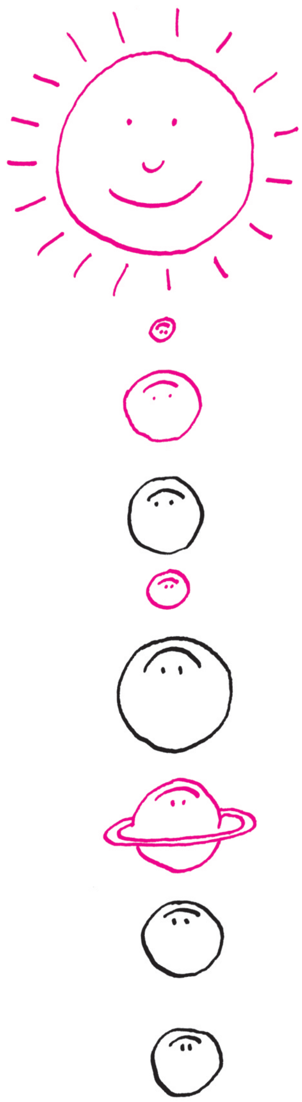


Niewymierność $\sqrt{2}$ i jeszcze większe niemożliwości

*Mariusz SKAŁBA**

Punktem wyjścia niech będzie najsłynniejsza chyba matematyczna konstatacja, ta mianowicie, że liczba $\sqrt{2}$ jest niewymierna. Można to wysłowić w następujący równoważny i tendencyjny sposób.

Twierdzenie 1. *Jeśli liczby całkowite x, y spełniają równanie $x^2 - 2y^2 = 0$, to $x = y = 0$.*

Czy twierdzenie to można wzmocnić? Okazuje się, że tak! Zachodzi mianowicie

Twierdzenie 2. *Jeśli $x, y, z \in \mathbb{Z}$ oraz $x^2 - 2y^2 - 3z^2 = 0$, to $x = y = z = 0$*

Zauważmy przede wszystkim, że jeśli liczba całkowita a nie dzieli się przez 3, to $a^2 \equiv 1 \pmod 3$. Ponieważ $x^2 - 2y^2 \equiv 0 \pmod 3$, więc $y \equiv 0 \pmod 3$ oraz $x \equiv 0 \pmod 3$. Zatem $3z^2 \equiv 0 \pmod 9$ i stąd również $z \equiv 0 \pmod 3$. Istnieją więc takie liczby całkowite x_1, y_1, z_1, że $x = 3x_1, y = 3y_1, z = 3z_1$ oraz $x_1^2 - 2y_1^2 - 3z_1^2 = 0$. Wynika stąd, że wyjściowe liczby x, y, z są podzielne przez dowolnie wysokie potęgi liczby 3, a to jest możliwe tylko dla $x = y = z = 0$.

Okazuje się, że można to jeszcze bardziej uogólnić!

Twierdzenie 3. *Jeśli $x, y, z, t \in \mathbb{Z}$ oraz $x^2 - 2y^2 - 3z^2 + 6t^2 = 0$, to $x = y = z = t = 0$.*

Z równości $x^2 + 6t^2 = 2y^2 + 3z^2$ wynika bowiem, że

$$(x^2 + 6t^2)^2 = (x^2 + 6t^2)(2y^2 + 3z^2) = 2(xy + 3zt)^2 + 3(xz - 2yt)^2.$$

Z twierdzenia 2 wynika teraz, że $x^2 + 6t^2 = 0$ i stąd $x = t = 0$. Z równości $-2y^2 - 3z^2 = 0$ otrzymujemy ostatecznie $y = z = 0$.

Jak Czytelnik słusznie przeczuwa, niemożliwości nie mogą rozpychać się w nieskończoność, a w naszym przypadku przygważdża je

Twierdzenie 4. *Dla każdej liczby całkowitej $m \neq 0$ istnieją takie liczby całkowite x, y, z, t, s, nie wszystkie równe 0, że*

$$x^2 - 2y^2 - 3z^2 + 6t^2 - ms^2 = 0.$$

Łatwo zauważyć, że powyższe twierdzenie można wypowiedzieć w następujący równoważny sposób:

Dla każdej liczby całkowitej $m \neq 0$ istnieją takie liczby **wymierne** *x, y, z, t, że*

$$x^2 - 2y^2 - 3z^2 + 6t^2 = m.$$

Kluczowy jest poniższy lemat.

