ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE XXX (1993)

wmptm 1897

Władysław Narkiewicz (Wrocław)

Ministerstwo Nauki i Szkolnictwa Wyższego

Wielkie Twierdzenie Fermata

1. *Nie można rozdzielić sześcianu na dwa sześciany, ani bikwadratu na dwa bikwadraty, ani, ogólniej, żadnej potęgi wyższej od drugiej na dwie takież potęgi. Znalazłem zaprawdę zadziwiający dowód tego, lecz margines ten jest zbyt wąski, by go zmieścić.*

Te dwa zdania, napisane przez Fermata ([Fe], Observatio 2) na marginesie rozdziału o kwadratowych równaniach diofantycznych w wydanych przez Bacheta dziełach Diofantesa, stoją u kolebki jednego z najsławniejszych zagadnień matematycznych. Polega ono na znalezieniu dowodu następującego twierdzenia, nazywanego zwykle Wielkim Twierdzeniem Fermata (WTF):

Twierdzenie 0. *Dla $n \geqslant 3$ równanie*

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

nie ma rozwiązań w liczbach naturalnych X, Y, Z.

Od 300 lat problem ten przyciąga uwagę zarówno specjalistów jak i amatorów. Naszym celem będzie przedstawienie jego związków z resztą matematyki.

Będziemy używali następujących oznaczeń:

$\mathbb{Z}$ oznacza pierścień liczb całkowitych, a $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ oznaczają odpowiednio ciało liczb wymiernych, rzeczywistych i zespolonych, $\mathbb{F}_l$ jest ciałem skończonym o l elementach, a literą $\mathbb{A}$ oznaczamy ciało wszystkich liczb algebraicznych. Przez $\mathbb{Q}_p$ będziemy oznaczali ciało liczb p-adycznych, a $\mathbb{Z}_p$ oznaczać będzie pierścień liczb całkowitych p-adycznych.

Wreszcie ζ_n będzie oznaczać n-ty pierwotny pierwiastek z jedności.

2. Nietrudno zauważyć, że ze słuszności WTF dla pewnego wykładnika n wynika jego prawdziwość dla wszystkich wielokrotności n. Ponieważ każda liczba naturalna większa od jedności i nie będąca potęgą dwójki ma nieparzysty dzielnik pierwszy, przeto wystarczy udowodnić WTF dla wszystkich n, będących liczbami pierwszymi $\neq 2$ oraz dla $n = 4$. W tym ostatnim przypadku dowód został podany przez Fermata ([Fe], Observatio 42), który

zastosował tu swoją „*metodę spadku*", wykorzystując znany już wówczas opis wszystkich rozwiązań równania Pitagorasa

$$X^2 + Y^2 = Z^2 \tag{2}$$

w liczbach całkowitych [1]. Fermat udowodnił w istocie nieco inne twierdzenie, dowodząc nieistnienia trójkąta prostokątnego o całkowitych bokach i polu, będącym kwadratem liczby naturalnej, ale po drodze jego rozumowanie daje następujący wynik:

TWIERDZENIE 1. *Równanie* $X^4+Y^4 = Z^2$ *nie ma rozwiązań naturalnych.*

D o w ó d. Załóżmy, że równanie

$$(X^2)^2 + (Y^2)^2 = X^4 + Y^4 = Z^2$$

ma rozwiązania naturalne i przyjmijmy, że $Z > 0$ jest minimalne. Bez szkody dla ogólności można założyć, że X jest liczbą parzystą, a Y nieparzystą. Z opisu rozwiązań równania Pitagorasa wynika istnienie względnie pierwszych liczb naturalnych $u > v$ takich, że $X^2 = 2uv, Y^2 = u^2 - v^2$ i $Z = v^2 + u^2$. Nietrudno zauważyć, że v musi być parzyste, a ponieważ $u^2 = Y^2 + v^2$, przeto powtarzając poprzednie rozumowanie otrzymujemy istnienie względnie pierwszych liczb całkowitych a, b, spełniających $v = 2ab$, $Y = a^2 - b^2$ i $u = a^2 + b^2$. To prowadzi do

$$X^2 = 2uv = 4ab(a^2 + b^2),$$

skąd wynika, że liczby a, b, $a^2 + b^2$ są kwadratami, ponieważ są parami względnie pierwsze:

$$a = x^2, \qquad b = y^2, \qquad a^2 + b^2 = z^2$$

Ostatecznie otrzymujemy

$$x^4 + y^4 = z^2,$$

co z uwagi na $0 < z < Z$ daje sprzeczność. □

Z uwagi na to twierdzenie w dalszym ciągu będziemy zajmowali się równaniem

$$X^p + Y^p = Z^p, \tag{3}$$

gdzie p jest nieparzystą liczbą pierwszą. Wygodnie jest czasem zapisać to równanie w postaci symetrycznej

$$X^p + Y^p + Z^p = 0, \tag{4}$$

Można przy tym założyć, że liczby X, Y, Z nie mają wspólnego dzielnika > 1, gdyż w przeciwnym razie podzielilibyśmy obie strony (4) przez jego p-tą

[1] Jeśli liczby X, Y, Z spełniają (2), X, Y są względnie pierwsze, a Y jest nieparzysta, to istnieją względnie pierwsze liczby całkowite u, v takie, że $X = 2uv$, $Y = u^2 - v^2$ i $Z = u^2 + v^2$.

potęgę. Tradycyjnie rozróżnia się tu dwa przypadki: tzw. *pierwszy przypadek* WTF, gdy dodatkowo zakładamy, że żadna z liczb X, Y, Z nie dzieli się przez p i *drugi przypadek*, gdy $p \mid XYZ$.

3. Na następny krok czekano ponad 100 lat. W 1770 roku ukazał się *Wstęp do algebry* Eulera [E], zawierający w §242 dowód WTF w przypadku $n = 3$. Euler korzystał w nim z pewnych własności arytmetycznych formy kwadratowej $x^2 + 3y^2$, nie podając ich uzasadnienia, tak więc przez długi czas uważano ten dowód za niekompletny. Sprawa wyjaśniła się dopiero w naszych czasach, gdy spostrzeżono, że brakujące uzasadnienie wynika bez większego trudu z jednej z prac Eulera z 1760 roku [2]. Gauss zauważył, że stosunkowo prosty dowód wyniku Eulera można uzyskać przy użyciu arytmetyki pierścienia $\mathbb{Z}[\zeta_3]$. Najprostszą znaną wersję tego dowodu podali H. B. Mann i W. A. Webb [MW] w 1978 roku:

TWIERDZENIE 2. *W przypadku $n = 3$ równanie (1) nie ma niezerowych rozwiązań całkowitych.*

D o w ó d. Niech liczby x, y, z będą całkowitymi rozwiązaniami (1) dla $n = 3$, dla których liczba $|xyz| > 0$ jest minimalna. Wtedy liczby te są parami względnie pierwsze. Gdyby żadna z nich nie dzieliła się przez 3, to ich trzecie potęgi dawałyby reszty 1 lub 8 z dzielenia przez 9, a zatem mielibyśmy

$$x^3 + y^3 \not\equiv z^3 \pmod 9.$$

Możemy więc bez szkody dla ogólności przyjąć, że z dzieli się przez 3, a nadto $x \equiv 1 \pmod 3$ i $y \equiv 2 \pmod 3$. Wówczas $z^3 \equiv 0 \pmod{27}$ i z uwagi na $z^3 = x^3 + y^3 = (x+y)(x^2 - xy + y^2)$ i $(x+y, x^2 - xy + y^2) = 3$ otrzymujemy $x + y = 9a^3$ oraz $x^2 - xy + y^2 = 3b^3$ przy odpowiednich całkowitych a, b, przy czym $3 \nmid b$.

