Równania diofantyczne liniowe

Definicja

Równaniem diofantycznym jest *dowolne* równanie typu $f(x_1, x_2, \ldots, x_n) = 0$, w którym szukane rozwiązanie $(x_1, x_2, \ldots, x_n)$ składa się z *liczb całkowitych*.

Takim równaniem było równanie określające wiek Diofantesa.
Jednak zwykle w równaniach diofantycznych mamy deficyt informacji w stosunku do liczby niewiadomych.
Na przykład:

$$43x + 7y + 17z = 400.$$

Oczywiście to *nie jest nic trudnego!*

Taktyka:

- Największy współczynnik ma x – liczba możliwości dla niego jest najmniejsza.
  Zaczynamy od określenia maksymalnej wartości x — $43 * 9 < 400$ a $43 * 10 > 400$ – stąd $x \in [1, 9]$.
- Połóżmy $x = 3$ mamy: $43(3) + 7y + 17z = 400$, albo $y = 38 - \frac{17z-5}{7}$.
- teraz pozostaje określenie z – tak aby ułamek był liczbą całkowitą (mniejszą od 38); to oznacza, że $7|(17z - 5)$.
  Biorę $z = 1, 2, \ldots$ – dopiero dla $z = 4$ mam $17 \cdot 4 - 5 = 63 = 7 \cdot 9$.
  Następne z będzie miało postać $4 + k \cdot 7 = 11, 18, \ldots$ ale już dla $z = 18$ mamy $38 - (18 \cdot 7 - 5)/7 = -5$.
- Stąd mam dwa rozwiązania $(x, y, z) = (3, 29, 4)$ i $(x, y, z) = (3, 12, 11)$ (dla wyboru $x = 3$).
- Analogiczne procedury należy powtórzyć dla innych wartości x. Voilà!

Odrobina historii: równaniem $ax + by = c$ ...

...zajmowali się w pierwszym rzędzie matematycy hinduscy: Arybatha (476), Bramhagupta (ca. 600) [!], Mahavira (ca 850) i Bhaskara (1114–1185).

Twierdzenie:

równanie diofantyczne $ax + by = c$ ma rozwiązanie wtedy i tylko wtedy gdy $d|c$, gdzie $d = NWD(a, b)$.

Innymi słowy: rozwiązanie x_0, y_0 ma własność

$$c = ax_0 + by_0 = rdx_0 + sdy_0 = d(rx_0 + sy_0).$$

Oczywiście, wynika stąd $d|c$.
Możemy odwrócić rozumowanie: jeżeli $d|c \rightarrow c = dt$, a jednocześnie $d = NWD(a, b)$ to ... *musi* istnieć para x_0, y_0:

$$d = ax_0 + by_0$$

(było takie twierdzenie!) – mnożymy stronami przez t

$$dt = c = (ax_0 + by_0)t = a(tx_0) + b(ty_0).$$

Twierdzenie:

równanie diofantyczne $ax + by = c$ ma rozwiązanie wtedy i tylko wtedy gdy $d|c$, gdzie $d = NWD(a, b)$; jeżeli x_0, y_0 jest takim rozwiązaniem, to wszystkie inne rozwiązania mają postać

$$x = x_0 + \frac{b}{d}t, \qquad y = y_0 - \frac{a}{d}t, \quad t \in \mathbb{N}.$$

Dowód:

x_0, y_0 jest rozwiązaniem, a także x', y'; tzn.

$$ax_0 + by_0 = c = ax' + by'.$$

$$a(x' - x_0) = b(y_0 - y').$$

$d = NWD(a, b) \rightarrow a = dr,\ b = ds$ (gdzie r i s są względnie pierwsze!) mamy

$$NWD(r, s) = NWD\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

podstawiamy

$$r(x' - x_0) = s(y_0 - y').$$

Z powyższego wynika $r|s(y_0 - y')$ ale – r i s są względnie pierwsze! – $r|(y_0 - y')$, a więc $(y_0 - y') = rt$ i podstawiając mamy

$$x' - x_0 = st.$$

no i już łatwo:

$$x' = x_0 + st = x_0 + \frac{b}{d}t, \quad y' = y_0 - rt = y_0 - \frac{a}{d}t,$$

Pozostaje (na wszelki wypadek, bardzo łatwe) wykazać:
$ax' + by' = c$.