# Zasady teoryi liczb Wrońskiego.

Przez

**S. Dicksteina.**

Rzecz przedstawiona na posiedzeniu Wydz. mat.-przyr. z 1 Lutego 1892; referent czł. Karliński.

Nieśmiertelne dzieło Gaussa „Disquisitiones arithmeticae“, wydane w r. 1801, jest podstawą całego rozwoju teoryi liczb w naszem stuleciu. Późniejsze odkrycia Dirichleta, Kummera i innych, które tak wzbogaciły naukę, są w znacznej części rozwinięciem pomysłów i metod wielkiego matematyka getyngskiego; duch jego nauki panuje, rzec można, dotąd nad poszukiwaniami w dziedzinie arytmetyki wyższej.

Nierzadkie to zjawisko w dziejach wiedzy, że przy wszechwładnem panowaniu pewnego kierunku badań, metody, odmienne od ogólnie przyjętych, nie zdobywają sobie uznania. Zjawisko to powtórzyło się w teoryi liczb z metodami Wrońskiego. Uczony ten w swem dziele: „Introduction à la philosophie des mathématiques“ 1811, w dziesięć lat po wydaniu dzieła Gaussa, ogłosił pomysły swoje w dziedzinie teoryi liczb. W owym czasie, gdy „Disquisitiones“ znane były zapewne nielicznej garstce specyjalistów, gdy teoryja liczb nie wchodziła jeszcze w zakres wykładów uniwersyteckich, Wroński, obeznany dokładnie z odkryciami Gaussa, ocenił ich doniosłość, nazywając teoryję kongruencyj „najpiękniejszem odkryciem, zrobionem w ciągu ostatnich lat pięćdziesięciu



www.rcin.org.pl

w matematyce czystej; epoką, z którą żadna inna w tym okresie równać się nie może“ [1]).

Oddawszy hołd należny genijuszowi Gaussa, nie poszedł wszakże Wroński wprost jego śladami. Już w dziele wyżej wspomnianem, poświęconem przeważnie filozofii matematyki, wyjaśnia on stanowisko teoryi liczb w systemie wiedzy matematycznej i znaczenie jej ogólnych zagadnień, przyczem wypowiada niektóre oryginalne poglądy godne poznania i podaje metodę bardzo ogólną rozwiązywania kongruencyj wszelkiego rzędu i stopnia. Metoda ta, którą w uproszczeniu w Nr. 4 podajemy, nie okazuje się dogodną w zastosowaniu, ale mimo to jest ciekawa, jako charakteryzująca drogę, na jakiej szukał Wroński najogólniejszego traktowania zagadnień matematycznych.

Inne swe badania z teoryi liczb ogłosił Wroński dopiero w r. 1847 w wielkiem dziele „Réforme du savoir humain“, w którego Tomie I poświęca stokilkadziesiąt stronic in folio temu przedmiotowi [2]). Tu punkt wyjścia stanowi kongruencyja $x^m \equiv a \pmod{M}$, a raczej trzy wzory do niej się odnoszące a wyrażające resztę $a$, moduł $M$ i pierwiastek $x$. Wzory te osłonił Wroński pewną tajemniczością, nazwawszy je „wielkiem trzeciem prawem algorytmii“ albo „wielkiem prawem teleologicznem“ i nie podał ich dowodu.

Wykład w „Reformie wiedzy“ stanowił właściwie przygotowanie do wielkiego traktatu, poświęconego specyjalnie teoryi liczb, w której wszystkie prawdy tej nauki miały być przedstawione i uzasadnione, „wszystkie zagadnienia ostatecznie rozwiązane“ [3]). Traktat ten nie ujrzał, niestety, światła dziennego. Mimo to jednak, już z prac poprzednio wymienionych można dokładnie poznać i ocenić pomysły naszego uczonego.

Badania Wrońskiego w dziedzinie teoryi liczb są dziś jeszcze prawie nieznane. Encyklopedyja Montferriera, w której znajdujemy wykład niektórych metod Wrońskiego, bez uzasadnienia atoli trzech wzorów teleologicznych [4]), niewielka nota Hanegraeffa, w której uzasadnienie

---

[1]) Introduction à la philosophie des mathématiques, str. 69.

[2]) Messianisme ou Réforme absolue du savoir humain etc. Paris, 1847. T. I. Réforme des mathématiques, od str. 75 do 255.

[3]) Dzieło to miało być ósmem z rzędu z szeregu wielkich dzieł, zapowiedzianych przez autora mesyanizmu. Porówn. Réforme I, str. 38, 82 i 128.

[4]) A. S. de Montferrier. Encyclopédie mathématique. T. III. Rozdział „Théorie des nombres“.

www.rcin.org.pl

to znajdujemy [1]) i wreszcie broszura Bukatego, poświęcona tymże wzorom [2]); oto jedyne prace, uwzględniające pomysły Wrońskiego; prace te wszakże pozostały, jak się zdaje, bez wpływu. Uczony znawca teoryi liczb Edward Lucas we wstępie historycznym do swojego obszernego dzieła, którego tom I niedawno się ukazał, o Wrońskim wcale nie wspomina [3]). W naszej literaturze o przedmiocie tym żadnej nie ogłoszono pracy.

W obec tego, uważaliśmy za rzecz właściwą poświęcić niniejszą niewielką pracę przedstawieniu i wyjaśnieniu ważniejszych pomysłów i metod Wrońskiego w dziedzinie teoryi liczb, kierując się przeświadczeniem, że te pomysły i metody mają nietylko historyczną wartość, ale że można je i dziś jeszcze stosować z pożytkiem w badaniach arytmetycznych.

## 1. Stanowisko teoryi liczb w systemie matematyki Wrońskiego.

Znaczenie teoryi liczb w systemie matematyki Wrońskiego wynika z jego poglądów filozoficznych na podstawy i zadania tej wiedzy. Nie wdając się tu w szczegółowy rozbiór tej rzeczy, którą zajmujemy się na innem miejscu [4]), powiemy tylko, że według teoryi Wrońskiego, algorytmy tak zwane pierwotne, t. j. działania elementarne, a mianowicie sumowanie (dodawanie i odejmowanie), stopniowanie (potęgowanie i pierwiastkowanie) i reprodukcyja (mnożenie i dzielenie) są co do swej istoty zasadniczo różne. Sumowanie i stopniowanie znajdują się, jak wyraża się Wroński, na przeciwległych biegunach intelektualnych, bo różnorodność ich tkwi w różnych władzach umysłu, które w działaniach tych udział biorą; reprodukcyja zaś zajmuje stanowisko pośrednie [5]). Tę

[1]) Hanegraeff. Note sur l'équation de congruence $x^m \equiv r \pmod{p}$, Paris, 1860.

[2]) A. Bukaty. Déduction et démonstration de trois lois primordiales de la congruence des nombres constituant la troisieme loi de l'Algorithmie donnée par Wroński. Paris, 1873. Dowód ten nie wydaje nam się zupełnie wystarczającym; jest on raczej sprawdzeniem niż dedukcyją wzorów Wrońskiego.

[3]) Edouard Lucas. Théorie des nombres, T. I. Paris, 1891. Préface. Lucas nie wymienia żadnej pracy poświęconej teoryi liczb a wydanej we Francyi od ogłoszenia francuskiego przekładu dzieła Gaussa (1807) aż do ukazania się rozprawy Poinsota: Reflexions sur les principes fondamentaux de la théorie des nombres" (1865). Cytuje bez bliższego wyjaśnienia „Fakultety arytmetyczne" oraz „Prawo najwyższe różnic" Wrońskiego w ustępie o potęgach wielomianów (str. 146).

[4]) S. Dickstein. Pojęcia i metody matematyki T. I. Warszawa, 1891. Wstęp i Rozdział I.

[5]) Upatrujemy pewną analogiję pomiędzy temi poglądami Wrońskiego a matematyka niemieckiego H. Schefflera. Porówn. tego ostatniego: »Die Theorie der Anschauung oder die mathematischen Gesetze«, Lipsk 1876, § 3, oraz »Die Grundlagen der Wissenschaft«. Lipsk 1889, str 159 i dalsze.

www.rcin.org.pl

różnorodność możemy sobie wyjaśnić na tej podstawie, że w samej rzeczy sumowanie samo przez się nie mogłoby doprowadzić do uważania ciągłości, która w algorytmii występuje dopiero po wprowadzeniu działań pozostałych. Sumowanie odnosi się przedewszystkiem do dziedziny wielkości przerywanych, stopniowanie z reprodukcyją odtwarzają nam ciągłość. Pierwsze, jak mówi Wroński, mieści w sobie pojęcie skończoności, w drugiem tkwi pojęcie nieskończoności [1]).

Stanowisko pośrednie algorytmu reprodukcyi pomiędzy algorytmami sumowania i stopniowania wyrażają dwa następujące związki:

$$A + B = M \,.\, N, \quad M \,.\, N = R^{\varepsilon},$$

stanowiące właściwy przedmiot teoryi liczb [2]).

Badanie takich związków ma jednak w tej nauce charakter odmienny niż w pozostałych gałęziach algorytmii. W tych ostatnich, przy szukaniu liczb, które czynią zadość pewnym związkom, nie stawiamy żadnych ograniczeń; liczby mogą być całkowite lub ułamkowe, wymierne i niewymierne, algebraiczne i przestępne, albo wyrażając się językiem dzisiejszych badań, dziedzinę liczb uważamy za continuum. W teoryi liczb przeciwnie; dziedzinę badań ograniczamy, specyjalizujemy, przyjmując do niej tylko liczby całkowite lub wymierne. Ztąd to, jak powiada Wroński, liczby nieznane, stanowiące przedmiot teoryi liczb, w skutek teleologizmu lub celowości, która jest ich charakterem wyróżniającym, nie ulegają prawu ciągłości, lecz podporządkowują się wyłącznie pod „prawo odosobnienia“ (loi d'isolement) albo „prawo szczególności“ (loi de singularité).

Ten szczególny charakter zagadnień teoryi liczb uwydatnił Wroński w metodach swoich rozwiązywania kongruencyj, a to przez wprowadzenie dwu liczb charakterystycznych, a mianowicie r o d z a j u (genre) i g a t u n k u (espèce). Odpowiedni wybór tych liczb w badaniach teoretyczno-liczbowych zakreśla granice, w których zmieniają się elementa zagadnień. Znaczenie liczb charakterystycznych podamy niżej (7).

## 2. Funkcyje alef.

Funkcyje alef odgrywają ważną rolę w wielu badaniach analitycznych Wrońskiego. Ponieważ algorytmom tym poświęciliśmy kilka

---

[1]) Réforme I. Système architectonique de l'Algorithmie, str. 65.

[2]) „Introduction etc“, str. 64.

[3]) „Réforme etc.“, str. 206.

www.rcin.org.pl

dawniejszych artykułów [1]), ograniczamy się tu przeto tylko do przytoczenia określeń i twierdzeń potrzebnych, w celu zrozumienia dalszego ciągu.

