O „wielkim twierdzeniu Fermata"

Dr Andrzej ROTKIEWICZ

Wielki matematyk angielski G. H. Hardy (zmarły w 1947 roku) napisał: „Elementarna teoria liczb powinna być uważana za jeden z najwłaściwszych przedmiotów w początkach wykształcenia matematycznego. Wymaga ona bardzo mało uprzedniej wiedzy, a przedmiot jej jest uchwytny i znajomy, metody rozumowania, które stosuje, są proste, ogólne i nieliczne, i nie ma sobie równej wśród nauk matematycznych w odwoływaniu się do naturalnej ludzkiej ciekawości". A według opinii jednego z największych matematyków w historii, którego prace leżą u podstaw wielu współczesnych działów matematyki, matematyka niemieckiego Gaussa (1777–1855), „matematyka jest królową nauk, a teoria liczb jest królową matematyki".

Przedmiotem teorii liczb są między innymi własności liczb pierwszych, a więc takich liczb naturalnych, które mają dokładnie dwa dzielniki naturalne, jak również na przykład teoria liczb zajmuje się rozwiązywaniem równań w liczbach całkowitych. Zagadnienia teorioliczbowe zawdzięczają zainteresowanie, jakie wzbudzają, nie temu, że mogą przyczynić się do postępu techniki nowoczesnej, lecz tajemnicy, jaką kryją w sobie liczby pierwsze, oraz trudnościom, jakie na przykład napotykamy przy rozwiązywaniu pewnych równań w liczbach całkowitych, których pokonanie wydaje się rzeczą niedostępną dla ludzkiej inteligencji. Teoria liczb, ta „wiecznie młoda" dziedzina matematyki, bo mająca wiele „wiecznie młodych" problemów, stanowi bardzo pociągający rezerwat dla tych, którzy chcą się odsunąć od cywilizacji współczesnej. Nie sposób w jednym artykule omówić tych wszystkich „wiecznie młodych" problemów. Zatrzymajmy się nad jednym z nich, historycznie bezsprzecznie najgłośniejszym, a zwanym „wielkim twierdzeniem Fermata".

Piotr Fermat (1601–1665) był prawnikiem z Tuluzy; matematyką zajmował się z amatorstwa. Położył on bardzo duże zasługi w teorii liczb, a ponadto jest uważany, obok Leibniza i Newtona, za jednego z twórców rachunku różniczkowego. Otóż Fermat czytając dzieło matematyka greckiego Diofantosa (Diofantos z Aleksandrii urodził się około 250 lat przed naszą erą i był pierwszym, który w sposób systematyczny zajął się rozwiązywaniem równań w liczbach całkowitych) napisał na marginesie ustępu traktującego o rozłożeniu kwadratu liczby naturalnej na sumę dwóch kwadratów liczb naturalnych notatkę następującej treści: „Tymczasem zupełnie niemożliwe jest rozłożenie sześcianu na sumę dwóch sześcianów ani potęgi czwartego stopnia na sumę dwóch potęg czwartych stopni, ani w ogóle jakiejkolwiek potęgi wyższego stopnia na sumę dwóch liczb w tejże potędze. Znalazłem istotnie zadziwiający dowód tego twierdzenia, ale brak tu miejsca, aby go umieścić". Tak więc Fermat sądził, że udowodnił twierdzenie nazwane później jego nazwiskiem. Jest to jednak mało prawdopodobne i wszyscy poważni matematycy są zdania, że Fermat dowodu poprawnego nie posiadał.

W tym miejscu należy jednak podkreślić, że próby udowodnienia „wielkiego twierdzenia Fermata" sprzyjały powstaniu i rozwojowi bardzo głębokich metod badań matematycznych. Sam Fermat rzeczywiście znalazł dowód dla $n = 4$. Dla $n = 3$ dowód znalazł Euler (1707–1783), wielki matematyk szwajcarski (wydanie zbiorowe jego dzieł obejmuje czterdzieści kilka dużych tomów; był on dziesięciokrotnie nagradzany przez Paryską Akademię Nauk), lecz jego dowód był niekompletny. Największe zasługi przy badaniu problemu Fermata położył matematyk niemiecki Kummer (1810–1893), który przy badaniu tego zagadnienia wprowadził liczby algebraiczne powstające z p-tych pierwiastków z jedności, co dało początek algebraicznej teorii liczb. Badania Kummera zostały później uogólnione przez Dedekinda i Kroneckera. Kummer zauważył zjawisko niejednoznaczności rozkładu na czynniki nierozkładalne w ciałach $Q(Z_p)$, gdzie Z_p oznacza p-ty pierwiastek z jedności. Każdy element ciała $Q(Z_p)$ jest postaci:

