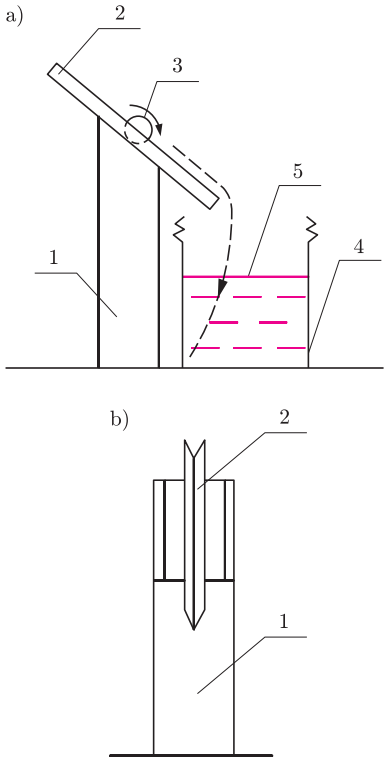


Rys. 4. Układ do badania efektu Magnusa w wodzie;
a) widok z boku:
1 – tekturowe pudełko,
2 – rynienka,
3 – kulka,
4 – akwarium lub duży słoik,
5 – woda,
b) widok z przodu.

ćwiczenie warto przeanalizować rozkład prędkości i kierunek dodatkowego ciśnienia Δp podczas obrotu walca w lewo. Zaobserwowany przez nas efekt odchylenia kierunku ruchu obracającego i przesuwającego się w płynie ciała stałego nazwany jest od nazwiska jego odkrywcy efektem Magnusa.

Działanie siły Magnusa powodującej zakrzywienie toru w efekcie Magnusa możemy również łatwo zaobserwować w przypadku kulek poruszających się w wodzie lub oleju. Ponieważ gęstość wody lub oleju jest szacunkowo około tysiąca razy większa od gęstości powietrza, tyleż razy będzie większa siła Magnusa. Wzór opisujący tę siłę jest następujący.

(2) $$P_m = \pi \rho_{\mathrm{p}} v u d l.$$

We wzorze (2) P_m oznacza wartość siły Magnusa, l – długość walca, d – jego średnicę, v, u – odpowiednio prędkość unoszenia i prędkość opływu walca w odległości, na której ruch jest niezaburzony, czyli w dostatecznie dużej odległości od walca, ρ_{p} – gęstość płynu. Jako ciekawostkę warto dodać, że niemiecki fizyk i chemik w jednej osobie, Kutta, oraz badacz rosyjski, Żukowski, podali prawie jednocześnie ten wzór na obliczenie siły Magnusa.

Przystąpimy teraz do zbadania efektu Magnusa w cieczach. Potrzebne będzie akwarium, które z powodzeniem można zastąpić pięciolitrowym słoikiem od przetworów spożywczych. Ponadto tekturowe pudełko dwukrotnie wyższe od słoika, dwie linijki o długości 50 cm oraz taśma klejąca i nożyczki. Nieco uwagi należy poświęcić kuleczce, która staczać się będzie do płynu. Powinna mieć ona średnicę około 1–2 cm i być wykonana z materiału o gęstości nieco większej od gęstości wody. Z powodzeniem można tu zastosować kulisty koralik z tworzywa sztucznego.

Tym razem przeprowadzamy doświadczenie w ten sposób, że umieszczamy kulkę w pobliżu szczytu rynienki i puszczamy ją swobodnie, pozwalając się jej stoczyć do wody. Obserwujemy uważnie ruch kuleczki w wodzie. Wbrew oczekiwaniom tor kuleczki w wodzie zakrzywia się i kuleczka zamiast po paraboli porusza się po torze o kształcie zbliżonym do odwróconej litery C. Z jeszcze bardziej kuriozalnym przypadkiem spotkali się żołnierze niemieccy, kiedy stwierdzili, że podczas strzelania z moździerza gładkimi pociskami jeden z nich poruszał się po pętli, a następnie spadł za strzelającymi. Na szczęście, mówiąc językiem wojskowym, obyło się bez strat siły żywej i sprzętu.

