, od jedności nie mniejszą, liczbę nazywa się jednostką rzędu $p$. Winniśmy dodać, że oznaczamy często przez wyraz „cyfra“ nie jeden z omówionych przed chwilą symbolów lecz samą liczbę, którą taki symbol przedstawia; nieporozumienia stąd nie może wyniknąć żadnego, bo sama budowa zdania, zawierającego wyraz „cyfra“, zawsze jasno wskazuje na znaczenie, w jakiem wyraz „cyfra“ ma być rozumiany.

Oznaczając w dalszym ciągu przez $\varrho$ podstawę numeracyi zwróćmy się do wzoru (1). Cyframi liczby $a$ będą oczywiście symbole specyficzne liczb $c_i$. Uważajmy jedną z liczb $c_i$, powiedzmy $c_p$; we wzorze (1) liczba $c_p$ będzie jednym ze współczynników iloczynu, którego drugim współczynnikiem będzie jednostka rzędu $p$; z tej przyczyny cyfra oznaczająca liczbę $c_p$ zowie się cyfrą jednostek rzędu $p$ w liczbie $a$, albo krócej cyfrą rzędu $p$ liczby $a$; cyfrę jednostek pierwszego rzędu jakiejkolwiek liczby nazywamy dla skrócenia cyfrą jedności tej liczby.

Należy odróżniać skrupulatnie cyfrę jednostek rzędu $p$ w pewnej liczbie $a$ od liczby jednostek rzędu $p$ w tejże liczbie $a$; pod liczbą jednostek rzędu $p$ w pewnej liczbie $a$ rozumiemy całkowitą część ilorazu liczby $a$ przez jednostkę rzędu $p$.

Zwracając się do części $A$) i $B$) dowodu twierdzenia z §-u poprzedzającego upewniamy się natychmiast, że zachodzą twierdzenia następujące:

**Tw. II.** W numeracyi o podstawie $\varrho$ liczba $n$ cyfr dowolnie przyjętej liczby $a$ równa się najmniejszej liczbie całkowitej $k$ sprawdzającej nierówność

$$\varrho^k > a.$$

**Tw III.** Jeżeli oznaczymy przez $n$ liczbę cyfr pewnej liczby $a$, to liczba jednostek rzędu $p$ w liczbie $a$ równa się zeru w razie, kiedy mamy

$$p \geqq n,$$

jeżeli zaś mamy

$$p < n,$$

to liczba jednostek rzędu $p$ w liczbie $a$ równa się liczbie, której symbol specyficzny wynika z symbolu specyficznego liczby $a$ przez proste usunięcie cyfr jednostek rzędu niższego od $p$.

Ponieważ, na podstawie tw. I, przy oznaczonej podstawie numeracyi cyfry oznaczonej liczby są określone w zupełności, przeto mamy:

**Tw. IV.** Żeby dwie liczby przedstawione w tej samej numeracyi były równe sobie, koniecznem jest i oczywiście wystarczającem, żeby liczby cyfr tych liczb były sobie równe i żeby każda cyfra każdej z uważanych liczb równała się cyfrze tego samego rzędu drugiej liczby. W innych wyrazach: żeby dwie liczby przedstawione w numeracyi o pewnej oznaczonej podstawie były sobie równe, koniecznym jest i wystarcza, żeby symbole specyficzne tych liczb były identyczne.

**Tw. V.** Jeżeli z dwóch liczb przedstawionych w tej samej numeracyi, liczba cyfr jednej większą jest od liczby cyfr drugiej, to liczba o większej liczbie cyfr większą jest od drugiej liczby. Jeżeli zaś liczby cyfr nierównych sobie liczb są sobie równe, to, żeby poznać która z tych liczb większą jest od drugiej, porównywamy poczynając od cyfry najwyższego rzędu kolejno każdą cyfrę jednej z nich, powiedzmy liczby $a$, z cyfrą tego samego rzędu drugiej liczby $b$. Oznaczmy tedy przez $\alpha$ pierwszą cyfrę liczby $a$, która odmienną byłaby od cyfry tego samego rzędu $\beta$ liczby $b$. Taką cyfrę $\alpha$ liczby $a$ spotkamy niezawodnie albowiem inaczej liczby $a$ i $b$ byłyby sobie równe. Jeżeli zachodzić będzie nierówność

(1) $$\alpha > \beta$$

to zachodzić będzie także nierówność

(2) $$a > b$$

gdybyśmy zaś mieli

(3) $$\alpha < \beta$$

to mielibyśmy także

(4) $$a < b.$$

Dowód. Pierwsza część twierdzenia tego wynika natychmiast z tw. II. Żeby uzasadnić część drugą oznaczmy przez $p$ wspólną wartość rzędów cyfr $\alpha$ i $\beta$ w liczbach $a$ i $b$, przez $a'$ i $b'$ liczby jednostek rzędu $p$ odpowiednio w tychże liczbach a przez $\varrho$ podstawę numeracyi. Będziemy wtedy mieli

$$a = a' \varrho^{p-1} + a'' \tag{5}$$

$$b = b' \varrho^{p-1} + b'' \tag{6}$$

oznaczając przez $a''$ i $b''$ liczby mniejsze od liczby $\varrho^{p-1}$. Załóżmy, że liczby $\alpha$ i $\beta$ sprawdzają nierówność (1). W takim razie mielibyśmy

$$a' > b'. \tag{7}$$

Gdyby bowiem liczba $p$ równała się wspólnej liczbie $n$ cyfr liczb $a$ i $b$, to mielibyśmy

$$a' = \alpha \text{ i } b' = \beta$$

i nierówność (7) oczywiście zachodziłaby na podstawie nierówności (1). Gdyby zaś liczba $p$ mniejszą była od liczby $n$, to mielibyśmy

$$a' = x \,.\, \varrho + \alpha$$
$$b' = x \,.\, \varrho + \beta$$

oznaczając przez $x$ pewną liczbę, o tylu cyfrach ile wynosi wyrażenie

$$n - p.$$

Zatem i w tym razie nierówność (1) pociągałaby za sobą nierówność (7). Mamy oczywiście:

$$a \geqq a' \varrho^{p-1},$$

z drugiej zaś strony mamy

$$b < (b' + 1) \varrho^{p-1}$$

ze względu na nierówność

$$b'' < \varrho^{p-1}.$$

A ponieważ na podstawie nierówności (7) mamy

$$a' \geqq b' + 1,$$

przeto mamy

$$a > b$$

o co właśnie chodziło. Gdybyśmy byli wyszli z założenia, iż zachodzi nierówność (3), to stwierdzilibyśmy w sposób analogiczny, że liczby $a$ i $b$ sprawdzają nierówność (4). Dowiedliśmy więc w zupełności twierdzenia, o które chodziło.

Żeby ustalić nazwy liczb przyjmując numeracyę o pewnej podstawie $\varrho$, nazywamy osobnymi wyrazami liczby jednocyfrowe. Nazwę zaś na liczbę kilkucyfrową tworzymy wymawiając kolejno nazwę każdej cyfry i nazwę rzędu odnośnej jednostki, poczynając od cyfry jednostek rzędu najwyższego. Czytelnik łatwo stwierdzi, że umowa ta daje możność nazwania każdej oznaczonej liczby.

§ 32. Przechodzimy do powszechnie przyjętej numeracyi, do tak zwanej numeracyi dziesiętnej. Liczby zero i jeden oznaczamy, jak to już nadmieniliśmy w rozdziale I, przez symbole

$$0 \text{ i } 1.$$

Wszystkie inne cyfry numeracyi dziesiętnej są:

$$2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 9.$$

Znaczenia cyfr tych określamy równościami następującemi:

$$\begin{aligned} 2 &= 1+1 \\ 3 &= 2+1 \\ 4 &= 3+1 \\ 5 &= 4+1 \\ 6 &= 5+1 \\ 7 &= 6+1 \\ 8 &= 7+1 \\ 9 &= 8+1. \end{aligned}$$

Zatem, podstawą numeracyi dziesiętnej jest liczba

$$9+1.$$

Liczbę tę nazywamy dziesięć, skąd też pochodzi nazwa nu-

meracyi dziesiętnej. Symbolem specyficznym liczby dziesięć w numeracyi dziesiętnej będzie oczywiście symbol

*10.*

Nazwy liczb jednocyfrowych

*2*, *3*, *4*, *5*, *6*, *7*, *8* i *9*

w numeracyi dziesiętnej są odpowiednio następujące: dwa, trzy, cztery, pięć, sześć, siedm, ośm i dziewięć.

Określone przed chwilą cyfry numeracyi dziesiętnej zowią się cyframi arabskiemi.

Stosując przy nazywaniu liczb sposób wskazany przy końcu paragrafu poprzedzającego, oczywiście nie mielibyśmy potrzeby wprowadzania innych osobnych nazw liczb prócz nazw już określonych; nawet wyraz dziesięć byłby zbyteczny, bo moglibyśmy wyraz ten zastąpić przez wyrażenie jednostka drugiego rzędu. Jednak, dla skrócenia mowy, posługujemy się nie tylko wyrazem dziesięć ale jeszcze wyrazami: sto, tysiąc, milion, bilion i trylion, które oznaczają odpowiednio jednostki trzeciego, czwartego, siódmego, dziesiątego i trzynastego rzędu. Nazwy na liczby mniejsze od tysiąca tworzymy w zasadzie w sposób wskazany przy końcu paragrafu poprzedzającego, wprowadzając jednak pewne, ogólnie przyjęte i niewątpliwie dobrze czytelnikowi znane zmiany.

Uważajmy teraz jakąkolwiek liczbę $a$, od tysiąca nie mniejszą, i oznaczmy: przez $t$ największą z liczb

$$10^3,\ 10^6,\ 10^9,\ 10^{12}$$

nie przekraczającą liczbę $a$, przez $q$ — całkowitą część ilorazu a przez $r$ — resztę podziału liczby $a$ przez liczbę $t$. Jeżeli mamy $q = 1$, to, żeby nazwać liczbę $a$, wymawiamy nazwę liczby $t$ a potem nazwę liczby $r$. Jeżeli zaś liczba $q$ jest od jedności większą, to wymawiamy nazwę liczby $q$, następnie nazwę liczby $t$ w pierwszym lub drugim przypadku deklinacyi liczby mnogiej zależnie od tego, czy liczba $q$ jest mniejszą czy nie od liczby pięć; nareszcie wymawiamy nazwę liczby $r$.

Nazwę jakiejkolwiek liczby $a$, przedstawionej przez jej symbol w numeracyi dziesiętnej, możemy natychmiast wymienić. Żeby się o tem przekonać oznaczmy przez litery $t$, $q$ i $r$ te same elementy, co przed chwilą, a przez $p$ — rząd jednostki, którą oznacza litera $t$. Jeżeli z symbolu specyficznego liczby $a$ usuniemy cyfry jednostek rzędu niższego od $p$, to otrzymamy symbol specyficzny liczby $q$; jeżeli zaś usuniemy cyfry jednostek rzędu $p$ i rzędów wyższych (o ile cyfry takie istnieją), to otrzymamy symbol specyficzny liczby $r$. Zatem, jeżeli liczba $a$ przedstawiona jest przez jej symbol specyficzny, to sprawa nazwania tej liczby sprowadza się natychmiast to kwestyi tego samego rodzaju co do liczb od niej mniejszych $q$ i $r$. Ponieważ zaś nazwy liczb aż do tysiąca włącznie uważamy za znane, przeto, na podstawie zasady indukcyi matematycznej, stwierdzamy, że przyjęte umowy dają istotnie możność natychmiast wyczytać nazwę liczby z jej symbolu w numeracyi dziesiętnej. Oczywiście odwrotnie, możemy natychmiast napisać symbol numeracyi dziesiętnej na liczbę, której wedle powyższych prawideł utworzona nazwa jest dana.

§ 33. Numeracya rzymska, używana niekiedy, jest w rzeczywistości zniekształconą postacią numeracyi dziesiętnej. W numeracyi tej nie istnieje cyfra na liczbę zero. Żeby wyprowadzić z symbolu, przedstawiającego w zwykłej numeracyi dziesiętnej pewną liczbę $a$ od zera odmienną, symbol tej liczby w numeracyi rzymskiej, postępujemy w sposób następujący: jeżeli cyfra jedności (czyli jednostek rzędu pierwszego) równa się zeru, to poprzestajemy na usunięciu tej cyfry; jeżeli zaś tak nie jest, to zastępujemy rozważaną cyfrę wedle reguł wyrażonych równościami następującemi:

$$1 = I,\ 2 = II,\ 3 = III,\ 4 = IV,\ 5 = V,$$
$$6 = VI,\ 7 = VII,\ 8 = VIII,\ 9 = IX.$$

Gdyby liczba $a$ była liczbą jednocyfrową, to wynikiem czynności poprzedzającej byłby żądany symbol. Jeżeli zaś liczba cyfr liczby $a$ większą jest od jedności, to z cyfrą dziesiątek operujemy podobnie jak z cyfrą jedności, z tą jednak odmianą,

że zamiast symbolów:

$$I,\ II,\ III,\ IV,\ V,\ VI,\ VII,\ VIII,\ IX \qquad (1)$$

piszemy odwowiednio symbole

$$X,\ XX,\ XXX,\ XL,\ L,\ LX,\ LXX,\ LXXX,\ XC. \qquad (2)$$

Jeżeli liczba $a$ jest liczbą dwucyfrową, to wynikiem dwóch czynności poprzedzających będzie żądany symbol, jeżeli zaś liczba cyfr liczby $a$ przekracza liczbę dwa, to z cyfrą setek postępujemy podobnie jak z cyfrą dziesiątek, zastępując jednak symbole (2) odpowiednio przez symbole następujące:

$$C,\ CC,\ CCC,\ CD,\ D,\ DC,\ DCC,\ DCCC,\ CM. \qquad (3)$$

Jeżeli liczba $a$ jest liczbą trójcyfrową, to, po wykonaniu czynności poprzedzających, uzyskamy symbol rzymski na liczbę $a$, jeżeli zaś liczba cyfr liczby $a$ jest większą od liczby trzy, to, żeby uzyskać żądany symbol na liczbę $a$, zastępujemy ogół cyfr rzędów wyższych od rzędu trzeciego przez liczbę $M$ powtórzoną tyle razy, ile wynosi liczba tysięcy liczby $a$.

Z poprzedniego jasno wynika, że, o ile chodzi o liczbę mniejszą od liczby *10000*, numeracya rzymska jest numeracyą dziesiętną zniekształconą; zniekształcenie polega na tem, że na cyfry odmiennych rzędów mamy symbole całkiem odmienne; powodem zaś tego zniekształcenia jest ta okoliczność, że numeracya rzymska nie posiada symbolu na liczbę zero. Co do liczb większych albo równych liczbie *10000*, to numeracya rzymska oczywiście traci charakter numeracyi dziesiętnej i zbliża się do numeracyi przyjętej prowizorycznie w rozdziale I. Wprawdzie możnaby oczywiście zachować numeracyi rzymskiej charakter numeracyi dziesiętnej dla wszystkich liczb mniejszych od dowolnie przyjętej potęgi $10^n$ $(n > 4)$ liczby *10*; należałoby tylko wprowadzić osobne symbole na liczby

$$10^4,\ 10^5,\ \ldots\ 10^{n-1},$$

ale oczywiście, po takiem uzupełnieniu, omawiana numeracya straciłaby charakter numeracyi dziesiętnej dla liczb większych od liczby $10^n$.

Ostatecznie dochodzimy do wniosku następującego.

Numeracya rzymska, chociażbyśmy ją uzupełnili wskazanym sposobem, zawsze straci charakter numeracyi dziesiętnej dla liczb przekraczających pewną liczbę. Widzimy jednocześnie, że numeracya dziesiętna, albo nawet ogólniej wszelka numeracya oparta na zasadach wyłożonych w § 31, jest numeracyą jednolitą dzięki wprowadzeniu symbolu specyficznego na liczbę zero i stosownemu użyciu tego symbolu.

Z powodu swojej niejednolitości numeracya rzymska nie nadaje się do celów naukowych i używaną bywa prawie wyłącznie do oznaczania numerów porządkowych elementów pewnych ciągów.

## VIII. Teorya wykonywania działań zasadniczych w numeracyi dziesiętnej.

§. 34. Działania zasadnicze są: dodawanie, odejmowanie, mnożenie i dzielenie.

Zadanie rozdziału niniejszego polega na ustanowieniu reguł, na podstawie których moglibyśmy przedstawić w numeracyi dziesiętnej wynik wykonania jednego z czterech działań zasadniczych nad oznaczonemi liczbami, przedstawionemi w tejże numeracyi.

W dalszym ciągu wyrażenie „wykonać pewne działanie“ równoważnem będzie wyrażeniu następującemu: „przedstawić w numeracyi dziesiętnej wynik rozważanego działania w razie, kiedy liczby, mające być objęte działaniem, przedstawione już są w rzeczonej numeracyi“; wyrażenie „wyznaczyć pewną liczbę całkowitą“ oznaczać będzie sprawę przedstawienia rzeczonej liczby w numeracyi dziesiętnej.

Czytelnik łatwo spostrzeże, że teorya, którą zamierzamy wyłożyć, mogłaby być rozszerzoną do przypadku, w którym podstawą numeracyi byłaby jakakolwiek liczba całkowita $\varrho$ ($\varrho > 1$).

§ 35. **Dodawanie.** W dalszym ciągu zobaczymy, że dzia-

działanie dodawania może być wykonane, wykonując kolejno pewną skończoną liczbę czynności, z których każda polega na wyznaczeniu sumy trzech liczb jednocyfrowych, z których jedna przynajmniej nie przekracza liczby jeden. Z tej przyczyny zajmiemy się przedewszystkiem sprawą wyznaczenia takiej sumy trzech liczb.

Sumę rzeczonego typu oczywiście przedstawić możemy w kształcie następującym:

$$(\alpha + \beta) + \gamma \qquad (1)$$

oznaczając przez $\alpha$, $\beta$ i $\gamma$ liczby jednocyfrowe, z których liczba $\alpha$ nie przekracza jedności.

Sumę $\alpha + \beta$ będziemy mogli oczywiście wyznaczyć bezpośrednio na podstawie definicyi dodawania i definicyi cyfr arabskich: wartością sumy tej oczywiście będzie mogła być którakolwiek z liczb od zera do dziesięciu włącznie i tylko jedna z tych liczb. Zatem wyznaczenie sumy (1) redukuje się natychmiast do wyznaczenia sumy kształtu

$$\delta + \gamma \qquad (2)$$

oznaczając przez $\gamma$ liczbę jednocyfrową a przez $\delta$ liczbę nie większą od dziesięciu. Gdybyśmy mieli $\delta = 10$, to suma (2) byłaby oczywiście liczbą dwucyfrową, w której cyfra dziesiątek byłaby jedynką a cyfra jedności cyfrą przedstawiającą liczbę $\gamma$. Pozostaje więc tylko do zbadania przypadek, kiedy w sumie (2) każda z liczb $\delta$ i $\gamma$ jest liczbą jednocyfrową. Gdyby jedna z liczb $\delta$ albo $\gamma$ równała się zeru, to suma (2) równałaby się drugiej z nich. Zatem, przy badaniu sumy (2), możemy poprzestać na przypadku, w którym żadna z jednocyfrowych liczb $\delta$ i $\gamma$ nie równa się zeru. Wartość sumy, o którą chodzi, będziemy mogli zawsze wyznaczyć w sposób wytłumaczony niżej według tabelki podanej na stronie następującej.

Sposób utworzenia górnego czyli pierwszego wiersza i skrajnej prawej, czyli ostatniej kolumny nie wymaga oczywiście żadnych wyjaśnień. Oznaczmy tedy przez $s$ którąkolwiek z tych liczb powyższej tabelki, które nie należą ani do

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 1 |
| | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 2 |
| | | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 3 |
| | | | 8 | 9 | 10 | 11 | 12 | 13 | 4 |
| | | | | 10 | 11 | 12 | 13 | 14 | 5 |
| | | | | | 12 | 13 | 14 | 15 | 6 |
| | | | | | | 14 | 15 | 16 | 7 |
| | | | | | | | 16 | 17 | 8 |
| | | | | | | | | 18 | 9 |

pierwszego wiersza ani do ostatniej kolumny. Przy układaniu tabelki przyjęliśmy za wartość liczby $s$ wynik dodania jedności do liczby położonej bezpośrednio nad liczbą $s$ w tej kolumnie, w której liczba ta znajduje się. Stosując tę zasadę, począwszy od wiersza drugiego od góry, kolejno do każdego wiersza wyznaczyliśmy wszystkie liczby umieszczone w tabelce i nie znajdujące się ani w pierwszym wierszu ani w ostatniej kolumnie. Na samej tabelce uwidocznioną jest ta okoliczność, że we wierszach 3-im, 4-ym, . . . 10ym od góry nie zapełniliśmy wcale pierwszej, dwóch pierwszych, . . . osiem skrajnych przedziałek po lewej stronie.

Z wyjaśnień poprzedzających wynika, że ułożenie powyższej tabelki wymaga tylko wyznaczenia pewnych sum postaci następującej:

$$a + 1.$$

Przypadek, w którymby liczba $a$ była liczbą jednocyfrową, mieliśmy już sposobność omówić wyżej. Gdyby liczba $a$ była liczbą dwucyfrową, której cyfra dziesiątek równałaby się jedynce a cyfra jedności pewnej liczbie $b$, to mielibyśmy

$$a = 10 + b,$$

skąd

$$a + 1 = 10 + (b + 1).$$

Gdyby więc zachodziła nierówność

$$b < 9,$$

to cyfra dziesiątek sumy $a + 1$ równałaby się jedności, a cyfra jedności — liczbie $b + 1$, którą moglibyśmy wyznaczyć bezpośrednio. Układając rozważaną tabelkę, stwierdzamy à posteriori, że przy tem, co do sumy

$$a + 1,$$

prócz omówionych już przypadków, żadne inne nie nadarzają się.

Ze sposobu utworzenia omówionej tabelki i z definicyi dodawania wynika, że sumę dwóch danych liczb jednocyfrowych od zera odmiennych znajdziemy zawsze w rzeczonej tabelce w sposób następujący: oznaczmy przez $x$ tę z danych liczb, która nie jest większą od drugiej liczby $y$; liczba $x$ równać się będzie pewnej liczbie $x'$ położonej w ostatniej kolumnie; oznaczmy przez $(W)$ ten wiersz tabelki, do którego należy liczba $x'$; w takim razie suma

$$x + y$$

równać się będzie liczbie położonej w tej przedziałce wiersza $(W)$ która należy do kolumny, u góry której umieszczona jest liczba równa liczbie $y$.

Na podstawie poprzedzającego, sprawa wyznaczania sumy trzech jednocyfrowych liczb, z których jedna nie przekracza jedności, jest załatwiona.

