

ANDRZEJ DĄBROWSKI (Szczecin)*

Modularność krzywych eliptycznych i Wielkie Twierdzenie Fermata

Pamięci Moich Rodziców

Artykuł jest rozszerzoną wersją wykładu „Modularność krzywych eliptycznych: dowód, zastosowania i uogólnienia”, wygłoszonego przez autora we wrześniu 2006 roku na I Forum Matematyków Polskich w Gdańsku.

Głównym jego celem jest przybliżenie kluczowych kroków dowodu Wielkiego Twierdzenia Fermata udowodnionego przez A. Wileasa w 1994 roku (związły szkic dowodu czytelnik znajdzie w paragrafie 16.6). W rozdziałach 18 i 19 formułujemy twierdzenia ogólniejsze od Wielkiego Twierdzenia Fermata oraz przytaczamy szereg otwartych problemów.

Proste wprowadzenie do tej problematyki w języku polskim czytelnik znajdzie w wartym polecenia artykule Narkiewicza [88] oraz ostatnim rozdziale książki Ribenoima [96].

Dowód Wielkiego Twierdzenia Fermata podany przez Wileasa [131] jest jednym z najdonioślejszych osiągnięć matematycznych XX wieku. Dzięki wcześniejszemu rezultatowi Ribeta [97], wystarczyło udowodnić tzw. hipotezę o modularności dla klasy semistabilnych krzywych eliptycznych. Dowód tej hipotezy jest głównym rezultatem Wileasa zastosowanym w dowodzie Wielkiego Twierdzenia Fermata. Realizacja tego programu, mimo przejrzystego planu, wymagała wypracowania i połączenia metod z wielu dziedzin matematyki.

Przedstawimy przykład ilustrujący wspomnianą hipotezę o modularności. Rozważmy ciąg $a_p := p - R_p$ liczb całkowitych indeksowany przez liczby pierwsze $p \geq 2$, gdzie R_p oznacza liczbę rozwiązań równania $y^2 = x^3 + 1$ w zbiorze $\{0, 1, \dots, p-1\}$. Łatwo sprawdzić, że $a_2 = 2$, $a_3 = a_5 = 0$, $a_7 = -4$,

* Artykuł został napisany podczas pobytu w Max-Planck-Institut für Mathematik w Bonn w semestrze jesienno-zimowym 2006/2007. Autor pragnie podziękować Instytutowi za wspaniałą atmosferę naukową i wsparcie finansowe.

$a_{11} = 0, a_{13} = 2, a_{17} = 0, a_{19} = 8, a_{23} = 0, \dots$. Niech $\sum_{n=1}^{\infty} b_n X^n$ będzie formalnym szeregiem potęgowym określonym następująco:

$$\begin{aligned} \sum_{n=1}^{\infty} b_n X^n &= X \prod_{n=1}^{\infty} (1 - X^{6n})^4 \\ &= X - 4X^7 + 2X^{13} + 8X^{19} - 5X^{25} + \dots \end{aligned}$$

Zauważmy, że $b_1 = 1$ oraz $a_p = b_p$ dla $p = 2, 3, \dots, 23$. Dowodzi się ponadto, że równość ta zachodzi dla wszystkich p . Czytelnik może się przekonać, że dla (małych) p i $r = 2, 3, \dots$ mamy $b_{pr} = b_p b_{p^{r-1}} - p b_{p^{r-2}}$ oraz $b_{mn} = b_m b_n$, gdy $(m, n) = 1$. Można oczywiście udowodnić te równości dla dowolnych p oraz r . Dalsze przykłady krzywych E stopnia 3, dla których istnieje szereg $\sum b_n(E) X^n$ spełniający $a_p(E) = b_p(E)$ oraz zachodzą relacje dla b_n , wynikają z analizy przykładów w rozdziałach 2.6 i 3.9.

Hipoteza Shimury-Taniyamy-Weila (STW) o modularności (rozdział 15) głosi, że zjawisko takie ma miejsce dla wszystkich krzywych eliptycznych określonych nad ciałem \mathbb{Q} liczb wymiernych. K. Ribet [97] udowodnił w 1986 roku, bazując na idei G. Freya [46], że prawdziwość powyższej hipotezy dla podklasy tzw. semistabilnych krzywych eliptycznych implikuje Wielkie Twierdzenie Fermata. Idea dowodu jest bardzo prosta (rozdz. 16.6; 12.2): z hipotetycznym, nietrywialnym, rozwiązaniem równania Fermata stowarzysza się krzywą eliptyczną o „dziwnych własnościach”, po czym dowodzi się, przy założeniu powyższej hipotezy, że taka krzywa nie istnieje. Od lata 1986 roku A. Wiles usilnie próbował udowodnić hipotezę STW. W 1993 roku przedstawił strategię dowodu, zaś w 1994 roku pełny dowód hipotezy w przypadku semistabilnym i tym samym, dowód Wielkiego Twierdzenia Fermata. Dowód zawarty jest w dwóch artykułach [131] i [123]; jeden wspólny z R. Taylorem. W 1999 roku C. Breuil, B. Conrad, F. Diamond i R. Taylor [10] uzyskali dowód hipotezy STW w pełnej ogólności. Hipoteza STW i jej uogólnienia (np. program Langlandsa), bogactwo aparatu wykorzystanego w dowodach oraz konsekwencje z pewnością pozostaną w centrum uwagi wielu pokoleń specjalistów pracujących w arytmetycznej geometrii algebraicznej.

Ribenboim [96] przedstawił badania nad Wielkim Twierdzeniem Fermata w ujęciu historycznym, dokonując także przeglądu błędnych dowodów. Książka Singha [118] jest niezwykle opowieścią o zmaganiach wielu pokoleń matematyków z tym najsłynniejszym problemem matematycznym. Wprowadzenia do artykułów Wileasa i Taylora adresowane dla szerokiego grona odbiorców na ogół nie zawierają szczegółów, jednak polecamy [88], [48], [42], [101], [24], [126]. Czytelnik z większym przygotowaniem matematycznym, pragnący poznać szczegóły, powinien dodatkowo zaopatrzyć się w [20], [16], [27], [57], [92], [106]; książka Diamonda i Shurmana [35] jest idealnym wstępem do wymienionych pozycji.

W artykule pragniemy jednocześnie przedstawić zwięzły wstęp do arytmetycznej teorii krzywych eliptycznych i form modularnych, podać wybrane szczegóły dowodu Wielkiego Twierdzenia Fermata i wprowadzić czytelnika w orbitę aktualnych rezultatów i hipotez. Lektura poniższej pracy może wymagać pewnego zaangażowania, ale mamy nadzieję, że pomoże lepiej zorientować się w tej pięknej i zarazem trudnej dziedzinie badań.

Systematyczny opis pojęć i rezultatów omawianych w pierwszych pięciu rozdziałach czytelnik znajdzie np. w [116], [35], [67]. Konstrukcje opisane w dalszej części artykułu są zaopatrzone w odnośniki do literatury.

Podstawowe pojęcia i rezultaty z algebry przemiennej (pierścienie przemienne, ciała, moduły) i elementy algebry homologicznej czytelnik znajdzie w [1], [11], [4], [3], [74]. Przystępne wprowadzenie do algebraicznej teorii liczb zawierają pozycje [8], [89], [128], [62], [38], [15]. Ponadto warto zaglądać do podręczników z geometrii algebraicznej [95], [109], [71], [53].

W dalszym ciągu symbolem \mathbb{Z} oznaczamy pierścień liczb całkowitych, zaś $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ są ciałami liczb wymiernych, rzeczywistych i zespolonych, odpowiednio. Przez \mathbb{Q}_p będziemy oznaczać ciało liczb p -adycznych, a przez \mathbb{Z}_p pierścień liczb całkowitych p -adycznych. \mathbb{F}_q jest ciałem skończonym o q elementach. \overline{K} oznacza domknięcie algebraiczne ciała K .

Podziękowanie. Składam gorące podziękowanie profesorowi Danielowi Simsonowi za cenne uwagi i zaproponowanie wielu poprawek, które pozwoliły ulepszyć tekst artykułu.

1. Krzywe eliptyczne

1.1. Podstawowe definicje. Zaczniemy od anegdoty. *Któregoś razu dwóch wybitnych specjalistów z geometrii algebraicznej, Chevalley i Zariski, rozpoczęło dyskusję przy tablicy na temat krzywych algebraicznych, przy czym nie mogli nawzajem siebie zrozumieć. W pewnym momencie Chevalley zapytał Zariskiego czym dla niego jest krzywa i sprawa natychmiast się wyjaśniła. Zariski bez wahania bowiem narysował przykład krzywej. W odpowiedzi Chevalley wyjaśnił, że dla niego krzywa to równanie $f(x, y) = 0$. Dla przykładu, krzywą o równaniu $x^2 + y^2 - 1 = 0$ każdy potrafi narysować, ale równanie $x^2 + y^2 + 1 = 0$ nie ma rozwiązań w zbiorze liczb rzeczywistych (w obu przypadkach zbiór wszystkich rozwiązań zespolonych tworzy „krzywą zespoloną”). Zauważmy ponadto, że pierwsze równanie posiada rozwiązanie w dowolnym ciele, zaś drugie nie posiada rozwiązań dla nieskończenie wielu ciał (np. dla dowolnego podciała ciała liczb rzeczywistych lub ciał \mathbb{F}_p dla $p \equiv 3 \pmod{4}$).*

Niech $\mathbb{A}^n = \mathbb{A}_K^n = \{(x_1, \dots, x_n) : x_i \in \overline{K}\}$ oznacza n -wymiarową przestrzeń afiniczną nad ciałem K . Niech $V \subset \mathbb{A}^n$ będzie zbiorem algebraicznym określonym nad K (tj. zbiorem zer układu wielomianów n zmiennych

o współczynnikach z K). Dla dowolnego rozszerzenia L ciała K , zawartego w \overline{K} , określamy *zbiór punktów L -wymiernych na V* jako $V(L) := \{(x_1, \dots, x_n) \in \mathbb{A}^n \cap V : x_i \in L\}$. Podobnie postępujemy dla zbiorów algebraicznych w przestrzeni rzutowej \mathbb{P}^n . Zauważmy, że V jest funktorem $L \mapsto V(L)$. Ogólniej, dla schematów X , S można określić $X(S)$ jako zbiór morfizmów $S \rightarrow X$. Ten punkt widzenia jest bardzo ważny we współczesnej geometrii algebraicznej.

Specjalista łatwo zrozumie następującą informację. *Krzywą eliptyczną* określoną nad ciałem K nazywamy nieosobliwą, rzutową krzywą algebraiczną E genuśu 1 z wyróżnionym punktem $P_0 \in E(K)$. Korzystając z twierdzenia Riemanna-Rocha można określić w naturalny sposób strukturę grupy abelowej na zbiorze $E(K)$, w taki sposób, że P_0 staje się elementem neutralnym działania grupowego (patrz np. [53]).

Niespecjaliście może być trudniej. Na szczęście dowolną krzywą eliptyczną można określić prościej – za pomocą jednego równania. Okazuje się bowiem, że krzywa eliptyczna określona nad ciałem K jest izomorficzna z nieosobliwą płaską krzywą rzutową zadaną (afinicznym) równaniem (tzw. *równanie lub model Weierstrassa*):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad \text{gdzie } a_i \in K.$$

W tym przypadku

$$E(L) := \{(\alpha, \beta) \in L \times L : \beta^2 + a_1\alpha\beta + a_3\beta = \alpha^3 + a_2\alpha^2 + a_4\alpha + a_6\} \cup \{\infty\}.$$

Struktura grupowa na $E(L)$ posiada prostą interpretację geometryczną: suma trzech punktów jest elementem neutralnym (w tym przypadku jest to punkt $[0, 1, 0]$ w nieskończoności) wtedy i tylko wtedy, gdy leżą one na jednej prostej. Stąd łatwo wyprowadzić jawne formuły na dodawanie punktów na krzywej eliptycznej. W przypadku krzywej eliptycznej E określonej nad \mathbb{C} , dodawanie na $E(\mathbb{C})$ można wyrazić w terminach funkcji eliptycznych.

Przyjmijmy:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, & b_4 &= a_1a_3 + 2a_4, & b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_2 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \end{aligned}$$

oraz

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6, \quad j = c_4^3/\Delta.$$

Niech $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ oznacza *wyróżnik* powyższego równania. Zatem warunek $\Delta \neq 0$ oznacza nieosobliwość krzywej zadanej tym równaniem.

Dwie krzywe eliptyczne określone nad K są *izomorficzne* (nad K), jeśli równanie jednej z nich może być otrzymane z równania drugiej za pomocą zamiany współrzędnych

$$x = u^2X + r, \quad y = u^3Y + su^2X + t$$

przy pewnych $r, s, t \in K$, $u \in K \setminus \{0\}$. Zatem współczynniki a'_i drugiej krzywej wyrażają się za pomocą współczynników a_i pierwszej krzywej następująco:

$$\begin{aligned} ua'_1 &= a_1 + 2s, \\ u^2a'_2 &= a_2 - sa_1 + 3r - s^2, \\ u^3a'_3 &= a_3 + ra_1 + 2t, \\ u^4a'_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st, \\ u^6a'_6 &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \end{aligned}$$

oraz

$$c'_4 = u^{-4}c_4, \quad c'_6 = u^{-6}c_6, \quad \Delta' = u^{-12}\Delta, \quad j' = j =: j_E.$$

W przypadku $K = \mathbb{Q}$ taka zamiana zmiennych, przy odpowiednim doborze u , prowadzi do równania (modelu) o współczynnikach całkowitych. Wśród wszystkich modeli ustalonej krzywej istnieje taki, dla którego $|\Delta|$ jest minimalne; nazywamy go *globalnym modelem minimalnym* (lub *globalnym minimalnym równaniem Weierstrassa*) krzywej eliptycznej E . Taki model nie jest wyznaczony jednoznacznie, ale izomorficzne modele minimalne spełniają warunki $u = \pm 1$, $r, s, t \in \mathbb{Z}$. Wśród wszystkich modeli minimalnych istnieje dokładnie jeden, tzw. *zredukowany globalny model minimalny*, spełniający $a_1, a_3 \in \{0, 1\}$, $a_2 \in \{-1, 0, 1\}$. Wyróżnik globalnego równania minimalnego krzywej eliptycznej E określonej nad \mathbb{Q} nazywamy *wyróżnikiem krzywej E* i oznaczamy Δ_E .

Niech K będzie skończonym rozszerzeniem ciała \mathbb{Q} oraz $h(K)$ liczbą klas ideałów (patrz, np. [89], [8]). Wiadomo [116], że krzywa eliptyczna określona nad K posiada globalny model minimalny (o współczynnikach algebraicznych całkowitych należących do K) wtedy i tylko wtedy, gdy $h(K) = 1$.

P r z y k ł a d. Ustalmy $a, b, c \in \mathbb{Z}$ ($abc \neq 0$ oraz $(a, b, c) = 1$) spełniające $a + b + c = 0$. Rozważmy krzywą eliptyczną $E_{a,b,c}$ nad \mathbb{Q} zadaną równaniem $y^2 = x(x - a)(x + b)$. Załóżmy, że $a \equiv -1 \pmod{4}$ oraz $16|b$. Zamiana zmiennych $x = 4X$, $y = 8Y + 4X$ prowadzi do równania (o całkowitych współczynnikach)

$$Y^2 + XY = X^3 + \frac{b - a - 1}{4}X^2 - \frac{ab}{16}X.$$

Mamy więc

$$c_4 = -(ab + ac + bc), \quad c_6 = \frac{(b - a)(c - b)(a - c)}{2}, \quad \Delta = \left(\frac{abc}{16}\right)^2.$$

W szczególności $(c_4, \Delta) = 1$. Zatem powyższe równanie zadaje globalny model minimalny krzywej $E_{a,b,c}$.

Równanie Weierstrassa o zerowym wyróżniku określa osobliwą krzywą sześcienną E . W tym przypadku E posiada dokładnie jeden punkt osobliwy, który może być *punktem podwójnym* (dwie różne styczne) lub *ostrzem* (jedna

styczna). Dla przykładu, $y^2 = x^2(x + 5)$ posiada punkt podwójny, zaś $y^2 = x^3$ posiada ostrze.

1.2. Redukcja krzywej eliptycznej. Niech E będzie krzywą eliptyczną określoną nad \mathbb{Q} . Dla liczby pierwszej p oznaczmy przez \overline{E}_p krzywą określoną nad \mathbb{F}_p , powstałą przez redukcję modulo p współczynników globalnego minimalnego równania Weierstrassa. Mówimy, że (i) E posiada *dobrą redukcję* w p , gdy \overline{E}_p jest nieosobliwa. (ii) E posiada *addytywną redukcję* w p , gdy \overline{E}_p posiada ostrze. (iii) E posiada *multyplikatywną redukcję* w p , gdy \overline{E}_p posiada punkt podwójny.

W sytuacjach (ii), (iii) mówimy, że E posiada *złą redukcję* w p . Typy redukcji można odczytać z globalnego minimalnego równania Weierstrassa w następujący sposób ([116], Prop. 5.1):

- (i) E posiada dobrą redukcję w p wtedy i tylko wtedy, gdy $v_p(\Delta_E) = 0$;
- (ii) E posiada addytywną redukcję w p wtedy i tylko wtedy, gdy $v_p(\Delta_E) > 0$, $v_p(c_4) > 0$;
- (iii) E posiada multiplykatywną redukcję w p wtedy i tylko wtedy, gdy $v_p(\Delta_E) > 0$, $v_p(c_4) = 0$.

Przyjmijmy $a_p := p + 1 - \#\overline{E}_p(\mathbb{F}_p)$. Przypomnijmy z ([116], p. 240) następujące kryterium:

Niech $p|\Delta_E$. Wówczas (i) E posiada addytywną redukcję w p wtedy i tylko wtedy, gdy $a_p = 0$; (ii) E posiada multiplykatywną redukcję w p wtedy i tylko wtedy, gdy $a_p = \pm 1$.

Krzywa eliptyczna określona nad \mathbb{Q} jest *semistabilna*, jeśli jej redukcja w p jest dobra lub multiplykatywna. Krzywa $E_{a,b,c}$ z Przykładu jest semistabilna, gdyż posiada dobrą redukcję w liczbach p względnie pierwszych z $\frac{abc}{16}$, oraz multiplykatywną redukcję w $p|\frac{abc}{16}$. Nietrudno udowodnić, że dla dowolnej krzywej eliptycznej E określonej nad \mathbb{Q} mamy $\Delta_E \neq \pm 1$. Przy tym, najniższa możliwa wartość $|\Delta_E|$ wynosi 11. Okazuje się, że zbiór klas \mathbb{Q} -izomorficznych krzywych eliptycznych określonych nad \mathbb{Q} , posiadających dobrą redukcję poza ustalonym skończonym zbiorem liczb pierwszych, jest skończony (tw. Shafarevicha; patrz [110], [105], [116]).

Przewodnik N_E krzywej eliptycznej E mierzy arytmetyczną złożoność krzywej: $N_E := \prod_{p|\Delta_E} p^{f_p}$, gdzie $f_p = 1$ (2, odpowiednio $2 + \delta_p$) jeśli E posiada multiplykatywną redukcję w p (posiada addytywną redukcję w $p \neq 2, 3$, odpowiednio posiada addytywną redukcję w $p = 2$ lub 3). Przy tym $0 \leq f_2 \leq 8$ oraz $0 \leq f_3 \leq 5$ (szczegóły w [117]).

L. Szpiro sformułował w 1983 roku następującą hipotezę: *dla dowolnego $\epsilon > 0$ istnieje $\kappa(\epsilon) > 0$ takie, że $|\Delta_E| < \kappa(\epsilon)N_E^{6+\epsilon}$ dla wszystkich E . Można pokazać, że 6 w wykładniku nie można zastąpić przez liczbę mniejszą.*

U w a g a. D. Masser i J. Oesterlé [91] sformułowali w 1985 roku następującą hipotezę (znaną obecnie pod nazwą *hipotezy abc*): dla dowolnego $\epsilon > 0$ istnieje $C(\epsilon) > 0$ takie, że

$$\max(|a|, |b|, |c|) \leq C(\epsilon)(\text{rad}(abc))^{1+\epsilon}$$

dla wszystkich trójek (a, b, c) niezerowych względnie pierwszych liczb całkowitych spełniających warunek $a + b + c = 0$; powyżej $\text{rad}(abc)$ oznacza iloczyn wszystkich liczb pierwszych dzielących abc .

Hipoteza Szpiro implikuje wariant hipotezy abc z wykładnikiem $6/5 + \epsilon$. Hipoteza abc implikuje hipotezę Szpiro (patrz [91]) i posiada szereg innych ważnych konsekwencji (patrz, np. [90]) oraz jest szczególnym przypadkiem hipotez Vojty [127] (arytmetyczny wariant teorii Nevanlinny) dotyczących wysokości punktów na rozmaitościach algebraicznych. Jednak wielu wybitnych specjalistów wątpi w jej prawdziwość.

1.3. L -funkcja krzywej eliptycznej. Niech E będzie krzywą eliptyczną określoną nad \mathbb{Q} . L -funkcją Hassego-Weila krzywej E nazywamy funkcję zespoloną $L(E, s)$ określoną przez iloczyn eulerowski

$$L(E, s) := \prod_p (1 - a_p p^{-s} + \varepsilon(p) p^{1-2s})^{-1}, \quad \text{Re}(s) > 3/2,$$

gdzie $\varepsilon(p) = 1$ (odpowiednio 0), jeśli E posiada dobrą (odpowiednio złą) redukcję w p . Postać czynnika eulerowskiego pochodzi od lokalnej zeta funkcji

$$Z(E/\mathbb{F}_p, T) = \frac{1 - a_p T + pT^2}{(1 - T)(1 - pT)}$$

redukcji E modulo p . Nierówność Hassego $|a_p| < 2\sqrt{p}$ implikuje, że powyższy iloczyn eulerowski jest zbieżny bezwzględnie w półpłaszczyźnie $\text{Re}(s) > 3/2$, gdzie zadaje funkcję holomorficzną.

Hasse w latach 30-tych ubiegłego stulecia wysunął przypuszczenie, że $L(E, s)$ przedłuża się do funkcji holomorficzej na całej płaszczyźnie zespolonej i spełnia równanie funkcyjne wiążące s z $2 - s$. W celu precyzyjnego sformułowania hipotezy przyjmijmy $\Lambda(E, s) := N_E^{s/2} (2\pi)^{-s} \Gamma(s) L(E, s)$, gdzie $\varepsilon(E) \in \{\pm 1\}$ oznacza tzw. *globalną liczbę pierwiastkową* [18], [50].

