KONSTRUOWANIE KRZYWYCH GENUSU 2 Z DANYM STOPNIEM ZANURZENIOWYM

Robert Dryło

Szkoła Główna Handlowa, Aleja Niepodległości 162, 02-554 Warszawa
Instytut Matematyczny PAN, ul. Śniadeckich 8, 00-950 Warszawa,
e-mail: rdrylo@sgh.waw.pl

Streszczenie. W kryptografii opartej na iloczynach dwuliniowych stosuje się specjalne krzywe, dla których iloczyny dwuliniowe Weila i Tate można efektywnie obliczyć. Takie krzywe, zwykle nazywane pairing-friendly, mają mały stopień zanurzeniowy i wymagają specjalnej konstrukcji. W praktyce stosuje się głównie krzywe eliptyczne i hipereliptyczne genusu 2. Konstrukcje takich krzywych opierają się na metodzie mnożeń zespolonych (CM metodzie) i stąd ograniczają się do krzywych, których pierścień endomorfizmów jakobianu jest generowany przez odpowiednio małe liczby. Aby skonstruować krzywą najpierw wyznacza się parametry jej jakobianu, które zwykle są dane przez liczby Weila dla krzywych genusu 2, a następnie stosuje się CM metodę, aby znaleźć równanie krzywej. Freeman, Scott i Teske zebrali i opisali w ujednolicony sposób metody konstruowania krzywych eliptycznych z danym stopniem zanurzeniowym. Istnieje kilka różnych podejść do konstruowania krzywych genusu 2, z których pierwsze podali Freeman, Stevenhagen i Streng, Kawazoe-Takahashi i Freeman-Satoh. W tym opracowaniu opisujemy podejście oparte na idei autora, w którym wykorzystujemy opowiednie wielomiany wielu zmiennych, aby jako ich wartości otrzymywać liczby Weila odpowiadające jakobianom krzywych genusu 2 z danym stopniem zanurzeniowym. Takie podejście pozwala konstruować zarówno krzywe genusu 2 o jakobianie absolutnie prostym oraz prostym, ale nie absolutnie prostym. Podajemy bezpośrednie wzory, które wyznaczają rodziny parametryczne krzywych genusu 2 z danym stopniem zanurzeniowym.

Słowa kluczowe: kryptografia oparta na iloczynach dwuliniowych, krzywe z danym stopniem zanurzeniowym, iloczyny dwuliniowe Weila i Tate, CM metoda, liczby Weila.

1. Wstęp

Zastosowanie iloczynów dwuliniowych pozwoliło otrzymać nowe protokoły kryptograficzne, m.in. szyfrowanie oparte na tożsamości [4], krótkie podpisy cyfrowe [5], lub ustalanie wspólnego tajnego klucza w jednej rundzie między trzema osobami [25]. W praktyce stosuje się iloczyny dwuliniowe Weila lub Tate głównie na krzywych eliptycznych lub w jakobianach krzywych hipereliptycznych genusu 2 (na ogół unika się krzywych wyższych genusów, ponieważ w ich przypadku istnieją efektywniejsze metody rozwiązywania problemu logarytmu dyskretnego). Dla tych zastosowań wymaga się specjalnych krzywych, zwykle nazywanych pairing-friendly, dla których iloczyny dwuliniowe można efektywnie obliczyć. Znalezienie odpowiednich krzywych przez losowy wybór jest praktycznie niemożliwe, dlatego takie krzywe muszą być specjalnie konstruowane.

Podstawowym parametrem wpływającym na bezpieczeństwo i efektywność kryptosystemów opartych na iloczynach dwuliniowych jest stopień zanurzeniowy k, który jest stopniem rozszerzenia ciała zawierającego wartości iloczynu dwuliniowego na punktach r-torsyjnych. Stopień zanurzeniowy k musi być odpowiednio mały, aby obliczenie iloczynu było efektywne. Z drugiej strony k musi być tak dobrane, aby zapewnić odpowiedni poziom bezpieczeństwa, ponieważ iloczyny dwuliniowe przenoszą problem logarytmu dyskretnego z jakobianu do ciała, gdzie może być atakowany przez podwykładnicze metody.

Na początku dla tych zastosowań proponowano krzywe supersingularne, które zawsze mają ograniczone stopnie zanurzeniowe (odpowiednio $k \leq 6, 12$ dla krzywych eliptycznych i krzywych genusu 2 [29, 21]). Dla wyższych poziomów bezpieczeństwa stosuje się krzywe zwykłe, które wymagają specjalnych konstrukcji. Konstruowanie takich krzywych przebiega w dwóch etapach. Najpierw dla danego stopnia zanurzeniowego k wyznacza się parametru jakobianu krzywej (w szczególności ciało $\mathbb{F}_q$ and którym zdefiniowana jest krzywa oraz liczbę pierwszą r, która jest rzędem podgrupy jakobianu ze stopniem zanurzeniowym k). Następnie stosuje się metodę mnożeń zespolonych (CM metodę), aby znaleźć równanie krzywej, której jakobian ma takie parametry. W praktyce CM metoda pozwala skonstruować taką krzywą jeśli pierścień endomorfizmów jakobianu jest ordynkiem w CM ciele generowanym przez odpowiednio małe liczby. Dlatego w praktyce z góry ustala się CM ciało i tak dobiera się parametry jakobianu, aby jego pierścień endomorfizmów był ordynkiem w tym CM ciele.

Dla zastosowań chcielibyśmy orzymać krzywe, dla których rząd r podgrupy ze stopniem zanurzeniowym k jest jak najbliższy rzędowi jakobianu, ponieważ wówczas krzywa jest zdefiniowana nad mniejszym ciałem i arytmetyka jest efektywniejsza. Różnicę między wielkościami tych rzędów wyraża parametr ρ. Dla krzywej $C/\mathbb{F}_q$ genusu g rząd jakobianu $\#\mathrm{Jac}(C)(\mathbb{F}_q)$ jest tej samej wielkości co q^g. Zatem parametr

$$\rho = \frac{g \log q}{\log r}$$

mówi nam ile razy wielkość rzędu jakobianu jest więsza od wielkości r. Przypadek optymalny $\rho \approx 1$ jest w praktyce bardzo trudny do osiągnięcia i głównym celem rozwijania metod konstruowania krzywych jest otrzymanie jak najmniejszego ρ. Znane są przykłady krzywych supersingularnych z parametrem $\rho \approx 1$. Aby zminimalizować ρ dla krzywych zwykłych stosuje się rodziny parametryczne (tzn. parametry jakobianu otrzymuje się jako wartości pewnych wielomianów na liczbach całkowitych). Dla krzywych eliptycznych konstrukcje rodzin parametrycznych z $\rho = 1$ są znane

dla $k = 3, 4, 6, 10, 12$ ([34, 1, 15]). Dla wielu innych stopni zanurzeniowych istnieją rodziny parametryczne krzywych eliptycznych z $1 < \rho < 2$ bliskim 1. Freeman, Scott i Teske [19] zebrali metody konstruowania krzywych eliptycznych z danym stopniem zanurzeniowym, podali jednolity opis i klasyfikację takich metod oraz podali rodziny o najmniejszym parametrze ρ dla $k \leq 50$.

Dla krzywych genusu 2 istnieje większa różnorodność metod. Ogólnie metody można podzielić na takie, które konstruują krzywe genusu 2 o jakobianie absolutnie prostym lub prostym, ale nie absolutnie prostym (tzn., jakobian rozpada się na produkt krzywych eliptycznych nad pewnym rozszerzeniem ciała bazowego krzywej. Stosowanie krzywych genusu 2, których jakobian rozpada się już nad ciałem bazowym nie daje korzyści i może zostać sprowadzone do krzywych eliptycznych). Większość metod dla krzywych eliptycznych można uogólnić na krzywe genusu 2. Freeman [16] i Freeman, Stevenhagen i Streng [20] podali pierwsze metody konstruowania takich krzywych (metoda [20] została podana dla dowolnych rozmaitości abelowych). Obie metody generycznie dają krzywe genusu 2 o jakobianie absolutnie prostym z parametrem $\rho \approx 8$. Freeman [17] uogólnił metodę [20] na rodziny parametryczne, która w przypadku krzywych genusu 2 pozwala konstruować rodziny z parametrem $\rho < 8$ (generycznie bliskim 8). Kawazoe i Takahashi [27] podali metodę konstruowania krzywych postaci $y^2 = x^5 + ax$, których jakobian nie jest absolutnie prosty i ma parametr $\rho \approx 4$ lub $\rho < 4$ dla rodzin parametrycznych. Freeman i Satoh [18] podali ogólną metodę opartą na technice restrykcji Weila konstruowania krzywych genusu 2 o jakobianie prostym, ale nie absolutnie prostym, również z parametrem $\rho \approx 4$ lub $\rho < 4$ dla rodzin parametrycznych.

Celem tego opracowania jest rozwinięcie podejścia do konstruowania krzywych genusu 2 przedstawionego w pracach autora [10, 11]. Podobnie jak w większości metod, aby skonstruować krzywą najpierw otrzymujemy liczbę Weila, która wyznacza parametry jakobianu, a następnie stosujemy CM metodę, aby skonstruować odpowiednią krzywą. Liczby Weila będziemy otrzymywać jako wartości pewnych wielomianów na liczbach całkowitych, których konstrukcje opisujemy w Rozdziale 3. Takie podejście pozwala jednocześnie opisać przypadek konstruowania krzywych o jakobianie prostym i absolutnie prostym. Przypadek generowania liczb Weila dla dowolnych rozmaitości abelowych nie jest istotnie trudniejszy niż dla powierzchni, dlatego tam gdzie jest to możliwe opisujemy metody w ogólnej sytuacji. W Rozdziale 4 podajemy streszczenie CM metody dla krzywych genusu 2. W Rozdziale 5 podajemy uogólnienie algorytmu Cocksa-Pincha dla krzywych eliptycznych na rozmaitości abelowe. Rozdział 6 zawiera uogólnienie algorytmu Brezing-Weng [6] konstruowania rodzin krzywych

eliptycznych z danym stopniem zanurzeniowym na rozmaitości abelowe zwykłe; podajemy bezpośrednie wzory, które wyznaczają rodziny parametryczne takich rozmaitości.

2. Podstawowe fakty z teorii rozmaitości abelowych

W tym rozdziale przypominamy pojęcia i twierdzenia z teorii rozmaitości abelowych, na których opierają się metody konstruowania krzywych. Ogólną teorię rozmaitości abelowych można znaleźć w książkach Mumforda [35] i [33]. Streszczenie teorii rozmaitości abelowych nad ciałami skończonymi znajduje się w opracowaniu Oorta [36].

Niech $\mathbb{F}$ będzie dowolnym ciałem charakterystyki $p \geq 0$ z domknięciem algebraicznym $\overline{\mathbb{F}}$. Rozmaitością abelową nad $\mathbb{F}$ nazywamy rozmaitość algebraiczną zupełną $A/\mathbb{F}$, która jest grupą algebraiczną. Rozmaitości abelowe są grupami abelowymi i zanurzają się w przestrzenie rzutowe.

Niech $A/\mathbb{F}$ będzie rozmaitością abelową wymiaru g. Dla dowolnego rozszerzenia ciał $\mathbb{F}'/\mathbb{F}$ zbiór punktów $\mathbb{F}'$-wymiernych $A(\mathbb{F}')$ jest grupą abelową. Niech $A[r] = \{P \in A(\overline{\mathbb{F}}) | rP = 0\}$ będzie podgrupą punktów r-torsyjnych na A, $r \in \mathbb{Z} \setminus 0$. Jeśli $\gcd(r, p) = 1$ lub $p = 0$, to $A[r] \cong \mathbb{Z}_r^{2g}$. Jeśli $p > 0$, to $A[p] \cong \mathbb{Z}_p^{\nu}$, gdzie $0 \leq \nu \leq g$. Rozmaitość A nazywamy *zwykłą* (odp. *supersingularną*) jeśli $\nu = g$ (odp. $\nu = 0$). Jeśli $\mathbb{F} = \mathbb{F}_q$ jest ciałem skończonym, to A jest zwykła dokładnie wtedy, gdy współczynnik a_g wielomianu charakterystycznego $f_q(x)$ (Twierdzenie 2.1 poniżej) jest względnie pierwszy z p.