Lemat 1. *Iloczyn i iloraz dwóch liczb postaci $x^2 - 2y^2 - 3z^2 + 6t^2$ jest też tej postaci.*

Dowód wynika z następujących tożsamości:

$$\begin{aligned}(x_1^2 - 2y_1^2 - 3z_1^2 + 6t_1^2)&(x_2^2 - 2y_2^2 - 3z_2^2 + 6t_2^2) = \\ &= (x_1x_2 + 2y_1y_2 + 3z_1z_2 - 6t_1t_2)^2 - 2(x_1y_2 + x_2y_1 - 3z_1t_2 + 3z_2t_1)^2 - \\ &\quad - 3(x_1z_2 + x_2z_1 + 2y_1t_2 - 2y_2t_1)^2 + 6(x_1t_2 + x_2t_1 + y_1z_2 - y_2z_1)^2\end{aligned}$$

oraz

$$(x_2^2 - 2y_2^2 - 3z_2^2 + 6t_2^2)^{-1} = \left(\frac{x_2}{w_2}\right)^2 - 2\left(\frac{y_2}{w_2}\right)^2 - 3\left(\frac{z_2}{w_2}\right)^2 + 6\left(\frac{t_2}{w_2}\right)^2,$$

gdzie oznaczyliśmy $w_2 = x_2^2 - 2y_2^2 - 3z_2^2 + 6t_2^2$.

*Instytut Matematyki, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Z lematu 1 wynika przede wszystkim, że dla dowodu twierdzenia 4 wystarczy rozpatrzyć tylko przypadek $m > 0$, gdyż

$$-1 = 1^2 - 2\cdot 1^2 - 3\cdot 0^2 + 6\cdot 0^2.$$

Dowód przeprowadzimy przez indukcję ze względu na m. Dla $m = 1$ oraz $m = 2$ mamy przedstawienia

$$1 = 1^2 - 2\cdot 0^2 - 3\cdot 0^2 + 6\cdot 0^2, \qquad 2 = 2^2 - 2\cdot 1^2 - 3\cdot 0^2 + 6\cdot 0^2.$$

Załóżmy z kolei, że $m \geqslant 3$ i teza zachodzi dla $1 \leqslant m' < m$. Rozróżniamy teraz dwa przypadki. Jeżeli m jest liczbą złożoną, to $m = m'\cdot m''$ gdzie $m' < m$ oraz $m'' < m$. Z lematu 1 wynika więc odpowiednie przedstawienie dla m. Jeżeli $m = p$ jest liczbą pierwszą, to sytuacja jest bardziej skomplikowana. Przyda się następujący

Lemat 2. *Jeśli p jest liczbą pierwszą, to istnieją takie liczby całkowite α, β, że*

$$\alpha^2 - 2\beta^2 - 3 \equiv 0 \pmod{p}.$$

Załóżmy od razu, że $p \neq 2$. Reszty mod p liczb

$$0^2 - 3,\ 1^2 - 3,\ \ldots,\ \left(\frac{p-1}{2}\right)^2 - 3$$

są parami różne i jest ich $(p+1)/2$. Podobnie, reszty mod p liczb

$$2\cdot 0^2,\ 2\cdot 1^2,\ \ldots,\ 2\left(\frac{p-1}{2}\right)^2$$

są parami różne i jest ich $(p+1)/2$. Ponieważ wszystkich reszt mod p jest tylko p, więc pewna reszta typu $\alpha^2 - 3$ pokrywa się z pewną resztą typu $2\beta^2$, co daje tezę lematu 2.

Ponieważ $x^2 \equiv (x-p)^2 \pmod{p}$ więc w lemacie 2 możemy założyć, że liczby całkowite α i β spełniają dodatkowo nierówności

$$|\alpha| < \frac{p}{2} \text{ oraz } |\beta| < \frac{p}{2}.$$

Mamy zatem oszacowania

$$-\frac{p^2}{2} - 3 \leqslant \alpha^2 - 2\beta^2 - 3 < \frac{p^2}{4}.$$

Ponieważ $p \geqslant 3$, więc

$$|\alpha^2 - 2\beta^2 - 3| < p^2.$$

Możemy zatem napisać

$$|\alpha^2 - 2\beta^2 - 3| = kp, \text{ przy czym } 1 \leqslant k < p.$$

Na mocy założenia indukcyjnego liczba naturalna k ma przedstawienie

$$k = x_2^2 - 2y_2^2 - 3z_2^2 + 6t_2^2, \text{ gdzie } x_2, y_2, z_2, t_2 \in \mathbb{Q}.$$

Wnosimy stąd na podstawie lematu 1, że liczba

$$p = \frac{kp}{k} = \frac{(\mp 1)(\alpha^2 - 2\beta^2 - 3\cdot 1^2 + 6\cdot 0^2)}{k}$$

też ma takie przedstawienie i to kończy dowód indukcyjny twierdzenia.