HIPOTEZA 1 (HASSE). *Funkcja zespolona $\Lambda(E, s)$ przedłuża się do funkcji całkowitej oraz spełnia równanie funkcyjne $\Lambda(E, s) = \varepsilon(E)\Lambda(E, 2 - s)$.*

Hipoteza powyższa jest obecnie udowodniona (patrz 15.3).

2. Formy modularne

2.1. Podstawowe definicje i własności. Przykłady krzywych eliptycznych znajdujemy w „Arytmetyce” Diofantosa (patrz np. [130], rozdz. 6).

Funkcje modularne (tj. formy modularne wagi zero) pojawiły się natomiast dopiero w XIX wieku; pierwszy systematyczny wykład na ten temat zawierał traktat F. Kleina i R. Frickego „Vorlesungen über die Theorie der elliptischen Modulfunktionen” z 1890 roku. Funkcje modularne można rozważać jako wariant konstrukcji krzywych eliptycznych: dziedzinę \mathbb{C} zastępujemy przez $H = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$, zaś kratę $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ przez grupę modularną $SL_2(\mathbb{Z})$. Funkcje modularne wystarczy zadać na dziedzinie fundamentalnej grupy $SL_2(\mathbb{Z})$ działającej na H za pomocą transformacji:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) = \frac{az + b}{cz + d}.$$

Określimy klasę podgrup odgrywających kluczową rolę w zastosowaniach do arytmetycznej teorii krzywych eliptycznych. Podgrupę $\Gamma \subset SL_2(\mathbb{Z})$ nazywamy *podgrupą kongruencyjną*, jeśli zawiera *główną podgrupę kongruencyjną* poziomu N (dla pewnej liczby naturalnej N) postaci

$$\Gamma(N) := \{\gamma \in SL_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}\}.$$

Bardzo ważnymi przykładami podgrup kongruencyjnych są:

$$\Gamma_0(N) := \{\gamma \in SL_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N}\}$$

oraz

$$\Gamma_1(N) := \{\gamma \in \Gamma_0(N) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N}\}.$$

Niech k będzie liczbą całkowitą nieujemną. *Formą modularną* f wagi k , względem podgrupy kongruencyjnej Γ , nazywamy funkcję holomorficzną $f : H \rightarrow \mathbb{C}$, holomorficzną w ostrzach oraz spełniającą warunek $f(\gamma(z)) = (cz+d)^k f(z)$ dla wszystkich $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ oraz $z \in H$. Forma modularna f spełnia $f(z) = f(z+h)$ dla pewnej liczby naturalnej h oraz wszystkich $z \in H$, oraz jest holomorficzną w $i\infty$, więc posiada rozwinięcie w szereg Fouriera $f(z) = \sum_{n \geq 0} a_n e^{2\pi i n z/h}$, $a_n \in \mathbb{C}$. Formę f nazywamy *formą paraboliczną*, jeśli znika we wszystkich ostrzach (wówczas, w szczególności, $a_0 = 0$). Formę paraboliczną nazywamy *znormalizowaną*, jeśli $a_1 = 1$.

Niech $M_k(\Gamma)$ (odpowiednio $S_k(\Gamma)$) oznacza zespoloną przestrzeń liniową (skończonego wymiaru) form modularnych (odpowiednio form parabolicznych) wagi k względem Γ .

Niech $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ będzie charakterem (odpowiadający charakter Dirichleta modulo N oznaczamy również przez χ). Określamy $M_k(\Gamma_0(N), \chi)$ (odpowiednio $S_k(\Gamma_0(N), \chi)$) jako podprzestrzeń w $M_k(\Gamma_1(N))$ (odpowiednio w $S_k(\Gamma_1(N))$) złożoną z funkcji f spełniających warunek $f(\gamma(z)) = \chi(d)(cz+d)^k f(z)$ dla wszystkich $\gamma \in \Gamma_0(N)$ oraz $z \in H$. W tym przypadku mówimy, że forma modularna f jest *wagi k , poziomu N*

i typu (lub charakteru) χ . Zauważmy, że $M_k(\Gamma_0(N), 1) = M_k(\Gamma_0(N))$ oraz $S_k(\Gamma_0(N), 1) = S_k(\Gamma_0(N))$.

2.2. Przykłady. Niech $k > 2$ będzie liczbą całkowitą parzystą. Rozważmy funkcję $G_k(z)$ określoną na H (szereg Eisensteina wagi k):

$$G_k(z) := \sum'_{(m,n)} \frac{1}{(mz+n)^k},$$

gdzie ' oznacza, że sumowanie obejmuje wszystkie pary liczb całkowitych (m, n) różne od $(0, 0)$. Skoro $k \geq 4$, to suma podwójna jest zbieżna bezwzględnie i jednostajnie na dowolnym zwartym podzbiornie w H , więc $G_k(z)$ jest holomorficzną na H . Oczywiście $G_k(z+1) = G_k(z)$ oraz $G_k(-1/z) = z^k G_k(z)$. Poza tym, $G_k(z)$ jest holomorficzną w nieskończoności, gdyż

$$\lim_{z \rightarrow i\infty} \sum'_{(m,n)} (mz+n)^{-k} = \sum_{n \neq 0} n^{-k} = 2\zeta(k).$$

Zatem $G_k(z)$ jest formą modularną wagi k względem $\Gamma_0(1)$. Łatwo wyznaczyć jej rozwinięcie w szereg Fouriera:

$$G_k(z) = 2\zeta(k) \left(1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \right),$$

gdzie $q = e^{2\pi iz}$ oraz B_k oznaczają liczby Bernoulliego.

Niech $g_2(L) := 60G_4(L)$, $g_3(L) := 140G_6(L)$ oznaczają współczynniki równania różniczkowego dla \wp -funkcji Weierstrassa odpowiadającej krzywej eliptycznej L (tj. współczynniki równania odpowiadającej krzywej eliptycznej). Niech $g_2(z) := 60G_4(z)$, $g_3(z) := 140G_6(z)$ (tj. $g_2(z) := g_2(L_z)$ oraz $g_3(z) := g_3(L_z)$). Niech $\Delta(z) := g_2(z)^3 - 27g_3(z)^2$ oznacza wyróżnik wielomianu $4x^3 - g_2(L_z)x - g_3(L_z)$. Bezpośrednio z konstrukcji widać, że jest to forma paraboliczna wagi 12 względem $\Gamma_0(1)$. Zauważmy, że $\Delta(z) = \prod_{n=1}^{\infty} (1 - q^n)^{24}$. Okazuje się, że Δ jest formą paraboliczną względem $\Gamma_0(1)$ najniższej możliwej wagi.

Na mniejszych podgrupach kongruencyjnych mogą istnieć formy paraboliczne niższych wag. Dla przykładu, $(\Delta(z)\Delta(Nz))^{1/(N+1)}$ jest formą paraboliczną wagi k i poziomu N , gdzie $k = k(N) = 24/(N+1)$ oraz $N \in \{2, 3, 5, 11\}$.

Niech $j(\tau) := 1728 \frac{g_2^3(\tau)}{\Delta(\tau)}$. Jest to funkcja modularna wagi 0 względem $\Gamma_0(1)$. Ponieważ jest ona holomorficzną i niezerową na H , więc posiada biegun rzędu 1 w nieskończoności. Dowodzi się, że indukowane odwzorowanie $j : \Gamma_0(1) \backslash H \rightarrow \mathbb{C}$ jest bijekcją. W konsekwencji, krzywe eliptyczne E_1, E_2 określone nad \mathbb{C} są izomorficzne wtedy i tylko wtedy, gdy $j_{E_1} = j_{E_2}$.

2.3. Twierdzenia Hecke'ego i Weila. Załóżmy, że forma paraboliczna $f = \sum a_n q^n$ wagi k względem $\Gamma_0(N)$ jest funkcją własną idempotentnego

operatora W_N określonego wzorem $(W_N f)(\tau) := i^k N^{-k/2} \tau^{-k} f(-1/N\tau)$. Hecke (patrz, np. [54], [35], [112], [67]) udowodnił, że $L(f, s)$ rozszerza się do funkcji całkowitej na całej płaszczyźnie zespolonej oraz spełnia równanie funkcyjne $\Lambda(f, s) = \varepsilon i^k \Lambda(f, k - s)$, gdzie $\Lambda(f, s) := N^{s/2} (2\pi)^{-s} \Gamma(s) L(f, s)$ oraz $\varepsilon = \pm 1$ jest wartością własną operatora W_N .

Szkic dowodu. Szereg $L(f, s)$ jest zbieżny (z definicji) dla $\operatorname{Re}(s) > \frac{k}{2} + 1$. Z warunku $W_N f = \varepsilon f$ otrzymujemy $f(i/N\sigma) = \varepsilon N^{k/2} i^k \sigma^k f(i\sigma)$. Poza tym mamy

$$\begin{aligned} \Lambda(f, s) &= N^{s/2} \int_0^\infty f(i\sigma) \sigma^{s-1} d\sigma \\ &= \varepsilon N^{\frac{1}{2}(k-s)} \int_{1/\sqrt{N}}^\infty f(i\sigma) \sigma^{k-s-1} d\sigma + N^{s/2} \int_{1/\sqrt{N}}^\infty f(i\sigma) \sigma^{s-1} d\sigma, \end{aligned}$$

tj. przedłużenie $\Lambda(f, s)$ do funkcji całkowitej na \mathbb{C} . Podstawiając $s \mapsto k - s$ i mnożąc przez εi^k , otrzymujemy $\varepsilon i^k \Lambda(f, k - s) = \Lambda(f, s)$.

Weil [129] udowodnił twierdzenie odwrotne w następującym sensie. Niech $L(s) := \sum_{n=1}^\infty c_n n^{-s}$ będzie szeregiem Dirichleta o współczynnikach rzeczywistych, spełniających $c_n = O(n^c)$ dla pewnej stałej $c > 0$. Ustalmy liczbę naturalną N . Dla dowolnego charakteru Dirichleta χ modulo m ($(m, N) = 1$) połóżmy $L_\chi(s) := \sum_{n=1}^\infty c_n \chi(n) n^{-s}$. Załóżmy, że zmodyfikowana funkcja $\Lambda_\chi(s) := (m^2 N)^{s/2} (2\pi)^{-s} \Gamma(s) L_\chi(s)$ jest całkowita, ograniczona w dowolnym pionowym pasie oraz spełnia równanie postaci

$$\Lambda_\chi(s) = \varepsilon (-1)^{k/2} \frac{\tau(\chi) \chi(-N)}{\tau(\bar{\chi})} \Lambda_{\bar{\chi}}(k - s),$$

gdzie $\varepsilon = \pm 1$ jest ustalone. Wówczas $f(\tau) := \sum_{n=1}^\infty c_n e^{2\pi i n \tau}$ jest formą paraboliczną wagi k względem $\Gamma_0(N)$.

2.4. Operatory Heckeego. Niech f będzie formą modularną wagi k , poziomu N i typu ε . Jeśli $f = \sum_{n=0}^\infty a_n q^n$ jest rozwinięciem w nieskończoności, to definiujemy $T_m f = \sum_{n=0}^\infty b_n q^n$, gdzie $b_n = \sum_{d|(m,n)} \varepsilon(d) d^{k-1} a_{mn/d^2}$. Otrzymujemy rodzinę operatorów liniowych T_m (tzw. *operatory Heckeego*), działających, w szczególności, na przestrzeni form parabolicznych. Operatory T_m komutują między sobą. Pierścień przemienny \mathbb{T} generowany przez operatory T_m nazywamy *algebrą Heckeego*. Jeśli $f = \sum_{n \geq 1} a_n q^n$ jest paraboliczną formą własną, to łatwo sprawdzić, że odwzorowanie $T_m \mapsto a_m$ rozszerza się do homomorfizmu pierścieni $\Theta : \mathbb{T} \rightarrow \mathbb{C}$.

Dla $f = \sum_{n \geq 1} a_n q^n \in S_k(\Gamma_0(N), \varepsilon)$ następujące warunki są równoważne: (i) f jest znormalizowaną formą własną; (ii) $\sum_{n \geq 1} a_n n^{-s} = \prod_p (1 - a_p p^{-s} + \varepsilon(p) p^{k-1-2s})^{-1}$.

2.5. Teoria Atkina-Lehnera. Niech $S_k^-(\Gamma_0(N))$ będzie podprzestrzenią w $S_k(\Gamma_0(N))$ generowaną przez wszystkie funkcje postaci $f(dz)$, gdzie $f \in S_k(\Gamma_0(N'))$ dla pewnego właściwego dzielnika $N'|N$ oraz d jest dzielnikiem N/N' . Niech $S_k^+(\Gamma_0(N))$ oznacza dopełnienie ortogonalne $S_k^-(\Gamma_0(N))$ w $S_k(\Gamma_0(N))$ względem iloczynu skalarnego Peterssona

$$\langle f, g \rangle := \int_{D_{\Gamma_0(N)}} f(z) \overline{g(z)} y^{k-2} dx dy,$$

gdzie $z = x + yi$ oraz $D_{\Gamma_0(N)}$ oznacza ustaloną dziedzinę fundamentalną działania $\Gamma_0(N)$ na H .

Element $f \in S_k^+(\Gamma_0(N))$ nazywamy *nową formą wagi k* względem podgrupy $\Gamma_0(N)$, jeśli f jest funkcją własną operatorów T_p dla wszystkich p względnie pierwszych z N . Atkin i Lehner [2] udowodnili, że nowe formy tworzą bazę w przestrzeni $S_k^+(\Gamma_0(N))$.

2.6. Konstrukcja form parabolicznych. η -funkcja Dedekinda jest określona za pomocą iloczynu nieskończonego

$$\eta(z) := e^{\pi iz/12} \prod_{n=1}^{\infty} (1 - e^{2\pi inz}), \quad \text{Im}(z) > 0.$$

Mamy $\eta(-1/z) = \sqrt{-iz} \eta(z)$. Poza tym, dla $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ mamy

$$\eta\left(\frac{az + b}{cz + d}\right) = (cz + d)^{1/2} v(M) \eta(z), \quad v(M)^{24} = 1.$$

Odnajmy następujące kryterium [80]. Ustalmy liczbę naturalną N . Dla $d|N$ połóżmy $d' := \frac{N}{d}$. Dla rodziny $r = (r_d)_{d|N}$ liczb całkowitych nieujemnych, indeksowanych przez zbiór dzielników naturalnych liczby N określmy formę modularną $g_r(z) := \prod_{d|N} \eta(dz)^{r_d}$. Załóżmy, że spełnione są następujące warunki: (i) $\sum_{d|N} r_d d' \equiv 0 \pmod{24}$; (ii) $\sum_{d|N} r_d d \equiv 0 \pmod{24}$; (iii) $\sum_{d|N} r_d = 4$; (iv) $\prod_{d|N} (d')^{r_d}$ jest kwadratem. Wówczas g_r jest formą paraboliczną wagi 2 względem grupy $\Gamma_0(N)$.

Zastosujemy przytoczone kryterium do konstrukcji nowych form wagi 2 względem $\Gamma_0(N)$ dla $N \in \{11, 14, 15, 20, 24, 27, 32, 36\}$. Bezpośrednio widać, że odpowiadającymi formami parabolicznymi wagi 2 są:

$$\begin{aligned} f_{11}(z) &:= \eta(z)^2 \eta(11z)^2 \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} + \dots \end{aligned}$$

$$\begin{aligned} f_{14}(z) &:= \eta(z) \eta(2z) \eta(7z) \eta(14z) \\ &= q - q^2 - 2q^3 + q^4 + 2q^6 + q^7 - q^8 + q^9 + \dots \end{aligned}$$

$$\begin{aligned}
f_{15}(z) &:= \eta(z)\eta(3z)\eta(5z)\eta(15z) \\
&= q - q^2 - q^3 - q^4 + q^5 + q^6 + 3q^8 + q^9 + \dots \\
f_{20}(z) &:= \eta(2z)^2\eta(10z)^2 \\
&= q - 2q^3 - q^5 + 2q^7 + q^9 + 2q^{13} + 2q^{15} - 6q^{17} + \dots \\
f_{24}(z) &:= \eta(2z)\eta(4z)\eta(6z)\eta(12z) \\
&= q - q^3 - 2q^5 + q^9 + 4q^{11} - 2q^{13} + 2q^{15} + \dots \\
f_{27}(z) &:= \eta(3z)^2\eta(9z)^2 \\
&= q - 2q^4 - q^7 + 5q^{13} + 4q^{16} - 7q^{19} - 5q^{25} + 2q^{28} + \dots \\
f_{32}(z) &:= \eta(4z)^2\eta(8z)^2 \\
&= q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} - q^{25} - 10q^{29} - 2q^{37} + \dots \\
f_{36}(z) &:= \eta(6z)^4 \\
&= q - 4q^7 + 2q^{13} + 8q^{19} - 5q^{25} - 4q^{31} - 10q^{37} + 8q^{43} + 9q^{49} + \dots
\end{aligned}$$

Dla wymienionych wartości N przestrzenie $S_2(\Gamma_0(N))$ są 1-wymiarowe, więc skonstruowane formy paraboliczne są nowymi formami. Przestrzenie $S_2(\Gamma_0(N))$ są 1-wymiarowe także dla $N \in \{17, 19, 21, 49\}$, jednak powyższe kryterium nie pozwala w tym przypadku skonstruować odpowiadających form parabolicznych. Okazuje się ([82]), Thm. 1), że powyższe 8 form parabolicznych, forma $f_{64}(z) := \eta(8z)^8\eta(4z)^{-2}\eta(16z)^{-2}$ poziomu 2^6 oraz formy:

$$\begin{aligned}
f_{48}(z) &:= \frac{\eta(4z)^4\eta(12z)^4}{\eta(2z)\eta(6z)\eta(8z)\eta(24z)}, & f_{80}(z) &:= \frac{\eta(4z)^6\eta(20z)^6}{\eta(2z)^2\eta(8z)^2\eta(10z)^2\eta(40z)^2}, \\
f_{144}(z) &:= \eta(12z)^{12}\eta(6z)^{-4}\eta(24z)^{-4}, & & \text{wyczerpują listę nowych form wagi 2} \\
& & & \text{postaci } \prod_{i=1}^{i=s} \eta(t_i z)^{r_i} \text{ (gdzie } t_1, \dots, t_s \text{ oznaczają liczby naturalne oraz } r_1, \dots, r_s \\
& & & \text{liczby całkowite).}
\end{aligned}$$

2.7. Formy modularne i reprezentacje automorficzne. Odnotujmy następujące ważne twierdzenie (dowód np. w artykule Gelbarta w [20]). *Istnieje wzajemnie jednoznaczna odpowiedniość między znormalizowanymi nowymi formami w $S_k(\Gamma_0(N), \psi)$ oraz nieprzywiedlnymi automorficznymi parabolicznymi reprezentacjami $\pi = \otimes_p \pi_p$ grupy adeli $GL_2(\mathbb{A})$, spełniającymi warunki: (a) χ_ψ jest centralnym charakterem reprezentacji π ; (b) π_p jest nierozgąłżona dla wszystkich $p \nmid N$; (c) π_∞ jest wagi k .*

3. Krzywe modularne

3.1. Definicje i podstawowe własności. Dla podgrupy kongruencyjnej Γ oznaczmy przez $Y_\Gamma := \Gamma \backslash H$ zbiór orbit działania grupy kongruencyjnej Γ na H . Y_Γ posiada naturalną strukturę (niezwartej) powierzchni Riemanna: struktura zespolona na Y_Γ pochodzi od projekcji $\pi : H \rightarrow Y_\Gamma$. Kompaktyfikację X_Γ powierzchni Y_Γ dokonuje się przez dołączenie skończonej liczby

ostrzy (orbit $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ względem działania grupy Γ) i zadanie odpowiedniej struktury zespolonej. Podamy teraz szczegóły.

Niech $H^* = H \cup \mathbb{P}^1(\mathbb{Q})$. Naturalne działanie $SL_2(\mathbb{Z})$ na H rozszerza się do działania na H^* zachowującego $\mathbb{P}^1(\mathbb{Q})$. Dla podgrupy kongruencyjnej Γ (ogólniej, dowolnej podgrupy skończonego indeksu w $SL_2(\mathbb{Z})$) mamy

$$\Gamma \setminus H^* = (\Gamma \setminus H) \cup (\Gamma \setminus \mathbb{P}^1(\mathbb{Q})).$$

Zbiór $\Gamma \setminus \mathbb{P}^1(\mathbb{Q})$ jest skończony, gdyż Γ jest podgrupą skończonego indeksu w $SL_2(\mathbb{Z})$ oraz $SL_2(\mathbb{Z})$ działa tranzytywnie na $\mathbb{P}^1(\mathbb{Q})$.

Wprowadzimy teraz topologię na $\Gamma \setminus H^*$. W tym celu wprowadzimy najpierw topologię na H^* . Dla $y_0 > 0$ oraz $c \in \mathbb{P}^1(\mathbb{Q})$ wybierzmy macierz $\delta \in SL_2(\mathbb{Z})$ spełniającą warunek $c = \delta\infty$, oraz przyjmijmy

$$U_{y_0} = \{x + yi \in \mathbb{C} : y > y_0\}, \quad U_{c,y_0}^o = \delta(U_{y_0}), \quad U_{c,y_0} = U_{c,y_0}^o \cup \{c\}.$$

Zauważmy, że zbiory U_{c,y_0}^o, U_{c,y_0} nie zależą od wyboru δ . Za bazę zbiorów otwartych w H^* wybieramy zbiory otwarte w H oraz zbiory postaci U_{c,y_0} . Topologia ilorazowa na $\Gamma \setminus H^*$, odpowiadająca naturalnej projekcji $\pi : H^* \rightarrow \Gamma \setminus H^*$, określa strukturę zwartej przestrzeni topologicznej.

