Konstrukcje w zadaniach z teorii liczb

*Navid SAFAEI**

* Dyrektor oddziału Matematyka Olimpijska w Salam Schools Complex, Teheran, Iran
Instytut Matematyki i Informatyki, Bułgarska Akademia Nauk, Sofia

Jak to? Przecież zadania konstrukcyjne dotyczą *geometrii*! To prawda, ale nie o zastosowaniu cyrkla i linijki będzie tu mowa. Naszym zadaniem będzie konstruowanie przykładów, a często nawet nieskończonego zbioru przykładów, dla pytań natury teorioliczbowej. Inspiracją do napisania tego tekstu było drugie zadanie z ubiegłorocznej Międzynarodowej Olimpiady Matematycznej (IMO).

Zadanie 1 (IMO 2024, Problem 2)**.** Wyznaczyć wszystkie pary (a, b) liczb całkowitych dodatnich, dla których istnieją takie liczby całkowite dodatnie g i N, że

$$\operatorname{nwd}(a^n + b, b^n + a) = g$$

dla wszystkich $n \geqslant N$.

Przez $\operatorname{nwd}(x, y)$ oznaczamy oczywiście największy wspólny dzielnik liczb x oraz y.

Nietrudno przekonać się, że $a = b = 1$ spełniają powyższy warunek. Czy istnieją jednak inne przykłady? Okazuje się, że nie, co można uzasadnić, powołując się na to, że pewien powiązany problem ma *nieskończenie wiele rozwiązań*. I właśnie tego typu zagadnieniom przyjrzymy się poniżej (przy okazji rozwiązując powyższe zadanie z IMO). Do dzieła!

Zadanie 2. Niech N będzie daną liczbą całkowitą dodatnią. Udowodnij, że istnieją parami względnie pierwsze liczby całkowite dodatnie $a, b, c > N$, takie że liczby $a + b + c$ oraz $ab + bc + ac$ mają te same dzielniki pierwsze.

Rozwiązanie. Pokażemy, jak skonstruować dowolnie duże liczby a, b, c takie, że

$$\frac{ab + ac + bc}{a + b + c} = 3^K$$

dla pewnej liczby całkowitej dodatniej K, oraz $a + b + c$ jest podzielne przez 3. Liczby te będą oczywiście spełniały warunki zadania.

Zachodzi równość:

$$\frac{ab + ac + bc}{a + b + c} = a + b - \frac{a^2 + ab + b^2}{a + b + c}.$$

Będziemy wybierali c takie, że $\frac{a^2+ab+b^2}{a+b+c} = 1$, czyli $c = a^2 + b^2 + ab - a - b$. Wystarczy dalej szukać względnie pierwszych liczb a, b takich, że $a + b - 1 = 3^K$ (oraz $3 \mid a + b + c$).

Istnieje nieskończenie wiele liczb pierwszych dających resztę 2 z dzielenia przez 3, co nietrudno wywnioskować z faktu, że każda liczba dająca resztę 2 z dzielenia przez 3 musi mieć dzielnik pierwszy o tej własności.
W ogólnej sytuacji kwestie tego typu rozstrzyga twierdzenie Dirichleta: dla względnie pierwszych r i d istnieje nieskończenie wiele liczb pierwszych dających resztę r z dzielenia przez d.

Niech $a > N$ będzie liczbą pierwszą spełniającą $a \equiv 2 \pmod 3$. Niech liczba K spełnia nierówność $3^K + 1 > 2a$. Wówczas liczba $b = 3^K + 1 - a$ jest większa od a (więc również od N) oraz daje resztę 2 z dzielenia przez 3. Możemy ponadto założyć, że liczba $3^K + 1$ nie jest podzielna przez a, gdyż w przeciwnym wypadku $3^{K+1} + 1 = 3(3^K + 1) - 2$ nie jest podzielne przez a i moglibyśmy pod K podstawić $K + 1$. Przy takim założeniu liczba b nie może być podzielna przez a, zatem jest z nią względnie pierwsza.

