

0.1 Liczba klas ciała kwadratowego

Przedstawimy dowód Twierdzenia Dirichleta o liczbie klas ciała kwadratowego. Istnieje również bardziej ogólna wersja tego twierdzenia dla ciał liczbowych.

Dirichlet udowodnił przypadek dla ciał kwadratowych w 1837 roku, używając w dowodzie form kwadratowych bardziej niż ciał kwadratowych. Potrzebował on tego wyniku dla dowodu twierdzenia o liczbach pierwszych w ciągach arytmetycznych.

Twierdzenie to pozwala na wyrażenie liczby klas ciała kwadratowego jako skończoną sumę łatwo obliczalnych składników. Dotychczas wszystkie zgrabne dowody tego wyniku używają nietrywialnej analizy.

Zdefiniujemy teraz pojęcia potrzebne do przeprowadzenia dowodu.

Potrzebne nam będą następujące uogólnienia pojęcia symbolu Legendra.

Definicja 0.1.1. Niech $n \geq 1$ będzie nieparzystą liczbą całkowitą. Niech:

$$n = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$$

będzie rozkładem n na czynniki pierwsze. Wówczas funkcję $\left(\frac{\cdot}{n}\right) : \mathbb{Z} \rightarrow \{0, \pm 1\}$ zadaną wzorem:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \dots \cdot \left(\frac{a}{p_r}\right)^{\alpha_r}$$

nazywamy symbolem Jacobiego, gdzie $\left(\frac{a}{p_i}\right)$ oznacza symbol Legendra.

Nietrudno zauważyć, że jeśli $(n, a) \neq 1$, to $\left(\frac{a}{n}\right) = 0$. Ponadto jeśli p jest liczbą pierwszą dzielącą n , wówczas:

$$\left(\frac{p^2 a}{n}\right) = \left(\frac{a}{n}\right) = \left(\frac{a}{p^2 n}\right)$$

Symbol Jacobiego $\left(\frac{a}{n}\right)$ zależy wyłącznie od $a \bmod n$. Prawo Wzajemności Reszt Kwadratowych Gaussa uogólnia się na symbol Jacobiego w następujący sposób.

Twierdzenie 0.1.1. Niech $a, n \in \mathbb{Z}_{>0}$ oraz $(a, n) = 1$. Wówczas:

$$\begin{aligned}\left(\frac{a}{n}\right) &= (-1)^{(a-1)(n-1)/4} \left(\frac{n}{a}\right) & \text{dla} \quad a, n \in 2\mathbb{Z} + 1 \\ \left(\frac{2}{n}\right) &= (-1)^{(n^2-1)/8} & \text{dla} \quad n \in 2\mathbb{Z} + 1.\end{aligned}$$

Dowód. Niech:

$$\begin{aligned}n &= p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r} \\ a &= q_1^{\beta_1} \cdot \dots \cdot q_m^{\beta_m}\end{aligned}$$

będą rozkładami n oraz a na czynniki pierwsze. Zauważmy, że dla dowolnych liczb całkowitych α, β mamy:

$$\alpha \cdot \beta \equiv \frac{(-1)^\beta - 1}{2} \cdot \frac{(-1)^\alpha - 1}{2} \pmod{2} \quad (1)$$

Możemy przyjąć, że:

$$\begin{aligned}p_1 &\equiv \dots \equiv p_k \equiv 3 \pmod{4} \\ p_{k+1} &\equiv \dots \equiv p_r \equiv 1 \pmod{4} \\ q_1 &\equiv \dots \equiv q_l \equiv 3 \pmod{4} \\ q_{l+1} &\equiv \dots \equiv q_m \equiv 1 \pmod{4}\end{aligned} \quad (2)$$

Przyjmijmy ponadto następujące oznaczenia:

$$\alpha_1 + \dots + \alpha_k = \alpha \quad \text{oraz} \quad \beta_1 + \dots + \beta_l = \beta$$

