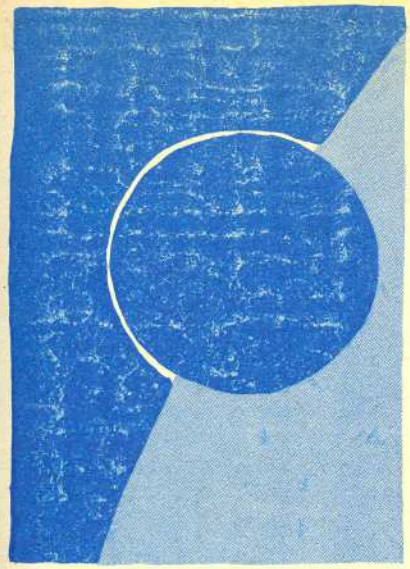


Co udowodnił Étienne Fouvry?

Doc. dr Jerzy BROWKIN

Omówimy pewne, uzyskane ostatnio, wyniki dotyczące rozwiązań równania Fermata

(1) $$x^n+y^n=z^n$$

w liczbach całkowitych x, y, z różnych od zera, gdzie n jest liczbą naturalną większą od 2.

Można zakładać, że liczby x, y, z nie mają wspólnego dzielnika większego od 1; można by bowiem przez taki wspólny dzielnik te liczby podzielić uzyskując znów rozwiązanie równania (1). Można również zakładać, że żadne dwie z liczb x, y, z nie mają wspólnego dzielnika większego od 1. Byłby on bowiem również dzielnikiem trzeciej liczby na mocy (1).

Już Pierre Fermat (1608—1665) udowodnił, że równanie (1) nie ma rozwiązań dla $n = 4$. Dowód tego faktu jest całkiem elementarny; można go znaleźć w każdej niemal książce z elementarnej teorii liczb, np. W. Sierpiński, *Wstęp do teorii liczb*, PZWS, Warszawa 1965.

Wobec tego wystarczy ograniczyć się do badania równania (1) w przypadku, gdy $n = p$ jest liczbą pierwszą większą od 2.

Oznaczając $w = -z$ i przenosząc wszystkie składniki na stronę lewą otrzymujemy więc równanie

(2) $$x^p+y^p+w^p=0.$$

Ograniczymy się w dalszym ciągu do rozważania tylko takich rozwiązań równania (2) w liczbach całkowitych x, y, w parami względnie pierwszych i różnych od zera, że żadna z tych liczb nie jest podzielna przez p. Jest to tak zwany *pierwszy przypadek* równania (2). Oczywiście, do zbadania wszystkich rozwiązań tego równania należy rozpatrzyć jeszcze drugi przypadek, gdy jedna z liczb x, y, w jest podzielna przez p. Tym drugim przypadkiem w niniejszym artykule zajmować się nie będziemy.

Na początku XIX wieku Sophie Germain (1776—1831) udowodniła, że dla wielu pierwszych p równanie (2) nie ma rozwiązań w pierwszym przypadku. Wykazała mianowicie, że *jeżeli również $q = 2p+1$ jest liczbą pierwszą, to równanie* (2) *nie ma rozwiązań w pierwszym przypadku.*

Dowód jest prosty i elementarny, więc go przytoczymy. Z konieczności został on zredagowany zwięźle, więc dokładne zrozumienie go będzie wymagało od Czytelnika pewnego samodzielnego wysiłku.

Udowodnimy najpierw kilka faktów pomocniczych.

9. Paradoks rozmiarów

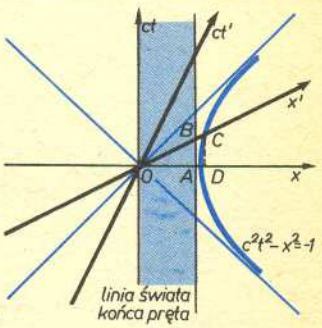
Względność równoczesności ma także wpływ na pomiar odległości. Na przykład długość pręta mierzy się wyznaczając w tej samej chwili współrzędne jego końców. Ponieważ zdarzenia równoczesne w jednym układzie inercjalnym nie są równoczesne w innym, wynik pomiaru zależy od układu odniesienia.

Niech pręt o jednostkowej długości spoczywa w układzie O, a obserwator znajduje się w układzie O' poruszającym się względem O z prędkością v. Na rysunku 9a przedstawione są linie świata końców pręta oraz fragment hiperboli jednostkowej. Dla O zdarzenia O i A są równoczesne i pomiar długości daje wynik 1. Dla O' równoczesne są zdarzenia O i B, a więc długość pręta l' jest mniejsza od 1 (OC jest jednostką długości w układzie O').