W teoryi liczb Wrońskiego występują funkcyje alef w dwojakiej postaci:

1) w formie:

$$\aleph\left[\frac{S}{R},\omega\right]^{(0)},\ \aleph\left[\frac{S}{R},\omega\right]^{(1)},\ \ldots\ \aleph\left[\frac{S}{R},\omega\right]^{(k)},\ \ldots\ ;$$

są one tu licznikami kolejnych reduktów, jakie otrzymujemy, zamieniając ułamek $\frac{S}{R}$ na ułamek ciągły. Jeżeli szereg ilorazów całkowitych, jakie przy tej zamianie znajdujemy, oznaczymy przez

$$a_1, a_2, \ldots a_k, \ldots a_\omega,$$

wtedy powyższe funkcyje alef czynić będą zadość związkom postaci

$$\aleph^{(0)} = 1, \quad \aleph^{(k)} = a_k\ \aleph^{(k-1)} + \aleph^{(k-2)}$$
$$k = 1, 2 \ldots \omega.$$

2) Jako funkcyje symetryczne pewnych elementów $n_1, n_2, \ldots n_\omega$. Podnosząc sumę $n_1 + n_2 + \ldots + n_\omega$ do potęgi $k$-ej i kładąc następnie jedności w miejsce współczynników rozwinięcia, otrzymujemy funkcyję alef, którą Wroński oznacza przez

$$\aleph\,[n_1 + n_2 + \ldots + n_\omega]^{(k)}.$$

Jeżeli $n_1, n_2, \ldots n_\omega$ uważać będziemy za pierwiastki równania stopnia $\omega$-go postaci:

$$x^\omega - A_1 x^{\omega-1} + A_2 x^{\omega-2} - A_3 x^{\omega-3} \ldots + (-1)^\omega A_\omega = 0,$$

wtedy można będzie, jak to z teoryi funkcyj symetrycznych wiadomo, wyrazić funkcyje alef za pomocą współczynników tego równania. Używając formy wyznacznikowej, możemy napisać:

$$\aleph\,[n_1 + n_2 + \ldots + n_\omega]^{(k)} = \begin{vmatrix} A_1, & A_2, & A_3 \ldots & A_k \\ 1, & A_1, & A_2 \ldots & A_{k-1} \\ 0, & 1, & A_1 \ldots & A_{k-2} \\ \cdot & \cdot & \cdot & \cdot \\ 0, & 0 \ldots & 1, & A_1 \end{vmatrix}$$

[1]) Pamiętnik Akademii Umiejętności w Krakowie, Tom XII (1886) i XVI (1888).

www.rcin.org.pl

Jeżeli sumę $n_1 + n_2 + \ldots + n_\omega$ oznaczymy przez $N$, wtedy na podstawie określenia funkcyj alef z łatwością okazać można prawdziwość wzoru następującego:

$$\aleph[N_\omega - n_p]^{(m)} - \aleph[N_\omega - n_q]^{(m)} = (n_q - n_p)\ \aleph[N_\omega]^{(m-1)},$$

w którym $n_p$ i $n_q$ są dwa którekolwiek z elementów $n_1, n_2, \ldots n_\omega$.

W dziele z r. 1811 nazywa Wroński wzór ten prawem „ogólnem i podstawowem“ teoryi liczb [1]). Opiera on na nim pojęcie kongruencyj i metody ich rozwiązywania, jak to zaraz pokażemy. Dodamy tu jeszcze, że wzór ten wyraża też według Wrońskiego zasadę rozkładu liczb na czynniki. Ponieważ różnica funkcyj $\aleph[N_\omega - n_p]^{(m)}$ i $\aleph[N_\omega - n_q]^{(m)}$ przy odpowiednim doborze elementów $n$ może wyrażać liczbę jakąkolwiek, strona przeto druga powyższego wzoru przedstawia możność istnienia czynnika $n_q - n_p$ tej liczby. W przypadku, gdy $n_q - n_p$ może mieć wartości jedynie równe jedności, uważana liczba jest liczbą pierwszą.

## 3. Kongruencyje.

Od ostatniego wzoru, podanego w poprzednim numerze, przechodzi Wroński do pojęcia kongruencyi [2]), którą według niego wyraża zupełna tożsamość budowy liczb $\aleph[N_\omega - n_p]^{(m)}$ i $\aleph[N_\omega - n_q]^{(m)}$. Liczby te, po podzieleniu przez $n_q - n_p$, którą nazywamy modułem, dają oczywiście reszty równe. Kongruencyją przedstawiamy według Gaussa w postaci:

$$\aleph[N_\omega - n_p]^{(m)} \equiv \aleph[N_\omega - n_q]^{(m)} \pmod{n_q - n_p}\ [3]).$$

Ogólna postać kongruencyj jest następująca:

$$F_1(A, B, C, \ldots) \equiv F_2(A, B, C \ldots) \pmod{f(A, B, C \ldots)},$$

gdzie $F_1$, $F_2$, $f$ są dowolnemi funkcyjami elementów $A, B, C \ldots$ Do badania takich kongruencyj sprowadza się ostatecznie zadanie teoryi liczb.

Wroński klasyfikuje kongruencyje [4]) według rzędu nieoznaczoności; t. j. według liczby ilości nieoznaczonych (niewiadomych) i według ich stopnia. Kongruencyje rzędu pierwszego mają postać:

$$A_1 + B_1 x \equiv A_2 + B_2 x \pmod{A + Bx},$$

---

[1]) Introduction str. 67. Prostszy dowód znaleść można w „Pojęciach i metodach matematyki“, T. I, str. 217.

[2]) „Introduction etc.“ str. 69.

[3]) Wroński pisze właściwie w ten sposób $A \equiv B$ (mod. $= M$), nie zaś $A \equiv B$ (mod. $M$).

[4]) Introduction etc. str. 141.

www.rcin.org.pl

jeżeli są stopnia pierwszego;

$$A_1+B_1x+C_1x^2 \equiv A_2+B_2x+C_2x^2 \text{ (mod. } A+Bx+Cx^2),$$

jeżeli są stopnia drugiego;

$$A_1+B_1x+C_1x^2+\ldots+K_1x^m \equiv A_2+B_2x+C_2x^2+\ldots+K_2x^m$$
$$\text{(mod. } A+Bx+Cx^2+\ldots+Kx^m),$$

jeżeli są stopnia $m$-go i t. d.

Kongruencyje rzędu drugiego mają postać:

$$A_1+B_1x_1+C_1x_2 \equiv A_2+B_2x_1+C_2x_2 \text{ (mod. } A+Bx_1+Cx_2),$$

jeżeli są stopnia pierwszego;

$$A+Bx_1+Cx_2+Dx_1^2+Ex_1x_2+Fx_2^2 \equiv A_2+B_2x_1+C_2x_2+D_2x_1^2$$
$$+E_2x_1x_2+F_2x_2^2 \text{ (mod. } A+Bx_1+Cx_2+Dx_1^2+Ex_1x_2+Fx_2^2)$$

jeżeli są stopnia drugiego, i t. d.

Z określenia kongruencyj wynikają następujące ich własności zasadnicze:

1) Jeżeli $A \equiv B \text{ (mod. } M)$,

to

$$A+\alpha M \equiv B+\beta M \text{ (mod. } M),$$

gdzie $\alpha$ i $\beta$ są dowolnemi liczbami całkowitemi.

2) Jeżeli

$$A_1 \equiv B_1, \quad A_2 \equiv B_2, \quad A_3 \equiv B_3, \ldots \text{ (mod. } M),$$

to:

$$\Omega_1 A_1^{\alpha_1}+\Omega_2 A_2^{\alpha_2}+\Omega_3 A_3^{\alpha_3}+\ldots \equiv \Omega_1 B_1^{\beta_1}+\Omega_2 B_2^{\beta_2}+\Omega_3 B_3^{\beta_3}+\ldots$$

gdzie $\alpha_1, \alpha_2, \alpha_3 \ldots \beta_1, \beta_2, \beta_3 \ldots$ są liczbami całkowitemi dowolnemi, zaś $\Omega_1, \Omega_2, \Omega_3 \ldots$ liczbami całkowitemi dodatniemi lub ujemnemi.

Metoda rozwiązania kongruencyj rzędu pierwszego i stopnia pierwszego, podana przez Wrońskiego, oparta jest na własnościach funkcyj alef w postaci pierwszej (Nr. 2), a więc nie różni się w istocie od metody podanej przez Eulera, Lagrangea i Gaussa [1]). Jeżeli daną jest kongruencyja postaci

$$Ax+B \equiv 0 \text{ (mod. } M),$$

to rozwiązanie jej przedstawia Wroński w postaci

$$x = (-1)^{\omega} B \cdot \aleph\left[\frac{B}{A}, \omega\right]^{\omega-1} + M_i$$

gdzie $i$ jest dowolną liczbą całkowitą.

---

[1]) »Introduction etc.« str. 266—269, Réforme, str. 105. Porówn. Disquisitiones Gaussa art. 27.

www.rcin.org.pl

Metoda ta stanowi zresztą przypadek szczególny metody ogólniejszej, którą zaraz przedstawimy.

## 4. Metoda ogólna rozwiązywania kongruencyj (dawniejsza).

Metoda dawniejsza (z r. 1811) [1]) polega, jak to już wyżej powiedziano, na sprowadzeniu kongruencyi danej do postaci wzoru:

$$(1) \qquad \aleph\,[N_\varepsilon - n_p]^{(m)} - \aleph\,[N_\omega - n_q]^{(m)} = (n_q - n_p)\,\aleph\,[N_\omega]^{(m-1)}.$$

Niechaj będzie kongruencyja rzędu pierwszego i stopnia, dajmy na to, $n^{go}$

$$X_1 \equiv X_2 \pmod{X},$$

gdzie więc $X_1$, $X_2$, $X$ są funkcyjami całkowitemi stopnia $n$-go o współczynnikach całkowitych.

