Teoria liczb
rozszerzenia całkowite $\mathbb{Z}$, 3-13 kwietnia

Zadanie 1. Ustalmy liczbę całkowitą $d \neq 0, 1$ bezkwadratową i niech $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ oznacza zbiór wszystkich elementów $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$, które są całkowite nad $\mathbb{Z}$.

(a) Pokaż, że $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

(b) Pokaż, że każdy element $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ spełnia równanie postaci $x^2 - ax + b = 0$, gdzie $a, b \in \mathbb{Z}$. Wywnioskuj, że jest on postaci $(a_1 + a_2\sqrt{d})/2$, gdzie $a_1, a_2 \in \mathbb{Z}$.

(c) Opisz $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. *Odpowiedź będzie zależała od reszty d z dzielenia przez 4.*

Rozwiązanie.
(a) Dla dowolnych $n_1, n_2 \in \mathbb{Z}$, element $n_1 + n_2\sqrt{d}$ jest pierwiastkiem wielomianu unormowanego $P(x) = (x - n_1)^2 - n_2^2 d \in \mathbb{Z}[x]$. To pokazuje, że $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.
(b) Przypomnijmy z algebry I, że każdy element $\mathbb{Q}(\sqrt{d})$ jest postaci $n_1 + n_2\sqrt{d}$, gdzie $n_1, n_2 \in \mathbb{Q}$. Weźmy element $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \subseteq \mathbb{Q}(\sqrt{d})$. Jeśli $\alpha \in \mathbb{Q}$, tzn. jeśli $n_2 = 0$, to z zadania 5 poprzedniej serii mamy $\alpha \in \mathbb{Z}$ i element ten jest pierwiastkiem wielomianu unormowanego $(x - \alpha)^2$.

Załóżmy zatem, że $\alpha \notin \mathbb{Q}$. Oznaczmy przez $f \in \mathbb{Z}[x]$ wielomian, którego pierwiastkiem jest α, taki wielomian istnieje z założenia, że α jest całkowity nad $\mathbb{Z}$. Wielomian $g(x) := (x - n_1)^2 - n_2^2 d \in \mathbb{Q}[x]$ jest minimalny dla α w sensie Algebry I, bowiem α nie jest pierwiastkiem wielomianu stopnia jeden o współczynnikach w $\mathbb{Q}$, bo α nie leży w $\mathbb{Q}$. Z minimalności, wielomian g dzieli f w $\mathbb{Q}[x]$, czyli istnieje $h \in \mathbb{Q}[x]$ taki, że $f = gh$. Wielomiany f i g są unormowane, więc i h jest unormowany. Wobec tego możemy zastosować zadanie 4 z poprzedniej serii (które fachowo nazywa się „lematem Gaussa"). Otrzymujemy, że g ma współczynniki całkowite! Wypiszmy te współczynniki wprost:

$$g(x) = x^2 - 2n_1 x + (n_1^2 - n_2^2 d).$$

Dowiadujemy się, że liczby $2n_1$ oraz $n_1^2 - n_2^2 d$ są całkowite. Zatem również $4(n_1^2 - n_2^2 d) - (2n_1)^2 = (2n_2)^2 d$ jest całkowita. Chcemy pokazać, że $2n_2$ jest całkowita. Zapiszmy $n_2 = p/q$, gdzie $p, q \in \mathbb{Z}$ są względnie pierwsze. Wtedy $(2n_2)^2 d = \frac{4p^2 d}{q^2}$, czyli q^2 dzieli $4d$. Ale liczba d jest bezkwadratowa, więc wynika stąd, że q^2 dzieli 4, czyli q dzieli 2, zatem $2n_2 = 2p/q$ jest całkowita.
(c) W punkcie (b) pokazaliśmy, że $n_1 + n_2\sqrt{d}$ jest całkowita wtedy i tylko wtedy, gdy współczynniki g są całkowite, czyli gdy $2n_1$ oraz $n_1^2 - n_2^2 d$ są całkowite. Pozostaje sprawdzić, kiedy to zachodzi. Wiemy już, że jeśli $n_1 + n_2\sqrt{d}$ jest całkowita, to $a_1 := 2n_1$, $a_2 := 2n_2$ są liczbami całkowitymi.[1] Mamy $n_1^2 - n_2^2 d = \frac{1}{4}(a_1^2 - a_2^2 d)$, co jest liczbą całkowitą wtedy i tylko wtedy, gdy $a_1^2 \equiv a_2^2 d \pmod 4$.

