ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE XXXIX (2003)

JERZY BROWKIN (Warszawa)

Siódmy problem milenijny: Hipoteza Bircha i Swinnertona-Dyera

Wstęp

1. Dla sformułowania hipotezy Bircha i Swinnertona-Dyera wystarczy kilka zdań. Mówi ona, jak wygląda pierwszy wyraz rozwinięcia na szereg funkcji L krzywej eliptycznej E w otoczeniu punktu $s = 1$.

Mianowicie

$$L_E(s) = A_r(s-1)^r + A_{r+1}(s-1)^{r+1} + \cdots,$$

gdzie r jest rangą grupy $E(\mathbb{Q})$ punktów wymiernych krzywej E, a współczynnik A_r jest różny od zera, a dokładniej, wyraża się wzorem

$$A_r = \Omega \cdot |Ш_E| \cdot R_E \cdot \Big(\prod_p c_p\Big) / |E(\mathbb{Q})_{\mathrm{tors}}|^2, \tag{1}$$

gdzie poszczególne litery mają odpowiednie znaczenia (patrz niżej).

Tak więc hipoteza Bircha i Swinnertona-Dyera składa się z dwóch części:

- Krotność zera funkcji $L_E(s)$ w punkcie $s = 1$ jest równa randze r grupy $E(\mathbb{Q})$.
- Współczynnik A_r wyraża się wzorem (1).

Korzystając ze znanego opisu krotności zera funkcji w danym punkcie za pomocą jej pochodnych w tym punkcie, możemy te warunki sformułować następująco:

- $L_E^{(k)}(1) = 0 \quad$ dla $\quad 0 \leqslant k < r \quad$ oraz $\quad L_E^{(r)}(1) \neq 0.$
- Liczba $\frac{1}{r!} L_E^{(r)}(1)$ jest równa prawej stronie wzoru (1),

gdzie r jest rangą grupy $E(\mathbb{Q})$.

2. Dla zrozumienia sformułowania hipotezy Bircha i Swinnertona-Dyera wystarczy więc wiedzieć, co to jest

Wcześniejsze wersje artykułu zechcieli przejrzeć A. Langer, W. Narkiewicz, D. Simson i A. Weber. Dziękuję im za uwagi i wskazówki, które pomogły ulepszyć tekst.

a) Krzywa eliptyczna E,
b) Funkcja L krzywej eliptycznej E,
c) Grupa $E(\mathbb{Q})$ punktów wymiernych krzywej E. Wtedy $E(\mathbb{Q})_{\text{tors}}$ jest podgrupą złożoną z elementów rzędu skończonego.
d) Grupa Tate'a-Szafarewicza $Ш_E$ krzywej E,
e) Regulator R_E krzywej E,
f) Forma różniczkowa ω na krzywej E. Liczba Ω jest z nią związana,
g) Redukcja krzywej eliptycznej modulo liczba pierwsza p. Prowadzi to do określenia liczb c_p. Przy tym $c_p \neq 1$ tylko gdy redukcja krzywej E modulo p jest zła. Zbiór takich liczb pierwszych p jest skończony.

Ponadto chciałoby się wiedzieć
A) Skąd się wzięła ta hipoteza i dlaczego miałaby być prawdziwa?
B) Co z niej wynika?
C) Dla jakich krzywych eliptycznych dotychczas ją udowodniono?

Samo sformułowanie hipotezy Birch a i Swinnertona-Dyera, jak na to kiedyś zwrócił uwagę Tate, zakłada prawdziwość dwóch innych hipotez:
I. Funkcja $L_E(s)$ jest określona tylko w półpłaszczyźnie $\text{Re}(s) > 3/2$. Dla rozpatrywania jej rozwinięcia w punkcie $s = 1$ należy więc przyjąć, że funkcję tę można przedłużyć analitycznie na pewien obszar zawierający otoczenie punktu 1.
II. Z określenia grupy $Ш_E$ nie widać, dlaczego miałaby ona być skończona. Co więcej, przez wiele lat nie umiano wyznaczyć grupy $Ш_E$ dla *żadnej* krzywej eliptycznej. Natomiast formułując hipotezę Birch a i Swinnerton-Dyera należy przyjąć, że grupa ta jest skończona dla *każdej* krzywej eliptycznej, ponieważ rząd tej grupy występuje we wzorze na współczynnik A_r.

3. Objaśnienie wymienionych wyżej pojęć wymagałoby co najmniej rocznego wykładu monograficznego, nie można tego zrobić w artykule o umiarkowanej objętości. Czytelnik może się więc nie obawiać, że będę pisał szczegółowo o wszystkich wspomnianych wyżej sprawach. Ograniczymy się tylko do zwięzłego omówienia podstawowych tematów licząc na to, że zainteresowani czytelnicy sięgną do odpowiednich monografii i prac oryginalnych podanych w bibliografii przy końcu artykułu i poprzez samodzielne studia poznają dokładniej tę piękną i głęboką teorię. Być może też podejmą samodzielne badania w tej dziedzinie.

4. Problem milenijny. Choć siódmy problem milenijny nosi nazwę „Hipoteza Birch a i Swinnertona-Dyera" i pełne sformułowanie tej hipotezy podaliśmy wyżej, to jednak z omówienia tego problemu w [57] wynika, że nagrodę można otrzymać za udowodnienie (lub obalenie) tylko pierwszej części tej hipotezy: Ranga krzywej eliptycznej E określonej nad $\mathbb{Q}$ jest równa

krotności zera funkcji $L_E(s)$ w punkcie $s = 1$. Można nie dowodzić, że współczynnik A_r wyraża się skomplikowanym wzorem (1), który objaśnimy szczegółowo w tym artykule.

Podstawowe definicje i fakty

Do zrozumienia niniejszego artykułu wystarczą wiadomości z algebry zawarte w podręczniku S. Langa [28]. Natomiast definicje i twierdzenia z teorii krzywych eliptycznych, które będziemy omawiali niżej, są przedstawione dokładniej w monografiach [23], [47], [48] i [49].

Ponieważ w sformułowaniu hipotezy Bircha i Swinnertona-Dyera pojęcie krzywej eliptycznej odgrywa podstawową rolę, więc nie będziemy oszczędzali miejsca, aby je dokładnie wyjaśnić.

5. Krzywe algebraiczne. Ustalamy dowolne ciało k, przez $\overline{k}$ oznaczamy jego algebraiczne domknięcie. Bierzemy skończony zbiór wielomianów n zmiennych o współczynnikach w ciele k :

$$f_1, \ldots, f_r \in k[X_1, \ldots, X_n].$$

Rozpatrujemy zbiór $V = V(f_1, \ldots, f_r)$ zer tego układu wielomianów, o współrzędnych w ciele $\overline{k}$:

$$V := \{(a_1, \ldots, a_n) \in \overline{k}^n : f_i(a_1, \ldots, a_n) = 0 \text{ dla } i = 1, \ldots, r\}.$$

W tej sytuacji V nazywamy zbiorem algebraicznym afinicznym określonym nad ciałem k. Stosując zwykłą procedurę ujednoradniania, tzn. zastępując wielomiany f_i przez odpowiednie wielomiany jednorodne

$$F_i(X_0, X_1, \ldots, X_n) := X_0^{r_i} \cdot f_i(X_1/X_0, \ldots, X_n/X_0),$$

gdzie $r_i = \deg f_i$, otrzymujemy zbiór algebraiczny rzutowy

$$\overline{V} := \{(a_0, a_1, \ldots, a_n) \in \mathbb{P}^n(\overline{k}) : F_i(a_0, a_1, \ldots, a_n) = 0 \text{ dla } i = 1, \ldots, r\}.$$

Ze zbiorem algebraicznym V związany jest ideał $I(V)$ pierścienia wielomianów $k[X_1, \ldots, X_n]$, mianowicie

$$I(V) := \{f \in k[X_1, \ldots, X_n] : f(a_1, \ldots, a_n) = 0 \text{ dla każdego } (a_1, \ldots, a_n) \in V\}.$$

Zbiór algebraiczny V nazywamy rozmaitością, jeżeli jest nierozkładalny, tzn. jeżeli nie jest sumą dwóch zbiorów algebraicznych mniejszych.

Dowodzi się, że V jest rozmaitością wtedy i tylko wtedy, gdy ideał $I(V)$ jest pierwszy. W tym przypadku pierścień ilorazowy $k[V] := k[X_1, \ldots, X_n]/I(V)$ nie ma dzielników zera. Istnieje więc jego ciało ułamków, które oznaczamy przez $k(V)$ i nazywamy ciałem funkcji wymiernych rozmaitości V. Jeżeli dla pewnych rozmaitości V_1 i V_2 ciała $k(V_1)$ i $k(V_2)$ są k-izomorficzne,

to mówimy, że V_1 i V_2 są biwymiernie równoważne nad k, albo, że są k-izomorficzne.

Łatwe ćwiczenie: Niech $\operatorname{char} k \neq 2$. Wtedy rozmaitości opisane w $\overline{k}^2$ za pomocą równań:

$$\begin{array}{lll} V_1 & : & X_2 = 0 \qquad\quad \text{(prosta)}, \\ V_2 & : & X_1^2 + X_2^2 - 1 = 0 \quad \text{(okrąg)} \end{array}$$

są biwymiernie równoważne nad k.

W dalszym ciągu przez *rozmaitość* będziemy rozumieli klasę abstrakcji rozmaitości biwymiernie równoważnych. O rozmaitościach biwymiernie równoważnych V_1 i V_2 opisanych za pomocą układów wielomianów będziemy mówili, że są modelami tej samej *rozmaitości*. Tak więc na przykład prosta i okrąg są modelami tej samej rozmaitości.

Rozmaitość V nazywamy krzywą (algebraiczną), jeżeli wymiar przestępny ciała $k(V)$ nad k jest równy 1.

Załóżmy, że ciało k jest algebraicznie domknięte. Wtedy punkty rzutowe P krzywej V odpowiadają waluacjom dyskretnym $v_P : k(V) \longrightarrow \mathbb{Z} \cup \{\infty\}$ ciała $k(V)$ trywialnym na podciele k. Ciałem reszt każdej takiej waluacji jest k.