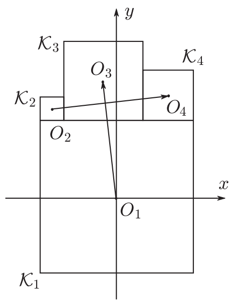
Wyniki przedstawione powyżej są kompletne, ale dość sztuczne. Szczęście nam sprzyjało, gdyż forma kwadratowa $x^2 - 2y^2 - 3z^2 + 6t^2$ jest tzw. formą normową dla algebry kwaternionowej $\left(\frac{2,3}{\mathbb{Q}}\right)$ – stąd wynika „cudowna” tożsamość wypisana w Lemacie 1. A gdyby nie pomagać szczęściu aż tak bardzo? Okazuje się, że prawdziwe jest następujące ogólne twierdzenie.

Twierdzenie 5. *Jeżeli liczby wymierne $a, b, c, d, -f$ są różne od zera oraz nie są wszystkie tego samego znaku to istnieją takie liczby wymierne x, y, z, t, że*

$$ax^2 + by^2 + cz^2 + dt^2 = f.$$

Dowód tego twierdzenia wymaga zastosowania poważnej i pięknej matematyki. Ważnymi jego składnikami są: prawo wzajemności dla reszt kwadratowych oraz twierdzenie Dirichleta o liczbach pierwszych w postępie arytmetycznym. To wszystko, i dużo więcej, znajdzie Czytelnik w zajmującej książce: Z.I. Borewicz, I.R. Szafarewicz, *Теория чисел*, Moskwa 1985 (istnieją tłumaczenia na angielski i niemiecki).

Rozwiązanie zadania M 1426.
Przyjmijmy, że bok kwadratu $\mathcal{K}_1$ ma długość 2, a kwadratów $\mathcal{K}_2, \mathcal{K}_3, \mathcal{K}_4$ – odpowiednio $2a, 2b, 2c$ (stąd $a+b+c=1$). Niech środek układu współrzędnych będzie ustawiony w środku kwadratu $\mathcal{K}_1$, a osie niech będą równoległe do jego boków (jak na rysunku). Oznaczmy środek kwadratu $\mathcal{K}_i$ przez O_i dla $1 \leqslant i \leqslant 4$.



Mamy $O_3 = (-1+2a+b, 1+b)$, więc $\overrightarrow{O_1O_3} = [-1+2a+b, 1+b]$. Podobnie, skoro $O_2 = (-1+a, 1+a)$, $O_4 = (1-c, 1+c)$ oraz $a+b+c=1$, to otrzymujemy $\overrightarrow{O_2O_4} = [2-a-c, c-a] = [1+b, 1-2a-b]$. Stąd w oczywisty sposób dostajemy $\overrightarrow{O_1O_3}\cdot\overrightarrow{O_2O_4} = 0$. Zauważmy, że wykazaliśmy nawet więcej. Z rozwiązania wynika również, że $O_1O_3 = O_2O_4$.

Rozwiązanie zadania M 1427.
Odp. Tak!
Liczbę $x \geqslant 0$ kolorujemy na kolor o numerze $\lfloor x \rfloor$ mod 4. Załóżmy, że $\frac{a+b}{2} = c+1$ dla pewnych liczb nieujemnych a, b, c i przyjmijmy, że $a \leqslant b$. Załóżmy, że a i b mają ten sam kolor. Niech $\lfloor a \rfloor = k$, czyli $a \in [k, k+1)$ dla pewnej liczby całkowitej $k \geqslant 0$. Wówczas $b \in [k+4l, k+4l+1)$ dla pewnej liczby całkowitej $l \geqslant 0$. Zatem $(a+b)/2 \in [k+2l, k+2l+1)$, więc $\lfloor c \rfloor = k+2l-1$. Ponieważ $2l$ mod $4 = 0$ lub 2, więc liczba c ma w opisanym przez nas kolorowaniu inny kolor niż liczby a i b.