$$a_0 + a_1 Z_p^1 + a_2 Z_p^2 + \dots + a_{p-1} Z_p^{p-1},$$

gdzie $a_0, a_1, \dots a_{p-1}$ są liczbami wymiernymi, $Z_p = e^{\frac{2\pi i}{p}}$.

W 1850 roku opublikował Kummer pracę, w której wyróżnił w ciałach $Q(Z_p)$ tzw. liczby idealne, przy pomocy których udało mu się stworzyć namiastkę twierdzenia o jednoznacznym rozkładzie na czynniki nierozkładalne, dzięki czemu w 1850 roku zdołał udowodnić następujące twierdzenie, zwane później „twierdzeniem Kummera": Jeżeli $p > 2$ jest liczbą pierwszą regularną (liczby pierwsze regularne

nazywa się też liczbami pierwszymi Kummera), to równanie $x^p+y^p = z^p$ nie ma rozwiązań w liczbach naturalnych x, y, i z.
Liczba pierwsza $p > 2$ nazywa się regularną, jeśli

$$p^2 \nmid 1^k+2^k+ \ldots +(p-1)^k \quad \text{dla} \quad k = 2, 3, 4, \ldots, p-1.$$

Symbol $a|b$ oznacza, że a jest dzielnikiem b, zaś symbol $a \nmid b$ oznacza, że a nie jest dzielnikiem b.
Czytelnik zechce sprawdzić, że liczby 3, 5 i 7 są regularne. Spośród liczb pierwszych nie przekraczających 100 wszystkie są regularne z wyjątkiem $p = 37$, 59 i 67. Do tej pory jednak nie wiemy, czy istnieje nieskończenie wiele liczb pierwszych regularnych. W 1915 roku K. L. Jensen udowodnił, że istnieje nieskończenie wiele liczb pierwszych nieregularnych. Spośród 302 liczb pierwszych < 2000 jest tylko 118 regularnych. Dziś wiemy, że równanie Fermata $x^n+y^n = z^n$ dla $2 < n < 25\,000$ nie ma rozwiązań w liczbach naturalnych x, y i z. Ten ostatni wynik został osiągnięty przy użyciu różnych twierdzeń i maszyn matematycznych dopiero w r. 1967.
W 1908 roku matematyk P. Wolfskehl z Darmstadtu zapisał Towarzystwu Naukowemu w Getyndze sto tysięcy marek, które miały być wypłacone jako nagroda temu, kto bądź znajdzie ogólny dowód twierdzenia Fermata, bądź wykaże jego fałszywość na jednym choćby przykładzie. Mimo że po 1918 roku nagroda ta uległa dewaluacji, wiele osób (przeważnie niematematyków) ogłaszało własnym nakładem coraz to nowe, ale stale błędne dowody tego twierdzenia. Jakkolwiek zrozumienie, o co idzie w wielkim twierdzeniu Fermata, wymaga zaledwie elementarnych wiadomości z arytmetyki, nie wynika stąd jednak, że istnieje elementarny dowód tego twierdzenia. F. Lindemann (ten sam, który w 1882 roku udowodnił przestępność liczby π) opublikował w 1901 roku 17-stronicową rozprawę mającą zawierać długo poszukiwany dowód. Gdy mu wskazywano zasadniczy błąd, Lindemann nie zrażony spędził większą część następnych 7 lat na próbach usunięcia błędnej przesłanki, nie dającej się naprawić, i w roku 1907 ogłosił 13-stronicowy dowód, który jednak był pozorny wskutek drobnej omyłki na samym początku.
Chociaż Kummer nie był kandydatem do nagrody Akademii Francuskiej (złoty medal wartości 3 000 franków), ufundowanej w 1849 roku za ewentualny dowód „wielkiego twierdzenia Fermata", jemu właśnie została ta nagroda przyznana za zasługi, jakie położył w dziedzinie liczb zespolonych.
Dickson w drugim tomie swej historii teorii liczb poświęca 46 stron druku samym sformułowaniom różnych twierdzeń związanych z „wielkim twierdzeniem Fermata", wymienia ponad 300 prac napisanych na ten temat. Wśród kilkuset autorów (237) tych prac występują nazwiska tak sławnych matematyków, jak: Cauchy, Dedekind, Dirichlet, Euler, Fermat, Gauss, Hilbert, Kronecker, Kummer, Lagrange, Lebesgue, Legendre, Lindemann, Liouville, Lucas, Mertens, Mirimanoff, Poincaré, Van der Corput, Vandiver, Wieferich.
Spośród twierdzeń o elementarnym sformułowaniu warto wymienić następujące twierdzenia:
Twierdzenie Wiefericha (z roku 1909):
Jeśli istnieją liczby naturalne x, y, z spełniające równość $x^p+y^p = z^p$, gdzie p jest liczbą pierwszą > 2, $(xyz, p) = 1$, wtedy $p^2|2^p-2$.