Element $a \in k(V)$ można traktować jako funkcję określoną w zbiorze punktów krzywej V o wartościach w ciele k. Mianowicie, jeżeli $v_P(a) \geqslant 0$, to wartością funkcji a w punkcie P jest element ciała reszt waluacji v_P wyznaczony przez a. Jeżeli $v_P(a) < 0$, to funkcja a w punkcie P nie jest określona. Mówimy wtedy, że punkt P jest *biegunem* funkcji a o krotności $-v_P(a)$. Podobnie, jeżeli $v_P(a) > 0$, to mówimy, że punkt P jest *zerem* funkcji a o *krotności* $v_P(a)$.

Dowodzi się, że liczba zer każdej takiej funkcji (z uwzględnieniem krotności) na krzywej rzutowej jest skończona i jest równa liczbie jej biegunów (też z uwzględnieniem krotności).

6. Krzywe eliptyczne. Nadal przyjmujemy założenie, że ciało k jest algebraicznie domknięte. Dla klasyfikacji krzywych algebraicznych wprowadza się pojęcie rodzaju. Krzywe rodzaju 0 to są krzywe biwymiernie równoważne prostej. Tak więc jest tylko jedna krzywa rodzaju 0, która ma wiele modeli.

Krzywe rodzaju 1 nazywamy krzywymi eliptycznymi, oznaczamy je przez E zamiast V i określamy następująco.

Niech krzywa E nie będzie prostą. Ustalamy dowolny punkt $\mathcal{O} \in E$ i żądamy, aby dla każdych punktów $P_1, P_2 \in E$ różnych od $\mathcal{O}$ istniała taka funkcja $a \in k(E)$, która ma zero w punkcie $\mathcal{O}$ i ma dokładnie dwa bieguny, mianowicie w punktach P_1 i P_2. Jeżeli $P_1 = P_2$, to a ma biegun dwukrotny w punkcie P_1.

Krzywe V wyższych rodzajów określa się podobnie żądając, aby w ciele $k(V)$ istniały funkcje spełniające odpowiednie warunki dotyczące ich zer i biegunów.

Funkcja $a \in k(E)$ występująca w definicji krzywej eliptycznej ma dwa bieguny i zero w punkcie $\mathcal{O}$. Ma więc jeszcze jedno zero w pewnym punkcie P. Jeżeli $P = \mathcal{O}$, to a ma zero dwukrotne w $\mathcal{O}$. Dowodzi się, że taki punkt P nie zależy od wyboru funkcji $a \in k(E)$. Nazywamy go sumą punktów P_1 i P_2 i piszemy $P = P_1 + P_2$. Przyjmujemy ponadto, że $P_1 + \mathcal{O} = P_1$ dla każdego $P_1 \in E$.

Tak określone dodawanie punktów wyznacza w zbiorze punktów krzywej eliptycznej E strukturę grupy abelowej. Jej elementem neutralnym jest ustalony na początku punkt $\mathcal{O}$.

Odrzućmy teraz założenie, że ciało k jest algebraicznie domknięte. Niech K będzie ciałem algebraicznie domkniętym zawierającym k. Dla każdego ciała k', gdzie $k \subset k' \subset K$, oznaczmy przez $E(k')$ zbiór punktów rzutowych krzywej E o współrzędnych należących do k'. Nazywamy je punktami k'-wymiernymi krzywej E. Jeżeli krzywa eliptyczna E jest określona nad k i wyróżniony punkt $\mathcal{O}$ ma współrzędne w k, to zdefiniowane wyżej dodawanie punktów określa strukturę grupy abelowej w zbiorze $E(k')$. W szczególności $E(k)$ jest podgrupą grupy $E(K)$.

Dla uproszczenia będziemy mówili, że krzywa eliptyczna $(E, \mathcal{O})$ jest określona nad k, jeżeli krzywa E jest określona nad k, a $\mathcal{O}$ jest pewnym jej punktem o współrzędnych (rzutowych) należących do k. Dowodzi się, że każda krzywa eliptyczna $(E, \mathcal{O})$ określona nad k ma model opisany za pomocą następującego równania

$$(2)\quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \text{ gdzie } a_j \in k.$$

Nazywamy je uogólnionym równaniem Weierstrassa. Ponadto na krzywej (2) nie ma punktów osobliwych. Ten ostatni warunek można zapisać w postaci

$$\Delta = \Delta(a_1, \ldots, a_6) \neq 0,$$

gdzie Δ jest pewnym (dość skomplikowanym – patrz niżej) wielomianem o współczynnikach całkowitych. Nazywamy go wyróżnikiem tego modelu krzywej eliptycznej. Na odwrót, dowolne równanie postaci (2), gdzie $\Delta(a_1, \ldots, a_6) \neq 0$, określa pewną krzywą eliptyczną E. Oczywiście punkt $\mathcal{O} := (0, 1, 0)$ należy do E i ma współrzędne w k.

7. Krzywe eliptyczne określone nad $\mathbb{Q}$. Hipoteza Birch a i Swinnertona-Dyera dotyczy krzywych eliptycznych $(E, \mathcal{O})$ określonych nad ciałem liczb wymiernych $\mathbb{Q}$, choć istnieją też ogólniejsze wersje tej hipotezy. Podamy więc dodatkowe informacje na temat takich krzywych.

Istnieje model krzywej E opisany za pomocą równania (2), w którym wszystkie współczynniki $a_1, \ldots, a_6$ są liczbami całkowitymi. Wtedy również

liczba $\Delta = \Delta(a_1, \ldots, a_6)$ jest całkowita i różna od zera. Wśród tych modeli danej krzywej E istnieje taki, dla którego wartość liczby $|\Delta|$ jest najmniejsza. Jest on wyznaczony (prawie) jednoznacznie. Nazywamy go modelem minimalnym krzywej E, a wyróżnik Δ tego modelu nazywamy wyróżnikiem minimalnym krzywej E i oznaczamy przez Δ_E.

Twierdzenie Mordella-Weila (patrz [45]) mówi, że grupa $E(\mathbb{Q})$ jest skończenie generowana. Z twierdzenia o strukturze grup abelowych skończenie generowanych wynika, że grupa $E(\mathbb{Q})$ ma rozkład na sumę prostą

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus E(\mathbb{Q})_{\text{free}},$$

gdzie $E(\mathbb{Q})_{\text{tors}}$ jest podgrupą elementów rzędu skończonego, a $E(\mathbb{Q})_{\text{free}}$ jest grupą abelową wolną rangi $r \geqslant 0$, to znaczy $E(\mathbb{Q})_{\text{free}} = \mathbb{Z}^r$. Liczbę r nazywamy rangą krzywej E.

Podgrupę $E(\mathbb{Q})_{\text{tors}}$ można łatwo wyznaczyć. Jej rząd nie przekracza 16 (twierdzenie B. Mazura [33], [34]) i znany jest prosty algorytm (twierdzenie E. Lutz [30] i T. Nagella [36]) pozwalający znaleźć wszystkie jej elementy, przynajmniej, gdy mamy model krzywej E w postaci Weierstrassa.

Dużo mniej wiadomo o randze r. Nie wiemy, czy ta liczba może być dowolnie duża. Znane są przykłady krzywych o rangach co najmniej 22, 23 i 24 podane przez S. Fermigiera, oraz R. Martina i W. McMillena (patrz [17] oraz [46], str. 100). Przypuszcza się, że istnieją krzywe eliptyczne określone nad $\mathbb{Q}$ dowolnie dużej rangi. Nie znamy jednak algorytmu dla wyznaczania rangi dowolnej krzywej eliptycznej.

Można więc sformułować następujący problem. Dana jest krzywa eliptyczna $(E, \mathcal{O})$ określona nad $\mathbb{Q}$, i jej model minimalny postaci (2). Chcemy wyznaczyć rangę tej krzywej.

Wystarczyłoby znać wszystkie rozwiązania równania (2) w liczbach wymiernych. Jednak bezpośrednie poszukiwanie takich rozwiązań nie rokuje nadziei na sukces. Współrzędne punktów z $E(\mathbb{Q})$ mają zwykle bardzo duże liczniki i mianowniki, więc przypadkowe natrafienie na taki punkt jest mało prawdopodobne.

W latach pięćdziesiątych XX wieku B. Birch i H. P. F. Swinnerton-Dyer ([2], [3]) wpadli na następujący pomysł. Równanie (2) zastąpili odpowiednią kongruencją modulo liczba pierwsza p i dla wielu liczb pierwszych p znajdowali wszystkie rozwiązania niezerowe takiej kongruencji z dokładnością do proporcjonalności. Niech $N_p = N_p(E)$ będzie liczbą tych rozwiązań.

Można oczekiwać, że jeżeli ranga r krzywej E jest duża, to i liczba rozwiązań N_p też na ogół będzie duża i znajomość liczb N_p pozwoli znaleźć rangę krzywej E.

Licząc na to wyznaczyli oni liczby $N_p(E)$ dla dużej liczby liczb pierwszych p i kilku tysięcy krzywych E. Początkowo wykonywali obliczenia na papierze, a potem skorzystali z pomocy pierwszych komputerów, które w owym

czasie były dostępne (EDSAC2 w Cambridge University). Wyniki tych obliczeń potwierdziły w większości przypadków, że zachodzi związek między wielkością rangi i wielkością liczb N_p. Próby ściślejszego sformułowania tego związku doprowadziły właśnie do hipotezy związanej z ich nazwiskami. W następnych punktach opiszemy to dokładniej.

Podstawowe pojęcia teorii krzywych eliptycznych

8. Redukcja krzywej eliptycznej. Niech $(E, \mathcal{O})$ będzie krzywą eliptyczną określoną nad $\mathbb{Q}$ i niech (2) będzie modelem minimalnym krzywej E. Ustalamy liczbę pierwszą p i zamiast równania (2) rozpatrujemy odpowiednią kongruencję modulo p. Tę kongruencję możemy traktować jako równanie o współczynnikach w ciele p-elementowym $\mathbb{F}_p$. Równanie to wyznacza więc pewien zbiór algebraiczny E_p określony nad ciałem $\mathbb{F}_p$. Nazywamy go redukcją krzywej E modulo p.

