Konstruowanie krzywych eliptycznych z podgrupą danego rzędu i z danym pierścieniem endomorfizmów

Robert Dryło[*], **Zbigniew Jelonek**[**]

[*] Szkoła Główna Handlowa, Aleja Niepodległości 162, 02-554 Warszawa
[*,**] Instytut Matematyczny PAN, ul. Śniadeckich 8, 00-950 Warszawa
rdrylo@sgh.waw.pl Z.Jelonek@impan.pl

Streszczenie. Metoda mnożeń zespolonych (CM metoda) pozwala skonstruować krzywą eliptyczną nad ciałem skończonych, której pierścień endomorfizmów jest ordynkiem maksymalnym w ciele urojonym kwadratowym o odpowiednio małym wyróżniku. Stosując CM metodę Lay i Zimmer oraz Bröker i Stevenhagen podali metodę konstruowania krzywej eliptycznej danego rzędu n nad pewnym ciałem prostym. Ich metoda ma heurystycznie wielomianowy czas działania, jeśli n nie ma zbyt wielu dzielników pierwszych. W tym opracowaniu pokażemy, że w analogiczny sposób można skonstruować krzywą eliptyczną, która zawiera podgrupę danego rzędu r i ma dany pierścień endomorfizmów o odpowiednio małym wyróżniku. Przy pewnych heurystycznych założeniach metoda ma wielomianowy czas działania, jeśli r jest liczbą pierwszą.
Słowa kluczowe: krzywe eliptyczne danego rzędu, CM metoda, algorytm Cornacchii, pierścień endomorfizmów.

1. Wstęp

Metoda mnożeń zespolonych (CM metoda) pozwala konstruować krzywe eliptyczne rzędu n nad ciałem skończonym $\mathbb{F}_q$, których pierścień endomorfizmów jest ordynkiem w ciele urojonym kwadratowym $K = \mathbb{Q}(\sqrt{-d})$ o odpowiednio małym wyróżniku. CM metoda została wprowadzona do zastosowań w [1], aby przyspieszyć generowanie krzywych eliptycznych używanym przy dowodzeniu pierwszości.

W kryptografii najczęściej stosuje się krzywe eliptyczne, których rząd n jest liczbą pierwszą lub $r = n/h$ jest liczbą piewszą dla małego h. Jeden z problemów, którego rozwiązanie opisali Lay i Zimmer [12], dotyczy konstruowania krzywej eliptycznej danego rzędu n nad pewnym ciałem prostym $\mathbb{F}_p$. Poszukiwanie takiego ciała polega na sprawdzaniu dla kolejnych liczb bezkadratowych d czy równanie $\mathbb{N}(\alpha) = \alpha\bar{\alpha} = n$ ma rozwiązania $\alpha \in \mathcal{O}_K$, takie że $p = \mathbb{N}(\alpha + 1)$ jest liczbą pierwszą, gdzie $\mathcal{O}_K$ jest pierścieniem liczb algebraicznych całkowitych w $K = \mathbb{Q}(\sqrt{-d})$. Jeśli otrzymamy liczbę pierwszą p, to istnieje krzywa eliptyczna $E/\mathbb{F}_p$ rzędu n, którą można skonstruować stosując CM metodę jeśli d jest odpowiednio małe. Bröker i Stevenhagen [4] pokazali, że można oczekiwać znalezienia liczby pierwszej

p dla $d = O(\ln^2 r)$ i podali dokładny opis algorytmu rozwiązującego ten problem, który ma koszt wielomianowy dla liczb n, których liczba dzielników pierwszych jest $\leq \ln \ln n$.

W tym opracowaniu zajmujemy się następującym analogicznym problem:

Problem 1.1. Niech $K = \mathbb{Q}(\sqrt{-d})$ będzie ciałem urojonym kwadratowym oraz r liczbą pierwszą. Skonstruować krzywą eliptyczną E nad pewnym ciałem prostym $\mathbb{F}_p$, która zawiera podgrupę rzędu r i $\mathrm{End}(E) = \mathcal{O}_K$.