Mamy wówczas:

$$\begin{aligned}n &\equiv (-1)^\alpha \pmod{4} \\ a &\equiv (-1)^\beta \pmod{4}\end{aligned} \quad (3)$$

Na mocy (1) i (3) mamy:

$$\frac{a-1}{2} \cdot \frac{n-1}{2} \equiv \frac{(-1)^\alpha - 1}{2} \cdot \frac{(-1)^\beta - 1}{2} \equiv \alpha \cdot \beta \pmod{2} \quad (4)$$

Wówczas na mocy Prawa Wzajemności Reszt Kwadratowych Gaussa, multiplikatywności oraz (1), (2) i (4) mamy:

$$\begin{aligned}
\left(\frac{a}{n}\right) &= \prod_{b=1}^r \left(\frac{a}{p_b}\right)^{\alpha_b} = \prod_{b=1}^r \prod_{c=1}^m \left(\frac{q_c}{p_b}\right)^{\alpha_b \cdot \beta_c} = \prod_{b=1}^r \prod_{c=1}^m (-1)^{\left(\frac{q_c-1}{2} \cdot \frac{p_b-1}{2}\right) \alpha_b \cdot \beta_c} \cdot \left(\frac{p_b}{q_c}\right)^{\alpha_b \cdot \beta_c} \\
&= \prod_{b=1}^r \prod_{c=1}^m (-1)^{\left(\frac{q_c-1}{2} \cdot \frac{p_b-1}{2}\right) \alpha_b \cdot \beta_c} \cdot \prod_{b=1}^r \prod_{c=1}^m \left(\frac{p_b}{q_c}\right)^{\alpha_b \cdot \beta_c} \\
&= \prod_{b=1}^k \prod_{c=1}^l (-1)^{\left(\frac{q_c-1}{2} \cdot \frac{p_b-1}{2}\right) \alpha_b \cdot \beta_c} \cdot \prod_{c=1}^m \prod_{b=1}^r \left(\frac{p_b}{q_c}\right)^{\alpha_b \cdot \beta_c} \\
&= \prod_{b=1}^k \prod_{c=1}^l (-1) \cdot \prod_{c=1}^m \left(\frac{n}{q_c}\right)^{\beta_c} = (-1)^{\alpha \cdot \beta} \cdot \left(\frac{n}{a}\right) \\
&= (-1)^{\frac{a-1}{2} \cdot \frac{n-1}{2}} \cdot \left(\frac{n}{a}\right)
\end{aligned}$$

Dowód drugiej równości przebiega podobnie, wykorzystuje ponadto fakt, że dla symbolu Legendra mamy:

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

□

Zauważmy, że symbol Jacobiego nie przenosi własności reszt kwadratowych w taki sposób jak symbol Legendra. Oczywiście, jeśli a jest resztą kwadratową modulo n taką, że $(a, n) = 1$, to $\left(\frac{a}{n}\right) = 1$. Jednakże odwrotne twierdzenie nie zachodzi.

Przykład. Ponieważ 2 nie jest resztą kwadratową modulo 3, zatem nie jest resztą kwadratową modulo 15. Jednakże z definicji mamy:

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

Definicja 0.1.2. Niech $n \neq 0$ będzie liczbą całkowitą. Funkcję $\left(\frac{\cdot}{n}\right) : \mathbb{Z} \rightarrow \{0, \pm 1\}$ o następujących własnościach:

$$(1). \quad \left(\frac{a}{n}\right) = 0 \quad \text{dla} \quad (a, n) > 1$$

$$(2). \left(\frac{a}{-1}\right) = \begin{cases} 1 & a > 0 \\ -1 & a < 0 \end{cases}$$

$$(3). \left(\frac{a}{2}\right) = \begin{cases} 1 & a \equiv \pm 1 \pmod{8} \\ -1 & a \equiv \pm 3 \pmod{8} \end{cases}$$

$$(4). \left(\frac{ab}{cd}\right) = \left(\frac{a}{c}\right) \cdot \left(\frac{b}{c}\right) \cdot \left(\frac{a}{d}\right) \cdot \left(\frac{b}{d}\right)$$

nazywamy symbolem Kroneckera.