Zadamy teraz strukturę zespoloną na $\Gamma \setminus H^*$. Niech \mathcal{F} będzie snopem funkcji ciągłych $\Gamma \setminus H^* \rightarrow \mathbb{C}$. Dla $x \in \Gamma \setminus H^*$ niech \mathcal{F}_x oznacza źdźbło snopa \mathcal{F} w x : jest to zbiór klas równoważności par (f, V) , gdzie V jest otoczeniem otwartym x oraz f jest ciągłą funkcją $V \rightarrow \mathbb{C}$; przy tym $(f, V) \simeq (g, U)$ jeśli $f = g$ na $V \cap U$. Określamy strukturę zespoloną jako podsноп \mathcal{O} snopa \mathcal{F} zadając dla każdego x źdźbło \mathcal{O}_x jako podpierścień pierścienia \mathcal{F}_x złożony z klas równoważności par (f, V) jednego z poniższych dwóch typów:

- istnieje $z \in H$ oraz otoczenie otwarte U punktu z takie, że $x = \pi(z)$, $V = \pi(U)$ oraz $f \circ \pi$ jest holomorficzną na U ;
- istnieją $c \in \mathbb{P}^1(\mathbb{Q})$ oraz $y_0 > 0$ takie, że $x = \pi(c)$, $V = \pi(U_{c,y_0})$, oraz $f \circ \pi$ spełnia następujący warunek. Wybierzmy $\delta \in SL_2(\mathbb{Z})$ takie, że $c = \delta\infty$, oraz niech M będzie liczbą naturalną spełniającą $(f \circ \pi \circ \delta)(z + M) = (f \circ \pi \circ \delta)(z)$ dla $z \in U_{y_0}$ (π jest Γ -niezmiennicza oraz Γ jest skończonego indeksu w $SL_2(\mathbb{Z})$, więc istnieje takie M). Połóżmy $r = e^{-2\pi y_0/M}$ oraz niech F będzie funkcją określoną na $D^0(r) = \{q \in \mathbb{C} : 0 < |q| < r\}$ spełniającą $(f \circ \pi \circ \delta)(z) = F(e^{2\pi z/M})$. Wówczas F jest holomorficzną na $D^0(r)$ oraz rozszerza się do funkcji holomorficznnej na $D(r) = \{q \in \mathbb{C} : |q| < r\}$.

Można sprawdzić, że każdy punkt $x \in \Gamma \setminus H^*$ posiada otoczenie otwarte V takie, że przestrzeń opierścieniona $(V, \mathcal{O}|_V)$ jest izomorficzna z przestrzenią opierścienioną dysku otwartego w \mathbb{C} , więc \mathcal{O} definiuje na $\Gamma \setminus H^*$ strukturę powierzchni Riemanna.

W przypadku grup kongruencyjnych $\Gamma_0(N)$ (odpow. $\Gamma_1(N)$ lub $\Gamma(N)$) powierzchnię Y_Γ oznaczamy przez $Y_0(N)$ (odpow. $Y_1(N)$ lub $Y(N)$). Podobnie dla X_Γ .

3.2. Ciało funkcji meromorficznych na $X_0(N)$. Okazuje się, że dowolna funkcja meromorficzna na $X_0(1)$ jest funkcją wymierną względem j . Ogólniej, ciało funkcji meromorficznych na $X_0(N)$ wynosi $\mathbb{C}(j, j_N)$, gdzie $j_N(\tau) := j(N\tau)$. Podkreślimy, że funkcje j oraz j_N są związane wielomianową zależnością $\Phi_N(j, j_N) = 0$ o współczynnikach wymiernych.

3.3. Krzywe modularne jako przestrzenie moduli. Istnieje bijekcja między $Y_0(N)$ i zbiorem klas równoważności par (E, C) , gdzie E jest krzywą eliptyczną określoną nad \mathbb{C} oraz $C \subset E(\mathbb{C})$ jest podgrupą cykliczną rzędu N . Dla $\tau \in H$ zdefiniujemy $E_\tau := (\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau, \frac{1}{N}\mathbb{Z}/\mathbb{Z})$. Wówczas dowolna para (E, C) jest równoważna parze postaci E_τ , przy czym E_τ i $E_{\tau'}$ są równoważne wtedy i tylko wtedy, gdy $\tau' \in \Gamma_0(N)\tau$. Żądana bijekcja jest więc realizowana przez $\tau \mapsto E_\tau$.

Podobnie, istnieje bijekcja między $Y_1(N)$ i zbiorem klas równoważności par (E, P) , gdzie E jest krzywą eliptyczną określoną nad \mathbb{C} oraz $P \in E(\mathbb{C})$ jest punktem rzędu N . Istotnie, dla $\tau \in \mathbb{C}$ weźmy parę $(\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau, 1/N \bmod \mathbb{Z} + \mathbb{Z}\tau)$. $Y_0(N)$ jest ilorzem $Y_1(N)$ względem działania grupy $(\mathbb{Z}/N\mathbb{Z})^\times$, przy czym naturalna projekcja $Y_1(N) \rightarrow Y_0(N)$ ma prostą interpretację: $(E, P) \mapsto (E, \langle P \rangle)$, gdzie $\langle P \rangle$ jest podgrupą generowaną przez P .

3.4. Model nad \mathbb{Q} . Można udowodnić, że dla podgrup Γ spełniających $\Gamma_1(N) \subset \Gamma \subset \Gamma_0(N)$, krzywa modularna X_Γ posiada model nad \mathbb{Q} . Odpowiedni rezultat dla $\Gamma = \Gamma_0(N)$ głosi, że istnieje nieosobliwa rzutowa krzywa algebraiczna X określona nad \mathbb{Q} oraz biholomorficzne odwzorowanie $\phi : X_0(N) \rightarrow X(\mathbb{C})$ takie, że

$$\phi^*(X(\mathbb{C})) = \mathbb{C}(j, j_N), \quad \phi^*(X(\mathbb{Q})) = \mathbb{Q}(j, j_N).$$

Krzywa X jest wyznaczona jednoznacznie z dokładnością do izomorfizmu określonego nad \mathbb{Q} oraz ϕ jest wyznaczone jednoznacznie przez zadanie izomorfizmu ciał $\mathbb{Q}(X) \simeq \mathbb{Q}(j, j_N)$.

3.5. Punkty wymierne na $X_0(15)$. Zauważmy, że $X_0(15)$ jest krzywą genusu jeden, posiadającą 4 ostrza. Z określenia działania grupy $G_{\mathbb{Q}}$ wynika, że wszystkie ostrza są wymierne nad \mathbb{Q} . Mamy: (i) $\#X_0(15)(\mathbb{Q}) = 8$; (ii) cztery punkty z $X_0(15)(\mathbb{Q})$ nie będące ostrzami, odpowiadają czterem parom $(E_i, C_{15}^{(i)})$, gdzie $j_{E_i} \in \{-25/2, -5^2 241^3/2^3, -5 \cdot 29^3/2^5, 5 \cdot 211^3/2^{15}\}$. Istotnie, $X_0(15)$ jest krzywą eliptyczną o równaniu $y^2 = x(x+9)(x-16)$ (por. 3.9), skąd łatwo wyznaczyć grupę jej punktów wymiernych (lub znaleźć w tablicach [21]). W tych samych tablicach znajdujemy cztery krzywe eliptyczne określone nad \mathbb{Q} , izogeniczne z krzywą $y^2 + xy + y = x^3 - x - 2$ i posiadające podgrupę wymierną rzędu 15. Reprezentują one wszystkie punkty z $X_0(15)(\mathbb{Q})$ nie będące ostrzami oraz mają j -niezmienniki wymienione powyżej.

Z powyższych rozważań wynika, że krzywa eliptyczna określona nad \mathbb{Q} z wymierną podgrupą torsyjną rzędu 15 nie jest semistabilna w 5. Wynik ten odgrywa ważną rolę w dowodzie Wileasa (patrz 16.3).

3.6. Punkty wymierne na $X_1(N)$. Problem istnienia krzywych eliptycznych określonych nad \mathbb{Q} z punktem wymiernym rzędu N sprowadza się do problemu istnienia punktów wymiernych (nie będących ostrzami) na $X_1(N)$. Dla $N = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$ krzywa $X_1(N)$ jest izomorficzna z \mathbb{P}^1 . W konsekwencji, dla wymienionych wartości N istnieje nieskończenie wiele krzywych eliptycznych określonych nad \mathbb{Q} z punktem wymiernym rzędu N . W 1976 r. Mazur [84], badając punkty wymierne na $X_1(N)$, udowodnił, że podgrupa torsyjna $E(\mathbb{Q})_{tors}$ grupy $E(\mathbb{Q})$ jest jedną z poniższych 15 grup: $\mathbb{Z}/N\mathbb{Z}$ ($N = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$); $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ ($N = 1, 2, 3, 4$).

Łatwo uzasadnić, że $E(\mathbb{Q})$ nie może zawierać punktu rzędu 11 lub 13. Genus krzywej $X_1(11)$ wynosi 1. Jest to krzywa eliptyczna, którą można zadać równaniem: $y^2 + y = x^3 - x^2$. Można sprawdzić, że $X_1(11)(\mathbb{Q}) = \{O, (0, 0), (1, -1), (1, 0), (0, -1)\}$. Ponieważ wszystkie wymienione punkty wymierne są ostrzami, więc nie istnieje krzywa eliptyczna określona nad \mathbb{Q} z punktem wymiernym rzędu 11. Podobnie dowodzi się, że nie istnieje krzywa eliptyczna określona nad \mathbb{Q} z punktem wymiernym rzędu 13.

3.7. Skręcenia krzywych modularnych. Ustalmy nieparzystą liczbę pierwszą p . Istnieje otwarta krzywa modularna Y_p określona nad \mathbb{Q} , której punkty odpowiadają klasom izomorfizmu par (E, ϕ) , gdzie E jest krzywą eliptyczną oraz $\phi : E[p] \rightarrow \mathbb{F}_p \times \mu_p$ jest izomorfizmem takim, że $\det(\phi) : \bigwedge^2 E[p] \rightarrow \mu_p$ jest odwzorowaniem Weila. Niech X_p oznacza kompaktyfikację Y_p .

Konstrukcję można uogólnić w następujący sposób. Niech V będzie 2-wymiarową przestrzenią liniową nad \mathbb{F}_p z działaniem $G_{\mathbb{Q}}$ oraz $\eta : \bigwedge^2 V \rightarrow \mu_p$ niezdegenerowanym alternującym dwuliniowym odwzorowaniem zadającym izomorfizm. Wówczas istnieje otwarta krzywa modularna X_V określona nad \mathbb{Q} , której punkty parametryzują klasy izomorfizmu par (E, ϕ) , gdzie E jest krzywą eliptyczną, oraz $\phi : E[p] \rightarrow V$ jest izomorfizmem takim, że $\eta \circ \det(\phi) : \bigwedge^2 E[p] \rightarrow \bigwedge^2 V \rightarrow \mu_p$ jest odwzorowaniem Weila. Niech X_V oznacza kompaktyfikację Y_V .

Niech E będzie krzywą eliptyczną, $V = E[5]$ oraz η odwzorowaniem Weila. Oznaczmy w tym przypadku $Y_E = Y_V$, $X_E = X_V$. Rubin i Silverberg [100] pokazali, że istnieje izomorfizm $\psi : \mathbb{P}^1 \rightarrow X_E$ określony nad \mathbb{Q} oraz wielomiany $f_E, g_E \in \mathbb{Q}[t]$ stopni 20 i 30 odpowiednio, takie że dla $t \in \mathbb{Q}$ spoza skończonego zbioru $\psi^{-1}(X_E(\mathbb{Q}) \setminus Y_E(\mathbb{Q}))$ punkt $\psi(t) \in Y_E(\mathbb{Q})$ jest reprezentowany przez krzywą eliptyczną $E_t : y^2 = x^3 + f_E(t)x + g_E(t)$. Dla takich t mamy, w szczególności, $\bar{\rho}_{E_t, 5} \simeq \bar{\rho}_{E, 5}$.

Określamy podobnie otwarte krzywe modularne Y'_E oraz Y''_E , które parametryzują klasy izomorfizmu trójek (E', ϕ, C_3) oraz $(E', \phi, \{C_3, C'_3\})$ odpowiednio, gdzie: E jest krzywą eliptyczną, $\phi : E'[5] \rightarrow E[5]$ jest izomorfizmem przeprowadzającym odwzorowanie Weila na $E'[5]$ na odwzorowanie Weila na $E[5]$ oraz C_3 i C'_3 są różnymi podgrupami rzędu 3 w $E'[3]$. Dowodzi się, że zbiory $Y'_E(\mathbb{Q})$, $Y''_E(\mathbb{Q})$ są skończone.

3.8. Model nad \mathbb{Z} . Dowód faktu, że X_Γ posiada model nad \mathbb{Z} , jest raczej skomplikowany. Dowód istnienia i opis kanonicznego właściwego modelu dla X_Γ nad $\text{Spec}(\mathbb{Z})$ można znaleźć w serii prac Igusy [61], Deligne'a-Rapoporta [30], Drinfeld'a (patrz, monografia Katza i Mazura [63]). Model taki pozwala, w szczególności, rozważać redukcję X_Γ nad \mathbb{F}_p .

3.9. Krzywe modularne eliptyczne. Istnieje dokładnie 12 krzywych modularnych $X_0(N)$ genusu 1. Odpowiadają one wartościom $N = 11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49$. Korzystając np. z klasycznych rezultatów Fricke, można łatwo wypisać równania minimalne dla wymienionych krzywych eliptycznych ([80]):

$$\begin{aligned} X_0(11) : & y^2 + y = x^3 - x^2 - 10x - 20, \\ X_0(14) : & y^2 + xy + y = x^3 + 4x - 6, \\ X_0(15) : & y^2 + xy + y = x^3 + x^2 - 10x - 10, \\ X_0(17) : & y^2 + xy + y = x^3 - x^2 - x - 14, \\ X_0(19) : & y^2 + y = x^3 + x^2 - 9x - 15, \\ X_0(20) : & y^2 = x^3 + x^2 + 4x + 4, \\ X_0(21) : & y^2 + xy = x^3 - 4x - 1, \\ X_0(24) : & y^2 = x^3 - x^2 - 4x + 4, \\ X_0(27) : & y^2 + y = x^3 - 7, \\ X_0(32) : & y^2 = x^3 + 4x, \\ X_0(36) : & y^2 = x^3 + 1, \\ X_0(49) : & y^2 + xy = x^3 - x^2 - 2x - 1. \end{aligned}$$

3.10. Twierdzenie Shimury. Niech $J_0(N)$ oznacza rozmaitość Jacobiego krzywej modularnej $X_0(N)$. Niech $f = \sum a_n q^n \in S_2(\Gamma_0(N))$ będzie funkcją własną operatorów Hecke'a. Shimura ([112], Thm. 7.14 oraz Thm. 7.15) dowodzi, że jeśli wszystkie współczynniki a_n są wymierne, to istnieje jednowymiarowa podrozmaitość abelowa A_f rozmaitości $J_0(N)$ określona nad \mathbb{Q} taka, że $L(f, s)$ oraz $L(A_f, s)$ pokrywają się z dokładnością do skończonej ilości czynników.

A. Krzywe eliptyczne o przewodniku 2^m . Istnieje 10 nowych form wagi 2 i poziomu 2^m ($5 \leq m \leq 8$) o wymiernych współczynnikach. Zatem istnieje 10 odpowiadających krzywych eliptycznych A_f , określonych nad \mathbb{Q} . Krzywe te nie są izogeniczne, gdyż posiadają różne L -funkcje. Igusa [61] udowodnił, że $J_0(N)$ posiada dobrą redukcję w p nie dzielącym N , więc

([108]) dowolna podrozmaitość abelowa określona nad \mathbb{Q} również ma dobrą redukcję w $p \nmid N$. W szczególności, w naszym przypadku, przewodniki odpowiadających krzywych eliptycznych są potęgami 2. Ale wszystkie takie krzywe eliptyczne zostały wyznaczone przez Ogga [93]; w szczególności, istnieje 10 klas izogenii takich krzywych. Klasy izogenii krzywych eliptycznych wyznaczonych przez Ogga pokrywają się z klasami izogenii reprezentowanych przez krzywe eliptyczne A_f otrzymane ze wspomnianych dziesięciu nowych form.

B. Krzywe modularne eliptyczne. Forma $f(z) := \eta(z)^2 \eta(11z)^2$ jest znormalizowaną nową formą wagi 2 względem $\Gamma_0(11)$. W tym przypadku $A_f = X_0(11) \simeq J_0(11)$. Podobne fakty są prawdziwe dla pozostałych krzywych eliptycznych postaci $X_0(N)$.

4. Reprezentacje Galois

4.1. Podstawowe definicje i przykłady. Niech $\overline{\mathbb{Q}}$ oznacza domknięcie algebraiczne ciała \mathbb{Q} liczb wymiernych w \mathbb{C} oraz \mathbb{Z} będzie pierścieniem wszystkich liczb algebraicznych całkowitych. Niech $G_{\mathbb{Q}} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ będzie absolutną grupą Galois ciała \mathbb{Q} . $G_{\mathbb{Q}}$ jest proskończoną grupą topologiczną względem tzw. topologii Krulla, w której bazę otwartych otoczeń jedynki tworzą podgrupy $\text{Gal}(\overline{\mathbb{Q}}/K)$, gdzie K przebiega skończone rozszerzenia \mathbb{Q} zawarte w $\overline{\mathbb{Q}}$ (patrz [11]).

Dla dowolnej liczby pierwszej p , niech \mathbb{Q}_p oznacza ciało liczb p -adycznych, tj. uzupełnienie \mathbb{Q} względem p -adycznej wartości bezwzględnej $|\cdot|_p$. Dla $l = \infty$ przyjmijmy $\mathbb{Q}_{\infty} := \mathbb{R}$, tj. uzupełnienie \mathbb{Q} względem zwykłej wartości bezwzględnej. Ustalmy domknięcie algebraiczne $\overline{\mathbb{Q}}_p$ ciała \mathbb{Q}_p , zanurzenie $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$ oraz zdefiniujmy $\overline{\mathbb{Q}}_{\infty} := \mathbb{C}$. Rozważmy lokalne absolutne grupy Galois $G_{\mathbb{Q}_p} := \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Skoro $|\cdot|_p$ przedłuża się jednoznacznie na $\overline{\mathbb{Q}}_p$, to $G_{\mathbb{Q}_p}$ utożsamia się z grupą automorfizmów ciała $\overline{\mathbb{Q}}_p$ zachowujących $|\cdot|_p$, lub równoważnie, z grupą ciągłych automorfizmów ciała $\overline{\mathbb{Q}}_p$.

Możemy ograniczyć dowolny automorfizm ciała $\overline{\mathbb{Q}}_p$ do automorfizmu ciała $\overline{\mathbb{Q}}$. Ponieważ $\overline{\mathbb{Q}}$ jest gęste w $\overline{\mathbb{Q}}_p$, to otrzymany homomorfizm grup $G_{\mathbb{Q}_p} \rightarrow G_{\mathbb{Q}}$ jest iniektywny. W ten sposób możemy (i będziemy) rozważać $G_{\mathbb{Q}_p}$ jako podgrupę w $G_{\mathbb{Q}}$ (należy podkreślić, że jako podgrupy w $G_{\mathbb{Q}}$ są one wyznaczone jedynie z dokładnością do sprzężenia, co jest związane z wyborem zanurzenia $\overline{\mathbb{Q}}$ w $\overline{\mathbb{Q}}_p$).

Zanurzenie ciał $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ indukuje zanurzenie grup $\{1, c\} = G_{\mathbb{R}} \hookrightarrow G_{\mathbb{Q}}$.

Dla $p \neq \infty$, grupa $G_{\mathbb{Q}_p}$ zachowuje pierścień $\overline{\mathbb{Z}}_p$ elementów całkowitych w $\overline{\mathbb{Q}}_p$ oraz ideał maksymalny $\lambda \subset \overline{\mathbb{Z}}_p$. Ciało $\overline{\mathbb{Z}}_p/\lambda$ jest domknięciem algebraicznym $\overline{\mathbb{F}}_p$ ciała \mathbb{F}_p . Otrzymujemy naturalny (surjektywny) homomorfizm $G_{\mathbb{Q}_p} \rightarrow G_{\mathbb{F}_p}$. Jego jądro I_p nazywa się *podgrupą inercji* w p . Grupa

$G_{\mathbb{F}_p}$ jest procykliczna; jej kanonicznym generatorem jest automorfizm σ_p określony przez $\sigma_p(x) = x^p$. Dla ideału maksymalnego $\mathfrak{p} \subset \overline{\mathbb{Z}}$ leżącego nad p , oznaczamy przez $\text{Fr}_{\mathfrak{p}} \in G_{\mathbb{Q}_p}/I_p$ element Frobeniusa nad p (tj. dowolny przeciwobraz σ_p); przez $\text{Fr}_p \in G_{\mathbb{Q}}$ oznaczamy dowolnego reprezentanta elementu $\text{Fr}_{\mathfrak{p}}$.

Reprezentacją n -wymiarową grupy $G_{\mathbb{Q}}$ nazywamy homomorfizm $G_{\mathbb{Q}} \rightarrow GL_n(K)$, gdzie K jest ciałem lub pierścieniem. Jeśli K (i w konsekwencji, $GL_n(K)$) jest wyposażone w topologię, to na ogół ograniczamy się do ciągłych reprezentacji.

Ponieważ dowolna jednowymiarowa reprezentacja ma abelowy obraz, więc twierdzenie Kroneckera-Webera (patrz np. [128]) pozwala opisać wszystkie jednowymiarowe reprezentacje grupy $G_{\mathbb{Q}}$ wraz z zachowaniem się na wszystkich podgrupach $G_{\mathbb{Q}_p}$.

P r z y k ł a d y. (i) *Reprezentacje Artina*, tj. ciągłe reprezentacje $G_{\mathbb{Q}} \rightarrow GL_n(\mathbb{C})$. Skoro zwarte, całkowicie niespójne podgrupy w $GL_n(\mathbb{C})$ są skończone, więc reprezentacje Artina mają obraz skończony.

(ii) *Reprezentacje l -adyczne*, tj. ciągłe reprezentacje $G_{\mathbb{Q}} \rightarrow GL_n(K)$, gdzie K jest skończonym rozszerzeniem ciała \mathbb{Q}_l . Przy ustalonych wyborach zanurzeń otrzymujemy bijekcję między klasami reprezentacji Artina i klasami reprezentacji l -adycznych ze skończonym obrazem. Zatem reprezentacje Artina są specjalnym przypadkiem reprezentacji l -adycznych.

(iii) *l -adyczny charakter cyklotomiczny*. Jest to (wyznaczony jednoznacznie) homomorfizm $\chi_l : G_{\mathbb{Q}} \rightarrow \mathbb{Z}_l^{\times} \subset \overline{\mathbb{Q}_l}^{\times}$ spełniający warunek $\sigma\zeta = \zeta^{\chi_l(\sigma)}$, gdzie $\sigma \in G_{\mathbb{Q}}$ oraz ζ jest pierwiastkiem stopnia l^m z jedyńki.