Przechodząc do sprawy wyznaczenia sumy dwóch liczb w przypadku ogólnym, zastąpimy to zagadnienie przez zagadnienie nieco ogólniejsze, polegające na wyznaczeniu sumy trzech liczb $a$, $b$ i $\gamma$, z których jedna, mianowicie $\gamma$, nie przekracza jedności.

Gdyby wyjątkowo liczba $\gamma$ i jedna przynajmniej z liczb $a$ i $b$ równały się zeru, to dodawanie zaznaczone w wyrażeniu:

$$a + b + \gamma$$

byłoby natychmiastowe. Zakładając, że okoliczność ta nie za-

chodzi, oznaczmy przez $n\,(n>1)$ liczbę cyfr tej z liczb $a$ albo $b$, której liczba cyfr nie jest mniejszą od liczby cyfr drugiej z nich. Oznaczmy dalej przez $\alpha$ i $\beta$ cyfry jedności liczb $a$ i $b$. Jeżeli tedy przyjmiemy

$$a = a' \,.\, 10 + \alpha$$
$$b = b' \,.\, 10 + \beta,$$

to żadna z liczb $a'$ albo $b'$ nie będzie miała więcej niż $n-1$ cyfr. Mamy

(1) $$a + b + \gamma = (a' + b') \,.\, 10 + (\alpha + \beta + \gamma).$$

Sumę

(2) $$\alpha + \beta + \gamma$$

potrafimy wyznaczyć na podstawie wyżej wyłożonego. Suma ta będzie liczbą najwyżej dwucyfrową i w takim razie, cyfra dziesiątek równać się będzie jedności, albowiem rozważana suma, jak łatwo stwierdzić można na podstawie przytoczonej wyżej tabelki, zawsze mniejsza jest od liczby 20.

Oznaczmy przez $\gamma'$ liczbę dziesiątek sumy $\alpha + \beta + \gamma$. Liczba $\gamma'$ na podstawie poprzedzającego będzie tylko mogła być albo zerem albo jednością. Oznaczmy jeszcze przez $x$ cyfrę jedności sumy (2); będziemy tedy mieli

$$\alpha + \beta + \gamma = \gamma' \,.\, 10 + x.$$

Na podstawie równości tej mamy z równości (1) równość:

(3) $$a + b + \gamma = (a' + b' + \gamma') \,.\, 10 + x.$$

Zatem: cyfra jednostek sumy $a + b + \gamma$ równa się liczbie $x$ a liczba dziesiątek — sumie $a' + b' + \gamma'$. Ponieważ zaś cyfra jednostek jakiegokolwiek rzędu $p$ liczby dziesiątek dowolnie przyjętej liczby $s$ $(s>9)$ równa się oczywiście cyfrze jednostek rzędu $p+1$ liczby $s$, przeto, na podstawie równości (3), wyznaczenie sumy $a + b + \gamma$ sprowadziliśmy do wyznaczenia sumy $a' + b' + \gamma'$. To ostatnie zadanie jest tego samego typu, co zadanie pierwsze, ale obejmuje liczby, z których żadna nie ma więcej niż $n-1$ cyfr a — jedna przynajmniej ma ich niezawodnie $n-1$.

Z poprzedzającego wnosimy, na podstawie zasady indukcyi matematycznej, że zgodnie z zapowiedzią sumę $a+b+\gamma$ a więc i sumę $a+b$ zdołamy wyznaczyć, wykonywając pewną liczbę czynności, z których każda polega na załatwieniu omówionej już sprawy wyznaczenia sumy trzech liczb jednocyfrowych, pomiędzy któremi jedna nie przekracza jedności; liczba wspomnianych czynności oczywiście nie może być większą od liczby, którą oznaczyliśmy wyżej przez $n$.

Ponieważ wyznaczenie sumy kilku liczb, na podstawie definicyi takiej sumy, wymaga tylko wykonania pewnej liczby czynności, z których każda polega na wyznaczeniu sumy dwóch liczb, przeto możemy uważać sprawę wyznaczania sumy w przypadku najogólniejszym za załatwioną.

Postępując wskazaną drogą, żądana suma będzie oczywiście ostatnim elementem pewnego ciągu sum, z których każda będzie sumą dwóch liczb.

Sumę kiku liczb możemy także wyznaczyć inną metodą, przy której wyznaczamy bezpośrednio w pewnym porządku, każdą cyfrę sumy.

Ta druga metoda wynika natychmiast z twierdzenia następującego: cyfra jedności sumy kilku liczb równa się cyfrze jedności sumy cyfr jedności składników a liczba dziesiątek — wynikowi dodania, do liczby dziesiątek sumy cyfr jedności składników, sumy liczb dziesiątek tych składników.

Czytelnik uzasadni to twierdzenie z największą łatwością i spostrzeże, w jaki sposób korzystać z niego można przy wyznaczaniu sumy kilku liczb.

§ 36. **Odejmowanie.** Oznaczmy przez $a$ i $b$ $(a \geqq b)$ dwie liczby dane. Właściwy cel tego paragrafu polega na wyznaczeniu różnicy kształtu

$$a - b.$$

Żeby jednak uzyskać większą prostotę wykładu, zastąpimy to zagadnienie przez zagadnienie nieco ogólniejsze, polegając na wyznaczeniu różnicy postaci następującej:

(1) $$a - (b + \gamma)$$

gdzie oznaczyliśmy przez $\gamma$ trzecią liczbę daną nie większą od jedności.

Celem skrócenia wprowadzamy wyrażenie „różnica typu $(A)$“; pod wyrażeniem tym rozumieć będziemy różnicę (1) w tym przypadku szczególnym, kiedy liczba $b$ i sama różnica równają się liczbom jednocyfrowym.

Zastąpmy w różnicy (1) liczbę $b$ przez liczbę jednocyfrową $\beta$ i zastanówmy się nad warunkami, przy których uzyskana w ten sposób różnica

$$a - (\beta + \gamma) \tag{2}$$

będzie różnicą typu $(A)$. Ponieważ mamy

$$\beta + \gamma \leqq 10,$$

przeto liczba $a$ winna będzie sprawdzać w każdym razie nierówność

$$a < 20. \tag{3}$$

Zatem liczba $a$ będzie albo liczbą jednocyfrową, albo liczbą dwucyfrową, w której cyfra dziesiątek równać się będzie jedności. W pierwszym przypadku różnica (2), o ile sensu nie będzie pozbawioną, oczywiście będzie równać się liczbie jednocyfrowej.

W drugim przypadku i w razie, kiedy mielibyśmy jednocześnie:

$$\beta + \gamma = 10,$$

nierówność (3) byłaby oczywiście warunkiem wystaczającym do tego, żeby różnica (2) równała się liczbie jednocyfrowej. Pozostaje więc do zbadania przypadek, kiedy mamy jednocześnie

$$a \geqq 10 \text{ i } \beta + \gamma < 10.$$

W takim razie suma $\beta + \gamma$ równałaby się liczbie jednocyfrowej $x$. Żeby różnica (2) równała się tedy liczbie jednocyfrowej oczywiście koniecznem byłoby i wystarczającem, żeby cyfra jedności liczby $a$ była mniejszą od liczby $x$.

Przechodzimy obecnie do sprawy wyznaczenia różnicy (2) w założeniu, że różnica ta jest typu $(A)$, że więc rozważana różnica równa się liczbie jednocyfrowej. Sumę $\beta + \gamma$ zdołamy oczywiście wyznaczyć natychmiast w każdym razie.

Gdybyśmy mieli

$$\beta + \gamma = 0,$$

a więc

$$\beta = \gamma = 0,$$

to różnica, o którą chodzi równałaby się liczbie $a$.

Gdyby zaś zachodziła równość

$$\beta + \gamma = 10$$

to liczba $a$ byłaby liczbą dwucyfrową a różnica (2) równałaby się tedy cyfrze jedności liczby $a$.

Gdybyśmy nareszcie mieli

$$0 < \beta + \gamma < 10,$$

to wyznaczylibyśmy oczywiście różnicę, o którą chodzi, posługując się stosownie tabelką podaną w paragrafie poprzedzającym.

Przechodzimy obecnie do sprawy wyznaczenia różnicy (1) w przypadku ogólnym, kiedy różnica (1) nie jest typu $(A)$, zakładając oczywiście, że warunek wykonalności odnośnego odejmowania jest spełniony.

Oznaczając przez $n$ liczbę cyfr liczby $a$ będziemy mieli

$$n > 1. \tag{4}$$

Wyjątkowo odejmowanie oznaczone w wyrażeniu (1) może być natychmiastowe: mianowicie kiedy obie liczby $b$ i $\gamma$ równają się zeru.

W takim razie żądana różnica równałaby się liczbie $a$.

Zwróćmy się do przypadku, kiedy ta okoliczność wyjątkowa nie zachodzi i oznaczmy przez $a'$ i $b'$ liczby dziesiątek liczb $a$ i $b$ a przez $\alpha$ i $\beta$ cyfry jedności tych liczb. Mamy:

$$(5) \qquad \begin{cases} a = a' \,.\, 10 + \alpha \\ b = b' \,.\, 10 + \beta. \end{cases}$$

Dwa przypadki mogą się nadarzyć: możemy mieć

(6) $$\alpha \geqq (\beta + \gamma)$$

albo

(7) $$\alpha < (\beta + \gamma).$$

W przypadku, kiedy zachodzi związek (6), mamy:

$$a' \geqq b'$$

inaczej bowiem mielibyśmy

$$a < b$$

i odejmowanie zaznaczone w wyrażeniu (1) byłoby niewykonalne. Na podstawie uwagi tej, oraz związków (5) i (6), mamy

(8) $$a - (b + \gamma) = (a' - b')\ 10 + \{\alpha - (\beta + \gamma)\}.$$

Ponieważ $\alpha$ jest liczbą jednocyfrową, przeto różnica

$$\alpha - (\beta + \gamma)$$

będzie także liczbą jednocyfrową. Wnosimy więc z równości (8), że, w rozważanym przypadku, cyfra jedności różnicy $a - (b + \gamma)$ równać się będzie różnicy $\alpha - (\beta + \gamma)$ a liczba dziesiątek różnicy $a' - b'$.

Przejdźmy do przypadku, kiedy zachodzi nierówność (7). Ze względu na tę nierówność zachodzić musi nierówność:

$$a' > b'$$

czyli

(9) $$a' \geqq b' + 1.$$

gdyby bowiem warunek ten spełniony nie był, to wyrażenie

$$a - (b + \gamma)$$

pozbawione byłoby sensu.

Na podstawie związku (9) i wzorów (5), oraz nierówności

$$10 + \alpha > \beta,$$

która oczywiście zachodzić będzie, mamy:

(10) $$a - (b + \gamma) = \{a' - (b' + 1)\}\ 10 + \{(10 + \alpha) - (\beta + \gamma)\}.$$

Na podstawie nierówności (7), która właśnie charakteryzuje rozważany przypadek, różnica

$$(10 + \alpha) - (\beta + \gamma) \qquad (11)$$

równać się będzie liczbie jednocyfrowej. Opierając się na tej uwadze, stwierdzamy na podstawie równości (10), że w rozważanym przypadku cyfra jedności różnicy (1) równa się różnicy (11) a liczba dziesiątek — wyrażeniu

$$a' - (b' + 1).$$

Z uzyskanych wyników wnosimy, że w obu przypadkach cyfra jedności wyrażenia (1) równa się różnicy typu $(A)$ a liczba dziesiątek wyrażeniu następującemu

$$a' - (b' + \gamma'),$$

gdzie $\gamma'$ równa się zeru albo jedności, mianowicie: zeru w przypadku, kiedy zachodzi związek (6) a jedności w przypadku, kiedy zachodzi nierówność (7). Ponieważ zaś liczba cyfr liczby $a'$ równa się różnicy $n - 1$, przeto dochodzimy do wyniku następującego: jeżeli liczby $b$ i $\gamma$ nie równają się obie zeru, jeżeli nadto różnica ta nie jest typu $(A)$, jeżeli więc jednem słowem różnica (1) nie da się wyznaczyć bezpośrednio, to, przez wyznaczenie pewnej różnicy typu $(A)$, możemy sprowadzić sprawę wyznaczenia rozważanej różnicy do wyznaczenia różnicy tego samego typu co ta różnica, ale takiej, w której liczba cyfr odjemnej jest o jedną jedność mniejszą od liczby cyfr odjemnej w różnicy danej.

Ponieważ zaś różnica (1) byłaby niewątpliwie typu $(A)$, gdyby liczba $a$ była jednocyfrową, przeto stwierdzamy na podstawie zasady indukcyi matematycznej, że wyznaczenie różnicy (1), jeżeli tylko odnośne odejmowanie jest wykonalne, zawsze uskutecznionem być może albo bezpośrednio, albo przez wyznaczenie najwyżej tylu różnic typu $(A)$, ile wynosi liczba cyfr odjemnej. Załatwiliśmy więc w zupełności sprawę wyzaczenia różnicy dwóch danych liczb.

§. 37. **Mnożenie.** Podobnie do tego, cośmy uczynili mówiąc o dodawaniu i o odejmowaniu i z analogicznej przy-

czyny, zastąpimy wyrażenie, którego wyznaczenie stanowi właściwy przedmiot naszych dociekań, przez wyrażenie nieco ogólniejsze. Zamiast rozważania iloczynu dwóch czynników $a$ i $b$, rozważać będziemy, przynajmniej na początku, wyrażenie następujące

(1) $$a \,.\, b + \gamma$$

gdzie oznaczyliśmy przez $\gamma$ liczbę jednocyfrową, sprawdzającą nierówność:

(2) $$\gamma \leqq 8.$$

W przypadku szczególnym, którym zajmiemy się najpierw, i w którym liczby $a$ i $b$ są liczbami jednocyfrowymi, $\alpha$ i $\beta$, nadamy, dla krótkości, wyrażeniu (1) miano wyrażenia typu $(A)$.

Wyznaczenie wyrażenia typu $(A)$, a więc wyrażenia

(3) $$\alpha \,.\, \beta + \gamma$$

gdzie oznaczyliśmy przez $\alpha$, $\beta$ i $\gamma$ liczby jednocyfrowe, z których $\gamma$ sprawdza warunek (2), sprowadza się oczywiście do wyznaczenia iloczynu

(4) $$\alpha \,.\, \beta.$$

Rozwiązanie tego zagadnienia jest natychmiastowe w razie, kiedy jedna z liczb $\alpha$ albo $\beta$ równa się jedności albo zeru. Żeby wyznaczyć iloczyn (4) we wszystkich innych przypadkach zwróćmy się do tabelki następującej:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | |
| 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 2 |
| | 9 | 12 | 15 | 18 | 21 | 24 | 27 | 3 |
| | | 16 | 20 | 24 | 28 | 32 | 36 | 4 |
| | | | 25 | 30 | 35 | 40 | 45 | 5 |
| | | | | 36 | 42 | 48 | 54 | 6 |
| | | | | | 49 | 56 | 63 | 7 |
| | | | | | | 64 | 72 | 8 |
| | | | | | | | 81 | 9 |

Budowa górnego czyli pierwszego wiersza i budowa skrajnej kolumny po prawej stronie, czyli kolumny ostatniej, nie wymagają wyjaśnień. Uważajmy więc jakąkolwiek liczbę $s$ należącą do tabelki ale nie położoną ani w pierwszym wierszu ani w ostatniej kolumnie. Oznaczmy przez $x$ tę liczbę, która znajduje się w przedziałce wspólnej pierwszemu wierszowi i tej kolumnie $(K)$, w której znajduje się liczba $s$. Za wartość liczby $s$ przyjęliśmy przy budowie rozważanej tabelki sumę liczby $x$ i tej liczby, która w kolumnie $(K)$ znajduje się bezpośrednio nad liczbą $s$. Ułożyliśmy więc tabelkę, o którą chodzi, nie posługując się żadnym innym działaniem prócz dodawania.

Ze sposobu ułożenia powyższej tabelki i z definicyi mnożenia wynika, że zapomocą tabelki tej, będziemy mogli wyznaczyć iloczyn (4) w sposób następujący: zakładając, że oznaczenia tak są dobrane, żebyśmy mieli

$$\alpha \geqq \beta$$

wyznaczymy tę kolumnę $(K)$, u góry której znajduje się liczba $\alpha$; następnie wyznaczymy ten wiersz $(W)$, do którego należy, liczbę $\beta$ zawierająca, przedziałka ostatniej kolumny; iloczyn (4) równać się tedy będzie liczbie zawartej w przedziałce wspólnej kolumnie $(K)$ i wierszowi $(W)$.

Omówiona tabelka zwie się tabelką mnożenia.

Na podstawie poprzedzającego możemy uważać sprawę wyznaczenia wartości wyrażenia typu $(A)$ za załatwioną. Zanim jednak przejdziemy do wyznaczenia wyrażenia (1) w przypadkach ogólniejszych — uczynimy uwagę następującą: liczba dziesiątek wyrażenia typu $(A)$ nigdy nie przekracza liczby 8. Istotnie, możliwie największą wartość tego wyrażenia otrzymamy przyjmując

$$\alpha = 9,\ \beta = 9,\ \gamma = 8.$$

Otóż na podstawie tabelki mnożenia i teoryi dodawania mamy:

$$9 \,.\, 9 + 8 = 89,$$

czem stwierdzamy słuszność wysłowionej uwagi.

Przechodzimy teraz do sprawy wyznaczenia wyrażenia (1) w założeniu, że mnożnik $b$ iloczynu $a \,.\, b$ równa się liczbie jednocyfrowej $\beta$, a mnożna $a$ — jakiejkolwiek $n$-cyfrowej liczbie ($n > 1$). Dla skrócenia nadamy, w rozważanym przypadku, wyrażeniu (1) nazwę „wyrażenia typu ($B$) rzędu $n$“. Mamy tedy

$$b = \beta$$
$$a = \alpha' \,.\, 10 + \alpha$$

oznaczając przez $\alpha$ cyfrę jedności a przez $\alpha'$ liczbę dziesiątek liczby $a$. Na podstawie równości poprzedzających mamy:

$$a \,.\, b + \gamma = 10 \,.\, \alpha' \,.\, \beta + \alpha \,.\, \beta + \gamma$$

skąd

(5) $$a \,.\, b + \gamma = (\alpha' \,.\, \beta + \gamma') \,.\, 10 + \alpha'$$

oznaczając przez $\alpha'$ cyfrę jedności a przez $\gamma'$ liczbę dziesiątek wyrażenia

$$\alpha \,.\, \beta + \gamma,$$

które oczywiście jest wyrażeniem typu ($A$). Ponieważ, na podstawie uwagi uczynionej wyżej, mamy niezawodnie

$$\gamma' \leqq 8,$$

ponieważ dalej liczba cyfr liczby $a'$ równa się $n - 1$, przeto wnosimy z równości (5) co następuje: jeżeli w wyrażeniu (1) liczba $b$ jest liczbą jednocyfrową a liczba $a$ — $n$-cyfrową ($n > 1$), to, po wyznaczeniu wartości pewnego jednego wyrażenia typu ($A$), wyznaczymy cyfrę jedności $\alpha'$ wyrażenia (1) a wyznaczenie liczby dziesiątek tego wyrażenia sprowadzimy do wyznaczenia wartości wyrażenia

$$\alpha' \,.\, \beta + \gamma',$$

które jest typu ($B$) rzędu $n - 1$.

Opierając się na zasadzie indukcyi matematycznej stwierdzamy na postawie tego wniosku, że wyznaczenie wartości wyrażenia (1), w razie kiedy wyrażenie to jest typu ($B$), może być uskutecznione, wyznaczając wartości tylu pewnych wy-

rażeń typu $(A)$, ile wynosi rząd wyrażenia $(B)$. Zatem sprawa wyznaczenia wyrażenia typu $(B)$ a więc i sprawa wyznaczenia iloczynu, którego jeden czynnik przynajmniej jest liczbą jednocyfrową, mogą być uważane za załatwione.

Zwracamy się obecnie do iloczynu, którego jeden czynnik $a$ jest jakikolwiek a drugi, $b$, — liczbą, w której tylko cyfra jednostek rzędu najwyższego jest od zera odmienną Iloczyn taki nazwiemy iloczynem typu $(C)$. Mamy

$$b = \beta \,.\, 10^{p-1}$$

oznaczając przez $\beta$ cyfrę najwyższego rzędu liczby $b$ a przez $p$ liczbę cyfr tej liczby. Gdybyśmy mieli $p = 1$, to rozważany iloczyn należałby do omówionych już iloczynów typu $(B)$. Założymy więc, że mamy $p > 1$.

Oczywiście

$$a \,.\, b = (a \,.\, \beta) \,.\, 10^{p-1}.$$

Stwierdzamy więc, że iloczyn $a \,.\, b$ ma w rozważanym przypadku wartość następującą: cyfra rzędu $p - 1$ i cyfry rzędów niższych równają się zeru, każda zaś cyfra rzędu $i$, $i \geqq p$, równa się cyfrze rzędu $i - p + 1$ iloczynu $a \,.\, \beta$.

Zatem sprawa wyznaczenia iloczynu typu $(C)$ może być uważana za załatwioną.

Przechodzimy nareszcie do przypadku ogólnego, kiedy chodzi o wyznaczenie iloczynu, którego jeden czynnik $a$ jest jakikolwiek, a drugi $b$ jest jakąkolwiek liczbą $p$-cyfrową $(p > 1)$. Mamy tedy

$$b = b_p \, 10^{p-1} + b'$$

oznaczając przez $b_p$ cyfrę rzędu $p$ liczby $b$ a przez $b'$ pewną liczbę, której liczba cyfr nie przekracza liczby $p - 1$. Na podstawie znanego twierdzenia mamy:

$$a \,.\, b = a \,.\, b_p \,.\, 10^{p-1} + a \,.\, b'.$$

Zatem wyznaczenie iloczynu $a \,.\, b$ może być uskutecznione wyznaczając pewien iloczyn typu $(C)$, mianowicie iloczyn

$$a \,.\, b_p \,.\, 10^{p-1}$$

i dodając do tego iloczynu pewien iloczyn, mianowicie iloczyn $a \,.\, b'$, w który przechodzi iloczyn $a \,.\, b$, zastępując czynnik $b$ przez taki czynnik, którego liczba cyfr o jedność przynajmniej mniejszą jest od liczby cyfr czynnika $b$.

Wnosimy stąd, na podstawie zasady indukcyi matematycznej, że iloczyn, którego jeden z czynników jest liczbą $p$-cyfrową, $(p > 1)$, zdołamy zawsze wyznaczyć, wyznaczając sumę pewnej liczby składników, składników, których liczba nie będzie większą od liczby $p$ i z których każdy będzie pewnym iloczynem typu $(C)$.

