

Co udowodnił Étienne Fouvry?

Doc. dr Jerzy BROWKIN

Omówimy pewne, uzyskane ostatnio, wyniki dotyczące rozwiązań równania Fermata

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

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

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

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

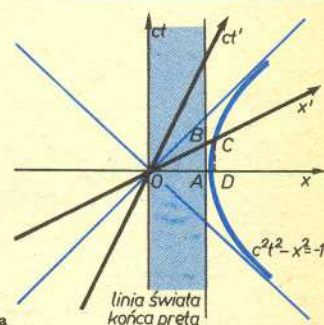
Względność równoczesności ma także wpływ na pomiar odległości. Na przykład długość pręta mierzy się wyznaczając w tej samej chwili współrzędne jego końców. Ponieważ zdarzenia równoczesne w jednym układzie inercyjnym nie są równoczesne w innym, wynik pomiaru zależy od układu odniesienia.

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 światła końców pręta oraz fragment hiperboli jednostkowej. Dla θ zdarzenia O i A są równoczesne i pomiar długości daje wynik 1. Dla θ' równoczesne są zdarzenia O i B , a więc długość pręta l' jest mniejsza od 1 (OC jest jednostką długości w układzie O').

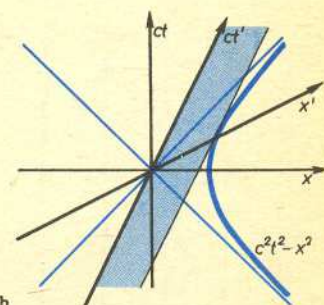
$$\text{Łatwo można uzyskać wynik ilościowy: } l' = \frac{OB}{OC} = \frac{OA}{OD},$$

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 $\pm 1 \pm 1 \pm 1$ (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 $T(x, y) = x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \dots - xy^{p-2} + y^{p-1}$.

Mamy tożsamość

$$(3) \quad (x+y) \cdot T(x, y) = x^p + y^p.$$

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:

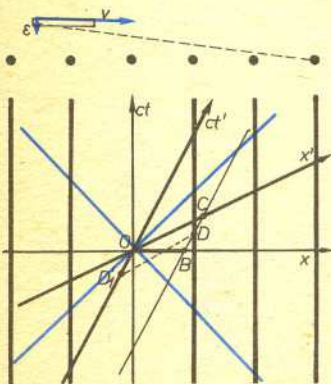
$$x^{p-1}, x^{p-2} \cdot (-y), x^{p-3} \cdot (-y)^2, \dots, x \cdot (-y)^{p-2}, (-y)^{p-1}$$

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

Rys. 9d

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 równoległe 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.