Jeżeli $P = (x, y, z)$ jest punktem rzutowym należącym do $E(\mathbb{Q})$, to możemy przyjąć, że $x, y, z \in \mathbb{Z}$ i $\mathrm{NWD}(x, y, z) = 1$, zastępując w razie potrzeby trójkę liczb wymiernych (x, y, z) przez odpowiednią trójkę liczb całkowitych do niej proporcjonalną.

Oznaczmy przez $\varphi_p : \mathbb{Z} \longrightarrow \mathbb{F}_p$ homomorfizm kanoniczny. Wtedy oczywiście $\varphi(P) := (\varphi_p(x), \varphi_p(y), \varphi_p(z)) \in E_p(\mathbb{F}_p)$. Określiliśmy w ten sposób odwzorowanie $\varphi : E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p)$.

Opiszemy dokładniej zbiór algebraiczny E_p dla różnych liczb pierwszych p.

Jeżeli $p \nmid \Delta_E$, to E_p jest krzywą eliptyczną określoną nad $\mathbb{F}_p$. Zatem $E_p(\mathbb{F}_p)$ jest grupą i odwzorowanie φ jest homomorfizmem grup. W tym przypadku mówimy, że redukcja krzywej E modulo p jest dobra.

Jeżeli $p|\Delta_E$, to zbiór algebraiczny E_p nie jest krzywą eliptyczną. W tym przypadku mówimy, że redukcja krzywej E modulo p jest zła.

Liczby pierwsze p, dla których redukcja krzywej E modulo p jest zła, można sklasyfikować następująco. Jeżeli redukcja krzywej E modulo p jest zła, to na krzywej E_p jest pewien punkt $P \in E_p(\mathbb{F}_p)$ osobliwy. Z postaci równania Weierstrassa wynika, że punkt osobliwy jest tylko jeden i ma on krotność 2.

W zbiorze punktów nieosobliwych

$$E_p^{\mathrm{ns}}(\mathbb{F}_p) := E_p(\mathbb{F}_p) \setminus \{P\}$$

(ns = nonsingular = nieosobliwy) można określić strukturę grupy wykorzystując działanie dodawania punktów w $E(\mathbb{Q})$.

Z elementarnej analizy wynika, że są następujące możliwości:

1. Styczna do krzywej E_p w punkcie P (osobliwym) jest podwójna. Wtedy grupa $E_p^{\mathrm{ns}}(\mathbb{F}_p)$ jest izomorficzna z grupą addytywną ciała $\mathbb{F}_p$. Ma więc p elementów.

2. W punkcie P są dwie styczne do krzywej E_p o równaniach określonych nad $\mathbb{F}_p$. Wtedy grupa $E_p^{\mathrm{ns}}(\mathbb{F}_p)$ jest izomorficzna z grupą multyplikatywną ciała $\mathbb{F}_p$. Ma więc $p-1$ elementów.
3. W punkcie P są dwie styczne do krzywej E_p o równaniach określonych nad rozszerzeniem kwadratowym $\mathbb{F}_{p^2}$ ciała $\mathbb{F}_p$ (lecz nie nad $\mathbb{F}_p$). Wtedy grupa $E_p^{\mathrm{ns}}(\mathbb{F}_p)$ jest izomorficzna z podgrupą $(p+1)$-elementową grupy multyplikatywnej ciała $\mathbb{F}_{p^2}$.

Tak więc są trzy rodzaje złych redukcji: Redukcja addytywna (przypadek 1), redukcja multyplikatywna rozpadająca się (przypadek 2) i redukcja multyplikatywna nierozpadająca się (przypadek 3).

Ponieważ wyróżnik minimalny Δ_E ma tylko skończoną liczbę dzielników pierwszych, więc tylko dla skończonej liczby liczb pierwszych p redukcja krzywej E modulo p jest zła.

Podobnie można określić odwzorowanie redukcji w następującej sytuacji. Niech E będzie krzywą eliptyczną określoną nad $\mathbb{Q}$ o modelu minimalnym (2). Rozpatrzmy grupę $E(\mathbb{Q}_p)$ punktów rzutowych krzywej E o współrzędnych p-adycznych. Zastępując współrzędne danego punktu przez odpowiednie współrzędne proporcjonalne można przyjąć, że te współrzędne należą do pierścienia $\mathbb{Z}_p$ liczb całkowitych p-adycznych i nie wszystkie są podzielne przez p. Wtedy homomorfizm kanoniczny $\varphi : \mathbb{Z}_p \longrightarrow \mathbb{F}_p$ wyznacza odwzorowanie $\varphi : E(\mathbb{Q}_p) \longrightarrow E_p(\mathbb{F}_p)$. Jeżeli $p \nmid \Delta_E$, to φ jest homomorfizmem grup. Natomiast, jeżeli $p|\Delta_E$, tzn. jeżeli redukcja krzywej E modulo p jest zła, to rozpatrzmy zbiór $E^0(\mathbb{Q}_p) := \varphi^{-1}(E_p^{\mathrm{ns}}(\mathbb{F}_p))$. Dowodzi się, że $E^0(\mathbb{Q}_p)$ jest podgrupą skończonego indeksu w grupie $E(\mathbb{Q}_p)$. Jeżeli redukcja krzywej E modulo p jest dobra, to przyjmujemy, że $E^0(\mathbb{Q}_p) = E(\mathbb{Q}_p)$.

Możemy teraz określić tak zwane liczby Tamagawy c_p występujące w sformułowaniu hipotezy Bircha i Swinnertona-Dyera. Mianowicie przyjmujemy

$$c_p = (E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)).$$

Tak więc $c_p = 1$, jeżeli redukcja krzywej E modulo p jest dobra. Zatem $c_p \neq 1$ tylko dla skończonej liczby liczb pierwszych p.

9. Funkcja L krzywej eliptycznej. W geometrii algebraicznej znana jest ogólna konstrukcja, która danemu zbiorowi algebraicznemu $V = V(f_1, \ldots, f_r)$ opisanemu przez układ równań $f_1 = 0, \ldots, f_r = 0$ (gdzie f_i są wielomianami o współczynikach całkowitych) przyporządkowuje funkcję analityczną $\zeta_V(s)$ zwaną funkcją zeta tego zbioru algebraicznego. Wyznacza się mianowicie liczbę rozwiązań $N_{p^n}(V)$ tego układu równań w ciele skończonym $\mathbb{F}_{p^n}$ o p^n elementach, a następnie posługując się liczbami $N_{p^n}(V)$ jako współczynnikami określa się odpowiednią funkcję analityczną. Można oczekiwać, że własności tej funkcji $\zeta_V(s)$ odzwierciedlają pewne własności samego zbioru V.

Pominiemy szczegóły, które można znaleźć w monografiach [23], [47] lub w artykule [22]. Zdarza się, że taka funkcja $\zeta_V(s)$ daje się w naturalny sposób przedstawić jako iloczyn (lub iloraz) pewnych funkcji prostszych, które nazywa się funkcjami L.

Ograniczymy się do podania definicji funkcji L krzywej eliptycznej E określonej nad $\mathbb{Q}$. Pominiemy uzasadnienie, że jest to szczególny przypadek ogólnej konstrukcji.

Mianowicie, dla każdej liczby pierwszej p określamy wielomian $L_p(X)$ następująco, w zależności od tego, jaka jest redukcja krzywej E modulo p.

$$L_p(X) := 1 + (N_p - p - 1)X + \varepsilon_p pX^2,$$

gdzie $N_p = |E_p(\mathbb{F}_p)|$ jest liczbą punktów rzutowych na krzywej E_p zredukowanej modulo p, o współrzędnych należących do $\mathbb{F}_p$, oraz $\varepsilon_p = 1$ lub 0, gdy redukcja krzywej E modulo p jest dobra, odpowiednio, zła.

Następnie przyjmujemy

$$L_E(s) := \prod_p L_p(p^{-s})^{-1},$$

gdzie p przebiega wszystkie liczby pierwsze.

H. Hasse udowodnił, że jeżeli redukcja krzywej E modulo p jest dobra, to liczba N_p spełnia nierówność

$$|N_p - p - 1| < 2\sqrt{p}.$$

Wykorzystując to można udowodnić, że iloczyn określający funkcję $L_E(s)$ jest zbieżny tylko dla $\mathrm{Re}(s) > 3/2$.

10. Grupa Tate'a–Szafarewicza krzywej E. Elementy grupy Tate'a–Szafarewicza danej krzywej eliptycznej E odpowiadają pewnym krzywym eliptycznym związanym z E. Przed podaniem dokładnej definicji musimy omówić szereg pojęć i zjawisk ogólnych związanych z krzywymi eliptycznymi.

10.1. Krzywe eliptyczne izomorficzne nad $\overline{k}$. Dana jest krzywa eliptyczna $(E, \mathcal{O})$ określona nad ciałem k za pomocą równania Weierstrassa (2). Chcemy opisać wszystkie krzywe eliptyczne E' określone nad k i izomorficzne z E nad $\overline{k}$. W tym celu definiujemy tak zwany niezmiennik j krzywej eliptycznej o modelu Weierstrassa (2) za pomocą wzoru

$$j = c_4^3/\Delta(a_1, \ldots, a_6), \qquad \text{gdzie} \quad c_4 = (a_1^2 + 4a_2)^2 - 24(a_1a_3 + 2a_4).$$

Dowodzi się, że ten niezmiennik nie zależy od wyboru modelu Weierstrassa danej krzywej, a ponadto krzywe E i E' są izomorficzne nad $\overline{k}$ wtedy i tylko wtedy, gdy ich niezmienniki j są równe, $j_E = j_{E'}$. Co więcej, dla każdego $a \in k$ istnieje krzywa eliptyczna określona nad k o niezmienniku j równym a.