Na podstawie poprzedzającego sprawa wyznaczenia iloczynu dwóch, a więc i jakiejkolwiek liczby czynników danych, może być uważana za załatwioną.

§ 38. **Dzielenie.** Ponieważ dzielenie prowadzi do oznaczonego wyniku tylko w przypadku, kiedy dzielnik jest od zera odmienny, przeto winniśmy i będziemy rozważać tylko przypadek, kiedy warunek ten jest spełniony.

**Tw. I.** Jeżeli oznaczymy przez $a$ dzielnę a przez $b$ dzielnik, to liczba jednostek jakiegokolwiek rzędu $p$ $(p > 1)$ całkowitej cześci ilorazu $q$ równa się całkowitej części ilorazu dzielenia liczby jednostek rzędu $p$ dzielnej $a$, przez liczbę $b$.

Żeby twierdzenie to uzasadnić oznaczamy przez $a'$ i $q'$ liczby jednostek rzędu $p$ odpowiednio dzielnej $a$ i całkowitej części ilorazu $q$.

Będziemy tedy mieli:

$$(1) \qquad \begin{cases} a = a' \,.\, 10^{p-1} + a'' \\ q = q' \,.\, 10^{p-1} + q'' \end{cases}$$

oznaczając przez $a''$ i $q''$ pewne liczby, sprawdzające nierówności następujące:

$$(2) \qquad \begin{cases} a'' < 10^{p-1} \\ q'' < 10^{p-1} \end{cases}$$

Oznaczając przez $r$ resztę podziału liczby $a$ przez liczbę $b$, mamy

$$a = b \,.\, q + r,$$

skąd

$$a = b \,.\, q' \,.\, 10^{p-1} + b \,.\, q'' + r. \tag{3}$$

Ze związków (1) i (2) mamy

$$a < (a' + 1)\, 10^{p-1},$$

przeto

$$b\, q' \,.\, 10^{p-1} < (a' + 1)\, 10^{p-1},$$

skąd

$$b\, q' < a' + 1$$

czyli

$$b\, q' \leqq a'. \tag{4}$$

Ponieważ

$$r < b,$$

przeto

$$b\, q'' + r < b\, (q'' + 1),$$

skąd

$$b\, q'' + r < b \,.\, 10^{p-1} \tag{5}$$

na podstawie jednej z nierówności (2).

Ze związków (3) i (5) mamy

$$a < b \,.\, (q' + 1)\, 10^{p-1},$$

z jednego zaś ze związków (1):

$$a' \,.\, 10^{p-1} \leqq a.$$

Zatem

$$a' < b' \,.\, (q' + 1). \tag{6}$$

Z nierówności (4) i (6) wynika, że $q'$ jest całkowitą częścią ilorazu podziału liczby $a'$ przez liczbę $b$, co było właśnie do okazania.

**Tw. II.** Zakładając, że dzielna $a$ nie jest mniejszą od dzielnika $b$, oznaczamy przez $m$ różnicę liczb cyfr dzielnej i dzielnika a przez $a'$ — liczbę jednostek rzędu $m + 1$ dzielnej. W takim razie liczba cyfr całkowitej części ilorazu równać się będzie liczbie $m$ w przypadku, kiedy zachodzi nierówność

$$a' < b, \tag{1}$$

a — liczbie $m+1$ w przypadku, kiedy mamy:

(2) $$a' \geqq b.$$

Żeby twierdzenie to uzasadnić zważmy, że liczba cyfr liczby $a'$ równa się oczywiście liczbie cyfr liczby $b$. Załóżmy na początek, że zachodzi nierówność (1). W takim razie będziemy mieli

(3) $$m \geqq 1$$

gdybyśmy bowiem mieli

$$m = 0$$

to mielibyśmy $a = a'$ i z nierówności (1) wynikałaby nierówność

$$a < b$$

co byłoby w sprzeczności z założeniem przyjętem w twierdzeniu.

Ze względu na nierówność (3) liczba $a$ posiadać będzie jednostki rzędu $m$ a liczba $a''$ tych jednostek będzie, na podstawie uwagi uczynionej co do liczby $a'$, liczbą $p+1$ cyfrową, oznaczając przez $p$ liczbę cyfr liczby $b$. Mamy zatem

(4) $$a'' > b.$$

A ponieważ liczba jednostek $q_m$ rzędu $m$ całkowitej części ilorazu $q$ liczby $a$ przez liczbę $b$ równa się (tw. poprzedzające) całkowitej części ilorazu liczby $a''$ przez liczbę $b$, przeto, na podstawie nierówności (4), liczba ta będzie od zera odmienną. Stwierdzamy więc, że liczba cyfr liczby $q$ nie będzie mniejszą od liczby $m$.

Ponieważ zaś mamy

$$a'' < (a'+1)\,10,$$

ponieważ nadto

$$a'+1 \leqq b$$

na podstawie nierówności (1), przeto mamy

$$a'' < b\,.\,10,$$

skąd wynika nierówność

$$q_m < 10.$$

Stwierdziliśmy więc, że liczba $q_m$ jednostek rzędu $m$ liczby $q$ jest liczbą jednocyfrową od zera odmienną. Zatem liczba cyfr liczby $q$ istotnie równa się w rozważanym przypadku dokładnie liczbie $m$.

Przechodząc do przypadku, w którym zachodzi związek (2), oznaczmy przez $q_{m+1}$ liczbę jednostek rzędu $m+1$ liczby $q$. Liczba $q_{m+1}$ (tw. poprzedzające) równać się będzie całkowitej części ilorazu liczby $a'$ przez liczbę $b$. Ze względu na związek (2) mamy:

$$q_{m+1} \geqq 1. \tag{5}$$

Ponieważ, na podstawie uwagi uczynionej na początku dowodu, liczba cyfr liczby $a'$ równa się liczbie cyfr liczby $b$, przeto liczba cyfr iloczynu $b \,.\, 10$ większą będzie od liczby cyfr liczby $a'$. Zatem

$$a' < 10 \,.\, b.$$

Stąd zaś wynika

$$q_{m+1} < 10 \tag{6}$$

Z nierówności (5) i (6) wypływa, że liczba $q_{m+1}$ jest liczbą jednocyfrową od zera odmienną. Przeto liczba cyfr liczby $q$ równa się dokładnie liczbie $m+1$. Uzasadniliśmy więc w zupełności twierdzenie, o które chodziło.

Przechodząc do sprawy wyznaczenia całkowitej części ilorazu $q$ przy danych dzielnej $a$ i dzielniku $b$, zwróćmy się najpierw do przypadku szczególnego, kiedy liczba $q$ jest liczbą jednocyfrową; ze względu na twierdzenie poprzedzające będziemy zawsze mogli stwierdzić, czy przypadek ten istotnie zachodzi.

Wiedząc, że liczba $q$ jest liczbą jednocyfrową, możemy, celem wyznaczenia tej liczby, wyznaczyć w ciągu iloczynów następujących:

$$b \,.\, 9;\ b \,.\, 8;\ b \,.\, 7;\ b \,.\, 6;\ b \,.\, 5;\ b \,.\, 4;\ b \,.\, 3;\ b \,.\, 2;\ b \,.\, 1;\ b \,.\, 0$$

pierwszy iloczyn nie przekraczający dzielnej $a$. Oznaczając iloczyn ten przez $b \,.\, i$ będziemy mieli

$$q = i,$$

albowiem ta wartość liczby $q$ sprawdzać będzie związki następujące:

$$a \geqq b \,.\, q$$
$$a < b \,.\, (q + 1),$$

które właśnie stanowią warunki konieczne i wystarczające na to, żeby liczba $q$ równała się całkowitej części ilorazu liczby $a$ przez liczbę $b$. Metoda ta wymaga oczywiście wyznaczenia

$$9 - q + 1$$

pierwszych iloczynów ciągu (7).

Jeżeli dzielnik jest liczbą jednocyfrową to stosujemy w praktyce powyższą metodę bez żadnej zmiany i dochodzimy szybko do wyniku dzięki tej okoliczności, iż mamy w pamięci tabelkę mnożenia. Jeżeli zaś liczba $b$ nie jest liczbą jednocyfrową, to wprowadzamy do oznaczonej metody pewne uzupełnienie, które często upraszcza sprawę wyznaczenia liczby $q$ i które wysnujemy z twierdzenia następującego.

**Tw. III.** Oznaczmy przez $b'$ liczbę jednostek rzędu $m$ $(m > 1)$ dzielnej $b$ zakładając jednocześnie, że liczba $m$ nie przekracza liczby cyfr liczby $b$. W takim razie całkowita część $q$ ilorazu podziału dzielnej $a$ przez dziejnik $b$ nie będzie większą od całkowitej części ilorazu liczby $a'$ jednostek rzędu $m$ liczby $a$, przez liczbę $b'$.

Żeby twierdzenie to uzasadnić zważmy, że mamy

$$a = a' \,.\, 10^{m-1} + a''$$

oznaczając przez $a''$ liczbę sprawdzającą nierówność następującą

$$a'' < 10^{m-1}.$$

Mamy więc:

$$a < (a' + 1)\, 10^{m-1}.$$

Na podstawie nierówności tej i nierówności

$$b \,.\, q \leqq a,$$

mamy

$$b \,.\, q < (a' + 1)\, 10^{m-1},$$

a ponieważ

$$b \geqq b' \,.\, 10^{m-1},$$

przeto

$$b' \,.\, q \,.\, 10^{m-1} < (a' + 1)\, 10^{m-1},$$

skąd

$$b' \,.\, q < a' + 1$$

czyli

$$b' \,.\, q \leqq a'.$$

Z nierówności tej wynika natychmiast twierdzenie, o dowód którego chodziło.

Zachowując oznaczenia twierdzenia poprzedzającego, oznaczmy jeszcze przez $Q$ całkowitą część ilorazu liczby $a'$ przez liczbę $b'$ i załóżmy, że liczba $q$ jest liczbą jednocyfrową. Gdybyśmy byli w możności szybko wyznaczyć liczbę $Q$ i gdyby liczba $Q$ wypadła mniejszą od liczby $9$, to, stosując w zasadzie wyżej wyłożoną metodę do wyznaczenia liczby $q$, moglibyśmy nie wyznaczać

$$9 - Q$$

pierwszych iloczynów ciągu (7), albowiem, na podstawie twierdzenia poprzedzającego, mielibyśmy pewność, że pierwszy liczbę $a$ nie przekraczający iloczyn ciągu (7) nie mógłby poprzedzać, w tym ciągu, iloczynu $b \,.\, Q$.

Liczbę $Q$ możemy zawsze łatwo wyznaczyć przyjmując za $b'$ cyfrę jednostek najwyższego rzędu liczby $b$. Dlatego też w praktyce wyznaczamy zwykle, przy takim wyborze liczby $b'$, liczbę $Q$ i korzystamy z tej liczby w sposób wytłómaczony przed chwilą. Na tem właśnie polega to uzupełnienie wyżej omówionej metody dzielenia, które mieliśmy na względzie.

Przy większej wprawie i w razie kiedy całkowita część $q$ ilorazu jest liczbą jednocyfrową, spostrzegamy wartość liczby $q$

prawie bezpośrednio, nie wykonywając w rzeczywistości wszystkich czynności przepisanych przez metodę wyłożoną przed chwilą.

Z tej przyczyny ważną jest rzeczą, ze stanowiska techniki rachunkowej, mieć metodę możliwie bezpośrednią do wyznaczenia reszty przy danych dzielnej, dzielniku i całkowitej części ilorazu w razie, kiedy ta ostatnia jest liczbą jednocyfrową.

Zagadnienie poprzedzające jest oczywiście przypadkiem szczególnym zagadnienia następującego: oznaczając przez $a$, $b$, $q$ i $\gamma$ cztery dane liczby, z których — $q$ i $\gamma$ są liczbami jednocyfrowemi, wyznaczyć wartość wyrażenia następującego

$$a - (b \cdot q + \gamma) \tag{1}$$

w sposób możliwie szybko prowadzący do celu.

Celem uproszczenia mowy i pisma nadamy wyrażeniu (1) miano wyrażenia typu $(A)$ w przypadku szczególnym, kiedy liczba $b$ i wartość samego wyrażenia (1) są liczbami jednocyfrowemi. Przy pewnej wprawie zdołamy zawsze, wykonywając rachunek pamięciowy, zdecydować czy wyrażenie (1) jest wyrażeniem typu $(A)$ i wyznaczyć, w razie gdyby okoliczność ta zachodziła i gdyby rozważane wyrażenie nie było pozbawione sensu, wartość tego wyrażenia. Załóżmy więc, że wyrażenie (1) nie jest typu $(A)$. Oznaczając tedy przez $n$ liczbę cyfr liczby $a$ będziemy mieli

$$n > 1.$$

Oznaczmy przez $\alpha$ i $\beta$ cyfry jedności a przez $a'$ i $b'$ liczby dziesiątek liczb $a$ i $b$. Mamy:

$$a = 10 \cdot a' + \alpha$$

$$b = 10 \cdot b' + \beta.$$

Zatem

$$a - (b \cdot q + \gamma) = \{10 \cdot a' + 10 \cdot \gamma' + \alpha\} - \{10 \cdot (b \cdot q' + \gamma') + \beta q + \gamma\} \tag{2}$$

oznaczając przez $\gamma'$ liczbę, którą określimy bliżej później.

Ponieważ mamy

$$\beta \leqq 9, \quad q \leqq 9 \quad \text{i} \quad \gamma \leqq 9,$$

przeto

$$\beta . q + \gamma \leqq 90 \tag{3}$$

Żeby określić liczbę $\gamma'$, oznaczmy przez $\xi$ i $\eta$ cyfrę jedności i liczbę dziesiątek wyrażenia

$$\beta . q + \gamma.$$

Gdybyśmy mieli

$$\xi \leqq \alpha$$

to przyjęlibyśmy

$$\gamma' = \eta. \tag{4}$$

Gdyby zaś zachodziła nierówność

$$\xi > \alpha \tag{5}$$

to przyjęlibyśmy

$$\gamma' = \eta + 1. \tag{6}$$

Powiadam, że w obu przypadkach zachodzić będzie nierówność następująca:

$$\gamma' \leqq 9. \tag{7}$$

Nierówność ta wynika bezpośrednio z nierówności (3) w razie, kiedy liczba $\gamma'$ ma wartość określoną równością (4). Jeżeli zaś mamy na $\gamma'$ wartość (6), to, ze względu na związki (3) i (5), mamy tedy

$$\eta \leqq 8.$$

Zatem i w tym przypadku liczba $\gamma'$ sprawdzać będzie nierówność (7).

Łatwo stwierdzimy, że, przy przyjętem określeniu liczby $\gamma'$, różnica

$$(10 . \gamma' + \alpha) - (\beta . q + \gamma) \tag{8}$$

nie będzie pozbawiona sensu i równać się będzie liczbie jednocyfrowej; jednem słowem różnica (8) będzie wyrażeniem typu $(A)$.

Ponieważ różnica (8) nie jest pozbawiona sensu, przeto możemy oczywiście nadać równości (2) kształt następujący:

$$(9) \qquad a-(b\,.\,q+\gamma)=$$
$$=[\{(10\,\gamma'+\alpha)-(\beta\,.\,q+\gamma)\}+10\,.\,a']-10\,(b'\,.\,q+\gamma').$$

Ponieważ dalej wyrażenie (8) przedstawia oczywiście liczbę jednocyfrową, przeto zachodzić musi związek następujący

$$a'\geqq b'\,.\,q+\gamma'$$

bo w razie przeciwnym różnica (9), a więc i wyrażenie (1), nie miałyby sensu.

Możemy więc nadać równości (9) kształt następujący:

$$a-(b\,.\,q+\gamma)=10\,.\,\{a'-(b'\,.\,q+\gamma')\}+$$
$$+\{10\,.\,\gamma'+\alpha)-(\beta\,.\,q+\gamma)\}.$$

Równość ta opiewa, że cyfra jedności wyrażenia (1) równa się wyrażeniu (8), a liczba dziesiątek — wyrażeniu

$$(10) \qquad a'-(b'\,.\,q+\gamma').$$

Ponieważ, na podstawie związku (7), wyrażenie (10) jest oczywiście tego samego typu, co wyrażenie (1), ponieważ dalej liczba cyfr liczby $a'$ jest o jedną jedność mniejszą od liczby cyfr liczby $a$, przeto przez wyznaczenie jednego wyrażenia typu $(A)$ sprowadzamy sprawę wyznaczenia wyrażenia (1) do sprawy wyznaczenia innego wyrażenia tegoż typu, ale z tem udogodnieniem, że liczba cyfr odjemnej, w nowem wyrażeniu, będzie o jedność mniejszą niż liczba cyfr odjemnej w wyrażeniu pierwotnem.

Z tego zaś wyprowadzamy łatwo wniosek następujący: jeżeli oznaczymy przez $n$ liczbę cyfr liczby $a$, to wartość wyrażenia (1) zdołamy wyznaczyć wyznaczając wartości $n—1$ albo najwyżej $n$ wyrażeń typu $(A)$.

Ze stanowiska techniki rachunku ważną jest okoliczność następująca: gdybyśmy przyjęli za całkowitą część $q$ ilorazu pewnej liczby $a$ przez pewną liczbę $b$ wartość jednocyfrową błędną, to błąd uwidoczniłby się przy stosowaniu, do wyzna-

czenia reszty, podanej przed chwilą metody. Istotnie, gdybyśmy przyjęli na $q$ wartość zbyt małą, to otrzymalibyśmy na wyrażenie

$$a - b \cdot q$$

wartość nie mniejszą od dzielnika $b$; gdybyśmy zaś przyjęli na $q$ wartość za wielką, to, oznaczając przez $n$ liczbę cyfr liczby $a$, trafilibyśmy, przystępując do wykonania $(n-1)$-ej albo $n$-tej czynności, przypisanej rozważaną metodą, na odejmowanie niewykonalne.

Prawidło dzielenia, w przypadku ogólnym, kiedy liczba cyfr całkowitej części ilorazu większą jest od jedności, opiera się na twierdzeniu następującem.

**Tw. IV.** Oznaczmy przez $q$ i $r$ całkowitą część ilorazu i resztę podziału pewnej liczby całkowitej $a$ przez pewną liczbę całkowitą $b$. Oznaczmy dalej, zakładając, że liczba cyfr liczby $q$ większą jest od jedności, przez $r'$ — resztę podziału liczby dziesiątków $a'$ dzielnej $a$ przez liczbę $b$, a przez $\alpha$ i $\gamma$ — cyfry jedności odpowiednio liczb $a$ i $q$. W takim razie liczba $\gamma$ równać się będzie całkowitej części ilorazu a liczba $r$ — reszcie podziału, przez liczbę $b$, liczby

$$10 \cdot r' + \alpha,$$

a więc liczby, której liczba dziesiątek równa się liczbie $r'$ a cyfra jedności — liczbie $\alpha$.

Dowód. Oznaczmy przez $q'$ liczbę dziesiątek liczby $q$. Będziemy tedy mieli (tw. I):

$$a' = b \cdot q' + r'. \tag{1}$$

Oznaczmy następnie przez $\gamma_1$ i $r_1$ całkowitą część ilorazu i resztę podziału liczby

$$10 \cdot r' + \alpha$$

przez liczbę $b$. W takim razie zachodzić będą związki następujące:

$$10 \cdot r' + \alpha = b \cdot \gamma_1 + r_1 \tag{2}$$

$$r_1 < b. \tag{3}$$

Z równości (1) mamy:

$$10 \cdot a' = 10\, q' \cdot b + 10 \cdot r'$$

skąd

$$10 \cdot a' + \alpha = 10 \cdot q' \cdot b + 10 \cdot r' + \alpha$$

czyli

$$a = 10 \cdot q' \cdot b + 10 \cdot r' + \alpha,$$

Ze względu na (2) mamy stąd:

$$a = 10 \cdot q' \cdot b + b \cdot \gamma_1 + r_1$$

czyli

$$a = (10 \cdot q' + \gamma_1) \cdot b + r_1 . \tag{4}$$

Na podstawie związków (3) i (4) liczby

$$10 \cdot q' + \gamma_1 \quad \text{i} \quad r_1$$

równają się odpowiednio całkowitej części ilorazu i reszcie podziału liczby $a$ przez liczbę $b$.

W innych wyrazach:

$$q = 10 \cdot q' + \gamma_1 \tag{5}$$

$$r = r_1 . \tag{6}$$

A ponieważ liczba $q'$ jest liczbą dziesiątek liczby $q$, przeto liczba $\gamma_1$ równa się cyfrze jedności liczby $q$, czyli

$$\gamma = \gamma_1 . \tag{7}$$

Równości (6) i (7) wyrażają właśnie twierdzenie, o dowód którego chodziło.

Powiadam, że na dzielenie mamy prawidło następujące: żeby wyznaczyć całkowitą część $q$ ilorazu i odnośną resztę przy danych dzielnej $a$ i dzielniku $b$ $(b > 0)$ należy przedewszystkiem wyznaczyć, na podstawie tw. II, liczbę cyfr $p$ całkowitej części ilorazu; jeżeli wypadnie $p = 1$, to dzielenie wykonywamy w sposób już omówiony wyżej; jeżeli zaś wypadnie $p > 1$ to wyznaczamy kolejno cyfry rzędów

$$p,\ p - 1,\ p - 2, \ldots$$

liczby $q$ w postaci całkowitych części ilorazów przy pewnych dzieleniach; za każdorazowy dzielnik przyjmujemy liczbę $b$, a więc dzielnik dzielenia, o wykonanie którego właściwie chodzi, dzielne zaś określamy w sposób następujący: przy pierwszem dzieleniu przyjmujemy za dzielnę — liczbę jednostek rzędu $p$ liczby $a$, a przy każdem dalszem — przyjmujemy za dzielnę tę liczbę, której liczba dziesiątek równa się reszcie ostatniego już wykonanego dzielenia, a cyfra jedności — tej cyfrze liczby $a$, której rząd równa się rzędowi mającej być przez rozważane dzielenie wyznaczonej cyfrze liczby $q$. Reszta dzielenia wykonanego przy wyznaczeniu cyfry jedności liczby $q$ równa się wtedy reszcie podziału liczby $a$ przez liczbę $b$.

