Teoria liczb
równania Diofantyczne, 11-15 maja

Zadanie 1. Okazuje się, że pierścień $\mathcal{O}_{\mathbb{Q}(\sqrt{-19})}$ ma jednoznaczność rozkładu, a równanie $y^2 = x^3 - 19$ ma rozwiązania w liczbach całkowitych. Jednak 19 nie jest postaci $3a^2 \pm 1$.

(a) Dlaczego nie stoi to w sprzeczności z zadaniem 1 z poprzedniej serii?

(b) Znajdź wszystkie rozwiązania powyższego równania (przy założeniu jednoznaczności rozkładu).

(c) $\star$ Uogólnij zadanie 1 z poprzedniej serii tak, by pokrywało ten przypadek.

Rozwiązanie.
(a) W języku zadania 1 z serii 8, mamy $d = 19$. Zatem $d \equiv 3 \pmod 4$, co jest sprzeczne z założeniami tamtego zadania.
(b) Jeśli x jest parzysta, to $y^2 \equiv -3 \equiv 5 \pmod 8$, ale kwadraty liczb przystają tylko do $0, 1, 4 \mod 8$, zatem sprzeczność. Liczba x jest więc nieparzysta.
Podobnie, jeśli istnieje wspólny dzielnik pierwszy $p \in \mathbb{P}$ liczb x oraz 19, to p dzieli $y^2 = x^3 - 19$, zatem p dzieli y. Wtedy jednak p^2 dzieli y^2 i x^3, więc p^2 dzieli 19, sprzeczność. To wszystko pokazuje, że liczba x jest względnie pierwsza z liczbą $2 \cdot 19$.

Niech

$$\Delta = \frac{1 + \sqrt{-19}}{2}$$

oraz $A = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \mathbb{Z}[\Delta]$, wtedy na mocy zadania 1 z serii 4 mamy $A = \mathcal{O}_{\mathbb{Q}(\sqrt{-19})}$. Załóżmy, że ideał $\mathfrak{m}$ zawiera $y - \sqrt{-19}$, $y + \sqrt{-19}$. Wtedy $\mathfrak{m} \cap \mathbb{Z}$ zawiera także

$$\sqrt{19} \cdot \left((y - \sqrt{-19}) - (y + \sqrt{-19})\right) = 2 \cdot 19,$$

oraz $x^3 = (y - \sqrt{-19})(y + \sqrt{-19})$. Ale stąd wynika, że $\mathfrak{m} \cap \mathbb{Z}$ zawiera także 1, sprzeczność. Zatem taki ideał $\mathfrak{m}$ nie istnieje; elementy $y \pm \sqrt{-19}$ są względnie pierwsze.

Z równania $x^3 = (y - \sqrt{-19})(y + \sqrt{-19})$ wynika teraz, że $y + \sqrt{-19} = J^3$, gdzie J jest pewnym ideałem w A. Skoro 3 nie dzieli rzędu grupy klas A, to J jest generowany przez jeden element z A, powiedzmy $J = (a + b\Delta)$. To implikuje, że

$$y + \sqrt{-19} = \pm (a + b\Delta)^3 . \tag{1.1}$$

Ewentualnie zmieniając a, b na odwrotności, możemy pozbyć się znaku $\pm$, tzn. ustalić go na 1. Wtedy mamy

$$y + \sqrt{-19} = y - 1 + 2\Delta = (a + b\Delta)^3 .$$

Obliczmy, że $\Delta^2 = \Delta - 5$, więc $\Delta^3 = \Delta^2 - 5\Delta = -4\Delta - 5$. Zatem

$$\begin{aligned}(a + b\Delta)^3 &= a^3 + 3a^2b\Delta + 3ab^2(\Delta - 5) + b^3(-4\Delta - 5) \\ &= \left(a^3 - 5(3ab^2 + b^3)\right) + \left(3a^2b + 3ab^2 - 4b^3\right)\Delta.\end{aligned}$$

Mamy więc $2 = b \cdot (3a^2 + 3ab - 4b^3)$ oraz $y - 1 = a^3 - 5(3ab^2 + b^3)$. Z pierwszego równania wynika, że b dzieli 2, więc $b \in \{-2, -1, 1, 2\}$. Na przykład sprawdzając wszystkie cztery przy-

padki, dowiadujemy się, że $b = 1$, $a \in \{-2, 1\}$. Stąd $y \in \{-18, 18\}$, więc $x^3 = 18^2 + 19 = 343$, więc rozwiązaniami są pary $(x, y) = (7, \pm 18)$.
(c) Metoda z podpunktu (b) uogólnia się, o ile $d \equiv 3 \pmod 8$. Jeśli $d \equiv 7 \pmod 8$, to dochodzi nowy przypadek x parzystego. Nie potrzeba tu nowych pomysłów, ale rozumowanie staje się dłuższe i nie zamieszczam go tutaj.

