

Wynika stąd, że iloczyn wszystkich liczb ciągu (35) przystaje modulo m do $(-1)^{\sigma/2}$, gdzie σ jest liczbą pierwiastków kongruencji (34). Lecz na mocy wniosku 2 jest w danym razie $\sigma=2$, zatem $(-1)^{\sigma/2}=-1$, gdy $m=4$, p^a lub $2p^a$ (gdzie p jest liczbą pierwszą nieparzystą), a $\sigma \equiv 0 \pmod{4}$, zatem $(-1)^{\sigma/2}=1$ dla wszystkich innych liczb naturalnych $m>2$. Tym samym twierdzenie jest dowiedzione.

ROZDZIAŁ XIV

TEORIA SYMBOLU LEGENDRE'A I SYMBOLU JACOBIEGO

§ 1. Lemat Gaussa. W poprzednim rozdziale pokazaliśmy, jaką rolę w rozwiązywaniu kongruencji drugiego stopnia gra rozstrzyganie, czy dana liczba D jest, czy nie jest resztą kwadratową danego modułu pierwszego nieparzystego p , innymi słowy — wyznaczanie wartości symbolu Legendre'a $\left(\frac{D}{p}\right)$.

W Rozdziale VIII (§ 11, str. 199) dowiedliśmy, że symbol Legendre'a $\left(\frac{D}{p}\right)$ (gdzie p jest liczbą pierwszą nieparzystą, D zaś — liczbą niepodzielną przez p) ma następujące dwie własności:

$$\text{I. Jeżeli } D \equiv D' \pmod{p}, \text{ to } \left(\frac{D}{p}\right) = \left(\frac{D'}{p}\right).$$

$$\text{II. Jeżeli } D \not\equiv 0 \pmod{p} \text{ i } D' \not\equiv 0 \pmod{p}, \text{ to } \left(\frac{DD'}{p}\right) = \left(\frac{D}{p}\right) \left(\frac{D'}{p}\right).$$

Nadto, z twierdzenia 3 Rozdziału IV (§ 1, str. 59) wynika, że

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

skąd wynika w szczególności własność

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

Zajmiemy się obecnie dowodem innych własności symbolu Legendre'a. W tym celu udowodnimy przede wszystkim następujący

Lemat Gaussa. Wartość symbolu Legendre'a $\left(\frac{D}{p}\right)$ równa jest liczbie $(-1)^\mu$, gdzie μ jest liczbą tych reszt liczb ciągu

$$(2) \quad D, 2D, 3D, \dots, \frac{p-1}{2}D$$

względ modulo p , które są większe od $p/2$.

Dowód. Wyznaczmy dla liczb ciągu (1) reszty najmniejsze co do wartości bezwzględnej. Te z nich, które są dodatnie, oznaczmy przez

$$\alpha_1, \alpha_2, \dots, \alpha_\lambda,$$

a te, które są ujemne — przez

$$-\beta_1, -\beta_2, \dots, -\beta_\mu.$$

Wszystkie liczby α i β są więc nieujemne, a ponieważ są one różne od 0 wobec założenia, że $D \not\equiv 0 \pmod{p}$, więc są naturalne i mniejsze od $\frac{p}{2}$ czyli nie większe od $\frac{p-1}{2}$ (ponieważ p jest liczbą nieparzystą).

Suma i różnica dwu jakichkolwiek różnych wyrazów ciągu (1) jest liczbą niepodzielną przez p , gdyż D jest z założenia liczbą pierwszą względem p , a współczynniki przy D , jako liczby naturalne nie przewyższające $\frac{p-1}{2}$, dają sumę i różnicę o wartości bezwzględnie mniejszej od p . Wnosimy stąd, że suma i różnica dwu jakichkolwiek różnych (co do miejsca) wyrazów ciągu

$$(3) \quad \alpha_1, \alpha_2, \alpha_3, \dots, \alpha_\lambda, -\beta_1, -\beta_2, \dots, -\beta_\mu,$$

które, jako reszty, przystają każdy do jednej z liczb ciągu (2), jest niepodzielna przez p . Stąd zaś wynika w jednej chwili, że żadne dwie spośród liczb

$$\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_\lambda, \beta_1, \beta_2, \dots, \beta_\mu$$

nie przystają do siebie według modulo p . Lecz liczb tych jest tyleż, ile wyrazów ciągu (1) i każda z nich jest liczbą naturalną nie większą od $\frac{p-1}{2}$, a ponieważ żadne dwie z nich nie przystają według modulo p , więc liczby te mogą się różnić co najwyżej porządkiem od liczb ciągu 1, 2, 3, ..., $(p-1)/2$, a w takim razie

$$(4) \quad \alpha_1 \cdot \alpha_2 \cdot \dots \cdot \alpha_\lambda \cdot \beta_1 \cdot \beta_2 \cdot \dots \cdot \beta_\mu = 1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2}.$$

Z tego zaś, że każdy wyraz ciągu (3) przystaje według modulo p do jakiegoś wyrazu ciągu (1), wnosimy, że

$$\alpha_1 \cdot \alpha_2 \cdot \dots \cdot \alpha_\lambda \cdot (-\beta_1) \cdot (-\beta_2) \cdot \dots \cdot (-\beta_\mu) \equiv D \cdot 2D \cdot 3D \cdot \dots \cdot \frac{p-1}{2}D \pmod{p}$$

czyli

$$(-1)^\mu \alpha_1 \alpha_2 \dots \alpha_\lambda \beta_1 \beta_2 \dots \beta_\mu \equiv D^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p},$$

skąd wobec (4)

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

Liczba

$$\left(\frac{p-1}{2}\right)! \left[(-1)^\mu - D^{\frac{p-1}{2}}\right]$$

jest zatem podzielna przez liczbę pierwszą p . Ponieważ zaś pierwszą jej czynnik $\left(\frac{p-1}{2}\right)!$ jest oczywiście przez p niepodzielny, więc

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

Kongruencja ta wraz z (1) daje $\left(\frac{D}{p}\right) \equiv (-1)^\mu \pmod{p}$, skąd $\left(\frac{D}{p}\right) = (-1)^\mu$, c. b. d. o.

Zbyteczne jest chyba dodawać, że powiedzieć: reszta z dzielenia przez p jakiejś liczby dodatniej niepodzielnej przez p jest większa od połowy liczby p , wychodzi na to samo, co powiedzieć, że reszta bezwzględnie najmniejsza tej liczby według modulo p jest ujemna. Tym samym lemat Gaussa został dowiedziony.

§ 2. Wartość symbolu $\left(\frac{2}{p}\right)$. Zastosujemy obecnie lemat Gaussa do przypadku $D=2$. Mamy więc obliczyć, ile liczb z ciągu

$$2, 4, 6, \dots, \frac{p-1}{2}2$$

daje przy dzieleniu przez p resztę większą od $p/2$. Ogólny wyraz tego ciągu jest postaci $2k \leq p-1$. Na to więc, by reszta z dzielenia $2k$ przez p była większa od połowy liczby p , wystarczy, by zachodziła nierówność $2k > p/2$ czyli $k > p/4$. Naj-

mniejszą wartością k , spełniającą tę nierówność, jest $E(p/4) + 1$. Liczba k może więc przybierać wartości:

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

których jest dokładnie $\frac{p-1}{2} - E\left(\frac{p}{4}\right)$.

Lecz z łatwością sprawdzamy, że dla p nieparzystych jest stale

$$(5) \quad \frac{p-1}{2} - E\left(\frac{p}{4}\right) \equiv \frac{p^2-1}{2} \pmod{2},$$

ponieważ każda liczba nieparzysta jest jednej z postaci:

$$8k+1, \quad 8k+3, \quad 8k+5, \quad 8k+7,$$

a kongruencja (5) zachodzi dla każdej z nich. Istotnie, pisząc:

$$f(p) = \frac{p-1}{2} - E\left(\frac{p}{4}\right), \quad \varphi(p) = \frac{p^2-1}{8},$$

otrzymujemy:

$$\begin{aligned} f(8k+1) &= 4k-2k=2k, & \varphi(8k+1) &= k(8k+2), \\ f(8k+3) &= 4k+1-2k=2k+1, & \varphi(8k+3) &= (4k+1)(2k+1), \\ f(8k+5) &= 4k+2-(2k+1)=2k+1, & \varphi(8k+5) &= (2k+1)(4k+3), \\ f(8k+7) &= 4k+3-(2k+1)=2k+2, & \varphi(8k+7) &= (4k+3)(2k+2), \end{aligned}$$

czyli kongruencję (5) dla wszystkich 4 postaci liczb nieparzystych. Wynika stąd, że

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{p^2-1}{8}}.$$

Otrzymaliśmy więc dla symbolu Legendre'a własność

$$\text{IV. } \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

§ 3. Prawo wzajemności liczb pierwszych. Przechodzimy teraz do wywodu własności symbolu Legendre'a, znanej pod nazwą *prawa wzajemności liczb pierwszych*. Zastosujemy w tym celu lemat Gaussa, zakładając że D jest liczbą pierwszą nieparzystą. Oznaczmy ją przez q .