Teraz wykorzystamy kilka prostych własności pierścienia Eisensteina

$$R = \{u + v\zeta_3 : u, v \in \mathbb{Z}\}.$$

Jest to pierścień z jednoznacznością rozkładu na czynniki nierozkładalne, a jedynymi jego elementami odwracalnymi są liczby $\pm 1, \pm\zeta_3$, oraz $\pm\zeta_3^2$. W R mamy rozkład

$$x^2 - xy + y^2 = (x + \zeta_3 y)(x + \zeta_3^2 y),$$

a z uwagi na $(x + \zeta_3 y, x + \zeta_3^2 y) = 1 - \zeta_3$ oraz $(1 - \zeta_3)^2 = -3\zeta_3$ otrzymujemy

$$x + \zeta_3 y = \alpha(1 - \zeta_3)(u + v\zeta_3)^3,$$

gdzie $\alpha \in R$ jest elementem odwracalnym, a $u, v \in \mathbb{Z}$. Dzieląc przez $1 - \zeta_3$ otrzymujemy

$$\alpha(u + v\zeta_3)^3 = c + 3a^3\zeta_3,$$

[2] Patrz [Ber].

przy czym $c = \frac{1}{3}(2x - y)$ jest liczbą całkowitą, nie dzielącą się przez 3. Stąd $\alpha(u^3 + v^3) \equiv c \pmod 3$, a zatem α przystaje mod 3 do pewnej liczby całkowitej wymiernej. Bezpośrednie sprawdzenie pokazuje, że jest to możliwe jedynie dla $\alpha = 1$ i $\alpha = -1$. Zmieniając w razie konieczności znaki liczb u i v możemy przyjąć, że $\alpha = 1$. Wówczas

$$c + 3a^3\zeta_3 = u^3 - 3uv^2 + v^3 + (3u^2v - 3uv^2)\zeta_3,$$

a więc $a^3 = uv(u - v)$. Liczby $u, v, u - v$ są parami względnie pierwsze, co daje ostatecznie $u = k^3$, $v = l^3$ i $u - v = m^3$; widzimy, że k, l, m spełniają $l^3 + m^3 = k^3$, co wobec $0 < |klm| < |xyz|$ jest sprzeczne z naszym założeniem. □

4. W następnych latach dowodzono WTF dla poszczególnych małych wykładników [3], ale dopiero E. E. Kummer w połowie ubiegłego stulecia dokonał istotnego kroku naprzód [4]. Zastosował on stworzoną przez siebie teorię tzw. *liczb idealnych* [5] do udowodnienia WTF dla dużej klasy wykładników pierwszych. By je sformułować, musimy wpierw zdefiniować *liczby pierwsze regularne*. Można to uczynić na kilka równoważnych sposobów. Używając terminologii algebraicznej teorii liczb najprościej powiedzieć, że *liczba pierwsza p jest regularna, jeśli liczba klas ideałów* [6] *pierścienia $\mathbb{Z}[\zeta_p]$ nie dzieli się przez p*. Można warunek ten sformułować też następująco: *jeśli I jest niegłównym ideałem w pierścieniu $\mathbb{Z}[\zeta_p]$, to I^p też nie jest ideałem głównym.*

Klasyczna definicja używa liczb Bernoulliego: *liczba pierwsza p jest regularna, jeśli licznik żadnej z liczb $B_2, B_4, \ldots, B_{p-3}$ nie dzieli się przez p.*

---

[3] Dla $n = 5$ Dirichlet [D1] i Legendre [Le1], [Le2], dla $n = 14$ Dirichlet [D2], dla $n = 7$ Lamé [L1].

[4] Cytowana czasem historia o tym, jakoby Kummer miał podać dowód WTF, w którym Dirichlet znalazł błąd, jest plotką, powstałą na zasadzie znanej opowieści „Czy to prawda, że w Moskwie na Placu Czerwonym rozdają samochody? W zasadzie prawda, ale nie w Moskwie...". Historia ta bierze swój początek w przemówieniu K. Hensela po śmierci Kummera i jest powtórzona w [Di], ale wydaje się, że w rzeczywistości sprawa dotyczy pracy G.Lamé [L2], opublikowanej w 1847 r., w której autor podał dowód WTF opierając się na twierdzeniu o jednoznaczności rozkładu w pierścieniach $Z[\zeta_p]$. Liouville [Li] zwrócił uwagę na brak dowodu tego twierdzenia, a Kummer w liście do Liouville'a [K1] stwierdził, że jest ono wręcz fałszywe. Szczegóły tej historii są opisane w [Bel].

[5] Teoria ta doprowadziła z czasem dzięki pracom R. Dedekinda do wytworzenia się podstawowych pojęć nowoczesnej algebry.

[6] Mówimy, że dwa ideały I, J w pierścieniu przemiennym R są *równoważne*, jeśli istnieją niezerowe elementy $\alpha, \beta \in R$ spełniające $\alpha I = \beta J$. W pierścieniach $Z[\zeta_p]$, rozważanych przez Kummera, ilość powstałych w ten sposób klas równoważności jest skończona i jest nazywana *liczbą klas*. Liczba ta mierzy odchylenie R od pierścieni z jednoznacznością rozkładu. Dla tych ostatnich liczba klas wynosi 1.

Przypomnijmy, że liczby Bernoulliego B_n są zdefiniowane przez równość [7]

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} z^n.$$

Istnieje także definicja zupełnie elementarna: *liczba pierwsza p jest regularna, jeśli dla $k = 1, 2, \ldots, (p-3)/2$ suma*

$$1 + 2^{2k} + 3^{2k} + \cdots + (p-1)^{2k}$$

nie dzieli się przez p^2.

Można sprawdzić, co uczynił już Kummer, że wśród liczb pierwszych mniejszych od 100 jedynie 37, 59 i 67 nie są regularne. W istocie, 67 dzieli licznik B_{58}, równy

844 836 133 488 004 186 204 675 994 036 021,

liczba 59 dzieli licznik B_{44} równy

27 833 269 579 301 024 235 023 = 11 · 59 · 8089 · 2 947 939 · 1 798 482 437,

a liczba 37 dzieli licznik B_{32} równy

7 709 321 041 217 = 37 · 683 · 305 065 927.