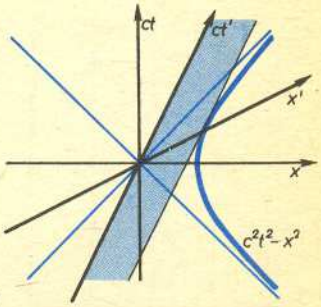
Łatwo można uzyskać wynik ilościowy: $l' = \dfrac{OB}{OC} = \dfrac{OA}{OD}$,

gdzie $OA = 1$, a OD otrzymujemy z warunku przecięcia hiperboli z osią Ox'. Stąd $l' = \sqrt{1-(v/c)^2}$.

Taki sam wynik otrzymujemy w przypadku, gdy pręt spoczywa w układzie O', a obserwator w O (rys. 9b).



Rys. 9a



Rys. 9b

Lemat 1. Jeżeli p oraz $q = 2p+1$ są liczbami pierwszymi i liczba u nie jest podzielna przez q, to liczba u^p daje resztę 1 lub -1 z dzielenia przez q.

Dowód. Skorzystamy z tzw. małego twierdzenia Fermata, które orzeka, że jeżeli liczba u nie jest podzielna przez liczbę q, to liczba $u^{q-1}-1$ jest podzielna przez q. Dowód tego twierdzenia można znaleźć w podanej wyżej książce. Mamy zatem

$$q \mid u^{q-1}-1 = u^{2p}-1 = (u^p-1)\cdot(u^p+1),$$

tzn. jedna z liczb u^p-1, u^p+1 jest podzielna przez q. Wynika stąd teza lematu.

Wniosek. Jeżeli liczba $a^p+b^p+c^p$ jest podzielna przez q, to jedna z liczb a, b, c jest podzielna przez q.

Dowód. Jeżeli żadna z liczb a, b, c nie jest podzielna przez q, to na mocy lematu 1 liczba $a^p+b^p+c^p$ przy dzieleniu przez q daje resztę $\pm1\pm1\pm1$ (przy odpowiednim wyborze znaków $+$ lub $-$). To znaczy, ta reszta jest równa 1, -1, 3 lub -3. Jest to niemożliwe, ponieważ liczba $a^p+b^p+c^p$ z założenia jest podzielna przez q bez reszty, a $q = 2p+1 > 3$. Uzyskana sprzeczność dowodzi, że wniosek jest prawdziwy.
Oznaczmy $T(x, y) = x^{p-1}-x^{p-2}y+x^{p-3}y^2-\ \ldots\ -xy^{p-2}+y^{p-1}$.
Mamy tożsamość

$$(x+y)\cdot T(x, y) = x^p+y^p. \tag{3}$$

Lemat 2. Jeżeli d jest dzielnikiem liczby $x+y$, to liczby $T(x, y)$ oraz px^{p-1} dają tę samą resztę z dzielenia przez d.

Dowód. Z założenia $d \mid x+y$ wynika, że liczby x oraz $-y$ dają tę samą resztę z dzielenia przez d. Zatem każda z p liczb:

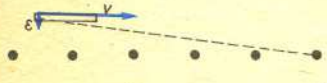
$$x^{p-1},\ x^{p-2}\cdot(-y),\ x^{p-3}\cdot(-y)^2,\ \ldots,\ x\cdot(-y)^{p-2},\ (-y)^{p-1}$$

daje tę samą resztę z dzielenia przez d. Teza lematu wynika więc ze wzoru określającego $T(x, y)$.

Przystępujemy teraz do dowodu twierdzenia Germain. Przypuśćmy, że liczby całkowite różne od zera x, y, w są parami względnie pierwsze i niepodzielne przez p oraz spełniają równanie (2). Z powyższego wniosku wynika, że jedna z nich jest podzielna przez q. Niech np. $q \mid w$. Liczby $x+y$ oraz $T(x, y)$ są względnie pierwsze, ponieważ na mocy lematu 2 każdy ich wspólny dzielnik d dzieliłby też liczbę px^{p-1} i na mocy (3) i (2) dzieliłby liczbę w^p. Z założenia jednak liczba w nie jest podzielna przez p, a liczby x i w są względnie pierwsze. Zatem $d = 1$.

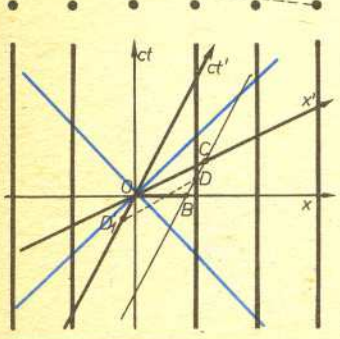
Na mocy (3) i (2) iloczyn liczb względnie pierwszych $x+y$ oraz $T(x, y)$ jest $p-$tą potęgą liczby całkowitej różnej od zera. Każda z tych liczb jest więc p-tą potęgą liczby całkowitej.
W szczególności $x+y = r^p$. Podobnie dowodzimy, że $x+w = s^p$, $y+w = t^p$ dla pewnych liczb całkowitych s i t.

