Kamil Sikorski

Prawa wzajemności Gaussa

Pytanie 1. *Dla jakich liczb pierwszych p kongruencja* $x^2 \equiv a(p)$ *ma rozwiązanie?*

1. Theorema Aureum

Celem tej części jest pokazanie, że $x^2 \equiv q(p)$ ma rozwiązanie $\Leftrightarrow$ ma je $x^2 \equiv p(q)$, gdzie p i q są różnymi, nieparzystymi liczbami pierwszymi.
Fakt ten zapisuje się także za pomocą tzw. symbolu Legendre'a

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

1.1. Reszty kwadratowe

Jeśli $(a, m) = 1$, to a jest zwane resztą kwadratową mod m jeśli kongruencja $x^2 \equiv a(m)$ ma rozwiązanie. W przeciwnym przypadku a jest nieresztą kwadratową mod m.
Na przykład 2 jest resztą kwadratową mod 7, ale 3 już nie. Rzeczywiście $1^2,\ 2^2,\ ,3^2,\ 4^2,\ 5^2$ *i* 6^2 przystają odpowiednio do 1, 4, 2, 2, 4 *i* 1. Stąd 1, 2 *i* 4 są resztami kwadratowymi, a 3, 5 *i* 6 nie.

Definicja 1.1.1. *Symbol* (a/p) *będzie mieć wartość 1 kiedy a jest resztą kwadratową mod p, -1 kiedy a jest nieresztą kwadratową mod p i 0 kiedy* $p \mid a$. (a/p) *jest zwany symbolem Legendre'a.*

Spośród własności symbolu Legendre'a warto wymienić
(a) $(a/p)(p) \equiv a^{(p-1)/2}$
(b) $(ab/p) = (a/p)(b/p)$
(c) Jeśli $a \equiv b$, *to* $(a/p) = (b/p)$
(d) $(-1/p) = (-1)^{(p-1)/2}$
(e) $(2/p) = (-1)^{(p^2-1)/8}$
(f) $(p/q)(q/p) = (-1)^{((p-1)/2))((q-1)/2)}$

Każda liczba nieparzysta jest postaci $4k + 1$ lub $4k + 3$. Ciekawy jest zwłaszcza podpunkt (d), który można przeformułować następująco: $x^2 \equiv -1(p)$ ma rozwiązanie $\Leftrightarrow$ p jest postaci $4k + 1$.
Natomiast podpunkt(f), którego dowód jest na końcu rozdziału, daje odpowiedź na początkowe pytanie.

Twierdzenie 1.1.1. *Niech q będzie nieparzystą liczbą pierwszą.*

(a) *Jeśli $q \equiv 1(4)$, to q jest resztą kwadratową mod $p \Leftrightarrow p \equiv r(q)$, gdzie r jest resztą kwadratową mod q.*

(b) *Jeśli $q \equiv 3(4)$, to q jest resztą kwadratową mod $p \Leftrightarrow p \equiv \pm b^2(4q)$, gdzie b jest nieparzystą liczbą względnie pierwszą z q.*

Uogólnieniem symbolu Legendre'a dla wszystkich liczb nieparzystych jest symbol Jacobiego

Definicja 1.1.2. *Niech b będzie nieparzystą, dodatnią liczbą całkowitą i a dowolne całkowite. Niech $b = p_1 p_2 \dots p_m$, gdzie p_i są pierwsze, niekoniecznie różne. Symbol (a/b) zdefiniowany następująco*

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_1}\right)$$

jest zwany symbolem Jacobiego.

Symbol Jacobiego ma bardzo zbliżone właściwości do symbolu Legendre'a, jednakże należy zaznaczyć, że (a/b) może być równe 1 i jednocześnie a nie musi być resztą kwadratową mod b. Na przykład $(2/15) = (2/3)(2/5) = (-1)(-1) = 1$, ale 2 nie jest resztą kwadratową mod 15. Jest prawdą natomiast, że jeśli $(a/b) = -1$, to a jest nieresztą kwadratową mod b.

1.2. Dowód prawa wzajemności reszt kwadratowych

Istnieją setki dowodów tego twierdzenia. My pokażemy dowód autorstwa Eisensteina.
Rozważmy funkcję $f(z) = e^{2\pi iz} - e^{-2\pi iz} = 2i \sin 2\pi z$. Spełnia ona warunek $f(-z) = -f(z)$.

