O rozwiązaniu kongruencyi

$$z^n - ay^n \equiv 0 \pmod{M}.$$

Przez

S. Dicksteina.

(Rzecz przedstawiona na posiedzeniu Wydziału mat.-przyr. w d. 7 listopada 1892 r.; referent czł. Karliński).

W rozprawie „Zasady teoryi liczb Wrońskiego“ [1]) podałem metodę rozwiązywania kongruencyi

$$z^n - ay^n \equiv 0 \pmod{M}. \tag{1}$$

Wartości niewiadomych przedstawia Wroński za pomocą wzorów:

$$y = h\,(1^{k+1})^2 + (-1)^{k+1} + Mi \tag{2}$$

$$z = h + (-1)^{\pi+k}\,\aleph\left[\frac{M}{(1^{k+1})^2}, \pi\right]^{(\pi-1)} + Mj \quad . \quad . \quad . \tag{3}$$

a warunek rozwiązalności kongruencyi (1) pod postacią

$$M = fact\,[a\,(1^{k+1})^{2n} - 1]$$

lub:

$$a\,(1^{k+1})^{2n} - 1 \equiv 0 \pmod{M} \tag{4}$$

[1]) Rozprawy Wydziału mat.-przyr. T. XXIV, str. 91.

Przypominamy, że $1^{k\,|\,1} = 1.2.3 \ldots . k$; funkcya alef $\aleph\left[\frac{M}{(1^{k\,|\,1})^2}, \pi\right]^{(\pi-1)}$ jest licznikiem przedostatniego z reduktów, jakie otrzymujemy, zamieniając ułamek $\frac{M}{(1^{k\,|\,1})^2}$ na ciągły; liczba całkowita k jest rodzajem, liczba całkowita h gatunkiem kongruencyi; i, j są liczby całkowite dowolne.

Warunek (4) należy rozumieć w ten sposób, że, jeżeli można znaleźć wartość całkowitą liczby k, która przy danych wartościach modułu M i reszty a, spełnia ten warunek, to rozwiązania kongruencyi (1) przedstawiają wzory (2) i (3).

Naprzykład dla kongruencyi [1])

$$z^3 - 17y^3 \equiv 0 \pmod{1087}$$

warunek (4) będzie kongruencyą

$$17\,(1^{k\,|\,1})^6 \equiv 1 \pmod{1087}.$$

Dla $k = 2$ jest $(1^{k\,|\,1})^6 = 2^6 = 64$, a ponieważ istotnie

$$17.64 \equiv 1 \pmod{1087},$$

ponieważ dalej:

$$\aleph\left[\frac{1087}{64}, \pi\right]^{[\pi-1]} = 272, \quad \pi = 3,$$

rozwiązania przeto ogólne kongruencyi danej są:

$$y = h - 272 + 1087\,i$$
$$z = 4h - 1 + 1087\,j.$$

Jeżeli niema liczby całkowitej k, czyniącej zadość, przy danych a i M, warunkowi (4), to, według Wrońskiego, kongruencya jest wtedy nierozwiązalna. Ściśle wprawdzie rzecz biorąc, wolno tylko twierdzić, że kongruencya (1) nie jest wtedy rozwiązalną pod postacią wzorów (2) i (3) [2]). Niespełnianie się bowiem warunku (4) przy żadnej wartości całkowitej liczby k nie usuwa wcale możliwości rozwiązań pod inną postacią, co właśnie postaramy się okazać w niniejszym artykule.

Zawdzięczam p. G. Vivanti'emu to spostrzeżenie [3]), że mimo, iż warunkowi (4) nie staje się zadość, kongruencya (1) może być rozwią-

---

[1]) Przykład wzięty z Wrońskiego: Réforme des Mathématiques str. 145.

[2]) W ten sposób należałoby zmienić ostatnie zdanie Nr. 9 w „Zasadach teoryi liczb Wrońskiego". l. c. str. 95.