TWIERDZENIE 3. (E. E. Kummer [K2], 1850) *Jeśli liczba pierwsza $p > 2$ jest regularna, to WTF jest prawdziwe dla wykładnika p.*

Nie wiemy do dzisiaj, czy liczby pierwsze, których to twierdzenie dotyczy, tworzą zbiór nieskończony [8].

W roku 1857 Kummer [K3] zastosował swą teorię do dowodu WTF dla niektórych liczb pierwszych nieregularnych, w tym dla $p = 37$, 59 i 67. W ten sposób otrzymał jego prawdziwość dla wszystkich wykładników pierwszych mniejszych od 100. Dowód ten miał pewne luki, wypełnione siedemdziesiąt lat później przez H. S. Vandivera [Va].

W ostatnich latach, dzięki technice komputerowej, metody Kummera i ich późniejsze wzmocnienia doprowadziły do udowodnienia WTF dla wszystkich wykładników pierwszych mniejszych od czterech milionów [Bu].

5. W 1909 roku istotny postęp został dokonany w pierwszym przypadku WTF. A. Wieferich [Wi] udowodnił, że jeśli w tym przypadku dla wykładnika p równanie (3) ma rozwiązanie, to zachodzi kongruencja

$$2^{p-1} \equiv 1 \pmod{p^2}. \tag{6}$$

[7] Ponieważ nietrudno spostrzec, że dla $k = 1, 2, \ldots$ mamy $B_{2k+1} = 0$, niektórzy autorzy używają innej numeracji dla liczb Bernoulliego, opuszczając te, które są równe 0.

[8] Za to od 1915 roku wiadomo, że nieregularnych liczb pierwszych jest nieskończenie wiele [J].

Znane są jedynie dwie liczby pierwsze p, spełniające tę kongruencję, a mianowicie 1093 i 3511, a jak sprawdził w 1984 roku D. H. Lehmer, nie ma innych w przedziale $[3512, 6 \cdot 10^9]$.

Wkrótce po wyniku Wiefericha D. Mirimanoff [Mi] udowodnił, że w wypadku fałszywości WTF dla wykładnika p w pierwszym przypadku, obok kongruencji (5) musi być także spełniony warunek

$$3^{p-1} \equiv 1 \pmod{p^2}. \tag{6}$$

Nie wiemy, czy istnieje choćby jedna liczba pierwsza, spełniająca równocześnie oba warunki (5) i (6). Dalszy rozwój wydarzeń doprowadził do istotnego wzmocnienia warunków koniecznych fałszywości WTF w tym przypadku. Niedawno A. Granville i M. B. Monagan [GM] pokazali, że jeśli WTF jest fałszywe w pierwszym przypadku dla wykładnika p, to dla wszystkich liczb $q \leqslant 89$ mamy

$$q^{p-1} \equiv 1 \pmod{p^2}.$$

Rezultat ten pozwolił na udowodnienie WTF w tym przypadku dla wszystkich liczb pierwszych $p < 7.568 \cdot 10^{17}$ [C].

6. Dalszy postęp w pierwszym przypadku WTF uzyskali w 1985 roku L. Adleman i D. R. Heath-Brown [AH] [8], dowodząc prawdziwości WTF w tym przypadku dla nieskończenie wielu wykładników pierwszych. Zastosowali oni metodę, która swój początek bierze w następującym elementarnym twierdzeniu, udowodnionym w 1823 roku przez Sophie Germain:

TWIERDZENIE 4. *Jeśli p i $q = 2p + 1$ są liczbami pierwszymi, to dla wykładnika p WTF jest prawdziwe w pierwszym przypadku.*

W podobny sposób Legendre [Le1] pokazał, że liczbę $2p + 1$ można tu zastąpić przez $2kp + 1$ dla $k = 2, 4, 5, 7$ i 8. Adleman i Heath-Brown zastosowali pomysł z pracy E. Wendta [We] z 1894 roku i udowodnili, że jeśli k nie dzieli się przez 3, pierwszy przypadek WTF jest fałszywy dla liczby pierwszej p, a $2kp + 1$ jest liczbą pierwszą, to p należy do pewnego skończonego zbioru T_k, mającego co najwyżej ck^2 elementów, gdzie c jest pewną stałą.

Niech teraz A oznacza zbiór wszystkich liczb pierwszych, dla których WTF jest w pierwszym przypadku fałszywe. Powyższe oszacowanie liczebności zbioru T_k łatwo prowadzi do stwierdzenia, że dla dowolnych liczb $y < x$ ilość par $[p, q]$ (gdzie p przebiega liczby pierwsze z A, zawarte w przedziale $(y, x]$, a $q = 2kp + 1$ jest liczbą pierwszą, przy czym $3 \nmid k$) nie przekracza $c_1(x/y)^3$ przy pewnej stałej c_1. Z drugiej strony E. Fouvry [Fo] pokazał, że dla $y = x^\vartheta$ przy pewnym $\vartheta > 2/3$ liczba $N_\vartheta(x)$ takich par, przy opuszczeniu warunku $p \in A$, spełnia

$$N_\vartheta(x) \geqslant c_2 \frac{x}{\log x}$$

[8] Por. [HB].

(przy pewnym $c_2 > 0$) i przez proste porównanie otrzymujemy istnienie liczby pierwszej $p > x^9$ nie należącej do A. Wobec dowolności x daje to nieskończenie wiele liczb pierwszych, dla których WTF jest prawdziwe w pierwszym przypadku.

7. Kolejny ważny krok został uzyskany w 1983 roku metodami geometrii algebraicznej. Wówczas G. Faltings [F1] udowodnił *hipotezę Mordella*, z której natychmiast wynika następujący wniosek:

TWIERDZENIE 5. *Dla każdej ustalonej liczby naturalnej $n \geqslant 4$ równanie (1) może mieć jedynie skończenie wiele względnie pierwszych rozwiązań całkowitych X, Y.*

Wniosek ten formułuje się zgrabniej w języku geometrycznym:

TWIERDZENIE 6. *Na krzywej o równaniu $X^n + Y^n = 1$ może leżeć co najwyżej skończenie wiele punktów o współrzędnych wymiernych.*

Inaczej,

TWIERDZENIE 7. *Na krzywej o równaniu*

$$X^n + Y^n + Z^n = 0 \tag{7}$$

na płaszczyźnie rzutowej może leżeć co najwyżej skończenie wiele punktów o współrzędnych wymiernych.

By sformułować hipotezę Mordella potrzebne jest pojęcie *rodzaju krzywej algebraicznej*. Ograniczymy się przy tym do krzywych bez punktów osobliwych. Niech Γ będzie krzywą na zespolonej płaszczyźnie rzutowej, określoną równaniem $f(X,Y,Z) = 0$, przy czym f jest jednorodnym wielomianem trzech zmiennych o zespolonych współczynnikach. Punkt $P = (x,y,z) \in \Gamma$ nazywa się *punktem osobliwym* krzywej Γ, jeśli

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = \frac{\partial f}{\partial z}(P) = 0.$$

Jeśli założymy, że Γ nie ma punktów osobliwych, czyli jest *krzywą nieosobliwą*, to jej *rodzaj* $g(\Gamma)$ definiuje się wzorem

$$g(\Gamma) = \frac{1}{2}(n-1)(n-2),$$

gdzie n oznacza stopień wielomianu f.

