Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

Bartosz Naskręcki

Rangi w rodzinach krzywych eliptycznych i formy modularne

Rozprawa doktorska z nauk matematycznych
w zakresie matematyki
napisana na Wydziale Matematyki i Informatyki
Uniwersytetu im. Adama Mickiewicza w Poznaniu
pod kierunkiem prof. dr. hab. Wojciecha Gajdy

Poznań 2014

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

ssdnm
środowiskowe
studia doktoranckie
z nauk matematycznych

UNIWERSYTET
IM. ADAMA MICKIEWICZA
W POZNANIU

UNIA EUROPEJSKA
FUNDUSZ SPÓJNOŚCI

Podziękowania

Pragnę podziękować Profesorowi Wojciechowi Gajdzie, mojemu promotorowi i Nauczycielowi, za wszelką okazaną pomoc i życzliwość przez wszystkie lata wspólnej pracy. Dziękuję również Gaborowi Wiese i Remke Kloosterman, którzy w szczególny sposób przyczynili się do powstania tej rozprawy. Dziękuję wszystkim osobom, które pomogły mi przy redakcji tej rozprawy oraz przygotowaniu publikacji. Pragnę również podziękować moim Rodzicom, którzy dali mi życie, piękne dzieciństwo i młodość pełną naukowej pasji. Dziękuję mojej Małżonce, której nieustanne wsparcie dawało mi siły i chęć do pracy. Pragnę również podziękować mojej Siostrze, z którą dzieliłem wszystkie radości i szczęścia dzieciństwa.

Mamie i Tacie
Monice i Dusi
Haroldowi

Niniejsza rozprawa została przygotowana w okresie, gdy autor był stypendystą Fundacji Uniwersytetu im. Adama Mickiewicza w Poznaniu oraz kierownikiem grantu NCN Preludium 2012/05/N/ST1/02871.

Spis treści

1 Wstęp **1**

2 Rodziny krzywych eliptycznych **7**
2.1 Preliminaria 7
2.2 Minimalny model Weierstrassa 12
2.3 Kohomologie ℓ-adyczne i ranga 31
2.4 Skręcenia krzywych eliptycznych 35
2.5 Rangi w rodzinach krzywych I 41
2.6 Rangi w rodzinach krzywych II 56

3 Formy modularne i kongruencje **72**
3.1 Preliminaria 72
3.2 Reprezentacje Galois 85
3.3 Kongruencje - warunki ogólne 90
3.4 Kongruencje - szczególne przypadki 94
3.5 Algorytmy 99
3.6 Dane numeryczne 103
3.7 Wnioski z danych i przykłady kongruencji 105

Bibliografia **114**

Rozdział 1

Wstęp

Rozwiązywanie równań diofantycznych stanowi jedno z centralnych zagadnień teorii liczb. Szczególnie ważna klasa tych równań, pochodząca od krzywych eliptycznych określonych nad ciałem liczb wymiernych, od ponad dwustu lat skupia uwagę wielu matematyków. Teoria krzywych eliptycznych w jej aspektach analitycznych jest ściśle związana z rozwijającą się równolegle teorią eliptycznych form modularnych. Podstawowy problem arytmetyki krzywych eliptycznych polega na wyznaczaniu struktury zbioru punktów wymiernych na krzywej, który na mocy twierdzenia L. Mordella jest grupą abelową skończenie generowaną. Pytanie dotyczące liczby generatorów tej grupy pozostaje do dzisiaj nierozstrzygniętym problemem. Niniejsza rozprawa wnosi do tej tematyki szereg wyników dotyczących badania nieskończonych rodzin krzywych eliptycznych nad ciałem liczb wymiernych oraz nad ciałami funkcyjnymi.

Sformułowana przez B. Bircha i P. Swinnertona-Dyera hipoteza wiążąca rangę grupy Mordella z rzędem znikania L-funkcji krzywej eliptycznej daje nam wgląd w skomplikowaną naturę badanych obiektów. Arytmetyka krzywych eliptycznych w ścisły sposób związana jest z badaniem analitycznych własności funkcji L stowarzyszonych z krzywymi eliptycznymi. Zasadniczy wkład w zrozumienie tych relacji wniósł A. Wiles wraz ze współpracownikami. Udowodnili oni w twierdzeniu o modularności, że każda krzywa eliptyczna nad ciałem liczb wymiernych jest w określony sposób stowarzyszona z eliptyczną formą modularną. Precyzyjna natura tej relacji jest wyrażona poprzez równość odpowiadających obu obiektom L-funkcji.

Rozwijana od początku XIX wieku teoria form modularnych, dzięki wspomnianemu powyżej twierdzeniu o modularności zyskała ponownie ważne miejsce w głównym nurcie teorii liczb. Warto zwrócić uwagę, że sformułowana przez Y. Taniyamę i G. Shimurę hipoteza wiążąca krzywe eliptyczne z formami modularnymi przez wiele lat była elementem zbliżającym arytmetykę krzywych eliptycznych z analityczną teorią liczb wyrażoną badaniem form modularnych.

Niezależnie od tych problemów lub raczej w równoległy sposób, P. Deligne, J.-P. Serre i G. Shimura pokazali, że trzeci główny nurt algebraicznej teorii liczb, związany z reprezentacjami Galois, w istotny sposób wiąże się z formami modularnymi. Udowodnione przez nich twierdzenia pozwalają nam konstruować stowarzyszone z formą modularną reprezentacje Galois, dając w ten sposób pełniejszy wgląd w

arytmetyczne własności współczynników Fouriera tych funkcji.

W tym świetle, twierdzenie o modularności stanowi rezultat łączący krzywe eliptyczne i formy modularne z reprezentacjami Galois. Ten związek jest obecnie intensywnie badany pod kątem porównywania reprezentacji pochodzących od różnych obiektów, między innymi od szeregów Eisensteina. Badanie takich związków dało początek problematyce kongruencji między formami modularnymi, której spektakularne osiągnięcia K. Ribeta i B. Mazura z lat siedemdziesiątych i osiemdziesiątych ubiegłego stulecia leżą u podstaw sukcesu tej dyscypliny. W trzeciej części rozprawy badamy kongruencje związane z formami modularnymi i szeregami Eisensteina, rozwijając teoretycznie i numerycznie pewne wyniki Ribeta i Mazura.

Krąg nakreślonych zagadnień zatacza koło, gdyż opisane w rozprawie wyniki dotyczące form modularnych w pewnych ważnych przypadkach wykorzystują własności krzywych eliptycznych określonych nad ciałem liczb wymiernych. Z drugiej strony, badanie rodzin krzywych eliptycznych w nieodzowny sposób powiązane jest z badaniem działania grupy Galois na kohomologiach etalnych związanych z powierzchniami eliptycznymi, dając w efekcie precyzyjne wyniki o randze grupy Mordella-Weila w nieskończonych rodzinach krzywych.

Przystępujemy do omówienia najważniejszych wyników dowiedzionych w niniejszej rozprawie. W Rozdziale 2 przedstawione zostały wyniki autora zawarte w [Nas13] oraz nowe rezultaty uzyskane już po opublikowaniu tej pracy. Badanym obiektem jest krzywa eliptyczna

$$y^2 = x(x - f^2)(x - g^2), \tag{1.1}$$

gdzie f i g są wielomianami jednej zmiennej o współczynnikach w pewnym ciele liczbowym lub w domknięciu algebraicznym $\overline{\mathbb{Q}}$ ciała liczb wymiernych. Po zastosowaniu twierdzenia o specjalizacji (Twierdzenie 2.5.22), z wyników o krzywych (1.1) otrzymujemy opis rodzin krzywych eliptycznych postaci

$$y^2 = x(x - \alpha a^2)(x - \beta b^2),$$

określonych nad $\mathbb{Q}$ i takich, że $\alpha a^2 + \beta b^2 = \gamma c^2$, $\alpha, \beta, \gamma \in \mathbb{Q}$. W tym miejscu warto zwrócić uwagę, że rozważana rodzina krzywych eliptycznych stanowi uzupełnienie rodziny krzywych Freya dla wykładnika $p = 2$, użytych do dowodu Wielkiego Twierdzenia Fermata. Gdy $\alpha = \beta = \gamma = 1$ udowadniamy następujące twierdzenie.

Twierdzenie 1.0.1 (Twierdzenie 2.1.9)**.** *Istnieje nieskończenie wiele trójek* (a, b, c) *liczb naturalnych takich, że* $a^2 + b^2 = c^2$ *oraz*

$$y^2 = x(x - a^2)(x - b^2)$$

jest krzywą eliptyczną, która posiada co najmniej 2 liniowo niezależne punkty $\mathbb{Q}$*-wymierne dane jawnymi wzorami.*

Następnym nowym rezultatem uzyskanym w tej rozprawie jest poniższe twierdzenie.

Twierdzenie 1.0.2 (Wniosek 2.6.19)**.** *Istnieje nieskończenie wiele trójek* (a, b, c) *liczb wymiernych takich, że* $-2a^2 + b^2 = -2c^2$ *oraz*

$$y^2 = x(x + 2a^2)(x - b^2)$$

jest krzywą eliptyczną, która posiada co najmniej 3 liniowo niezależne punkty $\mathbb{Q}$*-wymierne dane jawnymi wzorami.*

Twierdzenia 1.0.1 i 1.0.2 wynikają z badania krzywych eliptycznych postaci (1.1) dla szczególnych typów wielomianów f i g. Następny rezultat daje precyzyjny opis grupy punktów $\overline{\mathbb{Q}}(t)$-wymiernych krzywych postaci (1.1) dla wielomianów stopnia co najwyżej 2.

Twierdzenie 1.0.3 (Twierdzenie 2.6.10)**.** *Niech* $f, g \in \overline{\mathbb{Q}}[t]$ *będą względnie pierwsze oraz niech istnieje* $h \in \overline{\mathbb{Q}}[t]$ *takie, że* $f^2 + g^2 = h^2$*. Załóżmy, że* $\deg f = 2$ *i* $1 \leq \deg g \leq 2$ *oraz* $f, g, f^2 - g^2$ *są rozdzielcze, a ponadto* $\deg(f^2 - g^2) = 2 \deg f$*. Niech* E *będzie krzywą eliptyczną określoną nad* $\overline{\mathbb{Q}}(t)$ *równaniem*

$$y^2 = x(x - f^2)(x - g^2).$$

Wówczas

$$E(\overline{\mathbb{Q}}(t)) \cong \mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Grupę $E(\overline{\mathbb{Q}}(t))$ *generują punkty*

$$\begin{aligned} P_1 =& (-(1+\sqrt{2})g(g-h), \sqrt{-1}(1+\sqrt{2})g(g-h)(\sqrt{2}g-h)), \\ P_2 =& ((f-h)(g-h), (f+g)(f-h)(g-h)), \\ T_1 =& (g^2, 0), \\ T_2 =& (fg, \sqrt{-1}f(f-g)g). \end{aligned}$$

W dowodzie następnego twierdzenia, które stanowi rozwinięcie [Nas13, Theorem 1.4] stosujemy metody kohomologii etalnych przedstawione w podrozdziałach 2.3, 2.4 oraz wykorzystujemy własności działania absolutnej grupy Galois na punktach $\overline{\mathbb{Q}}(t)$-wymiernych krzywych postaci (1.1).

Twierdzenie 1.0.4 (Twierdzenie 2.6.15)**.** *Niech* E *będzie krzywą eliptyczną nad* $\mathbb{Q}(t)$ *określoną równaniem*

$$E : y^2 = x(x + 2(u^2 + 2^5)^2)(x - (-2^4 u)^2), \quad u = \frac{-2^4 t}{-10 + t^2}.$$

Wówczas grupa punktów $\mathbb{Q}(t)$*-wymiernych jest postaci*

$$E(\mathbb{Q}(t)) \cong \mathbb{Z}^3 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Wynik sformułowany w Twierdzeniu 1.0.2 jest konsekwencją zastosowania Twierdzenia 1.0.4. Dolne ograniczenie rangi uzyskane w Twierdzeniu 1.0.2 otrzymujemy stosując Twierdzenie 2.5.22 o specjalizacji.

W Rozdziale 3 rozprawy badamy kongruencje pomiędzy współczynnikami Fouriera $a_n(f)$ oraz $a_n(E)$, odpowiednio nowych form parabolicznych f i form Eisensteina E

$$a_n(f) \equiv a_n(E) \pmod{\lambda^r}, \tag{1.2}$$

gdzie λ jest ideałem maksymalnym w ciele liczbowym generowanym przez współczynniki Fouriera formy f, natomiast r jest dodatnią liczbą naturalną. Punktem początkowym dla całej teorii jest kongruencja odkryta przez S. Ramanujana pomiędzy

$$f = q\prod_{k=1}^{\infty}(1-q^k)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$$

oraz szeregiem Eisensteina wagi 12 zadanym równaniem

$$E = \frac{691}{65520} + \sum_{n=1}^{\infty}\sigma_{11}(n)q^n,$$

gdzie $\sigma_{11}(n) = \sum_{d|n} d^{11}$ oraz $q = e^{2\pi i\tau}$ i $\tau \in \mathbb{C}$ takie, że $\Im\tau > 0$. Dla dowolnego $n \geq 0$ zachodzi kongruencja

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}.$$

Badamy kongruencje, w których formy f oraz E należą do przestrzeni form modularnych $\mathcal{M}_k(\Gamma_0(N))$ wagi k i poziomu N i są wektorami własnymi algebry Hecke $\mathbb{T}_N$, por. podrozdział 3.1. W pracy autora [Nas14] udowodnione zostały ograniczenia na wykładnik r kongruencji (1.2) dla poziomów N, które są liczbami pierwszymi. Istotną częścią [Nas14] jest rachunek numeryczny oraz nowe przykłady kongruencji. W Rozdziale 3 rozprawy rozszerzamy wyniki teoretyczne z [Nas14] na przypadek poziomów N wolnych od kwadratów. Ponadto przedstawiamy obszerny materiał numeryczny, uzyskany za pomocą pakietu MAGMA. Stanowi on znaczące rozszerzenie zbioru przykładów podanego w pracy [Nas14]. Podrozdział 3.7 zawiera wnioski sformułowane na podstawie przeprowadzonych obliczeń numerycznych. Jednym z głównych wyników tej części pracy jest następujące twierdzenie.

Twierdzenie 1.0.5 (Wniosek 3.3.11)**.** *Niech $p_1, \ldots, p_t$ będą parami różnymi liczbami pierwszymi oraz niech $k > 2$ będzie liczbą naturalną parzystą. Niech $N = p_1 \cdot \ldots \cdot p_t$ oraz $f \in \mathcal{S}_k(\Gamma_0(N))^{new}$ będzie nową formą własną. Niech E będzie formą własną z $\mathcal{E}_k(\Gamma_0(N))$ taką, że $a_0(E) \neq 0$. Załóżmy, że dla ustalonego ideału maksymalnego z ciała współczynników formy f i dla pewnego $r > 0$ zachodzą kongruencje*

$$a_n(f) \equiv a_n(E) \ (mod\ \lambda^r)$$

dla wszystkich $n \geq 0$. Jeśli ℓ jest charakterystyką ciała reszt ideału λ oraz $\ell \nmid N$, to

$$r \leq ord_\lambda(\ell) \cdot v_\ell\left(-\frac{B_k}{2k}\prod_{i=1}^{t}(1-p_i)\right),$$

gdzie ord_λ jest waluacją względem λ, v_ℓ jest waluacją ℓ-adyczną oraz B_k jest k-tą liczbą Bernoulliego.

W dowodzie Twierdzenia 1.0.5 wykorzystujemy opis bazy wektorów własnych przestrzeni $\mathcal{E}_k(\Gamma_0(N))$ z podrozdziału 3.1.7. Opis tej bazy dla $k = 2$ został podany wcześniej w pracy [Yoo13a]. Dla $k > 2$, zgodnie z wiedzą autora, opis bazy przestrzeni $\mathcal{E}_k(\Gamma_0(N))$ został wykonany po raz pierwszy w tej rozprawie. Dla reprezentacji Galois stowarzyszonych z formami modularnymi f i E Twierdzenie 1.0.5 podaje górne ograniczenie na wykładnik kongruencji pomiędzy zadanymi reprezentacjami Galois.

Jeśli założymy, że ciało współczynników formy f jest ciałem liczb wymiernych, to uzyskujemy następującą charakteryzację kongruencji typu (1.2).

Twierdzenie 1.0.6 (Twierdzenia 3.4.5, 3.4.8)**.** *Niech N będzie liczbą wolną od kwadratów. Niech $f \in \mathcal{S}_2(\Gamma_0(N))^{new}$ będzie nową formą własną o wymiernych współczynnikach Fouriera. Niech ℓ będzie liczbą pierwszą taką, że dla pewnego $r > 0$ kongruencja*

$$a_n(f) \equiv a_n(E) \ (mod\ \ell^r)$$

zachodzi dla każdego $n \geq 0$ i pewnej formy własnej Eisensteina $E \in \mathcal{E}_2(\Gamma_0(N))$. Wówczas spełniony jest jeden z warunków:

(1) $N = 19$ *lub* $N = 37$ *i* $\ell^r = 3$,

(2) $N = 11$ *i* $\ell^r = 5$,

(3) $N = 17$ *i* $\ell^r = 2$,

(4) N *jest liczbą pierwszą postaci* $u^2 + 64$, *gdzie* u *liczbą całkowitą nieparzystą i* $\ell^r = 2$,

(5) N *jest iloczynem dwóch różnych liczb pierwszych i* $\ell^r \in \{2, 3, 4, 5, 7\}$,

(6) N *ma więcej niż dwa czynniki pierwsze i wtedy* $\ell^r \in \{2, 3, 4, 5, 7, 8, 9\}$.

Gdy N jest iloczynem dwóch różnych liczb pierwszych i $\ell^r = 7$, to istnieje dokładnie jedna forma E spełniająca kongruencję.

W dowodzie Twierdzenia 1.0.6 istotnie wykorzystujemy fakt, że forma f odpowiada pewnej krzywej eliptycznej nad $\mathbb{Q}$. Następnie stosujemy twierdzenie B. Mazura o punktach torsyjnych na krzywych eliptycznych nad $\mathbb{Q}$ [Maz77, Theorem 8] wraz z twierdzeniem N. Katza o części torsyjnej grupy Mordella-Weila [Kat81, Theorem 2].

Omówimy teraz strukturę pracy. W Rozdziale 2 wprowadzamy pojęcia potrzebne do sformułowania Twierdzeń 1.0.1, 1.0.2, 1.0.3 i 1.0.4. Następnie omawiamy model minimalny Weierstrassa oraz przedstawiamy niezbędny w rachunkach algorytm Tate'a. Wprowadzamy model Kodairy-Nérona powierzchni eliptycznej stowarzyszonej z krzywą eliptyczną nad ciałem funkcyjnym oraz twierdzenia o dobrej redukcji. Następnie podajemy górne oszacowania na rangę grupy Nérona-Severiego, które stanowią kluczowy punkt dowodu wymienionych wyżej twierdzeń. Podstawowy rachunek rangi grupy Mordella-Weila został przeprowadzony w rozdziale o kohomologiach ℓ-adycznych i o skręceniach krzywych eliptycznych.

Podrozdział 2.5.2 zawiera opis działania absolutnej grupy Galois na punktach $\overline{\mathbb{Q}}(t)$-wymiernych krzywej wykorzystany w dowodzie Twierdzenia 1.0.4. Następnie omawiamy twierdzenie o specjalizacji dla krzywych eliptycznych, aby zastosować je do dowodu Twierdzeń 1.0.1, 1.0.2. W podrozdziale 2.6 omawiamy szczegółowo teorię wysokości potrzebną do dowodu Twierdzenia 1.0.3. Ostatnia część Rozdziału 2 poświęcona jest przykładom oraz dowodowi Twierdzenia 1.0.4.

W Rozdziale 3 wprowadzamy definicję badanych w rozprawie form modularnych oraz algebry Hecke działającej na przestrzeni form. Następnie omawiamy konstrukcję baz wektorów własnych w podprzestrzeni form Eisensteina. W podrozdziale 3.2 dyskutujemy związek kongruencji form modularnych z reprezentacjami Galois. W kolejnym podrozdziale omawiamy istnienie kongruencji podanych przez nas typów, a następnie formułujemy i dowodzimy Twierdzenia 1.0.5 i 1.0.6. W podrozdziale 3.5 został przedstawiony opis stosowanych algorytmów potrzebnych do numerycznego poszukiwania kongruencji. Przykłady podane w podrozdziale 3.6 zostały wybrane z bazy danych, w której są skatalogowane wszystkie uzyskane przykłady kongruencji. Autor udostępni bazę danych na wyraźne życzenie zainteresowanych.

Rozdział 2

Rodziny krzywych eliptycznych

W tym rozdziale rozważamy rodziny krzywych eliptycznych postaci

$$E_{f(t),g(t),h(t)} : y^2 = x(x - f(t)^2)(x - g(t)^2),$$

zadane przez wielomiany $f(t), g(t), h(t) \in K[t]$, które spełniają relację $f(t)^2 + g(t)^2 = h(t)^2$, gdzie K jest ciałem liczbowym lub $\overline{\mathbb{Q}}$. Przedstawiamy strukturę grupy torsyjnej $E_{f(t),g(t),h(t)}(K(t))_{tors}$ oraz opisujemy zmiany rangi w zależności od wyboru f, g i h. Dla wielomianów stopnia co najwyżej dwa uzyskujemy pełen opis rangi generycznej tej rodziny. Wyniki te zastosujemy do opisu rodzin krzywych eliptycznych postaci

$$y^2 = x(x - \alpha a^2)(x - \beta b^2),$$

określonych nad $\mathbb{Q}$ i takich, że $\alpha a^2 + \beta b^2 = \gamma c^2$, $\alpha, \beta, \gamma \in \mathbb{Q}$.

2.1 Preliminaria

Niech dane będzie równanie Pitagorasa $a^2 + b^2 = c^2$, gdzie a, b, c są liczbami wymiernymi. Rozważamy stowarzyszoną z nim krzywą eliptyczną daną równaniem afinicznym

$$E_{(a,b,c)} : y^2 = x(x - a^2)(x - b^2).$$

Aby opisana krzywa była gładka, zakładamy, że $ab \neq 0$, co jest równoważne faktowi, że wyróżnik równania $E_{(a,b,c)}$ jest niezerowy. Rodzina $E_{(a,b,c)}$ jest podobna do innej rodziny, opisanej równaniem

$$y^2 = x(x - a^2)(x + b^2),$$

która jest szczególnym przypadkiem tzw. krzywej w postaci Freya.

Rozważmy następujące zbiory trójek liczb całkowitych

$$\mathcal{P} = \{(a, b, c) \in \mathbb{Z}^3 : a^2 + b^2 = c^2\}$$

$$\mathcal{P}_0 = \{(a, b, c) \in \mathbb{Z}^3 : a^2 + b^2 = c^2, ab \neq 0\}$$

$$\mathcal{P}_1 = \{(P^2 - Q^2, 2PQ, P^2 + Q^2) \in \mathbb{Z}^3 : P, Q \in \mathbb{Z} \text{ takie, że } \frac{P}{Q} = \frac{2pq}{p^2 + 5q^2} \text{ dla pewnych } p, q \in \mathbb{Z} \setminus \{0\}\}.$$

Jest jasne, że $\mathcal{P}_1 \subsetneq \mathcal{P}_0 \subsetneq \mathcal{P}$.

2.1.1 Własności geometryczne krzywych $E_{(a,b,c)}$

Wyróżnik równania $E_{(a,b,c)} : y^2 = x(x-a^2)(x-b^2)$, gdzie $(a,b,c) \in \mathcal{P}$ dany jest wzorem

$$\Delta(a,b,c) = 16(a-b)^2(a+b)^2a^4b^4.$$

Niezmiennik j krzywej $E_{(a,b,c)}$ dany jest wzorem

$$j(a,b,c) = 256\frac{(a^4-a^2b^2+b^4)^3}{a^4b^4(a-b)^2(a+b)^2}.$$

Lemat 2.1.1. *Trójka (a,b,c) należy do $\mathcal{P}_0$ wtedy i tylko wtedy, gdy (a,b,c) należy do $\mathcal{P}$ oraz $\Delta(a,b,c) \neq 0$.*

Dowód. Wystarczy zauważyć, że $\Delta(a,b,c) = 0$ zachodzi wtedy i tylko wtedy, gdy $(a^2-b^2)^2a^2b^2 = 0$. Gdyby $a^2-b^2 = 0$, wówczas $2a^2 = c^2$, co na mocy założenia, że $a,b,c \in \mathbb{Q}$ implikuje, że $a,b,c = 0$. W pozostałych przypadkach zachodzi, że $a = 0$ lub $b = 0$. Zatem łącznie zachodzi warunek

$$\Delta(a,b,c) = 0 \Leftrightarrow ab = 0.$$

□

Przykład 2.1.2. Rozważmy przypadek trójki $(a,b,c) = (3,4,5)$. Otrzymujemy krzywą eliptyczną $E_{(3,4,5)} : y^2 = x(x-3^2)(x-4^2)$. Punkty $(9,0)$ i $(16,0)$ generują część torsyjną grupy $E_{(3,4,5)}(\mathbb{Q})$. Punkt $(18,-18)$ jest punktem nieskończonego rzędu, który generuje część wolną grupy Mordella-Weila $E_{(3,4,5)}(\mathbb{Q})$.

Wprowadzimy teraz pewną relację równoważności na zbiorze $\mathcal{P}_0$. Pozwoli to na opisanie nowego modelu dla krzywej $E_{(a,b,c)}$, który zależy od jednego parametru wymiernego t. Dzieki temu możemy udowodnić podstawowe twierdzenia tego rozdziału w ogólnej postaci.

Definicja 2.1.3. Niech (a,b,c) oraz (A,B,C) będą elementami z $\mathcal{P}_0$. Mówimy, że trójki te są równoważne

$$(a,b,c) \sim (A,B,C)$$

wtedy i tylko wtedy, gdy stowarzyszone z nimi krzywe eliptyczne $E_{(a,b,c)}$ oraz $E_{(A,B,C)}$ są izomorficzne nad $\mathbb{Q}$.

Stwierdzenie 2.1.4. *Dwie trójki (a,b,c) oraz (A,B,C) są w relacji $(a,b,c) \sim (A,B,C)$ wtedy i tylko wtedy, gdy istnieją liczby $u \in \mathbb{Q}^\times$ oraz $\epsilon_1,\epsilon_2,\epsilon_3 \in \{-1,1\}$ takie, że*

$$(a,b,c) = (\epsilon_1 uA, \epsilon_2 uB, \epsilon_3 uC) \quad lub \quad (a,b,c) = (\epsilon_1 uB, \epsilon_2 uA, \epsilon_3 uC).$$

Dowód. Wynika ze wzoru na zamianę współrzędnych dwóch równań w postaci Weierstrassa, patrz (2.4). □

Zauważmy, że relacja $\sim$ na zbiorze $\mathcal{P}_0$ jest relacją równoważności.

Wprowadzamy następujące podzbiory liczb wymiernych

$$\begin{aligned}\mathcal{T} &= \mathbb{Q},\\ \mathcal{T}_0 &= \mathbb{Q} \setminus \{0, \pm 1\},\\ \mathcal{T}_1 &= \{\frac{2t}{5+t^2} : t \in \mathbb{Q} \setminus \{0\}\}.\end{aligned}$$

Definiujemy odwzorowanie wymierne schematów

$$t : \mathbb{A}^3_{\mathbb{Q}} \to \mathbb{A}^1_{\mathbb{Q}} : (a,b,c) \mapsto \frac{b}{c-a}.$$

Na zbiorze

$$\{(a,b,c) \in \mathbb{A}^3 : a^2+b^2-c^2, ab \neq 0\}$$

odwzorowanie t jest morfizmem. Na punktach domkniętych, w szczególności na punktach ze zbioru $\mathcal{P}_0$ otrzymujemy

$$t(\mathcal{P}_0) = \mathcal{T}_0.$$

Surjektywność odwzorowania t na $\mathcal{P}_0$ wynika z następujących formuł:

$$\frac{t^2-1}{t^2+1} = \frac{a}{c}, \tag{2.1}$$

$$\frac{2t}{t^2+1} = \frac{b}{c}, \tag{2.2}$$

gdzie $t = t(a,b,c)$.
Definiujemy krzywą eliptyczną E_t nad $\mathbb{Q}(t)$, gdzie t oznacza zmienną wolną:

$$E_t : y^2 = x(x-(t^2-1)^2)(x-4t^2).$$

Liniowa zamiana zmiennych

$$x \mapsto x\frac{4}{(a-c)^2}, \quad y \mapsto y\frac{8}{(c-a)^3}$$

określa $\mathbb{Q}$-izomorfizm krzywych eliptycznych $E_{(a,b,c)}$ i $E_{b/(c-a)}$. Analogicznie jak dla krzywej $E_{(a,b,c)}$ definiujemy wyróżnik i j-niezmiennik krzywej E_t

$$\Delta(t) = 256t^4\left(-1+t^2\right)^4\left(1-6t^2+t^4\right)^2,$$

$$j(t) = \frac{16\left(1-8t^2+30t^4-8t^6+t^8\right)^3}{t^4\left(-1+t^2\right)^4\left(1-6t^2+t^4\right)^2}.$$

W szczególności zbiór tych liczb wymiernych $t_0 \in \mathbb{Q}$, dla których $\Delta(t_0) \neq 0$ jest równy $\mathcal{T}_0$.

Stwierdzenie 2.1.5. *Dwie krzywe E_t i $E_{t'}$ są $\mathbb{Q}$-izomorficzne wtedy i tylko wtedy, gdy*

$$t' \in \left\{t, -t, \frac{1}{t}, -\frac{1}{t}, \frac{1+t}{1-t}, \frac{1-t}{1+t}, -\frac{1-t}{1+t}, -\frac{1+t}{1-t}\right\}.$$

Dowód. Wystarczy zauważyć, że żądany izomorfizm ma zachowywać model Weierstrassa obu krzywych. □

Na zbiorze $\mathcal{T}_0$ można wprowadzić relację równoważności $\sim$ (analogicznie do identycznie oznaczanej relacji na $\mathcal{P}_0$). Mówimy, że elementy t_0 i t_1 są w relacji $t_0 \sim t_1$ wtedy i tylko wtedy, gdy odpowiadające im krzywe eliptyczne E_{t_0} oraz E_{t_1} są $\mathbb{Q}$-izomorficzne. Równoważnie oznacza to, że element t' jest równy $s(t)$, gdzie s jest złożeniem odpowiednią liczbę razy funkcji s_1 i s_2 danych wzorami $s_1(t) = -t$ oraz $s_2(t) = \frac{1+t}{1-t}$.

Stwierdzenie 2.1.6. *Niech $R(t)$ oznacza zbiór wszystkich funkcji postaci $s(t)$, gdzie s jest złożeniem skończonego ciągu funkcji $s_{i_1}, s_{i_2}, \ldots, s_{i_r}$ dla pewnego $r \geq 1$, $i_k \in \{1, 2\}$. Wówczas*

$$R(t) = \left\{t, -t, \frac{1}{t}, -\frac{1}{t}, \frac{1+t}{1-t}, \frac{1-t}{1+t}, -\frac{1-t}{1+t}, -\frac{1+t}{1-t}\right\}.$$

Dowód. Po pierwsze zauważmy, że funkcje s_1, s_2 są odwracalne oraz generują w zbiorze funkcji wymiernych (ze względu na operację składania funkcji) grupę skończoną, ośmioelementową o relacjach $s_1^2 = id$ oraz $s_2^4 = id$ oraz $s_1 \circ s_2 \circ s_1 = s_2^3$. Stąd wynika, że zbiór $R(t)$ jest skończony i składa się z dokładnie 8 elementów. Dla zakończenia dowodu wystarczy wypisać wszystkie nieskracalne słowa w grupie generowanej przez s_1 oraz s_2. □

Relacja $\sim$ na zbiorze $\mathcal{T}_0$ utożsamia elementy wymierne $t, t' \in \mathcal{T}_0$, które spełniają $t' = s(t)$ dla pewnej funkcji $s(t) \in R(t)$.

Stwierdzenie 2.1.7. *Każda klasa abstrakcji ze względu na relację $\sim$ na zbiorze $\mathcal{T}_0$ ma dokładnie 8 elementów. W szczególności, zbiór klas abstrakcji $\mathcal{T}_0/\sim$ jest nieskończony przeliczalny.*

Dowód. Wystarczy sprawdzić, że jeśli $s(t_0) = t_0$ dla pewnego $s(t) \in R(t)$ i $t_0 \in \mathbb{Q}$, to wtedy $t_0 \notin \mathcal{T}_0$. □

Każda klasa abstrakcji $[t]_\sim$ zbioru $\mathcal{T}_0/\sim$ reprezentuje jedną klasę $\mathbb{Q}$-izomorfizmu krzywych eliptycznych postaci E_t dla $t \in \mathcal{T}_0$.

Lemat 2.1.8 ([Nas13, Prop. 2.1])**.** *Odwzorowanie $t : (a, b, c) \mapsto \frac{b}{c-a}$ indukuje bijekcję zbiorów $\mathcal{P}_0/\sim \longrightarrow \mathcal{T}_0/\sim$. Odwzorowanie odwrotne jest dane przez*

$$\frac{p}{q} \mapsto (p^2 - q^2, 2pq, p^2 + q^2).$$

Ponadto odwzorowanie t przekształca bijektywnie zbiór $\mathcal{P}_1/\sim$ na zbiór $\mathcal{T}_1/\sim$.

Dowód. Sprawdzenie, że złożenie obu odwzorowań daje identyczność na klasach abstrakcji jest trywialne. Ponadto kładąc $t_0 = \frac{p}{q}$ łatwo sprawdzić, że $\frac{2t}{5+t^2} = \frac{2pq}{p^2+5q^2}$ i możemy wybrać reprezentanta (a,b,c) w klasie $[(a,b,c)] \in \mathcal{P}_1/\sim$ takiego, że $(a,b,c) = (P^2-Q^2, 2PQ, P^2+Q^2)$, gdzie $\frac{P}{Q} = \frac{2pq}{p^2+5q^2}$. □

Niech zbiory $\mathcal{C}_i$ stanowią klasy abstrakcji ze względu na relację $\sim$ na $\mathcal{P}_1$. Wówczas $\mathcal{P}_1$ równa się $\bigcup_{i=1}^{\infty} \mathcal{C}_i$. Dla ustalonego i zbiór $\mathcal{C}_i$ reprezentuje klasę $\mathbb{Q}$-izomorfizmu krzywych $E_{(a,b,c)}$ takich, że $(a,b,c) \in \mathcal{C}_i$. W szczególności dwie krzywe reprezentowane przez elementy ze zbiorów $\mathcal{C}_i$ i $\mathcal{C}_j$ dla $i \neq j$ nie są $\mathbb{Q}$-izomorficzne.

Twierdzenie 2.1.9. *Niech S oznacza skończony podzbiór zbioru liczb naturalnych. Wówczas trójka $(a,b,c) \in \bigcup_{i \notin S} \mathcal{C}_i$ reprezentuje krzywą eliptyczną*

$$y^2 = x(x-a^2)(x-b^2)$$

której grupa punktów $\mathbb{Q}$-wymiernych ma rangę co najmniej 2. Istnieją dwa liniowo niezależne punkty nieskończonego rzędu

$$Q_1 = \left(\frac{1}{2}(a+b-c)^2, \frac{1}{2}(a+b)(a+b-c)^2\right),$$

$$Q_2 = \left(\frac{1}{2}a(a-c), \frac{1}{2}ab\frac{1}{k^2}\left(p^4-25q^4\right)\right),$$

gdzie $k = NWD(2pq, p^2+5q^2)$, a p i q są ustalonymi liczbami wymiernymi, które spełniają warunek $\frac{P}{Q} = \frac{2pq}{p^2+5q^2}$ oraz $(a,b,c) = (P^2-Q^2, 2PQ, P^2+Q^2)$.

Dowód. Dowód zostanie podany w paragrafie 2.5.3. □

2.1.2 Określenie powierzchni eliptycznej

W tej części przedstawimy główne wyniki dotyczące obliczania rangi grupy Mordella-Weila dla krzywych eliptycznych nad $\mathbb{Q}(t)$ oraz $\overline{\mathbb{Q}}(t)$. Wprowadzamy pojęcia z geometrii algebraicznej takie jak powierzchnia eliptyczna oraz związane z nią grupa Nérona-Severiego i model Kodairy-Nérona. Korzystamy przy tym z prac [SS10],[Shi90].

Definicja 2.1.10 (Powierzchnia eliptyczna)**.** Niech k będzie ciałem algebraicznie domkniętym. Niech dana będzie gładka krzywa rzutowa C nad ciałem k oraz gładka powierzchnia rzutowa S nad k. *Powierzchnią eliptyczną* nazywamy trójkę (S, C, π), gdzie $\pi : S \to C$ jest surjektywnym morfizmem rozmaitości algebraicznych takim, że:

- istnieje niepusty podzbiór skończony $B \subset C(k)$, taki, że dla $v \in C(k) \setminus B$ włókno $\pi^{-1}(v)$ jest gładką krzywą genusu 1,
- istnieje morfizm $e : C \to S$ taki, że $\pi \circ e = id_C$,
- żadne włókno morfizmu π nie zawiera krzywych wyjątkowych (patrz Definicja 2.2.25).

Definicja 2.1.11. Dla danej powierzchni eliptycznej $\mathcal{E} = (S, C, \pi)$ dowolny morfizm $s : C \to S$ spełniający

$$\pi \circ s = \mathrm{id}_C$$

nazywamy *cięciem* powierzchni eliptycznej $\mathcal{E}$.

Uwaga 2.1.12. Włókno generyczne morfizmu $\pi : S \to C$ nad punktem generycznym η_C jest krzywą gładką genusu 1 nad $k(C)$. W szczególności z istnienia cięcia $e : C \to S$ wynika, że $\pi^{-1}(\eta_C)$ posiada co najmniej jeden punkt $k(C)$-wymierny, czyli jest krzywą eliptyczną nad $k(C)$.

Uwaga 2.1.13. W sytuacjach, gdy nie prowadzi to do nieporozumienia skracamy notację $\mathcal{E} = (S, C, \pi)$ i oznaczamy powierzchnię eliptyczną $\mathcal{E}$ przez S jeśli z kontekstu wiadome jest jak określone są C i π.

Zbiór cięć $\mathcal{P} = \{s : C \to S : \pi \circ s = id_C\}$ powierzchni eliptycznej (S, C, π) posiada naturalnie określoną operację dodawania

$$+ : \mathcal{P} \times \mathcal{P} \to \mathcal{P}.$$

Dla dwóch cięć $s_1, s_2 \in \mathcal{P}$ definiujemy cięcie $s_1 + s_2 : C \to S$ wzorem $(s_1 + s_2)(v) := s_1(v) + s_2(v)$ dla v takiego, że $\pi^{-1}(v)$ jest nieosobliwe. Korzystamy tutaj z faktu, że każde gładkie włókno $\pi^{-1}(v)$ ma naturalnie określoną strukturę krzywej eliptycznej nad k z punktem zerowym zadanym przez $e(v)$, gdzie e jest cięciem, z definicji powierzchni eliptycznej. Z gładkości krzywej C oraz powierzchni S wynika, że odwzorowanie wymierne $s_1 + s_2 : C \to S$ przedłuża się do morfizmu na C. W sytuacjach, gdy cięcie e, podane w definicji powierzchni eliptycznej, zadaje punkt zerowy $e(v)$ w gładkich włóknach $\pi^{-1}(v)$, oznaczać je będziemy również przez O.

2.2 Minimalny model Weierstrassa

W tym paragrafie opiszemy model minimalny równania Weierstrassa dla krzywej eliptycznej. Niech K oznacza cialo z waluacją dyskretną $v : K \to \mathbb{Z} \cup \{\infty\}$. Niech

$$R = \{x \in K : v(x) \geq 0\}$$

będzie pierścieniem lokalnym z ideałem maksymalnym

$$\mathcal{M} = \{x \in K : v(x) > 0\}.$$

Dowolnie ustalony element $\pi \in R$ spełniający $v(\pi) = 1$ nazywamy *elementem uniformizującym* pierścienia R. Ponadto przez k oznaczać będziemy ciało $R/\mathcal{M}$ nazywane odtąd *ciałem reszt* ze względu na waluaję v. Zbiór $R^\times = \{x \in K : v(x) = 0\}$ jest grupą *jedności* pierścienia R. Dodatkowo zakładamy, że ciało k jest *doskonałe*. W większości sytuacji zakładać będziemy, że k jest algebraicznie domknięte.

Niech E/K będzie krzywą eliptyczną o równaniu Weierstrassa

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.3}$$

c_4	$(a_1^2 + 4a_2)^2 - 24(a_1a_3 + 2a_4)$
c_6	$-(a_1^2 + 4a_2)^3 + 36(a_1^2 + 4a_2)(a_1a_3 + 2a_4) - 216(a_3^2 + 4a_6)$
Δ	$(c_4^3 - c_6^2)/1728$
j	c_4^3/Δ

Tabela 2.1: Wielkości stowarzyszone z modelem Weierstrassa

gdzie $a_1, a_2, a_3, a_4, a_6 \in K$. Mówimy, że model Weierstrassa jest *całkowity* jeśli $a_i \in R$ dla wszystkich i. Wprowadzamy oznaczenia, patrz [Tat75].
Łatwo sprawdzić, że Δ należy do pierścienia $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$. Załóżmy, że krzywe eliptyczne E i E' określone nad ciałem K są K-izomorficzne przy izomorfizmie $f : E \xrightarrow{\cong} E'$ i f przekształca punkt 0_E na $0_{E'}$. Niech dane będą modele Weierstrassa

$$\begin{aligned} E &: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \\ E' &: (y')^2 + a_1'x'y' + a_3'y' = (x')^3 + a_2'(x')^2 + a_4'x' + a_6' \end{aligned}$$

tych krzywych. Na mocy [Sil86, III, Proposition 3.1] istnieją elementy $u \in K^\times$, $r, s, t \in K$ spełniające zależność

$$\begin{cases} x' \circ f = u^2x + r, \\ y' \circ f = u^3y + su^2x + t. \end{cases} \tag{2.4}$$

Bezpośrednim rachunkiem można sprawdzić, że wtedy $c_4u^4 = c_4'$, $c_6u^4 = c_6'$, $\Delta u^{12} = \Delta'$ oraz $j = j'$.

Definicja 2.2.1. Mówimy, że model (2.3) Weierstrassa krzywej E nad K jest minimalny ze względu na v jeśli $v(a_i) \geq 0$ oraz waluacja $v(\Delta)$ wyróżnika równania (2.3) jest minimalna, tj. dla dowolnego innego modelu całkowitego krzywej E o współczynnikach $a_i' \in R$ odpowiadający mu wyróżnik Δ' spełnia $v(\Delta') \geq v(\Delta)$.

Twierdzenie 2.2.2 ([Sil86, VII, Proposition 1.3])**.** *Dla dowolnej krzywej eliptycznej E nad ciałem K istnieje model minimalny, który jest jedyny z dokładnością do zamiany zmiennych postaci*

$$x \mapsto u^2x' + r, \quad y \mapsto u^3y' + u^2sx' + t,$$

gdzie $u \in R^\times$, $r, s, t \in R$.

Twierdzenie 2.2.3 ([Sil86, VII, Remark 1.1])**.** *Niech K będzie ciałem charakterystyki różnej od 2 i 3. Wówczas całkowity model Weierstrasa (2.3) krzywej E nad ciałem K jest v-minimalny wtedy i tylko wtedy, gdy $v(c_4) < 4$ lub $v(c_6) < 6$.*

Niech F będzie dowolnym ciałem doskonałym oraz $F(t)$ będzie ciałem funkcji wymiernych o współczynnikach w F. Dla każdego $a \in F$ określamy waluację

$$\begin{aligned} v_a : F(t) &\to \mathbb{Z} \cup \{\infty\} \\ g(t) &\mapsto \operatorname{ord}_{t-a}(g(t)) \\ 0 &\mapsto \infty, \end{aligned} \tag{2.5}$$

gdzie $ord_{t-a}(g(t))$ oznacza rząd zera lub bieguna funkcji $g(t)$ w punkcie a. W naturalny sposób waluacja v_a przedłuża się do waluacji dyskretnej na ciele $K = F((t-a))$ szeregów Laurenta zmiennej $t-a$. Pierścień $R = \{x \in K : v_a(x) \geq 0\}$ jest lokalny z ideałem maksymalnym $(t-a)R$ i elementem uniformizującym $t-a$. Ustalamy naturalne zanurzenie $F(t) \hookrightarrow F((t-a))$ oraz $F[t] \hookrightarrow R$.

Uwaga 2.2.4. Niech dana będzie krzywa eliptyczna E określona nad ciałem $F(t)$ oraz jej model Weierstrassa (2.3) określony nad $F[t]$. Mówimy, że model (2.3) jest v_a-*minimalny* wtedy, gdy jest v_a-minimalny jako model krzywej E nad ciałem $K = F((t-a))$.

Konstrukcja modelu globalnie minimalnego, [SS10, §8.2]: Niech dana będzie powierzchnia eliptyczna $\mathcal{E} = (S, \mathbb{P}^1_F, \pi)$, gdzie F jest pewnym ustalonym ciałem algebraicznie domkniętym. Przeciwobraz $\pi^{-1}(\eta)$ punktu generycznego η w $\mathbb{P}^1_F$ jest krzywą eliptyczną E nad ciałem funkcyjnym $F(\mathbb{P}^1_F)$. W zależności od wyboru funkcji regularnej generującej ciało $F(\mathbb{P}^1_F)$ otrzymamy dwa modele Weierstrassa. Dla $t \in F(\mathbb{P}^1_F)$ takiego, że $t([X:Y]) = X/Y$ otrzymamy model

$$E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_2, a_3, a_4, a_6 \in F(t).$$

Dla funkcji $s \in F(\mathbb{P}^1_F)$ takiej, że $s([X:Y]) = Y/X$ otrzymamy model

$$E_2 : (y')^2 + a'_1x'y' + a'_3y' = x'^3 + a'_2x'^2 + a'_4x' + a'_6, \quad a'_1, a'_2, a'_3, a'_4, a'_6 \in F(s).$$

Jeśli model E_1 ma współczynniki a_i należące do $F[t]$ i są one v_a-minimalne, to niekoniecznie model E_2 musi być całkowity nad $F[s]$. W tym przypadku, aby uzyskać model *globalnie minimalny* postępujemy według następującej procedury.

1. Rozpoczynając od modelu E_1 nad $F(t)$ dokonujemy takiej zamiany zmiennych, aby uzyskać model v_a-minimalny dla wszystkich $a \in F$. Odtąd model E_1 oznaczać będzie model v_a-minimalny dla wszystkich $a \in F$.

2. Zastępując t przez $1/s$ otrzymujemy model E_2 nad $F(s)$, który może nie być minimalny ze względu na waluację stowarzyszoną z s. Dokonujemy zatem zamiany zmiennych $(x, y) \mapsto (x/s^{2n}, y/s^{3n})$ i wybieramy najmniejsze naturalne n takie, że $\deg_t(a_i(t)) \leq ni$ dla $i \in \{1, 2, 3, 4, 6\}$. Otrzymany nowy model będzie miał współczynniki $a'_i(s) = s^{ni}a_i(1/s) \in F[s]$.

3. Sprawdzamy minimalność modelu E_2 ze współczynnikami a'_i ze względu na waluację v_s stowarzyszoną z s.

Jeśli uzyskany model E_1 jest v_a-minimalny dla wszystkich $a \in F$ oraz model E_2 jest v_s-minimalny, to mówimy, że tak wybrany model E_1 jest *globalnie minimalny*.

Uwaga 2.2.5. Pierścień wielomianów $F[t]$ jest dziedziną ideałów głównych, więc dla krzywej eliptycznej E nad $F[t]$ zawsze istnieje model E_1 Weierstrassa, który jest v_a-minimalny dla wszystkich $a \in F$ jednocześnie, patrz [Sil86, VIII,§8]. Ponadto z minimalności wyboru n w punkcie 2. powyższej procedury, wynika, że odpowiadający mu model E_2 nad $F[s]$ jest v_s-minimalny. Zatem dla każdej krzywej E nad $F(t)$ istnieje model globalnie minimalny. Odtąd v_s-minimalność nazywać będziemy *minimalnością w* ∞.

Poniższe twierdzenie zostało sformułowane w [SS10, §8.2] bez dowodu. Przytaczamy własny dowód tego faktu. To twierdzenie wykorzystamy wielokrotnie w dalszej części tekstu przy okazji obliczeń związanych z algorytmem Tate'a. Dzięki Twierdzeniu 2.2.6 można odczytać minimalność modelu Weierstrassa bezpośrednio ze współczynników równania (2.3).

Twierdzenie 2.2.6. *Niech E będzie krzywą eliptyczną określoną nad $F(t)$, gdzie F jest ciałem algebraicznie domkniętym, a t zmienną wolną. Wówczas model Weierstrassa krzywej E o współczynnikach $a_i(t) \in F(t)$ jest globalnie minimalny wtedy i tylko wtedy, gdy istnieje liczba $n \in \mathbb{N}$ taka, że zachodzą warunki*

(i) dla każdego i współczynnik $a_i(t)$ należy do $F[t]$,

(ii) dla każdego i zachodzi nierówność $\deg_t(a_i(t)) \leq ni$,

(iii) istnieje i takie, że $\deg_t(a_i(t)) \geq (n-1)i$,

(iv) dla każdego $a \in F$ istnieje i takie, że $v_a(a_i) < i$.

Dowód. ($\Rightarrow$) Załóżmy, że model krzywej E jest globalnie minimalny. Wówczas na mocy definicji, współczynniki $a_i \in F[t]$ oraz dla każdego $a \in F$ istnieje taki współczynnik a_i, że $v_a(a_i) < i$. W przeciwnym razie dla każdego i oraz pewnego $a \in F$ mielibyśmy $v_a(a_i) \geq i$ i zamiana zmiennych $(x, y) \mapsto (x/(t-a)^2, y/(t-a)^3)$ obniżałaby waluację a_i, zachowując jednocześnie całkowitość współczynników. Ponadto jeśli model jest globalnie minimalny, to jest w szczególności minimalny w ∞. Zatem istnieje taka liczba naturalna $n \in \mathbb{N}$, że $s^{ni}a_i(1/s) \in F[s]$, co jest równoważne z tym, że $\deg_t(a_i) \leq ni$. Ponadto z minimalności w ∞ wynika, że istnieje takie i, że $v_s(a_i'(s)) \leq i$, równoważnie, że $\deg_t(a_i(t)) \geq (n-1)i$. To kończy dowód implikacji.
($\Leftarrow$) Udowodnimy implikację

(*) Jeśli model E nie jest globalnie minimalny, to dla każdego $n \in \mathbb{N}$ zachodzi alternatywa zaprzeczeń warunków (i),(ii),(iii) i (iv).

Niech model E nie będzie globalnie minimalny. Jeśli dla pewnego i zachodzi $a_i \notin F[t]$, to nie zachodzi warunek (i), więc implikacja (*) jest prawdziwa.
Zakładamy odtąd, że (i) jest spełniony. Jeśli dla pewnego $a \in F$ model E nie jest v_a-minimalny to warunek (iv) nie zachodzi i implikacja (*) jest prawdziwa.
Zakładamy odtąd, że zachodzi (i) oraz (iv). Dla $n \in \mathbb{N}$ dostatecznie małych istnieje takie i, że $\deg_t(a_i(t)) > ni$. Wówczas warunek (ii) nie zachodzi i implikacja (*) jest prawdziwa.
Zakładamy odtąd, że n jest dostatecznie duże, więc zachodzą (i), (ii) oraz (iv). Jeśli model E nie jest globalnie minimalny i zachodzi (iv), to E nie może być minimalny w ∞. Ale z warunku (ii) wynika, że współczynniki $a_i'(s) \in F[s]$. Zatem dla wszystkich i zachodzi nierówność $v_s(a_i') > i$, co jest równoważne $ni - \deg_t(a_i(t)) > i$, czyli nie zachodzi warunek (iii), więc implikacja (*) jest prawdziwa. □

Definicja 2.2.7 (Dywizor kanoniczny)**.** Z powierzchnią eliptyczną (S, C, π) nad ciałem k stowarzyszony jest snop różniczek $\Omega_{S/k}$ oraz snop kanoniczny $\omega_S = \bigwedge^2 \Omega_{S/k}$. Dowolny dywizor K w klasie równoważności liniowej, odpowiadający ω_S nazywać będziemy *dywizorem kanonicznym* i oznaczać będziemy przez K_S. Liczba samoprzecięcia K_S^2 zależy tylko od powierzchni S, patrz [Har77, V,Example 1.4.4].

Twierdzenie 2.2.8 ([Har77, V, Remark 1.6.1])**.** *Niech S będzie gładką powierzchnią rzutową nad algebraicznie domkniętym ciałem k. Zachodzi równość*

$$\chi(S) = K_S^2 + c_2(S), \tag{2.6}$$

gdzie $\chi(S) = \chi(S, \mathcal{O}_S)$ oraz $c_2(S)$ jest drugą liczbą Cherna stowarzyszoną z S.

Równość 2.6 nazywać będziemy *formułą Noethera* od nazwiska Maxa Noethera, który jako pierwszy podał jej dowód.

Twierdzenie 2.2.9 ([Shi90, Theorem 2.8])**.** *Niech (S, C, π) będzie powierzchnią eliptyczną. Wówczas $K_S^2 = 0$, więc*

$$\chi(S) = c_2(S).$$

Twierdzenie 2.2.10 ([Ogu90, Theorem 1])**.** *Niech (S, C, π) będzie powierzchnią eliptyczną nad ciałem k takim, że $char(k) \neq 2, 3$. Niech B będzie zbiorem punktów w $C(k)$ złej redukcji oraz $F_v = \pi^{-1}(v)$. Zachodzi równość*

$$c_2(S) = \sum_{v \in B} e(F_v),$$

gdzie liczby $e(F_v)$ zależą od typu Kodairy włókna w następujący sposób.

