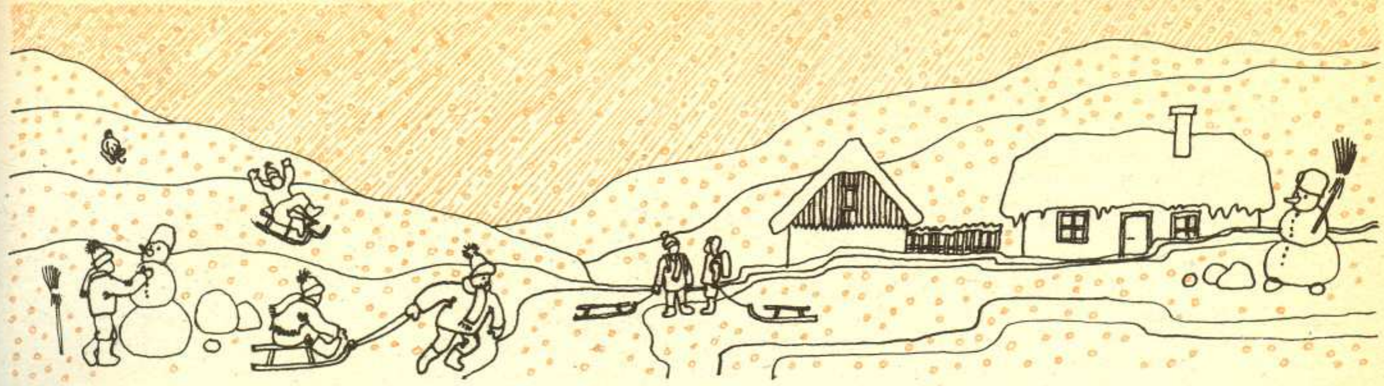


Co udowodnił Gerd Faltings?

Doc. dr Jerzy BROWKIN

Będziemy się zajmowali równaniami postaci $f(x, y) = 0$, gdzie f jest wielomianem o współczynnikach całkowitych, a więc na przykład równaniami:

$$3x-y+1 = 0, \tag{1}$$

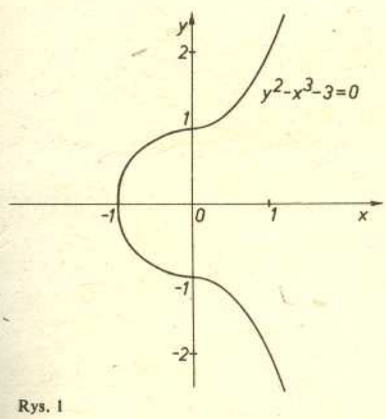
$$x^2+y^2-1 = 0, \tag{2}$$

$$y^2-x^3-3 = 0, \tag{3}$$

$$x^4+y^4-2 = 0. \tag{4}$$

Pytamy, czy każde takie równanie ma nieskończenie wiele rozwiązań w liczbach *wymiernych*. To znaczy, czy istnieje nieskończenie wiele takich różnych par liczb wymiernych a, b, że $f(a, b) = 0$.

Każde takie równanie opisuje pewną krzywą na płaszczyźnie. Na przykład równanie (1) opisuje linię prostą, równanie (2) — okrąg, równanie (3) pewną inną krzywą (zwaną krzywą eliptyczną — rys. 1), równanie (4) — krzywą podaną na rys. 2. Nasze pytanie można więc sformułować tak: Czy na każdej krzywej opisanej wielomianem o współczynnikach całkowitych leży nieskończenie wiele punktów o współrzędnych wymiernych?



Rys. 1

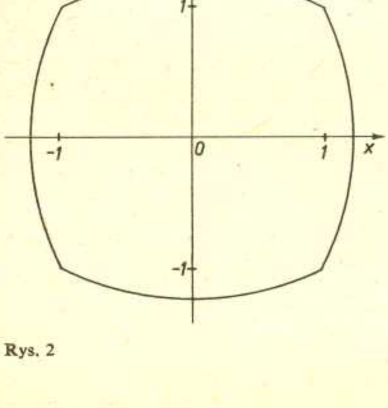
Spróbujmy znaleźć odpowiedź na to pytanie w przypadku krzywych opisanych równaniami (1) — (4).

Oczywiście na linii prostej (1) leży nieskończenie wiele punktów o współrzędnych wymiernych. Wystarczy mianowicie przyjąć za x dowolną liczbę wymierną a, zaś jako y wziąć liczbę $3a+1$. Para liczb $x = a$, $y = 3a+1$ spełnia to równanie i obie te liczby są wymierne. Ponieważ liczbę a możemy obierać na nieskończenie wiele sposobów, więc otrzymujemy w ten sposób nieskończenie wiele rozwiązań równania (1) w liczbach wymiernych.

Również równanie (2) ma nieskończenie wiele takich rozwiązań. Weźmy mianowicie dowolną liczbę wymierną a i przyjmijmy

$$x = \frac{a^2-1}{a^2+1}, \quad y = \frac{2a}{a^2+1}.$$

Nietrudno sprawdzić (a sumienny Czytelnik powinien to zrobić!), że te liczby x i y spełniają równanie (2) i obie są wymierne.