Krzywe z danym pierścieniem endomorfizmów mogą być użyteczne przy mnożeniu punktów przez skalary. Dla krzywych, które mają efektywnie obliczalne endomorfizmy istnieją efektywniejsze metody mnożenia punktów [9], [8], [10]. Na przykład, krzywe $y^2 = x^3 + a$ i $y^2 = x^3 + ax$ mają odpowiednio automorfizmy postaci $(x, y) \to (\zeta_3 x, y)$ i $(x, y) \to (-x, iy)$.

Poszukiwanie rozwiązania Problemu 1.1 polega na sprawdzaniu dla kolejnych $h \in \mathbb{N}$ czy równanie $\mathrm{N}(\alpha) = hr$ ma rozwiązanie $\alpha \in \mathcal{O}_K$, takie że $p = \mathrm{N}(\alpha + 1)$ jest liczbą pierwszą. Jeśli to równanie ma rozwiązania dla $h < r$, to r musi rozpadać się w K. Wówczas przy pewnych heurystycznych założeniach można oczekiwać znalezienia rozwiązania dla $h \leq O(\sqrt{d} \ln^{1+\varepsilon}(\sqrt{d}r))$, gdzie $\varepsilon > 0$ (Stwierdzenie 5.1). Metodę można w oczywisty sposób rozszerzyć na liczby r, które nie są pierwsze, ale znana jest faktoryzacja r, która jest wymagana do rozwiązania równania $\mathrm{N}(\alpha) = hr$.

W rozdziałach 2 i 3 przypominamy podstawowe fakty o krzywych eliptycznych i CM metodzie. W rozdziale 4 szczegółowo opisujemy metodę rozwiązywania równania $\mathrm{N}(\alpha) = n$. W rozdziale 5 podajemy algorytm rowiązywania Problemu 1.1. Podajemy również prostszą wersję gdy $\mathcal{O}_K$ jest dziedziną ideałów głównych. Wykorzystaliśmy program Magma, aby zaimplementować te algortymy i podać przykłady krzywych.

2. Krzywe eliptyczne

Endomorfizm Frobeniusa stopnia q na krzywej eliptycznej $E/\mathbb{F}_q$ spełnia równanie charakterystyczne

$$\pi_q^2 - t\pi_q + q = 0,$$

gdzie liczbę $t \in \mathbb{Z}$ nazywamy śladem krzywej. Ślad ma następujące własności:

(1) $|t| \leq 2\sqrt{q}$

(2) $\#E(\mathbb{F}_q) = q + 1 - t$.

W szczególności stąd $(\sqrt{q}-1)^2 \leq \#E(\mathbb{F}_q) \leq (\sqrt{q}+1)^2$.

Krzywą E nazywamy zwykłą jeśli $\gcd(t,q) = 1$. Jest to równoważne, temu że krzywa ma niezerowe punkty p-torsyjne nad $\overline{\mathbb{F}}_p$. Krzywą, która nie jest zwykła nazywamy spersingularną. Jeśli E jest krzywą zwykłą, to wyróżnik równania charakterystycznego możemy zapisać w postaci $t^2 - 4q = -dy^2$, gdzie $d \in \mathbb{N}$ jest liczbą bezkwadratową oraz $y \in \mathbb{Z}$. Wówczas endomorfizm Frobeniusa możemy utożsamiać z jednym z pierwiastków $\pi = \frac{t \pm y\sqrt{-d}}{2}$ równania charakterystycznego oraz pierścień endomorfizmów $\mathrm{End}(E)$ jest izomorficzny z ordynkiem w ciele urojonym kwadratowym $K = \mathbb{Q}(\sqrt{-d})$.

Ordynki w K są podpierścieniami $\neq \mathbb{Z}$ pierścienia liczb algebraicznych całkowitych. Dla ustalonego $c \in \mathbb{Z}_{>0}$ są to podpierścienie postaci

$$\mathcal{O}_c = \begin{cases} \{x + yc\sqrt{-d} \mid x, y \in \mathbb{Z}\}, d \equiv 1, 2 \bmod 4 \\ \{x + yc\dfrac{1+\sqrt{-d}}{2} \mid x, y \in \mathbb{Z}\}, d \equiv 3 \bmod 4. \end{cases} \tag{2.1}$$

Jeśli $c_1 \mid c_2$, to $\mathcal{O}_{c_2} \subset \mathcal{O}_{c_1}$. Ordynek maksymalny $\mathcal{O}_1$, który oznaczamy przez $\mathcal{O}_K$, składa się z liczb algebraicznych całkowitych w K.