Przypuśćmy, że liczby b i c mają wspólny dzielnik pierwszy p. Zgodnie z definicją c liczba p musiałaby wtedy dzielić $a^2 - a = a(a - 1)$. Ponieważ a i b są względnie pierwsze, to musiałoby zachodzić $p \mid (a - 1)$, a skoro $(a - 1) + b = 3^K$, otrzymalibyśmy $p \mid 3^K$, czyli $p = 3$. Jest to jednak sprzeczność, gdyż $b \equiv 2 \pmod 3$. Analogicznie dowodzimy, że $\operatorname{nwd}(a, c) = 1$.

Polecamy Czytelnikowi zastanowienie się nad tym, dlaczego w tym rozwiązaniu nie moglibyśmy rozważyć liczby 2^K zamiast 3^K.

Pozostaje zauważyć, że jeśli $a \equiv b \equiv 2 \pmod 3$, to liczba $a + b + c = a^2 + ab + b^2$ jest podzielna przez 3. □

Zadanie 3. Udowodnij, że dla każdej liczby całkowitej dodatniej n istnieje $2n$ takich parami różnych liczb całkowitych dodatnich $a_1, \ldots, a_{2n}$, że dla dowolnych i, j spełniających $1 \leqslant i < j \leqslant 2n$ zachodzi

$$(a_i^k + a_j^k) \mid (a_i^{k+1} + a_j^{k+1}) \quad \text{dla } k = 1, 2, \ldots, n.$$

Rozwiązanie. Niech $x_1, \ldots, x_{2n}$ będą różnymi liczbami całkowitymi dodatnimi, określmy ponadto:

$$D = \prod_{1 \leqslant i < j \leqslant 2n} \prod_{1 \leqslant k \leqslant n} (x_i^k + x_j^k)$$

oraz $a_i = Dx_i$ dla $i = 1, \ldots, n$. Oczywiście $x_i^k + x_j^k \mid D$, zatem $D^k(x_i^k + x_j^k) \mid D^{k+1}$, więc tym bardziej $D^k(x_i^k + x_j^k) \mid D^{k+1}(x_i^{k+1} + x_j^{k+1})$. Lewa strona tej podzielności to $a_i^k + a_j^k$, zaś prawa to $a_i^{k+1} + a_j^{k+1}$, co kończy uzasadnienie. □

W kolejnych zadaniach będziemy stosować *małe twierdzenie Fermata*, zgodnie z którym jeśli p jest liczbą pierwszą oraz $p \nmid a$, to $a^{p-1} \equiv 1 \pmod{p}$. W prosty sposób wynika stąd, że jeśli $x \equiv y \pmod{p-1}$, to $a^x \equiv a^y \pmod{p}$.

Eleganckie uzasadnienie małego twierdzenia Fermata można znaleźć w krótkim tekście Tomasza Kazany w Δ_{17}^4.

Zadanie 4. Niech a, b będą liczbami całkowitymi dodatnimi, przy czym $a > 1$. Udowodnij, że istnieje nieskończenie wiele takich liczb całkowitych dodatnich n, że $n^b + 1$ nie dzieli $a^n + 1$.

Rozwiązanie. Niech p będzie liczbą pierwszą dzielącą $(2a)^b + 1$, wtedy oczywiście $\operatorname{nwd}(p,\ 2a) = 1$. Ustalmy dowolnie $\ell > \frac{2a}{p}$ i przyjmijmy $n = (p-1)(\ell p - 2a)$. Wtedy $n \equiv 2a \pmod{p}$, a zatem

$$n^b + 1 \equiv (2a)^b + 1 \equiv 0 \pmod{p}.$$

Jednocześnie $(p-1) \mid n$, więc na mocy małego twierdzenia Fermata mamy $a^n + 1 \equiv 2 \pmod{p}$, co wyklucza podzielność $a^n + 1$ przez $n^b + 1$ i kończy rozwiązanie. □

Kolejny problem jest mocno związany z problemem z IMO 2024, od którego zaczęliśmy ten artykuł.