Tak więc krzywe eliptyczne określone nad ciałem algebraicznie domkniętym $\overline{k}$ są scharakteryzowane przez elementy samego ciała $\overline{k}$.

Sytuacja znacznie się komplikuje, gdy ciało k nie jest algebraicznie domknięte. Z tego, że niezmienniki j krzywych eliptycznych określonych nad k są równe, nie wynika na ogół, że same krzywe są izomorficzne nad k.

10.2. Przestrzenie jednorodne. Dla ustalonej krzywej eliptycznej $(E, \mathcal{O})$ określonej nad k na ogół jest wiele krzywych eliptycznych E' określonych nad k, które są izomorficzne z E nad $\overline{k}$, lecz nie nad k. Ograniczymy się więc do krzywych E' spełniających pewien dodatkowy warunek. W tym celu wprowadzimy następującą definicję.

Powiemy, że krzywa $(E, \mathcal{O})$ działa na krzywej E', jeżeli istnieje przekształcenie regularne

$$\mu : E \times E' \longrightarrow E'$$

określone nad k (to znaczy opisane za pomocą wielomianów o współczynnikach w k), spełniające następujące warunki:

(i) $\mu(\mathcal{O}, P') = P' \qquad$ dla $\quad P' \in E'(\overline{k})$,

(ii) $\mu(P_1, \mu(P_2, P')) = \mu(P_1 + P_2, P') \qquad$ dla $\quad P_1, P_2 \in E(\overline{k})$, $P' \in E'(\overline{k})$,

(iii) Dla każdych P_1', $P_2' \in E'(\overline{k})$ istnieje dokładnie jeden taki punkt $P \in E(\overline{k})$, że $\mu(P, P_1') = P_2'$.

Inaczej mówiąc, grupa $E(\overline{k})$ działa na zbiorze $E'(\overline{k})$ w sposób przechodni i wierny.

Zamiast $\mu(P, P')$ piszemy zwykle $P + P'$, choć znak $+$ nie oznacza tu działania w żadnej grupie.

W tej sytuacji mówimy, że E' jest przestrzenią jednorodną nad krzywą eliptyczną $(E, \mathcal{O})$. Dowodzi się, że każda przestrzeń jednorodna E' jest izomorficzna z E nad $\overline{k}$, lecz nie na odwrót. Zamiast więc rozpatrywać wszystkie krzywe eliptyczne E' określone nad k i izomorficzne z E nad $\overline{k}$, ograniczymy się do przestrzeni jednorodnych nad E.

Wnikliwy czytelnik zapewne zauważył, że definicja przestrzeni jednorodnej nad krzywą eliptyczną E przypomina definicję przestrzeni afinicznej A nad przestrzenią liniową L. Mianowicie przestrzeń liniowa L, która jest grupą, działa w zbiorze punktów przestrzeni afinicznej A za pomocą przesunięć. Działanie to jest przechodnie i wierne, a zbiór A nie ma struktury przestrzeni liniowej. Nie jest bowiem określone dodawanie punktów przestrzeni afinicznej A.

10.3. O kocyklach. Niech grupa G działa na grupie abelowej A. Odwzorowanie $f : G \longrightarrow A$ nazywamy kocyklem jednowymiarowym (albo homomorfizmem skośnym), jeżeli spełnia warunek

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau) \qquad \text{dla} \quad \sigma, \tau \in G.$$

Na przykład, ustalając $a \in A$ możemy określić odwzorowanie $f_a : G \longrightarrow A$ za pomocą wzoru $f_a(\sigma) = \sigma(a) - a$ dla $\sigma \in G$. Łatwo sprawdzić, że f_a jest kocyklem. Taki kocykl nazywamy kobrzegiem.

Zbiór wszystkich kocykli jest grupą ze względu na dodawanie odwzorowań, zbiór wszystkich kobrzegów jest jej podgrupą. Grupę ilorazową nazywamy pierwszą grupą kohomologii i oznaczamy przez

$$H^1(G, A) := \text{kocykle/kobrzegi}.$$

10.4. Grupa Weila–Châteleta krzywej E. Niech $(E, \mathcal{O})$ będzie krzywą eliptyczną określoną nad k i niech krzywa eliptyczna E' określona nad k będzie przestrzenią jednorodną nad $(E, \mathcal{O})$. Wtedy w zbiorze $E'(\overline{k})$ działa grupa $E(\overline{k})$. W zbiorze tym działa również grupa Galois $G_k := \mathrm{Gal}(\overline{k}/k)$, ponieważ krzywa E' jest określona nad k. Korzystając z tych działań zdefiniujemy odwzorowanie

$$f : G_k \longrightarrow E(\overline{k}),$$

jak następuje. Ustalamy punkt $P' \in E'(\overline{k})$ i dla $\sigma \in G_k$ jako $f(\sigma)$ przyjmujemy punkt $P \in E(\overline{k})$ spełniający $P + P' = \sigma(P')$. Jak wiemy z określenia przestrzeni jednorodnej, taki punkt P istnieje i tylko jeden. Sprawdza się, że odwzorowanie f jest kocyklem zależnym od wyboru punktu $P' \in E'(\overline{k})$. Wybierając inny punkt $P'' \in E'(\overline{k})$ otrzymamy kocykl różniący się od f o kobrzeg. W ten sposób krzywa E', która jest przestrzenią jednorodną nad $(E, \mathcal{O})$, wyznacza element grupy kohomologii $H^1(G_k, E(\overline{k}))$ o reprezentancie f.

Dowodzi się, że ta odpowiedniość jest wzajemnie jednoznaczna, to znaczy, elementy tej grupy kohomologii opisują z dokładnością do k-izomorfizmu wszystkie krzywe eliptyczne E' określone nad k, które są przestrzeniami jednorodnymi nad E. Przy tym sama krzywa E odpowiada elementowi zerowemu grupy kohomologii.

W ten sposób w zbiorze przestrzeni jednorodnych nad E mamy określoną strukturę grupy abelowej. Nosi ona nazwę grupy Weila–Châteleta krzywej E, oznaczamy ją przez $\mathrm{WC}(E)$, patrz [11].

10.5. Grupa Tate'a–Szafarewicza krzywej E. Dla krzywej eliptycznej $(E, \mathcal{O})$ określonej nad dowolnym ciałem k grupa $\mathrm{WC}(E)$ jest na ogół bardzo duża. W przypadku pewnych ciał k wyróżnimy w niej odpowiednią mniejszą podgrupę. Mianowicie, jako k bierzemy ciało $\mathbb{Q}$ liczb wymiernych, ogólniej jako k można wziąć dowolne ciało globalne, to znaczy rozszerzenie skończone ciała $\mathbb{Q}$ lub ciała $\mathbb{F}_q(T)$ funkcji wymiernych zmiennej T nad ciałem skończonym $\mathbb{F}_q$ o q elementach.

Mamy więc krzywą eliptyczną E' określoną nad $\mathbb{Q}$, która jest przestrzenią jednorodną nad krzywą eliptyczną $(E, \mathcal{O})$ określoną nad $\mathbb{Q}$. Jeżeli na E' jest punkt o współrzędnych wymiernych, to jest ona izomorficzna z E nad $\mathbb{Q}$ i przestrzeni jednorodnej E' nad E odpowiada element zerowy grupy $\mathrm{WC}(E)$.

Załóżmy więc, że na E' nie ma punktów o współrzędnych wymiernych. Może się jednak zdarzyć, że dla każdej liczby pierwszej p na E' istnieją punkty o współrzędnych p-adycznych, a także punkty o współrzędnych rzeczywistych. Mówimy wtedy, że na krzywej E' lokalnie istnieją punkty wymierne, lecz nie ma na niej punktów wymiernych globalnie. Ciała $\mathbb{Q}_p$ oraz $\mathbb{R}$ są bowiem wszystkimi lokalizacjami ciała globalnego $\mathbb{Q}$, to znaczy uzupełnieniami ciała $\mathbb{Q}$ względem odpowiednich metryk.

Dowodzi się, że elementy grupy $H^1(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}}))$ odpowiadające przestrzeniom jednorodnym nad E, które mają punkty wymierne lokalnie, tworzą podgrupę. Jest to właśnie grupa Tate'a–Szafarewicza $Ш_E$ krzywej eliptycznej E.

10.6. Co wiadomo o grupie $Ш_E$.

- Grupa $Ш_E$ jest abelowa i torsyjna, co znaczy, że każdy jej element ma rząd skończony.
- Dla każdej liczby naturalnej n w grupie $Ш_E$ istnieje tylko skończenie wiele elementów a spełniających $na = 0$.
- Jeżeli grupa $Ш_E$ jest skończona, to jej rząd jest kwadratem.
- Dla odpowiedniej krzywej E, grupa $Ш_E$ zawiera podgrupę skończoną dowolnie dużego rzędu, patrz [4], [9].
- Przypuszcza się, że dla każdej krzywej eliptycznej E określonej nad $\mathbb{Q}$ grupa $Ш_E$ jest skończona.

Dalsze informacje o grupie $Ш_E$ podajemy przy końcu artykułu.

11. Regulator krzywej eliptycznej. Z kolei przejdziemy do definicji regulatora krzywej eliptycznej określonej nad $\mathbb{Q}$. Wymaga to omówienia kilku spraw pomocniczych.

11.1. Objętość kraty. W algebrze liniowej znana jest następująca konstrukcja. Niech Λ będzie kratą, to znaczy, skończenie generowaną grupą abelową wolną, i niech $v_1, \ldots, v_n$ będzie jej bazą. Załóżmy, że na Λ dana jest dodatnio określona forma kwadratowa q o wartościach rzeczywistych. Wtedy odwzorowanie

$$\langle \cdot\,, \cdot \rangle : \Lambda \times \Lambda \longrightarrow \mathbb{R}$$

określone za pomocą wzoru $\langle x, y\rangle = \frac{1}{2}\,(q(x+y) - q(x) - q(y))$ jest formą dwuliniową symetryczną i niezdegenerowaną, to znaczy, że zachodzi implikacja

$$\Big(\bigwedge_{x\in\Lambda} \langle x, y\rangle = 0\Big) \qquad \Longrightarrow \qquad y = 0.$$

Ponadto mamy $\langle x, x\rangle = q(x)$.