Mamy więc obliczyć, ile liczb z ciągu

$$q, \quad 2q, \quad 3q, \quad \dots, \quad \frac{p-1}{2}q$$

daje przy dzieleniu przez p resztę większą od $p/2$. Niech r_k będzie resztą wyrazu kq ; zatem

$$kq = px_k + r_k,$$

gdzie iloraz x_k jest całkowity nieujemny. Obchodzą nas jedynie liczby kq , dla których

$$p/2 < r_k < p,$$

a więc dla których $p/2 < kq - px_k < p$ czyli $kq - px_k - p/2 > 0$ i $kq - px_k - p < 0$, skąd

$$\left(kq - px_k - \frac{p}{2}\right)(kq - px_k - p) < 0.$$

Niech $x = x_k + 1$. Zatem

$$x = x_k + 1 = \frac{kq - r_k}{p} + 1.$$

Lecz $k \leq \frac{p-1}{2}$ i $r_k > \frac{p}{2}$. Zatem $kq - r_k < \frac{p-1}{2}q - \frac{p}{2}$, skąd $x < \frac{(p-1)q - p}{2p} + 1 = \frac{(p-1)q + p}{2p} < \frac{pq + p}{2p}$, czyli $x < \frac{q+1}{2}$, co wobec nieparzystości liczby q jest równoważne warunkowi

$$x \leq \frac{q-1}{2}.$$

Z drugiej strony jest $x = x_k + 1 \geq 1$, gdyż iloraz całkowity x_k jest nieujemny. Możemy więc powiedzieć, że jeżeli $r_k > p/2$, to wśród wyrazów ciągu

$$1, \quad 2, \quad 3, \quad \dots, \quad \frac{q-1}{2}$$

istnieje co najmniej jedna liczba x , dla której

$$(6) \quad \left(kq - px + \frac{p}{2}\right)(kq - px) < 0.$$

Okażemy, że wśród wyrazów tego ciągu taka liczba x jest co najwyżej jedna.

Istotnie, dla $x > x_k + 1$ czyli $x \geq x_k + 2$ jest

$$kq - px + \frac{p}{2} \leq kq - p(x_k + 2) + \frac{p}{2} = kq - px_k - \frac{3p}{2} = r_k - \frac{3p}{2} < 0,$$

tym bardziej więc $kq - px < 0$, skąd

$$\left(kq - px + \frac{p}{2}\right)(kq - px) > 0,$$

co niemożliwe wobec (6).

Natomiast dla $x < x_k + 1$ czyli $x \leq x_k$ jest

$$kq - px \geq kq - px_k = r_k > 0,$$

tym bardziej więc $kq - px + \frac{p}{2} > 0$, skąd znowu

$$\left(kq - px + \frac{p}{2}\right)(kq - px) > 0$$

wbrew (6).

Widzimy zatem, że jeżeli $r_k > p/2$, to

$$(7) \quad \prod_{x=1}^{\frac{q-1}{2}} \left(kq - px + \frac{p}{2}\right)(kq - px) < 0.$$

Analogicznie dowiedzimy, że jeżeli $r_k < p/2$, to iloczyn (7) jest dodatni. Istotnie, dla $x \leq x_k$ jest

$$kq - px \geq kq - px_k = r_k > 0,$$

tym bardziej więc $kq - px + p/2 > 0$, skąd

$$\left(kq - px + \frac{p}{2}\right)(kq - px) > 0.$$

Natomiast dla $x > x_k$ czyli $x \geq x_k + 1$ jest

$$kq - px + \frac{p}{2} \leq kq - px_k - \frac{p}{2} = r_k - \frac{p}{2} < 0,$$

tym bardziej więc $kq - px < 0$, skąd znowu

$$\left(kq - px + \frac{p}{2}\right)(kq - px) > 0.$$

Widzimy zatem, że dla $r_k < p/2$ wszystkie czynniki iloczynu (7), a więc i sam iloczyn (7) jest dodatni.

Oznaczmy ogólnie symbolem $R(kq)$ najmniejszą co do wartości bezwzględnej resztę liczby kq według modułu p , a symbo-

lem $\text{sign } z$ — znak liczby z , tj. liczbę $+1$ dla $z > 0$ i liczbę -1 dla $z < 0$. Zatem

$$\text{sign } R(kq) = \begin{cases} +1 & \text{dla } r_k < p/2 \\ -1 & \text{dla } r_k > p/2 \end{cases}$$

i w każdym razie

$$(8) \quad \text{sign } R(kq) = \text{sign} \prod_{x=1}^{\frac{q-1}{2}} \left(kq - px + \frac{p}{2}\right)(kq - px).$$

W tym znakowaniu lemat Gaussa daje

$$\left(\frac{q}{p}\right) = \prod_{k=1}^{\frac{p-1}{2}} \text{sign } R(kq),$$

skąd wobec (8)

$$\left(\frac{q}{p}\right) = \text{sign} \prod_{k=1}^{\frac{p-1}{2}} \prod_{x=1}^{\frac{q-1}{2}} \left(kq - px + \frac{p}{2}\right)(kq - px).$$

Możemy też oczywiście napisać

$$(9) \quad \left(\frac{q}{p}\right) = \text{sign} \prod_{k=1}^{\frac{p-1}{2}} \prod_{x=1}^{\frac{q-1}{2}} \left(kq - px + \frac{p}{2}\right) \text{sign} \prod_{k=1}^{\frac{p-1}{2}} \prod_{x=1}^{\frac{q-1}{2}} (kq - px).$$

Niech

$$x = \frac{q+1}{2} - l.$$

Wtedy $l = \frac{q+1}{2} - x$, a więc jeżeli x przebiega liczby

$$1, 2, 3, \dots, \frac{q-1}{2},$$

to l przebiega liczby

$$\frac{q-1}{2}, \dots, 3, 2, 1$$

i na odwrót. Ponieważ jednak porządek czynników nie wpływa na wartość iloczynu, więc

$$\prod_{x=1}^{\frac{q-1}{2}} \left(kq - px + \frac{p}{2}\right) = \prod_{l=1}^{\frac{q-1}{2}} \left(kq + lp - \frac{pq}{2}\right).$$

Oczywiście

$$\prod_{x=1}^{\frac{q-1}{2}} (kq - px) = \prod_{l=1}^{\frac{q-1}{2}} (kq - lp),$$

skąd wobec (9)

$$\left(\frac{q}{p}\right) = \text{sign} \prod_{k=1}^{\frac{p-1}{2}} \prod_{l=1}^{\frac{q-1}{2}} \left(kq + lp - \frac{pq}{2}\right) (kq - lp).$$

Wzór ten wyprowadzony został dla wszelkich liczb pierwszych nieparzystych p i q . Pozostanie on więc prawdziwy, jeżeli w nim zastąpimy wszędzie p przez q , a k przez l i na odwrót. Otrzymamy wówczas

$$\left(\frac{p}{q}\right) = \text{sign} \prod_{l=1}^{\frac{q-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} \left(lp + kq - \frac{qp}{2}\right) (lp - kq).$$

Z dwu ostatnich wzorów, łącząc odpowiednie czynniki, otrzymujemy

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = \text{sign} \prod_{k=1}^{\frac{p-1}{2}} \prod_{l=1}^{\frac{q-1}{2}} \left(kq + lp - \frac{qp}{2}\right)^2 [-(kq - lp)^2].$$