Typ F_v	$I_n (n \geq 1)$	II	III	IV	$I_n^* (n \geq 0)$	II^*	III^*	IV^*
$e(F_v)$	n	2	3	4	$n+6$	10	9	8

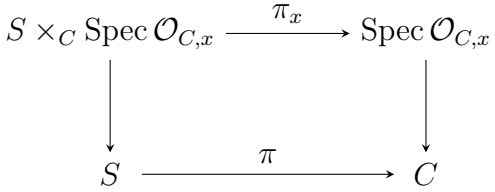
Tabela 2.2: Liczby $e(F_v)$.

Lemat 2.2.11. *Niech K będzie ciałem charakterystyki różnej od 2 i 3. Niech E będzie krzywą eliptyczną nad $K(t)$. Wówczas liczba $\chi(S) = \chi(S, \mathcal{O}_S)$ powierzchni eliptycznej $(S, \mathbb{P}^1_{\overline{K}}, \pi)$ stowarzyszonej z E jest równa liczbie n z Twierdzenia 2.2.6.*

Dowód. Niech dany będzie model globalnie minimalny krzywej E, którego wyróżnik oznaczymy przez Δ. Z formuły Noethera dla powierzchni eliptycznej mamy $12\chi(S) = e(S)$. Z kolei $e(S) = \sum_{v \in B} e(F_v)$, gdzie $e(F_v)$ jest równe 0 dla $F_v = \pi^{-1}(v)$, włókna gładkiego, $e(F_v) = m_v$ dla włókna F_v z redukcją multiplikatywną oraz $e(F_v) = m_v + 1$ dla włókna z redukcją addytywną, co wynika z Twierdzenia 2.2.10 i z Tabeli 2.3. Z drugiej strony, z Tabeli 2.3 odczytujemy, że $v(\Delta) = e(F_v)$. Jeśli n jest liczbą określoną w Twierdzeniu 2.2.6 dla modelu globalnie minimalnego krzywej E, to wówczas $v_\infty(\Delta) = v_s(s^{12n}\Delta(1/s)) = 12n - \deg_t(\Delta(t))$. Ponadto $\sum_{B \setminus \{\infty\}} e(F_v) = \deg_t(\Delta(t))$. Łącząc obie równości otrzymujemy $\sum_{v \in B} e(F_v) = 12n$. Stąd wynika, że $n = \chi(S)$.

□

2.2.1 Algorytm Tate'a



Rysunek 2.1: Lokalizacja powierzchni $S \to C$

Niech dana będzie dowolna powierzchnia eliptyczna $\mathcal{E} = (S, C, \pi)$. Dla punktu domkniętego $x \in C$ możemy rozważyć cofnięcie morfizmu π przez odwzorowanie $\operatorname{Spec} \mathcal{O}_{C,x} \to C$, które istnieje na mocy [Liu02, Example 2.3.16]. W szczególności otrzymujemy diagram przemienny przedstawiony na Rysunku 2.1. Niech S_x oznacza $S \times_C \operatorname{Spec} \mathcal{O}_{C,x}$ oraz $R = \mathcal{O}_{C,x}$. Zachodzi równość $\operatorname{Spec} R = \{\eta, s\}$ i włókno nad η jest krzywą eliptyczną E nad $K(C)$ oraz włókno $\pi_x^{-1}(s)$ nad s jest izomorficzne z włóknem $\pi^{-1}(x)$ nad punktem $x \in C$. Schemat $S_x \to \operatorname{Spec} R$ jest regularny na mocy regularności $S \to C$ oraz rzutowy. Ponadto jest minimalny w tym sensie, że jeśli istnieje schemat $T \to \operatorname{Spec} R$ rzutowy regularny 2-wymiarowy taki, że $S_x \to \operatorname{Spec} R$ faktoryzuje się

$$S_x \to T \to \operatorname{Spec} R$$

oraz włókna generyczne są izomorficzne nad $K(C)$, to S_x jest izomorficzny z T jako $\operatorname{Spec} R$ – schemat. Na mocy [Sil86, Append.C, Thm. 15.2] typ włókna specjalnego można wyznaczyć na podstawie modelu krzywej E nad $K(C)$. Ponadto pierścień R jest pierścieniem z waluacją dyskretną v, [Har77, I Thm. 5.1, I Thm.6.2 A]. Ciało ułamków $\operatorname{Frac} R = K(C)$. Jeśli model Weierstrassa krzywej E jest v-minimalny to Tabela 2.3 określa wszystkie możliwe postaci włókna specjalnego nad s.

W szczególności dla włókna osobliwego $F_v = \pi^{-1}(s)$ jego typ $S(F_v)$ jest określony w Tabeli 2.4. Niech m_v oznacza liczbę składowych nierozkładalnych w zadanym włóknie F_v. Każda składowa jest izomorficzna z $\mathbb{P}^1_k$. Przedstawione tu konfiguracje włókien dotyczą wyłącznie sytuacji, gdy $\operatorname{char} k \neq 2, 3$ oraz k jest algebraicznie domknięte. Ponadto $v(\Delta)$ jest wyróżnikiem modelu v-minimalnego krzywej E oraz $v(j)$ jest j-niezmiennikiem dla tego samego modelu. Na mocy algorytmu Tate'a [Tat75, §0, §6, §7, §8] typ włókna osobliwego można odczytać z modelu v-minimalnego znając $v(\Delta)$ oraz $v(j)$.

Maksymalny w sensie inkluzji otwarty podschemat $\mathcal{N}$ w S_x jest schematem grupowym nad $\operatorname{Spec} R$. Ponadto $\mathcal{N}$ jest modelem Nérona dla $E/K(C)$ co wynika z [Sil94, IV,§9]. W szczególności włókno specjalne $\widetilde{\mathcal{N}} = \mathcal{N} \times_R k$ jest grupą algebraiczną nad k, gdzie $k = R/m_R$ jest ciałem reszt. Składowa identyczności w $\widetilde{\mathcal{N}}$ oznaczana będzie przez $\widetilde{\mathcal{N}}^0$. Jeśli F_v jest włóknem specjalnym morfizmu $S_x \to \operatorname{Spec} R$, to *grupą składowych* włókna F_v nazywać będziemy grupę

$$G(F_v) = \widetilde{\mathcal{N}}(k)/\widetilde{\mathcal{N}}^0(k). \tag{2.7}$$

$\mathbf{S}(\mathbf{F_v})$	I_0	$I_n(n \geq 1)$	II	III	IV	I_0^*	$I_n^*(n \geq 1)$	IV^*	III^*	II^*
$\mathbf{m_v}$	1	n	1	2	3	5	$5+n$	7	8	9
$\mathbf{G}(\mathbf{F_v})$	$\{0\}$	$\mathbb{Z}/n\mathbb{Z}$	$\{0\}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$(\mathbb{Z}/2\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2$, gdy $2 \mid n$, $\mathbb{Z}/4\mathbb{Z}$, gdy $2 \nmid n$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\{0\}$
$\mathbf{v}(\boldsymbol{\Delta})$	0	n	2	3	4	6	$6+n$	8	9	10
$\mathbf{v}(\mathbf{j})$	≥ 0	$= -n$	≥ 0	$= 0$	≥ 0	≥ 0	$= -n$	≥ 0	$= 0$	≥ 0

Tabela 2.3: Typy włókien specjalnych, char $k \neq 2, 3$, $k = \overline{k}$

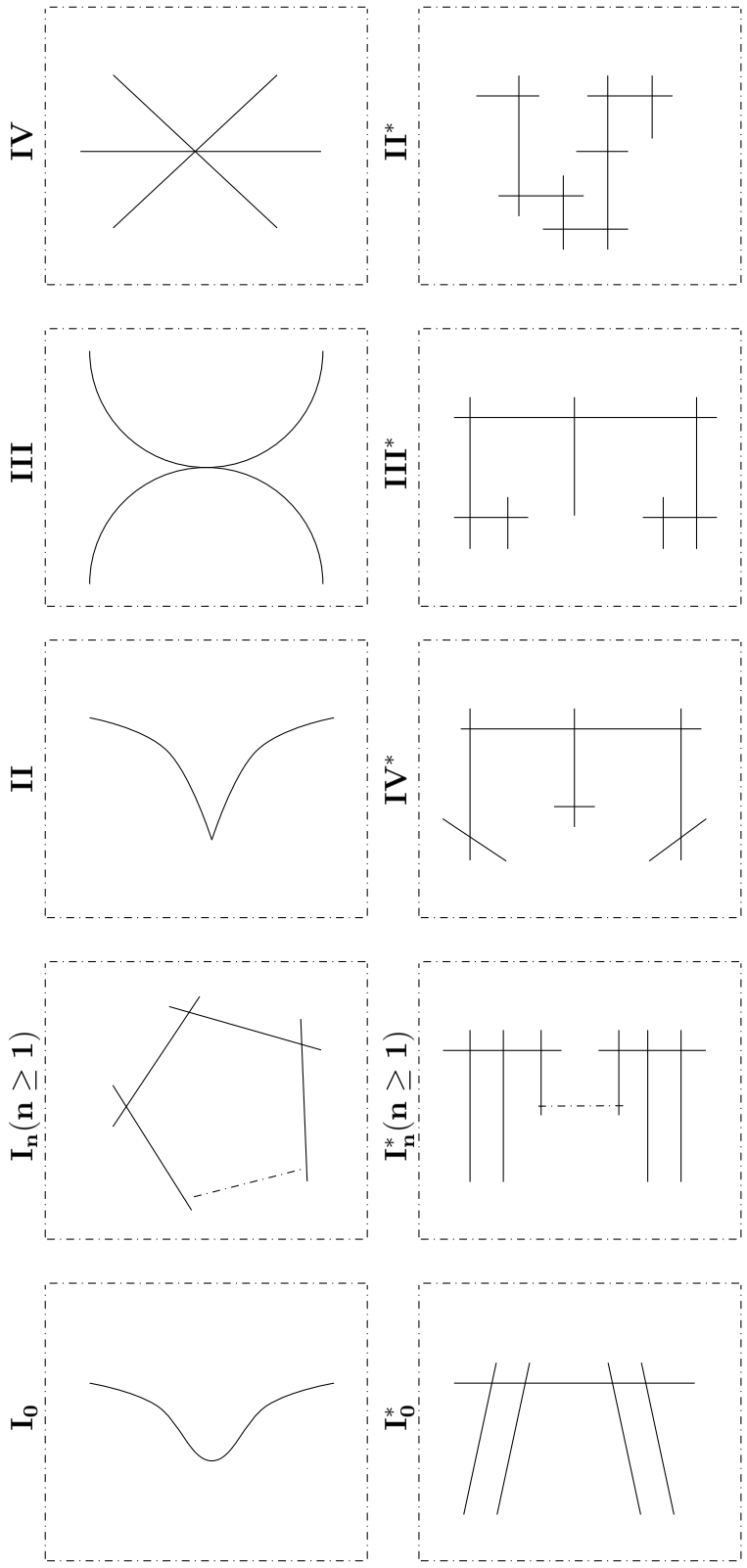


Tabela 2.4: Konfiguracja włókien specjalnych

2.2.2 Twierdzenie o dobrej redukcji

Niech R będzie pierścieniem z zadaną waluacją dyskretną. Niech π będzie elementem uniformizującym względem waluacji na R i niech $k = R/\pi R$ będzie ciałem reszt. Wówczas $\operatorname{Spec} R = \{\eta, s\}$ składa się z dwóch punktów. Punkt $\eta = (0)$ jest otwarty i w jego domknięciu leży punkt $s = (\pi)$. Niech dana będzie powierzchnia eliptyczna $(S, \mathbb{P}^1_{\overline{K}}, \pi)$, gdzie $\overline{K}$ jest domknięciem algebraicznym ciała ułamków $K = \operatorname{Frac} R$. Mówimy, że S ma *model nad* R jeśli istnieje schemat $\mathcal{S} \to \operatorname{Spec} R$ gładki rzutowy relatywnego wymiaru 2, dla którego włókno generyczne $\mathcal{S}_\eta$ jest izomorficzne nad $\overline{K}$ z powierzchnią S. Ponadto jeśli istnieje faktoryzacja

$$\mathcal{S} \to \mathbb{P}^1_R \to \operatorname{Spec} R$$

oraz

$$\pi_{\overline{K}} : \mathcal{S}_\eta \times \operatorname{Spec} \overline{K} \to \mathbb{P}^1_{\overline{K}}$$
$$\mathcal{S}_s \times \operatorname{Spec} \overline{k} \to \mathbb{P}^1_{\overline{k}}$$

zadają powierzchnie eliptyczne nad $\overline{K}$ oraz $\overline{k}$, odpowiednio, a także $\pi_{\overline{K}} = \pi$, to mówimy, że $\mathcal{S} \to \operatorname{Spec} R$ ma *dobrą redukcję w* s.

Dla wielomianu $F \in \mathbb{Z}[t]$ oznaczamy przez $c(F)$ największy wspólny dzielnik wszystkich współczynników wielomianu F. Ponadto dla $F \in \mathbb{Z}[t]$ niech F_0 oznacza wielomian unormowany w $\mathbb{Z}[t]$ spełniający równość $F = c(F)F_0$. Niech $bk(F) \in \mathbb{Z}[t]$ oznacza maksymalny ze względu na stopień bezkwadratowy dzielnik wielomianu F. W szczególności zbiory zer wielomianów $bk(F)$ i F w $\overline{\mathbb{Q}}$ są równe. Ponadto niech $d(F)$ oznacza wyróżnik wielomianu F.

Twierdzenie 2.2.12. *Niech E będzie krzywą eliptyczną nad $\mathbb{Q}(t)$, która posiada model Weierstrassa*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.8}$$

globalnie minimalny nad $\mathbb{Q}(t)$ oraz taki, że $a_i \in \mathbb{Z}[t]$. Niech $\Delta \in \mathbb{Z}[t]$ będzie wyróżnikiem tego równania oraz $j \in \mathbb{Q}(t)$ jego j-niezmiennikiem. Ponadto niech $f, g \in \mathbb{Z}[t]$ będą względnie pierwsze oraz $j = f/g$. Niech p będzie liczbą pierwszą $p > 5$, która spełnia

$$p \nmid d(h)$$

dla każdego h ze zbioru

$$\{bk(a_1), bk(a_2), bk(a_3), bk(a_4), bk(a_6), bk(\Delta), bk(f), bk(g)\}.$$

Załóżmy, że redukcja modulo p współczynników a_i z równania Weierstrassa dla E zadaje krzywą eliptyczną $\widetilde{E}$. Niech model Weierstrassa zadany współczynnikami $\widetilde{a}_i \in \mathbb{F}_p[t]$ będzie minimalny oraz dla każdego $h \in \{bk(\Delta), bk(f), bk(g)\}$ niech wielomian $\widetilde{h} \in \mathbb{F}_p[t]$ będzie rozdzielczy. Wówczas istnieje gładki rzutowy schemat $S \to \mathbb{Z}_{(p)}$ relatywnego wymiaru 2 spełniający następujące warunki

- *włókno $S_{\mathbb{Q}}$ zadaje powierzchnię eliptyczną $((S_{\mathbb{Q}})_{\overline{\mathbb{Q}}}, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi_1)$, której włóknem generycznym jest E nad $\overline{\mathbb{Q}}(t)$.*

- *włókno $S_{\mathbb{F}_p}$ zadaje powierzchnię eliptyczną $((S_{\mathbb{F}_p})_{\overline{\mathbb{F}_p}}, \mathbb{P}^1_{\overline{\mathbb{F}_p}}, \pi_2)$, której włóknem generycznym jest $\widetilde{E}$ nad $\overline{\mathbb{F}_p}(t)$.*

Dowód. Niech K oznacza ciało rozkładu wielomianów $a_i(t)$, $\Delta(t)$, $f(t)$ oraz $g(t)$. W pierścieniu liczb całkowitych $\mathcal{O}_K$ ciała K ustalamy ideał pierwszy $\mathfrak{p}$ dzielący p. Zadany jest homomorfizm redukcji $\phi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$. Warunki narzucone na liczbę pierwszą p wraz z algorytmem Tate'a pociągają, że otrzymamy te same typy włókien złej redukcji nad punktami a oraz $\phi(a)$, gdzie a jest pierwiastkiem $\Delta_0(t)$. W szczególności krzywa E i krzywa $\widetilde{E}$ są włóknami generycznymi powierzchni eliptycznych o tej samej konfiguracji włókien osobliwych. Niech $W \to \mathbb{P}^1_{\mathbb{Z}_{(p)}}$ będzie schematem, który uzyskujemy z równania (2.8) przez domknięcie rzutowe i wybór tej składowej, która zawiera afiniczny schemat zadany równaniem (2.8). Włókno $W_0 \to \mathbb{P}^1_{\mathbb{Q}}$ zadaje powierzchnię, która nad $\overline{\mathbb{Q}}$ posiada tylko osobliwości wymierne, czyli izolowane punkty podwójne, por. [CD89, Proposition 5.5.7]. Podobnie włókno w charakterystyce p, tzn. $W_p \to \mathbb{P}^1_{\mathbb{F}_p}$ zadaje powierzchnię, która nad $\overline{\mathbb{F}_p}$ ma również tylko osobliwości wymierne. Z klasyfikacji typów osobliwości wymiernych na powierzchniach nad algebraicznie domkniętym ciałem charakterystyki 0 lub $p > 5$ wynika, że rozwiązywanie tych osobliwości odbywa się identycznie we wszystkich charakterystykach i nie zależy od ich wyboru, por. [CD89, Proposition 0.2.6]. Efektywny sposób znalezienia rozwiązania osobliwości stanowi algorytm Tate'a, por. [Sil94, §9, IV]. Poczynione założenia gwarantują nam, że rozwiązanie osobliwości dla W_p i W_0 z wykorzystaniem algorytmu Tate'a da te same typy włókien Kodairy, więc również te same typy osobliwości wymiernych. Oznacza to, że istnieje gładki rzutowy schemat $S \to \mathbb{P}^1_{\mathbb{Z}_{(p)}}$ taki, że $S \to W$ stanowi rozwiązanie osobliwości. Ponadto włókno $S_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ zadaje powierzchnię eliptyczną nad $\overline{\mathbb{Q}}$. Analogicznie włókno $S_{\mathbb{F}_p} \to \mathbb{P}^1_{\mathbb{F}_p}$ zadaje powierzchnię eliptyczną nad $\overline{\mathbb{F}_p}$. □

Uwaga 2.2.13. Na mocy podanych wyżej definicji schemat $S \to \mathbb{Z}_{(p)}$ zadaje model nad $\mathbb{Z}_{(p)}$ powierzchni eliptycznej, której włóknem generycznym jest E. Ponadto warunki twierdzenia narzucają, że p jest liczbą pierwszą dobrej redukcji.

Uwaga 2.2.14. Szczególny przypadek Twierdzenia 2.2.12 jest zawarty w [vL07, Proposition 7.1]. Ze względu na specyfikę zastosowań autor przeprowadza w loc. cit. rozumowanie tylko dla włókien osobliwych z redukcją typu I_n.

2.2.3 Model Kodairy-Nérona

Opiszemy teraz w skrócie konstrukcję, która pozwala na przypisanie dowolnej krzywej eliptycznej E, nad ciałem funkcyjnym $k(C)$ ustalonej gładkiej krzywej rzutowej C nad algebraicznie domkniętym ciałem k, powierzchni eliptycznej (S, C, π), która spełnia $\pi^{-1}(\eta_C) = E$.

Niech dana będzie krzywa eliptyczna E nad ciałem funkcyjnym $k(C)$ pewnej gładkiej krzywej rzutowej C nad ciałem $k = \overline{k}$. Model Weierstrassa (2.3) krzywej E zadaje schemat $\mathcal{E} \to C^0$, gdzie C^0 jest krzywą C z wyrzuconymi punktami domkniętymi, w których funkcje $a_i \in k(C)$ mają bieguny. Schemat $\mathcal{E}$ jest otwartym podschematem w $\mathbb{P}^2 \times C$. Biorąc jego domknięcie w sensie Zariskiego w $\mathbb{P}^2 \times C$,

otrzymamy powierzchnię rzutową $\mathcal{E}^{cl}$. Włókna powierzchni $\mathcal{E}^{cl}$ nad punktami z C^0 są gładkimi krzywymi genusu 1. Ponadto istnieje cięcie zerowe jak w Definicji 2.1.10

$$O : C \to \mathcal{E}^{cl}.$$

Powierzchnia $\mathcal{E}^{cl}$ może nie być relatywnie minimalna, więc stosując algorytm Tate'a dla włókien osobliwych dokonujemy minimalnego rozdmuchania punktów osobliwych we włóknach specjalnych. Po skończonej liczbie kroków otrzymamy model $\mathcal{E}'$ biwymiernie równoważny powierzchni $\mathcal{E}^{cl}$, który jest relatywnie minimalny.

Definicja 2.2.15. Model $\mathcal{E}'$ nazywać będziemy *modelem Kodairy-Nérona* stowarzyszonym z krzywą E.

Definicja 2.2.16 (Grupa Nérona-Severiego)**.** Niech V będzie zupełną, geometrycznie nierozkładalną rozmaitością algebraiczną nad ciałem k. Wówczas grupę dywizorów $Div(V)$ podzieloną przez relację algebraicznej równoważności dywizorów nazywamy grupą Nérona-Severiego rozmaitości V i oznaczamy $NS(V_{\overline{k}})$.

W przypadku powierzchni eliptycznych relację algebraicznej równoważności dywizorów można zastąpić relacją numerycznej równoważności dywizorów (Shioda, [Shi90]). Przytaczamy poniżej twierdzenie o skończonej generowalości grupy Nérona-Severiego.

Twierdzenie 2.2.17 ([Shi90],Corollary 3.2)**.** *Niech (S, C, π) będzie powierzchnią eliptyczną. Wówczas grupa Nérona-Severiego $NS(S)$ jest skończenie generowana i beztorsyjna.*

Dla powierzchni eliptycznej $\mathcal{E} = (S, C, \pi)$ rangę grupy $NS(S)$ oznaczymy przez $\rho(S)$ i nazywać będziemy *liczbą Picarda*. Jeśli będzie wynikać to jednoznacznie z kontekstu, to napiszemy $\rho(\mathcal{E})$ zamiast $\rho(S)$ i podobnie $NS(\mathcal{E})$ zamiast $NS(S)$.

Twierdzenie 2.2.18 (Formuła Shiody-Tate'a, [Shi90, Corollary 5.3])**.** *Niech (S, C, π) będzie powierzchnią eliptyczną. Niech B oznacza zbiór punktów domkniętych v, dla których włókno $\pi^{-1}(v)$ jest osobliwe. Przez m_v oznaczamy liczbę składowych nierozkładalnych włókna $\pi^{-1}(v)$. Niech ponadto E będzie krzywą eliptyczną zadaną przez włókno $\pi^{-1}(\eta_C)$ nad punktem generycznym η_C krzywej C. Wówczas*

$$\rho(S) = 2 + \sum_{v \in B} (m_v - 1) + ranga\, E(k(C)).$$

Twierdzenie 2.2.19 (Szacowanie liczby Picarda)**.** *Niech k będzie ciałem algebraicznie domkniętym, a (S, C, π) niech będzie powierzchnią eliptyczną nad k. Niech ponadto $\chi = \chi(S, \mathcal{O}_S)$ oraz $g = genus(C)$. Zachodzą następujące oszacowania na liczbę $\rho(S)$.*

(i) Jeśli char $k \geq 0$, to $\rho(S) \leq 12\chi - 2 + 4g$.

(ii) Jeśli char $k = 0$, to $\rho(S) \leq 10\chi + 2g$.

Dowód. Niech $b_i(X)$ oznacza i-tą liczbę Bettiego rozmaitości X rozumianą jako $\dim_{\mathbb{C}} H^i(X,\mathbb{C})$ w charakterystyce zero i jako $\dim_{\mathbb{Q}_\ell} H^i_{\text{et}}(X,\mathbb{Q}_\ell)$, gdy $\operatorname{char} k \neq \ell$. Na mocy [CD89, Corollary 5.2.2] zachodzi równość $b_1(S) = b_1(C)$. Na mocy formuły Noethera oraz [CD89, Proposition 5.1.6] dostajemy, że $12\chi = e(S)$, gdzie $e(S) = \sum_{i=0}^{i=4}(-1)^i b_i(S)$. Dualność Poincaré dla kohomologii singularnych i ℓ-adycznych daje (patrz [Har77, Appendix C.3.4])

$$b_2(S) = e(S) - 2(1 - b_1(C)).$$

Ponadto $b_1(C) = 2g$: gdy $\operatorname{char} k > 0$, patrz [Del77, Arcata, Corollary 3.5]; gdy $\operatorname{char} k = 0$ krzywa C może być zrealizowana jako krzywa nad $\mathbb{C}$ i jest zwartą domkniętą powierzchnią orientowalną nad $\mathbb{R}$, wiec stosujemy [Hat02, Example 3.3.1]. Łącząc fakty otrzymujemy

$$b_2(S) = 12\chi - 2 + 4g. \tag{2.9}$$

Ponadto na mocy [Shi90, Theorem 2.1] wiemy, że $\rho(S) \leq b_2(S)$. Stąd wynika oszacowanie podane w (i).

Jeśli $\operatorname{char} k = 0$, to powierzchnię S możemy traktować jako określoną nad $\mathbb{C}$. Niech $h^{p,q} = \dim_{\mathbb{C}} H^q(X, \Omega^p_{X/\mathbb{C}})$. Przestrzeń rzutowa $\mathbb{P}^n_{\mathbb{C}}$ posiada metrykę Fubiniego-Study, która jest metryką Kählera. Jeśli S jest podrozmaitością analityczną w pewnej przestrzeni rzutowej $\mathbb{P}^n_{\mathbb{C}}$, to obcięcie metryki Fubiniego-Study do rozmaitości S zadaje metrykę Kählera na S, patrz [Huy05, Example 3.1.9] oraz [Huy05, Proposition 3.1.10]. W takim przypadku istnieje rozkład Hodge'a dla rozmaitości S (por. [Huy05, Corollary 3.2.12])

$$H^k(S,\mathbb{C}) = \bigoplus_{p+q=k} H^q(S, \Omega^p_{S/\mathbb{C}}).$$

Ponadto istnienie metryki Kählera implikuje, że $h^{p,q} = h^{q,p}$ oraz dualność Serre'a pociąga, że $h^{p,q} = h^{2-p,2-q}$, patrz [Huy05, Corollary 3.2.12]. Formuła Noethera implikuje, że $12\chi(S) = c_2(S)$, ale [Huy05, §5.1] pociąga, że $e(S) = c_2(S)$, gdzie $e(S) = b_0 - b_1 + b_2 - b_3 + b_4$. Ponadto z dualności Poincaré otrzymujemy, że $b_{4-i} = b_i$. Rozmaitość S jest zwarta i spójna, więc $b_0 = 1$. Zatem zachodzi równość

$$12\chi(S) = 2 - 2b_1 + b_2. \tag{2.10}$$

Na mocy rozkładu Hodge'a mamy również $b_2 = h^{2,0} + h^{1,1} + h^{0,2}$. Z podanych własności liczb $h^{p,q}$ otrzymujemy

$$b_2 = 2h^{0,2} + h^{1,1}. \tag{2.11}$$

Z pierwszej części dowodu wiemy, że $b_1(S) = 2g$, zatem równość (2.10) można przekształcić do postaci

$$b_2 = 12\chi(S) - 2 + 4g. \tag{2.12}$$

Ponadto z definicji

$$\chi(S) = \dim_{\mathbb{C}} H^0(X,\mathcal{O}_S) - \dim_{\mathbb{C}} H^1(X,\mathcal{O}_S) + \dim_{\mathbb{C}} H^2(X,\mathcal{O}_S) = h^{0,0} - h^{0,1} + h^{0,2}.$$

Powierzchnia S jest rzutowa, więc $h^{0,0} = 1$. Ponownie stosując rozkład Hodge'a otrzymamy $b_1 = 2h^{0,1}$, a więc również $g = h^{0,1}$. Ostatecznie

$$h^{0,2} = \chi(S) - 1 + g. \tag{2.13}$$

Przyrównując (2.12) i (2.11) z (2.13) otrzymujemy

$$h^{1,1} = 10\chi(S) + 2g. \tag{2.14}$$

Krótki ciąg dokładny snopów na S

$$0 \to \mathbb{Z} \to \mathcal{O}_S \xrightarrow{exp} \mathcal{O}_S^{\times} \to 1$$

indukuje długi ciąg dokładny kohomologii

$$\ldots \to H^1(S, \mathbb{Z}) \to H^1(S, \mathcal{O}_S) \to H^1(S, \mathcal{O}_S^{\times}) \xrightarrow{\delta} H^2(S, \mathbb{Z}) \to \ldots.$$

Zachodzą równości $Pic(S) = H^1(S, \mathcal{O}_S^{\times})$ oraz $NS(S) = Pic(S)/\ker\delta$. Inkluzja snopów $\mathbb{Z} \subset \mathbb{C}$ nad S indukuje odwzorowanie $H^2(S, \mathbb{Z}) \to H^2(S, \mathbb{C})$. Obraz złożenia

$$Pic(S) \xrightarrow{\delta} H^2(S, \mathbb{Z}) \to H^2(S, \mathbb{C})$$

jest zawarty w

$$H^{1,1}(S, \mathbb{Z}) := Im(H^2(S, \mathbb{Z}) \to H^2(S, \mathbb{C})) \cap H^{1,1}(S).$$

Indukowane odwzorowanie $Pic(S) \to H^{1,1}(S, \mathbb{Z})$ jest surjektywne. Własność ta nazywana jest twierdzeniem o (1,1)-klasach Lefschetza, por. [Huy05, Proposition 3.3.2]. W szczególności implikuje ono, że $ranga\, NS(S) = ranga\, H^{1,1}(S, \mathbb{Z})$. Otrzymujemy ograniczenie $\rho(S) \leq h^{1,1}$, które w połączeniu z równością (2.14) daje tezę (ii). □

2.2.4 Iloczyn przecięcia i wysokość punktów

Niech $\mathcal{E} = (S, C, \pi)$ będzie dowolną powierzchnią eliptyczną. Grupa NS(S) jest skończenie generowana i beztorsyjna. Dla dwóch nierozkładalnych krzywych $C_1, C_2 \subset S$ określamy iloczyn przecięcia

$$C_1 \cdot C_2 = \sharp\{p \in S(k) : p \in C_1(k) \cap C_2(k)\}$$

przy założeniu, że C_1 i C_2 przecinają się transwersalnie w każdym punkcie. Istnieje dokładnie jedno odwzorowanie dwuliniowe symetryczne

$$(\ ,\ ) : \mathrm{Div}(S) \times \mathrm{Div}(S) \to \mathbb{Z}, \tag{2.15}$$

które spełnia $(C_1, C_2) = C_1 \cdot C_2$ dla krzywych C_1, C_2 przecinających się transwersalnie. Ponadto dla dwóch dywizorów liniowo równoważnych $D \sim D'$ zachodzi równość $(D, D'') = (D', D'')$ dla dowolnego dywizora $D'' \in \mathrm{Div}(S)$, [Sil94, III,§7 Theorem 7.2]. Indukuje to odwzorowanie dwuliniowe $(\ ,\ )$ na grupie NS(S). W szczególności, na mocy [Shi90, Theorem 3.1], odwzorowanie dwuliniowe na

$\mathrm{NS}(S)$ jest również niezdegenerowane. Para $(\mathrm{NS}(S), (\ ,\ ))$ jest więc kratą, tj. $\mathrm{NS}(S)$ jest wolnym $\mathbb{Z}$-modułem skończonej rangi z zadanym odwzorowaniem $(\ ,\ ) : \mathrm{NS}(S) \times \mathrm{NS}(S) \to \mathbb{Q}$, które jest dwuliniowe, symetryczne i niezdegenerowane. Odwzorowanie $(\ ,\ )$ nazywać będziemy *iloczynem przecięcia* lub *formą przecięcia*.

W kracie $\mathrm{NS}(S)$ wyróżniamy podkratę $T(S)$ generowaną przez obraz cięcia zerowego O, przez dowolne włókno F oraz przez składowe włókien osobliwych $\Theta_{v,i}$ dla $v \in B$ oraz $i \in \{1, m_v - 1\}$. Przypominamy, że $B \subset C(k)$ oznacza zbiór punktów, nad którymi włókna względem π są osobliwe. Definiujemy kratę $L(S)$ jako dopełnienie ortogonalne do $T(S)$,

$$L(S) = T(S)^{\perp} = \{x \in \mathrm{NS}(S) : (x, y) = 0 \text{ dla } y \in T(S)\}.$$

Krata $L(S)$ wyznacza odwzorowanie przestrzeni liniowych nad $\mathbb{Q}$

$$\phi : \mathrm{NS}(S)_{\mathbb{Q}} \to L(S)_{\mathbb{Q}},$$

gdzie $\mathrm{NS}(S)_{\mathbb{Q}} := \mathrm{NS}(S) \otimes_{\mathbb{Z}} \mathbb{Q}$ oraz $L(S)_{\mathbb{Q}} := L(S) \otimes_{\mathbb{Z}} \mathbb{Q}$. Odwzorowanie ϕ jest projekcją ortogonalną ze względu na podprzestrzeń $T(S)_{\mathbb{Q}}$. Ponadto jeśli E jest włóknem generycznym morfizmu π nad $K = K(C)$, to mamy izomorfizm grup

$$\begin{aligned} E(K) &\cong \mathrm{NS}(S)/T(S) \\ P &\mapsto \overline{P} + T(S), \end{aligned}$$

gdzie $\overline{P}$ jest obrazem cięcia wyznaczonego przez punkt P na włóknie E, por. [Shi90, Lemma 5.2]. Z tego wynika, że odwzorowanie ϕ indukuje odwzorowanie z $E(K)$ do $L(S)_{\mathbb{Q}}$.

Definicja 2.2.20. Niech $E(K)$ będzie określone jak wyżej. Dla dwóch punktów $P, Q \in E(K)$ definiujemy ich *iloczyn skalarny*

$$\langle P, Q \rangle = -(\phi(P), \phi(Q)).$$

Przez *wysokość punktu* P rozumieć będziemy liczbę $\langle P, P \rangle$.

Z definicji wynika, że wartość $\langle P, Q \rangle$ jest liczbą wymierną. Krata $(L(S), (\ ,\ ))$ jest ujemnie określona na mocy [Shi90, Theorem 7.4], więc $\langle P, Q \rangle \geq 0$ dla dowolnych $P, Q \in E(K)$. Ponadto iloczyn $\langle P, Q \rangle$ jest efektywnie obliczalny o ile znamy typy włókien złej redukcji przy zadanym morfizmie $\pi : S \to C$ oraz wiemy, które składowe włókien przecinają krzywe $\overline{P}$ i $\overline{Q}$, [Shi90, Lemma 8.1] oraz [Shi90, Theorem 8.6]. Określamy podgrupę w $E(K)$

$$E_0(K) = \{R \in E(K) : \overline{R} \text{ przecina składową } \Theta_{v,0} \text{ włókna nad } v \in C(k)\},$$

gdzie $\Theta_{v,0}$ jest składową, którą przecina obraz cięcia zerowego dla każdego włókna $v \in C(k)$.

Stwierdzenie 2.2.21 ([Shi90, Thm.8.6])**.** *Niech E będzie krzywą eliptyczną nad ciałem K zdefiniowaną jak wyżej. Wówczas dla punktów $P, Q \in E(K)$ mamy równość*

$$\langle P, Q\rangle = \chi(S) + \overline{P}.\overline{O} + \overline{Q}.\overline{O} - \overline{P}.\overline{Q} - \sum_{v\in B} c_v(P, Q).$$

Liczby $c_v(P, Q) \in \mathbb{Q}$ są wyznaczone na podstawie konfiguracji włókna nad punktem v oraz informacji o tym jak krzywe $\overline{P}$ i $\overline{Q}$ przecinają poszczególne składowe włókna nad v. Ponadto jeśli $P \in E(K)_{tors}$, to $\langle P, Q\rangle = 0$ dla dowolnego $Q \in E(K)$.
Jeśli $P \in E_0(K)$, $Q \in E(K)$, to wówczas

$$\langle P, Q\rangle = \chi(S) + \overline{P}.\overline{O} + \overline{Q}.\overline{O} - \overline{P}.\overline{Q},$$

$$\langle P, P\rangle = 2\chi(S) + 2\overline{P}.\overline{O}.$$

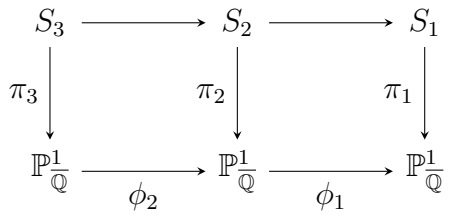
Dowód. Jawny wzór na liczby c_v jest podany w dowodzie [Shi90, Theorem 8.6]. Ponadto, gdy $P \in E(K)_{\text{tors}}$ jest punktem torsyjnym, to na mocy [Shi90, Lemma 8.2] otrzymujemy $\langle P, Q\rangle = 0$ dla dowolnego $Q \in E(K)$. Ostatnie dwie własności wynikają bezpośrednio z definicji podgrupy $E_0(K)$ oraz z faktu, że liczby $c_v(P, Q)$ są zerami wtedy, gdy jedna z krzywych $\overline{P}$ lub $\overline{Q}$ przecina w każdym włóknie składową krzywej $\overline{O}$ wyznaczonej przez cięcie zerowe $O : C \to S$. Ponadto zachodzi wzór $\overline{P}.\overline{P} = -\chi(S)$, patrz [Shi90, Theorem 2.8]. □

Gdy P należy do $E(K)$, to $\langle P, P\rangle = 0$ wtedy i tylko wtedy, gdy $P \in E(K)_{tors}$, por. [Shi90, Theorem 8.4]. Grupa ilorazowa $E(K)/E(K)_{tors}$ wraz z iloczynem $\langle , \rangle_E$ indukowanym z $\langle , \rangle$ na $E(K)$ jest dodatnio określoną kratą. Parę $(E(K)/E(K)_{tors}, \langle , \rangle_E)$ nazywać będziemy *kratą Mordella-Weila.*
Poniższy lemat można odnaleźć w [SS10, Corollary 7.5]. Przedstawiamy dowód tego faktu.

Lemat 2.2.22. *Niech E będzie krzywą eliptyczną nad $\overline{\mathbb{Q}}(t)$, która jest włóknem generycznym powierzchni eliptycznej $\mathcal{E} = (S, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi)$. Niech $B \subset \mathbb{P}^1_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}})$ oznacza zbiór miejsc złej redukcji dla π oraz $F_v = \pi^{-1}(v)$. Niech $G(F_v)$ oznacza grupę określoną w równości (2.7). Wówczas istnieje monomorfizm*

$$\phi : E(\overline{\mathbb{Q}}(t))_{tors} \to \prod_{v\in B} G(F_v).$$

Dowód. Niech $K = \overline{\mathbb{Q}}(t)$. Definiujemy odwzorowanie ϕ, które dla każdego $v \in B$ przyporządkowuje punktowi $P \in E(K)$ element z $G(F_v)$ odpowiadający składowej włókna F_v przecinającej cięcie $\overline{P}$. Odwzorowanie ϕ jest homomorfizmem, [Sil94, Propostion 6.10]. Niech teraz P oraz Q będą punktami z $E(K)_{\text{tors}}$, które spełniają $\phi(P) = \phi(Q)$. Oznacza to, że cięcia $\overline{P}$ oraz $\overline{Q}$ dla każdego v przecinają tę samą składową włókna F_v. W szczególności $c_v(P, Q) = c_v(P, P) = c_v(Q, Q)$. Ponadto na mocy Stwierdzenia 2.2.21 mamy $\langle P, Q\rangle = \langle P, P\rangle = \langle Q, Q\rangle = 0$. Jeśli $\chi = \chi(S)$, to na mocy poprzedniej równości oraz Stwierdzenia 2.2.21 otrzymujemy $\overline{P}.\overline{O} = \overline{Q}.\overline{O}$ oraz $\overline{P}.\overline{Q} = -\chi$. Dla powierzchni eliptycznej $\mathcal{E}$ zachodzi $\chi > 0$, natomiast dywizory $\overline{P}, \overline{Q}$ są nierozkładalnymi krzywymi. Gdy $\overline{P} \neq \overline{Q}$, to $\overline{P}.\overline{Q} \geq 0$. Zatem $\overline{P} = \overline{Q}$, czyli $P = Q$. □



Rysunek 2.2: Zamiana bazy dla powierzchni S_1, S_2 i S_3

Uwaga 2.2.23. Z Definicji 2.1.10 wynika, że zbiór B z Lematu 2.2.22 jest skończony, więc na mocy Tabeli 2.3 iloczyn $\prod_{v\in B} G(F_v)$ jest grupą skończoną. Z istnienia monomorfizmu ϕ wynika, że grupa $E(\overline{\mathbb{Q}}(t))_{\text{tors}}$ jest skończona.

2.2.5 Powierzchnie eliptyczne nad $\mathbb{P}^1$

Rozważymy kilka powierzchni eliptycznych zdefiniowanych nad prostą rzutową $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ nad ciałem liczb algebraicznych $\overline{\mathbb{Q}}$. Określamy morfizmy:

$$\phi_1 : \mathbb{P}^1_{\overline{\mathbb{Q}}} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}, \quad \phi_1(t) = t^2,$$
$$\phi_2 : \mathbb{P}^1_{\overline{\mathbb{Q}}} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}, \quad \phi_2(t) = \frac{2t}{5+t^2}.$$

Stwierdzenie 2.2.24. *Morfizmy ϕ_1 i ϕ_2 mają stopień dwa. Morfizm ϕ_1 jest rozgałęziony w punktach $\{1, \infty\}$. Morfizm ϕ_1 jest rozgałęziony w punktach $\{\pm\frac{1}{\sqrt{5}}\}$. Rozgałęzienie w obu przypadkach i w każdym z wymienionych punktów jest całkowite.*

Dowód. Teza wynika z bezpośredniego rachunku. □

Określamy powierzchnię eliptyczną $\mathcal{E}_1 = (S_1, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi_1)$, której włókno generyczne

$$y^2 = x(x-(t-1)^2)(x-4t).$$

jest krzywą eliptyczną nad $\overline{\mathbb{Q}}(t)$. Biorąc przeciągnięcie odwzorowania $\pi_1 : S_1 \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ przez $\phi_1 : \mathbb{P}^1_{\overline{\mathbb{Q}}} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ otrzymamy nową powierzchnię eliptyczną $\mathcal{E}_2 = (S_2, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi_2)$, której włókno generyczne ma postać

$$y^2 = x(x-(t^2-1)^2)(x-4t^2).$$

Stosując ponownie zamianę bazy poprzez morfizm ϕ_2 otrzymamy z powierzchni $\mathcal{E}_2$ nową powierzchnię $\mathcal{E}_3 = (S_3, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi_3)$, której włóknem generycznym jest krzywa eliptyczna

$$y^2 = x(x-(u^2-1))(x-4u^2), \quad u = \frac{2t}{5+t^2}.$$

Gładkie powierzchnie rzutowe można sklasyfikować ze względu na ich wymiar Kodairy. Stosując tę klasyfikację dla powierzchni eliptycznych nad $\mathbb{P}^1$ podamy górne oszacowania na liczbę Picarda powierzchni $\mathcal{E}_1, \mathcal{E}_2$ i $\mathcal{E}_3$.

Definicja 2.2.25 (Krzywa wyjątkowa)**.** Gładką krzywą C zanurzoną w gładkiej powierzchni X nazywamy *wyjątkową*, gdy jej iloczyn samoprzecięcia $C.C$ jest równy -1 oraz $C \cong \mathbb{P}^1$.

Definicja 2.2.26 (Wymiar Kodairy)**.** Niech X będzie gładką powierzchnią algebraiczną nad ciałem k dowolnej charakterystyki oraz niech X nie zawiera krzywych wyjątkowych. Niech ponadto K_X będzie dywizorem kanonicznym powierzchni X oraz $\Gamma(X, \mathcal{O}(nK_X))$ dla dowolnego $n \geq 0$ będzie k-przestrzenią liniową globalnych przekrojów snopa $\mathcal{O}(nK_X)$. Wówczas liczbę

$$\kappa = \text{tr.deg.}_k \left[\bigoplus_{n=0}^{\infty} \Gamma(X, \mathcal{O}(nK_X)) \right] - 1$$

nazywać będziemy *wymiarem Kodairy* powierzchni X

Twierdzenie 2.2.27. *Niech $\mathcal{E} = (S, C, \pi)$ będzie powierzchnią eliptyczną. Wówczas wymiar Kodairy powierzchni $\kappa(S)$ przyjmuje wartości $-1, 0$ lub 1 i mówimy, że powierzchnia jest*

- ***wymierna**, gdy $\kappa(S) = -1$,*
- ***typu K3**, gdy $\kappa(S) = 0$,*
- ***eliptyczna ogólnego typu**, gdy $\kappa(S) = 1$.*

Ponadto dla $\chi := \chi(S, \mathcal{O}_S)$, jeśli $\kappa = -1$, to $\chi = 1$, jeśli $\kappa = 0$, to $\chi = 2$ oraz jeśli $\kappa = 1$, to $\chi > 2$.

Dowód. Twierdzenie to jest szczególnym wnioskiem z twierdzenia klasyfikującego dla powierzchni algebraicznych. Dowód tego faktu, niezależny od charakterystyki ciała bazowego jest zawarty w [BM77] oraz [Mum69].

□

Twierdzenie 2.2.28. *Niech $\mathcal{E} = (S, \mathbb{P}^1_k, \pi)$ będzie powierzchnią eliptyczną oraz niech k będzie ciałem algebraicznie domkniętym $char(k) \neq 2, 3$. Załóżmy, że model minimalny Weierstrassa włókna generycznego powierzchni $\mathcal{E}$ ma postać*

$$y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t),$$

gdzie $a_i(t) \in k[t]$. Niech n będzie liczbą określoną w Twierdzeniu 2.2.6. Wtedy wymiar Kodairy $\kappa(S)$ wynosi odpowiednio

- *$\kappa(S) = -1$, gdy $n = 1$,*
- *$\kappa(S) = 0$, gdy $n = 2$,*
- *$\kappa(S) = 1$, gdy $n \geq 3$.*

Dowód. Na mocy Lematu 2.2.11 liczba n jest równa $\chi(S, \mathcal{O}_S)$. Wystarczy teraz skorzystać z Twierdzenia 2.2.27. □

Lemat 2.2.29 ([Nas13, Lemma 3.6]). *Wymiary Kodairy powierzchni $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ wynoszą, odpowiednio $-1, 0, 1$.*

Dowód. Sprawdzamy, że włókna generyczne E_1, E_2 mają zadane równania Weierstrassa w postaci globalnie minimalnej, por. Tabele 2.5, 2.6. Dla krzywej E_3 odpowiedni model globalnie minimalny E_3^{min} uzyskany po wyrugowaniu mianowników ma włókna osobliwe opisane w Tabeli 2.7. Na mocy Twierdzenia 2.2.6 liczba n określona w Twierdzeniu 2.2.28 wynosi dla E_1, E_2 i E_3^{min}, odpowiednio $1, 2$ i 4. Zastosowanie Twierdzenia 2.2.28 kończy dowód.

□

Miejsce v	$\mathbf{S(F_v)}$	$\mathbf{G(F_v)}$
$t = 1$	I_4	$\mathbb{Z}/4\mathbb{Z}$
$t = 0$	I_2	$\mathbb{Z}/2\mathbb{Z}$
pierwiastek $1 - 6t + t^2 = 0$	I_2	$\mathbb{Z}/2\mathbb{Z}$
$t = \infty$	I_2	$\mathbb{Z}/2\mathbb{Z}$

Tabela 2.5: Włókna osobliwe, $E_1 : y^2 = x(x - (t-1)^2)(x - 4t)$

Miejsce v	$\mathbf{S(F_v)}$	$\mathbf{G(F_v)}$
$t = 1$	I_4	$\mathbb{Z}/4\mathbb{Z}$
$t = 0$	I_4	$\mathbb{Z}/4\mathbb{Z}$
$t = -1$	I_4	$\mathbb{Z}/4\mathbb{Z}$
pierwiastek $-1 - 2t + t^2 = 0$	I_2	$\mathbb{Z}/2\mathbb{Z}$
pierwiastek $-1 + 2t + t^2 = 0$	I_2	$\mathbb{Z}/2\mathbb{Z}$
$t = \infty$	I_4	$\mathbb{Z}/4\mathbb{Z}$

Tabela 2.6: Włókna osobliwe, $E_2 : y^2 = x(x - (t^2-1)^2)(x - 4t^2)$

Lemat 2.2.30 ([Nas13, Lemma 3.7]). *Ranga grupy $E_1(\overline{\mathbb{Q}}(t))$ jest równa 1.*

Dowód. Powierzchnia $\mathcal{E}_1$ jest wymierna na mocy Lematu 2.2.29. Na mocy Twierdzenia 2.2.19 wiemy, że $\rho(\mathcal{E}_1) \leq 10$. Na mocy Twierdzenia 2.2.18 oraz Tabeli 2.5 dostajemy

$$\text{ranga}(E_1(\overline{\mathbb{Q}}(t))) = \rho(\mathcal{E}_1) - 2 - \sum_{v \in B}(m_v - 1) \leq 10 - 2 - 7 = 1.$$

Ponadto punkt

$$P = (-4t, 4\sqrt{-2}t(t+1))$$

Miejsce v	$\mathbf{S(F_v)}$	$\mathbf{G(F_v)}$
$t = 0$	I_4	$\mathbb{Z}/4\mathbb{Z}$
pierwiastek $5 + t^2 = 0$	I_4	$\mathbb{Z}/4\mathbb{Z}$
pierwiastek $5 - 2t + t^2 = 0$	I_4	$\mathbb{Z}/4\mathbb{Z}$
pierwiastek $5 + 2t + t^2 = 0$	I_4	$\mathbb{Z}/4\mathbb{Z}$
pierwiastek $(5 - 2t + t^2)^2 = 8t^2$	I_2	$\mathbb{Z}/2\mathbb{Z}$
pierwiastek $(5 + 2t + t^2)^2 = 8t^2$	I_2	$\mathbb{Z}/2\mathbb{Z}$
$t = \infty$	I_4	$\mathbb{Z}/4\mathbb{Z}$

Tabela 2.7: Włókna osobliwe, $E_3 : y^2 = x(x - (u^2 - 1)^2)(x - 4u^2)$, $u = \frac{2t}{5+t^2}$

leży na krzywej E_1 i jest punktem nieskończonego rzędu na mocy Lematu 2.2.22, bo $2P$ oraz $4P$ są różne od zera. □

Uwaga 2.2.31. Punkt $P = (-4t, 4\sqrt{-2}t(t+1))$ leżący na krzywej E_1 nie generuje części wolnej grupy Mordella-Weila $E_1(\overline{\mathbb{Q}}(t))$. Łatwo sprawdzić, że

$$P = 2Q + (0, 0),$$

gdzie $Q = (2\left(-1 + \sqrt{2}\right)(-1 + t)t, -2\sqrt{-1}(-1 + t)t\left(1 - 3t + 2\sqrt{2}t\right))$. Wysokość tego punktu wynosi $1/4$ i można pokazać, że punkt ten generuje część wolną grupy Mordella-Weila, por. Lemat 2.5.17.

Lemat 2.2.32 (Lemma 3.8, [Nas13])**.** *Grupa $E_2(\overline{\mathbb{Q}}(t))$ ma rangę 2.*

Dowód. Na mocy Lematu 2.2.29 powierzchnia eliptyczna $\mathcal{E}_2$ stowarzyszona z krzywą E_2 jest typu K3. Na mocy Twierdzenia 2.2.19 otrzymujemy, że $\rho(\mathcal{E}_2) \leq 20$ dla powierzchni nad ciałem charakterystyki 0. Z formuły Shiody-Tate'a oraz Tabeli 2.6 otrzymujemy, że

$$ranga\, E_2(\overline{\mathbb{Q}}(t)) \leq 2.$$

Punkty

$$P = (-4t^2, 4\sqrt{-2}t^2(t^2 + 1)),$$
$$Q = (2(t - 1)^2, 2(-1 + t)^2(-1 + 2t + t^2)).$$

są nieskończonego rzędu na mocy Lematu 2.2.22. Ponadto wartość iloczynu skalarnego na punktach P, Q wynosi $\langle P, P\rangle = 2$, $\langle Q, Q\rangle = 1$ i $\langle P, Q\rangle = \langle Q, P\rangle = 0$. Stąd wynika, że punkty są liniowo niezależne w grupie $E_2(\overline{\mathbb{Q}}(t))$, por. Lemat 2.6.8. □

Poniższy lemat podaje zgrubne oszacowanie rangi w grupie $E_3(\overline{\mathbb{Q}}(t))$. Aby istotnie poprawić ten wynik, w dalszej części rozdziału zastosujemy silniejsze narzędzia niż formuła Shiody-Tate'a.

Lemat 2.2.33. *Grupa $E_3(\overline{\mathbb{Q}}(t))$ ma rangę r, gdzie $3 \leq r \leq 6$.*

Dowód. Dana jest powierzchnia eliptyczna $\mathcal{E}_3$ stowarzyszona z E_3. Z Lematu 2.2.29 wynika, że wymiar Kodairy tej powierzchni wynosi 1 oraz $\chi(S) = 4$, gdzie $\mathcal{E}_3 = (S, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi)$, więc na mocy Twierdzenia 2.2.27 oraz Twierdzenia 2.2.19 liczba Picarda $\rho(\mathcal{E}_3)$ jest co najwyżej równa 40. Stosując formułę Shiody-Tate'a mamy zatem:

$$40 \geq \rho(\mathcal{E}_3) = 2 + \sum_{v \in B}(m_v - 1) = 2 + 8(4-1) + 8(2-1) + r = 34 + r$$

i stąd $r \leq 6$. Na krzywej E_3 znajdziemy 3 punkty liniowo niezależne i $\overline{\mathbb{Q}}(t)$-wymierne:

$$\begin{aligned}
P_1 &= (2(1+\sqrt{2})(-1+u)^2 u, 2\sqrt{-1}(1+\sqrt{2})(-1+(\sqrt{2}-u)^2)(-1+u)^2 u),\\
P_2 &= (2(u-1)^2, 2(-1+u)^2(-1+2u+u^2)),\\
P_3 &= \left(1-u^2, \frac{(-5+t^2)\,u\,(-1+u^2)}{5+t^2}\right),
\end{aligned}$$

gdzie $u = \frac{2t}{5+t^2}$. Ponadto $\langle P_i, P_j \rangle = 0$, gdy $i \neq j$ oraz $\langle P_i, P_i \rangle = i$ dla $i \in \{1,2,3\}$, więc punkty $\{P_1, P_2, P_3\}$ są liniowo niezależne, por. Lemat 2.6.4. □

2.3 Kohomologie ℓ-adyczne i ranga

W tym podrozdziale rozwiniemy techniki szacowania rangi grupy Nérona-Severiego, które pozwolą nam poprawić wynik z Lematu 2.2.33 i podać dokładną wartość rangi grupy $E_3(\overline{\mathbb{Q}}(t))$.