Krzywe eliptyczne (krzywe genusu 1) są dokładnie rozmaitościami abelowymi wymiaru 1. Rozmaitości abelowe wymiaru 2 nazywamy powierzchniami abelowymi. Jeśli $C/\mathbb{F}$ jest krzywą genusu g zawierającą punkt $\mathbb{F}$-wymierny, to jej jakobian $\mathrm{Jac}(C)$ jest rozmaitością abelową nad $\mathbb{F}$ wymiaru g. Punkty $\mathbb{F}$-wymierne $\mathrm{Jac}(C)(\mathbb{F})$ można utożsamiać z klasami dywizorów w grupie Picarda $\mathrm{Pic}^0_{\mathbb{F}}(C) = \mathrm{Div}^0_{\mathbb{F}}(C)/\mathrm{Prin}_{\mathbb{F}}(C)$ dywizorów stopnia 0 nad $\mathbb{F}$ modulo dywizory główne nad $\mathbb{F}$.

Każde odwzorowanie wymierne $f : A \to B$ rozmaitości abelowych jest regularne. Jeśli $f(0) = 0$, to f jest homomorfizmem grup. Mówimy, że f jest *izogenią*, jeśli $\dim A = \dim B$, $f(0) = 0$ i $\ker f$ jest skończone. Istnienie izogenii między rozmaitościami abelowymi jest relacją równoważności, oznaczaną $A \sim B$.

Mówimy, że rozmaitość A jest *prosta* nad $\mathbb{F}$, jeśli A nie jest izogeniczna nad $\mathbb{F}$ z produktem niezerowych rozmaitości abelowych nad $\mathbb{F}$. A jest prosta dokładnie wtedy, gdy nie zawiera właściwych niezerowych podrozmaitości abelowych. Każda rozmaitość A jest izogeniczna nad $\mathbb{F}$ z produktem $A_1^{n_1} \times \cdots \times A_s^{n_s}$ rozmaitości abelowych prostych $A_i/\mathbb{F}$, które są

wyznaczone jednoznacznie z dokładnością do izogenii. Mówimy, że A jest *absolutnie prosta* jeśli A jest prosta nad $\overline{\mathbb{F}}$. Jeśli A nie jest prosta nad $\mathbb{F}$, to mówimy że A rozpada się nad $\mathbb{F}$. Rozmaitość może być prosta nad $\mathbb{F}$ i rozpadać się nad pewnym rozszerzeniem.

Niech $A \subset \mathbb{P}^n$ będzie rozmaitością abelową wymiaru g nad ciałem skończonym $\mathbb{F}_q$. Podstawową rolę w teorii rozmaitości abelowych nad ciałami skończonymi pełni *endomorfizm Frobeniusa* nad $\mathbb{F}_q$, $\pi_q : A \to A$, $\pi_q(x_0, \ldots, x_n) = (x_0^q, \ldots, x_n^q)$.

Twierdzenie 2.1. (Weil) *Endomorfizm Frobeniusa π_q spełnia równanie charakterystyczne o współczynnikach całkowitych postaci*

$$f_q(x) = x^{2g} + a_1 x^{2g-1} + \ldots + a_g x^g + q a_{g-1} x^{g-1} + \cdots + q^{g-1} a_1 x + q^g = 0.$$

(1) *Pierwiastki zespolone $\pi \in \mathbb{C}$ wielomianu $f_q(x)$ spełniają $\pi\bar{\pi} = q$, gdzie $\bar{\cdot}$ jest sprzężeniem zespolonym.*
(2) *Rząd $\#A(\mathbb{F}_q) = f_q(1)$.*

Z powyższego twierdzenia wynika, że rząd $\#A(\mathbb{F}_q)$ jest wielkości q^g. (Jest to główna motywacja dla stosowania krzywych wyższych genusów. Aby otrzymać grupę, której rząd jest wielkości n-bitów możemy użyć krzywej eliptycznej nad ciałem n-bitowym, lub jakobianu krzywej genusu 2 nad ciałem $n/2$-bitowym.)

Kluczową rolę dla konstruowania rozmaitości odgrywa pierścień endomorfizmów i liczby Weila. Pierścień endomorfizmów nad $\mathbb{F}_q$ rozmaitości A, $\mathrm{End}_{\mathbb{F}_q}(A)$, jest skończenie generowanym $\mathbb{Z}$ modułem rangi $\leq 4g^2$. Jeśli A jest prosta nad $\mathbb{F}_q$, to $\mathrm{End}_{\mathbb{F}_q}(A)$ nie zawiera dzielników zera i $\mathrm{End}_{\mathbb{F}_q}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ jest algebrą z dzieleniem, której centrum jest podciało $\mathbb{Q}(\pi_q)$. Liczbę algebraiczną całkowitą π nazywamy *liczbą q-Weila* jeśli dla każdego zanurzenia $\varphi : \mathbb{Q}(\pi) \to \mathbb{C}$ mamy $\varphi(\pi)\overline{\varphi(\pi)} = q$. Z Twierdzenia 2.1 endomorfizm Frobeniusa rozmaitości prostej nad $\mathbb{F}_q$ jest liczbą q-Weila.

Twierdzenie 2.2. (Honda-Tate [43]) *Przyporządkowanie rozmaitości abelowej prostej nad $\mathbb{F}_q$ jej endomorfizmu Frobeniusa π_q zadaje bijekcję między klasami izogenicznych rozmaitości abelowym prostych nad $\mathbb{F}_q$, a klasami sprzężonych nad $\mathbb{Q}$ liczb q-Weila.*

Ciało liczbowe K nazywamy *CM ciałem* jeśli K jest urojonym kwadratowym rozszerzenim ciała totalnie rzeczywistego K_0 (K_0 jest totalnie rzeczywiste jeśli $\varphi(K_0) \subset \mathbb{R}$ dla każdego zanurzenia $\varphi : K_0 \to \mathbb{C}$). Zatem CM ciało K jest postaci $K = K_0(\sqrt{-\alpha})$, gdzie $\alpha \in K_0$ i $\varphi(\alpha) > 0$ dla każdego zanurzenia $\varphi : K_0 \to \mathbb{R}$. CM ciało K ma automorfizm, oznaczany $\bar{\cdot}$, który dla każdego zanurzenia $K \to \mathbb{C}$ jest przemienny ze sprzężeniem zespolonym; jest to nietrywialny automorfizm grupy dwuelementowej

$\mathrm{Gal}(K/K_0)$. CM ciała tworzą klasę zamkniętą na składanie ciał. W szczególności domknięcie normalne CM ciała jest CM ciałem. Pierścień liczb algebraicznych całkowitych w ciele K oznaczamy przez $\mathcal{O}_K$.

Twierdzenie 2.3. ([45]) *Niech $A/\mathbb{F}_q$ będzie rozmaitością abelową prostą wymiaru g z algebrą endomorfizmów $K = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$. Rozmaitość A jest zwykła dokładnie wtedy, gdy K jest CM ciałem stopnia $2g$ oraz $\pi_q, \overline{\pi}_q$ są względnie pierwsze w $\mathcal{O}_K$ (tzn. generują ideał (1)). Wówczas $K = \mathbb{Q}(\pi_q)$, $f_q(x)$ jest wielomianem minimalnym π_q oraz*

$$\#A(\mathbb{F}_q) = f_q(1) = \mathrm{N}_{K/\mathbb{Q}}(\pi_q - 1). \tag{2.1}$$

Opiszemy teraz liczby Weila odpowiadające rozmaitościom zwykłym i prostym, które nie są absolutnie proste.

Twierdzenie 2.4. *Niech $A/\mathbb{F}_q$ będzie rozmaitością zwykłą i prostą o liczbie q-Weila π. A rozpada się nad $\mathbb{F}_{q^n}$ dokładnie wtedy, gdy $\mathbb{Q}(\pi^n) \subsetneq \mathbb{Q}(\pi)$. Wówczas A jest izogeniczna z potęgą rozmaitości prostej $B/\mathbb{F}_{q^n}$ odpowiadającej liczbie q^n-Weila π^n.*

Dowód. Pierwsza część jest szczególnym przypadkiem [23, Lemat 4]. Druga część jest również dobrze znana. Powyższy fakt łatwo wynika z własności wielomianu charakterystycznego i z twierdzeń Tate [44]. Jeśli $f_{A,q}(x) = \prod_{i=1}^{2g}(x - \pi_i)$, to $f_{A,q^n}(x) = \prod_{i=1}^{2g}(x - \pi_i^n)$. Ponieważ A jest zwykła i prosta, wielomian $f_{A,q}$ jest nierozkładalny, stąd liczby π_i są sprzężone. Jeśli $\mathbb{Q}(\pi^n) \subsetneq \mathbb{Q}(\pi)$, to f_{A,q^n} jest podzielny przez wielomian minimalny π^n stopnia $< \deg f_{A,q^n}$, stąd A musi rozpadać się nad $\mathbb{F}_{q^n}$. Odwrotnie, jeśli $A \sim B_1 \times \cdots \times B_m$ dla rozmaitości prostych $B_i/\mathbb{F}_{q^n}$, to $f_{A,q^n} = f_{B_1,q^n} \cdots f_{B_m,q^n}$. Ponieważ B_i muszą być zwykłe, f_{B_i,q^n} jest nierozkładalny. Liczby $\pi_1^n, \ldots, \pi_{2g}^n$ są sprzężone, stąd są pierwiastkami każdego f_{B_i,q^n}. Zatem wszystkie wielomiany f_{B_i,q^n} są równe i z twierdzenia Tate [44] rozmaitości B_i są isogeniczne nad $\mathbb{F}_{q^n}$, więc $A \sim B_1^m$. □

Wniosek 2.5. *Niech $A/\mathbb{F}_q$ będzie rozmaitością abelową zwykłą i prostą o liczbie q-Weila π oraz niech $E/\mathbb{F}_q$ będzie krzywą eliptyczną o liczbie q-Weila π_0.*

(1) *Wówczas A jest izogeniczna z E^g nad $\mathbb{F}_{q^n}$ dokładnie wtedy, gdy $\pi = \zeta_s \pi_0$, gdzie ζ_s jest s-tym pierwotnym pierwiastkiem z jedynki i $s \mid n$.*
(2) *Jeśli $2 \mid s$, to A rozpada się nad $\mathbb{F}_{q^{s/2}}$.*
(3) *Jeśli $\pi = \zeta_s \pi_0$, to $\mathbb{Q}(\pi) = \mathbb{Q}(\zeta_s, \sqrt{-d})$, gdzie $\pi_0 \in \mathbb{Q}(\sqrt{-d})$ i $d \in \mathbb{Z}_{>0}$ jest bezkwadratowa.*

Dowód. (1) Z Twierdzenia 2.4 mamy $A \sim E^g$ nad $\mathbb{F}_{q^n}$ dokładnie wtedy, gdy $\pi^n = \pi_0^n$. Jeśli $s \in \mathbb{Z}_{>0}$ jest najmniejszą liczbą, taką że $\pi^s = \pi_0^s$, to $\pi = \zeta_s \pi_0$ i $s \mid n$.
(2) Wynika stąd, że $\pi^{s/2} = \zeta_s^{s/2} \pi_0^{s/2} = -\pi_0^{s/2} \in \mathbb{Q}(\pi_0)$.
(3) Ponieważ E jest zwykła, π_0^s i $\bar{\pi}_0^s$ są względnie pierwsze. Stąd $\pi^s \notin \mathbb{Z}$ i π^s generuje $\mathbb{Q}(\sqrt{-d})$, zatem $\mathbb{Q}(\pi) = \mathbb{Q}(\zeta_s, \sqrt{-d})$.

3. Wyznaczanie liczb Weila w CM ciałach

Dla standardowego szyfrowania opartego na schemacie ElGamala lub podpisów cyfrowych DSA na krzywych eliptycznych lub hipereliptycznych wymagane są grupy rzędu pierwszego lub prawie pierwszego. Najogólniejszym wyborem krzywej jest jej wylosowanie, obliczenie rzędu i sprawdzenie czy ma wymaganą własność. Niestety obecnie znane metody obliczania rzędu jakobianu krzywych genusu 2 nad dużymi ciałami prostymi są zbyt wolne w praktyce, aby ten sposób był efektywny. Alternatywne podejście polega na skonstruowaniu krzywej przy pomocy CM metody. Wówczas ograniczamy się do krzywych, których pierścień endomorfizmów jakobianu jest ordynkiem w CM ciele generowanym przez odpowiednio małe liczby. Obecnie nie są znane żadne powody, dla których problem logarytmu dyskretnego dla takich krzywych byłby łatwiejszy do rozwiązania. CM metodę stosujemy również, gdy chcemy skonstruować krzywe, których parametry jakobianu spełniają pewne dodatkowe własności, jak w przypadku krzywych z danym stopniem zanurzeniowym.