Z algebry liniowej wiadomo, że liczba

$$R(\Lambda, q) := \det(\langle v_i, v_j\rangle),$$

zwana objętością tej kraty, albo jej regulatorem, jest różna od zera i nie zależy od wyboru bazy $v_1, \ldots, v_n$.

Niech $(E, \mathcal{O})$ będzie krzywą eliptyczną określoną nad $\mathbb{Q}$. Z twierdzenia Mordella–Weila wynika, że $E(\mathbb{Q})_{\text{free}}$ jest skończenie generowaną grupą abelową wolną (kratą). Chcąc więc zdefiniować regulator krzywej eliptycznej E według powyższego ogólnego schematu musimy określić odpowiednią formę kwadratową na tej kracie.

Do tego celu służy pojęcie wysokości punktu na krzywej eliptycznej, które teraz zdefiniujemy.

11.2. Wysokość punktu krzywej eliptycznej. Niech krzywa eliptyczna $(E, \mathcal{O})$ określona nad $\mathbb{Q}$ ma model Weierstrassa postaci (2). Niech punkt $P = (x, y, z) \in E(\mathbb{Q})$. Jeżeli $z \neq 0$, to zapiszmy liczbę wymierną x/z w postaci skróconej $x/z = m/n$, gdzie $m, n \in \mathbb{Z}$ oraz $(m, n) = 1$.

Zdefiniujemy najpierw tak zwaną naiwną wysokość logarytmiczną h punktu P przyjmując

$$h(P) := \begin{cases} \log(\max(|m|, |n|)), & \text{gdy } z \neq 0, \\ 0, & \text{gdy } z = 0. \end{cases}$$

Oczywiście ta wysokość zależy od wyboru modelu Weierstrassa krzywej E. Tę naiwną wysokość h można tak zmodyfikować, aby otrzymać dodatnio określoną formę kwadratową na grupie $E(\mathbb{Q})_{\text{free}}$ niezależną od wyboru modelu krzywej E.

Dowodzi się mianowicie, że dla każdego $P \in E(\mathbb{Q})$ istnieje następująca granica

$$\widehat{h}(P) := \lim_{n \to \infty} \frac{h(2^n P)}{4^n},$$

gdzie $2^n P = P + \cdots + P$ (2^n razy) jest sumą elementów grupy $E(\mathbb{Q})$. Ponadto wartość funkcji $\widehat{h}$ nie zależy od wyboru modelu krzywej E, to znaczy, jeżeli punkt P' należący do drugiego modelu krzywej E odpowiada punktowi P, to $\widehat{h}(P) = \widehat{h}(P')$. Następnie, $\widehat{h}(P) = 0$ wtedy i tylko wtedy, gdy $P \in E(\mathbb{Q})_{\text{tors}}$. Zatem $\widehat{h}(P) \neq 0$, jeżeli $P \in E(\mathbb{Q})_{\text{free}}$, $P \neq \mathcal{O}$. Wreszcie funkcja $\widehat{h} : E(\mathbb{Q})_{\text{free}} \longrightarrow \mathbb{R}$ jest dodatnio określoną formą kwadratową. Liczbę $\widehat{h}(P)$ nazywamy wysokością Nérona–Tate'a punktu P.

11.3. Regulator krzywej eliptycznej. Wobec powyższego regulator R_E krzywej eliptycznej $(E, \mathcal{O})$ określonej nad $\mathbb{Q}$ definiuje się następująco. Wybieramy bazę $P_1, \ldots, P_r$ grupy abelowej wolnej $E(\mathbb{Q})_{\text{free}}$ i przyjmujemy

$$R_E := \det(\langle P_i, P_j \rangle),$$

gdzie $\langle P, Q \rangle := \frac{1}{2}\left(\widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q)\right)$. Jak wiemy, regulator nie zależy od wyboru modelu krzywej E ani od wyboru bazy grupy $E(\mathbb{Q})_{\text{free}}$.

Z definicji tej wynika, że jeżeli ranga krzywej eliptycznej E jest równa zeru, to jej regulator R_E jest równy 1. Jest to bowiem wyznacznik macierzy kwadratowej o 0 wierszach.

Zauważmy, że poszukując algorytmu dla obliczania regulatora krzywej eliptycznej E musimy znać algorytmy dla znajdowania jej rangi oraz znajdowania bazy grupy $E(\mathbb{Q})_{\text{free}}$. Takich algorytmów dotyczących dowolnych krzywych eliptycznych jednak nie znamy.

12. Forma różniczkowa ω. Niech $(E, \mathcal{O})$ będzie krzywą eliptyczną określoną nad $\mathbb{Q}$ o modelu (2). Wtedy krzywa płaska rzeczywista $E(\mathbb{R}) \subset \mathbb{P}^2(\mathbb{R})$ ma strukturę grupy topologicznej zwartej. Można dowieść, że forma różniczkowa

$$\omega := \frac{\mathrm{d}x}{2y + a_1 x + a_3},$$

gdzie a_1, a_3 są współczynnikami w równaniu Weierstrassa (2), określona na tej grupie jest holomorficzna na $E(\mathbb{C})$ i niezmiennicza. Jest to jedyna taka forma różniczkowa z dokładnością do czynnika stałego.

Przyjmujemy wtedy

$$\Omega := \int_{E(\mathbb{R})} |\omega|.$$

Hipoteza Bircha i Swinnertona-Dyera

13. Wyniki częściowe na temat hipotezy Bircha i Swinnertona-Dyera. Niech E będzie krzywą eliptyczną określoną nad $\mathbb{Q}$. Z prac B. H. Grossa i D. B. Zagiera [21], V. A. Kolyvagina [25], [26] i K. Rubina [40] wynika, że jeżeli funkcja $L_E(s)$ ma w punkcie $s = 1$ zero r-krotne, gdzie $r = 0$ lub 1, to ranga krzywej eliptycznej E jest równa r i grupa $Ш_E$ jest skończona.

Ponadto, jeżeli $r = 0$, to dla pewnej klasy krzywych eliptycznych wzór (1) zachodzi z dokładnością do potęg dwójki.

Jeżeli ciało liczb wymiernych zastąpimy przez rozszerzenie skończone K ciała $\mathbb{F}_q(T)$ funkcji wymiernych zmiennej T nad ciałem q-elementowym $\mathbb{F}_q$, to dla krzywych eliptycznych E określonych nad K możemy sformułować hipotezę analogiczną do hipotezy Bircha i Swinnertona-Dyera.

J. Tate [51] i J. Milne [35] udowodnili tę hipotezę, lecz tylko dla krzywych E o „stałych" współczynnikach, to znaczy należących do $\mathbb{F}_q$. W ogólnym przypadku nie wiadomo nawet, czy grupa $Ш_E$ jest skończona.

J. E. Cremona [13] przeprowadził obszerne obliczenia i wyznaczył wszystkie krzywe eliptyczne określone nad $\mathbb{Q}$ o przewodniku $N \leqslant 20\,000$. Przewodnik $N = N_E$ krzywej eliptycznej E określonej nad $\mathbb{Q}$ to jest pewien dodatni

dzielnik jej wyróżnika minimalnego Δ_E. Nie otrzymał on sprzeczności z hipotezą Birch a i Swinnerton-Dyera. W szczególności wykazał, że dla tych krzywych liczba występująca we wzorze (1) oznaczona przez $|Ш_E|$ zawsze jest kwadratem.

14. Wnioski z hipotezy Birch a i Swinnerton-Dyera. Zakładając prawdziwość hipotezy Birch a i Swinnerton-Dyera dla krzywej eliptycznej $(E, \mathcal{O})$ określonej nad $\mathbb{Q}$ możemy znaleźć jej rangę, a jeżeli ponadto potrafimy wyznaczyć wolne generatory grupy $E(\mathbb{Q})_{\text{free}}$, to będziemy mogli również obliczyć rząd grupy $Ш_E$.

Dokładniej, znając model minimalny (2) krzywej E potrafimy obliczyć numerycznie wartości funkcji $L_E(s)$ i jej pochodnych w punkcie $s = 1$. Korzystając z pierwszej części hipotezy Birch a i Swinnerton-Dyera możemy więc wyznaczyć rangę krzywej E.

Znając wolne generatory grupy $E(\mathbb{Q})_{\text{free}}$ możemy obliczyć regulator R_E krzywej E. Istnieją też algorytmy do obliczania wszystkich pozostałych wielkości występujących we wzorze (1), prócz $|Ш_E|$. Zatem korzystając z tego wzoru możemy wyznaczyć rząd grupy Tate'a–Szafarewicza krzywej E.

Jak wiemy, jeżeli $L_E(1) \neq 0$, to $r = 0$ i $R = 1$. Zatem w tym przypadku łatwiej jest stosować wzór (1).

Bez zakładania hipotezy Birch a i Swinnerton-Dyera o grupie $Ш_E$ niewiele możemy udowodnić. Wprawdzie wyznaczono tę grupę dla pewnej liczby konkretnych krzywych eliptycznych, lecz nawet wskazanie niezerowego elementu tej grupy wymaga na ogół nietrywialnych rozumowań (patrz przykład 2, niżej).

Znajomość rangi krzywej eliptycznej pozwala znaleźć odpowiedź na następujące pytanie pochodzące jeszcze ze starożytności.

Liczbę naturalną n nazywamy kongruentną, jeżeli istnieje trójkąt prostokątny o polu n, którego boki są liczbami wymiernymi. Na przykład liczba 6 jest kongruentna, ponieważ pole trójkąta prostokątnego o bokach 3, 4 i 5 jest równe 6.

Problem polega na znalezieniu algorytmu dla rozstrzygania, czy dana liczba n jest kongruentna, czy nie.