Przedstawione poniżej definicje i twierdzenia zostały zaczerpnięte z pracy N. Katza [Kat], która zbiera podstawowe własności kohomologii étale udowodnione przez Grothendiecka, Deligne'a i ich współpracowników w SGA. Niech X będzie rozmaitością rzutową nad algebraicznie domkniętym ciałem dowolnej charakterystyki $p \geq 0$. Ustalmy liczbę pierwszą $\ell \neq p$. Przez $\mathbb{Z}_\ell$ oznaczamy pierścień liczb ℓ-adycznych oraz przez $\mathbb{Q}_\ell$ jego ciało ułamków. Dla dowolnego $i \geq 0$ oraz dowolnego $n \geq 1$, niech $H^i_{\text{ét}}(X, \mathbb{Z}/\ell^n\mathbb{Z})$ oznacza i-tą grupę kohomologii étale, gdzie $\mathbb{Z}/\ell^n\mathbb{Z}$ jest snopem stałym. Dla dowolnego $i \geq 0$ definiujemy

$$H^i_{\text{ét}}(X, \mathbb{Q}_\ell) := \left(\varprojlim_n H^i_{\text{ét}}(X, \mathbb{Z}/\ell^n\mathbb{Z})\right) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Grupę $H^i_{\text{ét}}(X, \mathbb{Q}_\ell)$ nazywamy i-tą *grupą kohomologii ℓ-adycznych.*

Twierdzenie 2.3.1 ([Kat])**.** *Niech X będzie rozmaitością gładką i rzutową nad ciałem k algebraicznie domkniętym wymiaru n. Grupy $H^i_{ét}(X, \mathbb{Q}_\ell)$ posiadają następujące własności.*

(1) $H^i_{ét}(X, \mathbb{Q}_\ell)$ jest przestrzenią liniową nad $\mathbb{Q}_\ell$ oraz $\dim_{\mathbb{Q}_\ell} H^i(X, \mathbb{Q}_\ell) = 0$ dla $i > 2n$. Przestrzenie te są skończenie wymiarowe dla $i \leq 2n$.

(2) Dla dowolnych i, j istnieje naturalnie określone odwzorowanie dwuliniowe ("cup product")

$$H^i_{ét}(X, \mathbb{Q}_\ell) \times H^j_{ét}(X, \mathbb{Q}_\ell) \to H^{i+j}_{ét}(X, \mathbb{Q}_\ell).$$

(3) Zachodzi równość $\dim_{\mathbb{Q}_\ell} H^{2n}_{ét}(X, \mathbb{Q}_\ell) = 1$ *i "cup product"*

$$H^i_{ét}(X, \mathbb{Q}_\ell) \times H^{2n-i}_{ét}(X, \mathbb{Q}_\ell) \to H^{2n}_{ét}(X, \mathbb{Q}_\ell) \approx \mathbb{Q}_\ell$$

jest niezdegenerowaną formą dwuliniową dla i spełniających $0 \leq i \leq 2n$.

(4) Jeśli X jest określona nad $\mathbb{C}$, to

$$H^i_{ét}(X, \mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} \mathbb{C} \cong H^i_{sing}(X_{an}, \mathbb{C}),$$

gdzie X_{an} oznacza gładką rozmaitość nad $\mathbb{C}$ stowarzyszoną z X oraz H^i_{sing} jest i-tą grupą kohomologii singularnych X_{an} ze współczynnikami w $\mathbb{C}$.

Grupy pierwiastków z jedności $\mu_{\ell^n} \subset \mathbb{F}_q$, $q = p^m$, $m \in \mathbb{N}$ tworzą system odwrotny $\{\mu_{\ell^n} \to \mu_{\ell^{n-1}} : \zeta \mapsto \zeta^\ell\}$. Granica $\mu_{\ell^\infty} = \varprojlim \mu_{\ell^n}$ w naturalny sposób jest $\mathbb{Z}_\ell$-modułem i działa na niej grupa Galois $G = Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Topologiczny generator $\sigma \in G : s \mapsto s^q$ działa na elementach $\zeta \in \mu$ jak mnożenie przez q: $\sigma(\zeta) = q \cdot \zeta$.

Definicja 2.3.2. Niech M będzie $\mathbb{Z}_\ell[G]$-modułem. Dla $r \in \mathbb{N}$ ustalonego r-tym *twistem Tate'a* nazywamy $\mathbb{Z}_\ell[G]$-moduł

$$M(r) := M \otimes (\mu_{\ell^\infty})^{\otimes r}.$$

Gdy X jest gładką rzutową rozmaitością nad $\mathbb{F}_q$, to definiujemy na X absolutny morfizm Frobeniusa

$$F_X : X \to X$$

jako identyczność na punktach X i spełniający warunek $F^\#_X : \mathcal{O}_X \to \mathcal{O}_X$, $F^\#_X(s) = s^p$ dla indukowanego odwzorowania na snopie strukturalnym. Na schemacie $\widetilde{X} = X \times_{\mathrm{Spec}k} \mathrm{Spec}\overline{k}$ mamy absolutny morfizm Frobeniusa

$$F_{\widetilde{X}} = F_X \times F_{\overline{k}}.$$

Morfizm $F_{\widetilde{X}}$ indukuje działanie na $H^i_{\text{ét}}(\widetilde{X}, \mathbb{Q}_l)(m)$ dla dowolnych i oraz m. Z pracy [Tat65, §3] wiemy, że działanie to jest identycznością. Zatem morfizmy $F_X \times id_{\mathrm{Spec}\overline{k}}$ oraz $id_X \times F_{\overline{k}}$ indukują na $H^i_{\text{ét}}(\widetilde{X}, \mathbb{Q}_l)(m)$ odwzorowania, które są wzajemnie odwrotne. Gdy dany jest generator $\sigma \in G$ mamy $\sigma = F^r_{\overline{k}}$, gdzie r wyznaczone jest przez $q = p^r$. Podobnie niech $\Phi_X = F^r_X$. Wówczas $\Phi_X \times \sigma = F^r_{\widetilde{X}}$. Oznaczmy przez $\Phi^{*(m)}_X$ oraz $\sigma^{*(m)}$ endomorfizmy indukowane na $H^i_{\text{ét}}(\widetilde{X}, \mathbb{Q}_l)(m)$. Jak wcześniej było powiedziane $\Phi^{*(m)}_X$ oraz $\sigma^{*(m)}$ są odwrotnościami jako endomorfizmy.

Wielomian charakterystyczny $char(\Phi^*_X)_{i,\ell} := \det(I \cdot x - \Phi^*_X | H^i_{\text{ét}}(\widetilde{X}, \mathbb{Q}_\ell))$ ma współczynniki w $\mathbb{Z}$ i nie zależy od wyboru $\ell \neq p$. Oznaczać go będziemy $char(\Phi^*_X)_i$ lub jeśli jasne jest z kontekstu jaki jest indeks i, będziemy pisać $char(\Phi^*_X)$. Z

hipotezy Riemanna dla rozmaitości nad ciałami skończonymi udowodnionej przez P. Deligne'a ([Del74, Théorème I.6]) wynika, że pierwiastki wielomianu $char(\Phi_X^*)_i$ mają moduł równy $q^{i/2}$. Ponadto wymiar $\dim_{\mathbb{Q}_\ell} H^i_{\text{ét}}(\widetilde{X}, \mathbb{Q}_\ell)$ nie zależy od wyboru liczby pierwszej ℓ.

Sformułujemy teraz dwa kluczowe twierdzenia, które pozwalają oszacować z góry rangę grupy Nérona-Severiego.

Twierdzenie 2.3.3 ([vL07, Proposition 6.2])**.** *Niech L będzie ciałem liczbowym oraz $\mathfrak{q}$ niech będzie ideałem maksymalnym w pierścieniu liczb całkowitych $\mathcal{O}_L$ ciała L. Niech ciało reszt $k = \mathcal{O}_L/\mathfrak{q}$ będzie równe $\mathbb{F}_q$. Oznaczmy przez A lokalizację $(\mathcal{O}_L)_\mathfrak{q}$ na ideale $\mathfrak{q}$. Niech S będzie schematem całkowitym*

$$S \to Spec\, A,$$

który jest rzutowy, gładki i wymiaru relatywnego 2. Załóżmy ponadto, że $\overline{S} = X \times Spec\, \overline{L}$ oraz $\widetilde{S} = S \times Spec\, \overline{k}$ są schematami całkowitymi. Wówczas, dla dowolnego $\ell \nmid q$ istnieją naturalne injekcje

$$NS(\overline{S}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \hookrightarrow NS(\widetilde{S}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \hookrightarrow H^2_{\acute{e}t}(\widetilde{S}, \mathbb{Q}_l)(1).$$

Druga injekcja jest niezmiennicza ze względu na działanie $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Pierwsza injekcja pochodzi od naturalnego zanurzenia

$$NS(\overline{S}) \hookrightarrow NS(\widetilde{S}).$$

Niech $\lambda(\lambda_0, T, V)$ oznacza krotność wartości własnej λ_0 operatora liniowego $T : V \to V$ działającego na skończenie wymiarowej przestrzeni liniowej V. Jeśli λ_0 nie jest wartością własną operatora T, to przyjmujemy $\lambda(\lambda_0, T, V) = 0$.

Wniosek 2.3.4 ([vL07, Corollary 2.3])**.** *Przy założeniach z poprzedniego twierdzenia, niech S_k będzie przeciwobrazem niezerowego $\mathfrak{q} \in Spec\, A$ względem morfizmu $S \to Spec\, A$. Zachodzą wtedy nierówności*

$$rangaNS(\overline{S}) \leq rangaNS(\widetilde{S}) \leq \sum_\zeta \lambda(\zeta q, \Phi^*_{S_k}, H^2_{\acute{e}t}(\widetilde{S}, \mathbb{Q}_l)),$$

gdzie suma przebiega po wszystkich pierwiastkach z jedności i jest skończona na mocy definicji λ.

Dowód. Zauważmy, że każdy element $NS(\widetilde{S})$ jest reprezentowany przez dywizory, które są określone nad pewnym rozszerzeniem ciała $\mathbb{F}_q$. Skoro grupa $NS(\widetilde{S})$ jest skończenie generowana, to istnieje takie rozszerzenie $\mathbb{F}_{q^N}$, że dywizory w $NS(\widetilde{S})$ są określone nad $\mathbb{F}_{q^N}$. Wtedy automorfizm $(\sigma^{*(1)})^N$ działający na $H^2_{\text{ét}}(\widetilde{S}, \mathbb{Q}_l)(1)$

jest identycznością na podprzestrzeni $NS(\widetilde{S}) \otimes \mathbb{Q}_\ell$. Stąd

$$\begin{aligned} ranga\, NS(\widetilde{S}) &\leq \lambda(1, (\sigma^{*(1)})^N, NS(\widetilde{S}) \otimes \mathbb{Q}_\ell) && (2.16)\\ &\leq \lambda(1, (\sigma^{*(1)})^N, H^2_{\text{ét}}(\widetilde{S}, \mathbb{Q}_l)(1)) && (2.17)\\ &\leq \sum_\zeta \lambda(\zeta, \sigma^{*(1)}, H^2_{\text{ét}}(\widetilde{S}, \mathbb{Q}_l)(1)) && (2.18)\\ &\leq \sum_\zeta \lambda(\zeta/q, \sigma^*, H^2_{\text{ét}}(\widetilde{S}, \mathbb{Q}_l)) && (2.19)\\ &\leq \sum_\zeta \lambda(\zeta \cdot q, \Phi^*_{S_k}, H^2_{\text{ét}}(\widetilde{S}, \mathbb{Q}_l)). && (2.20) \end{aligned}$$

Sumy przebiegają po wszystkich pierwiastkach z jedności. Nierówność (2.16) wynika z tego, że $(\sigma^{*(1)})^N$ jest identycznością na $NS(\widetilde{S}) \otimes \mathbb{Q}_\ell$. Nierówność (2.17) indukuje injekcja z Twierdzenia 2.3.3. Operator $(\sigma^{*(1)})^N$ ma wartości własne, które są N-tymi potęgami wartości własnych operatora $(\sigma^{*(1)})$, stąd (2.18). Nierówność (2.19) wynika z faktu, że σ działa na module Tate'a $\mu_{\ell\infty}$ przez mnożenie przez q. Ostatnia nierówność wynika z tego, że σ^* jest odwrotnością $\Phi^*_{S_k}$. □

W celu wykorzystania w praktyce powyższego wniosku, należy obliczyć wielomian charakterystyczny operatora $\Phi^*_{S_k}$. Wykorzystamy do tego celu formułę Lefschetza udowodnioną przez Grothendiecka.

Twierdzenie 2.3.5 ([Mil80, VI,Theorem 12.3])**.** *Niech X będzie gładką rozmaitością rzutową nad $\mathbb{F}_q$, wymiaru n. Dla dowolnej liczby pierwszej $\ell \nmid q$ oraz dowolnego m zachodzi równość*

$$\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2n} (-1)^i\, Tr((\Phi^*_X)^m | H^i_{\acute{e}t}(\widetilde{X}, \mathbb{Q}_l)).$$

Wyrażenie z lewej strony równości oznacza liczbę punktów $\mathbb{F}_{q^m}$-wymiernych na rozmaitości X. Symbol Tr oznacza operator śladu endomorfizmu.

Wykorzystamy elementarną metodę rekonstrukcji wielomianu charakterystycznego operatora $T : V \to V$ na skończenie wymiarowej przestrzeni liniowej V, przy zadanych śladach $t_n = Tr(T^n)$ dla dowolnych $n \geq 0$. Niech $p(x) = \det(I \cdot x - T)$ będzie wielomianem charakterystycznym operatora T na przestrzeni V. Niech dany będzie formalny szereg $exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$. Zachodzi tożsamość

$$p(x) = \frac{x^{\dim V}}{exp(\sum_{r=1}^{\infty} t_r \frac{x^{-r}}{r})}.$$

Otrzymujemy z tego następujące klasyczne wzory na kolejne współczynniki wielo-

mianu $p(x) = x^n + c_1 x^{n-1} + \ldots + c_n$

$$\begin{aligned} c_1 &= -t_1, \\ c_2 &= \frac{1}{2}(t_1^2 - t_2), \\ c_3 &= \frac{1}{6}(-t_1^3 + 3t_1 t_2 - 2t_3), \\ c_4 &= \frac{1}{24}(t_1^4 - 6t_1^2 t_2 + 3t_2^2 + 8t_1 t_3 - 6t_4), \\ &\ldots \end{aligned} \tag{2.21}$$

2.3.1 Obliczanie wielomianu charakterystycznego Frobeniusa na powierzchniach eliptycznych

Zastosujemy ogólny sposób postępowania z poprzedniego paragrafu do sytuacji, gdy zadana jest powierzchnia gładka X nad ciałem skończonym $\mathbb{F}_q$ taka, że $(\widetilde{X}, \mathbb{P}^1_{\overline{\mathbb{F}_q}}, \pi)$ jest powierzchnią eliptyczną, gdzie $\widetilde{X} = X_{\overline{\mathbb{F}_q}}$ oraz $\pi : \widetilde{X} \to \mathbb{P}^1_{\overline{\mathbb{F}_q}}$.

Na mocy [Kle68, Corollary 2A10] oraz [CD89, Corollary 5.2.2] wymiary $\dim_{\mathbb{Q}_\ell} H^1_{\text{ét}}(\widetilde{X}, \mathbb{Q}_\ell)$ oraz $\dim_{\mathbb{Q}_\ell} H^3_{\text{ét}}(\widetilde{X}, \mathbb{Q}_\ell)$ wynoszą zero. Automorfizm Φ^*_X działa na $H^4_{\text{ét}}(\widetilde{X}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$ przez mnożenie przez q^2, natomiast na $H^0_{\text{ét}}(\widetilde{X}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$ jako identyczność. Z Twierdzenia 2.3.5 wynika, że dla powierzchni $\widetilde{X}$ zachodzi równość

$$Tr((\Phi^*_X)^m \mid H^2_{\text{ét}}(\widetilde{X}, \mathbb{Q}_l)) = \#X(\mathbb{F}_{q^m}) - 1 - q^{2m}.$$

W grupie Nérona-Severiego powierzchni $\widetilde{X}$ wyróżniamy podgrupę $V \subset NS(\widetilde{X})$, która jest generowana przez obraz cięcia zerowego, dowolnie ustalone włókno nieosobliwe oraz składowe włókien osobliwych. Niech W oznacza iloraz $H^2_{\text{ét}}(\widetilde{X}, \mathbb{Q}_l)/V$ uzyskany przez utożsamienie V z jej obrazem przy naturalnym odwzorowaniu kocyklu $NS(\widetilde{X}) \hookrightarrow H^2_{\text{ét}}(\widetilde{X}, \mathbb{Q}_l)$. Chwilowo nie bierzemy pod uwagę działania grupy Galois, stąd brak skręcenia przez moduł Tate'a μ_{ℓ^∞}. Operator Φ^*_X indukuje operatory liniowe $\Phi^*_X|V : V \to V$ oraz $\Phi^*_X|W : W \to W$. Wielomiany charakterystyczne spełniają równość

$$char(\Phi^*_X) = char(\Phi^*_X|V) \cdot char(\Phi^*_X|W)$$

ze względu na multiplikatywność wielomianu charakterystycznego na ciągach dokładnych. Dla dowolnej liczby naturalnej m mamy analogiczną równość dla operatora śladu

$$Tr((\Phi^*_X)^m) = Tr((\Phi^*_X|V)^m) + Tr((\Phi^*_X|W)^m).$$

2.4 Skręcenia krzywych eliptycznych

Niech C będzie gładką krzywą rzutową określoną nad algebraicznie domkniętym ciałem k. W całym paragrafie zakładamy, że ciało k ma charakterystykę różną

od 2 i 3. Oznaczmy przez $k(C)$ ciało funkcji wymiernych na C. Dana jest krzywa eliptyczna E o równaniu Weierstrassa

$$E : y^2 = x^3 + Ax^2 + Bx,$$

gdzie $A, B \in k(C)$ i takie, że $\Delta = 16B^2\,(A^2 - 4B) \neq 0$ jako funkcja w $k(C)$.

Definicja 2.4.1. Niech dany będzie element $u \in k(C)^*$. Krzywa eliptyczna $E^{(u)}$ o równaniu

$$uy^2 = x^3 + Ax^2 + Bx$$

nazywana będzie *skręceniem kwadratowym* krzywej E przez element u.

Standardowa postać Weierstrassa dla krzywej $E^{(u)}$ jest zadana równaniem

$$y^2 = x^3 + Aux^2 + Bu^2x.$$

Pomiędzy obydwoma postaciami można przechodzić poprzez zamianę zmiennych $(x, y) \mapsto (x/u, y/u^2)$. Przy takiej reparametryzacji będziemy utożsamiać zbiory punktów $k(C)$ wymiernych na obu modelach krzywej. Dla elementu $u \in k(C)$ możemy znaleźć w domknięciu algebraicznym $\overline{k(C)}$ element v spełniający $v^2 = u$. Rozszerzenie $k(C)(v)$ oznaczać będziemy $k(C)(\sqrt{u})$. Poniższe stwierdzenie jest dobrze znane, jednak ze względu na brak precyzyjnego uzasadnienia tego faktu w znanej autorowi literaturze, prezentujemy tu szczegółowy dowód (patrz również [Sil86, Exercise 10.16] oraz [SS10, §7.11]).

Stwierdzenie 2.4.2. *Niech E będzie krzywą eliptyczną nad ciałem funkcyjnym $k(C)$. Niech $u \in k(C)^*$ będzie takim elementem, że $k(C)(\sqrt{u}) \neq k(C)$. Załóżmy ponadto, że ani krzywa E, ani krzywa $E^{(u)}$ nie są izomorficzne nad $k(C)$ z krzywymi określonymi nad k. Zachodzi wtedy równość:*

$$ranga\, E(k(C)) + ranga\, E^{(u)}(k(C)) = ranga\, E(k(C)(\sqrt{u})).$$

Dowód. Niech K oznacza ciało $k(C)$. Grupa $G = Gal(K(\sqrt{u})/K)$ jest dwuelementowa i generowana przez $\sigma : \sqrt{u} \mapsto -\sqrt{u}$. Definiujemy dwie podgrupy w $E(K)$

$$H = \{P \in E(K(\sqrt{u})) : P = \sigma(P)\},$$
$$\widetilde{H} = \{P \in E(K(\sqrt{u})) : P = -\sigma(P)\}.$$

Element $P = (x, y)$ niezerowy w H spełnia $\sigma(x, y) = (x, y)$, czyli $\sigma(x) = x$ i $\sigma(y) = y$, stąd $x, y \in K$ i $P \in E(K)$. Na odwrót, każdy element z $E(K)$ również należy do H i mamy $H = E(K)$. Zauważmy ponadto, że krzywa $E : y^2 = x^3 + Ax^2 + Bx$ jest $K(\sqrt{u})$-izomorficzna z krzywą $E^{(u)} : y^2 = x^3 + Aux^2 + Bu^2x$, gdzie izomorfizm jest dany odwzorowaniem $f : (x, y) \mapsto (xu, yu\sqrt{u})$. Niezerowy punkt $P \in \widetilde{H}$ dany jest w postaci $P = (\alpha, \beta\sqrt{u})$, $\alpha, \beta \in K$, co wynika z równości $\sigma(P) = -P$. Izomorfizm f przekształca punkty z $\widetilde{H}$ następująco

$$f(\alpha, \beta\sqrt{u}) = (\alpha u, \beta u^2).$$

Daje nam to izomorfizm grup $\widetilde{H}$ i $E^{(u)}(K)$. Łącząc obie obserwacje dostajemy, że $H \times \widetilde{H} \cong E(K) \times E^{(u)}(K)$.

Rozważmy teraz odwzorowanie

$$\phi_1 : E(K(\sqrt{u})) \to H \times \widetilde{H} : Q \mapsto (Q + \sigma(Q), Q - \sigma(Q)).$$

Jeśli $\phi_1(Q) = 0$, to $Q = \sigma(Q)$ oraz $2Q = 0$, co daje $Q \in E(K)[2]$. Zatem jądro ϕ_1 jest skończoną podgrupą. Określamy odwzorowanie

$$\phi_2 : H \times \widetilde{H} \to E(K(\sqrt{u})) : (P, Q) \mapsto P + Q.$$

W tym przypadku warunek $\phi_2(P, Q) = 0$ implikuje równość $P = -Q$. Skoro

$$\begin{array}{ccccc} E(K(\sqrt{u})) & \xrightarrow{\phi_1} & H \times \widetilde{H} & \xrightarrow{\phi_2} & E(K(\sqrt{u})) \\ & & \downarrow \cong & & \\ & & E(K) \times E^{(u)}(K) & & \end{array}$$

Rysunek 2.3: Odwzorowania ϕ_1 i ϕ_2.

$(P, Q) \in H \times \widetilde{H}$, to $P = \sigma(P)$ oraz $Q = -\sigma(Q)$. Łącząc trzy ostatnie równości otrzymujemy $2P = 0$ oraz $P = Q$, czyli $\ker \phi_2 \subset (H \times \widetilde{H})[2] = H[2] \times \widetilde{H}[2]$. Zatem jądro ϕ_2 jest skończone. W oczywisty sposób oba odwzorowania ϕ_1 oraz ϕ_2 są homomorfizmami grup. Odwzorowania ϕ_1 i ϕ_2 są injekcjami z dokładnością do elementów 2-torsyjnych, więc

$$ranga\, E(K(\sqrt{u})) \leq ranga(H \times \widetilde{H}) \leq ranga\, E(K(\sqrt{u})).$$

Ponadto $ranga(H \times \widetilde{H}) = ranga\, H + ranga\, \widetilde{H} = ranga\, E(K) + ranga\, E^{(u)}(K)$ i w końcu

$$ranga\, E(K) + ranga\, E^{(u)}(K) = ranga\, E(K(\sqrt{u})).$$

□

Definicja 2.4.3. Niech $\mathcal{E} = (S, C, \pi)$ będzie powierzchnią eliptyczną nad ciałem k. Niech E będzie włóknem generycznym morfizmu π. Powierzchnię eliptyczną $\mathcal{E}' = (S', C, \pi')$ nazywamy *skręceniem powierzchni* $\mathcal{E}$ względem punktów $P, Q \in C(k)$ jeśli włókno generyczne morfizmu π' jest $k(C)$-izomorficzne z krzywą eliptyczną $E^{(u)}$ oraz

$$\begin{aligned} &\mathrm{ord}_P(u) \equiv 1 \, mod\, 2, \\ &\mathrm{ord}_Q(u) \equiv 1 \, mod\, 2, \\ &\mathrm{ord}_R(u) \equiv 0 \, mod\, 2, \text{ dla każdego } R \neq P, Q. \end{aligned}$$

Powierzchnię $\mathcal{E}'$ oznaczamy $\mathcal{E}^{(P,Q)}$.

Uwaga 2.4.4. Zauważmy, że dla dowolnej pary punktów $P, Q \in C(k)$ istnieje funkcja u spełniająca warunki Definicji 2.4.3. Istotnie, grupa $Pic^0(C)$ jest równa grupie punktów k-wymiernych na jakobianie $Jac(C)$. Ciało k jest algebraicznie domknięte z definicji powierzchni eliptycznej, więc grupa $Jac(C)(k)$ jest podzielna. W szczególności istnieje klasa $[D]$, $D \in Div^0(C)$ taka, że $[(P) - (Q)] = 2[D]$ i stąd $(P) - (Q) = 2D + div(f)$ dla pewnej funkcji $f \in k(C)^*$. Kładziemy $u := f$.

Uwaga 2.4.5. Gdy $C = \mathbb{P}^1$, to skręcenie jest wyznaczone jednoznacznie przez zadaną parę punktów P, Q. W przypadku, gdy krzywa C ma genus g większy niż zero, jej jakobian jest nietrywialny i elementy P, Q wyznaczają funkcję u tylko z dokładnością do 2^{2g} punktów 2-torsyjnych na jakobianie $Jac(C)$. Dokładniej, gdy $u, u' \in k(C)^*$ są funkcjami, które spełniają warunki definicji, wtedy

$$div(u) = (P) - (Q) + 2D,$$

$$div(u') = (P) - (Q) + 2D',$$

gdzie $D, D' \in Div^0(C)$. Zatem $T = D - D'$ wyznacza klasę $[T] \in Pic^0(C)[2] = Jac(C)(k)[2]$. Jeśli k jest algebraicznie domkniętym ciałem, to $\# Jac(C)(k)[2] = 2^{2g}$, ponieważ $\dim Jac(C) = 2g$.

Lemat 2.4.6 ([Nas13, Lemma 4.3])**.** *Niech (S, C, π) będzie powierzchnią eliptyczną nad ciałem k oraz niech $P, Q \in C(k)$ będą ustalonymi punktami. Niech powierzchnia eliptyczna $\mathcal{E}^{(P,Q)} = (S^{(P,Q)}, \pi^{(P,Q)}, C)$ będzie skręceniem powierzchni $\mathcal{E}$ przez punkty P, Q. Wówczas istnieje krzywa C' nad k oraz surjektywny morfizm $\phi : C' \to C$ stopnia 2 taki, że $\pi_{C'} : S \times_C C' \to C'$ oraz $\pi_{C'}^{(P,Q)} : S^{(P,Q)} \times_C C' \to C'$ mają modele relatywnie minimalne i nieosobliwe, które są izomorficzne jako powierzchnie rozwłóknione nad C'*

Dowód. Oznaczmy przez E włókno generyczne morfizmu π. Wówczas z Definicji 2.4.3 wynika, że istnieje funkcja $u \in k(C)$ taka, że włókno generyczne morfizmu $\pi^{(P,Q)}$ jest $k(C)$ izomorficzne z $E^{(u)}$. Ponadto funkcja u ma nieparzysty rząd znikania na punktach P oraz Q i parzysty dla wszystkich pozostałych punktów z $C(k)$. W ciele $\overline{k(C)}$ istnieje element v taki, że $v^2 = u$. Tworzymy nowe ciało $K = k(C)(v)$, które jest kwadratowe nad $k(C)$. Na mocy [Har77, I,Corollary 6.12] istnieje gładka krzywa rzutowa C' oraz izomorfizm $\iota : K \to k(C')$. Oznaczmy przez $\phi : C' \to C$ morfizm odpowiadający złożeniu $k(C) \hookrightarrow k(C)(v) \xrightarrow{\iota} k(C')$. Wówczas $u \circ \phi = w^2$ dla pewnego $w \in k(C')$. Przez $e_\phi(R)$ oznaczmy stopień rozgałęzienia morfizmu ϕ w punkcie R znajdującym się we włóknie nad punktem $\phi(R) \in C(k)$. Na mocy Definicji 2.4.3 $div(u) = (P) + (Q) + 2D$, $D \in Div(C)$. Ponadto $2\, div(w) = div(u \circ \phi) = \phi^*(div(u))$, gdzie $\phi^* : Div(C) \to Div(C')$ jest cofnięciem dywizora przez odwzorowanie ϕ. Stąd

$$\sum_{R \in \phi^{-1}(P)} e_\phi(R)(R) + \sum_{R' \in \phi^{-1}(Q)} e_\phi(R')(R') + 2\phi^* D = \phi^*(div\, u) = 2\, div(w). \quad (2.22)$$

Odwzorowanie ϕ jest stopnia 2, więc

$$2 = deg\, \phi = \sum_{R \in \phi^{-1}(P)} e_\phi(R) = \sum_{R' \in \phi^{-1}(Q)} e_\phi(R').$$

Przypuśćmy, że punkty P i Q są oba nierozgałęzione. Istnieją zatem pary punktów R_1, R_2, gdzie $R_1 \neq R_2$ oraz R_3, R_4, gdzie $R_3 \neq R_4$ takie, że $\phi(R_1) = \phi(R_2) = P$, $\phi(R_3) = \phi(R_4) = Q$ oraz $e_\phi(R_1) = e_\phi(R_2) = e_\phi(R_3) = e_\phi(R_4) = 1$. Z równania 2.22 wynika, że

$$(R_1) + (R_2) + (R_3) + (R_4) \in 2\, Div(C').$$

W takim wypadku musiałoby zachodzić $R_1 = R_3$ lub $R_1 = R_4$, ale punkty te należą do różnych włókien, stąd sprzeczność. Podobnie jeśli tylko jeden z punktów P lub Q jest nierozgałęziony, dochodzimy do sprzeczności. Zatem P i Q są oba rozgałęzione z dokładnie jednym elementem w przeciwobrazie i o stopniu rozgałęzienia równym 2.

Oznaczmy przez $S_1 = S \times_C C'$ oraz przez $S_2 = S^{(P,Q)} \times_C C'$ zamiany bazy powierzchni S i $S^{(P,Q)}$ względem morfizmu ϕ. Morfizmy π oraz $\pi^{(P,Q)}$ są rzutowe na mocy definicji. Z [Har77, II,Corollary 4.8(c)] wynika, że morfizmy $\pi_{C'}$ i $\pi^{(P,Q)}_{C'}$ są rzutowe. Ciało bazowe k jest algebraicznie domknięte, zatem tylko skończenie wiele włókien tych morfizmów nie jest krzywymi eliptycznymi. Przez $\widetilde{S}_i$ oznaczamy relatywnie minimalny nieosobliwy model powierzchni S_i, zachowujący rozwłóknienie nad C', patrz Definicja 2.2.15. Niech krzywa eliptyczna E nad $k(C)$ będzie włóknem generycznym powierzchni eliptycznej (S, C, π). Włókna generyczne morfizmów $\widetilde{S}_1 \to C'$ oraz $\widetilde{S}_2 \to C'$ są równe odpowiednio E oraz $E^{(u)}$ jako krzywe eliptyczne nad $k(C')$. Są one izomorficzne nad $k(C')$ skoro $E^{(u)}$ jest skręceniem krzywej E. W szczególności oznacza to, że istnieje biwymierne odwzorowanie

$$\psi : \widetilde{S}_1 \dashrightarrow \widetilde{S}_2.$$

Odwzorowanie takie musi być złożeniem odwzorowań typu "blow-up" i "blow-down". Ponadto powierzchnie $\widetilde{S}_1$ oraz $\widetilde{S}_2$ nie zawierają żadnych krzywych wyjątkowych (patrz Definicja 2.2.25 i uwaga przed nią), więc ψ jest trywialnym złożeniem odwzorowań typu "blow-up" i "blow-down" i ψ przedłuża się do izomorfizmu. □

Poniżej zostaną wprowadzone powierzchnie eliptyczne, na których będziemy wykonywać obliczenia potrzebne do dowodu Wniosku 2.4.8 i Wniosku 2.5.15. Istotą wprowadzenia tych obiektów jest fakt, że bezpośrednia praca z powierzchnią eliptyczną $\mathcal{E}_3$ jest trudniejsza.

(1) Niech $\mathcal{E}_1 = (S_1, \mathbb{P}^1_{\overline{\mathbb{Q}}}, S_1 \to \mathbb{P}^1_{\overline{\mathbb{Q}}})$ będzie powierzchnią eliptyczną z włóknem generycznym
$$E_1 : y^2 = x(x - (t-1)^2)(x - 4t).$$

(2) Oznaczamy przez $\mathcal{E}'_1 = \mathcal{E}_1^{(\frac{1}{5},\infty)} = (S'_1, \mathbb{P}^1_{\overline{\mathbb{Q}}}, S'_1 \to \mathbb{P}^1_{\overline{\mathbb{Q}}})$ skręcenie powierzchni $\mathcal{E}_1$ względem punktów $\frac{1}{5}$ i ∞. Włókno generyczne powierzchni $\mathcal{E}'_1$ ma postać
$$E'_1 : -(-1+5t)y^2 = x(x - (t-1)^2)(x - 4t).$$

(3) Oznaczmy przez $\mathcal{E}''_1 = \mathcal{E}_1^{(0,\frac{1}{5})} = (S''_1, \mathbb{P}^1_{\overline{\mathbb{Q}}}, S''_1 \to \mathbb{P}^1_{\overline{\mathbb{Q}}})$ skręcenie powierzchni $\mathcal{E}_1$ względem punktów 0 i $\frac{1}{5}$. Włókno generyczne powierzchni $\mathcal{E}''_1$ ma postać
$$E''_1 : -t(-1+5t)y^2 = x(x - (t-1)^2)(x - 4t).$$

(4) Niech $\mathcal{E}_2 = (S_2, \mathbb{P}^1_{\overline{\mathbb{Q}}}, S_2 \to \mathbb{P}^1_{\overline{\mathbb{Q}}})$ będzie powierzchnią eliptyczną z włóknem generycznym
$$E_2 : y^2 = x(x - (t^2-1)^2)(x - 4t^2).$$

(5) Oznaczmy przez $\mathcal{E}_2' = \mathcal{E}_2^{(\frac{-1}{\sqrt{5}}, \frac{1}{\sqrt{5}})} = (S_2', \mathbb{P}^1_{\overline{\mathbb{Q}}}, S_2' \to \mathbb{P}^1_{\overline{\mathbb{Q}}})$ skręcenie powierzchni $\mathcal{E}_2$ względem punktów $\frac{-1}{\sqrt{5}}$ i $\frac{1}{\sqrt{5}}$. Włókno generyczne powierzchni $\mathcal{E}_2'$ ma postać
$$E_2' : -(-1+5t^2)y^2 = x(x - (t^2-1)^2)(x - 4t^2).$$

(6) Niech $\mathcal{E}_3 = (S_3, \mathbb{P}^1_{\overline{\mathbb{Q}}}, S_3 \to \mathbb{P}^1_{\overline{\mathbb{Q}}})$ będzie powierzchnią eliptyczną z włóknem generycznym
$$E_3 : y^2 = x(x - ((\frac{2t}{5+t^2})^2 - 1)^2)(x - 4(\frac{2t}{5+t^2})^2).$$

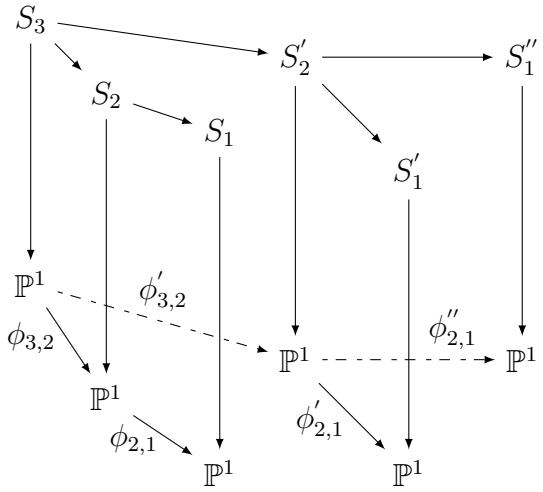
Niech S_ϕ oznacza iloczyn rozwłókniony $S \times_C C'$ powstały z pary morfizmów $S \to C$ i $\phi : C' \to C$. Ponadto niech $\widetilde{S_\phi}$ oznacza model relatywnie minimalny nieosobliwy dla powierzchni S_ϕ.

Stwierdzenie 2.4.7. *Niech $\phi_{2,1}, \phi_{3,2}, \phi'_{3,2}, \phi'_{2,1}, \phi''_{2,1}$ będą morfizmami $\mathbb{P}^1_{\overline{\mathbb{Q}}} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ zadanymi wzorami*
$$\begin{aligned}
\phi_{2,1} &: t \mapsto t^2 \\
\phi_{3,2} &: t \mapsto \frac{2t}{5+t^2} \\
\phi'_{3,2} &: t \mapsto \frac{2t}{5+t^2} \\
\phi'_{2,1} &: t \mapsto t^2 \\
\phi''_{2,1} &: t \mapsto t^2
\end{aligned}$$

Wówczas $S_3 \cong \widetilde{S_{2,\phi_{3,2}}}$, $S_2 \cong \widetilde{S_{1,\phi_{2,1}}}$, $S_3 \cong \widetilde{S'_{2,\phi'_{3,2}}}$, $S'_2 \cong \widetilde{S'_{1,\phi'_{2,1}}}$ oraz $S'_2 \cong \widetilde{S''_{1,\phi''_{2,1}}}$. Ponadto wskazane izomorfizmy zadają izomorfizmy odpowiadających powierzchni rozwłóknionych, więc również odpowiadających powierzchni eliptycznych. Sytuację obrazuje Rysunek 2.4.

Dowód. Wystarczy zastosować dowód Lematu 2.4.6 i sprawdzić, że przeciągnięcia odpowiednich włókien generycznych przez zadane morfizmy są izomorficzne □

Wniosek 2.4.8 ([Nas13, Corollary 4.5])**.** *Zachodzą równości*
$$ranga\, E_3(\overline{\mathbb{Q}}(t)) = ranga\, E_2(\overline{\mathbb{Q}}(t)) + ranga\, E_2'(\overline{\mathbb{Q}}(t)),$$
$$ranga\, E_2'(\overline{\mathbb{Q}}(t)) = ranga\, E_1'(\overline{\mathbb{Q}}(t)) + ranga\, E_1''(\overline{\mathbb{Q}}(t)).$$



Rysunek 2.4: Konfiguracja powierzchni eliptycznych powstałych ze skręceń

Dowód. Niech $r = -(-1 + 5t^2)$. Sprawdzamy, że zachodzą na mocy definicji skręcenia krzywej eliptycznej równości $E_2' = E_2^{(r)}$ oraz $E_1'' = (E_1')^{(t)}$. Jeśli izomorfizm ciał $\sigma : \overline{\mathbb{Q}}(t)(\sqrt{r}) \to \overline{\mathbb{Q}}(t)$ jest zadany wzorem $\sigma(t) = \frac{2t}{5+t^2}$, to $E_2(\overline{\mathbb{Q}}(t)(\sqrt{r})) \cong E_2^{\sigma}(\sigma(\overline{\mathbb{Q}}(t)(\sqrt{r}))) = E_3(\overline{\mathbb{Q}}(t))$, por. (2.43). Ustalając izomorfizm $\sigma : \overline{\mathbb{Q}}(t)(\sqrt{t}) \to \overline{\mathbb{Q}}(t)$ zadany wzorem $\sigma(t) = t^2$ otrzymujemy $E_1'(\overline{\mathbb{Q}}(t)(\sqrt{t})) \cong E_2'(\overline{\mathbb{Q}}(t))$. Stwierdzenie 2.4.2 implikuje równości podane w tezie. □

2.5 Rangi w rodzinach krzywych I

Zastosujemy teraz rezultaty przedstawione w podrozdziale 2.3.1 do obliczenia rangi grupy Mordella-Weila $E_1'(\overline{\mathbb{Q}}(t))$. Wynik ten pochodzi z pracy [Nas13] i jest jednym z głównych składników dowodu Wniosku 2.5.15.

Twierdzenie 2.5.1. *Ranga grupy $E_1'(\overline{\mathbb{Q}}(t))$ wynosi* 0.

Dowód twierdzenia będzie podzielony na szereg lematów.

Lemat 2.5.2. *Powierzchnia eliptyczna $\mathcal{E}_1'$ jest typu K3 (w sensie Twierdzenia 2.2.27). Włókna osobliwe morfizmu $S_1' \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ opisane są w Tabeli 2.8.*

Dowód. Stosując algorytm Tate'a dla modelu globalnie minimalnego krzywej E_1' (patrz dowód Lematu 2.5.3) otrzymamy, że nad punktem $t = 1$ mamy włókno typu I_4, nad punktem $t = 0$ włókno typu I_2 i nad punktami będącymi pierwiastkami $1 - 6t + t^2 = 0$ otrzymamy włókna typu I_2. Nad punktem $t = \infty$ otrzymamy włókno I_2^* oraz włókno nad punktem $t = \frac{1}{5}$ typu I_0^*. Korzystając z Twierdzenia 2.2.6 oraz Twierdzenia 2.2.27 dochodzimy do wniosku, że powierzchnia $\mathcal{E}_1'$ jest typu K3. □

Lemat 2.5.3. *Istnieje powierzchnia $(S_1')_{\mathbb{Q}}$, która jest modelem nad $\mathbb{Q}$ powierzchni S_1'. Istnieje morfizm schematów $\pi : S \to Spec\,\mathbb{Z}_{(17)}$, który jest gładki rzutowy i*

Miejsce v	$\mathbf{S(F_v)}$	$\mathbf{G(F_v)}$
$t = 1$	I_4	$\mathbb{Z}/4\mathbb{Z}$
$t = 0$	I_2	$\mathbb{Z}/2\mathbb{Z}$
$t = \frac{1}{5}$	I_0^*	$(\mathbb{Z}/2\mathbb{Z})^2$
$t = 3 \pm 2\sqrt{2}$	I_2	$\mathbb{Z}/4\mathbb{Z}$
$t = \infty$	I_2^*	$(\mathbb{Z}/2\mathbb{Z})^2$

Tabela 2.8: Włókna osobliwe, $E_1^{'} : -(-1+5t)y^2 = x(x-(t-1)^2)(x-4t)$

relatywnego wymiaru 2 *oraz włókno nad punktem generycznym jest powierzchnią* $(S_1^{'})_{\mathbb{Q}}$. *W szczególności włókno specjalne* π *definiuje powierzchnię eliptyczną typu* $K3$.

Uwaga 2.5.4. Włókno specjalne morfizmu π nazywamy "redukcją" modulo 17 powierzchni $\mathcal{E}_1^{'}$. Wybór liczby pierwszej 17 jest istotny ze względu na fakt, że π jest gładkim morfizmem. Ponadto jest to najmniejsza liczba pierwsza dobrej redukcji, dla której można uzyskać ograniczenie $ranga\, NS(\mathcal{E}_1^{'}) \leq 18$ metodami opisanymi w Lemacie 2.5.5 i w dowodzie Twierdzenia 2.5.1.

Dowód. Krzywa E_1' ma model globalnie minimalny Weierstrassa nad $\mathbb{Q}(t)$ postaci

$$y^2 = x^3 + ((1+t)^2(-1+5t))x^2 + 4(-1+t)^2t(-1+5t)^2x. \tag{2.23}$$

Wyróżnik tego równania wynosi $\Delta(t) = 256(-1+t)^4t^2(-1+5t)^6(1-6t+t^2)^2$, a wyróżnik części wolnej od kwadratów $disc(2(-1+t)t(-1+5t)(1-6t+t^2)) = 2^{25}$. Powierzchnia $(S_1^{'})_{\mathbb{Q}}$ będąca modelem Kodairy-Nérona podanego wyżej modelu równania E_1' jest określona nad $\mathbb{Q}$ na mocy algorytmu Tate'a. Z warunku na wyróżnik i Twierdzenia 2.2.12 powierzchnia $(S_1^{'})_{\mathbb{Q}}$ ma dobrą redukcję na liczbie pierwszej $p = 17$. Redukując współczynniki równania (2.23) modulo 17 otrzymamy równanie Weierstrassa włókna generycznego powierzchni eliptycznej $S_{17} = \pi^{-1}(\mathfrak{p})$, gdzie $\mathfrak{p} = 17\mathbb{Z}_{(17)}$. Równanie globalnie minimalne nad $\mathbb{F}_{17}[t]$ ma postać

$$y^2 = x^3 + 5(1+t)^2(10+t)x^2 + 15t(10+t)^2(16+t)^2x \tag{2.24}$$

Z Twierdzenia 2.2.28 wynika, że wymiar Kodairy powierzchni eliptycznej

$$((S_{17})_{\overline{\mathbb{F}_{17}}}, \mathbb{P}^1_{\overline{\mathbb{F}_{17}}}, (S_{17})_{\overline{\mathbb{F}_{17}}} \to \mathbb{P}^1_{\overline{\mathbb{F}_{17}}})$$

wynosi 0, więc jest ona typu K3. □

Lemat 2.5.5. *Niech* $\widetilde{S}$ *będzie zamianą bazy do* $\overline{\mathbb{F}_{17}}$ *włókna specjalnego* $S_{\mathbb{F}_{17}}$ *morfizmu* π *z Lematu 2.5.3. Niech* $\ell \neq 17$ *będzie liczbą pierwszą. Wielomian operatora Frobeniusa* $\Phi^*_{S_{\mathbb{F}_{17}}}$ *działającego na* $H^2_{\acute{e}t}(\widetilde{S}, \mathbb{Q}_\ell)$ *jest postaci*

$$char(\Phi^*_{S_{\mathbb{F}_{17}}})(x) = (x-17)^{18}(x^4 - 8x^3 + 238x^2 - 2312x + 83521).$$

Dowód. Z Lematu 2.5.3 wiemy, że powierzchnia $\widetilde{S}$ jest $K3$, więc $\chi(\widetilde{S}) = 2$. To implikuje, że grupa $H^2_{\text{ét}}(\widetilde{S}, \mathbb{Q}_\ell)$ ma wymiar 22 na mocy równości (2.9) z dowodu Twierdzenia 2.2.19. Twierdzenie 2.3.3 implikuje istnienie zanurzenia

$$NS(\widetilde{S}) \otimes \mathbb{Q}_\ell \hookrightarrow H^2_{\text{ét}}(\widetilde{S}, \mathbb{Q}_\ell(1)).$$

W szczególności zachodzi nierówność $ranga\, NS(\widetilde{S}) \leq 22$. Oznaczmy przez V podprzestrzeń w $NS(\widetilde{S}) \otimes \mathbb{Q}_\ell$ generowaną przez składowe włókien osobliwych morfizmu π, obraz cięcia zerowego oraz dowolne włókno nieosobliwe. Za pomocą algorytmu Tate'a [Sil94, IV,9.4] sprawdzamy, że wszystkie składowe włókien osobliwych rozwłóknienia $\pi : \widetilde{S} \to \mathbb{P}^1_{\overline{\mathbb{F}_{17}}}$ są określone nad $\mathbb{F}_{17}$. Zatem automorfizm $\sigma^{*(1)} \in End(H^2_{\text{ét}}(\widetilde{S}, \mathbb{Q}_\ell(1)))$ indukowany przez $\sigma \in Gal(\overline{\mathbb{F}_{17}}/\mathbb{F}_{17}) : x \mapsto x^{17}$ działa jak identyczność na $V \subset NS(\widetilde{S}) \otimes \mathbb{Q}_\ell \hookrightarrow H^2_{\text{ét}}(\widetilde{S}, \mathbb{Q}_\ell(1))$. To oznacza, że $\Phi^*_{S_{\mathbb{F}_{17}}}$ działa jak mnożenie przez 17 na V traktowanej jako podprzestrzeń w $H^2_{\text{ét}}(\widetilde{S}, \mathbb{Q}_\ell)$. Zatem

$$char(\Phi^*_{S_{\mathbb{F}_{17}}}|V)(x) = \det(Id \cdot x - \Phi^*_{S_{\mathbb{F}_{17}}}|V) = (x-17)^{\dim V}.$$

Z Tabeli 2.8 odczytujemy typy włókien osobliwych i na podstawie Tabeli 2.3 obliczamy liczbę składowych w każdym z włókien. Wymiar V jest równy $2 + \sum_{v \in B}(m_v - 1)$, gdzie B oznacza zbiór punktów złej redukcji, a m_v liczbę składowych włókna osobliwego nad v. Ostatecznie otrzymujemy $\dim V = 18$.

Niech $H = H^2_{\text{ét}}(\widetilde{S}, \mathbb{Q}_\ell)$. Interesuje nas rozkład wielomianu charakterystycznego

$$char(\Phi^*_{S_{\mathbb{F}_{17}}}|H) = char(\Phi^*_{S_{\mathbb{F}_{17}}}|V) \cdot char(\Phi^*_{S_{\mathbb{F}_{17}}}|H/V).$$

Ponadto wiemy, że

$$Tr((\Phi^*_{S_{\mathbb{F}_{17}}})^m|H) = Tr((\Phi^*_{S_{\mathbb{F}_{17}}})^m|V) + Tr((\Phi^*_{S_{\mathbb{F}_{17}}})^m|H/V)$$

oraz $Tr((\Phi^*_{S_{\mathbb{F}_{17}}})^m|V) = 18 \cdot 17^m$. Z dyskusji w podrozdziale 2.3.1 oraz z Twierdzenia 2.3.5 wynika, że

$$Tr((\Phi^*_{S_{\mathbb{F}_{17}}})^m|H) = \#\widetilde{S}(\mathbb{F}_{17^m}) - 1 - 17^{2m}.$$

Łącząc powyższe równości otrzymujemy

$$Tr((\Phi^*_{S_{\mathbb{F}_{17}}})^m|H/V) = \#\widetilde{S}(\mathbb{F}_{17^m}) - 1 - 17^{2m} - 18 \cdot 17^m.$$

Przestrzeń liniowa H/V jest wymiaru 4. Zatem wielomian charakterystyczny $char(\Phi^*_{S_{\mathbb{F}_{17}}}|H/V)$ jest postaci $x^4 + c_1x^3 + c_2x^2 + c_3x + c_4$, gdzie współczynniki c_i są dane jako funkcje wielomianowe śladów $t_m = Tr((\Phi^*_{S_{\mathbb{F}_{17}}})^m|H/V)$ następującymi wzorami (por. (2.21))

$$\begin{aligned}
c_1 &= -t_1, \\
c_2 &= \frac{1}{2}(t_1^2 - t_2), \\
c_3 &= \frac{1}{6}(-t_1^3 + 3t_1t_2 - 2t_3), \\
c_4 &= \frac{1}{24}(t_1^4 - 6t_1^2t_2 + 3t_2^2 + 8t_1t_3 - 6t_4).
\end{aligned}$$

Wystarczy teraz obliczyć liczbę punktów $\mathbb{F}_{17^m}$-wymiernych nad $\widetilde{S}$ dla $m = 1, 2, 3, 4$. Bezpośrednie obliczenia wykonane pakietem MAGMA są przedstawione w Tabeli 2.9.

m	1	2	3	4
$\#\widetilde{S}(\mathbb{F}_{17^m})$	604	88312	24227740	6977057176

Tabela 2.9: Liczba punktów $\mathbb{F}_{17^m}$-wymiernych na powierzchni $\widetilde{S}$.

Uzyskujemy wielomian charakterystyczny $char(\Phi^*_{S_{\mathbb{F}_{17}}}|H/V)(x) = x^4 - 8x^3 + 238x^2 - 2312x + 83521$, co daje nam ostatecznie

$$char(\Phi^*_{S_{\mathbb{F}_{17}}}|H)(x) = (x-17)^{18}(x^4 - 8x^3 + 238x^2 - 2312x + 83521).$$

□

Dowód Twierdzenia 2.5.1. Z Lematu 2.5.5 wiemy, że wielomian charakterystyczny $char(\Phi^*_{S_{\mathbb{F}_{17}}}|H)$ ma co najmniej 18 pierwiastków postaci 17ζ, gdzie ζ jest pierwiastkiem z jedności. Udowodnimy, że czynnik $x^4 - 8x^3 + 238x^2 - 2312x + 83521$ nie ma pierwiastków postaci 17ζ. Gdyby zachodziła równość $x = 17\zeta$, wówczas mielibyśmy

$$4913(17\zeta^4 - 8\zeta^3 + 14\zeta^2 - 8\zeta + 17) = 0.$$

Ale wtedy element ζ byłby pierwiastkiem wielomianu $17x^4 - 8x^3 + 14x^2 - 8x + 17$, który jest nierozkładalny w $\mathbb{Z}[x]$. Zatem ζ nie może być liczbą algebraiczną całkowitą, w szczególności nie może być pierwiastkiem z jedności. Wniosek 2.3.4 implikuje, że ranga grupy $NS(\mathcal{E}_1') = NS(S_{\overline{\mathbb{Q}}})$ jest co najwyżej równa 18. Twierdzenie 2.2.18 pozwala nam udowodnić, że ranga grupy $E_1'(\overline{\mathbb{Q}}(t))$ jest równa 0. □

2.5.1 Hipoteza Tate'a i Artina-Tate'a

Celem tego podrozdziału jest udowodnienie następującego twierdzenia.