(iv) *Reprezentacje stowarzyszone z formami modularnymi i krzywymi eliptycznymi* (rozdział 5, 6).

Reprezentacje l -adyczne w naturalny sposób pojawiają się w geometrii arytmetycznej. Niech X będzie gładką rzutową rozmaitością algebraiczną określoną nad \mathbb{Q} . Naturalne działanie $G_{\mathbb{Q}}$ na kohomologiach l -adycznych $H^i(X(\mathbb{Q}), \overline{\mathbb{Q}_l})$ określa reprezentację l -adyczną. Reprezentacje takie posiadają szereg ważnych własności:

(i) są nierozgałęzione poza skończonym zbiorem liczb pierwszych (Grothendieck);

(ii) są reprezentacjami de Rhama, tj. ograniczenie do podgrupy $G_{\mathbb{Q}_l}$ jest de Rhama (Fontaine et al.).

Istnieje przypuszczenie (Hipoteza Fontaine'a i Mazura), że dowolna nieprzywiedlna reprezentacja l -adyczna grupy $G_{\mathbb{Q}}$ posiadająca własności (i), (ii) „pochodzi z geometrii”. Przypuszczenie to wynika z teorii ciał klas w przypadku reprezentacji jednowymiarowych; w ogólnym przypadku znane są jedynie częściowe rezultaty (patrz 19.1).

Niech A będzie zupełną noetherowską lokalną \mathbb{Z}_p -algebrą. Rozważmy dwuwymiarową ciągłą reprezentację $\rho : G_{\mathbb{Q}} \rightarrow GL_2(A)$. Reprezentację ρ nazywamy:

- (i) *nieparzystą*, jeśli $\det \rho(c) = -1$;
- (ii) *nierozgałęzioną w l* , jeśli $I_l \subseteq \text{Ker}(\rho|_{G_{\mathbb{Q}_l}})$;
- (iii) *płaską w p* , jeśli dla każdego ideału I skończonego indeksu w A , redukcja $\rho|_{G_{\mathbb{Q}_p}}$ modulo I jest reprezentacją stowarzyszoną z $\overline{\mathbb{Q}_p}$ -punktami skończonego płaskiego schematu grupowego nad \mathbb{Z}_p (patrz np. [117], rozdz. 4 lub artykuły Tate'a i Conrada w [20]).

4.2. Deformacje reprezentacji Galois. Ustalmy grupę proskończoną G , ciało skończone k oraz ciągłą reprezentację $\bar{\rho} : G \rightarrow GL_n(k)$. Rozważmy kategorię \mathcal{C}_k , której obiektami są zupełne noetherowskie lokalne przemienne pierścienie R takie, że $R/m_R \simeq k$, zaś morfizmami są homomorfizmy pierścieni $\phi : R \rightarrow S$ spełniające $\phi(m_R) \subset m_S$ oraz takie, że indukowany izomorfizm $R/m_R \rightarrow S/m_S$ jest identycznością na k .

Podniesieniem $\bar{\rho}$ do $R \in \text{Ob}(\mathcal{C}_k)$ nazywamy ciągłą reprezentację $\rho : G \rightarrow GL_n(R)$ spełniającą $\rho \bmod m_R \simeq \bar{\rho}$. Podniesienia ρ_1, ρ_2 ustalonej reprezentacji $\bar{\rho}$ są *ściśle równoważne*, jeśli istnieje $M \in \text{Ker}(GL_n(R) \rightarrow GL_n(k))$ spełniające $\rho_2 = M^{-1}\rho_1 M$. *Deformacją* reprezentacji $\bar{\rho}$ jest klasa ścisłej równoważności podniesień.

Grupa proskończona G spełnia *warunek* (Υ) , jeśli maksymalny elementarny l -abelowy iloraz każdej otwartej podgrupy jest skończony. Z teorii ciał klas wynika, że grupy $G_{\mathbb{Q}_p}$ oraz $G_{\mathbb{Q},S}$ (grupa Galois maksymalnego rozszerzenia algebraicznego ciała \mathbb{Q} zawartego w $\overline{\mathbb{Q}}$, nierozgałęzionego poza skończonym zbiorem liczb pierwszych S) spełniają warunek (Υ) .

Mazur [83] udowodnił, że jeśli G spełnia warunek (Υ) oraz $\bar{\rho}$ jest absolutnie nieprzywiedlna, to istnieje $R(\bar{\rho}) \in \text{Ob}(\mathcal{C}_k)$ i deformacja $\rho^{univ} : G \rightarrow GL_n(R(\bar{\rho}))$, która jest uniwersalna w następującym sensie: dla dowolnego podniesienia $\rho : G \rightarrow GL_n(R)$ istnieje dokładnie jeden homomorfizm $h : R(\bar{\rho}) \rightarrow R$ w \mathcal{C}_k taki, że $h \circ \rho^{univ} = \rho$. Innymi słowy, functor $D_{\bar{\rho}} : \mathcal{C}_k \rightarrow \text{Sets}$, $D_{\bar{\rho}}(R) :=$ zbiór deformacji $\bar{\rho}$ do R , jest reprezentowalny przez $R(\bar{\rho})$: $D_{\bar{\rho}}(R) \simeq \text{Hom}_{W(k)\text{-alg}}(R(\bar{\rho}), R)$. Pierścień $R(\bar{\rho})$ nazywamy *uniwersalnym pierścieniem deformacji* dla $\bar{\rho}$.

Istnieją różne dowody twierdzenia Mazura: oryginalny wykorzystujący kryterium reprezentowalności Schlessingera, konstrukcja Faltingsa pierścienia $R(\bar{\rho})$ w terminach generatorów i relacji, konstrukcja Lenstry i de Smita. Ramakrishna [94] uogólnił rezultat Mazura, rozważając rodziny reprezentacji spełniające dodatkowe warunki (np. semistabilność).

4.3. Deformacje i rozszerzenia. Niech R będzie przemiennym pierścieniem z jedyneką. Niech M będzie wolnym R -modułem rangi n . Załóżmy, że grupa G działa na M , przy czym jest ono zgodne ze strukturą R -modułu.

Otrzymujemy reprezentację $\rho : G \rightarrow GL_n(R)$. Niech $R[\varepsilon]$ oznacza pierścień liczb dualnych. *Deformacją infinitesimalną* reprezentacji ρ nazywamy reprezentację $\rho' : G \rightarrow GL_n(R[\varepsilon])$, będącą rozszerzeniem reprezentacji ρ , tj. $\rho' \mapsto \rho$ przy $\varepsilon \mapsto 0$. Okazuje się, że następujące zbiory są równoliczne: (i) $H^1(G, \text{Ad}\rho)$; (ii) $\text{Ext}^1(M, M)$; (iii) klasy równoważności deformacji infinitesimalnych reprezentacji ρ .

W zastosowaniach często żąda się, aby deformacje spełniały pewne warunki. W świetle powyższej bijekcji odpowiada to rozważaniu klas kohomologii leżących w pewnych podzbiorach zbioru $H^1(G, \text{Ad}\rho)$.

Artykuły Mazura [85], [83] zawierają przystępne wprowadzenie do teorii deformacji i zagadnień pokrewnych.

5. Moduł Tate'a krzywej eliptycznej

5.1. Podstawowe własności. Niech E będzie krzywą eliptyczną określoną nad \mathbb{Q} . Wówczas $G_{\mathbb{Q}}$ działa na grupach $E[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^2$ p^n -torsyjnych punktów na $E(\overline{\mathbb{Q}})$. Działanie $G_{\mathbb{Q}}$ jest przemienne z mnożeniem przez p , więc otrzymujemy naturalną strukturę $G_{\mathbb{Q}}$ -modułu na

$$T_p(E) := \varprojlim E[p^n] \simeq \mathbb{Z}_p^2$$

(tzw. **moduł Tate'a**), i w konsekwencji p -adyczną reprezentację Galois

$$\rho_{E,p} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}_p)$$

stowarzyszoną z E . Przytoczymy własności $\rho_{E,p}$ (dowody w [104], [105]):

- (a) Wyznacznik reprezentacji $\rho_{E,p}$ wynosi χ_p .
- (b) $\rho_{E,p}$ jest nierozgałęziona poza pN_E .
- (c) $\rho_{E,p}$ jest absolutnie nieprzywiedlna dla każdego p . Dla ustalonej krzywej eliptycznej E , $\bar{\rho}_{E,p}$ jest absolutnie nieprzywiedlna dla prawie wszystkich p .
- (d) Jeśli E nie dopuszcza mnożenia zespolonego, to $\rho_{E,p}$ (zatem także $\bar{\rho}_{E,p}$) jest surjektywna dla prawie wszystkich p .
- (e) Załóżmy, że E ma dobrą redukcję w p . Wówczas dla każdego $n \geq 1$ istnieje skończony płaski schemat grupowy F_n/\mathbb{Z}_p taki, że $E[p^n](\overline{\mathbb{Q}}_p) \simeq F_n(\overline{\mathbb{Q}}_p)$ jako $G_{\mathbb{Q}_p}$ -moduły.
- (f) Załóżmy, że E jest semistabilna. Wówczas:
 - Jeśli $l \neq p$, to $\bar{\rho}_{E,p}$ jest nierozgałęziona w l wtedy i tylko wtedy, gdy $p \mid \text{ord}_l(\Delta_E)$;
 - $\bar{\rho}_{E,p}$ jest płaska w p wtedy i tylko wtedy, gdy $p \mid \text{ord}_p(\Delta_E)$.

5.2. Twierdzenie Mazura [84], [86]. *Jeśli wszystkie punkty rzędu 2 krzywej eliptycznej E są wymierne, to $\bar{\rho}_p$ jest absolutnie nieprzywiedlna, dla $p \geq 5$.*

5.3. Przykład. Ustalmy liczbę pierwszą $p \geq 5$. Załóżmy, że $a, b, c \in \mathbb{Z}$ ($abc \neq 0$ oraz $(a, b, c) = 1$) spełniają $a^p + b^p + c^p = 0$, tzn. istnieje nietrywialne rozwiązanie tego równania. Bez utraty ogólności możemy założyć, że

$a \equiv -1 \pmod{4}$ oraz $2|b$. Niech $E_{a^p, b^p, c^p} : y^2 = x(x - a^p)(x + b^p)$ oznacza stowarzyszoną krzywą eliptyczną. Przyjmijmy $\rho_{a^p, b^p, c^p} := \rho_{E_{a^p, b^p, c^p}, p}$. Okazuje się, że reprezentacja $\bar{\rho}_{a^p, b^p, c^p}$ jest absolutnie nieprzywiedlna, nieparzysta, nierozgałęziona poza $2p$, płaska w p i semistabilna w 2 .

6. Reprezentacje Galois stowarzyszone z formami modularnymi. Niech $f \in S_k(\Gamma_1(N))$ będzie znormalizowaną nową formą. Teoria Eichlera-Shimury [112] dla $k = 2$, konstrukcja Deligne'a [28] dla $k > 2$ oraz konstrukcja Deligne-Serre'a [31] dla $k = 1$ pozwalają stowarzyszyć z f zgodny system reprezentacji Galois.

6.1. Teoria Eichlera-Shimury. Niech $f = \sum a_n q^n$ będzie znormalizowaną nową formą wagi 2 i poziomu N o współczynnikach wymiernych. Wówczas dla każdej liczby pierwszej l istnieje półprosta ciągła reprezentacja $\rho = \rho_{f, l} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Q}_l)$, która jest nierozgałęziona poza lN i spełnia dwa warunki: $\text{tr}(\rho(\text{Fr}_p)) = a_p$, $\det \rho(\text{Fr}_p) = p$.

Dla dowodu rozważmy moduł Tate'a

$$T_l(J_0(N)) := \varprojlim J_0(N)[l^n] \simeq \mathbb{Z}_l^{2g}$$

rozmaitości Jacobiego $J_0(N)$ krzywej $X_0(N)$. Działanie operatorów Heckeego T_m na $J_0(N)$ indukuje odpowiednie działanie na $T_l(J_0(N))$. Otrzymujemy w ten sposób strukturę wolnego $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}_l$ -modułu rangi 2 na $T_l(J_0(N)) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, i w konsekwencji, reprezentację $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}_l)$. Homomorfizm pierścieni $\mathbb{T} \rightarrow \mathcal{O}_f := \mathbb{Z}\{a_n\}$ (rozszerzający odwzorowanie $T_m \mapsto a_m$) indukuje homomorfizm $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}_l \rightarrow \mathbb{Q}_l$, skąd otrzymujemy reprezentację o żądanych własnościach. Otrzymana reprezentacja jest w istocie równoważna reprezentacji $\rho_{A_f, l}$ stowarzyszonej z rozmaitością A_f z punktu 3.10.

6.2. Twierdzenie Deligne'a-Serre'a. Hipoteza Shimury-Taniyamy-Weila głosi, że każda krzywa eliptyczna E określona nad \mathbb{Q} jest modularna, tj. $L(E, s) = L(f, s)$ dla pewnej formy modularnej f wagi 2 i poziomu N_E . Langlands zasugerował analogiczną hipotetyczną odpowiedniość między pewnymi L -funkcjami Artina i formami parabolicznymi wagi 1 względem $\Gamma_0(N)$. Istnienie rozkładu na iloczyn eulerowski oraz równania funkcyjnego dla szeregów Dirichleta stowarzyszonych z formami modularnymi wagi 1 sugerują, że odpowiadają one L -funkcjom Artina wagi 2 nad \mathbb{Q} , tj. 2-wymiarowym zespolonym reprezentacjom grupy $G_{\mathbb{Q}}$. Deligne i Serre ([31], Th. 4.1) udowodnili to przypuszczenie w postaci następującego twierdzenia.

Niech N będzie liczbą naturalną, ε nieparzystym charakterem Dirichleta modulo N , oraz f formą modularną typu $(1, \varepsilon)$ względem $\Gamma_0(N)$ będącą funkcją własną operatorów Heckeego T_p dla $p \nmid N$. Wówczas istnieje reprezentacja liniowa $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{C})$, nierozgałęziona poza N oraz spełniająca warunki $\text{Tr}(\rho(\text{Fr}_p)) = a_p$, $\det(\rho(\text{Fr}_p)) = \varepsilon(p)$ dla wszystkich $p \nmid N$. Reprezentacja ρ jest nieprzywiedlna wtedy i tylko wtedy, gdy f jest formą paraboliczną.

6.3. Konstrukcja Deligne'a: przypadek wagi $k > 2$. Deligne [28] skonstruował l -adyczne reprezentacje stowarzyszone z formami parabolicznymi wagi ≥ 2 na podgrupach kongruencyjnych w $SL_2(\mathbb{Z})$ jako podgrupy w kohomologiach l -adycznych tzw. rozmaitości Kugi-Sato (gładkich rzutowych rozmaitości algebraicznych określonych nad \mathbb{Q} , będących odpowiednim uzwarzeniem rodzin produktów krzywych eliptycznych).

7. Uniwersalny modułarny pierścień deformacji. Ustalmy nieprzywiedlną reprezentację $\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(k)$, gdzie k jest ciałem skończonym charakterystyki $l > 2$. Załóżmy: (a) $\bar{\rho}|_{G_{\mathbb{Q}_l}}$ jest skończona płaska lub zwyczajna (ang. „ordinary”); (b) $\det \bar{\rho}$ jest charakterem cyklotomicznym; (c) przewodnik $N(\bar{\rho})$ (patrz 12.1) jest liczbą bezkwadratową; (d) $\bar{\rho}$ jest modułarna.

Szczegóły dotyczące warunku (a) oraz materiału zawartego w tym rozdziale można znaleźć w artykułach de Shalita oraz Diamonda i Ribeta w [20].

Niech λ będzie ideałem maksymalnym w \mathcal{O}_f ; oznaczmy przez $\mathcal{O}_{f,\lambda}$ uzupełnienie \mathcal{O}_f względem λ . Warunek (d) oznacza, że $\bar{\rho}$ jest równoważna redukcji reprezentacji $\rho_{f,\lambda}$ stowarzyszonej z formą modułarną f . Reprezentacja $\rho_{f,\lambda} : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{O}_{f,\lambda})$ jest absolutnie nieprzywiedlna oraz wyznaczona, z dokładnością do izomorfizmu, przez warunki: (i) $\rho_{f,\lambda}$ jest nierozgałęziona w p dla $p \nmid lN_f$; (ii) $\text{tr } \rho_{f,\lambda}(\text{Fr}_p) = a_p(f)$, $\det \rho_{f,\lambda}(\text{Fr}_p) = p$. Redukcja $\bar{\rho}_{f,\lambda} : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{O}_f/\lambda)$ jest dobrze określona „z dokładnością do półprostoty”.

Założmy, że $\bar{\rho}$ jest równoważna nad $\bar{\mathbb{Q}}_l$ z pewną $\bar{\rho} = \bar{\rho}_{f,\lambda}$ (istnienie jednej takiej formy f implikuje istnienie nieskończenie wielu). Dla ustalonego skończonego zbioru Σ liczb pierwszych można zapytać, które spośród takich form f mają reprezentacje $\rho_{f,\lambda}$ typu Σ , tj. są semistabilne w l oraz zbiór dzielników pierwszych $N(\rho_{f,\lambda})/N(\bar{\rho})$ zawiera się w Σ ? Okazuje się, że warunkiem koniecznym i dostatecznym na to by f posiadała taką własność jest $N_f|N_{\Sigma}$, gdzie $N_{\Sigma} := N(\bar{\rho}) \prod_{p \in \Sigma} p^{m_p}$ oraz m_p są określone następująco: (i) $m_p = 2$, gdy $p \nmid lN(\bar{\rho})$; (ii) $m_p = 1$, gdy $p \neq l$ oraz $p|N(\bar{\rho})$; (iii) $m_l = 1$ gdy $\bar{\rho}$ jest skończona płaska i zwyczajna w l ; (iv) $m_l = 0$ w pozostałych przypadkach.

7.1. Konstrukcja Wilesa uogólnionej algebry Hecke'go \mathbb{T}_{Σ} . Niech Φ_{Σ} będzie zbiorem nowych form f wagi 2 i poziomu dzielącego N_{Σ} ; okazuje się, że $\Phi_{\Sigma} \neq \emptyset$. Rozważmy pierścień $\mathbb{T}_{\Sigma} := \prod_{f \in \Phi_{\Sigma}} \mathcal{O}_{f,\lambda}$. Dla $p \notin \Sigma$ połóżmy $T_p := (a_p(f))_{f \in \Phi_{\Sigma}} \in \mathbb{T}_{\Sigma}$. Określamy *algebrę Hecke'go \mathbb{T}_{Σ}* jako \mathbb{Z}_l -podalgebrę w \mathbb{T}_{Σ} generowaną przez elementy T_p dla $p \notin \Sigma \cup \{l\}$.

Podamy teraz alternatywną konstrukcję uogólnionej algebry Hecke'go. Rozważmy podpierścień $\mathbb{T} \subset \text{End}(S)$ (gdzie $S := S_2(\Gamma_0(N_{\Sigma}))$), generowany przez operatory Hecke'go T_p dla wszystkich liczb pierwszych p . Dla

$f \in \Phi_\Sigma$ niech f_Σ oznacza \mathbb{T} -formę własną w S , dla której f jest stowarzyszoną nową formą. Taka f_Σ jest scharakteryzowana przez własności: (i) dla $p \in \Sigma \cup \{l\}$ mamy $a_p(f_\Sigma) = 0$; (ii) dla $l|N_\Sigma$ współczynnik $a_l(f_\Sigma)$ jest jednością l -adyczną.

Odwzorowanie $T_p \mapsto$ redukcja $a_p(f_\Sigma)$ modulo λ określa homomorfizm $\mathbb{T} \rightarrow \overline{\mathbb{F}}_l$. Niech \mathbb{T}_m oznacza uzupełnienie \mathbb{T} względem jądra m tego homomorfizmu. Istnieje izomorfizm $\mathbb{T}_\Sigma \simeq \mathbb{T}_m$ taki, że $T_p \mapsto T_p$ dla wszystkich $p \notin \Sigma$.

7.2. Uniwersalność uogólnionej algebry Hecke. Algebra \mathbb{T}_Σ jest uniwersalnym modularnym pierścieniem deformacji w następującym sensie:

- (i) \mathbb{T}_Σ jest zupełną noetherowską lokalną \mathcal{O} -algebrą;
- (ii) istnieje homomorfizm algebr $\mathbb{T} \rightarrow \mathbb{T}_\Sigma$ taki, że \mathbb{T}_Σ jest generowana nad \mathcal{O} przez obrazy operatorów Hecke T_q , dla $q \notin \Sigma$;
- (iii) istnieje Σ -podniesienie $\rho_{\mathbb{T}_\Sigma} : G_\mathbb{Q} \rightarrow GL_2(\mathbb{T}_\Sigma)$ reprezentacji $\bar{\rho}$ takie, że $\text{tr}(\rho_{\mathbb{T}_\Sigma}(\text{Fr}_q)) = T_q$, dla wszystkich $q \notin \Sigma$;
- (iv) jeśli $\rho : G_\mathbb{Q} \rightarrow GL_2(A)$ jest modularna i jest Σ -podniesieniem reprezentacji $\bar{\rho}$, to istnieje dokładnie jeden homomorfizm \mathcal{O} -algebr $\psi_\rho : \mathbb{T}_\Sigma \rightarrow A$ spełniający własność uniwersalności.

Niech $\rho_\Sigma^{\text{univ}} : G_\mathbb{Q} \rightarrow GL_2(R_\Sigma)$ będzie uniwersalną deformacją typu Σ reprezentacji $\bar{\rho}$. Jeśli $\bar{\rho}$ jest modularna oraz $f \in \Phi_\Sigma$, to $\rho_{f,\lambda} : G_\mathbb{Q} \rightarrow GL_2(A_f)$ jest również deformacją typu Σ reprezentacji $\bar{\rho}$ (tutaj A_f oznacza podpierścień pierścienia $\mathcal{O}_{f,\lambda}$, złożony z elementów, których redukcja modulo λ leży w k). Na podstawie uniwersalności R_Σ , istnieje (jedyne) homomorfizm $\pi_{f,\Sigma} : R_\Sigma \rightarrow A_f$ taki, że złożenie $G_\mathbb{Q} \rightarrow GL_2(R_\Sigma) \rightarrow GL_2(A_f)$ jest równoważne z $\rho_{f,\lambda}$. Skoro R_Σ jest (topologicznie) generowany przez elementy postaci $\text{tr}\rho_\Sigma^{\text{univ}}(\text{Fr}_p)$, dla $p \notin \Sigma \cup \{l\}$, więc obrazem odwzorowania $R_\Sigma \rightarrow \tilde{\mathbb{T}}_\Sigma$, $r \mapsto (\pi_{f,\Sigma}(r))_{f \in \Phi_\Sigma}$ jest \mathbb{T}_Σ , tj. otrzymujemy epimorfizm $\Phi_\Sigma : R_\Sigma \rightarrow \mathbb{T}_\Sigma$.