Równanie Pitagorasa w kongruencjach

Anna SILKA [*], *Tomasz SZEMBERG* [*]

W 1994 roku Andrew Wiles udowodnił sformułowane w XVII wieku Wielkie Twierdzenie Fermata, które głosi, że równanie

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

dla $n \geqslant 3$ nie ma nietrywialnych (tj. takich, że wszystkie liczby x, y, z są różne od zera) rozwiązań w zbiorze liczb całkowitych.

Z drugiej strony wiadomo, że dla $n = 2$ równanie

(2) $$x^2 + y^2 = z^2,$$

którego nie sposób nie skojarzyć z imieniem Pitagorasa, ma nieskończenie wiele rozwiązań całkowitych.

W tym artykule chcemy się zastanowić, ile rozwiązań ma równanie Pitagorasa w ciele $\mathbb{Z}_p$, dla ustalonej nieparzystej liczby pierwszej p. Mówiąc nieco górnolotnie, będziemy się zajmować geometrią algebraiczną nad pewnymi ciałami skończonymi. Liczenie rozwiązań pewnych równań typu (1) modulo p stanowiło istotny element dowodu Wilesa.

Przypomnijmy, że ciało $\mathbb{Z}_p$ to zbiór reszt z dzielenia przez p, tzn. $\mathbb{Z}_p = \{0, 1, 2, 3, \ldots, (p-2), (p-1)\}$, w którym działania określone są niemal

[*] Akademia Pedagogiczna, Kraków

jak zwykłe dodawanie i mnożenie liczb całkowitych, przy czym wynikiem jest reszta z dzielenia przez p zwykłego wyniku.

Przykładowo:

$$2 \cdot 2 = 4 = 3 + 1 = 1 \quad \text{w } \mathbb{Z}_3,$$

a w $\mathbb{Z}_5$ mnożenie odbywa się według reguł:

$$2 \cdot 2 = 4,\ 2 \cdot 3 = 1,\ 2 \cdot 4 = 3,\ 3 \cdot 3 = 4,\ 3 \cdot 4 = 2 \ \text{ i } \ 4 \cdot 4 = 1$$

(mnożenie przez 0 i 1 jest oczywiste, podobnie jak fakt, że jest to działanie przemienne).

Ze względu na to, iż zajmujemy się tu kwadratami liczb, naturalnie i wygodnie jest korzystać z nieco innego (oczywiście równoważnego) zbioru reszt. Dla p nieparzystego mamy

$$\mathbb{Z}_p = \left\{ -\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-3}{2}, \frac{p-1}{2} \right\}.$$

Zauważmy, że ponieważ $\mathbb{Z}_p$ składa się z p elementów, to mamy do rozważenia co najwyżej p^3 trójek liczb (x, y, z). W szczególności liczba rozwiązań równania (2) jest zawsze skończona. Naturalne jest pytanie, ile tych rozwiązań dokładnie jest. Odpowiedź stanowi treść następującego twierdzenia.

Twierdzenie. *Równanie Pitagorasa ma dokładnie p^2 rozwiązań w ciele $\mathbb{Z}_p$.*

Zanim udowodnimy ten ogólny wynik, spójrzmy na kilka rozwiązań w konkretnych przypadkach. Taka analiza zbioru rozwiązań dla małych wartości p pozwoliła nam sformułować hipotezę dotyczącą ogólnego wzoru oraz wyznaczyła kolejne redukcje w dowodzie.