Rozważmy dwa/trzy przypadki:

- $d \equiv 0 \pmod 4$. Ten przypadek nie może zachodzić, bo d jest bezkwadratowa.
- $d \equiv 2, 3 \pmod 4$. W tym przypadku d nie jest resztą kwadratową modulo 4. Zatem równanie $a_1^2 \equiv a_2^2 d \pmod 4$ nie ma rozwiązań w $\mathbb{Z}_4^*$. Wynika stąd, że a_1, a_2 są parzyste, czyli n_1, n_2 są całkowite. W tym przypadku

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}].$$

[1] Podkreślam tutaj, że n_1, n_2 niekoniecznie są całkowite.

- $d \equiv 1 \pmod 4$. Liczba d jest nieparzysta, zatem kongruencja $n_1^2 \equiv n_2^2 d \pmod 4$ implikuje, że n_1, n_2 są obie parzyste lub obie nieparzyste. Ale też w drugą stronę, jeśli założymy, że n_1, n_2 są obie nieparzyste (lub obie parzyste), to spełniają one tę kongruencję. To daje odpowiedź. Można tę odpowiedź zapisać ładniej, mianowicie

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]. \tag{1.1}$$

Powyższa równość znaczy, że $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{\frac{a_1+a_2\sqrt{d}}{2} \mid a_1 \equiv a_2 \pmod 2\right\}$. By jej dowieść, obliczmy, że $\left(\frac{1+\sqrt{d}}{2}\right)^2 = \frac{1+\sqrt{d}}{2} - \frac{d-1}{4}$, więc każdy element pierścienia $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ zapisuje się jako $m_1 + m_2\frac{1+\sqrt{d}}{2}$, gdzie $m_1, m_2 \in \mathbb{Z}$ i faktycznie ma żądaną postać. Udowodniliśmy zawieranie $\subseteq$ w (1.1). Z drugiej strony, dla danego elementu $\frac{a_1+a_2\sqrt{d}}{2}$, gdzie $a_2 \equiv a_1 \pmod 2$, możemy zapisać

$$\frac{a_1+a_2\sqrt{d}}{2} = a_2 \cdot \frac{1+\sqrt{d}}{2} + \frac{a_1-a_2}{2},$$

co jest elementem $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. To daje zawieranie $\supseteq$ w (1.1) i kończy dowód.

Zadanie 2 (Pierścień Eisensteina)**.** Niech $d = -3$ i rozważmy pierścień $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\omega_3]$, gdzie $\omega_3 = \cos(2\pi/3) + i\sin(2\pi/3) = \frac{-1+i\sqrt{3}}{2}$. Możesz założyć, że pierścień ten jest dziedziną z jednoznacznością rozkładu.

(a) Oblicz kwadrat normy zespolonej elementu $a + b\omega_3$, gdzie $a, b \in \mathbb{Z}$.

(b) Niech $\mathfrak{p} \subseteq \mathbb{Z}[\omega_3]$ będzie ideałem maksymalnym. Pokaż, że $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ dla pewnej liczby pierwszej p. Wywnioskuj, że jeśli α jest generatorem $\mathfrak{p}$, to $|\alpha|^2 = p$ lub $|\alpha|^2 = p^2$.