Niech $\mathrm{N} : K \to \mathbb{Q}$ będzie normą, $\mathrm{N}(\alpha) = \alpha\bar{\alpha} = x^2 + dy^2$ dla $\alpha = x + y\sqrt{-d}$, $x, y \in \mathbb{Q}$. Jeśli $\pi \in \mathcal{O}_K$ odpowiada endomorfizmowi Frobeniusa, to $(x - \pi)(x - \bar{\pi}) = x^2 - tx + q$. Stąd $t = \pi + \bar{\pi}$,

$$q = \mathrm{N}(\pi)$$

oraz z (2) wynika, że

$$\#E(\mathbb{F}_q) = \mathrm{N}(\pi - 1). \tag{2.2}$$

Odwrotnie z Twierdzenia 3.1 wynika, że jeśli $\pi \in \mathcal{O}_K$ spełnia $\pi\bar{\pi} = q$ i $t = \pi + \bar{\pi}$ jest względnie pierwsza z q, to istnieje krzywa eliptyczna zwykła $E/\mathbb{F}_q$, taka że $\mathrm{End}(E) = \mathcal{O}_K$ oraz π odpowiada jej endomorfizmowi Frobeniusa. W szczególności rzędy krzywych eliptycznych zwykłych nad $\mathbb{F}_q$ są dokładnie liczbami $n \in [(\sqrt{q}-1)^2, (\sqrt{q}+1)^2]$, takimi że $\gcd(t,q) = 1$, gdzie $t = q + 1 - n$.

Uwaga. Powyższy fakt jest szczególnym przypadkiem ogólnego twierdzenia Hondy i Tate, które mówi, że istnieje bijekcja między klasami isogenicznych rozmaitości abelowych prostych nad $\mathbb{F}_q$, a klasami sprzężonych

liczb q-Weila (liczbę algebraiczną całkowitą π nazywamy liczbą q-Weila, jeśli $q = \varphi(\pi)\overline{\varphi(\pi)}$ dla każdego zanurzenia $\varphi : \mathbb{Q}(\pi) \to \mathbb{C}$).

Jeśli wiemy, że pierścień endomorfizmów krzywej eliptycznej $E/\mathbb{F}_q$ jest ordynkiem w ciele urojonym kwadratowym $K = \mathbb{Q}(\sqrt{-d})$, to możemy dużo efektywniej niż przy pomocy algorymu Schoofa [13], [14], obliczyć rząd krzywej $\#E(\mathbb{F}_q)$. Możemy znaleźć rozwiązania równania $N(\pi) = q$ w $\mathcal{O}_K$ i sprawdzić czy dla losowo wybranego punktu $P \in E(\mathbb{F}_q)$ mamy $nP = 0$, gdzie $n = \mathrm{N}(\pi - 1)$. Wówczas z dużym prawdopodobieństwem n jest rzędem E.

3. Metoda mnożeń zespolonych

Następujące twierdzenie jest wnioskiem z twierdzeń Deuringa.

Twierdzenie 3.1. *Niech $K = \mathbb{Q}(\sqrt{-d})$ będzie ciałem urojonym kwadratowym oraz p liczbą pierwszą. Wówczas istnieją krzywe eliptyczne zwykłe nad $\overline{\mathbb{F}}_p$, takie że $\mathrm{End}(E) = \mathcal{O}_K$ dokładnie wtedy, gdy p rozpada się w K. Takie krzywe istnieją nad ciałem $\mathbb{F}_q$, gdzie $q = p^m$ i $m > 0$ jest najmniejszą liczbą, taką że ideał P^m jest główny, gdzie $P \subset \mathcal{O}_K$ jest ideałem pierwszym leżącym nad p (wówczas generator P^m odpowiada endomorfizmowi Frobeniusa π_q). Wielomian klas Hilberta $H_K(x) \bmod p$ ma w $\mathbb{F}_q$ wszystkie pierwiastki, które są dokładnie j-niezmiennikami krzywych eliptycznych $E/\overline{\mathbb{F}}_p$ z $\mathrm{End}(E) = \mathcal{O}_K$.*

Następujący algorytm pozwala skonstruować krzywe eliptyczne zwykłe danego rzędu, takie że $\mathrm{End}(E)$ jest ordynkiem maksymalnym w ciele urojonym kwadratowym $K = \mathbb{Q}(\sqrt{-d})$ o odpowiednio małym wyróżniku.