Twierdzenie 2.5.6. *Ranga grupy $E_1''(\overline{\mathbb{Q}}(t))$ wynosi 1.*

Zastosowanie metod z poprzedniego paragrafu wymaga pewnego uzupełnienia. Dla powierzchni eliptycznej $\mathcal{E}_1''$, której włókno generyczne jest krzywą eliptyczną E_1'' możemy podobnie jak wcześniej znaleźć model całkowity $S \to \mathbb{Z}_{(p)}$ dla liczby pierwszej p dobrej redukcji, np. $p = 11, 17$. Okaże się jednak, że próba obliczenia rangi grupy Nérona-Severiego $NS(\mathcal{E}_1'')$ da nam (przy użyciu metod z poprzedniego podrozdziału) wyłącznie oszacowanie z góry przez 20. W rzeczywistości ranga tej grupy wynosi, jak udowodnimy, dokładnie 19. Użyjemy do dowodu teorii krat oraz kluczowych w tym rozdziale hipotez Tate'a i Artina-Tate'a, które dla powierzchni typu $K3$ są twierdzeniami, patrz [ASD73], [Mil75], [Mil86].

Hipoteza 2.5.7 (Tate)**.** *Niech X będzie gładką rozmaitością rzutową określoną nad ciałem $\mathbb{F}_q$, gdzie q jest potęgą liczby pierwszej. Wówczas*

$$ranga\, NS(X_{\overline{\mathbb{F}_q}}) = \sum_{\zeta} \lambda(\zeta \cdot q, \Phi_X^*, H^2_{\acute{e}t}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l)),$$

gdzie $\ell \nmid q$ oraz suma przebiega po wszystkich pierwiastkach z jedności. Suma jest skończona na mocy definicji λ podanej przed Wnioskiem 2.3.4.

Do wysłowienia drugiej hipotezy wprowadzamy szereg oznaczeń. Oznaczmy przez $Br(X)$ grupę Brauera rozmaitości X, tj. $H^2_{\text{ét}}(X, \mathbb{G}_m)$. Niech $\alpha(X)$ będzie równe $\chi(X, \mathcal{O}_X) - 1 + \dim Pic^0(X)$, gdzie $\chi(X, \mathcal{O}_X)$ to charakterystyka Eulera powierzchni X i $Pic^0(X)$ jest grupą wiązek liniowych stopnia zero na X. Niech $\rho'(X)$ oznacza rangę podgrupy w $NS(X_{\overline{\mathbb{F}_q}})$ rozpiętej przez wszystkie dywizory określone nad $\mathbb{F}_q$. Oznaczmy ponadto przez $P(x)$ wielomian $\det(Id - x\Phi_X^* | H^2_{\acute{e}t}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l))$, gdzie $\ell \nmid q$. Wielomian $P(x)$ nie zależy od wyboru ℓ, na mocy hipotez Weila.

Hipoteza 2.5.8 ([Tat66, (C)],[Mil75, (A-T)])**.** *Niech X będzie gładką rozmaitością rzutową określoną nad ciałem $\mathbb{F}_q$, gdzie q jest potęgą liczby pierwszej. Wówczas grupa Brauera $Br(X)$ jest skończona oraz*

$$\lim_{s \to 1} \frac{P(q^{-s})}{(1 - q^{1-s})^{\rho'(X)}} = \frac{(-1)^{\rho'(X)-1} \sharp Br(X) \Delta(NS(X_{\mathbb{F}_q}))}{q^{\alpha(X)} (\sharp NS(X_{\mathbb{F}_q})_{tor})^2},$$

gdzie $\Delta(NS(X_{\mathbb{F}_q}))$ jest wyróżnikiem macierzy Grama formy przecięcia, na podgrupie $NS(X_{\overline{\mathbb{F}_q}})$ generowanej przez dywizory $\mathbb{F}_q$-wymierne.

Twierdzenie 2.5.9. *Niech X będzie powierzchnią eliptyczną typu $K3$ określoną nad ciałem skończonym $\mathbb{F}_q$. Wówczas Hipoteza 2.5.7 i Hipoteza 2.5.8 są prawdziwe. Ponadto jeśli q jest potęgą liczby pierwszej o parzystym wykładniku oraz grupa $NS(X_{\overline{\mathbb{F}_q}})$ jest generowana przez dywizory $\mathbb{F}_q$-wymierne, to*

$$\Delta(NS(X_{\overline{\mathbb{F}_q}})) \equiv - \lim_{s \to 1} \frac{P(q^{-s})}{(1 - q^{1-s})^{\rho(X)}} \ (mod\ (\mathbb{Q}^\times)^2).$$

Dowód. Hipoteza Tate'a dla powierzchni $K3$ została udowodniona w [ASD73, Theorem 5.2]. J. Milne w [Mil75, Theorem 6.1] oraz [Mil86, Theorem 0.4b] dowodzi, że prawdziwość hipotez Tate'a dla powierzchni implikuje prawdziwość hipotezy Artine'a-Tate'a. W [Klo07, Proposition 4.7] R. Kloosterman wyprowadza wniosek podany w tezie twierdzenia. □

Sformułujemy lemat (za [Klo07, Proposition 4.4]), który uzasadniania konieczność użycia dwóch liczb pierwszych do badania rangi grupy Nérona-Severiego w niektórych przypadkach.

Lemat 2.5.10. *Niech X będzie gładką rzutową powierzchnią określoną nad ciałem $\mathbb{F}_q$, dla której zachodzi Hipoteza 2.5.7. Niech $\ell \nmid q$. Wówczas*

$$\dim H^2_{\acute{e}t}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l) - \rho(X) = r,$$

gdzie $\rho(X)$ jest rangą grupy $NS(X)$ oraz r jest liczbą wartości własnych operatora Φ_X^* działającego na $H^2_{\acute{e}t}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l)$, które nie są postaci $q\zeta$, dla pewnego pierwiastka z jedności ζ. Ponadto r jest parzysta.

Dowód. Bez utraty ogólności, kosztem powiększenia ciała definicji $\mathbb{F}_q$, możemy założyć, że grupa $NS(X_{\overline{\mathbb{F}_q}})$ jest generowana przez $\mathbb{F}_q$-wymierne dywizory. Dla powierzchni X, wielomian charakterystyczny operatora Φ_X^* działającego na $\dim H^2_{\acute{e}t}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l)$ ma postać $g(x)(x-q)^{\rho(X)}$ i $\deg g = r$. Pierwiastki wielomianu g nie są postaci ζq na mocy Hipotezy 2.5.7. W szczególności $g(q), g(-q) \neq 0$. Ponadto wszystkie pierwiastki mają normę zespoloną q, stąd g nie ma żadnych zer rzeczywistych. To implikuje, że wielomian g ma stopień parzysty, zatem również r jest liczbą parzystą. □

Lemat 2.5.10 jest prawdziwy np. dla powierzchni X, które są eliptyczne typu $K3$ nad ciałem skończonym. Dla tych powierzchni zachodzi $\dim H^2_{\acute{e}t}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_l) = 22$ i skoro r jest parzyste, to z Lematu 2.5.10 wynika, że ranga grupy $NS(X_{\overline{\mathbb{F}_q}})$ jest parzysta. Jeśli dana jest powierzchnia eliptyczna typu $K3$ nad $\mathbb{Q}$ z modelem całkowitym $S \to \mathbb{Z}_{(p)}$ takim, że włókno specjalne jest powierzchnią $\widetilde{S}$ nad $\overline{\mathbb{F}_p}$ oraz włókno generyczne $\overline{S}$ jest powierzchnią nad $\overline{\mathbb{Q}}$, to z Twierdzenia 2.3.3 wiemy, że

$$\rho(\overline{S}) \leq \rho(\widetilde{S}).$$

Jeśli $\rho(\overline{S})$ jest nieparzyste, to powyższa nierówność na mocy Lematu 2.5.10 jest ostra i nie oszacujemy precyzyjnie rangi grupy Nérona-Severiego z wykorzystaniem jednej liczby pierwszej. Uzyskamy takie oszacowanie dzięki wykorzystaniu dwóch liczb pierwszych i Twierdzenia 2.5.9.

Lemat 2.5.11. *Niech G będzie ustaloną grupą abelową wolną skończonej rangi. Niech L będzie podgrupą skończonego indeksu w G. Niech dana będzie na G forma dwuliniowa $\langle \cdot, \cdot \rangle : G \times G \to \mathbb{R}_{\geq 0}$, która jest dodatnio określona. Oznaczmy przez $\Delta(G)$ wyznacznik macierzy*

$$(\langle e_i, e_j \rangle)_{i,j},$$

gdzie $\{e_k\}$ jest bazą w G. Podobnie oznaczmy przez $\Delta(L)$ wyznacznik analogicznie zdefiniowanej macierzy zadanej przez iloczyny $\langle f_i, f_j \rangle$, gdzie $\{f_k\}$ stanowi bazę w L. Wówczas zachodzi równość

$$\Delta(G)[G : L]^2 = \Delta(L).$$

Dowód. Przy zamianie bazy w G wyznacznik $\Delta(G)$ nie zmienia się na mocy [Ser73, IV,§1.1]. Z twierdzenia o zgodnej bazie możemy wybrać taką bazę $\{e_k\}_{k=1}^n$ w G, że $\{a_k e_k\}_{k=1}^n$ jest bazą w L, gdzie $a_i \in \mathbb{N}$. Z dwuliniowości $\langle \cdot, \cdot \rangle$ mamy $\Delta(L) = (a_1 \cdot \ldots \cdot a_n)^2 \Delta(G)$, ale $[G : L] = a_1 \cdot \ldots \cdot a_n$. □

Lemat 2.5.12. *Powierzchnia $\mathcal{E}_1''$ z podrozdziału 2.4 jest typu $K3$. Powierzchnia $\mathcal{E}_1''$ ma model określony nad $\mathbb{Q}$ oraz ma dobrą redukcję w liczbach pierwszych p=11, 17, tzn. istnieje morfizm gładki i rzutowy $S_p \to \mathbb{Z}_{(p)}$ taki, że włókno generyczne jak i specjalne są powierzchniami typu $K3$ oraz włókno generyczne jest modelem powierzchni $\mathcal{E}_1''$ nad $\mathbb{Q}$.*

Dowód. Stosując algorytm Tate'a z podrozdziału 2.2.1 uzyskamy opis włókien specjalnych rozwłóknienia $\mathcal{E}_1'' \to \mathbb{P}^1_{\mathbb{Q}}$, przedstawiony w Tabeli 2.10. Następnie stosujemy Twierdzenie 2.2.12 dla liczb pierwszych $p = 11$ i $p = 17$. Typ powierzchni odczytujemy z twierdzenia 2.2.28. □

Miejsce v	$\mathbf{S}(\mathbf{F_v})$	$\mathbf{G}(\mathbf{F_v})$
$t = 1$	I_4	$\mathbb{Z}/4\mathbb{Z}$
$t = \infty$	I_2	$\mathbb{Z}/2\mathbb{Z}$
$t = 0$	I_2^*	$(\mathbb{Z}/2\mathbb{Z})^2$
$t = \frac{1}{5}$	I_0^*	$(\mathbb{Z}/2\mathbb{Z})^2$
$t = 3 + 2\sqrt{2}$	I_2	$(\mathbb{Z}/2\mathbb{Z})$
$t = 3 - 2\sqrt{2}$	I_2	$(\mathbb{Z}/2\mathbb{Z})$

Tabela 2.10: Włókna osobliwe, $E_1'' : -t(-1+5t)y^2 = x(x-(t-1)^2)(x-4t)$

Lemat 2.5.13. *Niech $\ell \neq 11, 17$ będzie liczbą pierwszą. Wielomian charakterystyczny operatora $\Phi^*_{S_{11}}$ działającego na $H^2_{\acute{e}t}((S_{11})_{\overline{\mathbb{F}_{11}}}, \mathbb{Q}_l)$ jest równy*

$$(x-11)^{19}(x+11)(x^2+20x+121).$$

Wielomian operatora $\Phi^*_{S_{17}}$ działającego na $H^2_{\acute{e}t}((S_{17})_{\overline{\mathbb{F}_{17}}}, \mathbb{Q}_l)$ jest równy

$$(x-17)^{20}(x^2-22x+289).$$

m	1	2	3	4
$\#\widetilde{S}(\mathbb{F}_{11^m})$	300	17220	1794780	214647384

Tabela 2.11: Liczba punktów $\mathbb{F}_{11^m}$-wymiernych na powierzchni $\widetilde{S}_{11}$.

m	1	2	3	4
$\#\widetilde{S}(\mathbb{F}_{17^m})$	618	89208	24217578	6977269656

Tabela 2.12: Liczba punktów $\mathbb{F}_{17^m}$-wymiernych na powierzchni $\widetilde{S}_{17}$.

Dowód. Wprowadzamy oznaczenia: $\widetilde{S}_{11} = (S_{11})_{\overline{\mathbb{F}_{11}}}$ oraz $\widetilde{S}_{17} = (S_{17})_{\overline{\mathbb{F}_{17}}}$. Za pomocą pakietu MAGMA obliczamy liczbę punktów $\mathbb{F}_{p^m}$-wymiernych na powierzchni $\widetilde{S}_p$ dla $m = 1, 2, 3, 4$, $p = 11, 17$. Odpowiednie obliczenia zawarte są w Tabeli 2.11 oraz Tabeli 2.12.

Niech B będzie zbiorem miejsc złej redukcji. Niech T będzie podgrupą w $NS(\widetilde{S}_{11})$ generowaną przez włókno generyczne F, obraz $\mathcal{O}$ cięcia zerowego $O : \mathbb{P}^1 \to \widetilde{S}_{11}$ oraz składowe $\Theta_{i,v}$ włókien osobliwych $\pi^{-1}(v)$, $v \in B$, $i \geq 0$. Tylko składowe $\Theta_{0,v}$ przecinają nietrywialnie $\mathcal{O}$. Bazę podgrupy T stanowią elementy $\{F, \mathcal{O}\} \cup \{\Theta_{i,v} : i > 0, v \in B\}$. Sprawdzamy za pomocą algorytmu Tate'a, że morfizm Frobeniusa $\Phi_{S_{11}}$ działa trywialnie na wszystkich składowych nieprzecinających $\mathcal{O}$ poza dwiema. We włóknach nad punktami $3 + 2\sqrt{2}$ i $3 - 2\sqrt{2}$ morfizm permutuje składowe $\Theta_{1,3+2\sqrt{2}}$ oraz $\Theta_{1,3-2\sqrt{2}}$. Wynika to z faktu, że $\sqrt{2} \in \mathbb{F}_{11^2} \setminus \mathbb{F}_{11}$. W szczególności, ślad operatora $(\Phi^*_{S_{11}})^m$, dla $m \geq 0$, działającego na $T \otimes \mathbb{Q}_\ell \subset H^2_{\text{ét}}(\widetilde{S}_{11}, \mathbb{Q}_l)$ wynosi

$$Tr((\Phi^*_{S_{11}})^m | T \otimes \mathbb{Q}_\ell) = 17 + (-1)^m.$$

Ponadto wielomian charakterystyczny $char(\Phi^*_{S_{11}}|V)$ jest równy $(x-11)^{17}(x+11)$ dla $V = T \otimes \mathbb{Q}_\ell$. Na mocy Twierdzenia 2.3.5 dostajemy dla $H = H^2_{\text{ét}}(\widetilde{S}_{11}, \mathbb{Q}_l)$

$$Tr((\Phi^*_{S_{\mathbb{F}_{17}}})^m | H/V) = \#\widetilde{S}(\mathbb{F}_{11^m}) - 1 - 11^{2m} - 17 \cdot 11^m - (-1)^m \cdot 11.$$

Obliczamy teraz wielomian charakterystyczny $char(\Phi^*_{S_{11}}|H/V)$ metodą z Lematu 2.5.5. Jest on wielomianem zmiennej x postaci

$$(x^2 + 20x + 121)(x - 11)^2.$$

Stąd wielomian $char(\Phi^*_{S_{11}}|H)$ jest równy $(x-11)^{19}(x+11)(x^2+20x+121)$. Stosując analogiczne rozumowanie w sytuacji, gdy zastąpimy liczbę 11 przez 17 otrzymamy wielomian charakterystyczny

$$char(\Phi^*_{S_{17}} | H^2_{\text{ét}}(\widetilde{S}_{17}, \mathbb{Q}_l)) = (x-17)^{20}(x^2 - 22x + 289).$$

W charakterystyce 17 mamy $\sqrt{2} \in \mathbb{F}_{17}$, dlatego morfizm $\Phi_{S_{17}}$ działa trywialnie na podgrupie w $NS(\widetilde{S}_{17})$ generowanej przez składowe włókien osobliwych. □

Lemat 2.5.14. *Ranga grupy $E_1''(\overline{\mathbb{Q}}(t))$ wynosi co najmniej 1.*

Dowód. Zauważmy, że punkt $M = (1-t, 1-t)$ leży na krzywej E_1''. Pokażemy, że jest on nieskończonego rzędu. Z Lematu 2.2.22 oraz Tabeli 2.10 otrzymujemy injekcję

$$E_1''(\overline{\mathbb{Q}}(t))_{\text{tors}} \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^7 \oplus \mathbb{Z}/4\mathbb{Z}.$$

Sprawdzamy, że gdyby $2M = 0$, to $M = -M$ i $y(M) = 0$, ale $y(M) = 1 - t$. Podobnie, gdyby $4M = 0$, to $2M = -2M$ i $y(2M) = 0$. Obliczamy

$$2M = \left(-\frac{(4t^2 - 5t + 1)^2}{4t(5t-1)}, \frac{(t-1)^2(4t-1)(6t-1)(t(4t+5)-1)}{8(1-5t)^2t^2} \right)$$

i w oczywisty sposób $y(2M) \neq 0$. Stąd wynika, że punkt M jest nieskończonego rzędu i ranga grupy $E_1''(\overline{\mathbb{Q}}(t))$ wynosi co najmniej 1. □

Dowód Twierdzenia 2.5.6. Niech $\ell \nmid 11 \cdot 17$ będzie liczbą pierwszą. Niech S_{11} i S_{17} będą powierzchniami z Lematu 2.5.13. Oznaczmy przez S'_{11} zamianę bazy $S_{11} \times Spec\,\mathbb{F}_{11^2}$ i podobnie $S'_{17} = S_{17} \times Spec\,\mathbb{F}_{17^2}$. Ponadto wprowadzamy oznaczenia $\widetilde{S}'_{11} = S'_{11} \times Spec\,\overline{\mathbb{F}_{11^2}}$ oraz $\widetilde{S}'_{17} = S'_{17} \times Spec\,\overline{\mathbb{F}_{17^2}}$. Wartości własne operatora $\Phi^*_{S'_p}$ działającego na $H^2_{\text{ét}}(\widetilde{S}'_p, \mathbb{Q}_l)$ są kwadratami wartości własnych operatora $\Phi^*_{S_p}$ działającego na $H^2_{\text{ét}}(\widetilde{S}_p, \mathbb{Q}_l)$ dla $p = 11, 17$. Zatem zachodzą równości

$$char(\Phi^*_{S'_{11}}) = (x - 11^2)^{20}(x^2 - 158x + 14641),$$
$$char(\Phi^*_{S'_{17}}) = (x - 17^2)^{20}(x^2 + 94x + 83521).$$

Hipoteza 2.5.7 dla powierzchni $K3$ pociąga, że $ranga\,NS(\widetilde{S}'_{11}) = ranga\,NS(\widetilde{S}'_{17}) = 20$. Zastosowanie Lematu 2.5.14 oraz Twierdzenia 2.2.18 do konfiguracji włókien osobliwych podanej w Tabeli 2.10 implikuje, że $ranga\,NS(\mathcal{E}''_1)$ wynosi co najmniej 19. Z Twierdzenia 2.2.19 oraz Lematu 2.5.12 wynika, że $ranga\,NS(\mathcal{E}''_1) \leq 20$. Załóżmy, że $ranga\,NS(\mathcal{E}''_1)$ jest równa dokładnie 20. Wówczas Twierdzenie 2.3.3 implikuje, że $N = NS(\mathcal{E}''_1)$ jest podgrupą skończonego indeksu zarówno w grupie $N_{11} = NS(\widetilde{S}'_{11})$ jak i w $N_{17} = NS(\widetilde{S}'_{17})$. W szczególności, na mocy Lematu 2.5.11 zachodzą równości

$$\Delta(N_{11})[N_{11} : N]^2 = \Delta(N),$$
$$\Delta(N_{17})[N_{17} : N]^2 = \Delta(N).$$

Z tego wynika, że $\Delta(N_{11}) \equiv \Delta(N_{17}) \bmod (\mathbb{Q}^\times)^2$. Z drugiej strony, Twierdzenie 2.5.9 implikuje równości

$$\Delta(N_{11}) \equiv -3 \cdot 7 \bmod (\mathbb{Q}^\times)^2,$$
$$\Delta(N_{17}) \equiv -2 \cdot 3 \cdot 7 \bmod (\mathbb{Q}^\times)^2.$$

Otrzymujemy sprzeczność z założeniem o randze grupy N. Zatem ranga grupy N jest równa 19. Lemat 2.5.14 oraz Twierdzenie 2.2.18 wraz z Tabelą 2.10 implikują, że $ranga\,E''_1(\overline{\mathbb{Q}}(t)) = 1$. □

Wniosek 2.5.15. *Ranga grupy $E_3(\overline{\mathbb{Q}}(t))$ wynosi 3.*

Dowód. Stosujemy Wniosek 2.4.8 wraz z Twierdzeniami 2.5.1, 2.5.6 oraz Lematem 2.2.32. □

2.5.2 Rodziny krzywych eliptycznych z parametrem

Lemat 2.5.16 ([Nas13, Lemma 6.1])**.** *Podgrupa punktów torsyjnych w $E_3(\overline{\mathbb{Q}}(t))$ jest izomorficzna z grupą $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Generatorami części torsyjnej $E_3(\overline{\mathbb{Q}}(t))_{tors}$ są punkty*

$$T_1 = (4u^2, 0),$$
$$T_2 = (2(-u + u^3), 2\sqrt{-1}(u^2 - 1)u(-1 - 2u + u^2)),$$

gdzie $u = \frac{2t}{5+t^2}$.

Dowód. Niech $K = \overline{\mathbb{Q}}(t)$. Z Tabeli 2.7 oraz Lematu 2.2.22 odczytujemy, że

$$E_3(K)_{\text{tors}} \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^8 \oplus (\mathbb{Z}/4\mathbb{Z})^8.$$

Grupa $E_3(K)[2]$ jest generowana przez punkty $P = (x, y)$ spełniające $y = 0$. W tym przypadku $E_3(K)[2] = \{O, T_1, 2T_2, T_1 + 2T_2\}$. Bezpośrednim rachunkiem można sprawdzić, że $2T_2 = (0, 0)$. Pokażemy teraz, że zarówno $T_1 \notin 2E_3(K)$ jak i $T_1 + (0, 0) \notin 2E_3(K)$. Niech $P = (x, y)$ będzie niezerowym punktem z $E_3(K)$. Wówczas pierwsza współrzędna punktu $2P$ ma postać

$$x(2P) = \frac{\left(4u^2 - 8u^4 + 4u^6 - x^2\right)^2}{4\left(4u^2 - x\right)\left(1 - 2u^2 + u^4 - x\right)x}.$$

Gdyby T_1 należało do $2E_3(K)$, to wtedy zachodziłaby równość $x(2P) = 4u^2$. W szczególności, otrzymalibyśmy równanie kwadratowe zmiennej x

$$16t^2(25 + 6t^2 + t^4)^2 - 32t^2(5 + t^2)^4 x + (5 + t^2)^6 x^2 = 0.$$

Istnieje rozwiązanie $x_0 \in K$ powyższego równania wtedy i tylko, gdy wyróżnik tego równania

$$-64t^2(5 + t^2)^6(625 - 100t^2 - 74t^4 - 4t^6 + t^8)$$

jest pełnym kwadratem w K. Sprawdzamy, że wielomian $625 - 100t^2 - 74t^4 - 4t^6 + t^8$ ma wyróżnik równy $2^{64}5^{12}$, a zatem jest rozdzielczy i nie może być pełnym kwadratem. Otrzymujemy sprzeczność, więc istotnie $T_1 \notin 2E_3(K)$. Analogicznie dowodzimy, że $((u^2 - 1)^2, 0) = T_1 + (0, 0) \notin 2E_3(K)$. □

Lemat 2.5.17 ([Nas13], Lemma 6.2)**.** *Grupa $E_3(\overline{\mathbb{Q}}(t))/E_3(\overline{\mathbb{Q}}(t))_{tors}$ jest wolną grupą abelową rangi* 3*. Generują ją warstwy punktów*

$$P_1 = (2(1 + \sqrt{2})(-1 + u)^2 u, 2\sqrt{-1}(1 + \sqrt{2})(-1 + (\sqrt{2} - u)^2)(-1 + u)^2 u),$$
$$P_2 = (2(u - 1)^2, 2(-1 + u)^2(-1 + 2u + u^2)),$$
$$P_3 = (1 - u^2, \frac{(-5 + t^2)u(-1 + u^2)}{5 + t^2}),$$

gdzie $u = \frac{2t}{5+t^2}$.

Dowód. Niech $K = \overline{\mathbb{Q}}(t)$. Para $(E_3(K)/E_3(K)_{\text{tors}}, \langle \cdot, \cdot \rangle_{E_3})$ jest kratą Mordella-Weila. Ze Stwierdzenia 2.2.21 oraz Tabeli 2.7 odczytujemy, że dla dowolnych $P, Q \in E_3(K)/E_3(K)_{\text{tors}}$ wartość iloczynu $\langle P, Q \rangle_{E_3}$ należy do $\frac{1}{4}\mathbb{Z}$. Z tego powodu definiujemy nową kratę $\Lambda = E_3(K)/E_3(K)_{\text{tors}}$ z iloczynem skalarnym $\langle \cdot, \cdot \rangle = 4\langle \cdot, \cdot \rangle_{E_3}$. Dzięki temu iloczyn dwóch elementów względem $\langle \cdot, \cdot \rangle$ zawsze jest liczbą całkowitą. Niech Λ' oznacza podkratę skończonego indeksu w Λ rozpiętą na punktach P_1, P_2, P_3. Oznaczmy przez n indeks $[\Lambda : \Lambda']$. Z formuł na iloczyn skalarny w Λ dostaniemy

$$\langle P_i, P_j \rangle = \begin{cases} 4i, & \text{gdy } i = j, \\ 0, & \text{gdy } i \neq j. \end{cases}$$

Zatem wyróżnik $\Delta(\Lambda') = 6 \cdot 4^3$ oraz na mocy Lematu 2.5.11

$$6 \cdot 4^3 = \Delta(\Lambda') = n^2\Delta(\Lambda).$$

Z tego wynika, że n dzieli 8. Udowodnimy, że $n = 1$. Korzystając z [Sil86, X,Proposition 1.4] wiemy, że istnieje injektywny homomorfizm

$$\psi : E_3(K)/2E_3(K) \hookrightarrow K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

Jeśli (x, y) jest punktem z $E_3(K) \setminus E_3(K)[2]$, to obraz $\psi(x, y)$ jest postaci

$$\psi(x, y) = (x, x - 4u^2).$$

Oznaczmy przez G grupę $E_3(K)$ oraz przez H podgrupę generowaną przez P_1, P_2, P_3, T_1, T_2. Indeks $[G : H]$ równa się n. Z twierdzenia o zgodnej bazie dla grup abelowych wynika, że istnieją $R_1, R_2, R_3 \in G$ takie, że G jest generowana przez R_1, R_2, R_3, T_1, T_2, a podgrupa H jest generowana przez $aR_1, bR_2, cR_3, T_1, T_2$ oraz $n = abc$ i $a \mid b$, $b \mid c$. Gdy $n = 8$, to $(a, b, c) \in \{(1, 1, 8), (1, 2, 4), (2, 2, 2)\}$. Gdy $n = 4$, to $(a, b, c) \in \{(1, 1, 4), (1, 2, 2)\}$ i gdy $n = 2$, to $(a, b, c) = (1, 1, 2)$.

Rozważmy pomocniczy homomorfizm $\phi : G \to G/2G$, $\phi(x) = x + 2G$ oraz złożenie $\eta = \psi \circ \phi$. Na podstawie Wniosku 2.5.15 oraz Lematu 2.5.16 wiemy, że $G/2G = (\mathbb{Z}/2\mathbb{Z})^4$. Ponadto skoro ψ jest injektywny, to $\eta(G) \cong (\mathbb{Z}/2\mathbb{Z})^4$. Dla $n = 8$ możliwe wybory trójek (a, b, c) implikują, że $\eta(H) \cong (\mathbb{Z}/2\mathbb{Z})^i$, $1 \leq i \leq 3$. Dla $n = 4$ dostajemy, że $\eta(H) \cong (\mathbb{Z}/2\mathbb{Z})^i$, $2 \leq i \leq 3$. Gdy $n = 2$, wówczas $\eta(H) \cong (\mathbb{Z}/2\mathbb{Z})^3$. Zatem, aby pokazać, że $H = G$, wystarczy udowodnić, że $\eta(H) = \eta(G) \cong (\mathbb{Z}/2\mathbb{Z})^4$. Numerycznie sprawdzamy, że

$$\begin{aligned}
\eta(P_1) &= \left((t(t^2+5), (t^2+5)t\left(-5 + \left(-2 + 2\sqrt{2}\right)t - t^2\right)\left(-5 + \left(2 + 2\sqrt{2}\right)t - t^2\right)\right), \\
\eta(P_2) &= (1, t^4 - 4t^3 + 6t^2 - 20t + 25), \\
\eta(P_3) &= (\left(t^2 - 2t + 5\right)\left(t^2 + 2t + 5\right), 1), \\
\eta(T_2) &= (t\left(t^2 - 2t + 5\right)\left(t^2 + 2t + 5\right)(t^2 + 5), t\left(t^4 + 4t^3 + 6t^2 + 20t + 25\right)(t^2 + 5)).
\end{aligned}$$

Obrazy $\eta(P_1), \eta(P_2), \eta(P_3), \eta(T_2)$ rozpinają w $K^\times/(K^\times)^2 \times K^\times/(K^\times)^2$ podgrupę rzędu 16 i skoro $\mid \eta(G) \mid = 16$, to $\eta(H) = \eta(G)$. □

Wniosek 2.5.18 ([Nas13, Corollary 6.3])**.** *Grupa $E_3(\mathbb{Q}(t))$ jest izomorficzna z $\mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Generatorami są punkty P_2, P_3 oraz T_1, $2T_2$.*

Dowód. Niech $H = E_3(\mathbb{Q}(t))$ oraz $G = E_3(\overline{\mathbb{Q}}(t))$. Istnieje naturalne działanie grupy Galois $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ na punktach z G. Niech $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ oraz $f(t) \in \overline{\mathbb{Q}}[t]$ będzie wielomianem postaci $f(t) = \sum_{i=0}^n a_i t^i$, $a_i \in \overline{\mathbb{Q}}$. Definiujemy $f^\sigma(t) = \sum_{i=0}^n \sigma(a_i)t^i$. Gdy $P = 0$ jest punktem zerowym w G, to kładziemy $\sigma(P) = P$. Gdy $0 \neq P = \left(\frac{x_1(t)}{x_2(t)}, \frac{y_1(t)}{y_2(t)}\right)$ jest punktem z G takim, że $x_1(t), x_2(t), y_1(t), y_2(t) \in \overline{\mathbb{Q}}[t]$, to definiujemy

$$\sigma(P) = \left(\frac{x_1^\sigma(t)}{x_2^\sigma(t)}, \frac{y_1^\sigma(t)}{y_2^\sigma(t)}\right).$$

W ten sposób otrzymujemy działanie grupy $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ na zbiorze G. Co więcej, działanie to zachowuje strukturę grupy w G, tzn. $\sigma(P+Q) = \sigma(P) + \sigma(Q)$ dla dowolnych $P, Q \in G$. Wynika to z faktu, że równanie krzywej E_3 jest określone nad $\mathbb{Q}$, a zatem morfizm $+ : G \times G \to G$ jest też określony nad $\mathbb{Q}$. Otrzymujemy w ten sposób reprezentację

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut(G).$$

Grupa H równa jest zbiorowi punktów stałych $G^{\rho(Gal(\overline{\mathbb{Q}}/\mathbb{Q}))}$. W szczególności, niech $\tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ będzie automorfizmem takim, że $\tau(\sqrt{-1}) = -\sqrt{-1}$ oraz $\tau(\sqrt{2}) = \sqrt{2}$. Jeśli $x = a_1P_1 + a_2P_2 + a_3P_3 + b_1T_1 + b_2T_2,\ a_1, a_2, a_3, b_1, b_2 \in \mathbb{Z}$ należy do H, to spełnia $\tau(x) = x$. Na generatorach mamy

$$\tau(P_1) = -P_1, \tau(P_2) = P_2, \tau(P_3) = P_3, \tau(T_1) = T_1, \tau(T_2) = -T_2.$$

Zatem z równości $\tau(x) = x$ wynika, że

$$2a_1P_1 + 2b_2T_2 = 0.$$

Mnożąc obustronnie przez dwa i korzystając z tego, że $4T_2 = 0$ oraz z tego, że rząd P_1 jest nieskończony, dostajemy $a_1 = 0$. Stąd na mocy powyższych równości

$$2b_2T_2 = 0,$$

co pociąga, że $b_2 = 2b_2', b_2' \in \mathbb{Z}$. Elementy $P_2, P_3, T_1, 2T_2$ należą do H, więc dowolny punkt $x \in H$ jest postaci

$$x = a_2P_2 + a_3P_3 + b_1T_1 + b_2'(2T_2).$$

Punkty P_2 i P_3 są liniowo niezależne i nieskończonego rzędu w G, więc grupa H ma rangę równą 2 i H/H_{tors} jest generowana przez P_2 i P_3. Ponadto część torsyjna H jest generowana przez T_1 i $2T_2 = (0, 0)$.

□

Lemat 2.5.19. *Grupa punktów torsyjnych w $E_2(\overline{\mathbb{Q}}(t))$ jest izomorficzna z $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ i generowana jest przez punkty*

$$T_1 = (4t^2, 0),$$
$$T_2 = (2(-t + t^3), 2\sqrt{-1}(t^2 - 1)t(-1 - 2t + t^2)).$$

Dowód. Dowód jest całkowicie analogiczny do dowodu Lematu 2.5.16. □

Lemat 2.5.20 ([Nas13, Lemma 6.5])**.** *Grupa $E_2(\overline{\mathbb{Q}}(t))$ jest izomorficzna z $\mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Część wolna jest generowana przez punkty*

$$P_1 = (2(1 + \sqrt{2})(-1 + t)^2t, 2\sqrt{-1}(1 + \sqrt{2})(-1 + (\sqrt{2} - t)^2)(-1 + t)^2t),$$
$$P_2 = (2(t - 1)^2, 2(-1 + t)^2(-1 + 2t + t^2)).$$

Część torsyjną generują punkty

$$T_1 = (4t^2, 0)$$
$$T_2 = (2(-t + t^3), 2\sqrt{-1}(t^2 - 1)t(-1 - 2t + t^2)).$$

Dowód. Struktura podgrupy punktów torsyjnych wynika z Lematu 2.5.19. Reszta dowodu przebiegać będzie analogicznie do dowodu Lematu 2.5.17. Niech $K = \overline{\mathbb{Q}}(t)$ oraz $(E_2(K)/E_2(K)_{\text{tors}}, \langle\cdot,\cdot\rangle_{E_2})$ będzie kratą Mordella-Weila. Z konfiguracji włókien osobliwych, podanej w Tabeli 2.6 otrzymamy $\langle P, Q\rangle_{E_2} \in \frac{1}{4}\mathbb{Z}$ dla dowolnych $P, Q \in E_2(K)/E_2(K)_{\text{tors}}$. Bezpośrednio obliczamy, że $\langle P_1, P_1\rangle_{E_2} = 1/2$ i $\langle P_2, P_2\rangle_{E_2} = 1$ oraz $\langle P_1, P_2\rangle_{E_2} = \langle P_2, P_1\rangle_{E_2} = 0$. Dla wygody rachunków normalizujemy iloczyn skalarny. Niech $\Lambda = E_2(K)/E_2(K)_{\text{tors}}$ będzie kratą z iloczynem $\langle\cdot,\cdot\rangle = 4\langle\cdot,\cdot\rangle_{E_2}$. Niech Λ' oznacza podkratę w Λ generowaną przez punkty P_1 i P_2. Krata Λ' jest indeksu n w Λ. Na mocy Lematu 2.5.11 otrzymujemy równość

$$8 = \Delta(\Lambda') = n^2\Delta(\Lambda).$$

Z tego wynika, że $n^2 \mid 8$, czyli $n \mid 2$. Niech G oznacza $E_2(K)$ i H będzie podgrupą generowaną przez P_1, P_2, T_1, T_2. Liczba n równa się $[G : H]$. Z twierdzenia o zgodnej bazie dla grup abelowych wynika, że istnieją $R_1, R_2 \in G$ takie, że G jest generowana przez R_1, R_2, T_1, T_2 oraz grupa H jest generowana przez aR_1, bR_2, T_1, T_2, gdzie $a \mid b$ oraz $ab = n$.
Podobnie jak w dowodzie Lematu 2.5.17 określamy homomorfizm

$$\psi : E_2(K)/2E_2(K) \hookrightarrow K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

Jeśli (x, y) jest punktem z $E_2(K) \setminus E_2(K)[2]$, to

$$\psi(x, y) = (x, x - 4t^2).$$

Rozważamy również $\phi : G \to G/2G$, $\phi(x) = x + 2G$ oraz definiujemy $\eta = \psi \circ \phi$. Na mocy Lematu 2.2.32 oraz Lematu 2.5.19 dostajemy, że $\eta(G) \cong (\mathbb{Z}/2\mathbb{Z})^3$.
Gdy $n = 2$, to wówczas $a = 1$, $b = 2$ i $\eta(H) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Do udowodnienia, że $G = H$ wystarczy pokazać, że $\eta(H) = \eta(G)$. Zatem elementy $\eta(P_1), \eta(P_2), \eta(T_2)$ generują grupę 8-elementową. Bezpośrednim rachunkiem sprawdzamy, że

$$\begin{aligned}
\eta(P_1) &= \left(t, t\left(-t + \sqrt{2} - 1\right)\left(-t + \sqrt{2} + 1\right)\right),\\
\eta(P_2) &= \left(1, \left(-t + \sqrt{2} - 1\right)\left(t + \sqrt{2} + 1\right)\right),\\
\eta(T_2) &= \left((-1 + t)t(1 + t), t\left(-t + \sqrt{2} + 1\right)\left(t + \sqrt{2} - 1\right)\right).
\end{aligned}$$

□

Dowód Lematu 2.5.20 stanowi modyfikację dowodu [Nas13, Lemma 6.5].

Wniosek 2.5.21. *Grupa $E_2(\mathbb{Q}(t))$ jest izomorficzna z $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Generatorami są punkty $P_1, P_2, T_1, 2T_2$.*

Dowód. Niech $G = E_2(\overline{\mathbb{Q}}(t))$ oraz $H = E_2(\mathbb{Q}(t))$. Wykorzystamy działanie grupy $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ na G, zdefiniowane analogicznie jak w dowodzie Wniosku 2.5.18. Niech dana będzie naturalna reprezentacja

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut(G).$$

Grupa H jest równa $G^{\rho(Gal(\overline{\mathbb{Q}}/\mathbb{Q}))}$. Dla $\tau \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ takiego, że $\tau(\sqrt{-1}) = -\sqrt{-1}$ i $\tau(\sqrt{2}) = \sqrt{2}$ oraz dowolnego $x = a_1P_1 + a_2P_2 + b_1T_1 + b_2T_2$, $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ otrzymamy

$$\tau(x) = -a_1P_1 + a_2P_2 + b_1T_1 - b_2T_2.$$

W szczególności, gdy $x \in H$, to $\tau(x) = x$, a stąd

$$2a_1P_1 + 2b_2T_2 = 0.$$

Z tego wynika, że $a_1 = 0$ oraz $2b_2T_2 = 0$ i $b_2 = 2b_2$, $b_2' \in \mathbb{Z}$. Zatem $P_2, T_1, 2T_2$ generują grupę H i P_2 generuje H/H_{tors}. □

2.5.3 Rodziny krzywych eliptycznych parametryzowane przez trójki pitagorejskie

Wykorzystując rezultaty uzyskane w poprzednim podrozdziale przeprowadzimy dowód Twierdzenia 2.1.9. Niech $\mathcal{E} = (S, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi)$ będzie ustaloną powierzchnią eliptyczną nad $\overline{\mathbb{Q}}$. Niech E będzie jej włóknem generycznym. Każdy punkt $P \in E(\overline{\mathbb{Q}}(t))$ wyznacza pewne cięcie $\sigma_P : \mathbb{P}^1_{\overline{\mathbb{Q}}} \to S$. Ustalamy element $t_0 \in \overline{\mathbb{Q}}$. Niech $\mathcal{E}_{t_0} = \pi^{-1}(t_0)$. Dane jest odwzorowanie

$$\sigma_{t_0} : E(\overline{\mathbb{Q}}(t)) \to \mathcal{E}_{t_0}(\overline{\mathbb{Q}}), \tag{2.25}$$

gdzie $\sigma_{t_0}(P) = \sigma_P(t_0)$. Jeśli włókno $\mathcal{E}_{t_0}$ jest nieosobliwe, to odwzorowanie σ_{t_0} jest homomorfizmem grup.

Twierdzenie 2.5.22 ([Sil94, III, Theorem 11.4])**.** *Niech $\mathcal{E} = (S, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi)$ będzie powierzchnią eliptyczną, a E jej włóknem generycznym. Istnieje skończony podzbiór $L \subset \mathbb{Q}$ taki, że odwzorowanie σ_{t_0} jest injektywne dla wszystkich $t_0 \in \mathbb{Q} \setminus L$.*

Uwaga 2.5.23. Jeśli krzywa eliptyczna E jest określona nad $\mathbb{Q}(t)$, to $E(\mathbb{Q}(t))$ jest podgrupą w $E(\overline{\mathbb{Q}}(t))$. Z konstrukcji modelu Kodairy-Nérona wiemy, że dla tak zadanej krzywej E powierzchnia S może być wybrana tak, aby była określona nad $\mathbb{Q}$ oraz wszystkie włókna nieosobliwe nad punktami z $\mathbb{Q}$ były krzywymi eliptycznymi nad $\mathbb{Q}$. Wybieramy $t_0 \in \mathbb{Q}$ takie, że krzywa $\mathcal{E}_{t_0}$ jest nieosobliwa. Zatem grupa $\mathcal{E}_{t_0}(\mathbb{Q})$ jest skończenie generowana. Twierdzenie 2.5.22 daje oszacowanie

$$ranga\, E(\mathbb{Q}(t)) \leq ranga\, \mathcal{E}_{t_0}(\mathbb{Q})$$

dla $t_0 \in \mathbb{Q} \setminus L$.

Dowód Twierdzenia 2.1.9. Na mocy Wniosku 2.5.18 oraz Twierdzenia 2.5.22 i Uwagi 2.5.23 otrzymujemy, że istnieje skończony zbiór S taki, że dla $t_0 \in \mathbb{Q} \setminus S$ krzywa eliptyczna

$$E_{t_0} : y^2 = x(x - ((\frac{2t_0}{5 + t_0^2})^2 - 1)^2)(x - 4(\frac{2t_0}{5 + t_0^2})^2)$$

ma grupę Mordella-Weila $E_{t_0}(\mathbb{Q})$ rangi co najmniej równej 2. Ponadto dwa punkty liniowo niezależne są postaci

$$P_2 = (2(u_0-1)^2, 2(-1+u_0)^2(-1+2u_0+u_0^2)),$$
$$P_3 = (1-u_0^2, \frac{(-5+t_0^2)u_0(-1+u_0^2)}{5+t_0^2}),$$

gdzie $u_0 = \frac{2t_0}{5+t_0^2}$. Element u_0 reprezentuje pewną klasę elementów ze zbioru $\mathcal{T}_1/\sim$. Na mocy Lematu 2.1.8 odpowiada jej klasa równoważności trójek $(a,b,c) \in \mathcal{P}_1$ spełniających równanie Pitagorasa $a^2+b^2=c^2$. Wówczas krzywa eliptyczna

$$E_{(a,b,c)} : y^2 = x(x-a^2)(x-b^2)$$

jest $\mathbb{Q}$-izomorficzna z krzywą E_{t_0}. Izomorfizm dany jest wzorem

$$\psi : E_{t_0} \to E_{(a,b,c)} : x \mapsto x\frac{(c-a)^2}{4}, \quad y \mapsto y\frac{(c-a)^3}{8}.$$

W szczególności ranga grupy $E_{(a,b,c)}(\mathbb{Q})$ również wynosi co najmniej 2. Ponadto dwa punkty liniowo niezależne na krzywej $E_{(a,b,c)}$ są dane wzorami

$$\psi(P_2) = \left(\frac{1}{2}(a+b-c)^2, \frac{1}{2}(a+b)(a+b-c)^2\right),$$
$$\psi(P_3) = \left(\frac{1}{2}a(a-c), \frac{1}{2}ab\frac{1}{k^2}\left(p^4-25q^4\right)\right),$$

gdzie $t_0 = \frac{p}{q}$, $p,q \in \mathbb{Z}$ oraz $k = NWD(2pq, p^2+5q^2)$. □

Uwaga 2.5.24. Na krzywej eliptycznej

$$E_{(a,b,c)} : y^2 = x(x-a^2)(x-b^2)$$

leży punkt (c^2, abc), por. [INK10]. Poprzez $\mathbb{Q}$-izomorfizm $\eta : E_{(a,b,c)} \to E_{b/(c-a)}$

$$\eta(x,y) = \left(x\frac{4}{(a-c)^2}, y\frac{8}{(c-a)^3}\right)$$

odwzorowujemy punkt (c^2, abc) w punkt

$$P = ((t^2+1)^2, -2t(t^4-1)), \quad t = b/(c-a).$$

Na krzywej E_t, punkt P jest podzielny przez -2, tzn.

$$P = -2(2(t-1)^2, 2(t-1)^2(-1+2t+t^2)).$$

Przykładając do równania izomorfizm η^{-1} otrzymujemy równość punktów na krzywej $E_{(a,b,c)}$

$$(c^2, abc) = -2\left(\frac{1}{2}(a+b-c)^2, \frac{1}{2}(a+b)(a+b-c)^2\right).$$

Stosując twierdzenie o specjalizacji do krzywej $y^2 = x(x-(t^2-1)^2)(x-4t^2)$ oraz korzystając z Lematu 2.5.20 otrzymamy, że punkt (c^2, abc) jest nieskończonego rzędu dla prawie wszystkich wyborów klas $[(a,b,c)]_\sim$ z $\mathcal{P}_0/\sim$.

2.6 Rangi w rodzinach krzywych II

W tym podrozdziale badamy zachowanie rangi grupy Mordella-Weila w rodzinie krzywych eliptycznych postaci

$$y^2 = x(x - f^2)(x - g^2) \tag{2.26}$$

gdzie f, g są wielomianami z $\overline{\mathbb{Q}}[t]$. Główne wyniki dotyczą przypadku, gdy istnieje wielomian $h \in \overline{\mathbb{Q}}[t]$, taki, że $f^2 + g^2 = h^2$.

Stwierdzenie 2.6.1. *Niech $f, g, h \in \overline{\mathbb{Q}}[t]$ będą wielomianami spełniającymi relację $f^2 + g^2 = h^2$. Załóżmy, że f i g są względnie pierwsze (nie mają wspólnych pierwiastków w $\overline{\mathbb{Q}}$). Wówczas istnieją wielomiany $h_1, h_2 \in \overline{\mathbb{Q}}[t]$, względnie pierwsze takie, że*

$$f = \frac{1}{2}(h_1^2 + h_2^2), \tag{2.27}$$

$$g = \frac{1}{2i}(h_1^2 - h_2^2), \quad i = \sqrt{-1}, \tag{2.28}$$

$$h = h_1 h_2. \tag{2.29}$$

Na odwrót, dla dowolnie wybranych wielomianów $h_1, h_2 \in \overline{\mathbb{Q}}[t]$ względnie pierwszych, wielomiany f, g i h określone wzorami (2.27), (2.28) oraz (2.29) spełniają $f^2 + g^2 = h^2$ oraz f, g są względnie pierwsze.

Dowód. Dowiedziemy najpierw istnienia rozkładu $h = h_1 h_2$ takiego, że f, g, które są dane w tezie spełniają równości (2.27) i (2.28). Zauważmy, że z założenia wynika, że wielomiany $f + ig$ i $f - ig$ są względnie pierwsze oraz $(f + ig)(f - ig) = h^2$. Z jednoznaczności rozkładu w pierścieniu $\overline{\mathbb{Q}}[t]$ wynika, że $f + ig$ i $f - ig$ są pełnymi kwadratami. Zatem istnieją $h_1, h_2 \in \overline{\mathbb{Q}}[t]$ takie, że $f + ig = h_1^2$, $f - ig = h_2^2$ oraz $h_1 h_2 = h$. Stąd otrzymujemy już wzory (2.27) i (2.28) poprzez dodanie lub odjęcie wcześniejszych równości stronami. Skoro $f + ig$ i $f - ig$ są względnie pierwsze, to tym bardziej h_1, h_2 są względnie pierwsze.

Na odwrót, mając dane wielomiany $h_1, h_2 \in \overline{\mathbb{Q}}[t]$ oraz wielomiany f, g dane wzorami (2.27), (2.28) oraz $h = h_1 h_2$ łatwo sprawdzamy, że zachodzi równość $f^2 + g^2 = h^2$. Niech h_1, h_2 będą względnie pierwsze. Gdyby dla pewnego $a \in \overline{\mathbb{Q}}$ zachodziło $f(a) = g(a)$, to na mocy równości (2.27), (2.28), otrzymalibyśmy, że $h_1^2(a) = h_2^2(a) = 0$, a więc również $h_1(a) = h_2(a) = 0$, co przeczy założeniu o h_1, h_2. □

Lemat 2.6.2. *Niech $f, g \in \overline{\mathbb{Q}}[t]$ będą względnie pierwsze. Wtedy równanie 2.26 jest globalnie minimalnym modelem Weierstrassa krzywej eliptycznej nad $\overline{\mathbb{Q}}(t)$.*

Dowód. Bez utraty ogólności możemy założyć, że $\deg g \leq \deg f$. Współczynniki równania (2.26) wynoszą $a_2 = -f^2 - g^2$ i $a_4 = f^2 g^2$ oraz $a_i = 0$ dla $i \in \{1, 3, 6\}$. W szczególności, spełniony jest warunek (i) z Twierdzenia 2.2.6. Kładziemy $n = \deg f$. Wówczas zachodzi nierówność $\deg a_2 \leq 2 \max\{\deg f, \deg g\} = 2n$. Ponadto

$\deg a_4 = 2(\deg f + \deg g) \leq 4 \deg f = 4n$, zachodzi więc warunek (ii) z Twierdzenia 2.2.6. Nierówność

$$\deg a_4 \geq (\deg f - 1) \cdot 4 \tag{2.30}$$

jest równoważna $2 \geq \deg f - \deg g$. Jeśli zachodzi nierówność (2.30), to spełniony jest warunek (iii) z Twierdzenia 2.2.6. Jeśli nierówność (2.30) nie jest spełniona, to $2 < \deg f - \deg g$, a więc $\deg(f^2+g^2) = 2\deg f$, zatem $\deg a_2 = 2\deg f > (\deg f - 1) \cdot 2$, więc spełniony jest ponownie warunek (iii) ze wspomnianego twierdzenia. Niech v_a oznacza waluację względem $a \in \overline{\mathbb{Q}}$ określoną w (2.5). Nierówność $v_a(a_2) < 2$ jest równoważna $v_a(f^2 + g^2) < 2$. Podobnie $v_a(a_4) < 4$ jest równoważne $v_a(f) + v_a(g) < 2$. Jeśli zachodzi nierówność $v_a(a_4) < 4$ dla a, to spełniony jest warunek (iv) z Twierdzenia 2.2.6 dla a. Gdy $v_a(a_4) \geq 4$, to zachodzi $v_a(f) \geq 2$ lub $v_a(g) \geq 2$, bo f, g są względnie pierwsze. Ale wtedy $(f^2 + g^2)(a) \neq 0$ i $v_a(a_2) = 0 < 2$, więc zachodzi ponownie warunek (iv) dla a.

Na mocy powyższych argumentów i Twierdzenia 2.2.6 równanie (2.26) określa model globalnie minimalny krzywej eliptycznej nad $\overline{\mathbb{Q}}(t)$.

□

Lemat 2.6.3. *Niech $f, g \in \overline{\mathbb{Q}}[t]$ będą względnie pierwsze. Krzywej eliptycznej E nad $\overline{\mathbb{Q}}(t)$ zadanej równaniem (2.26) odpowiada powierzchnia eliptyczna $\mathcal{E} = (S, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi)$, której włókna osobliwe mają redukcję typu I_n dla odpowiednich n. Dokładniej, wyróżnik równania (2.26) jest dany wzorem*

$$\Delta = 16 f^4 g^4 \left(f^2 - g^2\right)^2.$$

Ponadto

(i) jeśli a jest zerem wielomianu f lub g, krotności e, to powierzchnia eliptyczna $\mathcal{E}$ ma nad punktem a włókno osobliwe typu I_{4e},

(ii) jeśli a jest zerem wielomianu $f^2 - g^2$, krotności e, to powierzchnia eliptyczna $\mathcal{E}$ ma nad punktem a włókno osobliwe typu I_{2e}.

(iii) jeśli $a = \infty$ i $\deg f \geq \deg g$, to powierzchnia eliptyczna $\mathcal{E}$ ma nad punktem a włókno osobliwe typu I_n, gdzie $n = 8\deg f - 4\deg g - 2\deg(f^2 - g^2)$.