(c) Pokaż, że jeśli $p \equiv 2 \pmod 3$, to w sytuacji powyżej $\mathfrak{p}$ jest generowany przez p. *Wskazówka: kongruencje w $\mathbb{Z}$.*

(d) Załóżmy, że $p \equiv 1 \pmod 3$. Pokaż, że istnieje liczba n taka, że $n \not\equiv 1 \pmod p$ oraz $n^3 \equiv 1 \pmod p$. Wywnioskuj, że w $\mathbb{Z}[\omega_3]$ mamy $(n-1)(n-\omega_3)(n-\omega_3^2) \in p\mathbb{Z}[\omega_3]$. Wywnioskuj, że p nie jest elementem pierwszym, a zatem w sytuacji powyżej mamy $|\alpha|^2 = p$. Wreszcie, wyciągnij wniosek, że $p = a^2 + ab + b^2$ dla pewnych całkowitych a, b.

Rozwiązanie.
(a) Skoro ω_3 jest pierwiastkiem trzeciego stopnia z jedynki, to $\omega_3^3 = 1$. Stąd wynika, że $\overline{\omega_3} = \omega_3^2$. Ponadto mamy $0 = \omega_3^3 - 1 = (\omega_3^2 + \omega_3 + 1)$, więc $\omega_3^2 + \omega_3 + 1 = 0$. Obliczamy kwadrat normy elementu:

$$|a + b\omega_3|^2 = (a + b\omega_3) \cdot \overline{(a + b\omega_3)} = (a + b\omega_3)(a + b\omega_3^2) = a^2 + ab(\omega_3 + \omega_3^2) + b^2\omega_3^2 = a^2 - ab + b^2.$$

Na potrzeby następnych podpunktów zauważmy, że jeśli element $\alpha \in \mathbb{Z}[\omega_3]$ ma kwadrat normy równy 1, to α jest odwracalny: faktycznie $\alpha \cdot \overline{\alpha} = 1$ oraz $\overline{\alpha} \in \mathbb{Z}[\omega_3]$.
(b) Skoro $\mathfrak{p}$ jest maksymalny, to $\mathfrak{p} \neq 0$. Niech $0 \neq \alpha \in \mathfrak{p}$. Wtedy $0 \neq \alpha\overline{\alpha} \in \mathfrak{p}$ a ponadto $\alpha\overline{\alpha} = |\alpha|^2 \in \mathbb{Z}$, więc wnioskujemy, że $\mathfrak{p} \cap \mathbb{Z} \neq 0$. Z klasyfikacji ideałów w $\mathbb{Z}$ wynika, że $\mathfrak{p} \cap \mathbb{Z} = n\mathbb{Z}$ dla pewnego $n \neq 0$.

Zauważmy, jeśli $n_1, n_2 \in \mathbb{Z}$ są takie, że $n_1 n_2 \in n\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ to z pierwszości ideału $\mathfrak{p}$ wynika, że $n_1 \in \mathfrak{p}$ lub $n_2 \in \mathfrak{p}$, zatem $n_1 \in n\mathbb{Z}$ lub $n_2 \in n\mathbb{Z}$. To implikuje, że liczba n jest pierwsza. Możemy więc wziąć $p = n$.[2] Niech $\alpha \in \mathbb{Z}[\omega_3]$ będzie generatorem ideału $\mathfrak{p}$. Skoro $p \in \mathfrak{p} \cap \mathbb{Z}$, to $p = \alpha \cdot \beta$ dla pewnego $\beta \in \mathbb{Z}[\omega_3]$. Stąd

