Największy wspólny dzielnik jako pewna kombinacja liniowa

Piotr WOJCIECHOWSKI

W chwili pisania artykułu Autor był uczniem II klasy XIV LO w Warszawie

Niezmierzone otchłanie teorii liczb wciąż przyciągają setki badaczy, chcących zaznać przyjemności poruszania się po gruncie dziedziny, którą Gauss nazwał Królową Matematyki. Spoglądając na jedno pojęcie teorii liczb, widzimy jednocześnie cały ogrom naszych możliwości budowania nowych problemów, czy nawet teorii. Może uda nam się pokazać fragmencik niekłamanego piękna tej dziedziny, tkwiący w jednym skromniutkim problemie, nad którym chcielibyśmy się tu zastanowić.

Spróbujemy udowodnić twierdzenie, które intuicyjnie nie jest zupełnie oczywiste, ale jego prawdziwość można pokazać, sięgając do zagadnień pozornie z nim nie związanych. Przed podaniem owego twierdzenia ustalimy oznaczenia oraz wspomnimy o klasach abstrakcji, za pomocą których dokonamy dowodu. Jeżeli dane są dwie liczby całkowite a i b, to ich największy wspólny dzielnik oznaczamy symbolem

$$(a, b).$$

Symbol ten ma sens tylko wtedy, gdy $a^2+b^2 > 0$.

Jeżeli dana jest relacja równoważności „$\sim$" określona w zbiorze X, to klasą abstrakcji tej relacji wyznaczoną przez $x \in X$ nazywamy zbiór $[x]$ zdefiniowany następująco:

$$[x] = \{y \in X: \quad y \sim x\}.$$

Zbiór wszystkich klas abstrakcji danej relacji równoważności określonej w zbiorze X oznaczamy $X/\sim$ (zbiór ten nazywamy przestrzenią ilorazową).

W zbiorze Z wszystkich liczb całkowitych możemy (przy założeniu, że $m \neq 0$) wprowadzić relację $\sim_m$ w następujący sposób:

$$\sim_m = \{\langle x, y\rangle : m|(x-y)\}.$$

Jest to relacja równoważności (dlaczego?), więc dzieli zbiór Z na klasy. Są to tzw. klasy modulo m. Łatwo zauważyć, że jeżeli wprowadzimy działania na klasach:

$$[x]\oplus[y] = [y+x], \quad [x]\circ[y] = [y\cdot x],$$

wówczas system $\langle Z/\sim_m, \oplus, \circ\rangle$ jest pierścieniem przemiennym z jednością. Podkreślamy dodatkowo, że zerem naszego pierścienia jest $[0]$, a jednością $[1]$.

Relacja R jest relacją równoważności, jeśli jest *zwrotna* (każdy element jest w tej relacji z samym sobą), *symetryczna* (jeśli xRy, to również yRx) oraz *przechodnia* (jeśli xRy i yRz, to xRz). Równość, dawanie tej samej reszty przy dzieleniu przez m — są przykładami relacji równoważności.

Pierścieniem przemiennym z jednością nazywa się trójka $\langle A, \oplus, \bigcirc\rangle$, gdzie A — zbiór, $\oplus$ i $\bigcirc$ — dwa działania w tym zbiorze, i przy tym spełnione są następujące warunki:
— $\oplus$ jest działaniem łącznym i przemiennym;
— istnieje taki element $0 \in A$, że dla każdego $x \in A$: $x\oplus 0 = x$,
— każdy element $x \in A$ ma element przeciwny $-x$ tzn. taki, że $x\oplus(-x) = 0$;
oraz
— $\bigcirc$ jest łączne i przemienne;
— istnieje element $I \in A$ taki, że dla każdego $x\in A: x\bigcirc I = x$; i ponadto
— Działanie $\bigcirc$ jest rozdzielne względem działania $\oplus$.
Przykładami pierścieni przemiennych z jednością są liczby rzeczywiste, liczby zespolone ze zwykłymi działaniami i przykład podany przez Autora.

Przy oznaczeniach klas abstrakcji opuściliśmy symbole relacji. Nie powinno to prowadzić do nieporozumień.

Możemy teraz przystąpić do omówienia zapowiedzianego twierdzenia.

Oto jego treść:

$$[(a,b) = n] \Leftrightarrow [n|a \wedge n|b \wedge \bigvee_{k,l\in Z} (ka+lb = n)].$$

Dowód: Dla przejrzystości prowadzonych rozumowań część „w prawo" ($\Rightarrow$) naszego twierdzenia rozważymy kolejno dla $n = 1$ i $n \neq 1$.