Oznaczając przez $\zeta_1$ i $\zeta_2$ dwie liczby całkowite nieoznaczone, możemy na podstawie własności, podanych w Nrze poprzedzającym, napisać

$$X_1 + \zeta_1 X \equiv X_2 + \zeta_2 X \pmod{X}.$$

Uczyńmy:

$$(2) \qquad \begin{aligned} X_1 + \zeta_1 X &= \aleph\,[N_\omega - n_q]^{(m)}, \\ X_2 + \zeta_2 X &= \aleph\,[N_\omega - n_p]^{(m)}, \\ X &= n_p - n_q; \end{aligned}$$

wtedy, na mocy wzoru (1), będzie

$$(3) \qquad X \cdot \aleph\,[N_\omega]^{(n-1)} = X_1 - X_2 + (\zeta_1 - \zeta_2)\,X.$$

Niechaj elementy $n_1, n_2, \ldots n_{\omega-2}, n_p$ w liczbie $\omega - 1$ będą pierwiastkami równania

$$(4) \qquad x^{\omega-1} - P_1 x^{\omega-2} + P_2 x^{\omega-3} - \ldots + (-1)^{\omega-1} P_{\omega-1} = 0;$$

elementy zaś $n_1, n_2, \ldots n_{\omega-2}, n_q$ także w liczbie $\omega - 1$ pierwiastkami równania

$$(5) \qquad x^{\omega-1} - Q_1 x^{\omega-2} + Q_2 x^{\omega-3} - \ldots + (-1)^{\omega-1} Q_{\omega-1} = 0.$$

Na zasadzie własności funkcyj alef drugiej postaci (Nr. 2) będzie:

$$(6) \qquad \begin{aligned} \aleph\,[N_\omega - n_q]^{(s)} &= P_s, \\ \aleph\,[N_\omega - n_p]^{(s)} &= Q_s, \end{aligned}$$

---

[1]) Introduction str. 146—151.

www.rcin.org.pl

$$\aleph[N_\omega - n_q]^{(m)} = X_1 + \zeta_1 X = \begin{vmatrix} P_1, & P_2 \ldots & P_m \\ 1, & P_1 \ldots & P_{m-1} \\ \cdot & \cdot \cdot \cdot & \cdot \\ 0, & 0 \ldots & P_1 \end{vmatrix} \tag{7}$$

$$\aleph[N_\omega - n_q]^{(m)} = X_1 + \zeta_2 X = \begin{vmatrix} Q_1, & Q_2 \ldots & Q_m \\ 1, & Q_1 \ldots & Q_{m-1} \\ \cdot & \cdot \cdot \cdot & \cdot \\ 0, & 0 \ldots & Q_1 \end{vmatrix} \tag{8}$$

Z równań (6), przy uwzględnieniu ostatniego z równań (2), otrzymujemy:

$$Q_1 - P_1 = X. \tag{9}$$

Ponieważ równania (4) i (5) mają $\omega - 2$ pierwiastków wspólnych $n_1, n_2 \ldots n_{\omega-2}$, więc pomiędzy ich współczynnikami zachodzić musi $\omega - 2$ związków, które na podstawie teoryi eliminacyi łatwo otrzymać można. Napiszmy je w postaci:

$$F_\mu(P_1, P_2 \ldots P_{\omega-1}, Q_1, Q_2 \ldots Q_{\omega-1}) = 0 \tag{10}$$

$$\mu = 1, 2 \ldots \omega - 2.$$

Wroński mówi tylko o zachodzeniu jednego tylko związku postaci (10). Mamy zatem pomiędzy $2\omega - 2$ współczynnikami $P$, $Q$ związki (7), (8), (9), (10), czyli razem $\omega + 1$ równań, tak, że możemy $\omega + 1$ z tych współczynników wyznaczyć za pomocą $\omega - 3$ pozostałych, które pozostają nieoznaczonemi [1]). Mając wyrażenia współczynników, rozwiązujemy jedno z równań (4) lub (5) i znajdujemy elementy $n_1, n_2, \ldots n_\omega$. Tworzymy z tych elementów wyrażenie $\aleph[N_\omega]^{m-1}$ i podstawiamy w równanie (3). Z tego równania znajdziemy wyrażenie liczby szukanej $x$. Ze względu na nieoznaczoność $\omega - 3$ współczynników, możemy jednemu lub kilku z elementów $n_1, n_2, \ldots n_\omega$ nadać wartości całkowite dowolne i takie, aby $\aleph[N_\omega]^{m-1}$ i wyrażenie szukanej $x$ były liczbami całkowitemi.

Taż sama metoda może być stosowaną i do kongruencyj wyższych rzędów, jeżeli liczba kongruencyj danych równa się liczbie niewiadomych.

Metoda ta w zastosowaniu nie jest dogodną. Przedewszystkiem, liczba elementów $\omega$ i stopień $m$ funkcyi alef nie są z góry dane i w każdym danym przypadku należy te dwie liczby odpowiednio do postaci kongruencyi dobierać. Przy niewysokim nawet stopniu równań (4) i (5)

[1]) Błędnie podaną w tekscie Philosophie des mathématiques str. 149 liczbę $2(\omega - 3)$ zamiast $\omega - 3$. Wroński w „Erratach“ zmienił na właściwą, pozostawiwszy wszakże bez zmiany to, że zachodzi tylko jeden związek postaci (10).



www.rcin.org.pl

eliminacyja w układzie, złożonym z równań (7), (8), (9), (10), może nie być łatwą, rozwiązanie jednego z równań (4) lub (5) — trudne; wreszcie zadośćuczynienie warunkom całkowitości wyrażenia szukanej $x$ wymaga nowego dochodzenia. Z tych zapewne powodów, Wroński do metody tej w późniejszych badaniach swych nie powrócił, obmyśliwszy metodę inną, wymagającą tylko rachunków elementarnych.

## 5. Twierdzenia Fermata i Wilsona.

Twierdzenia te wyraża Wroński w jednym wzorze ogólnym postaci: [1])

$$(1) \qquad (a\omega+1)^{k\,|\,1}.\,(b\omega+1)^{\omega-k-1\,|\,1}+(-1)^k x^{\omega-1} \equiv 0 \pmod{\omega}$$

w którym $\omega$ jest liczbą pierwszą, $a$ i $b$ dowolnemi liczbami całkowitemi, $x$ liczbą całkowitą niepodzielną przez $\omega$, $k$ liczbą całkowitą, przybierającą wartości $0, 1, 2 \ldots \frac{\omega-1}{2}$. Liczba $k$ stanowi tu „rodzaj“ kongruencyi. Czynniki pierwszego wyrazu strony pierwszej są faktoryjalne, mające znaczenie następujące:

$$(2) \qquad \begin{aligned} (a\omega+1)^{k\,|\,1} &= (a\omega+1)(a\omega+2)\ldots(a\omega+k) \\ (b\omega+1)^{\omega-k-1\,|\,1} &= (b\omega+1)(b\omega+2)\ldots(b\omega+\omega-k-1) \end{aligned}$$

Wzór (1), jako charakteryzujący wyłącznie liczby pierwsze $\omega$, nazywa Wroński „istotną zasadą teleologiczną liczb pierwszych.“

Z łatwością możemy uzasadnić wzór ten (którego dowód Wroński pominął), opierając się na twierdzeniach Fermata i Wilsona, z których pierwsze wyraża się, jak wiadomo, wzorem

$$(3) \qquad x^{\omega-1} \equiv 1 \pmod{\omega},$$

drugie zaś wzorem

$$(4) \qquad 1.2.3\ldots(\omega-1) \equiv -1 \pmod{\omega}.$$

Napisawszy kongruencyją (4) w postaci

$$1.2.3\ldots(\omega-1) \equiv (\omega-1) \pmod{\omega},$$

i dzieląc obie jej strony przez $\omega-1$, otrzymujemy:

$$1.2.3\ldots(\omega-2) \equiv 1 \pmod{\omega}$$

Mnożąc obie strony tej kongruencyi przez $-2$, pisząc po drugiej stronie $\omega-2$ zamiast $-2$ i dzieląc następnie obie strony przez $\omega-2$, znajdujemy:

$$1.2.1.2.3\ldots(\omega-3) \equiv -1 \pmod{\omega}.$$

---

[1]) Réforme, str. 166.

www.rcin.org.pl

Mnożąc tu obie strony przez $3$, pisząc po stronie drugiej $\omega-3$ zamiast $-3$ i skracając przez $\omega-3$, otrzymujemy:

$$1.2.3.1.2.3\ldots(\omega-4)\equiv 1 \pmod{\omega}..$$

W ten sam sposób postępując dalej, dochodzimy do związku

$$1.2.3\ldots k.1.2.3\ldots(\omega-k-1)\equiv(-1)^{k-1} \pmod{\omega} \quad (5)$$

$$k = 0,\ 1,\ 2\ldots\frac{\omega-1}{2}$$

Zauważmy dalej, że dla dowolnych liczb całkowitych $a$ i $b$ zachodzą kongruencyje

$$1\equiv a\omega+1,\ 2\equiv a\omega+2,\ 3\equiv a\omega+3,\ldots,\ k\equiv a\omega+k \pmod{\omega}$$

$$1\equiv b\omega+1,\ 2\equiv b\omega+2,\ 3\equiv b\omega+3,\ldots,\omega-k-1\equiv b\omega+\omega-k-1 \pmod{\omega}$$

Uwzględniając te związki i równania (2), możemy zamiast (5) napisać

$$(a\omega+1)^{k\,|\,1}.(b\omega+1)^{\omega-k-1\,|\,1}\equiv(-1)^{k-1} \pmod{\omega}. \quad (6).$$

Jeżeli do kongruencyi (6) dodamy kongruencyję (3), po pomnożeniu obu stron tej ostatniej przez $(-1)^k$, otrzymamy wzór Wrońskiego (1).

Wzór (5), który można napisać tak:

$$1^{k\,|\,1}\ 1^{\omega-k-1\,|\,1}\equiv(-1)^{k-1} \pmod{\omega}$$

wynika oczywiście ze wzoru (1) przy założeniu $a=0$, $b=0$, $x=1$; kładąc tu jeszcze $k=\frac{\omega-1}{2}$, otrzymujemy znane twierdzenie

$$\left(1.2.3\ldots\frac{\omega-1}{2}\right)^2\equiv(-1)^{\frac{\omega+1}{2}} \pmod{\omega}. \quad (7)$$

Wzory Fermata i Wilsona wyprowadza Wroński metodą Gaussa [1]), przyjmując tylko nieco ogólniejszy punkt wyjścia. Gauss, wychodząc z równości

$$s=n_1+n_2+\ldots+n_x,$$

podnosi obie jej strony do potęgi $\omega$ i dochodzi do kongruencyi

$$s^\omega\equiv n_1^\omega+n_2^\omega+\ldots+n_x^\omega \pmod{\omega};$$

Wroński zamiast potęg używa faktoryjalnych, t. j. kładzie

$$s^{\omega\,|\,\mu\omega}\equiv\{n_1+n_2+\ldots+n_x\}^{\omega\,|\,\mu\omega}$$

---

[1]) Gauss. Disquisitiones art. 51, 76; Wroński. Réforme, str. 171—173.

www.rcin.org.pl

i dochodzi do kongruencyi

$$s^{\omega} \mid \mu\omega \equiv n_1{}^{\omega} \mid \mu\omega + n_2{}^{\omega} \mid \mu\omega + \ldots + n_x{}^{\omega} \mid \mu\omega \pmod{\omega}.$$

Założywszy w tej ostatniej $n_1 = n_2 = \ldots = n_x = n$, znajduje

$$(xn)^{\omega} \mid \mu\omega \equiv x\,(n)^{\omega} \mid \mu\omega \pmod{\omega},$$

co sprowadzić można do wzoru

$$(xn + \mu\omega)^{\omega-1} \mid \mu\omega - (n + \mu\omega)^{\omega-1} \mid \mu\omega \equiv 0 \pmod{\omega}$$

z którego przy $\mu = 0$ wynika twierdzenie Fermata.

Twierdzenie Wilsona wyprowadza z poprzedzającego sposobem Gaussa.

## 6. Prawo wzajemności liczb pierwszych.

Prawo wzajemności liczb pierwszych co do reszt kwadratowych uważa Wroński za prosty wynik z twierdzenia Fermata.

