Ziemiolubne liczby i ulotne reszty

*Mariusz SKAŁBA**

* Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Człowiek twardo stąpa po ziemi, a z nim pojęcia, które stworzył. Na przykład liczby są tylko tym, do czego człowiekowi służą: porządkowe, kardynalne i inne. W skończonych zastosowaniach są to liczby naturalne $1, 2, 3, \ldots$ i ich uogólnienia: liczby całkowite, wymierne, rzeczywiste i zespolone. Słowo *skończone* w poprzednim zdaniu odnosi się wyłącznie do opisywanego atrybutu *liczonego* obiektu: a to jego rangi, a to mocy, a to fizycznych rozmiarów. W matematyce teoretycznej liczb praktycznie zawsze potrzebujemy nieskończenie wiele!

Wróćmy zatem na ubitą przez tysiąclecia glebę teorii liczb. Jak udowodnić najprościej, że równanie

$$x^2 - 20xy + y^2 = 100000000003$$

nie ma rozwiązań w liczbach całkowitych x, y? Można na przykład zauważyć, że odpowiednia kongruencja mod 4 nie ma rozwiązań. Wynika to stąd, że kwadrat liczby całkowitej zawsze przystaje do 0 lub 1 modulo 4, a zatem lewa jej strona przystaje do $0, 1, 2$ modulo 4, a prawa do 3.

Nie zawsze jest tak łatwo i o tym właśnie jest ten artykuł. Rozważmy mianowicie równanie

$$x^4 - 2y^4 = 7z^2 \tag{1}$$

i zapytajmy o jego rozwiązania w liczbach całkowitych nieujemnych x, y, z. Jeśli x, y, z jest takim rozwiązaniem oraz $x = 0$, to $-2y^4 = 7z^2$, a więc również $y = z = 0$. Załóżmy teraz nie wprost, że istnieje rozwiązanie, w którym $x > 0$, i rozważajmy dalej jedno z rozwiązań, w których x przyjmuje wartość dodatnią najmniejszą z możliwych. Udowodnimy przede wszystkim, że wówczas

$$(x, y) = (x, z) = (y, z) = 1. \tag{2}$$

((a, b) oznacza największy wspólny dzielnik liczb całkowitych a, b.) Niech $\mathbb{P} = \{2, 3, 5, \ldots\}$ oznacza dalej zbiór wszystkich liczb pierwszych. Załóżmy, że istnieje takie $q \in \mathbb{P}$, że $x = qx_1$, $y = qy_1$ dla pewnych $x_1, y_1 \in \mathbb{N}_0$, przy czym $x_1 > 0$. Po podstawieniu tych wartości do równania (1) otrzymujemy

$$q^4(x_1^4 - 2y_1^4) = 7z^2$$

i stąd dostajemy, że $z = q^2 z_1$, gdzie $z_1 \in \mathbb{N}_0$ (również dla $q = 7$). Liczby x_1, y_1, z_1 spełniają zatem równanie (1), przy czym $0 < x_1 = x/q < x$, sprzeczność z wyborem x. Udowodniliśmy więc, że $(x, y) = 1$. Analogicznie wykazujemy, że $(x, z) = (y, z) = 1$. Z (1) i (2) wynika, że wszystkie liczby x, y, z są nieparzyste. Rzeczywiście, gdyby x była parzysta, to z (1) wynika, że również z byłaby parzysta, skąd $(x, z) \geqslant 2$, sprzeczność z (2). Podobnie z jest nieparzysta. Gdyby y była parzysta to mielibyśmy kongruencję

$$x^4 \equiv 7z^2 \pmod 8,$$

ale to nie jest możliwe, gdyż kwadrat liczby nieparzystej przystaje do 1 mod 8:

$$(2k+1)^2 = 4k(k+1) + 1 = 8m + 1, \quad \text{gdzie } m \in \mathbb{N}_0.$$

Zatem y jest również nieparzysta. Wykażemy teraz, że

$$z \equiv \pm 1 \pmod 8. \tag{3}$$

Jeśli $z = 1$, to (3) oczywiście zachodzi. Gdy $z > 1$, rozpatrujemy dowolny dzielnik pierwszy p liczby z. Mamy $p \neq 2$ oraz z równania (1) wynika kongruencja

$$x^4 - 2y^4 \equiv 0 \pmod p.$$

Ponieważ $z \equiv 0 \pmod p$, więc $y \not\equiv 0 \pmod p$ na mocy (2). Niech t będzie takie, że $yt \equiv 1 \pmod p$. Wówczas

$$(xt)^4 \equiv 2(yt)^4 \equiv 2 \pmod p,$$

czyli kongruencja $r^2 \equiv 2 \pmod p$ ma rozwiązanie, np. $r = (xt)^2$. Teraz trzeba przywołać słynne twierdzenie z teorii reszt kwadratowych. Jako pierwszy udowodnił je Gauss:

Jeśli $p \in \mathbb{P} \setminus \{2\}$, to kongruencja $r^2 \equiv 2 \pmod p$ ma rozwiązanie wtedy i tylko wtedy, gdy $p \equiv \pm 1 \pmod 8$.