Dowód. Na mocy Tabeli 2.1 otrzymujemy podany wzór na wyróżnik równania Weierstrassa postaci (2.26). Ponadto j-niezmiennik tego równania wynosi

$$j = \frac{256\left(f^4 - f^2 g^2 + g^4\right)^3}{f^4 g^4 \left(f^2 - g^2\right)^2}.$$

Lemat 2.6.2 implikuje, że równanie (2.26) jest modelem globalnie minimalnym dla krzywej E. Na mocy algorytmu Tate'a (patrz §2.2.1) oraz Tabeli 2.3 odczytujemy, że zachodzą warunki (i) oraz (ii). Na mocy założenia $\deg f \geq \deg g$ w punkcie (iii), Lematu 2.2.11 oraz dowodu Lematu 2.6.2 otrzymujemy, że $\chi(S) = \chi(S, \mathcal{O}_S) = \deg f$ oraz $v_\infty(\Delta) = 12\deg f - \deg(\Delta)$. Ponadto zamiana zmiennych $(x, y) \mapsto (x/s^{2\chi(S)}, y/s^{3\chi(S)})$ opisana po Uwadze 2.2.4 pozwala stwierdzić, że redukcja w punkcie ∞ jest typu I_n, gdzie $n = v_\infty(\Delta)$ na mocy algorytmu Tate'a, co kończy dowód punktu (iii). □

Lemat 2.6.4. *Niech $f, g \in \overline{\mathbb{Q}}[t]$ będą względnie pierwsze. Krzywej eliptycznej E nad $\overline{\mathbb{Q}}(t)$ zadanej równaniem (2.26) odpowiada powierzchnia eliptyczna $\mathcal{E} = (S, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi)$. Niech $P = (x, y)$ będzie punktem z grupy $E(\overline{\mathbb{Q}}(t))$. Wówczas wysokość punktu P rozumiana w sensie Definicji 2.2.20 wynosi*

$$\langle P, P\rangle = 2\chi(S) + 2\overline{P}.\overline{O} - \sum_{a\in B} c_a(P, P). \tag{2.31}$$

Niech B będzie zbiorem złożonym z punktów, nad którymi powierzchnia $\mathcal{E}$ ma złą redukcję. Zachodzi wzór

$$\overline{P}.\overline{O} = -\frac{1}{2}\sum_{a\in\mathbb{P}^1_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}})} \min\{0, v_a(x)\}. \tag{2.32}$$

Niech $a \in B$. Jeśli krzywa $\overline{P}$ przecina we włóknie nad a tę samą składową co $\overline{O}$, to kładziemy $c_a(P, P) = 0$. W przeciwnym przypadku, niech $n = \min\{v_a(y), v_a(\Delta)/2\}$, gdzie Δ jest wyróżnikiem równania (2.26). Wówczas

$$c_a(P, P) = \frac{n(N-n)}{N} \tag{2.33}$$

o ile włókno nad a jest typu I_N.

Dowód. Niech P będzie punktem określonym w tezie. Na mocy Stwierdzenia 2.2.21 otrzymujemy równość (2.31). Formuła (2.32) jest przedstawiona w [Sil94, III,§9]. Równość (2.33) wynika z dowodu [Shi90, Theorem 8.6] oraz [Cre08, §1], [Sil88, §5, (28)]. □

Lemat 2.6.5. *Niech $f, g \in \overline{\mathbb{Q}}[t]$ będą względnie pierwsze. Niech E nad $\overline{\mathbb{Q}}(t)$ będzie krzywą eliptyczną określoną równaniem (2.26). Wówczas punkty*

$$\begin{aligned} T_1 &= (g^2, 0),\\ T_2 &= (fg, \sqrt{-1}f(f-g)g) \end{aligned}$$

rozpinają w $E(\overline{\mathbb{Q}}(t))$ podgrupę izomorficzną z $\mathbb{Z}/2 \oplus \mathbb{Z}/4\mathbb{Z}$.

Dowód. Niech $P = (x, y) \in E(\overline{\mathbb{Q}}(t))$ będzie pewnym ustalonym punktem. Gdy P jest rzedu 2, to $P = -P$ i $y = 0$, więc $P \in \{(0, 0), (g^2, 0), (f^2, 0)\}$. Gdy P nie jest punktem rzędu 2, to korzystając z formuły na podwojenie punktu otrzymujemy wzór na pierwszą współrzędną punktu $2P$

$$x(2P) = \frac{(x - fg)^2(fg + x)^2}{4x\,(x - f^2)\,(x - g^2)}. \tag{2.34}$$

Załóżmy, że P jest takim punktem, że $2P = (0, 0)$. Oznacza to, że $(x - fg)^2(fg + x)^2 = 0$. Otrzymujemy cztery punkty,

$$P_{\epsilon_1,\epsilon_2} = (\epsilon_1 fg, \epsilon_2\sqrt{-1}fg(f - \epsilon_1 g)), \quad \epsilon_1, \epsilon_2 \in \{\pm 1\}.$$

Każdy z punktów $P_{\epsilon_1,\epsilon_2}$ jest rzędu 4, bo $4P = O$ i $2P = (0, 0) \neq O$. Ponadto zauważmy, że zbiór $\{P_{1,1}, P_{-1,1}, P_{1,-1}, P_{-1,-1}\}$ jest równy zbiorowi $\{P_{1,1}, P_{1,1} + (g^2, 0), P_{1,1} + (f^2, 0), P_{1,1} + (0, 0)\}$. W szczególności, punkty $(g^2, 0)$ oraz $P_{1,1}$ rozpinają grupę izomorficzną z $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. □

Przykład 2.6.6. Niech $f = -1 + t^2$ i $g = 1 + t^2$. Jeśli krzywa E jest dana równaniem (2.26), to $E(\overline{\mathbb{Q}}(t))_{\text{tors}} \cong \mathbb{Z}/4 \oplus \mathbb{Z}/4\mathbb{Z}$. Zauważmy, że w tej sytuacji $f^2 + g^2$ nie jest kwadratem w $\overline{\mathbb{Q}}[t]$. Punkt T_2 z poprzedniego lematu oraz T_3, który spełnia $2T_3 = (g^2, 0)$ generują całą grupę $E(\overline{\mathbb{Q}}(t))[4]$. Powierzchnia eliptyczna stowarzyszona z E ma wszystkie włókna złej redukcji typu I_4, więc na mocy Lematu 2.2.22 otrzymujemy $E(\overline{\mathbb{Q}}(t))_{\text{tors}} = E(\overline{\mathbb{Q}}(t))[4]$.

Wniosek 2.6.7. *Niech $f, g \in \overline{\mathbb{Q}}[t]$ będą względnie pierwsze. Niech $\deg f = 2$ i $1 \leq \deg g \leq 2$. Niech $f, g, f^2 - g^2$ będą rozdzielcze oraz $\deg(f^2 - g^2) = 2\deg f$. Niech E nad $\overline{\mathbb{Q}}(t)$ będzie krzywą eliptyczną określoną równaniem (2.26). Wówczas $E(\overline{\mathbb{Q}}(t))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.*

Dowód. Niech $\mathcal{E} = (S, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi)$ będzie powierzchnią eliptyczną, której włóknem generycznym jest E. Na mocy Lematu 2.6.3 wszystkie włókna złej redukcji dla $\mathcal{E}$ są typu I_2 lub I_4. Z Lematu 2.2.22 wynika, że w grupie $E(\overline{\mathbb{Q}}(t))_{\text{tors}}$ mogą istnieć tylko elementy rzędów podzielnych przez 4. Zauważmy, że punkty 2 torsyjne w $E(\overline{\mathbb{Q}}(t))_{\text{tors}}$ są postaci $(f^2, 0), (g^2, 0)$ lub $(0, 0)$. Na mocy Lematu 2.6.5 wystarczy pokazać, że nie istnieje punkt $P \in E(\overline{\mathbb{Q}}(t))_{\text{tors}}$ taki, że $2P = (g^2, 0)$ lub $2P = (f^2, 0)$. Przypuśćmy, że $P = (x, y)$ oraz $2P = (g^2, 0)$. Ze wzorów na podwojenie punktu otrzymujemy

$$\frac{(x - fg)^2(fg + x)^2}{4x\,(x - f^2)\,(x - g^2)} - g^2 = 0$$

lub równoważnie

$$-f^2g^2 + 2g^2x - x^2 = 0.$$

Wyróżnik tego równania kwadratowego względem x wynosi $-4(f - g)g^2(f + g)$. Z założeń lematu wynika jednak, że $f^2 - g^2$ jest rozdzielczy, więc nie jest pełnym kwadratem, a zatem nie istnieje $x \in \overline{\mathbb{Q}}(t)$ będące rozwiązaniem ostatniego równania. Argumentacja jest identyczna w przypadku, gdy $2P = (f^2, 0)$. Zatem podgrupa punktów torsyjnych w $E(\overline{\mathbb{Q}}(t))_{\text{tors}}$ podana w Lemacie 2.6.5 jest w istocie całą grupą punktów torsyjnych. □

Lemat 2.6.8. *Niech $f, g \in \overline{\mathbb{Q}}[t]$ będą względnie pierwsze oraz niech istnieje $h \in \overline{\mathbb{Q}}[t]$ taki, że $f^2 + g^2 = h^2$. Ponadto załóżmy, że $\deg g \leq \deg f$ oraz $\deg f > 0$. Niech E nad $\overline{\mathbb{Q}}(t)$ będzie krzywą eliptyczną określoną równaniem (2.26). Wówczas punkty*

$$\begin{aligned} Q_1 &= (-g^2, \sqrt{-2}g^2h) \\ Q_2 &= (h^2, fgh) \end{aligned}$$

są nieskończonego rzędu oraz $\langle Q_1, Q_2 \rangle = \deg f$ i $\langle Q_2, Q_2 \rangle = 2\deg f$. Grupa generowana przez Q_1, Q_2 ma rangę 2.

Dowód. Niech $\mathcal{E} = (S, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi)$ będzie powierzchnią eliptyczną stowarzyszoną z E. Z dowodu Lematu 2.6.3 wynika, że $\chi(S) = \deg f$. W szczególności, dla parametru s takiego, że $t = 1/s$ zachodzi równość

$$Q_1 = (-g(1/s)^2 s^{2\deg f}, \sqrt{-2}g(1/s)^2 h(1/s) s^{3\deg f}). \tag{2.35}$$

Zatem dla waluacji w nieskończoności $v_\infty = v_s$ mamy $v_s(x(Q_1)) = 2\deg f - 2\deg g \geq 0$. Niech $a \in \overline{\mathbb{Q}}$. Dla waluacji v_a rozważamy punkt Q_1 w układzie współrzędnych ze zmienną t. Zauważmy, że $v_a(x(Q_1)) = v_a(-g^2) \geq 0$. Na mocy równości (2.32) z Lematu 2.6.4 otrzymujemy

$$\overline{Q_1}.\overline{O} = 0.$$

Niech B oznacza zbiór punktów w $\mathbb{P}^1_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}})$ złej redukcji dla powierzchni eliptycznej $\mathcal{E}$. Ze względu na Lemat 2.6.3 oznacza to, że $a \in B$ wtedy i tylko wtedy, gdy $(f \cdot g \cdot (f^2 - g^2))(a) = 0$ lub $a = \infty$. Krzywa $\overline{Q_1}$ przecina tę samą składową, co $\overline{O}$ we włóknie nad $a \in B \setminus \{\infty\}$, wtedy gdy $g(a) \neq 0$. Jeśli $a \in B \setminus \{\infty\}$ spełnia $g(a) = 0$, to punkt Q_1 redukuje się we włóknie do punktu osobliwego $(0, 0)$. Zatem krzywa $\overline{Q_1}$ we włóknie nad a przecina inną składową niż $\overline{O}$. Zauważmy, że $v_a(y(Q_1)) = v_a(\sqrt{-2}g^2h) = \frac{1}{2}v_a(\Delta)$. Niech $n = \min\{v_a(y(Q_1)), v_a(\Delta)/2\}$, wtedy $n = 2v_a(g)$. Włókno nad punktem a ma typ redukcji $I_{4v_a(g)}$, a więc ma $N = 4v_a(g)$ składowych. Ze wzoru (2.33) z Lematu 2.6.4 odczytujemy

$$c_a(P, P) = v_a(g).$$

Jeśli $a = \infty$ i $a \in B$, to wykorzystujemy wzór (2.35) w lokalnym układzie współrzędnych wokół nieskończoności. W tym przypadku krzywa $\overline{Q_1}$ nie przecina tej samej składowej, co $\overline{O}$ nad punktem a dokładnie wtedy, gdy $2\deg f > 2\deg g$ i $3\deg f > 2\deg g + \deg h$. Jeśli zatem $\deg f > \deg g$, to również $\deg h = \deg f$, bo $h^2 = f^2 + g^2$. Włókno nad a ma $N = 12\deg f - \deg\Delta$ składowych, czyli $N = 4(\deg f - \deg g)$. Ponadto $n = \min\{v_a(y(Q_1)), v_a(\Delta)/2\} = \min\{2(\deg f - \deg g), 2(\deg f - \deg g)\} = 2(\deg f - \deg g)$. Stosując ponownie wzór (2.33) otrzymujemy

$$c_a(P, P) = \deg f - \deg g.$$

Stosując równość (2.31) dostajemy

$$\langle Q_1, Q_1\rangle = 2\deg f - \deg g - (\deg f - \deg g) = \deg f.$$

Dla $t = 1/s$, analogicznie do równości (2.35), otrzymujemy wzór

$$Q_2 = (h(1/s)^2 s^{2\deg f}, f(1/s)g(1/s)h(1/s)s^{3\deg f}). \tag{2.36}$$

Rozumując analogicznie jak w przypadku punktu Q_1 otrzymamy $\overline{Q_2}.\overline{O} = 0$. Wielomiany h^2, fgh i Δ są względnie pierwsze. Zatem dla $a \in B \setminus \{\infty\}$ krzywa $\overline{Q_2}$ przecina tę samą składową co $\overline{O}$ we włóknie nad a. Jeśli $a = \infty$, to krzywa $\overline{Q_2}$ nie przecina składowej $\overline{O}$ we włóknie nad a wtedy i tylko wtedy, gdy $2\deg f > 2\deg h$ i $2\deg f > \deg g + \deg h$. Pierwsza nierówność implikuje, że $\deg f = \deg g$ na mocy definicji h. Ponadto jeśli $f^2 = a_m t^m + \ldots$ i $g^2 = b_m t^m + \ldots$, to $a_m = -b_m \neq 0$, więc $f^2 - g^2 = 2a_m t^m + \ldots$, zatem $\deg(f^2 - g^2) = \deg(f^2) = 2\deg f$. Włókno nad a ma

$$N = 12\deg f - \deg\Delta = 4\deg f - 2\deg(f^2 - g^2)$$

składowych. Zatem, gdyby $\overline{Q_2}$ nie przecinało nad a składowej $\overline{O}$, to włókno nad a miałoby $N = 0$ składowych, co jest niemożliwe, bo włókno ma co najmniej 1 składową. Zatem $c_\infty(Q_2, Q_2) = 0$. Stosując równość (2.31) otrzymujemy

$$\langle Q_2, Q_2\rangle = 2\deg f.$$

Dowód Stwierdzenia 2.2.21 implikuje, że punkty Q_1 i Q_2 są nieskończonego rzędu, bo ich wysokość jest większa od 0. Ponadto zauważmy, że punkty Q_1, Q_2 są liniowo niezależne dokładnie wtedy, gdy wyznacznik macierzy Grama względem $\langle , \rangle$ jest niezerowy. Sprawdzamy, że

$$\det \begin{pmatrix} \langle Q_1, Q_1\rangle & \langle Q_1, Q_2\rangle \\ \langle Q_2, Q_1\rangle & \langle Q_2, Q_2\rangle \end{pmatrix} = 2(\deg f)^2 - \langle Q_1, Q_2\rangle^2. \tag{2.37}$$

Ale równość $2(\deg f)^2 - \langle Q_1, Q_2\rangle^2 = 0$ jest niemożliwa, bo $\langle Q_1, Q_2\rangle$ jest liczbą wymierną, a $\deg f > 0$.

□

Wniosek 2.6.9. *Przy założeniach i oznaczeniach z poprzedniego lematu, punkty*

$$\begin{aligned} P_1 =&(-(1+\sqrt{2})g(g-h), \sqrt{-1}(1+\sqrt{2})g(g-h)(\sqrt{2}g-h)),\\ P_2 =&((f-h)(g-h), (f+g)(f-h)(g-h)) \end{aligned}$$

są nieskończonego rzędu i liniowo niezależne w $E(\overline{\mathbb{Q}}(t))$. Macierz Grama względem $\langle , \rangle$ ma postać

$$\begin{pmatrix} \langle P_1, P_1\rangle & \langle P_1, P_2\rangle \\ \langle P_2, P_1\rangle & \langle P_2, P_2\rangle \end{pmatrix} = \begin{pmatrix} \frac{1}{4}\deg f & 0 \\ 0 & \frac{1}{2}\deg f \end{pmatrix} \tag{2.38}$$

oraz zachodzą równości

$$Q_1 = -2P_1, \tag{2.39}$$
$$Q_2 = -2P_2. \tag{2.40}$$

Dowód. Zauważmy, że równości (2.39) oraz (2.40) wynikają z faktu, że $f^2 + g^2 = h^2$ oraz bezpośredniego rachunku na współrzędnych. Na mocy Lematu 2.6.8 mamy równość $\langle Q_1, Q_1\rangle = \deg f$. Iloczyn skalarny $\langle , \rangle$ jest dwuliniowy, więc $\langle -2P_1, -2P_1\rangle = \deg f$ i dalej $\langle P_1, P_1\rangle = \frac{1}{4}\deg f$. Analogicznie otrzymujemy równość $\langle P_2, P_2\rangle = \frac{1}{2}\deg f$. Wysokości punktów P_1 i P_2 są dodatnie na mocy założenia $\deg f > 0$, więc oba punkty są nieskończonego rzędu. Wyznacznik macierzy Grama (2.38) jest równy $\frac{1}{8}(\deg f)^2 - \langle P_1, P_2\rangle^2$ i nie może być równy zero, bo $\langle P_1, P_2\rangle$ jest liczbą wymierną na mocy definicji iloczynu $\langle , \rangle$. Zatem punkty P_1 i P_2 są liniowo niezależne. Wykażemy teraz, że zachodzi równość $\langle P_1, P_2\rangle = 0$. Ze względu na relacje (2.39) i (2.40) wystarczy udowodnić, że $\langle Q_1, Q_2\rangle = 0$. Z własności formy dwuliniowej dostajemy równość

$$\langle Q_1+Q_2, Q_1+Q_2\rangle = \langle Q_1, Q_1\rangle + \langle Q_2, Q_2\rangle + 2\langle Q_1, Q_2\rangle = 3\deg f + 2\langle Q_1, Q_2\rangle.$$

Zatem $\langle Q_1, Q_2\rangle = 0$ wtedy i tylko wtedy, gdy $\langle Q_1+Q_2, Q_1+Q_2\rangle = 3\deg f$. Wykażemy, że zachodzi ostatnia równość. Ze wzorów na dodawanie punktów w grupie $E(\overline{\mathbb{Q}}(t))$ otrzymujemy $Q := Q_1 + Q_2 = (x, y)$, gdzie

$$x = \frac{-f^4 - 2\sqrt{-2}f^3g + 3f^2g^2 + g^4}{\left(f + \sqrt{-2}g\right)^2}, \tag{2.41}$$

$$y = \frac{gh\left(-f^4 - \sqrt{-2}f^3g - 2f^2g^2 - 4\sqrt{-2}fg^3 + 3g^4\right)}{\left(f + \sqrt{-2}g\right)^3}. \tag{2.42}$$

Wprowadzamy oznaczenia

$$\begin{aligned} F_1 :=& -f^4 - 2\sqrt{-2}f^3g + 3f^2g^2 + g^4, \\ F_2 :=& gh\left(-f^4 - \sqrt{-2}f^3g - 2f^2g^2 - 4\sqrt{-2}fg^3 + 3g^4\right), \\ H :=& f + \sqrt{-2}g. \end{aligned}$$

Niech $\mathcal{E} = (S, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi)$ będzie powierzchnią eliptyczną stowarzyszoną z E. Niech B oznacza zbiór punktów złej redukcji w $\mathbb{P}^1_{\overline{\mathbb{Q}}}(\overline{\mathbb{Q}})$ dla powierzchni eliptycznej $\mathcal{E}$. Zatem $a \in B$ wtedy i tylko wtedy, gdy $(f \cdot g \cdot (f^2 - g^2))(a) = 0$ lub $a = \infty$. Obliczamy najpierw przecięcie $\overline{Q}.\overline{O}$. Zauważmy, że x ma biegun w $a \in \overline{\mathbb{Q}}$, gdy $v_a(F_1) < 2v_a(H)$. Ale jeśli $H(a) = 0$, to $F_1(a) \neq 0$, więc $v_a(x) = -2\deg H$. Z kolei, gdy $a = \infty$, to zapisując punkt Q w lokalnym układzie współrzędnych, dla którego $t = 1/s$, otrzymujemy

$$Q = \left(\frac{F_1(1/s)}{(H(1/s))^2}s^{2\deg f}, \frac{F_2(1/s)}{(H(1/s))^3}s^{3\deg f}\right).$$

Jeśli $\deg f > \deg g$, to $\deg F_1 = 4\deg f$ oraz $\deg H = \deg f$ i $v_s(x) = 0$.

Jeśli $\deg f = \deg g$, to analizę rozbijamy na dwa kolejne przypadki.

1° Niech $\deg H < \deg f$. Jeśli $f = a_m t^m + \ldots$ oraz $g = b_m t^m + \ldots$, to $a_m + \sqrt{-2}b_m = 0$, $a_m \neq 0, b_m \neq 0$. Współczynnik wiodący wielomianu F_1 ma postać

$$A := -a_m^4 - 2\sqrt{-2}a_m^3 b_m + 3a_m^2 b_m^2 + b_m^4.$$

Ze względu na równość $a_m = -\sqrt{-2}b_m$ liczba $A \neq 0$, więc $\deg F_1 = 4\deg f$. Zachodzi zatem równość $v_s(x) = -(2\deg f - 2\deg H)$.

2° Niech $\deg H = \deg f$. Wówczas $\deg F_1 \leq 4\deg f$ i $v_s(x) = 4\deg f - \deg F_1 \geq 0$. Łącząc powyższe przypadki i korzystając z formuły (2.32) otrzymujemy równość

$$\overline{Q}.\overline{O} = \deg f.$$

Udowodnimy teraz, że $\sum\limits_{a \in B} c_a(Q, Q) = 0$. Zauważmy najpierw, że jeśli $a \in B \setminus \{\infty\}$, to $x(a) \neq 0$, więc wówczas $c_a(Q, Q) = 0$. Jeśli $a = \infty$, to na podstawie wcześniejszych obliczeń mamy:

(i) jeśli $\deg f > \deg g$, to $v_\infty(x) = v_s(x) = 0$, więc $c_\infty(Q, Q) = 0$,

(ii) jeśli $\deg f = \deg g$ i $\deg H < \deg f$, to $v_\infty(x) < 0$, więc $c_\infty(Q, Q) = 0$,

(iii) jeśli $\deg f = \deg g$ i $\deg H = \deg f$, to $v_\infty(x) \geq 0$ oraz $v_\infty(y) \geq 0$.

Kontynuujemy rozumowanie z punktu (iii). Gdyby krzywa $\overline{Q}$ nie przecinała tej samej składowej, co $\overline{O}$ we włóknie nad a, to musiałoby zachodzić $v_a(x) > 0$ i $v_a(y) > 0$. Ale to jest możliwe tylko wtedy, gdy $\deg F_1 < 4 \deg f$ oraz $\deg F_2 < 6 \deg f$. Pierwsza nierówność oznacza, że $A = 0$, druga zaś oznacza, że

$$B := b_m\sqrt{a_m^2 + b_m^2}\left(-a_m^4 - \sqrt{-2}a_m^3 b_m - 2a_m^2 b_m^2 - 4\sqrt{-2}a_m b_m^3 + 3b_m^4\right) = 0.$$

Ale równości $A = 0$ i $B^2 = 0$ nie mogą zachodzić jednocześnie. Wystarczy zauważyć, że jeśli potraktujemy a_m i b_m jako zmienne, a i b, odpowiednio, to szukamy rozwiązań w zmiennych a, b, s układu równań

$$\begin{aligned} b^2(a^2 + b^2)(-a^4 - 2a^2b^2 + 3b^4 - a^3bs - 4ab^3s)^2 &= 0 \\ -a^4 + 3a^2b^2 + b^4 - 2a^3bs &= 0 \\ 2 + s^2 &= 0 \end{aligned}$$

Jeśli $b = 0$, to $a = 0$, ale to oznacza, że $a_m = b_m = 0$, co jest sprzeczne z założeniem, że a_m i b_m są współczynnikami wiodącymi wielomianów f i g. Jeśli $a^2 = -b^2$, to drugie równanie redukuje się do $-b^3(3b - 2as) = 0$ i ponownie $a = b = 0$. Pozostaje do rozważenia przypadek, gdy $-a^4 - 2a^2b^2 + 3b^4 - a^3bs - 4ab^3s = 0$. Stosując pakiet MAGMA sprawdzamy, że ideał

$$I = (-a^4 - 2a^2b^2 + 3b^4 - a^3bs - 4ab^3s, -a^4 + 3a^2b^2 + b^4 - 2a^3bs, s^2 + 2) \subset \mathbb{Q}[a, b, s]$$

można zapisać również (przy pomocy bazy Gröbnera) następująco

$$\begin{aligned} I = (a^4 + 7a^2b^2 + 8ab^3s - 5b^4, a^3b + \frac{5}{2}a^2b^2s - 4ab^3 - b^4s, a^2b^3 + \\ \frac{2}{3}ab^4s, ab^5 + \frac{9}{14}b^6s, b^7, s^2 + 2) \subset \mathbb{Q}[a, b, s]. \end{aligned}$$

Zatem układ

$$\begin{aligned} -a^4 - 2a^2b^2 + 3b^4 - a^3bs - 4ab^3s &= 0 \\ -a^4 + 3a^2b^2 + b^4 - 2a^3bs &= 0 \\ 2 + s^2 &= 0 \end{aligned}$$

jest równoważny $a = b = s^2 + 2 = 0$. Ostatecznie na mocy (2.31) zachodzi równość

$$\langle Q, Q \rangle = 3 \deg f.$$

□

Twierdzenie 2.6.10. *Niech $f, g \in \overline{\mathbb{Q}}[t]$ będą względnie pierwsze oraz niech istnieje $h \in \overline{\mathbb{Q}}[t]$ takie, że $f^2 + g^2 = h^2$. Załóżmy, że $\deg f = 2$ i $1 \leq \deg g \leq 2$ oraz $f, g, f^2 - g^2$ są rozdzielcze, a ponadto $\deg(f^2 - g^2) = 2 \deg f$. Niech E będzie krzywą eliptyczną określoną nad $\overline{\mathbb{Q}}(t)$ równaniem (2.26). Wówczas*

$$E(\overline{\mathbb{Q}}(t)) \cong \mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Grupę $E(\overline{\mathbb{Q}}(t))$ generują punkty

$$\begin{aligned}
P_1 =&(-(1+\sqrt{2})g(g-h), \sqrt{-1}(1+\sqrt{2})g(g-h)(\sqrt{2}g-h)),\\
P_2 =&((f-h)(g-h), (f+g)(f-h)(g-h)),\\
T_1 =&(g^2, 0),\\
T_2 =&(fg, \sqrt{-1}f(f-g)g).
\end{aligned}$$

Dowód. Niech $\mathcal{E} = (S, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi)$ będzie powierzchnią eliptyczną stowarzyszoną z E. Dla rozwłóknienia π oznaczymy przez N_∞ liczbę składowych włókna nad punktem w nieskończoności. Z Lematu 2.6.3 otrzymujemy, że $N_\infty = 8 - 4\deg g$. Niech r oznacza rangę grupy $E(\overline{\mathbb{Q}}(t))$. Na mocy Twierdzenia 2.2.18 liczba Picarda $\rho(S)$ powierzchni S jest równa

$$\rho(S) = 12 + 3\deg g + r + \max\{N_\infty - 1, 0\}.$$

Z założenia $\chi(S) = \deg f = 2$. Twierdzenie 2.2.19 daje górne ograniczenie

$$\rho(S) \leq 20.$$

Oznacza to, że $r \leq 8 - \max\{N_\infty - 1, 0\} - 3\deg g$. Jeśli $\deg g = 1$, to $N_\infty = 4$ i $r \leq 2$. Gdy $\deg g = 1$, to $N_\infty = 0$ (nie ma złej redukcji w ∞), więc $r \leq 2$. Wniosek 2.6.9 gwarantuje nam, że $r \geq 2$, więc $r = 2$.

Struktura grupy punktów torsyjnych została wyznaczona we Wniosku 2.6.7. Wykażemy teraz, że punkty P_1 i P_2 generują część wolną grupy $E(\overline{\mathbb{Q}}(t))$. Niech $(E(\overline{\mathbb{Q}}(t))/E(\overline{\mathbb{Q}}(t))_{\text{tors}}, \langle\cdot,\cdot\rangle_E)$ będzie kratą z iloczynem skalarnym $\langle\cdot,\cdot\rangle_E$ określonym jak w Definicji 2.2.20. Z konfiguracji włókien osobliwych dla π otrzymujemy $\langle P, Q\rangle_E \in \frac{1}{4}\mathbb{Z}$ dla $P, Q \in E(\overline{\mathbb{Q}}(t))/E(\overline{\mathbb{Q}}(t))_{\text{tors}}$. Na mocy Wniosku 2.6.9 uzyskujemy $\langle P_1, P_1\rangle_E = 1/2$ i $\langle P_2, P_2\rangle_E = 1$ oraz $\langle P_1, P_2\rangle_E = \langle P_2, P_1\rangle_E = 0$. Definiujemy kratę $\Lambda = E(\overline{\mathbb{Q}}(t))/E(\overline{\mathbb{Q}}(t))_{\text{tors}}$ z iloczynem skalarnym $\langle\cdot,\cdot\rangle = 4\langle\cdot,\cdot\rangle_E$. Dalej przeprowadzamy rozumowanie w pełni analogiczne do dowodu Lematu 2.5.20. W tym przypadku $G = E(\overline{\mathbb{Q}}(t))$, $\psi(x, y) = (x, x - f^2)$, $\phi : G \to G/2G$, $\phi(x) = x + 2G$ oraz $\eta = \psi \circ \phi$. Do udowodnienia, że punkty P_1 i P_2 generują część wolną grupy G wystarczy wykazać, że $G \cong (\mathbb{Z}/2\mathbb{Z})^3$. Trzeba zatem uzasadnić, że $\eta(P_1), \eta(P_2)$ i $\eta(T_2)$ generują grupę 8-elementową. Niech $\zeta = e^{2\pi\sqrt{-1}/8}$ będzie pierwiastkiem pierwotnym stopnia 8 z jedności. Korzystając ze Stwierdzenia 2.6.1 możemy napisać

$$\begin{aligned}
\eta(P_1) &= \left((h_1 - h_2)(h_1 + h_2), (\zeta h_1 + h_2)(\zeta^3 h_1 + h_2)\right),\\
\eta(P_2) &= \left(1, (\zeta h_1 + h_2)(\zeta^5 h_1 + h_2)\right),\\
\eta(T_2) &= \left((h_1 - h_2)(h_1 + h_2)(h_1^2 + h_2^2), (\zeta^2 h_1 + h_2)(\zeta^3 h_1 + h_2)(\zeta^6 h_1 + h_2)(\zeta^7 h_1 + h_2)\right).
\end{aligned}$$

dla pewnych h_1, h_2 określonych w Stwierdzeniu 2.6.1. Zauważmy, że pierwsza współrzędna $\eta(P_1)$ jest równa g z dokładnością do kwadratów, więc na mocy założenia nie jest równa 1 modulo $((\overline{\mathbb{Q}}(t))^\times)^2$, czyli $\eta(P_1)$ ma rząd 2.

Z założenia $\deg f = 2$ możemy przyjąć, że $h_1 = a(t-b)$, $h_2 = c(t-d)$ dla pewnych $a, b, c, d \in \overline{\mathbb{Q}}$. Wielomiany f, g nie mają wspólnych pierwiastków, więc $b \neq d$. Druga współrzędna $\eta(P_2)$ jest równa

$$(-\sqrt{-1})a^2b^2 + c^2d^2 + t\left(-2c^2d + 2\sqrt{-1}a^2b\right) + t^2\left(c^2 - \sqrt{-1}a^2\right).$$

Wyróżnik tego wielomianu jest równy $4\sqrt{-1}a^2c^2(b-d)^2$. Oznacza to, że druga współrzedna jest różna od 1 modulo $((\overline{\mathbb{Q}}(t))^\times)^2$, więc $\eta(P_2)$ ma rząd równy 2.

Pierwsza współrzędna punktu $\eta(T_2)$ jest równa

$$a^4b^4 - c^4d^4 + t\left(4c^4d^3 - 4a^4b^3\right) + t^2\left(6a^4b^2 - 6c^4d^2\right) + t^3\left(4c^4d - 4a^4b\right) + t^4\left(a^4 - c^4\right).$$

Wyróżnik tego wielomianu wynosi $-256a^{12}c^{12}(b-d)^{12}$. Jest on niezerowy, więc wielomian nie jest pełnym kwadratem i $\eta(T_2)$ ma rząd równy 2.

Zauważmy teraz, że $\eta(P_1) \neq \eta(P_2)$ oraz $\eta(P_2) \neq \eta(T_2)$ na mocy podanych już argumentów. Z dokładnością do kwadratów $h_1^2 + h_2^2$ jest równe f, więc $\eta(P_1) \neq \eta(T_2)$. W takim razie elementy $\eta(P_1), \eta(P_2)$ rozpinają grupę $(\mathbb{Z}/2\mathbb{Z})^2$. Wraz z $\eta(T_2)$, elementy $\eta(P_1)$ i $\eta(P_2)$ rozpinają grupę $(\mathbb{Z}/2\mathbb{Z})^3$ dokładnie wtedy, gdy $\eta(P_1) \cdot \eta(P_2) \neq \eta(T_2)$. Ale ostatnia nierówność jest spełniona, bo f jest rozdzielczy i $h_1^2 + h_2^2$ nie jest pełnym kwadratem. □

Uwaga 2.6.11. Warunek $\deg f = 2$ z powyższego twierdzenia jest niezbędny, aby przy podanych pozostałych założeniach uzyskać dokładną wartość rangi generycznej, bez używania dodatkowych środków. Zauważmy, że w ogólności, gdy $f, g, f^2 - g^2$ są rozdzielcze oraz $\deg(f^2 - g^2) = 2\deg f$, to $r \geq 2$ oraz

$$2 + 3\deg f + 3\deg g + 2\deg f + r + \max\{4(\deg f - \deg g) - 1, 0\} \leq 10\deg f.$$

Gdy $\deg f = \deg g$, to

$$4 \leq 2 + r \leq 2\deg f.$$

Zatem gdy $\deg f = \deg g = 2$, to $r = 2$. Gdy $\deg f > \deg g$, to

$$3 \leq 1 + r \leq \deg g + \deg f.$$

W tej sytuacji jeśli $\deg f = 2$, to otrzymujemy $r = 2$.

Wniosek 2.6.12. *Niech spełnione będą założenia Twierdzenia 2.6.10. Przyjmijmy, że $f, g, h \in \mathbb{Q}[t]$. Wówczas krzywa E jest określona nad $\mathbb{Q}(t)$ oraz*

$$E(\mathbb{Q}(t)) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

i generatorami tej grupy są $P_2, T_1, 2T_2$.

Dowód. Dowód jest analogiczny do dowodu Wniosku 2.5.21. □

Porzucając założenie $f, g, h \in \mathbb{Q}[t]$ z Wniosku 2.6.12 można otrzymać krzywą E postaci (2.26) określoną nad $\mathbb{Q}(t)$, która ma wyższą rangę grupy $E(\mathbb{Q}(t))$ niż ta podana we Wniosku 2.6.12 lub większy rząd grupy $\mathbb{Q}(t)$-wymiernych punktów torsyjnych.

Przykład 2.6.13. Wybierając w odpowiedni sposób $h_1, h_2 \in \overline{\mathbb{Q}}[t]$ można podać przykład krzywej E postaci (2.26) określonej nad $\mathbb{Q}(t)$, która spełnia warunek $rangaE(\mathbb{Q}(t)) = 2$. Niech

$$h_1 = (-2)^{1/4}(4\sqrt{2} - t),$$
$$h_2 = (-2)^{1/4}(4\sqrt{2} + t).$$

Ze wzorów (2.27) i (2.28) wynikają równości $f = \sqrt{-2}(t^2 + 2^5)$, $g = -2^4 t$ oraz $h = \sqrt{-2}(2^5 - t^2)$ i krzywa zadana równaniem (2.26)

$$E : y^2 = x(x + 2(t^2 + 2^5)^2)(x - (-2^4 t)^2)$$

jest określona nad $\mathbb{Q}(t)$. Ponadto na mocy Lematu 2.6.8 punkty

$$Q_1 = (-g^2, \sqrt{-2}g^2 h) = (-2^8 t^2, 2^9 t^2(t^2 - 2^5)),$$
$$Q_2 = (h^2, fgh) = (-2(2^5 - t^2)^2, -2^5 t(t^4 - 2^{10}))$$

są liniowo niezależne. Stosując metodę z Wniosku 2.5.21 otrzymamy, że Q_1, Q_2 wraz z T_1 i $2T_2$ generują całą grupę $E(\mathbb{Q}(t))$.

Przykład 2.6.14. Niech $a^2 + b^2 - 2c^2$ będzie formą kwadratową. Wybieramy parametryzację $\mathbb{Q}$-wymierną $a = 1 + 2t - t^2$, $b = -1 + 2t + t^2$, $c = 1 + t^2$. Niech $f = \sqrt{-1}(1 + 2t - t^2)$, $g = \sqrt{-1}(-1 + 2t + t^2)$ i $h = \sqrt{-2}(1 + t^2)$. Zachodzi równość $f^2 + g^2 = h^2$ oraz krzywa zadana równaniem (2.26)

$$E : y^2 = x(x + (1 + 2t - t^2)^2)(x + (-1 + 2t + t^2)^2)$$

jest określona nad $\mathbb{Q}(t)$. Grupa punktów torsyjnych $E(\mathbb{Q}(t))_{\text{tors}}$ jest izomorficzna z $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Generatorami grupy $E(\mathbb{Q}(t))_{\text{tors}}$ są

$$T_1 = (g^2, 0) = (-(-1 + 2t + t^2)^2, 0),$$
$$T_2 = (fg, \sqrt{-1}f(f - g)g) = (1 - 6t^2 + t^4, 2(-1 + 7t^2 - 7t^4 + t^6)).$$

Ponadto grupa $E(\mathbb{Q}(t))$ jest rangi 1, a generatorem jej części wolnej jest punkt

$$Q_2 = (-g^2, \sqrt{-2}g^2 h) = ((-1 + 2t + t^2)^2, 2(1 + t^2)(-1 + 2t + t^2)^2).$$

Niech dane będzie ustalone ciało K charakterystyki 0 i określona nad nim krzywa eliptyczna

$$E : y^2 = x^3 + Ax^2 + Bx$$

taka, że $A, B \in K$. Jeśli dany jest automorfizm $\sigma : K \to K$, to krzywa

$$E^\sigma : y^2 = x^3 + \sigma(A)x^2 + \sigma(B)x$$

jest również niesobliwa (więc automatycznie eliptyczna) oraz określona nad K. Ponadto odwzorowanie

$$\begin{aligned} E(K) &\to E^\sigma(K) \\ (x, y) &\mapsto (\sigma(x), \sigma(y)) \\ O &\mapsto O \end{aligned} \tag{2.43}$$

ustala izomorfizm grup Mordella-Weila $E(K)$ i $E^\sigma(K)$.

Niech $K = \overline{\mathbb{Q}}(t)$ oraz niech E_3 będzie krzywą eliptyczną nad $\mathbb{Q}(t)$ określoną równaniem

$$E_3 : y^2 = x(x - (u_3^2 - 1)^2)(x - 4u_3^2), \quad u_3 = \frac{2t}{5 + t^2}.$$

Niech E_4 będzie krzywą eliptyczną nad $\mathbb{Q}(t)$ określoną równaniem

$$E_4 : y^2 = x(x + 2(u_4^2 + 2^5)^2)(x - (-2^4 u_4)^2), \quad u_4 = \frac{-2^4 t}{-10 + t^2}.$$

Wówczas automorfizm $\sigma : K \to K$ taki, że $\sigma(t) = \frac{1}{\sqrt{-2}}t$ indukuje izomorfizm grup $E_3(K) \cong E_3^\sigma(K)$. Ponadto mamy K-izomorfizm krzywych eliptycznych

$$\begin{aligned} &\phi : E_3^\sigma \to E_4, \\ &(x, y) \mapsto (s^2 x, s^3 y), \quad s = -2^5\sqrt{-2}. \end{aligned}$$

W szczególności, ϕ indukuje izomorfizm grup $E_3^\sigma(K) \cong E_4(K)$. Niech

$$f_3 = u_3^2 - 1, \quad g_3 = 2u_3, \quad h_3 = u_3^2 + 1$$

oraz

$$f_4 = \sqrt{-2}(u_4^2 + 2^5), \quad g_4 = -2^4 u_4, \quad h_4 = \sqrt{-2}(2^5 - u_4^2).$$

Dla $i \in \{3, 4\}$ definiujemy punkty

$$\begin{aligned} P_{1,i} =&(-(1 + \sqrt{2})g_i(g_i - h_i), \sqrt{-1}(1 + \sqrt{2})g_i(g_i - h_i)(\sqrt{2}g_i - h_i)), \\ P_{2,i} =&((f_i - h_i)(g_i - h_i), (f_i + g_i)(f_i - h_i)(g_i - h_i)), \\ T_{1,i} =&(g_i^2, 0), \\ T_{2,i} =&(f_i g_i, \sqrt{-1} f_i (f_i - g_i) g_i). \end{aligned}$$

Ponadto określamy punkty

$$\begin{aligned} P_{3,3} &= \left(-f_3, \frac{(-5 + t^2)u_3(-1 + u_3^2)}{5 + t^2} \right) \in E_3(K), \\ P_{3,4} &= \left(-\frac{2^6}{\sqrt{-2}} f_4, \frac{2^9 \left(t^2 + 10\right) u_4 \left(2^5 + u_4^2\right)}{10 - t^2} \right) \in E_4(K). \end{aligned}$$

Zachodzą wtedy równości

$$\begin{aligned} \phi(P_{1,3}) &= -P_{1,4} + T_{1,4} + 2T_{2,4}, \\ \phi(P_{2,3}) &= -P_{2,4} + 2T_{2,4}, \\ \phi(T_{1,3}) &= T_{1,4}, \\ \phi(T_{2,3}) &= T_{2,4}, \\ \phi(P_{3,3}) &= P_{3,4}. \end{aligned}$$

Twierdzenie 2.6.15. *Grupa $E_i(K)$ jest generowana przez $P_{1,i}, P_{2,i}, P_{3,i}$, $T_{1,i}, T_{2,i}$ oraz*

$$E_i(K) \cong \mathbb{Z}^3 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

dla $i \in \{3, 4\}$. Grupa $E_3(\mathbb{Q}(t))$ jest generowana przez $P_{2,3}, P_{3,3}$, $T_{1,3}, 2T_{2,3}$, więc

$$E_3(\mathbb{Q}(t)) \cong \mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Grupa $E_4(\mathbb{Q}(t))$ jest generowana przez $2P_{1,4}, 2P_{2,4}, P_{3,4}$, $T_{1,4}, 2T_{2,4}$, więc

$$E_4(\mathbb{Q}(t)) \cong \mathbb{Z}^3 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Dowód. Istnienie izomorfizmu $E_3(K) \cong E_3^\sigma(K)$ indukowanego przez σ jest konsekwencją uwag poprzedzających twierdzenie. Odwzorowanie ϕ jest w oczywisty sposób izomorfizmem. Dalsze własności wynikają z rachunku, który został przeprowadzony z użyciem pakietu MAGMA. Ponadto własności krzywej E_3 oraz grup $E_3(K)$ i $E_3(\mathbb{Q}(t))$ zostały opisane w Lemacie 2.5.16 i 2.5.17. Struktura grupy $E_4(K)$ jest konsekwencją istnienia izomorfizmu grup $E_3^\sigma(K)$ i $E_4(K)$. Opis struktury grupy $E_4(\mathbb{Q}(t))$ uzyskujemy za pomocą analogicznego rachunku, do tego z dowodu Wniosku 2.5.18. □

2.6.1 Zastosowania do rodzin parametryzowanych przez formy kwadratowe

W tym paragrafie wykorzystamy wyniki poprzedniego podrozdziału do opisu rangi w rodzinach krzywych eliptycznych parametryzowanych przez formy kwadratowe.

Niech dane będzie ciało liczbowe K i niech $\alpha, \beta, \gamma \in K^\times$. Załóżmy, że dana jest forma kwadratowa $\alpha a^2 + \beta b^2 - \gamma c^2$. Rozważamy sytuację, gdy istnieje trójka liczb $a_0, b_0, c_0 \in K$ spełniających $a_0 b_0 c_0 \neq 0$ i takich, że $\alpha a_0^2 + \beta b_0^2 = \gamma c_0^2$. Wówczas możemy znaleźć wielomiany $f_1, g_1, h_1 \in K[t]$ spełniające warunek

$$\alpha \frac{f_1^2}{h_1^2} + \beta \frac{g_1^2}{h_1^2} = \gamma \tag{2.44}$$

i takie, że f_1 i g_1 nie mają wspólnych pierwiastków. Ponadto zamieniając ewentualnie rolami f_1 i g_1 można przyjąć, że $\deg f_1 \geq \deg g_1$. Z tego, że w ten sposób otrzymujemy parametryzację kwadrygi $\alpha X^2 + \beta Y^2 = \gamma$ wynika, że jest możliwy wybór f_1 taki, że $\deg f_1, \deg g_1 \leq 2$, więc również $\deg h_1 \leq 2$. Wybierając $t \in K$ otrzymujemy parametryzację rozwiązań K-wymiernych równania $\alpha a^2 + \beta b^2 = \gamma c^2$ w postaci

$$\frac{a}{c} = \frac{f_1}{h_1}, \quad \frac{b}{c} = \frac{g_1}{h_1}.$$

Niech dana będzie krzywa nad K określona równaniem Weierstrassa

$$E_{(a,b,c)} : y^2 = x(x - \alpha a^2)(x - \beta b^2). \tag{2.45}$$

Jeśli wyróżnik $16a^4\alpha^2 b^4 \beta^2 \left(a^2\alpha - b^2\beta\right)^2$ stowarzyszony z podanym równaniem (por. Tabela 2.1) jest niezerowy, to równanie (2.45) definiuje krzywą eliptyczną określoną

nad K. Dla ustalonych α, β, γ chcemy wskazać takie parametry a, b, c, dla których ranga grupy Mordella Weila $E_{(a,b,c)}(K)$ jest dodatnia. W szczególności pokażemy w jaki sposób można w tym celu zastosować rezultaty poprzedniego podrozdziału.

Zauważmy, że przy ustalonych $a_0, b_0, c_0 \in K$, $a_0 b_0 c_0 \neq 0$ i ustalonej formie kwadratowej $q(a, b, c) = \alpha a^2 + \beta b^2 - \gamma c^2$ z parametrami α, β, γ określonymi jak wyżej, gdy $q(a_0, b_0, c_0) = 0$, to możemy znaleźć parametr t_0 taki, że $\frac{a_0}{c_0} = \frac{f_1(t_0)}{h_1(t_0)}$ oraz $\frac{b_0}{c_0} = \frac{g_1(t_0)}{h_1(t_0)}$. Zamiana zmiennych na

$$x = x' \left(\frac{c_0}{h_1(t_0)} \right)^2, \quad y = y' \left(\frac{c_0}{h_1(t_0)} \right)^3 \tag{2.46}$$

pozwala przekształcić równanie $E_{(a_0,b_0,c_0)}$ do postaci

$$(y')^2 = x'(x' - \alpha f_1(t_0))^2)(x' - \beta g_1(t_0)^2), \tag{2.47}$$

gdzie $\alpha f_1(t_0)^2 + \beta g_1(t_0)^2 = \gamma h_1(t_0)^2$ i krzywa jest określona nad K. Definiujemy $f = \sqrt{\alpha} f_1$, $g = \sqrt{\beta} g_1$ oraz $h = \sqrt{\gamma} h_1$. Konstruujemy krzywą postaci (2.26)

$$(y')^2 = x'(x' - (f)^2)(x' - (g)^2)$$

określoną nad $K(t)$. Na mocy Lematu 2.6.8 mamy dwa punkty $\overline{\mathbb{Q}}(t)$-wymierne na tej krzywej

$$Q_1 = (-g^2, \sqrt{-2} g^2 h) = (-\beta g_1^2, \sqrt{-2} \beta \sqrt{\gamma} g_1^2 h_1), \tag{2.48}$$

$$Q_2 = (h^2, fgh) = (\gamma h_1^2, \sqrt{\alpha}\sqrt{\beta}\sqrt{\gamma} f_1 g_1 h_1). \tag{2.49}$$

Wielomiany f, g, h spełniają warunki Lematu 2.6.8, więc punkty Q_1, Q_2 rozpinają podgrupę rangi 2. Ponadto punkt Q_1 jest $K(t)$-wymierny dokładnie wtedy, gdy $\sqrt{-2}\sqrt{\gamma} \in K$. Punkt Q_2 jest $K(t)$-wymierny wtedy i tylko wtedy, gdy $\alpha\beta\gamma$ jest kwadratem w K.

Uwaga 2.6.16. Rozważana w Przykładzie 2.6.13 rodzina spełnia podane wyżej warunki i punkty Q_1, Q_2 są $\mathbb{Q}(t)$-wymierne i liniowo niezależne.

Wniosek 2.6.17. *Niech dane będzie ciało liczbowe K oraz $\alpha, \beta, \gamma \in K \setminus \{0\}$. Istnieje nieskończenie wiele trójek $a, b, c \in K$ spełniających $\alpha a^2 + \beta b^2 = \gamma c^2$, dla których krzywa*

$$E_{(a,b,c)} : y^2 = x(x - \alpha a^2)(x - \beta b^2)$$

jest eliptyczna oraz grupa $E_{(a,b,c)}(K)$ ma rangę równą co najmniej

(i) 1, *gdy* $-2\gamma \in (K^\times)^2$,

(ii) 1, *gdy* $\alpha\beta\gamma \in (K^\times)^2$,

(iii) 2, *gdy* $\alpha\beta\gamma \in (K^\times)^2$ *i* $-2\gamma \in (K^\times)^2$.

Ponadto trójki $a, b, c \in K$ podane powyżej zadają nieskończony podzbiór w zbiorze otwartym

$$\mathbb{P}^2(K) \setminus \{[a:b:c] \in \mathbb{P}^2(K) : \alpha a^2 + \beta b^2 = \gamma c^2, ab\left(a^2\alpha - b^2\beta\right) = 0\}.$$

Dowód. Z założeń oraz poprzedzającej wniosek dyskusji wynika, że istnieją wielomiany $f_1, g_1, h_1 \in K[t]$ takie, że $\alpha f_1^2 + \beta g_1^2 = \gamma h_1^2$ oraz $\deg g_1 \leq \deg f_1 \leq 2$. Na krzywej eliptycznej

$$E_t : y^2 = x(x - \alpha f_1^2)(x - \beta g_1^2),$$

określonej nad $K(t)$ zadane są dwa liniowo niezależne i $\overline{\mathbb{Q}}(t)$-wymierne punkty (2.48), (2.49), patrz Lemat 2.6.8. Niech dana będzie powierzchnia eliptyczna $\mathcal{E} = (S, \mathbb{P}^1_{\overline{\mathbb{Q}}}, \pi)$, której włóknem generycznym jest krzywa E nad $K(t)$. Z konstrukcji modelu Kodairy-Nérona możemy wybrać S w ten sposób, że jest powierzchnią określoną nad K i włókna $\pi^{-1}(t_0)$ dla $t_0 \in K$ jeśli są nieosobliwe, to definiują krzywe eliptyczne nad K. Twierdzenie 2.5.22 zastosowane w tym kontekście (por. [Sil86, Theorem 20.3]) implikuje, że dla nieskończenie wielu parametrów $t_0 \in K$ zachodzi nierówność

$$ranga\, E_t(K(t)) \leq ranga\, E_{t_0}(K). \tag{2.50}$$

Krzywa E_{t_0} jest określona równaniem (2.47). Gdy trójka a, b, c jest wyznaczona przez $f_1(t_0), g_1(t_0), h_1(t_0)$ jako

$$\frac{a}{c} = \frac{f_1(t_0)}{h_1(t_0)}, \quad \frac{b}{c} = \frac{g_1(t_0)}{h_1(t_0)},$$

to zamiana współrzędnych (2.46) pozwala nam określić punkty na $E_{(a,b,c)}$

$$\begin{aligned}\widetilde{Q}_1 =& (-\beta b^2, \sqrt{-2}\beta\sqrt{\gamma} b^2 c),\\ \widetilde{Q}_2 =& (\gamma c^2, \sqrt{\alpha}\sqrt{\beta}\sqrt{\gamma} abc).\end{aligned}$$

Liniowa niezależność punktów $\widetilde{Q}_1$ i $\widetilde{Q}_2$ wynika z faktu, że homomorfizm specjalizacji σ_{t_0} określony w (2.25) jest injektywny. Stosując założenia podane w podpunktach (i),(ii) i (iii) oraz nierówność (2.50) otrzymujemy ostatnią część tezy. □

Przykład 2.6.18. Niech $\alpha = -2$, $\beta = 1$ i $\gamma = -2$, patrz Przykład 2.6.13. Wówczas spełnione są założenia punktu (iii) z Wniosku 2.6.17. Równanie $-2a^2 + b^2 = -2c^2$ posiada parametryzację rozwiązań nad $\mathbb{Q}$, np.

$$f_1 = t^2 + 2^5, \quad g_1 = -2^4 t, \quad h_1 = -(t^2 - 2^5).$$

Wówczas krzywa

$$E_{(a,b,c)} : y^2 = x(x + 2a^2)(x - b^2), \quad -2a^2 + b^2 = -2c^2$$

określona nad $\mathbb{Q}$ jest nieosobliwa dla nieskończenie wielu trójek $a, b, c \in \mathbb{Q}$ oraz spełnia warunek $ranga\, E_{(a,b,c)}(\mathbb{Q}) \geq 2$, gdzie dwa punkty liniowo niezależne są dane jawnie w postaci

$$\begin{aligned}\widetilde{Q}_1 =& (-b^2, -2b^2 c),\\ \widetilde{Q}_2 =& (-2c^2, -2abc).\end{aligned}$$

Wniosek 2.6.19. *Niech dany będzie zbiór*

$$S = \left\{ \left(f_1(\frac{-2^4 t}{-10+t^2}), g_1(\frac{-2^4 t}{-10+t^2}), h_1(\frac{-2^4 t}{-10+t^2}) \right) : t \in \mathbb{Q}^\times \right\}.$$

Istnieje skończony zbiór $S_0 \subset S$ taki, że dla dowolnego $(a,b,c) \in S \setminus S_0$ krzywa

$$E_{(a,b,c)} : y^2 = x(x+2a^2)(x-b^2), \quad -2a^2+b^2 = -2c^2$$

jest eliptyczna oraz ranga grupy $E_{(a,b,c)}(\mathbb{Q})$ wynosi co najmniej 3. Wyrażenie $2(-32+a)(64a+b^2)$ jest kwadratem w $\mathbb{Q}$. Mamy wtedy trzy liniowo niezależne $\mathbb{Q}$-wymierne punkty $\widetilde{Q}_1$, $\widetilde{Q}_2$,

$$\widetilde{Q}_3 = \left(-2^6 a, 2^3 a \sqrt{2(-32+a)(64a+b^2)} \right).$$

Dowód. W Przykładzie 2.6.18 podana została parametryzacja $\mathbb{Q}$-wymierna równania $-2a^2+b^2 = -2c^2$. Konstrukcja zbioru S gwarantuje nam, że wyróżnik równania krzywej $E_{(a,b,c)}$ jest różny od zera, więc krzywa jest eliptyczna. Na mocy Twierdzenia 2.6.15 oraz Twierdzenia 2.5.22 otrzymujemy, że ranga grupy $E_{(a,b,c)}(\mathbb{Q})$ wynosi co najmniej 3. Mamy dane jawnie punkty $\mathbb{Q}(t)$-wymierne, liniowo niezależne i leżące na krzywej E_4 z Twierdzenia 2.6.15. Korzystając z zamiany zmiennych (2.46) otrzymujemy punkty podane w tezie Wniosku 2.6.19. □

Rozdział 3

Formy modularne i kongruencje

W tym rozdziale przedstawione zostaną wyniki teoretyczne oraz numeryczne dotyczące kongruencji pomiędzy formami parabolicznymi a szeregami Eisensteina. Podstawowym odniesieniem będzie praca [Nas14]. Zamieszczamy tutaj także nowe wyniki, które znacząco rozszerzają zakres parametrów wagi i poziomu formy, dla których wykonano rachunki w [Nas14].

