ROZDZIAŁ VIII

TWIERDZENIE EULERA, TWIERDZENIE LAGRANGE'A, PIERWIASTKI PIERWOTNE I WSKAŹNIKI

§ 1. Dowód twierdzenia Eulera. Niech $m>1$ będzie liczbą naturalną, a

(1) $$r_1, r_2, \ldots, r_{\varphi(m)}$$

— ciągiem wszystkich liczb naturalnych, niewiększych od m i pierwszych względem m. Niech dalej a będzie jakąkolwiek liczbą pierwszą względem m. Oznaczmy ogólnie przez ϱ_k resztę z dzielenia iloczynu ar_k przez liczbę m. Zatem dla $k=1,2,\ldots,\varphi(m)$ jest

(2) $$\varrho_k \equiv ar_k \pmod m$$

czyli

(3) $$\varrho_k = ar_k + t_k m,$$

gdzie t_k są liczbami całkowitymi.

Dowiedziemy, że ciąg

(4) $$\varrho_1, \varrho_2, \ldots, \varrho_{\varphi(m)}$$

różni się od ciągu (1) co najwyżej porządkiem wyrazów. W tym celu wystarczy oczywiście okazać, że:

1° każdy wyraz ciagu (4) jest liczbą naturalną nie większą od m i pierwszą względem m,

2° wszystkie wyrazy ciągu (4) są różne.

Niech $d_k=(\varrho_k, m)$; z równości (3) wnosimy, że liczba

$$ar_k = \varrho_k - t_k m$$

ma dzielnik d_k wspólny z liczbą m. Lecz zarówno a jak r_k są pierwsze względem m. Musi więc być $d_k=1$, czyli liczba ϱ_k jest pierwsza względem m. Z drugiej strony ϱ_k, jako reszta z dzielenia liczby ar_k przez m, spełnia nierówności

$$0 \leqslant \varrho_k < m,$$

gdzie równość $\varrho_k=0$ jest wyłączona wobec $(\varrho_k, m)=1$. Dowiedliśmy więc, że wyrazy ciągu (4) mają własność 1°.

Przypuśćmy teraz, że dla dwu różnych wskaźników i i j z ciągu $1,2,\ldots,\varphi(m)$ jest

$$\varrho_i = \varrho_j.$$

Wobec (2) mielibyśmy

$$\varrho_i \equiv ar_i \pmod m \quad \text{i} \quad \varrho_j \equiv ar_j \pmod m,$$

skąd w myśl przypuszczenia

$$ar_i \equiv ar_j \pmod m \quad \text{i} \quad a(r_i - r_j) \equiv 0 \pmod m.$$

Iloczyn $a(r_i-r_j)$ byłby więc podzielny przez m. Lecz a jest liczbą pierwszą względem m, a liczba r_i-r_j dzielić się przez m nie może, gdyż r_i i r_j, jako różne wyrazy ciągu (1), są różnymi liczbami naturalnymi niewiększymi od m. Dowiedliśmy więc, że wyrazy ciągu (1) mają własność 2°.

Wyrazy ciągu (4) różnią się zatem co najwyżej porządkiem od wyrazów ciągu (1); przeto

$$\varrho_1 \varrho_2 \ldots \varrho_{\varphi(m)} = r_1 r_2 \ldots r_{\varphi(m)}.$$

Oznaczmy przez P wspólną wartość tych iloczynów. P jest oczywiście liczbą pierwszą względem m, gdyż każdy z jej czynników jest pierwszy względem m.

Mnożąc stronami kongruencje (2) dla $k=1,2,3,\ldots,\varphi(m)$, otrzymujemy

$$\varrho_1 \varrho_2 \ldots \varrho_{\varphi(m)} \equiv a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \pmod m$$

czyli $P \equiv a^{\varphi(m)} P \pmod m$, skąd wnosimy, że iloczyn $P(a^{\varphi(m)}-1)$ jest podzielny przez m. Z uwagi na to, że $(P,m)=1$, wnosimy stąd o podzielności liczby $a^{\varphi(m)}-1$ przez m.

Udowodniliśmy tym samym następujące

Twierdzenie 1 (Eulera). *Dla każdej liczby całkowitej a, pierwszej względem m, zachodzi kongruencja*

(5) $$a^{\varphi(m)} \equiv 1 \pmod m.$$

Twierdzenie to można uważać za uogólnienie małego twierdzenia Fermata (p. str. 59). Istotnie jeżeli w szczególności $m=p$, gdzie p jest liczbą pierwszą, to $\varphi(p)=p-1$ (p. str. 141) i kongruencja (5) daje

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

dla każdej liczby a pierwszej względem p, tj. niepodzielnej przez liczbę pierwszą p.

Jako wniosek z dowiedzionego twierdzenia Eulera udowodnimy następujące

Twierdzenie 2. *Z każdego postępu arytmetycznego nieskończonego o wyrazach całkowitych można wyjąć postęp geometryczny nieskończony.*

Dowód. Niech dany będzie postęp arytmetyczny nieskończony

$$a, \quad a+r, \quad a+2r, \quad \ldots \tag{6}$$

o wyrazach całkowitych. Dla $r=0$ sam postęp (6) byłby zarazem geometryczny. Dla $r<0$ wystarczyłoby dowieść twierdzenia dla postępu otrzymanego z (6) przez zmianę znaku wszystkich wyrazów. Tym sposobem dowód twierdzenia sprowadza się do przypadku, gdy r jest liczbą naturalną.

Możemy nadto założyć, że $(a, r)=1$, gdyż w razie $d=(a, r)>1$ mielibyśmy $a=da'$ i $r=dr'$, gdzie $(a', r')=1$, i wystarczyłoby dowieść twierdzenia dla postępu $a', a'+r', \ldots$

Wreszcie, wobec $r>0$, dostatecznie dalekie wyrazy postępu (6) są większe od 1, możemy więc dla dowodu twierdzenia odrzucić wcześniejsze i założyć od razu, że $a>1$.

Otóż w myśl twierdzenia Eulera jest $a^{\varphi(r)}\equiv 1 \pmod r$, skąd dla n naturalnych $a^{n\varphi(r)}\equiv 1 \pmod r$ i przeto liczby

$$k_n=\frac{aa^{n\varphi(r)}-a}{r}$$

są całkowite. Lecz

$$a+k_n r=a(a^{\varphi(r)})^n \qquad \text{dla } n=1, 2, \ldots,$$

przy czym wobec $a>1$ mamy

$$0\leqslant k_1<k_2<k_3<\ldots$$

i liczby

$$a+k_1 r, \quad a+k_2 r, \quad a+k_3 r, \quad \ldots$$

tworzą postęp geometryczny, c. b. d. o.

Z twierdzenia 2 wynika natychmiast, że *w każdym postępie arytmetycznym nieskończonym o wyrazach całkowitych istnieje nieskończenie wiele wyrazów, mających te same dzielniki pierwsze* [1]).

[1]) Por. G. Pólya i G. Szegö, *Aufgaben und Lehrsätze der Analysis*, tom II, Berlin 1925, str. 344.

Z twierdzenia 2 wynika też łatwo, że z każdego postępu arytmetycznego nieskończonego o wyrazach wymiernych można wyjąć postęp geometryczny nieskończony.

Natomiast można okazać, że jeżeli a jest liczbą niewymierną, to z postępu arytmetycznego nieskończonego $a, a+1, a+2, \ldots$ nie można wyjąć żadnego postępu geometrycznego nieskończonego. Podobnie — z postępu arytmetycznego $i, i+1, i+2, \ldots$, gdzie $i=\sqrt{-1}$.

Pozostawiamy czytelnikowi do udowodnienia, że *na to, by z postępu arytmetycznego nieskończonego o wyrazach zespolonych można było wyjąć postęp geometryczny nieskończony, potrzeba i wystarcza, żeby stosunek $a:r$ był liczbą wymierną.*

ĆWICZENIA. 1. Dowieść, że każda liczba naturalna, niepodzielna przez 2 ani przez 5, jest dzielnikiem pewnej liczby, której wszystkie cyfry (w układzie dziesiętnym) są jedynkami (por. Rozdział IV, § 2, str. 66, ćwiczenie 19).

Dowód. Jeżeli $(n, 10)=1$, to również $(9n, 10)=1$ i w myśl twierdzenia Eulera jest $10^{\varphi(9n)}\equiv 1 \pmod{9n}$, skąd $10^{\varphi(9n)}-1=9nk$, gdzie k jest liczbą całkowitą. Stąd $\frac{10^{\varphi(9n)}-1}{9}=nk$ i — jak łatwo widzieć — wszystkie cyfry tej liczby w układzie dziesiętnym są jedynkami.

2. Dowieść, że jeżeli a jest liczbą całkowitą, a s i m — takimi liczbami naturalnymi, że $a^s\equiv 1 \pmod m$ i $(s, \varphi(m))=1$, to $a\equiv 1 \pmod m$.

Wskazówka. Należy się oprzeć na twierdzeniu Eulera oraz na tym, że wobec $(s, \varphi(m))=1$ istnieją takie liczby całkowite k i l, że $ks+l\varphi(m)=1$.

3. Dowieść, że jeżeli liczby naturalne a i b są względnie pierwsze, to

$$\mathrm{E}\left(\frac{b}{a}\right)+\mathrm{E}\left(\frac{2b}{a}\right)+\ldots+\mathrm{E}\left(\frac{(a-1)b}{a}\right)=\mathrm{E}\left(\frac{a}{b}\right)+\mathrm{E}\left(\frac{2a}{b}\right)+\ldots+\mathrm{E}\left(\frac{(b-1)a}{b}\right)=$$
$$=\tfrac{1}{2}(a-1)(b-1).$$

Dowód. Oznaczmy przez r_k resztę z dzielenia kb przez a. Wobec $(a, b)=1$, jak to z łatwością wynika z twierdzenia 6 Rozdziału I (§ 7, str. 6), jest

$$r_1+r_2+\ldots+r_{a-1}=1+2+\ldots+(a-1)=\frac{(a-1)a}{b}.$$

Lecz $\mathrm{E}\left(\frac{kb}{a}\right)=\frac{kb}{a}-\frac{rk}{a}$, skąd

$$\mathrm{E}\left(\frac{b}{a}\right)+\mathrm{E}\left(\frac{2b}{a}\right)+\ldots+\mathrm{E}\left(\frac{(a-1)b}{a}\right)=$$
$$=\frac{b}{a}(1+2+\ldots+a-1)-\frac{1+2+\ldots+a-1}{a}=$$
$$=\frac{b-1}{a}\cdot\frac{a(a-1)}{2}=\tfrac{1}{2}(a-1)(b-1).$$

Wystarczy teraz zamienić a na b i na odwrót.

4. Dowieść, że w postępie arytmetycznym o n wyrazach

$$a,\quad a+r,\quad a+2r,\quad \ldots,\quad a+(n-1)r,$$

gdzie r jest liczbą pierwszą względem n, istnieje jeden i tylko jeden wyraz podzielny przez n.

5. Dowieść, że jeżeli dla liczby naturalnej $p>2$ istnieje taka liczba całkowita a, że $a^k \not\equiv 1 \pmod p$ dla $k=1,2,\ldots,p-2$ i $a^{p-1}\equiv 1 \pmod p$, to p jest liczbą pierwszą.

Dowód. Jak łatwo widzieć, wobec $a^{p-1}\equiv 1 \pmod p$ mamy $(a,p)=1$, skąd $a^{\varphi(p)}\equiv 1 \pmod p$ w myśl twierdzenia Eulera. Gdyby liczba p była złożona, byłoby $k=\varphi(p)<p-1$ wbrew założeniu, że $a^k \not\equiv 1 \pmod p$ dla naturalnych $k<p-2$.

Uwaga. Dowiedzione twierdzenie może być uważane za odwrócenie małego twierdzenia Fermata [1]). Udowodnimy w § 5 (p. str. 185), że *jeżeli p jest liczbą pierwszą, to istnieje taka liczba naturalna a, że $a^k \not\equiv 1 \pmod p$ dla $k=1,2,\ldots,p-2$ i $a^{p-1}\equiv 1 \pmod p$.*

Taką liczbę a nazywamy *pierwiastkiem pierwotnym* dla modułu pierwszego p.

Wynika stąd, że jeżeli p jest liczbą pierwszą, to $p-1$ jest najmniejszym takim wykładnikiem naturalnym k, że $a^k\equiv 1 \pmod p$ przy wszelkim całkowitym a, niepodzielnym przez p.

6. Dowieść, że reszty z dzielenia kolejnych wyrazów postępu arytmetycznego nieskończonego $ax+b$ (gdzie a i b są danymi liczbami całkowitymi, a $x=0,1,2,\ldots$) przez liczbę naturalną m tworzą ciąg nieskończony okresowy o okresie czystym, złożonym z $m:(a,m)$ różnych wyrazów.