Udowodniono, że liczba n jest kongruentna wtedy i tylko wtedy, gdy ranga krzywej eliptycznej E o równaniu

$$Y^2 = X^3 - n^2 X$$

jest dodatnia. Z hipotezy Birch a i Swinnerton-Dyera wynika więc, że liczba n jest kongruentna wtedy i tylko wtedy, gdy $L_E(1) = 0$. Ten ostatni warunek można zapisać w całkiem elementarnej postaci ([24], [54]).

Uwagi końcowe

15. Hipoteza Shimury i Taniyamy. Od dawna znana była pewna konstrukcja, która dawała przykłady krzywych eliptycznych określonych nad $\mathbb{Q}$.

Są to tak zwane krzywe eliptyczne modularne. Udowodniono wiele własności krzywych eliptycznych modularnych i nie umiano tych wyników przenieść na przypadek wszystkich krzywych eliptycznych określonych nad $\mathbb{Q}$.

W latach pięćdziesiątych XX wieku sformułowano nawet hipotezę, zwaną dziś hipotezą Shimury i Taniyamy, że każda krzywa eliptyczna określona nad $\mathbb{Q}$ jest modularna. Wówczas nie wydawała się ona bardzo prawdopodobną.

Z biegiem czasu uzyskiwano jednak wyniki potwierdzające szczególne przypadki tej hipotezy, a ostatnio została ona udowodniona w pełnej ogólności przez A. Wilesa, R. Taylora, C. Breuila, B. Conrada, i H. Diamonda, patrz [56], [53], [6].

Dostarczyło to nowych narzędzi do badania krzywych eliptycznych określonych nad $\mathbb{Q}$.

Dokładniej, punktem wyjścia są tak zwane formy paraboliczne f wagi 2 dla podgrup $\Gamma_0(N)$ grupy $\mathrm{SL}_2(\mathbb{Z})$. Są to funkcje analityczne określone na górnej półpłaszczyźnie spełniające odpowiednie warunki, a grupa $\Gamma_0(N)$ składa się z takich macierzy $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, że $N \mid c$.

Każdej takiej formie parabolicznej f można przyporządkować krzywą eliptyczną E_f określoną nad $\mathbb{Q}$ i funkcję L_f określoną na całej płaszczyźnie. Dowodzi się, że funkcją L krzywej E_f jest właśnie L_f, a liczba N jest przewodnikiem krzywej E_f.

Krzywe eliptyczne odpowiadające formom parabolicznym f nazywa się krzywymi modularnymi. Tak więc hipoteza Shimury i Taniyamy mówi, że każda krzywa eliptyczna określona nad $\mathbb{Q}$ odpowiada pewnej formie parabolicznej. Forma paraboliczna f pozwala uzyskać dodatkowe informacje o krzywej E_f, które trudno byłoby otrzymać na innej drodze. Przykładem tego jest dowód Wielkiego Twierdzenia Fermata.

16. Dowód Wielkiego Twierdzenia Fermata. Wiadomo, że nie ma krzywych eliptycznych określonych nad $\mathbb{Q}$, które miałyby dobrą redukcję modulo każda liczba pierwsza. Dla każdej krzywej eliptycznej E istnieje więc taka liczba pierwsza p, że redukcja E modulo p jest zła. Jeżeli jednak redukcję multyplikatywną uważać za umiarkowanie złą, a redukcję addytywną za bardzo złą (co można w pewien sposób uzasadnić), to istnieją takie krzywe eliptyczne, których redukcja modulo p nie jest bardzo zła (czyli addytywna) dla żadnej liczby pierwszej p. Są to tak zwane krzywe eliptyczne semistabilne.

W dowodzie Wielkiego Twierdzenia Fermata występują tak zwane krzywe eliptyczne Freya. Mianowicie, jeżeli liczby całkowite a, b, c różne od zera spełniają równanie Fermata

$$a^n + b^n = c^n,$$

to krzywą eliptyczną Freya określamy następująco

$$Y^2 = X(X - a^n)(X + b^n).$$

Dowodzi się, że krzywe Freya są semistabilne. A. Wiles i R. Taylor ([56], [53]) udowodnili, że każda krzywa eliptyczna semistabilna jest modularna i ta własność została wykorzystana w istotny sposób w dowodzie. Mianowicie wcześniej K. Ribet [38] udowodnił, że jeżeli krzywa Frey'a jest modularna, to zachodzi Wielkie Twierdzenie Fermata.

17. Punkty wymierne na krzywych algebraicznych. Można sformułować problem ogólny. Dana jest krzywa algebraiczna E określona nad ciałem liczb wymiernych. Pytamy, czy są na niej punkty o współrzędnych wymiernych i czy jest ich nieskończenie wiele.

Okazuje się, że odpowiedź na to pytanie zależy w dużym stopniu od rodzaju g krzywej E.

Hipoteza Mordella mówiła, że jeżeli $g \geqslant 2$, to na krzywej E jest tylko skończenie wiele punktów o współrzędnych wymiernych. Udowodnił ją G. Faltings w 1983 r. Niestety jednak nie potrafimy na ogół tych punktów wyznaczyć ani określić ich liczby.

W przypadku krzywych rodzaju 0 odpowiedź jest znana. Taka krzywa E jest izomorficzna nad $\mathbb{Q}$ z prostą lub z kwadryką i znane są efektywne metody znajdowania punktów $\mathbb{Q}$-wymiernych na tych krzywych.

Pozostaje więc przypadek, gdy $g = 1$, czyli przypadek krzywych eliptycznych. Jak wiemy, ranga r krzywej E decyduje o tym, czy liczba punktów $\mathbb{Q}$-wymiernych na tej krzywej jest skończona. Dokładniej, ta liczba jest skończona wtedy i tylko wtedy, gdy $r = 0$. Niestety nie jest znany algorytm, który pozwala to badać. Natomiast przyjmując prawdziwość hipotezy Bircha i Swinnertona-Dyera otrzymujemy, że $r = 0$ wtedy i tylko wtedy, gdy $L_E(1) \neq 0$.

Jeżeli stwierdzimy numerycznie, że $L_E(1) \neq 0$, to liczba punktów $\mathbb{Q}$-wymiernych na krzywej E jest skończona, nie przekracza 16 i potrafimy je efektywnie wyznaczyć.

Jeżeli stwierdzimy, że $L_E(1) = 0$ i $L'_E(1) \neq 0$, to wiemy, że liczba punktów $\mathbb{Q}$-wymiernych na E jest nieskończona. Nie znamy jednak ogólnego algorytmu, który pozwoliłby je wyznaczyć, choć znanych jest kilka algorytmów, które można próbować użyć bez gwarancji powodzenia.

Jeżeli zaś $L_E(1) = L'_E(1) = 0$, to niczego na temat punktów $\mathbb{Q}$-wymiernych na ogół nie potrafimy powiedzieć, choć hipoteza Bircha i Swinnertona-Dyera zapewnia, że jest ich nieskończenie wiele. Co więcej, nie znamy żadnej krzywej eliptycznej E, dla której potrafilibyśmy udowodnić, że $L_E(1) = L'_E(1) = L''_E(1) = 0$, choć znamy krzywe o randze $\geqslant 3$.

18. Inne hipotezy. Z każdą krzywą eliptyczną E określoną nad $\mathbb{Q}$ są związane trzy liczby: Minimalny wyróżnik Δ_E, przewodnik N_E oraz rząd grupy Tate'a–Szafarewicza $Ш_E$ (przyjmujemy, że ta grupa jest skończona).

Obserwacje oparte na obliczeniach wykonanych dla tysięcy krzywych eliptycznych wskazują, że te trzy liczby nie są niezależne. Wiemy na przykład, że zawsze $N_E \mid \Delta_E$. Doprowadziło to do sformułowania następujących hipotez, patrz [18].

Hipoteza L. Szpiro: Dla każdego $\varepsilon > 0$ istnieje taka stała C_ε, że dla każdej krzywej eliptycznej E określonej nad $\mathbb{Q}$ zachodzi nierówność

$$|\Delta_E| \leqslant C_\varepsilon N_E^{6+\varepsilon}.$$

Hipoteza D. Goldfelda i L. Szpiro: Dla każdego $\varepsilon > 0$ i liczby całkowitej nieujemnej r istnieje taka stała $C_{\varepsilon,r}$, że dla każdej krzywej eliptycznej E rangi r określonej nad $\mathbb{Q}$ zachodzi nierówność

$$|Ш_E| \leqslant C_{\varepsilon,r} N_E^{\frac{1}{2}+\varepsilon}.$$

Uzyskano też pewne wyniki teoretyczne, które potwierdzają prawdziwość tych hipotez w szczególnych przypadkach.

Obie hipotezy udowodniono w przypadku ciał funkcyjnych (to znaczy, gdy krzywa jest określona nad skończonym rozszerzeniem ciała $\mathbb{F}_q(T)$ funkcji wymiernych zmiennej T nad ciałem q-elementowym), drugą przy założeniu, że grupa $Ш_E$ jest skończona.

W przypadku ciała liczb wymiernych $\mathbb{Q}$ udowodniono równoważność tych hipotez tylko przy założeniu hipotezy Bircha i Swinnertona-Dyera, patrz [18].

Przykłady i algorytmy

19. Tablice. J. E. Cremona wyznaczył modele minimalne i wartości różnych parametrów wszystkich krzywych eliptycznych (modularnych) określonych nad $\mathbb{Q}$ o przewodnikach $N \leqslant 20\,000$. Są 132 524 takie krzywe.

Tablice dotyczące krzywych o przewodnikach $N \leqslant 1000$ zostały opublikowane, a pełne tablice dla $N \leqslant 20\,000$ są dostępne przez Internet, patrz [13].

Wśród tych krzywych jest tylko jedna spełniająca $|Ш_E| = 13^2$, a dla pozostałych mamy $|Ш_E| \leqslant 11^2$. W większości przypadków (bo aż dla 126 317 krzywych) mamy $|Ш_E| = 1$. Przy tych obliczeniach zakładano (w razie potrzeby), że grupa $Ш_E$ jest skończona i że zachodzi wzór (1) z hipotezy Bircha i Swinnertona-Dyera.

