Teoria liczb
równania Diofantyczne, 4-8 maja

Zadanie 1. Niech $d > 1$ będzie bezkwadratową dodatnią liczbą całkowitą taką, że $d \not\equiv 3 \pmod 4$. Celem tego zadania jest rozwiązanie równania $y^2 = x^3 - d$ przy pewnych dodatkowych założeniach.

(a) Załóżmy, że $(x, y) \in \mathbb{Z}^2$ jest rozwiązaniem. Pokaż, że x jest liczbą nieparzystą i względnie pierwszą z d.

(b) Pokaż, że $y - \sqrt{-d}$ oraz $y + \sqrt{-d}$ nie mają nietrywialnych wspólnych dzielników w $\mathbb{Z}[\sqrt{-d}]$.

(c) Załóżmy, że $\mathbb{Z}[\sqrt{-d}]$ jest dziedziną z jednoznacznością rozkładu. Z równania $x^3 = y^2+d$ wywnioskuj, że $y + \sqrt{-d} = \pm(a + b\sqrt{-d})^3$ dla pewnych $a, b \in \mathbb{Z}$. Oblicz, że $b = \pm 1$, $d = 3a^2 \pm 1$ oraz $x = a^2 + d$, $y = -8a^3 \pm 3a$.

(d) Powtórz rozumowanie z poprzedniego podpunktu, zakładając jedynie, że grupa klas $\mathbb{Z}[\sqrt{-d}]$ jest skończona i ma rząd niepodzielny przez 3.

Rozwiązanie.
(a) Jeśli liczba pierwsza p dzieli x oraz d, to p dzieli $x^3 - d = y^2$, więc p dzieli y. Wtedy p^2 dzieli x^3 oraz y^2, więc p^2 dzieli $x^3 - y^2 = d$. To przeczy założeniu, że d jest bezkwadratowa. Zatem x oraz d są względnie pierwsze.

Jeśli x jest parzysta, to $x^3 \equiv 0 \pmod 4$. Z założenia mamy $-d \not\equiv 1 \pmod 4$. Zatem $y^2 = x^3 - d \not\equiv 1 \pmod 4$. Ale gdyby y było nieparzyste, to $y^2 \equiv 1 \pmod 4$. Zatem y jest parzysta. Ale wtedy 4 dzieli y^2 i x^3, więc 4 dzieli $x^3 - y^2 = d$. To ponownie przeczy bezkwadrowości liczby d.
(b) Ze względu na podpunkt (d), przeprowadzimy rozumowanie w języku ideałów. Załóżmy, że nietrywialny (tzn. nieodwracalny) wspólny dzielnik istnieje. Implikuje to, że elementy $y - \sqrt{-d}$, $y + \sqrt{-d}$ leżą w pewnym ideale maksymalnym $\mathfrak{m} \subsetneq \mathbb{Z}[\sqrt{-d}]$. Wtedy również element $x^3 = (y - \sqrt{-d})(y + \sqrt{-d})$ należy do $\mathfrak{m}$. Ponadto element

$$2\sqrt{-d} = (y + \sqrt{-d}) - (y - \sqrt{-d})$$

należy do $\mathfrak{m}$, więc również $2d = 2\sqrt{-d} \cdot (-\sqrt{-d})$ należy do $\mathfrak{m}$. Podsumowując, ideał $\mathfrak{m}$ zawiera, między innymi, elementy x^3 oraz $2d$. Z podpunktu (a) wynika, że $\mathrm{NWD}(x^3, 2d) = 1$. Na mocy rozszerzonego algorytmu Euklidesa, element 1 można zapisać jako $1 = ax^3 + b(2d)$, gdzie $a, b \in \mathbb{Z}$. Skoro $x^3, 2d$ należą do $\mathfrak{m}$, to również 1 należy do $\mathfrak{m}$. To daje sprzeczność: ideał $\mathfrak{m}$ nie może być całym pierścieniem.
(c) Zapiszmy rozkład na czynniki pierwsze w $\mathbb{Z}[\sqrt{-d}]$, tzn., zapiszmy $x = up_1^{e_1} \dots p_r^{e_r}$, gdzie u jest odwracalny, $p_1, \dots, p_r \in \mathbb{Z}[\sqrt{-d}]$ są elementami pierwszymi, zaś $e_1, \dots, e_r$ są całkowite nieujemne. Zapiszmy podobnie

$$y + \sqrt{-d} = u' p_1^{f_1} \dots p_r^{f_r} \qquad \text{oraz} \qquad y - \sqrt{-d} = u'' p_1^{g_1} \dots p_r^{g_r}.$$

Równość $x^3 = y^2 + d = (y - \sqrt{-d})(y + \sqrt{-d})$ pociąga za sobą równość

$$u^3 p_1^{3e_1} \dots p_r^{3e_r} = u'u'' p_1^{f_1+g_1} \dots p_r^{f_r+g_r}, \tag{1.1}$$

a stąd $3e_i = f_i + g_i$ dla każdego i. Gdyby istniało i takie, że $f_i, g_i > 0$, to p_i dzieliłoby obie liczby $y + \sqrt{-d}$, $y - \sqrt{-d}$, co jest sprzecznością z podpunktem (b). Zatem dla każdego i zachodzi $f_i = 0$

i $g_i = 3e_i$ lub $f_i = 3e_i$ i $g_i = 0$. W szczególności, dla każdego i liczba f_i jest podzielna przez 3, powiedzmy $f_i = 3k_i$.