Zadanie 2. Pokaż, że liczby wymierne x, y spełniają równanie $y^2 = x^3 - x^2$ wtedy i tylko wtedy, gdy istnieje liczba wymierna t taka, że $x = t^2 + 1$, $y = t^3 + t$. *Wskazówka: są co najmniej 2 różne sposoby: (a) dla danych (x, y) zgadnąć wartość t (b) imitować dowód lematu o rozwiązaniach wymiernych $x^2 + y^2 = 1$.*

Rozwiązanie.

Załóżmy, że $x \neq 0$. (Jeśli $x = 0$ to $y = 0$ i otrzymujemy rozwiązanie sprzeczne z treścią zadania. Zatem formalnie mówiąc, zadanie jest fałszywe: działa tylko przy założeniu $x \neq 0$.)

Po pierwsze, warto zaznaczyć, że jeśli $x = t^2 + 1$, $y = t^3 + t$, to $t = y/x$. Weźmy więc *dowolne* wymierne (x, y) takie, że $x \neq 0$ oraz $y^2 = x^3 - x^2$ i połóżmy $t = y/x$. Wtedy

$$t^2 + 1 = \frac{y^2}{x^2} + 1 = \frac{x^3 - x^2}{x^2} + \frac{x^2}{x^2} = \frac{x^3}{x^2} = x$$

i podobnie $t^3 + t = t \cdot (t^2 + 1) = t \cdot x = \frac{y}{x} \cdot x = y$. To daje rozwiązania.
Geometryczna interpretacja tego wyniku jest następująca: t jest kątem nachylenia prostej przechodzącej przez $(0, 0)$ oraz przez (x, y).

Zadanie 3. Niech ξ będzie liczbą niewymierną. Pokaż, że istnieje nieskończenie wiele par liczb całkowitych x, y, takich, że $y > 0$ oraz $|x - y\xi| < 1/y$.

Rozwiązanie.

Ustalmy dowolną liczbę całkowitą dodatnią n. Niech $\{\alpha\}$ oznacza część ułamkową liczby rzeczywistej α, zaś $\lfloor \alpha \rfloor$ jej część całkowitą. Mamy więc $\alpha = \lfloor \alpha \rfloor + \{\alpha\}$ oraz $\{\alpha\} \in [0, 1)$.

Podzielmy przedział $[0, 1)$ na n przedziałów $\left[\frac{i}{n}, \frac{i+1}{n}\right]$, gdzie $i = 0, \ldots, n-1$. Rozważmy części ułamkowe liczb $0 \cdot \xi$, $1 \cdot \xi$, $\ldots$, $n \cdot \xi$. Z zasady szufladkowej Dirichleta, pewne dwie z nich leżą w tym samym przedziale, niech będą to części ułamkowe liczb $a\xi$ oraz $b\xi$ dla $0 \leq a < b \leq n$. Dowiadujemy się więc, że $|\{a\xi\} - \{b\xi\}| \leq \frac{1}{n}$.

Niech $y = b - a$ i niech $x = \lfloor b\xi \rfloor - \lfloor a\xi \rfloor$. Wtedy

$$|x - y\xi| = |\lfloor b\xi \rfloor - \lfloor a\xi \rfloor - b\xi + a\xi| = |-\{b\xi\} + \{a\xi\}| \leq \frac{1}{n} < \frac{1}{b-a} = \frac{1}{y}.$$

Znaleźliśmy w ten sposób, dla każdego n, parę (x, y) spełniającą warunki zadania. Pozostaje uzasadnić, dlaczego te pary są różne. Ale to wynika z powyższej nierówności: para otrzymana z liczby n spełnia $0 < |x - y\xi| < \frac{1}{n}$. Gdyby było tylko skończenie wiele par, to istniałoby N takie, że wszystkie z nich spełniają $\frac{1}{N} < |x - y\xi|$, a to pokazuje, że para otrzymana z $n = N$ nie jest jedną z tych par, sprzeczność.