$$p^2 = |p|^2 = |\alpha|^2 \cdot |\beta|^2,$$

zatem $|\alpha|^2$ jest dodatnim dzielnikiem p^2. Element α nie jest odwracalny, więc na mocy uwagi w (a) stwierdzamy, że $|\alpha|^2$ nie jest równy jeden. Stąd wynika, że $|\alpha|^2 \in \{p, p^2\}$.
(c) Zapiszmy $\alpha = a + b\omega_3$. Wtedy $|\alpha|^2 = a^2 - ab + b^2 = (a+b)^2 - 3ab$. Zatem $|\alpha|^2 \equiv 1 \pmod 3$ lub $|\alpha|^2 \equiv 0 \pmod 3$. W szczególności, mamy $|\alpha|^2 \neq p$, zatem $|\alpha|^2 = p^2$. W równaniu z poprzedniego podpunktu mamy $|\beta|^2 = 1$, stąd z uwagi w punkcie (a) element β jest odwracalny w $\mathbb{Z}[\omega_3]$ a to znaczy, że ideały generowane przez α oraz $p = \alpha\beta$ pokrywają się.
(d) Grupa $\mathbb{Z}_p^*$ jest cykliczna i ma $p-1$ elementów, więc istnieje element n taki, że $n \not\equiv 1 \pmod p$ oraz $n^3 \equiv 1 \pmod p$. (By znaleźć taki element można wybrać generator g i wziąć $n = g^{\frac{p-1}{3}}$.) Zachodzi

$$(n-1)(n-\omega_3)(n-\omega_3^2) = n^3 - 1 \in p\mathbb{Z} \subseteq p\mathbb{Z}[\omega_3]. \tag{1.2}$$

Ponadto $p\mathbb{Z}[\omega_3] = \{a + b\omega_3 \mid a, b \in p\mathbb{Z}\}$. Skoro $n \not\equiv 1 \pmod 3$, to $n - 1 \notin p\mathbb{Z}[\omega_3]$. Ponadto $-1 \notin p\mathbb{Z}$, więc $n - \omega_3 \notin p\mathbb{Z}[\omega_3]$. Wreszcie, mamy $n - \omega_3^2 = (n+1) + \omega_3$ i ten element nie leży w $p\mathbb{Z}[\omega_3]$ bo $1 \notin p\mathbb{Z}$. Żaden ze składników iloczynu po lewej stronie (1.2) nie leży w $p\mathbb{Z}[\omega_3]$, więc ideał $p\mathbb{Z}[\omega_3]$ nie jest pierwszy. W szczególności, nie może zachodzi $p\mathbb{Z}[\omega_3] = \mathfrak{p}$, więc argumentując jak w końcowej części podpunktu (c), widzimy, że nie może zachodzić $|\alpha|^2 = p^2$. Zachodzi więc $|\alpha|^2 = p$, czyli $a^2 - ab + b^2 = p$ i stąd $(-a)^2 + (-a)b + b^2 = p$.

Zadanie 3. Niech $p \in \mathbb{P}$. Niech $\omega_p := \exp(2\pi i/p) = \cos(2\pi/p) + i\sin(2\pi/p) \in \mathbb{C}$ będzie pierwiastkiem z jedynki stopnia p. Niech $F(x) := x^{p-1} + \ldots + x + 1 \in \mathbb{Z}[x]$ będzie wielomianem.

(a) Pokaż, że $F(\omega_p) = 0$ oraz $F(1) = p$. Załóżmy, że F jest rozkładalny na wielomiany $G, H \in \mathbb{Q}[x]$. Pokaż, że po ewentualnym domnożeniu przez stałą można założyć, że G, H mają współczynniki całkowite. Pokaż, że można dodatkowo założyć, że $G(1) = 1$.

(b) Pokaż, że $F \equiv (x-1)^{p-1} \pmod p$. Wywnioskuj, że $G \equiv (x-1)^s \pmod p$ dla pewnego s. Z równości $G(1) = 1$ wywnioskuj, że $s = 0$, zatem $G = 1$. To pokazuje, że F jest nierozkładalny, więc jest wielomianem minimalnym ω_p.

(c) Pokaż, że jeśli nie założymy, że p jest pierwsza, to może się zdarzyć, że F jest rozkładalny.

(d) Oblicz $\sum_{i=0}^{p-1} \omega_p^{ai}$ w zależności od liczby całkowitej a.