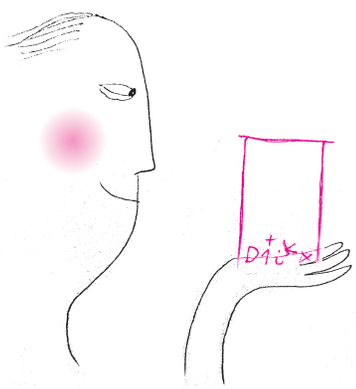
Zadanie 5. Niech a, b, c będą liczbami naturalnymi. Udowodnij, że istnieje nieskończenie wiele liczb całkowitych dodatnich k takich, że

$$\operatorname{nwd}(a^k + bc,\ c^k + ab,\ b^k + ac) > 1.$$

Rozwiązanie. Niech p będzie liczbą pierwszą dzielącą $1 + abc$. Wówczas p nie dzieli żadnej z liczb a, b, c. Wybierzmy $k = \ell(p-1) - 1$ dla pewnej liczby całkowitej dodatniej ℓ. Wtedy zgodnie z małym twierdzeniem Fermata

$$a(a^k + bc) = a^{k+1} + abc \equiv 1 + abc \equiv 0 \pmod{p}.$$

Ponieważ $p \nmid a$, więc $p \mid (a^k + bc)$. To samo dotyczy $c^k + ab$ oraz $b^k + ac$, stąd p dzieli $\operatorname{nwd}(a^k + bc,\ c^k + ab,\ b^k + ac)$. □



Powyższe rozważania mogą nas naprowadzić na rozwiązanie **Zadania 1**. Wstawiając $c = 1$ w rozumowaniu wyżej, a następnie przyjmując za p dowolny dzielnik pierwszy liczby $1 + ab$, otrzymujemy, że p dzieli $a^k + b$ i $b^k + a$ dla nieskończenie wielu wykładników k.

Załóżmy, że $(a, b) \neq (1, 1)$, i przypuśćmy, że istnieją N i g takie, że dla dowolnego $n \geqslant N$ zachodzi $\operatorname{nwd}(a^n + b, b^n + a) = g$. W połączeniu z poprzednią obserwacją oznaczałoby to, że p dzieli g. Zwróćmy uwagę, że reszty z dzielenia pary (a^n, b^n) przez p powtarzają się cyklicznie z okresem $p - 1$. Skoro więc p dzieli $\operatorname{nwd}(a^n + b, b^n + a)$ dla wszystkich $n \geqslant N$, to jest to prawdą dla dowolnego $n \geqslant 0$.

Podstawiając $n = 0$ i $n = 1$, otrzymujemy, że $a+1, b+1, a+b$ są podzielne przez p. Zatem p dzieli również $2b = (a+b) - (a+1) + (b+1)$. Skoro p jest względnie pierwsze z b, to $p = 2$, a więc $ab + 1 = 2^t$ dla pewnej liczby całkowitej dodatniej t, a skoro $(a, b) \neq (1, 1)$, musi być $t \geqslant 2$, czyli $4 \mid ab + 1$. Analiza reszt z dzielenia przez 4 liczb a i b prowadzi do wniosku, że a i b to liczby nieparzyste spełniające $b \equiv -a \pmod{4}$. Przeczy to założeniom zadania, ponieważ $\operatorname{nwd}(a^n + b, b^n + a)$ dla n nieparzystego jest podzielne przez 4, a dla n parzystego nie jest. □

W rozwiązaniu zadania 4 potrafiliśmy wskazać dowolnie duże liczby n, które są podzielne przez $p-1$ i dawały zadaną resztę $2a$ z dzielenia przez p. Obserwację tę uogólnia następujący

Lemat. Niech a, x, y będą dowolnymi liczbami naturalnymi, przy czym $a \geqslant 1$. Wówczas istnieje nieskończenie wiele liczb naturalnych n, dla których $n \equiv x \pmod{a}$ oraz $n \equiv y \pmod{a-1}$.

Czytelnicy znający chińskie twierdzenie o resztach z pewnością zauważą, że nasz lemat jest jego szczególnym przypadkiem. Tym, którzy nie znają tego twierdzenia i chcieliby zmienić ten stan rzeczy, polecamy krótki artykuł *Resztki* z Δ^4_{18}.

Dowód. Nietrudno sprawdzić, że dla dowolnej liczby całkowitej ℓ liczba

$$n = x + (y-x)a + \ell a(a-1)$$

daje resztę x z dzielenia przez a oraz resztę y z dzielenia przez $a-1$. Aby zachodziło $n \geqslant 0$, wystarczy wziąć dowolne $\ell \geqslant x$. □

Powyższy lemat wykorzystamy w rozwiązaniu kolejnych dwóch zadań.