Ponieważ w iloczynie po prawej stronie wszystkie czynniki $\left(kq + lp - \frac{qp}{2}\right)^2$ są dodatnie, więc możemy napisać

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = \text{sign} \prod_{k=1}^{\frac{p-1}{2}} \prod_{l=1}^{\frac{q-1}{2}} [-(kq - lp)^2].$$

Wszystkie czynniki po prawej stronie są teraz ujemne, a jest ich $\frac{p-1}{2} \cdot \frac{q-1}{2}$, gdyż k może przyjmować $\frac{p-1}{2}$, l zaś $\frac{q-1}{2}$ wartości. Zatem prawa strona ostatniego wzoru równa jest $(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$. Otrzymaliśmy więc dla symbolu Legendre'a własność

V. Prawo wzajemności liczb pierwszych ¹⁾. Jeżeli p i q są liczbami pierwszymi nieparzystymi, to

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

§ 4. Obliczanie wartości symbolu Legendre'a na podstawie jego zasadniczych własności. Pokażemy obecnie, w jaki sposób na podstawie 5 wyprowadzonych własności symbolu Legendre'a można obliczyć jego wartość. Dla ułatwienia napiszmy wszystkie te własności razem:

$$\text{I. } \left(\frac{D}{p}\right) = \left(\frac{D'}{p}\right) \text{ dla } D \equiv D' \pmod{p}.$$

$$\text{II. } \left(\frac{DD'}{p}\right) = \left(\frac{D}{p}\right) \left(\frac{D'}{p}\right).$$

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

$$\text{IV. } \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

$$\text{V. } \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \text{ dla } p \text{ i } q \text{ pierwszych nieparzystych.}$$

Niech p będzie daną liczbą pierwszą nieparzystą, a D — daną liczbą całkowitą, niepodzielną przez p . Aby obliczyć wartość symbolu $\left(\frac{D}{p}\right)$, oznaczmy przez r resztę liczby D według modułu p . Na mocy własności I jest

$$\left(\frac{D}{p}\right) = \left(\frac{r}{p}\right), \quad \text{gdzie } 0 < r < p.$$

Rozróżnimy dalej dwa przypadki: $r = 1$ i $r > 1$.

Dla $r = 1$ mamy na mocy własności II

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

skąd na mocy własności III

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

¹⁾ Gauss sam podał aż 7 różnych dowodów prawa wzajemności liczb pierwszych. Tablicę chronologiczną 45 dowodów tego prawa (od 1796 r. do 1897 r.) znajdzie czytelnik w książce P. Bachmanna, *Niedere Zahlentheorie*, Część I, Lipsk 1901, str. 203.

Dla $r > 1$ rozwińmy liczbę r na czynniki pierwsze:

$$r = 2^{\alpha} q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k}.$$

Wszystkie czynniki nieparzyste q są oczywiście nie większe od r , a więc mniejsze od p . Na mocy własności II mamy

$$\left(\frac{D}{p}\right) = \left(\frac{r}{p}\right) = \left(\frac{2}{p}\right)^{\alpha} \left(\frac{q_1}{p}\right)^{\alpha_1} \left(\frac{q_2}{p}\right)^{\alpha_2} \dots \left(\frac{q_k}{p}\right)^{\alpha_k}.$$

Pierwszy czynnik po prawej stronie obliczymy na mocy własności IV, a dla obliczenia pozostałych wystarczy, jeżeli potrafimy obliczyć $\left(\frac{q}{p}\right)$, gdzie q jest liczbą pierwszą, mniejszą od p . Lecz na mocy własności V jest

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

wystarczy więc, jeżeli potrafimy obliczyć wartość symbolu $\left(\frac{D'}{q}\right)$, gdzie q jest liczbą pierwszą nieparzystą mniejszą od p .

Tak więc obliczanie wartości symbolu $\left(\frac{D}{p}\right)$ możemy zawsze sprowadzić do obliczania wartości symbolu $\left(\frac{D'}{q}\right)$, gdzie q jest liczbą pierwszą nieparzystą, mniejszą od p .

Ponieważ jednak liczb pierwszych nieparzystych mniejszych od p jest tylko liczba skończona, więc stosując wskazane operacje dostatecznie wielką (skończoną) liczbę razy, dojdziemy wreszcie do symboli, które dadzą się już obliczyć na podstawie tylko czterech pierwszych własności symbolu Legendre'a.

PRZYKŁAD. Obliczmy $\left(\frac{1000}{641}\right)$.

Na mocy własności I $\left(\frac{1000}{641}\right) = \left(\frac{359}{641}\right)$. Liczba 359 jest pierwsza. Stąd na mocy własności V $\left(\frac{359}{641}\right) = \left(\frac{641}{359}\right)$, a na mocy własności I $\left(\frac{641}{359}\right) = \left(\frac{282}{359}\right)$. Lecz $282 = 2 \cdot 3 \cdot 47$, więc na mocy własności II

$$\left(\frac{282}{359}\right) = \left(\frac{2}{359}\right) \left(\frac{3}{359}\right) \left(\frac{47}{359}\right).$$

Na mocy własności IV $\left(\frac{2}{359}\right) = +1$, a na mocy własności V $\left(\frac{3}{359}\right) = -\left(\frac{359}{3}\right)$. Ale na mocy własności I $\left(\frac{359}{3}\right) = \left(\frac{2}{3}\right)$, na mocy zaś własności IV $\left(\frac{2}{3}\right) = -1$; zatem $\left(\frac{3}{359}\right) = +1$.

Na mocy własności V i I znajdujemy kolejno

$$\left(\frac{47}{359}\right) = -\left(\frac{359}{47}\right) = -\left(\frac{30}{47}\right),$$

na mocy zaś własności II $\left(\frac{30}{47}\right) = \left(\frac{2}{47}\right) \left(\frac{3}{47}\right) \left(\frac{5}{47}\right)$. Na mocy własności IV $\left(\frac{2}{47}\right) = +1$, a na mocy własności V $\left(\frac{3}{47}\right) = -\left(\frac{47}{3}\right)$. Ale na mocy własności I $\left(\frac{47}{3}\right) = \left(\frac{2}{3}\right)$, na mocy zaś własności IV $\left(\frac{2}{3}\right) = -1$; zatem $\left(\frac{3}{47}\right) = +1$.

Wreszcie na mocy własności V $\left(\frac{5}{47}\right) = \left(\frac{47}{5}\right)$, a na mocy własności I $\left(\frac{47}{5}\right) = \left(\frac{2}{5}\right)$; na mocy własności IV $\left(\frac{2}{5}\right) = -1$; zatem $\left(\frac{5}{47}\right) = -1$.

Tak więc $\left(\frac{30}{47}\right) = \left(\frac{2}{47}\right) \left(\frac{3}{47}\right) \left(\frac{5}{47}\right) = -1$, skąd $\left(\frac{47}{359}\right) = -\left(\frac{359}{47}\right) = -\left(\frac{30}{47}\right) = +1$. Zatem

$$\begin{aligned} \left(\frac{1000}{641}\right) &= \left(\frac{359}{641}\right) = \left(\frac{641}{359}\right) = \left(\frac{282}{359}\right) = \left(\frac{2}{359}\right) \left(\frac{3}{359}\right) \left(\frac{47}{359}\right) = \\ &= (+1) \cdot (+1) \cdot (+1) = +1 \end{aligned}$$

czyli ostatecznie

$$\left(\frac{1000}{641}\right) = +1.$$

Do tego samego wyniku doszlibyśmy, obliczając wartość tegoż symbolu inaczej. Mianowicie moglibyśmy napisać na mocy własności II

$$\left(\frac{1000}{641}\right) = \left(\frac{2}{641}\right)^3 \left(\frac{5}{641}\right)^3.$$

Na mocy własności IV $\left(\frac{2}{641}\right) = +1$, na mocy zaś własności V $\left(\frac{5}{641}\right) = \left(\frac{641}{5}\right)$. Na mocy własności I $\left(\frac{641}{5}\right) = \left(\frac{1}{5}\right)$, a na mocy własności II i III $\left(\frac{1}{5}\right) = \left(\frac{-1}{5}\right) \left(\frac{-1}{5}\right) = 1$.

Zatem

$$\left(\frac{1000}{641}\right) = (+1)(+1) = +1,$$

jak wyżej.