Weźmy element $p_1^{k_1} \dots p_r^{k_r} \in \mathbb{Z}[\sqrt{-d}]$ i zapiszmy

$$a + b\sqrt{-d} := p_1^{k_1} \dots p_r^{k_r},$$

gdzie a, b są pewnymi liczbami całkowitymi. Wtedy

$$y + \sqrt{-d} = u'(a + b\sqrt{-d})^3. \tag{1.2}$$

Analizując normę zespoloną jak np. w w zadaniu 1 serii 4, stwierdzamy, że element u' jest równy ± 1. Ewentualnie zamieniając a, b na odwrotności, możemy założyć, że $u' = 1$. Zatem

$$y + \sqrt{-d} = (a + b\sqrt{-d})^3 = (a^3 - 3ab^2d) + (3a^2b - b^3d)\sqrt{-d}.$$

Wynika stąd w szczególności, że $1 = 3a^2b - b^3d = b(3a^2 - b^2d)$. Zatem mamy dwa przypadki

(a) $b = 1$. Wtedy $d = 3a^2 - 1$, $y = -8a^3 + 3a$, $x = a^2 + d$

(b) $b = -1$. Wtedy $d = 3a^2 + 1$, $y = -8a^3 - 3a$, $x = a^2 + d$.

To kończy ten podpunkt. Warto dodać, że dla dowolnego a powyższe wartości x, y, d spełniają $y^2 = x^3 - d$, zatem faktycznie otrzymaliśmy satysfakcjonujący opis rozwiązań całkowitych równania z zadania.

(d) Dążymy do uzyskania równania (1.2). Po jego uzyskaniu reszta rozwiązania nie korzysta z jednoznaczności rozkładu. Rozwiązanie jest w większej części analogiczne do tego w (c), ale jest sformułowane w innym języku.

Zauważmy, że $\mathbb{Z}[\sqrt{-d}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$. Z twierdzenia o istnieniu i jednoznaczności rozkładu na *ideały* pierwsze, możemy zapisać

$$(x) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r},$$

gdzie $(x) := x\mathbb{Z}[\sqrt{-d}]$ jest ideałem generowanym przez x, $\mathfrak{p}_1$, …,$\mathfrak{p}_r$ są parami różnymi ideałami pierwszymi, zaś e_i są liczbami nieujemnymi. Podobnie możemy zapisać

$$y + \sqrt{-d} = \mathfrak{p}_1^{f_1} \dots \mathfrak{p}_r^{f_r} \qquad \text{oraz} \qquad y - \sqrt{-d} = \mathfrak{p}_1^{g_1} \dots \mathfrak{p}_r^{g_r}.$$

Równość $x^3 = y^2 + d = (y - \sqrt{-d})(y + \sqrt{-d})$ pociąga za sobą równość

$$\mathfrak{p}_1^{3e_1} \dots \mathfrak{p}_r^{3e_r} = \mathfrak{p}_1^{f_1+g_1} \dots \mathfrak{p}_r^{f_r+g_r}, \tag{1.3}$$

a stąd $3e_i = f_i + g_i$ dla każdego i. Gdyby istniało i takie, że $f_i, g_i > 0$, to ideał $\mathfrak{p}_i$ zawierałby obie liczby $y + \sqrt{-d}$, $y - \sqrt{-d}$, co jest sprzecznością z podpunktem (b). Zatem dla każdego i zachodzi $f_i = 0$ i $g_i = 3e_i$ lub $f_i = 3e_i$ i $g_i = 0$. W szczególności, dla każdego i liczba f_i jest podzielna przez 3, powiedzmy $f_i = 3k_i$.

Weźmy ideał $J := \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} \subseteq \mathbb{Z}[\sqrt{-d}]$. Chcemy pokazać, że J jest generowany przez jeden element. Wiemy, że $J^3 = (y - \sqrt{-d})$ jest generowany przez jeden element. Teraz używamy założenia o grupie klas. Niech G będzie grupą klas $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$. Wtedy $[J^3] \in G$ jest równe $[(y - \sqrt{-d})]$, zatem jest elementem neutralnym. Ale wtedy w grupie G mamy $1_G = [J^3] = [J]^3$. Jeśli $[J] \neq 1_G$,

to rząd elementu $[J]$ wynosi 3. Z założenia, rząd grupy G jest skończony i niepodzielny przez 3, zatem rząd elementu $[J]$ nie może być równy 3. To pokazuje, że $[J] = 1_G$. To zaś mówi dokładnie, że J jest generowany przez jeden element, powiedzmy $J = (a + b\sqrt{-d})$. Wtedy

$$(y + \sqrt{-d}) = J^3 = (a + b\sqrt{-d})^3, \tag{1.4}$$

więc $y + \sqrt{-d} = u(a + b\sqrt{-d})^3$ dla pewnego odwracalnego $u \in \mathbb{Z}[\sqrt{-d}]$ i dalej argumentujemy jak w (c).