Aby skonstruować krzywą, której jakobian ma rząd pierwszy lub prawie pierwszy postępujemy następująco. Najpierw w ustalonym CM ciele K wybieramy liczby $\pi \in \mathcal{O}_K$ odpowiedniej wielkości spełniające $\pi\bar{\pi} \in \mathbb{Z}$ dopóki nie znajdziemy, takiej że $q = \pi\bar{\pi}$ jest liczbą pierwszą oraz rząd $n = \mathrm{N}_{K/\mathbb{Q}}(\pi - 1)$ jest liczbą pierwszą lub prawie pierwszą. Następnie stosujemy CM metodę aby skonstrupwać krzywą, której jakobian realizuje znalezioną liczbę q-Weila π.

Pierwszy problem, który wymaga omówienia to sposób otrzymywania liczb $\pi \in \mathcal{O}_K$, takich że $\pi\bar{\pi} \in \mathbb{Z}$. Jeśli konstruujemy krzywe eliptyczne, to $K = \mathbb{Q}(\sqrt{-d})$ jest ciałem urojonym kwadratowym i oczywiście każda liczba $\pi \in \mathcal{O}_K$ ma normę $\pi\bar{\pi} \in \mathbb{Z}$. Dla CM ciał wyższych stopni liczby $\pi \in \mathcal{O}_K$ spełniające warunek $\pi\bar{\pi} \in \mathbb{Z}$ są zawarte w pewnym właściwym podzbiorze algebraicznym, dlatego potrzebujemy odpowiedniej metody aby je znaleźć. Można je otrzymywać jako wartości na liczbach całkowitych wielomianów $w(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ spełniających warunek

$$(x_1, \ldots, x_n) = w(x_1, \ldots, x_n)\overline{w}(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n], \qquad (3.1)$$

gdzie $\bar{\cdot}$ jest sprzężeniem zespolonym współczynników w. Omówimy teraz metody otrzymywania takich wielomianów. (W przypadku ciała urojonego kwadratowego możemy oczywiście wziąć $w(x_1, x_2) = x_1 + x_2\sqrt{-d}$.) Omówimy najpierw ideę geometrycznej metody [10] otrzymywania takich wielomianów dla CM ciał stopnia 4, a następnie opiszemy ogólą metodę algebraiczną dla dowolnych CM ciał.

Niech $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d_0}})$ będzie CM ciałem stopnia 4, gdzie $a, b, d_0 \in \mathbb{Z}_{>0}$, d_0 jest bezkwadratowa i $-a + b\sqrt{d_0} < 0$ (wówczas $\mathbb{Q}(\sqrt{d_0})$ jest podciałem kwadratowym rzeczywistym). Niech $b_1, \ldots, b_4 \in \mathcal{O}_K$ będzie bazą $K/\mathbb{Q}$. Istnieją formy kwadratowe $F_1, F_2 \in \mathbb{Q}[X_1, \ldots, X_4]$, takie że dla każdego $(x_1, \ldots, x_4) \in \mathbb{Q}^4$ mamy

$$\big(\sum x_i b_i\big)\overline{\big(\sum x_i b_i\big)} = F_1(x_1, \ldots, x_4) + F_2(x_1, \ldots, x_4)\sqrt{d_0}.$$

Wówczas współrzędne w bazie $\{b_i\}$ liczb $\pi \in K$ spełniających $\pi\bar{\pi} \in \mathbb{Q}$ odpowiadają punktom wymiernym na kwadryce

$$S = \{F_2 = 0\} \subset \mathbb{Q}^4.$$

Np. w bazie $b_1 = 1$, $b_2 = \sqrt{d_0}$, $b_3 = \sqrt{-a + b\sqrt{d_0}}$, $b_4 = b_2 b_3$ mamy

$$F_2 = 2X_1X_2 + 2aX_3X_4 - bX_3^2 - bdX_4^2.$$

Jedynym punktem osobliwym na S jest początek układu O (pochodne cząstkowe $\partial F_2/\partial X_i$, $i = 1, \ldots, 4$, znikają tylko w O). Stąd rzutowanie z dowolnego punktu wymiernego $A \neq O$ na dowolną podprzestrzeń afiniczną $M \subset \mathbb{Q}^4$ wymiaru 3, indukuje odzorowanie biwymierne $f : \mathbb{Q}^3 \to S$ (gdzie M traktujemy jako $\mathbb{Q}^3$ wprowadzając układ współrzędnych). Jako punkt wymierny $A \in S$ możemy np. wziąć punkt odpowiadający $1 \in K$. Jeśli otrzymane odwzorowanie biwymierne $f : \mathbb{Q}^3 \to S$ pomnożymy przez wielomian, który jest wspólnym mianownikiem jego współrzędnych, to otrzymamy odwzorowanie $(f_1, \ldots, f_4) : \mathbb{Q}^3 \to S$, którego współrzędne są formami kwadratowymi (szczegóły można znaleźć w [10]). (Mnożąc odwzorowanie $f : \mathbb{Q}^3 \to S$ przez dowolną funkcję otrzymujemy w dalszym ciągu odwzorowanie o wartościach w S, ponieważ S jest dana przez równanie jednorodne $F_2 = 0$). Podobnie możemy założyć, że współczynniki form f_i są całkowite. Stąd odwzorowanie wielomianowe $f = (f_1, \ldots, f_4) : \mathbb{Q}^3 \to S$ wyznacza wielomian $w(x_1, x_2, x_3) = \sum_{i=1}^{4} f_i(x_1, x_2, x_3)b_i \in K[x_1, x_2, x_3]$ stopnia 2, który spełnia (3.1).

3.1. Reflex norma

Reflex norma została wprowadzona w teorii mnożeń zespolonych rozmaitości abelowych. Jej podstawowe własności można znaleźć w książce Shimury [38]. Freeman, Stevenhagen i Streng [20] i Freeman [17] wykorzystali reflex normę do konstruowania rozmaitości abelowych z danym stopniem zanurzeniowym. Poniżej podajemy podstawowe własności reflex normy, których dowody można znaleźć również w wykładzie Milne [33, str. 12–15].

Niech K będzie CM ciałem stopnia $2g$ o domknięciu normalnym K_1 (które również jest CM ciałem). Niech $\Phi = \{\varphi_1, \ldots, \varphi_g\}$ będzie zbiorem zanurzeń $\varphi_i : K \to K_1$. Mówimy, że Φ jest *CM typem* na K, jeśli żadne zanurzenie w Φ nie powstaje przez sprzężenie zespolone innego (tzn., $\varphi_i \neq \overline{\varphi}_j$ dla $i, j = 1, \ldots, g$). *Normą względem CM typu* Φ nazywamy odwzorowanie

$$\mathrm{N}_\Phi : K \to K_1,\ \mathrm{N}_\Phi(x) = \varphi_1(x) \cdots \varphi_g(x).$$

Oczywiście mamy $\mathrm{N}_{K/\mathbb{Q}}(x) = \mathrm{N}_\Phi(x)\overline{\mathrm{N}_\Phi(x)} \in \mathbb{Q}$. Stąd jeśli K jest Galois, możemy użyć normy N_Φ, aby otrzymywać jako jej wartości liczby $\pi = \mathrm{N}_\Phi(x)$, takie że $\pi\bar{\pi} \in \mathbb{Z}$. W ustalonej bazie $\{b_i\}$ ciała $K/\mathbb{Q}$ możemy zapisać normę N_Φ jako wielomian jednorodny stopnia g o współczynnikach w K_1

$$\mathrm{N}_\Phi\big(\sum_j x_j b_j\big) = \big(\sum_j x_j \varphi_1(b_j)\big) \cdots \big(\sum_j x_j \varphi_g(b_j)\big) \quad \text{dla} \quad x_j \in \mathbb{Q},$$

który spełnia (3.1). Jeśli ciało K nie jest Galois, to na ogół $\mathrm{N}_\Phi(x) \notin K$ dla $x \in K$, ale istnieje CM podciało $K^* \subset K_1$ wraz z CM typem Φ^*, takie że $\mathrm{N}_{\Phi^*}(x) \in K$ dla $x \in K^*$. Wówczas jako wartości normy N_{Φ^*} będziemy otrzymywać liczby $\pi = \mathrm{N}_{\Phi^*}(x) \in K$, takie że $\pi\overline{\pi} \in \mathbb{Z}$. Omówimy teraz konstrukcję takiego podciała K^*

Jeśli $K_0 \subset K$ jest CM podciałem z CM typem Φ_0, to biorąc wszystkie możliwe rozszerzenia zanurzeń z Φ_0 na ciało K otrzymujemy CM typ na K i mówimy że taki CM typ na K powstaje przez rozszerzenie Φ_0. Jeśli CM typ Φ nie powstaje przez rozszerzenie CM typu z właściwego CM podciała, to mówimy że Φ jest *prymitywmy*.

Niech Φ_1 będzie CM typem na K_1, który jest rozszerzeniem Φ oraz niech

$$H = \{\sigma \in \mathrm{Gal}(K_1/\mathbb{Q}) : \Phi_1\sigma = \Phi_1\}.$$

Wówczas ciało stałe K_0 podgrupy H jest CM ciałem zawartym w K oraz zawężenie CM typu Φ do K_0 jest CM typem Φ_0 na K_0. Ciało K_0 jest najmniejszym podciałem, takim że Φ powstaje przez rozszerzenie CM typu, które nazywamy *podciałem prymitywnym* dla pary (K, Φ).

Dla podciała $K^* \subset K_1$ następujące dwa warunki są równoważne (1) K^* jest podciałem stałym grupy $\{\sigma \in \mathrm{Gal}(K_1/\mathbb{Q}) : \sigma\Phi_1 = \Phi_1\}$ (2) K^* jest generowane nad $\mathbb{Q}$ przez zbiór $\{\sum_{\varphi\in\Phi} \varphi(x) : x \in K\}$. Ciało K^* nazywamy *reflex ciałem* względem CM typu Φ na K. Jeśli Φ powstaje przez rozszerzenie CM typu Φ_0 na K_0, to $K_0^* = K^*$. W reflex ciele K^* wprowadzamy następujący CM typ. Niech Φ_1 będzie rozszerzeniem Φ na K_1. Wówczas $\Phi_1^{-1} = \{\varphi^{-1} : \varphi \in \Phi_1\}$ jest CM typem na K_1, którego podciałem prymitywnym jest reflex ciało K^*. CM typ indukowany na K^* przez Φ_1^{-1} oznaczamy przez Φ^*. Wówczas norma względem Φ^* przyjmuje wartości w K,

$$K^* \ni x \mapsto \mathrm{N}_{\Phi^*}(x) \in K.$$

3.2. CM ciała postaci $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$

Jeśli CM typ Φ na K nie jest prymitywny, to reflex norma $\mathrm{N}_{\Phi^*}(x)$ dla $x \in K^*$ przyjmuje wartości w podciele prymitywnym $K_0 \subset K$ dla Φ. Zatem nie możemy jej użyć, aby otrzymywać liczby Weila $\pi = \mathrm{N}_{\Phi^*}(x)$, które generują K. Taka sytuacja np. zawsze zachodzi gdy K jest CM ciałem stopnia 4 zawierającym podciało urojone kwadratowe L; takie ciało K nazywamy *nieprymitywnym*. (Wówczas jeśli $L = \mathbb{Q}(\sqrt{-d}) \subset K$ jest podciałem urojonym kwadratowym i $\mathbb{Q}(\sqrt{d_0}) \subset K$ jest podciałem rzeczywistym, to K zawiera drugie podciało urojone kwadratowe $L' = \mathbb{Q}(\sqrt{-dd_0})$. Stąd K jest Galois jako złożenie ciał kwadratowych i każdy CM typ na K powstaje przez rozszerzenie CM typu na L lub L'. Np. rozszerzeniem CM typu $\{\mathrm{id}_L\}$ na L jest $\{\mathrm{id}_K, i_{L'}\}$, gdzie automorfizm $i_{L'}$ jest stały na L i jest sprzężeniem zespolonym na L'. Wówczas $\mathrm{N}_{\mathrm{id},i_{L'}}(x) \in L$ dla dowolnego $x \in K$, ponieważ jest elementem stałym względem $\{\mathrm{id}, i_{L'}\}$.)