Stwierdzenie 1.2.1. *Niech n będzie dodatnie, nieparzyste i całkowite i $f(z) = e^{2\pi iz} - e^{-2\pi iz}$, wtedy*

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right)$$

Stwierdzenie 1.2.2. *Jeśli p jest nieparzysta i pierwsza, $a \in \mathbb{Z}$ i $p \nmid a$, to*

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{la}{p}\right) = \left(\frac{a}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right)$$

Dowód prawa wzajemności reszt kwadratowych. Niech p i q będą nieparzyste i pierwsze. Wtedy z poprzedniego stwierdzenia

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{lq}{p}\right) = \left(\frac{q}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right)$$

Ze Stwierdzenia 1.2.1

$$\frac{f(ql/p)}{f(l/p)} = \prod_{m=1}^{(q-1)/2} f\left(\frac{l}{p} + \frac{m}{q}\right) f\left(\frac{l}{p} - \frac{m}{q}\right)$$

Co razem daje

$$\left(\frac{q}{p}\right) = \prod_{m=1}^{(q-1)/2} \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p} + \frac{m}{q}\right) f\left(\frac{l}{p} - \frac{m}{q}\right)$$

W ten sam sposób znajdujemy

$$\left(\frac{p}{q}\right) = \prod_{m=1}^{(q-1)/2} \prod_{l=1}^{(p-1)/2} f\left(\frac{m}{q} + \frac{l}{p}\right) f\left(\frac{m}{q} - \frac{l}{p}\right)$$

A skoro $f(m/q - l/p) = -f(l/p - m/q)$ widać więc, że

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

Stąd dostajemy

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

■

2. Prawo wzajemności reszt sześciennych i dwukwadratowych

Zanim przejdziemy do omawiania reszt sześciennych wprowadzimy kilka pojęć potrzebnych później.

2.1. Sumy Gaussa i Jacobiego

Charakterem multiplikatywnym na $F_p = \mathbb{Z}/p\mathbb{Z}$ nazywamy odwzorowanie χ z F_p^* do liczb zespolonych bez zera, które spełnia

$$\chi(ab) = \chi(a)\chi(b) \text{ dla każdego } a,\ b \in F_p^*$$

Symbol Legendre'a jest przykładem takiego charakteru, jeśli rozpatrywać go jako funkcję warstwy a modulo p. Innym przykładem jest charakter trywialny $\varepsilon(a) = 1$ dla każdego $a \in F_p$.

Charaktery multiplikatywne tworzą grupę w sensie następującej definicji.

(1) Jeśli χ *i* λ są charakterami, to $\chi\lambda$ jest odwzorowaniem, które przekształca $a \in F_p^*$ *do* $\chi(a)\lambda(a)$

(2) Jeżeli χ jest charakterem, to χ^{-1} jest odwzorowaniem, które przekształca $a \in F_p^*$ *do* $\chi(a)^{-1}$

Jedynką tej grupy jest oczywiście charakter trywialny ε.

Stwierdzenie 2.1.1. *Grupa charakterów jest cykliczną grupą rzędu* $p - 1$. *Jeśli* $a \in F_p^*$ *i* $a \neq 1$, *to istnieje charakter* χ *taki, że* $\chi(a) \neq 1$.

Wniosek 2.1.1. *Jeśli* $a \in F_p^*$ *i* $a \neq 1$, *to* $\sum_\chi \chi(a) = 0$, *gdzie sumujemy po wszystkich charakterach.*

Definicja 2.1.1. *Niech χ będzie charakterem na F_p i $a \in F_p$. Niech $g_a(\chi) = \sum_t \chi(t)\zeta^{at}$, gdzie sumujemy po wszystkich t w F_p i $\zeta = e^{2\pi i/p}$. $g_a(\chi)$ jest tzw. sumą Gaussa na F_p charakteru χ.*

Oznaczamy $g_1(\chi)$ *jako* $g(\chi)$.