ĆWICZENIA: 1. Dowieść, że jeżeli $p = 4k + 3$ jest liczbą pierwszą, to

$$(*) \quad p \mid 2^{2k+1} + (-1)^k \quad (\text{Storchi}).$$

Dowód. W myśl wzoru (14) z Rozdziału II (str. 36) jest $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} \pmod{p}$.

skąd w myśl własności IV symbolu Legendre'a $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{8}} \pmod{p}$. Ponieważ w danym razie jest $\frac{p-1}{2} = 2k+1$, a $\frac{p^2-1}{8} = (2k+1)(k+1)$, więc $2^{2k+1} \equiv (-1)^{k+1} \pmod{p}$ czyli (*), c. b. d. o.

Tak np. $3 \mid 2+1$, $7 \mid 2^2-1$, $11 \mid 2^2+1$, $19 \mid 2^2+1$, $23 \mid 2^3-1$.

2. Dowieść, że jeżeli p jest liczbą pierwszą postaci $40k \pm 1$, to

$$p \mid 10^{\frac{p-1}{2}} - 1 \quad (\text{Euler}).$$

Dowód. Jak wiemy z definicji symbolu Legendre'a (p. wzór, (17), str. 62),

wobec $(10, p) = 1$ jest $10^{\frac{p-1}{2}} \equiv \left(\frac{10}{p}\right) \pmod{p}$; wystarczy więc okazać, że $\left(\frac{10}{p}\right) = 1$.

Lecz $\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right) \left(\frac{5}{p}\right)$. Wobec $p = 40k \pm 1$ jest $\frac{p^2-1}{8} \equiv 0 \pmod{2}$, skąd $\left(\frac{2}{p}\right) = 1$ w myśl własności IV symbolu Legendre'a. Na mocy zaś własności V mamy $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, a w myśl własności I i III $\left(\frac{p}{5}\right) = \left(\frac{40k \pm 1}{5}\right) = \left(\frac{\pm 1}{5}\right) = 1$. Jest więc $\left(\frac{5}{p}\right) = 1$, zatem $\left(\frac{10}{p}\right) = 1$, c. b. d. o.

Tak więc np. $41 \mid 10^{20} - 1$, $79 \mid 10^{40} - 1$.

3. Dowieść, że jeżeli p jest liczbą pierwszą postaci $40k \pm r$, gdzie $r = 7, 11, 17$ lub 19 , to $p \mid 10^{\frac{p-1}{2}} + 1$; jeżeli zaś p jest liczbą pierwszą postaci $40k \pm r$, gdzie $r = 3, 9$ lub 13 , to $p \mid 10^{\frac{p-1}{2}} - 1$

(Euler).

4. Znaleźć wszystkie liczby pierwsze nieparzyste $p \neq 7$, dla których liczba 7 jest resztą kwadratową.

Rozwiązanie. Na mocy definicji symbolu Legendre'a (str. 62) wystarczy znaleźć wszystkie liczby pierwsze nieparzyste p , dla których $\left(\frac{7}{p}\right) = 1$. Liczba pierwsza nieparzysta p musi być jednej z postaci $28k \pm r$, gdzie $r = 1, 3, 5, 9, 11$ lub 13 . W myśl własności V symbolu Legendre'a jest $\left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{7}\right)$. Lecz, w myśl własności I tego symbolu jest $\left(\frac{p}{7}\right) = \left(\frac{28k \pm r}{7}\right) = \left(\frac{\pm r}{7}\right)$, a że w myśl własności III $\left(\frac{-1}{7}\right) = -1$, więc $\left(\frac{p}{7}\right) = \pm \left(\frac{r}{7}\right)$ na mocy własności II. Mamy dalej $\left(\frac{1}{7}\right) = 1$ w myśl własności III, a w myśl własności V, I i II

$$\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Stosując w dalszym ciągu własności symbolu Legendre'a, znajdujemy

$$\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1, \quad \left(\frac{9}{7}\right) = \left(\frac{5}{7}\right)^2 = 1, \quad \left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 = 1, \quad \left(\frac{13}{7}\right) = \left(\frac{-1}{7}\right) = -1.$$

Tak więc $\left(\frac{7}{p}\right) = 1$ dla $p = 28k + r$, gdzie $r = 1, 3, 9, 19, 25$ lub 27 , i $\left(\frac{7}{p}\right) = -1$ dla $p = 28k + r$, gdzie $r = 5, 11, 13, 15, 17$ lub 23 .

Zatem; na to, by liczba 7 była resztą kwadratową dla liczby pierwszej nieparzystej p , potrzeba i wystarcza, żeby liczba p była postaci $28k + r$, gdzie $r = 1, 3, 9, 19, 25$ lub 27 .

5. Znaleźć wszystkie niepodzielne przez 7 (i różne od 1), liczby naturalne $m \leq 100$, dla których liczba 7 jest resztą kwadratową.

Rozwiązanie. Opierając się na wynikach ćwiczenia 4 oraz na wniosku 1 ze str. 320, znajdujemy z łatwością, że są to następujące liczby m :

$$2, 3, 6, 9, 18, 19, 27, 29, 31, 37, 38,$$

$$47, 53, 54, 57, 58, 59, 62, 74, 81, 94.$$

§ 5. Symbol Jacobiego i jego zasadnicze własności. W celu uniknięcia rozwijania liczby D na czynniki pierwsze przy obliczaniu wartości symbolu Legendre'a $\left(\frac{D}{p}\right)$, C. Jacobi wprowadził symbol ogólniejszy $\left(\frac{D}{p}\right)$, definiując go dla przypadków, kiedy P jest jakąkolwiek liczbą nieparzystą większą od jedności, D zaś — jakąkolwiek liczbą całkowitą pierwszą względem P .

Definicja Jacobiego jest następująca: jeżeli P rozwija się na czynniki pierwsze (oczywiście wszystkie nieparzyste)

$$P = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

to

$$(10) \quad \left(\frac{D}{P}\right) = \left(\frac{D}{p_1}\right)^{\alpha_1} \left(\frac{D}{p_2}\right)^{\alpha_2} \dots \left(\frac{D}{p_k}\right)^{\alpha_k},$$

gdzie po prawej stronie mamy symbole Legendre'a.

Z definicji tej wynika natychmiast, że w razie, kiedy P jest liczbą pierwszą, symbol Jacobiego jest identyczny z symbolem Legendre'a. Gdybyśmy więc znaleźli jakiś prosty sposób wyznaczania wartości symbolu Jacobiego, to moglibyśmy wyznaczać zarazem wartości symbolu Legendre'a.

Jednakże dla reszt kwadratowych symbol Jacobiego nie gra już tej roli, co symbol Legendre'a.

Z równości bowiem $\left(\frac{D}{P}\right) = -1$ można wprawdzie wywnioskować, że D nie jest resztą kwadratową dla P , ponieważ gdy równość ta zachodzi, to przynajmniej jeden z czynników prawej strony wzoru (10) musi być liczbą -1 , np. $\left(\frac{D}{p_1}\right) = -1$, a wówczas kongruencja $x^2 \equiv D \pmod{p_1}$, tym bardziej więc kongruencja $x^2 \equiv D \pmod{P}$, nie byłaby rozwiązalna. Jeżeli natomiast zachodzi równość $\left(\frac{D}{P}\right) = +1$, to jeszcze stąd nie wynika, że D jest resztą kwadratową liczby P . Oto przykład:

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1,$$

gdy tymczasem kongruencja $x^2 \equiv 2 \pmod{15}$ nie jest rozwiązalna, nierozwiązalna jest już bowiem kongruencja $x^2 \equiv 2 \pmod{3}$.

Dla symbolu Legendre'a wyprowadziliśmy pięć zasadniczych własności. Okażemy obecnie, że wszystkie te własności posiada również symbol Jacobiego.

Przedstawmy liczbę P w formie

$$P = p p' p'' \dots,$$

gdzie po prawej stronie mamy same czynniki pierwsze (nieparzyste), między którymi mogą się też znajdować równe. Na mocy definicji symbolu Jacobiego możemy napisać

$$(11) \quad \left(\frac{D}{P}\right) = \left(\frac{D}{p}\right) \left(\frac{D}{p'}\right) \left(\frac{D}{p''}\right) \dots,$$

gdzie po prawej stronie mamy symbole Legendre'a.