Definicja 0.1.3. Niech I będzie niezerowym ideałem pierścienia $\mathcal{O}_{\mathbb{K}}$, $N(I)$ oznacza normę tego ideału oraz $s \in \mathbb{C}$, wówczas:

$$\zeta_{\mathbb{K}}(s) = \sum_I N(I)^{-s}$$

nazywamy dztę Dedekinda (suma przebiega po wszystkich niezerowych idealach w $\mathcal{O}_{\mathbb{K}}$).

Twierdzenie 0.1.2. Niech $\zeta_{\mathbb{K}}$ oznacza dztę Dedekinda kwadratowego ciała liczbowego o wyznaczniku D . Niech h oznacza liczbę klas pierścienia $\mathcal{O}_{\mathbb{K}}$, w - liczbę jedności w $\mathcal{O}_{\mathbb{K}}$ oraz u - jedność podstawową w $\mathcal{O}_{\mathbb{K}}^*$. Wówczas:

$$\lim_{s \rightarrow 1} (s-1)\zeta_{\mathbb{K}}(s) = \rho_{\mathbb{K}} = \begin{cases} \frac{2h \log u}{\sqrt{D}} & \text{dla } D > 0 \\ \frac{2\pi h}{w\sqrt{|D|}} & \text{dla } D < 0 \end{cases}$$

Dowód. Dowód można znaleźć w paragrafie 11.2 w [1]. □

Definicja 0.1.4. Niech D będzie wyznacznikiem ciała kwadratowego $\mathbb{Q}(\sqrt{d})$ dla bezkwadratowej liczby całkowitej d . Wówczas funkcję $\chi : \mathbb{Z} \rightarrow \{0, \pm 1\}$ zadaną wzorem:

$$\chi(n) = \left(\frac{D}{n}\right)$$

nazywamy charakterem Dirichleta modulo $|D|$.

Twierdzenie 0.1.3 (WZÓR NA LICZBĘ KLAS). *Niech D będzie wyznacznikiem ciała kwadratowego $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. Wówczas liczba klas h pierścienia $\mathcal{O}_{\mathbb{K}}$ dana jest wzorem:*

$$h = \begin{cases} -\frac{1}{2 \cdot \log u} \sum_{a=1}^{D-1} \chi(a) \log(2 \sin(a\pi/D)) & D > 0 \\ -\frac{w}{2 \cdot |D|} \sum_{a=1}^{|D|-1} \chi(a) \cdot a & D < 0 \end{cases}$$

gdzie w oznacza liczbę pierwiastków z jedynki w $\mathbb{K}$, u jest jednością podstawową $\mathbb{K}$, a χ oznacza zdefiniowany powyżej charakter.

Następujące twierdzenie jest specjalnym przypadkiem powyższego twierdzenia pokazujący niezwykle związek pomiędzy jednościami w rzeczywistym ciele kwadratowym.

Twierdzenie 0.1.4. *Niech $q > 0$ będzie liczbą pierwszą przystającą do 1 modulo 4. Wówczas liczba:*

$$v = \prod_{a=1}^{(q-1)/2} \sin(a\pi/q)^{-\left(\frac{a}{q}\right)}$$

jest jednością w $\mathbb{Z}[(1 + \sqrt{q})/2]$, pierścieniu liczb algebraicznych w $\mathbb{Q}(\sqrt{q})$. Jedność ta jest związana z jednością podstawową następującym równaniem:

$$v = u^h$$

gdzie h oznacza liczbę klas ciała $\mathbb{Q}(\sqrt{q})$.

0.2 Dowód Twierdzenia o liczbie klas

Udowodnimy najpierw kilka ważnych lematów.