Dla $p = 3$ i $p = 5$ liczby, które spełniają równanie (2), to np:

$$\mathbb{Z}_3 :\ (0,\,0,\,0),\ (0,\,1,\,1),\ (0,\,2,\,1),\ (1,\,0,\,1),\ (2,\,0,\,1),$$

$$\mathbb{Z}_5 :\ (0,\,0,\,0),\ (0,\,1,\,1),\ (1,\,0,\,1),\ (0,\,4,\,1),\ (4,\,0,\,1),\ (2,\,1,\,0),\ (3,\,1,\,0).$$

Zauważmy, że, jeśli mamy rozwiązanie (x, y, z) równania (2), to (kx, ky, kz) dla każdego $k \in \mathbb{Z}_p$ też jest rozwiązaniem. Zbiór punktów postaci $k \cdot (x, y, z)$ to nic innego jak prosta przechodząca przez początek układu współrzędnych w przestrzeni $(\mathbb{Z}_p)^3$. Wszystkie te proste mają jeden wspólny punkt $(0, 0, 0)$. Oznaczmy przez $\sim$ relację proporcjonalności (czyli należenia do jednej prostej). W naszych konkretnych przypadkach mamy dla $\mathbb{Z}_3$:

$$(0,\,1,\,1) \sim (0,2,2),\ (0,\,2,\,1) \sim (0,\,1,\,2),\ (1,\,0,\,1) \sim (2,0,2),\ (2,\,0,\,1) \sim (1,0,2)$$

i dla $\mathbb{Z}_5$

$$\begin{gathered}
(0,\,1,\,1) \sim (0,\,2,\,2) \sim (0,\,3,\,3) \sim (0,\,4,\,4),\\
(0,\,4,\,1) \sim (0,\,1,\,4) \sim (0,\,2,\,3) \sim (0,\,3,\,2),\\
(1,\,0,\,1) \sim (2,\,0,\,2) \sim (3,\,0,\,3) \sim (4,\,0,\,4),\\
(4,\,0,\,1) \sim (1,\,0,\,4) \sim (2,\,0,\,3) \sim (3,\,0,\,2),\\
(2,\,1,\,0) \sim (3,\,4,\,0) \sim (1,\,3,\,0) \sim (4,\,2,\,0),\\
(3,\,1,\,0) \sim (2,\,4,\,0) \sim (4,\,3,\,0) \sim (1,\,2,\,0).
\end{gathered}$$

Zauważmy, że na każdej z takich prostych leży dokładnie tyle samo, tj. $p - 1$ punktów różnych od $(0, 0, 0)$.

Dla znalezienia wszystkich (różnych od $(0,\,0,\,0)$) rozwiązań równania (2) wystarczy zatem odnaleźć po jednym rozwiązaniu w każdej klasie rozwiązań proporcjonalnych. W szczególności w klasie (czyli na prostej) rozwiązania $(x,\,y,\,z)$, gdy tylko $z \neq 0$, poszukiwać będziemy rozwiązania $(\frac{x}{z},\,\frac{y}{z},\,1)$. Dzieląc równanie (2) stronami przez z^2, otrzymamy równanie

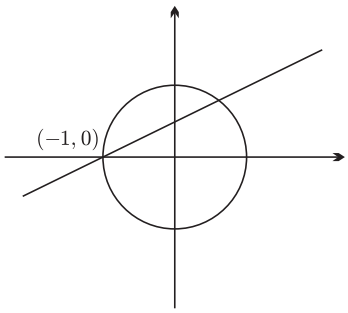
$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1.$$

W istocie, jest to równanie o dwóch zmiennych. Oznaczając je także x i y, otrzymujemy zatem równanie

$$x^2 + y^2 = 1. \tag{3}$$

Uwaga. *Liczba rozwiązań równania* (2) *to zatem liczba rozwiązań równania* (3) *pomnożona przez liczbę punktów na prostej bez zera, czyli* $(p-1)$*, plus rozwiązanie trywialne* $(0, 0, 0)$ *i rozwiązania, dla których* $z = 0$.