Stwierdzenie 2.1.2. *Jeśli $a \neq 0$ i $\chi \neq \varepsilon$, to $g_a(\chi) = \chi(a^{-1})g_1(\chi)$. Jeśli $a \neq 0$ i $\chi = \varepsilon$, to $g_a(\varepsilon) = 0$. Jeśli $a = 0$ i $\chi \neq \varepsilon$, to $g_0(\chi) = 0$. Jeśli $a = 0$ i $\chi = \varepsilon$, to $g_0(\varepsilon) = p$.*

Rozważmy równanie $x^2+y^2 = 1$, które nad ciałem F_p ma skończenie wiele rozwiązań. Ich liczbę oznaczmy jako $N(x^2 + y^2 = 1)$ i zauważmy, że

$$N(x^2 + y^2 = 1) = \sum_{a+b=1} N(x^2 = a)N(y^2 = b),$$

gdzie sumujemy po wszystkich parach $a,\ b \in F_p$ spełniających warunek $a + b = 1$. Jako, że $N(x^2 = a) = 1 + (a/p)$, otrzymujemy przez podstawienie, że

$$N(x^2 + y^2 = 1) = p + \sum_a \left(\frac{a}{p}\right) + \sum_b \left(\frac{b}{p}\right) + \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Pierwsze dwie sumy są równe zero, więc pozostaje obliczyć trzecią sumę, która jak się okazuje wynosi $-(-1)^{(p-1)/2}$. Stąd $N(x^2+y^2 = 1)$ *wynosi* $p-1$ jeśli $p \equiv 1\ (4)$ *i* $p+1$ *gdy* $p \equiv 3\ (4)$.

Definicja 2.1.2. *Niech χ i λ będą charakterami w F_p i niech $J(\chi,\ \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$. $J(\chi,\ \lambda)$ jest zwane sumą Jacobiego.*

Stwierdzenie 2.1.3. *Załóżmy, że $p \equiv 1\ (n)$ i χ jest charakterem rzędu $n > 2$. Wtedy*

$$g(\chi)^n = \chi(-1)pJ(\chi,\ \chi)J(\chi,\ \chi^2)\dots J(\chi,\ \chi^{n-2})$$

2.2. Reszty sześcienne

Celem tej części jest pokazanie, że podobnie jak między kongruencjami kwadratowymi, tak i między kongruencjami sześciennymi istnieje zależność. Mianowicie $x^3 \equiv q(p)$ ma rozwiązanie $\Leftrightarrow$ ma je $x^3 \equiv p(q)$

Na początek rozważmy równanie $x^3 = 1$. Jako, że $x^3 - 1 = (x - 1)(x^2 + x + 1)$, więc pierwiastkami tego równania są $1\ i\ (-1 \pm \sqrt{-3})/2$. Niech $\omega = (-1+\sqrt{-3})/2$. Łatwo sprawdzić, że $\omega^2 = (-1-\sqrt{-3})/2$ i $1+\omega+\omega^2 = 0$. Rozważmy zbiór $\mathbb{Z}[\omega] = \{a+b\omega | a,\ b \in \mathbb{Z}\}$. Tworzy on pierścień z dodawaniem i mnożeniem, który jest zamknięty ze względu na operację sprzężenia, oraz jest dziedziną z jednoznacznością rozkładu. Dla elementu $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ definiujemy normę $\alpha,\ N\alpha = \alpha\overline{\alpha} = a^2 - ab + b^2$, gdzie $\overline{\alpha}$ oznacza sprzężenie α. Będziemy stosować notację $\lambda(\alpha)$ zamiast $N\alpha$ oraz $D = \mathbb{Z}[\omega]$.

Warto wymienić parę właściwości pierścienia D

(a) $\alpha \in D$ jest jednością $\Leftrightarrow\ N\alpha = 1$. Jednościami w D są $1,\ -1,\ \omega,\ -\omega,\ \omega^2\ i\ -\omega^2$.

(b) Jeśli π jest elementem pierwszym w D, to istnieje liczba pierwsza całkowita taka, że $N\pi = p\ lub\ p^2$. W pierwszym przypadku π nie jest stowarzyszona z liczbą pierwszą całkowitą; w drugim jest stowarzyszona z p.

(c) Jeśli $\pi \in D$ jest takie, że $N\pi = p$ jest liczbą pierwszą całkowitą, to π jest elementem pierwszym w D.

(d) Załóżmy, że p i q są liczbami pierwszymi całkowitymi. Jeśli $q \equiv 2\ (3)$, to q jest elementem pierwszym w D. Jeśli $p \equiv 1\ (3)$, to $p = \pi\overline{\pi}$, gdzie π jest pierwszy w D. Wtedy też $3 = -\omega^2(1-\omega)^2$ i $1-\omega$ jest pierwsze w D.