Zadanie 2. Rozwiąż równanie $y^2 = x^3 - 4$ w liczbach całkowitych, imitując argument powyżej.

Rozwiązanie.

Rozważmy najpierw przypadek x nieparzystego. Również y jest liczbą nieparzystą. Pierwszym pomysłem byłoby rozważenie $\mathbb{Z}[\sqrt{-4}]$, ale ten pierścień nie jest równy $\mathcal{O}_{\mathbb{Q}(\sqrt{-4})}$, bo $\mathbb{Q}(\sqrt{-4}) = \mathbb{Q}(\sqrt{-1})$. Ogólniej, $\mathbb{Z}[\sqrt{-4}]$ nie ma dobrych własności. O wiele lepiej jest rozważyć $\mathbb{Z}[i]$. Zapisujemy

$$x^3 = (y + 2i)(y - 2i). \tag{1.5}$$

Jeśli jakiś element pierwszy p dzieli $y + 2i$, $y - 2i$ to element ten dzieli również x^3 oraz $4i$, a więc dzieli on x^3 i 4. Ale x^3 i 4 są względnie pierwsze, więc 1 jest ich kombinacją liniową. To pokazuje, że element powyżej dzieli 1, a więc jest odwracalny, więc $y + 2i$, $y - 2i$. Wnioskujemy stąd, że

$$y + 2i = u(a + bi)^3,$$

gdzie $u \in \mathbb{Z}[i]$ jest odwracalny. Grupa elementów odwracalnych w $\mathbb{Z}[i]$ to $\{\pm 1, \pm i\}$, każdy z tych elementów jest sześcianem innego, więc możemy zapisać $u = v^3$ i wciągnąć v pod sześcian. W tym sposób powyższe równanie upraszcza się do

$$y + 2i = (a + bi)^3,$$

więc $2 = 3a^2b - b^3$, a stąd $(a, b) \in \{(-1, -2), (-1, 1), (1, -2), (1, 1)\}$ i $y = a^3 - 3ab^2$. Daje to $y = 11, 2, -11, -2$ odpowiednio. Wcześniej założyliśmy, że y jest nieparzysta, zatem $y = \pm 11$ i otrzymujemy dwa rozwiązania $(\mathbf{x}, \mathbf{y}) = (\mathbf{5}, \pm\mathbf{11})$.

Jeśli x jest liczbą parzystą, to y również. Ponadto $y^2 = x^3 - 4 \equiv 4 \pmod 8$, więc możemy zapisać $y = 4k + 2$. Ponownie mamy równanie (1.5). W tym wypadku 2 jest wspólnym dzielnikiem $y + 2i$, $y - 2i$, więc nie możemy bezpośrednio wywnioskować, że $y + 2i$ jest sześcianem. Musimy dokładniej przeanalizować ten największy wspólny dzielnik. Niech α będzie największym wspólnym dzielnikiem. Wtedy α dzieli $4i$, więc α dzieli 4.

W pierścieniu $\mathbb{Z}[i]$ mamy $4 = -(1+i)^4$, gdzie element $1+i$ jest pierwszy. Wobec tego $\alpha = (1+i)^e$, gdzie $e \in \{0, 1, 2, 3, 4\}$. Mamy $4\mathbb{Z}[i] = \{a + bi \mid a, b \in 4\mathbb{Z}\}$, więc 4 nie dzieli $y + 2i$. Zatem $e < 4$. Pokażemy, że faktycznie $(1 + i)^3$ dzieli obie liczby. Obliczamy, że

$$y + 2i = 2\,(2k + 1 + i) = 2(i + 1) + 4k,$$

jest podzielne przez $(1 + i)^3$, bowiem zarówno $2(i + 1)$ jak i $4 = -(1 + i)^3$ są podzielne przez ten element. Podobnie, $y - 2i = 2\,(2k + 1 - i) = 2 \cdot (2k + 2) - 2(1 + i)$ jest podzielne przez $(1 + i)^3$.

Z równania (1.5) wnioskujemy teraz, że

$$y + 2i = (1 + i)^3 \cdot u(a + bi)^3,$$

gdzie $u \in \{1, -1, i, -i\}$ oraz $a, b \in \mathbb{Z}$. Jak poprzednio, możemy zapisać $u = v^3$ i zwinąć wszystko do jednego sześcianu, otrzymując $y + 2i = (a' + b'i)^3$. Dalej argumentujemy jak w przypadku powyżej, otrzymując rozwiązania $(\mathbf{x}, \mathbf{y}) = (\mathbf{2}, \pm\mathbf{2})$.

Ostatecznie, mamy cztery rozwiązania $(5, \pm 11)$, $(2, \pm 2)$.