Istotnie, gdyby prawidło poprzedzające uzasadnionem było w przypadku, w którymby liczba $p$ nie była większą od pewnej liczby $k$, $(k \geqq 1)$, to, opierając się na tw. I, łatwo dowiedlibyśmy, że prawidło to zastosowane do przypadku, w którym mielibyśmy $p = k + 1$, doprowadziłoby do poprawnego wyznaczenia cyfr liczby dziesiątek żądanego ilorazu $q$; nadto, reszta dzielenia, dostarczającego *cyfrę* dziesiątek liczby $q$, równałaby się reszcie podziału *liczby* dziesiątek liczby $a$ przez liczbę $b$. Zatem, na podstawie tw. IV, omawiane prawidłowo dostarczyłoby w rozważanym przypadku także poprawne wartości na cyfrę jedności liczby $q$ i na resztę podziału liczby $a$ przez liczbę $b$. Gdyby więc roztrząsane prawidło poprawnem było w przypadku, gdy mamy $p \leqq k$, to prawidło to byłoby poprawnem i w tym razie, w którym mielibyśmy $p = k + 1$. Ponieważ zaś prawidło, o które chodzi, oczywiście poprawnem jest gdy mamy $p = 1$, przeto prawidło to uzasadnionem jest we wszystkich przypadkach.

Ponieważ, przy wykonaniu dzielenia, łatwo wkraść się może błąd rachunkowy, przeto celem upewnienia się, że błędu niema, mnożymy dzielnik przez uzyskaną wartość całkowitej cześci ilorazu i sprawdzamy, czy wynik dodania do tego iloczynu znalezionej wartości na resztę równa się, jak być powinno, dzielnej.

Na tem właśnie polega tak zwana próba dzielenia.

§ 39. Każde z działań zasadniczych wykonywamy na piśmie trzymając się pewnych form, które wyrobiły się wiekową praktyką i których znaczenie polega na tem, iż przy zachowaniu tychże jesteśmy mniej narażeni na błędy rachunkowe aniżeli w razie przeciwnym. Ponieważ wspomniane formy niewątpliwie są czytelnikowi doskonale znane, przeto pomijamy omówienie tych form.

## IX. Podstawowe twierdzenia o podzielności. Pewne cechy podzielności.

§ 40. Mieliśmy już sposobność powiedzieć (§ 25), że jeżeli do dwóch danych liczb całkowitych $a$ i $b$ można dobrać trzecią liczbę całkowitą $m$, sprawdzającą równość

$$a = m \,.\, b,$$

to okoliczność tę wysławiamy przez jedno z orzeczeń następujących: liczba $a$ podzielną jest przez liczbę $b$; liczba $a$ jest wielokrotnością liczby $b$; liczba $b$ jest podwielokrotnością liczby $a$. Rozważaną okoliczność wysławiamy także niekiedy w postaci następującej: liczba $b$ jest dzielnikiem liczby $a$.

**Tw. I.** Jeżeli każda z dwóch liczb $a$ i $b$ podzielną jest pewną trzecią liczbę $c$, to suma i różnica tych liczb także podzielne są przez liczbę $c$.

Dowód. Mamy

$$a = p \,.\, c$$
$$b = q \,.\, c$$

oznaczając przez $p$ i $q$ pewne liczby całkowite. Z równości poprzedzających mamy:

$$a + b = (p + q) \,.\, c$$

oraz

$$a - b = (p - q) \,.\, c,$$

zakładając, że oznaczenia tak są przyjęte, żebyśmy mieli

$$a \geqq b.$$

Uzyskane równości wyrażają właśnie twierdzenie, o które chodziło.

**Tw. II.** Jeżeli jeden z czynników jakiegokolwiek iloczynu $p$, liczb całkowitych, podzielny jest przez pewną liczbę $c$, to uważany iloczyn także podzielny jest przez liczbę $c$.

Dowód. Oznaczmy przez $a$ ten czynnik iloczynu $p$, który podzielny jest przez liczbę $c$ — a przez $b$ iloczyn wszystkich innych czynników albo, gdyby iloczyn $p$ był iloczynem dwóch tylko czynników — drugi czynnik. Mamy tedy

$$p = a \,.\, b$$

oraz

$$a = q \,.\, c$$

oznaczając przez $q$ pewną liczbę całkowitą. Z równości poprzedzających mamy:

$$p = (q \,.\, b) \,.\, c.$$

Równość ta oczywiście wyraża twierdzenie, o które chodziło.

**Tw. III.** Jeżeli dwie liczby całkowite różnią się od siebie tylko o wielokrotność pewnej liczby całkowitej $c$ od zera odmiennej, to reszty podziału tych liczb przez liczbę $c$ są sobie równe.

Dowód. Uważajmy dwie liczby całkowite $a$ i $b$ znajdujące się z liczbą $c$ w związku następującym:

$$a = b + m\,c \tag{1}$$

oznaczając przez $m$ pewną liczbę całkowitą.

Mamy

$$b = q \,.\, c + r \tag{2}$$

i

$$r < c \tag{3}$$

oznaczające przez $q$ całkowitą część ilorazu a przez $r$ resztę podziału liczby $b$ przez liczbę $c$. Z równości (1) i (2) mamy:

$$a = (m + q) \,.\, c + r$$

skąd, opierając się na nierówności (3), wnosimy, że reszta podziału liczby $a$ przez liczbę $c$ równa się reszcie $r$ podziału liczby $b$ przez liczbę $c$, co było do okazania.

§ 41. Przy pewnych szczególnych wartościach dzielnika reszta dzielenia wyznaczoną być może szybciej aniżeli przez wykonanie samego dzielenia.

W takich przypadkach mamy oczywiście (§ 25, tw. IV), do stwierdzenia podzielności dzielnej przez rozważany dzielnik, kryteryum, którego zastosowanie nie wymaga wykonania dzielenia.

Kryteryum tego rodzaju zwie się cechą podzielności przez odnośny dzielnik.

Ustęp ten poświęcamy omówieniu najważniejszych ze stanowiska techniki rachunkowej przypadków, w których reszta podziału liczby całkowitej przez pewną liczbę może być wyznaczona bez wykonywania odnośnego dzielenia.

Dzielnik postaci $10^p$ $(p \geqq 1)$. Ponieważ wszelka liczba całkowita $a$, której liczba cyfr $n$ sprawdza nierówność

$$n \leqq p$$

mniejszą jest od liczby $10^p$, przeto reszta podziału takiej liczby przez $10^p$ równa się samej tej liczbie.

Gdybyśmy zaś mieli

$$n > p$$

to, z definicyi numeracyi dziesiętnej wynika natychmiast, że reszta $r$, podziału liczby $a$ przez $10^p$, równałaby się liczbie, którą przedstawia układ tylu najniższych rzędów cyfr liczby $a$, ile wynosi liczba $p$; właściwie tak jest tylko pod warunkiem, że cyfra rzędu $p$ liczby $a$ zerem nie jest; żeby ograniczenie to usunąć, wprowadzamy umowę następującą: Mając na pewną liczbę $L$ wzór następujący:

$$L = \sum_{i=1}^{m} a_i \cdot 10^{i-1}$$

gdzie każdy z symbolów

(1) $$a_1, \quad a_2, \quad a_m, \ldots$$

oznacza jedną z cyfr numeracyi dziesiętnej, uważać będziemy w *każdym* razie symbol, który, gdybyśmy mieli

$$a_m \neq 0,$$

byłby symbolem specyficznym liczby $L$, za symbol oznaczający tę liczbę, nazywając jednocześnie ogólnie cyfrę $a_i$ cyfrą rzędu $i$ liczby $L$. Umowa poprzedzająca nie może stać się powodem żadnego nieporozumienia, albowiem w każdym przypadku szczególnym łatwo będzie spostrzedz, czy wyrażenie „cyfra pewnej liczby“ użyte jest w znaczenie pierwotnem, czy też w znaczeniu szerszem, wprowadzonem obecnie.

Na podstawie tej umowy możemy oczywiście przedstawić każdą $k$-cyfrową liczbę $r$ w postaci liczby $p$-cyfrowej ($p > k$), przyjmując oczywiście wartość zero na każdą cyfrę rzędu wyższego od $k$.

Powracając do właściwego przedmiotu naszych obecnych rozważań, stwierdzamy natychmiast, że cecha podzielności liczby całkowitej przez dzielnik postaci $10^p$ polega na tem, żeby każda cyfra tej liczby rzędu niższego od $p+1$ równała się zeru.

Dzielnik postaci $2^p$ albo $5^p$ ($p \geqq 1$). Oznaczmy przez $a$ jakąkolwiek liczbę $n$-cyfrową ($n > p$), przez $a'$ — liczbę jednostek rzędu $p+1$ liczby $a$, a przez $r$ — liczbę, którą przedstawia układ $p$ najniższych rzędów cyfr liczby $a$. Mamy tedy

$$a = a' \,.\, 10^p + r.$$

Ponieważ

$$10^p = 2^p \,.\, 5^p,$$

przeto iloczyn (tw. II) $a' \,.\, 10^p$ jest wielokrotnością każdej z liczb $2^p$ i $5^p$. Zatem (tw. III) reszta podziału liczby $a$ przez $2^p$ albo przez $5^p$ równa się reszcie podziału liczby $r$ przez rozważany dzielnik.

Z tego wynika, że cecha podzielności liczby $n$-cyfrowej przez dzielnik równający się jednej z liczb $2^p$ albo $5^p$ ($p \geqq 1$) polega na podzielności przez rozważany dzielnik liczby, którą przedstawia układ $p$ najniższego rzędu cyfr liczby $a$.

Stąd wnosimy w szczególności:

1°. Żeby liczba całkowita podzielną była przez liczbę 5 koniecznem jest i wystarczającem, żeby cyfra jedności tej liczby była cyfrą 0 albo cyfrą 5.

2°. Żeby liczba całkowita była parzystą, to znaczy podzielną przez 2, koniecznem jest i wystarczającem, żeby cyfra jedności tej liczby była parzystą.

Dzielnik postaci 3 albo 9. Reszta podziału liczby postaci $10^p$ przez 9 równa się jedności. Istotnie okoliczność ta zachodzi oczywiście w razie, kiedy mamy $p = 0$. Załóżmy chwilowo, że ta sama okoliczność zachodzi także w przypadku, kiedy mamy $p = k$. W takim razie mielibyśmy

$$10^k = b \,.\, 9 + 1,$$

oznaczając przez $b$ pewną liczbę całkowitą. Z równości poprzedzającej wynika, że:

$$10^{k+1} = b \,.\, 10 \,.\, 9 + 10$$

czyli

$$10^{k+1} = b \,.\, 10 \,.\, 9 + 9 + 1,$$

skąd

$$10^{k+1} = (b \,.\, 10 + 1) \,.\, 9 + 1.$$

Przeto, na podstawie zasady indukcyi matematycznej, reszta podziału jakiejkolwiek potęgi liczby 10 przez liczbę 9 równa się rzeczywiście jedności [1]).

Uważajmy teraz jakąkolwiek $n$ cyfrową liczbę $a$ $(n > 1)$. Mamy

$$(1) \qquad a = \sum_{i=1}^{n} \alpha_i \, 10^{i-1}$$

oznaczając ogólnie przez $\alpha_i$ cyfrę rzędu $i$ liczby $a$.

---

[1]) Łatwo doszlibyśmy do tego samego wyniku wychodząc ze znanej równości:

$$a^p - b^p = (a - b) \sum_{i=0}^{p-1} a^{p-1-i} \, b^i \,;$$

należałoby tylko w równości tej przyjąć $a = 10$ oraz $b = 1$.

Na podstawie wyniku uzyskanego przed chwilą mamy:

$$10^{i-1} = b_i \,.\, 9 + 1 \qquad (2)$$

oznaczając przez $b_i$ pewną liczbę całkowitą.

Z równości (1) i (2) mamy:

$$a = 9 \,.\, \sum_{i=2}^{n} a_i \,.\, b_i + \sum_{i=1}^{n} a_i .$$

Zatem (tw. III) reszta podziału liczby $a$ przez którąkolwiek z liczb $3$ albo $9$ równa się reszcie podziału przez rozważany dzielnik sumy cyfr liczby $a$.

Ponieważ suma cyfr liczby $n$-cyfrowej $a$ $(n > 1)$ oczywiście zawsze mniejszą jest od tej liczby, przeto stosując należytą ilość razy twierdzenie poprzedzające zdołamy zawsze wyznaczyć liczbę jednocyfrową $r$, której reszta podziału przez którąkolwiek z liczb 3 albo 9 równać się będzie reszcie podziału liczby $a$ przez rozważany dzielnik; w przeciwnym bowiem razie liczba nierównych sobie liczb całkowitych od liczby $a$ mniejszych i stanowiących ciąg, w którym każda nowa liczba równałaby się sumie cyfr liczby poprzedzającej, byłaby nieskończonością — a wiemy przecież, że liczba liczb całkowitych od liczby $a$ mniejszych jest skończoną i równa się samej liczbie $a$. Z drugiej strony liczba $r$ zerem być nie może. Ponieważ zaś pomiędzy liczbami jednocyfrowemi, od zera odmiennemi, prócz liczb 3 i 9 nie istnieje żadna, która podzielną byłaby przez 3, ponieważ nadto pomiędzy rzeczonemi liczbami liczba 9 jest jedyną liczbą podzielną przez 9, przeto: żeby liczba $a$ podzielną była przez liczbę 3 koniecznem jest i wystarczającem, żeby określona przed chwilą liczba $r$ równała się jednej z liczb 3 albo 9; żeby zaś liczba $a$ podzielną była przez 9, koniecznem jest i wystarczającem, żeby liczba $r$ równała się dziewięciu. Możemy oczywiście dodać, że, gdyby na liczbę $r$ wypadła wartość od liczby 9 mniejsza, to liczba ta równałaby się reszcie podziału liczby $a$ przez 9.

Dzielnik 11. Jakąkolwiek liczbę całkowitą oznaczylibyśmy przez $p$, mamy

(1) $$10^{2p} = b \,.\, 11 + 1$$

oznaczając przez $b$ pewną liczbę całkowitą.

Czyli: reszta podziału parzystej potęgi liczby *10* przez dzielnik 11 równa się jedności. Twierdzenie to zachodzi oczywiście w przypadku kiedy mamy

$$p = 0.$$

Gdybyśmy zaś mieli

$$10^{2k} = m \,.\, 11 + 1$$

oznaczając przez $k$ pewną liczbę całkowitą, to mielibyśmy

$$10^{2(k+1)} = m \,.\, 100 \,.\, 11 + 100$$

a ponieważ

$$100 = 9 \,.\, 11 + 1,$$

przeto

$$10^{2(k+1)} = (m \,.\, 100 + 9) \,.\, 11 + 1.$$

Wnosimy stąd, że związek (1) zachodzi rzeczywiście przy każdej wartości liczby całkowitej $p$.

Z równości (1) mamy:

$$10^{2p+1} = b \,.\, 10 \,.\, 11 + 10 = b \,.\, 10 \,.\, 11 + 11 - 1$$

czyli

(2) $$10^{2p+1} = (b \,.\, 10 + 1) \,.\, 11 - 1.$$

A ponieważ wszelką liczbę nieparzystą możemy przedstawić w postaci:

$$2p + 1$$

albowiem reszta podziału liczby nieparzystej przez 2 oczywiście równa się jedności (bo jedność jest jedyną liczbą od zera odmienną i mniejszą od liczby 2), przeto związek (2) wyraża twierdzenie następujące: wszelka nieparzysta potęga liczby *10* może być uważaną za resztę odjęcia jedności od pewnej wielokrotności liczby *11*.

Uważajmy jakąkolwiek $n$-cyfrową ($n > 1$) liczbę $a$. Mamy

$$a = \sum_{i=1}^{n} \alpha_i \, 10^{i-1},$$

oznaczając ogólnie przez $\alpha_i$ cyfrę jednostek rzędu $i$ liczby $a$.

Oznaczmy przez $q$ całkowitą część ilorazu liczby $n$ przez dzielnik 2 a przez $\varepsilon$ odnośną resztę i przyjmijmy

$$p = q - (1 - \varepsilon)$$

Będziemy mieli tedy

$$a = \sum_{t=0}^{p} \alpha_{2t+1} \, . \, 10^{2t} + \sum_{s=1}^{q} \alpha_{2s} \, . \, 10^{2s-1}. \tag{3}$$

Na podstawie twierdzeń polegających na związkach (1) i (2) możemy przyjąć:

$$10^{2t} = b_t \, . \, 11 + 1,$$
$$10^{2s-1} = c_s \, . \, 11 - 1,$$

oznaczając przez $b_t$ i $c_s$ pewne liczby całkowite. Na podstawie wzorów poprzedzających wyprowadzamy z równości (3) równość następującą:

$$a = 11 \, . \, h + \sum_{t=0}^{p} \alpha_{2t+1} - \sum_{s=1}^{q} \alpha_{2s}, \tag{4}$$

przyjmując:

$$h = \sum_{t=0}^{p} \alpha_{2t+1} \, . \, b_t + \sum_{s=1}^{q} \alpha_{2s} \, . \, c_s \, .$$

Oznaczmy przez $d$ różnicę sum następujących

$$\sum_{t=0}^{p} \alpha_{2t+1} \text{ i } \sum_{s=1}^{q} \alpha_{2s}. \tag{5}$$

Będziemy tedy mieli

$$a = 11 \, . \, h + d \tag{6}$$

albo

$$a = 11 \cdot h - d \tag{7}$$

zależnie od względnego położenia wartości sum (5) w ciągu naturalnym liczb całkowitych.

Opierając się na tw. I stwierdzimy natychmiast, że w obu przypadkach podzielność liczby $d$ przez liczbę $11$ jest warunkiem podzielności liczby $a$ przez ten dzielnik. Jeżeli liczba $d$ przez $11$ podzielną nie jest, to, w razie związku (6), reszta podziału liczby $a$ przez $11$ równa się (tw. III) reszcie podziału liczby $d$ przez ten dzielnik. Zwróćmy się nareszcie do przypadku, kiedy zachodzi związek (7) i kiedy jednocześnie liczba $d$ przez liczbę $11$ podzielną nie jest. Mamy tedy

$$d = k \cdot 11 + r \tag{8}$$

$$0 < r < 11, \tag{9}$$

oznaczając przez $k$ i $r$ całkowitą część ilorazu i resztę podziału liczby $d$ przez $11$.

Z równości (7) i (8) oraz na podstawie jednej z nierówności (9) mamy

$$a = (h - k - 1) \cdot 11 + (11 - r), \tag{10}$$

a ponieważ

$$11 - r < 11$$

na podstawie jednej z nierówności (9), przeto równość (10) wyraża, że reszta podziału liczby $a$ przez liczbę $11$ równa się różnicy

$$11 - r$$

czyli uzupełnieniu liczby $r$ do jedenastu.

Uzyskane wyniki możemy wysłowić w sposób następujący: cecha podzielności liczby wielocyfrowej $a$ przez dzielnik $11$ polega na podzielności przez ten dzielnik różnicy $d$ sumy cyfr rzędów nieparzystych i sumy cyfr rzędów parzystych rozważanej liczby; jeżeli liczba $d$ przez $11$ nie jest podzielną, to reszta podziału liczby $a$ przez dzielnik $11$ równa się albo reszcie podziału liczby $d$ przez ten dzielnik albo

uzupełnieniu do jedenastu tej reszty; pierwszy z tych dwóch przypadków zachodzi, kiedy suma cyfr rzędów nieparzystych liczby $a$ większą jest od sumy cyfr rzędów parzystych, drugi — w razie przeciwnym.

§ 42. Czytelnik zauważył niezawodnie zasadniczą różnicę pomiędzy twierdzeniami z § 40-go a twierdzeniami paragrafu poprzedzającego. W osnowie twierdzeń paragrafu poprzedzającego leży to założenie, iż liczby przedstawione są w numeracyi dziesiętnej; twierdzenia te stanowią zatem pewne własności numeracyi dziesiętnej. Twierdzenia zaś z § 40-go są całkiem niezależne od rodzaju przyjętej numeracyi. Oczywiście możemy podzielić ogół twierdzeń i pojęć z teoryi liczb całkowitych na twierdzenia i pojęcia znajdujące się w związku z powszechnie przyjętą numeracyą dziesiętną i twierdzenia i pojęcia całkiem niezależne od rodzaju przyjętej numeracyi. Twierdzenia ostatniej kategoryi mają oczywiście charakter daleko większej bezwzględności od twierdzeń kategoryi pierwszej. Dlatego też, żeby należycie ocenić doniosłość każdego twierdzenia lub pojęcia, należy uprzytomnić sobie do jakich z wymienionych dwóch kategoryi twierdzeń lub pojęć należy rozważane twierdzenie albo pojęcie. Uwaga ta ma tem większe znaczenie, że twierdzenia obu kategoryi spotykamy ciągle jedne obok drugich. Oczywiście możnaby wyłożyć ogół wszystkich twierdzeń i pojęć niezależnych od rodzaju przyjętej numeracyi, a mających być w wykładzie uwzględnionych, przed teoryą numeracyi dziesiętnej oraz pojęciami i twierdzeniami z nią związanymi. Taki jednak sposób traktowania przedmiotu byłby niewątpliwie bardzo uciążliwym.

## X. Teorya największego wspólnego dzielnika i najmniejszej wspólnej wielekrotności dwóch albo kilku liczb.

§ 43. Samo brzmienie wyrażeń „wspólny dzielnik pewnych liczb“ i „wspólna wielokrotność tych liczb“ wskazuje na to,

że pierwsze z nich oznacza liczbę przez którą każda z uważanych liczb byłaby podzielną a drugie — liczbę, która byłaby podzielną przez każdą z tych liczb.

Jeżeli pewna liczba $d$ jest wspólnym dzielnikiem pewnych liczb, jeżeli nadto niema żadnego wspólnego dzielnika tych liczb większego od liczby $d$, to liczba $d$ zwie się największym wspólnym dzielnikiem rozważanych liczb.

Jeżeli pewna liczba $w$ od zera odmienna jest wspólną wielokrotnością pewnych liczb, jeżeli nadto nie istnieje żadna, od zera odmienna, wspólna wielokrotność tych liczb mniejsza od liczby $w$, to liczba $w$ zwie się najmniejszą wspólną wielokrotnością rozważanych liczb.

Z definicyi poprzedzających wynikają natychmiast konsekwencye następujące: największy wspólny dzielnik oznaczonych liczb, o ile istnieje, jest określony w zupełności; najmniejsza wspólna wielokrotność oznaczonych liczb, o ile istnieje, określona jest w zupełności.

Ponieważ reszta podziału liczby całkowitej $a$, od zera odmiennej, przez liczbę od niej większą równa się samej tej liczbie $a$ i jest zatem od zera odmienną, przeto żadna liczba od zera odmienna nie posiada dzielnika od niej większego.

Ponieważ dalej żadna liczba od zera odmienna przez zero podzielną nie jest, przeto liczba dzielników liczby od zera odmiennej w żadnym razie od samej tej liczby większą być nie może. Z tego wynika, że liczba wspólnych dzielników dowolnej liczby liczb całkowitych, pomiędzy któremi znajduje się przynajmniej jedna liczba $a$ od zera odmienna, najwyżej równać się może liczbie $a$ i jest zatem skończoną.

