Twierdzenia Fermata różnej wielkości

Mariusz SKAŁBA, Warszawa*

Jest to tekst związany z odczytem wygłoszonym na LVI Szkole Matematyki Poglądowej, *Matematyzacja*, Wola Ducka, sierpień 2017.

Redakcja

Pierre de Fermat był Francuzem i żył w pierwszej połowie XVII wieku (1601–1665). Jako radca prawny praktykował w sądzie w Tuluzie na południu Francji. Naukami ścisłymi, a w szczególności matematyką, interesował się jako amator, ale wniósł potężny wkład do ich rozwoju. Szczególnie spektakularne są jego osiągnięcia w teorii liczb i o nich traktuje niniejszy artykuł. Wszyscy wiedzą, że jest Wielkie Twierdzenie Fermata (WTwF), Małe Twierdzenie Fermata (MTwF) i jeszcze inne twierdzenia Fermata dotyczące teorii liczb – ale które z nich jest największe?

Liczby fascynowały *człowieka* na długo przed Fermatem, a właściwie to już od *jego* zejścia z drzewa. Z tego długiego okresu uwzględnimy tylko Diofantosa, tworzącego (a zatem żyjącego) w starożytnej Grecji, gdyż jest on jednym z bohaterów opowiadanej historii. Najważniejszymi aktorami są jednak tytułowe twierdzenia. Oto one.

Nie jest to całkiem pewne, a na pewno nie jest do końca udokumentowane.

Małe Twierdzenie Fermata. *Jeśli n jest liczbą pierwszą oraz a jest liczbą całkowitą niepodzielną przez n, to*

$$a^{n-1} \equiv 1 \pmod{n}. \tag{1}$$

W obecnej erze komputerów małe twierdzenie Fermata bywa stosowane do sprawdzania, czy dana (duża) liczba naturalna n jest pierwsza. Zilustrujemy to na przykładzie. Niech

$$n = 2^{64} + 3 = 18446744073709551619.$$

Jak sprawdzić, czy liczba n jest pierwsza? Można, oczywiście, dzielić ją przez kolejne liczby naturalne d i czekać na przypadek, że dzielenie da się wykonać bez reszty. Wtedy $n = d \cdot n/d$ i liczba n jest, oczywiście, złożona. Wystarczy używać $d \leqslant \sqrt{n}$. W naszym przypadku $\sqrt{n} > 4 \cdot 10^9$, a zatem grozi nam wiele dzieleń z resztą, chyba że n ma mały dzielnik $d > 1$. Poniżej przedstawiono istotny fragment tabeli, w której przedstawiono reszty liczb 2^{2^k} przy dzieleniu przez n dla $k = 1, 2, 3, \ldots, 62, 63, 64$:

k	$2^{2^k} \mod n$
1	4
2	16
3	256
...	...
62	4533606947906510852
63	14661455517267343339
64	12163041602066973456

Mamy zatem

$$2^{n-1} = 2^{2^{64}} \cdot 2^2 \equiv 4 \cdot 12163041602066973456 \equiv 11758678260848790586 \not\equiv 1 \pmod{n}$$

i to na mocy małego twierdzenia Fermata kończy dowód, że n nie jest liczbą pierwszą. Proszę zauważyć, że przeprowadzone rachunki nie dają żadnego nietrywialnego dzielnika d liczby n. Używając innych metod, można wykazać, że

$$n = 467443687 \cdot 39463029637$$

jest rozkładem n na czynniki pierwsze. Niestety, są liczby złożone n, które bardzo sprytnie podszywają się pod liczby pierwsze – to tak zwane liczby Carmichaela. Liczbę złożoną n nazywamy liczbą Carmichaela, gdy dla każdej liczby całkowitej a względnie pierwszej z n zachodzi kongruencja (1). Najmniejszą taką liczbą jest $n = 561 = 3 \cdot 11 \cdot 17$ i wiadomo, że jest ich nieskończenie wiele.

*Wydział Matematyki, Informatyki i Mechaniki UW, skalba@mimuw.edu.pl

Dzieło Diofantosa istnieje ponad wszelką wątpliwość.