Zadanie 4 (Dużo elementów odwracalnych w $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, $d > 0$.)**.** Niech $d > 0$ będzie liczbą bezkwadratową. Parę (x, y) nazwiemy rozwiązaniem równania Pella jeśli $x^2 - dy^2 = 1$. W tym ćwiczeniu opiszemy rozwiązania. Zauważmy, że w szczególnym przypadku $d \not\equiv 1 \pmod 4$ mamy $x^2 - dy^2 = N(x \pm y\sqrt{d})$, gdzie norma jest brana w $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Zatem w tym przypadku rozwiązania równania Pella to elementy odwracalne w $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

(a) Z poprzedniego zadania wywnioskuj, że istnieje nieskończenie wiele par liczb całkowitych dodatnich x, y takich, że $|x^2 - dy^2| < 2\sqrt{d} + 1$. Wywnioskuj, że istnieje $m \in \mathbb{Z}$, $m \neq 0$, taka, że istnieje nieskończenie wiele par powyżej z $x^2 - dy^2 = m$.

(b) Pokaż, że istnieją pary (x_1, y_1), (x_2, y_2) jak wyżej, takie, że $x_1 \equiv x_2 \pmod{m}$ oraz $y_1 \equiv y_2 \pmod{m}$. Pokaż, że $(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = m(u + v\sqrt{d})$, gdzie $u, v \in \mathbb{Z}$, $v \neq 0$ oraz $u^2 - v^2 d = 1$. Zatem istnieje rozwiązanie $(u, v) \neq \{(1, 0), (-1, 0)\}$.

(c) Załóżmy, że (u_1, v_1), (u_2, v_2) są rozwiązaniami. Pokaż, że jeśli $u_3 + v_3\sqrt{d} = (u_1 + v_1\sqrt{d}) \cdot (u_2 + v_2\sqrt{d})$ lub $u_3 + v_3\sqrt{d} = (u_1 + v_1\sqrt{d}) \cdot (u_2 + v_2\sqrt{d})^{-1}$, to (u_3, v_3) też jest rozwiązaniem.

(d) Załóżmy, że $(x_1, y_1) \in \mathbb{Z}^2_{>0}$ jest rozwiązaniem w liczbach dodatnich z najmniejszą wartością $x_1 + y_1\sqrt{d}$. Rozwiązanie to nazwiemy *fundamentalnym*. Pokaż, że jeśli $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$, to (x_n, y_n) są parami różnymi rozwiązaniami w liczbach dodatnich.

(e) Załóżmy, że (x', y') jest rozwiązaniem w liczbach dodatnich. Niech k będzie takie, że $x_n + y_n\sqrt{d} \leq x' + y'\sqrt{d} < x_{n+1} + y_{n+1}\sqrt{d}$. Pokaż, że $(x', y') = (x_n, y_n)$. Zatem „potęgi" rozwiązania fundamentalnego są jedynymi rozwiązaniami w liczbach całkowitych dodatnich.

Rozwiązanie fundamentalne może być paskudnie duże, np. $(x_1, y_1) = (1766319049, 226153980)$ dla $d = 61$ podczas gdy $(x_1, y_1) = (63, 8)$ dla $d = 62$. Fermat potrafił być paskudnie wredny: reklamował dokładnie $d = 61$ jako łatwy przypadek równania do przemyślenia przed rozwiązaniem ogólnego przypadku d. Rozwiązanie fundamentalne można znaleźć algorytmicznie, ale nie będziemy tego robić.

Rozwiązanie.

(a) Z zadania 3 wynika, że istnieje nieskończenie wiele par liczb całkowitych (x, y) takich, że $|x - \sqrt{d}y| < \frac{1}{y}$ oraz $y > 0$. Stąd wynika też, że $x > 0$. Weźmy dowolną z tych par. Mamy

$$|x + \sqrt{d}y| \leq |x - \sqrt{d}y| + 2\sqrt{d}|y| < \frac{1}{y} + 2\sqrt{d}|y|.$$

Stąd $|x^2 - dy^2| < 2\sqrt{d} + \frac{1}{y^2} < 2\sqrt{d} + 1$. Skoro istnieje nieskończenie wiele par (x, y) oraz dla każdej pary $0 < |x^2 - dy^2| < 2\sqrt{d} + 1$ jest liczbą całkowitą, to wyrażenie $|x^2 - dy^2|$ przyjmuje pewną wartość m nieskończenie wiele razy.

(b) By wykazać istnieje par (x_1, y_1), (x_2, y_2) takich, że $x_1 \equiv x_2$ oraz $y_1 \equiv y_2$ argumentujemy jak wyżej: jest skończenie wiele reszt z dzielenia przez m, więć pewna para reszt musi być przyjmowana nieskończenie wiele razy.