Algorytm 3.2. Input: Potęga liczby pierwszej q, $n \in [(\sqrt{q}-1)^2, (\sqrt{q}+1)^2]$, taka że $t^2 - 4q = -dy^2$, gdzie $d, y \in \mathbb{Z}_{>0}$, $d \neq 1, 3$ jest bezkwadratowa oraz $t = q + 1 - n$.
Output: Krzywa eliptyczna zwykła $E/\mathbb{F}_q$ rzędu n.

(1) Oblicz wielomian klas Hilberta $H_K(x) \in \mathbb{Z}[x]$ ciała urojonego kwadratowego $K = \mathbb{Q}(\sqrt{-d})$.
(2) Wyznacz pierwiastek $j \in \mathbb{F}_q$ wielomianu $H_K(x) \bmod p$.
(3) Utwórz krzywą eliptyczną $E : y^2 = x^3 + ax - a$, gdzie $a = \frac{27j}{4(1728-j)}$.
(4) Wybierz losowy punkt $P \in E(\mathbb{F}_q)$.
(5) Jeśli $nP = 0$, zwróć E. W przeciwnym razie zwróć skręcenie kwadratowe $E' : y^2 = x^3 + ac^2x - ac^3$, gdzie $c \in {\mathbb{F}_q}^* \setminus (\mathbb{F}_q^*)^2$ jest nieresztą kwadratową w $\mathbb{F}_q$.

Uwaga 3.3. Powyższy algorytm można łatwo rozszerzyć dla $d = 1, 3$ dołączając wzory na skręcenia takich krzywych. W tym przypadku istnieje alternatywna prosta metoda konstruowania krzywych rzędu n. Dla $d = 1, 3$ mamy odpowiednio $\mathcal{O}_K = \mathbb{Z}[i]$ lub $\mathbb{Z}[\zeta_3]$. Są to dziedziny ideałów głównych, więc liczba klas ciała K jest równa jeden. Stąd wszystkie krzywe eliptyczne z $\mathrm{End}(E) = \mathbb{Z}[i]$ lub $\mathbb{Z}[\zeta_3]$ są izomorficzne. Krzywe

(1) $E_a : y^2 = x^3 + ax$,
(2) $E_a : y^2 = x^3 + a$

mają automorfizmy odpowiednio stopnia 4 i 3 dane wzorem $(x, y) \mapsto (-x, iy)$ i $(x, y) \mapsto (\zeta_3 x, y)$. Stąd jeśli te krzywe są zwykłe, to odpowiednio $\mathrm{End}(E_a) = \mathbb{Z}[i]$ lub $\mathrm{End}(E_a) = \mathbb{Z}[\zeta_3]$. Krzywe (1) i (2) są zwykłe nad $\mathbb{F}_p$ dokładnie wtedy, gdy odpowiednio $p \equiv 1 \bmod 4$ lub $p \equiv 1 \bmod 3$ (tj. p rozpada się w $\mathbb{Z}[i]$ lub $\mathbb{Z}[\zeta_3]$).

Aby w praktyce znaleźć krzywą rzędu n z $d = 1, 3$ wystarczy na ogół sprawdzać czy dla kolejnych małych $a \in \mathbb{F}_q^*$ i dla losowego punktu $P \in E_a(\mathbb{F}_q)$ mamy $nP = 0$.

4. Rozwiązywanie równania $N(\alpha) = n$

Niech $K = \mathbb{Q}(\sqrt{-d})$ będzie ciałem urojonym kwadratowym, gdzie $d \in \mathbb{N}$ jest liczbą bezwkadratową. Podamy własności pierścienia $\mathcal{O}_K$ liczb algebraicznych całkowitych w K, które pozwolą wyznaczć wszystkie rozwiązania $\alpha \in \mathcal{O}_K$ równania $\mathrm{N}(\alpha) = n$.