Lemat 0.2.1. *Niech N, a będą liczbami rzeczywistymi takimi, że $N > 1$ oraz $1 \leq a < N$. Wówczas:*

$$-\log\left(1 - e^{2\pi ai/N}\right) = -\log\left(2 \sin \frac{\pi a}{N}\right) + \frac{\pi i}{2} \left(1 - \frac{2a}{N}\right)$$

Dowód. Będziemy korzystać z następujących wzorów:

$$\begin{aligned}
\cos \alpha &= \cos(-\alpha), \quad \sin(-\alpha) = -\sin \alpha, \quad \cos 2\alpha = 1 - 2\sin^2 \alpha, \\
\sin 2\alpha &= 2\sin \alpha \cdot \cos \alpha, \quad \sin(\alpha + \beta) = \sin \alpha \cdot \cos \beta + \cos \alpha \cdot \sin \beta, \\
\cos(\alpha + \beta) &= \cos \alpha \cdot \cos \beta - \sin \alpha \cdot \sin \beta, \quad \cos\left(\frac{\pi}{2}\right) = 0, \quad \sin\left(\frac{\pi}{2}\right) = 1, \\
e^{i\theta} &= \cos \theta + i \sin \theta.
\end{aligned}$$

Przekształćmy wyrażenie:

$$\begin{aligned}
e^{(-2\pi ia)/N} - 1 &= \cos\left(-\frac{2\pi a}{N}\right) + i \sin\left(-\frac{2\pi a}{N}\right) - 1 = \cos\left(\frac{2\pi a}{N}\right) - i \sin\left(\frac{2\pi a}{N}\right) - 1 \\
&= 1 - 2\sin^2\left(\frac{\pi a}{N}\right) - i \sin\left(\frac{2\pi a}{N}\right) - 1 = -2\sin^2\left(\frac{\pi a}{N}\right) - i \sin\left(\frac{2\pi a}{N}\right) \\
&= -2\sin^2\left(\frac{\pi a}{N}\right) - 2i \sin\left(\frac{\pi a}{N}\right) \cdot \cos\left(\frac{\pi a}{N}\right) \\
&= 2\sin\left(\frac{\pi a}{N}\right) \cdot \cos\left(\frac{\pi}{2}\right) \cdot \cos\left(\frac{\pi a}{N}\right) - 2\sin\left(\frac{\pi a}{N}\right) \cdot \sin\left(\frac{\pi}{2}\right) \cdot \sin\left(\frac{\pi a}{N}\right) \\
&\quad - 2i \sin\left(\frac{\pi a}{N}\right) \cdot \sin\left(\frac{\pi}{2}\right) \cdot \cos\left(\frac{\pi a}{N}\right) - 2i \sin\left(\frac{\pi a}{N}\right) \cdot \cos\left(\frac{\pi}{2}\right) \cdot \sin\left(\frac{\pi a}{N}\right) \\
&= 2\sin\left(\frac{\pi a}{N}\right) \cdot \left(\cos\left(\frac{\pi}{2} + \frac{\pi a}{N}\right) - i \sin\left(\frac{\pi}{2} + \frac{\pi a}{N}\right)\right) \\
&= 2\sin\left(\frac{\pi a}{N}\right) \cdot e^{-i\left(\frac{\pi}{2} + \frac{\pi a}{N}\right)}
\end{aligned}$$

Mnożąc stronami przez $e^{(2\pi ia)/N}$ dostajemy:

$$1 - e^{(2\pi ia)/N} = 2\sin\left(\frac{\pi a}{N}\right) \cdot e^{-i\left(\frac{\pi}{2} + \frac{\pi a}{N}\right)} \cdot e^{(2\pi ia)/N} = 2\sin\left(\frac{\pi a}{N}\right) \cdot e^{i\left(\frac{\pi a}{N} - \frac{\pi}{2}\right)}$$