8. Sformułowanie głównego rezultatu Wilesa. Niech p będzie liczbą pierwszą nieparzystą. Niech \mathcal{O} oznacza pierścień elementów całkowitych w skończonym rozszerzeniu K ciała \mathbb{Q}_p z ciałem reszt k . Niech $\mathcal{C}_\mathcal{O}$ oznacza kategorię zupełnych noetherowskich lokalnych \mathcal{O} -algebr z ciałem reszt k . Niech $A \in \text{Ob}(\mathcal{C}_\mathcal{O})$ będzie wolny i skończenie generowany jako \mathcal{O} -moduł. A nazywamy *pełnym przecięciem*, jeśli dla pewnej liczby całkowitej nieujemnej r oraz pewnych $f_1, \dots, f_r \in \mathcal{O}[[T_1, \dots, T_r]]$ mamy izomorfizm $A \simeq \mathcal{O}[[T_1, \dots, T_r]]/(f_1, \dots, f_r)$.

Centralnym rezultatem pracy Wilesa [131] jest następujące twierdzenie.

TWIERDZENIE. *Załóżmy, że reprezentacja $\bar{\rho} : G_\mathbb{Q} \rightarrow GL_2(k)$ jest semistabilna, absolutnie nieprzywiedlna, modularna, $\bar{\rho}_{G_{\mathbb{Q}(\sqrt{-3})}}$ jest modularna,*

oraz $\det \bar{\rho} = \chi_p$. Rozważmy deformacje ρ reprezentacji $\bar{\rho}$ typu D , tj. spełniające w szczególności warunki: $\det(\rho) = \chi_p$, ρ jest semistabilna poza zbiorem skończonym Σ_D oraz nierozgałęziona poza Σ_D , p i punktami rozgałęzienia reprezentacji $\bar{\rho}$. Jeśli ponadto $p \notin \Sigma_D$ oraz $\bar{\rho}$ jest płaska w p , to żądamy, aby ρ była płaska w p . Wówczas kanoniczny homomorfizm $\phi_D : R_D \rightarrow \mathbb{T}_D$ jest izomorfizmem pełnych przecięć.

WNIOSEK. Przy powyższych założeniach, każda deformacja typu D reprezentacji $\bar{\rho}$ jest modularna.

Następne trzy rozdziały zawierają idee oraz szkic dowodu powyższego rezultatu. Podstawowa literatura dotycząca szczegółów dowodu obejmuje [131], [123], [106], [92], [101], [27], [20]. Wstępne definicje i konstrukcje potrzebne dla zrozumienia sformułowanych rezultatów czytelnik znajdzie w [3], [4], [15], [71], [24].

9. Numeryczne kryterium Wilesa-Lenstry. Niech \mathcal{O} oznacza pierścień elementów całkowitych w skończonym rozszerzeniu K ciała \mathbb{Q}_l z ciałem reszt k . Niech $\mathcal{C}_{\mathcal{O}}$ oznacza kategorię zupełnych noetherowskich lokalnych \mathcal{O} -algebr z ciałem reszt k . Niech $\mathcal{C}_{\mathcal{O}}^*$ oznacza kategorię pierścieni z augmentacją, tj. par (A, π_A) , gdzie A jest obiektem z $\mathcal{C}_{\mathcal{O}}$ oraz $\pi_A : A \rightarrow \mathcal{O}$ jest surjektywnym homomorfizmem \mathcal{O} -algebr. Morfizmami w $\mathcal{C}_{\mathcal{O}}^*$ są lokalne homomorfizmy, zgodne w naturalny sposób z augmentacją.

Z parą (A, π_A) stowarzyszamy dwa podstawowe niezmienniki: przestrzeń kostyczną $\Phi_A := (\text{Ker } \pi_A)/(\text{Ker } \pi_A)^2$ oraz ideał kongruencyjny $\eta_A := \pi_A(\text{Ann}_A \text{Ker } \pi_A)$. Φ_A jest przestrzenią kostyczną schematu $\text{Spec}(A)$ w punkcie $\text{Ker } \pi_A$, stąd nazwa. Jest to skończenie generowany \mathcal{O} -moduł.

9.1. Podstawowe własności Φ_A oraz η_A . Załóżmy, że $\phi : A \rightarrow B$ jest surjektywnym homomorfizmem obiektów z $\mathcal{C}_{\mathcal{O}}^*$. Wówczas (i) ϕ indukuje homomorfizm surjektywny $\tilde{\phi} : \Phi_A \rightarrow \Phi_B$; w szczególności $\#\Phi_A \geq \#\Phi_B$ oraz $\eta_A \subset \eta_B$. (ii) $\#\Phi_A \geq \#(\mathcal{O}/\eta_A)$.

9.2. Twierdzenie o izomorfizmie. Załóżmy, że $\phi : A \rightarrow B$ jest surjektywnym homomorfizmem obiektów z $\mathcal{C}_{\mathcal{O}}^*$. (i) Jeśli B jest pełnym przecięciem, $\tilde{\phi}$ jest izomorfizmem, oraz Φ_A jest skończone, to ϕ jest izomorfizmem. (ii) Jeśli A jest pełnym przecięciem, $\eta_A = \eta_B \neq (0)$ oraz A, B są wolnymi \mathcal{O} -modułami skończonej rangi, to ϕ jest izomorfizmem.

9.3. Obiekty kategorii $\mathcal{C}_{\mathcal{O}}^*$ można zastępować pełnymi przecięciami. Niech $A \in \text{Ob}(\mathcal{C}_{\mathcal{O}}^*)$. Jeśli A jest wolnym \mathcal{O} -modułem skończonej rangi, to istnieje pełne przecięcie \tilde{A} i epimorfizm $\tilde{A} \rightarrow A$ taki, że indukowany homomorfizm $\Phi_{\tilde{A}} \rightarrow \Phi_A$ jest izomorfizmem.

9.4. Kryterium Wilesa-Lenstry. Poniższe kryterium udowodnił Lenstra [79]. Różni się ono od oryginalnego kryterium Wilesa ([131], Appendix), gdzie dodatkowo żądano, aby T był pierścieniem Gorensteina.

Niech $\phi : R \rightarrow T$ będzie surjektywnym morfizmem w $\mathcal{C}_\mathcal{O}^*$. Załóżmy, że T jest skończenie generowany, beztorsyjny jako \mathcal{O} -moduł oraz $\eta_T \neq (0)$. Następujące warunki są równoważne: (a) $\#\Phi_R \leq \#(\mathcal{O}/\eta_T)$; (b) $\#\Phi_R = \#(\mathcal{O}/\eta_T)$; (c) pierścienie R i T są pełnymi przecięciami oraz ϕ jest izomorfizmem.

Udowodnimy implikację (a) \Rightarrow (c). Z założenia i 9.1 otrzymujemy

$$\#(\mathcal{O}/\eta_T) \geq \#\Phi_R \geq \#\Phi_T \geq \#(\mathcal{O}/\eta_T),$$

skąd $\#(\mathcal{O}/\eta_T) = \#\Phi_T$. Korzystając z 9.3, otrzymujemy

$$\#(\mathcal{O}/\eta_T) = \#\Phi_T = \#\Phi_{\tilde{T}} \geq \#(\mathcal{O}/\eta_{\tilde{T}}),$$

co w połączeniu z $\eta_{\tilde{T}} \subset \eta_T$, daje $\eta_{\tilde{T}} = \eta_T$. Korzystając z 9.2 otrzymujemy izomorfizm $\tilde{T} \simeq T$, więc T jest pełnym przecięciem. Inną konsekwencją nierówności z początku dowodu tego punktu jest równość $\#\Phi_R = \#\Phi_T$, więc ponowne zastosowanie 9.2 implikuje, że ϕ jest izomorfizmem.

10. Redukcja dowodu twierdzenia Wilesa do przypadku $\Sigma = \emptyset$

10.1. Grupy Selmera. Przyjmijmy $\mathcal{O} = \mathcal{O}_{f,\lambda}$, $p_\Sigma = \Phi_{R_\Sigma}$ oraz $\eta_\Sigma = \eta_{T_\Sigma}$. \mathcal{O} -moduł p_Σ/p_Σ^2 można opisać w terminach kohomologii Galois. Niech M_f oznacza \mathcal{O}^2 z działaniem Galois zadany przez ρ_f ; niech E_f oznacza $\text{ad}^0 M_f$. Przyjmijmy $E_{f,n} := E_f \otimes_{\mathcal{O}} \lambda^{-n} \mathcal{O}/\mathcal{O}$ oraz

$$E_{f,\infty} := \lim_{\rightarrow} E_{f,n} \simeq E_f \otimes_{\mathcal{O}} K/\mathcal{O} \simeq E_f \otimes_{\mathbb{Z}_l} \mathbb{Q}_l/\mathbb{Z}_l.$$

Mamy kanoniczny izomorfizm $\text{Hom}(p_\Sigma/p_\Sigma^2, K/\mathcal{O}) \simeq H_D^1(G_{\mathbb{Q}, \Sigma \cup \{l\}}, E_{f,\infty})$.

Dla porównania długości \mathcal{O} -modułów p_Σ/p_Σ^2 oraz $p_{\Sigma'}/p_{\Sigma'}^2$, rozważamy kojądro naturalnego zanurzenia $H_D^1(G_{\mathbb{Q}, \Sigma \cup \{l\}}, E_{f,\infty}) \rightarrow H_{D'}^1(G_{\mathbb{Q}, \Sigma \cup \{l\}}, E_{f,\infty})$. Otrzymujemy nierówność $\text{length}_{\mathcal{O}}(p_{\Sigma'}/p_{\Sigma'}^2) \leq \text{length}_{\mathcal{O}}(p_\Sigma/p_\Sigma^2) + v_\lambda(c_p)$, gdzie $c_p := (1-p)((1+p)^2 - a_p^2)$ jeśli $p \nmid N(\bar{p})$, oraz $c_p := 1-p^2$ w pozostałych przypadkach. Podkreślimy, że w przypadku $p = l$ oraz $p|N(\bar{p})$ dowód jest bardzo subtelny.

10.2. Moduły kongruencyjne. Należy udowodnić nierówność

$$\text{length}_{\mathcal{O}}(\mathcal{O}/\eta_{\Sigma'}) \leq \text{length}_{\mathcal{O}}(\mathcal{O}/\eta_\Sigma) + v_\lambda(c_p),$$

lub równoważnie, $\eta_{\Sigma'} \subset c_p \eta_\Sigma$. Niech m oznacza ideał maksymalny w $T \otimes \mathcal{O}$, zawierający jądro homomorfizmu $T \otimes \mathcal{O} \rightarrow \mathcal{O}$ wyznaczonego przez f_Σ . Określamy $M_\Sigma := (T_l(J_0(N)) \otimes_{\mathbb{Z}_l} \mathcal{O})_m$. Skoro \mathcal{O} -algebra T_Σ jest izomorficzna z $(T \otimes \mathcal{O})_m$, to możemy rozważać M_Σ jako T_Σ -moduł, więc także jako R_Σ -moduł. Okazuje się, że M_Σ jest wolnym T_Σ -modułem rangi 2.

W celu porównania η_Σ i $\eta_{\Sigma'}$, określimy $T_{\Sigma'}$ -ekwiwariantny homomorfizm $M_{\Sigma'} \rightarrow M_\Sigma$. Rozważmy morfizmy $X_0(N_{\Sigma'}) \rightarrow X_0(N_\Sigma)$ indukowane

przez odwzorowania $\tau \mapsto p^i \tau$, $0 \leq i \leq m_p$. Biorąc pod uwagę funktorialność Albanese, otrzymujemy morfizmy $J_0(N_{\Sigma'}) \rightarrow J_0(N_{\Sigma})$, i w konsekwencji, homomorfizmy $\delta_i : T_i(J_0(N_{\Sigma'})) \otimes_{\mathbb{Z}_i} \mathcal{O} \rightarrow T_i(J_0(N_{\Sigma})) \otimes_{\mathbb{Z}_i} \mathcal{O} \rightarrow M_{\Sigma}$. Określamy $\beta : M_{\Sigma'} \rightarrow M_{\Sigma}$ jako T_{Σ} -liniową kombinację powyższych homomorfizmów. Niech β' oznacza odwzorowanie dołączone względem naturalnych iloczynów skalarnych $\langle \cdot, \cdot \rangle_{\Sigma}$ oraz $\langle \cdot, \cdot \rangle_{\Sigma'}$. Dla uzasadnienia nierówności sformułowanej na początku podrozdziału, dowodzi się, że β' posiada beztorsyjne kojądro. Wówczas z bazy $\{x, y\}$ w M_{Σ} otrzymujemy bazę $\{\beta'(x), \beta'(y)\}$ w $M_{\Sigma'}$, co w konsekwencji daje $\eta_{\Sigma'} = (\langle \beta'(x), \beta'(y) \rangle_{\Sigma'}) = c_p(\langle x, y \rangle_{\Sigma}) = c_p \eta_{\Sigma}$.

10.3. Redukcja do przypadku $\Sigma = \emptyset$. Niech $\Sigma' := \Sigma \cup \{p\}$. Przyjmijmy $a_{\Sigma} := \text{length}_{\mathcal{O}}(p_{\Sigma}/p_{\Sigma}^2)$, $b_{\Sigma} := \text{length}_{\mathcal{O}}(\mathcal{O}/\eta_{\Sigma})$. Podobnie określamy $a_{\Sigma'}$ oraz $b_{\Sigma'}$. Wówczas $a_{\Sigma'} \leq a_{\Sigma} + v_{\lambda}(c_p)$, $b_{\Sigma'} \geq b_{\Sigma} + v_{\lambda}(c_p)$. W konsekwencji równość $a_{\Sigma} = b_{\Sigma}$ implikuje nierówność $a_{\Sigma'} \leq b_{\Sigma'}$. Stosując kryterium Wilesa-Lenstry (patrz 9.4) wnioskujemy, że $\Phi_{\Sigma'}$ jest izomorfizmem oraz $R_{\Sigma'}$, $T_{\Sigma'}$ są pełnymi przecięciami. Wynika stąd następujący kluczowy rezultat:

Jeśli ϕ_{Σ} jest izomorfizmem pełnych przecięć dla $\Sigma = \emptyset$, to jest izomorfizmem pełnych przecięć dla dowolnego zbioru skończonego Σ .

11. Dowód twierdzenia Wilesa w przypadku $\Sigma = \emptyset$. Wiles skonstruował, bazując na ideach prac Kolyvagina [69] i Flachy [43], tzw. system Eulera jedności modularnych. Przy pewnych założeniach potrafił wyprowadzić z jego własności (nie)równość w kryterium Wilesa-Lenstry dla $R = R_{\emptyset}$, $T = T_{\emptyset}$, co kończyło dowód głównego rezultatu. Okazało się jednak, że udowodnione własności systemu Eulera nie są wystarczające w przypadku dowolnej semistabilnej krzywej eliptycznej. Wiles [123] (wspólnie z R. Taylorem) znalazł alternatywny dowód, wykorzystujący fakt, że T_{\emptyset} jest pełnym przecięciem; G. Faltings zaproponował pewne uproszczenia.

11.1. Lemat Taylora-Wilesa-Faltingsa. Niech $\phi : R \rightarrow T$ będzie surjektywnym homomorfizmem lokalnych, zupełnych noetherowskich \mathcal{O} -algebr, przy czym T jest skończona i płaska nad \mathcal{O} . Załóżmy, że istnieje liczba naturalna r oraz dla dowolnej liczby naturalnej n istnieją lokalne, zupełne, noetherowskie \mathcal{O} -algebry R_Q, T_Q oraz przemienny diagram

$$\begin{array}{ccc} \mathcal{O}[[S_1, \dots, S_r]] & \rightarrow & R_Q \rightarrow R \\ & & \downarrow \quad \downarrow \\ & & T_Q \rightarrow T, \end{array}$$

w którym wszystkie cztery homomorfizmy w prawym kwadracie diagramu są surjektywne,

(i) $(S_1, \dots, S_r)R_Q = \text{Ker}(R_Q \rightarrow R)$;

(ii) $(S_1, \dots, S_r)T_Q = \text{Ker}(T_Q \rightarrow T)$;

(iii) $b := \text{Ker}(\mathcal{O}[[S_1, \dots, S_r]] \rightarrow T_Q) \subset ((1 + S_1)^{p^n}, \dots, (1 + S_r)^{p^n})$ oraz T_Q jest wolnym modulem skończonej rangi nad $\mathcal{O}[[S_1, \dots, S_r]]/b$;

(iv) R_Q jest topologicznie generowany jako \mathcal{O} -algebra przez r elementów. Wówczas ϕ jest izomorfizmem pełnych przecięć.

11.2. Struktura algebry Hecke. Niech \mathcal{O} będzie pierścieniem elementów całkowitych w skończonym rozszerzeniu ciała liczb p -adycznych \mathbb{Q}_p , λ ideałem maksymalnym w \mathcal{O} oraz $k := \mathcal{O}/\lambda$. Niech Σ będzie zbiorem liczb pierwszych, gdzie $\bar{\rho}$ jest rozgałęziona. Rozważmy dodatkowy skończony zbiór liczb pierwszych $Q = \{q_1, \dots, q_r\}$, spełniający warunki:

- (i) jeśli $q_i \equiv 1 \pmod{p}$, to $q_i \notin \Sigma$;
- (ii) dla $q \in Q$ macierz $\bar{\rho}(\text{Fr}_q)$ posiada różne wartości własne zawarte w k .

Niech Δ_q oznacza q -podgrupę Sylowa w $(\mathbb{Z}/q\mathbb{Z})^\times$, oraz $\Delta_Q = \prod_{q \in Q} \Delta_q$. Okazuje się, że przy powyższych założeniach: (i) moduł T_Q jest skończony i wolny nad $\Lambda_Q = \mathcal{O}[\Delta_Q]$; (ii) $\text{rank}_{\Lambda_Q} T_Q = \text{rank}_{\mathcal{O}} T$ oraz $T_Q/a_Q T_Q \simeq T$, gdzie a_Q oznacza ideał argumentacji w Λ_Q .

11.3. Struktura uniwersalnego pierścienia deformacji. Istnieje liczba naturalna r taka, że dla dowolnej liczby naturalnej n , istnieje zbiór Q , złożony z r liczb pierwszych, rozłączny z Σ i spełniający warunki: (i) dowolna $q \in Q$ spełnia $q \equiv 1 \pmod{p^n}$; (ii) dla dowolnego $q \in Q$ macierz $\bar{\rho}(\text{Fr}_q)$ ma różne wartości własne, należące do k ; (iii) R_Q jako \mathcal{O} -algebra jest generowany topologicznie przez r elementów.

11.4. Szkic dowodu zasadniczego twierdzenia. Dowód polega na wyznaczeniu r w terminach $\bar{\rho}$ oraz umiejętnym wybraniu, dla każdego $n \geq 1$, r -elementowego zbioru Q_n złożonego z liczb pierwszych przystających do 1 modulo p^n tak, aby spełniony był warunek (iv) lematu Taylora-Wilesa-Faltingsa. Niech R_Q (odpowiednio \mathbb{T}_Q) oznacza uniwersalny (odpowiednio uniwersalny modularny) pierścień deformacji typu Q . Wtedy mamy naturalny epimorfizm $R_Q \rightarrow \mathbb{T}_Q$, natomiast homomorfizm $\mathcal{O}[[S_1, \dots, S_r]] \rightarrow R_Q$ określamy jednoznacznie, żądając aby elementy $1 + S_i$ ($i = 1, \dots, r$) odwzorowały się na ustalone generatory w Δ_{q_i} . Jeśli $p^{n_i} = |\Delta_{q_i}|$, to pierścienie Λ_Q oraz $\mathcal{O}[[S_1, \dots, S_r]]/b$ można utożsamić, gdzie $b := ((1 + S_1)^{p^{n_1}} - 1, \dots, (1 + S_r)^{p^{n_r}} - 1)$ oraz ideał argumentacji a_Q można utożsamić z $(S_1, \dots, S_r)/b$. Dowód (i) wynika bezpośrednio z konstrukcji. Dowody punktów (ii) i (iii) wynikają z kongruencji $q_i \equiv 1 \pmod{p^n}$ oraz z 11.2. Dowód punktu (iv) wynika z 11.3. Jest to najtrudniejszy fragment dowodu.

11.5. Uwagi. Trzeci rozdział monografii Hidy [57] zawiera (prawie) pełny dowód twierdzenia Wilesa w przypadku minimalnym. Metoda opiera się na koncepcji tzw. systemów Taylora-Wilesa wprowadzonych przez Fujiwarę [47]. W swojej nowej monografii [58], Hida podaje szczegółowy dowód ogólniejszego rezultatu (izomorfizm odpowiednich pierścieni deformacji w przypadku form modularnych Hilberta).

12. Hipoteza Serre'a o modularności

12.1. Sformułowanie hipotezy. Hipoteza Serre'a [103] głosi, że dowolną ciągłą nieparzystą nieprzywiedlną dwuwymiarową reprezentację $G_{\mathbb{Q}} \rightarrow GL_2(\overline{\mathbb{F}}_p)$ można otrzymać z formy modularnej modulo p , której wagę, poziom i charakter wyznacza się w terminach reprezentacji. Jest to odpowiednik „filozofii Langlandsa” w charakterystyce p (patrz 19.4). Z niej łatwo wynikają: Wielkie Twierdzenie Fermata i Hipoteza Shimury-Taniyamy-Weila.

HIPOTEZA 2 (Serre [103]). *Każda ciągła nieparzysta nieprzywiedlna reprezentacja*

$$\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(\overline{\mathbb{F}}_p)$$

jest modularna.