W algorytmach stosowanych przez Cremonę zakładano, że krzywa E jest modularna, tzn. wykorzystywano odpowiadającą jej formę paraboliczną f. Dziś wiemy, że każda krzywa eliptyczna określona nad $\mathbb{Q}$ jest modularna. Założenie to można więc pominąć.

20. Przykład 1. Równanie Fermata. Podamy prosty przykład ilustrujący powyższą teorię. Rozpatrzmy krzywą określoną za pomocą równania Fermata

$$u^3 + v^3 = w^3. \tag{3}$$

Podstawiając tu

$$u = 36Z + Y, \quad v = 36Z - Y, \quad w = 6X$$

otrzymamy

$$Y^2Z = X^3 - 432Z^3. \tag{4}$$

Na odwrót, podstawiając

$$X = 12w, \quad Y = 36(u - v), \quad Z = u + v$$

otrzymamy (3). Zatem krzywe określone równaniami (3) i (4) są biwymiernie równoważne nad $\mathbb{Q}$. Wobec tego (3) i (4) są modelami tej samej krzywej E określonej nad $\mathbb{Q}$.

Równanie (4) ma postać Weierstrassa. Korzystając z ogólnego wzoru na wyróżnik krzywej opisanej za pomocą równania Weierstrassa (2):

$$\Delta(a_1, \ldots, a_6) = (c_4^3 - c_6^2)/12^3,$$

gdzie

$$c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

i z kolei

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6,$$

otrzymujemy, że wyróżnik krzywej (4) jest równy $\Delta = -2^{12} \cdot 3^9 \neq 0$.

Zatem E jest krzywą eliptyczną. Jej model (4) nie jest minimalny, ponieważ dokonując podstawienia

$$X = 4X_1, \quad Y = 8Y_1 + 4Z_1, \quad Z = Z_1$$

otrzymamy równanie

$$Y_1^2Z_1 + Y_1Z_1^2 = X_1^3 - 7Z_1^3 \tag{5}$$

o wyróżniku $\Delta = -3^9$ mniejszym co do wartości bezwzględnej od wyróżnika modelu (4). Można dowieść, że (5) jest modelem minimalnym krzywej E. Zatem $\Delta_E = -3^9$ jest jej wyróżnikiem minimalnym.

W tablicach Cremony znajdujemy krzywą E pod numerem 27A1. Z tych tablic odczytujemy dalsze informacje o niej:

$$N = 27, \qquad |E(\mathbb{Q})_{\text{tors}}| = 3, \qquad r = 0.$$

Zatem na krzywej E, a więc i na każdym jej modelu, są dokładnie trzy punkty o współrzędnych wymiernych.

Można tego dowieść bezpośrednio. Jak wiemy, na krzywej Fermata (3) są dokładnie trzy punkty rzutowe o współrzędnych wymiernych (Wielkie Twierdzenie Fermata!):

$$(u, v, w) = (1, 0, 1), \quad (0, 1, 1), \quad (1, -1, 0).$$

Stosując powyższe podstawienia otrzymujemy trzy punkty $\mathbb{Q}$-wymierne na krzywych (4) i (5) odpowiednio:

$$(X, Y, Z) = (12, 36, 1), \quad (12, -36, 1), \quad (0, 72, 0) = (0, 1, 0)$$

oraz

$$(X_1, Y_1, Z_1) = (3, 4, 1), \quad (3, -5, 1), \quad (0, 1, 0)$$

Ponieważ 3 jest jedynym dzielnikiem pierwszym wyróżnika minimalnego $\Delta_E = -3^9$, więc krzywa E ma dobrą redukcję modulo p dla każdej liczby pierwszej $p \neq 3$. Jej redukcja modulo 3 jest zła. Jedynym punktem osobliwym krzywej zredukowanej E_3 jest $P = (0, 1, 1)$ i można sprawdzić, że do $E_3(\mathbb{F}_3)$ należą tylko trzy punkty nieosobliwe $(1, 0, 1)$, $(0, 1, 0)$, $(2, 1, 2)$. Grupa $E_3^{\mathrm{ns}}(\mathbb{F}_3)$ ma więc $p = 3$ elementy. Zatem redukcja krzywej E modulo 3 jest addytywna.

Można to odczytać również z tablic Cremony. Następne informacje o E zawarte w tych tablicach:

$c_3 = 3$ (liczba Tamagawy),
$\Omega = 1.7666387503$,
$L_E(1) = 0.588795834 \qquad (= \frac{1}{3}\Omega)$.

Ponieważ $L_E(1) \neq 0$, więc $r = 0$ i $R = 1$. Wobec tego grupa $Ш_E$ jest skończona. Zakładając prawdziwość hipotezy Birch a i Swinnertona-Dyera ze wzoru (1) otrzymujemy

$$|Ш_E| = L_E(1) \cdot |E(\mathbb{Q})_{\mathrm{tors}}|^2 / \Omega \cdot c_3 = 1.$$

21. Przykład 2. Nietrywialny element grupy Tate'a–Szafarewicza. Rozpatrzmy krzywą eliptyczną E' określoną nad $\mathbb{Q}$ za pomocą równania

$$3X^3 + 4Y^3 = 5Z^3.$$

Wiadomo, że

- Na E' nie ma punktów o współrzędnych wymiernych (patrz [5], III. §7. Zad. 23).
- Dla każdej liczby pierwszej p na E' są punkty o współrzędnych p-adycznych oraz punkty o współrzędnych rzeczywistych (patrz [5] I. §5, Zad. 8).
- E' jest przestrzenią jednorodną nad krzywą eliptyczną $(E, \mathcal{O})$ określoną nad $\mathbb{Q}$, gdzie

$$E: \ X^3 + Y^3 = 60Z^3, \qquad \mathcal{O} = (1, -1, 0).$$

Postępując podobnie jak w poprzednim przykładzie (tzn. podstawiając $X = U + V$, $Y = U - V$, $Z = W$, mnożąc przez $2 \cdot 3^5 \cdot 5^2$ itd.) otrzymujemy inny model krzywej E :

$$Y^2 Z = X^3 - 24\,300 Z^3, \qquad \mathcal{O}' = (0, 1, 0) \tag{6}$$

i oba modele są $\mathbb{Q}$-izomorficzne.

Dla uzyskania dalszych informacji o krzywej E wykorzystamy pakiet PARI/GP, wersja 2.1.0 [1] (szczegóły objaśnimy niżej). Otrzymujemy następujące wyniki:

- Model (6) krzywej E jest minimalny.
- $N_E = 24\,300 = 2^2 \cdot 3^5 \cdot 5^2$, $\quad \Delta_E = -2^8 \cdot 3^{13} \cdot 5^5$.
- Na E jest tylko jeden punkt torsyjny o współrzędnych wymiernych. Jest to $\mathcal{O}$ lub $\mathcal{O}'$ w zależności od modelu.
- Liczba Tamagawy $\prod_p c_p$ jest równa 1.
- $L_E(1) = 4.06137581$,
- $\Omega = 0.45126397$.

Z $L_E(1) \neq 0$ wynika, że $r = 0$ i $R = 1$ i grupa $Ш_E$ jest skończona. Ponieważ na krzywej E' nie ma punktów wymiernych globalnie, lecz są wszędzie punkty wymierne lokalnie, więc E' wyznacza niezerowy element grupy $Ш_E$. Wiemy więc bez żadnych hipotez, że $|Ш_E| > 1$.

Załóżmy teraz prawdziwość hipotezy Bircha i Swinnertona-Dyera. Zachodzi więc wzór (1). Korzystając z wyników powyższych obliczeń i ze wzoru (1) otrzymujemy $|Ш_E| = L_E(1)/\Omega = 9$.

Zauważmy, że $N_E = 24\,300 > 20\,000$, a więc krzywa E nie występuje w tablicach Cremony.

Tak więc pakiet PARI/GP daje możliwość samodzielnego badania krzywych eliptycznych określonych nad $\mathbb{Q}$, gdy znamy ich modele Weierstrassa. Omówimy to trochę dokładniej w następnym punkcie.

22. Pakiet PARI/GP, wersja 2.1.0. Opiszemy, jak korzystając z tego pakietu (patrz [1]) uzyskiwać informacje o krzywej eliptycznej określonej nad $\mathbb{Q}$ znając jej model Weierstrassa. Model ten może nie być minimalny, lecz współczynniki a_j powinny być całkowite.

Wydajemy kolejno następujące polecenia:

```
e = ellinit([a1, a2, a3, a4, a6])
```

Przy tym a_j muszą być konkretnymi liczbami całkowitymi. Na ekranie otrzymujemy wektor o 19 współrzędnych, pewne z nich też są wektorami. Aby wykorzystać te informacje pytamy o poszczególne współrzędne następująco:

`e[12]` Otrzymujemy wyróżnik Δ_E.
`e[13]` Otrzymujemy niezmiennik j.
`e[15]` Otrzymujemy liczbę Ω.

Teraz możemy pytać o dalsze informacje o krzywej E, którą komputer zna już jako `e`. Piszemy `elltors(e)`

Otrzymujemy wektor o trzech współrzędnych. Podają one rząd grupy $E(\mathbb{Q})_{\text{tors}}$, jej strukturę i generatory.

Badamy, czy model krzywej E jest minimalny pisząc

```
e1=ellglobalred(e)
```

Otrzymujemy wektor, który m.in. podaje

`e1[1]` – przewodnik N_E krzywej E.

`e1[3]` – liczbę Tamagawy $\prod_p c_p$ krzywej E.

Jeżeli `e1[2]` jest wektorem $[1,0,0,0]$, to model krzywej E był minimalny. Jeżeli nie, to otrzymamy model minimalny krzywej E pisząc

```
e2=ellchangecurve(e,e1[2])
```

Otrzymamy wynik podobny do tego, który dawało polecenie `ellinit`, lecz teraz informacje dotyczą modelu minimalnego (tzw. zredukowanego) krzywej E. W szczególności pierwszych pięć liczb w `e2` to są współczynniki a_j tego modelu minimalnego, a `e2[12]` jest wyróżnikiem minimalnym krzywej E.