7. Dowieść, że przy a całkowitym reszty z dzielenia kolejnych wyrazów postępu geometrycznego nieskończonego $a, a^2, a^3, \ldots$ przez liczbę naturalną m tworzą ciąg okresowy o okresie, który może nie być czystym.

Dowód. Liczba reszt modulo m jest skończona, muszą się więc one powtarzać. Lecz jeżeli $a^k\equiv a^l \pmod m$, to $a^{k+j}\equiv a^{l+j} \pmod m$; stąd okresowość. Dla $a=2$ i $m=12$ okres nie jest czysty.

§ 2. Wnioski z twierdzenia Eulera. Z twierdzenia Eulera wynika, że jeżeli liczby a i m są względnie pierwsze, to kongruencja wykładnicza

$$a^x\equiv 1 \pmod m \tag{7}$$

ma zawsze pierwiastek naturalny, mianowicie $x=\varphi(m)$. Z drugiej strony jasne jest, że kongruencja (7) może mieć pierwiastek naturalny tylko wtedy, gdy a jest pierwsze względem m.

Jeżeli $x=\delta$ jest najmniejszym pierwiastkiem naturalnym kongruencji (7), mówimy, że *liczba a należy według modułu m do wykładnika δ.*

[1]) Por. M. Kraïtchik, *Théorie des Nombres*, tom II, Paryż 1929, str. 134.

Jasne jest, że liczby przystające modulo m zawsze należą według modułu m do tego samego wykładnika: wystarczy zauważyć, że jeżeli $a\equiv b \pmod m$, to każdy pierwiastek naturalny kongruencji $a^x\equiv 1 \pmod m$ jest zarazem pierwiastkiem naturalnym kongruencji $b^x\equiv 1 \pmod m$, gdyż przy wszelkim naturalnym x jest $a^x=b^x \pmod m$, skoro a i b przystają według modułu m.

Okażemy, że *każdy pierwiastek kongruencji (7) jest podzielny przez wykładnik δ, do którego należy liczba a według modułu m.*

Istotnie, niech x będzie liczbą całkowitą, spełniającą kongruencję (7), r — resztą z dzielenia x przez δ, a k — odpowiednim ilorazem. Ponieważ $x=k\delta+r$, więc

$$a^x=a^{k\delta}a^r. \tag{8}$$

Lecz skoro a należy według modułu m do wykładnika δ, to $a^\delta\equiv 1 \pmod m$. Jest więc

$$a^{k\delta}\equiv 1 \pmod m. \tag{9}$$

Równość (8) daje na mocy (7) i (9)

$$a^r\equiv 1 \pmod m.$$

Gdyby reszta r była dodatnia, to $x=r$ byłoby pierwiastkiem naturalnym kongruencji (7), mniejszym od δ wbrew określeniu liczby δ. Jest więc $r=0$, czyli x podzielne przez δ, c. b. d. o.

Przyjmijmy w szczególności $x=\varphi(m)$; jest to w myśl (5) pierwiastek kongruencji (7). Stąd

Twierdzenie 3. *Wykładnik, do którego jakakolwiek liczba należy według modułu m, jest zawsze dzielnikiem liczby $\varphi(m)$.*

W szczególności te liczby, które należą według modułu m do wykładnika $\varphi(m)$, tj. do możliwie największego wykładnika, do jakiego mogą należeć liczby według modułu m, nazywamy *pierwiastkami pierwotnymi* liczby m (zakładając przy tym zwykle, że $m\neq 1$).

Tak np. liczba 3 jest pierwiastkiem pierwotnym liczby 10, gdyż

$$3^1\equiv 3,\quad 3^2\equiv 9,\quad 3^3\equiv 7,\quad 3^4\equiv 1 \pmod{10},$$

przy czym $\varphi(10)=4$. Liczba 10 nie jest jednak pierwiastkiem pierwotnym liczby 3, gdyż wobec $10\equiv 1 \pmod 3$, liczba 10 należy według modułu 3 do wykładnika 1, gdy tymczasem $\varphi(3)=2$.

Okażemy teraz, że *jeżeli a należy według modułu m do wykładnika δ, to reszty z dzielenia liczb*

$$a^0, a^1, a^2, \ldots, a^{\delta-1} \tag{10}$$

przez liczbę m są wszystkie różne.

Istotnie, przypuśćmy, że dwa wyrazy ciągu (10) dają przy dzieleniu przez m jednakowe reszty. Oznaczając przez a^k ten z nich, który jest wcześniejszy, możemy oznaczyć drugi przez a^{k+l}, gdzie l jest liczbą naturalną i $l<\delta$. W myśl przypuszczenia, że wyrazy te dają przy dzieleniu przez m jednakowe reszty, zachodzi kongruencja

$$a^k \equiv a^{k+l} \pmod m,$$

skąd wniosek, że liczba $a^k(a^l-1)$ jest podzielna przez m. Lecz pierwszy jej czynnik jest wobec $(a, m)=1$ liczbą pierwszą względem m; zatem a^l-1 musi być podzielne przez m, czyli liczba naturalna $l<\delta$ byłaby pierwiastkiem kongruencji (7), wbrew określeniu liczby δ. Tak więc reszty z dzielenia wyrazów ciągu (10) przez m są wszystkie różne.

W szczególności jeżeli a jest pierwiastkiem pierwotnym liczby m, to reszty z dzielenia liczb

$$1, a, a^2, \ldots, a^{\varphi(m)-1}$$

przez m są wszystkie różne, a że jest ich $\varphi(m)$ i wszystkie są wobec $(a, m)=1$ pierwsze względem m, więc wnosimy, że ciąg tych reszt różni się co najwyżej porządkiem wyrazów od ciągu wszystkich $\varphi(m)$ liczb naturalnych pierwszych względem m i niewiększych od m.

Możemy zatem wypowiedzieć następujące

Twierdzenie 4. *Jeżeli a jest pierwiastkiem pierwotnym liczby m, n zaś jest liczbą pierwszą względem a, to wśród liczb* $0, 1, 2, \ldots, \varphi(m)-1$ *istnieje jedna i tylko jedna, która spełnia kongruencję*

$$a^x \equiv n \pmod m.$$

Liczbę taką nazywamy *wskaźnikiem (indeksem) liczby n według modułu m przy zasadzie a* i oznaczamy symbolem

$$\operatorname{ind}_a n.$$

Definicja wskaźników jest więc analogiczna do definicji logarytmów. Wskaźniki grają też w Teorii liczb rolę analogiczną do roli logarytmów w Analizie.

PRZYKŁADY. Niech będzie $m=7$ i $a=3$. Mamy:

$$3^0 \equiv 1, \quad 3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5 \pmod 7,$$

a więc dla modułu 7:

$$\operatorname{ind}_3 1=0, \ \operatorname{ind}_3 2=2, \ \operatorname{ind}_3 3=1, \ \operatorname{ind}_3 4=4, \ \operatorname{ind}_3 5=5, \ \operatorname{ind}_3 6=3.$$

Dla modułu 13 i pierwiastka pierwotnego 2 czytelnik zechce sam sprawdzić następujące tablice:

$\operatorname{ind}_2 x$	0	1	2	3	4	5	6	7	8	9	10	11	12
x	1	2	4	8	3	6	12	11	9	5	10	7	1

x	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind}_2 x$	0	1	4	2	9	5	11	3	8	10	7	6

Pierwsza z nich służy do obliczania x przy danym $\operatorname{ind}_2 x$, a druga — odwrotnie.

§ 3. Warunek konieczny istnienia pierwiastków pierwotnych liczby *m*. Samo przez się nasuwa się teraz pytanie: jakie liczby posiadają pierwiastki pierwotne?

Załóżmy, że liczba m posiada pierwiastek pierwotny a. Niech

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

będzie rozkładem liczby m na czynniki pierwsze.

Liczba a, jako pierwsza względem m, jest pierwsza względem każdego z czynników $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$; mamy więc w myśl twierdzenia Eulera:

$$\begin{aligned} a^{\varphi(p_1^{\alpha_1})} &\equiv 1 \pmod{p_1^{\alpha_1}}, \\ a^{\varphi(p_2^{\alpha_2})} &\equiv 1 \pmod{p_2^{\alpha_2}}, \\ &\ldots\ldots\ldots \\ a^{\varphi(p_k^{\alpha_k})} &\equiv 1 \pmod{p_k^{\alpha_k}}. \end{aligned} \tag{11}$$

Jeżeli N jest jakąkolwiek liczbą naturalną, podzielną przez każdą z liczb

$$\varphi(p_1^{\alpha_1}), \quad \varphi(p_2^{\alpha_2}), \quad \ldots, \quad \varphi(p_k^{\alpha_k}), \tag{12}$$

to wobec (11) będzie tym bardziej:

$$\begin{aligned} a^N &\equiv 1 \pmod{p_1^{\alpha_1}}, \\ a^N &\equiv 1 \pmod{p_2^{\alpha_2}}, \\ &\ldots\ldots \\ a^N &\equiv 1 \pmod{p_k^{\alpha_k}}. \end{aligned}$$

Różnica a^N-1 jest zatem podzielna przez każdą z liczb $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$, a więc i przez liczbę m; mamy stąd kongruencję

$$a^N \equiv 1 \pmod m. \tag{13}$$

Gdyby wśród liczb (12) było dwie lub więcej parzystych, to moglibyśmy oczywiście przyjąć

$$N = {}^1/_2\,\varphi(p_1^{\alpha_1})\cdot\varphi(p_2^{\alpha_2})\cdot\ldots\cdot\varphi(p_k^{\alpha_k}) = {}^1/_2\,\varphi(m),$$

gdyż liczba ta byłaby podzielna przez każdą z liczb (12), i mielibyśmy w myśl (13) $a^{{}^1/_2\varphi(m)} \equiv 1 \pmod m$ wbrew założeniu, że a należy według modułu m do wykładnika $\varphi(m)$.

W ciągu (12) jest więc co najwyżej jedna liczba parzysta. Lecz na mocy wzoru dla funkcji Gaussa (wzór (12), str. 140) jest

$$\varphi(p^\alpha) \equiv p^{\alpha-1}(p-1);$$

jest to liczba parzysta dla p nieparzystego oraz dla $p=2$ i $\alpha>1$.

Jeżeli więc liczba m ma czynnik pierwszy nieparzysty, to czynnik taki może być tylko jeden i wtedy liczba 2 może wchodzić do rozwinięcia liczby m co najwyżej w pierwszej potędze czyli musi być wtedy albo $m=p^\alpha$, albo $m=2p^\alpha$, gdzie p jest liczbą pierwszą nieparzystą.

Jeżeli zaś liczba m nie ma żadnego czynnika pierwszego nieparzystego, to $m=2^\alpha$; skąd $\varphi(m)=\varphi(2^\alpha)=2^{\alpha-1}$.

Wtedy jednak musi być $\alpha \leqslant 2$. Istotnie, liczba a, jako pierwsza względem $m=2^\alpha$, a zatem nieparzysta, jest postaci $4k\pm1$ czyli

$$a = \pm 1 + 2^2 k,$$

gdzie k jest liczbą całkowitą. Podnosząc obie strony do kwadratu, dostajemy

$$a^2 = 1 \pm 2^3 k + 2^4 k^2 = 1 + 2^3 k_1, \tag{14}$$

gdzie $k_1 = \pm k + 2k^2$ jest liczbą całkowitą. Załóżmy, że przy pewnym n jest

$$a^{2^n} = 1 + 2^{n+2} k_n, \tag{15}$$

gdzie k_n jest liczbą całkowitą. Na mocy (14) jest to prawdziwe dla $n=1$. Podnosząc obie strony równości (15) do kwadratu, dostajemy

$$a^{2^{n+1}} = 1 + 2^{n+3} k_n + 2^{2n+4} k_n^2 = 1 + 2^{n+3} k_{n+1},$$

gdzie $k_{n+1} = k_n + 2^{n+1} k_n^2$ jest znowu liczbą całkowitą. Wnosimy więc przez indukcję, że wzór (15) zachodzi przy wszelkim naturalnym n. Stąd w szczególności dla liczby $n=\alpha-2$, która jest naturalna, jeżeli przypuścić, że $\alpha>2$, byłoby $a^{2^{\alpha-2}} = 1 + 2^\alpha k_{\alpha-2}$, zatem $a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$ czyli $a^{{}^1/_2\varphi(m)} \equiv 1 \pmod m$, wbrew założeniu, że a należy według modułu m do wykładnika $\varphi(m)$.