Własność I. Jeżeli $D \equiv D' \pmod{P}$, to $\left(\frac{D}{P}\right) = \left(\frac{D'}{P}\right)$.

Dowód. W myśl (11):

$$(12) \quad \left(\frac{D}{P}\right) = \left(\frac{D}{p}\right) \left(\frac{D}{p'}\right) \left(\frac{D}{p''}\right) \dots, \quad \left(\frac{D'}{P}\right) = \left(\frac{D'}{p}\right) \left(\frac{D'}{p'}\right) \left(\frac{D'}{p''}\right) \dots$$

Lecz jeżeli $D \equiv D' \pmod{P}$, to tym bardziej

$$D \equiv D' \pmod{p}, \quad D \equiv D' \pmod{p'}, \quad D \equiv D' \pmod{p''} \quad \text{itd.},$$

wobec czego na mocy własności I symbolu Legendre'a

$$\left(\frac{D}{p}\right) = \left(\frac{D'}{p}\right), \quad \left(\frac{D'}{p'}\right) = \left(\frac{D}{p'}\right), \quad \dots$$

Każdy z czynników prawej strony pierwszego ze wzorów (12) jest więc równy odpowiedniemu czynnikowi drugiego z tych wzorów, skąd $\left(\frac{D}{P}\right) = \left(\frac{D'}{P}\right)$, c. b. d. o.

Własność II. $\left(\frac{DD'}{P}\right) = \left(\frac{D}{P}\right) \left(\frac{D'}{P}\right)$.

Dowód. W myśl (11) zachodzą wzory (12), skąd

$$\left(\frac{D}{P}\right) \left(\frac{D'}{P}\right) = \left(\frac{D}{p}\right) \left(\frac{D}{p'}\right) \left(\frac{D}{p''}\right) \left(\frac{D'}{p}\right) \left(\frac{D'}{p'}\right) \left(\frac{D'}{p''}\right) \dots$$

Lecz na mocy własności II symbolu Legendre'a

$$\left(\frac{D}{p}\right) \left(\frac{D'}{p}\right) = \left(\frac{DD'}{p}\right), \quad \left(\frac{D}{p'}\right) \left(\frac{D'}{p'}\right) = \left(\frac{DD'}{p'}\right), \dots,$$

skąd

$$\left(\frac{D}{P}\right) \left(\frac{D'}{P}\right) = \left(\frac{DD'}{p}\right) \left(\frac{DD'}{p'}\right) \left(\frac{DD'}{p''}\right) \left(\frac{DD'}{p'''}\right) \dots$$

Z drugiej strony w myśl (11) jest

$$\left(\frac{DD'}{P}\right) = \left(\frac{DD'}{p}\right) \left(\frac{DD'}{p'}\right) \left(\frac{DD'}{p''}\right) \dots,$$

więc

$$\left(\frac{DD'}{P}\right) = \left(\frac{D}{p}\right) \left(\frac{D'}{p'}\right), \quad \text{c. b. d. o.}$$

Własność III. $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}.$

Dowód. W myśl (11)

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p}\right) \left(\frac{-1}{p'}\right) \left(\frac{-1}{p''}\right) \dots$$

Po prawej stronie mamy symbole Legendre'a, możemy więc na mocy ich własności III napisać

$$(15) \quad \left(\frac{-1}{P}\right) = (-1)^{\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \dots}$$

W tożsamości

$$P = pp'p'' \dots = [(p-1)+1][(p'-1)+1][(p''-1)+1] \dots$$

wszystkie liczby $p-1$, $p'-1$, $p''-1$, ... są oczywiście parzyste; iloczyn dwu lub więcej takich czynników jest więc podzielny przez 4. Zatem

$$P = 4k + 1 + (p-1) + (p'-1) + (p''-1) + \dots,$$

skąd

$$(14) \quad \frac{P-1}{2} = 2k + \frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \dots,$$

więc

$$(-1)^{\frac{P-1}{2}} = (-1)^{\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \dots}$$

Na mocy (15) jest przeto $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$, [c. b. d. o

Własność IV. $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$

Dowód. W myśl (11)

$$\left(\frac{2}{P}\right) = \left(\frac{2}{p}\right) \left(\frac{2}{p'}\right) \left(\frac{2}{p''}\right) \dots,$$

skąd na zasadzie własności IV symbolu Legendre'a

$$(15) \quad \left(\frac{2}{P}\right) = (-1)^{\frac{p^2-1}{8} + \frac{p'^2-1}{8} + \frac{p''^2-1}{8} + \dots}$$

Ponieważ kwadrat każdej liczby nieparzystej jest formy $8k+1$, więc w tożsamości

$$P^2 = [(p^2-1)+1][(p'^2-1)+1][(p''^2-1)+1] \dots$$

każda z różnic p^2-1 , p'^2-1 , p''^2-1 , ... jest podzielna przez 8. Iloczyn dwu lub więcej takich różnic jest przeto podzielny przez 64. Zatem

$$P^2 = 64k + 1 + (p^2-1) + (p'^2-1) + (p''^2-1) \dots,$$

skąd

$$\frac{P^2-1}{8} = 8k + \frac{p^2-1}{8} + \frac{p'^2-1}{8} + \frac{p''^2-1}{8} + \dots,$$

więc

$$(-1)^{\frac{P^2-1}{8}} = (-1)^{\frac{p^2-1}{8} + \frac{p'^2-1}{8} + \frac{p''^2-1}{8} + \dots},$$

a stąd na mocy (15) $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$, c. b. d. o.

Własność V. $\left(\frac{P}{Q}\right) \left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \frac{Q-1}{2}}$ dla P i Q nieparzystych względnie pierwszych.

Dowód. Dla skrócenia oznaczmy ogólnie przez $\prod_p f(p)$ iloczyn $f(p)f(p')f(p'') \dots$ rozciągnięty na wszystkie czynniki rozkładu $P = pp'p'' \dots$, a przez $\prod_{p,q} f(p,q)$ takż iloczyn rozciągnięty na wszystkie pary p,q , gdzie p jest jednym z czynników iloczynu $pp'p'' \dots$, a q — jednym z czynników iloczynu $qq'q'' \dots$

Dla rozkładów $\prod_p$ i $\prod_q$ liczb P i Q na same czynniki pierwsze:

$$P = p p' p'' \dots \quad \text{i} \quad Q = q q' q'' \dots$$

jest więc w myśl (11) $\left(\frac{P}{Q}\right) = \prod_q \left(\frac{P}{q}\right)$, gdzie w myśl własności II

$$\left(\frac{P}{q}\right) = \prod_p \left(\frac{p}{q}\right), \quad \text{skąd} \quad \left(\frac{P}{Q}\right) = \prod_q \prod_p \left(\frac{p}{q}\right) = \prod_{p,q} \left(\frac{p}{q}\right).$$

Podobnie $\left(\frac{Q}{P}\right) = \prod_{p,q} \left(\frac{q}{p}\right)$, skąd $\left(\frac{P}{Q}\right) \left(\frac{Q}{P}\right) = \prod_{p,q} \left(\frac{p}{q}\right) \left(\frac{q}{p}\right)$, zatem na mocy prawa wzajemności liczb pierwszych

$$(16) \quad \left(\frac{P}{Q}\right) \left(\frac{Q}{P}\right) = \prod_{p,q} (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = (-1)^{\sum_{p,q} \frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Lecz — jak łatwo stwierdzić — suma $\sum_{p,q} \frac{p-1}{2} \cdot \frac{q-1}{2}$, rozciągnięta na wszystkie pary p, q , gdzie p przebiega liczby $p, p', p'', \dots$, a q — liczby $q, q', q'', \dots$, równa jest iloczynowi

$$\left(\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \dots\right) \left(\frac{q-1}{2} + \frac{q'-1}{2} + \frac{q''-1}{2} + \dots\right).$$

W myśl (14) jest

$$\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \dots = \frac{P-1}{2} - 2k$$

i podobnie

$$\frac{q-1}{2} + \frac{q'-1}{2} + \frac{q''-1}{2} + \dots = \frac{Q-1}{2} - 2l,$$

skąd

$$\sum_{p,q} \frac{p-1}{2} \cdot \frac{q-1}{2} = \prod_p \frac{p-1}{2} \prod_q \frac{q-1}{2} = \frac{P-1}{2} \cdot \frac{Q-1}{2} + 2u,$$

gdzie liczba $u = 2kl - \frac{P-1}{2}l - \frac{Q-1}{2}k$ jest całkowita. Zatem

$$(-1)^{\sum_{p,q} \frac{p-1}{2} \cdot \frac{q-1}{2}} = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}},$$

czyli wobec (16) $\left(\frac{P}{Q}\right) \left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$, c. b. d. d.