Rozwiązanie.
(a) Mamy $F(x) = \frac{x^p-1}{x-1}$, zatem $F(\omega_p) = \frac{\omega_p^p - 1}{\omega_p - 1} = \frac{1-1}{\omega_p - 1} = 0$. Równość $F(1) = p$ wynika wprost z podstawienia jedynki do wyjściowego wielomianu. Załóżmy, że $F = G \cdot H$, gdzie $G, H \in \mathbb{Q}[x]$. Przeskalujmy G, H tak, by G był unormowany. Skoro F i G są unormowane, to H również. Z lematu Gaussa (zadanie 4, poprzednia seria) wynika, że $G, H \in \mathbb{Z}[x]$. W szczególności, mamy równość liczb całkowitych $G(1) \cdot H(1) = F(1) = p$. Zatem któraś z liczb $G(1), H(1)$ jest równa ± 1. Załóżmy, że $G(1) = \pm 1$. Domnażając G i H przez -1 otrzymujemy $G(1) = 1$. (Potencjalnie

[2] Argument tutaj jest całkowicie formalny i automatycznie uogólnia się do stwierdzenia „jeśli $\mathfrak{p}$ w jakimś pierścieniu R jest pierwszy, zaś $S \subseteq R$ jest podpierścieniem, to $\mathfrak{p} \cap S$ także jest pierwszy.

domnożenie mogło zniszczyć unormowanie wielomianów, ale nie obchodzi to nas.)
(b) Wielomian $x-1$ jest niezerowy modulo p oraz $x^p-1 \equiv (x-1)^p \pmod p$, więc mamy

$$F(x) = \frac{x^p-1}{x-1} \equiv \frac{(x-1)^p}{x-1} = (x-1)^{p-1} \pmod p.$$

Z jednoznaczności rozkładu wielomianów (która zachodzi modulo p, bo $\mathbb{Z}_p$ jest ciałem) wynika, że $G \equiv (x-1)^s \pmod p$ dla pewnego s. Ewaluując obie strony w $x=1$ otrzymujemy dla $s>0$ równość $G(1) = 1 \equiv 0 \pmod p$. Zatem $s=0$, czyli $G=1$ jako wielomiany. W szczególności, F nie posiada rozkładu na wielomiany nieodwracalne, zatem F jest nierozkładalny. To pokazuje, że jest on wielomianem minimalnym dla ω_p.
(c) Jeśli $p=ab$ dla $a,b>1$ to

$$F(x) = \frac{x^p-1}{x-1} = \frac{(x^a)^b-1}{x-1} = \left(x^{a-1}+x^{a-2}+\ldots+1\right)\cdot\left(x^{a(b-1)}+x^{a(b-2)}+\ldots+1\right),$$

więc F jest rozkładalny.
(d) Mamy $\sum_{i=0}^{p-1} \omega_p^{ai} = F(\omega_p^a)$. Jeśli $a \equiv 0 \pmod p$, to ω_p^a i $F(\omega_p^a) = p$. W przeciwnym przypadku obliczamy jak w (a), że $F(\omega_p^a) = 0$.

Zadanie 4. Niech $p \in \mathbb{P}$ będzie liczbą nieparzystą. Niech $\omega_p := \exp(2\pi i/p) = \cos(2\pi/p) + i\sin(2\pi/p) \in \mathbb{C}$ będzie pierwiastkiem z jedynki stopnia p.

(a) Pokaż, że jeśli $p=3$ to $\omega_p - \omega_p^2 = \sqrt{-3}$.

(b) Dla liczby całkowitej a, zdefiniujmy *sumę Gaussa* $g_a := \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \omega_p^{at}$. Pokaż, że $g_a = \left(\frac{a}{p}\right) g_1$.

(c) Używając (b), pokaż, że suma $\sum_{a=0}^{p-1} g_a g_{-a}$ jest równa $(-1)^{\frac{p-1}{2}}(p-1)g_1^2$.