W pierścieniu D możemy wprowadzić pojęcie kongruencji. Jeśli $\alpha,\ \beta,\ \gamma \in D\ i\ \gamma \neq 0$ nie jest jednością(jest nieodwracalna), to mówimy, że $\alpha \equiv \beta\ (\gamma)$ jeśli $\gamma\ dzieli\ \alpha - \beta$. Tak jak w $\mathbb{Z}$ i tu możemy stworzyć pierścień $D/\gamma D$ z klas reszt modulo γ, który dla $\gamma \in D$ będących elementami pierwszymi tworzy skończone ciało z $N\gamma$ elementami.

W tym miejscu należy przywołać wynik z teorii ciał skończonych.

Stwierdzenie 2.2.1. *Niech F będzie skończonym ciałem z q elementami, $\alpha \in F^*$. Wtedy $x^n = \alpha$ ma rozwiązanie $\Leftrightarrow\ \alpha^{(q-1)/d} = 1$, gdzie $d = (n,\ q-1)$. Jeśli istnieją rozwiązania, to jest ich dokładnie d.*

Teraz, podobnie jak w poprzednim rozdziale, wprowadzamy symbol, którym będziemy posługiwać się przy sprawdzaniu czy dana liczba jest resztą sześcienną.

Definicja 2.2.1. *Jeśli $N\pi \neq 3$, to charakter reszty sześciennej liczby α modulo π jest dany następująco*

(a) $(\alpha/\pi)_3 = 0\ gdy\ \pi \mid \alpha$

(b) $\alpha^{(N\pi-1)/3} \equiv (\alpha/\pi)_3\ (\pi)\ i\ (\alpha/\pi)_3\ wynosi\ 1,\ \omega\ lub\ \omega^2$.

$(\alpha/\pi)_3$ jest odpowiednikiem symbolu Legendre'a i posiada wiele analogicznych własności.

Stwierdzenie 2.2.2. **(a)** $(\alpha/\pi)_3 = 1\ \Leftrightarrow\ x^3 \equiv \alpha\ (\pi)$ *ma rozwiązanie, tzn.* $\Leftrightarrow\ \alpha$ *jest resztą sześcienną*

(b) $\alpha^{(N\pi-1)/3} \equiv (\alpha/\pi)_3$

(c) $(\alpha\beta/\pi)_3 = (\alpha/\pi)_3(\beta/\pi)_3$

(d) *Jeśli* $\alpha \equiv \beta\ (\pi),\ to\ (\alpha/\pi)_3 = (\beta/\pi)_3$

Dowód. Część (a) jest szczególnym przypadkiem Stwierdzenia 2.2.1. Biorąc $F = D/\pi D,\ q = N\pi\ i\ n = 3$ dostajemy tezę.
Część (b) wynika natychmiast z definicji.
Część (c): $(\alpha\beta/\pi)_3 \equiv (\alpha\beta)^{(N\pi-1)/3} \equiv \alpha^{(N\pi-1)/3}\beta^{(N\pi-1)/3} \equiv (\alpha/\pi)_3(\beta/\pi)_3\ (\pi)$

Z czego wynika teza.
Część (d): Jeśli $\alpha \equiv \beta\ (\pi),\ to\ (\alpha/\pi)_3 \equiv \alpha^{(N\pi-1)/3} \equiv \beta^{(N\pi-1)/3} \equiv (\beta/\pi)_3\ (\pi)$, więc $(\alpha/\pi)_3 = (\beta/\pi)_3$.

Od tej pory będziemy stosować notację $\chi_\pi(\alpha) = (\alpha/\pi)_3$
Warto przyjrzeć się też właściwościom charakterów przy operacji sprzężenia.

Stwierdzenie 2.2.3. **(a)** $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$
(b) $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$
(c) $\chi_q(\overline{\alpha}) = \chi_q(\alpha^2)$ *i* $\chi_q(n) = 1$ *jeśli n jest liczbą pierwszą całkowitą względnie pierwszą z q.*

Z podpunktu (c) wynika, że n jest resztą sześcienną modulo q. Stąd jeśli $q_1 \neq q_2$ są dwiema liczbami pierwszymi przystającymi do 2 modulo 3, wtedy trywialnie mamy $\chi_{q_1}(q_2) = \chi_{q_2}(q_1)$. Jest to przypadek szczególny prawa wzajemności reszt sześciennych. Aby sformułować ogólne prawo musimy wprowadzić pojęcie liczb pierwszych prymarnych.