$(n, k) = 1$ oznacza, że liczby n i k są względnie pierwsze, to znaczy nie mają wspólnego dzielnika różnego od 1.

Twierdzenie Mirimanoffa (z 1910 roku):
Przy założeniach poprzedniego twierdzenia mamy $p^2|3^p-3$.
Wniosek z twierdzenia Fürtwanglera udowodniony przez różnych autorów:
Przy założeniach twierdzenia Wiefericha mamy $p^2|a^p-a$ dla każdego a mniejszego od 44.
Korzystając z tego wniosku i maszyn matematycznych, matematyk amerykański Lehmer udowodnił, że w przypadku $(xyz,p) = 1$ „wielkie twierdzenie Fermata" jest prawdziwe dla wszystkich $p < 253\,747\,887$.
Jeśli $x^n+y^n = z^n$, $n > 2$, to oczywiście nie może być $x = y$, bo wtedy $2x^n = z^n$, co jest niemożliwe.
Udowodnimy teraz następujące twierdzenie Grunerta z roku 1856 (dowód twierdzenia Grunerta był też tematem czwartego zadania na finałach dwudziestej drugiej Olimpiady Matematycznej w 1971 roku):
Jeśli liczby naturalne x, y, z, n spełniają warunki:

$$x^n+y^n = z^n, \quad n > 2, \quad \text{to} \quad x > n \quad \text{i} \quad y > n.$$

Dowód:

Nie uszczuplając ogólności możemy założyć, że $x \leqslant y < z$.
Zatem wobec $x^n+y^n = z^n$ mamy

$$x^n = z^n-y^n = (z-y)\,(z^{n-1}+z^{n-2}y^1+ \ldots +y^{n-1}) > 1 \cdot ny^{n-1} \geqslant nx^{n-1},$$

stąd $x > n$, a ponieważ $x \leqslant y$ więc także $y > n$.

Nierówność $y > n$ można dowieść inaczej:

Ponieważ $\left(1+\dfrac{1}{n}\right)^n > 2$ dla $n = 2, 3, \ldots$, więc

$$y^n < x^n+y^n < 2y^n < \left(1+\frac{1}{n}\right)^n \cdot y^n = \left(y+\frac{y}{n}\right)^n, \text{ czyli}$$

$$y^n < z^n < \left(y+\frac{y}{n}\right)^n, \text{ skąd } y < z < y+\frac{y}{n}, \text{ i gdyby } y \leqslant n, \text{ to } y < z < y+1, \text{ co jest}$$

niemożliwe, bo nie istnieje liczba naturalna między dwiema kolejnymi liczbami naturalnymi.

Pomysł zastosowany w drugim dowodzie pozwala udowodnić następujące twierdzenie:

Jeśli $x_1^n+x_2^n+\ldots+x_k^n = t^n$, gdzie $x_1, x_2, \ldots, x_k$, t oznaczają liczby naturalne, $k \geqslant 2$ i $x_1 < x_2 < \ldots < x_k$, to $x_k > n$.