3.1 Preliminaria

3.1.1 Formy modularne

Niech $\mathcal{H} = \{\tau \in \mathbb{C} : \Im\tau > 0\}$ oznacza górną półpłaszczyznę, na której działa w naturalny sposób grupa $GL_2^+(\mathbb{R})$ macierzy o dodatnim wyróżniku

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d},$$

dla $\tau \in \mathcal{H}$ i $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbb{R})$. Przez $\Gamma(1)$ oznaczać będziemy grupę macierzy $SL_2(\mathbb{Z})$. Niech N będzie dodatnią liczbą całkowitą. Przez $\Gamma(N)$ oznaczać będziemy grupę, która jest jądrem naturalnego homomorfizmu redukcji $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : N \mid c, N \mid b, N \mid (a-1), N \mid (d-1) \right\}.$$

Każdą podgrupę Γ w $\Gamma(1)$ spełniającą $\Gamma(N) \subset \Gamma \subset \Gamma(1)$ dla pewnego N nazywać będziemy *grupą kongruentną*. W szczególności, każda grupa kongruentna Γ jest skończonego indeksu w $\Gamma(1)$. Przez $\Gamma_0(N)$ oznaczymy następującą grupę kongruentną

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : N \mid c \right\}.$$

Ponadto dla grupy $\Gamma(1)$ określamy również działanie zbiorze punktów wymiernych, tj. punktów $x+iy$, takich, że $x \in \mathbb{Q}$ i $y=0$ lub $x=0$ i $y=\infty$. Niech

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{p}{q} = \begin{cases} \frac{ap+bq}{cp+dq}, & \text{gdy } cp+dq \neq 0 \\ i\infty, & \text{gdy } cp+dq = 0. \end{cases}$$

Ponadto

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} i\infty = \begin{cases} \frac{a}{c}, & \text{gdy } c \neq 0, \\ i\infty, & \text{gdy } c = 0. \end{cases}$$

Na górnej półpłaszczyźnie $\mathcal{H}$ określamy *funkcje automorficzne* ze względu na działanie grupy $\Gamma_0(N)$. Niech $f : \mathcal{H} \to \mathbb{C}$ będzie funkcją holomorficzną. Mówimy, że f jest automorficzna wagi k ze względu na działanie grupy $\Gamma_0(N)$ jeśli dla dowolnej macierzy $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ w $\Gamma_0(N)$ i dla dowolnego $\tau \in \mathcal{H}$ zachodzi równość

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau\right) = (c\tau + d)^k f(\tau).$$

Dla dowolnego $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbb{Q})$ przez $f \mid_k \gamma$ oznaczamy funkcję

$$(\det \gamma)^{k-1} f(\gamma\tau)(c\tau + d)^{-k}.$$

Ponadto niech $j(\tau, \gamma)$ oznacza wyrażenie $(c\tau + d)$. Wówczas warunek automorficzności można zapisać

$$f \mid_k \gamma = f$$

dla $\gamma \in \Gamma_0(N)$.

Zauważmy, że macierz $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ należy do $\Gamma_0(N)$ dla dowolnego N. Zatem funkcja automorficzna f wagi k spełnia równość

$$f(\tau + 1) = f(\tau).$$

W szczególności istnieje rozwinięcie f w szereg Fouriera

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n q^n,$$

gdzie $q = e^{2\pi i\tau}$. Jeśli dla wszystkich $n < 0$ zachodzi $a_n = 0$, to mówimy, że funkcja f jest *holomorficzna w nieskończoności*.

Dla dowolnego $\gamma \in \Gamma(1)$ funkcja $f_\gamma = f \mid_k \gamma$ jest holomorficzna na górnej półpłaszczyźnie oraz jest automorficzna ze względu na grupę $\gamma^{-1}\Gamma_0(N)\gamma$. Grupa ta zawiera macierz $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$, stąd f_γ spełnia równość

$$f_\gamma(\tau + N) = f_\gamma(\tau).$$

Istnieje zatem rozwinięcie f_γ w szereg Fouriera

$$f_\gamma(\tau) = \sum_{n=-\infty}^{\infty} b_n q_N^n,$$

gdzie $q_N = e^{2\pi i\tau/N}$. Funkcja f_γ jest holomorficzna w nieskończoności jeśli $b_n = 0$ dla $n < 0$.
Jeśli funkcja automorficzna f wagi k ze względu na grupę $\Gamma_0(N)$ spełnia warunek: $f\mid_k \gamma$ jest holomorficzna w nieskończoności dla dowolnego $\gamma \in \Gamma(1)$, to wówczas funkcję f nazywamy *formą modularną* wagi k ze względu na grupę $\Gamma_0(N)$.

W dalszej części tekstu będziemy rozważać tylko formy modularne ze względu na $SL_2(\mathbb{Z}) = \Gamma_0(1)$ i $\Gamma_0(N)$, więc zazwyczaj będziemy pisać po prostu: forma modularna wagi k i poziomu 1 lub N, odpowiednio.

Zbiór form modularnych wagi k i poziomu N tworzy podprzestrzeń liniową $\mathcal{M}_k(N) = \mathcal{M}_k(\Gamma_0(N))$ przestrzeni wszystkich funkcji holomorficznych na $\mathcal{H}$ z dodawaniem po wartościach funkcji. Formę f należącą do $\mathcal{M}_k(N)$ nazywać będziemy *paraboliczną* jeśli dla dowolnego $\gamma \in \Gamma(1)$ funkcja $f\mid_k \gamma$ ma zerowy współczynnik Fouriera równy 0. Zbiór takich form tworzy podprzestrzeń oznaczaną przez $\mathcal{S}_k(N)$

3.1.2 Algebra Hecke

Na przestrzeni $\mathbb{C}$-liniowej $\mathcal{M}_k(\Gamma_0(N))$ działa algebra endomorfizmów $End(\mathcal{M}_k(N))$, w której wyróżnimy pewną podaglebrę $\mathbb{T}_N$. Z definicji, algebra $\mathbb{T}_N$ jest generowana przez operatory T_p, gdzie p jest liczba pierwszą. Na elemencie $f \in \mathcal{M}_k(N)$ operator T_p działa następująco

$$T_p f = \begin{cases} \sum_{j=0}^{p-1} f\mid_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}, & \text{jeśli } p \mid N, \\ \sum_{j=0}^{p-1} f\mid_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} + f\mid_k \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, & \text{jeśli } p \nmid N. \end{cases} \tag{3.1}$$

Działanie operatorów $(\cdot)\mid_k \gamma$ jest dobrze określone i liniowe, więc element $T_p f$ należy do przestrzeni $M_k(N)$, patrz [DS05, Chap. 5, §5.1].

Lemat 3.1.1 ([DS05, Proposition 5.2.2])**.** *Niech $f \in \mathcal{M}_k(N)$ będzie formą modularną wagi k i poziomu N, której rozwinięcie Fouriera ma postać*

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n.$$

Wówczas forma $T_p f$ ma rozwinięcie Fouriera następującej postaci

$$T_p f = \sum_{n=0}^{\infty} a_{np} q^n + \epsilon p^{k-1} \sum_{n=0}^{\infty} a_n q^{np},$$

gdzie $\epsilon = 1$ dla $p \nmid N$ oraz $\epsilon = 0$ dla $p \mid N$.

Dowód. Obliczamy rozwinięcie Fouriera funkcji $f_j = f \mid_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}$. Z definicji otrzymamy

$$f_j(\tau) = \frac{1}{p}\sum_{n=0}^{\infty} a_n(f)e^{2\pi in(\tau+j)/p} = \frac{1}{p}\sum_{n=0}^{\infty} a_n(f)q_p\mu_p^{nj},$$

gdzie $a_n(f)$ jest n-tym współczynnikiem Fouriera formy f, $q_p = e^{2\pi i\tau/p}$ oraz $\mu_p = e^{2\pi i/p}$ jest pierwiastkiem pierwotnym stopnia p z jedynki. Dla $p \mid N$ zachodzi równość $\sum_{j=0}^{p-1}\mu_p^{nj} = p$ i dla $p \nmid N$ suma ta wynosi 0. Stąd dla $p \mid N$ otrzymujemy

$$T_p f = \sum_{p|n} a_n(f)q_p^n = \sum_k a_{kp}(f)q^k.$$

Ponadto z definicji zachodzi równość

$$f \mid_k \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}(\tau) = p^{k-1}f(p\tau) = p^{k-1}\sum_{n=0}^{\infty} a_n(f)q^{np}.$$

Łącząc ostatnie równanie z poprzednimi obliczeniami otrzymujemy tezę dla $p \nmid N$. □

Na mocy powyższego lematu można bezpośrednim rachunkiem sprawdzić, że dla p, q operatory T_p i T_q komutują. Dla dowolnej liczby naturalnej n możemy teraz określić operator T_n następująco

(i) dla $n = 1$ ustalamy z definicji, że T_1 jest operatorem identycznościowym,

(ii) dla $n = p^r$, gdzie $r > 1$ i p jest liczbą pierwszą, określamy rekurencyjnie

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1}T_{p^{r-2}}$$

dla $p \nmid N$ oraz $T_{p^r} = T_p T_{p^{r-1}}$ dla $p \mid N$,

(iii) dla $n = m_1m_2$ takich, że $(m_1, m_2) = 1$ przyjmujemy $T_n = T_{m_1}T_{m_2}$.

Operatory T_n i T_m komutują ze sobą dla dowolnych m i n.

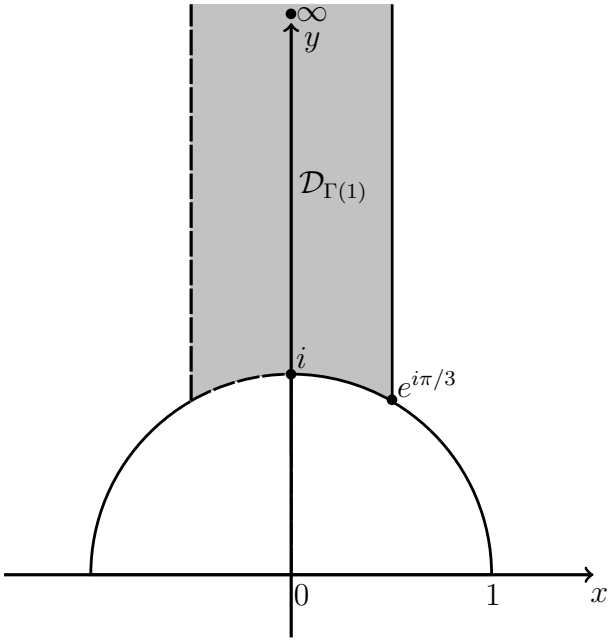
3.1.3 Obszar fundamentalny

Dla dowolnej grupy kongruentnej Γ obszar fundamentalny $\mathcal{D}_\Gamma$ będzie oznaczał taki podzbiór $\mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$, który spełnia własność: jeśli $x \in \mathcal{D}_\Gamma$ oraz $\gamma \in \Gamma$ i zachodzi $\gamma x \in \mathcal{D}_\Gamma$, to wówczas $\gamma x = x$. W przypadku, gdy $\Gamma = \Gamma(1)$ obszar fundamentalny można zdefiniować nastepująco

$$\mathcal{D}_{\Gamma(1)} = \{\tau \in \mathcal{H} : |\Re(\tau)| < 1/2, \mid \tau \mid > 1\} \cup \{1/2 + iy : y > \sqrt{3}/2\}$$
$$\cup \{e^{i\pi\theta} : 1/3 \le \theta \le 1/2\} \cup \{\infty\}.$$

Obszar $\mathcal{D}_{\Gamma(1)}$ jest przedstawiony na Rysunku 3.1. Dla dowolnej grupy kongruentnej Γ jeśli dany jest rozkład $\Gamma(1) = \bigcup\{\pm 1\}\Gamma\gamma_j$ na rozłączne podzbiory, tzn. $\{\pm 1\}\Gamma\gamma_j \cap \{\pm 1\}\Gamma\gamma_k = \emptyset$ dla $j \neq k$, to z dokładnością do zbiorów miary zero obszar fundamentalny $\mathcal{D}_\Gamma$ można zapisać jako

$$\bigcup \gamma_j \mathcal{D}_{\Gamma(1)}.$$



Rysunek 3.1: Obszar fundamentalny $\mathcal{D}_{\Gamma(1)}$

3.1.4 Iloczyn Peterssona

Na górnej półpłaszczyźnie $\mathcal{H}$ mamy zadaną miarę $GL_2^+(\mathbb{R})$-niezmienniczą $d\mu(x+iy) = \frac{dxdy}{y^2}$. Dla dowolnego $\alpha \in \Gamma(1)$ oraz dowolnej funkcji $f : \mathcal{H} \to \mathbb{C}$ ciągłej i ograniczonej całka

$$\int_{\mathcal{D}_{\Gamma(1)}} f(\alpha\tau)d\mu(\tau)$$

jest zbieżna. W szczególności dla dowolnej grupy kongruentnej Γ oraz funkcji f jak wyżej całka

$$\int_{\mathcal{D}_\Gamma} f(\tau)d\mu(\tau) = \sum_j \int_{\mathcal{D}_{\Gamma(1)}} f(\gamma_j\tau)d\mu(\tau)$$

jest zbieżna.

Definicja 3.1.2 (Iloczyn Peterssona)**.** Niech f, g będą dwiema formami z $\mathcal{S} = \mathcal{S}_k(\Gamma_0(N))$. Określamy odwzorowanie

$$\langle , \rangle : \mathcal{S} \times \mathcal{S} \to \mathbb{C}$$

wzorem

$$\langle f, g\rangle = \int_{\mathcal{D}_{\Gamma_0(N)}} f(\tau)\overline{g(\tau)}\Im(\tau)^k d\mu(\tau).$$

Uwaga 3.1.3. Funkcja $f(\tau)\overline{g(\tau)}\Im(\tau)^k$ jest ograniczona na $\mathcal{H}$ i na mocy wcześniejszych obliczeń całka jest dobrze określona. Ponadto odwzorowanie jest dwuliniowe i dodatnio określone, zatem zadaje na $\mathcal{S}_k(\Gamma_0(N))$ iloczyn skalarny (hermitowski).

Uwaga 3.1.4. Zazwyczaj w literaturze przyjmuje się w definicji iloczynu skalarnego Peterssona pewną normalizację całki, aby zachować niezmienniczość przy definicji iloczynu dla innych grup kongruentnych. W dalszej części będziemy odwoływać się wyłącznie do iloczynu skalarnego dwóch form modularnych ze względu na grupę $\Gamma_0(N)$, więc iloczyn pozostawiamy nieznormalizowany.

Operatory Hecke T_p dla $p \nmid N$ są samosprzężone względem iloczynu Peterssona, patrz [DS05, §5.5]

$$\langle T_p f, g\rangle = \langle f, T_p g\rangle.$$

Twierdzenie 3.1.5 ([DS05, Theorem 5.5.4])**.** *Przestrzeń $\mathcal{S}_k(N)$ posiada bazę ortogonalną względem iloczynu Peterssona, złożoną z wektorów własnych ze względu na operatory Hecke T_n dla $(n, N) = 1$.*

Dowód. Na mocy twierdzenia spektralnego dla przemiennych rodzin operatorów samosprzężonych działających na skończenie wymiarowej przestrzeni, istnieje baza ortogonalna wektorów własnych względem tej rodziny. □

3.1.5 Formy własne

Dla dwóch liczb całkowitych M, N spełniających warunek $Md = N$, $d \in \mathbb{N}$, definiujemy operatory podnoszenia poziomu dla form modularnych z $\mathcal{S}_k(M)$

$$\alpha_d : \mathcal{S}_k(M) \to \mathcal{S}_k(N) : f(\tau) \mapsto f(d \cdot \tau).$$

Podprzestrzeń $\sum_{d|N} Im(\alpha_d)$ nazywać będziemy *przestrzenią starych form* i oznaczać przez $\mathcal{S}_k(\Gamma_0(N))^{\text{old}}$ lub $\mathcal{S}_k(N)^{\text{old}}$.

Dopełnienie ortogonalne przestrzeni $\mathcal{S}_k(N)^{\text{old}}$ ze względu na iloczyn Peterssona nazywać będziemy *przestrzenią form nowych* i oznaczać $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ lub $\mathcal{S}_k(N)^{\text{new}}$. Rozkład na sumę prostą

$$\mathcal{S}_k(N) = \mathcal{S}_k(N)^{\text{new}} \oplus \mathcal{S}_k(N)^{\text{old}}$$

jest zachowywany przez operatory Hecke, patrz [DS05, Proposition 5.6.2].

Formę modularną f należącą do $\mathcal{S}_k(N)^{\text{new}}$, dla której $a_1(f) = 1$ oraz f jest wektorem własnym operatorów T_n dla dowolnego n, nazywać będziemy *nową formą własną*. Wartość własna formy f względem operatora T_n jest równa $a_n(f)$. Zbiór nowych form własnych wagi k i poziomu N tworzy bazę przestrzeni $\mathcal{S}_k(N)^{\text{new}}$, patrz [DS05, Thm. 5.8.2]. Ponadto jeśli f jest nową formą własną poziomu N i wagi k, to wówczas na mocy definicji operatorów Hecke oraz postaci wartości własnych dla f mamy

(i) $a_1(f) = 1$,

(ii) $a_{p^r} = a_p(f)a_{p^{r-1}}(f) - p^{k-1}a_{p^{r-2}}(f)$ dla $r \geq 2$ i $p \nmid N$,

(iii) $a_{p^r} = a_p(f)^r$ dla $r \geq 1$ i $p \mid N$,

(iii) $a_{mn}(f) = a_m(f)a_n(f)$ dla m i n względnie pierwszych.

Twierdzenie 3.1.6 ([Shi71, Theorem 3.48(3), Theorem 3.51(1)]). *Niech dane będą liczby całkowite k i N takie, że $k \geq 2$, $N \geq 1$. Niech f będzie nową formą własną w $\mathcal{S}_k(\Gamma_0(N))^{new}$. Wówczas współczynniki $a_n(f)$ rozwinięcia Fouriera formy f są całkowitymi liczbami algebraicznymi. Ponadto ciało $\mathbb{Q}(\{a_n(f)\}_{n\in\mathbb{N}})$ generowane nad $\mathbb{Q}$ przez współczynniki Fouriera formy f jest ciałem liczbowym.*

Dla danej nowej formy własnej $f \in \mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ oznaczmy przez $\mathcal{O}_f$ pierścień liczb algebraicznych całkowitych ciała liczbowego $\mathbb{Q}(\{a_n(f)\}_{n\in\mathbb{N}})$. Przez K_f będziemy oznaczać ciało $\mathbb{Q}(\{a_n(f)\}_{n\in\mathbb{N}})$.

3.1.6 Szeregi Eisensteina

W tym podrozdziale zebraliśmy podstawowe fakty o szeregach Eisensteina. Korzystamy przy tym z [DS05, Chapter 4].

Niech $k > 2$ będzie liczbą całkowitą parzystą. Definiujemy szereg

$$G_k(\tau) = \sum_{(c,d)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(c\tau+d)^k}.$$

Szereg $G_k(\tau)$ jest absolutnie zbieżny na górnej półpłaszczyźnie oraz niemal jednostajnie zbieżny, więc zadaje funkcję holomorficzną na $\mathcal{H}$. Ponadto dla dowolnego $\gamma \in \Gamma(1)$ spełnione jest równanie modularne

$$G_k(\gamma\tau) = j(\gamma,\tau)^k G_k(\tau)$$

oraz G_k jest ograniczony, gdy $\Im\tau \to \infty$. Z tego wynika, że G_k jest formą modularną wagi k i poziomu 1. Ponadto ma rozwinięcie Fouriera

$$G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n,$$

gdzie $q = e^{2\pi i\tau}$ oraz

$$\sigma_{k-1}(n) = \sum_{m|n} m^{k-1}.$$

Zachodzi ponadto równość $a_0(G_k) = 2\zeta(k)$, gdzie ζ jest funkcją dzeta Riemanna. Zatem $G_k(\tau)$ nie jest formą paraboliczną. Normalizacja względem współczynnika $a_1(G_k)$ określa funkcję $E_k(\tau) = \frac{G_k(\tau)}{a_1(G_k(\tau))}$, gdzie $a_0(E_k) = -\frac{B_k}{2k}$ oraz B_k jest k-tą liczbą Bernoulliego określoną szeregiem

$$\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_k\frac{t^k}{k!}.$$

Dla dowolnego $N \in \mathbb{N}$, $k > 2$ funkcje $E_k(r\tau)$ dla $r \mid N$ rozpinają podprzestrzeń liniową przestrzeni form modularnych $\mathcal{M}_k(\Gamma_0(N))$. Obliczając iloczyn Peterssona dowolnej z funkcji $E_k(r\tau)$, $r \mid N$ z formą paraboliczną $f \in \mathcal{S}_k(\Gamma_0(N))$ otrzymamy zero. Zatem funkcje $E_k(r\tau)$ należą do dopełnienia ortogonalnego przestrzeni $\mathcal{S}_k(\Gamma_0(N))$ w $\mathcal{M}_k(\Gamma_0(N))$. Przestrzeń dopełniającą $\mathcal{S}_k(\Gamma_0(N))$ względem iloczyny Peterssona oznaczamy symbolem $\mathcal{E}_k(\Gamma_0(N))$ i nazywamy przestrzenią form

Eisensteina. Dowolny niezerowy element przestrzeni $\mathcal{E}_k(\Gamma_0(N))$ nazywamy formą Eisensteina.

Dla $k = 2$ szereg $G_2(\tau)$ jest tylko warunkowo zbieżny. Prawdą jest jednak, że szereg $G_2(\tau) - NG_2(N\tau)$ jest formą modularną należącą do $\mathcal{M}_2(\Gamma_0(N))$. Podobnie dla $d \mid N$ szereg $G_2(\tau) - dG_2(d\tau)$ należy do $\mathcal{M}_2(\Gamma_0(N))$. Również w tym przypadku szeregi te są ortogonalne, względem iloczynu Peterssona, do form parabolicznych.

Twierdzenie 3.1.7. *Niech N będzie poziomem, a k wagą przestrzeni $\mathcal{M}_k(N)$. Podprzestrzeń $\mathcal{E}_k(N)$ ma wymiar równy*

$$d := \sum_{r|N} \phi((r, N/r)) - \epsilon(k),$$

gdzie $\epsilon(2) = 1$ i $\epsilon(k) = 0$ dla $k > 2$. W szczególności, jeśli N jest liczbą pierwszą, to $d = 1$ dla $k = 2$ oraz $d = 2$ dla $k > 2$. Dla N będącego iloczynem dwóch różnych liczb pierwszych $d = 3$ dla $k = 2$ oraz $d = 4$ dla $k > 2$. Ogólniej jeśli N jest iloczynem t różnych liczb pierwszych, to $d = 2^t - 1$ dla $k = 2$ i $d = 2^t$ dla $k > 2$.

Dowód. Wystarczy zastosować [DS05, Theorem 3.5.1]. □

3.1.7 Baza form własnych

W tym podrozdziale udowodnimy, że w przestrzeni $\mathcal{E}_k(\Gamma_0(N))$ istnieje baza wektorów własnych ze względu na działanie algebry Hecke $\mathbb{T}_N$. Zazwyczaj tego typu rezultaty podaje się dla operatorów Hecke o indeksach względnie pierwszych z poziomem grupy kongruentnej. Wszędzie, gdzie mówimy o przestrzeniach form modularnych zakładamy, że waga k jest liczbą parzystą.

Na potrzeby tego podrozdziału wprowadzimy dodatkowe oznaczenie U_p na operator Hecke T_p dla $p \mid N$. Ponadto przez A_d oznaczać będziemy operator działający z $\mathcal{M}_k(\Gamma_0(N))$ do $\mathcal{M}_k(\Gamma_0(Nd))$ zadany formułą $f(\tau) \mapsto f(d\tau)$. Zauważmy, że jeśli

$$\gamma = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix},$$

to $A_d(f) = d^{1-k} f \mid_k \gamma$.

Twierdzenie 3.1.8 ([AL70, Lemma 15])**.** *Niech f będzie formą modularną z przestrzeni $\mathcal{M}_k(\Gamma_0(N))$. Wówczas zachodzą równości*

$$(T_q \circ U_p)(f) = (U_p \circ T_q)(f) \quad \text{dla } p \neq q, \tag{3.2}$$
$$(T_q \circ A_d)(f) = (A_d \circ T_q)(f) \quad \text{dla } (q, d) = 1, \tag{3.3}$$
$$(U_q \circ A_d)(f) = (A_d \circ U_q)(f) \quad \text{dla } (q, d) = 1. \tag{3.4}$$

Szereg Eisensteina $E_k = -\frac{B_k}{2k} + \sum_{i=1}^{\infty} \sigma_{k-1}(n) q^n$ jest formą modularną w $\mathcal{M}_k(\Gamma(1))$ dla $k > 2$. Wykażemy, że E_k jest formą własną ze względu na działanie wszystkich operatorów Hecke.

Lemat 3.1.9. *Niech $n \in \mathbb{N}$ oraz p będzie liczbą pierwszą taką, że $p \mid n$. Wówczas dla $k \geq 2$ zachodzą równości*

$$\sigma_{k-1}(np) + p^{k-1}\sigma_{k-1}(n/p) = \sigma_{k-1}(p)\sigma_{k-1}(n), \tag{3.5}$$

$$\sigma_{k-1}(n) - p^{k-1}\sigma_{k-1}(n/p) = \sigma_{k-1}(np) - p^{k-1}\sigma_{k-1}(n), \tag{3.6}$$

$$\sigma_{k-1}(np) - \sigma_{k-1}(n) = p^{k-1}(\sigma_{k-1}(n) - \sigma_{k-1}(n/p)). \tag{3.7}$$

Dowód. Niech k będzie ustalone. Kładziemy $\sigma := \sigma_{k-1}$. Z definicji funkcji σ wynika, że $\sigma(nm) = \sigma(n)\sigma(m)$ dla m, n względnie pierwszych. Ponadto $\sigma(p^\alpha) = 1 + p + \cdots + p^\alpha$ dla $\alpha > 0$.

Dowód równości (3.5): Z założenia mamy $n = p^\alpha n'$, dla $p \nmid n'$. Lewa stronę równości (3.5) można zapisać

$$\sigma(n'p^{\alpha+1}) + p^{k-1}\sigma(n'p^{\alpha-1}) = \sigma(n')(\sigma(p^{\alpha+1}) + p^{k-1}\sigma(p^{\alpha-1})).$$

Wyrażenie w ostatnim nawiasie ma wartość

$$\sigma(p^{\alpha+1}) + p^{k-1}\sigma(p^{\alpha-1}) = (1 + p^{k-1})\sigma(p^\alpha).$$

Korzystając z multiplikatywności, otrzymujemy

$$\sigma(n')(1 + p^{k-1})\sigma(p^\alpha) = (1 + p^{k-1})\sigma(n).$$

Dowód równości (3.6): Równość (3.5) jest równoważna równości (3.6) po przeniesieniu wyrazów z prawej i lewej strony, ponieważ $\sigma(p) = 1 + p^{k-1}$.

Dowód równości (3.7): Równość (3.5) jest równoważna równości (3.7) po przeniesieniu wyrazów z prawej i lewej strony, gdyż $\sigma(p) = 1 + p^{k-1}$.

□

Lemat 3.1.10. *Niech T_n będzie n-tym operatorem Hecke działającym na $\mathcal{M}_k(\Gamma(1))$ dla $k > 2$. Wówczas*

$$T_n(E_k) = a_n(E_k)E_k = \sigma_{k-1}(n)E_k.$$

Dowód. Niech p będzie liczbą pierwszą. Wówczas zachodzi równość $a_n(T_p(E_k)) = a_{np}(E_k) + p^{k-1}a_{n/p}(E_k)$, gdzie przyjmujemy $a_r(E_k) = 0$ dla $r \in \mathbb{Q} \setminus \mathbb{Z}$. Stąd dla $p \nmid n$ otrzymamy

$$a_n(T_p(E_k)) = \sigma_{k-1}(np) = \sigma_{k-1}(n)\sigma_{k-1}(p) = a_n(E_k)a_p(E_k).$$

Dla $p \mid n$ po zastosowaniu równości (3.5) z Lematu 3.1.9 otrzymamy

$$a_n(T_p(E_k)) = \sigma_{k-1}(np) + p^{k-1}\sigma_{k-1}(n/p) = \sigma_{k-1}(p)\sigma_{k-1}(n) = a_p(E_k)a_n(E_k).$$

Niech $n = p^r$, gdzie p jest liczbą pierwszą i $r > 1$ jest liczbą naturalną. Ze wzoru rekurencyjnego

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1}T_{p^{r-2}} \tag{3.8}$$

wynika, że E_k jest wektorem własnym operatora T_{p^r}. Ponadto stosując równość (3.5) z Lematu 3.1.9 dla $n = p^{r-1}$ i przenosząc wyrazy stronami otrzymamy

$$\sigma_{k-1}(p)\sigma_{k-1}(p^{r-1}) - p^{k-1}\sigma_{k-1}(p^{r-2}) = \sigma_{k-1}(p^r). \tag{3.9}$$

Łącząc tę równość ze wzorem rekurencyjnym na T_{p^r} otrzymujemy, że $T_{p^r}E_k = a_{p^r}(E_k)E_k$.

Dla $n = kl$, gdzie k, l są względnie pierwsze, dostajemy z definicji operatora Hecke równość $T_n = T_kT_l = T_lT_k$. Stosując poprzednie przypadki dla rozkładu n na potęgi czynników pierwszych oraz multiplikatywność funkcji σ_{k-1} otrzymamy równość $T_n(E_k) = a_n(E_k)E_k$. Z definicji mamy $T_1 = id$, więc $T_1(E_k) = E_k = a_1(E_k)E_k$. □

Dla dowolnego d naturalnego definiujemy dwa operatory liniowe

$$[d]^+ := T_1 - d^{k-1}A_d : \mathcal{M}_k(\Gamma_0(N)) \to \mathcal{M}_k(\Gamma_0(Nd)),$$
$$[d]^- := T_1 - A_d : \mathcal{M}_k(\Gamma_0(N)) \to \mathcal{M}_k(\Gamma_0(Nd)).$$

Lemat 3.1.11. *Dla dowolnych $d, e \in \mathbb{N}$ oraz $\delta, \epsilon \in \{+, -\}$ zachodzą równości*

$$[d]^\epsilon \circ [e]^\delta = [e]^\delta \circ [d]^\epsilon.$$

Dowód. Równości są oczywistą konsekwencją faktu, że $A_d \circ A_e = A_e \circ A_d$. □

Lemat 3.1.12. *Niech E_k będzie szeregiem Eisensteina z $\mathcal{M}_k(\Gamma(1))$ dla $k > 2$. Jeśli p jest liczbą pierwszą to zachodzą równości*

$$U_p([p]^+E_k) = [p]^+E_k, \tag{3.10}$$
$$U_p([p]^-E_k) = p^{k-1}[p]^-E_k. \tag{3.11}$$

Dowód. Niech $F = [p]^+E_k$. Forma F należy do $\mathcal{M}_k(\Gamma_0(p))$. Obliczamy n-ty współczynnik Fouriera formy U_pF

$$a_n(U_pF) = a_{np}(F) = a_{np}(E_k - p^{k-1}A_pE_k) = a_{np}(E_k) - p^{k-1}a_n(E_k).$$

Korzystając z definicji E_k otrzymujemy

$$a_n(U_pF) = \sigma_{k-1}(np) - p^{k-1}\sigma_{k-1}(n).$$

Z drugiej strony, n-ty współczynnik Fouriera formy F wynosi

$$\sigma_{k-1}(n) - p^{k-1}\sigma_{k-1}(n/p),$$

gdzie zgodnie z konwencją $\sigma_{k-1}(r) = 0$ dla $r \in \mathbb{Q} \setminus \mathbb{Z}$. Stosując równość (3.6) z Lematu 3.1.9 otrzymujemy $U_pF = F$.

Niech $F = [p]^-E_k$. Forma F należy do $\mathcal{M}_k(\Gamma_0(p))$. Stosując analogiczne rozumowanie jak w pierwszym przypadku oraz równość (3.7) z Lematu 3.1.9 otrzymujemy $U_pF = p^{k-1}F$. □

Lemat 3.1.13. *Niech $k > 2$ będzie liczbą całkowitą. Ustalamy liczbę naturalną t oraz liczby pierwsze $p_1, \ldots, p_t$, parami różne. Niech $N = p_1 \cdot \ldots \cdot p_t$. Forma*

$$e = [p_1]^+ \circ \ldots \circ [p_r]^+ \circ [p_{r+1}]^- \circ \ldots \circ [p_t]^- E_k \in \mathcal{E}_k(\Gamma_0(N))$$

jest formą własną ze względu na algebrę Hecke $\mathbb{T}_N$. Ponadto

$$\begin{array}{ll} T_n e = \sigma_{k-1}(n)e, & (n, N) = 1 \\ U_{p_i} e = e, & 1 \leq i \leq r \\ U_{p_i} e = p_i^{k-1} e, & r+1 \leq i \leq t \end{array}$$

Dowód. Niech ℓ będzie liczbą pierwszą taką, że $\ell \nmid N$. Na mocy równości (3.3) w Twierdzeniu 3.1.8 oraz definicji operatorów $[p]^+$ oraz $[p]^-$ otrzymujemy równości $T_\ell \circ [p_i]^+ = [p_i]^+ \circ T_\ell$ oraz $T_\ell \circ [p_i]^- = [p_i]^- \circ T_\ell$. Z tego wynika, że

$$T_\ell e = [p_1]^+ \circ \ldots \circ [p_r]^+ \circ [p_{r+1}]^- \circ \ldots \circ [p_t]^- (T_l E_k).$$

Na mocy Lematu 3.1.10 otrzymujemy $T_\ell e = \sigma_{k-1}(\ell)e$. Operator T_{l^s}, $s > 1$ jest równy $P(T_\ell)$ dla pewnego $P \in \mathbb{Z}[x]$, więc zachodzi również $T_{\ell^s} e = P(\sigma_{k-1}(\ell))e$. Wielomian P jest wyznaczony za pomocą wzoru rekurencyjnego (3.8). Z kolei równanie (3.9) pociąga równość $P(\sigma_{k-1}(\ell)) = \sigma_{k-1}(\ell^s)$, więc $T_{\ell^s} e = \sigma_{k-1}(\ell^s)e$. Dla danego n względnie pierwszego z N otrzymujemy $T_n e = \sigma_{k-1}(n)e$, co wynika z definicji operatora T_n oraz z tego, że funkcja σ_{k-1} jest multiplikatywna.

Niech i będzie ustalone i spełnia warunek $1 \leq i \leq r$. Wówczas na mocy równości (3.4) w Twierdzeniu 3.1.8 otrzymujemy równości $U_{p_j} \circ [p_i]^+ = [p_i]^+ \circ T_{p_j}$ oraz $U_{p_j} \circ [p_i]^- = [p_i]^- \circ T_{p_j}$ dla $i \neq j$. Na mocy Lematu 3.1.11 formę e możemy zapisać jako

$$e = [p_1]^+ \circ \ldots \circ [p_{i-1}]^+ \circ [p_{i+1}]^+ \circ \ldots \circ [p_r]^+ \circ [p_{r+1}]^- \circ \ldots \circ [p_t]^- \circ [p_i]^+ E_k.$$

Zatem

$$U_{p_i} e = [p_1]^+ \circ \ldots \circ [p_{i-1}]^+ \circ [p_{i+1}]^+ \circ \ldots \circ [p_r]^+ \circ [p_{r+1}]^- \circ \ldots \circ [p_t]^- \circ U_{p_i} [p_i]^+ E_k.$$

Pierwsza równość w Lemacie 3.1.12 implikuje, że $U_{p_i} e = e$. Dla $i > r$ analogiczne rozumowanie daje $U_{p_i} e = p_i^{k-1} e$. Algebra Hecke $\mathbb{T}_N$ jest generowana przez operatory T_n dla $(n, N) = 1$ oraz operatory U_{p_i}, więc powyższy rachunek dowodzi, że e jest formą własną względem wszystkich operatorów Hecke. □

Twierdzenie 3.1.14. *Niech $k > 2$ będzie liczbą całkowitą. Ustalamy liczbę naturalną t oraz liczby pierwsze $p_1, \ldots, p_t$, parami różne. Niech $N = p_1 \cdot \ldots \cdot p_t$. Zbiór form*

$$B = \{e_{\epsilon_1, \ldots, \epsilon_t} : \epsilon_i \in \{+, -\}\}$$

takich, że

$$e_{\epsilon_1, \ldots, \epsilon_t} = [p_1]^{\epsilon_1} \circ \ldots \circ [p_t]^{\epsilon_t} E_k,$$

tworzy bazę przestrzeni $\mathbb{C}$-liniowej $\mathcal{E}_k(\Gamma_0(N))$ złożoną z wektorów własnych algebry Hecke $\mathbb{T}_N$.

Dowód. Formy ze zbioru B są liniowo niezależne, ponieważ względem algebry Hecke mają różne systemy wartości własnych, patrz Lemat 3.1.13. Oprócz tego mamy dokładnie 2^t różnych wyborów ciągów $(\epsilon_1, \ldots, \epsilon_t)$. Na mocy Twierdzenia 3.1.7 wiemy, że wymiar przestrzeni $\mathcal{E}_k(\Gamma_0(N))$ wynosi dokładnie 2^t, więc elementy z B tworzą bazę tej przestrzeni liniowej, która składa się z wektorów własnych. □

Lemat 3.1.15. *Niech $k > 2$ będzie liczbą całkowitą. Ustalamy liczbę naturalną t oraz liczby pierwsze $p_1, \ldots, p_t$, parami różne. Zachodzą równości*

$$\begin{aligned} &a_0(e_{\epsilon_1,\ldots,\epsilon_t}) = -\tfrac{B_k}{2k} \prod_{i=1}^{t} (1 - p_i^{k-1}), && \text{dla } \epsilon_1 = \ldots = \epsilon_t = +, \\ &a_0(e_{\epsilon_1,\ldots,\epsilon_t}) = 0, && \text{w pozostałych przypadkach.} \end{aligned}$$

Dowód. Zauważmy, że dla dowolnej formy f mamy $a_0([p]^- f) = 0$. Jeśli istnieje i takie, że $\epsilon_i = -$, to z przemienności operatorów $[\cdot]^+$ i $[\cdot]^-$ otrzymujemy $a_0(e_{\epsilon_1,\ldots,\epsilon_t}) = 0$. Z równości $a_0([p]^+ f) = a_0(f)(1 - p^{k-1})$ dla dowolnej formy f wnioskujemy, że w przypadku, gdy $\epsilon_i = +$ dla każdego i, to $a_0(e_{\epsilon_1,\ldots,\epsilon_t}) = -\frac{B_k}{2k} \prod_{i=1}^{t} (1 - p_i^{k-1})$. □

Uwaga 3.1.16. Gdy waga k jest równa 2, to powyższe twierdzenia należy nieco zmodyfikować. Szereg $E_2 = -\frac{B_2}{4} + \sum_{i=1}^{\infty} \sigma_1(n) q^n$ nie jest formą modularną wagi 2 względem $SL_2(\mathbb{Z})$, ale dla dowolnego p pierwszego szereg $[p]^+ E_2$ określa formę modularną wagi 2 i poziomu $\Gamma_0(p)$.

Lemat 3.1.17. *Niech p będzie liczbą pierwszą. Forma $[p]^+ E_2 \in \mathcal{E}_2(\Gamma_0(p))$ jest formą własną algebry Hecke $\mathbb{T}_p$. Ponadto $a_1([p]^+ E_2) = 1$, dla liczby pierwszej $q \neq p$ zachodzi $a_q([p]^+ E_2) = 1 + q$ oraz*

$$\begin{aligned} &U_p([p]^+ E_2) = [p]^+ E_2, \\ &T_n([p]^+ E_2) = a_n(E_2)[p]^+ E_2, \quad \text{dla } (n, Np) = 1. \end{aligned}$$

Dowód. Niech $\ell \neq p$ będzie liczbą pierwszą. Dla ustalonego n otrzymujemy

$$a_n(T_\ell([p]^+ E_2)) = \sigma_1(n\ell) - p\sigma_1(n\ell/p) + \ell\sigma_1(n/\ell) - \ell p \sigma_1(n/(\ell p)).$$

Zgodnie z przyjętą konwencją $\sigma(r) = 0$, gdy $r \in \mathbb{Q} \setminus \mathbb{Z}$. Z drugiej strony

$$(1 + \ell) a_n([p^+] E_2) = (1 + \ell)(\sigma_1(n) - p\sigma_1(n/p)).$$

Stosując równość (3.5) z Lematu 3.1.9, z definicji funkcji E_2 i operatora T_ℓ otrzymamy

$$a_n(T_\ell([p]^+ E_2)) = (1 + \ell) a_n([p^+] E_2).$$

Po zadziałaniu operatorem U_p na $[p]^+ E_2$ otrzymujemy formę z n-tym współczynnikiem Fouriera

$$a_n(U_p[p]^+ E_2) = a_{np}([p]^+ E_2) = \sigma_1(np) - p\sigma_1(n) = \sigma_1(n) - p\sigma_1(n/p) = a_n([p]^+ E_2).$$

Pierwsza, druga i czwarta równość wynikają z definicji E_2 i operatora U_p. Trzecia równość jest konsekwencją równania (3.6) z Lematu 3.1.9. Algebra Hecke $\mathbb{T}_p$ jest generowana przez operatory T_ℓ oraz U_p, więc forma $[p]^+ E_2$ jest formą własną całej algebry Hecke. Druga równość z tezy wynika z definicji operatora T_n oraz multiplikatywności funkcji σ_1. Z definicji otrzymujemy $a_1([p]^+ E_2) = a_1(E_2) = \sigma_1(1) = 1$ oraz $a_q([p]^+ E_2) = a_q(E_2) = \sigma_1(q) = 1 + q$ dla q pierwszego, $q \neq p$. □

Lemat 3.1.18. *Niech $N > 1$ będzie liczbą naturalną wolną od kwadratów. Niech $f \in \mathcal{E}_2(\Gamma_0(N))$ będzie formą własną algebry Hecke $\mathbb{T}_N$ taką, że $a_1(f) = 1$ i $a_q(f) = 1 + q$ dla q pierwszego, $q \nmid N$. Dla ustalonej liczby pierwszej $p \nmid N$ formy $[p]^+f, [p]^-f \in \mathcal{M}_2(\Gamma_0(Np))$ są formami własnymi ze względu na algebrę $\mathbb{T}_{Np}$. Spełnione są przy tym równości*

$$\begin{aligned} U_p([p]^+f) &= [p]^+f, \\ U_p([p]^-f) &= p \cdot [p]^-f, \\ T_n([p]^+f) &= a_n(f)[p]^+f, \quad \textit{dla } (n, Np) = 1, \\ T_n([p]^-f) &= a_n(f)[p]^-f, \quad \textit{dla } (n, Np) = 1. \end{aligned}$$

Ponadto $a_1([p]^\pm f) = 1$ oraz $a_q([p]^\pm f) = 1 + q$ dla liczby pierwszej $q \nmid Np$.

Dowód. Niech ℓ będzie liczbą pierwszą i $\ell \nmid Np$. Na mocy (3.3) z Twierdzenia 3.1.8 otrzymujemy $(T_\ell \circ [p]^+)f = ([p]^+ \circ T_\ell)f$. Forma f jest znormalizowaną formą własną, więc $T_\ell f = a_\ell(f)f$. Wynika z tego równość $T_\ell([p]^+f) = a_\ell(f)[p]^+f$. Analogiczne rozumowanie prowadzi do równości $T_\ell([p]^-f) = a_\ell(f)[p]^-f$. Z multiplikatywności σ_1, definicji E_2 i definicji operatora T_n dla $(n, Np) = 1$ otrzymujemy trzecią i czwartą równość z tezy.

Równość $U_p([p]^-f) = p \cdot [p]^-f$ jest równoważna temu, że

$$a_{np}(f) - a_n(f) = p(a_n(f) - a_{n/p}(f)), \tag{3.12}$$

przy standardowej konwencji $a_r(f) = 0$ dla $r \in \mathbb{Q} \notin \mathbb{Z}$. Forma f jest znormalizowaną formą własną dla $\mathbb{T}_N$, więc w przypadku $p \nmid n$ zachodzi równość $a_{np} = a_n(f)a_p(f)$ oraz skoro $p \nmid N$, to $a_p(f) = 1 + p$, czyli równanie (3.12) jest spełnione. W przypadku, gdy $n = n'p^\alpha$ i $\alpha > 0$ równość (3.12) jest równoważna

$$a_{p^{\alpha+1}}(f) = (p+1)a_{p^\alpha}(f) - pa_{p^{\alpha-1}}(f).$$

Równość ta jest prawdziwa skoro f jest formą własną algebry $\mathbb{T}_N$ i z definicji operator $T_{p^{\alpha+1}} = T_p T_{p^\alpha} - pT_{p^{\alpha-1}}$ oraz $a_p(f) = 1 + p$. Równość $U_p([p]^+f) = [p]^+f$ dowodzimy analogicznie jak poprzedni przypadek. Równości $a_1([p]^\pm f) = 1$ oraz $a_q([p]^\pm f) = 1 + q$ wynikają z założeń o formie f oraz definicji $[p]^\pm$. □

Twierdzenie 3.1.19. *Niech $t > 0$ będzie liczbą naturalną. Ustalamy liczby pierwsze $p_1, \ldots, p_t$, parami różne. Niech $N = p_1 \cdot \ldots \cdot p_t$. Dla $0 < s < t$ ustalamy $\epsilon_1 = \ldots = \epsilon_s = -$, $\epsilon_{s+1} = \ldots = \epsilon_t = +$. Niech będą dane $N^- = \prod_{i=1}^s q_i \mid N$ oraz $N^+ = N/N^- = \prod_{i=s+1}^t q_i$, gdzie q_i są liczbami pierwszymi. Dla $s = 0$ niech $N^- = 1$ i $N^+ = N = \prod_{i=1}^t q_i$. Przy takich założeniach szereg*

$$E_{N^-,N^+} = [q_1]^{\epsilon_1} \circ \ldots \circ [q_t]^{\epsilon_t} E_2$$

zadaje znormalizowaną formę własną z $\mathcal{E}_2(\Gamma_0(N))$ względem algebry Hecke $\mathbb{T}_N$. Dla ustalonego s otrzymujemy $\binom{t}{s}$ różnych form określonych wyborami dzielnika N^-. Zbiór wszystkich takich form dla $s \in \{1, \ldots, t\}$ zadaje bazę przestrzeni $\mathbb{C}$-liniowej w $\mathcal{E}_2(\Gamma_0(N))$.

Dowód. Dla $t = 1$ mamy tylko jeden szereg $[p_1]^+E_2$, który spełnia warunki twierdzenia na mocy Lematu 3.1.17. Dla $t > 1$ stosujemy wielokrotnie Lemat 3.1.18 oraz Lemat 3.1.11. Zbiór form postaci E_{N^-,N^+} składa się z elementów liniowo niezależnych, bo każda forma ma inny system wartości własnych względem algebry Hecke. Ponadto dla ustalonego $s < t$ mamy $\binom{t}{s}$ wyborów dzielnika N^-. Sumując po s dostajemy $2^t - 1$ liniowo niezależnych form. Stosujemy Lemat 3.1.7, z którego wynika, że wymiar przestrzeni $\mathcal{E}_2(\Gamma_0(N))$ wynosi również $2^t - 1$, co kończy dowód twierdzenia. □

Uwaga 3.1.20. Twierdzenie 3.1.19 jest dowiedzione w pracy [Yoo13a, §2]. Autor tej pracy korzysta jednak z dodatkowych faktów, których użycie w naszej wersji dowodu udało się pominąć.

Wniosek 3.1.21. *Niech $N = \prod_{i=1}^{t} p_i$ będzie liczbą naturalną wolną od kwadratów, a p_i będą pierwsze, parami różne. Niech $N^- \mid N$, $N^+ = N/N^-$ oraz $E = E_{N^-,N^+}$. Wówczas*

$$a_0(E) = \begin{cases} -\frac{B_2}{4} \prod_{i=1}^{t} (1 - p_i), & \text{dla } N^- = 1, \\ 0, & \text{dla } N^- > 1. \end{cases}$$

Dowód. Zauważmy, że dla dowolnej formy h współczynnik $a_0([p]^-h) = 0$. Zatem dla $N^- > 1$ forma E ma postać $[p_j]^-g$, gdzie $g \in \mathcal{E}_2(\Gamma_0(N/p_j))$, więc $a_0(E) = 0$. W przypadku, gdy $N^- = 1$ na mocy równości $a_0([p]^+h) = a_0(h)(1 - p)$ otrzymujemy, że $a_0(E) = a_0(E_2) \prod_{i=1}^{t} (1 - p_i) = -\frac{B_2}{4} \prod_{i=1}^{t} (1 - p_i)$. □

3.2 Reprezentacje Galois

Zasadniczym powodem badania kongruencji pomiędzy formami modularnymi, które są wektorami własnymi algebry Hecke jest próba porównania reprezentacji Galois odpowiadających tym formom. Badanie kongruencji między formami parabolicznymi i szeregami Eisensteina odpowiada w tej sytuacji szukaniu kryteriów, dla których reprezentacje pochodzące od form parabolicznych po redukcji i semisymplifikacji przystają do reprezentacji pochodzących od form własnych Eisensteina. Jedną z pierwszych prac, w której kongruencje pomiędzy formami modularnymi były badane z punktu widzenia stowarzyszonych z nimi reprezentacji Galois jest artykuł H.P.F. Swinnertona-Dyera [SD73].

Przykład 3.2.1. Klasycznym wynikiem jest kongruencja zaobserwowana przez S. Ramanujana

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}, \tag{3.13}$$

dla $n \geq 0$, gdzie $\tau(n)$ jest współczynnikiem przy n-tej potędze rozwinięcia w szereg iloczynu

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n).$$

Bezpośredni dowód polega na obserwacji, że

$$\Delta = 2^6 \cdot 5^3 E_4^3 - 3 \cdot 7^2 E_6^2$$

oraz

$$E_{12} = \frac{2^8 \cdot 3^3 \cdot 5^2 \cdot 7}{13} E_4^3 + \frac{2^3 \cdot 3^2 \cdot 5^2 \cdot 7}{13} E_6^2.$$

Dla dowodu kongruencji Ramanujana wystarczy zauważyć, że współczynniki przy E_4^3 i E_6^2 dla form Δ i E_{12} przystają do siebie modulo 691. Forma modularna Δ jest generatorem jednowymiarowej $\mathbb{C}$-liniowej przestrzeni $\mathcal{S}_{12}(\Gamma(1))$. Kongruencje (3.13) są równoważne temu, że forma Δ przystaje do szeregu Eisensteina E_{12} modulo 691.

Niech $\overline{\mathbb{Q}}$ będzie ustalonym domknięciem algebraicznym ciała $\mathbb{Q}$. Niech $G_{\mathbb{Q}}$ oznacza absolutną grupę Galois ciała liczb wymiernych złożoną z automorfizmów $\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$. Grupa $G_{\mathbb{Q}}$ jest grupą topologiczną proskończoną wraz z topologią Krulla. Niech R będzie pierścieniem przemiennym z jedynką i ustaloną topologią. Grupa $GL_n(R)$ macierzy odwracalnych o wymiarze n posiada indukowaną topologię z podprzestrzeni R^{n^2}. Ciągły homomorfizm

$$\rho : G_{\mathbb{Q}} \to GL_n(R)$$

będziemy nazywać *reprezentacją Galois* grupy $G_{\mathbb{Q}}$ w grupie $GL_n(R)$.