Prawa strona otrzymanego wzoru jest — jak łatwo wiedzieć — równa -1 tylko wtedy, gdy obie liczby P i Q są formy $4k+3$. Gdy bowiem choć jedna z tych liczb miała formę $4k+1$, to wykładnik po prawej stronie byłby oczywiście parzysty i mielibyśmy $+1$.

Wyprowadzone własności zastosujemy do wywodu reguły, służącej do wyznaczania wartości symbolu Jacobiego bez rozwijania liczb na czynniki pierwsze. Jest to tzw. *prawidło Eisensteina*.

§ 6. Prawidło Eisensteina. Zauważmy przede wszystkim, że obliczanie wartości symbolu $\left(\frac{D}{P}\right)$ możemy sprowadzić zawsze do obliczania wartości symbolu $\left(\frac{Q}{P}\right)$, gdzie Q jest liczbą naturalną nieparzystą. Istotnie, niech

$$D = (-1)^{\alpha} 2^{\beta} Q,$$

gdzie Q jest iloczynem wszystkich czynników nieparzystych rozwinięcia liczby D . Dla wyznaczenia liczby Q nie potrzebujemy jednak rozwijać D na czynniki pierwsze: wystarczy wyznaczyć najwyższą potęgę dwójki, dzielącą liczbę D . Możemy ją znaleźć, dzieląc kolejno D przez 2, póki to jest możliwe, i obliczając liczbę takich dzieleni.

Na mocy własności II, III i IV symbolu Jacobiego możemy napisać

$$\left(\frac{D}{P}\right) = (-1)^{\frac{P-1}{2} \alpha + \frac{P-1}{8} \beta} \left(\frac{Q}{P}\right);$$

pozostają więc do obliczenia tylko wartości symbolu $\left(\frac{Q}{P}\right)$ dla Q nieparzystych.

Oznaczmy przez R resztę liczby Q według modułu P ; jest to więc jedna z liczb

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

i liczba $P-R$ jest również jedną z liczb tego ciągu. Możemy napisać

$$Q = Pt + R, \quad Q = P(t+1) - (P-R).$$

Z liczb R i $P-R$, których suma P jest nieparzysta, jedna jest parzysta, a druga nieparzysta. Oznaczmy przez P_1 tę z nich, która jest nieparzysta. Jeżeli jest nią liczba R , to $Q = P + P_1$, jeżeli zaś jest nią liczba $P-R$, to $Q = P(t+1) - P_1$; w każdym więc razie

$$Q = Pk + \varepsilon_1 P_1,$$

gdzie ε_1 jest równe albo $+1$, albo -1 .

Zauważmy też, że k musi być liczbą parzystą. Istotnie, w przeciwnym razie nieparzystą byłaby liczba

$$Pk = Q - \varepsilon_1 P_1,$$

gdy tymczasem po prawej stronie mamy liczbę parzystą jako różnicę lub sumę dwu liczb nieparzystych. Niech więc $k = 2k_1$; zatem

$$Q = 2k_1 P + \varepsilon_1 P_1.$$

Jeżeli $P_1 \neq 1$, to możemy postąpić z liczbami P i P_1 tak, jak postąpiliśmy z liczbami Q i P ; otrzymamy równość

$$P = 2k_2 P_1 + \varepsilon_2 P_2,$$

gdzie $\varepsilon_2 = \pm 1$, a P_2 jest liczbą naturalną nieparzystą.

Jeżeli zaś $P_2 \neq 1$, to otrzymamy podobnie

$$P_1 = 2k_3 P_2 + \varepsilon_3 P_3 \quad \text{itd.}$$

Liczby $P, P_1, P_2, P_3, \dots$ stale maleją, gdyż $P_1 \leq P-1, P_2 \leq P_1-1$ itd. Ciąg otrzymanych równości nie może więc być nieskończony (bo liczb naturalnych nieparzystych mniejszych od P jest liczba skończona). Dojdziemy więc do ostatniej równości

$$P_{n-2} = 2k_n P_{n-1} + \varepsilon_n P_n,$$

w której $P_n = 1$ (ponieważ gdyby było $P_n \neq 1$, moglibyśmy jeszcze napisać równość następną). W ciągu otrzymanych równości:

$$\begin{aligned} Q &= 2k_1 P + \varepsilon_1 P_1, \\ P &= 2k_2 P_1 + \varepsilon_2 P_2, \\ P_1 &= 2k_3 P_2 + \varepsilon_3 P_3, \\ &\dots \dots \dots \\ P_{n-3} &= 2k_{n-1} P_{n-2} + \varepsilon_{n-1} P_{n-1}, \\ P_{n-2} &= 2k_n P_{n-1} + \varepsilon_n P_n \end{aligned} \quad (17)$$

(gdzie $P_n = 1$) pierwsza równość daje na mocy własności I i II symbolu Jacobiego

$$(18) \quad \left(\frac{Q}{P}\right) = \left(\frac{\varepsilon_1}{P}\right) \left(\frac{P_1}{P}\right).$$

Jeżeli w niej $\varepsilon_1 = 1$, to

$$\left(\frac{\varepsilon_1}{P}\right) = 1 = (-1)^{\frac{P-1}{2} \frac{1-1}{2}} = (-1)^{\frac{P-1}{2} \frac{1-\varepsilon_1}{2}},$$

jeżeli zaś $\varepsilon_1 = -1$, to

$$\left(\frac{\varepsilon_1}{P}\right) = (-1)^{\frac{P-1}{2}} = (-1)^{\frac{P-1}{2} \frac{1+1}{2}} = (-1)^{\frac{P-1}{2} \frac{1-\varepsilon_1}{2}}.$$

W każdym więc razie

$$\left(\frac{\varepsilon_1}{P}\right) = (-1)^{\frac{P-1}{2} \frac{1-\varepsilon_1}{2}}.$$

Na mocy własności V symbolu Jacobiego jest

$$\left(\frac{P_1}{P}\right) = \left(\frac{P}{P_1}\right) (-1)^{\frac{P-1}{2} \frac{P_1-1}{2}},$$

gdzie właściwie powinniśmy mieć w mianowniku po prawej stronie $\left(\frac{P}{P_1}\right)^2$, ale liczba ta jest równa $+1$. Stąd na mocy (18)

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \frac{1-\varepsilon_1}{2} + \frac{P-1}{2} \frac{P_1-1}{2}} \left(\frac{P}{P_1}\right).$$

Lecz

$$\begin{aligned} \frac{P-1}{2} \frac{1-\varepsilon_1}{2} + \frac{P-1}{2} \frac{P_1-1}{2} &= \frac{P-1}{2} \frac{P_1-\varepsilon_1}{2} = \frac{P-1}{2} \frac{\varepsilon_1 P_1 - \varepsilon_1^2}{2\varepsilon_1} = \\ &= \frac{P-1}{2} \frac{\varepsilon_1 P_1 - 1}{2}, \end{aligned}$$

gdyż $\varepsilon_1^2 = 1$, a ponieważ jest oczywiście

$$(19) \quad (-1)^{\frac{a}{\varepsilon_1}} = (-1)^a \quad \text{dla } \varepsilon_1 = \pm 1,$$

więc

$$(-1)^{\frac{P-1}{2} \frac{1-\varepsilon_1}{2} + \frac{P-1}{2} \frac{P_1-1}{2}} = (-1)^{\frac{P-1}{2} \frac{\varepsilon_1 P_1 - 1}{2}}$$

i przeto

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \frac{\varepsilon_1 P_1 - 1}{2}} \left(\frac{P}{P_1}\right).$$