Zadanie 6. Niech a, b będą dodatnimi liczbami całkowitymi. Udowodnij, że istnieje nieskończenie wiele liczb całkowitych dodatnich n takich, że

$$\operatorname{nwd}(a^n + n^b,\ b^n + n^a) > 1.$$

Rozwiązanie. Jeśli $\operatorname{nwd}(a,b) = D > 1$, to dla $n = Dk$, gdzie k jest dowolną liczbą całkowitą dodatnią, obie liczby $a^n + n^b$ oraz $b^n + n^a$ są podzielne przez D. Załóżmy teraz, że $\operatorname{nwd}(a,b) = 1$ oraz $a \geqslant b$. Niech p będzie liczbą pierwszą dzielącą $a^a + b^b$. Zgodnie z lematem istnieje nieskończenie wiele liczb całkowitych dodatnich $n \geqslant 0$ spełniających

$$n \equiv ab \pmod{p} \quad \text{oraz} \quad n \equiv a+b \pmod{p-1}.$$

Wtedy, znów powołując się na małe twierdzenie Fermata,

$$a^n + n^b \equiv a^{a+b} + (ab)^b \equiv a^b(a^a + b^b) \equiv a^a + b^b \equiv 0 \pmod{p},$$

skąd dostajemy $p \mid a^n + n^b$. Analogicznie dowodzimy $p \mid b^n + n^a$. □

Zadanie 7. Niech $a \geqslant 1$ oraz $b \geqslant 2$ będą danymi liczbami całkowitymi dodatnimi. Udowodnij, że nie istnieje żaden taki niezerowy wielomian $f(x)$ o współczynnikach całkowitych, że dla każdej liczby całkowitej dodatniej n mamy $\operatorname{nwd}(f(n^a), f(b^n)) = 1$.

Rozwiązanie. Załóżmy przeciwnie: istnieje wielomian $f(x)$ o współczynnikach całkowitych o takiej własności, że dla każdej liczby całkowitej dodatniej n mamy $\operatorname{nwd}(f(n^a), f(b^n)) = 1$. Wynika z tego, że $\operatorname{nwd}(f(b^a), f(b^b)) = 1$. Stąd b jest względnie pierwsze z wyrazem wolnym wielomianu f, czyli $\operatorname{nwd}(b, f(0)) = 1$. Ustalmy m, a następnie wybierzmy dzielnik pierwszy p liczby $f(b^{am})$. Zachodzi wówczas $\operatorname{nwd}(p,b) = 1$. Na mocy lematu istnieje taka dodatnia liczba całkowita n, że $n \equiv b^m \pmod{p}$ i $n \equiv am \pmod{p-1}$. Wówczas

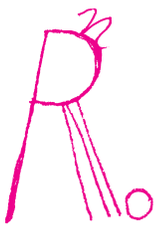
$$f(n^a) \equiv f(b^{ma}) \equiv 0 \pmod{p}.$$

Z drugiej strony, $f(b^{ma}) \equiv f(b^n) \pmod{p}$, stąd $p \mid \operatorname{nwd}(f(n^a), f(b^n))$. Uzyskana sprzeczność kończy dowód. □

Nasz przegląd zadań konstrukcyjnych zakończymy następującym zadaniem.

Zadanie 8. Czy istnieje nieskończenie wiele liczb całkowitych a, b takich, że $a+b$ dzieli $a^b + b^a$?

Rozwiązanie. Cóż, najkrótsze rozwiązanie tego problemu wymaga znacznie mniej technicznych umiejętności niż rozwiązania poprzednich zadań – wystarczy bowiem „wpaść” na odpowiedni przykład. A jest nim $a = 2n-1$ oraz $b = 2n+1$ dla dowolnej nieparzystej liczby naturalnej n! Aby udowodnić podzielność $a^b + b^a$ przez $a + b = 4n$, wystarczy osobno wykazać podzielność przez 4 oraz przez n, co pozostawiamy Czytelnikowi jako nietrudne ćwiczenie. □



W tym artykule przedstawiliśmy kilka problemów wymagających teorioliczbowych konstrukcji. Jak można było zobaczyć, odrobina kreatywności w połączeniu z dobrze znanymi faktami z elementarnej teorii liczb doprowadziła nas aż na poziom olimpijski.