Jeżeli daną jest kongruencyja $m$-go stopnia

$$x^m \equiv q \pmod{p},$$

gdzie $p$ i $q$ są liczbami pierwszemi, to kongruencyja ta wtedy tylko jest możliwą, jeżeli $q$ jest resztą potęgi $m$-ej względem liczby $p$. Podnieśmy obie strony do potęgi $(p-1)$-ej, t. j. napiszmy

$$(x^{p-1})^m \equiv q^{p-1} \pmod{p}$$

i dajmy, że $d$ jest największym wspólnym dzielnikiem liczb $p-1$ i $d$. Kładąc $\frac{m}{d} = r$, możemy poprzedzającą kongruencyję napisać tak:

$$[x^{(p-1)r}]^d \equiv \left(q^{\frac{p-1}{d}}\right)^d \pmod{p}.$$

Według twierdzenia Fermata, jeżeli $x$ jest liczbą niepodzielną przez $p$, jest:

$$x^{p-1} \equiv 1 \pmod{p},\ x^{(p-1)r} \equiv 1 \pmod{p},$$

będzie przeto:

$$\left(q^{\frac{p-1}{d}}\right)^d - (1)^d \equiv 0 \pmod{p}.$$

Rozkładając stronę pierwszą, jako różnicę potęg, na iloczyn

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

www.rcin.org.pl

i oznaczając czynnik drugi, według przyjętego znakowania, przez

$$\aleph\left[q^{\frac{p-1}{d}}+1\right]^{(d-1)},$$

otrzymujemy

$$\left(q^{\frac{p-1}{d}}-1\right)\aleph\left[q^{\frac{p-1}{d}}+1\right]^{(d-1)} \equiv 0 \pmod{p}.$$

Tak więc kongruencyja dana $x^m \equiv q \pmod{p}$ rozkłada się na dwie kongruencyje

$$q^{\frac{p-1}{d}}-1 \equiv 0 \pmod{p},$$

$$\aleph\left[q^{\frac{p-1}{d}}+1\right]^{(d-1)} \equiv \pmod{p}.$$

Jeżeli staje się zadość pierwszej, wtedy liczba $q$ jest resztą potęgi $m$ względem liczby $p$ i kongruencyja $x^m \equiv q \pmod{p}$ jest możliwą; jeżeli staje się zadość drugiej, wtedy liczba $q$ nie jest resztą potęgi $m$ względem liczby $p$ i kongruencyja $x^m \equiv q$ jest niemożliwą [1]).

W przypadku $m = 2$, jest $d = 2$ i obie kongruencyje warunkowe przyjmują postać

$$q^{\frac{p-1}{2}}-1 \equiv 0 \pmod{p}, \quad q^{\frac{p-1}{2}}+1 \equiv 0 \pmod{p} \qquad (1)$$

Jeżeli staje się zadość pierwszej, $q$ jest resztą kwadratową, jeżeli drugiej — nie jest resztą kwadratową względem liczby $p$. Podobnież liczba $p$ będzie resztą lub nieresztą kwadratową liczby $q$, stosownie do tego, czy zachodzi pierwsza lub druga z kongruencyj:

$$p^{\frac{q-1}{2}}-1 \equiv 0 \pmod{q}, \quad p^{\frac{q-1}{2}}+1 \equiv 0 \pmod{q}. \qquad (2)$$

Prawo wzajemności liczb pierwszych Legendre'a wyraża, że gdy obie liczby $p$ i $q$ lub jedna z nich jest postaci $4n+1$, wtedy pierwszej z kongruencyj (1) odpowiada pierwsza z kongruencyj (2), drugiej zaś druga; gdy zaś obie liczby są postaci $4n+3$, wtedy pierwszej z kongruencyj (1) odpowiada druga z kongruencyj (2), drugiej zaś pierwsza.

Dowód ścisły tej wzajemności nie był rzeczą łatwą i wymagał nie małego kunsztu matematycznego, dzięki któremu Gauss dał sześć różnych dowodów twierdzenia Legendre'a. Późniejsi matematycy wymyślili

[1]) Réforme, str. 175.

www.rcin.org.pl

wiele innych dowodów [1]) tego ważnego twierdzenia, Wroński odmiennie zapatruje się na ten przedmiot. Widzi on w prawie wzajemności liczb pierwszych co do reszt kwadratowych tylko „fragment“ licznych twierdzeń, które na podstawie zasadniczych własności kongruencyj, a głównie trzeciego prawa zasadniczego, (o którem będzie mowa w Nrze następnym), otrzymać można. Pod tym względem winniśmy przyznać słuszność słowom Wrońskiego. Co się zaś tyczy samego dowodu prawa wzajemności odnośnie do reszt kwadratowych, to Wroński opiera go jedynie na rozkładzie pierwszych stron kongruencyj Fermata

$$p^{q-1} \equiv 1 \pmod{q}, \qquad q^{p-1} \equiv 1 \pmod{p}$$

na czynniki w sposób następujący:

Zakładając we wzorze 1 Nr. 5 najprzód $a=1$, $p=1$, $x=p$, $\omega=p$, $k=\frac{p-1}{2}$, następnie $a=1$, $b=1$, $x=q$, $\omega=p$, $k=\frac{q-1}{2}$ i stosując wzór (7) tegoż Nru, otrzymuje z łatwością

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

(3)

$$\left\{p^{\frac{q-1}{2}} - (-1)^{\frac{q+1}{2}}\right\}\left\{p^{\frac{q-1}{2}} + (-1)^{\frac{q+1}{2}}\right\} \equiv 0 \pmod{q}.$$

Te dwie kongruencyje zachodzą zawsze jednocześnie, dzięki temu, że w każdym danym przypadku jeden z czynników strony pierwszej każdej z nich, t. j. albo czynnik pierwszy, albo czynnik drugi, staje się $\equiv 0$, według odpowiedniego modułu. Pozostaje zatem tylko rozstrzygnąć pytanie, który z czynników drugiej kongruencyi staje się $\equiv 0 \pmod{q}$, jeżeli jeden z czynników pierwszej staje się $\equiv 0 \pmod{p}$ i odwrotnie. Wroński rozstrzyga to pytanie za pomocą następującego rozumowania, które, gdyby było a priori przekonywającem — a takiem nie jest ono, zdaniem naszem — uczyniłoby jego dowód prawa wzajemności jednym z najprostszych, jakie dotąd ogłoszono. Twierdzi on mianowicie, że, „w systemie wzajemności, jakie tworzą kongruencyje (3) jest rzeczą widoczną, że aby obie mogły sprawdzać się jednocześnie, musi to stawać się za pomocą czynników przeciwległych, gdyż w razie

[1]) Rozbiór historyczno-krytyczny wszystkich znanych dowodów prawa wzajemności liczb pierwszych odnośnie do reszt kwadratowych znaleść można w rozprawie Oswalda Baumgarta, Ueber das quadratische Reciprocitätsgesetz (Zeitschrift für Mathematik und Physik, XXX, 1885. Historisch-literarische Abtheilung. Prac Wrońskiego Baumgart nie zna.

www.rcin.org.pl

przeciwnym jeden z czynników byłby zbytecznym, co się sprzeciwia naturze twierdzenia Fermata, w którem mamy dwa czynniki“ [1]. Po tej uwadze ustanawia Wroński wzajemność

$$\begin{aligned} q^{\frac{p-1}{2}} \mp (-1)^{\frac{p+1}{2}} &\equiv 0 \pmod{p} \\ p^{\frac{q-1}{2}} \pm (-1)^{\frac{q+1}{2}} &\equiv 0 \pmod{q} \end{aligned} \qquad (4)$$

i rozważa następujące trzy przypadki:

1) Obie liczby $p$ i $q$ mają postać $4n+3$; wtedy z kongruencyi (4) otrzymujemy wprost:

$$q^{\frac{p-1}{2}} \mp 1 \equiv 0 \pmod{p} \qquad p^{\frac{q-1}{2}} \pm 1 \equiv 0 \pmod{q}.$$

2) Jedna z liczb jest postaci $4n+1$, druga postaci $4n+3$; wtedy otrzymujemy:

$$q^{\frac{p-1}{2}} \mp 1 \equiv 0 \pmod{p}, \quad p^{\frac{q-1}{2}} \mp 1 \equiv 0 \pmod{q}.$$

3) Obie liczby są postaci $4n+1$; wtedy kładzie Wroński:

$$(-1)^{\frac{p+1}{2}} = \left[(-1)^2\right]^{\frac{2n_1+1}{2}} = (\sqrt{1})^{2n_1+1}$$

$$(-1)^{\frac{q+1}{2}} = \left[(-1)^2\right]^{\frac{2n_2+1}{2}} = (\sqrt{1})^{2n_2+1};$$

i dla utrzymania owego „przeciwieństwa systematycznego kongruencyj“ (3), przyjmuje w jednej z ostatnich dwóch równości $\sqrt{1}$ ze znakiem dodatnim, w drugiej z ujemnym, przez co dochodzi do kongruencyj

$$q^{\frac{p-1}{2}} \mp 1 \equiv 0 \pmod{p}, \quad p^{\frac{q-1}{2}} \mp 1 \equiv 0 \pmod{q}.$$

## 7. Trzy prawa teleologiczne.

Jeżeli dana jest kongruencyja

$$x^m \equiv a \pmod{M},$$

---

[1]) Oto jego słowa (Réforme, str. 178): „Or dans le système de reciprocité que forment les présentes congruences déterminées, il est manifeste que, pour pouvoir être réalisées à la fois, elles doivent l'être généralement par leurs facteurs opposés parce que, dans le cas contraire, l'un de leurs facteurs systématiques serait superflu; ce qui est contraire à la nature du théorème de Fermat qui se décompose nécessairement en ses deux facteurs.“

www.rcin.org.pl

to związek pomiędzy modułem $M$, resztą $a$ i pierwiastkiem $x$ wyrażają następujące trzy wzory, podane przez Wrońskiego bez dowodu [1]):

$$(1)\quad a=(-1)^{\omega+s}\left\{h(1^{k|s})^2+(-1)^{k+s}\right\}^m \aleph\left[\frac{M}{(1^{k|s})^{2m}},\ \omega\right]^{(\omega-s)}+Mi$$

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

$$(3)\quad M=\text{fact.}\left[a(1^{k|s})^{2m}-\left\{h(1^{k|s})^2+(-1)^{k+s}\right\}^m\right].$$

Ostatnie równanie oznacza, że moduł $M$ ma być czynnikiem wyrażenia, zawartego w nawiasie [ ]; $i$, $j$ są liczbami całkowitemi dowolnemi. Szczególnie ważne znaczenie mają liczby całkowite $k$ i $h$. Pierwsza z nich, nazwana r o d z a j e m, może przybierać w ogóle wartości całkowite $0, 1, 2 \ldots \frac{M-1}{2}$, gdy $M$ jest liczbą pierwszą; gdy zaś $M$ jest liczbą złożoną, to liczba $k$ zmienia się w ogóle od $0$ do liczby równej połowie zmniejszonego o jedność najmniejszego dzielnika prostego liczby $M$. Liczba $h$, zwana g a t u n k i e m, może przyjmować w ogóle wszystkie wartości całkowite od $0$ do $M-1$ lub też wartości całkowite dodatnie i ujemne, nie przechodzące połowy modułu. Liczby te w metodach Wrońskiego, jak to zaraz zobaczymy, służą nie tylko do otrzymywania różnych rozwiązań kongruencyj, ale zarazem i do wykrywania niemożliwości rozwiązań.