TWIERDZENIE 8. (Twierdzenie Faltingsa — Hipoteza Mordella) *Jeśli wielomian f ma współczynniki wymierne, krzywa Γ jest nieosobliwa oraz $g(\Gamma) \geqslant 2$, to na Γ leży jedynie skończenie wiele punktów o współrzędnych wymiernych* [10].

[10] Liczby wymierne można tu zastąpić przez liczby z dowolnego ustalonego skończonego rozszerzenia ciała liczb wymiernych.

Ponieważ krzywa (7) jest nieosobliwa, zatem jej rodzaj dla $n \geqslant 4$ jest równy co najmniej 2 i można do niej stosować wynik Faltingsa. Niestety, żaden ze znanych dowodów ([Bo], [F1], [F2], [V2]) tego wyniku nie jest efektywny, tj. nie daje możliwości wyznaczenia wszystkich punktów wymiernych na (7). Jednakże A. N. Paršin [11] pokazał, że przy zastosowaniu metod D. Mumforda [Mu] i S. J. Arakelova [Ar] z dowodu Faltingsa można otrzymać efektywne oszacowanie liczby tych punktów.

8. W ostatnich latach odkryto powiązania twierdzenia Fermata z krzywymi eliptycznymi, formami modułowymi i reprezentacjami grupy Galois ciała $\mathbb{A}$. By móc je opisać, przytoczymy krótko podstawowe pojęcia i fakty tych teorii [12].

Niech $\mathbf{G}$ będzie grupą Galois rozszerzenia $\mathbb{A}/\mathbb{Q}$, tj. grupą wszystkich automorfizmów ciała $\mathbb{A}$. Przyjmując za bazę otoczeń jedności rodzinę grup Galois rozszerzeń $\mathbb{A}/K$, przy czym K przebiega wszystkie skończone rozszerzenia $\mathbb{Q}$, wprowadza się w $\mathbf{G}$ topologię, tzw. *topologię Krulla.* W tej topologii $\mathbf{G}$ staje się zwartą grupą topologiczną, a przy tym istnieje wzajemnie jednoznaczna odpowiedniość pomiędzy podciałami ciała $\mathbb{A}$ a domkniętymi podgrupami $H \subset \mathbf{G}$, dana przez

$$H \longleftrightarrow \mathbb{A}^H = \{a \in \mathbb{A} : h(a) = a \text{ dla wszystkich } h \in H\}.$$

Przyda się też później informacja, że do każdej liczby pierwszej l istnieje w $\mathbf{G}$ pewna klasa elementów sprzężonych (tzw. *automorfizmy Frobeniusa*), złożona z wszystkich elementów $g \in \mathbf{G}$ o następującej własności:

Jeśli liczba l jest nierozgałęziona [13] *w rozszerzeniu $K/\mathbb{Q}$, a M jest dowolnym ideałem maksymalnym pierścienia $\mathbb{Z}_K$ liczb całkowitych K, który zawiera l, to dla wszystkich $x \in \mathbb{Z}_K$ mamy*

$$g(x) - x^l \in M.$$

Przez Frob_l będziemy oznaczali dowolny automorfizm Frobeniusa, odpowiadający liczbie l.

9. Przejdziemy teraz do krzywych eliptycznych i rozpoczniemy od klasycznego przypadku krzywych zdefiniowanych nad ciałem liczb zespolonych.

---

[11] Dowód jest przedstawiony w odczytach M. Raynaud i L. Szpiro w [Sz].

[12] Przystępne wprowadzenia do tych teorii znaleźć można np. w [Hu], [Ko], [La1], [La2], [S1], [S2], [Si].

[13] Liczba pierwsza l jest *nierozgałęziona* w skończonym rozszerzeniu M/Q, jeśli nie dzieli wyróżnika $d(M)$ ciała M, lub, co na jedno wychodzi, ideał generowany przez l w pierścieniu liczb całkowitych ciała M nie jest zawarty w kwadracie żadnego ideału maksymalnego tego pierścienia.

Krzywą eliptyczną będziemy nazywać nieosobliwą krzywą $E \subset \mathbb{C}^2$, o równaniu

$$Y^2 = f(X), \tag{8}$$

gdzie f jest wielomianem 3 stopnia o współczynnikach zespolonych. Łatwo widzieć, że tym wypadku nieosobliwość oznacza, że wielomian f nie ma pierwiastków wielokrotnych. Przez nieosobliwe przekształcenie liniowe można każdą taką krzywą sprowadzić do postaci

$$Y^2 = 4X^3 + aX + b, \tag{9}$$

przy czym $a, b \in \mathbb{C}$. Jest to tzw. *postać weierstrassowska krzywej eliptycznej*. Do tak zdefiniowanej krzywej dołącza się jeszcze punkt w nieskończoności, tak by otrzymać krzywą zwartą.

Z klasycznej teorii funkcji eliptycznych wynika istnienie liniowo niezależnych (nad $\mathbb{R}$) liczb zespolonych ω_1, ω_2 takich, że jeśli $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subset \mathbb{C}^2$ jest generowaną przez nie grupą addytywną, to związana z nią funkcja Weierstrassa

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

spełnia równanie różniczkowe

$$\wp'(z)^2 = 4\wp(z)^3 + a\wp(z) + b,$$

a zatem dla dowolnego $z \in \mathbb{C} \setminus \Lambda$ punkt $P(z) = (\wp(z), \wp'(z))$ leży na E. Funkcja $\wp(z)$ jest dwuokresowa z okresami podstawowymi ω_1, ω_2, a przeto można ją traktować jako funkcję określoną na grupie ilorazowej $\mathbb{C}/\Lambda$. Nietrudno pokazać, że układ

$$\wp(z) = z_1, \qquad \wp'(z) = z_2$$

ma przy dowolnych z_1, z_2 dokładnie jedno rozwiązanie $z \in \mathbb{C}/\Lambda$, przeto odwzorowanie $\mathbb{C}/\Lambda \longrightarrow E$ dane przez $z \mapsto P(z)$ jest wzajemnie jednoznaczne.

Odwzorowanie to pozwala przenieść z $\mathbb{C}/\Lambda$ na E strukturę grupy abelowej. Grupa ta jest izomorficzna z torusem $\mathbb{R}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Z}$, a zatem jej podgrupa torsyjna E_{tor}, złożona z elementów rzędu skończonego, jest sumą prostą 2 egzemplarzy podgrupy torsyjnej grupy $\mathbb{R}/\mathbb{Z}$. Ponieważ $\mathbb{R}/\mathbb{Z}$ jest izomorficzna z multyplikatywną grupą liczb zespolonych o module 1, jej podgrupa torsyjna jest izomorficzna z grupą wszystkich pierwiastków z jedności, a stąd wynika w szczególności, że podgrupa E_N grupy E złożona z elementów $x \in E$ spełniających $Nx = 0$ jest dla każdego naturalnego N izomorficzna z $C_N \oplus C_N$.