Znany jest następujący paradoks. Wzdłuż szeregu przeszkód porusza się z dużą prędkością pręt (rys. 9c). Długość pręta i odległości między przeszkodami mierzone we własnych układach odniesienia są takie same. Pręt zaczyna zbliżać się do przeszkód z niewielką prędkością. Czy może je minąć? W układzie związanym z przeszkodami pręt ulega skróceniu i minięcie przeszkód jest możliwe. Inaczej jest w układzie związanym z prętem. Teraz skróceniu ulega odległość między przeszkodami i przejście pręta nie jest możliwe.



Rys. 9c

Na rysunku 9d widoczny jest ,,przekrój" czasoprzestrzeni, do którego należą przeszkody. Przedstawione na nim linie świata końców pręta są rzutami rzeczywistych linii świata w trójwymiarowej czasoprzestrzeni. W układzie O długość pręta OB jest mniejsza od odległości między przeszkodami. W układzie tym oba końce pręta dochodzą równocześnie do szeregu przeszkód (zdarzenia O i B). W układzie O' prawy koniec pręta dochodzi do przeszkód (zdarzenie D równoczesne z D_1) wcześniej niż lewy (zdarzenie O'). Ciąg przeszkód nie jest więc w tym układzie równoległy do pręta i mimo że przeszkody rozmieszczone są gęściej, pręt może je minąć. W ten sposób paradoks został rozwikłany. Jego źródłem jest ,,względność równoległości". Dwa poruszające się względem siebie odcinki mogą być równoległe tylko w jednym układzie odniesienia. Dlatego gdy mówimy o pręcie poruszającym się równolegle do przeszkód, musimy określić, w którym układzie ma miejsce ta równoległość. My wybraliśmy układ związany z przeszkodami. Czytelnikom pozostawiamy przedyskutowanie przypadku, gdy pręt jest równoległy do przeszkód w układzie odniesienia związanym z prętem.



Rys. 9d

Ponieważ $q|w$, więc $q\nmid x$ i $q\nmid y$. Stąd $q\nmid s$ i $q\nmid t$. Ze wzoru $x+w=s^p$ wynika więc, że liczby x i s^p dają tę samą resztę z dzielenia przez q, mianowicie resztę 1 lub -1 na mocy lematu 1. Wobec tego resztą z dzielenia liczby px^{p-1} przez q jest liczba $p\cdot(\pm 1)^{p-1}=p$. Mamy $2w=(x+w)+(y+w)-(x+y)=s^p+t^p+(-r)^p$. Ponieważ $q|w$, $q\nmid s$, $q\nmid t$, więc z wniosku otrzymujemy, że $q|r$, a zatem $q|x+y$. Wobec tego $q\nmid T(x,y)$ bowiem liczby $x+y$ i $T(x,y)$ są względnie pierwsze.

Ponieważ $T(x,y)$ jest p-tą potęgą, więc z lematu 1 otrzymujemy, że reszta z dzielenia $T(x,y)$ przez q jest równa 1 lub -1. Z drugiej strony z lematu 2 wynika, że liczba $T(x,y)$ przy dzieleniu przez q daje taką resztę, jak liczba px^{p-1}, tzn. resztę p. Uzyskaliśmy sprzeczność, gdyż liczby 1, -1 i p dają różne reszty z dzielenia przez $q=2p\pm 1$.

Sprzeczność ta dowodzi, że równanie (2) nie ma rozwiązań w pierwszym przypadku, jeżeli liczba $q=2p+1$ jest pierwsza.

Z udowodnionego twierdzenia wynika na przykład, że równanie (2) nie ma rozwiązań w pierwszym przypadku dla $p=3$ (ponieważ liczba $2\cdot 3+1=7$ jest pierwsza) i podobnie dla $p=5, 11, 23$ itd.