Określmy teraz przewodnik Artina reprezentacji. Niech F będzie ciałem skończonym charakterystyki nieparzystej l . Niech $\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(F)$ będzie ciągłą dwuwymiarową reprezentacją Galois; niech V oznacza odpowiadającą dwuwymiarową przestrzeń liniową nad F . Dla $p \neq l$, rozważmy lokalną reprezentację $\bar{\rho}_p : G_{\mathbb{Q}_p} \rightarrow GL_2(F)$. Niech \mathbb{G}_i będzie (skończonym) obrazem i -tej rozgałęzionej podgrupy w $G_{\mathbb{Q}_p}$. Niech $V_i := V^{\mathbb{G}_i}$. Zdefiniujemy

$$n(p, \bar{\rho}) := \sum_{i=0}^{\infty} \frac{\dim(V/V_i)}{\#(\mathbb{G}_0/\mathbb{G}_1)}.$$

Wiadomo, że $n(p, \bar{\rho})$ są liczbami całkowitymi nieujemnymi; przy tym mamy $n(p, \bar{\rho}) = 0$ wtedy i tylko wtedy, gdy $V = V_0$ (wtedy i tylko wtedy, gdy $\bar{\rho}_p$ jest nierozgałęziona). Liczbę $N(\bar{\rho}) := \prod_{p \neq l} p^{n(p, \bar{\rho})}$ nazywamy *przewodnikiem Artina* reprezentacji $\bar{\rho}$.

Określmy teraz tzw. typ („Nebentypus”) reprezentacji. Obraz homomorfizmu $\det \bar{\rho}$ jest abelowy, więc faktoryzuje się przez $\text{Gal}(L/\mathbb{Q})$ dla pewnego skończonego abelowego rozszerzenia L ciała \mathbb{Q} . Z twierdzenia Kroneckera-Webera wynika istnienie najmniejszej liczby naturalnej m dla której $L \subset \mathbb{Q}(\zeta_m)$; można pokazać, że $m = lN(\bar{\rho})$. \det określa charakter $(\mathbb{Z}/m\mathbb{Z})^{\times} \rightarrow \mathbb{C}^{\times}$. Ale $(\mathbb{Z}/m\mathbb{Z})^{\times} \simeq (\mathbb{Z}/l\mathbb{Z})^{\times} \times (\mathbb{Z}/N(\bar{\rho})\mathbb{Z})^{\times}$, więc ograniczając ten charakter do drugiego czynnika, otrzymujemy homomorfizm $\bar{\varepsilon} : (\mathbb{Z}/N(\bar{\rho})\mathbb{Z})^{\times} \rightarrow F^{\times} \hookrightarrow \overline{F}^{\times}$. Podnosząc go do $\mathbb{Z} \subset \mathbb{C}$, otrzymujemy żądany „Nebentypus” $\varepsilon(\bar{\rho}) : (\mathbb{Z}/N(\bar{\rho})\mathbb{Z})^{\times} \rightarrow \mathbb{C}^{\times}$.

Żądając by $\det \bar{\rho} = \varepsilon(\bar{\rho}) \chi_l^{k(\bar{\rho})-1}$, wyznaczmy $k(\bar{\rho})$ modulo $l-1$ (pomiary dokładną definicję $k(\bar{\rho})$). Odnotujmy następujący użyteczny rezultat: $\bar{\rho}$ jest semistabilna wtedy i tylko wtedy, gdy $N(\bar{\rho})$ jest bezkwadratowa, $\varepsilon(\bar{\rho})$ jest trywialny oraz $k(\bar{\rho}) = 2$ lub $l+1$.

HIPOTEZA 3 (Serre) – mocna wersja. *Dla ciągłej nieparzystej nieprzywiedlnej reprezentacji $\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(\overline{\mathbb{F}}_p)$ istnieje paraboliczna forma*

własna f wagi $k(\bar{\rho})$, poziomu $N(\bar{\rho})$ i charakteru $\varepsilon(\bar{\rho})$, taka, że $\bar{\rho}$ jest jej stowarzyszoną reprezentacją residualną, z możliwymi wyjątkami: (a) $p = 2$ oraz $\bar{\rho}$ jest indukowane z charakteru grupy $G_{\mathbb{Q}(\sqrt{-1})}$, (b) $p = 3$ oraz $\bar{\rho}$ jest indukowane z charakteru grupy $G_{\mathbb{Q}(\sqrt{-3})}$.

12.2. Hipoteza Serre'a implikuje Wielkie Twierdzenie Fermata. Ustalmy liczbę pierwszą $p \geq 5$. Załóżmy, że $a, b, c \in \mathbb{Z}$ ($abc \neq 0$ oraz $(a, b, c) = 1$) spełniają $a^p + b^p + c^p = 0$, tzn. istnieje nietrywialne rozwiązanie tego równania. Bez utraty ogólności możemy założyć, że $a \equiv -1 \pmod{4}$ oraz $2|b$. Niech $E_{a^p, b^p, c^p} : y^2 = x(x - a^p)(x + b^p)$ oznacza stowarzyszoną krzywą eliptyczną Freya-Hellegouarcha [46], [55], która jest semistabilna (patrz 1.2). Przyjmijmy $\rho_{a^p, b^p, c^p} := \rho_{E_{a^p, b^p, c^p}, p}$. Mamy: (i) $\bar{\rho}_{a^p, b^p, c^p}$ jest nieparzysta i nieprzywiedlna (patrz 5.2), (ii) jej niezmienniki (N, k, ϵ) wynoszą $(2, 2, 1)$. Ponieważ $\dim S_2(\Gamma_0(2)) = g(X_0(2)) = 0$, więc otrzymujemy sprzeczność, która kończy dowód implikacji.

Krzywe postaci E_{a^p, b^p, c^p} badał Hellegouarch [55] na początku lat sześćdziesiątych ubiegłego stulecia. Frey [46] w 1985 roku podjął (nieudaną) próbę wywnioskowania Wielkiego Twierdzenia Fermata z Hipotezy Shimury-Taniyamy-Weila. Pełny dowód tej implikacji podał Ribet w 1986 roku (patrz następny rozdział).

12.3. Udowodnione przypadki. Serre podał szereg przykładów potwierdzających swoją hipotezę. Ważny szczególny przypadek hipotezy Serre'a został udowodniony przez Ribeta (patrz rozdział 13). Ponadto Shepherd-Barron i Taylor [111], Breuil, Conrad, Diamond i Taylor [10], Manoharmayum [81] oraz Ellenberg [40] udowodnili ogólne rezultaty dla reprezentacji o wartościach w $GL_2(\mathbb{F}_q)$ ($q = 4, 5, 7, 9$), potwierdzające hipotezę. Khare [132] udowodnił hipotezę Serre'a dla nieparzystych, nieprzywiedlnych reprezentacji $\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(\overline{\mathbb{F}}_p)$, nierozgałęzionych poza p (tj. $N(\bar{\rho}) = 1$).

13. Twierdzenie Ribeta. Ustalmy liczbę naturalną M oraz dwie liczby pierwsze p, q względnie pierwsze z M . Niech $\overline{\mathbb{T}}$ oznacza pq -nową część algebry \mathbb{T}_{Mpq} . Niech m będzie ideałem maksymalnym w $\overline{\mathbb{T}}$ oraz $k_m = \overline{\mathbb{T}}/m$. Niech $\rho_m : G_{\mathbb{Q}} \rightarrow GL_2(k_m)$ będzie odpowiadającą reprezentacją. Ribet [97] udowodnił następujący przypadek hipotezy Serre'a.

Założmy, że charakterystyka l ciała k_m jest nieparzysta i względnie pierwsza z Mq oraz $q \not\equiv 1 \pmod{l}$. Jeśli ρ_m jest nieprzywiedlna i skończona w p , to jest modularna poziomu Mq .

Z powyższego faktu Ribet wyprowadził następujący rezultat, kluczowy dla dowodu Wielkiego Twierdzenia Fermata.

Niech f będzie nową formą wagi 2 i poziomu Nl , gdzie l jest liczbą pierwszą nie dzielącą N . Załóżmy, że $\bar{\rho}_f : G_{\mathbb{Q}} \rightarrow GL_2(\overline{\mathbb{F}}_p)$ jest nieprzywiedlna, oraz spełniony jest jeden z poniższych warunków: (i) $\bar{\rho}_f$ jest nierozgałęzioną w l ; (ii) $l = p$ i $\bar{\rho}_f$ jest płaska w p . Wówczas istnieje nowa forma g wagi 2 i poziomu N taka, że $\bar{\rho}_f \simeq \bar{\rho}_g$.

14. Twierdzenie Langlandsa-Tunnella. Niech $\sigma : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{C})$ będzie reprezentacją nieparzystą, nieprzywiedlną, z rozwiązalnym obrazem w $PGL_2(\mathbb{C})$. Wówczas istnieje znormalizowana forma paraboliczna $\sum_{n \geq 1} b_n e^{2\pi i n z}$ wagi 1 względem pewnej grupy $\Gamma_1(N)$, będąca funkcją własną dla odpowiadającej algebry operatorów Hecke oraz taka, że $b_q = \text{tr}(\sigma(\text{Fr}_q))$ dla prawie wszystkich liczb pierwszych q [76], [125].

Idea dowodu. (i) Twierdzenie można przeformułować w terminach istnienia reprezentacji automorficznej $\pi(\sigma)$. (ii) Teoria zamiany bazy Langlandsa ([76]) opisuje odpowiedniość między reprezentacjami automorficznymi grup $GL_n(A_F)$ i $GL_n(A_E)$, gdzie E jest cyklicznym rozszerzeniem prostego stopnia l ciała liczbowego F . Korzystając z niej, konstruuje się pewną reprezentację $\pi_{ps}(\sigma)$. (iii) Korzystając z własności L -funkcji typu Rankina-Selberga dla $GL(3) \times GL(3)$, dowodzi się, że jest to szukana reprezentacja $\pi(\sigma)$.

15. Hipoteza Shimury-Taniyamy-Weila. Krzywa eliptyczna E określona nad \mathbb{Q} jest *modularna*, jeśli istnieje nowa forma f wagi 2 i poziomu N_E taka, że $L(f, s) = L(E, s)$.

HIPOTEZA 4 (O MODULARNOŚCI) (SHIMURA-TANIYAMA-WEIL). *Dowolna krzywa eliptyczna określona nad \mathbb{Q} jest modularna.*

Powyższa hipoteza, w mniej dokładnej formie, została po raz pierwszy sformułowana przez Taniyamę [114] podczas międzynarodowego sympozjum w Tokio w 1955 r. Sama hipoteza w przeszłości przyjmowała różne nazwy. Van der Poorten ([126], str. 121) wspomina następującą zabawną sytuację: wspólnie z Coatesem zaczęli sprawdzać „hipotezę Weila” dla krzywych eliptycznych o przewodniku 11; gdy jednak praca była na ukończeniu, Coates zaproponował nazwę „hipoteza Taniyamy-Weila” jako bardziej aktualną. Z kolei Lang [73] przytacza argumenty, aby nazywać ją hipotezą Shimury-Taniyamy. Jednak bez wątplenia jej obecny kształt jest zasługą rezultatów Shimury [112], [113] oraz Weila [129].

15.1. Równoważne warunki modularności. Niech E będzie dowolną krzywą eliptyczną określoną nad \mathbb{Q} . Następujące warunki są równoważne:

- (a) E jest modularna;
- (b) $\rho_{E,p}$ jest modularna dla pewnej liczby pierwszej p ;
- (c) $\rho_{E,p}$ jest modularna dla każdej liczby pierwszej p ;
- (d) istnieje niestały morfizm $X_0(N_E) \rightarrow E$ krzywych algebraicznych określonych nad \mathbb{Q} ;
- (e) E jest izogeniczna z rozmaiutością abelową A_f stowarzyszoną z pewną nową formą f wagi 2 i poziomu N_E .

D o w ó d. (a) \Leftrightarrow (c). Mamy $L(E, s) = \prod_p L_p(E, p^{-s})^{-1}$, gdzie $L_p(E, X) := \det(1 - \rho_{E,l}(F_r)X|_{V_l(E)^{I_p}})$. Teraz należy zastosować 6.1.

(b) \Rightarrow (c). Załóżmy, że dla pewnej formy f reprezentacje $\rho_{E,p}$ oraz $\rho_{f,p}$ są równoważne. Wówczas, dla prawie wszystkich liczb pierwszych l , mamy $\text{tr}(\rho_{f,p}(\text{Fr}_l)) = \text{tr}(\rho_{E,p}(\text{Fr}_l))$. Korzystając z własności reprezentacji $\rho_{E,p}$ oraz $\rho_{f,p}$, otrzymujemy $a_l(f) = l + 1 - \#\overline{E}_l(\mathbb{F}_l) \in \mathbb{Z}$ dla prawie wszystkich liczb pierwszych. Stosując twierdzenie Chebotarewa o gęstości (patrz, np. [15], rozdz. 8) otrzymujemy równoważność $\rho_{E,p}$ i $\rho_{f,p}$ dla wszystkich p .

(c) \Rightarrow (e). Ostatnia identyczność zachodzi dla wszystkich liczb pierwszych l nie dzielących $N_f = N_E$. Skoro $\det(\rho_{f,p}) = \det(\rho_{E,p}) = \varepsilon$, to ψ_f jest trywialny. Poza tym $a_l \in \{0, 1, -1\}$ dla $l|N_f$. Zatem $K_f = \mathbb{Q}$ i A_f jest krzywą eliptyczną określoną nad \mathbb{Q} . Twierdzenie Faltingsa o izogenii [41] implikuje, że E jest izogeniczna z A_f .

(d) \Rightarrow (e). Niestaly morfizm $\pi : X_0(N_E) \rightarrow E$ indukuje surjektywne odwzorowanie rozmaitości Jacobiego $\pi_* : J_0(N_E) \rightarrow E$. Skoro $J_0(N_E)$ jest izogeniczna z produktem rozmaitości abelowych postaci A_f , gdzie f przebiega nowe formy wagi 2 i poziomu N_f dzielącego N_E , więc dla pewnej takiej nowej formy istnieje surjektywne odwzorowanie $A_f \rightarrow E$. Skoro A_f jest prostą rozmaitością abelową, to nasze odwzorowanie jest izogenią.

(e) \Rightarrow (d). Na podstawie założenia, istnieje surjektywne odwzorowanie $J_0(N_E) \rightarrow E$. Składając je z odwzorowaniem Abela-Jacobiego $X_0(N_E) \rightarrow J_0(N_E)$ otrzymujemy niestaly morfizm $X_0(N_E) \rightarrow E$.

Z powyższego kryterium otrzymujemy bezpośrednio następujące wnioski: (i) Krzywa eliptyczna $X_0(11)$, i ogólniej, dowolna krzywa $X_0(N)$ genusu 1, jest modularna. (ii) Krzywa eliptyczna (określona nad \mathbb{Q}) izogeniczna z krzywą eliptyczną modularną jest modularna.

15.2. *Przypadek krzywych eliptycznych z CM.* Krzywe eliptyczne z mnożeniem zespolonym nie są semistabilne. Modularność tej klasy krzywych wynika z klasycznych rezultatów Deuringa [32] i Shimury [112], [113].

15.3. *Z hipotezy Shimury-Taniyamy-Weila wynika hipoteza Hassego.* Zakładając hipotezę Shimury-Taniyamy-Weila dla E , otrzymujemy $L(E, s) = L(f, s)$, gdzie f jest pewną nową formą wagi 2 i poziomu $N = N_E$. W tym przypadku hipoteza Hassego (patrz 1.3) wynika bezpośrednio z twierdzenia Heckeego (patrz 2.3).

15.4. *Mocna wersja hipotezy Serre'a implikuje hipotezę Shimury-Taniyamy-Weila.* Niech E będzie krzywą eliptyczną określoną nad \mathbb{Q} , oraz niech $L(E, s) = \sum_{n \geq 1} a_n n^{-s}$ oznacza stowarzyszoną L -funkcję. Z hipotezy Serre'a wynika, że dla prawie wszystkich liczb pierwszych l istnieją: system $(a_{p,l})_{p \nmid N_E}$ wartości własnych powstały z $S_2(\Gamma_0(N_E))$, oraz przedłużenie v_l waluacji p -adycznej z \mathbb{Q} na $\overline{\mathbb{Q}}$ takie, że $\forall_{p \nmid N_E} v_l(a_{p,l} - a_p) > 0$. Ponieważ na przestrzeni $S_2(\Gamma_0(N_E))$ mamy jedynie skończenie wiele takich systemów, więc nasz system jest jednym z nich. Zatem krzywa E jest modularna, co kończy dowód.

15.5. Parametryzacja hiperboliczna krzywej eliptycznej. Belyi [6] udowodnił, że dowolna krzywa algebraiczna X określona nad ciałem liczbowym K dopuszcza nakrycie (określone nad K) $X \rightarrow \mathbb{P}^1$, rozgałęzione tylko w trzech punktach $0, 1, \infty$. W konsekwencji, dowolna krzywa eliptyczna określona nad ciałem liczb wymiernych dopuszcza uniformizację za pomocą form modularnych względem pewnej podgrupy Γ skończonego indeksu w $\Gamma_0(1)$ (patrz [107], str. 71). Rezultat ten nie implikuje hipotezy Shimury-Taniyamy-Weila, gdyż podgrupy skończonego indeksu w $\Gamma_0(1)$ nie muszą być kongruencyjne.

16. Modularność krzywych eliptycznych. I. Przypadek semistabilny. Rozdział zawiera pewne szczegóły ostatniej części artykułu Wilesa [131].

16.1. Dowód hipotezy Serre'a dla $p = 3$. Wiles dowodzi, że jeśli $\rho_0 : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}_3)$ jest nieprzywiedlna i nieparzysta, to jest modularna.

D o w ó d. Rozważmy złożenie $\sigma = \Psi \circ \rho_0$, gdzie Ψ jest zanurzeniem

$$\Psi : GL_2(\mathbb{F}_3) \hookrightarrow GL_2(\mathbb{Z}[\sqrt{-2}]) \subset GL_2(\mathbb{C})$$

zadany na generatorach $\alpha = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ grupy $GL_2(\mathbb{F}_3)$ za pomocą formuł:

$$\Psi(\alpha) = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \quad \Psi(\beta) = \begin{pmatrix} -1 & 1 \\ -\sqrt{-2} & -1 + \sqrt{-2} \end{pmatrix}.$$

Okazuje się, że reprezentacja σ jest rozwiązalna, nieparzysta i nieprzywiedlna. Stosując twierdzenie Langlandsa-Tunnella (patrz rozdz. 14), otrzymujemy znormalizowaną formę własną $g(z) = \sum_{n \geq 1} b_n q^n$ wagi 1 i poziomu N , spełniającą $b_q = \text{tr } \sigma(Fq)$ dla prawie wszystkich liczb pierwszych q .

Rozważmy $E(z) := 1 + 6 \sum_{n \geq 1} \sum_{d|n} \chi(d) e^{2\pi i n z}$, gdzie χ jest nieparzystym charakterem Dirichleta modulo 3. Wówczas E jest formą modularną wagi 1 i poziomu 3. Iloczyn $g(z)E(z) = \sum_{n \geq 1} c_n e^{2\pi i n z}$ jest formą paraboliczną wagi 2 względem $\Gamma_0(N)$, spełniającą $c_n \equiv b_n \pmod{\mathfrak{p}}$ dla ideału pierwszego \mathfrak{p} leżącego nad 3. Teraz zastosujemy rezultat Deligne-Serre'a ([31], 6.10), biorąc $f_1 = gE$. Otrzymujemy znormalizowaną formę paraboliczną $f \in S_2(\Gamma_0(N), \psi)$ taką, że $T_p f = a_p f$ oraz $a_p \equiv c_p \equiv b_p \pmod{\mathfrak{p}}$ dla wszystkich p , co kończy dowód.

Odnajdujemy jeszcze ważny wniosek.

Niech E będzie krzywą eliptyczną określoną nad \mathbb{Q} . Jeśli $\bar{\rho}_{E,3}$ jest nieprzywiedlna, to jest modularna.

16.2. Konstrukcja pomocniczej krzywej eliptycznej. Niech E będzie krzywą eliptyczną określoną nad \mathbb{Q} . Załóżmy, że E jest semistabilna oraz

$\bar{\rho}_{E,5}$ jest nieprzywiedlna. Wówczas istnieje semistabilna krzywa eliptyczna E' określona nad \mathbb{Q} taka, że (i) $\bar{\rho}_{E',3}$ jest nieprzywiedlna oraz (ii) $\bar{\rho}_{E',5} \simeq \bar{\rho}_{E,5}$.

D o w ó d. Wiles konstruuje taką krzywą eliptyczną E' , stosując twierdzenie Hilberta o nieprzywiedlności do pewnej przestrzeni parametrów krzywych eliptycznych. Niech X oznacza „twist” krzywej modularnej $X(5)$ przez kocykl indukowany przez $\bar{\rho}_{E,5}$, oraz niech S będzie zbiorem ostrzy krzywej X . Wówczas X jest określona nad \mathbb{Q} , oraz posiada następujące własności: (i) elementy zbioru $(X \setminus S)(\mathbb{Q})$ odpowiadają klasom izomorfizmu par (E', ϕ) , gdzie E' jest krzywą eliptyczną określoną nad \mathbb{Q} , oraz $\phi : E'[5] \rightarrow E'[5]$ jest izomorfizmem $G_{\mathbb{Q}}$ -modułów; (ii) $(X \setminus S)(\mathbb{C})$ jest (jako rozmaitość zespolona) sumą czterech kopii $Y(5)$.

Wiadomo, że $Y(5)$ jest genusu zero. $X(\mathbb{Q}) \neq \emptyset$, gdyż zawiera punkt wymierny odpowiadający (E, id) , zatem jedna ze składowych X^0 krzywej X jest krzywą (genusu zero) określoną nad \mathbb{Q} , zawierającą nieskończenie wiele punktów wymiernych. Dowodzi się (stosując twierdzenie Hilberta o nieprzywiedlności), że nieskończenie wiele spośród takich punktów odpowiada krzywymi eliptycznym E' dla których $\bar{\rho}_{E',3}$ jest nieprzywiedlna.

16.3. Nieprzywiedlność $\bar{\rho}_{E,3}$ lub $\bar{\rho}_{E,5}$. Niech E będzie krzywą eliptyczną określoną nad \mathbb{Q} . Jeśli E jest semistabilna, to przynajmniej jedna z reprezentacji $\bar{\rho}_{E,3}$, $\bar{\rho}_{E,5}$ jest nieprzywiedlna.

D o w ó d. Załóżmy nie wprost, że reprezentacje $\bar{\rho}_{E,3}$, $\bar{\rho}_{E,5}$ są przywiedlne. Wówczas $E(\mathbb{Q})$ zawiera podgrupę rzędu 15. Z 3.5 wynika więc, że E nie może być semistabilna.

16.4. Nieprzywiedlność i modularność $\bar{\rho}_{E,p}$ implikuje modularność E . Niech E będzie krzywą eliptyczną określoną nad \mathbb{Q} . Załóżmy, że E jest semistabilna. Jeśli dla pewnej nieparzystej liczby pierwszej p reprezentacja $\bar{\rho}_{E,p}$ jest nieprzywiedlna i modularna, to E jest modularna.