Otrzymane wyniki możemy wypowiedzieć jako następujące

Twierdzenie 5. *Pierwiastki pierwotne mają co najwyżej następujące liczby:*

1° *potęgi liczb pierwszych nieparzystych* ($m=p^\alpha$),

2° *podwojone potęgi liczb pierwszych nieparzystych* ($m=2p^\alpha$),

3° *liczba 2 i liczba 4.*

Że każda z wymienionych tu liczb istotnie ma co najmniej jeden pierwiastek pierwotny, udowodnimy w § 7 (p. str. 193). Dla liczb 2 i 4 rzecz ta nie przedstawia trudności, gdyż wobec $\varphi(2)=1$ jasne jest, że pierwiastkiem pierwotnym liczby 2 jest 1, wobec zaś $\varphi(4)=2$, pierwiastkiem pierwotnym liczby 4 jest 3.

§ 4. Twierdzenie Lagrange'a i wnioski z niego. Zajmiemy się przede wszystkim przypadkiem liczby pierwszej nieparzystej. Będzie nam w tym celu potrzebne pewne twierdzenie pomocnicze z teorii kongruencji algebraicznych, mianowicie tak zwane

Twierdzenie Lagrange'a. *Jeżeli $f(x)$ jest wielomianem całkowitym n-tego stopnia względem x o spółczynnikach całkowitych i jeżeli spółczynnik przy x^n nie jest podzielny przez liczbę pierwszą p, to kongruencja $f(x) \equiv 0 \pmod p$ ma co najwyżej n pierwiastków.*

Dowód. Na mocy twierdzenia 2 Rozdziału III (§ 5, str. 52) twierdzenie Lagrange'a zachodzi dla kongruencji stopnia pierwszego. Załóżmy, że jest ono prawdziwe dla kongruencji stopnia $n=k-1$ i weźmy pod uwagę kongruencję k-tego stopnia

$$f(x) \equiv 0 \pmod p, \tag{16}$$

gdzie $f(x) = A_0 x^k + A_1 x^{k-1} + \ldots + A_{k-1} x + A_k$ i wszystkie liczby $A_0, A_1, \ldots A_k$ są całkowite, a nadto A_0 jest niepodzielne przez liczbę pierwszą p.

Niech a będzie jednym z pierwiastków kongruencji (16):

$$f(a) \equiv 0 \pmod p$$

czyli

$$A_0 a^k + A_1 a^{k-1} + \ldots + A_{k-1} a + A_k \equiv 0 \pmod p.$$

Zatem przy wszelkim całkowitym x

$$f(x)\equiv f(x)-f(a)\pmod p$$

czyli

$$f(x)\equiv A_0(x^k-a^k)+A_1(x^{k-1}-a^{k-1})+\ldots+A_{k-1}(x-a)\pmod p.$$

Lecz

$$x^i-a^i=(x-a)(x^{i-1}+ax^{i-2}+a^2x^{i-3}+\ldots+a^{i-1})$$

dla $i=k, k-1, \ldots, 1$. Biorąc to pod uwagę, możemy napisać

$$f(x)\equiv(x-a)g(x)\pmod p, \tag{18}$$

gdzie $g(x)$ jest wielomianem całkowitym $(k-1)$-go stopnia względem x o spółczynnikach całkowitych, a nadto spółczynnikiem przy x^{k-1} jest — jak łatwo obliczyć — liczba A_0, więc liczba niepodzielna przez p. Wielomian $g(x)$ spełnia zatem (w myśl założenia, przyjętego na początku dowodu) wszystkie warunki twierdzenia Lagrange'a i przeto kongruencja

$$g(x)\equiv 0\pmod p \tag{19}$$

ma co najwyżej $k-1$ pierwiastków.

Gdyby kongruencja (16), wbrew twierdzeniu Lagrange'a, miała więcej niż k pierwiastków, tj. prócz pierwiastka a jeszcze co najmniej k pierwiastków $a_1, a_2, \ldots, a_k$, różnych między sobą i od liczby a, to mielibyśmy dla $i=1,2,\ldots,k$

$$f(a_i)\equiv 0\pmod p,$$

a zatem wobec kongruencji (18), zachodzącej przy wszelkim całkowitym x, $(a_i-a)g(a_i)\equiv 0\pmod p$, skąd $p\mid(a_i-a)g(a_i)$. Ponieważ jednak a_i są pierwiastkami różnymi od a, więc liczby a_i-a są niepodzielne przez p. Stąd wniosek, że $g(a_i)$ musi być podzielne przez p, czyli że $g(a_i)\equiv 0\pmod p$ dla $i=1,2,\ldots,k$. Wynikałoby stąd, że kongruencja (19), która jest z założenia stopnia $n=k-1$, ma więcej niż $k-1$ pierwiastków, a więc sprzeczność.

Tak więc prawdziwość twierdzenia Lagrange'a dla kongruencji stopnia $n=k-1$ pociąga za sobą jego prawdziwość dla kongruencji stopnia $n=k$. Ponieważ twierdzenie Lagrange'a zachodzi dla kongruencji stopnia 1, więc jego prawdziwość jest dowiedziona przez indukcję dla kongruencji każdego stopnia.

Zauważmy, że jeżeli $f(k)$ jest wielomianem całkowitym n-tego stopnia względem x, w którym współczynnik przy x^n jest pierwszy względem liczby złożonej m, to kongruencja $f(k)\equiv 0\pmod m$ może mieć więcej niż n pierwiastków.

Np. kongruencja $x^2\equiv 1\pmod 8$ ma 4 pierwiastki: 1, 3, 5 i 7. Tak samo kongruencja $x^2+3x+2\equiv 0\pmod 6$ ma 4 pierwiastki: 1, 2, 4 i 5.

Z twierdzenia Langrange'a wyprowadzimy teraz następujący

Wniosek. *Jeżeli kongruencja n-tego stopnia o spółczynnikach całkowitych i module pierwszym p ma więcej niż n pierwiastków, to jest tożsamościowa* (tj. spełnia ją każda liczba całkowita).

Dowód. Niech w kongruencji (16)

$$f(x)=A_0x^n+A_1x^{n-1}+\ldots+A_{n-1}x+A_n,$$

gdzie nie wszystkie spółczynniki $A_0, A_1, \ldots, A_{n-1}$ są podzielne przez p; niech A_m będzie pierwszym z niepodzielnych przez p. Byłoby więc dla wszelkich x

$$f(x)\equiv A_mx^{n-m}+A_{m+1}x^{n-m-1}+\ldots+A_n\pmod p,$$

gdzie $0\leqslant m\leqslant n-1$ czyli $1\leqslant n-m\leqslant n$. Wielomian po prawej stronie tej kongruencji spełniałby więc wszystkie warunki twierdzenia Lagrange'a, a jednocześnie wbrew temu twierdzeniu byłby stopnia niewiększego niż n, posiadając wszystkie pierwiastki kongruencji (16), czyli więcej niż n pierwiastków.

Wynika stąd, że każdy ze spółczynników $A_1, A_2, \ldots, A_{n-1}$ jest podzielny przez p, skąd

$$f(x)\equiv A_n\pmod p \tag{20}$$

dla wszelkiego całkowitego x.

Pozostaje do okazania, że również A_m jest podzielne przez p. Otóż w myśl założenia kongruencja (16) jest rozwiązalna; oznaczając przez a jeden z jej pierwiastków, mamy

$$f(a)\equiv 0\pmod p; \tag{21}$$

z drugiej strony, kongruencja (20) daje dla $x=a$

$$f(a)\equiv A_n\pmod p,$$

skąd na mocy (21)

$$A_n\equiv 0\pmod p.$$

Tak więc wszystkie spółczynniki wielomianu $f(x)$ są podzielne przez p, wobec czego kongruencja (16) zachodzi przy wszelkim całkowitym x, c. b. d. o.

Jednym z zastosowań udowodnionego wniosku jest następujący dowód twierdzenia Wilsona, dowiedzionego na innej drodze w Rozdziale IV (§ 1, str. 57).

Istotnie, kongruencja $(p-2)$-go stopnia

$$(22) \qquad (x-1)(x-2)\dots(x-p+1)-x^{p-1}+1\equiv 0 \pmod p$$

ma $p-1$ pierwiastków:

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

gdyż dla $x=1,2,\dots,p-1$ jest oczywiście

$$(x-1)(x-2)\dots(x-p+1)\equiv 0 \pmod p$$

(wówczas bowiem jeden z czynników staje się zerem), z drugiej zaś strony

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

na podstawie małego twierdzenia Fermata (str. 59).

Kongruencja (22) jest więc w myśl wniosku z twierdzenia Lagrange'a spełniona przez każdą liczbę x całkowitą, w szczególności przez $x=0$. Podstawiając tę wartość do kongruencji (22), otrzymujemy dla p pierwszych nieparzystych (z uwagi na to, że $(-1)^{p-1}=1$)

$$1\cdot 2\cdot 3\cdot\dots\cdot(p-1)+1\equiv 0 \pmod p,$$

czyli twierdzenie Wilsona.

Kongruencję o module pierwszym p można zawsze sprowadzić za pomocą twierdzenia Fermata do kongruencji stopnia niższego od p. Mamy bowiem przy wszelkim całkowitym x:

$$x^p\equiv x \pmod p, \qquad x^{p+1}\equiv x^2 \pmod p \qquad \text{itd.},$$

co pozwala na pozbycie się wyrazów, zawierających niewiadomą w potęgach p, $p+1$, ...

ĆWICZENIA. 1. Dowieść, że twierdzenie Lagrange'a zachodzi dla kongruencji o module 4 w tym sensie, że jeżeli $f(x)=a_0x^n+a_1x^{n-1}+\dots+a_n$ jest wielomianem o współczynnikach całkowitych, gdzie a_0 jest liczbą pierwszą względem 4, to kongruencja $f(x)\equiv 0 \pmod m$ ma nie więcej niż n różnych pierwiastków.

Dowód. Skoro $(a_0,4)=1$, to $a_0\equiv\pm 1 \pmod 4$ i możemy założyć, że $a_0=1$ (gdyż w razie $a_0=-1$ pomnożylibyśmy kongruencję przez -1). Ponieważ każda kongruencja ma według modułu 4 co najwyżej cztery pierwiastki (mianowicie 0, 1, 2 i 3), więc możemy założyć, że $n<4$.

Niech $n=3$. Gdyby kongruencja

$$x^3+a_1x^2+a_2x+a_3\equiv 0 \pmod 4$$

miała więcej niż 3 pierwiastki, byłaby prawdziwa dla $x=0,1,2$ i 3 i mielibyśmy

$$a_3\equiv 0, \qquad 1+a_1+a_2\equiv 0, \qquad 2a_2\equiv 0, \qquad 3+a_1+3a_2\equiv 0 \pmod 4,$$

skąd $3(1+a_1+a_2)-(3+a_1+3a_2)\equiv 0$, zatem $2a_1\equiv 0$ i $2+2a_1+2a_2\equiv 2 \pmod 4$, wbrew $1+a_1+a_2\equiv 0 \pmod 4$.

Niech teraz $n=2$. Przypuśćmy, że kongruencja

$$(*) \qquad x^2+a_1x+a_2\equiv 0 \pmod 4$$

ma więcej niż 2 pierwiastki. Gdyby ich miała 4, to kongruencja

$$x^3+a_1x^2+a_2x\equiv 0 \pmod 4$$

też miałaby 4 pierwiastki, co — jak dowiedliśmy — jest niemożliwe. Gdyby zaś kongruencja $(*)$ miała 3 pierwiastki, to oznaczając przez α tę spośród liczb 0, 1, 2 i 3, która nie jest jej pierwiastkiem, stwierdzilibyśmy, że kongruencja

$$(x-\alpha)(x^2+a_1x+a_2)\equiv 0 \pmod 4$$

musiałaby mieć 4 pierwiastki, co — jak dowiedliśmy — jest niemożliwe.

Wreszcie, niech $n=1$. Kongruencja $x+a_1\equiv 0 \pmod 4$ ma oczywiście jeden tylko pierwiastek $x\equiv -a_1 \pmod 4$.

Tym samym dowód został zakończony.

2. Dowieść, że w ćwiczeniu 1 nie można zastąpić modułu 4 przez żadną inną liczbę złożoną.

Dowód. 1°. Niech $m=p^\alpha$, gdzie $p=2$ i $\alpha>2$ albo $p>2$ i $\alpha\geqslant 2$. Różnymi pierwiastkami kongruencji $x^\alpha\equiv 0 \pmod m$ są oczywiście liczby:

$$0,\ p,\ 2p,\ \dots,\ (p^{\alpha-1}-1)p,$$

których jest $p^{\alpha-1}$. Lecz $2^{\alpha-1}>\alpha$ dla $\alpha>2$ oraz $p^{\alpha-1}>\alpha$ dla $p\geqslant 3$ i $\alpha\geqslant 2$. Kongruencja miałaby zatem więcej pierwiastków niż wynosi jej stopień.