O MTwF można by mówić w nieskończoność – należy więc przejść do omówienia Wielkiego Twierdzenia Fermata. Na marginesie czytanej książki Diofantosa Fermat zanotował zdanie równoważne następującemu

Wielkie Twierdzenie Fermata. *Jeśli liczby całkowite dodatnie x, y, z, n spełniają warunek $n > 2$, to na pewno*

$$x^n + y^n \neq z^n.$$

Nieudane próby udowodnienia (lub obalenia) tej hipotezy były podejmowane do 1993 roku, kiedy to wreszcie pełny dowód podał Andrew Wiles z Cambridge. Wielokrotnie i wyczerpująco opisywano, jak te wysiłki przyczyniły się do rozwoju współczesnej matematyki, przynajmniej w jej części algebraicznej i geometrycznej. My ograniczymy się do zaprezentowania jednego podejścia, które dość szybko okazuje się zupełnie nieskuteczne, ale co zaskakujące, również ono wpłynęło na rozwój matematyki! Oprócz równania rozważymy także kongruencję

$$x^n + y^n \equiv z^n \pmod{q}. \tag{2}$$

Wówczas WTwF dla wykładnika $n \geqslant 3$ wynika łatwo z następującego lematu.

Lemat. *Jeśli $n \geqslant 3$, to dla nieskończenie wielu liczb pierwszych q wszystkie rozwiązania kongruencji* (2) *spełniają $xyz \equiv 0 \pmod{q}$.*

Rzeczywiście, rozważmy hipotetyczne rozwiązanie równania $x^n + y^n = z^n$ w liczbach całkowitych dodatnich i liczbę pierwszą $q > \max(x, y, z)$. Wówczas kongruencja (2) ma, oczywiście, rozwiązanie spełniające $xyz \not\equiv 0 \pmod{q}$ – ta konstatacja jest jednak sprzeczna z tezą Lematu.

Niestety, taki atak na WTwF nie może się udać! Pokażemy teraz na dwa sposoby, że powyższy Lemat nie jest prawdziwy.

Pierwszy sposób oparty jest na słynnym twierdzeniu Schura.

Twierdzenie Schura. *Załóżmy, że liczby $1, 2, \ldots, \lfloor e \cdot n! \rfloor$ podzielono na n (rozłącznych) klas. Wówczas przynajmniej jedna z tych klas zawiera dwie liczby c, b oraz ich różnicę $c - b$.*

Stosując twierdzenie Schura, wykażemy przykładowo, że Lemat nie jest prawdziwy dla $n = 7$ (dla dowolnego n rozumowanie jest analogiczne). Rozróżniamy dwa przypadki:

1. $q \not\equiv 1 \pmod{7}$. Homomorfizm $\varphi : \mathbb{Z}_q \longrightarrow \mathbb{Z}_q$ dany wzorem $\varphi(t) = t^7$ spełnia $\ker(\varphi) = \{1\}$, gdyż $7 \not| q - 1$. Zatem ϕ jest "1-1" a zatem "na". Oznacza to, że każda reszta mod q jest siódmą potęgą, a zatem kongruencja (2) ma mnóstwo nietrywialnych rozwiązań.
2. $q \equiv 1 \pmod{7}$. Tutaj załóżmy, że $q > 7!e \approx 13700,1$. Liczby $c, b \in \{1, 2, \ldots, q-1\}$ zaliczamy do tej samej klasy, gdy (z definicji) kongruencja $c \equiv bs^7 \pmod{q}$ ma rozwiązanie. Jest 7 klas (abstrakcji) i na mocy twierdzenia Schura $bs^7 - b \equiv bt^7 \pmod{q}$ dla pewnych b, s, t. Mamy więc $t^7 + 1^7 \equiv s^7 \pmod{q}$ i, oczywiście, $q \not| t \cdot 1 \cdot s$.

A oto kolejny dowód na to, że rzekoma teza Lematu nie jest prawdziwa. Tym razem rozumowanie korzysta ze słynnego oszacowania na liczbę rozwiązań kongruencji. Ogólna wersja tego oszacowania dla dowolnych gładkich rozmaitości nad ciałem skończonym, znana w ramach hipotez Weila jako hipoteza Riemanna dla rozmaitości, opierała się wysiłkom matematyków przez wiele lat. W końcu udowodnił ją w całej okazałości Pierre Deligne w 1973 roku i zastosował w tym dowodzie cały arsenał nowoczesnej geometrii algebraicznej.

Otrzymał za to Medal Fieldsa na Międzynarodowym Kongresie Matematycznym w 1978 roku.