Logarytmując stronami i mnożąc przez (-1) dostajemy tezę. $\square$

Lemat 0.2.2. Niech χ oznacza zdefiniowany powyżej charakter i $\zeta = e^{2\pi i/|D|}$ oraz:

$$G = \sum_{a=1}^{|D|-1} \chi(a) \zeta^a \quad (5)$$

Wówczas:

$$G^2 = D \quad (6)$$

Ponadto dla każdego n :

$$\chi(n) = \frac{1}{G} \sum_{a=1}^{|D|-1} \chi(a) \zeta^{an} \quad (7)$$

Dowód. Zauważmy, że iloczyn G^2 można zapisać w następujący sposób:

$$G^2 = \sum_{\substack{a=1 \\ (a,|D|)=1}}^{|D|-1} \chi(a) \zeta^a \sum_{\substack{r=1 \\ (r,|D|)=1}}^{|D|-1} \chi(ar) \zeta^{ar} = \sum_{\substack{a=1 \\ (a,|D|)=1}}^{|D|-1} \sum_{\substack{r=1 \\ (r,|D|)=1}}^{|D|-1} \chi(r) \zeta^{a(r+1)} \quad (8)$$

Zauważmy ponadto, że:

$$0 = \sum_{\substack{a=1 \\ (a,|D|)=1}}^{|D|-1} \sum_{\substack{r=1 \\ (r,|D|)>1}}^{|D|-1} \chi(r) \zeta^{a(r+1)} \quad (9)$$

oraz:

$$0 = \sum_{\substack{a=1 \\ (a,|D|)>1}}^{|D|-1} \sum_{r=1}^{|D|-1} \chi(r) \zeta^{a(r+1)} \quad (10)$$

Ponadto:

$$0 = \sum_{r=1}^{|D|-1} \left(\frac{r}{D} \right) \zeta^{0(1-r)} \quad (11)$$

Na mocy (9), (10) i (11) z (8) dostajemy:

$$\begin{aligned} G^2 &= \sum_{a=1}^{|D|-1} \sum_{r=1}^{|D|-1} \chi(r) \zeta^{a(r+1)} = \sum_{a=1}^{|D|-1} \sum_{r=1}^{|D|-1} \chi(-r) \zeta^{a(1-r)} \\ &= \left(\frac{-1}{D} \right) \sum_{a=1}^{|D|-1} \sum_{r=1}^{|D|-1} \left(\frac{r}{D} \right) \zeta^{a(1-r)} = \left(\frac{-1}{D} \right) \sum_{a=0}^{|D|-1} \sum_{r=1}^{|D|-1} \left(\frac{r}{D} \right) \zeta^{a(1-r)} \quad (12) \\ &= \left(\frac{-1}{D} \right) \sum_{r=1}^{|D|-1} \left(\frac{r}{D} \right) \sum_{a=0}^{|D|-1} \zeta^{a(1-r)} \end{aligned}$$

Z kryterium Eulera składnik z $r = 1$ wynosi:

$$\left(\frac{-1}{D} \right) |D| = (-1)^{(|D|-1)/2} |D| \quad (13)$$

Twierdzimy, że pozostałe składniki w równaniu (12) są zerami. Niech $r \neq 1$ oraz $\eta = \zeta^{1-r}$. Wówczas η jest nietrywialnym pierwiastkiem stopnia $|D|$ z jedynki. Pokażemy, że:

$$S = 1 + \eta + \dots + \eta^{|D|-1} = 0 \quad (14)$$

Zauważmy, że:

$$\eta \cdot S = \eta + \eta^2 \dots + \eta^{|D|-1} + \eta^{|D|} = \eta + \eta^2 \dots + \eta^{|D|-1} + 1 = S$$

Ponieważ $\eta \neq 1$, zatem $S = 0$. Wstawiając (13), (14) do (12) dostajemy:

$$G^2 = D$$

Dla $(n, D) = 1$ mamy:

$$\sum_{a=1}^{|D|-1} \chi(a) \zeta^{an} = \sum_{a=1}^{|D|-1} \chi(an^2) \zeta^{an} = \chi(n) \sum_{a=1}^{|D|-1} \chi(an) \zeta^{an} = \chi(n) G \quad (15)$$