2° Jeżeli liczba złożona m nie jest potęgą liczby pierwszej, to posiada co najmniej dwa różne dzielniki pierwsze i możemy przyjąć, że $m=m_1m_2$, gdzie $(m_1,m_2)=1$, $m_1>1$ i $m_2>1$. Jak łatwo widzieć, każda liczba całkowita spełnia kongruencję $(x-1)(x-2)\dots(x-m_1-m_2)\equiv 0 \pmod m$, gdyż dla każdego całkowitego x lewa strona jest podzielna zarówno przez m_1 jak przez m_2, a zatem (wobec $(m_1,m_2)=1$) też przez $m_1m_2=m$. Lecz kongruencja ta jest stopnia $m_1+m_2<m$, gdyż wobec $(m_1,m_2)=1$ mamy $m_1\neq m_2$, skąd wobec $m_1>1$ i $m_2>1$ wynika, że $m_1+m_2<m_1m_2$.

3. Dowieść, że jeżeli p jest liczbą pierwszą, to dla każdej liczby naturalnej $n\leqslant p$ istnieje kongruencja n-tego stopnia

$$x^n+a_1x^{n-1}+a_2x^{n-2}+\dots+a_n\equiv 0 \pmod p,$$

mająca dokładnie n pierwiastków.

Wskazówka. Jest to kongruencja $(x-1)(x-2)\dots(x-n)\equiv 0 \pmod p$.

Jak byłoby tutaj, gdybyśmy liczbę p zastąpili przez liczbę złożoną?

4. Dowieść, że dla każdej liczby naturalnej $m>1$ istnieje taki wielomian $f(x)$ stopnia niższego od m o współczynnikach całkowitych, że przy wszelkim całkowitym x jest

$$x^m \equiv f(x) \pmod m.$$

Dowód. Niech $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ będzie rozkładem liczby m na czynniki pierwsze. W myśl małego twierdzenia Fermata mamy przy wszelkim całkowitym x kongruencję $(x^{p_i} - x)^{\alpha_i} \equiv 0 \pmod{p^{\alpha_i}}$ dla $i = 1, 2, \dots, k$; zatem

$$\prod_{i=1}^{k} (x^{p_i} - x)^{\alpha_i} \equiv 0 \pmod m.$$

Wobec $p_1^{\alpha_1} + p_2^{\alpha_2} + \dots + p_k^{\alpha_k} \leqslant m$ wystarczy więc przyjąć

$$f(x) = x^m - x^{m-(p_1^{\alpha_1} + p_2^{\alpha_2} + \dots + p_k^{\alpha_k})} \prod_{i=1}^{k} (x^{p_i} - x)^{\alpha_i}.$$

5. Dowieść, że dla wszelkich całkowitych x jest

$$(2x+1)^5 - 2x - 1 \equiv 0 \pmod{240}\ ^{1}).$$

6. Dowieść, że dla wszelkich całkowitych x jest

$$x(x^2-49)(x^2+49) \equiv 0 \pmod{30}\ ^{2}).$$

7. Rozsegregować liczby naturalne mniejsze od 23 podług wykładników, do których należą one według modułu 23.

Odpowiedź. Do wykładnika 1 należy tylko liczba 1, do wykładnika 2 — tylko liczba 22, do wykładnika 11 — tylko liczby:

2, 3, 4, 6, 8. 9, 12, 13, 16 i 18,

pozostałe zaś 10 liczb naturalnych, mniejszych od 23, należą do wykładnika 22 (a więc są pierwiastkami pierwotnymi liczby pierwszej 23).

8. Rozsegregować liczby naturalne niewiększe od 30 i pierwsze względem 30 podług wykładników, do których należą one według modułu 30.

Odpowiedź. Liczba 1 należy do wykładnika 1, liczby 11, 19 i 29 — do wykładnika 2, wreszcie liczby 7, 13, 17 i 23 — do wykładnika 4. Jak stąd widać, liczba 30 nie posiada pierwiastków pierwotnych (które musiałyby być liczbami, należącymi do wykładnika 8).

9. Rozsegregować liczby naturalne niewiększe od 25 i pierwsze względem 25 podług wykładników, do których należą one według modułu 25.

Odpowiedź. Do wykładnika 1 należy liczba 1, do wykładnika 2 — liczba 24, do wykładnika 4 — liczby 7 i 18, do wykładnika 5 — liczby 6, 11, 16 i 21, do wykładnika 10 — liczby 4, 9, 14 i 19, do wykładnika 20 — liczby

2, 3, 8, 12, 13, 17, 22 i 23.

Liczba 25 ma więc 8 pierwiastków pierwotnych.

[1]) J. Fitz-Patrick, *Exercices d'Arithmétique*, Wyd. 3-e, Paryż 1914, str. 65, zadanie 430.

[2]) Ob. tamże str. 66, zadanie 435.

10. Rozsegregować liczby naturalne niewiększe od 27 i pierwsze względem 27 podług wykładników, do których należą one według modułu 27.

Odpowiedź. Do wykładnika 1 należy liczba 1, do wykładnika 2 — liczba 26, do wykładnika 3 — liczby 10 i 19, do wykładnika 6 — liczby 8 i 17, do wykładnika 9 — liczby 7, 13, 16, 22, 23 i 25, a do wykładnika 18 — liczby

2, 4, 5, 11, 14 i 20.

Liczba 27 ma więc 6 pierwiastków pierwotnych.

11. Rozsegregować liczby naturalne niewiększe od 32 i pierwsze względem 32 podług wykładników, do których należą one według modułu 32.

Odpowiedź. Do wykładnika 1 należy liczba 1, do wykładnika 2 — liczby 15, 17 i 31, do wykładnika 4 — liczby 7, 9, 23 i 25, do wykładnika 8 — liczby 3, 5, 11, 13, 19, 21, 27 i 29. Pierwiastków pierwotnych liczba 32 nie posiada.

12. Sprawdzić, że dla modułów $m = 2, 3, 6, 12$ i 24 każda taka liczba naturalna n, że $1 < n \leqslant m$ i $(m, n) = 1$, należy do wykładnika 2.

Można dowieść, że innych modułów m o tej własności nie ma.

§ 5. Dowód istnienia pierwiastków pierwotnych liczb pierwszych. Powróćmy do dowodu istnienia pierwiastków pierwotnych. Jako szczególny przypadek twierdzenia 3, gdy za m podstawić liczbę pierwszą p, otrzymujemy następujący

Wniosek. *Według modułu pierwszego p liczby całkowite mogą należeć tylko do wykładników będących dzielnikami liczby $p-1$.*

Niech δ będzie jakimkolwiek dzielnikiem liczby $p-1$. Oznaczmy przez $\psi(\delta)$ liczbę liczb ciągu

$$1, 2, \dots, p-1, \tag{23}$$

należących do wykładnika δ. Ponieważ każda z liczb tego ciągu musi należeć do pewnego wykładnika δ, będącego dzielnikiem liczby $p-1$, więc

$$\sum_{\delta \mid p-1} \psi(\delta) = p-1.$$

Z drugiej strony, jest dla funkcji Gaussa (p. str. 144)

$$\sum_{\delta \mid p-1} \varphi(\delta) = p-1.$$

Zatem

$$\sum_{\delta \mid p-1} [\varphi(\delta) - \psi(\delta)] = 0. \tag{24}$$

Dowiedziemy, że jest stale $\psi(\delta) \leqslant \varphi(\delta)$.

Gdy $\psi(\delta) = 0$, jest to oczywiste; możemy więc założyć, że $\psi(\delta) \neq 0$, czyli że do wykładnika δ należy (według modułu p) co najmniej jedna liczba ciągu (24), np. liczba a. Jest więc

$$a^{\delta} \equiv 1 \pmod p.$$

Liczba a jest przeto jednym z pierwiastków kongruencji

$$x^\delta - 1 \equiv 0 \pmod p. \tag{25}$$

Reszty z dzielenia liczb

$$a^0, a^1, a^2, \ldots, a^{\delta-1}$$

przez p są — jak dowiedliśmy w § 2 (p. str. 174) — wszystkie różne. Oznaczmy ogólnie przez r_k (dla $k=0,1,2,\ldots,\delta-1$) resztę z dzielenia liczby a^k przez p. Zatem

$$r_k{}^\delta \equiv (a^k)^\delta \equiv (a^\delta)^k \equiv 1 \pmod p.$$

Liczby

$$r_0, r_1, r_2, \ldots, r_{\delta-1} \tag{26}$$

są więc wszystkie pierwiastkami kongruencji (25). Lecz kongruencja ta jest stopnia δ i spełnia warunki twierdzenia Lagrange'a, nie może zatem mieć innych pierwiastków prócz δ i liczb (26), które są wszystkie różne, jako różne liczby ciągu (23).

Z drugiej strony, każda liczba należąca do wykładnika δ musi spełniać kongruencję (25); wnosimy stąd, że każda liczba ciągu (23), należąca do wykładnika δ, znajdzie się wśród liczb (26). Zapytamy obecnie, które z liczb (26) istotnie należą do wykładnika δ.

Okażemy, że na to, by liczba r_k należała do wykładnika δ, potrzeba i wystarcza, żeby było $(k,\delta)=1$.

Załóżmy, że warunek $(k,\delta)=1$ jest spełniony. Liczba r_k nie może należeć do wykładnika większego od δ, gdyż spełnia ona w każdym razie kongruencję (25). Liczba r_k należy więc do wykładnika $\delta' \leqslant \delta$ czyli $r_k{}^{\delta'} \equiv 1 \pmod p$, skąd wobec $a^k \equiv r_k \pmod p$ otrzymujemy $a^{k\delta'} \equiv 1 \pmod p$, co dowodzi, że liczba $k\delta'$ jest jednym z pierwiastków kongruencji wykładniczej

$$a^x \equiv 1 \pmod p.$$

W myśl dowiedzionej w § 2 (p. str. 173) własności pierwiastków kongruencji (7) liczba $k\delta'$ musi więc być podzielna przez δ, skąd wynika wobec $(k,\delta)=1$, że δ' jest podzielne przez δ, a zatem wobec $\delta' \leqslant \delta$, że $\delta'=\delta$. Warunek $(k,\delta)=1$ jest więc wystarczający na to, by liczba r_k należała do wykładnika δ.

Załóżmy teraz, że $(k,\delta)=d>1$, skąd

$$k = dk_1 \quad \text{i} \quad \delta = d\delta_1,$$

gdzie $\delta_1 < \delta$. Stąd $k\delta_1 = dk_1\delta_1 = k_1\delta$, a zatem

$$r_k{}^{\delta_1} \equiv a^{k\delta_1} \equiv (a^{k_1})^\delta \equiv 1 \pmod p$$

czyli $r_k{}^{\delta_1} \equiv 1 \pmod p$ dla $\delta_1 < \delta$. Znaczy to, że liczba r_k należy do wykładnika niższego niż δ. Warunek $(k,\delta)=1$ jest więc konieczny, by liczba r_k należała do wykładnika δ.

Streszczając, możemy powiedzieć, że wszystkimi liczbami ciągu (23), należącymi według modułu p do wykładnika δ, są te spośród liczb (26), których wskaźniki są pierwsze względem δ. Takich wskaźników jest oczywiście $\varphi(\delta)$. Dowiedliśmy więc, że gdy $\psi(\delta) \neq 0$, to zachodzi równość $\psi(\delta) = \varphi(\delta)$. W każdym więc razie jest $\psi(\delta) \leqslant \varphi(\delta)$.

Wynika stąd, że żaden ze składników sumy po lewej stronie wzoru (24) nie jest ujemny. Suma składników nieujemnych może jednak być zerem tylko wtedy, gdy każdy z nich jest zerem. Jest więc $\psi(\delta) = \varphi(\delta)$ dla każdego dzielnika δ liczby $p-1$.

Udowodniliśmy w ten sposób

Twierdzenie 6. *Do każdego dzielnika δ liczby $p-1$ należy według modułu p dokładnie $\varphi(\delta)$ różnych liczb ciągu $1,2,\ldots,p-1$.*

Stąd w szczególności dla $\delta = p-1$ otrzymujemy

Wniosek. *Każda liczba pierwsza p ma dokładnie $\varphi(p-1)$ pierwiastków pierwotnych w ciągu liczb $1,2,\ldots,p-1$.*

Jeżeli g jest pierwiastkiem pierwotnym liczby pierwszej p, to wszystkie pozostałe jej pierwiastki pierwotne z ciągu (23) otrzymamy jako reszty (według modułu p) tych wyrazów ciągu

$$g^0,\ g^1,\ g^2,\ \ldots,\ g^{p-2},$$

których wykładniki są pierwsze względem liczby $p-1$. Wobec tego w tablicach pierwiastków pierwotnych podaje się jeden tylko pierwiastek, zwykle najmniejszy.

Będziemy go oznaczali przez $\gamma(p)$.