W dowodzie powyższych wzorów korzystamy z noty Hanegraeffa [2]).

Niechaj będzie dana kongruencyja stopnia $m$-go

$$(4)\qquad x^m \equiv a \pmod{M}.$$

Badanie tej kongruencyi sprowadzamy do badania dwóch kongruencyj stopnia pierwszego w sposób następujący:

Niechaj $K$ będzie liczba całkowita, pierwsza względem modułu $M$ i czyniąca zadość kongruencyi

$$(5)\qquad a\,K^m \equiv (-1)^{(k+1)m} \pmod{M}$$

gdzie $k$ jest liczbą całkowitą, mogącą przyjmować wartości w granicach wyżej wskazanych.

---

[1]) Réforme, str. 81. W dziele z r. 1811 tych wzorów jeszcze nie ma.

[2]) Hanegraeff, l. c.

[3]) Réforme, str. 82.

www.rcin.org.pl

Mnożąc obie strony kongruencyi (4) przez $K^m$, otrzymujemy, na podstawie związku (5):

$$(Kx)^m \equiv (-1)^{(k+1)m} \pmod{M}$$

zkąd

$$Kx \equiv (-1)^{k+1} \pmod{M} \tag{6}$$

kongruencyje (5) i (6) zastępują kongruencyję daną (4); w samej rzeczy, jeżeli zachodzą kongruencyje (5) i (6), to musi zachodzić kongruencyja (4); i naodwrót, jeżeli zachodzi kongruencyja (4), to przy określeniu liczby $K$ za pomocą związku (5), musi zachodzić i związek (6).

Rozwiązując kongruencyję (5) względem liczby $a$, uważanej za niewiadomą, na podstawie wzoru podanego w końcu Nr. 3, otrzymujemy:

$$a = (-1)^{\omega} . (-1)^{m(k+1)-1} \aleph \left[ \frac{M}{K^m}, \omega \right]^{(\omega-1)} + Mi$$

lub (7)

$$a = (-1)^{\omega+1} \{(-1)^{k+1}\}^m \aleph \left[ \frac{M}{K^m}, \omega \right]^{(\omega-1)} + Mi;$$

rozwiązując zaś kongruencyję (8) względem ilości $x$, znajdujemy na podstawie tego samego wzoru:

$$x = (-1)^{\pi+k} \aleph \left[ \frac{M}{K}, \pi \right]^{(\pi-1)} + Mj \tag{8}$$

Przyjmijmy teraz ogólniej

$$x = h + (-1)^{\pi+k} \aleph \left[ \frac{M}{K}, \pi \right]^{(\pi-1)} + Mj, \tag{9}$$

gdzie $h$ jest liczbą całkowitą, zmieniającą się od $0$ do $M-1$, i zobaczmy, jaką postać odpowiednią przyjmuje reszta $a$. Ponieważ wartość $x-h$, wzięta z wzoru (9), czyni oczywiście zadość kongruencyi (6), gdy w niej zamiast $x$ napiszemy $x-h$, będzie zatem

$$K(x-h) \equiv (-1)^{k+1} \pmod{M},$$

zkąd

$$Kx \equiv [hK + (-1)^{k+1}] . \pmod{M}.$$

Ta kongruencyja różni się od kongruencyi (6) tem, że w niej zamiast $(-1)^{k+1}$ mamy $hK + (-1)^{k+1}$; w skutek tej zmiany, kongruencyja (5) przybierze postać

$$aK^m \equiv [hK + (-1)^{k+1}]^m \pmod{M}, \tag{10}$$



www.rcin.org.pl

ztąd zaś otrzymamy nową wartość reszty:

$$a=(-1)^{\omega+1}\left\{hK+(-1)^{k+1}\right\}^m \aleph\left[\frac{M}{K},\ \omega\right]^{(\omega-1)}+Mi \qquad (11)$$

Z kongruencyi (10) widzimy bezpośrednio, że różnica

$$aK^m-\left\{hK+(-1)^{k+1}\right\}^m$$

jest podzielna bez reszty przez liczbę $M$, albo innemi słowy, że liczba $M$ jest dzielnikiem tej różnicy, co możemy napisać w ten sposób:

$$M=\text{fact}\cdot\left[aK^m-\left\{hK+(-1)^{k+1}\right\}\right]^m \qquad (12)$$

Nie uczyniliśmy dotąd żadnego założenia o postaci liczby $K$, która to postać jest w pewnej mierze dowolną. Wroński przyjmuje

$$K=(1.2.3\ldots k)^2=(1^{k\,|\,1})^2. \qquad (13)$$

Wprowadzając tę wartość we wzory (9), (10), (12), otrzymamy bezpośrednio wzory zasadnicze (1), (2) i (3).

Wzory te wyrażają związki, jakie istnieć muszą pomiędzy elementem kongruencyi danej (4) dla wszelkich rodzajów i gatunków. Ze względu na te związki, kongruencyja (4) przyjąć może postać ogólniejszą

$$X(k,\ h)^m \equiv A(k,\ h) \pmod{M},$$

gdzie właśnie zależność reszty i pierwiastka od liczb $k$ i $h$ jest zaznaczoną; gdzie więc

$$A(k,\ h)=(-1)^{\omega+1}\left\{h\,.\,(1^{k\,|\,1})^2+(-1)^{k+1}\right\}^m \aleph\left[\frac{M}{(1^{k\,|\,1})^{2m}},\omega\right]^{(\omega-1)}+Mi,$$

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

Zakładając $h=0$, otrzymujemy

$$A(k,\ 0)=(-1)^{(k+1)m+\omega+1}\aleph\left[\frac{M}{(1^{k\,|\,1})^{2m}},\ \omega\right]^{(\omega-1)}+Mi,$$

$$X(k,\ 0)=(-1)^{\pi+k}\aleph\left[\frac{M}{(1^{k\,|\,1})^2},\ \pi\right]^{(\pi-1)}+Mj,$$

ztąd zaś

$$A(k,\ h)=(-1)^{(k+1)m}.\,A(k,\ 1)\left\{h\,.\,(1^{k\,|\,1})^2(-1)^{k+1}\right\}^m+Mi,$$

$$X(k,\ h)\ =\ h+X(k,\ 0).$$

www.rcin.org.pl

Mając zatem dla danego rodzaju resztę i pierwiastek przy wartości gatunku $h=0$, możemy z łatwością znaleźć wyrażenia reszty z pierwiastka dla każdej innej wartości gatunku.

Wzory zasadnicze (1), (2), (3) stanowią główną podstawę, na której opiera Wroński metody rozwiązania kongruencyj wszelkiego rzędu i stopnia.

## 8. Metoda rozwiązania kongruencyj.

$$x^m \equiv a \pmod{M}.$$

Niechaj będzie kongruencyja

$$x^m \equiv a \pmod{M}, \tag{1}$$

w której reszta $a$ i moduł $M$ są liczbami danemi; szukamy wartości pierwiastka $x$.

Na podstawie wzoru zasadniczego (3) w Nrze poprzedzającym, będzie

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

Należy tu oznaczyć stałe $k$ i $h$ z danych liczb $a$ i $M$. Według wzoru (4) w Nrze poprzedzającym, liczba $a$ powinna dać się wyrazić w postaci:

$$a=(-1)^{\omega+1}\left\{h(1^{k+1})^2+(-1)^{k+1}\right\}^m \aleph\left[\frac{M}{(1^{k+1})^{2m}},\ \omega\right]^{(\omega-1)}+Mi;$$

oznaczając przeto dla krótkości

$$\left\{h(1^{k+1})^2+(-1)^{k+1}\right\}^m \text{ przez } H,$$

$$\aleph\left[\frac{M}{(1^{k+1})^{2m}},\ \omega\right]^{(\omega-1)} \text{ przez } N,$$

będziemy mieli

$$a=(-1)^{\omega+1} HN+Mi,$$

zkąd

$$(-1)^{\omega} a+HN \equiv 0 \pmod{M}. \tag{3}$$

Liczba $a$ jest dana, $H$ — niewiadoma; rozwiązując tę kongruencyję względem $H$, znajdziemy na podstawie wzoru w N-rze 3:

$$H=(-1)^{\omega+\rho}\, a\,.\, \aleph\left[\frac{M}{N},\ \rho\right]^{(\rho-1)}+Mi \tag{4}$$

www.rcin.org.pl

Jeżeli przy pomocy tego wzoru, na liczbę $H$ otrzymamy zupełną potęgę pewnej liczby całkowitej $R$, t. j. jeżeli

$$H = R^m + Mj, \tag{5}$$

w takim razie będzie

$$h\,(1^{k+1})^2 + (-1)^{k+1} \equiv R \pmod{M}.$$

Tę kongruencyją możemy rozwiązać względem szukanej liczby $h$, i znajdziemy

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

a wstawiając tę wartość w wyrażenie (2), otrzymamy

$$x = (-1)^{\pi+1}\,R\,.\,\aleph\left[\frac{M}{(1^{k+1})^2},\ \pi\right]^{(\pi-1)} + Mj. \tag{6}$$

Jeżeli z wzoru (3) nie otrzymujemy wprost na $H$ zupełnej potęgi $R^m$, w takim razie potęgi tej szukamy na mocy związku (5), t. j. szukamy liczby $R$, czyniącej zadość kongruencyi

$$R^m \equiv H \pmod{M}$$

i do rozwiązania tej kongruencyi używamy metody, dopieroco stosowanej. Postępowanie to powtarzamy dopóty, dopóki nie dojdziemy do zupełnej potęgi $m$-ej, lub do reszty raz już poprzednio otrzymanej. Oznaczając przez $H$, $H_1$, $H_2$ ... $H_\mu$ ... szereg kolejnych reszt, przez $R$, $R_1$ ... $R_\mu$ szereg odpowiadających im pierwiastków, otrzymamy oczywiście związki następujące:

$$H_\mu = H_{\mu-1}\,(-1)^{\omega+\rho}\,\aleph\left[\frac{M}{N},\ \rho\right]^{(\rho-1)} + Mi,$$

$$R_{\mu-1} = R_\mu\,(-1)^{\pi+1}\,\aleph\left[\frac{M}{(1^{k+1})^2},\ \pi\right]^{\pi-1} + Mj,$$

ztąd przez kolejne podstawienia znajdziemy

$$H_\mu = a\left\{(-1)^{\omega+\rho}\,\aleph\left[\frac{M}{N},\ \rho\right]^{(\rho-1)}\right\}^\mu + Mi,$$

$$x = R_\mu\left\{(-1)^{\pi+1}\,\aleph\left[\frac{M}{(1^{k+1})^2},\ \pi\right]^{\pi-1}\right\}^\mu + Mj,$$

gdzie $H_\mu = R_\mu^m + Mi$.