[3]) Zakomunikowane w liście prywatnym.

zalną. Jako przykład podaje p. Vivanti kongruencyę

$$z^3 - 2y^3 \equiv 0 \pmod{15}.$$

Z warunku (4), oznaczając w nim dla krótkości $(1^{k+1})^3$ przez x, otrzymuje p. Vivanti

$$2x^2 - 1 \equiv 0 \pmod{15}$$

lub, co na jedno wychodzi,

$$x^2 \equiv 8 \pmod{15}.$$

Ponieważ liczba 8 nie jest resztą kwadratową względem modułu 15, niema przeto liczby całkowitej x, czyniącej zadość tej kongruencyi, a zatem i niema liczby całkowitej k, spełniającej warunek (4); gdy tymczasem, jak to łatwo sprawdzić, kongruencyi $z^3 - 2y^3 \equiv 0 \pmod{15}$ czynią zadość układy wartości:

$$y = 2,\ z = 1;\quad y = 7,\ z = 11;\ \text{i t. d.}$$

W odpowiedzi przesłanej p. Vivanti'emu zauważyłem, że gdy w kongruencyi warunkowej położymy nie $(1^{k+1})^3$, lecz $(1^{k+1})^2 = x$, to dla jego przykładu będzie

$$2x^3 - 1 \equiv 0 \pmod{15}$$

a ta kongruencya sprawdza się dla wartości $x \equiv 2$ i $x \equiv 7 \pmod{15}$. Jeżeli we wzorach (2) i (3) napiszemy w miejsce $(1^{k+1})^2$ liczbę 2 lub 7, a liczbę całkowitą k w wykładnikach wyrazu -1 pozostawimy nieoznaczoną, to znajdziemy rozwiązania kongruencyi $z^3 - 2y^3 \equiv 0 \pmod{15}$ pod postacią ogólną

$$y = 2h + (-1)^{k+1},\quad z = h + (-1)^{k+2} \cdot 7$$

lub pod postacią

$$y = 7h + (-1)^{k+1},\quad z = h + (-1)^{k+2} \cdot 2.$$

Można sprawdzić bezpośrednio, że tak jeden jak i drugi z tych układów czyni zadość kongruencyi; dla szczególnych zaś wartości liczb k i h otrzymujemy układy szczególne. Tak n. p. z pierwszego układu dla $h = 8$, $k = 1$ będzie:

$$y \equiv 16 + (-1)^2 \equiv 17 \equiv 2 \pmod{15},\ z \equiv 8 - 7 \equiv 1 \pmod{15},$$

dla $h = 3$, $k = 1$ zaś

$$y \equiv 6 + 1 \equiv 7 \pmod{15},\ z \equiv 3 - 7 \equiv -4 \equiv 11 \pmod{15}$$

są to rozwiązania podane przez p. Vivanti'ego.

Już z tego przykładu widać, że we wzorach (2) i (3) wyraz postaci specyalnej $(1^{k+1})^2$ zastąpić należy wyrazem ogólniejszym. W samej

rzeczy, zastąpmy w tych wzorach $(1^{k+1})^2$ liczbą całkowitą K względnie pierwszą z modułem M, czyniącą zadość kongruencyi warunkowej

$$aK^n - 1 \equiv 0 \pmod{M} \tag{4'}$$

i napiszmy rozwiązania kongruencyi (1) pod postacią

$$y = hK + (-1)^{k+1} + Mi. \tag{2'}$$

$$z = h + (-1)^{\pi+k} \aleph \left[\frac{M}{K}, \pi \right]^{[\pi-1]} + Mj. \tag{3'}$$

Przedewszystkiem sprawdzimy, że wyrażenia (2') i (3') przy warunku (4') zamieniają istotnie kongruencyę daną na tożsamość. Z (2') i (3) mamy bezpośrednio (opuszczając wyrazy podzielne przez M):

$$y^n \equiv h^n K^n + nh^{n-1} K^{n-1}(-1)^{k+1} + \frac{n(n-1)}{1 \cdot 2} h^{n-2} K^{-2} \cdot (-1)^{2[k+1]} + \ldots,$$

$$z^n \equiv h^n + nh^{n-1} (-1)^{\pi+k} \aleph + \frac{n(n-1)}{1 \cdot 2} (-1)^{2[\pi+k]} \aleph^2 + \ldots;$$

dla skrócenia piszemy $\aleph$ zamiast $\aleph \left[\frac{M}{K}, \pi \right]^{[\pi-1]}$.