Dzieląc stronami (15) przez G , dostajemy (7) - przypadek dla $(n, D) > 1$ jest trywialny. $\square$

Uwaga. Zauważmy, że G jest elementem ciała kwadratowego - to czy jest to element rzeczywisty zależy od znaku D . Jeśli $D > 0$, to wówczas z (7) wynika, że G jest rzeczywiste, w tym przypadku $G = \pm\sqrt{D}$ z równania (6). Jeśli $D < 0$ to z równania (6) wynika, że $G = \pm i\sqrt{|D|}$. Przeprowadzimy teraz dowód Wzoru Na Liczbę Klas z dokładnością do znaku.

Dowód. (TWIERDZENIA 0.1.2.) Zaczniemy od formalnych przekształceń $L(\chi, 1)$ dowodząc zbieżności później. Z definicji:

$$L(\chi, 1) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}$$

Korzystając z (7) i przedstawiając wyrazy sumy mamy:

$$L(\chi, 1) = \frac{1}{G} \sum_{a=1}^{|D|-1} \chi(a) \sum_{n=1}^{\infty} \frac{1}{n} e^{2\pi i a n / |D|} \quad (16)$$

Wewnętrzna suma jest równa $-\log(1 - e^{2\pi i a / |D|})$ więc stosując Lemat 0.2.1. z $N = |D|$ otrzymujemy:

$$L(\chi, 1) = -\frac{1}{G} \sum_{a=1}^{|D|-1} \chi(a) \left[\log \left(2 \sin \frac{\pi a}{|D|} \right) - \frac{\pi i}{2} \left(1 - \frac{2a}{|D|} \right) \right]. \quad (17)$$

W tym momencie trzeba rozpatrzyć dwa przypadki, w zależności od znaku D . Jeśli $D > 0$ to G jest rzeczywiste, a ponieważ wiemy, że $L(\chi, 1)$ jest rzeczywiste, więc urojona część równania (17) musi zniknąć. Mamy więc:

$$L(\chi, 1) = -\frac{1}{G} \sum_{a=1}^{|D|-1} \chi(a) \log \left(2 \sin \frac{\pi a}{|D|} \right) \quad (18)$$

Na mocy Twierdzenia [] powyższe wyrażenie jest równe $2h \log u / \sqrt{|D|}$. Ponieważ $G = \pm \sqrt{|D|}$, otrzymujemy:

$$h = \mp \frac{1}{2 \cdot \log u} \sum_{a=1}^{D-1} \chi(a) \log(2 \sin(a\pi/D))$$

Pierwszy przypadek jest udowodniony z dokładnością do znaku.

Jeśli $D < 0$, to suma Gaussa G jest czysto urojona, zatem z równania (17) otrzymujemy:

$$L(\chi, 1) = -\frac{\pi i}{G|D|} \sum_{a=1}^{|D|-1} \chi(a) a \quad (19)$$

Z Twierdzenia [] powyższe wyrażenie jest równe $\frac{2\pi h}{w\sqrt{|D|}}$, ponadto $G = \pm i\sqrt{|D|}$, zatem:

$$h = \mp \frac{w}{2 \cdot |D|} \sum_{a=1}^{|D|-1} \chi(a) \cdot a \quad (20)$$

Drugi przypadek jest udowodniony z dokładnością do znaku.

Równanie (16) może być uzyskane za pomocą Wzoru Sumacyjnego Abela, jedyne czego w tym przypadku potrzebujemy to jednostajna ograniczoność $\sum_{a \leq x} \chi(a)$. $\square$

Uwaga. Dowód poprawności wyboru znaku w powyższym Twierdzeniu można znaleźć w paragrafie 11.4 w książce [1].

Bibliografia

- [1] Graham Everest, Thomas Ward *An Introduction to Number Theory*. Springer, London, 2005.