Niech $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$, gdzie ζ_s jest s-tym pierwotnym pierwiastkiem z 1 i $d \in \mathbb{Z}_{>0}$ jest bezkwadratowa (K jest CM ciałem jako złożenie CM ciał $\mathbb{Q}(\zeta_s)$ i $\mathbb{Q}(\sqrt{-d})$). Dla dowolnej liczby q-Weila $\pi_0 \in \mathbb{Q}(\sqrt{-d})$, $\pi = \zeta_s\pi_0$ jest liczbą q-Weila w K odpowiadającą rozmaitści abelowej, która nad rozszerzeniem stopnia s jest izogeniczna z potęgą krzywej eliptycznej odpowiadającej π_0 (Wniosek 2.5). Zatem liczby Weila w K takiej postaci możemy otrzymywać jako wartości na liczbach całkowitych wielomianu

$$w(x_1, x_2) = \zeta_s(x_1 + x_2\sqrt{-d}).$$

3.3. Otrzymywanie liczb Weila jako wartości wielomianów

Jeśli wielomian $w(x_1, \ldots, x_n)$ spełnia (3.1), to problem czy obraz $w(\mathbb{Z}^n)$ zawiera nieskończenie wiele liczb Weila jest na ogół bardzo trudny

i otwarty od strony teoretycznej. Ograniczymy się jedynie do podania pewnych warunków koniecznych, które zwykle są wystarczające dla praktycznych zastoswań. Powyższy problem sprowadza się do problemu przyjmowania przez wielomian o współczynnikach wymiernych nieskończenie wielu wartości pierwszych. Łatwo podać następujące warunki konieczne dla wielomianów jednej zmiennej.

Stwierdzenie 3.1. *Jeśli wielomian $q(x) \in \mathbb{Q}[x]$ przyjmuje nieskończenie wiele wartości pierwszych dla $x \in \mathbb{Z}_{>0}$, to*
(1) *$q(x)$ jest nierozkładalny,*
(2) *zbiór $S = \{q(x) : x, q(x) \in \mathbb{Z}\}$ jest niepusty i $\gcd(S) = 1$,*
(3) *$q(x)$ ma dodatni współczynnik wiodący.*

Hipoteza Buniakowskiego-Schinzla mówi, że powyższe warunki są również wystarczające, aby wielomian przyjmował nieskończenie wiele wartości pierwszych. Bateman i Horn [2] podali hipotezę o gęstości liczb pierwszych w zbiorze wartości wielomianu. Zgodnie z terminologią wprowadzoną w [19] mówimy, że wielomian *reprezentuje liczby pierwsze* jeśli spełnia warunki Stwierdzenia 3.1. Jeśli dla takiego wielomianu przyjmiemy heurystyczne założenie, że liczby pierwsze są rozłożone równomiernie w zbiorze wartości $q(\mathbb{Z})$ tak samo jak w dużych przedziałach, to z twierdzenia o liczbach pierwszych możemy oczekiwać, że $q(x)$ będzie liczbą pierwszą z prawdopodobieństwem około $1/\deg q(x) \log N$ dla $x \in \{1, \ldots, N\}$.

Jeśli $q(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ przyjmuje wartości nieujemne (w szczególności wielomian spełniający (3.1)), $q(x_1, \ldots, x_n)$ jest nierozkładalny i zbiór $S = \{q(x) : x \in \mathbb{Z}^n, q(x) \in \mathbb{Z}\} \neq \emptyset$ ma $\gcd(S) = 1$, to w praktyce taki wielomian również wydaje się przyjmować wartości pierwsze dla pewnej części punktów całkowitych w $\mathbb{Z}^n$, ale podanie nawet dla wielomianów dwóch zmiennych podobnej heurystyki jak wyżej nie jest oczywiste. Dla dalszych zastosowań będziemy zakładali, że mamy wielomian, którego obraz zawiera dostatecznie wiele liczb pierwszych (lub liczb Weila), przez co rozumiemy, że oczekujemy otrzymania liczb pierwszych (lub liczb Weila) z pewnym dodatnim prawdopodobieństwem.

4. Metoda mnożeń zespolonych

Metoda mnożeń zespolonych (CM metoda) pozwala konstruować krzywe eliptyczne lub krzywe genusu 2 nad ciałami skończonymi, których pierścień endomorfizmów jakobianu jest ordynkiem maksymalnym w danym CM ciele K odpowiednio stopnia 2 lub 4. Wówczas jakobian takiej

krzywej lub jej skręcenia realizuje liczbę Weila $\pi \in K$. Aby wybrać odpowiednią krzywą w praktyce wystarczy sprawdzić czy dla losowego punktu P z jakobianu mamy $nP = 0$, gdzie $n = \mathrm{N}_{K/\mathbb{Q}}(\pi - 1)$ jest rzędem jakobianu, który chcemy otrzymać. W praktyce CM metoda jest efektywna dla CM ciał generowanych przez odpowiednio małe liczby.

Poniżej opiszemy w dużym uproszczeniu główną ideę CM metody dla krzywych eliptycznych i krzywych genusu 2. CM metodę dla krzywych eliptycznych wykorzystuje się również do konstruowania krzywych genusu 2 o rozkładalnym jakobianie. Teoria na której opiera się CM metoda dla krzywych eliptycznych znajduje się w książkach [39, 9, 28], streszczenie można znaleźć np. w [8, 12].

Niech $K = \mathbb{Q}(\sqrt{-d})$ będzie ciałem urojonym kwadratowym, gdzie $d \in \mathbb{Z}_{>0}$ jest liczbą bezkwadratową. Dla danego ciała $\mathbb{F}$ o domknięciu algebraicznym $\overline{\mathbb{F}}$ niech $\mathcal{C}_{K,\overline{\mathbb{F}}}$ będzie zbiorem klas izomorficznych krzywych eliptycznych $E/\overline{\mathbb{F}}$, takich że $\mathrm{End}(E) = \mathcal{O}_K$ jest ordynkiem maksymalnym w K. Dowodzi się, że zbiór $\mathcal{C}_{K,\mathbb{C}}$ jest skończony, j-niezmienniki krzywych eliptycznych w $C_{K,\mathbb{C}}$ są sprzężonymi nad $\mathbb{Q}$ liczbami algebraicznymi całkowitymi, których wielomian minimalny

$$H_K(x) = \prod_{E \in \mathcal{C}_{K,\mathbb{C}}} (x - j(E)) \in \mathbb{Z}[x]$$

nazywa się *wielomianem klas Hilberta* ciała urojonego kwadratowego K. Stopień i współczynniki wielomianu Hilberta są wielkości $O(\sqrt{d})$ dlatego w praktyce można go obliczyć tylko dla odpowiednio małych d (obecnie $d \leq 10^{12}$). Istnieje kilka metod obliczania wielomianu klas [3, 7, 13, 42].

Jeśli w charakterystyce p istnieją krzywe eliptyczne zwykłe, których pierścień endomorfizmów jest ordynkiem w K, to również zbiór $\mathcal{C}_{K,\overline{\mathbb{F}}_p}$ jest niepusty oraz redukcja modulo p indukuje bijekcję $\mathcal{C}_{K,\mathbb{C}} \to C_{K,\overline{\mathbb{F}}_p}$. Wówczas j-niezmienniki krzywych w $\mathcal{C}_{K,\overline{\mathbb{F}}_p}$ są dokładnie pierwiastkami w $\overline{\mathbb{F}}_p$ wielomianu klas Hiberta mod p. Stąd aby skonstruować krzywą eliptyczną w $\mathcal{C}_{K,\overline{\mathbb{F}}_p}$ wystarczy znaleźć pierwiastek $j \in \overline{\mathbb{F}}_p$ wielomianu $H_K(x) \bmod p$ i utworzyć krzywą eliptyczną o j-niezmienniku j.

Idea CM metody dla krzywych genusu 2 jest analogiczna jak dla krzywych eliptycznych, ale metoda opiera się na dużo trudniejszej teorii i jest mniej efektywna w praktyce. Niech K będzie CM ciałem prymitywnym stopnia 4, tzn. K nie zawiera podciała urojonego kwadratowego (obecnie CM metoda nie jest rozwinięta dla CM ciał nieprymitywnych). Krzywe genusu 2 nad $\mathbb{F}$ są z dokładnością do izomorfizmu nad $\overline{\mathbb{F}}$ wyznaczone przez trzy niezmienniki Igusy j_1, j_2, j_3 [24]. Algorytm Mestre [30] pozwala dla

danych niezmienników Igusy utworzyć równanie krzywej genusu 2 o tych niezmiennikach. Niech $\mathcal{C}_{K,\overline{\mathbb{F}}}$ będzie zbiorem klas izomorficznych krzywych genusu 2 $C/\overline{\mathbb{F}}$, takich że $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$ jest ordynkiem maksymalnym w K. Wówczas zbiór $\mathcal{C}_{K,\mathbb{C}}$ jest skończony, niezmienniki Igusy krzywych w $\mathcal{C}_{K,\mathbb{C}}$ są liczbami algebraicznymi, oraz następujące trzy *wielomiany Igusy* mają współczynniki wymierne

$$H_{K,i}(x) = \prod_{C \in \mathcal{C}_{K,\mathbb{C}}} (x - j_i(C)) \in \mathbb{Q}[x] \text{dla} i = 1, 2, 3.$$

Podobnie jak dla wielomianu klas Hilberta istnieje kilka metod obliczania wielomianów Igusy [14, 40, 41], które w praktyce są efektywne jeśli ciało K jest generowane przez małe liczby.

Jeśli charakterystyce p istnieją krzywe genusu 2, których jakobian jest ordynkiem w CM ciele K, to zbiór $\mathcal{C}_{K,\overline{\mathbb{F}}_p}$ jest niepusty oraz redukcja mod p indukuje bijekcję $\mathcal{C}_{K,\mathbb{C}} \to \mathcal{C}_{K,\overline{\mathbb{F}}_p}$. Wówczas niezmienniki Igusy krzywych w $\mathcal{C}_{K,\overline{\mathbb{F}}_p}$ otrzymuje się jako pierwiastki w $\overline{\mathbb{F}}_p$ wielomianów Igusy $H_{K,i}(x) \bmod p$. Dla znalezionych niezmienników Igusy krzywej $C \in \mathcal{C}_{K,\overline{\mathbb{F}}_p}$ stosuje się algortym Mestre aby znaleźć równanie C.

Przykład 4.1. Następujący przykład pokazuje zastosowanie CM metody, aby efektywnie znaleźć krzywą genusu 2 nad dużym ciałem $\mathbb{F}_p$, której jakobian ma rząd pierwszy (poniższe obliczenia z wykorzystaniem programu Magma zajmują kilka sekund). Ciało cyklotomiczne $K = \mathbb{Q}(\zeta_5)$ jest CM ciałem stopnia 4. Aby otrzymywać liczby Weila w K wykorzystamy normę względem CM typu $\Phi = \{\mathrm{id}_K, \varphi\}$, gdzie φ jest automorfizmem K, $\zeta_5 \to \zeta_5^2$. Wówczas w bazie $1, \zeta_5, \zeta_5^2, \zeta_5^3$ norma względem CM typu Φ ma postać

$$\mathrm{N}_\Phi(x_1, \ldots, x_4) = (x_1 + \zeta_5 x_2 + \zeta_5^2 x_3 + \zeta_5^3 x_4)(x_1 + \zeta_5^2 x_2 + \zeta_5^4 x_3 + \zeta_5^6 x_4).$$

Przyjmując np. $x_1 = x_2 = x_3 = 1$ otrzymujemy jednoparametrową rodzinę liczb Weila w K:

$$\begin{aligned} \pi(x) &= \mathrm{N}_\Phi(1,1,1,x) = -(\zeta_5^3 + \zeta_5^2 + \zeta_5 + 1)x^2 + (2\zeta_5^3 + 2\zeta_5^2 + \zeta_5 + 1)x - \zeta_5^3 \\ q(x) &= \pi(x)\bar{\pi}(x) = x^4 - 3x^3 + 4x^2 - 2x + 1 \end{aligned}$$

Wówczas wielomiany $q(x)$ i $n(x) = \mathrm{N}_{K/\mathbb{Q}}(\pi(x) - 1) \in \mathbb{Z}[x]$ reprezentują liczby pierwsze. Ponieważ $n(x)$ jest stopnia 8, aby otrzymać liczbę Weila powierzchni abelowej, której rząd jest np. liczbą pierwszą o około 200 bitach powinniśmy jej szukać jako wartości $\pi(x)$ na liczbach $x \in \mathbb{Z}$ około