Stąd:

$$\begin{aligned} z^n - ay^n \equiv\ & h^n (1 - aK^n) \\ & + nh^{n-1} \{ (-1)^{\pi+k} \aleph - a (-1)^{k+1} K^{n-1} \} \\ & + \frac{n(n-1)}{1 \cdot 2} h^{n-2} \{ (-1)^{2[\pi+k]} \aleph^2 - a (-1)^{2[k+1]} K^{n-2} \} \\ & + \ldots\ldots\ldots \end{aligned} \tag{5}$$

Lecz na podstawie warunku (4') jest

$$1 - aK^n \equiv 0 \pmod{M},$$

według zaś określenia funkcyi $\aleph$ i znanej własności ułamków ciągłych jest:

$$\aleph K - MQ = (-1)^{\pi-1}$$

gdzie Q oznacza mianownik reduktu, którego $\aleph$ jest licznikiem. Z ostatniej równości wynika kongruencya

$$\aleph K \equiv (-1)^{\pi-1} \pmod{M},$$

lub

$$(-1)^{\pi+k} \aleph K \equiv (-1)^{k-1} \pmod{M}.$$

Z drugiej strony z warunku (4′) mamy:

$$(-1)^{k-1} a K^{n-1} . K \equiv (-1)^{k-1} \pmod{M}.$$

Odejmując od siebie dwie ostatnie kongruencye i zważając, że liczba K jest pierwszą względem M, znajdziemy

$$(-1)^{\pi+k} \aleph - a(-1)^{k-1} aK^{n-1} \equiv 0 \pmod{M}.$$

Tym samym sposobem dowieść można, że wszystkie współczynniki rozwiązania (5) są $\equiv 0 \pmod{M}$.

Wyrażenia (2′) i (3′) są więc w każdym razie formalnemi rozwiązaniami kongruencyi (1) bez względu na to, czy przez K rozumiemy liczbę całkowitą czy symbol, określony za pomocą warunku (4′). Jeżeli liczba całkowita K istnieje, to (2′) i (3′) dają nam rozwiązania istotne w liczbach całkowitych.

Wywód tych wzorów ogólniejszych od wzorów Wrońskiego jest prosty. Dość bowiem we wzorze (12), podanym w Nr. 7 poprzedniej pracy [1]) założyć $y = hK + (-1)^{k+1}$, aby stąd, gdy K jest liczbą pierwszą względem M, otrzymać kongruencyę warunkową (4′). Wartość zaś na niewiadomą x otrzymujemy bezpośrednio ze wzoru (9) Nr. 7 wspomnianej rozprawy [2]).

Już w tej poprzedniej pracy naszej, mianowicie we wywodzie trzech wzorów teleologicznych (Nr. 7) [3]), wprowadziliśmy [4]) liczbę K ogólniejszą od przyjętej przez Wrońskiego liczby $(1^{k+1})^2$, ale w traktowaniu specyalnych zagadnień poszliśmy za Wrońskim.

Z przedstawienia niniejszego wnieść można, jak sądzimy, że metody Wrońskiego wymagają modyfikacyi we wskazanym kierunku. Już samo pojęcie r o d z a j u kongruencyi stosować się daje tylko do tych przypadków, w których postać szczegółowa $(1^{k+1})^2$ jest wystarczająca [5]).

[1]) Rozprawy Wydz. mat.-przyr. T. XXIV, str. 90.

[2]) Tamże, str. 89 i „Sprostowania".

[3]) Tamże, str. 88 i „Sprostowania".

[4]) Uczynił to przed nami Hanegraef w rozprawie: „Note sur l'équation de congruence $x^m \equiv r \pmod{p}$. Paryż, 1860". Rozważa on wszakże tylko przypadek, kiedy moduł jest liczbą pierwszą.

[5]) Zwrócimy tu za [illegible]skim uwagę na to, że zakładając w kongruencyi (1) $z = xy$, sprowadzamy ją do kongruencyi $x^m \equiv a \pmod{M}$, którą rozwiązawszy, znajdziemy wartości dla y i z, czyniące zadość kongruencyi danej. Ta postać rozwiązań jest mniej ogólna od podanej w tekście, bo tu wartość z jest zawsze wielokrotnością wartości y.