Obliczeniowa teoria równań diofantycznych

Przyjmujemy, że 0 jest liczbą naturalną.

1 Wielomiany

Wielomianem jednej zmiennej nazywamy funkcję postaci

$$W(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

Liczby a_i to współczynniki wielomianu (na warsztatach będziemy się zajmowali wielomianami o współczynnikach całkowitych), a n to stopień wielomianu. Wielomian wielu zmiennych definiujemy analogicznie - jest to suma skończenie wielu wyrażeń postaci $a_{v_1,\ldots,v_m} x_1^{v_1} \ldots x_m^{v_m}$ dla $v_i \in \mathbb{N}$.

2 Równania diofantyczne

Równaniem diofantycznym nazywamy równanie postaci

$$D(x_1, \ldots, x_n) = 0$$

gdzie D jest wielomianem n zmiennych o współczynnikach całkowitych. Na warsztatach (i w zadaniach) interesować na będą rozwiązania w liczbach naturalnych (chociaż rozstrzyganie istnienia rozwiązań w liczbach całkowitych jest problemem równoważnym - $U(x_1, \ldots) = 0$ ma rozwiązanie w $\mathbb{N}^m$ wtw gdy $U(a_1^2 + b_1^2 + c_1^2 + d_1^2, \ldots) = 0$ ma rozwiązanie w $\mathbb{Z}^{4m}$, a $V(y_1, \ldots) = 0$ ma rozwiązania w $\mathbb{Z}^n$ wtw gdy $V(e_1 - f_1, \ldots) = 0$ ma rozwiązania w $\mathbb{N}^{2n}$).
Równaniem z parametrami nazywamy równanie postaci $D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$, w którym a_i są parametrami, a x_j zmiennymi.

3 Układy równań diofantycznych

Układem równań diofantycznych nazywamy koniunkcję skończonej liczby równań diofantycznych:

$$\begin{cases} D_1(x_1, \ldots, x_n) = 0 \\ \ldots \\ D_k(x_1, \ldots, x_n) = 0 \end{cases}$$

Warto zauważyć, że powyższy układ równań można skompresować do pojedynczego równania:

$$D_1(x_1, \ldots, x_n)^2 + \cdots + D_k(x_1, \ldots, x_n)^2 = 0$$

które posiada rozwiązania wtedy i tylko wtedy, gdy rozwiązanie ma układ równań.
Każde równanie diofantyczne można sprowadzićdo układu równań postaci $x = y + z$ oraz $x = yz$. Równanie

$$3a^3 + gh^2 - 7j = 0$$

ma rozwiązania wtedy i tylko wtedy, gdy rozwiązania ma układ

$$\begin{cases} b = 3a \\ c = ab \\ d = ac \\ e = gh \\ f = eh \\ i = 7j \\ i = d + f \end{cases}$$

4 Zbiory diofantyczne

Mówimy, że zbiór $\mathfrak{M} \subseteq \mathbb{N}^n$ jest diofantyczny, gdy istnieje taki wielomian D, że równanie diofantyczne $D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ ma rozwiązanie w $x_1, \ldots, x_m \in \mathbb{N}$ wtedy i tylko wtedy, gdy krotka $(a_1, \ldots, a_n)$ należy do zbioru $\mathfrak{M}$, tzn. dla pewnego wielomianu D

$$(a_1, \ldots, a_n) \in \mathfrak{M} \Leftrightarrow \exists_{x_1,\ldots,x_m \in \mathbb{N}} D(a_1, \ldots, x_1, \ldots) = 0$$

Suma i przecięcie zbiorów diofantycznych są diofantyczne (dlaczego?).
Relacją diofantyczną nazywamy taką relację, że zbiór liczb dla których jest spełniona jest diofantyczny, a funkcją diofantyczną taką funkcję, że zbiór krotek $(F(a_1, \ldots), a_1, \ldots)$ jest diofantyczny.
Łatwo zauważyć, że diofantyczne są następujące relacje i funkcje:

- Relacja $\leqslant$ $(a \leqslant b \Leftrightarrow \exists_x a + x = b)$
- Relacja $<$
- Relacja $\neq$ $(a \neq b \Leftrightarrow \exists_x (a-b)^2 = x + 1)$
- Relacja podzielności $(a|b \Leftrightarrow \exists_x ax = b)$
- Kongruencja
- Funkcja reszty z dzielenia $(a = R(b, c) \Leftrightarrow a < c \wedge a \equiv_c b)$
- Funkcja NWD $(a = \mathrm{NWD}(b, c) \Leftrightarrow a|b \wedge a|c \wedge \exists_{x,y} a = bx - cy)$