Ponieważ zaś liczba *jeden* jest dzielnikiem każdej liczby, przeto dochodzimy do wniosku następującego: jeżeli pomiędzy liczbami należącemi do pewnego układu $(U)$, zawierającego dowolną liczbę liczb całkowitych, znajduje się choć jedna liczba od zera odmienna, to liczba $p$ wspólnych dzielników liczb stanowiących układ $(U)$ jest zawsze skończoną i nigdy mniejszą od jedności nie jest; jeżeli mamy $p=1$, to jedyny wspólny dzielnik liczb stanowiących układ $(U)$ jest oczywi-

ście jednocześnie największym wspólnym dzielnikiem tych liczb, jeżeli zaś mamy $p > 1$, to (tw. XII, § 7) jeden ze wspólnych dzielników rozważanych liczb będzie większy od wszystkich innych. Ten dzielnik wspólny liczb układu $(U)$ będzie oczywiście największym wspólnym dzielnikiem tych liczb. Ostatecznie dochodzimy do wniosku następującego:

Jeżeli pomiędzy liczbami, należącemi do pewnego układu $(U)$ liczb całkowitych, znajduje się choć jedna liczba od zera odmienna, to istnieje największy wspólny dzielnik liczb należących do układu $(U)$; musimy oczywiście dodać, że w razie gdyby wszystkie liczby układu $(U)$ równały się zeru, nie istniałby największy wspólny dzielnik tych liczb, albowiem każda liczba całkowita byłaby wspólnym dzielnikiem rozważanych liczb.

Przechodzimy teraz do zbadania sprawy istnienia najmniejszej wspólnej wielokrotności liczb należących do oznaczonego układu $(U)$.

Ponieważ żadna od zera odmienna liczba nie jest podzielną przez liczbę zero, przeto, gdyby choć jedna liczba układu $(U)$ równała się zeru, to liczba zero byłaby jedyną wspólną wielokrotnością liczb stanowiących układ $(U)$. Zatem w tym przypadku nie byłoby najmniejszej wspólnej wielokrotności liczb należących do układu $(U)$. Załóżmy więc, że liczba zero do układu $(U)$ nie należy. Ponieważ od zera odmienna wspólna wielokrotność pewnych jakichkolwiek liczb nie może być mniejszą od żadnej z tych liczb, przeto, żeby istniała najmniejsza wspólna wielokrotność liczb stanowiących układ $(U)$, koniecznem jest żeby istniała oznaczona liczba całkowita $M$, którą żadna liczba układu $(U)$ nie mogłaby przekroczyć.

Warunek ten w połączeniu z uczynionem już założeniem, że liczba zero do układu $(U)$ nie należy, zapewnia istnienie najmniejszej wspólnej wielokrotności liczb należących do układu $(U)$. Istotnie gdyby wyjątkowo wszystkie liczby układu $(U)$ były sobie równe, to wspólna ich wartość oczywiście byłaby najmniejszą wspólną wielokrotnością rozważanych liczb. Gdyby zaś nie wszystkie liczby układu $(U)$ były sobie równe, to moglibyśmy rozumować w sposób następujący.

Oznaczmy przez $(z)$ układ wszystkich odmiennych od siebie liczb należnych do układu $(U)$; ponieważ żadna z liczb układu $(z)$ nie mogłaby być większą od liczby $M$, którą nie przekracza żadna liczba układu $(U)$, przeto liczba liczb zbioru $(z)$ byłaby skończoną. Powiadam, że istnieje niezawodnie najmniejsza wspólna wielokrotność liczb zbioru $(z)$. Istotnie — oznaczamy przez $P$ iloczyn liczb zbioru $(z)$. Ponieważ żadna liczba zbioru $(z)$ zeru nie równa się, przeto liczba $P$ będzie od zera odmienną. Z drugiej strony liczba $P$ jest oczywiście wspólną wielokrotnością liczb zbioru $(z)$. Jeżeli niema żadnej wspólnej wielokrotności liczb zbioru $(z)$ od liczby $P$ mniejszej i od zera odmiennej, to liczba $P$ będzie sama najmniejszą wspólną wielokrotnością liczb zbioru $(z)$. Gdyby zaś okoliczność poprzedzająca nie zachodziła, to ze względu na to, iż liczba wspólnych wielokrotności liczb zbioru $(z)$ od liczby $P$ nie większych a od zera odmiennych oczywiście skończoną będzie, znajdzie się pomiędzy temi liczbami zawsze jedna, $P'$, (tw. XII, § 7), która będzie mniejszą od wszystkich innych. Liczba $P'$ będzie oczywiście najmniejszą wspólną wielokrotnością liczb zbioru $(z)$.

Stwierdziliśmy więc, że najmniejsza wspólna wielokrotność liczb stanowiących zbiór $(z)$ istnieje w każdym razie. Oznaczmy ją przez $w$. Liczba $w$ jest wspólną wielokrotnością liczb układu $(U)$ albowiem każda z liczb tego układu równa się pewnej liczbie zbioru $(z)$ a więc liczbie, która jest dzielnikiem liczby $w$. Żadna od zera odmienna wspólna wielokrotność $w'$ liczb układu $(U)$ nie może być mniejszą od liczby $w$ albowiem liczba $w'$ oczywiście zawsze będzie wspólną wielokrotnością liczb zbioru $(z)$ — skąd wynika, że w razie nierówności:

$$w' < w,$$

liczba $w$ wbrew założeniu nie byłaby najmniejszą wspólną wielokrotnością liczb zbioru $(z)$. Ostatecznie dochodzimy do wyniku następującego: żeby najmniejsza wspólna wielokrotność liczb całkowitych stanowiących pewien układ $(U)$ istniała, koniecznem jest i wystarczającem, żeby żadna liczba układu $(U)$

zeru nie równała się i żeby istniała oznaczona liczba, którą nie przekraczałaby żadna z tych licz.

Z stwierdzenia tego wynika w szczególności, że zawsze istnieje najmniejsza wspólna wielokrotność skończonej liczby oznaczonych liczb całkowitych, od liczby zero odmiennych.

Do ogólników poprzedzających winniśmy jeszcze dołączyć uwagę następującą: jeżeli liczby należące do pewnego układu ($U$) posiadają najmniejszą wspólną wielokrotność, to liczby te posiadają nieskończenie wiele odmiennych od siebie wspólnych wielokrotności, albowiem wszelka wielokrotność najmniejszej wspólnej wielokrotności $w$, rozważanych liczb, jest oczywiście wspólną ich wielokrotnością.

Z poprzedniego wynika w szczególności, że liczba wielokrotności wspólnych skończonej liczby oznaczonych liczb całkowitych, z których żadna zeru nie równa się, jest nieskończonością.

§ 44. Teorya największego wspólnego dzielnika dwóch liczb opiera się na pewnych własnościach dzielenia. Własności te podajemy w postaci twierdzeń następujących.

**Tw. I.** Zbiór wspólnych dzielników dwóch od zera odmiennych liczb identyczny jest zbiorowi wspólnych dzielników którejkolwiek z tych liczb i reszty podziału przez tę liczbę drugiej z nich.

Dowód. Oznaczmy przez $q$ i $r$ całkowitą część ilorazu i resztę podziału pewnej liczby $a$ przez pewną liczbę $b$, od zera odmienną. Będziemy tedy mieli

$$a = q \,.\, b + r \tag{1}$$

skąd

$$r = a - q \,.\, b \tag{2}$$

Oznaczmy przez $(z)$ zbiór wspólnych dzielników liczb $a$ i $b$ a przez $(z')$ zbiór wspólnych dzielników liczb $b$ i $r$. Jeżeli pewna liczba $l$ należy do zbioru $(z)$ to, na podstawie równości (2), liczba ta jest (§ 40, tw. I i tw. II) dzielnikiem liczby $r$. A ponieważ liczba $l$, jako wspólny dzielnik liczb $a$ i $b$, jest

dzielnikiem liczby $b$, przeto liczba $l$ jest wspólnym dzielnikiem liczb $b$ i $r$ i z tej przyczyny należy do zbioru $(z')$. Stwierdzamy więc, że każda liczba zbioru $(z)$ należy do zbioru $(z')$. Całkiem analogiczne rozumowanie da nam możność wywnioskowania z równości (1), że każda liczba zbioru $(z')$ należy do zbioru $(z)$. Dowiedliśmy więc, że zbiory $(z)$ i $(z')$ zlewają się ze sobą. O to właśnie chodziło.

Wniosek. Największy wspólny dzielnik, dwóch od zera odmiennych liczb, który jak wiemy (§ 43) istnieje, równa się największemu wspólnemu dzielnikowi którejkolwiek z tych liczb i reszty podziału przez tę liczbę drugiej z nich.

Uwaga: Przy dowodzie twierdzenia poprzedzającego opieraliśmy się wyłącznie na równości (1), bynajmniej nie odwołując się do nierówności

$$r < b.$$

Zatem, w rozumowaniu naszem istotną była tylko ta okoliczność, iż różnica liczb $a$ i $r$ była wielokrotnością liczby $b$.

Z tego zaś wynika, że w rzeczywistości uzasadniliśmy twierdzenie ogólniejsze od twierdzenia wysłowionego, mianowicie — twierdzenie następujące: zbiór wspólnych dzielników dwóch liczb nie ulegnie zmianie, jeżeli zastąpimy jedną z nich przez liczbę różniącą się od niej o dowolną wielokrotność drugiej. (Zastrzenie żeby uważane liczby były od zera odmienne pominęliśmy, bo, w twierdzeniu wyżej udowodnionem, zastrzeżenie to było koniecznem tylko dlatego, żeby zapewnić wykonalność dzielenia).

**Tw. II.** Oznaczmy przez $a$, $b$, $a'$, $b'$, i $d$ pięć liczb od zera odmiennych, sprawdzających równości następujące:

$$(1) \qquad \begin{cases} a = d \,.\, a' \\ b = d \,.\, b' \end{cases}$$

Jeżeli oznaczymy przez $q$ i $r$ całkowitą część ilorazu i resztę podziału liczby $a$ przez liczbę $b$ a przez $q'$ i $r'$ całkowitą część ilorazu i resztę podziału liczby $a'$ przez liczbę $b'$, to liczby $q$, $q'$, $r$ i $r'$ sprawdzać będą związki następujące:

$$\begin{cases} r = d \,.\, r' \\ q = q' \end{cases} \tag{2}$$

Dowód. Mamy:

$$r' < b' \tag{3}$$

oraz

$$a' = b' \,.\, q' + r' \tag{4}$$

Ze związków (3) i (4) mamy:

$$d \,.\, r' < d \,.\, b'$$

$$d \,.\, a' = d \,.\, b' \,.\, q' + d \,.\, r'$$

czyli

$$\begin{cases} d \,.\, r' < b \\ a = b \,.\, q' + d \,.\, r' \end{cases} \tag{5}$$

na podstawie równości (1).

Ze związków (5) wynika, że liczba $q'$ i iloczyn $d \,.\, r'$ równają się odpowiednio całkowitej części ilorazu i reszcie podziału liczby $a$ przez liczbę $b$. Stwierdzamy zatem, że liczby $q$ i $r$ sprawdzają związki (2), co było do okazania.

Twierdzenie poprzedzające często wysławianem bywa zwięźle, ale niejasno i nieściśle, w sposób następujący: jeżeli przy dzieleniu pomnożymy albo podzielimy dzielną i dzielnik przez tę samą liczbę, która w drugim przypadku winna być wspólnym dzielnikiem dzielnej i dzielnika, to całkowita część ilorazu nie ulegnie zmianie a reszta zostanie pomnożoną albo podzieloną przez rozważoną liczbę.

Przechodzimy teraz do sprawy wyznaczenia największego wspólnego dzielnika dwóch liczb danych. Oczywiście winniśmy, co też uczynimy, założyć, że jedna przynajmniej z tych liczb jest od zera odmienna, albowiem gdyby obie te liczby równały się zeru, to (§ 43) liczby te nie miałyby największego wspólnego dzielnika. Gdyby jedna z dwóch liczb, o największy wspólny dzielnik których chodzi, była równa zeru, to, jak z łatwością stwierdzić możemy, największy wspólny dzielnik równałby się drugiej z nich. Gdyby zaś te liczby były sobie

równe, to największy wspólny dzielnik oczywiście równałby się wspólnej ich wartości. Zatem wysławiamy regułę do wyznaczenia największego wspólnego dzielnika dwóch liczb w założeniu, że te liczby nie są sobie równe i są obie od zera odmienne.

Tw. III. (Reguła). Żeby wyznaczyć największy wspólny dzielnik dwóch danych, od zera odmiennych, nie równych sobie liczb, tworzymy ciąg liczb, który, jeżeli oznaczymy ogólnie przez $r_i$ liczbę stanowiącą w nim element rzędu $i$, określonym być może w sposób następujący.

1) Pierwszy element $r_1$, omawianego ciągu, równa się większej $a$ z dwóch liczb danych.

2) Drugi element $r_2$ równa się drugiej danej liczbie $b$.

3) Element $r_i$ jakiegokolwiek rzędu $i$, $(i > 2)$, o ile istnieje, równa się reszcie podziału liczby $r_{i-2}$ przez liczbę $r_{i-1}$.

4) Element ostatni $r_n$ równa się zeru.

Przy takiej budowie ciągu

$$(1) \qquad r_1, r_2, \ldots, r_n$$

największy wspólny dzielnik danych liczb $a$ i $b$ równać się będzie liczbie $r_{n-1}$, stanowiącej przedostatni element tego ciągu.

Żeby regułę tę uzasadnić winniśmy przedewszystkiem okazać, że ciąg (1) zawsze może być utworzony. Liczby $r_1$, $r_2$ i $r_3$ możemy oczywiście zawsze tak wyznaczyć, żeby ciąg

$$r_1, r_2, r_3$$

sprawdzał trzy pierwsze warunki, którym miałby zadość czynić ciąg (1). Załóżmy chwilowo, że zdołaliśmy tak wyznaczyć ciąg następujący:

$$(2) \qquad r_1, r_2 \ldots r_p \qquad (p \geqq 3)$$

żeby ciąg ten sprawdzał rozważane przed chwilą trzy warunki. Gdyby na liczbę $r_p$ wypadła wartość od zera odmienna, gdyby więc ciąg (2) nie był ciągiem, o istnienie którego chodzi, to dzielenie liczby $r_{p-1}$ przez liczbę $r_p$ byłoby wykonalne.

Dołączając tedy do ciągu (2) resztę $r_{p+1}$ tego dzielenia otrzymalibyśmy nowy ciąg:

$$r_1, r_2, r_3 \cdots r_p, r_{p+1}$$

który sprawdzałby te same trzy warunki, co ciąg (2) i który nadto zawierałby o jedność więcej elementów, niż ten ciąg. Gdyby więc pomiędzy ciągami sprawdzającymi trzy pierwsze warunki, którym ciąg (1) miałby czynić zadość, nie było ciągu sprawdzającego warunek czwarty, to, na podstawie zasady indukcyi matematycznej, moglibyśmy tak utworzyć ciąg (2), żeby ciąg ten, przy dowolnie à prioni danej, od liczby 2 większej wartości, liczby $p$, sprawdzał owe trzy pierwsze warunki. Okoliczność ta nadarzyć się nie może. Jezeli bowiem ciąg (2) sprawdza trzy kilkakrotnie wspominane warunki, to musi zachodzić nierówność

$$p \leqq r_1 + 1$$

czyli

$$p \leqq a + 1$$

albowiem elementy rozważanego ciągu stanowią układ odmiennych od siebie, liczbę $a$ nie przekraczających, liczb całkowitych; taki zaś układ liczb całkowitych nie może zawierać więcej niż $a + 1$ liczb a to z tej przyczyny, iż liczba wszystkich odmiennych od siebie liczb całkowitych, liczbę $a$ nie przekraczających, wynosi $a + 1$. Stwierdzamy zatem, że elementy ciągu (1) zawsze będą mogły być tak wyznaczone, żeby ciąg ten czynił zadość wszystkim czterem, w regule wysłowionym, warunkom. Winniśmy więc tylko dowieść, że jeżeli, jak założymy, ciąg (1) czyni tym warunkom zadość, to liczba $r_{n-1}$ jest największym wspólnym dzielnikiem liczb $a$ i $b$ czyli liczb $r_1$ i $r_2$. Żeby punkt ten uzasadnić, powiadam przedewszystkiem, że największy wspólny dzielnik dwóch jakichkolwiek wyrazów sąsiednich $r_i$ i $r_{i+1}$ ciągu (1) równa się największemu wspólnemu dzielnikowi liczb $a$ i $b$. Istotnie, zdanie to przemienia się w prostą tautologię w razie, kiedy znamy $i = 1$; gdyby zaś zdanie to uzasadnionem było przy pewnej wartości $i = k$

wzkaźnika $i$, to, na mocy wniosku z tw. I, zdanie to oczywiście jeszcze byłoby uzasadnionem przy $i = k + 1$. Stwierdzamy więc, że wysłowione zdanie uzasadnionem jest w każdym razie. Z tego zaś wynika w szczególności, że największy wspólny dzielnik liczb $a$ i $b$ równa się największemu wspólnemu dzielnikowi liczb $r_{n-1}, r_n$. Ponieważ mamy

$$r_n = 0,$$

przeto, na podstawie uwagi, którą mieliśmy sposobność uczynić wyżej, największy wspólny dzielnik liczb $r_{n-1}$ i $r_n$, a więc i największy wspólny dzielnik liczb $a$ i $b$, równają się liczbie $r_{n-1}$. Zatem uzasadniliśmy w zupełności regułę, o którą chodziło.

**Tw. IV.** Zbiór dzielników wspólnych dwóch liczb zlewa się ze zbiorem dzielników ich największego wspólnego dzielnika.

Dowód. Jedna przynajmniej z dwóch uważanych liczb będzie od zera odmienną, bo w przeciwnym razie liczby te (§ 43) nie posiadałyby największego wspólnego dzielnika. W przypadku szczególnym, kiedy jedna z rzeczonych liczb równa się zeru albo kiedy liczby te są sobie równe, twierdzenie jest natychmiastowe. Żeby twierdzenie uzasadnić w przypadku ogólnym, kiedy chodzi o dwie od zera odmienne nierówne sobie liczby $a$ i $b$, zwróćmy się do ciągu $(C)$, który należałoby utworzyć, żeby zastosować do liczb $a$ i $b$, przed chwilą uzasadnione prawidło wyznaczania największego wspólnego dzielnika dwóch liczb. Opierając się na tw. I stwierdzimy łatwo, metodą indukcyi matematycznej, że zbiór wspólnych dzielników liczb $a$ i $b$ zlewa się ze zbiorem wspólnych dzielników dwóch jakichkolwiek sąsiednich a więc i ostatnich wyrazów ciągu $(C)$. Ponieważ zaś ostatni wyraz ciągu tego równa się zeru a przedostatni największemu wspólnemu dzielnikowi $d$ liczb $a$ i $b$, przeto wnosimy, że omawiany zbiór identyczny jest ze zbiorem dzielników liczby $d$, co było do okazania.

**Tw. V.** Oznaczmy przez $m$ jakąkolwiek liczbę całkowitą

od zera odmienną, a przez $a$, $b$, $a'$, $b'$ cztery liczby całkowite z których nie każda równałaby się zeru i które sprawdzałyby związki następujące:

$$\begin{cases} a = m \,.\, a' \\ b = m \,.\, b' \end{cases} \tag{1}$$

Jeżeli tedy oznaczymy przez $d$ największy wspólny dzielnik liczb $a$ i $b$ a przez $d'$ największy wspólny dzielnik liczb $a'$ i $b'$, to liczby $d$ i $d'$ sprawdzać będą związek następujący:

$$d = m \,.\, d' \tag{2}$$

Dowód. Przedewszystkiem winniśmy upewnić się, że liczby $d$ i $d'$, przy uczynionych założeniach, zawsze istnieją. W tym zaś celu należy tylko dowieść (§ 43), że jedna przynajmniej z liczb $a$ i $b$ i jedna przynajmniej z liczb $a'$ i $b'$ są od zera odmienne. Otóż okoliczność ta zachodzi niozawodnie, w przeciwnym bowiem razie wynikłoby ze związków (1), że liczby $a$, $b$, $a'$ i $b'$ równe są wszystkie zeru co byłoby w sprzeczności z założeniem, iż jedna z nich przynajmniej jest od zera odmienną.

Gdyby wyjątkowo jedna z liczb $a'$ albo $b'$ równała się zeru to, na podstawie związków (1), jedna z liczb $a$ albo $b$ także równałaby się zeru. W takim zaś razie twierdzenie byłoby natychmiastowem. Rozważane twierdzenie byłoby oczywiście też natychmiastowem i w tym szczególnym przypadku, w którym liczby $a'$ i $b'$ byłyby sobie równe. Zakładamy więc, że liczby $a'$ i $b'$ są dwie nierówne sobie i od zera odmienne liczby całkowite. W takim razie [związki (1)] liczby $a$ i $b$ byłyby także od zera odmiennemi, nierównemi sobie liczbami. Oznaczmy przez $(C)$ i $(C')$ ciągi liczb całkowitych, które należałoby utworzyć pragnąc wyznaczyć, na podstawie podanego wyżej prawidła, największy wspólny dzielnik liczb $a$ i $b$ oraz największy wspólny dzielnik liczb $a'$ i $b'$. Ze względu na związki (1) stwierdzimy łatwo metodą indukcyi matematycznej, opierając się przy tem na tw. II, że ciąg $(C')$ przemieni się w ciąg $(C)$, jeżeli zastąpimy każdy wyraz ciągu tego przez jego iloczyn przez liczbę $m$. Zatem, w szczególności, przedostatni wyraz $d$

ciągu $(C)$ równać się będzie iloczynowi przez $m$ przedostatniego wyrazu $d'$ ciągu $(C')$. Stwierdzamy więc, że liczby $d$ i $d'$ sprawdzać będą związek (2), co było do okazania.

Jeżeli największy wspólny dzielnik dwóch liczb całkowitych równa się jedności, to liczby te zowią się pierwszemi pomiędzy sobą.

**Tw. VI.** Ilorazy podziału dwóch liczb całkowitych przez ich największy wspólny dzielnik są liczbami pierwszemi pomiędzy sobą. Odwrotnie: jeżeli ilorazy dwóch liczb całkowitych przez pewien wspólny dzielnik są liczbami całkowitemi pierwszemi pomiędzy sobą, to ten wspólny dzielnik jest największym wspólnym dzielnikiem rozważanych liczb.