Równanie (3) to, oczywiście, równanie okręgu jednostkowego, tylko tym razem na płaszczyźnie $(\mathbb{Z}_p)^2$. Co prawda trzeba pamiętać, że rozważamy ciała skończone i ten okrąg składa się tylko ze skończonej liczby punktów, ale dla dalszych rozważań celowe jest chwilowe pozostanie przy tradycyjnej wizualizacji okręgu jednostkowego w $\mathbb{R}^2$.



Wykorzystamy klasyczny pomysł na szukanie trójek pitagorejskich oparty na obserwacji, że przecięcie okręgu (jednostkowego) z prostą o współczynnikach wymiernych albo daje dwa punkty o współrzędnych wymiernych, albo nie daje żadnego. Inaczej mówiąc, jeśli prosta o współczynnikach wymiernych przecina okrąg w punkcie o współrzędnych wymiernych, to drugi punkt przecięcia też musi mieć takie współrzędne. W naszej sytuacji słowo „wymierny" zastępujemy przez „określony nad $\mathbb{Z}_p$".

Oczywistym rozwiązaniem równania (3) jest para liczb $(-1, 0)$. Każda prosta przechodząca przez ten punkt ma równanie postaci $y = ax + a$. Szukamy rozwiązań układu równań:

$$\begin{cases} y &= ax + a \\ x^2 + y^2 &= 1 \end{cases}$$

Wstawiając pierwsze równanie do drugiego i porządkując współczynniki, dostajemy

$$(1 + a^2) \cdot x^2 + 2a^2 \cdot x + (a^2 - 1) = 0$$

Zauważmy, że od wartości współczynnika $(1 + a^2)$ zależy, czy mamy do czynienia z równaniem pierwszego, czy drugiego stopnia.

Jeśli $1 + a^2 = 0$, to $a^2 = -1$ i jedynym rozwiązaniem jest $x = -\frac{a^2-1}{2a^2} = -1$, czyli nie dostajemy nic nowego. Jeśli równanie jest jednak kwadratowe, to na podstawie twierdzenia Bezouta lewa strona dzieli się przez dwumian $(x + 1)$. Konkretnie mamy:

$$((1 + a^2)x^2 + 2a^2x + (a^2 - 1)) : (x + 1) = (1 + a^2)x + (a^2 - 1).$$

Zatem rozwiązaniami naszego układu są $x = -1$ (co nie jest żadną nowością) oraz $x = \frac{1-a^2}{1+a^2}$, gdzie $a \in \mathbb{Z}_p$.

Łatwo można sprawdzić, że $\frac{1-a^2}{1+a^2}$ nigdy nie jest równe -1 dla $p \geqslant 3$, czyli znaleźliśmy nowy punkt na okręgu:

$$\left(\frac{1 - a^2}{1 + a^2}, \frac{2a}{1 + a^2}\right),$$

który wyznacza punkt na prostej $(1 - a^2, 2a, 1 + a^2)$. Dla różnych wartości parametru $a \in \mathbb{Z}_p$ otrzymujemy przy tym różne proste.

Wartości funkcji x^2:

w $\mathbb{Z}_3$

$\pm a$	0	1
a^2	0	1

w $\mathbb{Z}_5$

$\pm a$	0	1	2
a^2	0	1	-1

w $\mathbb{Z}_7$

$\pm a$	0	1	2	3
a^2	0	1	4	2

w $\mathbb{Z}_{11}$

$\pm a$	0	1	2	3	4	5
a^2	0	1	4	9	5	3

w $\mathbb{Z}_{13}$

$\pm a$	0	1	2	3	4	5	6
a^2	0	1	4	9	3	-1	10

Aby znaleźć liczbę rozwiązań równania (3), musimy zastanowić się, czy i kiedy $a^2 = -1$. Gdy przyjrzymy się wartościom funkcji x^2 dla kilku wartości p (patrz margines), nasuwa się następujący lemat.