Rozwiązanie zadania F 1002.
Gdyby do Ziemi nie docierał strumień energii ze Słońca, to temperatura jej powierzchni miałaby wartość, przy której strumień energii dopływającej z wnętrza Ziemi byłby równy strumieniowi energii wypromieniowanej.
Wartość strumienia ciepła dostarczanego w procesie przewodnictwa cieplnego wynosi

$$q_p = \lambda \frac{dT}{dx},$$

gdzie x oznacza głębokość. Strumień energii wypromieniowanej z powierzchni:

$$q_w = \sigma T^4.$$

Drugie równanie opisuje promieniowanie ciała doskonale czarnego i w przypadku powierzchni ciał „rzeczywistych” jego prawą stronę należy pomnożyć przez zdolność emisyjną powierzchni α. Dla powierzchni Ziemi α jest bliskie 1, a dla materiałów tworzących skały powierzchniowe mieści się w granicach $1 > \alpha > 0{,}2$.
Przyjmijmy $\alpha = 1$ oraz $dT/dx = 30$ K/km. Równość obu strumieni energii prowadzi do oszacowania:

$$T = \left(\frac{q_p}{\sigma}\right)^{1/4} \approx 32\ \text{K}.$$

Uwzględnienie zdolności emisyjnej powierzchni wprowadziłoby dodatkowy czynnik równy co najwyżej $5^{1/4} \approx 1{,}5$, a więc prowadzi do co najwyżej $T \approx 48$ K.

Dominującym źródłem energii we wnętrzu Ziemi są najprawdopodobniej rozpady jąder ^{232}Th o czasie połowicznego rozpadu $\tau \approx 14 \cdot 10^9$ lat, ^{238}U, $\tau \approx 4{,}47 \cdot 10^9$ lat oraz ^{40}K, $\tau \approx 1{,}25 \cdot 10^9$ lat.

Podsumujmy: liczba z jest iloczynem swoich czynników pierwszych p, a zatem (3) zachodzi. Skoro $z = 8k \pm 1$, więc $z^2 = 16(4k^2 \pm k) + 1$, czyli $z^2 \equiv 1 \pmod{16}$. Z podobnych powodów $x^4 \equiv 1 \equiv y^4 \pmod{16}$. Zatem lewa L i prawa P strona równania (1) spełniają następujące kongruencje:

$$L \equiv 1 - 2 \cdot 1 \equiv 15 \pmod{16}, \quad P \equiv 7 \cdot 1 \equiv 7 \pmod{16},$$

co daje upragnioną sprzeczność.

Jedynym rozwiązaniem równania (1) w liczbach całkowitych jest więc trójka $x = y = z = 0$. W finale dowodu rozstrzygającą rolę odegrały rozważania modulo 16. Nie jest jednak prawdą, że kongruencja

$$x^4 - 2y^4 \equiv 7z^2 \pmod{16}$$

nie ma rozwiązań w liczbach nieparzystych. Wystarczy wziąć $x = 1$, $y = 1$, $z = 3$.

Nie jest to przypadek. W pozostałej części artykułu pokażemy, że dla każdej liczby $m > 1$ istnieją liczby całkowite x, z spełniające kongruencję

$$x^4 - 2 \equiv 7z^2 \pmod{m}. \tag{4}$$

Oznacza to, że strategia dowodu, że równanie (1) nie ma całkowitych rozwiązań poza $x = y = z = 0$, polegająca na szukaniu liczby m, dla której kongruencja

$$x^4 - 2y^4 \equiv 7z^2 \pmod{m}$$

nie ma rozwiązań x, y, z spełniających $(x, y, z, m) = 1$, nie może się powieść.