Twierdzenie (oszacowanie Hasse–Weila dla krzywej Fermata).
Dla każdej liczby pierwszej q niech $N(q)$ oznacza liczbę rozwiązań $\neq (0,0,0)$ kongruencji (2), przy czym dwa rozwiązania (x_1,y_1,z_1), (x_2,y_2,z_2) utożsamiamy, gdy istnieje takie $t\in\mathbb{Z}$, że

$$x_2 \equiv tx_1,\ y_2 \equiv ty_1,\ z_2 \equiv tz_1 \pmod q.$$

Wówczas mamy oszacowanie

$$|N(q) - q - 1| \leqslant (n-1)(n-2)\sqrt{q}.$$

Wynika stąd natychmiast, że dla ustalonego n i dla dostatecznie dużej liczby pierwszej $q \geqslant q(n)$ istnieją rozwiązania kongruencji (2) spełniające $xyz \not\equiv 0 \pmod q$.

Po dwakroć zatem porzućmy wszelkie nadzieje na to, że WTwF można udowodnić poprzez rozważanie kongruencji. Z drugiej strony zarówno twierdzenie Schura, jak i powyższy szczególny przypadek hipotez Weila dla krzywych nad ciałami skończonymi, wywarły duży wpływ na rozwój kombinatoryki i geometrii algebraicznej. Tak więc pomysły, które całkowicie zawodzą w potencjalnie słynnym zastosowaniu, okazują swoją użyteczność jako zalążki nowych interesujących teorii.

I wreszcie jako *the last but not the least* omówimy twierdzenie Fermata bezprzymiotnikowe. Dotyczy ono przedstawialności liczb pierwszych w postaci sumy dwóch kwadratów liczb całkowitych.

Twierdzenie (Fermat). *Liczba pierwsza p jest postaci*

(3) $$p = x^2 + y^2, \quad \text{gdzie } x,y\in\mathbb{N},$$

wtedy i tylko wtedy, gdy $p=2$ lub $p\equiv 1 \pmod 4$.

Jedyna i istotna trudność w dowodzie tego twierdzenia to pokazanie, że każda liczba pierwsza p postaci $4k+1$ jest postaci (3). Czasem dopowiada się, że przedstawienie (3) jest tylko jedno, ale to jest łatwe. Powyższe wspaniałe twierdzenie Fermata jest zaczynem algebraicznej teorii liczb, jednego z ważnych działów matematyki współczesnej głównego nurtu.

Czy to sprawiedliwe, że na margines zepchnąłem informację o tym, że pierwszy dowód tego twierdzenia Fermata podał Euler po ponad stu latach? Po prostu tytuł zobowiązuje!

Mianowicie, można je sformułować tak:

- jeśli liczba pierwsza p jest postaci $4k+3$, to p jest elementem nierozkładalnym w pierścieniu $\mathbb{Z}[i] = \{a+bi | a,b\in\mathbb{Z}\}$,
- jeśli liczba pierwsza p nie jest postaci $4k+3$, to jest elementem rozkładalnym w $\mathbb{Z}[i]$, tzn.

  (4) $$p = (a+bi)(c+di), \quad \text{gdzie } a+bi, c+di \notin \{1,-1,i,-i\}.$$

Rzeczywiście, z (4) wynika, że

$$(a-bi)(c-di) = p,$$

skąd po pomnożeniu obu ostatnich wzorów stronami otrzymujemy

$$(a^2+b^2)(c^2+d^2) = p^2.$$

Ponieważ p jest liczbą pierwszą, więc musi być

$$a^2+b^2 = p = c^2+d^2.$$

Odwrotnie, jeśli $p = a^2+b^2$, to liczba p jest rozkładalna w $\mathbb{Z}[i]$, gdyż

$$p = (a+bi)(a-bi).$$

Prawa rozkładu liczb pierwszych w innych pierścieniach typu $\mathbb{Z}[\sqrt{-d}]$ wiążą się w subtelny sposób z próbami przeniesienia powyższego twierdzenia Fermata na przedstawienia typu

$$p = x^2 + dy^2.$$

Z powyżej napisanego nie wynika w żaden sposób, które z omówionych teorioliczbowych twierdzeń Fermata jest *największe*. Wierzę jednak, że każde z nich potrafi zainfekować Czytelnika teorią liczb równie mocno, a o to tylko tu chodzi.