Pierścień $\mathcal{O}_K$ ma bazę $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$, gdzie

$$\omega = \begin{cases} \sqrt{-d}, & d \equiv 1, 2 \bmod 4 \\ (1 + \sqrt{-d})/2, & d \equiv 3 \bmod 4. \end{cases} \tag{4.1}$$

Wielomianem minimalnym ω jest

$$f_\omega = \begin{cases} x^2 + d, & d \equiv 1, 2 \bmod 4. \\ x^2 - x + \dfrac{1+d}{4}, & d \equiv 3 \bmod 4. \end{cases} \tag{4.2}$$

Wyróżnikiem ciała K jest

$$D = \begin{vmatrix} 1 & \omega \\ 1 & \bar{\omega} \end{vmatrix}^2 = \begin{cases} -4d, & d \equiv 1, 2 \bmod 4 \\ -d, & d \equiv 3 \bmod 4. \end{cases} \tag{4.3}$$

Wyróżnik D jest równy wyróżnikowi wielomianu f_ω.

Pierścień $\mathcal{O}_K$ można traktować jako 2-wymiarową kratę dyskretną w $\mathbb{C}$. W szczególności dla $n \in \mathbb{N}$ istnieje skończenie wiele liczb $\alpha \in \mathcal{O}_K$ o module $\sqrt{n}$, które są dokładnie rozwiązaniami równania $\mathrm{N}(\alpha) = n$.

Grupa jedności $\mathcal{O}_K^*$ składa się z liczb $\alpha \in \mathcal{O}_K$ o normie $\mathrm{N}(\alpha) = 1$. Jest to grupa skończona, więc jedności są pierwiastkami z jedynki. Dla k-tego pierwotnego pierwiastka z jedynki $\zeta_k \in \mathbb{C}$ ciało $\mathbb{Q}(\zeta_k)$ ma stopień $\varphi(k)$. Mamy $\varphi(k) = 2$ dla $k = 3, 4, 6$. Stąd grupa jedności jest postaci

$$\mathcal{O}_K^* = \begin{cases} \pm 1, & d \neq 1, 3 \\ \pm 1, \pm i, & d = 1 \\ \pm 1, \pm\zeta_3, \pm\zeta_3^2, & d = 3. \end{cases}$$

Podamy teraz rozkład liczby pierwszej p na iloczyn ideałów pierwszych w $\mathcal{O}_K$.

(1) Jeśli $f_\omega(x) \bmod p \equiv (x - a_1)(x - a_2) \bmod p$ ma dwa różne pierwiastki w $\mathbb{F}_p$, gdzie $a_1, a_2 \in \mathbb{Z}$, to p rozpada się w $\mathcal{O}_K$ na iloczyn dwóch ideałów pierwszych. Wówczas $p\mathcal{O}_K = P\overline{P}$, gdzie $P = (p, \omega - a_1)$, $\overline{P} = (p, \omega - a_2)$ oraz $\mathbb{F}_p = \mathcal{O}_K/P = \mathcal{O}_K/\overline{P}$.

(2) Jeśli $f_\omega(x) \bmod p$ jest nierozkładalny nad $\mathbb{F}_p$, to p pozostaje liczbą pierwszą w $\mathcal{O}_K$. Wówczas $p\mathcal{O}_K = P$ jest ideałem pierwszym oraz $\mathbb{F}_{p^2} = \mathcal{O}_K/P$.

(3) Jeśli $f_\omega(x) \bmod p \equiv (x - a)^2 \bmod p$ ma pierwiastek podwójny w $\mathbb{F}_p$, gdzie $a \in \mathbb{Z}$, to p rozgałęzia się w $\mathcal{O}_K$. Wówczas $p\mathcal{O}_K = P^2$, gdzie $P = (p, \omega - a)$ oraz $\mathbb{F}_p = \mathcal{O}_K/P$.