Ustalamy liczbę pierwszą ℓ oraz domknięcie algebraiczne $\overline{\mathbb{Q}_\ell}$ ciała liczb ℓ-adycznych z topologią określoną przez waluację ℓ-adyczną. Rozważać będziemy reprezentacje Galois

$$\rho : G_{\mathbb{Q}} \to GL_n(\overline{\mathbb{Q}_\ell}).$$

Przykład 3.2.2 (Charakter cyklotomiczny)**.** Dla dowolnego $n \in \mathbb{N}$ ustalamy zbiór $\{\zeta_{\ell^n}\}$ pierwiastków pierwotnych z jedności takich, że $\zeta_{\ell^{n+1}}^{\ell} = \zeta_{\ell^n}$. Ustalamy izomorfizmy $\phi_n : Gal(\mathbb{Q}(\zeta_{\ell^n})/\mathbb{Q}) \to (\mathbb{Z}/\ell^n\mathbb{Z})^\times$, które spełniają $\phi_n(\zeta_{\ell^n} \mapsto \zeta_{\ell^n}^m) = m$. Dla danego automorfizmu $\sigma \in G_{\mathbb{Q}}$ kładziemy $a_n(\sigma) = m$, jeśli $\phi_n(\sigma|_{\mathbb{Q}(\zeta_{\ell^n})}) = m$. Niech $\chi_\ell : G_{\mathbb{Q}} \to \overline{\mathbb{Q}_\ell}^\times$ będzie reprezentacją Galois określoną następująco

$$\chi_\ell(\sigma) = (a_1(\sigma), a_2(\sigma), \ldots, a_n(\sigma), \ldots) \in \varprojlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^\times \cong \mathbb{Z}_\ell^\times \subset \overline{\mathbb{Q}_\ell}^\times.$$

Reprezentacja χ_ℓ jest nierozgałęziona poza ℓ, tj. χ_ℓ jest trywialna na grupie inercji $I_p \subset G_{\mathbb{Q}}$, gdzie p jest liczbą pierwszą różną od ℓ. Ponadto $\chi_\ell(Frob_p) = p$, gdzie $Frob_p$ jest absolutnym automorfizmem Frobeniusa dla p, patrz [DS05, §9.3].

Jeśli K jest ciałem liczbowym, to przez K_λ oznaczamy uzupełnienie ciała K względem ideału maksymalnego λ w $\mathcal{O}_K$.

Następne twierdzenie jest ważnym wynikiem, który pozwala skonstruować reprezentację Galois stowarzyszoną z dowolną nową formą własną w $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$. Dla wagi $k = 2$ opis konstrukcji tej reprezentacji jest następujący. Niech $X_0(N)$ będzie krzywą modularną dla grupy $\Gamma_0(N)$, patrz [DS05, §2.4]. Niech $J_0(N)$ będzie jakobianem krzywej $X_0(N)$, który jest rozmaitością abelową wymiaru $2g$, gdzie g oznacza genus krzywej $X_0(N)$. Niech ℓ będzię liczbą pierwszą, wówczas $T_\ell(J_0(N)) := \varprojlim J_0(N)[\ell^n](\overline{\mathbb{Q}})$ jest ℓ-adycznym modułem Tate'a jakobianu $J_0(N)$. Na punktach ℓ^n-torsyjnych $J_0(N)[\ell^n](\overline{\mathbb{Q}})$ działa grupa Galois $G_{\mathbb{Q}}$. Działanie to

przedłuża się do przestrzeni liniowej $V_\ell(J_0(N)) := T_\ell(J_0(N)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, która ma wymiar $2g$. Na $V_\ell(J_0(N))$ działa $\mathbb{Z}$-algebra $\mathcal{T}_N$ taka, że $\mathcal{T}_N \otimes_{\mathbb{Z}} \mathbb{C} \cong \mathbb{T}_N$. Przestrzeń $V_\ell(J_0(N))$ jest wolnym $R_{N,\ell} := \mathcal{T}_N \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$-modułem rangi 2. Wybierając ideał pierwszy λ nad ℓ w $\mathcal{O}_f$ dla nowej formy własnej $f \in \mathcal{S}_2(\Gamma_0(N))^{new}$ otrzymamy przestrzeń $K_{f,\lambda}$-liniową $V_{f,\lambda} := V_\ell(J_0(N)) \otimes_{R_{N,\ell}} K_{f,\lambda}$, na której działa grupa Galois $\mathbb{G}_\mathbb{Q}$. Homomorfizm $R_{N,\ell} \to K_{f,\lambda}$ pochodzi od działania algebry Hecke $\mathcal{T}_N \otimes_{\mathbb{Z}} \mathbb{C}$ na przestrzeni $S_2(\Gamma_0(N))$. Reprezentacja $\rho_{f,\lambda} : G_\mathbb{Q} \to GL(V_{f,\lambda}) \cong GL_2(K_{f,\lambda})$ jest opisana w poniższym twierdzeniu, por. [DS05, Theorem 9.5.4]. Deligne w pracy [Del69] dla wagi $k > 2$ w analogiczny sposób skonstruował przestrzenie $K_{f,\lambda}$-liniowe $V_{f,\lambda}$ wymiaru 2, jednak zamiast modułu Tate'a $V_\ell(J_0(N))$ wykorzystał przy tym kohomologie ℓ-adyczne rozmaitości Kuga-Sato. W rezultacie otrzymujemy następujące ważne twierdzenie.

Twierdzenie 3.2.3. *Niech N będzie liczbą naturalną i $k \geq 2$ będzie liczbą parzystą. Niech $f \in \mathcal{S}_k(\Gamma_0(N))^{new}$ będzie nową formą własną. Ustalamy ideał maksymalny λ w $\mathcal{O}_f$ leżący nad ℓ. Istnieje wtedy nierozkładalna reprezentacja Galois*

$$\rho_{f,\lambda} : G_\mathbb{Q} \to GL_2(K_{f,\lambda})$$

spełniająca warunki.

(i) Dla liczby pierwszej $p \notin \ell N$ reprezentacja $\rho_{f,\lambda}$ jest nierozgałęziona, tj. $\rho_{f,\lambda}(I_p) = \{1\}$ oraz

$$Tr(\rho_{f,\lambda}(Frob_p)) = a_p(f).$$

(ii) Zachodzi równość $\det(\rho_{f,\lambda}(\sigma)) = \chi_\ell^{k-1}(\sigma)$ dla dowolnego $\sigma \in G_\mathbb{Q}$.

Ponadto reprezentacja $\rho_{f,\lambda}$ jest jedyna z dokładnością do sprzężenia w $GL_2(K_{f,\lambda})$.

Uwaga 3.2.4. Zauważmy, że mając daną znormalizowaną formę własną $E \in \mathcal{E}_k(\Gamma_0(N))$, gdzie N jest wolne od kwadratów i $k \geq 2$ zachodzą równości $a_p(E) = 1 + p^{k-1}$ dla liczby pierwszej $p \nmid N$. Określamy reprezentację Galois

$$\rho = 1 + \chi_\ell^{k-1} : G_\mathbb{Q} \to GL_2(\mathbb{Z}_\ell).$$

Reprezentacja jest nierozgałęziona dla $p \neq \ell$ oraz dla $p \nmid N\ell$ spełnia równości

$$Tr(\rho(Frob_p)) = 1 + \chi_\ell^{k-1}(Frob_p) = 1 + p^{k-1} = a_p(E).$$

$$\det(\rho(\sigma)) = \chi_\ell^{k-1}(\sigma).$$

Można ponadto pokazać, że tak jak w przypadku form parabolicznych reprezentacja stowarzyszona z szeregiem Eisensteina E spełniająca podane warunki na ślad i wyznacznik jest jedyna z dokładnością do sprzężenia w $GL_2(\mathbb{Q}_\ell)$. Reprezentacja $1 + \chi_\ell^{k-1}$ jest rozkładalna, więc nie może być izomorficzna z reprezentacją $\rho_{f,\lambda}$ pochodzącą od nowej formy własnej f. Reprezentacja $\rho_{f,\lambda}$ nie musi posiadać współczynników w pierścieniu elementów całkowitych ciała $K_{f,\lambda}$. Zachodzi jednak poniższe stwierdzenie.

Stwierdzenie 3.2.5 ([DS05, Proposition 9.3.5]). *Niech L będzie skończonym rozszerzeniem $\mathbb{Q}_\ell$ dla pewnego ℓ pierwszego. Niech $\rho : G_\mathbb{Q} \to GL_d(L)$ będzie reprezentacją Galois. Istnieje macierz $A \in GL_d(L)$ taka, że reprezentacja sprzężona $\rho' = A\rho A^{-1}$ spełnia warunek $\rho'(G_\mathbb{Q}) \subset GL_d(\mathcal{O}_L)$, gdzie $\mathcal{O}_L$ jest domknięciem całkowitym $\mathbb{Z}_\ell$ w L.*

Wynika z tego, że jeśli dana jest reprezentacja $\rho_{f,\lambda}$ stowarzyszona z nową formą własną f i ideałem maksymalnym λ, to istnieje takie $A \in GL_2(K_{f,\lambda})$, że obraz $\rho'_{f,\lambda} = A\rho_{f,\lambda}A^{-1}$ leży w $GL_2(\mathcal{O}_{K_{f,\lambda}})$. Ślad i wyznacznik każdego elementu jest taki sam jak w wyjściowej reprezentacji. Ponadto reprezentacja pozostaje rozgałęziona dokładnie w tych samych liczbach pierwszych. Bez utraty ogólności możemy założyć, że reprezentacja $\rho_{f,\lambda}$ przekształca elementy z $G_\mathbb{Q}$ na macierze o współczynnikach w pierścieniu $\mathcal{O}_{K_{f,\lambda}}$. Odwzorowanie redukcji $\pi : \mathcal{O}_{K_{f,\lambda}} \to \mathcal{O}_{K_{f,\lambda}}/\lambda \cong \mathbb{F}$ pozwala nam określić reprezentację $\tilde{\rho}_{f,\lambda} : G_\mathbb{Q} \to GL_2(\mathbb{F})$, gdzie $\mathbb{F}$ jest pewnym ciałem skończonym charakterystyki ℓ. Reprezentacja jest nierozgałęziona dla $p \nmid N\ell$ i $Tr(\tilde{\rho}_{f,\lambda}(Frob_p)) = \pi(a_p(f))$. Taka reprezentacja może być rozkładalna.

Interesują nas przypadki, gdy reprezentacja $\tilde{\rho}_{f,\lambda}$ jest rozkładalna. Zastępując ją przez jej semisymplifikację, otrzymamy reprezentację, która jest sumą dwóch charakterów o wartościach w $\mathbb{F}^\times$. Ponadto dla formy modularnej f reprezentacja nad $GL_2(\mathbb{F})$ spełniająca podane wyżej warunki również jest jedyna z dokładnością do sprzężenia. W szczególności reprezentacja taka jest sprzężona z reprezentacją

$$1 + \tilde{\chi}_\ell^{k-1} : G_\mathbb{Q} \xrightarrow{1+\chi_\ell^{k-1}} GL_2(\mathbb{Z}_\ell) \twoheadrightarrow GL_2(\mathbb{F}_\ell) \hookrightarrow GL_2(\mathbb{F})$$

pochodzącą od formy Eisensteina $E \in \mathcal{E}_k(\Gamma_0(N))$. Stąd dla prawie wszystkich liczb pierwszych p otrzymujemy kongruencje

$$a_p(f) \equiv a_p(E) \pmod{\lambda}.$$

Na odwrót, mając dany system kongruencji tego typu dla formy parabolicznej f oraz formy Eisensteina E wiemy, że odpowiadające im zredukowane reprezentacje Galois (z dokładnością do semisymplifikacji) będą izomorficzne.

Przykład 3.2.6. Niech $\ell = 691$. Semisymplifikacja reprezentacji $\tilde{\rho}_{\ell,\Delta} : G_\mathbb{Q} \to GL_2(\mathbb{F}_\ell)$ odpowiadającej formie Δ z Przykładu 3.2.1 jest izomorficzna z reprezentacją $1 + \tilde{\chi}_\ell^{11}$ na mocy kongruencji (3.13).

Dokonując redukcji $\mathcal{O}_{K_{f,\lambda}} \to \mathcal{O}_{K_{f,\lambda}}/\lambda^r$ dla pewnego $r > 1$ nie możemy spodziewać się izomorfizmu odpowiadających formom f i E reprezentacji zredukowanych, ale możemy wciąż pytać dla jakiego r prawdziwe są kongruencje

$$a_p(f) \equiv a_p(E) \pmod{\lambda^r}$$

dla prawie wszystkich liczb pierwszych p. Badania nad tym problemem zostały zainicjowane w pracy [TiVW10]. W rozdziale 3.5.1 opiszemy algorytm, który pozwala sprawdzać za pomocą obliczeń wykonanych dla skończonej liczby współczynników Fouriera, kiedy dwie formy f i E przystają do siebie modulo λ^r. Z

przyczyn praktycznych, algorytm ten podamy w wersji, która uwzględnia również współczynniki a_p dla $p \mid N\ell$. Z punktu widzenia teorii reprezentacji, kongruencje na tych współczynnikach nie są istotne. Mimo tego, próba pominięcia tych współczynników wymusza wzrost stałej Sturma B z Twierdzenia 3.5.1. Takie wyniki zostały uzyskane w pracy [Ras, Proposition 2.12] dla kongruencji pomiędzy reprezentacjami odpowiadającymi dwóm formom parabolicznym. W praktyce zmodyfikowana stała B podana przez autora tej pracy uniemożliwiałaby wykonanie obliczeń w znaczącym zakresie wag i poziomów.

Jednym z pierwszych wyników dotyczących badanych w tej rozprawie kongruencji jest klasyczny rezultat B. Mazura.

Twierdzenie 3.2.7 ([Maz77])**.** *Niech N będzie liczbą pierwszą większą od 11. Jeśli ℓ jest liczbą pierwszą większą od 3, która dzieli $N-1$, to wówczas istnieje nowa forma własna $f \in \mathcal{S}_2(\Gamma_0(N))^{new}$ taka, że dla pewnego ideału maksymalnego λ w $\mathcal{O}_f$ leżącego nad ℓ zachodzą kongruencje*

$$a_p(f) \equiv 1 + p \ (mod\ \lambda)$$

dla prawie wszystkich p pierwszych. W szczególności redukcja i semisymplifikacja reprezentacji $\rho_{f,\lambda}$ daje reprezentację $1 + \tilde{\chi}_\ell$.

Uwaga 3.2.8. Jednym z zastosowań tego twierdzenia jest klasyfikacja wszystkich grup torsyjnych punktów $\mathbb{Q}$-wymiernych na krzywych eliptycznych nad $\mathbb{Q}$, patrz [Maz77, Theorem 8].

Poniższe twierdzenie pochodzące od Swinnertona-Dyera wskazuje kryteria istnienia kongruencji między parabolicznymi formami własnymi i formami Eisensteina w przypadku, gdy poziom $N = 1$.

Twierdzenie 3.2.9. *Niech $k \geq 2$ będzie liczbą naturalną. Niech f będzie formą własną na $\mathcal{S}_k(\Gamma(1))$ taką, że $a_1(f) = 1$ oraz dla dowolnego $n \in \mathbb{N}$ zachodzi $a_n(f) \in \mathbb{Z}$. Niech ℓ będzie liczbą pierwszą i $\rho_{f,\ell} : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_\ell)$ będzie reprezentacją Galois stowarzyszoną z f i $\ell\mathbb{Z}$ z Twierdzenia 3.2.3. Załóżmy, że obraz reprezentacji zredukowanej $\tilde{\rho}_{f,\ell} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_\ell)$ nie zawiera podgrupy $SL_2(\mathbb{F}_\ell)$. Wówczas zachodzi jeden z trzech przypadków.*

(i) Istnieje liczba całkowita m taka, że $a_n(f) \equiv n^m \sigma_{k-1-2m}(n)\ (mod\ \ell)$ dla wszystkich n względnie pierwszych z ℓ.

(ii) Jeśli n spełnia $\left(\frac{n}{\ell}\right) = -1$, to $a_n(f) \equiv 0\ (mod\ \ell)$.

(iii) Jeśli p jest liczbą pierwszą różną od ℓ, to $p^{1-k}a_p^2(f) \equiv 0, 1, 2, 4\ (mod\ \ell)$.

Każdy z wymienionych przypadków zachodzi dokładnie wtedy, gdy obraz reprezentacji $\tilde{\rho}_{\ell,f}$ spełnia pewne dodatkowe warunki, patrz [SD73, Corollary 1,2].

3.3 Kongruencje - warunki ogólne

Niech N będzie liczbą wolną od kwadratów oraz niech $E \in \mathcal{E}_k(\Gamma_0(N))$ będzie formą własną algebry Hecke $\mathbb{T}_N$. Załóżmy, że dla pewnej nowej formy własnej $f \in \mathcal{S}_k(\Gamma_0)^{\text{new}}$ i dla ustalonego ideału $\lambda \in \mathcal{O}_f$ zachodzą kongruencje

$$a_n(f) \equiv a_n(E) \pmod{\lambda^r} \tag{3.14}$$

dla każdego $n \geq 0$. Interesują nas następujące problemy:

(i) Przy ustalonej formie E danego poziomu N i wagi k rozstrzygnąć dla jakich λ istnieje nietrywialna rodzina kongruencji (3.14) dla pewnego $r > 0$.

(ii) Czy można podać górne oszacowanie na wykładnik r w zależności od formy E i poziomu N?

(iii) Ile form parabolicznych f danego poziomu N i wagi k może przystawać jednocześnie do tej samej formy E?

3.3.1 Istnienie kongruencji

Odpowiedź na pytanie (i) z poprzedniego paragrafu jest znana tylko w niektórych przypadkach. Przywołamy tu twierdzenia, które gwarantują istnienie kongruencji postaci (3.14), zazwyczaj dla współczynników o indeksach n względnie pierwszych z pewną ustaloną liczbą.

Poniższe twierdzenie jest konsekwencją Twierdzenia 3.2.7.

Twierdzenie 3.3.1 ([Maz77, Proposition 5.12])**.** *Niech N będzie liczbą pierwszą większą od 11. Jeśli ℓ jest liczbą pierwszą większą od 3, która dzieli $N-1$, to wówczas istnieje nowa forma własna $f \in \mathcal{S}_2(\Gamma_0(N))^{new}$ taka, że dla pewnego ideału maksymalnego λ w $\mathcal{O}_f$ leżącego nad ℓ zachodzą kongruencje*

$$a_n(f) \equiv a_n([N]^+ E_2) \ (mod\ \lambda)$$

dla wszystkich $n \geq 0$ takich, że $(N, n) = 1$.

Następne twierdzenie stanowi wariant Twierdzenia 3.3.1 dla wag $k \geq 4$. Istotny jest nadal fakt, że wskazane w sformułowaniu kongruencje nie muszą zachodzić dla wszystkich współczynników Fouriera. Podstawowym narzędziem w dowodzie jest forma Eisensteina w $\mathcal{E}_k(\Gamma_0(N))$ dla N pierwszego, która nie jest formą własną ze względu na operator Hecke U_N.

Twierdzenie 3.3.2 ([FD14, Theorem 1.1])**.** *Niech N będzie liczbą pierwszą oraz $k \geq 4$ będzie liczbą parzystą. Załóżmy, że $\ell > 3$ jest liczbą pierwszą, dla której $v_\ell((N^k - 1)(B_k/2k)) > 0$. Istnieje znormalizowana forma $f \in \mathcal{S}_k(\Gamma_0(N))$, która jest wektorem własnym dla operatorów Hecke T_n spełniających $(n, N) = 1$ oraz istnieje ideał $\lambda \in \mathcal{O}_f$ leżący nad ℓ taki, że*

$$a_n(f) \equiv a_n([N]^+ E_k) \ (mod\ \lambda)$$

dla wszystkich $n \geq 0$ spełniających $(N, n) = 1$.

Uwaga 3.3.3. Omówione w podrozdziale 3.6 wyniki wskazują, że wskazane w Twierdzeniu 3.3.2 kongruencje zachodzą w wielu przypadkach dla wszystkich współczynników Fouriera.

Sformułowane poniżej twierdzenia podają przykładowe warunki dostateczne, które gwarantują istnienie kongruencji pomiędzy pewną nową formą własną i formą własną w przestrzeni Eisensteina dla poziomów, które są liczbami złożonymi oraz dla wagi $k = 2$. Praca [Yoo13b] nie zawiera wyników dla wyższych wag k. W podrozdziale 3.6 wskazujemy przykłady kongruencji spełniających założenia podanych niżej twierdzeń, zmodyfikowane względem wagi $k > 2$.

Twierdzenie 3.3.4 (Ribet, [Yoo13b, Theorem 4.1.2])**.** *Niech t będzie liczbą nieparzystą i $p_1, \ldots, p_t$ będą parami różnymi liczbami pierwszymi. Niech $\ell \geq 5$ będzie liczbą pierwszą taką, że $\ell \mid \prod_{i=1}^{t}(p_i - 1)$. Wówczas istnieje nowa forma własna $f \in \mathcal{S}_2(\Gamma_0(p_1 \cdot \ldots \cdot p_t))^{new}$ spełniająca warunki*

(i) $a_{p_i}(f) = 1$ *dla dowolnego i,*

(ii) istnieje ideał maksymalny $\lambda \subset \mathcal{O}_f$ leżący nad ℓ oraz spełniona jest kongruencja

$$a_q(f) \equiv 1 + q \pmod{\lambda}$$

dla dowolnej liczby pierwszej q różnej od p_i, gdzie $1 \leq i \leq t$.

Twierdzenie 3.3.5 (Ribet, [Yoo13b, Theorem 4.1.2])**.** *Niech t będzie liczbą parzystą i niech $p_1, \ldots, p_t$ będą parami różnymi liczbami pierwszymi. Niech $\ell \geq 5$ będzie liczbą pierwszą taką, że $\ell \mid \prod_{i=1}^{t}(p_i - 1)$ oraz $p_t \equiv -1 \pmod{\ell}$. Wówczas istnieje nowa forma własna $f \in \mathcal{S}_2(\Gamma_0(p_1 \cdot \ldots \cdot p_t))^{new}$ spełniająca warunki:*

(i) $a_{p_i}(f) = 1$ *dla dowolnego $i \leq t - 1$,*

(ii) $a_{p_t}(f) = -1$,

(iii) istnieje ideał maksymalny $\lambda \subset \mathcal{O}_f$ leżący nad ℓ oraz spełniona jest kongruencja

$$a_q(f) \equiv 1 + q \pmod{\lambda}$$

dla dowolnej liczby pierwszej q różnej od p_i dla $1 \leq i \leq t$.

3.3.2 Ograniczenie górne na wykładnik kongruencji

W tym paragrafie przedstawimy główne wyniki autora dotyczące górnego ograniczenia na wykładnik kongruencji pomiędzy nową formą własną a formą własną Eisensteina. Wniosek 3.3.11 zawiera uogólnienie głównego wyniku z pracy [Nas14].

Lemat 3.3.6 ([AL70, Theorem 3])**.** *Niech $t \geq 1$ będzie liczbą naturalną, a $p_1, \ldots, p_t$ będą parami różnymi liczbami pierwszymi oraz niech $k \geq 2$ będzie liczbą naturalną parzystą. Niech $N = p_1 \cdot \ldots \cdot p_t$ oraz $f \in \mathcal{S}_k(\Gamma_0(N))^{new}$ będzie nową formą własną. Wówczas*

$$a_{p_i}(f) = -\lambda_{p_i} p_i^{k/2-1},$$

gdzie $\lambda_{p_i} \in \{\pm 1\}$.

Definicja 3.3.7. Jeśli K jest ciałem liczbowym i $\mathcal{O}_K$ pierścieniem liczb całkowitych tego ciała, to dla ideału maksymalnego $\lambda \subset \mathcal{O}_K$ i elementu $\alpha \in \mathcal{O}_K$ przez $ord_\lambda(\alpha)$ oznaczamy liczbę naturalną, która spełnia warunek

$$n \leq ord_\lambda(\alpha) \quad \Longleftrightarrow \quad \lambda^n \mid \alpha\mathcal{O}_K.$$

Ponadto dla dowolnego $x \in K^\times$ definiujemy $ord_\lambda(x) = ord_\lambda(\alpha) - ord_\lambda(\beta)$, gdy $x = \alpha/\beta$ i $\alpha, \beta \in \mathcal{O}_K$ oraz $\beta \neq 0$.

Uwaga 3.3.8. Równość $x = \alpha/\beta = \alpha'/\beta'$ pociąga $\alpha\beta' = \beta\alpha'$. Addytywność ord_λ implikuje $ord_\lambda(\alpha) + ord_\lambda(\beta') = ord_\lambda(\beta) + ord_\lambda(\alpha')$, więc

$$ord_\lambda(\alpha) - ord_\lambda(\beta) = ord_\lambda(\alpha') - ord_\lambda(\beta').$$

Zatem definicja $ord_\lambda(x)$ nie zależy od postaci ułamka x.

Definicja 3.3.9. Niech ℓ będzie liczbą pierwszą i niech $x = \frac{\ell^r p}{q}$ będzie liczbą wymierną taką, że $\ell \nmid p$ oraz $\ell \nmid q$. Definiujemy waluację ℓ-adyczną liczby x

$$v_\ell(x) := r.$$

Uwaga 3.3.10. Niech λ będzie dowolnym ideałem maksymalnym w $\mathcal{O}_K$ dla pewnego ciała liczbowego K. Dla dowolnego $a \in \mathbb{Q}^\times$ zachodzi oczywista równość $ord_\lambda(a) = ord_\lambda(\ell)v_\ell(a)$, jeżeli ℓ jest charakterystyką ciała $\mathcal{O}_K/\lambda$.

Wniosek 3.3.11. *Niech $p_1, \ldots, p_t$ będą parami różnymi liczbami pierwszymi oraz niech $k > 2$ będzie liczbą naturalną parzystą. Niech $N = p_1 \cdot \ldots \cdot p_t$ oraz $f \in \mathcal{S}_k(\Gamma_0(N))^{new}$ będzie nową formą własną. Niech $E = [p_1]^+ \circ \cdots \circ [p_t]^+ E_k$ będzie formą własną z $\mathcal{E}_k(\Gamma_0(N))$ (patrz Twierdzenia 3.1.14 i 3.1.19). Załóżmy, że dla ustalonego ideału maksymalnego $\lambda \subset \mathcal{O}_f$ i dla pewnego $r > 0$ zachodzą kongruencje*

$$a_n(f) \equiv a_n(E) \ (mod\ \lambda^r)$$

dla wszystkich $n \geq 0$. Jeśli ℓ jest charakterystyką ciała $\mathcal{O}_f/\lambda$ oraz $\ell \nmid N$, to

$$r \leq ord_\lambda(\ell) \cdot v_\ell\left(-\frac{B_k}{2k}\prod_{i=1}^{t}(1-p_i)\right).$$

Dowód. Dla każdego p_i na mocy Lematu 3.3.6 zachodzi równość $a_{p_i}(f) = -\lambda_{p_i} p_i^{k/2-1}$ dla pewnego $\lambda_{p_i} \in \{\pm 1\}$. Z drugiej strony, $a_{p_i}(E) = a_1(U_{p_i}E)$ i na mocy Lematu 3.1.18

$$a_{p_i}(E) = 1.$$

Z założenia zachodzi $a_{p_i}(f) \equiv a_{p_i}(E) \pmod{\lambda^r}$, więc $-\lambda_{p_i} p_i^{k/2-1} \equiv 1 \pmod{\lambda^r}$. Podnosząc ostatnią kongruencję obustronnie do kwadratu otrzymamy

$$1 - p_i^{k-2} \equiv 0 \pmod{\lambda^r}. \tag{3.15}$$

Ponadto $a_0(E) \equiv 0 \pmod{\lambda^r}$, ponieważ f jest z założenia paraboliczna. Zatem pierwsza równość w Lemacie 3.1.15 implikuje

$$-\frac{B_k}{2k}\prod_{i=1}^{t}(1-p_i^{k-1}) \equiv 0 \pmod{\lambda^r}.$$

Zauważmy, że $1-p_i^{k-1} = (1-p_i^{k-2}) + p_i^{k-2}(1-p_i)$. W połączeniu z kongruencją (3.15) i założeniem $\ell \nmid N$ daje to

$$-\frac{B_k}{2k}\prod_{i=1}^{t}(1-p_i) \equiv 0 \pmod{\lambda^r}.$$

Skoro $k > 2$, to $ord_\lambda(1-p_i^{k-1}) \geq ord_\lambda(1-p_i)$, więc

$$r \leq ord_\lambda\left(-\frac{B_k}{2k}\prod_{i=1}^{t}(1-p_i)\right)$$

i korzystając z Uwagi 3.3.10 otrzymujemy tezę. □

Wniosek 3.3.12. *Przy tych samych założeniach na N, k i f, co we Wniosku 3.3.11, niech $E = [p_1]^{\epsilon_1} \circ \ldots \circ [p_t]^{\epsilon_t}$ będzie formą własną z $\mathcal{E}_k(\Gamma_0(N))$ taką, że $a_0(E) = 0$. Ponadto niech $p_i \nmid N$ jeżeli $\epsilon_i = -$. Jeśli kongruencja*

$$a_n(f) \equiv a_n(E) \ (mod\ \lambda^r)$$

zachodzi dla każdego $n \geq 0$, to

$$r \leq \min\{\min_{i,\epsilon_i=+} ord_\lambda(1-p_i^{k-2}), \min_{i,\epsilon_i=-} ord_\lambda(1-p_i^k)\}.$$

Ponadto dla i takiego, że $\epsilon_i = +$ liczba p_i nie należy do ideału λ.

Dowód. Stosujemy Lemat 3.3.6. Podnosząc obie strony kongruencji $a_{p_i}(f) \equiv a_{p_i}(E) \pmod{\lambda^r}$ do kwadratu otrzymujemy warunek

$$p_i^{k-2} \equiv \begin{cases} 1, & \text{gdy } \epsilon_i = +, \\ p_i^{2(k-1)}, & \text{gdy } \epsilon_i = -. \end{cases} \tag{3.16}$$

Wykładnik r jest co najwyżej równy $ord_\lambda(1-p_i^{k-2})$ dla $\epsilon_i = +$. Podobnie, r jest co najwyżej równy $ord_\lambda(1-p_i^k)$ dla $\epsilon_i = -$, bo $p_i \nmid N$ z założenia. Kongruencja (3.16) dla i takiego, że $\epsilon_i = +$ pociąga, że $1-p_i^{k-2} \in \lambda^r$. Zatem $1-p_i^{k-2} \in \lambda$, więc gdyby p_i należało do λ, to $1 \in \lambda$. Sprzeczność, bo λ jest ideałem właściwym. □

Wniosek 3.3.13. *Niech $k = 2$ i niech $N = p$ będzie liczbą pierwszą. Niech nowa forma własna $f \in \mathcal{S}_k(\Gamma_0(N))^{new}$ oraz forma własna $E = [p]^+E_2 \in \mathcal{E}_k(\Gamma_0(N))$ spełniają kongruencje*

$$a_n(f) \equiv a_n(E) \ (mod\ \lambda^r)$$

dla każdego $n \geq 0$, gdzie $\lambda \subset \mathcal{O}_f$ jest ideałem maksymalnym oraz $r > 0$. Wówczas

$$p \notin \lambda.$$

Dowód. Zauważmy, że z kongruencji z założenia dla $n = 0$ oraz Wniosku 3.1.21 otrzymujemy

$$ord_\lambda \left(-\frac{1}{24}(1-p)\right) \geq r \geq 1,$$

więc $1 - p \in \lambda$, co implikuje, że $p \notin \lambda$. □

Uwaga 3.3.14. Jeśli N jest iloczynem większej liczby czynników pierwszych, to może się zdarzyć, że $N \in \lambda$. Można podać odpowiedni przykład dla $N = 5 \cdot 31$, gdy pewna nowa forma własna f przystaje do szeregu $[5]^+[31]^+E_2$ modulo 5. Na mocy kongruencji (3.16), gdy $E = [p_1]^{\epsilon_1} \circ \ldots \circ [p_t]^{\epsilon_t} E_2$ przystaje do nowej formy własnej f, to $p_i \notin \lambda$ o ile $\epsilon_i = -$. W Tabeli 3.1 zostały zebrane przykłady takich kongruencji dla wag $k = 2, 4$. Opis notacji jest podany w podrozdziale 3.6.

	N	N^-	N^+	k	ℓ	m	forma	λ	r	e	f	d
1	102	2	51	4	2	1	f_1	λ_1	2	2	1	2
2	102	6	17	4	2	1	f_1	λ_1	1	1	1	1
3	102	2	51	4	2	1	f_1	λ_1	1	1	1	2
4	102	2	51	4	2	1	f_1	λ_1	1	1	1	1
5	102	6	17	4	3	1	f_1	λ_1	1	1	1	1
6	679	97	7	2	7	2	f_1	λ_1	2	1	1	14
7	745	149	5	2	5	2	f_1	λ_1	2	1	1	14
8	995	199	5	2	5	2	f_1	λ_2	2	1	1	19
9	1010	101	10	2	5	2	f_1	λ_1	2	1	1	7
10	1010	1	1010	2	5	2	f_1	λ_1	2	1	1	7

Tabela 3.1: $a_n(f_i) \equiv a_n(E_{N^-,N^+}) \pmod{\lambda^r},\ n \geq 0,\ f_i \in \mathcal{S}_k(\Gamma_0(N))^{\text{new}},\ \ell \mid N$

3.4 Kongruencje - szczególne przypadki

W poprzednim podrozdziale omówiliśmy ograniczenie wykładnika r kongruencji (3.14) w ogólnej sytuacji. W tej części przedstawiamy dokładniejszy opis kongruencji postaci (3.14), gdy ciało K_f nowej formy własnej f jest równe $\mathbb{Q}$. Stosując podane w podrozdziale twierdzenia ograniczamy zbiór ideałów λ występujących w kongruencji (3.14) do skończonego zbioru $\{2\mathbb{Z}, 3\mathbb{Z}, 5\mathbb{Z}, 7\mathbb{Z}\}$. Dla poziomów N, które są liczbami pierwszymi lub iloczynami dwóch różnych liczb pierwszych podajemy dokładniejszą charakteryzację kongruencji postaci (3.14) przy założeniu $K_f = \mathbb{Q}$. Głównymi wynikami tego podrozdziału są Twierdzenia 3.4.5 i 3.4.8. Na koniec, w Uwadze 3.4.9 przytaczamy przykłady kongruencji (3.14), gdzie $K_f = \mathbb{Q}$ oraz poziom N jest iloczynem więcej niż dwóch czynników pierwszych.

Twierdzenie 3.4.1 ([Kat81, Theorem 2])**.** *Niech E będzie krzywą eliptyczną nad ciałem liczbowym K oraz niech $m \geq 2$ będzie liczbą całkowitą. Dla dowolnego ideału maksymalnego λ w $\mathcal{O}_K$, dla którego krzywa E ma dobrą redukcję, oznaczmy*

przez $N(\lambda)$ liczbę punktów $\mathcal{O}_K/\lambda$-wymiernych na E modulo λ. Jeśli zachodzi

$$N(\lambda) \equiv 0 \ (mod\ m)$$

dla λ ze zbioru ideałów pierwszych o gęstości 1, wówczas istnieje krzywa E' nad K, która jest K-izogeniczna z E oraz taka, że liczba punktów torsyjnych w $E'(K)$ jest podzielna przez m.

Twierdzenie 3.4.2 ([Miy73])**.** *Niech E będzie krzywą eliptyczną nad $\mathbb{Q}$ o przewodniku p, który jest liczbą pierwszą. Załóżmy, że grupa punktów torsyjnych T w $E(\mathbb{Q})$ ma rząd większy niż 2. Wówczas $p \in \{11, 17, 19, 37\}$ i istnieje tylko skończona lista krzywych E o tak zadanych własnościach.*

(i) Jeśli $p = 11$, to $T \cong \mathbb{Z}/5\mathbb{Z}$.

(ii) Jeśli $p = 17$, to $T \cong \mathbb{Z}/4\mathbb{Z}$ lub $T \cong (\mathbb{Z}/2\mathbb{Z})^2$.

(iii) Jeśli $p = 19$, to $T \cong \mathbb{Z}/3\mathbb{Z}$.

(iv) Jeśli $p = 37$, to $T \cong \mathbb{Z}/3\mathbb{Z}$.

Uwaga 3.4.3. Jeśli E jest krzywą eliptyczną o przewodniku pierwszym p, to $p \geq 11$. W takim razie każda taka krzywa ma dobrą redukcję modulo 2. Na mocy nierówności Hasse dla krzywych eliptycznych [Sil86, V,Theorem 1.1] zachodzi wtedy nierówność

$$|E(\mathbb{F}_2)| \leq 5.$$

Odwzorowanie redukcji $E(\mathbb{Q}) \to E(\mathbb{F}_2)$ jest injektywne po ograniczeniu do punktów m-torsyjnych jeśli $2 \nmid m$. Zatem grupa punktów torsyjnych T ma rząd $|T| = 2^m \cdot s$, gdzie $s \in \{1, 3, 5\}$ na mocy nierówności Hasse. Dowód Twierdzenia 3.4.2 polega na sprawdzeniu, które przypadki grupy torsyjnej są dopuszczalne i dla jakich krzywych eliptycznych. Zauważmy, że twierdzenie to nie wymaga wykorzystania klasyfikacji wymiernych punktów torsyjnych na krzywych eliptycznych podanej przez B. Mazura w pracy [Maz77].

Twierdzenie 3.4.4 ([Set75, Theorem 2])**.** *Niech E będzie krzywą eliptyczną nad $\mathbb{Q}$ o przewodniku p, który jest liczbą pierwszą. Jeśli $p > 17$ oraz grupa punktów torsyjnych w $E(\mathbb{Q})$ jest rzędu 2, to $p = u^2+64$, gdzie u jest pewną liczbą nieparzystą. Z dokładnością do izogenii istnieje dokładnie jedna taka krzywa dla danego p i jest to krzywa zadana równaniem*

$$y^2 = x^3 + ux^2 - 16x.$$

Jesteśmy teraz gotowi do sklasyfikowania wszystkich kongruencji postaci (3.14) w sytuacji, gdy $N = p$ jest liczbą pierwszą oraz $K_f = \mathbb{Q}$ dla nowej formy własnej f oraz $k = 2$. Na mocy Twierdzenia 3.1.19 przestrzeń $\mathcal{E}_2(\Gamma_0(N))$ jest jednowymiarowa i generowana przez nową formę własną $[p]^+E_2$. Dla $\ell > 2$ otrzymujemy skończoną listę kongruencji typu (3.14).

Twierdzenie 3.4.5. *Niech p będzie liczbą pierwszą. Niech $f \in \mathcal{S}_2(\Gamma_0(p))^{new}$ będzie nową formą własną o wymiernych współczynnikach Fouriera. Niech ℓ będzie liczbą pierwszą taką, że dla pewnego $r > 0$*

$$a_n(f) \equiv a_n([p]^+ E_2) \ (mod\ \ell^r)$$

zachodzi dla każdego $n \geq 0$. Wówczas spełniony jest jeden z warunków

(1) $\ell = 3$, $r = 1$ i $p = 19$ lub $p = 37$,

(2) $\ell = 5$, $r = 1$ i $p = 11$,

(3) $\ell = 2$, $r = 1$ i $p = 17$,

(4) $\ell = 2$, $r = 1$ i $p = u^2 + 64$, gdzie u liczbą całkowitą nieparzystą.

Dowód. Forma f ma współczynniki Fouriera należące do $\mathbb{Z}$ na mocy [DS05, Theorem 6.5.1]. Ponadto dla liczby pierwszej $q \neq p$ z kongruencji odczytujemy, że

$$a_q(f) \equiv 1 + q \ (\text{mod } \ell^r).$$

Z formą modularną f stowarzyszona jest krzywa eliptyczna E nad $\mathbb{Q}$ o przewodniku p taka, że jeśli q jest liczbą pierwszą dobrej redukcji dla E, to $a_q(f) = q+1-|E(\mathbb{F}_q)|$, por. [Cre97, Chapter II, §2.6]. Wówczas mamy

$$|E(\mathbb{F}_q)| \equiv 0 \ (\text{mod } \ell^r).$$

Na mocy Twierdzenia 3.4.1 istnieje krzywa E' izogeniczna z E nad $\mathbb{Q}$ taka, że $E'(\mathbb{Q})$ zawiera punkt ℓ^r torsyjny. Wówczas na mocy Twierdzenia 3.4.2 oraz Twierdzenia 3.4.4 liczba ℓ^r należy do zbioru $\{2, 3, 4, 5\}$.

Przypadek $\ell^r = 5$: Na mocy Twierdzenia 3.4.2 punkt (i) otrzymujemy, że $p = 11$. Przestrzeń $\mathcal{S}_2(\Gamma_0(11))$ jest wymiaru 1 i jest generowana przez nową formę własną

$$f = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 + \dots$$

Szereg $[11]^+ E_2$ ma rozwinięcie

$$[11]^+ E_2 = \frac{5}{12} + q + 3q^2 + 4q^3 + 7q^4 + 6q^5 + 12q^6 + \dots$$

Stała Sturma z Twierdzenia 3.5.1 wynosi w tym przypadku 2, więc porównując współczynniki obu form łatwo zauważyć, że przystają do siebie modulo 5 dla $n \leq 2$, zatem na mocy Twierdzenia 3.5.1 kongruencje

$$a_n(f) \equiv a_n([11]^+ E_2) \ (\text{mod } 5)$$

zachodzą dla każdego $n \geq 0$.

Przypadek $\ell^r = 3$: Na mocy Twierdzenia 3.4.2 punkt (iii) oraz (iv) otrzymujemy, że $p = 19$ lub $p = 37$. Dla $p = 19$ przestrzeń $\mathcal{S}_2(\Gamma_0(19))$ jest jednowymiarowa i generowana przez nową formę własną

$$f = q - 2q^3 - 2q^4 + 3q^5 - q^7 + q^9 + 3q^{11} + \dots$$

Porównujemy ją z szeregiem

$$[19]^+E_2 = 3/4+q+3q^2+4q^3+7q^4+6q^5+12q^6+8q^7+15q^8+13q^9+18q^{10}+12q^{11}+\dots$$

Stała Sturma wynosi 10/3, więc porównując współczynniki modulo 3 dla $n \leq 3$ otrzymujemy

$$a_n(f) \equiv a_n([19]^+E_2) \pmod 3$$

dla każdego $n \geq 0$.
Gdy $p = 37$ przestrzeń $\mathcal{S}_2(\Gamma_0(37))$ ma wymiar 2 i jest generowana przez dwie nowe formy własne f_1 i f_2

$$\begin{aligned} f_1 =& q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 6q^9 + 4q^{10} - 5q^{11} + \dots \\ f_2 =& q + q^3 - 2q^4 - q^7 - 2q^9 + 3q^{11} + \dots \end{aligned}$$

Porównujemy obie formy z szeregiem

$$[37]^+E_2 = 3/2+q+3q^2+4q^3+7q^4+6q^5+12q^6+8q^7+15q^8+13q^9+18q^{10}+12q^{11}+\dots$$

Stała Sturma wynosi w tym przypadku 19/3. Porównanie współczynników modulo 3 dla $n \leq 6$ wskazuje, że tylko forma f_2 przystaje do $[37]^+E_2$ modulo 3.

Przypadek $\ell^r = 2^r$: W tym przypadku albo $p = 17$, albo $p = u^2+64$ dla pewnego u. Pierwszy przypadek redukuje się do sprawdzenia, że nowa forma własna f, która generuje $\mathcal{S}_2(\Gamma_0(17))$

$$f = q - q^2 - q^4 - 2q^5 + 4q^7 + 3q^8 - 3q^9 + 2q^{10} + \dots$$

przystaje do

$$[17]^+E_2 = 2/3 + q + 3q^2 + 4q^3 + 7q^4 + 6q^5 + 12q^6 + 8q^7 + 15q^8 + 13q^9 + 18q^{10} + \dots$$

tylko modulo 2. Stała Sturma wynosi w tym przypadku 3. □

Uwaga 3.4.6. Istnienie nieskończonego ciągu liczb pierwszych postaci $u^2 + 64$ jest problemem otwartym. Na podstawie obliczeń numerycznych możemy wskazać poziomy $p = u^2 + 64$, dla których pewna nowa forma własna przystaje do szeregu $[p]^+E_2$ modulo 2. Zachodzi to na przykład dla

$$p = 113, 353, 593, 1153, 2273, 3089, 3313, 4289, 5393, 9473.$$

Jeśli założymy, że poziom N nie jest liczbą pierwszą, to najprostszą metodą uzyskania odpowiedzi, dla jakich λ i r zachodzą kongruencje (3.14) dla $K_f = \mathbb{Q}$ jest zastosowanie poniższego twierdzenia, udowodnionego przez B. Mazura.

Twierdzenie 3.4.7 ([Maz77, Theorem 8])**.** *Niech E będzie krzywą eliptyczną określoną nad $\mathbb{Q}$. Niech T będzie podgrupą punktów torsyjnych w grupie Mordella-Weila $E(\mathbb{Q})$. Wówczas T jest izomorficzna z*

(i) $\mathbb{Z}/n\mathbb{Z}$ dla pewnego $1 \leq n \leq 10$, albo $n = 12$, albo

(ii) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, *gdzie* $n \leq 4$.

Dla dowolnego N wolnego od kwadratów otrzymujemy, że $\lambda^r = \ell^r\mathbb{Z}$ w kongruencji (3.14) musi spełniać warunek $\ell^r \in \{2, 3, 4, 5, 7, 8, 9\}$. Gdy $N = pq$ jest iloczynem dwóch różnych liczb pierwszych p, q, to możemy wykluczyć istnienie kongruencji (3.14) spełniających $\ell^r \in \{8, 9\}$. Gdy N jest iloczynem więcej niż dwóch czynników pierwszych, to w Uwadze 3.4.9 wskazujemy przykłady kongruencji spełniających warunek $\ell^r \in \{8, 9\}$.

Twierdzenie 3.4.8. *Niech p, q będą różnymi liczbami pierwszymi. Niech $f \in \mathcal{S}_2(\Gamma_0(pq))^{new}$ będzie nową formą własną o wymiernych współczynnikach Fouriera. Niech E będzie formą własną z $\mathcal{E}_2(\Gamma_0(pq))$. Niech ℓ będzie liczbą pierwszą taką, że dla pewnego $r > 0$ kongruencja*

$$a_n(f) \equiv a_n(E) \ (mod\ \ell^r)$$

zachodzi dla każdego $n \geq 0$. Wówczas spełniony jest jeden z warunków

(1) $\ell^r \in \{2, 3, 4, 5\}$,

(2) $\ell^r = 7$ *i* $E = [13]^-[2]^+E_2$.

Dowód. Stosując argumentację z początku dowodu Twierdzenia 3.4.5 dochodzimy do wniosku, że krzywa eliptyczna F stowarzyszona z formą f spełnia

$$|F(\mathbb{F}_s)| \equiv 0 \ (\text{mod } \ell^r)$$

dla dowolnej liczby pierwszej s dobrej redukcji. Z Twierdzenia 3.4.1 wynika, że istnieje krzywa F' izogeniczna z F nad $\mathbb{Q}$, która posiada wymierny punkt ℓ^r torsyjny. Na mocy Twierdzenia 3.4.7 liczba ℓ^r należy do zbioru $\{2, 3, 4, 5, 6, 7, 8, 9\}$. Jeśli $\ell^r \in \{8, 9\}$, to stosując [Sad14, Theorem 3.7, 3.8] dostajemy $N = 6$, ale przestrzeń $\mathcal{S}_2(\Gamma_0(6))$ ma wymiar zero.

Jeśli $\ell^r = 7$, to [Sad14, Theorem 3.6] implikuje, że $N = 26$. Przestrzeń $\mathcal{S}_2(\Gamma_0(26))^{\text{new}}$ jest dwuwymiarowa i rozpinają ją nowe formy własne f_1, f_2 o rozwinięciach Fouriera

$$f_1 = q - q^2 + q^3 + q^4 - 3q^5 - q^6 - q^7 - q^8 - 2q^9 + 3q^{10} + 6q^{11} + \dots$$
$$f_2 = q + q^2 - 3q^3 + q^4 - q^5 - 3q^6 + q^7 + q^8 + 6q^9 - q^{10} - 2q^{11} + \dots$$

Przestrzeń $\mathcal{E}_2(\Gamma_0(26))$ ma bazę złożoną z 3 form własnych $[2]^-[13]^+E_2, [13]^-[2]^+E_2$ i $[2]^+[13]^+E_2$. Zauważmy, że na mocy Lematu 3.1.18

$$a_2([2]^-[13]^+E_2) = 2,$$
$$a_2([13]^-[2]^+E_2) = 1,$$
$$a_2([2]^+[13]^+E_2) = 1.$$

Stała Sturma B z Twierdzenia 3.5.2 wynosi 7. Sprawdzamy, że forma f_2 przystaje do $E = [13]^-[2]^+E_2$ modulo 7. Forma f_1 przystaje do szeregu Eisensteina $E = [2]^-[13]^+E_2$ modulo 3 i nie przystaje modulo 7 do żadnego z podanych szeregów Eisensteina. □

Uwaga 3.4.9. Jeśli rozważamy przypadek, gdy poziom N ma więcej niż dwa czynniki pierwsze, to istnieją nowe formy własne przystające do szeregów Eisensteina modulo ℓ^r, gdzie $\ell^r \in \{8, 9\}$. Przykłady takich form są podane w Tabelach 3.2 i 3.3.

	N	N^-	N^+	forma
1	714	17	42	f_9
2	1482	1	1482	f_{12}
3	1482	19	78	f_{12}
4	1554	1	1554	f_{14}
5	1554	37	42	f_{14}

Tabela 3.2: $a_n(f_i) \equiv a_n(E_{N^-,N^+}) \pmod{2^3},\ n \geq 0,\ f_i \in \mathcal{S}_2(\Gamma_0(N))^{\text{new}}$

	N	N^-	N^+	forma
1	102	17	6	f_3
2	210	7	30	f_5
3	690	23	30	f_{11}
4	930	31	30	f_{15}
5	1974	329	6	f_9
6	4074	97	42	f_{12}
7	4074	1	4074	f_{12}
8	4290	1	4290	f_{29}

Tabela 3.3: $a_n(f_i) \equiv a_n(E_{N^-,N^+}) \pmod{3^2},\ n \geq 0,\ f_i \in \mathcal{S}_2(\Gamma_0(N))^{\text{new}}$

3.5 Algorytmy

W tym podrozdziale przedstawiamy teoretyczny opis algorytmów, które zostały zaimplementowane przez autora w celu poszukiwania kongruencji pomiędzy formami parabolicznymi i szeregami Eisensteina. W podrozdziale 3.6 zostaną zaprezentowane szczegóły technicznie dotyczące samych obliczeń oraz tabele z podsumowaniem przeprowadzonych rachunków.

3.5.1 Algorytm Sturma

Twierdzenie 3.5.1 ([Ste07, Corollary 9.19])**.** *Niech będą ustalone liczby naturalne $k \geq 2$ i $N > 0$. Niech dane będą dwie formy modularne $f, g \in \mathcal{M}_k(\Gamma)$, gdzie Γ jest grupą kongruentną poziomu N. Załóżmy, że formy f i g mają q-rozwinięcia, których współczynniki należą do pierścienia $\mathcal{O}_K$ liczb algebraicznych całkowitych ustalonego ciała liczbowego K. Definiujemy stałą $B = \frac{km}{12}$, gdzie $m = [\Gamma(1) : \Gamma]$.*

Niech λ będzie ideałem maksymalnym w $\mathcal{O}_K$. Jeśli dla $0 \leq n \leq B$ zachodzą kongruencje

$$a_n(f) \equiv a_n(g) \ mod \ \lambda, \tag{3.17}$$

to kongruencje (3.17) zachodzą dla każdego $n \geq 0$.

Stałą B z Twierdzenia 3.5.1 nazywamy *stałą Sturma*.

Poniższe twierdzenie jest modyfikacją [CKR10, Proposition 1] zaadoptowaną przez autora rozprawy na potrzeby kongruencji pomiędzy formami parabolicznymi i szeregami Eisensteina.

Twierdzenie 3.5.2. *Niech $p_1, \ldots, p_t$ będą parami różnymi liczbami pierwszymi oraz niech $k \geq 2$ będzie liczbą naturalną parzystą. Niech $N = p_1 \cdot \ldots \cdot p_t$ oraz niech $f \in \mathcal{S}_k(\Gamma_0(N))$ będzie nową formą własną. Ustalamy r naturalne oraz ideał maksymalny λ w $\mathcal{O}_f$. Niech E będzie formą własną z $\mathcal{E}_k(\Gamma_0(N))$. Jeśli dla $n \leq k(\prod_i(p_i+1))/12$ zachodzi*

$$a_n(f) \equiv a_n(E) \ mod \ \lambda^r, \tag{3.18}$$

to wówczas kongruencje (3.18) są prawdziwe dla dowolnego $n \geq 0$.

Dowód. Oznaczmy przez B liczbę $k(\prod_i(p_i+1))/12$. Niech ℓ będzie charakterystyką ciała reszt $\mathcal{O}_f/\lambda$. Ponadto oznaczmy przez m mianownik ułamka

$$-\frac{B_k}{2k}\prod_{i=1}^{t}(1-p_i^{k-1}),$$

jeśli $a_0(E) \neq 0$. W przeciwnym przypadku kładziemy $m = 1$. Z założeń wynika, że $\ell \nmid m$ oraz współczynniki formy mE należą do $\mathbb{Z}$. Zauważmy, że $[\Gamma(1) : \Gamma_0(N)] = \prod_i(1+p_i)$ i stała B jest stałą Sturma z Twierdzenia 3.5.1. Jeśli dla $r = 1$ oraz dla $0 \leq n \leq B$ zachodzą kongruencje

$$a_n(mf) \equiv a_n(mE) \pmod{\lambda},$$

to z Twierdzenia 3.5.1 wnioskujemy, że kongruencje zachodzą dla $n \geq 0$. Skoro $m \notin \lambda$, to również $a_n(f) \equiv a_n(E) \pmod{\lambda}$ dla $n \geq 0$.