Jeżeli dla danego rodzaju $k$ otrzymujemy szereg reszt peryjodyczny, w takim razie stosujemy powyższe postępowanie do innego ro-

www.rcin.org.pl

dzaju. Jeżeli różne liczby rodzajowe oznaczymy przez $k_1, k_2, \ldots k_\nu \ldots$, odpowiadające im wyrażenie $N$, t. j.

$$\aleph\left[\frac{K}{(1^{k_\nu}|^1)^{2m}}, \omega_\nu\right]^{(\omega_\nu-1)} \text{ przez } N_\nu,$$

i wprowadzimy prócz tego oznaczenia

$$\begin{aligned} P_\nu &= (-1)^{\omega_\nu+\rho_\nu}\aleph\left[\frac{M}{N_\nu}, \rho_\nu\right]^{(\rho_\nu-1)}, \\ Q_\nu &= (-1)^{\pi_\nu+1}\aleph\left[\frac{M}{(1^{k_\nu}|^1)^2}, \pi_\nu\right]^{(\pi_\nu-1)}; \end{aligned} \tag{7}$$

w takim razie z uwagi, że

$$R_\mu = H_\mu^{\frac{1}{m}} = a\, P_1^{\mu_1}\, P_2^{\mu_2}\, P_3^{\mu_3} \ldots,$$

znajdziemy:

$$x = \left[a\left\{P_1^{\mu_1}\, P_2^{\mu_2}\, P_3^{\mu_3}\ldots\right\} + Mi\right]^{\frac{1}{m}} \cdot \left\{Q_1^{\mu_1}\, Q_2^{\mu_2}\, Q_3^{\mu_3}\ldots\right\} + Mj \tag{8}$$

To wyrażenie pierwiastka możemy jeszcze przekształcić na zasadzie następującego spostrzeżenia. Z postaci wyrażenia $N_\nu$ wynika, że jest ono pierwiastkiem kongruencyi

$$N_\nu (1^{k_\nu|^1})^{2m} + (-1)^\omega \equiv 0 \pmod{M};$$

rozwiązując zaś tę kongruencyję względem $(1^{k_\nu|^1})^{2m}$, otrzymamy

$$(1^{k_\nu|^1})^{2m} = (-1)^{\omega+1}\aleph\left[\frac{M}{N_\nu}, \rho_\nu\right]^{(\rho_\nu-1)} + Mj.$$

Widzimy więc, że $(1^{k_\nu|^1})^{2m} \equiv P_\nu \pmod{M}$ tak, że w równaniu (7) możemy $P_\nu$ zastąpić przez $(1^{k_\nu|^1})^{2m}$, skutkiem czego znajdziemy następujące wyrażenie pierwiastka kongruencyi danej:

$$x \equiv \left[a(1^{k_1|^1})^{2m\mu_1}.(1^{k_2|^1})^{2m\mu_2}.(1^{k_3|^1})^{2m\mu_3}\ldots Mi\right]^{\frac{1}{m}} Q_1^{\mu_1}\, Q_2^{\mu_2}\, Q_3^{\mu_3}\ldots \pmod{M}. \tag{9}$$

Wzór (9) przedstawia najogólniejszą postać rozwiązania kongruencyi (1). Możnaby się łatwo przekonać, że formalnie wyrażenie (9) czyni zadość kongruencyi danej bez względu na to, czy kongruencyja dana jest rozwiązalna w liczbach całkowitych czy nie. Faktyczne zaś rozwiązania otrzymamy, jeżeli znajdziemy takie wartości liczb $k$ i $\mu$, przy których wyrażenie zawarte w nawiasie jest potęgą $m$-ą liczby całkowitej. Przy danych wartościach liczebnych modułu $M$ i reszty $a$ rachunek ten wykonywa się przy pomocy działań elementarnych, przyczem stosować

www.rcin.org.pl

można rozmaite ułatwienia. Ponieważ wykładamy tu tylko zasady, przeto nie załączamy przykładów liczebnych, obficie w dziele Wrońskiego podanych [1]).

Powiemy jeszcze, że w szczególnym przypadku, gdy liczba czynników w wyrażeniu (9) sprowadza się do jedności, t. j. gdy dostateczna uważać jeden tylko rodzaj $k$, będzie

$$(10)\quad x \equiv [a(1^{k+1})^{2m\mu} + Mi]^{\frac{1}{m}} \cdot (-1)^{\pi+1} \aleph \left[\frac{M}{(1^{k+1})^2}, \pi\right]^{\pi-1} \pmod{M}$$

Kwestyi co do liczby różnych rozwiązań kongruencyi (1) Wroński nie rozbiera szczegółowo, podając tylko następujące uwagi: [2])

Ze związku (3), gdy w nim zamiast $H$ równego $\{h(1^{k+1})^2 + (-1)^{k+1}\}^m$ napiszemy $J^m$, mamy

$$(-1)^\omega a + NJ^m \equiv 0 \pmod{M};$$

związek zaś (5) doprowadza podobnie do kongruencyi

$$(-1)^\omega a + NR^m \equiv 0 \pmod{M}.$$

Z tych dwóch związków otrzymujemy

$$J^m - R^m \equiv 0 \pmod{M}.$$

Strona pierwsza w przypadku wykładnika parzystego rozkłada się w sposób następujący:

$$(J^2 - R^2)(J^{m-2} + A_1 J^{m-4} + \ldots\ldots A_m) \equiv 0 \pmod{M},$$

w przypadku zaś $m$ nieparzystego, w ten sposób:

$$(J - R)(J^{m-1} + B_2 J^{m-4} + \ldots\ldots + B_m) \equiv 0 \pmod{M}.$$

W pierwszym przypadku mamy dwa pierwiastki $+R$ i $-R$; istnienie innych pierwiastków zależy od równania

$$J^{m-2} + A_1 J^{m-4} + \ldots\ldots + A_m = 0,$$

pierwiastkom urojonym tego równania odpowiadać będą rozwiązania niemożliwe kongruencyi danej.

---

[1]) Dla ułatwienia tych rachunków, Wroński (Réforme, str. 110 i nast.) wprowadza liczby $R_\mu$, które są resztami liczb $(1^{k(\epsilon)})^{2mp}$ względem modułu $M$, liczby $S_\mu$, będące takiemiż resztami liczb $Q_\mu$, wreszcie liczby $T_\mu$ będące resztami liczb $R_\mu$. Prócz tego umieszcza w swojem dziele tablicę potęg od pierwszej do szóstej włącznie wszystkich liczb całkowitych od 1 do 100 (str. 130).

[2]) Réforme, str. 128—129; 250—251. Przedmiot ten miał być traktowany obszernie w zapowiedzianym traktacie.

www.rcin.org.pl

W drugim przypadku, prócz pierwiastka $+R$, o istnieniu innych rozstrzyga równanie

$$J^{m-1} + B_1 J^{m-2} \ldots\ldots + B_m = 0,$$

którego pierwiastkom urojonym odpowiadają również rozwiązania niemożliwe kongruencyi danej.

## 9. Metoda rozwiązania kongruencyi rzędu drugiego

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

Stosując do kongruencyi

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

wzór zasadniczy (3), Nr. 7, przy założeniu

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

otrzymujemy

$$M = \text{fact.} \{ a(1^{k+1})^{2n} - 1 \}, \tag{3}$$

jako warunek jej możliwości; pierwszy zaś z wzorów zasadniczych tegoż Nru daje

$$z = h + (-1)^{\pi+1} \aleph \left[ \frac{M}{(1^{k+1})^2}, \pi \right]^{\pi-1} + Mj. \tag{4}$$

Wzory (2) i (4) przedstawiają rozwiązanie kongruencyi danej. Z warunku zaś (3) napisanego w postaci:

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

kładąc w nim kolejno za $k$ wartości $0, 1, 2 \ldots$ znajdziemy te wartości liczby rodzajowej, którym odpowiada rozwiązanie kongruencyi. Jeżeli przy żadnej wartości $k$ nie spełnia się ten warunek, kongruencyja jest nierozwiązalną.

## 10. Rozkład liczb całkowitych na czynniki.

Sławne w teoryi liczb zagadnienie rozkładu liczb całkowitych na czynniki, rozwiązuje Wroński na podstawie teoryi, podanej w Nrze poprzedzającym [1]).

Dajmy, że mamy rozłożyć na czynniki liczbę $M$. Napiszmy kongruencyję

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

[1]) Réforme, str. 143 i dalsze.

www.rcin.org.pl

będzie zatem, według Nru poprzedzającego:

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

$$y=h(1^{k+1})^2+(-1)^{k+1}+Mj'';$$

lub wprowadzając oznaczenie

$$Q=(-1)^{\pi+1}\,\aleph\left[\frac{M}{(1^{k+1})^2},\ \pi\right]^{(\pi-1)},$$

$$z=h-(-1)^k\,Q+Mj' \tag{2}$$

$$y=h\,(1^{k+1})^2-(-1)^k+Mj''. \tag{3}$$

Według warunku (3) w poprzedzającym numerze, jest

$$a\,(1^{k+1})^{2n}-1\equiv 0\ (\text{mod. } M),$$

zkąd

$$a=(-1)^{\omega+1}\,\aleph\left[\frac{M}{(1^{k+1})^{2n}},\ \omega\right]^{(\omega-1)}+Mi.$$

Jeżeli liczba $a$ jest resztą potęgi $m$-ej względem modułu $M$, t. j. gdy czyni zadość kongruencyi

$$x^n\equiv a\ (\text{mod. } M),$$

w takim razie, na podstawie wzoru (10) w Nrze 7, możemy napisać:

$$x=[a\,(^{k+1})^{2n\mu}+Mi]^{\frac{1}{n}}\cdot Q^{\mu}+Mj. \tag{4}$$

Z drugiej strony kongruencyja (1) przyjmuje postać

$$z^n-(xy)^n\equiv 0\ (\text{mod. } M).$$

Strona pierwsza rozkłada się tu na czynniki. Jednym z czynników jest $z-xy$, kładąc więc za $x$ i $y$ wartości z wzorów (2) i (3), otrzymujemy czynnik szukany w postaci:

$$[h-(-1)^k\,Q+Mj'']-x\,[h\,(1^{k+1})^2-(-1)^k+Mj''],$$

lub

$$\{1-x\,(1^{k+1})^2\}\,h+(-1)^k\,(x-Q).$$

Oznaczając

$$\begin{aligned}1-x\,(1^{k+1})^2&=A,\\ x-Q&=B,\end{aligned} \tag{5}$$

znajdujemy następujące wyrażenie czynnika liczby $M$:

$$Ah+(-1)^k\,B,$$

www.rcin.org.pl

gdzie $A$ i $B$ mają znaczenie, określone wzorami (5), $x$ zaś wyraża się wzorem (4).

## 11. Rozwiązywanie kongruencyj

$$A_0+A_1x+A_2x^2+\ldots+A_m x^m \equiv 0 \text{ (mod. } M).$$

Metoda rozwiązania kongruencyi [1])

$$A_0+A_1x+A_2x^2+\ldots+A_m x^m \equiv 0 \text{ (mod. } M) \qquad (1)$$

polega na sprowadzeniu jej do postaci kongruencyi dwumiennej.

