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.

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 $x^2 + y^2 = 1$.*

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

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.