Jeśli p jest nieparzysta, to ze wzorów na pierwiastki równania kwadratowego otrzymujemy, że p odpowiednio rozpada się, pozostaje pierwsza lub rozgałęzia się w $\mathcal{O}_K$ dokładnie wtedy, gdy wyróżnik $D \bmod p$ jest resztą kwadratową, nieresztą kwadratową, lub $D \bmod p = 0$; równoważnie symbol Legendra $(\frac{D}{p}) = 1, -1, 0$.

Liczba $p = 2$ rozgałęzia się w $\mathcal{O}_K$ dokładnie wtedy, gdy $D \bmod 2 \equiv 0$, czyli dla $d \equiv 1, 2 \bmod 4$. Jeśli $d \equiv 3 \bmod 4$, to dla $d = 3 + 8k$ wielomian $f_\omega(x) \bmod 2 \equiv x^2 + x + 1 \bmod 2$ jest nierozkładalny nad $\mathbb{F}_2$, więc 2 pozostaje liczbą pierwszą w $\mathcal{O}_K$. Jeśli $d = 7 + 8k$, to $f_\omega(x) \bmod 2 \equiv x^2 + x \bmod 2$ ma dwa pierwiastki w $\mathbb{F}_2$, więc 2 rozpada się w $\mathcal{O}_K$.

Opiszemy teraz metodę rozwiązywania równanie $\mathrm{N}(\alpha) = n$ dla $\alpha \in \mathcal{O}_K$.

Normą niezerowego ideału $I \subset \mathcal{O}_K$ nazywamy liczbę

$$\mathrm{N}(I) = \#\mathcal{O}_K/I.$$

Aby rozwiązać równanie $\mathrm{N}(\alpha) = n$ wyznaczamy wszystkie ideały o normie n, a następnie wybieramy z pośród nich ideały główne i ich generatory. Jeśli I jest ideałem głównym o generatorze α, to

$$\mathrm{N}(I) = \mathrm{N}(\alpha).$$

Jeśli $I = \prod P_i^{v_i}$ jest iloczynem ideałów pierwszych, to

$$\mathrm{N}(I) = \prod \mathrm{N}(P_i)^{v_i}. \tag{4.4}$$

Dla ideału pierwszego P leżącego nad liczbą pierwszą p mamy $\mathrm{N}(P) = p$ jeśli p rozpada się lub rozgałęzia się w $\mathcal{O}_K$ oraz $\mathrm{N}(P) = p^2$ jeśli p pozostaje pierwsza w $\mathcal{O}_K$.

Niech $n = \prod_{i=1}^{k} p_i^{n_i}$ będzie liczbą o znanej faktoryzacji, przy czym liczby pierwsze p_i są uporządkowane, tak że $p_1, \ldots, p_{k_1}$ rozpadają się w $\mathcal{O}_K$, $p_{k_1+1}, \ldots, p_{k_2}$ pozostają pierwsze w $\mathcal{O}_K$, oraz $p_{k_2+1}, \ldots, p_k$ rozgałęziają się w K. Niech ideały pierwsze $P_i, \overline{P}_i$ leżą nad p_i dla $1 \leq i \leq k_1$ oraz P_i leżą nad p_i dla $k_1 < i \leq k$. Jeśli istnieją w $\mathcal{O}_K$ ideały o normie n, to z (4.4) n_i są parzyste dla $k_1 < i \leq k_2$. Wówczas wszystkie takie ideały są postaci

$$I = \prod_{1 \leq i \leq k_1} P_i^{u_i} \overline{P}_i^{n_i - u_i} \prod_{k_1 < i \leq k_2} P_i^{n_i/2} \prod_{k_2 < i \leq k} P_i^{n_i}, \tag{4.5}$$

gdzie $0 \leq u_i \leq n_i$ dla $1 \leq i \leq k_1$. Mamy $(n_1 + 1) \cdots (n_{k_1} + 1)$ ideałów o normie n. Zatem liczba takich ideałów rośnie wykładniczo wraz z liczbą dzielników pierwszych n, które rozpadają się w K.
Ponieważ $p_i \mathcal{O}_K = P_i \overline{P}_i$ dla $1 \leq i \leq k_1$ oraz $p_i \mathcal{O}_K = P_i$ dla $k_1 < i \leq k_2$, więc ideały o normie n możemy również zapisać w postaci

$$I = \prod_{1 \leq i \leq k_1} Q_i^{n_i - 2u_i} p_i^{u_i} \prod_{k_1 < i \leq k_2} p_i^{n_i/2} \prod_{k_2 < i \leq k} P_i^{n_i},$$

gdzie $0 \leq u_i \leq \lfloor n_i/2 \rfloor$, $Q_i \in \{P_i, \overline{P}_i\}$ dla $1 \leq i \leq k_1$.