25-bitowych. Sprawdzając po kolei liczby $x \geq 2^{25}$ znajdujemy x_0, takie że $q(x_0)$ i $n(x_0)$ są liczbami pierwszymi

$$\begin{aligned}
x_0 &= 2^{25} + 1102,\\
\pi = \pi(x_0) &= -1125973794914089\zeta_5^3 - 1125973794914088\zeta_5^2 - 1125973828469622\zeta_5\\
&\quad - 1125973828469622\\
n &= \mathrm{N}_{K/\mathbb{Q}}(\pi - 1)\\
&= 160736000790588183264167820823508884078378008053346901078857 1\\
&\qquad \text{(200 bitowa liczba pierwsza)}\\
q &= \pi\bar{\pi} = 126781702461588691395166477398 1 \quad \text{(100 bitowa liczba pierwsza)}
\end{aligned}$$

Aby znaleźć krzywą genusu 2, której jakobian realizuje powyższe parametry w przypadku CM ciała $K = \mathbb{Q}(\zeta_5)$ możemy uniknąć ogólnej CM metody. Zauważmy, że krzywe

$$C_a : y^2 = x^5 + a$$

mają automorfizm stopnia 5, $(x, y) \mapsto (\zeta_5 x, y)$, stąd $\mathrm{End}(\mathrm{Jac}(C_a)) = \mathcal{O}_K = \mathbb{Z}[\zeta_5]$ w charakterystyce p jeśli $\mathrm{Jac}(C_a)$ jest zwykły. Krzywe C_a są dokładnie skręceniami krzywej $y^2 = x^5 + 1$, stąd aby w praktyce znaleźć odpowiednie $a \in \mathbb{F}_q$, które realizuje powyższe parametry wystarczy na ogół po kolei sprawdzać małe $a \in \mathbb{F}_p$ dopóki nie znajdziemy odpowiedniej krzywej. Dla ustalonego a wybieramy losowo punkt $P \in \mathrm{Jac}(C_a)(\mathbb{F}_p)$ i jeśli $nP = 0$, to z dużym prawdopodobieństwem C_a jest szukaną krzywa. W naszym przypadku taką krzywą jest

$$y^2 = x^5 + 6.$$

4.1. CM metoda dla CM ciał stopnia 4 postaci $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$

Dla liczb Weila w nieprymitywnych CM ciałach stopnia 4 nie zostały rozwinięte ogólne metody konstruowania krzywych genusu 2, których jakobian realizuje takie liczby, przy założeniu, że takie krzywe istnieją (liczby Weila w CM ciałach nieprymitywnych mogą nie być realizowane przez jakobiany krzywych). Opiszemy teraz częściowe rozwiązanie problemu konstruowania takich krzywych podane przez Freemana i Satoha [18] dla CM ciał stopnia 4 postaci $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$, gdzie $d \in \mathbb{Z}_{>0}$ jest bezkwadratowa. Metoda pozwala zrealizować pewną część liczb Weila w takich CM ciałach

jako jakobiany krzywych postaci (4.1) i (4.2). Ponieważ ciało cyklotomiczne $\mathbb{Q}(\zeta_s)$ ma stopień równy funkcji Eulera $\varphi(s)$, mamy $\varphi(s) = 2$ lub 4, stąd $s = 3, 4, 6$ lub $s = 8, 12$ (CM ciało $\mathbb{Q}(\zeta_5)$ jest prymitywne, CM ciała $\mathbb{Q}(\zeta_8)$ i $\mathbb{Q}(\zeta_{12})$ zawierają odpowiednio $\sqrt{-1}, \sqrt{-2}$ i $\sqrt{-1}, \sqrt{-3}$).

Powierzchnie abelowe realizujące liczby Weila $\pi \in \mathbb{Q}(\zeta_s, \sqrt{-d})$ mają automorfizm rzędu s odpowiadający ζ_s. Ponieważ $3 \mid s$ lub $4 \mid s$ najpierw naturalnie jest sprawdzić czy liczba Weila π nie jest realizowana przez jakobian krzywych postaci

$$y^2 = x^6 + ax^3 + b, \tag{4.1}$$

$$y^2 = x^5 + ax^3 + bx, \tag{4.2}$$

które mają automorfizmy rzędu 3 i 4 odpowiednio dane przez $(x, y) \mapsto (\zeta_3 x, y)$ i $(-x, \zeta_4 y)$. Metoda opiera się na następującym fakcie.

Lemat 4.2. ([18, Propositions 4.1 and 4.2]) *Krzywa C dana równaniem (4.1) lub (4.2) jest odpowiednio izomorficzna z krzywą $y^2 = x^6 + cx^3 + 1$ lub $y^2 = x^5 + cx^3 + x$, gdzie $c = a/\sqrt{b}$. Ponadto* $\mathrm{Jac}(C)$ *jest izogeniczny nad pewnym rozszerzeniem z E^2, gdzie E jest krzywą eliptyczną odpowiednio o j-niezmienniku*

$$j(E) = 2^8 3^3 \frac{(2c-5)^3}{(c-2)(c+2)^3}, \tag{4.3}$$

lub

$$j(E) = 2^6 \frac{(3c-10)^3}{(c-2)(c+2)^2}. \tag{4.4}$$

Dla naszych zastosowań jesteśmy zainteresowani znalezieniem krzywej, której jakobian realizuje liczbę Weila postaci $\pi = \zeta_s \pi_0$, gdzie $\pi_0 \in \mathbb{Q}(\sqrt{-d})$. Jeśli π jest realizowana przez jakobian krzywej C postaci (4.1) lub (4.2), to nad pewnym rozszerzeniem mamy isogenie $\mathrm{Jac}(C) \sim E^2 \sim E_0^2$, gdzie E jest krzywą eliptyczną o j-niezmienniku (4.3) lub (4.4) oraz E_0 jest krzywą eliptyczną o liczbie Weila π_0. Stąd liczba Weila krzywej E należy do ciała $\mathbb{Q}(\sqrt{-d})$. Jeśli pierścień endomorfizmów krzywej E jest ordynkiem maksymalnym $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$, to j-niezmiennik $j(E)$ jest pierwiastkiem wielomianu klas Hilberta $H_{\mathbb{Q}(\sqrt{-d})}$. Stąd otrzymujemy następujący algorytm.

Algorytm 4.3. Input: Liczba bezkwadratowa $d \in \mathbb{Z}_{>0}$, $s = 3, 4$, liczba q-Weila $\pi = \zeta_s \pi_0$, gdzie $\pi_0 \in K_0 = \mathbb{Q}(\sqrt{-d})$.
Output: Krzywa genusu 2 nad $\mathbb{F}_q$, której jakobian odpowiada π lub $\emptyset$.

(1) Oblicz wielomian klas Hilberta $H_{\mathbb{Q}(\sqrt{-d})}(x)$ ciała urojonego kwadratowego $\mathbb{Q}(\sqrt{-d})$.

(2) Dla dowolnego pierwiastka $j \in \overline{\mathbb{F}}_q$ wielomianu $H_{\mathbb{Q}(\sqrt{-d})}(x)$ niech S_1 i S_2 będą zbiorami rozwiązań $c \in \overline{\mathbb{F}}_q$ odpowiednio równań (4.3) i (4.4).
(3) Dla $i = 1, 2$ oraz dla $c \in S_i$ wykonuj: jeśli $i = 1$ połóż $C : y^2 = x^6 + cx^3 + 1$, w przeciwnym razie połóż $C : y^2 = x^5 + cx^3 + x$. Usuń C jeśli nie jest hipereliptyczna (tzn. prawa strona ma pierwiastki wielokrotne).
(4) Jeśli wszystkie niezmienniki Igusy krzywej C leżą w $\mathbb{F}_q$, wyznacz jej model $C_0/\mathbb{F}_q$.
(5) Wyznacz wszystkie skręcenia C_0' nad $\mathbb{F}_q$ krzywej C_0.
(6) Dla każdego skręcenia C_0' wybierz losowy punkt $P \in \mathrm{Jac}(C_0')(\mathbb{F}_q)$ i oblicz nP, gdzie $n = \mathrm{N}_{K/\mathbb{Q}}(\pi - 1)$.
(7) Zwróć C_0' jeśli $nP = 0$.

5. Uogólniony algorytm Cocksa-Pincha

Algorytm Cocksa-Pincha [19, Tw. 4.1] jest podstawową metodą konstruowania krzywych eliptycznych z danych stopniem zanurzeniowym, którego uogólnienia na rozmaitości abelowe zostały podane w [16, 19, 18, 10]. Poniżej opiszemy podejście do jego uogólnienia przedstawione w [10]. Zaczniemy od przypomnienia podstawowych pojęć. Niech $A/\mathbb{F}_q$ będzie rozmaitością abelową oraz r liczbą pierwszą, taką że $r \mid \#A(\mathbb{F}_q)$ i $r \neq \mathrm{char}\mathbb{F}_q$. Niech $\mu_r = \{\zeta \in \overline{\mathbb{F}}_q | \zeta^r = 1\}$ będzie grupą r-tych pierwiastków z 1. *Stopniem zanurzeniowym* A względem r nazywamy liczbę całkowitą k, taką że $\mathbb{F}_{q^k} = \mathbb{F}_q(\mu_r)$. Stopień zanurzeniowy jest najmniejszą liczbą $k \in \mathbb{Z}_{>0}$, taką że $r \mid (q^k - 1)$, lub równoważnie jest to rząd $q \bmod r$ w grupie $\mathbb{F}_r^*$. Na rozmaitości abelowej A istnieją dwa iloczyny dwuliniowe Weila i Tate

$$e_W : A[r] \times A[r] \longrightarrow \mu_r \subset \mathbb{F}_{q^k},$$

$$e_T : A(\mathbb{F}_{q^k})[r] \times A(\mathbb{F}_{q^k})/rA(\mathbb{F}_{q^k}) \longrightarrow \mu_r \subset \mathbb{F}_{q^k}.$$

Ciało $\mathbb{F}_{q^k}$ jest najmniejszym rozszerzeniem $\mathbb{F}_q$, w którym iloczyny dwuliniowe przyjmują wartości. Algorytm Millera [33, 22] pozwala obliczyć iloczyny dwulinowe na krzywych eliptycznych i w jakobianach krzywych hipereliptycznych, jeśli stopień k jest odpowiednio mały. W praktyce na ogół stosuje się iloczyn Tate, który można efektywniej obliczyć od iloczynu Weila.

Konstrukcje rozmaitości abelowych opierają się na następującym fakcie, który opisuje liczby Weila odpowiadające rozmaitościom z danym stopniem zanurzeniowym.

Lemat 5.1. ([20, Proposition 2.1]) *Niech $K = \mathbb{Q}(\pi)$ będzie CM ciałem stopnia $2g$, gdzie π jest liczbą q-Weila, taką że π i $\bar{\pi}$ są względnie pierwsze w $\mathcal{O}_K$. Wówczas rozmaitość abelowa $A/\mathbb{F}_q$ odpowiadająca liczbie q-Weila π ma stopień zanurzeniowy k względem liczby pierwszej r, gdzie $r \nmid kq$, dokładnie wtedy gdy*
(1) $r \mid \mathrm{N}_{K/\mathbb{Q}}(\pi - 1)$,
(2) $r \mid \Phi_k(q)$, *gdzie $\Phi_k(x)$ jest k-tym wielomianem cyklotomicznym.*

Proof. Warunek (1) oznacza z Twierdzenia 2.3, że $r \mid \#A(\mathbb{F}_q)$. Przypomnijmy, że wielomiany cyklotomiczne $\Phi_l(x) \in \mathbb{Z}[x]$ spełniają

$$x^k - 1 = \prod_{l|k} \Phi_l(x).$$

Pierwiastki $\Phi_k(x)$ w dowolnym ciele algebraicznie domkniętym $\mathbb{F}$, takim że $\mathrm{char}\mathbb{F} \nmid k$ są dokładnie k-tymi pierwotnymi pierwiastkami z 1. Stąd warunek (2) oznacza, że $q \bmod r$ jest k-tym pierwotnym pierwiastkiem z 1, czyli k jest stopniem zanurzeniowym względem r. kwadrat

Przypomnijmy, że dla podgrupy rzędu r w $A(\mathbb{F}_q)$ definiujemy parametr

$$\rho = \frac{g \log q}{\log r},$$

gdzie $g = \dim A$. Ponieważ rząd $\#A(\mathbb{F}_q)$ jest wielkości q^g, parametr ρ mówi nam ile razy wielkość $\#A(\mathbb{F}_q)$ jest więsza od wielkości r.