Dowód:

Wobec $x_1 < x_2 < \ldots < x_k$ jest:

$$(1) \qquad x_k \geqslant k.$$

Przypuśćmy, że $x_k \leqslant n$. Wobec (1) mamy $k \leqslant x_k \leqslant n$, skąd

$$(2) \qquad n-k+1 > 0.$$

Wobec $x_k \leqslant n$, $x_1 < x_2 < \ldots < x_k$ mamy:

$$(3) \quad x_1^n+x_2^n+\ldots+x_k^n \leqslant x_k^n+(x_k-1)^n+\ldots+[x_k-(k-1)]^n = x_k^n\left[1+\left(1-\frac{1}{x_k}\right)^n+\right.$$

$$\left.+\ldots+\left(1-\frac{k-1}{x_k}\right)^n\right] \leqslant x_k^n\left[1+\left(1-\frac{1}{n}\right)^n+\ldots+\left(1-\frac{k-1}{n}\right)^n\right].$$

Ponieważ $e^x > 1+x$, dla każdego rzeczywistego x, więc $e^{\frac{x}{n}} > 1+\dfrac{x}{n}$, skąd

$$e^x > \left(1+\frac{x}{n}\right)^n \text{ dla } n = 1, 2, \ldots;\ n > -x.$$

Zatem (3) daje

$$x_1^n+x_2^n+\ldots+x_k^n < x_k^n\left(1+\frac{1}{e}+\frac{1}{e^2}+\ldots+\frac{1}{e^{k-1}}\right) < x_k^n\left(1+\frac{1}{2}+\frac{1}{4}+\ldots\right) =$$

$$= 2x_k^n < \left(1+\frac{1}{n}\right)^n x_k^n = \left(x_k+\frac{x_k}{n}\right)^n.$$

Zatem

$$x_k^n < x_1^n+x_2^n+\ldots+x_k^n < \left(x_k+\frac{x_k}{n}\right)^n$$

i wobec

$$x_1^n+x_2^n+\ldots+x_k^n = t^n$$

mamy

$$x_k^n < t^n < \left(x_k+\frac{x_k}{n}\right)^n,$$

skąd

$$x_k < t < x_k+\frac{x_k}{n}.$$

Zatem wobec $x_k \leqslant n$ jest $x_k < t < x_k+1$, co jest oczywiście niemożliwe.

W związku z ostatnim twierdzeniem zauważmy, że Euler w 1778 roku wyraził przypuszczenie, że dla k i n naturalnych, spełniających nierówność $2 < k < n$, równanie

$$x_1^n+x_2^n+\ldots+x_k^n = x_{k+1}^n$$

nie ma rozwiązań w liczbach naturalnych $x_1, \ldots, x_{k+1}$.

Przypuszczenie to zostało obalone w 1966 roku.

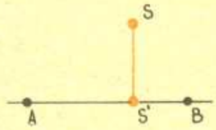
Mamy mianowicie

$$27^5+84^5+110^5+133^5 = 144^5.$$

Wynik ten został uzyskany przy pomocy maszyny OCD-66000, która to maszyna sprawdziła też, że każda piąta potęga mniejsza od 144^5 nie jest sumą czterech piątych potęg liczb naturalnych. Przypuszczenie Eulera po 188 latach zostało w ten sposób obalone. A może podobny los czeka „wielkie twierdzenie Fermata"? Nie wiadomo.

Rozwiązanie zadania M. 30

Zauważmy najpierw, że szkoła powinna być wybudowana na prostej przechodzącej przez A i B, gdyż w przeciwnym przypadku, przy umieszczeniu jej w punkcie S byłoby oczywiście $AS' < AS$ i $S'B < SB$, a więc i $60AS'+90S'B < 60AS+90SB$.



Nie może też ona leżeć zewnątrz odcinka AB. Niech odległość AB wynosi a, zaś odległość od A do szkoły — x. Wszystkie dzieci przebywają więc w drodze do szkoły odległość $60x+90(a-x) = 90a-30x = f(x)$. Funkcja $f(x)$ jest malejąca, a więc najmniejszą wartość przyjmuje dla możliwie największego x, to znaczy dla $x = a$. Szkołę więc należy wybudować we wsi B. Zauważmy, że gdyby liczby dzieci mieszkających w obydwu wioskach były równe, to szkołę można byłoby wybudować w dowolnym punkcie między A i B.

Czytelnik zechce się zastanowić, jak wygląda rozwiązanie analogicznego zadania w przypadku trzech wiosek.