Sophie Germain udowodniła twierdzenie ogólniejsze:
Jeżeli dla pewnej liczby naturalnej m liczba $q=2mp+1$ jest pierwsza oraz
(*) *wśród reszt, jakie dają przy dzieleniu przez q liczby $1^p, 2^p, 3^p, \ldots, (q-1)^p$ nie ma liczby p ani nie ma dwóch liczb kolejnych,*
to równanie (2) *nie ma rozwiązań w pierwszym przypadku.*

Zastosujemy to ogólniejsze twierdzenie do liczby $p=7$. Biorąc $m=2$ stwierdzamy, że liczba $q=2mp+1=29$ jest pierwsza. Sprawdzimy warunek (*). Znajdujemy więc reszty, jakie dają liczby $1^7, 2^7, 3^7, \ldots 27^7, 28^7$ przy dzieleniu przez 29. Po wykonaniu odpowiednich obliczeń stwierdzamy, że wśród tych reszt są tylko liczby 1, 12, 17, i 28. Nie ma tu ani liczby 7, ani dwóch liczb kolejnych. Zatem na mocy ogólniejszego twierdzenia Germain równanie (2) przy $p=7$ nie ma rozwiązań w pierwszym przypadku.

Twierdzenie Germain było uogólniane przez wielu autorów na różne sposoby. Zastępowano warunek (*) innymi, zwykle dość skomplikowanymi, warunkami na liczbę m, przy których spełnieniu równanie (2) nie ma rozwiązań w pierwszym przypadku.

Posługując się takimi warunkami sprawdzono, że równanie (2) nie ma rozwiązań w pierwszym przypadku dla wielu miliardów początkowych liczb pierwszych p. Nie umiano jednak udowodnić tymi metodami (ani żadnymi innymi), że *dla nieskończenie wielu* liczb pierwszych p równanie (2) nie ma rozwiązań w pierwszym przypadku.

Dopiero ostatnio to udowodniono wykorzystując m.in. ideę Sophie Germain, by badać liczby pierwsze postaci $2mp+1$.

Mianowicie L. M. Adleman i D. R Heath-Brown udowodnili, że jeżeli jest „dostatecznie dużo" liczb pierwszych postaci $2mp+1$, gdzie m i p spełniają odpowiednie warunki, to wśród rozważanych tu liczb pierwszych p istnieją takie, dla których równanie (2) nie ma rozwiązań w pierwszym przypadku.

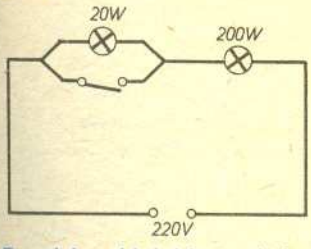
Mówiąc dokładniej: Ustalamy (dużą) liczbę X oraz liczbę Θ spełniającą $\frac{2}{3}<\Theta<1$ i rozważamy wszystkie takie liczby pierwsze p, że $X^\Theta<p<X$. Jeżeli liczb pierwszych q mniejszych od X, postaci $q=2mp+1$, gdzie $3\nmid m$, jest dostatecznie dużo, tzn. więcej niż $C\frac{X}{\log X}$, gdzie C jest pewną stałą dodatnią niezależną od X i Θ, to wśród rozważanych tu liczb pierwszych p są i takie, że równanie (2) nie ma rozwiązań w pierwszym przypadku.

Tak więc problem został sprowadzony do zbadania, czy jest dostatecznie dużo liczb pierwszych q spełniających powyższe warunki.

Otóż Étienne Fouvry w pracy opublikowanej w 1985 roku w czasopiśmie *Inventiones Mathematicae* stosując m.in. metodę sita oraz przeprowadzając długie i skomplikowane rachunki udowodnił, że przy $\Theta=0{,}6687$ liczba liczb pierwszych q opisanych wyżej jest większa niż $C\frac{X}{\log X}$, gdzie C jest pewną stałą dodatnią niezależną od X.

Ponieważ $\Theta=0{,}6687>\frac{2}{3}$, więc na mocy sformułowanego wyżej wyniku Adlemana i Heath-Browna otrzymujemy, że dla każdej dostatecznie dużej liczby X istnieje liczba pierwsza p większa od X^Θ, dla której równanie (2) nie ma rozwiązań w pierwszym przypadku. Liczb pierwszych p o tej własności jest więc nieskończenie wiele.

Rozwiązanie zadania F 185. Nominalna moc żarówki P wynosi V^2/R, gdzie V — napięcie skuteczne sieci elektrycznej, R — oporność włókna.



Ze względu na dziesięciokrotną różnicę oporności żarówek przy otwartym włączniku (patrz rysunek) napięcie na żarówce o mocy 20 W jest bliskie napięciu sieci, a napięcie na żarówce 200 W około 10 razy mniejsze. Oznacza to, że moc wydzielona w żarówce 20 W jest bliska nominalnej, a moc żarówki 200 W około 100 razy mniejsza od nominalnej, czyli żarówka ta praktycznie nie zaświeci.

Gdy klucz jest zamknięty, świeci się tylko żarówka 200 W, bo napięcie na żarówce 20 W jest znikomo małe.