Pisząc `elllseries(e,s)` otrzymujemy wartość $L_E(s)$. Tu za s trzeba podstawiać konkretne liczby. Funkcja $L_E(s)$ krzywej E nie zależy od jej modelu. Zatem w naszej sytuacji liczby `elllseries(e,s)` i `elllseries(e2,s)` są równe.

Na przykład polecenie `elllseries(e,1)` obliczy wartość $L_E(1)$. Jeżeli ta liczba będzie równa zeru, to dla obliczenia pochodnej $L'_E(1)$ możemy postępować następująco. Określamy `f(k)=elllseries(e,1+10^(-k))*10^k`

Obliczając następnie `f(1)`, `f(2)`, `f(3)`, ... otrzymamy ciąg zbieżny do pochodnej $L'_E(1)$, jak to wynika z elementarnej analizy.

Jeżeli wyrazy tego ciągu będą zbiegały wyraźnie do liczby różnej od zera, to ranga krzywej E będzie równa $r = 1$.

Możliwości pakietu PARI/GP są jednak ograniczone. Nie pozwala on wyznaczyć rangi r dowolnej krzywej eliptycznej (chyba, że przyjmiemy hipotezę Bircha i Swinnertona-Dyera). Nawet, jeżeli wiemy, że $r \geqslant 1$, to nie daje on sposobu na znalezienie elementu rzędu nieskończonego w grupie $E(\mathbb{Q})$, choć wiemy, że taki element istnieje. Tym bardziej ten pakiet nie daje możliwości wyznaczenia bazy grupy abelowej wolnej $E(\mathbb{Q})_{\text{free}}$, a więc i regulatora krzywej E. Nie znamy bowiem odpowiednich algorytmów, które można byłoby zastosować do dowolnej krzywej eliptycznej określonej nad $\mathbb{Q}$.

Bibliografia

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, *Pakiet PARI/GP.* `ftp://megrez.math.u-bordeaux.fr/pub/pari/`.

[2] B. Birch, H. P. F. Swinnerton-Dyer, *Notes on elliptic curves, I*, J. Reine Angew. Math. **212** (1963) 7–25.

[3] —, *Notes on elliptic curves, II*, J. Reine Angew. Math., **218** (1965) 79–108.

[4] R. Bölling, *Die Ordnung der Schafarewitsch-Tate Gruppe kann beliebig gross werden*, Math. Nachr., **67** (1975) 157–179.

[5] Z. I. Borewicz, I. R. Szafarewicz, *Teoria Liczb* (ros.), Moskwa, Nauka, 1964.

[6] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves: Wild 3-adic exercises*, J. Amer. Math. Soc., **14** (2001), no. 4, 843–939.

[7] A. Brumer, O. McGuinness, *The behaviour of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc., **23** (1990) 375–382.

[8] J. P. Buhler, B. H. Gross, D. B. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank* 3, Math. Comp., **44** (1985), no. 170, 473–481.

[9] J. W. S. Cassels, *Arithmetic on curves of genus* 1, (VI). *The Tate-Šafarevič group can be arbitrarily large*, J. Reine Angew. Math., **214/5** (1964) 65–70.

[10] —, *Arithmetic on curves of genus* 1, (VIII). *On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math., **217** (1965) 180–199.

[11] —, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc., **41** (1966) 193–291.

[12] J. E. Cremona, *The analytic order of* Ш *for modular elliptic curves*, J. Théor. Nombres, Bordeaux, **5** (1993), no. 1, 179–184.

[13] —, *Algorithms for modular elliptic curves*, 2. wyd., Cambridge Univ. Press, Cambridge, 1997
`http://www.maths.nott.ac.uk/personal/jec/packages.html`

[14] J. E. Cremona, B. Mazur, *Visualizing elements of the Shafarevich-Tate group*, Exper. Math., **9** (2000), no. 1, 13–28.

[15] A. Dąbrowski, M. Wieczorek, *Arithmetic on certain families of elliptic curves*, Bull. Austral. Math. Soc., **61** (2000) 319–327.

[16] F. Keqin, *Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture*, Acta Arith., **75** (1996), no. 1, 71–83.

[17] S. Fermigier, *Une courbe elliptique définie sur* $\mathbb{Q}$ *de rang* $\geqslant 22$, Acta Arith., **82** (1997), no. 4, 359–363.

[18] D. Goldfeld, L. Szpiro, *Bounds for the order of the Tate-Shafarevich group*, Compositio Math., **97** (1995) 71–87.

[19] R. Greenberg, *On the Birch and Swinnerton-Dyer conjecture*, Invent. Math., **72** (1983) 241–265.

[20] B. H. Gross, *Kolyvagin's work on elliptic curves*, in: L-functions and Arithmetic (J. Coates, M. J. Taylor, eds.), London Math. Soc. Lecture Note Series, vol. 153, Cambridge Univ. Press, Cambridge, 1991, 235–256.

[21] B. H. Gross, D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math., **84** (1986), no. 2, 225–320.

[22] J. Kaczorowski, *Czwarty problem milenijny: Hipoteza Riemanna*, Wiadom. Mat., **38** (2002), 91–120.

[23] A. W. Knapp, *Elliptic Curves*, Math. Notes, vol. 40, Princeton University Press, Princeton, 1992.

[24] N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1984.

[25] V. A. Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and* Ш$(E, \mathbb{Q})$ *for a subclass of Weil curves*, (ros.), Izv. Akad. Nauk SSSR, Ser. Mat., **52** (1988), no. 3, 523–540.

[26] —, *The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves*, (ros.), Izv. Akad. Nauk SSSR, Ser. Mat., **52** (1988), no. 6, 1154–1180.

[27] —, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curve*, Proc. Intern. Congr. Math., Kyoto 1988. **I** (1990), 429–436.

[28] S. Lang, *Algebra*, wyd. 2, PWN, Warszawa, 1984.

[29] Delang Li, Ye Tian, *On the Birch-Swinnerton-Dyer conjecture*, Acta Math. Sinica, English Series, **16** (2000), no. 2, 229–236.

[30] E. Lutz, *Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p-adiques*, J. Reine Angew. Math., **177** (1937) 238–247.
[31] W. G. McCallum, *Kolyvagin's work on Shafarevich-Tate groups*, in: *L*-functions and Arithmetic (J. Coates, M. J. Taylor, eds), London Math. Soc. Lecture Note Series, vol. 153, Cambridge Univ. Press, Cambridge, 1991, 295–316.
[32] Yu. I. Manin, *Cyclotomic fields and modular curves* (ros.), Uspehi Mat. Nauk, **26** (1971), no. 6, (162), 7–71.
[33] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES, **47** (1977) 33–186.
[34] —, *Rational isogenies of prime degree*, Invent. Math., **44** (1978) 129–162.
[35] J. S. Milne, *The Tate-Šafarevič group of a constant abelian variety*, Invent. Math., **6** (1968) 91–105.
[36] T. Nagell, *Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre*, Wid. Akad. Skrifter, Oslo, **1** (1935), no. 1, 1–25.
[37] A. Nitaj, *Invariants des courbes de Frey-Hellegouarch et grandes groupes de Tate-Shafarevich*, Acta Arith., **93** (2000) 303–327.
[38] K. A. Ribet, *On modular representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms*, Invent. Math., **100** (1990), 431–476.
[39] H. E. Rose, *On some elliptic curves with large Sha*, Exper. Math., **9** (2000), no. 1, 85–89.
[40] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, Invent. Math., **64** (1981), 455–470.
[41] —, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math., **89** (1987), no. 3, 527–559.
[42] —, *The „main conjecture" of Iwasawa theory for imaginary quadratic fields*, Invent. Math., **103** (1991), 25–68.
[43] —, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, in: J. Coates, R. Greenberg, K.A. Ribet, K. Rubin, Arithmetic Theory of Elliptic Curves (Cetraro, Italy 1997), Lecture Notes in Math. 1716 (C. Viola, eds.), Springer-Verlag, Berlin, 1999, 167–234.
[44] K. Rubin, A. Silverberg, *Ranks of elliptic curves*, Bull. Amer. Math. Soc., **39** (2002) 455–474.
[45] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Friedr. Vieweg & Sohn, Braunschweig, 1989.
[46] A. Silverberg, *Open questions in arithmetic algebraic geometry*, in: Arithmetic Algebraic Geometry (B. Conrad, K. Rubin, eds.), IAS/Park City Mathematics Series, vol. 9, Providence, RI, AMS, 2001, 83–142.
[47] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, Vol. 108, Springer-Verlag, New York, 1986.
[48] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.
[49] J. H. Silverman, J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.
[50] N. M. Stephens, *The diophantine equation $X^3 + Y^3 = DZ^3$ and the conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math., **231** (1968) 121–162.
[51] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analogue*, Séminaire Bourbaki (1965/66), no. 306, 415–440.
[52] —, *The arithmetic of elliptic curves*, Invent. Math., **23** (1974) 179–206.
[53] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math., **141** (1995), no. 3, 553–572.

[54] J. Tunnell, *A classical Diophantine problem and modular form of weight* 3/2, Invent. Math., **72** (1983), 323–334.
[55] B. M. M. de Weger, $A+B=C$ *and big* Ш*'s*, Quart. J. Math. Oxford, **49** (1998) 105–128.
[56] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math., **141** (1995), no. 3, 443–551.
[57] —, *The Birch and Swinnerton-Dyer conjecture* `http://www.claymath.org/prizeproblems/birchsd.htm`
[58] S. Zhang, *A note on Sha of some elliptic curves*, Adv. Math. (China), **26** (1997), no. 6, 551–555.

Jerzy Browkin

Instytut Matematyki
Uniwersytet Warszawski
ul. Banacha 2, 02–097 Warszawa

e-mail: bro@mimuw.edu.pl