Działanie na krzywej (8) można wyrazić przez współrzędne, używając funkcji wymiernych. Pozwala to na wprowadzenie (po dodaniu do tej krzywej tzw. punktu w nieskończoności) struktury grupy abelowej na zbiorach $E =$

$\Gamma \cup \{\infty\}$, gdzie Γ jest nieosobliwą krzywą w k^2 (przy czym k jest dowolnym ciałem), zdefiniowaną przez równanie postaci

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{10}$$

($a_i \in k$), a punkt ∞ jest zerem E (por. [T]). W przypadku ciał o charakterystyce różnej od 2 i 3, łatwo sprowadzić to równanie do postaci (9).

W dalszym ciągu ograniczymy się do krzywych eliptycznych, które są zdefiniowane przez równanie o współczynnikach wymiernych.

Niech $E \subset \mathbb{C}^2 \cup \{\infty\}$ będzie taką krzywą, zadaną równaniem postaci (10). *Wyróżnik* $\Delta(E)$ definiujemy dość zawiłym wzorem

$$\Delta(E) = 9b_2b_4b_6 - 27b_6^2 - 8b_4^3 - b_2^2b_8,$$

przy czym

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = a_1a_3 + 2a_4,$$
$$b_6 = a_3^2 + 4a_6, \qquad b_8 = (b_2b_6 - b_4^2)/4.$$

W przypadku, gdy E jest dana równaniem (8), nietrudno dostrzec związek $\Delta(E)$ z wyróżnikiem wielomianu f.

Niech teraz l będzie liczbą pierwszą. Przez odpowiednią zmianę układu współrzędnych możemy doprowadzić równanie E do takiej postaci, w której wszystkie współczynniki a_i mają mianowniki niepodzielne przez l, a licznik wyróżnika $\Delta(E)$ jest podzielny przez możliwie najmniejszą potęgę l. Taką postać nazywamy *postacią minimalną równania krzywej* E względem liczby l lub też *modelem minimalnym* E. Załóżmy, że równanie (10) ma postać minimalną. Jeśli zastąpimy w nim każdy ze współczynników przez jego resztę z dzielenia przez l, to otrzymamy pewną krzywą w $\mathbb{F}_l^2$, którą oznaczmy przez $E^{(l)}$. Jeśli jest ona nieosobliwa, to mówimy, że E ma *dobrą redukcję* mod l. Zachodzi to dokładnie wtedy, gdy licznik $\Delta(E)$ nie dzieli się przez l. Jeśli ten przypadek nie zachodzi, ale licznik $b_2^2 - 24b_4$ nie dzieli się przez l, to mówimy, że E ma *multyplikatywną redukcję* mod l.

Jeśli dla każdej liczby pierwszej krzywa E ma redukcję dobrą lub multyplikatywną, to mówimy, że E jest *semistabilna*.

10. Z tego, iż równanie E ma współczynniki wymierne, wynika bez trudu, że współrzędne elementów rzędu skończonego grupy E są liczbami algebraicznymi i że grupa Galois $\mathbf{G}$ rozszerzenia $\mathbb{A}/\mathbb{Q}$ działa na grupie E_{tor} wszystkich takich elementów jako grupa automorfizmów. Przy tym grupy $E_N \subset E_{\text{tor}}$ są niezmiennicze, tj. dla dowolnego automorfizmu $\sigma \in \mathbf{G}$ mamy

$$\sigma(E_N) = E_N.$$

Niech p będzie nieparzystą liczbą pierwszą, dla której krzywa (10) ma dobrą redukcję; rozpatrzmy ciąg grup

$$E_p \subset E_{p^2} \subset \ldots \subset E_{p^n} \subset \ldots$$

wraz z homomorfizmami $E_{p^n} \longrightarrow E_{p^{n-1}}$, wyznaczonymi przez mnożenie przez p. Otrzymujemy w ten sposób granicę wsteczną $T_p(E)$ grup E_{p^n}. Iloczyn tensorowy $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, gdzie $\mathbb{Q}_p$ oznacza ciało liczb l-adycznych, a $\mathbb{Z}_p$ pierścień jego liczb całkowitych, nazywa się *modułem Tate'a* krzywej E. Ponieważ grupa E_{p^k} jest izomorficzna z $C_{p^k} \oplus C_{p^k}$, przeto działanie $\sigma \in \mathbf{G}$ na E_{p^k} można opisać za pomocą pewnej macierzy z $GL_2(\mathbb{Z}/p^k\mathbb{Z})$. W ten sposób każdemu elementowi $\sigma \in \mathbf{G}$ można przypisać pewną macierz z $GL_2(\mathbb{Z}/p^k\mathbb{Z})$. Przyporządkowanie to jest homomorfizmem, a zatem otrzymujemy rodzinę dwuwymiarowych reprezentacji G nad pierścieniami reszt mod p^k:

$$\varphi_{p^k} : \mathbf{G} \longrightarrow GL_2(\mathbb{Z}/p^k\mathbb{Z}).$$

Nietrudno zauważyć, że odwzorowanie φ_{p^k} jest ciągłe, a nadto w przypadku $k_1 \geqslant k_2$ dla dowolnego $\sigma \in \mathbf{G}$ mamy

$$\varphi_{p^{k_1}}(\sigma) \bmod p^{k_2} = \varphi_{p^{k_2}}(\sigma).$$

Ten ostatni warunek pokazuje, że grupa $\mathbf{G}$ działa na V_p jako grupa automorfizmów, przy czym grupę V_p traktujemy tu jako $\mathbb{Z}_p$-moduł. W ten sposób otrzymujemy ciągłą reprezentację

$$\pi_p : \mathbf{G} \longrightarrow GL_2(\mathbb{Z}_p). \tag{11}$$

Nakładając na nią redukcję mod p, otrzymujemy reprezentację

$$\varphi_p : \mathbf{G} \longrightarrow GL_2(\mathbb{F}_p), \tag{12}$$

11. Oznaczmy przez $E(\mathbb{Q})$ zbiór punktów E o wymiernych współrzędnych. Okazuje się, że jest on podgrupą grupy E. L. J. Mordell [Mo] udowodnił w 1922 roku, że grupa $E(\mathbb{Q})$ jest postaci $F \oplus Z^r$, przy czym $r \geqslant 0$, a F jest grupą skończoną [14]. Strukturę tej grupy [15] opisał B. Mazur [M], pokazując, że jest ona cykliczna rzędu m przy $m \leqslant 10$ lub $m = 12$, lub też jest postaci $C_2 \oplus C_{2m}$ dla $m \leqslant 4$. W szczególności grupa ta nie zawiera elementów rzędu p, gdy p jest liczbą pierwszą większą od 7.