Jeżeli we wzorze zasadniczym (1) Nr. 7, kładąc $n$ za $m$, oznaczymy

$$(-1)^{\omega+1} \aleph\left[\frac{M}{(1^{k+1})^{2n}},\ \omega\right]^{(\omega-1)} \text{ przez } N_n,$$

$$\left\{h(1^{k+1})^2+(-1)^{k+1}\right\}^{(n)} \text{ przez } H_n,$$

otrzymamy

$$a=N_n H^n+Mi;$$

pierwiastek zaś kongruencyi

$$x^n \equiv N_n H^n \text{ (mod. } M), \qquad (2)$$

odpowiadający tej reszcie $a$ i modułowi $M$, będzie

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

kładąc w kongruencyi (2) za $n$ kolejno: $0, 1, 2 \ldots m$ i podstawiając tak otrzymane wartości potęg: $x, x^2, \ldots x^m$ w kongruencyję daną, znajdziemy:

$$A_0+A_1N_1H+A_2N_1H^2+\ldots+A_m N_m H^m \equiv 0 \text{ (mod. } M), \qquad (4)$$

lub, po pomnożeniu wszystkich wyrazów przez $(1^{k+1})^{2m}$ i przy uwadze, że

$$(1^{k+1})^{2n} N_n \equiv 1 \text{ (mod. } M): \qquad (5)$$

$$A_0(1^{k+1})^{2m}+A_1(1^{k+1})^{2(m-1)}H+A_2(1^{k+1})^{2(m-2)}H^2+\ldots+A_mH^m \equiv 0 \text{ (mod. } M).$$

Wynika stąd, że moduł $M$ kongruencyi danej musi zadość czynić warunkowi

$$M=\text{fact. } [A_0(1^{k+1})^{2m}+A_1(1^{k+1})^{2(m-1)}H+\ldots+A_m H^m]. \qquad (6)$$

Przy tym warunku, równanie (3) przedstawia rozwiązanie kongruencyi (1).

Jeżeli moduł jest dany, wtedy przy pomocy wyrażenia (6), możemy wyznaczyć liczby rodzajową i gatunkową pierwiastka (3). Kładąc

$$W_\rho=(-1)^{2(m-1)\rho} H^\rho,$$

[1]) Réforme, str. 187.



www.rcin.org.pl

otrzymujemy z (6)

$$M = \text{fact.}\ (A_0 W_0 + A_1 W_1 + \ldots + A_m W_m).$$

Tu stronę drugą jako funkcyję liczb $k$ i $h$ oznaczmy przez $F(k, h)$, t. j. połóżmy:

$$F(k, h) = A_0 W_0 + A_1 W_1 + \ldots + A_m W_m.$$

Uważając $F(k, h)$ jako funkcyję ilości $h$, zmieniającej się w sposób ciągły, możemy do niej zastosować wzór Taylora, który dla przyrostu równego $\pm 1$ przybierze postać:

$$(7) \quad F(k, h \pm 1) = F(k, h) + \frac{1}{1} \frac{dF(k, h)}{dh} + \frac{1}{1^{2|1}} \frac{d^2F(k, h)}{dh^2} + \ldots$$

Pochodne, występujące po stronie drugiej, otrzymamy z łatwością, biorąc ogólne pochodne rzędu $\mu$-go funkcyi $F(k, h)$, przy pomocy wzoru:

$$\frac{1}{1^{\mu|1}} \frac{d^\mu F(k, h)}{dh^\mu} = A_\mu . W_0 + \frac{\mu+1}{1} A_{\mu+1} W_1 + \frac{(\mu+2)^{2|-1}}{1^{2|1}} A_{\mu+2} W_2 + \ldots$$

$$+ \frac{m^{m-\mu|-1}}{1^{m-\mu|1}} A_m W_{m-\mu}$$

i zakładając kolejno $\mu = 1, 2 \ldots$

Podstawiając wartości tak otrzymane we wzorze (7), dojdziemy do wyrażenia

$$(8) \quad F(k, h \pm 1) = B_0 W_0 + B_1 W_1 + \ldots + B_m W_m,$$

w którem współczynniki $B$ mają wartości następujące:

$$B_0 = A_0 \pm A_1 + A_2 \pm A_3 \ldots + (\pm 1^m) A_m,$$

$$B_1 = A_1 \pm 2A_2 + 3A_3 + 4A_3 \ldots + (\pm 1)^{m-1} A_m,$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

$$B_m = (\pm 1)^{m-m} A_m = A_m.$$

Współczynniki $B$, jak widzimy, za pomocą łatwych działań oznaczyć można ze współczynników danych $A$, a ztąd i łatwo znaleźć wartość funkcyi $F(k, h \pm 1)$. Tym sposobem, poczynając od $h = 0$, otrzymać możemy kolejno $F(k, 0)$, $F(k, 1)$, $F(k, 2)$, ..., a ztąd i oznaczyć te wartości gatunku $h$, które przy danym module $M$ odpowiadają danemu rodzajowi $k$. Co się zaś tyczy samego rodzaju $k$, to wprowadzając zań kolejno różne wartości $1, 2, 3 \ldots$, będziemy mogli znaleźć te wartości,

www.rcin.org.pl

którym odpowiadają oraz te, którym nie odpowiadają rozwiązania kongruencyi danej.

## 12. Rozwiązywanie kongruencyj rzędów wyższych [1]).

Niechaj będzie kongruencyja, dajmy na to, rzędu drugiego i stopnia dowolnego postaci:

$$\begin{aligned} &A_{0,0}+A_{1,0}x+A_{2,0}x^2+\ldots\ldots \\ &+A_{0,1}y+A_{1,1}xy+\ldots\ldots \\ &+A_{0,2}y^2+\ldots\ldots \\ &+\ldots\ldots \equiv 0 \pmod{M}. \end{aligned} \tag{1}$$

Oznaczmy liczby rodzajowe i gatunkowe, niewiadomej $x$ przez $k_1$, $h_1$, — niewiadomej $y$ przez $k_2$, $h_2$ i wprowadźmy oznaczenia

$$N_{1,n}=(-1)^{\omega_1+1}\aleph\left[\frac{M}{(1^{k_1+1})^{2n}},\ \omega_1\right]^{(\omega_1-1)},$$

$$H_1=\left\{h_1(1^{k_1+1})^2+(-1)^{k_1+1}\right\}^n,$$

$$N_{2,n}=(-1)^{\omega_2+1}\aleph\left[\frac{M}{(1^{k_2+1})^{2n}},\ \omega_2\right]^{(\omega_2-1)},$$

$$H_2=\left\{h_2(1^{k_2+1})^2+(-1)^{k_2+1}\right\}^n,$$

Na podstawie wzoru zasadniczego (1) $N^{ro}$ 7 wyrażenia: reszty $a_1$, odpowiadającej ilościom $N_{1,n}$, $H_1$, oraz reszty $a_2$, odpowiadającej ilościom $N_{2,n}$, $H_2$ będą:

$$a_1=N_{1,n}H_1^n+Mi_1,$$

$$a_2=N_{2,n}H_2^n+Mi_2,$$

a odpowiadające resztom tym kongruencye będą

$$\begin{aligned} x^n &\equiv N_{1,n}H_1^n \pmod{M}, \\ y^n &\equiv N_{2,n}H_2^n \pmod{M}. \end{aligned} \tag{2}$$

Ich rozwiązania mają postać

$$\begin{aligned} x&=h_1+(-1)^{\pi_1+k_1}\aleph\left[\frac{M}{(1^{k_1+1})^2},\ \pi_1\right]^{(\pi_1-1)}+Mj_1, \\ y&=h_2+(-1)^{\pi_2+k_2}\aleph\left[\frac{M}{(1^{k_2+1})^2},\ \pi_2\right]^{(\pi_2-1)}+Mj_2. \end{aligned} \tag{3}$$

---

[1]) Réforme str. 187 i dalsze.

[1]) Réforme, str. 196—208.

www.rcin.org.pl

Kładąc w równaniach (2) kolejno $n=1, 2, 3 \ldots$ i otrzymane ztąd wartości na $x_1\ x^2 \ldots xy, \ldots y, y^2 \ldots$ podstawiając w równanie dane, znajdziemy

$$\begin{aligned} &A_{0,0} + A_{1,0} N_{1,1} H_1 + A_{2,0} N_{1,2} H^2 + \ldots \\ &\quad + A_{0,1} N_{2,1} H_2 + A_{1,1} A_{1,n} N_{2,n} H_1 H_2 + \ldots \\ &\qquad + A_{0,2} N_{2n} H_2^2 + \ldots \\ &\qquad\qquad + \ldots \equiv 0 \pmod{M}. \end{aligned} \tag{4}$$

Mnożąc obie strony tej kongruencyi (4) przez $(1^{k_1})^2$ w potędze równej stopniom kongruencyi danej, z uwagi na związek

$$(1^{k_1})^{2n} N_n \equiv 1 \pmod{M},$$

i przy wprowadzeniu oznaczeń

$$W_{1,\rho_1} = (1^{k_1})^{2(m_1 - \rho_1)} H_1^{\rho_1},$$

$$W_{2,\rho_2} = (1^{k_2})^{2(m_2 - \rho_2)} H_2^{\rho_2},$$

otrzymamy z łatwością warunek następujący możliwości kongruencyi danej:

$$\begin{aligned} M = \text{fact.} \{ &A_{0,0} W_{1,0} W_{2,0} + A_{1,0} W_{1,1} W_{2,0} + A_{2,0} W_{1,2} W_{2,0} + \ldots \\ &+ A_{0,1} W_{1,0} W_{2,1} + A_{1,1} W_{1,1} W_{1,2} + \ldots \\ &+ A_{0,2} W_{1,0} W_{1,2} + \ldots \\ &+ \ldots \} \end{aligned} \tag{5}$$

Przy istnieniu tego warunku, związki (3) przedstawiają rozwiązanie kongruencyi. Z równania warunkowego (5) znajdziemy wartości liczb rodzajowych i gatunkowych, którym odpowiadają rozwiązania danego zagadnienia.

Wroński podaje następującą metodę ogólną do oznaczania liczb rodzajowych i gatunkowych, dla których istnieją rozwiązania.