(d) Oblicz bezpośrednio, że $\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{a=0}^{p-1}\sum_{x,y} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\omega_p^{a(x-y)}$. Pokaż, że to wyrażenie wynosi $p(p-1)$ i wywnioskuj, że $g_1^2 = (-1)^{\frac{p-1}{2}}p$. To pokazuje, że zawsze mamy $\sqrt{(-1)^{\frac{p-1}{2}}p} = \pm g_1 \in \mathbb{Z}[\omega_p]$!

Rozwiązanie.
Przypomnienie: $\left(\frac{a}{p}\right)$ oznacza symbol Legendre'a. W rozwiązaniu wielokrotnie korzystamy z jego multiplikatywności.
(a) Mamy $\omega_p - \omega_p^2 = \frac{-1+i\sqrt{3}}{2} - \frac{-1-i\sqrt{3}}{2} = i\sqrt{3} = \sqrt{-3}$. (Porównaj z podpunktem (d).)
(b) Jeśli $a \equiv 0 \pmod p$, to $g_a = \sum_{t=1}^{p-1}\left(\frac{t}{p}\right) = 0$, bo jest tyle samo elementów, które są resztami kwadratowymi i nie są resztami kwadratowymi w $\mathbb{Z}_p^*$. W tym przypadku również $\left(\frac{a}{p}\right) = 0$, więc $g_a = 0 = \left(\frac{a}{p}\right) g_1$.

Załóżmy, że $a \not\equiv 0 \pmod p$. Wtedy

$$g_a\left(\frac{a}{p}\right) = \sum_{t=1}^{p-1}\left(\frac{t}{p}\right)\left(\frac{a}{p}\right)\omega_p^{at} = \sum_{t=1}^{p-1}\left(\frac{at}{p}\right)\omega_p^{at} = \sum_{u=1}^{p-1}\left(\frac{u}{p}\right)\omega_p^{u} = g_1,$$

gdzie wykorzystaliśmy fakt, że $\{a, 2a, \ldots, (p-1)a\}$ jest modulo p tym samym zbiorem co zbiór $\{1,2,\ldots,p-1\}$. Obliczamy teraz, że $g_a = g_a\left(\frac{a}{p}\right)^2 = g_1\left(\frac{a}{p}\right)$, gdzie $\left(\frac{a}{p}\right)^2 = 1$ wynika z tego, że $\left(\frac{a}{p}\right) \in \{-1,1\}$.

(c) Przypomnijmy z podpunktu (a), że $g_0 = 0$. Obliczamy, że

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{a=1}^{p-1} g_a g_{-a} = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) g_1 \left(\frac{-a}{p}\right) g_1 = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)^2 \left(\frac{-1}{p}\right) g_1^2 = \sum_{a=1}^{p-1} (-1)^{\frac{p-1}{2}} g_1^2 = (-1)^{\frac{p-1}{2}} (p-1) g_1^2.$$

(d) Obliczamy, że

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{a=0}^{p-1} \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \omega_p^{a(x-y)} = \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \left(\sum_{a=0}^{p-1} \omega_p^{a(x-y)} \right).$$

Korzystając z poprzedniego zadania, stwierdzamy, że $\sum_{a=0}^{p-1} \omega_p^{a(x-y)}$ jest równa 0, o ile $x-y$ nie jest podzielna przez p oraz jest równa p gdy $x-y$ jest podzielna przez p. Zatem mamy

$$\sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \left(\sum_{a=0}^{p-1} \omega_p^{a(x-y)} \right) = \sum_{x=1}^{p-1} \sum_{y=x} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) p = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right)^2 p = (p-1)p.$$

Porównując wyrażenia $(-1)^{\frac{p-1}{2}}(p-1)g_1^2$ i $(p-1)p$, otrzymujemy $g_1^2 = (-1)^{\frac{p-1}{2}} p$.
Komentarz: istnienie pierwiastka z $(-1)^{\frac{p-1}{2}} p$ w $\mathbb{Z}[\omega_p]$ jest wbrew pozorom jednym z fundamentalnych wyników dla różnorakich obliczeń sum; patrz przykładowo rozdział 6 w Ireland-Rosen.