Definicja 2.2.2. *Jeśli π jest pierwsze w D, to mówimy, że π jest prymarne jeśli $\pi \equiv 2\ (3)$.*
Jeśli $\pi = q$ jest całkowite, to nie wprowadzamy nic nowego. Jeśli natomiast $\pi = a + b\omega$ jest liczbą pierwszą zespoloną, to definicja jest równoznaczna z $a \equiv 2\ (3)$ i $b \equiv 0\ (3)$.
Pojęcie prymarności jest potrzebne, aby pozbyć się niejednoznaczności związanej z faktem, że każdy niezerowy element D ma sześć elementów stowarzyszonych.

Stwierdzenie 2.2.4. *Załóżmy, że $N\pi = p \equiv 1\ (3)$. Wśród elementów stowarzyszonych z π dokładnie jeden jest prymarny.*

Twierdzenie 2.2.1. *(Prawo wzajemności reszt sześciennych) Niech π_1 i π_2 będą prymarne, $N\pi_1,\ N\pi_2 \neq 3$, i $N\pi_1 \neq N\pi_2$. Wtedy*

$$\chi_{q_1}(q_2) = \chi_{q_2}(q_1)$$

(a) Należy rozpatrzyć trzy przypadki. Mianowicie obie liczby π_1 i π_2 są całkowite, π_1 jest całkowite i π_2 jest zespolone, oraz obie π_1 i π_2 są zespolone. Pierwszy przypadek jest trywialny.
(b) Charakter sześcienny jedności rozstrzyga się następująco. Z tego, że $-1 = (-1)^3$ mamy $\chi_\pi(-1) = 1$ dla wszystkich elementów pierwszych π. Jeśli $N\pi \neq 3$, wtedy ze Stwierdzenia 2.2.2 podpunktu (b) wynika, że $\chi_\pi(\omega) = \omega^{(N\pi-1)/3}$. Stąd $\chi_\pi(\omega) = 1,\ \omega\ lub\ \omega^2$ w zależności, czy $N\pi \equiv 1,\ 4\ czy\ 7\ modulo\ 9$.

2.3. Dowód prawa zależności dla reszt sześciennych

Niech π będzie liczbą pierwszą zespoloną taką, że $N\pi = p \equiv 1\ (3)$. Z tego, że $D/\pi D$ jest skończonym ciałem charakterystyki p wynika, że zawiera ono kopię $\mathbb{Z}/p\mathbb{Z}$. Oba ciała mają p elementów, więc możemy je utożsamiać. Dzięki temu możemy rozważać χ_π jako charakter sześcienny na $\mathbb{Z}/p\mathbb{Z}$ w sensie sum Gaussa i Jacobiego. Zachodzą wtedy tożsamości
(a) $g(\chi)^3 = pJ(\chi,\ \chi)$
(b) Jeśli $J(\chi,\ \chi) = a + b\omega$, to $a \equiv -1\ (3)\ i\ b \equiv 0\ (3)$
(c) $(\chi_\pi,\ \chi_\pi) = \pi$
(d) $g(\chi_\pi)^3 = p\pi$

Dowód prawa wzajemności. Rozważmy najpierw przypadek $\pi_1 = q \equiv 2\ (3)\ i\ \pi_2 = \pi,\ gdzie\ N\pi = p$.
Podnosząc obie strony równania $g(\chi_\pi)^3 = p\pi$ do potęgi $(g^2-1)/3$otrzymujemy $g(\chi_\pi)^{q^2-1} = (p\pi)^{(q^2-1)/3}$. Biorąc kongruencję modulo q widzimy, że

$$g(\chi_\pi)^{q^2-1} \equiv \chi_q(p\pi)\ (q).$$

$\chi_q(p) = 1$ co daje

$$g(\chi_\pi)^{q^2} \equiv \chi_q(\pi)g(\chi_\pi)\ (q). \tag{1}$$

Przeanalizujemy teraz lewą stronę:

$$g(\chi_\pi)^{q^2} = \left(\sum \chi_\pi(t)\zeta^t\right)^{q^2} \equiv \sum \chi_\pi(t)^{q^2}\zeta^{q^2t}\ (q).$$