Oto najmniejsze pierwiastki pierwotne liczb pierwszych nieparzystych p, mniejszych od 100:

p	3	5	7	11	13	17	19	23	29	31	37	41
$\gamma(p)$	2	2	3	2	2	3	2	5	2	3	2	6

p	43	47	53	59	61	67	71	73	79	83	89	97
$\gamma(p)$	3	5	2	2	2	2	7	5	3	2	3	5

Nie wiadomo, ile jest liczb pierwszych, dla których pierwiastkiem pierwotnym jest liczba 2.

Nie posiadamy dotąd bezpośredniej metody wyznaczania pierwiastków pierwotnych [1]).

Jak widzimy z tabliczki, dla liczb pierwszych $p<100$ jest $\gamma(p)\leqslant 7$. Dla liczb pierwszych $p<191$ jest także $\gamma(p)\leqslant 7$, lecz $\gamma(191)=19$; dla liczb pierwszych $p<409$ jest $\gamma(p)\leqslant 19$, lecz $\gamma(409)=21$; dla liczb pierwszych $p<3361$ jest $\gamma(p)\leqslant 21$, lecz $\gamma(3361)=22$; dla liczb pierwszych $p<5711$ jest $\gamma(p)\leqslant 22$, lecz $\gamma(5711)=29$; dla liczb pierwszych $p<5881$ jest $\gamma(p)\leqslant 29$, lecz $\gamma(5881)=31$ [2]).

Z istnienia pierwiastków pierwotnych liczb pierwszych wynika, że jeżeli liczba naturalna n jest pierwsza, to istnieje taka liczba naturalna g, że

$$n \mid g^{n-1}-1 \tag{27}$$

i że $n-1$ jest najmniejszym wykładnikiem naturalnym o własności (27).

Łatwo widzieć, że i na odwrót: jeżeli dla liczby naturalnej $n>1$ istnieje taka liczba naturalna g, to liczba n jest pierwsza.

Istotnie, przypuśćmy, że liczba n jest złożona. Jeżeli dla pewnego naturalnego g zachodzi podzielność (27), to musi być $(g,n)=1$, a zatem $n \mid g^{\varphi(n)}-1$ w myśl twierdzenia Eulera. Lecz skoro liczba n jest złożona, mamy $\varphi(n)<n-1$.

Możemy więc wypowiedzieć następujące

Twierdzenie 7. *Na to, by liczba naturalna $n>1$ była pierwsza, potrzeba i wystarcza, żeby istniała taka liczba naturalna g, że $n \mid g^{n-1}-1$ i że dla żadnej liczby naturalnej $x<n-1$ nie jest $n \mid g^x-1$.*

W związku z wyznaczaniem pierwiastków pierwotnych, obliczano tablice [3]), dające dla liczb pierwszych p taki najmniejszy wykładnik naturalny x, że

$$2^x \equiv 1 \pmod{p}.$$

[1]) Więcej szczegółów o wyznaczaniu pierwiastków pierwotnych znajdzie czytelnik w monografii: E. Poznański, *Pierwiastki pierwotne liczb pierwszych*, Warszawa 1901, 63 stronice.

[2]) Według tablic podanych w książce: G. Wertheim, *Anfangsgründe der Zahlenlehre*, Brunświk 1902, str. 406-409.

[3]) Ob. np. N. G. W. H. Berger, New Archiv Wiskunde (2), tom 20 (1940), str. 307 i 308 oraz tom 22 (1948) str. 310 i 311.

§ 6. Pierwiastki pierwotne dla modułów p^α i $2p^\alpha$. Zajmiemy się teraz przypadkiem, kiedy moduł jest potęgą liczby pierwszej nieparzystej.

Udowodnimy przede wszystkim następujący

Lemat. *Jeżeli dla pewnego g całkowitego oraz n i s naturalnych jest*

$$g^n = 1 + kp^s, \tag{28}$$

gdzie k jest liczbą całkowitą, to

$$g^{np} = 1 + lp^{s+1},$$

gdzie l jest liczbą całkowitą; nadto jeżeli k jest niepodzielne przez p, to i l jest niepodzielne przez p.

Dowód. W myśl (28) jest

$$g^{np} = (1+kp^s)^p = 1 + \frac{p}{1}kp^s + \frac{p(p-1)}{1\cdot 2}k^2p^{2s} + \ldots,$$

gdzie wszystkie składniki, poczynając od trzeciego, są oczywiście podzielne przez p^{2s+1}, a zatem i przez p^{s+2} (wobec $2s+1 \geqslant s+2$, gdyż s jest naturalne). Możemy więc napisać

$$g^{np} = 1 + kp^{s+1} + k'p^{s+2} = 1 + lp^{s+1},$$

gdzie wobec całkowitości liczby k' liczba $l=k+k'p$ jest całkowita i — w razie niepodzielności liczby k przez p — również niepodzielna przez p.

Twierdzenie 8. *Na to, by liczba g była pierwiastkiem pierwotnym liczby p^α, gdzie p jest liczbą pierwszą nieparzystą i $\alpha>1$, potrzeba i wystarcza, żeby liczba g była takim pierwiastkiem pierwotnym liczby p, dla którego liczba $g^{p-1}-1$ nie jest podzielna przez p^2.*

Dowód. Załóżmy, że liczba g jest pierwiastkiem pierwotnym liczby p^α, gdzie $\alpha>1$. Niech δ będzie wykładnikiem, do którego należy liczba g według modułu p. Jest więc

$$g^\delta \equiv 1 \pmod{p}$$

czyli różnica $g^\delta-1$ jest podzielna przez p. Oznaczając teraz przez p^s najwyższą potęgę liczby p, przez którą różnica $g^\delta-1$ jest podzielna, możemy napisać

$$g^\delta = 1 + kp^s, \tag{29}$$

gdzie k jest liczbą całkowitą niepodzielną przez p, a s — liczbą naturalną. W myśl dowiedzionego lematu, dostajemy stąd

$$g^{\delta p}=1+k_1 p^{s+1},$$

gdzie $k_1\not\equiv 0 \pmod p$. Stosując ten lemat jeszcze raz (dla $n=\delta p$), otrzymujemy

$$g^{\delta p^2}=1+k_2 p^{s+2},$$

dalej w ten sam sposób

$$g^{\delta p^3}=1+k_3 p^{s+3},$$

. . . . . .

$$g^{\delta p^{\alpha-2}}=1+k_{\alpha-2} p^{s+\alpha-2} \tag{30}$$

i wreszcie

$$g^{\delta p^{\alpha-1}}=1+k_{\alpha-1} p^{s+\alpha-1}, \tag{31}$$

gdzie $k, k_1, \ldots, k_{\alpha-1}$ są liczbami całkowitymi. Równość (31) daje wobec $s\geqslant 1$ kongruencję

$$g^{\delta p^{\alpha-1}}\equiv 1 \pmod{p^\alpha}, \tag{32}$$

a że — jak założyliśmy — liczba g należy według modułu p^α do wykładnika $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$, więc z kongruencji (32) wynika, że liczba $\delta p^{\alpha-1}$ jest podzielna przez $p^{\alpha-1}(p-1)$, skąd wnosimy, że liczba δ jest podzielna przez $p-1$. Ponieważ zaś δ, jako wykładnik, do którego należy g według modułu p, musi być dzielnikiem liczby $\varphi(p)=p-1$, więc $\delta=p-1$. Liczba g jest zatem pierwiastkiem pierwotnym liczby p.

Otóż gdyby liczba $g^{p-1}-1$ była podzielna przez p^2, to moglibyśmy napisać $g^{p-1}=1+kp^2$ przy k całkowitym i przeto, wobec $\delta=p-1$, przyjąć $s=2$ we wzorze (29). Byłoby więc $s+\alpha-2\geqslant\alpha$, skąd w myśl (30) $g^{(p-1)p^{\alpha-2}}\equiv 1 \pmod{p^\alpha}$ wbrew założeniu, że g jest pierwiastkiem pierwotnym liczby p^α. Dowiedliśmy więc, że jeżeli g jest pierwiastkiem pierwotnym liczby p^α, gdzie p jest liczbą pierwszą i $\alpha>1$, to g jest też pierwiastkiem pierwotnym liczby p i liczba $g^{p-1}-1$ nie jest podzielna przez p^2. Warunek jest więc konieczny.

By udowodnić, że jest zarazem dostateczny, załóżmy, że g jest takim pierwiastkiem pierwotnym liczby p, dla którego $g^{p-1}-1$ jest niepodzielne przez p^2. Możemy więc napisać

$$g^{p-1}=1+kp, \tag{33}$$

gdzie k jest liczbą całkowitą niepodzielną przez p (różnica $g^{p-1}-1$ jest w każdym razie podzielna przez p, skoro g jest pierwiastkiem pierwotnym liczby p).

W myśl lematu jest

$$g^{(p-1)p}=1+k_1 p^2,$$

gdzie k_1 jest liczbą całkowitą niepodzielną przez p. Stosując lemat w dalszym ciągu, otrzymujemy

$$g^{(p-1)p^2}=1+k_2 p^3, \quad \ldots, \quad g^{(p-1)p^{\alpha-2}}=1+k_{\alpha-2}p^{\alpha-1},$$

gdzie liczby $k_2, k_3, \ldots, k_{\alpha-2}$ są całkowite i niepodzielne przez p. Ostatnia z tych równości wskazuje, że

$$g^{(p-1)p^{\alpha-2}}\not\equiv 1 \pmod{p^\alpha}. \tag{34}$$

Oznaczmy przez d wykładnik, do którego należy g według modułu p^α. Jest więc

$$g^d\equiv 1 \pmod{p^\alpha} \tag{35}$$

i tym bardziej $g^d\equiv 1 \pmod p$, skąd wobec założenia, że g jest pierwiastkiem pierwotnym liczby p, wynika, że d jest podzielne przez $p-1$, czyli że

$$d=l(p-1), \tag{36}$$

gdzie l jest całkowite.

Z drugiej strony, g może według modułu p^α należeć tylko do wykładnika, który jest dzielnikiem liczby $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$; zatem $p^{\alpha-1}(p-1)$ jest podzielne przez $l(p-1)$, czyli $p^{\alpha-1}$ przez l, skąd $l=p^\beta$, gdzie $\beta\leqslant\alpha-1$.

Wynika stąd na mocy (36), że $d=p^\beta(p-1)$, gdzie $\beta\leqslant\alpha-1$. Gdyby było $\beta<\alpha-1$ czyli $\beta\leqslant\alpha-2$, to d byłoby dzielnikiem liczby $p^{\alpha-2}(p-1)$ i wobec (35) mielibyśmy kongruencję

$$g^{(p-1)p^{\alpha-2}}\equiv 1 \pmod{p^\alpha}$$

wbrew (34). Jest więc $\beta=\alpha-1$ czyli $d=p^{\alpha-1}(p-1)=\varphi(p^\alpha)$, co dowodzi, że liczba g jest pierwiastkiem pierwotnym liczby p^α. Warunek jest więc dostateczny, c. b. d. d.

Wniosek 1. *Każda liczba p^α, gdzie p jest liczbą pierwszą nieparzystą i $\alpha>1$, ma co najmniej jeden pierwiastek pierwotny.*

Dowód. W myśl twierdzenia 8 wystarczy okazać, że istnieje taki pierwiastek pierwotny g liczby pierwszej nieparzystej p, dla którego liczba $g^{p-1}-1$ nie jest podzielna przez p^2. Niech g_0 bę-

dzie jakimkolwiek pierwiastkiem pierwotnym liczby p. Jest więc $g_0^{p-1} \equiv 1 \pmod p$ czyli

$$g_0^{p-1} = 1 + k_0 p, \tag{37}$$

gdzie k_0 jest liczbą całkowitą niepodzielną przez p. Kongruencja

$$g_0^{p-2} x \equiv k_0 - 1 \pmod p$$

jest rozwiązalna, gdyż g_0, a więc i g_0^{p-2}, jest liczbą pierwszą względem modułu p. Niech x_0 będzie pierwiastkiem tej kongruencji. Zatem

$$g_0^{p-2} x_0 = k_0 - 1 + tp, \tag{38}$$

gdzie t jest liczbą całkowitą.

