Warsztaty KFnrD, *Równania diofantyczne*, Lista 1, 6.12.2019 (piątek)

$\mathbb{N} = \{0, 1, 2, \ldots\}$ oznacza zbiór liczb naturalnych, $\mathbb{Z}$ zbiór liczb całkowitych, $\mathbb{Q}$ zbiór liczb wymiernych, $\mathbb{R}$ zbiór liczb rzeczywistych i $\mathbb{C}$ zbiór liczb zespolonych.
Mówimy, że liczba $a \in \mathbb{C}$ jest *algebraiczna*, gdy istnieją $n \in \mathbb{N}_{>0}$ oraz $q_0, \ldots, q_{n-1} \in \mathbb{Q}$, takie że:

$$q_0 + q_1 a + \ldots + q_{n-1} a^{n-1} + a^n = 0.$$

Liczba $a \in \mathbb{C}$ jest *algebraiczna stopnia* n, oznaczane $\deg(a) = n$, gdy powyższe n jest najmniejsze.

(1) Załóżmy, że $x, y, z \in \mathbb{N}_{>0}$ oraz:

$$x^2 + y^2 = z^2.$$

Udowodnić, że:

(a) liczba x jest parzysta lub liczba y jest parzysta (**wsk.**: „popatrzeć modulo 4");

(b) jeśli powyższe x, y, z są parami względnie pierwsze i istnieją $a, b, c \in \mathbb{N}$, takie że:

$$y = 2a, \quad z - x = 2b, \quad z + x = 2c,$$

to b i c są względnie pierwsze.

(2) Załóżmy, że $n, m \in \mathbb{N}_{>0}$ są względnie pierwsze oraz, że istnieje $c \in \mathbb{Z}$, taki że $nm = c^2$.

(a) Udowodnić szczegółowo, że istnieją $a, b \in \mathbb{Z}$, takie że $n = a^2$ i $m = b^2$.

(b) Podać kontrprzykład na podpunkt (a) przy założeniu $n, m \in \mathbb{Z} \setminus \{0\}$.

(c) Sformułować i udowodnić wersję podpunktu (a) przy założeniu $n, m \in \mathbb{Z} \setminus \{0\}$.

(3) Przedstawić definicję *ułamka łańcuchowego skończonego* oraz *ułamka łańcuchowego nieskończonego* (**wsk.**: `https://pl.wikipedia.org/wiki/U%C5%82amek_%C5%82a%C5%84cuchowy`).

(4) Udowodnić, że:

(a) każdą liczbę rzeczywistą można zapisać w postaci ułamka łańcuchowego;

(b) liczbom wymiernym odpowiadają ułamki łańcuchowe skończone;

(c) liczbom niewymiernym odpowiadają ułamki łańcuchowe nieskończone.

(5) Weźmy $\alpha \in \mathbb{C} \setminus \mathbb{Z}$, taką że $\alpha^2 \in \mathbb{Z}$. Rozważmy następujący podzbiór $\mathbb{C}$:

$$\mathbb{Q}[\alpha] := \{q + r\alpha \mid q, r \in \mathbb{Q}\}.$$

Udowodnić, że:

(a) podzbiór $\mathbb{Q}[\alpha]$ jest podciałem $\mathbb{C}$;

(b) dla każdych $q, q', r, r' \in \mathbb{Q}$ jeśli

$$q + r\alpha = q' + r'\alpha,$$

to wtedy $q = q'$ i $r = r'$;

(c) funkcja (dobrze określona na mocy (b))

$$N : \mathbb{Q}[\alpha] \longrightarrow \mathbb{Q}, \qquad N(q + r\alpha) := q^2 - r^2\alpha^2$$

jest *multyplikatywna*, tzn. dla każdych $q, q', r, r' \in \mathbb{Q}$ mamy:

$$N\left((q + r\alpha)(q' + r'\alpha)\right) = N(q + r\alpha)N(q' + r'\alpha);$$

(d) dla każdego $x \in \mathbb{Z}[\alpha]$ zachodzi $N(x) \in \mathbb{Z}$.

(6) Udowodnić, że następujący podzbiór jest podciałem $\mathbb{C}$:

$$\mathbb{Q}\left[\sqrt[3]{2}\right] = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\right\}.$$

(7) Udowodnić, że:

$$\deg(\zeta_3) = 2 = \deg(\zeta_6),$$

gdzie dla $n \in \mathbb{N}_{>0}$:

$$\zeta_n = \cos(2\pi/n) + i\sin(2\pi/n),$$

czyli ζ_n jest *n-tym pierwotnym pierwiastkiem z jedynki* (w $\mathbb{C}$).