Opiszemy teraz uogólnienie algorytmu Cocksa-Pincha przedstawione w [10]. Niech K będzie CM ciałem. Dla wielomianu $w(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ definiujemy normę

$$N_{K/\mathbb{Q}}(w(x_1, \ldots, x_n)) = \prod_{\varphi: K \to \overline{K}} \varphi(w(x_1, \ldots, x_n)),$$

gdzie dowolne zanurzenie $\varphi : K \to \overline{K}$ rozszerzamy do zanurzenia $\varphi : K(x_1, \ldots, x_n) \to \overline{K}(x_1, \ldots, x_n)$ przyjmując $\varphi(x_i) = x_i$ dla $i = 1, \ldots, n$. Wówczas $N_{K/\mathbb{Q}}(w) \in \mathbb{Q}[x_1, \ldots, x_n]$, ponieważ jest to norma $N_{K(x_1,\ldots,x_n)/\mathbb{Q}(x_1,\ldots,x_n)}$.

Załóżmy, że dany jest wielomian $w(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, taki że

$$\begin{aligned} &q(x_1, \ldots, x_n) = w(x_1, \ldots, x_n)\overline{w}(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n] \quad \text{oraz} \\ &w(\mathbb{Z}^n) \quad \text{zawiera dostatecznie wiele liczb Weila w } K \end{aligned} \tag{5.1}$$

(gdzie „dostatecznie wiele" rozumiemy tak jak w Rozdziale 3.3). Chcemy otrzymać liczbę Weila $\pi = w(x_1, \ldots, x_n)$ dla pewnego $(x_1, \ldots, x_n) \in \mathbb{Z}^n$, która odpowiada rozmaitości abelowej ze stopniem zanurzeniowym k względem liczby piewszej r. Wówczas $(x_1, \ldots, x_n) \bmod r$ jest z Lematu 5.1 rozwiązaniem w $\mathbb{F}_r^n$ układu równań wielomianowych o współczynnikach całkowitych

$$\begin{cases} \mathrm{N}_{K/\mathbb{Q}}(w(x_1, \ldots, x_n) - 1) = 0 \bmod r \\ \Phi_k(q(x_1, \ldots, x_n)) = 0 \bmod r \end{cases}$$

Stąd wynika następujący algorytm, który uogólnia algorytm Cocksa-Pincha.

Twierdzenie 5.2. *Niech $k \in \mathbb{Z}_{>0}$, K będzie CM ciałem stopnia $2g$ oraz $w(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ spełnia (5.1)*

(1) Niech r będzie liczbą pierwszą, taką że $k \mid r - 1$.
(2) Niech $Z \subset \mathbb{F}_r^n$ będzie pewnym zbiorem rozwiązań układu (5.2).
(3) Dla dowolnego rozwiązania $(a_1, \ldots, a_n) \in Z$ niech $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ będzie jego podniesieniem.
(4) Niech $\pi = w(x_1, \ldots, x_n)$.

sl Jeśli π jest liczbą Weila, $K = \mathbb{Q}(\pi)$ i $(\pi, \overline{\pi}) = (1)$, to π odpowiada rozmaitości abelowej zwykłej wymiaru g ze stopniem zanurzeniowym k względem r.

Warunek $k \mid r - 1$ jest konieczny, aby układ (5.2) miał rozwiązania w ciele $\mathbb{F}_r$, ponieważ $q(x_1, \ldots, x_n) \bmod r$ jest k-tym pierwotnym pierwiastkiem z 1. W praktyce możemy losowo wybierać liczby pierwsze r odpowiedniej wielkości i sprawdzać czy znajdziemy rozwiązania w ciele $\mathbb{F}_r$. Możemy to robić np. ustalając $n - 2$ zmienne z $\mathbb{F}_r$ i wyznaczać rozwiązania układu z dwiema zmiennymi np. stosując rugowniki. Jeśli w ten sposób nie znajdziemy rozwiązań nad $\mathbb{F}_r$ próbując podstawiać pewną liczbę $n - 2$ zmiennych, to wybieramy inną liczbę pierwszą r. W następnym rozdziale podamy wzory na rozwiązania układu (5.2) w ciałach liczbowych w przypadku gdy $w(x_1, \ldots, x_n)$ jest reflex normą lub $w(x_1, x_2) = \zeta_s(x_1 + x_2\sqrt{-d})$ dla CM ciała $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$. Wówczas te wzory opisują również rozwiązania w ciałach skończonych dla liczb pierwszych r, które całkowicie rozpadają się w CM ciele K (tzn. nad r leży $2g$ ideałów pierwszych w $\mathcal{O}_K$). Na ogół rozwiązania układu (5.2) nad ciałem $\mathbb{F}_r$ są podobnej wielkości jak r, stąd zwykle otrzymujemy rozmaitości abelowe w parametrem

$$\rho \approx 2g \deg w(x_1, \ldots, x_n).$$

Dla krzywych eliptycznych mamy $\rho \approx 2$ jeśli $K = \mathbb{Q}(\sqrt{-d})$ jest ciałem urojonym kwadratowym i $w(x_1, x_2) = x_1 + x_2\sqrt{-d}$. Jeśli K jest CM ciałem

prymitywnym stopnia 4 i $w(x_1, \ldots, x_4)$ jest reflex normą, to otrzymujemy powierzchnie abelowe absolutnie proste z parametrem $\rho \approx 8$. Jeśli $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$ jest CM ciałem stopnia 4 i $w(x_1, x_2) = \zeta_s(x_1 + x_2\sqrt{-d})$, to otrzymujemy powierzchnie abelowe proste, które nie są absolutnie proste z parametrem $\rho \approx 4$.

6. Rodziny parametryczne rozmaitości abelowych

Stosując uogólniony algorytm Cocksa-Pincha otrzymujemy rozmaitości abelowe z parametrem $\rho \approx 2g \deg w(x_1, \ldots, x_n)$. Aby otrzymać mniejszy parametr ρ używamy rodzin parametrycznych. Dla danego stopnia zanurzeniowego k rodzina parametryczna składa się z pary wielomianów $(r(x), \pi(x))$, gdzie $r(x) \in \mathbb{Q}[x]$ i $\pi(x) \in K[x]$, takich że dla wielu $x_0 \in \mathbb{Z}$ otrzymujemy liczbę pierwszą $r(x_0)$ i liczbę Weila $\pi(x_0)$ w K, która odpowiada rozmaitości abelowej zwykłej ze stopniem zanurzeniowym k względem $r(x_0)$. Dokładna definicja jest następująca.

Definicja 6.1. ([17]) Niech K będzie CM ciałem stopnia $2g$. Mówimy, że para wielomianów $(r(x), \pi(x))$, gdzie $r(x) \in \mathbb{Q}[x]$ i $\pi(x) \in K[x]$, *parametryzuje rodzinę rozmaitości abelowych ze stopniem zanurzeniowym* k jeśli
(1) $q(x) = \pi(x)\overline{\pi}(x) \in \mathbb{Q}[x]$,
(2) $q(x)$ reprezentuje liczby pierwsze,
(3) $r(x)$ reprezentuje liczby pierwsze,
(4) $r(x)$ dzieli $N_{K/\mathbb{Q}}(\pi(x) - 1)$,
(5) $r(x)$ dzieli $\Phi_k(q(x))$.

Trzy pierwsze warunki są konieczne, aby dla nieskończenie wielu $x_0 \in \mathbb{Z}$ otrzymać liczbę pierwszą $r(x_0)$ i liczbę Weila $\pi(x_0)$. Z dwóch ostatnich warunków wynika, że $r(x_0)$ dzieli rząd $\mathrm{N}_{K/\mathbb{Q}}(\pi(x_0) - 1)$ rozmaitości odpowiadającej liczbie Weila $\pi(x_0)$ i k jest stopniem zanurzeniowym względem $r(x_0)$. Parametry ρ rozmaitości abelowych parametryzowanych przez rodzinę $(r(x), \pi(x))$ dążą do parametru ρ rodziny

$$\rho = \frac{g \deg q(x)}{\deg r(x)}.$$

Podobnie jak w uogólnionym algorytmie Cocksa-Pincha rodziny parametryczne możemy otrzymywać przy pomocy wielomianów $w(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ spełniających (5.1). Chcemy otrzymywać rodziny $(r(x), \pi(x))$, gdzie $\pi(x) = w(f_1(x), \ldots, f_n(x))$ dla pewnych $f_i(x) \in \mathbb{Q}[x]$.

Wówczas $(f_1(x),\dots,f_n(x)) \bmod r(x)$ jest rozwiązaniem nad ciałem liczbowym $L=\mathbb{Q}[x]/(r(x))$ układu równań wielomianowych o współczynnikach całkowitych

$$\begin{cases} \mathrm{N}_{K/\mathbb{Q}}(w(x_1,\dots,x_n)-1)=0 \\ \Phi_k(q(x_1,\dots,x_n))=o \end{cases} \tag{6.1}$$

Stąd otrzymujemy następujące uogólnienie algorytmu Brezing-Weng ([6] lub [19, Tw. 6.1]) dla krzywych eliptycznych.

Twierdzenie 6.2. *Niech $k\in\mathbb{Z}_{>0}$, K będzie CM ciałem i $w(x_1,\dots,x_n)\in K[x_1,\dots,x_n]$ spełnia (5.1).*
(1) Znajdź ciało liczbowe L, w którym układ (6.1) ma rozwiązania.
(2) Wyznacz pewien zbiór rozwiązań $Z\subset L^n$ układu (6.1).
(3) Przedstaw L jako ciało ilorazowe $L=\mathbb{Q}[x]/(r(x))$, gdzie $r(x)\in\mathbb{Q}[x]$.
(4) Dla każdego rozwiązania $(a_1,\dots,a_n)\in Z$ weź jego podniesienie $(f_1(x),\dots,f_n(x))\in\mathbb{Q}[x]^n$, gdzie $\deg f_i(x)<\deg r(x)$ dla $i=1,\dots,n$.
(5) Niech $\pi(x)=w(f_1(x),\dots,f_n(x))$.

Jeśli $q(x)=\pi(x)\overline{\pi}(x)$ reprezentuje liczby pierwsze, to $(r(x),\pi(x))$ jest rodziną rozmaitości abelowych ze stopniem zanurzeniowym k o parametrze

$$\rho=\frac{2g\deg w(x_1,\dots,x_n)\max\{\deg f_1(x),\dots,\deg f_n(x)\}}{\deg r(x)}.$$

Stąd otrzymujemy rodziny z parametrem $\rho<2g\deg w(x_1,\dots,x_n)$, chociaż generycznie bliskim tej wartości. Dla krzywych eliptycznych mamy $\rho<2$ jeśli $K=\mathbb{Q}(\sqrt{-d})$ jest ciałem urojonym kwadratowym i $w(x_1,x_2)=x_1+x_2\sqrt{-d}$. Jeśli K jest CM ciałem prymitywnym stopnia 4 i $w(x_1,\dots,x_4)$ jest reflex normą, to otrzymujemy powierzchnie abelowe absolutnie proste z parametrem $\rho<8$. Jeśli $K=\mathbb{Q}(\zeta_s,\sqrt{-d})$ jest CM ciałem stopnia 4 i $w(x_1,x_2)=\zeta_s(x_1+x_2\sqrt{-d})$, to otrzymujemy powierzchnie abelowe proste, które nie są absolutnie proste z parametrem $\rho<4$.

Nietrywialą częścią powyższego algorytmu jest wyznaczenie rozwiązań układu (6.1) w pewnym ciele liczbowym. Ogólnie pewne rozwiązania można znaleźć przy pomocy rugowników, które również pozwalają skonstruować ciało liczbowe L zawierające odpowiednie rozwiązania ([10]). Jednak ta metoda wymaga następnie zapisania ciała L jako ilorazu $L=\mathbb{Q}[x]/(r(x))$ dla wielomianu $r(x)$ o możliwie małych współczynikach (jeśli $r(x)$ ma duże współczynniki, to zwykle wielomian $\pi(x)$, który otrzymujemy ma współczynniki wymierne o dużych mianownikach i $q(x)=\pi(x)\overline{\pi}(x)$ rzadko reprezentuje liczby pierwsze). Aby znaleźć taki wielomian $r(x)$ wykorzystuje

się LLL algortym redukcji krat i w przypadku ciał L wyższych stopni jest to dość wolna metoda w praktyce.