D o w ó d. Mamy $\det \bar{\rho}_{E,p} = \chi_p$. Jeśli E jest semistabilna, to $\bar{\rho}_{E,p}$ jest semistabilna dla dowolnego p . Z twierdzenia Serre'a ([104], Prop. 21) wynika, że semistabilność E implikuje surjektywność lub przywiedlność $\bar{\rho}_{E,p}$ dla $p \geq 3$. Zatem dla $p \geq 3$ absolutna nieprzywiedlność $\bar{\rho}_{E,p}$ jest równoważna jej nieprzywiedlności, zaś w przypadku $p = 3$ jest równoważna absolutnej nieprzywiedlności reprezentacji $\bar{\rho}_{E,p}|_{G_{\mathbb{Q}(\sqrt{-3})}}$. Teza lematu wynika teraz z centralnego rezultatu Wilesa (rozdział 8).

16.5. Dowód modularności krzywych eliptycznych w przypadku semistabilnym według A. Wilesa. Niech E będzie semistabilną krzywą eliptyczną określoną nad \mathbb{Q} . Jeśli $\bar{\rho}_{E,3}$ jest nieprzywiedlna, to korzystając z 16.1

oraz 16.4 otrzymujemy modularność E . Załóżmy więc, że $\bar{\rho}_{E,3}$ nie jest nieprzywiedlna. Z 16.3 wynika, że $\bar{\rho}_{E,5}$ jest nieprzywiedlna. Z 16.2 otrzymujemy istnienie modularnej krzywej eliptycznej E' określonej nad \mathbb{Q} spełniającej $\bar{\rho}_{E',5} \simeq \bar{\rho}_{E,5}$. W szczególności $\bar{\rho}_{E,5}$ jest modularna, więc z 16.4 otrzymujemy modularność E .

16.6. Dowód Wielkiego Twierdzenia Fermata. Ustalmy liczbę pierwszą $p \geq 5$. Załóżmy, że $a, b, c \in \mathbb{Z}$ ($abc \neq 0$ oraz $(a, b, c) = 1$) spełniają $a^p + b^p + c^p = 0$, tzn. istnieje nietrywialne rozwiązanie tego równania. Możemy założyć, bez utraty ogólności, że $a \equiv -1 \pmod{4}$ oraz $2|b$. Niech $E_{a^p, b^p, c^p} : y^2 = x(x - a^p)(x + b^p)$ oznacza stowarzyszoną krzywą eliptyczną. Połóżmy $\rho_{a^p, b^p, c^p} := \rho_{E_{a^p, b^p, c^p}, p}$. Wtedy E_{a^p, b^p, c^p} jest semistabilna (1.2). Z twierdzenia Wilesa wynika, że jest ona modularna, więc istnieje nowa forma f_{a^p, b^p, c^p} poziomu $N_{E_{a^p, b^p, c^p}}$ spełniająca $\rho_{a^p, b^p, c^p} \simeq \rho_{f_{a^p, b^p, c^p}, p}$. Korzystając z 5.3 otrzymujemy, że residualna reprezentacja $\bar{\rho}_{a^p, b^p, c^p}$ jest absolutnie nieprzywiedlna, nierozgałęziona poza $2p$ i płaska w p . Z twierdzenia Ribeta wynika istnienie nowej formy g wagi 2 i poziomu 2 spełniającej $\bar{\rho}_{g, p} \simeq \rho_{a^p, b^p, c^p}$. Jednak $\dim S_2(\Gamma_0(2)) = g(X_0(2)) = 0$ i otrzymujemy sprzeczność z istnieniem takiej nowej formy (z definicji jest to forma niezerowa). Dowód Wielkiego Twierdzenia Fermata jest więc zakończony.

16.7. Podejście Kharego. Khare [64] podał nowy dowód głównego rezultatu Wilesa, bez wykorzystania tzw. systemów Taylora-Wilesa. W jego metodzie, dowód twierdzenia Wilesa dla przypadku minimalnego (tj. $\Sigma = \emptyset$) jest zastąpiony przez dowód izomorficzności tzw. nowych ilorazów: $R_{\mathbb{Q}}^{Q-new} \simeq \mathbb{T}_{\mathbb{Q}}^{Q-new}$. W [65] Khare proponuje podejście do dowodu modularności p -adycznej reprezentacji Galois z pominięciem teorii deformacji, które w pewnych przypadkach pozwala znacznie uprościć dowód rezultatów Wilesa i Taylora.

17. Modularność krzywych eliptycznych. II. Przypadek ogólny

17.1. Twierdzenie Diamonda.¹ Diamond uogólnił rezultat Wilesa i Taylora następująco ([33], [34], [99]): *Jeśli E posiada semistabilną redukcję w 3 i 5, to jest modularna.* Jego dowód wynika z twierdzenia Langlandsa-Tunnella oraz następującego rezultatu (również udowodnionego przez Diamonda). Niech E będzie krzywą eliptyczną określoną nad \mathbb{Q} oraz p nieparzystą liczbą pierwszą spełniającą warunki: (i) E jest semistabilna w p ;

¹ Autor nie był obecny na słynnych wykładach Wilesa w czerwcu 1993 roku, miał za to przyjemność wysłuchania wykładów Diamonda i innych na seminarium z teorii liczb podczas swojego pobytu w 1995 roku na Wydziale Matematyki i Statystyki Uniwersytetu w Cambridge. Dowód rezultatu omówionego w 17.1 Diamond referował wiosną 1995 r.

(ii) $\bar{\rho}_{E,p}$ ograniczona do podgrupy $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{(-1)^{p-1}/2p}))$ jest absolutnie nieprzywiedlna; (iii) $\bar{\rho}_{E,p}$ jest modularna. Wówczas E jest modularna.

Idea dowodu głównego rezultatu. Przytoczony rezultat dla $p = 3$ oraz twierdzenie Langlandsa-Tunnella implikują twierdzenie Diamonda przy założeniu, że $\bar{\rho}_{E,3}$ ograniczona do podgrupy $G_{\mathbb{Q}(\sqrt{-3})}$ jest absolutnie nieprzywiedlna. Jeśli $\bar{\rho}_{E,3}$ ograniczona do podgrupy $G_{\mathbb{Q}(\sqrt{-3})}$ nie jest absolutnie nieprzywiedlna, to stosujemy wspomniany rezultat dla $p = 5$. Oczywiście należy sprawdzić, że spełnione są założenia, co wynika z dwóch rezultatów pomocniczych. Pierwszy z nich podaje warunki konieczne na to, aby reprezentacja $\bar{\rho}_{E,5}$ ograniczona do podgrupy $G_{\mathbb{Q}(\sqrt{5})}$ była absolutnie nieprzywiedlna. Drugi z rezultatów podaje warunki konieczne na to, aby reprezentacja $\bar{\rho}_{E,5}$ była modularna.

17.2. Przypadek $27 \nmid N_E$. Centralnym narzędziem w dowodzie hipotezy Shimury-Taniyamy-Weila w przypadku semistabilnym, jak też jego rozszerzenia do przypadku semistabilnej redukcji w 3 i 5, jest teoria deformacji reprezentacji Galois. Conrad [18] rozwinął odpowiednią teorię deformacji, którą można zastosować w przypadkach nie-semistabilnych. Conrad, Diamond i Taylor [19] zastosowali wariant tej teorii dla pewnej klasy reprezentacji Galois typu Barsotti-Tate'a, co w połączeniu z metodą Wileasa [131] pozwoliło im uzyskać modularność krzywych eliptycznych o przewodnikach nie podzielnych przez 27. Zauważmy, że $27 \nmid N_E$ wtedy i tylko wtedy, gdy E posiada semistabilną redukcję nad łagodnie rozgałęzionym rozszerzeniem ciała \mathbb{Q}_3 . Dla dowodu głównego twierdzenia wystarczy rozważać reprezentacje pochodzące od grup l -podzielnych nad pewnymi łagodnie rozgałęzionymi rozszerzeniami ciała \mathbb{Q}_l .

Idea dowodu. Załóżmy, że E jest krzywą eliptyczną nad \mathbb{Q} , posiadającą semistabilną redukcję w 3. Korzystając z [33], [34] dowodzi się, że albo $\bar{\rho}_{E,5}$ jest przywiedlna (wówczas E jest modularna), albo $\bar{\rho}_{E,5}$ jest nieprzywiedlna i modularna. W drugim przypadku, jeśli E posiada potencjalnie zwyczajną lub potencjalnie moltiplikatywną redukcję w 5, to (zastępując E przez skrócenie) można założyć, że E posiada dobrą redukcję nad $K = \mathbb{Q}_5(5^{1/3})$. Teraz stosuje się metodę Wileasa biorąc $p = 5$ oraz rozważając „potencjalnie płaskie” deformacje zamiast „płaskich”.

17.3. Ogólny przypadek. C. Breuil, B. Conrad, F. Diamond i R. Taylor [10] udowodnili modularność dowolnej nieprzywiedlnej reprezentacji $\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}_5)$ z charakterem cyklotomicznym. Dla dowodu tego rezultatu, autorzy dzielą rozważane reprezentacje na sześć klas w zależności od pewnych 3-adycznych własności. Następnie dowodzą modularności reprezentacji należących do każdej z klas oddzielnie, korzystając z twierdzenia Langlandsa-Tunnella oraz metod Wileasa i Wileasa-Taylora. Biorąc pod uwagę wcześniejszą pracę [19], to daje dowód hipotezy Shimury-Taniyamy-Weila w pełnej ogólności (patrz także przeglądowy artykuł Edixhovena [37]).

18. Zastosowania

18.1. Zastosowanie do równań diofantycznych. Metodę dowodu Wielkiego Twierdzenia Fermata można przenieść na ogólniejszą klasę równań. Niech $l \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}$ oraz $p \geq 11$ będzie liczbą pierwszą różną od l . Wówczas dla dowolnej liczby całkowitej nieujemnej α równanie $x^p + l^\alpha y^p + z^p = 0$ nie posiada nietrywialnych całkowitych rozwiązań [103], [26].

Ustalmy niezerowe, względnie pierwsze liczby całkowite A, B, C . Kraus [70] udowodnił, że uogólnione równanie Fermata $Ax^p + By^p + Cz^p = 0$ nie posiada nietrywialnych rozwiązań przy $p > f(A, B, C)$, gdzie $f(A, B, C)$ jest stałą efektywną. Halberstadt i Kraus [51] udowodnili, przy założeniu nieparzystości iloczynu ABC , że istnieje taki zbiór $\Pi = \Pi(A, B, C)$ liczb pierwszych o dodatniej gęstości, że dla dowolnego $p \in \Pi$ równanie $Ax^p + By^p + Cz^p = 0$ nie posiada nietrywialnych całkowitych rozwiązań.

Darmon i Granville [25] udowodnili w 1993 roku (jeszcze przed słynnymi wykładami Wilesa w Cambridge) następujący ważny rezultat. Ustalmy niezerowe liczby całkowite A, B, C oraz liczby naturalne p, q, r spełniające warunek $1/p + 1/q + 1/r < 1$. Wówczas równanie $Ax^p + By^q = Cz^r$ posiada skończenie wiele prymitywnych rozwiązań w zbiorze liczb całkowitych.

Czytelnik może spróbować zmierzyć się z następującym problemem, zaproponowanym przez Tijdemana i Zagiera.

Ustalmy liczby naturalne p, q, r spełniające warunek $1/p + 1/q + 1/r < 1$. Wówczas równanie $x^p + y^q = z^r$ nie posiada nietrywialnych prymitywnych rozwiązań w zbiorze liczb całkowitych, z wyjątkiem następujących 10 przypadków:

$$\begin{aligned} 1^p + 2^3 &= 3^2, & 2^5 + 7^2 &= 3^4, & 7^3 + 13^2 &= 2^9, \\ 2^7 + 17^3 &= 71^2, & 3^5 + 11^4 &= 122^2, & 33^8 + 1549034^2 &= 15613^3 \\ 17^7 + 76271^3 &= 21063928^2, & 1414^3 + 2213459^2 &= 65^7, \\ 9262^3 + 15312283^2 &= 113^7, & 43^8 + 96222^3 &= 30042907^2. \end{aligned}$$

W przypadku $1/p + 1/q + 1/r = 1$ istnieje dokładnie jedno nietrywialne prymitywne rozwiązanie całkowite, odpowiadające $(p, q, r) = (6, 3, 2)$: $1^6 + 2^3 = 3^2$. W przypadku $1/p + 1/q + 1/r > 1$ równanie $x^p + y^q = z^r$ posiada nieskończenie wiele nietrywialnych całkowitych rozwiązań. W tym miejscu należy wspomnieć o Hipotezie Catalana (udowodnionej niedawno przez Mihăilescu [87]): $3^2 - 2^3 = 1$ jest jedynym rozwiązaniem równania $x^p - y^q = 1$ w liczbach całkowitych x, y, p, q większych od jedynki.

Warianty dowodu Wielkiego Twierdzenia Fermata można zastosować do pewnych niejednorodnych równań, jednak w tych przypadkach wybór krzywej eliptycznej odpowiadającej hipotetycznemu rozwiązaniu jest bardziej subtelny ([7], [26], [39], [25], [22]). Np. w przypadku równania $x^p + y^p = z^3$, $p \geq 7$, krzywą zadaje się następująco [26]:

$$Y^2 + b^p Y = X^3 - \frac{3}{2}c\left(\frac{c^3}{8} + b^p\right)X - \frac{c^3}{8}\left(\frac{c^3}{4} - 5b^p\right), \text{ gdy } 2|c;$$

$$Y^2 + cXY = X^3 - c^2 X^2 - \frac{3}{2}cb^2 X + b^p\left(a^p + \frac{5}{4}b^p\right), \text{ gdy } 2|ab.$$

W rozważanym przypadku mamy $27|N_E$, więc powyższe krzywe eliptyczne nie są semistabilne.

Dla dowodu nieistnienia nietrywialnych rozwiązań całkowitych równania $x^4 + y^2 = z^p$, $p \geq 211$, Ellenberg [39] rozważa krzywe eliptyczne określone nad ciałami kwadratowymi urojonymi.

Darmon badał w [23] związki między istnieniem rozwiązań uogólnionego równania $x^p + y^q = z^r$ oraz pewnymi hipotezami dotyczącymi reprezentacji Galois stowarzyszonych z różnicami Hilberta-Blumenthala nad dowolnym ciałem liczbowym.

Bugeaud, Mignotte i Siksek [13], [14] stosując „techniki modularne” połączone z teorią Bakera szacowania form liniowych od logarytmów liczb algebraicznych, (1) udowodnili, że jedynymi potęgami pierwszymi w ciągu Fibonacciego (odpowiednio Lucasa) są 0, 1, 8 i 144 (odpowiednio 1 i 4); (2) wyznaczyli wszystkie rozwiązania równania Lebesgue-Nagella $x^2 + D = y^n$ względem zmiennych całkowitych x, y oraz naturalnego $n \geq 3$ w przedziale $1 \leq D \leq 100$.

18.2. Zastosowanie do krzywych eliptycznych. Niech E będzie krzywą eliptyczną określoną nad \mathbb{Q} . Dla rozszerzenia K ciała \mathbb{Q} zbiór $E(K)$ jest grupą abelową z naturalnym działaniem dodawania punktów i wyróżnionym punktem ∞ . Kluczowym rezultatem arytmetycznej teorii krzywych eliptycznych jest następujący rezultat Mordella-Weila: *$E(K)$ jest skończenie generowana dla dowolnego skończonego rozszerzenia K ciała \mathbb{Q} .*

Położmy: $r_g(E) := \text{rank } E(\mathbb{Q})$, $r_a(E) := \text{ord}_{s=1} L(E, s)$ (w ogólnym przypadku istnienie $r_a(E)$ wynika z modularności krzywej eliptycznej). Hipoteza Bircha i Swinnertona-Dyera (słaba wersja) głosi, że $r_g(E) = r_a(E)$. Kolyvagin [68], oraz Gross i Zagier [49] udowodnili następujące ogólne rezultaty, potwierdzające hipotezę: $r_a(E) = 0 \Rightarrow r_g(E) = 0$, $r_a(E) = 1 \Rightarrow r_g(E) = 1$. Proste wprowadzenie do tej problematyki znajduje się w artykule Browkina [12].

Istnienie parametryzacji modularnej pozwala konstruować punkty na E o współrzędnych w abelowych rozszerzeniach pewnych ciał kwadratowych urojonych, co odegrało ważną rolę we wspomnianych pracach Kolyvagina oraz Grossa i Zagiera. Ważną konsekwencją pracy [49] jest następujący rezultat: wszystkie wyróżniki $d < 0$, dla których ciało kwadratowe $\mathbb{Q}(\sqrt{d})$ ma daną liczbę klas ideałów, daje się efektywnie wyznaczyć (rozwiązanie problemu Gaussa).

19. Warianty i uogólnienia

19.1. Hipoteza Fontaine–Mazura. Mówimy, że reprezentacja p -adyczna $\rho : G_{\mathbb{Q}} \rightarrow GL_n(\overline{\mathbb{Q}}_p)$ jest *geometryczna*, jeśli jest nierozgałęziona poza skończonym zbiorem liczb pierwszych oraz jest potencjalnie semistabilna (por. 4.1). Reprezentacja *pochodzi z geometrii algebraicznej*, jeśli jest podkreśnieniem à la Tate działania $G_{\mathbb{Q}}$ na kohomologiach etalnych pewnej gładkiej i rzutowej rozmaitości algebraicznej określonej nad \mathbb{Q} . Fontaine i Mazur [44] sformułowali przypuszczenie, że ρ jest geometryczna wtedy i tylko wtedy, gdy pochodzi z geometrii algebraicznej. W szczególności dostajemy (hipotetyczny) warunek konieczny i dostateczny na to, aby reprezentacja nieprzywiedlna $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\overline{\mathbb{Q}}_p)$ była reprezentacją stowarzyszoną z nową formą wagi $k + 1$ (czysty motyw (nad \mathbb{Q}) rangi 2 i typu Hodge’a $\{(0, k), (k, 0)\}$ „pochodzi” od nowej formy wagi $k + 1$). Zatem hipoteza Fontaine–Mazura implikuje hipotezę Shimury–Taniyamy–Weila.

Oczywiście dowód hipotezy Shimury–Taniyamy–Weila ([131], [123], [33], [34], [19], [10]) stanowi znaczące potwierdzenie hipotezy Fontaine–Mazura. Dalszy postęp uzyskano w serii prac Skinnera i Wilesa [119], [120], Taylora [122], Kisina [66] i Savitta [102]. Implikacja „ \Leftarrow ” hipotezy Fontaine–Mazura została udowodniona przez Tsuji [124] w 1999 roku.

19.2. Modularność rozmaitości Calabi–Yau. Gładka rzutowa rozmaitość d -wymiarowa X jest *Calabi–Yau*, jeśli (i) $H^i(X, \mathcal{O}_X) = 0$ dla $0 \leq i \leq d$ oraz (ii) K_X jest trywialna. Na przykład, jednowymiarowe rozmaitości Calabi–Yau to krzywe eliptyczne, dwuwymiarowe rozmaitości Calabi–Yau to K3-powierzchnie. (Rigid) trójwymiarowa rozmaitość Calabi–Yau X określona nad \mathbb{Q} jest *modularna*, jeśli $L(X, s) = L(f, s)$ dla pewnej formy parabolicznej f wagi 4. Oczekuje się, że dowolna 3-wymiarowa rozmaitość Calabi–Yau określona nad \mathbb{Q} jest modularna (w przypadku non-rigid hipotezę o modularności należy sformułować w terminach podmotywu rangi 2 w $H_{\text{ét}}^3(X, \mathbb{Q}_l)$). Przegląd ostatnich rezultatów dotyczących tego zagadnienia zawiera artykuł [60].

19.3. Ribet: GL_2 -rozmaitości abelowe. Nazwiemy rozmaitość abelową określoną nad \mathbb{Q} *modularną*, jeśli jest ona izogeniczna z rozmaitością abelową postaci A_f dla pewnej nowej formy f względem $\Gamma_1(N)$. Nie oczekuje się, że każda rozmaitość abelowa określona nad \mathbb{Q} jest modularna, gdyż rozmaitości postaci A_f są bardzo specjalne, np. posiadają „dużo” endomorfizmów. Ribet [98] proponuje następującą definicję: g -wymiarowa rozmaitość abelowa A nad \mathbb{Q} jest *typu GL_2* , jeśli $\text{End}_{\mathbb{Q}}(A)$ zawiera podpierścień będący \mathbb{Z} -kratą ciała liczbowego stopnia g . Wówczas mamy następujące uogólnienie hipotezy Shimury–Taniyamy–Weila: dowolna prosta rozmaitość abelowa typu GL_2 , określona nad \mathbb{Q} jest modularna. Ribet pokazał, że ten wariant hipotezy Shimury–Taniyamy–Weila również wynika z hipotezy Serre’a.

19.4. *Langlands: dowolna motywiczna L -funkcja jest automorficzną L -funkcją.* Niech F będzie ciałem globalnym, tj. ciałem liczbowym lub ciałem funkcji wymiernych na krzywej algebraicznej określonej nad ciałem skończonym. Langlands [77] sformułował przypuszczenie, że istnieje wzajemnie jednoznaczna odpowiedniość między n -wymiarowymi reprezentacjami grupy G_F oraz nieprzywiedlnymi automorficznymi reprezentacjami grupy $GL_n(\mathbb{A}_F)$ w przestrzeni funkcji na $GL_n(F) \backslash GL_n(\mathbb{A}_F)$. Przy tym, nieprzywiedlne n -wymiarowe reprezentacje grupy G_F powinny odpowiadać parabolicznym reprezentacjom grupy $GL_n(\mathbb{A}_F)$.

Przypadek $n = 1$ jest klasyczny: redukuje się do abelowej teorii ciał klas. Dowód hipotezy Shimury-Taniyamy-Weila jest potwierdzeniem przypuszczenia Langlandsa dla $F = \mathbb{Q}$, $n = 2$.

Przypuszczenie Langlandsa dla przypadku funkcyjnego zostało udowodnione przez Drinfelda ([36], $n = 2$) i Lafforgue'a ([72], n dowolne). Autorzy tego wyniku zostali uhonorowani medalami Fieldsa (Drinfeld w 1990 r. oraz Lafforgue w 2002 r.). Artykuł Langerera [76] zawiera proste wprowadzenie do rezultatów Lafforgue'a.