Załóżmy teraz, że $r > 1$. Przeprowadzimy dowód przez indukcję względem r. Załóżmy więc, że spełnione są kongruencje $a_n(f) \equiv a_n(E) \pmod{\lambda^{r-1}}$ dla $n \geq 0$. Niech $a_n(f) \equiv a_n(E) \pmod{\lambda^r}$ dla $0 \leq n \leq B$. Ustalamy liczbę algebraiczną $\pi \in \lambda \setminus \lambda^2$. Wówczas funkcja $\frac{1}{\pi^{r-1}}(f-E)$ należy do $\mathcal{M}_k(\Gamma_0(N))$ i jej współczynniki Fouriera należą do lokalizacji $(\mathcal{O}_f)_\lambda$ pierścienia $\mathcal{O}_f$ w ideale λ. Na mocy twierdzenia Shimury [Shi71, Theorem 3.52] przestrzeń liniowa $\mathcal{S}_k(\Gamma_0(N))$ ma bazę liniową składającą się z form o współczynnikach Fouriera należących do $\mathbb{Z}$. Podobnie przestrzeń liniowa $\mathcal{E}_k(\Gamma_0(N))$ ma taką bazę na mocy Twierdzenia 3.1.14 i Twierdzenia 3.1.19. Zatem forma $\frac{1}{\pi^{r-1}}(f-E)$ jest skończoną kombinacją liniową $\sum_i \alpha_i f_i$ form f_i o współczynnikach całkowitych, gdzie $\alpha_i \in (\mathcal{O}_f)_\lambda$. To pociąga,

że istnieje $\alpha \in \mathcal{O}_f \setminus \lambda$ takie, że forma $\frac{\alpha}{\pi^{r-1}}(f - E)$ ma współczynniki w $\mathcal{O}_f$. Dla $0 \leq n \leq B$ zachodzą kongruencje

$$\frac{\alpha}{\pi^{r-1}}(f - E) \equiv 0 \pmod{\lambda}.$$

Na mocy Twierdzenia 3.5.1 zachodzą one dla $n \geq 0$, ale to oznacza, że $\alpha(f - E) \equiv 0 \pmod{\lambda^r}$ dla $n \geq 0$ i skoro $\alpha \notin \lambda$, to zachodzi teza indukcyjna.

□

Lemat 3.5.3. *Przy założeniach z poprzedniego twierdzenia jeśli dla dowolnej liczby pierwszej $n = q$ takiej, że*

$$q \leq k(\prod_i (p_i + 1))/12$$

zachodzi kongruencja

$$a_n(f) \equiv a_n(E) \ mod \ \lambda^r, \tag{3.19}$$

to wówczas kongruencja (3.19) jest spełniona dla dowolnego $n \geq 0$.

Dowód. Formy f oraz E są formami własnymi względem algebry Hecke $\mathbb{T}_N$. Ponadto dla obu zachodzi równość $a_1(f) = 1 = a_1(E)$. Z definicji formy własnej i operatora Hecke $a_{nm}(f) = a_n(f)a_m(f)$ dla $(n, m) = 1$ i analogicznie dla E. Wystarczy zatem sprawdzić kongruencje dla współczynników o indeksach q^m, gdzie q pierwsze i $q \leq k(\prod_i (p_i + 1))/12$. Dla każdego m istnieje wielomian $P_{m,q} \in \mathbb{Z}[x]$ taki, że $a_{q^m}(f) = P_{m,q}(a_q(f))$ i również $a_{q^m}(E) = P_{m,q}(a_q(E))$. Zatem jeśli $a_q(f) \equiv a_q(E) \pmod{\lambda^r}$, to wykonując standardowe operacje wielomianowe na kongruencji uzyskujemy $P_{m,q}(a_q(f)) \equiv P_{m,q}(a_q(E)) \pmod{\lambda^r}$. Sprawdzając kongruencje dla wszystkich $q \leq k(\prod_i (p_i + 1))/12$ dochodzimy do wniosku, że kongruencja jest prawdziwa dla wszystkich n naturalnych spełniających $n \leq k(\prod_i (p_i + 1))/12$, więc na mocy Twierdzenia 3.5.1 kongruencje zachodzą dla $n \geq 0$. □

3.5.2 Poszukiwanie kongruencji - algorytm

Algorytm 1:
Opis algorytmu: Wskazuje jaka może być charakterystyka ciała reszt ideału pierwszego λ, dla którego może istnieć kongruencja postaci $a_n(f) \equiv a_n(E) \pmod{\lambda^r}$ pomiędzy nową formą własną f i formą własną $E \in \mathcal{E}_k(\Gamma_0(N))$, gdzie N jest wolne od kwadratów, $k \geq 2$ oraz $r > 0$.

Wejście: $k \geq 2$ liczba parzysta, $t \geq 1$ liczba naturalna, $(p_1, \ldots, p_t)$ ciąg parami różnych liczb pierwszych, ciąg $(\epsilon_1, \ldots, \epsilon_t)$ symboli $\epsilon_i \in \{+, -\}$

Kroki algorytmu

(1) Jeśli $k \geq 2$ i $\epsilon_1 = \ldots = \epsilon_t = +$, to zwróć na wyjście czynniki pierwsze występujące w liczniku wyrażenia $-\frac{B_k}{2k} \prod_i (1 - p_i)$. Przejdź do końca algorytmu.

(2) Jeśli $k = 2$ oraz $\epsilon_i = -$ dla pewnego i, to zwróć na wyjście te dzielniki pierwsze ℓ liczby $(1 - p_i^2)$, które spełniają $\ell \mid (1 - p_j^2)$ dla $j \neq i$, $\epsilon_j = -$. Przejdź do końca algorytmu.

(3) Jeśli $k > 2$ oraz $\epsilon_i = -$ dla pewnego i, to zwróć na wyjście te dzielniki pierwsze ℓ liczby $(1 - p_i^k)$, które spełniają $\ell \mid (1 - p_j^k)$ dla $j \neq i$, $\epsilon_j = -$ oraz $\ell \mid (1 - p_j^{k-2})$ dla $j \neq i$, $\epsilon_j = +$. Przejdź do końca algorytmu.

Wyjście: Ciąg liczb pierwszych $(\ell_1, \ldots, \ell_j)$ spełniających warunek: gdy $a_n(f) \equiv a_n(E) \pmod{\lambda^r}$ dla $r > 0$, to $\#(\mathcal{O}_f/\lambda) \in \{\ell_1, \ldots, \ell_j\}$. Uwaga: lista może być pusta, tj. $j = 0$.

Poprawność algorytmu: Zauważmy, że łącznie trzy przypadki obejmują wszystkie możliwości dla $k \geq 2$ i dowolnej formy własnej $E \in \mathcal{E}_k(\Gamma_0(N)$, gdzie N jest wolne od kwadratów. Poprawność algorytmu jest konsekwencją Wniosku 3.3.12, Wniosku 3.3.11 oraz definicji $a_0(E)$, gdy $E = [p_1]^+ \circ \ldots \circ [p_t]^+ E_2$.

Algorytm 2:
Opis algorytmu: Dla ustalonej liczby $k \geq 2$ parzystej, N wolnego od kwadratów, ustalonego ℓ pierwszego oraz formy własnej $E \in \mathcal{E}_k(\Gamma_0(N))$, algorytm sprawdza, które nowe formy własne $f \in \mathcal{S}_k(\Gamma_0(N))$ spełniają kongruencję $a_n(f) \equiv a_n(E) \pmod{\lambda^r}$, $n \geq 0$ dla pewnego λ i maksymalnego możliwego r, $\ell \in \lambda$ oraz $r > 0$.

Wejście: $k \geq 2$ liczba parzysta, $N > 1$ liczba naturalna wolna od kwadratów, ℓ liczba pierwsza oraz $E \in \mathcal{E}_k(\Gamma_0(N))$ forma własna.

Kroki algorytmu

(0) Sprawdź czy $a_0(E) = 0$. Jeśli tak, przejdź do Kroku 1. Jeśli nie, sprawdź czy ℓ dzieli licznik $a_0(E)$. Jeśli tak, przejdź do Kroku 1. Jeśli nie, zakończ algorytm.

(1) Wyznacz rozłączne zbiory C_i nowych form własnych w $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ takie, że dowolne dwa elementy z C_i są Galois sprzężone.

(2) Dla każdego zbioru C_i wybierz jeden jego element i utwórz zbiór $F_{N,k}$ tak wybranych elementów.

(3) Oblicz stałą Sturma $B = (k/12)[\Gamma(1) : \Gamma_0(N)]$.

(4) Dla każdego elementu $f \in F_{N,k}$ wyznacz ciało liczbowe K_f rozwinięcia Fouriera formy f.

(5) Dla każdego elementu $f \in F_{N,k}$ utwórz zbiór $S_{\ell,f}$ składający się z ideałów maksymalnych wchodzących w rozkład na czynniki pierwsze ideału $\ell\mathcal{O}_f$.

(6) Dla każdego elementu $f \in F_{N,k}$ i każdego $\lambda \in S_{\ell,f}$ oblicz

$$r_\lambda = \min \{ord_\lambda (a_q(f) - a_q(E)) \mid q \leq B\}.$$

Minimum przebiega po liczbach pierwszych q. Zwróć na wyjście trójkę (f, λ, r_λ) o ile $r_\lambda > 0$.

Wyjście: Ciąg trójek postaci (f, λ, r) spełniających warunek:

$$a_n(f) \equiv a_n(E) \pmod{\lambda^r}.$$

dla $n \geq 0$. Uwaga: lista może być pusta.

Poprawność algorytmu: W Kroku 0 sprawdzamy czy kongruencja może w ogóle istnieć. Krok 1 jest wykonalny, ponieważ zbiór nowych form własnych jest skończony dla danego poziomu N i wagi k oraz każdą formę można reprezentować w sposób skończony. Wyznaczona w Kroku 6 liczba r_λ spełnia warunki wyjściowe ze względu na Lemat 3.5.3. Stała B podana w algorytmie jest równa stałej z Lematu 3.5.3, ponieważ N jest wolne od kwadratów.

3.6 Dane numeryczne

Autor rozprawy w pracy [Nas14] rozpoczął zbieranie danych numerycznych dotyczących kongruencji między formami parabolicznymi a szeregami Eisensteina. W pracy [Nas14] przedstawione są wyniki numerycznego badania kongruencji dla poziomów N będących liczbami pierwszymi oraz dla szeregu Eisensteina $[N]^+E_k$, gdzie waga k zmieniała się w zakresie $2 \leq k \leq 24$. Celem niniejszego podrozdziału jest omówienie wyników obliczeń przeprowadzonych dla poziomów N wolnych od kwadratów i dla wag k w zakresach ujętych w Tabeli 3.4. Głównym zasobem obliczeniowym był klaster Gauss na uniwersytecie w Luksemburgu. Podczas przygotowywania tej rozprawy dostępu do niego użyczył Gabor Wiese. Komputer posiada 20 jednostek CPU typu Intel(R) Xeon(R) CPU E7- 4850 @ 2.00GHz oraz około 200 GB pamięci RAM. Przeprowadzone obliczenia wykorzystywały pakiet numeryczny MAGMA [BCP97] oraz zestaw instrukcji MONTES [GMN12] znacząco poprawiający wydajność obliczeń na ciałach liczbowych, w stosunku do oryginalnej implementacji w pakiecie MAGMA.

k	2	4	6	8	10	12	14	16	18	20	22	24
$N \leq$	4559	922	302	202	193	102	94	94	94	94	94	94

Tabela 3.4: Waga k i maksymalny zakres poziomu N.

Podstawowy sposób zbierania danych polegał na konsekwentnym przeprowadzaniu obliczeń opisanych w Algorytmach 1 i 2 z podrozdziału 3.5.2. Wyniki

zostały skatalogowane w formie plików tekstowych, a następnie umieszczone w interaktywnej bazie danych opartej na systemie PostgreSQL 9.1.9. Zawartość bazy zostanie udostępniona przez autora na życzenie.

Opis danych zawartych w tabelach. Zaprezentowane dane dotyczą następującej sytuacji. Dana jest nowa forma własna $f \in \mathcal{S}_k(\Gamma_0(N))^{\text{new}}$, gdzie $k \geq 2$ oraz N jest wolne od kwadratów. Niech $N = p_1 \cdot \ldots \cdot p_t$ dla pewnego $t > 0$, gdzie p_i są różnymi liczbami pierwszymi. Niech dane będą $N^- = \prod_{i=1}^{s} q_i \mid N$ oraz $N^+ = N/N^-$, gdzie q_i są liczbami pierwszymi. Szereg

$$E_{N^-,N^+} = [q_1]^{\epsilon_1} \circ \ldots \circ [q_t]^{\epsilon_t} E_k$$

jest formą własną należącą do przestrzeni $\mathcal{E}_k(\Gamma_0(N))$. Dany jest ideał maksymalny $\lambda \subset \mathcal{O}_f$ oraz pewna liczba dodatnia $r > 0$. Wiersze w przedstawionych tabelach opisują kongruencje

$$a_n(f) \equiv a_n(E_{N^-,N^+}) \pmod{\lambda^r} \tag{3.20}$$

zachodzące dla wszystkich $n \geq 0$. Niech ℓ oznacza charakterystykę ciała $\mathbb{F} = \mathcal{O}_f/\lambda$, natomiast f jest liczbą $[\mathbb{F} : \mathbb{F}_\ell]$. Liczba d oznacza stopień $[K_f : \mathbb{Q}]$. Liczba e jest równa $ord_\lambda(\ell)$. Liczba m jest maksimum po s, dla których jednocześnie zachodzą kongruencje

$$a_{p_i}(f) \equiv a_{p_i}(E_{N^-,N^+}) \pmod{\ell^s}, \quad 1 \leq i \leq t,$$
$$a_0(f) \equiv a_0(E_{N^-,N^+}) \pmod{\ell^s}.$$

Zauważmy, że m jest zależne od wyboru N, N^+, N^-, f, E_{N^-,N^+} oraz λ. Górnym ograniczeniem na wykładnik kongruencji r jest $m \cdot e$. Ponadto liczba ta może być mniejsza niż górne ograniczenie podane we Wnioskach 3.3.11, 3.3.12.
Numeracja nowych form własnych w $\mathcal{S}_k(\Gamma_0(N))$ jest oparta na algorytmie sortowania stosowanym w [Cre97, Chapter IV]. Szczegóły algorytmu zostały opisane w podręczniku użytkownika pakietu MAGMA dostępnym online[1]. Numeracja ideałów maksymalnych w rozkładzie $\ell\mathcal{O}_f$ została opisana w dokumentacji pakietu MONTES[2]. W kolumnie nazwanej „forma" stosować będziemy ustaloną numerację nowych form własnych: jeśli i jest numerem, który zwraca algorytm, w tabeli umieścimy symbol f_i. W kolumnie oznaczonej przez λ stosujemy notację λ_i, gdzie i jest numerem ideału zwracanym przez algorytm, zgodnie z numeracją stosowaną w pakiecie Montes.

Przykład 3.6.1. W Tabeli 3.5 zaprezentowany został przykładowy wiersz danych. Można z niego odczytać, że forma $f_1 \in \mathcal{S}_2(\Gamma_0(2651))$ przystaje do szeregu Eisensteina $E_{1,2651}$ modulo λ_1^2. Ideał λ_1 ma charakterystykę ciała reszt równą 5 i jest rozgałęziony, stopień rozgałęzienia $e = 2$. Ponadto stopień ciała liczbowego K_f nad $\mathbb{Q}$ wynosi 35 i ciało reszt $\mathcal{O}_f/\lambda_1 = \mathbb{F}_5$. Górne teoretyczne ograniczenie na wykładnik r jest równe $m \cdot e = 4$, lecz kongruencja zachodzi tylko dla $r = 2$.

W dalszym ciągu prezentujemy część nowych wyników obliczeń numerycznych. Dane zapisane w Tabeli 3.6 zostały wybrane w taki sposób, aby każdej parze

[1] `http://magma.maths.usyd.edu.au/magma/handbook/text/1545`
[2] `http://www-ma4.upc.edu/~guardia/MontesAlgorithm.html`

N	N^-	N^+	k	ℓ	m	forma	λ	r	e	f	d
2651	1	2651	2	5	2	f_1	λ_1	2	2	1	35

Tabela 3.5: Przykładowy wiersz danych

(r, ℓ) przyporządkować jedną kongruencję, dla której wartość r jest maksymalna możliwa w całym zakresie danych ustalonym w Tabeli 3.4. Wybór k jest losowy jeśli do dyspozycji było więcej kongruencji dla ustalonej pary (r, ℓ). Ponadto dane są posortowane malejąco ze względu na wartość r. W Tabeli 3.8 znalazły się dane dotyczące kongruencji, które spełniają warunek $N^- = 1$. Ponadto wybór kongruencji był podyktowany tym, aby w i-tym wierszu znalazła się kongruencja spełniająca $d \geq 10i$ przy najmniejszym możliwym N. Wszystkie wartości N podane w tej tabeli są liczbami pierwszymi.

	N	N^-	N^+	k	ℓ	m	forma	λ	r	e	f	d
1	2	2	1	22	2	10	f_1	λ_1	8	1	1	1
2	2159	127	17	2	2	7	f_1	λ_1	7	1	1	56
3	78	78	1	8	2	3	f_1	λ_1	6	2	1	2
4	34	2	17	10	2	4	f_1	λ_1	5	2	1	2
5	1459	1	1459	2	3	5	f_1	λ_1	5	1	1	71
6	94	2	47	18	2	7	f_1	λ_2	4	1	1	18
7	146	2	73	6	3	2	f_1	λ_3	4	2	1	9
8	78	2	39	22	2	3	f_1	λ_4	3	1	1	5
9	163	1	163	10	3	4	f_1	λ_1	3	1	1	62
10	443	443	1	4	5	4	f_1	λ_1	3	1	1	60
11	1373	1	1373	2	7	3	f_1	λ_1	3	1	1	60
12	2663	1	2663	2	11	3	f_1	λ_2	3	1	1	132
13	239	239	1	4	13	4	f_1	λ_1	3	1	1	37

Tabela 3.6: Kongruencje spełniające $r > 2$ i $m > 1$, po jednej na parę (r, ℓ)

3.7 Wnioski z danych i przykłady kongruencji

W podrozdziale 3.5 przedstawiliśmy algorytmy do znajdowania kongruencji postaci (3.20). Omówienie danych numerycznych z podrozdziału 3.6 wymaga dalszego rozwinięcia, co jest celem niniejszego podrozdziału. W paragrafie 3.7.1 omawiamy wyniki zawarte w pracy [Nas14] autora rozprawy. Szczegółowo omawiamy kilka wybranych przykładów kongruencji. W paragrafie 3.7.2 opisujemy nowe wyniki, uzyskane po opublikowaniu pracy [Nas14]. Zakres przebadanych wag i poziomów znacząco wykracza poza materiał opublikowany w pracy [Nas14], patrz Tabela 3.4. Przedstawiamy w paragrafie 3.7.2 te wnioski płynące z zebranych danych numerycznych, które w odczuciu autora rozprawy wydają się być interesujące.

	N	N^-	N^+	k	ℓ	m	forma	λ	r	e	f	d
1	31	31	1	10	5	2	f_1	λ_3	1	2	1	13
2	33	11	3	12	11	2	f_1	λ_4	1	2	1	6
3	33	11	3	12	11	2	f_1	λ_4	1	2	1	5
4	35	5	7	6	5	2	f_1	λ_1	1	2	1	2
5	35	5	7	6	5	2	f_1	λ_1	1	2	1	4
6	35	35	1	8	5	2	f_1	λ_2	1	2	1	5
7	35	35	1	12	5	2	f_1	λ_3	1	2	1	4
8	35	35	1	12	5	2	f_1	λ_3	1	2	1	6
9	35	5	7	14	5	2	f_1	λ_3	1	2	1	6
10	35	5	7	14	5	2	f_1	λ_3	1	2	1	8
11	35	35	1	16	5	2	f_1	λ_3	2	3	1	7
12	35	35	1	16	5	2	f_1	λ_4	1	2	1	9
13	35	35	1	16	5	2	f_1	λ_3	2	3	1	9
14	55	5	11	12	5	2	f_1	λ_2	1	2	1	11
15	55	5	11	12	5	2	f_1	λ_2	1	2	1	8
16	79	79	1	6	7	2	f_1	λ_1	1	2	1	19
17	79	79	1	12	7	2	f_1	λ_1	1	2	1	33
18	101	101	1	4	5	2	f_1	λ_1	1	3	1	9
19	101	101	1	8	5	2	f_1	λ_2	1	3	1	26
20	101	101	1	12	5	2	f_1	λ_2	1	3	1	42
21	107	107	1	4	5	2	f_1	λ_1	1	2	1	16
22	107	107	1	8	5	2	f_1	λ_1	1	2	1	28
23	133	7	19	8	7	3	f_1	λ_3	1	3	1	16
24	133	7	19	8	7	3	f_1	λ_3	1	3	1	16

Tabela 3.7: Przykładowe kongruencje spełniające $e > 1$, $m > 1$, $\ell > 3$

Ponadto na ich bazie można sformułować szereg przypuszczeń, co do ogólnej natury kongruencji typu (3.20), patrz Wniosek 3.7.8.

3.7.1 Kongruencje dla $N = p$ i $k = 2$

Wnioski z danych numerycznych sformułowane w tym podrozdziale pochodzą z pracy autora [Nas14].

Przy założeniach, że waga $k = 2$ i poziom $N = p$ jest liczbą pierwszą przestrzeń $E_2(\Gamma_0(N))$ jest jednowymiarowa i generowana przez formę własną $[p]^+E_2$. Asymptotycznie wymiar przestrzeni $\mathcal{S}_2(\Gamma_0(p))$ jest równy $(p+1)/12+O(1/p)$ przy $p \to \infty$. Jeśli przestrzeń jest generowana przez orbity Galois co najwyżej dwóch form własnych, stopień ciała współczynników może wynosić około $(p+1)/24$. W praktyce oznacza to, że bardzo trudno jest wykonywać obliczenia dla dużych liczb pierwszych, spodziewając się rozkładu przestrzeni $\mathcal{S}_2(\Gamma_0(p))$ na małą liczbę podprzestrzeni generowanych przez nowe formy własne i ich Galois sprzężone elementy.

	N	N^-	N^+	k	ℓ	m	forma	λ	r	e	f	d
1	131	1	131	2	13	1	f_1	λ_1	1	1	1	10
2	311	1	311	2	5	1	f_1	λ_1	1	1	1	22
3	479	1	479	2	239	1	f_1	λ_3	1	1	1	32
4	719	1	719	2	359	1	f_1	λ_2	1	1	1	45
5	839	1	839	2	419	1	f_1	λ_1	1	1	1	51
6	1031	1	1031	2	5	1	f_1	λ_1	1	1	1	60
7	1399	1	1399	2	233	1	f_1	λ_2	1	1	1	71
8	1487	1	1487	2	743	1	f_1	λ_1	1	1	1	80
9	1559	1	1559	2	19	1	f_1	λ_2	1	1	1	90
10	1931	1	1931	2	5	1	f_1	λ_1	1	1	1	101
11	2111	1	2111	2	5	1	f_1	λ_2	1	1	1	112
12	2351	1	2351	2	5	2	f_1	λ_1	1	1	1	123
13	2591	1	2591	2	5	1	f_1	λ_2	1	1	1	136
14	2879	1	2879	2	1439	1	f_1	λ_1	1	1	1	148
15	2903	1	2903	2	1451	1	f_1	λ_2	1	1	1	150
16	2999	1	2999	2	1499	1	f_1	λ_1	1	1	1	161
17	3359	1	3359	2	23	1	f_1	λ_1	1	1	1	174
18	3659	1	3659	2	31	1	f_1	λ_1	1	1	1	181
19	3671	1	3671	2	5	1	f_1	λ_1	1	5	1	193
20	3911	1	3911	2	5	1	f_1	λ_1	1	2	1	202
21	4079	1	4079	2	2039	1	f_1	λ_2	1	1	1	212
22	4391	1	4391	2	5	1	f_1	λ_4	1	1	1	222

Tabela 3.8: Wybrane kongruencje posortowane ze względu na stopień d.

Przypadek $r = m$ i $e = 1$

Niech $p = 109$ oraz α niech będzie pierwiastkiem wielomianu $x^4+x^3-5x^2-4x+3$. Wybieramy formę $f \in \mathcal{S}_2(\Gamma_0(p))^{new}$ o rozwinięciu

$$f = q + \alpha q^2 + (1 + 4\alpha - \alpha^3)q^3 + (\alpha^2 - 2)q^4 - \alpha q^5 + \dots$$

Ciało K_f jest równe $\mathbb{Q}(\alpha)$ oraz pierścień liczb całkowitych $\mathcal{O}_f = \mathbb{Z}[\alpha]$. Zachodzi równość $a_0([109]^+E_2) = 9/2$. Rozkład ideału $(3) = 3\mathcal{O}_f$ jest postaci

$$(3) = (3, \alpha)(3, 2 + \alpha + \alpha^2 + \alpha^3).$$

Za pomocą Algorytmu 2 sprawdzamy, że dla $\lambda = (3, \alpha)$ zachodzą kongruencje

$$a_n(f) \equiv a_n([109]^+E_2) \pmod{\lambda^2}$$

dla wszystkich $n \geq 0$. Ponadto $ord_\lambda(a_0([109]^+E_2)) = 2$, bo ideał jest nierozgałęziony, więc znaleziona kongruencja jest spełniona z maksymalnym dopuszczalnym wykładnikiem.

Przypadek $m > r > 1$ **i** $e = 1$

Niech $p = 487$. Przestrzeń $\mathcal{S}_2(\Gamma_0(487))$ jest wymiaru 40 i zawiera pięć klas sprzężoności Galois nowych form własnych, które rozpinają przestrzenie wymiarów $2, 2, 3, 16, 17$. Dla formy f zawartej w przestrzeni własnej wymiaru 16 zachodzą kongruencje z szeregiem $[487]^+E_2$. Niech α będzie pierwiastkiem wielomianu

$$\begin{aligned} x^{16} - 7x^{15} - 5x^{14} + 131x^{13} - 132x^{12} - 977x^{11} + 1666x^{10} + 3671x^9 \\ -8191x^8 - 7212x^7 + 20571x^6 + 6937x^5 - 27100x^4 - 2748x^3 \\ +17207x^2 + 360x - 3825. \end{aligned}$$

Wybieramy formę $f = q + \alpha q + \dots$ w $\mathcal{S}_2(\Gamma_0(487))$. Jej ciało współczynników $K_f = \mathbb{Q}(\alpha)$ ma stopień 16 nad $\mathbb{Q}$ oraz pierścień liczb całkowitych $\mathcal{O}_f$ zawiera $\mathbb{Z}[\alpha]$ jako podgrupę indeksu 105. Ze względu na równość $a_0([487]^+E_2) = 81/4$ rozważamy kongruencje dla ideałów pochodzących z rozkładu

$$3\mathcal{O}_f = \lambda_1\lambda_2\lambda_3\lambda_4.$$

Wyróżnik pierścienia $\mathcal{O}_f$ jest równy $19^2 \cdot 59 \cdot 623519211698413571686763$ w rozkładzie na czynniki pierwsze, więc ideały maksymalne λ_i są nierozgałęzione i parami różne. Wybieramy $\lambda_1 = (3, \frac{1}{105}\beta)$, gdzie

$$\begin{aligned} \beta = 2\alpha^{15} + 106\alpha^{14} + 50\alpha^{13} + 112\alpha^{12} + 156\alpha^{11} + 161\alpha^{10} + 392\alpha^9 + 307\alpha^8 \\ +148\alpha^7 + 126\alpha^6 + 192\alpha^5 + 194\alpha^4 + 280\alpha^3 + 279\alpha^2 + 124\alpha + 705. \end{aligned}$$

Algorytm 2 pozwala nam ustalić, że zachodzi kongruencja między f i $[487]^+E_2$ modulo λ_1^3. Teoretyczne górne ograniczenie m na wykładnik kongruencji wynosi 4, więc $m > r > 1$.

Przypadek $0 < r < e < m$ **i** $e > 1$

Niech $p = 3001$. Przestrzeń $\mathcal{S}_2(\Gamma_0(3001))$ jest suma prostą trzech podprzestrzeni wymiarów $2, 115$ i 132. Podprzestrzeń wymiaru 2 jest generowana przez dwie nowe formy własne Galois sprzężone f_1 i f_2

$$f_i = q + \alpha_i q^2 + (\alpha_i + 1)q^3 + (\alpha_i - 1)q^4 + 2\alpha_i q^5 + (2\alpha_i + 1)q^6 + \cdots,$$

gdzie α_1 i α_2 są pierwiastkami wielomianu $x^2 - x - 1$. Ustalamy, że $\alpha_1 = (1+\sqrt{5})/2$ jest dodatnim pierwiastkiem i ciało współczynników formy f_1 to $K_{f_1} = \mathbb{Q}(\alpha_1)$. Jego pierścień liczb całkowitych $\mathcal{O}_{f_1} = \mathbb{Z}[\alpha_1]$. Ideał $5\mathcal{O}_{f_1}$ jest równy λ^2, gdzie

$$\lambda = (5, 2 + \frac{1+\sqrt{5}}{2}).$$

Współczynnik $a_0([3001]^+E_2) = 125$ i $ord_\lambda(125) = 6$. Algorytm 2 pozwala nam ustalić, że forma f_1 przystaje do $[3001]^+E_2$ modulo λ. Zauważmy, że

$$a_2(f_1) - a_2([3001]^+E_2) = \frac{1+\sqrt{5}}{2} - 3 \notin \lambda^2.$$

Duże ciało reszt

Niech $p = 401$. Przestrzeń $S_2(\Gamma_0(401))$ rozkłada się na dwie podprzestrzenie wymiarów 12 i 21. Forma $f = q + \alpha q^2 + \ldots$ generuje wraz z formami sprzężonymi przestrzeń wymiaru 21. Liczba algebraiczna α jest pierwiastkiem wielomianu

$$\begin{aligned} -44 + 1058x - 4111x^2 - 24699x^3 + 12831x^4 + 93934x^5 - 14353x^6 - 152221x^7 \\ +8292x^8 + 132085x^9 - 2749x^{10} - 67876x^{11} + 519x^{12} + 21617x^{13} - 51x^{14} \\ -4305x^{15} + 2x^{16} + 521x^{17} - 35x^{19} + x^{21}. \end{aligned}$$

Ciało K_f jest równe $\mathbb{Q}(\alpha)$. Ideały wchodzące w rozkład $5\mathcal{O}_f$ są nierozgałęzione, w szczególności ideał maksymalny $\lambda = (5, \beta/8)$, dla którego

$$\begin{aligned} \beta = 32 + 48\alpha + 82\alpha^2 + 75\alpha^3 + 66\alpha^4 + 70\alpha^5 + 39\alpha^6 + 62\alpha^7 + 50\alpha^8 + 37\alpha^9 \\ +22\alpha^{10} + 56\alpha^{11} + 17\alpha^{12} + 2\alpha^{13} + 16\alpha^{14} + 26\alpha^{15} + 3\alpha^{16} + 7\alpha^{17} + \alpha^{18} + \alpha^{19}. \end{aligned}$$

Można sprawdzić, że $\mathcal{O}_f/\lambda \cong \mathbb{F}_{25}$, jednak dla odwzorowania redukcji $\pi : \mathcal{O}_f \to \mathcal{O}_f/\lambda$ obraz $\pi(\mathbb{Z}[\{a_n(f)\}_{n\in\mathbb{N}}])$ jest podciałem $\mathbb{F}_5 \subsetneq \mathcal{O}_f/\lambda$. Algorytm 2 pozwala sprawdzić, że forma f przystaje do $[401]^+E_2$ modulo λ i teoretyczne ograniczenie górne wynosi 2 w tym przypadku, więc $r < m$ oraz $e = 1$.

W dalszej części podrozdziału omawiamy kilka wniosków z pracy [Nas14], podsumowując przeprowadzone obliczenia dla poziomów N będących liczbami pierwszymi i wagi $k = 2$.

Wniosek 3.7.1 ([Nas14, Observation 1.3])**.** *Niech k będzie liczbą parzystą z przedziału $2 \leq k \leq 22$. Niech p będzie liczbą pierwszą mniejszą niż $p_{max}(k)$ określone poniżej.*

k	2	4	6	8	10	12	14	16	18	20	22
$p_{max}(k)$	1789	397	229	193	109	113	97	71	67	67	59

Niech ℓ będzie liczbą pierwszą większą od 2 spełniającą nierówność

$$v_\ell(a_0([p]^+E_2)) > 0.$$

Niech $f \in \mathcal{S}_2(\Gamma_0(p))^{new}$ będzie nową formą własną, a $\lambda \subset \mathcal{O}_f$ ideałem maksymalnym nad ℓ, rozgałęzionym w ℓ, tzn. $ord_\lambda(\ell) = e > 1$. Jeśli zachodzą kongruencje

$$a_n(f) \equiv a_n([p]^+E_2) \ (mod\ \lambda^r)$$

dla wszystkich $n \geq 0$ i dla pewnego $r > 0$, to $r \leq e$.

Uwaga 3.7.2. W przebadanym zakresie podanym we wniosku sprawdzono wszystkie możliwe kongruencje pomiędzy formami f i szeregami $[p]^+E_2$. Wniosek ten nie jest prawdziwy dla $\ell = 2$. Na przykład, gdy $p = 257$ znajdujemy formę f, która przystaje do $[p]^+E_2$ modulo λ^5, gdzie λ zawiera 2 i $ord_\lambda(2) = 2$. Ponadto, gdy poziom N jest iloczynem większej liczby czynników pierwszych, to istnieją przypadki, gdy wniosek również nie zachodzi.

Wniosek 3.7.3 ([Nas14, Proposition 1.6]). *Istnieje liczba pierwsza $p > 2$ i dwie nowe formy własne $f_1, f_2 \in \mathcal{S}_2(\Gamma_0(p))$, które nie należą do tej samej orbity działania grupy $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ i spełnione są kongruencje*

$$a_n(f_1) \equiv a_n([p]^+E_2) \ (mod\ \lambda_1^{r_1})$$

oraz

$$a_n(f_1) \equiv a_n([p]^+E_2) \ (mod\ \lambda_2^{r_2})$$

dla wszystkich $n \geq 0$ oraz dla pewnych $r_1, r_2 > 0$. Ideały maksymalne $\lambda_1 \subset \mathcal{O}_{f_1}$ oraz $\lambda_2 \subset \mathcal{O}_{f_2}$ mają tę samą charakterystykę ciała reszt.

Dowód. Kładziemy $p = 353$. Twierdzenie jest spełnione dla ideałów λ_1, λ_2 o charakterystyce ciała reszt równej 2. W tym przypadku istnieją dokładnie 3 formy, które nie należą do jednej orbity działania grupy Galois, które spełniają tezę.

Kładziemy $p = 487$. Twierdzenie jest spełnione dla ideałów λ_1, λ_2 o charakterystyce ciała reszt równej 3. □

Uwaga 3.7.4. Barry Mazur sformułował w [Maz77, II.19] hipotezę, że powyższy wniosek zachodzi dla nieskończenie wielu poziomów p i ideałów o charakterystyce ciała reszt równej 2.

Wniosek 3.7.5 ([Nas14, §5.7]). *Istnieje taka liczba pierwsza p oraz nowa forma własna $f \in \mathcal{S}_2(\Gamma_0(p))$, że dla pewnego ideału maksymalnego $\lambda \in \mathcal{O}_f$ i pewnego $r > 0$ zachodzi*

$$a_n(f_1) \equiv a_n([p]^+E_2) \ (mod\ \lambda^r)$$

dla wszystkich $n \geq 0$ i $\mathbb{Z}[\{a_n(f)\}_{n\in\mathbb{N}}] \subsetneq \mathcal{O}_f$.

Dowód. Niech $p = 401$. W jednym z wcześniejszych paragrafów omówiliśmy przykład kongruencji pomiędzy nową formą własną $f \in \mathcal{S}_2(\Gamma_0(p))$, dla której ciało $K_f = \mathbb{Q}(\{a_n(f)\}_{n\in\mathbb{N}})$ ma stopień 21 nad $\mathbb{Q}$ oraz formą Eisensteina $[p]^+E_2$, która przystaje modulo λ do f, dla ideału maksymalnego $\lambda \in \mathcal{O}_f$ o charakterystyce ciała reszt równej 5. Zachodzi równość $K_f = \mathbb{Q}(a_2(f))$. Ponadto można sprawdzić, że $\mathcal{O} := \mathbb{Z}[\{a_n(f)\}_{n\in\mathbb{N}}] = \mathbb{Z}[a_2(f), a_3(f), a_5(f)]$. Pierścień liczb algebraicznych całkowitych $\mathcal{O}_f$ ciała K_f spełnia warunek $[\mathcal{O}_f : \mathcal{O}] = 5$. Zatem pierścień $\mathcal{O}$ jest 5-maksymalnym ordynkiem pierścienia $\mathbb{Z}[a_2(f)]$, patrz [Nas14, §4.1]. □

3.7.2 Kongruencje dla N wolnych od kwadratów

Dla uproszczenia formy ekspozycji wyników zastosujemy w tym paragrafie następującą konwencję. Będziemy mówili, że *zachodzi kongruencja spełniająca warunek $\mathcal{W}$* jeśli dla pewnego k oraz pewnego N wolnego od kwadratów istnieje nowa forma własna $f \in \mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ oraz forma własna $E \in \mathcal{E}_k(\Gamma_0(N))$ spełniające kongruencje

$$a_n(f) \equiv a_n(E) \ (\text{mod}\ \lambda^r) \tag{3.21}$$

dla pewnego ideału maksymalnego $\lambda \subset \mathcal{O}_f$, $r > 0$ i dla dowolnego $n \geq 0$. Wartości $r, d, e, f, N^-, N^+, \ell$ oraz m stowarzyszone z tą kongruencją są określone przez warunek $\mathcal{W}$. Stosownie do potrzeby ograniczeniu ulegać mogą również wartości k oraz N.

Wniosek 3.7.6. *Niech N będzie dowolną liczbą wolną od kwadratów ograniczoną w zależności od wagi jak podano w Tabeli 3.4. Wówczas w podanych w Tabeli 3.9 zakresach istnieje następująca liczba kongruencji postaci (3.21) w zależności od wartości r oraz k.*

k	$r \geq 0$	$r > 0$	$m \cdot e = r > 0$	$m \cdot e > r > 0$
2	277447	62937	38805	24132
4	64232	13922	9208	4714
6	17300	3629	2475	1154
8	10755	2149	1517	632
10	9248	1483	1106	377
12	5738	1055	787	268
14	5276	1020	756	264
16	6010	1113	817	296
18	6995	1235	922	313
20	10735	1914	1428	486
22	8853	1425	1025	400
24	10359	1555	1153	402

Tabela 3.9: Liczba kongruencji typu (3.21) dla ustalonych wag k.

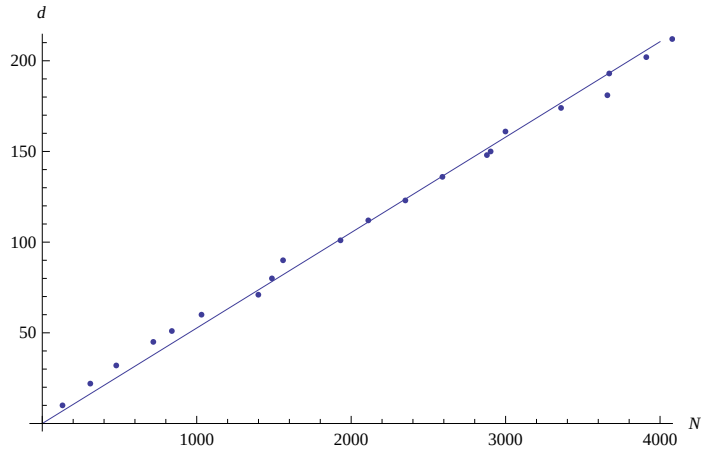
Uwaga 3.7.7. Kolumna oznaczona przez $r \geq 0$ podaje liczbę znalezionych par f, λ wytypowanych przez Algorytm 2 z podrozdziału 3.5.2.

Wniosek 3.7.8. *Niech N i k będą jak podano w Tabeli 3.4. Istnieje 96 kongruencji spełniających $e > 1$, $m > 1$ i $\ell > 3$. Poza przypadkami opisanymi w Tabeli 3.10 zachodzi również zawsze $r \leq e$.*

	N	N^-	N^+	k	ℓ	m	forma	λ	r	e	f	d
1	2495	499	5	2	5	3	f_1	λ_1	3	2	1	55
2	3998	1999	2	2	5	3	f_1	λ_1	3	2	1	44

Tabela 3.10: Kongruencje spełniające $e > 1$, $m > 1$, $\ell > 3$ i $r > e$.

Uwaga 3.7.9. Część wskazanych przykładów można odnaleźć w Tabeli 3.7. Powyższy wniosek znacząco rozszerza podobne obliczenia przedstawione dla poziomów N, które są liczbami pierwszymi z pracy [Nas14], patrz Wniosek 3.7.1. Dla poziomów N, które są liczbami pierwszymi oraz $k = 2$ autor sprawdził również, że własność kongruencji $r \leq e$ zachodzi dla szeregów Eisensteina $[N]^+E_2$ w zakresie dla $N \leq 13009$. Czy taka własność zachodzi dla nieskończenie wielu kongruencji spełniających $\ell > 3$ jest (w momencie pisania tej rozprawy) pytaniem, na które nie znamy odpowiedzi.



Rysunek 3.2: Wzrost stopnia d jako funkcja poziomu N dla danych z Tabeli 3.8.

Wniosek 3.7.10. *Niech $k = 2$. Dla $N \leq 4559$ wolnego od kwadratów i dla dowolnego $d \leq 222$ istnieją kongruencje postaci (3.21) o ile $d \notin D$, gdzie*

$$D = \{169, 175, 178, 192, 197, 204, 207, 208, 211, \\ 214, 215, 216, 217, 218, 219, 220, 221\}.$$

Uwaga 3.7.11. W pracy [DJUK11] autorzy badają istnienie nowych form własnych f dla poziomów N wolnych od kwadratów, które mają duży stopień ciała współczynników K_f. Obliczenia opisane we Wniosku 3.7.10 oraz w Tabeli 3.8 pokazują, że dla wielu poziomów możemy znaleźć nowe formy własne, które dodatkowo przystają do szeregów Eisensteina i mają jednocześnie duży stopień. Ponadto, jak widać z Rysunku 3.2, wzrost najmniejszego poziomu N wraz z wyborem stopnia d opisany w Tabeli 3.8 ma charakter liniowy.

Wniosek 3.7.12. *Dla $k = 2$ i dowolnego $11 \leq N \leq 4559$ wolnego od kwadratów istnieją kongruencje pomiędzy nowymi formami własnymi i szeregami Eisensteina, za wyjątkiem poziomów $N = 13, 22$, dla których przestrzeń $\mathcal{S}_2(\Gamma_0(N))^{new}$ jest zerowa.*

Wniosek 3.7.13. *Jeśli $k = 2$ i $N^- > 1$, to istnieje 54077 kongruencji dla poziomów $N \leq 4559$ oraz 8860 kongruencji dla $N^- = 1$ i poziomów $N \leq 4559$.*

Uwaga 3.7.14. Założenia Twierdzeń 3.3.4 i 3.3.5 są spełnione dla niektórych przypadków wymienionych w poprzednim wniosku. Co więcej, wskazane twierdzenia nie zakładają istnienia kongruencji dla współczynników a_p dla $p \mid N$. W znalezionych przykładach kongruencja zachodzi również dla tych współczynników. Ponadto wiele ze znalezionych przykładów nie spełnia założeń Twierdzeń 3.3.4 i 3.3.5, co sugeruje, że założenia w podanych twierdzeniach można znacząco osłabić.

Wniosek 3.7.15. *Niech N będzie liczbą wolną od kwadratów ograniczoną w zależności od wagi k jak podano w Tabeli 3.4. Wówczas w podanych zakresach istnieje*

następująca liczba kongruencji (l.k.) spełniających warunek $f > 2$. Wartości podano w Tabeli 3.11.

k	2	4	6	8	10	12	14	16	18	20	22	24
l.k.	993	177	20	4	0	0	0	2	4	2	0	0

Tabela 3.11: Waga k i liczba kongruencji spełniających $f > 2$.

Wniosek 3.7.16. *Dla $k = 2$ i $N \leq 4559$ istnieją kongruencje takie, że $\ell \leq 2273$ i ℓ nie należy do zbioru*

$$\{353, 389, 457, 463, 523, 541, 569, 571, 587, 599, 613, 617, 631, 643, 647, 677, 701, 733, 757, 769, 773, 787, 797, 821, 823, 827, 839, 857, 859, 863, 881, 887, 907, 929, 941, 947, 971, 977, 983, 991, 1021, 1051, 1061, 1091, 1097, 1109, 1117, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1423, 1427, 1429, 1433, 1447, 1453, 1459, 1471, 1483, 1487, 1489, 1493, 1523, 1531, 1543, 1549, 1553, 1567, 1571, 1579, 1597, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1907, 1913, 1933, 1949, 1951, 1979, 1987, 1993, 1997, 1999, 2011, 2017, 2027, 2029, 2053, 2081, 2083, 2087, 2089, 2099, 2111, 2113, 2131, 2137, 2143, 2153, 2161, 2179, 2203, 2207, 2213, 2221, 2237, 2239, 2243, 2251, 2267, 2269\}.$$

Wniosek 3.7.17. *Dla $N \leq 4559$ wolnych od kwadratów i $k = 2$ istnieje 30 kongruencji spełniających warunki $e = 17$ i $\ell = 2$. Ponadto nie istnieje w tym zakresie żadna kongruencja, dla której $e > 17$.*

Wniosek 3.7.18. *Niech N będzie liczbą wolną od kwadratów ograniczoną w zależności od wagi k jak podano w Tabeli 3.4. Wówczas w podanych zakresach istnieje następująca liczba kongruencji (l.k.) spełniających warunek $\ell \mid N$. Wartości podano w Tabeli 3.12.*

k	2	4	6	8	10	12	14	16	18	20	22	24
l.k.	27771	4839	1366	1070	609	583	605	708	726	1323	990	1033

Tabela 3.12: Waga k i liczba kongruencji spełniających $\ell \mid N$.

Bibliografia

[AL70] Arthur Atkin, Joseph Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[ASD73] Michael Artin, Peter Swinnerton-Dyer. The Shafarevich-Tate conjecture for pencils of elliptic curves on $K3$ surfaces. *Invent. Math.*, 20:249–266, 1973.

[BCP97] Wieb Bosma, John Cannon, Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BM77] Enrico Bombieri, David Mumford. Enriques' classification of surfaces in char. p. ii. *Complex analysis and algebraic geometry*, strony 23–42. Iwanami Shoten, Tokyo, 1977.

[CD89] François Cossec, Igor Dolgachev. *Enriques surfaces. I*, wolumen 76 serii *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1989.

[CKR10] Imin Chen, Ian Kiming, Jonas Rasmussen. On congruences mod p^m between eigenforms and their attached Galois representations. *J. Number Theory*, 130(3):608–619, 2010.

[Cre97] John Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, wydanie second, 1997.

[Cre08] John Cremona. Computing in component groups of elliptic curves. *Algorithmic number theory*, wolumen 5011 serii *Lecture Notes in Comput. Sci.*, strony 118–124. Springer, Berlin, 2008.

[Del69] Pierre Deligne. Formes modulaires et représentations l-adiques. *Séminaire N. Bourbaki, 1968-1969*, 355:139–172, 1969.

[Del74] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[Del77] Pierre Deligne. *Cohomologie étale*. Lecture Notes in Mathematics, Vol. 569. Springer-Verlag, Berlin, 1977.

[DJUK11] Luis Dieulefait, Jorge Jimenez-Urroz, Ribet Kenneth. Modular forms with large coefficient fields via congruences. *ArXiv e-prints*, 2011. arXiv:1111.5592v1.

[DS05] Fred Diamond, Jerry Shurman. *A first course in modular forms*, wolumen 228 serii *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[FD14] Daniel Fretwell, Neil Dummigan. Ramanujan-style congruences of local origin. strony 1–11, 2014. http://www.neil-dummigan.staff.shef.ac.uk/papers.html.

[GMN12] Jordi Guardia, Jesus Montes, Enric Nart. Higher Newton polygons and integral bases. *ArXiv e-prints*, 2012. arXiv:0902.3428v3.

[GP13] Wojciech Gajda, Sebastian Petersen. Independence of ℓ-adic Galois representations over function fields. *Compos. Math.*, 149(7):1091–1107, 2013.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Hat02] Allen Hatcher. *Algebraic topology*. Cambridge University Press, Cambridge, 2002.

[Huy05] Daniel Huybrechts. *Complex geometry*. Universitext. Springer-Verlag, Berlin, 2005.

[INK10] F. A. Izadi, K. Nabardi, F. Khoshnam. On a Family Of Elliptic Curves With Positive Rank arising from Pythagorean Triples. *ArXiv e-prints*, 2010. arXiv:1012.5837v4.

[Kat] Nicholas M. Katz. Review of l-adic cohomology. *Motives (Seattle, WA, 1991)*, wolumen 55 serii *Proc. Sympos. Pure Math.*, strony 21–30.

[Kat81] Nicholas Katz. Galois properties of torsion points on abelian varieties. *Invent. Math.*, 62(3):481–502, 1981.

[Kle68] Steven Kleiman. Algebraic cycles and the Weil conjectures. *Dix esposés sur la cohomologie des schémas*, strony 359–386. North-Holland, Amsterdam, 1968.

[Klo07] Remke Kloosterman. Elliptic $K3$ surfaces with geometric Mordell-Weil rank 15. *Canad. Math. Bull.*, 50(2):215–226, 2007.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, wolumen 6 serii *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002.

[Maz77] Barry Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186, 1977.

[Mil75] James Milne. On a conjecture of Artin and Tate. *Ann. of Math. (2)*, 102(3):517–533, 1975.

[Mil80] James Milne. *Étale cohomology*, wolumen 33 serii *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[Mil86] James Milne. Values of zeta functions of varieties over finite fields. *Amer. J. Math.*, 108(2):297–360, 1986.

[Miy73] Isao Miyawaki. Elliptic curves of prime power conductor with q-rational points of finite order. *Osaka J. Math.*, 10:309–323, 1973.

[Mum69] David Mumford. Enriques' classification of surfaces in char p.I. *Global Analysis (Papers in Honor of K. Kodaira)*, strony 325–339. Univ. Tokyo Press, Tokyo, 1969.

[Nas10] Bartosz Naskręcki. Infinite family of elliptic curves of rank at least 4. *Involve*, 3(3):297–316, 2010.

[Nas13] Bartosz Naskręcki. Mordell-Weil ranks of families of elliptic curves associated to Pythagorean triples. *Acta Arithmetica*, 160(2):159–183, 2013.

[Nas14] Bartosz Naskręcki. On higher congruences between cusp forms and Eisenstein series. Gebhard Böckle, Gabor Wiese, redaktorzy, *Computations with Modular Forms*, wolumen 6 serii *Contributions in Mathematical and Computational Sciences*, strony 257–277. Springer, 2014.

[Ogu90] Keiji Oguiso. An elementary proof of the topological Euler characteristic formula for an elliptic surface. *Comment. Math. Univ. St. Paul.*, 39(1):81–86, 1990.

[Ras] Jonas Rasmussen. Higher congruences between modular forms. *University of Copenhagen*. http://www.math.ku.dk/ jonas/Thesis.pdf.

[Sad14] Mohammad Sadek. On elliptic curves whose conductor is a product of two prime powers. *Math. Comp.*, 83(285):447–460, 2014.

[SD73] Peter Swinnerton-Dyer. On l-adic representations and congruences for coefficients of modular forms. *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, strony 1–55. Lecture Notes in Math., Vol. 350. Springer, Berlin, 1973.

[Ser73] Jean-Pierre Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[Set75] Bennett Setzer. Elliptic curves of prime conductor. *J. London Math. Soc. (2)*, 10:367–378, 1975.

[Shi71] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. Kanô Memorial Lectures, No. 1.

[Shi90] Tetsuji Shioda. On the Mordell-Weil lattices. *Comment. Math. Univ. St. Paul.*, 39(2):211–240, 1990.

[Sil86] Joseph Silverman. *The arithmetic of elliptic curves*, wolumen 106 serii *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Sil88] Joseph Silverman. Computing heights on elliptic curves. *Math. Comp.*, 51(183):339–358, 1988.

[Sil94] Joseph Silverman. *Advanced topics in the arithmetic of elliptic curves*, wolumen 151 serii *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[SS10] Tetsuji Shioda, Matthias Schütt. Elliptic surfaces. *ArXiv e-prints*, 2010. arXiv:0907.0298v3.

[Ste07] William Stein. *Modular forms, a computational approach*, wolumen 79 serii *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007.

[Tat65] John Tate. Algebraic cycles and poles of zeta functions. *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, strony 93–110. Harper & Row, New York, 1965.

[Tat66] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. *Séminaire N. Bourbaki, 1964-1966*, 306:415–440, 1966.

[Tat75] John Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, wolumen 476, strony 33–52. Springer, Berlin, 1975. Lecture Notes in Math.

[TiVW10] Xavier Taixés i Ventosa, Gabor Wiese. Computing congruences of modular forms and Galois representations modulo prime powers. *Arithmetic, geometry, cryptography and coding theory 2009*, wolumen 521 serii *Contemp. Math.*, strony 145–166. Amer. Math. Soc., 2010.

[vL07] Ronald van Luijk. An elliptic $K3$ surface associated to Heron triangles. *J. Number Theory*, 123(1):92–119, 2007.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[Yoo13a] Hwajong Yoo. The index of an Eisenstein ideal and multiplicity one. *ArXiv e-prints*, 2013. arXiv:1311.5275v1.

[Yoo13b] Hwajong Yoo. Modularity of residually reducible Galois representations and Eisenstein ideals. 2013. Ph.D. thesis.