A jako, że $q^2 \equiv 1\ (3)\ i\ \chi_\pi(t)$ jest pierwiastkiem sześciennym z 1, mamy

$$g(\chi_\pi)^{q^2} \equiv g_{q^2}(\chi_\pi)\ (q). \tag{2}$$

Ze stwierdzenia 2.1.2. $g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})g(\chi_\pi) = \chi_\pi(q)g(\chi_\pi)$. Łącząc równania (1) i (2)

$$\chi_\pi(q)g(\chi_\pi) \equiv \chi_q(\pi)g(\chi_\pi)(q).$$

Mnożymy obie strony tej kongruencji przez $g(\overline{\chi_\pi})$. Jako, że $g(\chi_\pi)g(\overline{\chi_\pi}) = p$,

$$\chi_\pi(q)p \equiv \chi_q(\pi)p(q)$$

albo

$$\chi_\pi(q) \equiv \chi_q(\pi)(q),$$

dając

$$\chi_\pi(q) = \chi_q(\pi).$$

Pozostaje rozpatrzyć przypadek dwóch zespolonych liczb pierwszych π_1 i π_2, gdzie $N\pi_1 = p_1 \equiv 1\ (3)\ i\ N\pi_2 = p_2 \equiv 1\ (3)$. Ten przypadek rozwiązuje się praktycznie tym samym sposobem, z pewną różnicą.
Niech $\gamma_1 = \overline{\pi}_1\ i\ \gamma_2 = \overline{\pi}_2$. $Wtedy\ \gamma_1\ i\ \gamma_2$ są prymarne i $p_1 = \pi_1\gamma_1\ i\ p_2 = \pi_2\gamma_2$. Zaczynając od równości $g(\chi_{\gamma_1})^3 = p_1\gamma_1$ i podnosząc ją do $(N\pi_2 - 1)/3 = (p_2 - 1)/3$ potęgi, oraz biorą kongruencję modulo π_2 otrzymujemy tą samą metodą jak powyżej równość

$$\chi_{\gamma_1}(p_2^2) = \chi_{\pi_2}(p_1\gamma_1). \tag{3}$$

Podobnie zaczynając od $g(\chi_{\pi_2})^3 = p_2\pi_2$, podnosząc do $(p_1 - 1)/3$ potęgi i biorąc kongruencję modulo π_1 otrzymamy

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2). \tag{4}$$

Potrzebujemy także równości $\chi_{\gamma_1}(p_2^2) = \chi_{\pi_1}(p_2)$, która wynika ze Stwierdzenia 2.2.3, ponieważ $\gamma_1 = \overline{\pi}_1$ *i* $\overline{p}_2 = p_2$. Możemy teraz obliczyć
$\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) = \chi_{\pi_1}(\pi_2)\chi_{\gamma_1}(p_2^2)$

z równania (3)

$= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) = \chi_{\pi_1}(p_2\pi_2)$

z powyższej uwagi

$= \chi_{\pi_2}(p_1^2) = \chi_{\pi_2}(p_1\pi_1\gamma_1)$

z równania (4)

$= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1)$.
Równając ze sobą pierwszy ostatni człon i skracając przez $\chi_{\pi_2}(p_1\gamma_1)$ dostajemy oczekiwany rezultat:

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

■

2.4. Prawo wzajemności reszt dwukwadratowych

W tej części D oznacza pierścień $\mathbb{Z}[i]$. Jeśli $\alpha \in D$, *to* $(\alpha) = \alpha D$ jest dziedziną ideałów głownych generowaną przez α. Jej jednościami są ± 1, $\pm i$.

Definicja 2.4.1. *Liczba nieodwracalna $\alpha \in D$ jest prymarna jeśli $\alpha \equiv 1(1+i)^3$.*

Zachodzą następujące twierdzenia

(a) Niech π będzie nierozkładalne w D. Pierścień klas reszt $D/\pi D$ jest skończonym ciałem z $N(\pi)$ elementami.
(b) Jeśli $\pi \nmid \alpha$, to $\alpha^{N\pi-1} \equiv 1(\pi)$.

Stwierdzenie 2.4.1.