Lemat. *Niech* p *będzie nieparzystą liczbą pierwszą. Wówczas*
(1) *jeśli* $p \equiv 1 \bmod 4$*, to istnieją dokładnie dwa takie elementy* $q \in \mathbb{Z}_p$*, że* $q^2 \equiv -1 \bmod p$*;*
(2) *jeśli* $p \equiv 3 \bmod 4$*, to dla każdego* $q \in \mathbb{Z}_p$ *mamy* $q^2 \not\equiv -1 \bmod p$.

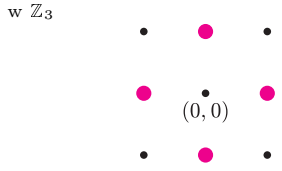
Dowód lematu wynika od razu z następującego Kryterium.

Kryterium Eulera. *Liczba* $x \in \mathbb{Z}_p$ *jest kwadratem w* $\mathbb{Z}_p$ *wtedy i tylko wtedy, gdy* $x^{(p-1)/2} \equiv 1 \bmod p$.

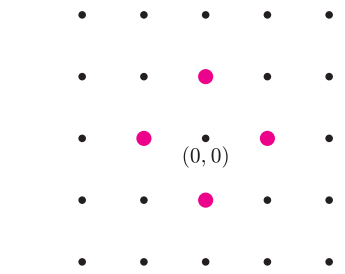
Istotnie, gdy $p \equiv 1 \bmod 4$, to $\frac{p-1}{2}$ jest liczbą parzystą, więc $(-1)^{(p-1)/2} = 1$, co oznacza, że -1 jest kwadratem. Natomiast gdy $p \equiv 3 \bmod 4$, to $\frac{p-1}{2}$ jest liczbą nieparzystą. Zatem $(-1)^{(p-1)/2} = -1$, a to na podstawie Kryterium kończy dowód Lematu.

Tak naprawdę wyglądają okręgi jednostkowe

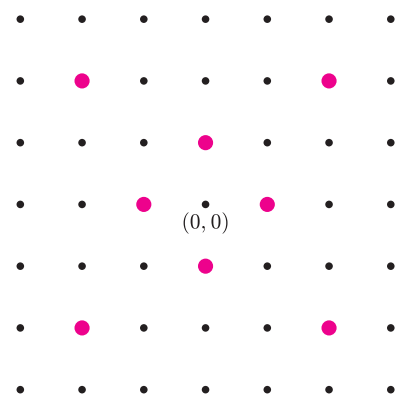
w $\mathbb{Z}_3$



w $\mathbb{Z}_5$



w $\mathbb{Z}_7$



Dla Czytelników zaawansowanych udowodnimy teraz to Kryterium.

Niech $\mathbb{Z}_p^*$ oznacza zbiór elementów niezerowych ciała $\mathbb{Z}_p$. Z Małego Twierdzenia Fermata mamy, że $x^{p-1} = 1 \bmod p$ dla dowolnego $x \in \mathbb{Z}_p^*$. Rozważmy następujące odwzorowanie:

$$\mathbb{Z}_p^* \ni x \longrightarrow x^2 \in \mathbb{Z}_p^*.$$

Ponieważ $x^2 = (-x)^2$ i $x \neq -x$, więc dokładnie połowa, czyli $\frac{p-1}{2}$ elementów w $\mathbb{Z}_p^*$ jest kwadratami. Weźmy teraz odwzorowanie:

$$\mathbb{Z}_p^* \ni x \longrightarrow x^{(p-1)/2} \in \mathbb{Z}_p^*.$$

Ponownie na podstawie Małego Twierdzenia Fermata $x^{p-1} = 1 \bmod p$ dla każdej liczby $x \in \mathbb{Z}_p^*$. Pierwiastki kwadratowe z 1 to 1 i -1, zatem

$$x^{(p-1)/2} = 1 \bmod p \quad \text{lub} \quad x^{(p-1)/2} = -1 \bmod p.$$

Każde z równań

$$x^{(p-1)/2} = 1 \quad \text{oraz} \quad x^{(p-1)/2} = -1$$

ma co najwyżej $\frac{p-1}{2}$ rozwiązań. Ale łącznie mają $p-1$ rozwiązań. Zatem każde z nich musi mieć dokładnie $\frac{p-1}{2}$ rozwiązań.