$1^\circ n = 1$. Zajmiemy się najpierw przypadkiem, gdy jedna z liczb a, b jest zerem. Wówczas automatycznie druga jest jednością i wystarczy przyjąć $k = l = 1$.

Obecnie załóżmy, że $a \neq 0$ i $b \neq 0$. Wprowadźmy relację $\sim_b$ i weźmy pod uwagę zbiór:

(*) $$U = \{[ta],\ t = 1, 2 \ldots, b\}.$$

Pokażemy, że

(**) $$U = Z/\sim_b.$$

Przede wszystkim zauważmy, że zbiór U jest b — elementowy — tak jak zbiór $Z/\sim_b$. Wystarczy teraz pokazać, że każde dwie klasy ze zbioru U są różne. Załóżmy przeciwnie, że dla pewnych i oraz j, $i \neq j$, zachodzi

$$[ia] = [ja].$$

Otrzymujemy:

$$[ia]\ominus[ja] = [0],$$

zatem

$$[a]\circ([i]\ominus[j]) = [0].$$

A więc $b|a\cdot(i-j)$.

Z założenia $(a, b) = 1$ wynika, że

$$b|(i-j).$$

Zatem i różni się od j o wielokrotność b, co przeczy definicji (*) zbioru U. Sprzeczność ta przekonuje nas, że każde dwa elementy zbioru U są różne, czyli że U jest zbiorem wszystkich klas modulo b. Jest to dla nas niesłychanie ważne, bo jeśli zachodzi (**), to dla każdej liczby całkowitej z znajdziemy taką klasę $[ak]$, by

$$[ak] = [z].$$

Połóżmy $z = 1$. Możemy tak dobrać liczbę k, by

$$[ak] = [1],$$

czyli, by $b|(ak-1)$.

Zatem istnieje taka liczba $-l$, że $\quad ak-1 = -lb,$

stąd $\quad ak+bl = 1.$

Czy cień jest ciekawy?
Nagrody w konkursie otrzymują:
Leonard Kasprzak z Ostrowa Wielkopolskiego
Bogusław Wasilewski z Suwałk.

2° Załóżmy teraz, że $(a, b) = n$, gdzie n jest dowolną liczbą naturalną. Jasne jest, że istnieją takie liczby α i β, że

$$a = \alpha n \wedge b = \beta n \wedge (\alpha, \beta) = 1.$$

Na mocy poprzednio udowodnionego faktu mamy dla pewnych k i l:

$$k\alpha + l\beta = 1.$$

Mnożąc tę równość stronami przez n otrzymujemy

$$ka + lb = n.$$

Przystąpimy teraz do drugiej części naszego dowodu.

$\Leftarrow$. Załóżmy, że n nie jest największym wspólnym dzielnikiem liczb a i b. tzn. że jest mniejsze od (a, b) (większe być nie może, ponieważ wtedy nie byłby spełniony warunek $n|a$ i $n|b$). Mamy więc:

$$(a, b) = n + p, \quad p > 0.$$

Niech dla pewnych k i l zachodzi:

$$ka + lb = n.$$

Podzielmy tę równość stronami przez $n+p$:

$$k\alpha + l\beta = \frac{n}{n+p},$$

gdzie α i β oznaczają ilorazy liczb a i b przez ich największy wspólny dzielnik.

Lewa strona otrzymanej równości jest całkowita, natomiast prawa nigdy nie jest całkowita, ponieważ $n > 0$.

Otrzymana sprzeczność kończy dowód naszego twierdzenia. Wiadomo, że warunek $\bigvee_{k,l} (ka + lb = n)$ można wypowiedzieć inaczej: „n jest kombinacją liniową liczb a i b". Zatem naszemu twierdzeniu nadamy taką „poważniejszą" postać:

$$[(a+b) = n] \Leftrightarrow [n|a \wedge n|b \wedge n \text{ jest kombinacją liniową liczb } a \text{ i } b].$$

Liczymy, że w wielu problemach, gdzie występować będzie największy wspólny dzielnik liczb całkowitych, przytoczone tu twierdzenie niejednokrotnie będzie pomocne.

Rozwiązanie zadania M89.

Rozróżniamy dwa przypadki: a) n jest liczbą nieparzystą, b) n jest liczbą parzystą.

a) Niech $n = 2k+1$. Wówczas przy pierwszej komendzie uczeń z numerem $k+1$ pozostaje na miejscu, a uczeń z numerem j ($j = 1, 2, \ldots, k$) zamienia się miejscem z uczniem o numerze $2k+2-j$. Otrzymujemy wtedy szereg, w którym uczniowie stoją według malejących numerów.