Dowód. Oznaczmy przez $d$ największy wspólny dzielnik dwóch liczb całkowitych $a$ i $b$. Będziemy wtedy mieli

$$(1) \qquad \begin{cases} a = a' \,.\, d \\ b = b' \,.\, d \end{cases}$$

oznaczając przez $a'$ i $b'$ odpowiednio ilorazy podziału liczb $a$ i $b$ przez $d$. Ponieważ liczby $a'$ i $b'$ obie zeru równać się nie mogą, przeto największy wspólny dzielnik $\delta$ tych liczb istnieć będzie niezawodnie. Przyjmijmy

$$(2) \qquad \begin{cases} a' = a'' \,.\, \delta \\ b' = b'' \,.\, \delta \end{cases}$$

Symbole $a''$ i $b''$ oczywiście oznaczać będą dwie liczby całkowite. Z równości (1) i (2) mamy:

$$a = a'' \,.\, (d \,.\, \delta)$$
$$b = b'' \,.\, (d \,.\, \delta)$$

Zatem iloczyn $d \,.\, \delta$ jest wspólnym dzielnikiem liczb $a$ i $b$ i jako taki sprawdzać będzie związek:

$$(3) \qquad d \,.\, \delta \leqq d.$$

Ponieważ liczba $\delta$ zeru równać się nie może, przeto związek (3) pociąga za sobą równość:

$$\delta = 1$$

Ze względu na znaczenie nadane literze $\delta$, równość ta wyraża, że liczby $a'$ i $b'$ są liczbami pierwszemi pomiędzy sobą. Uzasadniliśmy więc pierwszą część twierdzenia.

Żeby uzasadnić drugą część zwróćmy się do równości (1) nie uważając już liczby całkowitej $d$ za największy wspólny dzielnik liczb $a$ i $b$ lecz zakładając natomiast, że liczby całkowite $a'$ i $b'$ są liczbami pierszemi pomiędzy sobą.

Ponieważ liczba $1$ jest największym wspólnym dzielnikiem liczb $a'$ i $b'$, ponieważ z tej przyczyny obie te liczby zeru równać się nie mogą, przeto, na podstawie twierdzenia poprzedzającego, iloczyn

$$1 . d$$

równać się będzie największemu wspólnemu dzielnikowi liczb $a$ i $b$. W innych wyrazach, wspomniany największy wspólny dzielnik równać się będzie liczbie $d$, co właśnie pozostawało jeszcze do okazania.

**Tw. VII.** Jeżeli pewna liczba całkowita $d$, jest dzielnikiem iloczynu pewnych dwóch czynników całkowitych $a$ i $b$, jeżeli nadto liczba $d$ i jeden z czynników, czynnik $b$, są liczbami pierwszemi pomiędzy sobą, to liczba $d$ jest dzielnikiem drugiego czynnika $a$.

Dowód. Gdyby liczba $a$ równała się zeru, to twierdzenie zachodziłoby oczywiście. Rozważane twierdzenie zachodziłoby też w przypadku szczególnym, w którym mielibyśmy

$$d = 0,$$

albowiem w takim razie mielibyśmy z konieczności $b = 1$ oraz $a = 0$.

Przechodzimy obecnie do przypadku ogólnego, kiedy żadna z liczb $a$ i $d$ zeru nie równa się. Ponieważ największy wspólny dzielnik liczb $b$ i $d$ równa się jedności, przeto (tw. V) największy wspólny dzielnik iloczynów $a . b$ i $a . d$ równać się będzie iloczynowi $a . 1$ czyli liczbie $a$. Zważmy teraz, że liczba $d$ jest wspólnym dzielnikiem iloczynów $a . b$ i $a . d$ albowiem, z założenia, liczba $d$, która oczywiście jest dzielni-

kiem iloczynu $a \cdot d$, jest także dzielnikiem iloczynu $a \cdot b$. Zatem (tw. IV) liczba $d$ jest dzielnikiem liczby $a$, co było do okazania.

§ 45. **Tw. VIII.** Największy wspólny dzielnik jakiejkolwiek skończonej liczby $n$ ($n > 2$) liczb od zera odmiennych, równa się największemu wspólnemu dzielnikowi którejkolwiek z nich i największego wspólnego dzielnika wszystkich liczb pozostałych; nadto zbiór wspólnych dzielników rozważanych $n$ liczb zlewa się ze zbiorem dzielników ich największego wspólnego dzielnika.

Dowód. Zwróćmy się najpierw do przypadku, w którym $n = 3$, i oznaczmy przez $d$ największy wspólny dzielnik dwóch liczb $a$ i $b$ z pomiędzy rozważanych trzech liczb $a$, $b$ i $c$. Ponieważ zbiór dzielników wspólnych liczb $a$ i $b$ zlewa się (tw. IV) ze zbiorem dzielników liczby $d$, przeto zbiór dzielników wspólnych liczb $a$, $b$ i $c$ zlewa się ze zbiorem dzielników wspólnych liczb $d$ i $c$. Z tego wynika, że największy wspólny dzielnik $d'$ liczb $a$, $b$ i $c$ równa się największemu wspólnemu dzielnikowi liczb $d$ i $c$. Jeżeli jeszcze zważymy że zbiór dzielników wspólnych liczb $d$ i $c$ zlewa się (tw. IV) ze zbiorem dzielników liczby $d'$, to z poprzedniego łatwo jeszcze wywnioskujemy, że zbiór dzielników wspólnych liczb $a$, $b$ i $c$ zlewa się ze zbiorem dzielników ich największego wspólnego dzielnika $d'$. Zatem, dla $n=3$, uzasadniliśmy twierdzenie w zupełności.

Załóżmy chwilowo, że twierdzenie zachodziłoby, gdybyśmy mieli $n=k$ ($k \geqq 3$), i rozważajmy przypadek, w którym mamy $n = k+1$. Oznaczmy tedy przez $a$ jedną którąkolwiek z rozważanych $k+1$ liczb a przez $(z)$ zbiór wszystkich liczb pozostałych. Ponieważ zbiór $(z)$ zawiera $k$ od zera odmiennych liczb całkowitych, przeto, na mocy chwilowo przyjętego założenia, zbiór wspólnych dzielników liczb stanowiących ten zbiór zlewa się ze zbiorem dzielników ich największego wspólnego dzielnika $d$. Zatem zbiór dzielników wspólnych uważanych $k+1$ liczb zlewa się ze zbiorem dzielników wspólnych liczb $a$ i $d$. Z tego wnosimy nasamprzód bezpośrednio, że

największy wspólny dzielnik uważanych $k+1$ liczb równa się największemu wspólnemu dzielnikowi $d'$ liczb $a$ i $d$, a następnie, na podstawie tw. IV, że zbiór dzielników wspólnych tych liczb zlewa się ze zbiorem dzielników liczby $d'$. Stwierdzamy więc, że słuszność twierdzenia dla $n = k$ pociągałaby za sobą słuszność tegoż przy $n=k+1$. Z uzyskanych wyników wnosimy natychmiast, że twierdzenie zachodzi w podanem brzmieniu.

Uwaga. Druga część twierdzenia poprzedzającego, ta mianowicie, która opiewa, że zbiór dzielników wspólnych jakiejkolwiek skończonej liczby oznaczonych liczb zlewa się ze zbiorem dzielników ich największego wspólnego dzielnika, zachodzi pod jedynym warunkiem, żeby największy wspólny dzielnik istniał, co jak wiemy ma miejsce byleby jedna przynajmniej z rozważanych liczb była od zera odmienną. Żeby przekonać się o tem, należy tylko uprzytomnić sobie, bardzo łatwą do stwierdzenia okoliczność następującą: jeżeli z pewnego zbioru $(z)$ liczb całkowitych możemy wyprowadzić inny zbiór $(z')$, usuwając z pierwszego zbioru liczbę zero, to zbiór dzielników wspólnych liczb należących do zbioru $(z)$ nie różni się od zbioru dzielników wspólnych liczb zbioru $(z')$.

Ze względu na twierdzenie poprzedzające oczywiście zawsze zdołamy załatwić sprawę wyznaczenia największego wspólnego dzielnika jakiejkolwiek skończonej liczby liczb całkowitych danych.

**Tw. IX.** Oznaczmy przez $m$ jakąkolwiek liczbę całkowitą od zera odmienną a przez

$$a_1, a_2, \ldots a_n \tag{1}$$

i

$$b_1, b_2, \ldots b_n \tag{2}$$

dwa układy liczb całkowitych sprawdzających równości następujące:

$$a_i = m \cdot b_i \quad (i = 1, 2, \ldots n). \tag{3}$$

Jeżeli choć jedna liczba w jednym z układów (1) albo (2) jest od zera odmienną, to największy wspólny dzielnik $d$

liczb układu (1) i największy wspólny dzielnik $\delta$ liczb układu (2) sprawdzają związek następujący:

$$d = m \,.\, \delta.$$

Dowód. Skoro jedna przynajmniej liczba w jednym z układów (1) albo (2) jest od zera odmienną, to, ze względu na równości (3), jedna przynajmniej liczba drugiego układu jest oczywiście też od zera odmienną. Zatem (§ 43) największe wspólne dzielniki $d$ i $\delta$ istnieją niezawodnie.

Twierdzenie obecne zachodzi oczywiście przy $n=2$, albowiem w tym przypadku nie różni się ono od tw. V. Załóżmy więc, że rozważane twierdzenie zachodzi dla $n = k$ i przyjmijmy

$$n = k + 1.$$

Gdyby jedna z liczb $b_p$ układu (2) równała się zeru, to jedna z liczb, mianowicie $a_p$, układu (1) też równałaby się zeru. W takim razie liczby $d$ i $\delta$ byłyby odpowiednio największymi wspólnymi dzielnikami liczb układów $(A)$ i $(B)$, w które przeszłyby układy (1) i (2) po usunięciu liczb $a_p$ i $b_p$. Zatem, w rozważanym przypadku szczególnym twierdzenie zachodziłoby na mocy chwilowo przyjętego założenia. Zwróćmy się teraz do przypadku ogólnego, kiedy żadna z liczb układu (2) zeru nie równa się i oznaczmy przez $d'$ największy wspólny dzielnik liczb

$$a_1, \; a_2 \ldots a_{n-1}$$

a przez $\delta'$ największy wspólny dzielnik liczb

$$b_1, \; b_2 \ldots b_{n-1}.$$

Na podstawie chwilowo przyjętego założenia, mamy

$$d' = m \,.\, \delta'. \tag{4}$$

Z drugiej strony (tw. VIII) liczba $d$ jest największym wspólnym dzielnikiem liczb $d'$ i $a_n$ a liczba $\delta$ — liczb $\delta'$ i $b_n$.

Ponieważ jedna z równości (3) jest równość:

$$a_n = m \,.\, b_n, \tag{5}$$

przeto z równości (4) wnosimy (tw. V), że

$$d = m \,.\, \delta.$$

Dowiedliśmy więc, że gdyby twierdzenie zachodziło przy $n=k$, to twierdzenie to zachodziłoby także przy $n=k+1$. Ponieważ zaś stwierdziliśmy wyżej, że twierdzenie zachodzi przy $n=2$, przeto wnosimy, że twierdzenie zachodzi w każdym razie, co było do okazania.

Podobnie do sposobu, w jaki wyprowadziliśmy z tw. V tw. VI, wyprowadzimy łatwo z twierdzenia poprzedzającego, tw. następujące.

**Tw. X.** Iloczyny podziału jakichkolwiek liczb, z których nie każda równa się zeru i których liczba jest skończoną, przez ich największy wspólny dzielnik, stanowią układ liczb, których największy wspólny dzielnik równa się jedności. Odwrotnie, jeżeli ilorazy podziału rzeczonych liczb przez pewien wspólny dzielnik $d$ stanowią układ liczb, których największy wspólny dzielnik równa się jedności, to liczba $d$ jest największym wspólnym dzielnikiem uważanych liczb.

§ 46. **Tw. XI.** Najmniejsza wspólna wielokrotność dwóch liczb $a$ i $b$, z konieczności (§ 43) od zera odmiennych, równa się ilorazowi ich iloczynu przez ich największy wspólny dzielnik; nadto wszelka wspólna wielokrotność rozważanych liczb podzielną jest przez najmniejszą wspólną wielokrotność tych liczb.

Dowód. Oznaczmy przez $a'$ i $b'$ ilorazy podziału liczb $a$ i $b$ przez ich największy wspólny dzielnik $d$. Mamy tedy:

$$a = a' \,.\, d \tag{1}$$
$$b = b' \,.\, d. \tag{2}$$

Oznaczmy przez $M$ jakąkolwiek wspólną wielokrotność liczb $a$ i $b$. Mamy:

$$\left.\begin{aligned} M &= x \,.\, a = x \,.\, a' \,.\, d, \\ M &= y \,.\, b = y \,.\, b' \,.\, d, \end{aligned}\right\} \tag{3}$$

oznaczając przez $x$ i $y$ pewne liczby całkowite.

Z równań (3) wynika: 1) że liczba $M$ podzielną jest przez liczbę $d$, 2) że oznaczając przez $M'$ odnośny iloraz mamy

$$M' = x \,.\, a' = y \,.\, b'. \tag{4}$$

Równości te uwidaczniają tę okoliczność, iż iloczyn $x \,.\, a'$ podzielnym jest przez liczbę $b'$. Ponieważ zaś liczby $a'$ i $b'$ są (tw. VI) liczbami pierwszemi pomiędzy sobą, przeto (tw. VII), liczba $b'$ jest dzielnikiem liczby $x$. Mamy więc

$$x = t \,.\, b' \tag{5}$$

oznaczając przez $t$ pewną liczbę całkowitą. Z równości (3), (4) i (5) mamy:

$$M = t \,.\, m \tag{6}$$

przyjmując

$$m = a' \,.\, b' \,.\, d. \tag{7}$$

Równość (6) opiewa, że wszelka wielokrotność wspólna liczb $a$ i $b$ a więc i najmniejsza wielokrotność tych liczb jest wielokrotnością liczby $m$, określonej wzorem (7). Ponieważ zaś z równości (1), (2) i (7) wynika natychmiast, że liczba $m$ jest sama wielokrotnością wspólną liczb $a$ i $b$, przeto wszelka wielokrotność liczby $m$ jest wielokrotnością wspólną liczb $a$ i $b$. Z poprzedniego wnosimy, że liczba $M$, uważana jako określona wzorem (6), równać się będzie najmniejszej wspólnej wielokrotności liczb $a$ i $b$, jeżeli liczba $t$ taką mieć będzie wartość, przy której iloczyn $t \,.\, m$ mieć będzie możliwie najmniejszą od zera odmienną wartość. Okoliczność ta oczywiście zajdzie, przyjmując $t=1$. Zatem liczba $m$, określona wzorem (7), jest najmniejszą wspólną wielokrotnością liczb $a$ i $b$. Ponieważ widzieliśmy, że liczba ta jest dzielnikiem wszelkiej wielokrotności wspólnej liczb $a$ i $b$, przeto wszelka wielokrotność tych liczb podzielną jest przez ich najmniejszą wspólną wielokrotność.

Ponieważ nareszcie, ze wzorów (1), (2) i (7), mamy

$$a \,.\, b = m \,.\, d,$$

przeto najmniejsza wielokrotność dwóch liczb jest ilorazem podziału iloczynu tych liczb przez ich największy wspólny dzielnik.

Dowiedliśmy więc w zupełności twierdzenia, o które chodziło.

§ 47. **Tw. XII.** Najmniejsza wspólna wielokrotność $n$ liczb ($n>2$), z konieczności (§ 43) od zera odmiennych, równa się najmniejszej wspólnej wielokrotności którejkolwiek z rozważanych liczb i najmniejszej wspólnej wielokrotności wszystkich liczb pozostałych; nadto wszelka wspólna wielokrotność rozważanych liczb jest wielokrotnością najmniejszej ich wspólnej wielokrotności.

Dowód. Uważajmy trzy od zera odmienne jakiekolwiek liczby całkowite $a$, $b$ i $c$ i oznaczmy przez $\mu$ najmniejszą wspólną wielokrotność liczb $a$ i $b$. Wszelka wielokrotność liczb $a$ i $b$, a zatem także wszelka wielokrotność wspólna liczb $a$, $b$ i $c$, podzielną jest (tw. XI) przez liczbę $\mu$.

Stwierdzamy więc, że wszelka wspólna wielokrotność liczb $a$, $b$ i $c$ jest wspólną wielokrotnością liczb $\mu$ i $c$ i jest, z tej przyczyny (tw. XI), podzielną przez najmniejszą wspólną wielokrotność $m$ liczb $\mu$ i $c$.

Ponieważ liczba $m$ jest oczywiście sama wspólną wielokrotnością liczb $a$, $b$ i $c$, przeto wnosimy natychmiast z poprzedniego, że twierdzenie, o dowód którego chodzi, zachodzi niezawodnie w przypadku kiedy mamy $n=3$. Załóżmy chwilowo, że twierdzenie to zachodzi w przypadku, kiedy mamy $n=k$ ($k\geqq 3$) i rozważajmy $k+1$, od zera odmiennych liczb

$$a_1, a_2, \ldots a_k, a_{k+1}. \tag{1}$$

Jeżeli oznaczymy tedy przez $\mu$ najmniejszą wspólną wielokrotność liczb następujących

$$a_1, a_2 \ldots a_k \tag{2}$$

to, na podstawie chwilowo przyjętego założenia, wszelka wspólna wielokrotność liczb (2) a więc w szczególności wszelka wspólna wielokrotność liczb (1) podzielną będzie przez liczbę $\mu$. Zatem wszelka wspólna wielokrotność liczb (1) będzie wspólną

wielokrotnością liczb $\mu$ i $a_{k+1}$. Stąd zaś wnosimy (tw. XI), że wszelka wspólna wielokrotność liczb (1) podzielną będzie przez najmniejszą wspólną wielokrotność $m$ liczb $\mu$ i $a_{k+1}$. Ponieważ zaś liczba $m$ jest oczywiście sama wspólną wielokrotnością liczb (1), przeto liczba $m$ będzie najmniejszą wspólną wielokrotnością tych liczb. Stwierdzamy więc co następuje: gdyby rozważane twierdzenie zachodziło w razie, kiedy $n=k$, to twierdzenie to zachodziłoby także przy $n = k + 1$. Ponieważ zaś widzieliśmy już, że omawiane twierdzenie zachodzi istotnie w razie kiedy mamy $n=3$, przeto wnosimy, że twierdzenie to zachodzi w podanem brzmieniu, co było do okazania.

Twierdzenie poprzedzające oczywiście sprowadza zadanie polegające na wyznaczeniu najmniejszej wspólnej wielokrotności kilku liczb do takiegoż zadania co do dwóch liczb Zatem sprawa wyznaczenia najmniejszej wspólnej wielokrotność kilku liczb uważana być może za załatwioną.

## XI. Liczby pierwsze.

§ 48. Wszelka liczba całkowita, podzielna tylko przez siebie samą i przez jedność zwie się liczbą pierwszą.

Ponieważ żaden dzielnik liczby całkowitej, od zera odmiennej, liczby tej przekroczyć nie może, przeto, jeżeli pewna liczba całkowita nie posiada żadnego od niej mniejszego lecz od jedności większego dzielnika, to liczba ta jest liczbą pierwszą. Na podstawie uwagi tej stwierdzamy łatwo, że liczba 7 n. p. jest liczbą pierwszą.

W § 44-ym wprowadziliśmy pojęcie liczb pierwszych pomiędzy sobą. Dwie liczby pierwsze pomiędzy sobą mogą nie być liczbami pierwszemi: n. p. liczby *4* i *9* są oczywiście liczbami pierwszemi pomiędzy sobą a jednak żadna z nich nie jest liczbą pierwszą. Okoliczność tą wystawiamy orzekając, iż pewna liczba może być względnie pierwszą, t. j. pierwszą w stosunku do innej lub do innych liczb, nie będąc liczbą bezwzględnie pierwszą.

Oczywiście dwie nierówne sobie liczby pierwsze są zawsze liczbami pierwszemi pomiędzy sobą.

§ 49. **Tw. I.** Jeżeli pewna liczba $a$ jest względnie pierwszą w stosunku do każdej liczby należącej do pewnego zbioru $(z)$, zawierającego skończoną liczbę $n$ $(n \geqq 1)$ liczb całkowitych, jeżeli nadto liczba $a$ jest dzielnikiem iloczynu $P$ pewnej liczby $b$ przez iloczyn liczb należących do zbioru $(z)$, to liczba $a$ jest dzielnikiem liczby $b$.

Dowód. W przypadku szczególnym, kiedy mamy $n = 1$, twierdzenie obecne nie różni się od uzasadnionego już tw. VII z § 44-go. Załóżmy chwilowo, że twierdzenie obecne zachodzi w razie, kiedy liczba $n$ równa się pewnej liczbie $k$ $(k \geqq 1)$ i zwróćmy się do przypadku, kiedy mamy

$$n = k + 1.$$

Oznaczmy tedy przez $c$ jedną z liczb należących do zbioru $(z)$ i niech symbol $P'$ przedstawia iloczyn, w który przeszedłby iloczyn $P$, gdybyśmy usunęli z niego czynnik $c$. Mamy

$$P = c \,.\, P'.$$

Liczba $a$ będzie więc (tw. VII, § 44) dzielnikiem iloczynu $P'$. Zatem, na podstawie chwilowo przyjętego założenia, liczba $a$ będzie dzielnikiem liczby $b$. Z poprzedniego wnosimy, opierając się na zasadzie indukcyi matematycznej, że rozważane twierdzenie zachodzi w podanem brzmieniu.

**Tw. II.** Jeżeli pewna liczba całkowita $a$ jest względnie pierwszą w stosunku do każdej liczby, należącej do pewnego zbioru $(z)$, zawierającego skończoną liczbę $n$ $(n > 1)$ liczb całkowitych, to liczba $a$ jest względnie pierwszą w stosunku do iloczynu $P$ liczb, należących do zbioru $(z)$.

Dowód. Oznaczmy przez $d$ największy wspólny dzielnik liczby $a$ i iloczynu $P$; tenże istnieć będzie niezawodnie, albowiem liczba $a$ i iloczyn $P$ nie mogą, jak to łatwo stwierdzić możemy, jednocześnie obrócić się w zero.

Oznaczmy przez $(z')$ zbiór, w który przeszedłby zbiór $(z)$ gdybyśmy usunęli z niego jedną liczbę $b$, do niego należącą i zważmy, że liczba $d$ będzie względnie pierwszą w stosunku

do każdej liczby zbioru ($z$), albowiem w przeciwnym przypadku liczba $a$, wbrew założeniu, nie byłaby względnie pierwszą w stosunku do każdej liczby tego zbioru. Z uwagi tej wynika, że:

1° liczba $d$ jest względnie pierwszą w stosunku do każdej liczby zbioru ($z'$)

2° liczba $d$ jest względnie pierwszą w stosunku do liczby $b$.