12. W zastosowaniu do twierdzenia Fermata fundamentalną rolę odgrywają krzywe eliptyczne zdefiniowane przez równanie postaci

$$Y^2 = X(X - A)(X + B), \tag{13}$$

[14] Wynik Mordella został przeniesiony przez A. Weila [W] na rozmaitości abelowe (rozmaitości algebraiczne, mające strukturę grupy abelowej, w której działanie jest zdefiniowane przez funkcje wymierne) nad dowolnym skończonym rozszerzeniem Q, a następnie A. Néron [N1] otrzymał ten wynik dla dowolnych ciał skończenie generowalnych nad swym podciałem prostym. Dowód znaleźć można także w [La3].

[15] O ile struktura grupy F jest dobrze zbadana, o tyle wielkość r pozostaje nadal tajemnicza. Nie wiadomo, na przykład, czy liczba ta może być dowolnie duża.

gdzie A, B są liczbami całkowitymi, przy czym $A \equiv 1 \pmod 4$ oraz $B \equiv 0 \pmod{2^5}$. Nietrudno pokazać, że dla nieparzystych liczb pierwszych l równanie (13) jest minimalne, co daje, że dla tych liczb pierwszych E ma dobrą redukcję wtedy i tylko wtedy, gdy l nie dzieli $AB(A+B)$, a jeśli warunek ten nie jest spełniony, to redukcja jest multyplikatywna. W przypadku $l = 2$ okazuje się [16], że również otrzymujemy multyplikatywną redukcję, a więc krzywa (13) jest semi-stabilna. Zobaczymy niżej, że fakt ten decyduje o sukcesie pomysłu zastosowania krzywych eliptycznych do problemu Fermata.

Przydatność krzywych (13) do zagadnienia Fermata zauważył G. Frey [Fr], a L. Szpiro [Sz2] pokazał, że stosując do nich jego hipotezę o wyróżniku można uzyskać twierdzenie Fermata. Hipoteza ta, postawiona w 1982 roku, głosi w przypadku krzywych eliptycznych E, zdefiniowanych nad ciałem liczb wymiernych, że dla każdego $\varepsilon > 0$ mamy

$$\Delta(E) \leqslant C(\varepsilon) N_E^{6+\varepsilon},$$

gdzie [17] N_E jest przewodnikiem E. Definicja przewodnika w ogólnym przypadku krzywej (10) jest zbyt skomplikowana, by ją tu przytaczać (korzysta się w niej z minimalnego modelu krzywej eliptycznej A. Nérona [N2] (p. także [Hu], rozdz. 14), ale dla naszych celów wystarczy wiedzieć, że przewodnikiem krzywej (13) jest iloczyn dzielników pierwszych liczby $AB(A+B)$.

13. Przechodzimy teraz do *parabolicznych form modułowych*. Oznaczmy przez Γ grupę macierzy 2×2 o całkowitych współczynnikach i wyznaczniku równym jedności, niech N będzie liczbą naturalną i niech

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma : N \mid c \right\}.$$

Ponadto niech $\mathcal{H}$ oznacza górną półpłaszczyznę zespoloną $\{z \in \mathbb{C} : \Im z > 0\}$ i niech $k \geqslant 2$. Funkcja $F(z)$ regularna na $\mathcal{H}$ nazywa się *paraboliczną formą modułową* typu (N, k), jeśli są spełnione następujące warunki:

(i) $F(z)$ przedstawia się w postaci szeregu

$$F(z) = \sum_{n=1}^{\infty} A_n q^n \tag{14}$$

zbieżnego dla wszystkich $z \in \mathcal{H}$, przy czym $q = \exp(2\pi i z)$;

(ii) Dla każdej macierzy $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$ funkcja

$$(cz+d)^{-k} F\left(\frac{az+b}{cz+d}\right)$$

---

[16] Patrz np. [Fr], [S3]

[17] Jak pokazał D. W. Masser [Ms] w nierówności tej nie można zastąpić wykładnika 6 przez liczbę mniejszą. Interesujące wnioski z hipotezy Szpiro są podane w [HS] i [V1].

da się przedstawić w postaci szeregu postaci

$$\sum_{n=1}^{\infty} A_n(\gamma)(\exp(2\pi iz/N)^n;$$

(iii) Dla $z \in \mathcal{H}$ i dla każdej macierzy $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$ mamy

$$F\left(\frac{az+b}{cz+d}\right) = (cz+d)^k F(z).$$

Pierwsze dwa warunki można sformułować też w inny sposób: grupa $\Gamma_0(N)$ działa przez homografie na $\mathcal{H}$ i ma tam spójny obszar fundamentalny D, który nie jest zwarty, ale daje się uzwarcić przez dodanie punktu w nieskończoności oraz skończenie wielu tzw. *punktów parabolicznych*, tj. takich punktów r na prostej rzeczywistej, dla których istnieje homografia $\gamma \in \Gamma_0(N)$, której r jest jedynym punktem stałym (γ ma tę własność wtedy i tylko wtedy, gdy $\pm\gamma$ nie jest macierzą jednostkową, a ślad γ jest równy ± 2). Bazą otoczeń takiego punktu jest rodzina zbiorów złożonych z r i z wnętrz okręgów leżących w $\mathcal{H}$ i stycznych do prostej rzeczywistej w punkcie r. Otrzymuje się w ten sposób zwartą przestrzeń topologiczną $X_0(N)$, mającą strukturę analityczną. Warunki (i) i (ii) oznaczają, że funkcja $F(z)$ przedłuża się w sposób ciągły na $X_0(N)$ i jest równa zeru w każdym punkcie zbioru $X_0(N) \setminus D$.

Nietrudno spostrzec, że zbiór $S(N,2)$ wszystkich form parabolicznych typu $(N,2)$ jest przestrzenią liniową nad $\mathbb{C}$. Dla dowodu twierdzenia Fermata ważny jest następujący wzór (patrz np. [CO], [Sh]:

$$\dim_{\mathbb{C}} S(2,2) = 0. \tag{15}$$

14. W przestrzeni $S(N,2)$ działa rodzina

$$\{T_p : p \text{ pierwsze}, \ p \nmid N\} \cup \{U_p : p \text{ pierwsze}, \ p|N\}$$

tzw. *operatorów Heckego* ([He], [AL]) zdefiniowanych dla form F postaci (14) poprzez

$$T_p(F) = \sum_n A_{pn} q^n + p \sum_n A_n q^{pn}$$

oraz

$$U_p(F) = \sum_n A_{pn} q^n.$$

Z formami parabolicznymi, które są wektorami własnymi dla wszystkich operatorów Heckego, związane jest pojęcie *reprezentacji modułowej*, które teraz omówimy. Niech f będzie taką niezerową formą typu $(N,2)$, dla której $A_1 = 1$ i która jest wektorem własnym dla wszystkich operatorów T_p. Załóżmy ponadto, że wszystkie współczynniki A_n w (14) są całkowite. Jak

pokazał P. Deligne (patrz [DS], tw. 6.1), istnieje wówczas ciągła reprezentacja

$$\rho_f : \mathbf{G} \longrightarrow GL_2(\mathbb{Z}_p) \tag{16}$$

grupy $\mathbf{G}$, spełniająca następujące warunki:

(i) Reprezentacja ρ_f jest półprosta,

(ii) Jeśli $l \nmid pN$, to ślad macierzy $\rho_f(\mathrm{Frob}_l)$ równy jest współczynnikowi a_l, a jej wyznacznik jest równy l.