Podobnie z drugiej równości ciągu (17) znajdujemy

$$\left(\frac{P}{P_1}\right) = (-1)^{\frac{P_1-1}{2} \frac{\varepsilon_1 P_1-1}{2}} \left(\frac{P_1}{P}\right)$$

itd., wreszcie z przedostatniej:

$$\left(\frac{P_{n-2}}{P_{n-1}}\right) = (-1)^{\frac{P_{n-2}-1}{2} \frac{\varepsilon_{n-1} P_{n-1}-1}{2}} \left(\frac{P_{n-1}}{P_{n-2}}\right).$$

Z ostatniej równości ciągu (17) mamy przede wszystkim

$$(20) \quad \left(\frac{P_{n-2}}{P_{n-1}}\right) = \left(\frac{\varepsilon_n}{P_{n-1}}\right),$$

gdyż $P_n = 1$. Lecz, dla $\varepsilon_n = \pm 1$ jest na mocy (19)

$$\left(\frac{\varepsilon_n}{P_{n-1}}\right) = (-1)^{\frac{P_{n-1}-1}{2} \frac{1-\varepsilon_n}{2}},$$

skąd na mocy (20) wobec $P_n = 1$

$$\left(\frac{P_{n-2}}{P_{n-1}}\right) = \left(\frac{\varepsilon_n}{P_{n-1}}\right) = (-1)^{\frac{P_{n-1}-1}{2} \frac{1-\varepsilon_n}{2}} = (-1)^{\frac{P_{n-1}-1}{2} \frac{\varepsilon_n P_{n-1}-1}{2}}.$$

Uwzględniając kolejno równości otrzymane dla

$$\left(\frac{Q}{P}\right), \left(\frac{P}{P_1}\right), \dots, \left(\frac{P_{n-1}}{P_{n-2}}\right),$$

dostajemy

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \frac{\varepsilon_1 P_1-1}{2} + \frac{P_1-1}{2} \frac{\varepsilon_2 P_2-1}{2} + \dots + \frac{P_{n-1}-1}{2} \frac{\varepsilon_n P_n-1}{2}}.$$

Znak prawej strony zależy od liczby składników nieparzystych w wykładniku. Iloczyn

$$\frac{P-1}{2} \frac{\varepsilon_1 P_1-1}{2}$$

— jak to od razu widzimy — jest liczbą nieparzystą wtedy i tylko wtedy, gdy obie liczby P i $\varepsilon_1 P_1$ są formy $4k+3$. Możemy więc napisać

$$(21) \quad \left(\frac{Q}{P}\right) = (-1)^m,$$

gdzie m wskazuje, ile razy liczby P_{i-1} i $\varepsilon_i P_i$ (dla $i=1, 2, \dots, n$) są jednocześnie obie formy $4k+3$. Stąd:

Prawidło Eisensteina. Liczymy, ile razy w równościach (17) liczby P_{i-1} i $\varepsilon_i P_i$ są obie jednocześnie formy $4k+3$; jeżeli m razy, to zachodzi równość (21).

Prawidło to — jak widzimy — istotnie pozwala się obyć w obliczaniu wartości symbolu Jacobiego bez rozwijania liczb na czynniki pierwsze.

PRZYKŁADY. 1. Obliczmy według prawidła Eisensteina wartość symbolu $\left(\frac{641}{257}\right)$. Sposobem (17) tworzymy równości:

$$641 = 2 \cdot 257 + 127,$$

$$257 = 2 \cdot 127 + 5,$$

$$127 = 42 \cdot 3 + 1.$$

Z par

$$257, 127, \quad 127, 5, \quad 5, 1$$

tylko w drugiej obie liczby są formy $4k+3$. Mamy więc w danym razie $m=1$ i przeto

$$\left(\frac{641}{257}\right) = -1.$$

Liczba 641 jest więc nieresztą kwadratową dla liczby 257.

2. Obliczmy wartość symbolu $\left(\frac{65537}{274177}\right)$. Otrzymujemy ciąg równości:

$$65537 = 0 \cdot 274177 + 65537,$$

$$274177 = 4 \cdot 65537 + 12029,$$

$$65537 = 6 \cdot 12029 - 6637,$$

$$12029 = 2 \cdot 6637 - 1245,$$

$$6637 = 6 \cdot 1245 - 833,$$

$$1245 = 2 \cdot 833 - 421,$$

$$833 = 2 \cdot 421 - 9,$$

$$421 = 46 \cdot 9 + 7,$$

$$9 = 2 \cdot 7 - 5,$$

$$7 = 2 \cdot 5 - 3,$$

$$5 = 2 \cdot 3 - 1.$$

Spośród par $P_{i-1}, \varepsilon_i P_i$ tylko w parach 7, -5 oraz 3, -1 obie liczby są formy $4k+3$. Mamy przeto $m=2$, skąd

$$\left(\frac{65537}{274177}\right) = 1.$$

3. Obliczmy wartość symbolu $\left(\frac{-104}{997}\right)$. Mamy

$$-104 = (-1) \cdot 2^3 \cdot 13,$$

więc

$$\left(\frac{-104}{997}\right) = \left(\frac{-1}{997}\right) \left(\frac{2}{997}\right)^3 \left(\frac{13}{997}\right).$$

Liczba 997 jest formy $4k+1$, zatem $\left(\frac{-1}{997}\right) = 1$; liczba 997 jest też formy $8k+5$, zatem $\left(\frac{2}{997}\right) = -1$. Stąd

$$\left(\frac{-104}{997}\right) = -\left(\frac{13}{997}\right).$$

Dla obliczenia wartości $\left(\frac{13}{997}\right)$ tworzymy ciąg równości:

$$\begin{aligned} 13 &= 0 \cdot 997 + 13, & 13 &= 2 \cdot 9 - 5, \\ 997 &= 76 \cdot 13 + 9, & 9 &= 2 \cdot 5 - 1. \end{aligned}$$

Nie ma tu ani jednej pary liczb $P_{i-1}, \varepsilon_i P_i$ formy $4k+3$, więc $m=0$, skąd $\left(\frac{13}{997}\right) = 1$ i przeto

$$\left(\frac{-104}{997}\right) = -1,$$

§ 7. Dowód istnienia nieskończenie wielu liczb pierwszych w postępach arytmetycznych $5k-1$, $8k-1$ i $12k-1$. Jako zastosowanie symbolu Legendre'a i jego własności udowodnimy, że w każdym z postępów arytmetycznych

$$5k-1, \quad 8k-1, \quad 12k-1$$

jest nieskończenie wiele liczb pierwszych.

Twierdzenie 1. *Liczb pierwszych formy $5k-1$ jest nieskończenie wiele.*

Dowód. Przypuśćmy przeciwnie, że liczb tych jest tylko n . Niech to będą liczby

$$(23) \quad p_1, p_2, \dots, p_n$$

i niech

$$(24) \quad P = p_1 p_2 \dots p_n.$$

Weźmy pod uwagę liczbę

$$(25) \quad N = 20P^2 - 1.$$

Jest to oczywiście liczba formy $5k-1$, nieparzysta i większa od jedności. Nie jest ona podzielna przez żadną z liczb (23), gdyż z równości $1 = 20P^2 - N$ wynika, że liczby P i N są względnie pierwsze.

Liczba N nie może być pierwsza, bo to przeczyłoby założeniu, że wszystkie liczby pierwsze formy $5k-1$ są czynnikami iloczynu P . Liczba N jest więc złożona, a ponieważ jest nieparzysta, więc wszystkie jej czynniki pierwsze są nieparzyste. Niech p będzie którymkolwiek z nich. Zatem $20P^2 - 1 \equiv 0 \pmod{p}$, skąd

$$(26) \quad 20P^2 \equiv 1 \pmod{p}.$$

Podnosząc obie strony do potęgi $\frac{p-1}{2}$, otrzymujemy

$$(27) \quad 20^{\frac{p-1}{2}} P^{p-1} \equiv 1 \pmod{p}.$$

W myśl (26) liczba P jest niepodzielna przez liczbę pierwszą p . Ale w takim razie na mocy małego twierdzenia Fermata

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

wobec czego na mocy kongruencji (27)

$$20^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

skąd na mocy twierdzenia Eulera

$$\left(\frac{20}{p}\right) = +1.$$

Lecz na mocy własności II i IV symbolu Legendre'a

$$\left(\frac{20}{p}\right) = \left(\frac{2}{p}\right)^2 \left(\frac{5}{p}\right) = \left(\frac{5}{p}\right),$$

na mocy zaś prawa wzajemności liczb pierwszych

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right),$$

skąd

$$(28) \quad \left(\frac{p}{5}\right) = +1.$$

Liczba p , jako niepodzielna przez 5, musi być formy $5k \pm 1$ lub $5k \pm 2$. Gdyby jednak było $p = 5k \pm 2$, to mielibyśmy

$$\left(\frac{p}{5}\right) = \left(\frac{5k \pm 2}{5}\right) = \left(\frac{\pm 2}{5}\right) = \left(\frac{\pm 1}{5}\right) \left(\frac{2}{5}\right) = -1$$

wbrew (28). Jest więc $p = 5k + 1$ lub $p = 5k - 1$.