Rys. 2

W przypadku równania (3) sytuacja jest bardziej skomplikowana. Dla równań (1) i (2) wskazaliśmy wzory zależne od dowolnej liczby wymiernej a opisujące pewne rozwiązania tych równań. Taką liczbę a nazywamy parametrem, a otrzymane rozwiązania — rozwiązaniami opisanymi parametrycznie.

Otóż można udowodnić, że równanie (3) nie ma rozwiązań, które dałyby się opisać parametrycznie. Niemniej również to równanie ma nieskończenie wiele rozwiązań w liczbach wymiernych! Uzyskuje się je jednak na innej drodze.

Mianowicie, zauważmy najpierw, że liczby $x_1 = 1$, $y_1 = 2$ spełniają równanie (3). Następnie weźmy liczby

$$x_2 = \frac{9x_1^4-8x_1y_1^2}{4y_1^2} = -\frac{23}{16}, \quad y_2 = \frac{27x_1^6-36x_1^3y_1^2+8y_1^4}{8y_1^3} = \frac{11}{64}.$$

Po dość uciążliwych rachunkach przekonujemy się, że również liczby x_2 i y_2 (które są wymierne!) spełniają równanie (3). Ogólnie, jeżeli liczby x_k, y_k spełniają (3), to również liczby x_{k+1} i y_{k+1} określone wzorami

$$x_{k+1} = \frac{9x_k^4 - 8x_k y_k^2}{4y_k^2}, \quad y_{k+1} = \frac{27x_k^6 - 36x_k^3 y_k^2 + 8y_k^4}{8y_k^3}$$

spełniają to równanie (Czytelnik zechce to sprawdzić). Można też pokazać, że wszystkie tak otrzymane pary (x_k, y_k) są różne. W ten sposób wychodząc z rozwiązania $x_1 = 1$, $y_1 = 2$ otrzymujemy nieskończenie wiele rozwiązań równania (3) w liczbach wymiernych.

Każde z rozpatrzonych przez nas dotychczas równań miało nieskończenie wiele rozwiązań w liczbach wymiernych. Jednak już równanie (4) nie ma tej własności. Można udowodnić, że ma ono tylko skończoną liczbę rozwiązań w liczbach wymiernych, mianowicie $(1,1)$, $(1,-1)$, $(-1,1)$ $(-1,-1)$.

Jakiej więc można oczekiwać odpowiedzi na pytanie postawione na początku artykułu?

Już w latach dwudziestych bieżącego stulecia matematyk angielski L. J. Mordell (1888—1972) sformułował przypuszczalną odpowiedź na to pytanie.

Mianowicie, znana jest ... (Ostrzeżenie: Od tego miejsca sformułowania w tym artykule są już mniej precyzyjne, a czasem wręcz nieścisłe!) ... bardzo ogólna klasyfikacja krzywych polegająca na tym, że każdej krzywej przypisuje się pewną liczbę całkowitą nieujemną zwaną jej rodzajem. Tak więc są krzywe rodzaju 0, krzywe rodzaju 1, krzywe rodzaju 2 itd. W tym artykule nie podamy definicji rodzaju krzywej (wymaga ona nieco rozleglejszej wiedzy niż zakładamy u Czytelnika), lecz można powiedzieć, że im krzywa ma większy rodzaj, tym jest „bardziej skomplikowana". Krzywe rodzaju 0 — to są krzywe, których punkty można opisać parametrycznie, krzywe rodzaju 1 — to są tzw. krzywe eliptyczne, ...

Otóż Mordell przypuszczał, że na każdej krzywej rodzaju większego od 1 jest tylko skończona liczba punktów o współrzędnych wymiernych.

Ta słynna hipoteza Mordella przez ponad 50 lat opierała się wysiłkom matematyków próbujących ją udowodnić. Chociaż uzyskano różne wyniki częściowe na jej temat, sama hipoteza pozostawała nieudowodniona.

Dopiero wiosną 1983 roku prof. Gerd Faltings z RFN hipotezę tę udowodnił i od tego czasu hipoteza Mordella nosi nazwę twierdzenia Faltingsa.

Omówimy pewien wniosek wynikający z twierdzenia Faltingsa. Istnieje przypuszczenie, że dla każdej liczby naturalnej n większej od 2 równanie $x^n + y^n = z^n$, zwane równaniem Fermata, nie ma rozwiązań w liczbach całkowitych x, y, z różnych od zera. Możemy przy tym bez zmniejszenia ogólności rozważań ograniczyć się do takich rozwiązań, że liczby x, y, z są względnie pierwsze. Dzieląc to równanie stronami przez z^n i przyjmując $X = \frac{x}{z}$, $Y = \frac{y}{z}$ możemy powyższe przypuszczenie sformułować w sposób równoważny, jak następuje:

Dla każdej liczby naturalnej n większej od 2 równanie

$$X^n + Y^n = 1 \tag{5}$$

nie ma rozwiązań w liczbach wymiernych X, Y różnych od zera, to znaczy jedynymi jego rozwiązaniami w liczbach wymiernych mogą być $X = 0$, $Y = \pm 1$ oraz $X = \pm 1$, $Y = 0$ — ma więc ono co najwyżej cztery rozwiązania.