Każda reprezentacja otrzymana w ten sposób nazywa się *modułowa*. Z każdą reprezentacją modułową ρ_p związana jest reprezentacja R_p nad ciałem p-elementowym $\mathbb{F}_p$, powstała przez zastąpienie elementów macierzy reprezentacji ρ_p przez ich reszty mod p.

Przypuszcza się (*hipoteza Weila-Taniyamy*), że jeśli E jest krzywą eliptyczną, l jest liczbą pierwszą, a reprezentacja π_l dana wzorem (11) jest nieprzywiedlna, to jest ona reprezentacją modułową, odpowiadającą pewnej formie modułowej typu $(N,2)$, gdzie N jest przewodnikiem E. Przy tym forma ta nie zależy od l. Krzywe E, dla których to zachodzi, nazywa się *krzywymi modułowymi*.

15. Teraz pokażemy, jak omówione pojęcia i rezultaty stosują się do problemu Fermata [18].

Niech $X = a$, $Y = b$, $Z = c$ będą liczbami naturalnymi, bez wspólnego dzielnika > 1, spełniającymi równanie (4), przy czym $p \geqslant 5$. Zamieniając ewentualnie rolami te liczby możemy, bez szkody dla ogólności, przyjąć, że $a \equiv 1 (\mathrm{mod}\ 4)$ oraz $b \equiv 0 (\mathrm{mod}\ 2)$. Niech $E_p(a,b,c)$ będzie krzywą eliptyczną o równaniu

$$y^2 = x(x - a^p)(x + b^p). \tag{17}$$

Jej przewodnik N jest równy iloczynowi liczb pierwszych dzielących abc.

TWIERDZENIE 9. *Krzywe $E_p(a,b,c)$ nie są krzywymi modułowymi.*

Załóżmy, że krzywa ta jest modułowa i niech reprezentacja φ_p będzie zadana przez (12). Jak pokazał J.P. Serre [S3], jej przywiedlność prowadziłaby do istnienia krzywej eliptycznej mającej punkt rzędu p o współrzędnych wymiernych, a to dla $p > 7$ nie jest możliwe, dzięki wynikowi B. Mazura [M]. Istnieje zatem forma paraboliczna $F \in S(N,2)$ o tej własności, że φ_p pokrywa się z reprezentacją R_p, związaną z F. Okazuje się, że istnieją formy paraboliczne o tej samej własności, należące do $S(M,2)$, przy czym M jest właściwym dzielnikiem N. Jest to konsekwencją wyniku B. Mazura i K. Ribeta [R], którzy pokazali, że jeśli

$$R_l : \mathbf{G} \longrightarrow GL(2,\mathbb{F}_l)$$

[18] Idea ta występuje po raz pierwszy w [Fr]. Por. [S3] i [R].

jest ciągłą modułową reprezentacją, odpowiadającą pewnej formie parabolicznej f typu $(2, N)$, p jest liczbą pierwszą dzielącą N, p^2 nie dzieli N, wówczas przy pewnych technicznych założeniach o R_l, jeśli $p \not\equiv 1 (\mathrm{mod}\ l)$ lub $(l, N) = 1$, to istnieje forma modułowa w $S(2, N/p)$, której odpowiada ta sama reprezentacja R_l. Spełnienie założeń tego twierdzenia w przypadku nieparzystych liczb pierwszych p i reprezentacji związanej z krzywą $E_p(a, b, c)$ wynika z rezultatów [S3]. Teraz łatwo widać, że ρ_p odpowiada pewnej formie parabolicznej typu (2,2) i wystarczy sobie przypomnieć, że wobec (15) forma ta musi być zerowa, co jest niemożliwe, bo φ_p jest nieprzywiedlna.

16. Ponieważ krzywe $E_p(a, b, c)$ są semistabilne, do dowodu twierdzenia Fermata pozostało pokazać, że każda semistabilna krzywa musi być modułowa. Dowód tego faktu zaprezentował A. Wiles w czerwcu 1993 na konferencji w Cambridge. Nie jest on jeszcze opublikowany, ale z krążących nieoficjalnych informacji wynika, że został on podzielony na pięć części i każda jest sprawdzana przez wybitnego specjalistę. Podobno dowód wymaga jeszcze pewnych uściśleń (mówi się, że jest luka w tej części dowodu, w której stosuje się grupy kohomologii), ale specjaliści są dobrej myśli i wiele wskazuje na to, że po trzystu latach doczekamy się rozwiązania jednego z najsławniejszych problemów matematyki.

Jak napisał hamburski tygodnik *Die Zeit*: „*Jetzt hat die liebe Seele Ruh.*"

Literatura

[AH] L. M. Adleman, D. R. Heath-Brown, *The first case of Fermat's last theorem*, Inv. Math. 79 (1985), 409–416.

[Ar] S. J. Arakelov, *Теория пересечений дивизоров на арифметической поверхности*, Izv. Akad. Nauk SSSR 38 (1974), 1179–1192.

[AL] A. O. L. Atkin, J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. 185 (1970), 134–160.

[Bel] B. Belhoste, *Augustin-Louis Cauchy*, Springer 1991.

[Ber] G. Bergmann, *Über Euler's Beweis des grossen Fermatschen Satzes für den Exponenten 3*, Math. Ann. 164 (1966), 159–175.

[Bo] E. Bombieri, *The Mordell conjecture revisited*, Ann. Scoula Norm. Sup Pisa, Cl. Sci. (4), 17 (1990), 615–640. Err. *ibidem*, (4), 18 (1991), 473.

[Bu] J. P. Buhler, R. E. Crandall, R. Ernvall, T. Metsänkylä, *Irregular primes and cyclotomic invariants to four milions*, Math. Comp. 61 (1993), 151–153.

[C] D. Coppersmith, *Fermat's Last Theorem (Case I) and the Wieferich criterion*, Math. Comp. 54 (1990), 895–902.

[CO] H. Cohen, J. Oesterlé, *Dimensions des espaces de formes modulaires*, Modular Functions of One Variable, VI, Lecture Notes in Math. 627 (1977), 69–78.

[DS] P. Deligne, J.-P. Serre, *Formes modulaires de poids 1*, Ann. Sci. Ec. Norm. Sup. 7 (1974), 507–530.

[Di] L. E. Dickson, *History of the Theory of Numbers*, Washington 1919–1923. Reprint: Chelsea 1952 i 1966.

[D1] P. G. L. Dirichlet, *Mémoire sur l'impossibilité de quelques équations indéterminées du 5^e degré*, J. reine angew. Math. 3 (1828), 354–375.