Poniżej podamy efektywne wzory na rozwiązania układu (6.1) w przypadku gdy wielomian $w(x_1,\dots,x_n)$ jest reflex normą lub $w(x_1,x_2) = \zeta_s(x_1+x_2\sqrt{-d})$. Zaczniemy od następującego uproszczenia układu (6.1). Niech K_1 będzie domknięciem normalnym K oraz L ciałem liczbowym zawierającym $\overline{K}(\zeta_k)$. Dla dowolnego k-tego pierwotnego pierwiastka z jedynki ζ_k układ (6.1) sprowadza się do następujących układów

$$\begin{cases} \prod\limits_{\sigma:K\to K_1} w^\sigma(x_1,\dots,x_n) - 1 = 0 \\ q(x_1,\dots,x_n) = \zeta_k \end{cases}$$

Dla dowolnego zanurzenia $\sigma : K \to \overline{K}_1$ mamy $q(x_1,\dots,x_n) = w^\sigma(x_1,\dots,x_n)\overline{w^\sigma}(x_1,\dots,x_n)$. Stąd dla dowolnego σ i ζ_k układ (6.1) możemy rozbić na następujące układy

$$\begin{cases} w^\sigma(x_1,\dots,x_n) = 1 \\ \overline{w^\sigma}(x_1,\dots,x_n) = \zeta_k \end{cases} \tag{6.2}$$

6.1. Rodziny parametryczne otrzymane przy pomocy reflex normy

Poniższa metoda może być traktowna jako alternatywna do metody Freemana [17], który podał inny algorytm oparty na reflex normie otrzymywania rodzin parametrycznych.

Niech K będzie CM ciałem stopnia $2g$ z CM typem prymitywnym Φ i z domknięciem normalnym K_1. Niech $K^* \subset K_1$ będzie reflex ciałem stopnia $2g^*$ względem (K,Φ) z CM typem dualnym $\Phi^* = \{\psi_1,\dots,\psi_{g^*}\}$. W ustalonej bazie $\{b_i\}$ ciała $K^*/\mathbb{Q}$ zapiszmy $\psi_i(\sum x_j b_j) = \sum_j x_j\alpha_{ij}$, gdzie $\alpha_{ij} = \psi_i(b_j) \in K_1$. Wówczas reflex normę możemy przedstawić jako wielomian

$$\mathrm{N}_{\Phi^*}(x_1,\dots,x_{2g^*}) = \big(\sum x_j\alpha_{1j}\big)\cdots\big(\sum x_j\alpha_{g^*j}\big) \in K[x_1,\dots,x_{2g^*}],$$

który spełnia $q(x_1,\dots,x_{2g^*}) = \mathrm{N}_{\Phi^*}(x_1,\dots,x_{2g^*})\overline{\mathrm{N}_{\Phi^*}}(x_1,\dots,x_{2g^*}) \in \mathbb{Q}[x_1,\dots,x_{2g^*}]$. Zapiszmy układ (6.1) z reflex normą

$$\begin{cases} \mathrm{N}_{K/\mathbb{Q}}(\mathrm{N}_{\Phi^*}(x_1,\dots,x_{2g^*}) - 1) = 0 \\ \Phi_k(q(x_1,\dots,x_{2g^*})) = 0 \end{cases} \tag{6.3}$$

Niech L będzie ciałem liczbowym zawierającym $K_1(\zeta_k)$. Po sprowadzeniu do postaci (6.2) powyższy układ rozpada się na na następujące układy dla dowolnego zanurzenia $\varphi : K \to K_1$ i k-tego pierwiastka z jedynki ζ_k

$$\begin{cases} \mathrm{N}^{\varphi}_{\Phi^*}(x_1, \ldots, x_{2g^*}) = 1 \\ \overline{\mathrm{N}^{\varphi}_{\Phi^*}}(x_1, \ldots, x_{2g^*}) = \zeta_k \end{cases}$$

Kładąc $\beta_{ij} = \varphi(\alpha_{ij})$, jest to układ postaci

$$\begin{cases} (\sum x_j\beta_{1j}) \cdots (\sum x_j\beta_{g^*j}) = 1 \\ (\sum x_j\overline{\beta}_{1j}) \cdots (\sum x_j\overline{\beta}_{g^*j}) = \zeta_k \end{cases}$$

Z twierdzenia Dirichleta o niezależności charakterów formy $\varphi\psi_1, \ldots, \varphi\psi_{g^*}, \overline{\varphi}\psi_1, \ldots, \overline{\varphi}\psi_{g^*}$ są liniowe niezależne. Stąd wszystkie rozwiązania w L ostatniego układu otrzymujemy wybierając dowolnie parametry $t_1, \ldots, t_{g^*-1}, s_1, \ldots, s_{g^*-1} \in L^*$ i wyznaczając jedyne rozwiązanie nad L układu równań liniowych

$$\begin{cases} \sum x_j\beta_{1j} = t_1 \\ \vdots \\ \sum x_j\beta_{g^*-1j} = t_{g^*-1} \\ \sum x_j\beta_{g^*j} = 1/t_1 \cdots t_{g^*-1} \\ \sum x_j\overline{\beta}_{1j} = s_1 \\ \vdots \\ \sum x_j\overline{\beta}_{g^*-1j} = s_{g^*-1} \\ \sum x_j\overline{\beta}_{g^*j} = \zeta_k/s_1 \cdots s_{g^*-1} \end{cases}$$

Stąd otrzymujemy następującą postać wszystkich rozwiązań układu (6.3) na ciałem L.

Lemat 6.3. *Wszystkie rozwiązania $(x_1, \ldots, x_{2g^*})$ układu (6.3) nad ciałem liczbowym L zawierającym $K_1(\zeta_k)$ mają następującą postać parame-*

tryczną dla dowolnych $t_i, s_i \in L^*$

$$\begin{bmatrix} x_1 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_{2g^*} \end{bmatrix} = \begin{bmatrix} \beta_{11} & \cdots & \cdots & \cdots & \beta_{12g^*} \\ & & \vdots & & \\ \beta_{g^*1} & \cdots & \cdots & \cdots & \beta_{g^*2g^*} \\ \overline{\beta}_{11} & \cdots & \cdots & \cdots & \overline{\beta}_{12g^*} \\ & & \vdots & & \\ \overline{\beta}_{g^*1} & \cdots & \cdots & \cdots & \overline{\beta}_{g^*2g^*} \end{bmatrix}^{-1} \begin{bmatrix} t_1 \\ \vdots \\ t_{g^*-1} \\ 1/t_1 \cdots t_{g^*-1} \\ s_1 \\ \vdots \\ s_{g^*-1} \\ \zeta_k/s_1 \cdots s_{g^*-1} \end{bmatrix}$$

gdzie ζ_k *jest dowolnym pierwiastkiem z 1 i* $\beta_{ij} = \varphi(\alpha_{ij})$ *dla dowolnego zanurzenia* $\varphi : K \to K_1$.

Przykład 6.4. Podamy rodzinę parametryczną powierzchni abelowych ze stopniem zanurzeniowym $k = 10$ i parametrem $\rho = 6$ dla CM ciała $K = \mathbb{Q}(\zeta_5)$. Do otrzymywania liczb Weila w K użyjemy normy względem tego samego CM typu Φ na K jak w Przykładzie 4.1. W powyższym lemacie bierzemy $L = \mathbb{Q}(\zeta_{10}) = \mathbb{Q}(\zeta_5)$, zapisujemy $L = \mathbb{Q}[x]/(\Phi_{10}(x))$ i przyjmujemy $t_1 = 1$ i $s_1 = \zeta_{10}$. Otrzymujemy następującą rodzinę powierzchni abelowych

$$\begin{aligned} r(x) &= \frac{1}{5}\Phi_{10}(x) = \frac{1}{5}(x^4 - x^3 + x^2 - x + 1), \\ \pi(x) &= \frac{1}{25}(-2\zeta_5^3 - \zeta_5^2 - 2\zeta_5)x^6 + \frac{1}{25}(9\zeta_5^3 + 6\zeta_5^2 + 11\zeta_5 + 4)x^5 \\ &\quad + \frac{1}{5}(-2\zeta_5^3 - 2\zeta_5^2 - 3\zeta_5 - 4)x^4 + \frac{1}{5}(\zeta_5^3 + 2\zeta_5^2 + 2\zeta_5 + 6)x^3 \\ &\quad + \frac{1}{5}(-3\zeta_5^3 - 3\zeta_5^2 - 5\zeta_5 - 5)x^2 + \frac{1}{25}(3\zeta_5^3 + 4\zeta_5^2 + 3\zeta_5 + 15)x \\ &\quad + \frac{1}{25}(-6\zeta_5^3 - 4\zeta_5^2 - 9\zeta_5 - 6). \end{aligned}$$

(współczynnik 1/5 przy $\Phi_{10}(x)$ został dobrany, aby wielomian $r(x)$ reprezentował liczby pierwsze). Ponieważ $\deg r(x) = 4$, aby otrzymać parametry powierzchni abelowej dla liczby pierwszej r około 160 bitowej powinniśmy jej szukać jako wartości rodziny na liczbach około 40 bitowych. Otrzymujemy np. następujące parametry powierzchni abelowej:

$x = 2^{41} + 122,$

$r = 467680524049462379265341443563849146990451355615 1$
(161 bitowa liczba pierwsza),

$q = 102293456564484173143227647315381238516094559060110416697138646037491288509997451320507386866442069603422190212059936958111847958211788729723539661$

Podobnie jak w Przykładzie 4.1 znajdujemy krzywą, której jakobian realizuje powyższe parametry

$$y^2 = x^5 + 2.$$

6.2. Rodziny parametryczne dla CM ciał postaci $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$

Podamy teraz wzory na rozwiązania układu (6.1) dla $w(x, y) = \zeta_s(x + y\sqrt{-d})$ i $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$. Zatem układ ma postać

$$\begin{cases} \mathrm{N}_{K/\mathbb{Q}}(\zeta_s(x + y\sqrt{-d}) - 1) = 0 \\ \Phi_k\big(x^2 + dy^2\big) = \ \ 0 \end{cases} \tag{6.4}$$

Lemat 6.5. *Niech L będzie ciałem liczbowym zawierającym $K(\zeta_k)$. Jeśli $\sqrt{-d} \notin \mathbb{Q}(\zeta_s)$, to dla dowolnych pierwotnych pierwiastków z jedynki ζ_s, ζ_k układ (6.4) ma rozwiązania postaci*

$$x = \frac{\zeta_s^{-1} + \zeta_k\zeta_s}{2}, \quad y = \pm\frac{\zeta_s^{-1} - \zeta_k\zeta_s}{2\sqrt{-d}}. \tag{6.5}$$

Jeśli $\sqrt{-d} \in \mathbb{Q}(\zeta_s)$, to jedna z tych par jest rozwiązaniem układu (6.4).

Proof. Zgodnie z (6.2) dla dowolnego $\sigma \in \mathrm{Aut}(K)$ i ζ_k układ (6.4) rozpada sią na następujące układy liniowe

$$\begin{cases} \ \ \sigma(\zeta_s)\big(x + y\sigma(\sqrt{-d})\big) = 1 \\ \sigma(\zeta_s^{-1})\big(x - y\sigma(\sqrt{-d})\big) = \zeta_k \end{cases}$$

Stąd

$$\begin{cases} x = \dfrac{\sigma(\zeta_s^{-1}) + \zeta_k \sigma(\zeta_s)}{2} \\ y = \dfrac{\sigma(\zeta_s^{-1}) - \zeta_k \sigma(\zeta_s)}{2\sigma(\sqrt{-d})} \end{cases}$$

Jeśli $\sqrt{-d} \notin \mathbb{Q}(\zeta_s)$, to każdy automorfizm ciała $\mathbb{Q}(\zeta_s)$ ma dwa rozszerzenia na K, więc rozwiązania są dokładnie postaci (6.5). Jeśli $\sqrt{-d} \in \mathbb{Q}(\zeta_s)$, to automorfizm σ jest jednoznacznie wyznaczony przez wartości na ζ_s. □

Przykład 6.6. W CM ciele $K = \mathbb{Q}(\zeta_8)$ stopnia 4 zawierającym $\sqrt{-2}$ użyjemy $w(x, y) = \zeta_8(x + y\sqrt{-2})$ do otrzymywania liczb Weila. Dla stopnia zanurzeniowego $k = 16$ otrzymujemy rodzinę z parametrem $\rho = 3.5$

$$\begin{aligned} r(x) &= \frac{1}{2}(x^8 + 1), \\ \pi(x) &= \frac{-1}{2}\zeta_8 x^7 - \frac{1}{2}\zeta_8 x^6 + \frac{1}{4}(\zeta_8^2 - 1)x^5 + \frac{1}{4}(-\zeta_8^2 + 1)x^4 + \frac{1}{4}(\zeta_8^2 - 1)x \\ &\quad + \frac{1}{4}(-\zeta_8^2 + 1), \end{aligned}$$

Dostajemy np. następujące parametry powierzchni abelowej

$x = 2^{20} + 2^{17} + 7477,$

$r = 39443151536018061988984356400108933448791503906 26$

(160 bitowa liczba pierwsza)

$q = 27598854348512437317747455665949090055277857991774554474931270244336463109 3882533297$

Aby zrealizować liczby Weila w K jako jakobiany krzywych genusu 2, na ogół wystarczy użyć krzywych $C_a : y^2 = x^5 + ax$, które mają automorfizm rzędu 8, $(x, y) \mapsto (\zeta_8^2 x, \zeta_8 y)$. Podobnie jak w Przykładzie 4.1 sprawdzając kolejne $a \in \mathbb{F}_p$ znajdujemy krzywą, której jakobian ma powyższe parametry

$$y^2 = x^5 + 14x.$$

Powyższa metoda zastosowana do CM ciała $K = \mathbb{Q}(\zeta_8)$ jest alternatywna do metody Kawazoe i Takahashi [27], którzy podali metodę konstruowania krzywych postaci $y^2 = x^5 + ax$ z danym stopniem zanurzeniowym opartą na wzorach na rząd jakobianu takich krzywych.