Z pierwszego z tych wniosków wypływa (tw. poprzedzające), że liczba $d$ jest dzielnikiem liczby $b$. Stwierdzamy więc, że największy wspólny dzielnik $d$ liczby $a$ i iloczynu $P$ byłby wspólnym dzielnikiem liczby $a$ i jednego z czynników $b$ rozważanego iloczynu.

Ponieważ, jakieśmy zaznaczyli przed chwilą, liczby $d$ i $b$ są liczbami pierwszemi pomiędzy sobą, przeto mamy $d = 1$. Zatem największy wspólny dzielnik $d$ liczby $a$ i iloczynu $P$ równa się jedności, czyli liczba $a$ i iloczyn $P$ są liczbami pierwszemi pomiędzy sobą, co było do okazania.

Wniosek. Jeżeli każdy czynnik pewnego iloczynu $P$ jest liczbą względnie pierwszą w stosunku do każdego czynnika pewnego innego iloczynu $P'$, to iloczyny $P$ i $P'$ są liczbami pierwszemi pomiędzy sobą.

Istotnie, na podstawie dowiedzionego przed chwilą twierdzenia, iloczyn $P$ jest liczbą pierwszą w stosunku do każdego czynnika iloczynu $P'$. Z tego zaś wyprowadzamy natychmiast, powołując się powtórnie na wspomniane twierdzenie, wniosek o który chodziło.

§ 50. **Tw. III.** Wszelka liczba całkowita od zera odmienna jest albo liczbą pierwszą albo iloczynem od jedności odmiennych liczb pierwszych, których zbiór określony jest w zupełności w zależności od uważanej liczby.

Dowód. Upewnijmy się na początek, że wszelka liczba całkowita, od zera odmienna, jest albo liczbą pierwszą albo iloczynem liczb pierwszych od jedności odmiennych, nie troszcząc się na razie o to, czy, w drugim przypadku, zbiór odnośnych liczb pierwszych określonym jest w zupełności w zależności od uważanej liczby.

W tym celu załóżmy, że wysłowiona okoliczność zachodzi przy każdej liczbie całkowitej, nie przekraczającej pewną liczbę $n$ od jedności większą i uważajmy liczbę $n+1$. Gdyby liczba $n+1$ liczbą pierwszą nie była, mielibyśmy

$$n+1=a.b \tag{1}$$

oznaczając przez $a$ i $b$ dwie liczby całkowite, sprawdzające nierówności

$$1<a<n+1$$
$$1<b<n+1,$$

czyli:

$$1<a\leqq n \tag{2}$$
$$1<b\leqq n. \tag{3}$$

Na podstawie chwilowo przyjętego założenia i nierówności (2) liczba $a$, jeżeli liczbą pierwszą nie jest, równać się będzie iloczynowi pewnych liczb pierwszych od jedności większych. Ze względu na nierówności (3) toż samo zachodzić będzie co do liczby $b$. Zatem, na podstawie równości (1) liczba $n+1$ byłaby, przy uczynionych założeniach, iloczynem liczb pierwszych od jedności większych. Zważmy teraz, że, jak też natychmiast sprawdzić możemy, chwilowo przyjęte założenie zgadza się z istotnym stanem rzeczy w przypadku szczególnym, kiedy mamy $n=2$. Wnosimy stąd, na podstawie zasady indukcyi matematycznej, że okoliczność, którą chcieliśmy uzasadnić, istotnie zachodzi przy wszelkiej liczbie całkowitej od zera odmiennej.

Winniśmy jeszcze okazać, że zbiór od jedności odmiennych liczb pierwszych, których iloczyn równa się oznaczonej liczbie $a$ (która oczywiście sama liczbą pierwszą być nie może) określony jest w zupełności. W tym celu oznaczmy przez $(z)$ i $(z')$ dwa takie zbiory od jedności odmiennych liczb pierwszych, żeby iloczyn liczb, stanowiących którykolwiek z tych zbiorów, równał się liczbie $a$. Załóżmy, że zbiór $(z)$ zawiera dokładnie $n$ liczb $(n\geqq 1)$ równych pewnej liczbie pierwszej $p$, $(p>1)$. Liczba $a$ będzie tedy podzielną przez $p^n$; a ponie-

waż iloczyn $P'$ liczb stanowiących zbiór $(z')$ równa się liczbie $a$, przeto iloczyn ten także podzielnym będzie przez $p^n$.

Z tego wynika, że zbiór $(z')$ zawierać będzie przynajmniej jedną liczbę równą liczbie pierwszej $p$, gdyby bowiem okoliczność ta nie zachodziła, to, ze względu na tw. II i odnośny wniosek, liczba $p^n$ byłaby w stosunku do iloczynu $P'$ liczbą względnie pierwszą i nie mogłaby, z powodu nierówności

$$p^n > 1,$$

być dzielnikiem tego iloczynu. Jeżeli tedy przyjmiemy

$$P' = p^k \cdot P'_1$$

oznaczając przez $P'_1$ iloczyn od liczby $p$ odmiennych liczb zbioru $(z')$, to będziemy mieli

$$k \geqq 1.$$

Liczba $p^n$ jest (tw. II i odnośny wniosek) liczbą względnie pierwszą w stosunku do iloczynu $P'_1$. Z drugiej strony, jak już mieliśmy sposobność podnieść, liczba $p^n$ jest dzielnikiem liczby $P'$ a więc i iloczynu $p^k \cdot P'_1$. Przeto (tw. I) liczba $p^n$ jest dzielnikiem liczby $p^k$. Ponieważ zaś liczba $p$ jest od liczby jeden większą, przeto wnosimy z poprzedniego, że mamy

$$k \geqq n, \tag{4}$$

w przeciwnym bowiem razie mielibyśmy

$$p^k < p^n$$

i reszta podziału liczby $p^k$ przez liczbę $p^n$ równałaby się samej liczbie $p^k$ i byłaby zatem od zera odmienną.

Ponieważ możemy w rozumowaniu poprzedzającem przemienić role zbiorów $(z)$ i $(z')$, przeto stwierdzamy, że prócz związku (4), mieć jeszcze będziemy

$$n \geqq k. \tag{5}$$

Ze związków (4) i (5) wynika z konieczności równość

$$n = k.$$

Dowiedliśmy więc, że jeżeli jeden ze zbiorów $(z)$ albo $(z')$ zawiera pewną liczbę liczb równych pewnej liczbie pierwszej $p$, to drugi zbiór zawiera tyleż liczb równych tej samej liczbie pierwszej. Zatem zbiory $(z)$ i $(z')$ są identyczne, co pozostawało jeszcze do okazania.

**Tw. IV.** Liczba liczb pierwszych jest nieograniczona. W innych wyrazach: liczba liczb pierwszych jest nieskończona.

Dowód. Ze względu na definicyę (§ 6, Def. XII) liczby „nieskończoność“ powinniśmy tylko dowieść, że, jakąkolwiek liczbę całkowitą oznaczylibyśmy przez $n$ $(n > 1)$, zawsze zdołamy wyznaczyć tyle odmiennych od siebie liczb pierwszych, ile wynosi liczba $n$.

Zagadnienie, polegające na wyznaczeniu $n$ odmiennych od siebie liczb pierwszych, rozwiązać możemy w przypadku szczególnym, kiedy mamy $n = 2$, albowiem liczby $1$ i $2$ są dwie odmienne od siebie liczby pierwsze.

Załóżmy chwilowo, że jesteśmy w stanie wyznaczyć tyle odmiennych od siebie liczb pierwszych, ile wynosi pewna liczba całkowita $k$ $(k > 1)$ i oznaczmy przez $p$ największą z tych $k$ liczb.

Oznaczmy tedy przez $A$ iloczyn wszystkich liczb całkowitych ciągu naturalnego od liczby $1$ do liczby $p$ włącznie i przyjmijmy

$$N = A + 1.$$

Liczba $N$ oczywiście nie posiada żadnego dzielnika większego od jedności i nie przekraczającego liczby $p$. Przeto, gdyby nawet liczba $N$ nie była pierwszą i posiadała zatem dzielniki pierwsze od niej mniejsze ale od jedności większe, to każdy z tych dzielników byłby większym od liczby $p$ a więc odmiennym od każdej z wyznaczonych już $k$ liczb pierwszych. Jeżeli więc dołączymy do wyznaczonych już $k$ odmiennych od siebie liczb pierwszych jeden z dzielników pierwszych od jedności większych liczby $N$, to uzyskamy układ $k + 1$ odmiennych od siebie liczb pierwszych.

Z poprzedniego wnosimy z łatwością, że twierdzenie, które pragnęliśmy uzasadnić, zachodzi istotnie.

§ 51. Przechodzimy obecnie do sprawy wyznaczenia wszystkich liczb pierwszych od jedności większych, nie przekraczających danej liczby całkowitej.

Oczywiście moglibyśmy powyróżniać wszystkie liczby pierwsze z pomiędzy liczb całkowitych nie przekraczających liczbę $a$, stosując kolejno do każdej z tych liczb znane (§ 48) nam już kryteryum następujące: jeżeli pewna liczba nie jest podzielną przez żadną od niej mniejszą ale od jedności większą liczbę, to liczba ta jest liczbą pierwszą. W praktyce jednak posługujemy się metodą szybciej do celu prowadzącą.

Żeby wyznaczyć wszystkie liczby pierwsze, od jedności odmienne, nie przekraczające danej liczby $a$, piszemy w porządku naturalnym ciąg $(C)$ wszystkich liczb całkowitych od liczby $2$ do liczby $a$ włącznie. Następnie wykonywamy pewien ciąg $(W)$ czynności, z których każda polega na stwierdzeniu, czy istnieją w ciągu $(C)$ od pewnej liczby tego ciągu większe wielokrotności tej samej liczby oraz na przekreśleniu tych wielokrotności, jeżeli one istnieją i jeżeli nie zostały już przekreślone przy jednej z czynności poprzedzających; każdą taką czynność nazwiemy dla skrócenia „próbą“ uważanej liczby. Pierwszej próbie podlega liczba $2$ a każdej dalszej — najmniejsza nie próbowana jeszcze i nie przekreślona liczba. Powiadam, że każda próbowana liczba będzie liczbą pierwszą. Istotnie, oznaczmy ogólnie przez $p_k$ liczbę próbowaną przy $k$-tej czynności ciągu $(W)$. W takim razie liczba $p_1$ będzie liczbą pierwszą, albowiem mamy

$$p_1 = 2;$$

jeżeli zaś przyjmiemy $k > 1$, to liczba $p_k$, o ile istnieje, będzie także liczbą pierwszą; rzeczywiście, ponieważ liczba $p_k$ większą jest od wszystkich poprzednio próbowanych liczb, przeto liczba ta jako nie przekreślona przy tych próbach, nie może być podzielną przez żadną z liczb próbowanych przed

nią; z tego zaś oczywiście wynika, że liczba $p_k$ nie może także być podzielną przez żadną z liczb przekreślonych przy próbach poprzedzających; a ponieważ każda liczba od jedności większa a od liczby $p_k$ mniejsza należy do ciągu $(C)$ i jest albo jedną z liczb próbowanych przed liczbą $p_k$ albo jedną z liczb, przy jednej z tych prób przekreślonych, przeto liczba $p_k$ nie jest podzielną przez żadną od niej mniejszą a od jedności większą liczbę; stwierdzamy więc, że, zgodnie z zapowiedzią, liczba $p_k$ jest liczbą pierwszą.

Zważmy teraz, że liczba liczb mogących podlegać omawianym próbom, jako w żadnym razie nie większa od liczby $a - 1$, jest skończoną. Zatem ciąg tych prób może zawsze być posunięty aż do pewnej $n$-tej próby, po której każda nie przekreślona liczba ciągu $(C)$ będzie liczbą próbowaną. Załóżmy, żeśmy wszystkie te próby wykonali. W takim razie zbiór liczb próbowanych stanowić będzie pełny układ liczb pierwszych od jedności większych, nie przekraczających liczby $a$. Istotnie, każda próbowana liczba będzie, jak widzieliśmy, liczbą pierwszą a każda inna liczba, od jedności większa i liczbę $a$ nie przekraczająca, będzie jedną z przekreślonych liczb ciągu $(C)$ i, jako taka, liczbą pierwszą nie będzie.

Poprzedzająca metoda do rozwiązywania zagadnienia wysłowionego na czele tego paragrafu, polega na przekreśleniu drogą kolejnych „prób“ wszystkich tych liczb ciągu $(C)$, które liczbami pierwszemi nie są. Liczbę tych „prób“ możemy zmniejszyć na podstawie uwagi następującej, która i w innych przypadkach użyteczną bywa: powiadam, że wszelka liczba nie pierwsza zawsze posiada jeden przynajmniej od jedności większy dzielnik, którego kwadrat nie jest od niej większym. Istotnie, jeżeli pewna liczba $l$ pierwszą nie jest, to liczba ta może być uważaną za iloczyn dwóch czynników od jedności większych. Oznaczmy te czynniki przez $d$ i $c$, dobierając oznaczenia tak, żebyśmy mieli

$$d \leqq c.$$

Z tej nierówności i z równości:

$$l = d \cdot c$$

wyprowadzamy nierówność

$$d^2 \leqq l,$$

z której powyższa uwaga natychmiast wypływa.

Z uwagi poprzedzającej wynika, ze względu na tw. III, że wszelka liczba $l$, nie pierwsza, podzielną jest przynajmniej przez jedną taką liczbę pierwszą, której kwadrat nie jest od niej większy.

Wracając do sprawy wyznaczenia wszystkich od jedności większych, danej liczby $a$ nie przekraczających, liczb pierwszych, uważajmy, w ciągu czynności czyli „prób“ przepisanych wyżej wyłożoną metodą, próbę jakiegokolwiek $k$-tego rzędu i liczbę $p_k$ mającą próbie tej uledz.

Ponieważ oczywiście liczby próbowane przed liczbą $p_k$ stanowią pełny zbiór od jedności większych ale od liczby $p_k$ mniejszych liczb pierwszych, przeto wszelka liczba $b$ nie pierwsza, do ciągu $(C)$ należąca i przy $(k-1)$ pierwszych próbach nie przekreślona, posiadać może tylko dzielniki pierwsze, nie mniejsze od liczby $p_k$. Zatem liczba $b$, ze względu na uwagę uczynioną wyżej, nie może być mniejszą od kwadratu liczby $p_k$. Gdyby więc kwadrat liczby $p_k$ równał się liczbie większej od ostatniej liczby $a$ ciągu $(C)$, to okoliczność ta byłaby oznaką tego, że wszystkie liczby nie pierwsze do ciągu $(C)$ należące, zostały już przekreślone. Zatem dalsze próby byłyby zbytecznemi.

Możemy więc do omawianej metody wprowadzić ulepszenia następujące: przed każdą próbą przepisaną tą metodą porównywamy kwadrat liczby mającej próbie uledz z ostatnią liczbą $a$ ciągu $(C)$; skoro tylko kwadrat ten okaże się większym od liczby $a$, to sprawa wyznaczenia żądanych liczb pierwszych będzie załatwioną, albowiem wszystkie nie pierwsze liczby ciągu $(C)$ będą już przekreślone.

§ 52. Ważnem ze względu na różne zastosowania jest zagadnienie następujące: rozpoznać, czy dana liczba całkowita

od jedności większa jest liczbą pierwszą i, gdyby pierwszą nie była, przedstawić ją w postaci iloczynu liczb pierwszych.

Celem skrócenia mowy określamy kilka wyrażeń: wyrażenie „czynnik pierwszy“ pewnej liczby $a$ oznacza liczbę pierwszą od jedności większą, przez którą liczba $a$ byłaby podzieloną; „zbiorem czynników pierwszych“, oznaczonej liczbą $a$ ($a > 1$) nazywamy, w przypadku wyjątkowym, kiedy liczba $a$ jest liczbą pierwszą, samą tę liczbę, w przypadku zaś, kiedy uważana liczba liczbą pierwszą nie jest — zbiór, od jedności większych liczb pierwszych, których iloczyn równa się tej liczbie.

Możemy tedy, uwzględniając w § 23 wprowadzoną umowę co do używania wyrazu „iloczyn“, powiedzieć, że każda liczba całkowita od jedności większa równa się iloczynowi swoich czynników pierwszych. Posługując się tą terminologią wysławiamy zagadnienie, postawione przed chwilą, w sposób następujący: rozłożyć daną liczbę całkowitą, od jedności większą, na czynniki pierwsze.

Wiemy już (tw. III), że zagadnienie to ma zawsze jedno i tylko jedno rozwiązanie; chodzi więc tylko o regularną metodę do rozwiązywania tego zagadnienia.

Każda liczba jest przez samą siebie podzielną a liczba dzielników (§ 43) każdej od zera odmiennej liczby jest skończoną, zatem: jakąkolwiek liczbę całkowitą od jedności większą oznaczylibyśmy przez $a$, zawsze istnieć będzie pewien taki, od jedności większy, dzielnik $p$ liczby $a$, żeby liczba ta nie posiadała żadnego od liczby $p$ mniejszego, lecz od jedności większego dzielnika. Liczbę $p$ nazwiemy tedy najmniejszym czynnikiem liczby $a$.

Najmniejszy czynnik jakiejkolwiek od jedności większej liczby $a$ jest zawsze liczbą pierwszą (oczywiście od jedności większą), gdyby bowiem pewien dzielnik $d$ liczby $a$ nie był liczbą pierwszą, gdyby więc liczba $d$ posiadała pewien dzielnik $d_1$ od niej mniejszy ale od jedności większy, to liczba $a$ posiadałaby od jedności większy ale od liczby $d$ mniejszy

dzielnik $d_1$, przeto liczba $d$ nie byłaby najmniejszym czynnikiem liczby $a$.

Najmniejszy czynnnik liczby pierwszej od jedności większej równa się oczywiście samej tej liczbie.

Żeby daną liczbę $a$ $(a > 1)$ rozłożyć na czynniki pierwsze wyznaczamy przedewszystkiem najmniejszy czynnik tej liczby. Oczywiście moglibyśmy wyznaczyć najmniejszy czynnik liczby $a$, próbując kolejno, w porządku naturalnym uważane, liczby całkowite, rozpoczynając te próby od liczby 2.

Metoda, którą posługujemy się w praktyce, jest tylko ulepszoną postacią metody poprzedzającej; ulepszenie polega na tem, że oszczędzamy sobie wszystkich tych prób, co do których à priori stwierdzić możemy, że są zbytecznemi.

W tym względzie korzystamy ze wszystkich wskazówek, które w każdym szczególnym przypadku nam są dostępne a nadto kierujemy się w każdym razie znanemi nam z rozdziału IX cechami podzielności oraz uwagami następującemi:

1) Ponieważ dzielnik, o wyznaczenie którego chodzi, jest liczbą pierwszą, przeto próba każdej liczby, którą poznalibyśmy jako liczbę nie pierwszą, albo na podstawie cech podzielności przytoczonych w rozdz. IX, albo ze znajdującej się w naszem rozporządzeniu tablicy liczb pierwszych, będzie mogła być zaniechaną.

2) Jeżeli przy próbie pewnej liczby $l$, próbie polegającej oczywiście na dzieleniu liczby $a$ przez liczbę $l$, stwierdzimy, że liczba $a$ przez $l$ nie jest podzielna i otrzymamy jednocześnie na całkowitą część ilorazu wartość nie większą od liczby $l$, to tem samem upewnimy się, że liczba $a$ nie posiada żadnego od jedności większego dzielnika, którego kwadrat od niej byłby nie większy. Ponieważ zaś (§ 51) w takim razie mielibyśmy pewność, że liczba $a$ jest liczbą pierwszą, przeto nie zachodziłaby już potrzeba wykonywania dalszych prób.

Jeżeli najmniejszy czynnik liczby $a$ okaże się równym samej liczbie $a$, jeżeli więc stwierdzimy, że liczba $a$ jest liczbą pierwszą, to sprawa rozłożenia liczby tej na czynniki pierwsze będzie oczywiście załatwioną. Pozostaje więc tylko

do omówienia przypadek, w którym, przy wyznaczeniu najmniejszego czynnika uważanej liczby $a$, stwierdzimy, że liczba ta pierwszą nie jest. Oznaczmy przez $n$ liczbę liczb pierwszych, których iloczyn równa się liczbie $a$ i pomyślmy te liczby pierwsze w oznaczonym porządku, mianowicie takim, żeby, oznaczając ogólnie przez $p_i$ liczbę rzędu $i$, stale zachodził związek następujący:

$$p_i \leqq p_{i+1}.$$

Załóżmy chwilowo, żeśmy już wyznaczyli $k$ $(1 \leqq k < n)$, pierwsze liczby z ciągu

$$p_1, p_2, \cdots p_n \qquad (1)$$

i oznaczmy przez $a_k$ iloraz podziału liczby $a$ przez iloczyn wyznaczonych $k$ pierwszych liczb z powyższego ciągu. Przy tych oznaczeniach liczba $p_{k+1}$ będzie, jak to łatwo możemy stwierdzić opierając się na tw. III, najmniejszym czynnikiem liczby $a_k$.

Wyznaczymy tedy liczbę $p_{k+1}$, wyznaczając omówioną wyżej metodą najmniejszy czynnik liczby $a_k$, ale winniśmy dodać, że próby przepisane wspomnianą metodą należy, w obecnym razie, rozpoczynać od liczby w żadnym razie nie mniejszej od liczby $p_k$, albowiem liczba $a_k$ oczywiście nie może być podzielną przez żadną liczbę od liczby $p_k$ mniejszą.

Zważmy, że w razie kiedy mamy $k = 1$, możemy uważać chwilowo wyżej przyjęte założenie za urzeczywistnione istotnie, albowiem posiadamy metodę do wyznaczenia najmniejszego czynnika danej jakiejkolwiek od jedności większej liczby całkowitej, a liczba $p_1$ będzie właśnie tym czynnikiem liczby $a$. Zatem, na podstawie zasady indukcyi matematycznej, wnosimy, że zdołamy wyznaczyć, w sposób omówiony wyżej, kolejno wszystkie liczby ciągu (1). Załatwiliśmy więc sprawę rozkładu danej liczby całkowitej od jedności większej na czynniki pierwsze.

§ 53. Jeżeli zbiór liczb pierwszych, od jedności większych, których iloczyn równa się pewnej liczbie $a$, zawiera dokładnie $k$ $(k \geqq 1)$, liczb równych pewnej liczbie pierwszej $p$,

od jedności większej, to okoliczność tę wysłowiamy krótko, orzekając, iż czynnik pierwszy $p$ wchodzi do liczby $a$ z wykładnikiem $k$, albo w potędze $k$; w przypadku szczególnym, kiedy mamy $k = 1$ i kiedy liczba $a$ jest liczbą pierwszą, orzeczenie poprzedzające wyraża, że liczba $a$ równa się liczbie $p$.