[D2] P. G. L. Dirichlet, *Démonstration du théorème de Fermat pour les 14^e puissances*, J. reine angew. Math. 9 (1832), 390–393.

[E] L. Euler, *Vollständige Anleitung in die Algebra*, St. Petersburg 1770. Przedruk: *Opera omnia* I. 1, Teubner 1911.

[F1] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inv. math. 73 (1983), 349–366. Err.: *ibidem* 75 (1984), 381.

[F2] G. Faltings, *Diophantine approximation on abelian varieties*, Annals of Math. (2), 133 (1991), 549–576.

[Fe] P. Fermat, *Observationes Domini Petri de Fermat*, Oeuvres, I, 289–342, Paris 1891.

[Fo] E. Fouvry, *Théorème de Brun-Titchmarsh. Application au théorème de Fermat*, Inv. math. 79 (1985), 383–407.

[Fr] G. Frey, *Links between stable elliptic curves and certain diophantine equations*, Ann. Univ. Saraviensis, ser. math. 1 (1986), 1–40.

[GM] A. Granville, M. B. Monagan, *The first case of Fermat's Last Theorem is true for all prime exponents up to 714 591 416 091 389*, Trans. Amer. Math. Soc. 306 (1988), 329–359.

[HB] D. R. Heath-Brown, *The first case of Fermat's Last Theorem*, Math. Intelligencer 7 (1985), No. 4, 40–47 i 55.

[HS] M. Hindry, J. H. Silverman, *The canonical height and integral points on elliptic curves*, Inv. math. 93 (1988), 419–450.

[Hu] D. Husemöller, *Elliptic curves*, Springer 1986.

[J] K. L. Jensen, *Om talteoretiske Egenskaber ved de Bernoulliske tal*, Nyt Tidsskr. Mat. B26 (1915), 73–83.

[K1] E. E. Kummer, *Extrait d'une lettre de M. Kummer à M. Liouville*, J. de math. pures et appl. 12 (1847), 136.

[K2] E. E. Kummer, *Allgemeiner Beweis des Fermatschen Satzes, daß die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenige Potenz-Exponenten λ, welche ungerade Primzahlen sind und in die Zählern der ersten $\frac{1}{2}(\lambda-3)$ Bernoulli'schen Zahlen als Factoren nicht vorkommen*, J. reine angew. Math. 40 (1850), 130–138.

[K3] E. E. Kummer, *Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten complexen Zahlen, für den Fall, daß die Klassenzahl durch λ theilbar ist, nebst Anwendungen derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes*, Math. Abhandl. Kgl. Preuß. Akad. Wiss. Berlin, 1857, 41–74.

[Ko] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer 1984.

[L1] G. Lamé, *Mémoire d'analyse indéterminée démontrant que l'equation $x^7+y^7 = z^7$ est impossible en nombres entiers*, J. de math. pures et appl. 5 (1840), 195–211.

[L2] G. Lamé, *Démonstration générale du théorème de Fermat sur l'impossibilité en nombres entiers de l'équation $x^n + y^n = z^n$*, Comptes Rendus Acad. Sci. Paris 24 (1847), 310–314.

[La1] S. Lang, *Elliptic functions*, Addison-Wesley 1973.

[La2] S. Lang, *Introduction to modular forms*, Springer 1976.

[La3] S. Lang, *Fundamentals of diophantine geometry*, Springer 1983.

[Le1] A. M. Legendre, *Sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat*, Mem. Acad. Roy. Sci. de l'Institut de France, 6 (1823), 1–60.

[Le2] A. M. Legendre, *Théorie des nombres*, III wydanie, Paris 1830.

[Li] J. Liouville, *Remarques à l'occasion d'une communication de M. Lamé sur un théorème de Fermat*, Comptes Rendus Acad. Sci. Paris 24 (1847), 315–316.

[M] B. Mazur, *Rational points on modular curves*, w: „Modular Functions in One Variable, V", Lecture Notes in Math. 601 (1976), 107–148.

[Mi] D. Mirimanoff, *Sur le dernier théorème de Fermat et le critérium de M. A. Wieferich*, Enseignement Math. 11 (1909), 455–459.

[Mo] L. J. Mordell, *On the rational solutions of the indeterminate equation of the third and the fourth degrees*, Proc. Cambridge Philos. Soc. 21 (1922), 179–192.

[Ms] D. W. Masser, *Note on a conjecture of Szpiro*, Astérisque, 183 (1990), 19–23.

[Mu] D. Mumford, *A remark on Mordell's conjecture*, American J. Math. 87 (1965), 1007–1016.

[MW] H. B. Mann, W. A. Webb, *A short proof of Fermat's theorem for $n = 3$*, Math. Student 46 (1978), 103–104.

[N1] A. Néron, *Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps*, Bull. Soc. Math. France, 80 (1952), 101–166.

[N2] A. Néron, *Modéles minimaux des variétés abéliennes sur les corps locaux et globaux*, Publ. Math. IHES 21 (1964), 361–482.

[Oe] J. Oesterlé, *Nouvelles approches du "théorème" de Fermat*, Astérisque 161–162 (1988), 165–186.

[R] K. Ribet, *On modular representations of $Gal(\bar{Q}/Q)$ arising from modular forms*, Inv. math. 100 (1990), 431–476.

[S1] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, Benjamin 1968.

[S2] J.-P. Serre, *Cours d'arithmétique*, Paris 1970.

[S3] J.-P. Serre, *Sur les représentations modulaires de degré 2 de $Gal(\bar{Q}/Q)$*, Duke Math. J. 54 (1987), 179–230.

[Sh] G. Shimura, *Introduction to Arithmetic Theory of Automorphic Functions*, Princeton 1971.

[Si] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer 1985.

[Sz1] G. Szpiro (redaktor), *Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell*, Astérisque 127 (1985).

[Sz2] — *Discriminant et conducteur des courbes elliptiques*, Astérisque, 183 (1990), 7–18.

[T] J. Tate, *The arithmetic of elliptic curves*, Inv. math. 23 (1974), 179–206.

[Va] H. S. Vandiver, *Summary of results and proofs concerning Fermat's last theorem*, Proc. Nat. Acad. Sci. U.S.A. 12 (1926), 106–109, 767–772.

[V1] P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Math. (1239), 1987.

[V2] P. Vojta, *Siegel's theorem in the compact case*, Annals of Math. (2), 133 (1991), 509–548.

[W] A. Weil, *L'arithmétique sur les courbes algébriques*, Acta Mathematica, 52 (1928), 281–315.

[We] E. Wendt, *Arithmetische Studien über den letzten Fermatschen Satz, welcher aussagt, daß die Gleichung $a^n = b^n + c^n$ für $n > 2$ in ganzen Zahlen nicht auflösbar ist*, J. reine angew. Math. 113 (1894), 335–346.

[Wi] A. Wieferich, *Zum letzten Fermat'schen Theorem*, J. reine angew. Math. 136 (1909), 293–302.