Określmy g wzorem

$$g = g_0 + x_0 p.$$

Wobec $g \equiv g_0 \pmod p$, liczba g jest pierwiastkiem pierwotnym liczby p oraz

$$g^{p-1} = (g_0 + x_0 p)^{p-1} =$$

$$= g_0^{p-1} + (p-1) g_0^{p-2} x_0 p + \frac{(p-1)(p-2)}{1 \cdot 2} g_0^{p-3} x_0^2 p^2 + \ldots,$$

gdzie wszystkie składniki szeregu po prawej stronie są, poczynając od trzeciego, podzielne przez p^2. Możemy więc napisać

$$g^{p-1} = g_0^{p-1} + (p-1) g_0^{p-2} x_0 p + k p^2,$$

gdzie k jest liczbą całkowitą. Stąd na mocy (37) i (38):

$$g^{p-1} = 1 + k_0 p + (p-1) p (k_0 - 1 + tp) + k p^2 =$$

$$= 1 + p + (k_0 - 1 + tp - t + k) p^2 = 1 + p + l p^2,$$

czyli $g^{p-1} - 1 = p + l p^2$ gdzie l jest liczbą całkowitą. Wynika stąd natychmiast, że $g^{p-1} - 1$ nie jest podzielne przez p^2, c. b. d. o.

Wniosek 2. *Każdy pierwiastek pierwotny nieparzysty liczby p^α (gdzie p jest liczbą pierwszą nieparzystą, a zaś — liczbą naturalną) jest zarazem pierwiastkiem pierwotnym liczby $2p^\alpha$.*

Dowód. Niech g będzie pierwiastkiem pierwotnym nieparzystym liczby p^α. Liczba g jest więc pierwsza względem $2p^\alpha$ i przeto należy według modułu $2p^\alpha$ do pewnego wykładnika (naturalnego) δ. Zatem $g^\delta \equiv 1 \pmod{2p^\alpha}$, a więc tym bardziej $g^\delta \equiv 1 \pmod{p^\alpha}$, skąd wnosimy (skoro g jest pierwiastkiem pierwotnym liczby p^α), że δ jest podzielne przez $\varphi(p^\alpha)$ i przeto że $\delta \geqslant \varphi(p^\alpha)$.

Lecz ze wzorów dla funkcji Gaussa (p. str. 140) wynika, że

$$\varphi(2p^\alpha) = \varphi(2)\varphi(p^\alpha) = \varphi(p^\alpha).$$

Zatem $\delta \geqslant \varphi(2p^\alpha)$, skąd wnosimy, że g należy według modułu $2p^\alpha$ do wykładnika $\varphi(2p^\alpha)$ czyli jest pierwiastkiem pierwotnym liczby $2p^\alpha$, c. b. d. d.

Z wniosków 1 i 2 wynika od razu, że *liczba* $2p^\alpha$ (gdzie p jest liczbą pierwszą nieparzystą i $\alpha \geqslant 1$) *posiada pierwiastek pierwotny.*

W tym celu wystarczy bowiem okazać, że istnieje pierwiastek pierwotny nieparzysty liczby p^α. Otóż na mocy wniosków 1 i 2 liczba p^α posiada co najmniej jeden pierwiastek pierwotny: jeżeli jest nim liczba g, to liczba $g + p^\alpha$, jako przystająca do g według modułu p^α, również jest pierwiastkiem pierwotnym liczby p^α, z dwu zaś liczb g i $g + p^\alpha$ (wobec nieparzystości liczby p) zawsze jedna jest nieparzysta.

§ 7. Liczba pierwiastków pierwotnych według jakiegokolwiek modułu. Załóżmy, że liczba m ma pierwiastek pierwotny g. Jak wiemy z twierdzenia 2, dla każdej liczby n, pierwszej względem m, istnieje w ciągu $0, 1, \ldots, \varphi(m) - 1$ jeden i tylko jeden taki wykładnik x, iż

$$g^x \equiv n \pmod m.$$

Jest to wykładnik $x = \operatorname{ind}_g n$ (ob. str. 174).

Niech a będzie liczbą pierwszą względem m, a δ — wykładnikiem, do którego należy a według modułu m. Niech dla skrócenia:

$$k = \operatorname{ind}_g a, \qquad s = \varphi(m), \qquad d = (k, s). \tag{39}$$

Udowodnimy następujące

Twierdzenie 9. $\delta = \frac{s}{d}$, *tj. wykładnik, do którego należy a według modułu m, jest równy ilorazowi z dzielenia liczby $\varphi(m)$ przez największy wspólny dzielnik liczb* $\operatorname{ind}_g a$ *i* $\varphi(m)$.

Dowód. Wyznaczmy liczby k, s i d ze wzorów (39) i przyjmijmy

$$h = \frac{s}{d}.$$

Na mocy określenia liczby k jest więc

$$a^h \equiv g^{kh} \pmod m, \tag{40}$$

gdzie $kh=s\frac{k}{d}$, a z określenia liczby d wynika, że k jest podzielne przez d; zatem kh jest podzielne przez $s=\varphi(m)$, wobec czego kongruencja (40) daje

$$a^h\equiv 1 \pmod m,$$

skąd $\delta\leqslant h$.

Z drugiej strony, ponieważ na mocy (39)

$$g^{k\delta}\equiv a^{\delta}\equiv 1 \pmod m,$$

więc (z uwagi, że g jest pierwiastkiem pierwotnym liczby m) jest $k\delta=ts$, gdzie t jest liczbą całkowitą. Stąd

$$\frac{k}{d}\delta=t\frac{s}{d},$$

a ponieważ $\left(\frac{k}{d},\frac{s}{d}\right)=1$, więc wnosimy, że δ jest podzielne przez $\frac{s}{d}=h$, czyli że $\delta\geqslant h$.

Nierówności $\delta\leqslant h$ i $\delta\geqslant h$ dają $\delta=h$ czyli $\delta=\frac{s}{d}$, c. b. d. o.

Udowodnione twierdzenie 9 pozwoli nam w założeniu, że istnieje przynajmniej jeden pierwiastek pierwotny g liczby m, obliczyć, ile jest w ciągu

(41) $$1,\ 2,\ \ldots,\ m$$

liczb, należących według modułu m do danego wykładnika δ, będącego dzielnikiem liczby $\varphi(m)$.

Jak wiemy (ob. str. 174), jeżeli g jest pierwiastkiem pierwotnym liczby m, to wyznaczając reszty z dzielenia przez m kolejnych potęg

(42) $$g^0, g^1, \ldots, g^{\varphi(m)-1},$$

otrzymamy wszystkie wyrazy ciągu (41), pierwsze względem m. Ponieważ liczby przystające do siebie według modułu m należą do tego samego wykładnika, więc wystarczy obliczyć, ile wyrazów ciągu (42) należy do wykładnika δ.

Oczywiście $\mathrm{ind}_g(g^k)=k$ dla $k=0,1,\ldots,\varphi(m)-1$; wskaźnikami liczb (42) są więc liczby

(43) $$0,\ 1,\ \ldots,\ \varphi(m)-1.$$

Wystarczy przeto z uwagi na wzór $\delta=\frac{s}{(k,s)}$ obliczyć, ile wyrazów ciągu (43) spełnia warunek $(k,s)=\frac{s}{\delta}$, tj. ile liczb z ciągu (43) ma z liczbą $\varphi(m)$ największy wspólny dzielnik $d=\frac{s}{\delta}$.

Na to, żeby liczba n miała z liczbą $\varphi(m)$ największy wspólny dzielnik d, potrzeba i wystarcza, iżby było $n=ld$, gdzie l jest liczbą pierwszą względem $\frac{\varphi(m)}{d}=\delta$ (p. Rozdział 1, § 3, str. 3); stąd obliczamy z łatwością, że w ciągu (43) jest $\varphi(\delta)$ liczb, mających z liczbą $\varphi(m)$ największy wspólny dzielnik d.

Udowodniliśmy więc następujące

Twierdzenie 10. *Jeżeli liczba m ma pierwiastek pierwotny, to w ciągu $1,2,\ldots,m$ jest dokładnie $\varphi(\delta)$ liczb należących do wykładnika δ, będącego dzielnikiem liczby $\varphi(m)$.*

Stąd w szczególności dla $\delta=\varphi(m)$, *jeżeli liczba m ma co najmniej jeden pierwiastek pierwotny, to ma ona w ciągu $1,2,\ldots,m$ dokładnie $\varphi(\varphi(m))$ pierwiastków pierwotnych.*

W szczególności więc, jeżeli p jest liczbą pierwszą nieparzystą, α zaś — liczbą naturalną, to każda z liczb p^α i $2p^\alpha$ ma $\varphi(p^{\alpha-1}(p-1))$ nieprzystających do siebie pierwiastków pierwotnych.

Na podstawie twierdzeń 6-10 i wniosków z nich możemy więc wypowiedzieć następujące

Twierdzenie 11. *Pierwiastki pierwotne mają tylko następujące liczby m:*

$$2,\quad 4,\quad p^\alpha\quad i\quad 2p^\alpha,$$

gdzie p jest liczbą pierwszą nieparzystą, α zaś — liczbą naturalną. Dla każdej z powyższych liczb m w ciągu $1,2,\ldots,m$ jest dokładnie $(\varphi(\varphi(m))$ pierwiastków pierwotnych.

§ 8. Moduł 2^α dla $\alpha\geqslant 3$. Własność liczby 5. Zajmiemy się obecnie modułem $m=2^\alpha$, gdzie $\alpha\geqslant 3$. Ponieważ $\varphi(2^\alpha)=2^{\alpha-1}$, więc liczby mogą należeć według modułu 2^α jedynie do tych wykładników δ, które są dzielnikami liczby $2^{\alpha-1}$ czyli mają postać $\delta=2^\nu$, gdzie $\nu\leqslant\alpha-1$. Dla $\alpha\geqslant 3$ nie ma — jak wiemy z twierdzenia 5 (§ 3, str. 177) — żadnej liczby, należącej według modułu 2^α do wykładnika $2^{\alpha-1}$; w razie więc $\alpha\geqslant 3$, musi być $\delta=2^\nu$, gdzie $\nu\leqslant\alpha-2$.

Okażemy, że (dla $\alpha \geqslant 3$) zawsze istnieje co najmniej jedna liczba, należąca według modułu 2^α do wykładnika $2^{\alpha-2}$, mianowicie, że taką liczbą jest 5.

Oznaczmy przez δ wykładnik, do którego liczba 5 należy według modułu 2^α; jak widzieliśmy, musi być $\delta = 2^\nu$. Przypuśćmy, że $\delta < 2^{\alpha-2}$; byłoby więc $\nu < \alpha-2$ czyli $\nu \leqslant \alpha-3$, a więc $2^{\alpha-3}$ byłoby w każdym razie podzielne przez $2^\nu = \delta$ i z kongruencji

$$5^\delta \equiv 1 \pmod{2^\alpha}$$

wynikałaby kongruencja

$$5^{2^{\alpha-3}} \equiv 1 \pmod{2^\alpha}. \tag{44}$$

Z drugiej strony jednak jest

$$5 = 1 + 1 \cdot 2^2.$$

Przypuśćmy, że dla pewnego n naturalnego jest

$$5^{2^{n-1}} = 1 + h_n 2^{n+1}, \tag{45}$$

gdzie h_n jest liczbą nieparzystą; jest to prawdziwe dla $n=1$. Podnosząc do kwadratu obie strony równości (45), dostalibyśmy

$$5^{2^n} = 1 + 2h_n \cdot 2^{n+1} + h_n^2 \cdot 2^{2n+2} = 1 + (h_n + 2^n h_n^2) 2^{n+2} = 1 + h_{n+1} 2^{n+2},$$

gdzie $h_{n+1} = h_n + 2^n h_n^2$ byłoby liczbą nieparzystą wobec nieparzystości liczby h_n i założenia, że $n \geqslant 1$. Wzór (45) zachodziłby więc dla wszelkiego n naturalnego, skąd dla $n = \alpha-2$ byłoby

$$5^{2^{\alpha-3}} = 1 + h_{\alpha-2} \cdot 2^{\alpha-1},$$

co dowodzi, że różnica $5^{2^{\alpha-3}} - 1 = h_{\alpha-2} \cdot 2^{\alpha-1}$ byłaby wobec nieparzystości liczby $h_{\alpha-2}$ niepodzielna przez 2^α, wbrew (44).

Jest więc $\delta \geqslant 2^{\alpha-2}$, a że z drugiej strony, jak wiemy, $\delta = 2^\nu$, gdzie $\nu \leqslant \alpha-2$, więc musi być $\delta = 2^{\alpha-2}$, c. b. d. o.

Udowodniliśmy zatem, że *dla* $\alpha \geqslant 3$ *liczba* 5 *należy według modułu* 2^α *do wykładnika* $2^{\alpha-2}$.

Wynika stąd pewna ciekawa własność liczby 5. Aby ją wyprowadzić, zauważymy przede wszystkim, że skoro 5 należy według modułu 2^α ($\alpha \geqslant 3$) do wykładnika $2^{\alpha-2}$, to reszty z dzielenia wyrazów ciągu

$$5^0,\ 5^1,\ 5^2,\ \ldots,\ 5^{2^{\alpha-2}-1} \tag{46}$$

przez liczbę 2^α są wszystkie różne (zob. § 2, str. 174). Stąd wynika natychmiast, że reszty z dzielenia wyrazów ciągu

$$-5^0,\ -5^1,\ -5^2,\ \ldots,\ -5^{2^{\alpha-2}-1} \tag{47}$$

przez liczbę 2^α też są wszystkie różne, gdyż w razie, gdyby $-5^\mu \equiv -5^\nu \pmod{2^\alpha}$, mielibyśmy zarazem $5^\mu \equiv 5^\nu \pmod{2^\alpha}$.