Ale nie wszystkie czynniki pierwsze liczby N mogą być formy $5k + 1$, gdyż wtedy N też byłoby liczbą tej formy wbrew (24). Jeden więc przynajmniej z czynników pierwszych liczby N jest formy $5k - 1$. Niech to będzie czynnik p_0 . Ponieważ — jak widzieliśmy — liczby N i P są względnie pierwsze, więc p_0 nie jest żadną z liczb pierwszych ciągu (23). Przeczy to przypuszczeniu, że iloczyn P obejmuje wszystkie liczby pierwsze formy $5k - 1$. W postępie arytmetycznym

$$4, 9, 14, 19, 24, 29, \dots$$

jest zatem nieskończenie wiele liczb pierwszych, c. b. d. o.

Twierdzenie 2. Liczb pierwszych formy $8k - 1$ jest nieskończenie wiele.

Dowód. Przypuśćmy, że tak nie jest, i niech ciąg skończony (23) zawiera wszystkie liczby tej formy.

Weźmy pod uwagę liczbę

$$N = 8P^2 - 1,$$

gdzie P jest określone wzorem (24). Liczba N , sama formy $8k - 1$ i pierwsza względem iloczynu P , nie może być pierwszą. Niech p będzie dzielnikiem pierwszym (nieparzystym) liczby P . Zatem $8P^2 - 1 \equiv 0 \pmod{p}$, skąd jak wyżej

$$\left(\frac{8}{p}\right) = +1.$$

Lecz $\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)^2 \left(\frac{2}{p}\right) = \left(\frac{2}{p}\right)$, więc $\left(\frac{2}{p}\right) = 1$, czyli na mocy włas-

ności IV symbolu Legendre'a $(-1)^{\frac{p^2-1}{8}} = 1$, i przeto wykładnik $\frac{p^2-1}{8}$ jest liczbą parzystą, skąd

$$(29) \quad p^2 \equiv 1 \pmod{16}.$$

Liczba p , jako nieparzysta, musi być formy $8k \pm 1$ lub $8k \pm 5$. Gdyby jednak było $p = 8k \pm 5$, to mielibyśmy

$$p^2 = 16(4k^2 \pm 5k) + 9 \equiv 9 \pmod{16}$$

wbrew (29). Jest więc $p = 8k + 1$ lub $p = 8k - 1$. Lecz nie wszystkie czynniki pierwsze liczby N są formy $8k + 1$, gdyż sama liczba N jest formy $8k - 1$; znajdzie się więc co najmniej jeden formy $8k - 1$. Czynniki ten nie jest żadną z liczb (23), gdyż N i P są względnie pierwsze. Przeczy to założeniu, że w iloczynie P zawarte są wszystkie liczby pierwsze formy $8k - 1$. W postępie arytmetycznym

$$7, 15, 23, 31, 39, 47, \dots$$

jest zatem nieskończenie wiele liczb pierwszych, c. b. d. o.

Twierdzenie 3. Liczb pierwszych formy $12k - 1$ jest nieskończenie wiele.

Dowód. Przypuśćmy, że ciąg (23) zawiera wszystkie liczby pierwsze formy $12k - 1$, i niech P będzie ich iloczynem (24). Weźmy pod uwagę liczbę

$$N = 12P^2 - 1.$$

Jak wyżej, dochodzimy do wniosku, że N ma czynnik pierwszy nieparzysty p , dla którego

$$\left(\frac{12}{p}\right) = +1.$$

Lecz $\left(\frac{12}{p}\right) = \left(\frac{2}{p}\right)^2 \left(\frac{3}{p}\right) = \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)$, skąd

$$(30) \quad (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = +1.$$

Liczba p , jako pierwsza względem 3, musi być jednej z form:

$$12k + 1, \quad 12k + 5, \quad 12k - 5, \quad 12k - 1.$$

Gdyby p było formy $12k+5$, to mielibyśmy

$$(-1)^{\frac{p-1}{2}} = (-1)^{6k+2} = +1 \quad \text{i} \quad \left(\frac{p}{5}\right) = \left(\frac{12k+5}{5}\right) = \left(\frac{2}{5}\right) = -1,$$

skąd $(-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right) = -1$ wbrew (30). Podobnie w razie $p=12k-5$ byłoby

$$(-1)^{\frac{p-1}{2}} = (-1)^{6k-3} = -1 \quad \text{i} \quad \left(\frac{p}{5}\right) = \left(\frac{12k-5}{5}\right) = \left(\frac{-5}{5}\right) = \left(\frac{1}{5}\right) = 1,$$

skąd $(-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right) = -1$ wbrew (30). Jest więc $p=12k+1$ albo $p=12k-1$. Lecz nie wszystkie czynniki pierwsze liczby N , która jest sama formy $12k-1$, mogą być formy $12k+1$; znajdzie się więc wśród nich co najmniej jeden formy $12k-1$. Stąd, jak wyżej, otrzymujemy wniosek sprzeczny z przypuszczeniem.

W postępie arytmetycznym

$$11, 23, 35, 47, 59, \dots$$

jest zatem nieskończenie wiele liczb pierwszych, c. b. d. o.

ROZDZIAŁ XV

ZARYS TEORII FORM KWADRATOWYCH

§ 1. Formy kwadratowe dwójkowe jednorodne i ich wyróżnik. Zagadnienie podstawowe teorii form kwadratowych. Formą kwadratową dwójkową jednorodną nazywamy wyrażenie

$$(1) \quad ax^2 + bxy + cy^2,$$

gdzie a, b i c są liczbami całkowitymi, a x i y — zmiennymi, przebiegającymi tylko wartości całkowite. Wyrażenie (1) oznaczamy przez

$$(a, b, c).$$

Liczbę

$$D = b^2 - 4ac$$

nazywamy *wyróżnikiem* (*dyskryminantą*) formy kwadratowej (1).

Będziemy zakładali, że D nie jest kwadratem liczby całkowitej, gdyż w przeciwnym razie forma (1) byłaby iloczynem dwu form liniowych. W razie bowiem $D = b^2 - 4ac = d^2$ i $a \neq 0$, byłoby $(b-d)(b+d) = 4ac$, skąd wnosimy z łatwością, że liczby $b-d$ i $b+d$ byłyby obie parzyste. Ale jeżeli $b-d = 2k$ i $b+d = 2l$, to $kl = ac$. Niech $(k, a) = \delta$. Wówczas byłoby $k = k_1\delta$ i $a = a_1\delta$, gdzie $(k_1, a_1) = 1$ i $k_1\delta l = a_1\delta c$, skąd $k_1 l = a_1 c$. Wobec $(k_1, a_1) = 1$ byłoby więc $a_1 | l$ czyli $l = l_1 a_1$, gdzie l_1 jest liczbą całkowitą, i mielibyśmy:

$$2ax + (b-d)y = 2\delta(a_1x + k_1y),$$

$$2ax + (b+d)y = 2a_1(\delta x + l_1y),$$

skąd wobec $d^2 = D$

$$4a(ax^2 + bxy + cy^2) = (2ax + b)^2 - D y^2 =$$

$$= [2ax + (b-d)y][2ax + (b+d)y] = 4a_1\delta(a_1x + k_1y)(\delta x + l_1y),$$

co daje wobec $a_1\delta = a$ po podzieleniu obu stron przez $4a$

$$ax^2 + bxy + cy^2 = (a_1x + k_1y)(\delta x + l_1y).$$