**Tw. V.** Żeby oznaczona liczba $a$ od zera odmienna podzielną była przez oznaczoną liczbę $b$ od jedności większą, koniecznym jest i wystarczającem, żeby każdy czynnik pierwszy liczby $b$ wchodził do liczby $a$ z wykładnikiem nie mniejszym od wykładnika, z którym ten czynnik pierwszy wchodzi do liczby $b$.

Dowód. 1° Podany warunek jest wystarczającym. Istotnie, jeżeli warunek ten jest spełniony, to zbiór czynników pierwszych liczby $b$ albo zlewa się ze zbiorem czynników pierwszych liczby $a$, i w takim razie mamy $a = b$, albo zbiór ten stanowi część zbioru czynników pierwszych liczby $a$, w którym to razie, zastępując w iloczynie czynników pierwszych liczby $a$ czynniki stanowiące zbiór czynników pierwszych liczby $b$ przez tę liczbę, wartości iloczynu nie zmienimy i przedstawimy zatem liczbę $a$ jako iloczyn, którego jeden czynnik równa się liczbie $b$.

Stwierdzamy więc, że w obu tych, jedynie możliwych przypadkach, liczba $a$ rzeczywiście podzielną będzie przez liczbę $b$.

2° Podany warunek jest koniecznym. Zakładamy, że liczba $a$ podzielną jest przez liczbę $b$ i oznaczamy przez $c$ odnośny iloraz. Mamy tedy:

$$a = b \cdot c. \tag{1}$$

Gdyby wyjątkowo liczba $c$ równała się jedności, to zbiór czynników pierwszych liczby $a$ oczywiście zlewałby się ze ze zbiorem czynników pierwszych liczby $b$ i każdy czynnik pierwszy liczby $b$ wchodziłby do liczby $a$ z tym wykładnikiem, z którym on wchodzi do liczby $b$. Gdyby zaś liczba $c$ miała jakąkolwiek wartość od jedności większą, to, ze względu

na równość (1), zbiór czyników pierwszych liczby $a$, który (tw. III) jest określonym w zupełności w zależności od liczby $a$, będziemy mogli uważać za wynik dołączenia do zbioru czynników pierwszych liczby $b$ zbioru czynników pierwszych liczby $c$. Z tego wynika, że w przypadku obecnym każdy czynnik pierwszy liczby $b$ wchodzić będzie do liczby $a$ z wykładnikiem nie mniejszym od wykładnika, z którym czynnik ten wchodzi do liczby $b$. Stwierdzamy więc, że omawiany warunek jest rzeczywiście koniecznym. Uzasadniliśmy więc w zupełności twierdzenie, o które chodziło.

Opierając się na twierdzeniu poprzedzającem, możemy łatwo wyznaczyć wszystkie dzielniki danej liczby całkowitej $a$, od zera odmiennej. Rzeczywiście, zwracając się do przypadku, w którym rozwiązanie nie jest natychmiastowe, w którym więc liczba $a$ nie jest potęgą liczby pierwszej oznaczmy przez

$$p_1, p_2, \cdots p_n$$

układ wszystkich odmiennych od siedie czynników pierwszych liczby $a$ a przez $\alpha_k$, wykładnik, z którym czynnik pierwszy $p_k$ wchodzi do uważanej liczby. Na podstawie twierdzenia poprzedzającego otrzymamy zbiór wszystkich dzielników liczby $a$ ze wzoru

$$p_1^{\beta_1} \cdot p_2^{\beta_2}, \quad \cdots \quad p_n^{\beta_n}$$

przyjmując na wykładniki $\beta_1, \beta_2, \ldots \beta_n$ wszystkie odmienne od siebie układy wartości, przy których dla każdej wartości na wskaźnik $k$ od jedności aż do $n$ zachodzi nierówność.

$$\beta_k \leqq \alpha_k.$$

Czytelnik łatwo stwierdzi, że liczba $x$ dzielników liczby $a$, jeżeli pomiędzy nimi uwzględnimy samą liczbę $a$ i jedności, równa się iloczynowi następującemu:

$$(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_n + 1).$$

**Tw. VI.** Uważajmy tyle liczb całkowitych

$$a_1, a_2, \ldots a_n \qquad (1)$$

od jedności większych ile wynosi pewna liczba całkowita $n$, od jedności większa. Jeżeli nie istnieje żaden czynnik pierwszy, wspólny uważanym liczbom, to największy wspólny dzielnik tych liczb równa się jedności, jeżeli zaś rozważane liczby posiadają przynajmniej jeden wspólny czynnik pierwszy to największy wspólny dzielnik tych liczb jest od jedności większy i równa się liczbie $d$, której wszystkie czynniki pierwsze są czynnikami pierwszymi wspólnymi liczb (1) i wchodzą do tej liczby z wykładnikami, z których każdy równa się najmniejszemu z wykładników, z którymi odnośny czynnik wchodzi do poszczególnych liczb układu (1).

Dowód. Załóżmy, że liczby (1) posiadają jeden przynajmniej wspólny dzielnik $\delta$ od jedności większy. Liczba $\delta$, jako od jedności większa, posiadać będzie (tw. III) jeden przynajmniej czynnik pierwszy. Z drugiej strony, na podstawie tw. V, każdy dzielnik pierwszy liczby $\delta$ wchodzić będzie do każdej z liczb (1) z wykładnikiem nie mniejszym od wykładnika, z którym czynnik ten wchodzi do liczby $\delta$. Z tego wynika przedewszystkiem, że największy wspólny dzielnik liczb (1) równałby się istotnie jedności, gdyby liczby te nie posiadały żadnego wspólnego czynnika pierwszego. Nadto, z tych samych uwag wnosimy, powołując się powtórnie na tw. V, że liczba $\delta$ będzie dzielnikiem liczby $d$ określonej przy wysłowieniu twierdzenia, które pragniemy uzasadnić. Zatem liczby (1) nie posiadają żadnego wspólnego dzielnika, większego od liczby $d$. Ponieważ zaś, znowu na podstawie tw. V, liczba $d$ *jest* wspólnym dzielnikiem liczb (1), przeto liczba ta jest największym wspólnym dzielnikiem uważanych liczb, co pozostawało jeszcze do okazania.

**Tw. VII.** Uważajmy znowu tyle liczb całkowitych

$$(1) \qquad a_1, a_2, \ldots a_n$$

od jedności większych, ile wynosi pewna liczba całkowita $n$. od jedności większa. Najmniejsza wspólna wielokrotność liczb (1) równać się będzie liczbie $w$, której każdy czynnik pierwszy będzie czynnikiem pierwszym jednej przynajmniej z liczb (1)

i wchodzić będzie do liczby $w$ z wykładnikiem równym wykładnikowi, z którym on wchodzi do tej z liczb (1), do której wchodziłby z największym wykładnikiem.

Dowód. Oznaczmy przez $W$ którąkolwiek wielokrotność od zera odmienną liczb (1). Na podstawie tw. V każdy czynnik pierwszy jednej z liczb (1) wchodzić będzie do liczby $W$ z wykładnikiem nie mniejszym od żadnego z wykładników, z którymi on wchodzi do liczb (1). Stąd znowu na podstawie tw. V wnosimy, że liczba $W$ podzielną jest przez liczbę $w$ i dlatego, jako od zera odmienna, od liczby $w$ mniejszą być nie może. Ponieważ zaś z tw. V wynika, że liczba $w$ *jest* wspólną wielokrotnością liczb (1), przeto z poprzedniego wnosimy, że liczba $w$ jest najmniejszą wspólną wielokrotnością liczb (1), co było do okazania.

W praktyce wyznaczamy najczęściej największy wspólny dzielnik kilku liczb albo ich najmniejszą wspólną wielokrotność odpowiednio na podstawie twierdzeń VI i VII.

## XII. Pogląd na cechy ścisłości matematycznej. Trudności połączone z uczeniem i poznawaniem teoryj matematycznych. Wskazówki natury pedagogicznej.

§ 55. Ścisłością jakichkolwiek dociekań nazywamy tę ich właściwość, której mniejszy lub większy stopień gwarantuje nam w mniejszym lub w większym stopniu pewność odnośnych wyników. Ze ścisłością znajduje się w nierozłącznym związku precyzyjność, albowiem oczywiście tylko precyzyjne zdanie, a więc takie, którego treść jest całkiem wyraźna, podlegać może ścisłemu uzasadnieniu. Zatem, orzekając, iż pewna metoda jest ścisłą, orzekamy tem samem, że metoda ta jest precyzyjną.

Ścisłość stanowi właściwą cechę metody naukowej czyli umiejętnej; ona właśnie wyróżnia metodę naukową od metody, którą pospolicie nazywamy „chłopskim rozumem“.

Z poprzedniego wynika, że ścisłość metod naukowych

stanowi właściwe źródło tych trudności, które muszą być pokonane przy poznawaniu i przy uczeniu tych metod. Zatem omawianie reguł pedagogii pewnej nauki z konieczności połączonem być musi ze zbadaniem warunków ścisłości metody tej nauki i połączonych z niemi trudności dla ucznia.

§ 56. Ogólnikowe skreślenie warunków ścisłości matematyki nie przedstawia trudności. Cechy ścisłości matematycznej są ogólnemi cechami ścisłości nauk dedukcyjnych, a w części — nauki wogóle. Ścisłość matematyczna polega na precyzyi języka i na tem, żeby podstawowe pojęcia oraz bez dodowodu przyjęte orzeczenia, czyli aksyomaty, były wyraźnie uwidocznione, żeby o ile możności żaden z aksyomatów nie był konsekwencyą pozostałych, żeby żaden z tychże wątpliwości nie ulegał i żeby nareszcie każde twierdzenie, a więc orzeczenie aksyomatem nie będące, było uzasadnione drogą poprawnie ułożonego układu syllogizmów. Te warunki ścisłości wysławiamy krótko w sposób następujący: ścisłość matematyczna polega na precyzyi języka i na poprawnem uzasadnieniu twierdzeń.

Winniśmy jednak podnieść, że, gdybyśmy chcieli powziąć wyobrażenie o ścisłości matematycznej, poprzestając wyłącznie o ogólnikach poprzedzających, to wyrobilibyśmy sobie o niej bardzo niezupełne pojęcie i nie bylibyśmy w stanie zdać sobie sprawy z trudności, z któremi połączone jest nabywanie i udzielanie wiadomości matematycznych.

Żeby dojść do wyników bardziej zadawalniających, musimy bliżej poznać w jaki sposób, w matematyce, czynimy zadość omówionym ogólnym warunkom ścisłości.

§ 57. Język matematyczny winien być precyzyjnym. Zatem znaczenie każdego wyrazu właściwego matematyce musi być określone odpowiednią definicyą. Należyte rozumienie definicyi bynajmniej dla początkującego łatwem nie jest. Jedno z najważniejszych źródeł trudności w tym względzie jest następujące. Często, drogą definicyi, wprowadzamy do matematyki wyraz używany także w mowie potocznej, nadając mu w takim razie znaczenie mniej lub więcej odmienne od jego

znaczenia w mowie potocznej. Taka zmiana bywa zazwyczaj konieczną albo dla tego, że znaczenie potoczne określonego wyrazu jest chwiejne i nie posiada tem samem należytej precyzyi, albo z tej przyczyny, że, w celu uproszczenia wysławiania się, dogodnem jest zmienić w pewnym stopniu znaczenie rozważanego wyrazu albo nareszcie z obu tych przyczyn. Otóż doświadczenie wykazuje, że uczeń z wielką trudnością przyzwyczaja się w takich przypadkach do dokładnego kojażenia z rozważanym wyrazem albo wyrażeniem znaczenia nadanego mu definicyą. Tak n. p. wyrażenie, „pewna liczba podzielną jest przez pewną inną liczbę“, określiliśmy w ten sposób, że liczba zero powinna być uważaną za liczbę podzielną przez każdą inną liczbę; otóż uczeń nie łatwo pogodzi się z tą konsekwencyą definicyi podzielności.

Często definicya pewnego wyrażenia stanowi konstrukcyę nowego pojęcia. Tu gromadzić się mogą dla ucznia różne trudności. Uczeń nie zawsze łatwo zrozumie, że taka definicya zawiera już w sobie pewne twierdzenie, mianowicie twierdzenie następujące: przedmiot odpowiadający pojęciu, wprowadzonemu rozważaną definicyą, istnieje. Jeżeli n. p. określamy liczbę pierwszą jako liczbę całkowitą, która prócz jedności i samej siebie, żadnego innego dzielnika nie posiada, to tem samem twierdzimy, że liczby takie istnieją. Trudnem może być także dla ucznia przedstawienie sobie przedmiotu, wprowadzonego przez pewną definicyę; okoliczność ta często się nadarza już w elementarnej geometryi.

§ 58. Twierdzenia powinny być poprawnie uzasadnione. Z tą zasadą połączone są dla ucznia bardzo poważne trudności. Konieczność trzymania się jej bynajmniej nie jest dla niego oczywistą; mając bardzo wygórowane pojęcie o wiarogodności intuicyi, byłby on zdania, że orzeczenia, które mu wydają się, oczywistemi powinnyby być przyjęte bez dowodu. W każdym razie żądałby on, żeby treść każdego aksyomatu była łatwo zrozumiała i żeby słuszność każdego z nich była całkiem oczywistą. Rzeczywisty stan rzeczy jest zgoła inny. Treść aksyomatu bywa niekiedy trudniejszą do

zrozumienia, a słuszność jego może wydawać się mniej oczywistą, niż treść i słuszność pewnego twierdzenia. Czytelnik uzna zapewne, że w takiem właśnie przeciwieństwie znajduje się aksyomat, któremu nadaliśmy nazwę zasady indukcyi matematycznej i twierdzenie, które opiewa, że pomiędzy kilkoma nierównemi sobie liczbami całkowitemi znajduje się zawsze pewna liczba najmniejsza i pewna liczba największa. Nie ulega kwestyi, że umówiona okoliczność tak dalece zdaje się być w sprzeczności ze „zdrowym rozumem“,że wytłumaczenie tej okoliczności nie będzie zbytecznem.

Ponieważ, jakieśmy już mieli sposobność nadmienić, historya rozwoju nauk ścisłych poucza, że orzeczenie, których słuszność uważaną była za całkiem oczywistą, okazały się, w pewnych przypadkach, błędnemi, przeto wiarę w nieomylność matematyki bynajmniej nie czerpiemy bezpośrednio stąd, że słuszność orzeczeń przyjętych za aksyomaty jest oczywistą. Prawdziwy stan rzeczy jest następujący: każda teorya matematyczna przedstawia układ orzeczeń tak ze sobą logicznie powiązanych, że upadek jednego z nich pociągnąłby za sobą upadek, jeżeli nie wszystkich innych z tych orzeczeń, to w każdym razie bardzo znacznej ich liczby. Możemy więc powiedzieć, że rzetelność jakiegokolwiek oddzielnie wziętego zdania w teoryi matematycznej, jest łącznie gwarantowaną przez rzetelność wszystkich z rozważanem zdaniem logicznie powiązanych zdań i dla tego wierzymy w matematykę.

Z poprzedniego wynika, że bezpośrednia oczywistość aksyomatów nie jest koniecznym warunkiem ścisłości matematycznej. W rzeczywistości ścisłość matematyczna wymaga, żeby przyjęty układ aksyomatów jak najlepiej nadawał się do koordynacyi orzeczeń, stanowiących odnośną teoryę matematyczną. Zatem, za aksyomaty pewnej teoryi matematycznej nie koniecznie przyjmujemy te prawdy rozważanej teoryi, które wydają się nam najbardziej oczywistemi. Proces ustawiania aksyomatów jest zgoła inny: porównywając orzeczenia poczytywane za najpewniejsze, usiłujemy wykryć takie orzeczenia, które razem wzięte mogłyby być uważane za wspólne

ich źródło. Może się tedy zdarzyć, że pewne z owych najpewniejszych orzeczeń przyjmiemy za aksyomaty, ale często bywa, że za aksyomat przyjmujemy orzeczenie nowe, nie mające cech bezpośredniej oczywistości.

Wnosimy stąd, co zresztą historya nauk ścisłych najzupełniej potwierdza, że układ aksyomatów stanowi w *istocie* swojej (bo szczegóły zależą w pewnej mierze od umysłowości poszczególnych autorów), owoc wiekowego rozwoju nauki i musi z postępem tejże ulegać pewnym wolnym zmianom. Tłómaczymy sobie jednocześnie, dlaczego wiarę w słuszność aksyomatów nabywamy stopniowo przy obeznawaniu się z teoryą, do której one należą. Nareszcie z poprzedzających rozważań wyprowadzamy bardzo ważny dla pedagogii wniosek następujący: należyte zrozumienie aksyomatów matematycznych nastąpić może tylko po poprzedniem obeznaniu się z pewną częścią prawd matematycznych.

§. 59. Jeżeli zastosujemy ogólne rozważania, wyłożone w paragrafach poprzedzających, do teoryi liczb całkowitych, to przyjdziemy do przekonania, że studyowanie teoryi tej wymaga już bardzo znacznego stopnia dojrzałości umysłowej.

Bliższe w tym względzie wskazówki możemy dać opierając się tylko na własnem doświadczeniu nauczycielskiem. Naszem zdaniem arytmetyka teoretyczna, a więc i teorya liczb całkowitych, może być z korzyścią wykładana tylko w najwyższej albo w dwóch najwyższych klasach gimnazyalnych. Ale, jakeśmy zaznaczyli w przedmowie, i w tych nawet klasach całkiem ścisły wykład nie dałby dobrych rezultatów.

Najważniejsze odstąpienie, przez nas zalecane, od ścisłości bezwzględnej polegałoby na pominięciu wykazu aksyomatów i dowodów twierdzeń podanych w rozdz. I. Naszem zdaniem należałoby rozpocząć wykład od teoryi działań zasadniczych, wysławiając przytem wspomniane aksyomaty i twierdzenia jako orzeczenia oczywiste w tych chwilach, kiedy przy wykładzie teoryi musimy powoływać się na nie.

Pozatem sądzilibyśmy, że, wprowadzając pewne niżej mające być omówione zmiany, możnaby trzymać się obecnego

dziełka. W szczególności doradzalibyśmy z naciskiem, żeby teorya numeracyi dziesiętnej wykładaną była, jakeśmy to uczynili w tem dziełku, po teoryi czterech działań zasadniczych. Powszechnie prawie przyjęty w podręcznikach arytmetyki porządek wykładu, polegający na traktowaniu o numeracyi dziesiętnej przed omówieniem teoryi działań zasadniczych, uważamy stanowczo za nielogiczny i niepedagogiczny. Ponieważ bowiem numeracya dziesiętna polega na przedstawieniu liczb całkowitych w postaci sum pewnych iloczynów, przeto, wykładając teoryę numeracyi musimy z konieczności jawnie albo skrycie posługiwać się teoryą działań zasadniczych. Gdybyśmy więc rozpoczęli teoryę liczb całkowitych od numeracyi dziesiętnej, to bylibyśmy zmuszeni wyłożyć jednocześnie skrycie część teoryi działań zasadniczych. Nagromadzilibyśmy tedy dla ucznia na samym wstępie trudności obu tych teoryi z tem jeszcze utrudnieniem, że wprowadzając teoryę działań skrycie, nie moglibyśmy posługiwać się terminologią tej teoryi właściwą i obciążylibyśmy zatem wykład skomplikowanemi zdaniami. W związku z radą poprzedzającą podnosimy, że, naszem zdaniem, należy, nie krępując się, posługiwać się literami do oznaczenia liczb od samego początku teoryi liczb całkowitych; wielokrotnie mieliśmy sposobność upewnić się, że ten sposób postępowania stanowi dla ucznia bardzo wielkie ułatwienie zrozumienia wykładu.

Przechodzimy obecnie do pewnych szczegółów. W dziełku obecnem rozczłonkowaliśmy pojęcia działań zasadniczych do ostatecznego kresu, albowiem wszystkie te pojęcia wyprowadziliśmy z pojęcia dodania jedności do liczby całkowitej. Z tej przyczyny wykład nasz teoryi działań zasadniczych jest bardzo abstrakcyjnym, zbyt abstrakcyjnym dla przeciętnego ucznia gimnazyalnego. Sądzimy więc, że wykład bardziej zbliżony do wykładu poglądowego byłby w gimnazyum odpowiedniejszym. Należałoby więc zastąpić podaną w tekście definicyę sumy przez definicyę następującą: sumą dowolnej liczby liczb nazywamy liczbę przedmiotów, którą zawierałby zbiór uzy-

skany przez połączenie w jeden zbiór zbiorów zawierających odpowiednio tyle przedmiotów, ile wynoszą rozważane liczby. Przyjmując tę definicyę zwolnieni bylibyśmy od właściwego uzasadnienia twierdzenia, które opiewa, że suma kilku liczb. od porządku dodawania nie zależy; należałoby tylko wytłumaczyć, że przy przyjętej definicyi twierdzenie to wyraża tę oczywistą prawdę, iż porządek, w którymbyśmy kolejno dołączali do pewnego zbioru inne zbiory na liczbę przedmiotów, którą zawierałby zbiór uzyskany po złączeniu wszystkich zbiorów, wpływu nie wywiera.

Podobnie, traktując o mnożeniu, możnaby za punkt wyjścia przyjąć sumę o równych sobie składnikach. Tę zaś okoliczność, że zamiana mnożnika i mnożnej na wartość iloczynu nie wpływa, należałoby uzasadnić poglądowo w sposób następujący: uważajmy w płaszczyźnie tablicy $a$ prostych pionowych i $b$ prostych poziomych. Te dwa układy prostych przetną się w pewnej liczbie punktów. Oznaczmy liczbę tę przez $N$. Proste pionowe przecinają każdą prostę poziomą w $a$ punktach. Zatem liczba $N$ równa się sumie tylu składników równych liczbie $a$, ile mamy prostych poziomych. Ponieważ mamy ich $b$, przeto liczba $N$ równa się sumie $b$ składników równych liczbie $a$, czyli

$$N = a \,.\, b.$$

Zważywszy, że proste poziome przecinają każdą prostę pionową w $b$ punktach, stwierdzamy łatwo, że mamy także

$$N = b \,.\, a.$$

Z równości poprzedzających wynika, że:

$$a \,.\, b = b \,.\, a,$$

co było do okazania.

Na zakończenie winniśmy podnieść, że dalecy byliśmy od zamiaru wyczerpującego omówienia sprawy uczenia arytmetyki teoretycznej w zakładach średnich. Właściwy cel tego

rozdziału polegał tylko na tem, żeby usunąć wszelkie nieporozumienia co do naszych poglądów na ten przedmiot i żeby tem samem zapobiedz nieodpowiedniemu posługiwaniu się tym dziełkiem.

Zaremba

ZARYS
TEORYI
LICZB