Okażemy, że każdy wyraz ciągu (46) daje przy dzieleniu przez 2^α resztę różną od reszty każdego z wyrazów ciągu (47).

Istotnie, gdyby było

$$5^\mu \equiv -5^\nu \pmod{2^\alpha},$$

to wobec $\alpha \geqslant 3$ byłoby tym bardziej

$$5^\mu \equiv -5^\nu \pmod 4,$$

a więc wobec $5 \equiv 1 \pmod 4$ również $1 \equiv -1 \pmod 4$, co niemożliwe.

Dowiedliśmy więc, że dzieląc każdą z $2^{\alpha-1}$ liczb

$$\begin{matrix} 5^0, & 5^1, & 5^2, & \ldots, & 5^{2^{\alpha-2}-1}, \\ -5^0, & -5^1, & -5^2, & \ldots, & -5^{2^{\alpha-2}-1} \end{matrix} \tag{48}$$

przez liczbę 2^α, otrzymujemy same różne reszty. Z drugiej strony reszty te muszą być wszystkie nieparzyste, gdyż liczby (48) są wszystkie nieparzyste. Ponieważ wreszcie wszystkich różnych reszt nieparzystych według modułu 2^α jest tylko $2^{\alpha-1}$, więc wnosimy, że reszty liczb (48) według modułu 2^α różnią się co najwyżej porządkiem od liczb ciągu

$$1,\ 3,\ 5,\ 7,\ \ldots,\ 2^\alpha - 1.$$

Wynika stąd, że każda liczba nieparzysta przystaje według modułu 2^α do jednej i tylko jednej z liczb (48). Możemy więc wypowiedzieć następujące

Twierdzenie 12. *Dla każdej liczby nieparzystej* n *(przy danym module* 2^α, *gdzie* $\alpha \geqslant 3$*) można wyznaczyć i to w jeden tylko sposób liczby całkowite* ε *i* η, *spełniające warunki:*

$$0 \leqslant \varepsilon \leqslant 1, \qquad 0 \leqslant \eta \leqslant 2^{\alpha-2} - 1, \qquad n \equiv (-1)^\varepsilon 5^\eta \pmod{2^\alpha}.$$

Układy wykładników ε, η grają więc dla modułu 2^α niejako rolę wskaźników.

Można by z łatwością dowieść, że wyprowadzoną własność liczby 5 posiada każda liczba formy $8k+5$, gdzie k jest liczbą

całkowitą. Rozumowanie byłoby takie samo, jak dla liczby 5; wystarczyłoby się tylko oprzeć na uwadze, że każda liczba formy $8k+5$ daje się przedstawić w postaci $1+2^2h$, gdzie h jest liczbą nieparzystą.

§ 9. Własności wskaźników. Zajmiemy się obecnie bliższym zbadaniem własności wskaźników (indeksów).

Niech g będzie jakimkolwiek pierwiastkiem pierwotnym liczby m. Póki będzie mowa o wskaźnikach przy jednej i tej samej podstawie g, będziemy pisali przez skrócenie $\operatorname{ind} x$ zamiast $\operatorname{ind}_g x$.

Udowodnimy następujące własności wskaźników:

I. *Liczby przystające według modułu m mają jednakowe wskaźniki* (oczywiście przy tej samej zasadzie i w założeniu, że liczby te są pierwsze względem m).

Istotnie, na mocy kongruencji

$$a \equiv b \pmod m,$$

oraz (w myśl definicji wskaźników) na mocy kongruencji

$$g^{\operatorname{ind} a} \equiv a \pmod m,$$

jest zarazem

$$g^{\operatorname{ind} a} \equiv b \pmod m. \tag{49}$$

Skoro g jest pierwiastkiem pierwotnym dla modułu m, to na mocy twierdzenia 4, str. 174, kongruencja wykładnicza

$$g^x \equiv b \pmod m$$

ma (wobec tego, że b jest pierwsze względem m) tylko jeden pierwiastek nieujemny mniejszy od $\varphi(m)$, który oznaczamy właśnie symbolem $\operatorname{ind} b$. Tym pierwiastkiem jest więc w myśl kongruencji (49) liczba $\operatorname{ind} a$, skąd

$$\operatorname{ind} a = \operatorname{ind} b,$$

c. b. d. o.

Wobec udowodnionej własności wskaźników, w tablicach wskaźników podawane są tylko ich wartości dla liczb naturalnych mniejszych od modułu (oczywiście pierwszych względem modułu).

II. *Wskaźnik iloczynu przystaje według modułu $\varphi(m)$ do sumy wskaźników czynników:*

$$\operatorname{ind}(ab) \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{\varphi(m)}. \tag{50}$$

Istotnie, w myśl definicji wskaźników (przy wszelkich a i b pierwszych względem m) mamy

$$g^{\operatorname{ind} a} \equiv a \pmod m, \qquad g^{\operatorname{ind} b} \equiv b \pmod m,$$

skąd, mnożąc stronami,

$$g^{\operatorname{ind} a + \operatorname{ind} b} \equiv ab \pmod m,$$

a że mamy również

$$g^{\operatorname{ind}(ab)} \equiv ab \pmod m,$$

więc

$$g^{\operatorname{ind} ab} \equiv g^{\operatorname{ind} a + \operatorname{ind} b} \pmod m. \tag{51}$$

Załóżmy, że przy wykładnikach całkowitych nieujemnych μ i ν zachodzi kongruencja

$$g^\mu \equiv g^\nu \pmod m.$$

Jeżeli $\mu \geqslant \nu$, to możemy tę kongruencję napisać w postaci

$$g^\nu (g^{\mu-\nu} - 1) \equiv 0 \pmod m,$$

skąd wynika wobec $(g, m) = 1$ podzielność różnicy $g^{\mu-\nu} - 1$ przez m czyli kongruencja

$$g^{\mu-\nu} \equiv 1 \pmod m.$$

Wnosimy stąd na mocy twierdzenia 3 (§ 2, str. 173), że $\mu - \nu$ jest podzielne przez $\varphi(m)$ czyli że

$$\mu \equiv \nu \pmod{\varphi(m)}.$$

Do tego samego wniosku dochodzimy oczywiście również przy założeniu, że $\nu \geqslant \mu$. Kongruencja (51) pociąga więc kongruencję (50), c. b. d. o.

Dowiedzioną własność możemy uogólnić od razu na dowolną liczbę czynników.

Jako natychmiastowy wniosek otrzymujemy własność

III. *Wskaźnik potęgi przystaje według modułu $\varphi(m)$ do iloczynu wykładnika przez wskaźnik podstawy:*

$$\operatorname{ind}(a^n) \equiv n \operatorname{ind} a \pmod{\varphi(m)}.$$

Wyprowadzimy obecnie zależność między indeksami przy różnych zasadach. Niech g i γ będą dwoma różnymi pierwiastkami pierwotnymi modułu m. Mamy w myśl definicji wskaźników

$$a \equiv g^{\operatorname{ind}_g a} \pmod m.$$

Biorąc po obu stronach wskaźniki przy zasadzie γ i stosując własności I i III, otrzymujemy

$$\operatorname{ind}_\gamma a \equiv \operatorname{ind}_g a \cdot \operatorname{ind}_\gamma g \pmod{\varphi(m)}. \tag{52}$$

Zatem, *chcąc zmienić zasadę wskaźników, trzeba je tylko wszystkie pomnożyć przez jedną i tę samą liczbę (mianowicie przez wskaźnik starej zasady przy nowej) i wyznaczyć odpowiednie reszty tych iloczynów według modułu* $\varphi(m)$.

§ 10. Zastosowania wskaźników. Własności charakterystyczne symbolu Legendre'a. Niech p będzie liczbą pierwszą nieparzystą, g — pierwiastkiem pierwotnym tej liczby, a D — liczbą niepodzielną przez p.

Twierdzenie 13. *Na to, by liczba* D *była resztą kwadratową liczby pierwszej nieparzystej* p, *potrzeba i wystarcza, by* $\operatorname{ind} D$ *był liczbą parzystą.*

Dowód. Załóżmy, że $\operatorname{ind}_g D = 2k$; zatem

$$g^{2k} \equiv D \pmod{p},$$

co dowodzi, że kongruencja

$$x^2 \equiv D \pmod{p}$$

ma pierwiastek $x = g^k$. Liczba D jest więc resztą kwadratową dla p. W ciągu

$$1, 2 \ldots, p-1$$

jest oczywiście $\frac{p-1}{2}$ liczb, których wskaźniki są parzyste (gdyż wskaźniki te różnią się co najwyżej porządkiem od wyrazów ciągu $0, 1, \ldots, p-2$, wśród których jest $\frac{p-1}{2}$ parzystych); każda z nich jest więc resztą kwadratową liczby p. Ale w ciągu liczb $1, 2, \ldots, p-1$ jest — jak wiadomo — tylko $\frac{p-1}{2}$ reszt kwadratowych liczby p. Stąd wniosek, że żaden wyraz tego ciągu o wskaźniku nieparzystym nie jest resztą kwadratową liczby p. Dowiedliśmy więc twierdzenia 13.

Wynika z niego też, że parzystość lub nieparzystość wskaźnika nie zależy od zasady wskaźników, lecz tylko od liczby D i od modułu p.

Z twierdzenia 13 i definicji symbolu Legendre'a (Rozdział IV, § 1, str. 62) wynika natychmiast, że

$$\left(\frac{D}{p}\right) = (-1)^{\operatorname{ind} D}$$

dla każdej liczby D niepodzielnej przez p. Jeżeli D i D' są liczbami niepodzielnymi przez p, to wynika stąd dalej:

$$\left(\frac{DD'}{p}\right) = (-1)^{\operatorname{ind} DD'},$$
$$\left(\frac{D}{p}\right)\left(\frac{D'}{p}\right) = (-1)^{\operatorname{ind} D + \operatorname{ind} D'}. \tag{53}$$

W myśl własności II jest wobec $\varphi(p) = p-1$

$$\operatorname{ind} DD' \equiv \operatorname{ind} D + \operatorname{ind} D' \pmod{p-1},$$

skąd wobec parzystości liczby $p-1$ tym bardziej

$$\operatorname{ind} DD' \equiv \operatorname{ind} D + \operatorname{ind} D' \pmod 2,$$

a zatem

$$(-1)^{\operatorname{ind} DD'} = (-1)^{\operatorname{ind} D + \operatorname{ind} D'}.$$

Wzory (53) dają więc

$$\left(\frac{DD'}{p}\right) = \left(\frac{D}{p}\right)\left(\frac{D'}{p}\right). \tag{54}$$

Wyznaczymy wszystkie rodzaje symboli $\left[\frac{D}{p}\right]$, mających oznaczoną wartość rzeczywistą dla każdej liczby całkowitej D niepodzielnej przez liczbę pierwszą nieparzystą p i spełniających następujące dwa warunki:

(A) $$\left[\frac{D}{p}\right] = \left[\frac{D'}{p}\right]$$

(B) $$\left[\frac{DD'}{p}\right] = \left[\frac{D}{p}\right]\left[\frac{D'}{p}\right]$$

dla $D \equiv D' \pmod{p}$.

Niech g będzie pierwiastkiem pierwotnym liczby p. Dla każdej liczby całkowitej D niepodzielnej przez p jest zatem

$$D \equiv g^{\operatorname{ind} D} \pmod{p},$$

skąd, stosując własność (A), a potem własność (B), dostajemy

$$\left[\frac{D}{p}\right] = \left[\frac{g^{\operatorname{ind} D}}{p}\right] = \left[\frac{g}{p}\right]^{\operatorname{ind} D}. \tag{55}$$

Niech $\left[\frac{g}{p}\right]=a$. Wobec kongruencji $g^{p-1}\equiv 1 \pmod p$ oraz własności (A) i (B) mamy

$$\left[\frac{g}{p}\right]^{p-1}=\left[\frac{g^{p-1}}{p}\right]=\left[\frac{1}{p}\right]. \tag{56}$$

Z równości (B) dostajemy dla $D=D'=1$

$$\left[\frac{1}{p}\right]=\left[\frac{1}{p}\right]^2,$$

skąd $\left[\frac{1}{p}\right]=0$ lub $\left[\frac{1}{p}\right]=1$. Wobec własności (B) mamy dla $D'=1$

$$\left[\frac{D}{p}\right]=\left[\frac{D}{p}\right]\left[\frac{1}{p}\right].$$

Jeżeli więc $\left[\frac{1}{p}\right]=0$, to jest stale $\left[\frac{D}{p}\right]=0$. Jeżeli zaś $\left[\frac{1}{p}\right]=1$, to wzór (56) daje $a^{p-1}=1$, co dowodzi, że liczba rzeczywista a jest pierwiastkiem równania $x^{p-1}=1$. Równanie to ma oczywiście (wobec nieparzystości liczby p) dwa pierwiastki rzeczywiste: 1 i -1. Jest więc albo $a=1$, albo $a=-1$. Jeżeli $a=1$, to na mocy (55) mamy stale $\left[\frac{D}{p}\right]=1$, jeżeli zaś $a=-1$, to znów na mocy (55) mamy stale $\left[\frac{D}{p}\right]=(-1)^{\operatorname{ind} D}$ czyli $\left[\frac{D}{p}\right]=\left(\frac{D}{p}\right)$.