Równanie warunkowe (4) lub (5) dla kongruencyj jakiegokolwiek rzędu ma oczywiście postać taką:

$$F(k_1, k_2, \ldots k_\mu, H_1, H_2 \ldots H_\mu) \equiv 0 \pmod{M}, \tag{6}$$

gdzie $k_1, k_2, \ldots k_\mu$ są liczby rodzajowe, zaś $H_1, H_2, \ldots H_\mu$ mają znaczenie wyżej określone. W funkcyi $F$ znajdują się wyrazy: 1) zawierające po jednej tylko z ilości $H$; 2) zawierające dwie lub więcej z tych ilości. Oznaczmy sumę wyrazów, zawierających jednę tylko ilość $H_i$, $(i=1, 2 \ldots \mu)$ przez $F_i$, $(i=1, 2 \ldots \mu)$, sumę wyrazów pozostałych

www.rcin.org.pl

przez $F_{\mu+1}$. Oznaczmy dalej przez $S_i$, $(i=1, 2 \ldots \mu)$ pewne ilości dopełniające, mające tę własność, że $S_i+F_i \equiv 0 \pmod{M}$, przez $S_{\mu+1}$ wreszcie ilość dopełniającą, dla której $S_{\mu+1}+F_{\mu+1} \equiv 0 \pmod{M}$. Przy tych założeniach, kongruencyję (6) będzie można zastąpić układem kongruencyj następujących:

$$\begin{aligned} S_1+F_1 \ (k_1, k_2 \ldots, k_\mu, H_1) &\equiv 0 \pmod{M} \\ S_2+F_2 \ (k_1, k_2 \ldots, k_\mu, H_2) &\equiv 0 \pmod{M} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ S_\mu+F_\mu \ (k_2, k_2 \ldots k_\mu, H_\mu) &\equiv 0 \pmod{M} \end{aligned} \tag{7}$$

$$S_{\mu+1}+F_{\mu+1} \ (k_1 k_2, \ldots 1 k_\mu, H_1, H_2 \ldots H_\mu) \equiv 0 \pmod{M}$$

przy warunku

$$S_1 + S_2 + \ldots + S_\mu + S_{\mu+1} \equiv 0 \pmod{M}. \tag{8}$$

Za pomocą metody, podanej w numerze poprzedzającym, można wyznaczyć wartości funkcyj $F_i$ w $\mu$ pierwszych równaniach (7), odpowiadające różnym wartościom liczb gatunkowych $h_1, h_2 \ldots h_\mu$, przy danych wartościach liczb rodzajowych $k_1, k_2 \ldots k_\mu$. Można będzie tedy oznaczyć wartości ilości dopełniających $S_1, S_2 \ldots S_\mu$, czyniące zadość pierwszym kongruencyjom (7). Rugując następnie z układu wszystkich $\mu+1$ kongruencyj (7) $\mu$ ilości $H_1, H_2, \ldots H_\mu$, otrzymamy związek pomiędzy ilościami $k_1, k_2 \ldots k_\mu, S_1, S_2, \ldots S_\mu, S_{\mu+1}$, który przy pomocy kongruencyi (8), przyjmuje ostatecznie postać:

$$\Phi(k_1, k_2, \ldots k_\mu, S_1, S_2 \ldots S_\mu) \equiv 0 \pmod{M}.$$

Z tej kongruencyi znajdziemy związek, jaki powinien zachodzić pomiędzy ilościami $S_1, S_2, \ldots S_\mu$, aby odpowiednie liczby gatunkowe prowadziły do rozwiązania zagadnienia.

## 13. Rozwiązywanie równań nieoznaczonych.

Rozwiązywanie równań nieoznaczonych uskutecznia się przez zamianę ich na kongruencyje i stosowanie następne metod podanych w N-rach poprzedzających [1]).

Niechaj będzie równanie nieoznaczone jakiegokolwiek rzędu i stopnia i niechaj zmiennemi będą $x, y, z \ldots$ Jeżeli to równanie jest zu-

[1]) Réforme, str. 210 i dalsze.

www.rcin.org.pl

pełnem, to znajduje się w niem wyraz, zawierający iloczyn $xyz\ldots$ wszystkich zmiennych. Jeżeli jest niezupełnem i wyrazu wzmiankowanego nie zawiera, to przez wprowadzenie nowych zmiennych za pomocą podstawienia linijowego można będzie wyraz taki wprowadzić, przyczem jeżeli stopień równania jest niższy od jego rzędu, trzeba najprzód równanie przekształcić, podnosząc jego stopień do liczby równej rzędowi przez pomnożenie wszystkich jego wyrazów przez odpowiednią potęgę jednej lub kiku zmiennych, co oczywiście istoty zagadnienia nie zmienia.

Można tedy równanie dane przedstawić zawsze w postaci:

$$F(x, y, z, \ldots) + Mxyz \ldots = 0, \tag{1}$$

gdzie $M$ jest współczynnikiem wyrazu, zawierającego $xyz\ldots$; temu zaś ostatniemu równaniu można dać postać kongruencyi

$$F(x, y, z \ldots) \equiv 0 \pmod{M}, \tag{2}$$

którą rozwiązawszy według metody podanej w Nrze poprzedzającym, znajdziemy pewne wyrażenia dla niewiadomych

$$x = X_1 + Mi_1, \quad y = Y_1 + Mi_2, \quad z = Z_1 + Mi_3 \ldots \tag{3}$$

gdzie $i_1, i_2, i_3 \ldots$ są stałemi nieoznaczonemi.

Jeżeli te wyrażenia wprowadzimy do równania (1), otrzymamy z niego związek pomiędzy liczbami $i_1, i_2, i_3 \ldots$, który niechaj wyobraża równanie

$$\Phi(i_1, i_2, i_3 \ldots) = 0. \tag{4}$$

Równanie to jest w ogóle tego samego rzędu i stopnia co dane, lecz zakładając, że jedna z liczb nieoznaczonych $i$ jest zerem, zniżymy rząd jego o jedność.

Stosując do tego równania rzędu o jedność niższego tęż samą metodę, dojdziemy do równania rzędu o dwie jedności niższego; z tego znów otrzymamy równanie rzędu o trzy jedności niższego i tak dalej postępując, dojdziemy ostatecznie do równania rzędu 1-go, t. j. z jedną niewiadomą.

Wroński podaje prócz tego metodę, pozwalającą odrazu zniżyć rząd równania o dwie lub więcej jedności. W tym celu należy po rozwiązaniu kongruencyi (2), napisać równanie dane w postaci:

$$f(x, y, z \ldots) + N = 0 \tag{5}$$

a raczej przedstawić je w postaci kongruencyi

$$f(x, y, z \ldots) \equiv \pmod{N}, \tag{6}$$

www.rcin.org.pl

gdzie $N$ jest wyrazem stałym równania danego. Rozwiązując kongruencyję (6), otrzymujemy

$$x = X_2 + Nj_1, \; z = Y_2 + Nj_2, \; z = Z_2 + Nj_3, \ldots \tag{7}$$

a porównywając rozwiązania (3) i (7), znajdziemy związki pomiędzy liczbami $i$ i $j$. Związki te mają postać

$$\begin{gathered} Mi_1 \equiv X_2 - X_1 \pmod{N} \\ \text{lub } Nj_1 \equiv X_1 - X_2 \pmod{M}, \end{gathered} \tag{8}$$

i podobną dla $i_2, j_2$, $i_3, j_3$. Rozwiązawszy kongruencyje (8), otrzymamy:

$$i_1 = (-1)^{\omega} (X_1 - X_2) \aleph \left[ \frac{N}{M}, \; \omega \right]^{(\omega - 1)} + Np_1$$

$$j_1 = (-1)^{\pi+1} (X_1 - X_2) \aleph \left[ \frac{M}{N}, \; \pi \right]^{(\pi - 1)} + Mq_1$$

. . . . . .

wstawiając zaś te wartości w (3) lub w (7) znajdziemy następujące wyrażenia pierwiastków

$$\begin{aligned} x &= X_1 + (-1)^{\omega} (X_3 - X_2) M \aleph \left[ \frac{N}{M}, \; \omega \right]^{(\omega - 1)} + MNp_1 \\ y &= Y_1 + (-1)^{\omega} (Y_1 - Y_2) M. \aleph \left[ \frac{N}{M}, \; \omega \right]^{\omega - 1} + MNp_2 \\ z &= Z_1 + (-1)^{\omega} (Z_1 - Z_2) M \aleph \left[ \frac{N}{M}, \; \omega \right]^{\omega - 1} + MNp_3 . \end{aligned} \tag{9}$$

Wartości (9), wprowadzone do równania danego, uczynią oczywiście pierwszą jego stronę podzielną przez $MN$ i dadzą związek pomiędzy liczbami $p$, z których teraz dwie którekolwiek mogą otrzymać wartości zupełnie dowolne, n. p. równe zeru; tym sposobem znajdziemy związek

$$\varphi (p_1 \; p_2 \; p_3 \ldots) = 0$$

rzędu o dwie jedności niższego niż równanie dane.

Za pomocą nowego przekształcenia równania danego na kongruencyją o module, równym współczynnikowi innego wyrazu równania, możnaby otrzymać nowe równanie rzędu o trzy jedności niższego i t. d.

Wroński stosuje wyłożoną tu metodę do równania nieoznaczonego

$$z^n - Ny^n = Mu^n . \tag{10}$$

www.rcin.org.pl

Aby równanie to rozwiązać, należy rozwiązać kongruencyje

$$z^n - Ny^n \equiv 0 \pmod{M} \tag{11}$$

$$z^n - Mu^n \equiv 0 \pmod{N} \tag{12}$$

Stosując metodę wyłożoną w Nrze 9, znajdziemy rozwiązania kongruencyi (11) w postaci:

$$z = A + Mi_1, \quad y = B + Mi_2 \tag{13}$$

rozwiązania zaś kongruencyi (12) w postaci

$$z = B + Nj_1, \quad u = Q + Nj_2. \tag{14}$$

Z porównania dwóch wyrazeń na $z$ otrzymamy według powyższej teoryi

$$z = A + (-1)^{\omega}(A-B)\, M \aleph \left[\frac{N}{M}, \omega\right]^{(\omega-1)} + Mnp.$$

lub

$$z = A + \zeta(A-B) + Mnp \tag{15}$$

gdzie

$$\zeta = (-1)^{\omega} M \aleph \left[\frac{N}{M}, \omega\right]^{(\omega-1)} \tag{16}$$

Wstawiając wartości na $y$ i $u$ z równań (13) i (14) oraz wartości na $z$ z równania (16) w równanie dane (10), znajdziemy następujący związek

$$\{A + \zeta(A-B) + MNp\}^n - N(P + Mi_2)^n = M(Q + Nj_2)^n. \tag{17}$$

Nadając tu liczbie $p$ wartość zupełnie dowolną, otrzymujemy równanie rzędu drugiego z dwiema niewiadomemi $i_2$ i $j_2$, a potem równanie rzędu o jedność niższego niż równanie dane (10).

www.rcin.org.pl

# SPROSTOWANIA.

Str. 75 przypisek 3 zamiast *1865* powinno być *1845*

„ 79 wiersz 2 od dołu $\frac{B}{A}$ „ „ $\frac{M}{A}$

„ „ „ „ „ $+ M$ „ „ $+ Mi$

„ 89 „ 4 od góry zamiast *zkąd* powinno być: *jeżeli* więc *przyjmiemy*, *że*

„ 89 „ 8 i 9 od góry od wyrazów *i naodwrót* aż do końca wiersza 9 wykreślić.

„ 89 „ 15 od góry zamiast (8) powinno być (6).

„ 90 we wzorze (11) zamiast $\frac{M}{K}$ powinno być $\frac{M}{K^m}$

„ 90 „ (12) wykładnik $m$ stojący za nawiasem ] powinien być za nawiasem }

„ 90 wiersz 2 od dołu przed $(-1)^{k+1}$ powinien być znak +

„ 95 wiersz 12 od dołu zamiast $a\ (1^{k-1})^2 - 1 \equiv 0 \pmod{M}$ powinno być $a\ (1^{k/1})^{2n} - 1 \equiv 0 \pmod{M}$.

„ 96 wiersz 11 od góry zamiast potęgi $m$-ej powinno być potęgi $n$-ej.

www.rcin.org.pl