Rozważmy teraz tzw. geometryczny wariant odpowiedniości Langlandsa. Punktem wyjścia jest obserwacja, że jeśli F jest ciałem funkcji wymiernych na krzywej algebraicznej X , to n -wymiarowe reprezentacje grupy G_F można rozważać jako systemy lokalne rangi n na X (takie systemy lokalne również istnieją, gdy X jest krzywą określoną nad \mathbb{C}). Geometryczny wariant odpowiedniości Langlandsa dotyczy bijekcji między systemami lokalnymi rangi n na X oraz pewnymi snopami (tzw. eigensheaves) na przestrzeni moduli wiązek rangi n na X . Taka odpowiedniość została niedawno opisana przez Frenkela, Gaitsgory'ego i Vilonena [45].

Można uogólnić odpowiedniość Langlandsa, zastępując GL_n przez dowolną grupę reduktywną. Odpowiedniość taka została opisana przez Beilinsona i Drinfelda [5] w przypadku dowolnej zespolonej półprostej grupy Liego.

Można sformułować lokalną wersję odpowiedniości Langlandsa (tj. nad ciałem lokalnym). Odpowiedniość taka została opisana w przypadku GL_n przez Laumon, Rapoport i Stuhlera [78] (w przypadku funkcyjnym) oraz przez Harrisa i Taylora [52] oraz Henniarta [56] w przypadku rozszerzenia ciała \mathbb{Q}_p .

19.5. *Hipoteza Sato-Tate'a.* Niech E będzie krzywą eliptyczną określoną nad \mathbb{Q} . Elkies udowodnił w 1986 roku, że $a_p := p + 1 - \#\overline{E}_p(\mathbb{F}_p)$ jest równe zero dla nieskończenie wielu liczb pierwszych p . Dla krzywych eliptycznych z mnożeniem zespolonym Deuring udowodnił o wiele mocniejszy rezultat: $a_p = 0$ dla „połowy” liczb pierwszych (taki rezultat nie może mieć jednak miejsca dla krzywych eliptycznych bez mnożenia zespolonego).

Skoro $|a_p| < 2\sqrt{p}$ (nierówność Hassego), więc możemy zapisać $a_p = 2\sqrt{p} \cos(\Theta_p)$. Załóżmy, że E nie posiada mnożenia zespolonego. Sato i Tate (niezależnie) na początku lat sześćdziesiątych ubiegłego stulecia wysunęli przypuszczenie, że ciąg $(\Theta_p)_p$ jest równomiernie rozmieszczony na przedziale $[0, \pi]$ względem miary $\frac{2}{\pi} \sin^2 \Theta d\Theta$.

Taylor [121] udowodnił hipotezę Sato-Tate'a dla krzywych eliptycznych posiadających moltiplikatywną redukcję przynajmniej dla jednej liczby pierwszej. Dowód opiera się na wcześniejszych jego wynikach uzyskanych wspólnie z innymi matematykami (L. Clozel, M. Harris, N. Shepherd-Barrow). Taylor dowodzi w istocie, że wszystkie L -funkcje $L(\text{Sym}^m E, s)$ posiadają przedłużenie do funkcji meromorficznej na całej płaszczyźnie zespolonej, spełniają odpowiednie równanie funkcyjne oraz nie znikają w półpłaszczyźnie $\text{Re}(s) \geq 1 + \frac{m}{2}$. Stąd hipoteza wynika prawie natychmiast ([105], rozdz. 1).

Wariant funkcyjny hipotezy Sato-Tate'a został udowodniony przez Deligne'a [29].

Literatura

- [1] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley 1969.
- [2] A. O. L. Atkin, J. Lehner, *Hecke operators on $\Gamma_0(N)$* , Math. Ann. **185** (1970), 134–160.
- [3] S. Balcerzyk, *Wstęp do Algebry Homologicznej*, Biblioteka Matematyczna **34**, PWN Warszawa 1972.
- [4] S. Balcerzyk, T. Józefiak, *Pierścienie Przemienne*, Biblioteka Matematyczna **58**, PWN Warszawa 1985.
- [5] A. Beilinson, V. Drinfeld, *Quantization of Hitchin's integrable system and Hecke eigensheaves*, preprint 2004.
- [6] G. V. Belyi, *On Galois extensions of a maximal cyclotomic field*, Math. USSR Izv. **14** (1980), 247–256; Izv. AN SSSR, ser. Mat. **43** (1979), 267–276.
- [7] M. A. Bennett, C. Skinner, *Ternary diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), 23–54.
- [8] Z. I. Borevich, I. R. Shafarevich, *Number Theory*, Moscow 1985 (ros.).
- [9] J.-F. Boutot, H. Carayol, *Uniformisation p -adique des courbes de Shimura: les théorèmes de Cerednik et Drinfeld*, Astérisque **196-197** (2001), 45–158.
- [10] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over \mathbb{Q} : wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.
- [11] J. Browkin, *Teoria Ciał*. Biblioteka Matematyczna **49**, PWN Warszawa 1977.
- [12] J. Browkin, *Siódmy problem milenijny: Hipoteza Bircha i Swinnertona-Dyera*, Wiadomości Matematyczne **39** (2003), 1–25.
- [13] Y. Bugeaud, M. Mignotte, S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Ann. Math. **163** (2006), 969–1018.
- [14] Y. Bugeaud, M. Mignotte, S. Siksek, *Classical and modular approaches to exponential Diophantine equations II. The Lebesgue-Nagell equation*, Compos. Math. **142** (2006), 31–62.

- [15] *Algebraic Number Theory* (J. W. S. Cassels, A. Fröhlich, eds). Academic Press 1967.
- [16] *Elliptic Curves, Modular Forms, and Fermat's Last Theorem* (J. Coates and al., eds.), Intern. Press, Cambridge 1995.
- [17] I. Connell, *Computing root numbers of elliptic curves over \mathbb{Q}* Manusc. Math. **82** (1994), 93–104.
- [18] B. Conrad, *Ramified deformation problems*, Duke Math. J. **97** (1999), 439–514.
- [19] B. Conrad, F. Diamond, R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), 521–567.
- [20] *Modular Forms and Fermat's Last Theorem* (G. Cornell, J. H. Silverman and G. Stevens, eds.), Springer 1997.
- [21] J. Cremona, *Algorithms for Modular Elliptic Curves*. Cambridge Univ. Press, Cambridge 1997.
- [22] A. Dąbrowski, *On the integers represented by $x^4 - y^4$* , Bull. Austral. Math. Soc. **76** (2007), 133–136.
- [23] H. Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's last theorem*, Duke Math. J. **102** (2000), 413–449.
- [24] H. Darmon, *The Shimura-Taniyama conjecture (d'après Wiles)*, Russian Math. Surveys **50** (1995), 503–548.
- [25] H. Darmon, A. Granville, *On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$* , Bull. London Math. Soc. **27** (1995), 513–543.
- [26] H. Darmon, L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. reine angew. Math. **490** (1997), 81–100.
- [27] H. Darmon, F. Diamond, R. Taylor, *Fermat's Last Theorem*. In: Current Developments in Mathematics, International Press 1995.
- [28] P. Deligne, *Formes modulaires et représentations l -adiques*, Sémin. Bourbaki No. 355, Lecture Notes in Math. **179**, Springer-Verlag 1971, 139–172.
- [29] P. Deligne, *La conjecture de Weil II*, Publ. Math. IHES **52** (1980), 137–252.
- [30] P. Deligne, M. Rapoport, *Les schémas de modules de courbes elliptiques*. In: Modular Functions of One Variable II, Lecture Notes in Math. **349**, Springer-Verlag 1973, 143–316.
- [31] P. Deligne, J.-P. Serre, *Formes modulaires de poids 1*, Ann. Sci. Ec. Norm. Sup. **7** (1974), 507–530.
- [32] M. Deuring, *Die Zetafunktion einer algebraischen Kurve vom Geschlecht Eins, I, II, III, IV*, Nachr. Akad. Wiss. Göttingen (1953), 85–94; (1955), 13–42; (1956), 37–76; (1957), 55–80.
- [33] F. Diamond, *On deformation rings and Hecke rings*, Ann. Math. **144** (1996), 137–166.
- [34] F. Diamond, *An extension of Wiles' results*. In: *Modular Forms and Fermat's Last Theorem* (eds. G. Cornell et al.), Springer-Verlag 1997, 475–489.
- [35] F. Diamond, J. Shurman, *A First Course in Modular Forms*. Graduate Texts in Math. **228**, Springer 2005.
- [36] V. G. Drinfeld, *Moduli varieties of F -sheaves*, Funct. Anal. Appl. **21** (1987), 107–122.
- [37] B. Edixhoven, *Rational elliptic curves are modular [after Breuil, Conrad, Diamond and Taylor]*, Sémin. Bourbaki, exp. **871** (1999–2000).
- [38] H. Edwards, *Fermat's Last Theorem, a Genetic Introduction to Algebraic Number Theory*. Graduate Texts in Math. **64**, Springer 1977.
- [39] J. Ellenberg, *Galois representations attached to \mathbb{Q} -curves and the generalized Fermat equation $A^4 + B^2 = C^p$* , Amer. J. Math. **126** (2004), 763–787.

- [40] J. Ellenberg, *Serre's conjecture over \mathbb{F}_9* , Ann. Math. **161** (2005), 1111–1142.
- [41] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366; Erratum: **75** (1984), 381.
- [42] G. Faltings, *The proof of Fermat's Last Theorem by R. Taylor and A. Wiles*, Notices of the Amer. Math. Soc. **42** (1995), 743–746.
- [43] M. Flach, *A finiteness theorem for the symmetric square of an elliptic curve*, Invent. Math. **109** (1992), 307–327.
- [44] J.-M. Fontaine, B. Mazur, *Geometric Galois representations*. In: *Elliptic Curves, Modular Forms, and Fermat's Last Theorem* (eds. J. Coates et al.), Intern. Press, Cambridge 1995, 41–78.
- [45] E. Frenkel, D. Gaitsgory, K. Vilonen, *On the geometric Langlands conjecture*, J. Amer. Math. Soc. **15** (2002), 367–417.
- [46] G. Frey, *Links between stable elliptic curves and certain diophantine equations*, Ann. Univ. Saraviensis, Ser. Math. **1** (1986), 1–40.
- [47] K. Fujiwara, *Deformation rings and Hecke algebras in totally real case*, preprint 1999.
- [48] F. Gouvea, *A marvelous proof*, Amer. Math. Monthly **101** (1994), 203–222.
- [49] B. H. Gross, D. B. Zagier, *Heegner points and derivatives of L -series*, Invent. Math. **84** (1986), 225–320.
- [50] E. Halberstadt, *Signes locaux des courbes elliptiques en 2 et 3*, C. R. Acad. Sci. Paris **326** (1998), 1047–1052.
- [51] E. Halberstadt, A. Kraus, *Courbes de Fermat: résultats et problèmes*, J. reine ang. Math. **548** (2002), 167–234.
- [52] M. Harris, R. Taylor, *The geometry and cohomology of some simple Shimura varieties*. Ann. Math. Studies **151**, Princeton Univ. Press 2001.
- [53] R. Hartshorne, *Algebraic Geometry*. Graduate Texts in Math. **52**, Springer 1977.
- [54] E. Hecke, *Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung*, Math. Ann. **112** (1936), 664–699.
- [55] Y. Hellegouarch, *Invitation aux Mathématiques de Fermat-Wiles*. Masson, Paris 1997.
- [56] G. Henniart, *Une preuve simple des conjectures de Langlands pour $GL(n)$ sur un corps p -adique*, Invent. Math. **139** (2000), 439–455.
- [57] H. Hida, *Modular Forms and Galois Cohomology*. Cambridge Studies in Adv. Math., Cambridge Univ. Press 2000.
- [58] H. Hida, *Hilbert Modular Forms and Iwasawa Theory*. Oxford Univ. Press 2006.
- [59] T. Honda, I. Miyawaki, *Zeta-functions of elliptic curves of 2-power conductors*, J. Math. Soc. Japan **26** (1974), 362–373.
- [60] K. Hulek, R. Kloosterman, M. Schütt, *Modularity of Calabi-Yau varieties*, arXiv:math.AG/0601238 v2, 31 Jan 2006.
- [61] J. Igusa, *Kroneckerian model of fields of elliptic modular functions*, Amer. J. Math. **81** (1959), 561–577.
- [62] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*. Graduate Texts in Math. **84**, Springer 1982.
- [63] N. Katz, B. Mazur, *Arithmetic Moduli of Elliptic Curves*. Annals of Math. Studies **108**, Princeton Univ. Press, Princeton 1985.
- [64] C. Khare, *On isomorphisms between deformation rings and Hecke rings*, Invent. Math. **154** (2003), 199–222.
- [65] C. Khare, *Modularity of p -adic Galois representations via p -adic approximations*, J. Théorie des Nombres de Bordeaux **16** (2004), 179–185.

- [66] M. Kisin, *Overconvergent modular forms and the Fontaine-Mazur conjecture*, Invent. Math. **153** (2003), 373–454.
- [67] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*. Graduate Texts in Math. **97**, Springer-Verlag 1984.
- [68] V. A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $\text{III}(E/\mathbb{Q})$ for a subclass of Weil curves* (Russian) Izv. Akad. Nauk Ser. Mat. **52** (1988), 1154–1180.
- [69] V. A. Kolyvagin, *Euler systems*. In: The Grothendieck Festschrift, vol. II (P. Cartier et al., eds.), Birkhäuser, Boston 1990, 435–483.
- [70] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Can. J. Math. **49** (1997), 1139–1161.
- [71] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser 1985.
- [72] L. Lafforgue, *Chtoucas de Drinfeld et correspondance de Langlands*, Invent. Math. **147** (2002), 1–241.
- [73] S. Lang, *Some history of the Shimura-Taniyama conjecture*, Notices Amer. Math. Soc. **42** (1995), 1301–1307.
- [74] S. Lang, *Algebra*. PWN, Warszawa 1983 (przekład z j. ang.).
- [75] A. Langer, *Program Langlandsa według Lafforgue'a*, Wiadomości Matematyczne **39** (2003), 39–46.
- [76] R. P. Langlands, *Base Change for $GL(2)$* . Annals of Math. Studies **96**, Princeton Univ. Press, Princeton 1980.
- [77] R. P. Langlands, *Problems in the theory of automorphic forms*. In: Lecture Notes in Math. **170** (1970), 18–61.
- [78] G. Laumon, M. Rapoport, U. Stuhler, *D-elliptic sheaves and the Langlands correspondence*, Invent. Math. **113** (1993), 217–338.
- [79] H. W. Lenstra, *Complete intersections and Gorenstein rings*. In: *Elliptic Curves, Modular Forms, and Fermat's Last Theorem* (eds. J. Coates et al.), Intern. Press, Cambridge 1995, 99–109.
- [80] M. Ligozat, *Courbes modulaires de genre 1*, Bull. Soc. Math. France, Suppl., Mém. **43** (1975), 80 stron.
- [81] J. Manoharmayum, *On the modularity of certain $GL_2(\mathbb{F}_7)$ Galois representations*, Math. Res. Letters **8** (2001), 703–712.
- [82] Y. Martin, K. Ono, *Eta-quotients and elliptic curves*, Proc. AMS **125** (1997), 3169–3176.
- [83] B. Mazur, *An introduction to the deformation theory of Galois representations*. In: *Modular Forms and Fermat's Last Theorem* (eds. G. Cornell et al.), Springer-Verlag 1997, 243–311.
- [84] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1977), 33–186.
- [85] B. Mazur, *Perturbations, deformations, and variations (and „nearl-misses”) in geometry, physics, and number theory*, Bull. Amer. Math. Soc. **41** (2004), 307–336.
- [86] L. Merel, *Arithmetic of elliptic curves and diophantine equations*, J. Théorie des Nombres de Bordeaux **11** (1999), 173–200.
- [87] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. reine angew. Math. **572** (2004), 167–195.
- [88] W. Narkiewicz, *Wielkie Twierdzenie Fermata*, Wiad. Mat. **30** (1993), 1–16.
- [89] W. Narkiewicz, *Teoria Liczb*. Biblioteka Matematyczna **50**, PWN Warszawa 1977.
- [90] A. Nitaj, *The abc conjecture homepage*, <http://www.math.unicaen.fr/~nitaj/abc.html>.

- [91] J. Oesterlé, *Nouvelles approches du théorème de Fermat*, Sémin. Bourbaki, exp. 694, Astérisque **161-162** (1988), 165–186.
- [92] J. Oesterlé, *Travaux de Wiles (et Taylor,...)*, Partie II. Sémin. Bourbaki, exp. 804, Astérisque **237** (1996), 333–355.
- [93] A. P. Ogg, *Abelian curves of 2-power conductor*, Proc. Camb. Phil. Soc. **62** (1966), 143–148.
- [94] R. Ramakrishna, *On a variation of Mazur's deformation functor*, Compos. Math. **87** (1993), 269–286.
- [95] M. Reid, *Undergraduate Algebraic Geometry*. London Math. Student Texts **12**, Cambridge Univ. Press 1988.
- [96] P. Ribenboim, *Wielkie Twierdzenie Fermata dla Laików*, WNT, Warszawa 2001 (przekład z j. ang.).
- [97] K. Ribet, *On modular representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms*, Invent. Math. **100** (1990), 431–476.
- [98] K. Ribet, *Abelian varieties over \mathbb{Q} and modular forms*. In: *Modular curves and abelian varieties*, Progress in Math. **224**, Birkhäuser 2004, 241–261.
- [99] K. Rubin, *Modularity of mod 5 representations*. In: *Modular Forms and Fermat's Last Theorem* (eds. G. Cornell et al.), Springer-Verlag 1997, 463–474.
- [100] K. Rubin, A. Silverberg, *Families of elliptic curves with constant mod p representations*. In: *Elliptic Curves, Modular Forms, and Fermat's Last Theorem* (eds. J. Coates et al.), Intern. Press, Cambridge 1995, 148–161.
- [101] K. Rubin, A. Silverberg, *A report on Wiles' Cambridge lectures*, Bull. Amer. Math. Soc. **31** (1994), 15–38.
- [102] D. Savitt, *Modularity of some potentially Barsotti-Tate Galois representations*, Compos. Math. **140** (2004), 31–63.
- [103] J.-P. Serre, *Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* , Duke Math. J. **54** (1987), 179–230.
- [104] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.
- [105] J.-P. Serre, *Abelian l -adic Representations and Elliptic Curves*. New York-Amsterdam 1968.
- [106] J.-P. Serre, *Travaux de Wiles (et Taylor,...)*, Partie I. Sémin. Bourbaki, exp. 803, Astérisque **237** (1996), 319–332.
- [107] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*. Aspects of Math. **15**, Braunschweig 1989.
- [108] J.-P. Serre, J. Tate, *Good reduction of abelian varieties*, Ann. Math. **88** (1968), 492–517.
- [109] I. R. Shafarevich, *Basic Algebraic Geometry*, Moscow 1988 (ros.).
- [110] I. R. Shafarevich, *Algebraic number fields*. In: Proc. Intern. Congr. Math., Stockholm 1962, 163–176.
- [111] N. I. Shepherd-Barron, R. Taylor, *Mod 2 and mod 5 icosahedral representations*, J. Amer. Math. Soc. **10** (1997), 283–298.
- [112] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*. Iwanami Shoten and Princeton Univ. Press, Princeton 1971.
- [113] G. Shimura, *On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields*, Nagoya Math. J. **43** (1971), 199–208.
- [114] G. Shimura, *Yutaka Taniyama and his time. Very personal recollections*, Bull. London Math. Soc. **21** (1989), 186–196.

- [115] A. Silverberg, *Explicit families of elliptic curves with prescribed mod N representations*. In: *Modular Forms and Fermat's Last Theorem* (eds. G. Cornell et al.), Springer-Verlag 1997, 447–461.
- [116] J. Silverman, *The Arithmetic of Elliptic Curves*. Graduate Texts in Math. **106**, Springer-Verlag 1985.
- [117] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Math. **151**, Springer-Verlag 1994.
- [118] S. Singh, *Tajemnica Fermata*, Prószyński i S-ka 1999 (przekład z j. ang.).
- [119] C. Skinner, A. Wiles, *Residually reducible representations and modular forms*, Publ. Math. IHES **89** (1999), 5–126.
- [120] C. Skinner, A. Wiles, *Nearly ordinary deformations of irreducible residual representations*, Ann. Fac. Sci. Toulouse Math. **10** (2001), 185–215.
- [121] R. Taylor, *Automorphy for some l -adic lifts of automorphic mod l representations II*, preprint 2006.
- [122] R. Taylor, *Remarks on a conjecture of Fontaine and Mazur*, J. Inst. Math. Jussieu **1** (2002), 1–19.
- [123] R. Taylor, A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Ann. Math. **141** (1995), 553–572.
- [124] T. Tsuji, *p -adic étale cohomology and crystalline cohomology in the semi-stable reduction case*, Invent. Math. **137** (1999), 233–411.
- [125] J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. A.M.S. **5** (1981), 173–175.
- [126] A. J. van der Poorten, *Notes on Fermat's Last Theorem*. Canadian Math. Soc. Series of Monographs and Adv. Texts, A Wiley-Interscience Publication 1996.
- [127] P. Vojta, *Diophantine Approximation and Value Distribution Theory*. Lect. Notes in Math. **476**, Springer 1987.
- [128] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. **83**, Springer 1997.
- [129] A. Weil, *Über die Bestimmung Dirichletscher Reichen durch Funktionalgleichungen*, Math. Ann. **168** (1967), 165–172.
- [130] W. Więsław, *Matematyka i Jej Historia*. Opole 1997.
- [131] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. **141** (1995), 443–551.
- [132] J.-P. Wintenberger, *La conjecture de modularité de Serre: le cas de conducteur 1 [d'après C. Khare]*, Sémin. Bourbaki, exp. **956** (2005–2006).

Dodane w korekcie

Khare i Wintenberger podali w pierwszej połowie 2007 roku dowód hipotezy Serre'a w pełnej ogólności. W drugiej połowie lipca odbyła się w Luminy specjalna konferencja „Summer School on Serre's Modularity Conjecture” poświęcona omówieniu szczegółów dowodu. W jednym z następnych tomów Wiadomości Matematycznych ukaze się artykuł na ten temat.

Andrzej Dąbrowski

Institut Matematyki Uniwersytetu Szczecińskiego

ul. Wielkopolska 15

70-451 Szczecin

e-mail: dabrowsk@sus.univ.szczecin.pl