Doszliśmy więc do wniosku, że jest stale:

$$\text{albo } \left[\frac{D}{p}\right]=0, \text{ albo } \left[\frac{D}{p}\right]=1, \text{ albo } \left[\frac{D}{p}\right]=\left(\frac{D}{p}\right).$$

Na odwrót, z łatwością sprawdzamy, że każdy z tych trzech rodzajów symboli istotnie spełnia warunki (A) i (B). Możemy więc wypowiedzieć następujące

Twierdzenie 14 [1]. *Dla każdej liczby pierwszej nieparzystej p istnieją trzy rodzaje symboli $\left[\frac{D}{p}\right]$, mających oznaczoną wartość rzeczywistą przy wszelkim całkowitym D niepodzielnym przez p i spełniających warunki* (A) *i* (B), *mianowicie: prócz symboli stale równych* 0 *lub stale równych* 1 *tylko symbole Legendre'a spełniają te warunki.*

[1]) Por. mój komunikat *O zależnościach między zasadniczymi własnościami symbolu Legendre'a*, Sprawozdania z posiedzeń Towarzystwa Naukowego Warszawskiego, tom 2 (1909), str. 272.

Gdybyśmy jednak nie zastrzegli, że wartość symbolu $\left[\frac{D}{p}\right]$ ma być rzeczywista, to moglibyśmy otrzymać więcej rodzajów symboli spełniających warunki (A) i (B). Czytelnik sprawdzi z łatwością, że np. symbole $\left[\frac{D}{5}\right]$, określone dla $k=0, \pm 1, \pm 2, \ldots$ przez warunki:

$$\left[\frac{5k+1}{5}\right]=1, \quad \left[\frac{5k+2}{5}\right]=i, \quad \left[\frac{5k+3}{5}\right]=-i, \quad \left[\frac{5k+4}{5}\right]=-1,$$

mają oznaczoną wartość (zespoloną) dla każdej liczby całkowitej D niepodzielnej przez 5 oraz spełniają warunki (A) i (B).

§ 12. Zastosowania wskaźników do rozwiązywania kongruencji. Niech p będzie liczbą pierwszą, a i b — liczbami pierwszymi względem p. Aby rozwiązać kongruencję

$$ax\equiv b \pmod p,$$

bierzemy wskaźniki po obu stronach i stosujemy własności I i II; otrzymujemy więc

$$\operatorname{ind} a+\operatorname{ind} x\equiv \operatorname{ind} b \pmod{(p-1)},$$

skąd

$$\operatorname{ind} x\equiv \operatorname{ind} b-\operatorname{ind} a \pmod{(p-1)}.$$

Liczba $\operatorname{ind} x$ jest zatem resztą z dzielenia różnicy $\operatorname{ind} b-\operatorname{ind} a$ przez liczbę $p-1$. Mając $\operatorname{ind} x$, wyznaczamy pierwiastek $x\equiv g^{\operatorname{ind} x} \pmod p$. Naturalnie, dla stosowania powyższej metody w praktyce należy mieć tablice wskaźników dla modułu p.

Niech teraz D będzie liczbą niepodzielną przez p, a n — wykładnikiem naturalnym. Weźmy pod uwagę kongruencję

$$x^n\equiv D \pmod p.$$

Z własności I i III wnosimy, że kongruencja ta jest równoważna kongruencji

$$n \operatorname{ind} x\equiv \operatorname{ind} D \pmod{p-1}.$$

W ten sposób rozwiązywanie kongruencji dwumiennych n-tego stopnia daje się sprowadzić do rozwiązywania kongruencji pierwszego stopnia.

Weźmiemy wreszcie pod uwagę kongruencję wykładniczą

$$a^x\equiv b \pmod p,$$

gdzie a i b są liczbami, niepodzielnymi przez p. Jak wyżej, kongruencję tę sprowadzamy natychmiast do kongruencji pierwszego stopnia

$$x \operatorname{ind} a \equiv \operatorname{ind} b \pmod{p-1}.$$

PRZYKŁADY. 1. Niech będzie dana kongruencja

$$6x \equiv 5 \pmod{13}.$$

Stąd

$$\operatorname{ind} x \equiv \operatorname{ind} 5 - \operatorname{ind} 6 \pmod{12}.$$

Z tablicy podanej na str. 175 znajdujemy $\operatorname{ind} 5 = 9$ i $\operatorname{ind} 6 = 5$. Jest więc

$$\operatorname{ind} x \equiv 9 - 5 \equiv 4 \pmod{12}$$

czyli $\operatorname{ind} x = 4$, skąd według tejże tablicy znajdujemy $x = 3$. Sprawdzamy: $6 \cdot 3 \equiv 5 \pmod{13}$.

2. Niech będzie dana kongruencja

$$9x \equiv 6 \pmod{13}.$$

Znajdujemy stąd przy pomocy tablicy

$$\operatorname{ind} x \equiv \operatorname{ind} 6 - \operatorname{ind} 9 \equiv 5 - 8 \equiv -3 \equiv 9 \pmod{12},$$

skąd $\operatorname{ind} x = 9$ i z tejże tablicy $x = 5$. Jakoż $9 \cdot 5 \equiv 6 \pmod{13}$.

3. Niech będzie dana kongruencja

$$(*) \qquad x^8 \equiv 3 \pmod{13}.$$

Znajdujemy stąd

$$8 \operatorname{ind} x \equiv \operatorname{ind} 3 \pmod{12},$$

a że według tablicy jest $\operatorname{ind} 3 = 4$, więc pisząc $\operatorname{ind} x = \xi$, mamy dla ξ kongruencję

$$8\xi \equiv 4 \pmod{12},$$

która jest równoważna równaniu $8\xi = 4 + 12\eta$ czyli $2\xi = 1 + 3\eta$. Równanie to możemy znów napisać w postaci $2\xi \equiv 1 \pmod 3$, skąd $4\xi \equiv 2 \pmod 3$, a ponieważ $4 \equiv 1 \pmod 3$, więc $\xi \equiv 2 \pmod 3$, co dowodzi, że ξ jest liczbą postaci $2 + 3k$.

Liczbami tej postaci, nie przystającymi do siebie modulo 12, są liczby 2, 5, 8 i 11. Takie więc są wszystkie pierwiastki kongruencji $8\xi \equiv 4 \pmod{12}$ czyli wartości $\operatorname{ind} x$, którym według tablicy odpowiadają wartości $x = 4$, 6, 9 i 7.

Kongruencja dwumienna (*) ma więc cztery pierwiastki:

$$4, \quad 6, \quad 7 \quad \text{i} \quad 9.$$

4. Na str. 175 jest podana tablica indeksów dla modułu 13 przy zasadzie 2. Innymi pierwiastkami pierwotnymi modułu 13 są — jak wiemy ze str. 185 — reszty potęg

$$2^5 \equiv 6, \qquad 2^7 \equiv 11, \qquad 2^{11} \equiv 7 \pmod{13}.$$

Weźmy np. ostatnią, 7, za nową zasadę. Będziemy tu mieli $11 \operatorname{ind}_7 2 \equiv \operatorname{ind}_7 7 \pmod{12}$, a więc $11 \operatorname{ind}_7 2 \equiv 1 \pmod{12}$. Ponieważ zaś $11 \equiv -1 \pmod{12}$, więc dostajemy $-\operatorname{ind}_7 2 \equiv 1 \pmod{12}$ czyli $\operatorname{ind}_7 2 \equiv -1 \pmod{12}$, a zatem

$$\operatorname{ind}_7 2 = 11.$$

Jest to liczba, przez którą wypadnie pomnożyć wszystkie indeksy przy zasadzie 2. Otrzymamy w ten sposób tablicę indeksów przy nowej zasadzie 7:

x	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind}_7 x$	0	11	8	10	3	7	1	9	4	2	5	6

ĆWICZENIA. Dowieść, że przy wszelkiej zasadzie indeksów jest dla każdego modułu pierwszego nieparzystego p

$$\operatorname{ind}(-1) = \operatorname{ind}(p-1) = \frac{p-1}{2}.$$

Wskazówka. Oprzeć się na małym twierdzeniu Fermata, na równości

$$g^{p-1} - 1 = (g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1)$$

i na tym, że jeżeli g jest pierwiastkiem pierwotnym dla modułu pierwszego p, to $g^{\frac{p-1}{2}} \not\equiv 1 \pmod p$.

2. Dowieść, że na to, by liczba g, pierwsza względem liczby p, była pierwiastkiem pierwotnym modułu p, potrzeba i wystarcza, żeby dla żadnego dzielnika pierwszego q liczby $p-1$ nie zachodziła kongruencja $g^{\frac{p-1}{q}} \equiv 1 \pmod p$.

Dowód. Jeżeli dla pewnego q pierwszego jest

$$q \mid p-1 \quad \text{oraz} \quad g^{\frac{p-1}{q}} \equiv 1 \pmod p,$$

to liczba g nie może należeć według modułu p do wykładnika $p-1$ i przeto nie jest pierwiastkiem pierwotnym tego modułu. Warunek jest więc konieczny.

Z drugiej strony, przypuśćmy, że warunek jest spełniony i że g nie jest pierwiastkiem pierwotnym modułu p. Liczba g należy więc do wykładnika

$\delta < p-1$ i — jak wiemy, ze str. 173 — jest $\delta | p-1$. Iloraz $(p-1)/\delta$ jest zatem większy od 1 i przeto zawiera czynnik pierwszy q. Jest więc $p-1 = \delta q t$, skąd

$$g^{\frac{p-1}{q}} \equiv (g^{\delta})^{t} \equiv 1 \pmod{p}$$

wbrew założeniu. Warunek jest więc dostateczny.

3. Dowieść, że liczba 4 nie jest pierwiastkiem pierwotnym żadnej liczby pierwszej.

Dowód. W myśl małego twierdzenia Fermata, dla p pierwszych nieparzystych zachodzi kongruencja $2^{p-1} \equiv 1 \pmod{p}$; zatem $4^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

ROZDZIAŁ IX

ROZWINIĘCIA SYSTEMATYCZNE PRZY DOWOLNEJ ZASADZIE NUMERACJI

§ 1. Rozwinięcia liczb całkowitych przy danej zasadzie. Niech g będzie liczbą naturalną większą od 1. *Rozwinięciem* liczby naturalnej N *przy zasadzie numeracji* g nazywamy szereg

$$N = c_m g^m + c_{m-1} g^{m-1} + \ldots + c_1 g + c_0, \tag{1}$$

gdzie m jest liczbą całkowitą nieujemną, a c_n dla $n = 0, 1, 2, \ldots, m$ są liczbami całkowitymi, spełniającymi nierówności

$$0 \leqslant c_n \leqslant g-1 \quad \text{i} \quad c_m > 0. \tag{2}$$

Jeżeli dla liczb ciągu

$$0,\ 1,\ 2,\ \ldots,\ g-1 \tag{3}$$

przyjęto osobne symbole, które nazywają się wówczas *cyframi* przy zasadzie numeracji g, to wzór (1) piszemy w postaci

$$N = (\gamma_m \gamma_{m-1} \ldots \gamma_1 \gamma_0)_g,$$

gdzie γ_n jest cyfrą, oznaczającą liczbę c_n.

Jeżeli $g \leqslant 10$, to za symbole liczb ciągu (3) przyjmujemy odpowiednie cyfry z ciągu

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9.$$

Np.:

$N = (10010)_2$ znaczy $N = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 0 = 18$,

$N = (5603)_7$ znaczy $N = 5 \cdot 7^3 + 6 \cdot 7^2 + 0 \cdot 7 + 3 = 2012$.

Twierdzenie 1. *Każda liczba naturalna daje się, i to w jeden tylko sposób, przedstawić przy danej zasadzie g w postaci szeregu* (1), *gdzie liczby całkowite c_n dla $n = 0, 1, 2, \ldots, m$ spełniają nierówności* (2).