Co udowodnił Preda Mihăilescu?

Jerzy BROWKIN

1. Liczbę naturalną nazywamy **potęgą**, jeżeli ma postać n^d, gdzie liczby n i d są naturalne i $d \geqslant 2$. W szczególności każdy kwadrat liczby naturalnej jest potęgą. Na przykład wszystkie potęgi mniejsze od 100 to: 1, $4=2^2$, $8=2^3$, $9=3^2$, $16=2^4=4^2$, $25=5^2$, $27=3^3$, $32=2^5$, $36=6^2$, $49=7^2$, $64=2^6=4^3=8^2$, $81=3^4=9^2$. Widać od razu, że większość potęg tu wypisanych to kwadraty i że wśród tych potęg tylko 8 i 9 są kolejnymi liczbami naturalnymi.

2. Od dawna bezskutecznie poszukiwano innych kolejnych liczb naturalnych, które są potęgami i w 1844 roku E. Catalan sformułował przypuszczenie, że liczb takich nie ma. Chodzi więc o dowód, że równanie

$$x^m - y^n = 1 \tag{1}$$

nie ma rozwiązań w liczbach naturalnych m, n, x, y, gdzie $m \geqslant 2$, $n \geqslant 2$, różnych od $x = n = 3$, $y = m = 2$. Oczywiście wystarczy ograniczyć się do przypadku, gdy m i n są liczbami pierwszymi, podobnie jak przy badaniu równania Fermata $x^n + y^n = z^n$ można przyjąć, że liczba n jest pierwsza.

3. Rozpatrywano różne przypadki szczególne równania (1) i uzyskano pewne wyniki częściowe. Na przykład udowodniono, że żadne z następujących równań nie ma rozwiązań (poza $3^2 - 2^3 = 1$), gdzie $x, y \geqslant 1, m, n \geqslant 2$:

$3^m - 2^n = \pm 1$	(Lewi ben Gerson (1288–1344)),
$x^2 - y^3 = \pm 1$	(L. Euler, 1738),
$x^m - y^2 = 1$	(V.A. Lebesgue, 1850),
$x^2 - y^n = 1$	(Chao Ko, 1965).

Korzystając z wyników Lebesgue'a i Chao Ko, można więc przyjąć, że wykładniki m i n w równaniu (1) są liczbami pierwszymi nieparzystymi.

4. Udowodniono też kilka ważnych własności hipotetycznego rozwiązania równania (1), które znacznie ograniczyły możliwość istnienia takiego rozwiązania. Mianowicie

Twierdzenie 1 (J.W.S. Cassels, 1953, 1960). *Jeżeli liczby naturalne x, y i liczby pierwsze nieparzyste p, q spełniają równanie*

$$x^p - y^q = 1, \tag{2}$$

to p dzieli y i q dzieli x.

Twierdzenie 2 (R. Tijdeman, 1976). *Istnieje taka stała C, że każde rozwiązanie równania* (1) *spełnia $m, n, x, y < C$.*

5. Z twierdzenia Tijdemana wynika oczywiście, że liczba rozwiązań równania (1) jest skończona. Niestety oszacowania stałej C występującej w tym twierdzeniu były zbyt duże, co nie pozwalało na przeszukanie wszystkich możliwych liczb m, n, x, y przy użyciu komputerów. Na przykład udowodniono, że każde rozwiązanie równania (2) spełnia

$$x, y < \exp(\exp(\exp(\exp(730)))) \quad \text{(M. Langevin, 1976)},$$

gdzie $\exp(t) = \mathrm{e}^t$, i $\mathrm{e} = 2{,}71828\ldots$ jest podstawą logarytmów naturalnych, oraz

$$p,\ q < 1{,}6 \cdot 10^{26} \quad \text{(M. Mignotte, 1992)}.$$

Oszacowania te potem były ulepszane, lecz ciągle były zbyt duże.

6. Udowodniono też, posługując się komputerami, że w poszukiwanym rozwiązaniu równania (2) wykładniki nie mogą być zbyt małe:

$$p > 10^5 \quad \text{i} \quad q > 10^5 \tag{3}$$

(K. Inkeri (1964, 1990) oraz M. Mignotte i Y. Roy (1995, 1997)). W 1999 roku P. Mihăilescu udowodnił, że zachodzą podzielności $p^2 \mid q^{p-1} - 1$ i $q^2 \mid p^{q-1} - 1$, co pozwoliło znacznie rozszerzyć obliczenia przy użyciu komputerów. Wykorzystując to M. Mignotte wzmocnił warunek (3) do następującej postaci: $p > 10^7$ i $q > 10^7$. Otrzymano też wiele innych warunków, które musi spełniać hipotetyczne rozwiązanie p, q, x, y równania (2). Miały one postać nierówności lub podzielności. Na przykład: $x > 4pq^p$ oraz $p^{q-1} \mid x - 1$. Warunki te ciągle jeszcze nie wystarczały do sprawdzenia, że równanie (2) nie ma rozwiązań poza $3^2 - 2^3 = 1$.

7. Dopiero w 2002 roku P. Mihăilescu zastosował z powodzeniem inną metodę badania rozwiązań równania (2), która w połączeniu z dotychczasowymi wynikami omówionymi wyżej i pewnymi ich ulepszeniami pozwoliła udowodnić, że poszukiwanych rozwiązań nie ma.

8. Omówienie metod użytych przez Mihăilescu wykracza poza zakres wiadomości, którymi rozporządza przeciętny czytelnik *Delty*. Zainteresowanych odsyłam więc do prac oryginalnych, a tu tylko wspomnę, że z równaniem (2) Mihăilescu wiąże tak zwany pierścień grupowy $\mathcal{F}_q[G]$ grupy cyklicznej G mającej $(p-1)/2$ elementów o współczynnikach w q-elementowym ciele $\mathcal{F}_q$. Gdyby istniało poszukiwane rozwiązanie równania (2), to ideały tego pierścienia grupowego miałyby pewną własność. Z drugiej strony, bezpośrednio dowodzi się, że tej własności nie mają. Otrzymujemy więc sprzeczność, a zatem poszukiwane rozwiązanie nie istnieje.

Tak więc po 158 latach hipoteza Catalana została udowodniona i to w stosunkowo prosty sposób.

9. Czytelników pragnących dokładniej zapoznać się z historią badania hipotezy Catalana odsyłam do książki Paulo Ribenboima *Catalan's Conjecture,* Academic Press 1994 (liczy ona ponad 350 stron!), w której omówione zostały szczegółowo wyniki na ten temat uzyskane przed 1994 rokiem. Nowsze wyniki sięgające roku 1999 zostały przedstawione w przeglądowej pracy M. Mignotte'a *Catalan's conjecture just before 2000* zamieszczonej w poświęconym pamięci K. Inkeriego tomie *Number Theory,* de Gruyter, Berlin 2001, który zredagowali M. Jutila i T. Metsänkylä.