Z twierdzenia chińskiego o resztach wynika, że można się ograniczyć do przypadku, gdy $m = p^k$, gdzie $p \in \mathbb{P}$. Najpierw rozpatrzmy przypadek $p = 2$ i połóżmy $x = 1$. Wykażemy, że dla każdego $k \geqslant 1$ istnieje z_k spełniające kongruencję

$$7z_k^2 + 1 \equiv 0 \pmod{2^k}. \tag{5}$$

Dla $k \leqslant 3$ bierzemy $z_k = 1$. Załóżmy teraz, że dla pewnego $k \geqslant 3$ istnieją takie z_k, t_k, że $7z_k^2 + 1 = t_k \cdot 2^k$. Wykażemy, że istnieją takie z_{k+1}, t_{k+1}, że $7z_{k+1}^2 + 1 = t_{k+1} \cdot 2^{k+1}$. Niech $z_{k+1} = z_k + u_k 2^{k-1}$, gdzie u_k dobierzemy za chwilę. Modulo 2^{k+1} mamy

$$\begin{aligned} 7z_{k+1}^2 + 1 = 7(z_k + u_k 2^{k-1})^2 + 1 \equiv \\ \equiv 7z_k^2 + 1 + u_k \cdot 7z_k 2^k = 2^k(t_k + u_k \cdot 7z_k). \end{aligned}$$

Liczbę u_k dobieramy tak, aby prawa strona powyższego wzoru była podzielna przez 2^{k+1}:

$$u_k = \begin{cases} 0 \text{ gdy } t_k \equiv 0 \pmod{2}, \\ 1 \text{ gdy } t_k \equiv 1 \pmod{2}. \end{cases}$$

To działa, gdyż $7z_k$ jest nieparzyste.

Zajmiemy się teraz kongruencją (4) dla $m = p^k$, gdzie $p \in \mathbb{P} \setminus \{2, 7\}$. Dla $x = 0, 1, 2$ otrzymujemy odpowiednio kongruencje

$$7z^2 \equiv -2 \pmod{p^k}, \quad 7z^2 \equiv -1 \pmod{p^k}, \quad 7z^2 \equiv 14 \pmod{p^k}.$$

Niech t spełnia warunek $7t \equiv 1 \pmod{p^k}$. Powyższe kongruencje są równoważne następującym:

$$z^2 \equiv -2t \pmod{p^k}, \quad z^2 \equiv -t \pmod{p^k}, \quad z^2 \equiv 2 \pmod{p^k}. \tag{6}$$

Ponieważ zredukowana grupa reszt modulo p^k jest cykliczna oraz

$$(-2t)(-t) \cdot 2 = (2t)^2,$$

więc przynajmniej jedna z kongruencji (6) ma rozwiązanie z (jedna lub wszystkie). W istocie chodzi tu o to, że iloczyn niereszt kwadratowych jest resztą kwadratową itd. Czytelnikowi pozostawiamy przypadek $m = 7^k$.

Podobną własność jak równanie (1) mają równania

$$3x^3 + 4y^3 + 5z^3 = 0 \quad \text{[E. Selmer, 1951]},$$
$$x^4 - 17y^4 = 2z^2 \quad \text{[H. Reichardt, 1942]}.$$

Były to w zasadzie pierwsze przykłady nietrywialnych równań diofantycznych, które nie spełniają *zasady lokalno-globalnej*, czyli nie mają nietrywialnych rozwiązań wymiernych, mimo że odpowiednie kongruencje mod m mają nietrywialne rozwiązania dla każdej liczby $m > 1$. Nie ma takich równań

Rozwiązanie zadania F 1001.
Temperatura powierzchni planety ustala się, gdy wartość strumienia energii docierającej do jej powierzchni równa się wartości energii wypromieniowanej. Ilość energii docierającej do Ziemi od Słońca w jednostce czasu to:

$$q_S = \pi(1 - A_Z)R^2 S,$$

gdzie R oznacza promień Ziemi. Przyjmując, że Ziemia promieniuje jak ciało doskonale czarne o temperaturze T_Z, jej powierzchnia wypromieniowuje w jednostce czasu energię równą:

$$q_w = 4\pi R^2 \sigma T_Z^4.$$

Równość obu strumieni prowadzi do wniosku, że:

$$T_Z = \left(\frac{(1 - A_Z)S}{4\sigma}\right)^{1/4} \approx 254 \text{ K}.$$

Dla Marsa, poza inną wartością albedo, należy uwzględnić większą odległość od Słońca:

$$T_M = \left(\frac{(1 - A_M)Sa_z^2}{4\sigma a_M^2}\right)^{1/4} \approx 208 \text{ K}.$$

Mierzone średnie temperatury powierzchni wynoszą odpowiednio $T_Z = 288$ K i $T_M = 210$ K. Duża różnica obliczonej i mierzonej temperatury dla Ziemi jest wynikiem istnienia atmosfery (ciśnienie „atmosferyczne” na Marsie wynosi 0,006 atm) i związanego z nią efektu cieplarnianego.