Przykład 6.7.. Niech $K = \mathbb{Q}(\zeta_{12}) = \mathbb{Q}(i, \sqrt{-3})$ i $w(x, y) = i(x + y\sqrt{-3})$. Dla $k = 12$ zapiszmy ciało $L = K$ jako iloraz $L = \mathbb{Q}[x]/(r_0(x))$, gdzie $r_0(x) = x^4 + 2x^3 + 6x^2 - 4x + 4$ otrzymujemy jako wielomian minimalny elementu $\zeta_{12} - \zeta_{12}^2 + \zeta_{12}^3$. Aby otrzymać jak najmniejszy parametr ρ próbujemy różnych reprezetacji ciała L jako ilorazu $\mathbb{Q}[x]/(r(x))$. Wielomiany $r(x)$ możemy otrzymywać jako wielomiany minimalne elementów prymitywnych w K (taka metoda dla krzywych eliptycznych została wprowadzona w [26]). Znajdujemy rodzinę powierzchni abelowych ze stopniem zanurzeniowym $k = 12$ i parametrem $\rho = 2$:

$$r(x) = \frac{1}{36}(x^4 + 2x^3 + 6x^2 - 4x + 4),$$
$$\pi(x) = \frac{i}{12}\big(x^2(-\sqrt{-3} + 1) - 2x(\sqrt{-3} + 1) - 6\sqrt{-3} - 2\big).$$

Dostajemy np. następujące parametry powierzchni abelowej

$$x = 87960930234340,$$

$$r = 16628640860680566448242922374371741145126878909008301229$$

(180 bitowa liczba pierwsza),

$$\pi = \frac{i}{2}(128952087461504213424246115 3 - 128952087461510077486261738 1\sqrt{-3}),$$

$$q = 16628640860680566448242922387266949891278180041809967 23,$$

Stosując Algorytm (4.3) znajdujemy krzywą, której jakobian realizuje powyższe parametry

$$y^2 = 3x^6 + 399087380656333594757830137294406797390676321003439214x^3$$
$$+ 840318388709976017122087137087102952585808061504841608$$

Literatura

[1] P.S.L.M. Barreto, M. Naehrig, *Pairing-friendly elliptic curves of prime order*, in Selected Areas in Cryptography–SAC 2005, Lecture Notes in Computer Science, vol. 3897 (Springer, Berlin, 2006), pp. 319–331.

[2] P. Bateman, R. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comput. 16, 363–367 (1962).

[3] J. Belding, R. Bröker, A. Enge, K. Lauter, *Computing Hilbert class polynomials*, Algorithmic Number Theory Symposium-ANTS VIII (A. J. van der Poorten and A. Stein, eds.), Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 282–295.

[4] D. Boneh, M. Franklin, *Identity-based encryption from the Weil pairing*, In Advances in Cryptology Crypto 2001. LNCS, vol. 2139, pp. 213–229. Springer, Berlin (2001). Full version: SIAM J. Comput. 32(3), 586–615 (2003).

[5] D. Boneh, B. Lynn, H. Shacham, *Short signatures from the Weil pairing*, In Advances in Cryptology Asiacrypt 2001, LNCS, vol. 2248, pp. 514–532. Springer, Berlin (2002). Full version: J. Cryptol. 17, 297–319 (2004).

[6] F. Brezing, A. Weng, *Elliptic curves suitable for pairing based cryptography*, Des. Codes Cryptogr. 37, 133–141 (2005).

[7] R. Bröker, *A p-adic algorithm to compute the Hilbert class polynomial*, Math. Comp. 77 (2008), 2417–2435.

[8] R. Bröker, P. Stevenhagen, *Efficient CM-constructions of elliptic curves over finite fields*, Math. Comp. 76 (2007), 2161–2179.

[9] D. Cox, *Primes of the form $x^2 + ny^2$. Fermat, Class Field Theory and Complex Multiplication*, John Wiley & Sons (1989).

[10] R. Dryło, *A New Method for Constructing Pairing-Friendly Abelian Surfaces*, In: Pairing-Based Cryptography – Pairing 2010. LNCS, vol. 6487, pp. 298-311. Springer, Heidelberg (2010).

[11] R. Dryło, *Constructing Pairing-Friendly Genus 2 Curves with Split Jacobian*, Lecture Notes in Computer Sciences (INDOCRYPT 2012) 7668 (2012), 437-458.

[12] R. Dryło, Z. Jelonek, *Krzywe eliptyczne z zadaną grupą endomorfizmów i podgrupą ustalonego rzędu*, Materiały z konferencji „Kryptografia i Bezpieczeństwo Informacji", Warszawa 2014.

[13] A. Enge, *The complexity of class polynomial computation via floating point approximations*, Math. Comp. 78 (2009), 1089–1107.

[14] K. Eisentrager, K. Lauter, *A CRT algorithm for constructing genus 2 curves over finite fields*, in Proceedings of AGCT 2005: Arithmetics, Geometry, and Coding Theory – Société Mathématique de France, 2011.

[15] D. Freeman, *Constructing pairing-friendly elliptic curves with embedding degree 10*, in Algorithmic Number Theory Symposium–ANTS-VII. Lecture Notes in Computer Science, vol. 4076 (Springer, Berlin, 2006), pp. 452–465.

[16] D. Freeman, *Constructing pairing-friendly genus 2 curves with ordinary Jacobians*,In Pairing-Based Cryptography – Pairing 2007, LNCS, vol. 4575, pp. 152–176. Springer, Verlag (2007).

[17] D. Freeman, *A generalized Brezing-Weng algorithm for constructing pairing-friendly ordinary abelian varieties*, In: Pairing-Based Crypto-

graphy – Pairing 2008, LNCS, vol. 5209, pp. 46–163, Springer, Heidelberg (2008).
[18] D. Freeman, T. Satoh, *Constructing pairing-friendly hyperelliptic curves using Weil restriction*, J. Number Theory 131, 959–983 (2011).
[19] D. Freeman, M. Scott, E. Teske, *A taxonomy of pairing-friendly elliptic curves*, J. Cryptol. 23, 224–280 (2010).
[20] D. Freeman, P. Stevenhagen, M. Streng, *Abelian varieties with prescribed embedding degree*, In: Algorithmic Number Theory – ANTS VIII. LNCS, vol. 5011, pp. 60–73, Springer, Heidelberg (2008).
[21] S. Galbraith, *Supersingular curves in cryptography*, In ASIACRYPT 2001, LNCS, 2248, pp. 495–513. Springer, Berlin (2001).
[22] S. Galbraith, F. Hess, F. Vercauteren, *Hyperelliptic pairings*, In Pairing-based cryptography – Pairing 2007, LNCS vol. 4575 108–131. Springer, Berlin, (2007).
[23] E. Howe, H. Zhu, *On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field*, J. Number Theory 92, 139–163 (2002).
[24] J. Igusa, *Arithmetic Variety of Moduli for Genus Two*, Ann. Math. 72, 612–649 (1960).
[25] A. Joux, *A one round protocol for tripartite Diffie–Hellman*, In Algorithmic Number Theory Symposium – ANTS-IV. LNCS, vol. 1838, pp. 385–393, Springer, Berlin (2000), Full version: J. Cryptol. 17, 263–276 (2004).
[26] E. Kachisa, E. Schaefer, M. Scott, *Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field*, In Pairing-Based Cryptography–Pairing 2008, LNCS, vol. 5209, pp. 126–135. Springer, Heidelberg (2008).
[27] M. Kawazoe, T. Takahashi, *Pairing-friendly ordinary hyperelliptic curves with ordinary Jacobians of type* $y^2 = x^5 + ax$, In: Pairing-Based Cryptography – Pairing 2008. LNCS, vol. 5209, pp. 164–177. Springer, Heidelberg (2008).
[28] S. Lang, *Elliptic functions*, Springer, 1987.
[29] A. Menezes, T. Okamoto, S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Trans. Inf. Theory 39, 1639–1646 (1993).
[30] J.F. Mestre, *Construction de courbes de genre 2 à partir de leurs modules*, In Effective methods in algebraic geometry (Castiglioncello, 1990), pages 313–334. Birkhäuser, Boston, MA (1991).
[31] V.S. Miller, *The Weil pairing, and its efficient calculation*, Journal of Cryptology, 17, 235–261, 2004.

[32] J.S. Milne, *Abelian varieties*, In G. Cornell, J. Silverman, (eds.) Arithmetic Geometry 103–150. Springer, New York (1986).
[33] J.S. Milne, *Complex multiplication* http://www.jmilne.org/math/CourseNotes/
[34] A. Miyaji, M. Nakabayashi, S. Takano, *New explicit conditions of elliptic curve traces for FR-reduction*, IEICE Trans. Fundam. E84-A(5), 1234–1243 (2001).
[35] D. Mumford, *Abelian varieties*, Oxford University Press 1970.
[36] F. Oort, *Abelian varieties over finite fields. Higher-dimensional varieties over finite fields*, Summer school in Göttingen, pp. 66, June 2007.
[37] K. Rubin, A. Silverberg, *Using abelian varieties to improve pairing-based cryptography*, J. Cryptol. 22, 330-364 (2009).
[38] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, 1998.
[39] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151. Springer-Verlag, New York (1994).
[40] M. Streng, *Complex multiplication of abelian surfaces*, PhD thesis, Universiteit Leiden (2010).
[41] M. Streng, *Computing Igusa Class Polynomials Mathematics of Computation*, Vol. 83, pp 275–309, (2014).
[42] A. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Math. Comp. 80, 501–538 (2011).
[43] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini*, (d'aprés T. Honda.) Séminarie Bourbaki 1968/69, exposé 352, Lect. Notes in Math., vol. 179, pp. 95–110. Springer (1971).
[44] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Inventiones Mathematicae 2 (1966).
[45] W.C. Waterhouse, J.S. Milne, *Abelian varieties over finite fields*, Proc. Symp. Pure Math. 20, 53–64 (1971).

CONSTRUCTING PAIRING-FRIENDLY GENUS 2 CURVES

Abstract. For applications in pairing-based cryptography we need special curves for which the Weil and Tate pairings can be efficiently computed. Such curves, commonly called pairing-friendly, require specific constructions. In practice we mainly use elliptic curves or hyperelliptic curves of genus 2. Methods for constructing pairing-friendly curves are based on the complex multiplication (CM) method, and thus are restricted to curves whose endomorphism ring of the Jacobian is generated by suitably small

numbers. To construct such a curve one first determines parameters of its Jacobian, which are usually given by Weil numbers for genus 2 curves, and then one uses the CM method to find a curve equation. Methods for constructing pairing-friendly elliptic curves were gathered and described in a coherent language by Freeman, Scott and Teske. There are several approaches to construct pairing-friendly genus 2 curves the first of which were developed by Freeman, Stevenhagen, and Streng, Kawazoe-Takahashi, and Freeman-Satoh. In this paper we describe an approach based on the idea of the author, where we use suitable polynomials of several variables to obtain as their values Weil numbers corresponding to Jacobians of pairing-friendly genus 2 curves. This approach can be used to construct both genus 2 with absolutely simple Jacobian, and with simple, but not absolutely simple. We give explicit formulas, which determine parametric families of pairing-friendly genus 2 curves.

Keywords: pairing-based cryptography, pairing-friendly curves, the Weil and Tate pairings, CM method, Weil numbers.