Na drugą komendę uczeń o numerze $2k+1$ pozostaje na miejscu, uczeń zaś o numerze i ($i = 1, 2, \ldots, k$) zamienia się miejscem z uczniem o numerze $2k+1-i$.

Uczniowie są teraz ustawieni zgodnie z treścią zadania.

b) Niech $n = 2k$. Przy pierwszej komendzie uczniowie z numerami 1 i $k+1$ pozostają na miejscu, a uczeń z numerem j ($j = 2, 3, \ldots, k$) zamienia się z uczniem o numerze $2k+2-j$.

Na drugą komendę uczeń o numerze i ($i = 1, 2, \ldots, k$) zamienia się miejscem z uczniem o numerze $2k+1-i$.

Teraz uczniowie są też ustawieni zgodnie z treścią zadania.

Rozwiązanie zadania F30.

Wprowadzamy prostokątny układ współrzędnych, jak pokazano na rysunku obok. Na pręt, w danej chwili czasu, działają następujące siły (patrz rysunek):

— siła ciężkości, $M \cdot g$, przyłożona w środku masy pręta,

— siła reakcji podłogi, N, skierowana wzdłuż osi y, przyłożona do dolnego końca pręta,

— siła reakcji ściany, T, skierowana wzdłuż osi x, przyłożona do górnego końca pręta.

Wartości N i T zmieniają się w czasie.

Ruch pręta, jako ciała sztywnego, możemy rozpatrywać jako ruch złożony z ruchu obrotowego wokół osi prostopadłej do płaszczyzny xy i przechodzącej przez środek masy pręta oraz ruchu postępowego środka masy pręta.

Równania ruchu do momentu oderwania się pręta od ściany są postaci:

(1)

ruch obrotowy: $$\frac{N \cdot L}{2} \cos\alpha - \frac{T \cdot L}{2} \sin\alpha = I \frac{d\omega}{dt},$$

ruch postępowy: $$T = M \cdot a_x$$ $$M \cdot g - N = M \cdot a_y,$$

gdzie:

I — jest momentem bezwładności pręta liczonym względem osi przechodzącej przez środek masy, $I = \frac{1}{12} M \cdot L^2$,

ω — prędkością kątową w ruchu obrotowym względem tej osi,

a_x, a_y — składowymi wektora przyspieszenia w ruchu postępowym.

Warunkiem przylegania górnego końca pręta do ściany jest występowanie siły reakcji T, czyli przyspieszenie a_x powinno być dodatnie. W momencie oderwania się końca pręta wartość a_x równa się 0. Natomiast składowa przyspieszenia a_y, zgodnie z warunkami zadania i z przyjętą konwencją współrzędnych, powinna zawsze mieć wartość ujemną.

Ponieważ siły T i N nie wykonują pracy, z zasady zachowania energii otrzymujemy następujący związek:

(2) $$\frac{M \cdot V^2}{2} + \frac{I \cdot \omega^2}{2} = M \cdot g \left(\frac{L}{2} - y\right) = M \cdot g \frac{L}{2}(1 - \sin\alpha.).$$

Z faktu ślizgania się końców pręta po podłodze i po ścianie wynikają związki między składowymi prędkości pręta w ruchu postępowym, a prędkością kątową ω. Ruch danego końca pręta rozpatrujemy jako wynik nałożenia się ruchu postępowego środka masy i ruchu obrotowego. Ponieważ dolny koniec porusza się tylko wzdłuż osi x, a górny koniec tylko wzdłuż osi y otrzymujemy:

(3) $$-V_y = \frac{\omega \cdot L}{2} \cos\alpha, \quad V_x = \frac{\omega \cdot L}{2} \sin\alpha.$$

Stąd wynika zależność: $V^2 = \frac{\omega^2 L^2}{4}$. Wykorzystując zasadę zachowania energii (2) otrzymujemy związek:

$$\frac{\omega^2 \cdot L}{3g} = 1 - \sin\alpha,$$

a następnie zależność: $$V_x = \frac{\omega \cdot L}{2}\left(1 - \frac{\omega^2 L}{3 \cdot g}\right).$$

Stąd: $$a_x = \frac{dV_x}{dt_x} = \frac{\frac{d\omega}{dt} \cdot L}{2} (3\sin\alpha - 2).$$

Widać, że górny koniec pręta oderwie się od ściany, gdy $\sin\alpha = \frac{2}{3}$.

Po oderwaniu się od ściany ruch pręta w kierunku poziomym będzie ruchem jednostajnym z prędkością $V_{x_0} = \frac{\omega_0 L}{3} = \frac{1}{3}\sqrt{g \cdot L}$. Natomiast równanie opisujące ruch środka masy w kierunku pionowym ma skomplikowaną postać matematyczną.