(a) *Jeśli $\pi \nmid \alpha$, to $\chi_\pi(\alpha) = 1 \Leftrightarrow x^4 \equiv \alpha(\pi)$ ma rozwiązanie w D.*
(b) $\chi_\pi(\alpha\beta) = \chi_\pi(\alpha) * \chi_\pi(\beta)$
(c) $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$
(d) *Jeśli π jest nierozkładalny i prymarny, to $\chi_\pi(-1) = (-1)^{(a-1)/2}$, gdzie $\pi = a + bi$.*
(e) *Jeśli $\alpha \equiv \beta(\pi)$ to $\chi_\pi(\alpha) = \chi_\pi(\beta)$*
(f) $\chi_\pi(\alpha) = \chi_\lambda(\alpha)$ *jeśli* $(\pi) = (\lambda)$

Twierdzenie 2.4.1. *Niech λ i π będą względnie pierwszymi prymarnymi elementami pierwszymi w D. Wtedy*

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{((N(\lambda)-1)/4)N(\pi)-1)/4}$$

2.5. Konstruowalność wielokątów foremnych

W *Disquisitiones Arithmeticae* Gauss udowodnił za pomocą "okresów cyklotomicznych", że jeśli p jest liczbą pierwszą postaci $2^n + 1$, to wielokąt foremny o p bokach jest konstruowalny za pomocą cyrkla i linijki. W tym rozdziale pokazany zostanie dowód tego faktu za pomocą sum Gaussa i Jacobiego. W rozpatrywanej sytuacji konstruwalne liczby zespolone to te liczby, które możemy uzyskać z $\mathbb{Q}$ poprzez skończoną liczbę operacji wymiernych i tworzenie pierwiastków kwadratowych.

Definicja 2.5.1. *Liczba zespolona $\alpha \in \mathbb{C}$ jest konstruowalna jeśli istnieją podciała ciała $\mathbb{C}$, $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n$ takie, że $\alpha \in K_n$ i $K_1 = K_{i-1}(\sqrt{\alpha_{i-1}})$ dla pewnego $\alpha_i \in K_i$, $i = 1, \ldots, n$.*

Widzimy, że α jest konstruowalna wtedy i tylko wtedy, gdy część rzeczywista i urojona liczby α są konstruowalne. Co więcej, jeśli α można skonstruować, to $\sqrt{\alpha}$ też.

Lemat 2.5.1. *Niech $\zeta_t = e^{2\pi i/t}$. Wtedy ζ_{2^n}, gdzie $n = 1, 2, \ldots$ jest konstruowalne.*

Dowód. Z tego, że $(\zeta_{2^n})^2 = \zeta_{2^{n-1}}$ i faktu, że ζ_2 jest konstruowalne poprzez indukcję dostajemy lemat.

■

Lemat 2.5.2.

$$\sum_{\chi} \chi(t) = \begin{cases} 1, & \text{jeśli } t=0, \\ p-1, & \text{jeśli } t=1, \\ 0, & \text{jeśli } t \neq 0,\ 1, \end{cases}$$

suma po wszystkich charakterach z F_p^*.

Dowód. Jeśli $\chi = \varepsilon$ jest charakterem trywialnym, wtedy $\varepsilon(0) = 1$ i teza zachodzi dla $t = 0$. Teza jest też prawdziwa dla $t = 1$ na mocy Stwierdzenia 2.1.1, a pozostałe przypadki rozstrzyga wniosek do tego stwierdzenia.

■

Twierdzenie 2.5.1. *Jeśli $p = 2^n + 1$ jest liczbą pierwszą Fermata, wtedy ζ_p jest konstruowalne.*

Dowód. Niech $g(\chi) = \sum_{t=0}^{p-1} \chi(t)\zeta_p^t$ jest sumą Gaussa związaną z χ, wtedy

$$\sum_{\chi} g(\chi) = \sum_{t=0}^{p-1} \left(\sum_{\chi} \chi(t) \right) \zeta_p^t = 1 + (p-1)\zeta_p.$$

Stąd $\zeta_p = (p-1)^{-1}(-1 + \sum_{\chi} g(\chi))$ i wtedy ζ_p jest konstruowalne jeśli każda suma $g(\chi)$ też jest. Jednakże $p - 1 = 2^n$ i skoro charaktery tworzą grupą rzędu $p-1$ widzimy, że rząd χ jest 2^m dla pewnego m. Używając Stwierdzenia 2.1.3 mamy $g(\chi)^{2m} = \chi(-1)pJ(\chi,\ \chi)J(\chi,\ \chi^2)\ldots J(\chi,\ \chi^l)$, gdzie $l = 2^m - 2$. Jednakże $J(\chi,\ \chi^l) \in \mathbb{Z}[\zeta_{2^n}]$, więc z Lematu 2.5.1 $g(\chi)^{2m}$ jest konstruowalne. Wynika z tego, że $g(\chi)$ też jest konstruowalne.

■

Literatura

K. Ireland, M. Rosen *A Classical Introduction to Modern Number Theory*