Jeśli $x^{(p-1)/2} = -1$, to x nie jest kwadratem w $\mathbb{Z}_p$. Gdyby istniało takie r, że $r^2 = x$, mielibyśmy

$$1 = r^{p-1} = (r^2)^{(p-1)/2} = x^{(p-1)/2} = -1,$$

a to daje sprzeczność. Biorąc pod uwagę wyliczoną wyżej liczbę kwadratów w Z_p^*, dostajemy tezę Kryterium.

Mamy już teraz w ręce wszystkie narzędzia potrzebne do dokładnego policzenia liczby rozwiązań równania Pitagorasa. Czyli przyszła pora na dokończenie artykułu.

Dowód Twierdzenia.
Gdy $p \equiv 3 \bmod 4$, to równanie (3) ma $p+1$ rozwiązań: punkt $(-1, 0)$ i po jednym punkcie dla każdej prostej $y = ax + x$, czyli dla każdego $a \in \mathbb{Z}_p$. Każde z nich odpowiada $p-1$ punktom w relacji $\sim$. Zatem mamy $(p+1) \cdot (p-1)$ rozwiązań plus rozwiązanie trywialne. Łatwo zauważyć na podstawie Kryterium, że w tej sytuacji równanie (2) nie ma rozwiązań, dla których $z = 0$. Korzystając z Uwagi, otrzymujemy zatem łącznie p^2 rozwiązań.

Z kolei gdy $p \equiv 1 \bmod 4$, to mamy dwa pierwiastki kwadratowe z -1, oznaczmy je q i $-q$. W tej sytuacji równanie (3) ma o dwa rozwiązania mniej niż poprzednio, czyli $p-1$. Każde z nich odpowiada jak poprzednio $p-1$ punktom w relacji $\sim$. W ten sposób dostajemy $(p-1)^2$ rozwiązań.

Brakujące rozwiązania dostajemy, analizując (2) dla $z = 0$. Wtedy dwa rozwiązania: $(1, q, 0)$ i $(1, -q, 0)$ znów reprezentują po $(p-1)$ punktów w relacji $\sim$.

Uwzględniając rozwiązanie trywialne, mamy łącznie

$$(p-1)^2 + 2 \cdot (p-1) + 1 = p^2.$$

A to kończy dowód Twierdzenia.

Uważny Czytelnik dostrzegł zapewne, że pominęliśmy dowód Twierdzenia, gdy $p = 2$. Mamy nadzieję, że taki Czytelnik jest w stanie uzupełnić tę lukę (w najgorszym razie licząc rozwiązania „na palcach", $\mathbb{Z}_2^3$ to tylko 8 punktów).

$$\star \quad \star \quad \star$$

Co można zrobić dalej? Można, na przykład, modyfikować współczynniki równania i badać, jak wpływają takie manipulacje na liczbę rozwiązań – na przykład dla równania

$$x^2 + 2y^2 = 3z^2.$$

Tego typu zabawy gorąco polecamy Czytelnikowi chcącemu sprawdzić, na ile sam opanował przedstawione tu idee.

Bardzo uważny Czytelnik zauważył, że nasze Twierdzenie zachodzi tylko dla *pewnych* ciał skończonej charakterystyki. Rozważanie innych ciał i podejście do **modularności** (pojęcie, które odegrało decydującą rolę w dowodzie Wielkiego Twierdzenie Fermata) równania Pitagorasa to temat, któremu sami chcemy się bliżej przyjrzeć.

Literatura

[Sie] Sierpiński, Wacław, *Trójkąty pitagorejskie*, PWN, Warszawa, 1954.

[Wil] Wiles, Andrew, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) 141 (1995), 443–551.