Wiadomo, że krzywa opisana równaniem (5) ma rodzaj równy $\frac{(n-1)(n-2)}{2}$. Liczba ta jest większa od 1 dla n większego od 3. Zatem z twierdzenia Faltingsa wynika, że dla $n \geqslant 4$ równanie (5) ma tylko skończoną liczbę rozwiązań w liczbach wymiernych.

Tak więc nadal nie znamy wszystkich rozwiązań równania Fermata w liczbach całkowitych x, y, z różnych od zera i względnie pierwszych. Wiemy jednak, że przy ustalonym n, jeżeli takie rozwiązania istnieją, to ich liczba jest skończona.

Jeszcze na zakończenie kilka uwag. Twierdzenie Faltingsa można inaczej sformułować tak: Jeżeli krzywa ma nieskończenie wiele punktów o współrzędnych wymiernych, to jest krzywą rodzaju 0 lub 1. Należy jednak ostrzec Czytelnika, że twierdzenie odwrotne nie jest prawdziwe. To znaczy, nie każda krzywa rodzaju 0 lub 1 ma nieskończenie wiele punktów o współrzędnych wymiernych.

Na przykład krzywa o równaniu $x^2 + y^2 = 3$ ma rodzaj 0, lecz nie leży na niej żaden punkt o współrzędnych wymiernych. Ten ostatni fakt może Czytelnik udowodnić samodzielnie — jest to nietrudne ćwiczenie.

Rozwiązanie zadania F 148. Sytuacja jest wręcz odwrotna. W punkcie a) strumień obejmowany przez obwód z galwanometrem wzrasta, lecz mimo to nie płynie w nim prąd, brak jest bowiem jakiejkolwiek siły zdolnej do „napędzania" nośników ładunku, w pozostałych punktach strumień magnetyczny przenikający obwody nie ulega zmianie — mimo to płyną w nich prądy, w układzie odniesienia związanym z polem magnetycznym nośniki ładunku poruszają się wraz z przewodnikami w polu magnetycznym i składowa magnetyczna siły Lorentza jest czynnikiem zapewniającym przepływ prądu. Prawo indukcji elektromagnetycznej nie jest więc prawem uniwersalnym i przytoczone przykłady dobrano właśnie ze względu na ich wyjątkowość. Prawo to jest dogodnym narzędziem ułatwiającym rachunki, lecz nie wyjawia mechanizmu powstawania siły elektromotorycznej indukcji.
W przypadkach wątpliwych należy rozpatrzeć siły będące przyczyną uporządkowanego ruchu nośników (siła Lorentza).

Rozwiązanie zadania M 356. Niech ad będzie środkową trójkąta abc. Mamy dla odpowiednich wektorów

$$|ad|^2 = \left|\frac{1}{2}(ab+ac)\right|^2 = \frac{1}{4}(|ab|^2 + |ac|^2 + {} + 2\langle ab, ac\rangle)$$

i ponieważ

$$|bc|^2 = |ac - ab|^2 = |ab|^2 + |ac|^2 - 2\langle ab, ac\rangle$$

jest $|ad|^2 = \frac{1}{4}(2|ab|^2 + 2|ac|^2 - |bc|^2)$.
Niech teraz $a, b, c, d \in A$, $d(a,b) = d(c,d) = D(A)$ i niech x będzie środkiem ab, y — środkiem cd.
Z trójkąta aby mamy

$$|xy|^2 = \frac{1}{4}(2|ay|^2 + 2|by|^2 - |ab|^2),$$

a z trójkątów acd i bcd mamy:

$$|ay|^2 = \frac{1}{4}(2|ac|^2 + 2|ad|^2 - |cd|^2) \text{ i}$$

$$|by|^2 = \frac{1}{4}(2|bc|^2 + 2|bd|^2 - |cd|^2).$$

Ponieważ jednak $|ac|$, $|ad|$, $|bc|$, $|bd|$ są nie większe niż $D(A)$, natomiast $|ab| = |cd| = D(A)$, mamy:

$$|ay|^2 \leqslant \frac{3}{4}(D(A))^2, \quad |by|^2 \leqslant \frac{3}{4}(D(A))^2$$

i wreszcie

$$|xy|^2 \leqslant \frac{1}{4}\cdot(3(D(A))^2 - (D(A))^2) = \frac{1}{2}(D(A))^2,$$

a więc $d(x, y) \leqslant \frac{\sqrt{2}}{2} D(A)$.
Wynika stąd, wobec dowolności w wyborze a, b, c, d, że

$$D(S(A)) \leqslant \frac{\sqrt{2}}{2} D(A) \qquad \text{c.n.d.}$$

Gdy teraz A jest czworościanem foremnym o krawędzi 1, zbiór $S(A)$ jest, jak łatwo sprawdzić, zbiorem środków krawędzi A i $D(S(A)) = \frac{\sqrt{2}}{2} D(A)$.