Mając rozwiązania (x_1, y_1) oraz (x_2, y_2) takie, że $x_1 \equiv x_2 \pmod{m}$ i $y_1 \equiv y_2 \pmod{m}$, obliczamy, że

$$(x_1 + y_1\sqrt{d}) \cdot (x_2 - y_2\sqrt{d}) = (x_1x_2 - y_1y_2d) + (x_2y_1 - x_1y_2)\sqrt{d}.$$

Ale $x_2y_1 \equiv x_1y_1 \equiv x_1y_2 \pmod{m}$ oraz $x_1x_2 - y_1y_2d \equiv x_1^2 - dy_1^2 = m \equiv 0 \pmod{m}$. Zatem $u = \frac{x_1x_2 - y_1y_2d}{m}$, $v = \frac{x_2y_1 - x_1y_2}{m}$ są liczbami całkowitymi takimi, że

$$(x_1 + y_1\sqrt{d}) \cdot (x_2 - y_2\sqrt{d}) = m \cdot (u + v\sqrt{d}). \tag{1.2}$$

Przypomnijmy, że $\mathbb{Q}(\sqrt{d})$ ma normę, taką, że $N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$. (To nie jest norma odziedziczona z liczb zespolonych! Ale jest multiplikatywna.) Mamy

$$(x_1^2 - dy_1^2) \cdot (x_2^2 - y_2^2 d) = m^2 \cdot (u^2 - v^2 d),$$

czyli $1 = u^2 - v^2 d$. Jeśli $v = 0$ to $u = \pm 1$ i z równania (1.2) mamy

$$m = (x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = m\frac{x_1 + y_1\sqrt{d}}{x_2 + y_2\sqrt{d}},$$

więc $x_1 + y_1\sqrt{d} = x_2 + y_2\sqrt{d}$. Ale to przeczy temu, że pary (x_1, y_1), (x_2, y_2) są różne. Pokazaliśmy więc, że $v \neq 0$.
(c) Jeśli (u_3, v_3) są zdefiniowane jak w jednym z równań, to biorąc normy, mamy $u_3^2 - dv_3^2 = 1$. Ponadto jeśli $u_3 + v_3\sqrt{d} = (u_1 + v_1\sqrt{d}) \cdot (u_2 + v_2\sqrt{d})$, to u_3, v_3 są całkowite. Jeśli zaś $u_3 + v_3\sqrt{d} = (u_1 + v_1\sqrt{d}) \cdot (u_2 + v_2\sqrt{d})^{-1}$ to

$$u_3 + v_3\sqrt{d} = (u_1 + v_1\sqrt{d}) \cdot (u_2 - v_2\sqrt{d}),$$

co również pokazuje, że u_3, v_3 są całkowite. Zatem (u_3, v_3) jest rozwiązaniem.
(d) Ma mocy poprzedniego podpunktu, (x_n, y_n) jest rozwiązaniem. Pozostaje pokazać, że $(x_n, y_n) \neq (x_m, y_m)$ dla $n < m$. Jeśli $(x_m, y_m) = (x_n, y_n)$, to znaczy, że $(x_1 + y_1\sqrt{d})^{n-m} = 1$. Ale to nonsens: liczba $x_1 + y_1\sqrt{d}$ jest równa co najmniej $1 + \sqrt{d} > 1$, więc jej potęga również.
(e) Niech

$$u' + v'\sqrt{d} = \frac{x' + y'\sqrt{d}}{x_n + y_n\sqrt{d}} = (x' + y'\sqrt{d}) \cdot (x_n - y_n\sqrt{d}) = (x' + y'\sqrt{d}) \cdot (x_1 - y_1\sqrt{d})^n. \tag{1.3}$$

Na mocy podpunktu (c), (u', v') jest rozwiązaniem, nie wiemy jednak a priori, czy u', v' są dodatnie. Na mocy (1.3) oraz założenia podpunktu, mamy

$$x_1 + y_1\sqrt{d} > u' + v'\sqrt{d} \geq 1.$$

Stąd $u' - v'\sqrt{d} = \frac{1}{u' + v'\sqrt{d}}$ leży w $(0, 1]$, w szczególności $u' - v'\sqrt{d} > 0$. Dodając dwie powyższe nierówności, otrzymujemy $2u' > 0$. Stąd $v'\sqrt{d} > u' - 1 \geq 0$. Jesli $v' = 0$, to $u' = 0$ i mamy, że $(u, v) = (x_n, y_n)$. Jeśli nie, to pokazaliśmy, że (u', v') jest rozwiązaniem w liczbach całkowitych dodatnich takim, że $x_1 + y_1\sqrt{d} > u' + v'\sqrt{d}$, co jest sprzecznością z określeniem (x_1, y_1).