Z pośród ideałów I o normie n musimy wybrać ideały główne i znaleźć ich generatory. Ideał o normie n jest główny oraz $\alpha \in I$ jest jego generatorem jeśli $\mathrm{N}(\alpha) = n$. Wówczas α jest liczbą w I o najmniejszej niezerowej normie. Traktując I jako 2-wymiarową kratę w $\mathbb{C}$ taką liczbę możemy znaleźć jako najkrótszy wektor w kracie. Stosując poniższy algorytm Gaussa, analogiczny do algorytmu Euklidesa, możemy znaleźć najkrótszy wektor w kracie. Najpierw musimy znaleźć bazę nad $\mathbb{Z}$ ideału I.

Jeśli znamy rozkład I na iloczyn ideałów pierwszych, to możemy wyznaczyć generatory I nad $\mathcal{O}_K$, a stąd generatory I nad $\mathbb{Z}$. Jeśli $a_i + b_i\omega$ są generatorami I nad $\mathbb{Z}$, gdzie $a_i, b_i \in \mathbb{Z}$ dla $1 \leq i \leq s$, to macierzą generującą dla I nazywamy macierz

$$M = \begin{pmatrix} a_1 & a_2 & \dots & a_s \\ b_1 & b_2 & \dots & b_s \end{pmatrix}. \tag{4.6}$$

Jeśli pomnożymy macierz złożoną z pierwszych dwóch kolumn przez macierz $G \in \mathrm{G}L_2(\mathbb{Z})$

$$\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} G = \begin{pmatrix} c_1 & c_2 \\ d_1 & d_2 \end{pmatrix}, \tag{4.7}$$

to $a_1 + b_1\omega$, $a_2 + b_2\omega$ i $c_1 + d_1\omega$, $c_2 + d_2\omega$ generują ten sam $\mathbb{Z}$-moduł. Niech $e = \gcd(b_1, b_2)$ oraz $x_1b_1 + x_2b_2 = e$ dla $x_1, x_2 \in \mathbb{Z}$. Wówczas w (4.7) dla macierzy

$$G = \begin{pmatrix} \frac{b_2}{e} & x_1 \\ \frac{-b_1}{e} & x_2 \end{pmatrix} \tag{4.8}$$

otrzymujemy $d_1 = 0$. Stąd możemy otrzymać macierz generującą (4.6) z $b_1 = 0$. Przez indukcję otrzymamy macierz generującą, taką że $b_1, \dots, b_{s-1} = 0$. Wówczas dla $a = \gcd(a_1, \dots, a_{s-1})$ macierzą generującą, której kolumny tworzą bazę I, jest

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \tag{4.9}$$

Możemy założyć, że $a, c > 0$ oraz $0 \leq b < a$ dzieląc z resztą b przez a.

Macierz generująca dla I postaci (4.9), taka że $a, c > 0$ i $0 \leq b < a$ jest wyznaczona jednoznacznie. Jeśli A i B są dwiema macierzami generującymi takiej postaci, to $AG = B$ dla $G \in \mathrm{G}L_2(\mathbb{Z})$. Stąd łatwo widać, że $g_{21} = 0$, $g_{11} = g_{22} = 1$ i $g_{12} = 0$.

Omówimy teraz algorytm Gaussa, który pozwala znaleźć najkrótszy wektor w kracie $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$, gdzie ω_1, ω_2 są liniowo niezależne nad $\mathbb{R}$.

Algorytm jest analogiczny do algorytmu Euklidesa i przez kolejne redukcje bazy ω_1, ω_2 pozwala otrzymać bazę ω_1', ω_2' dla L, taką że ω_1' jest najkrótszym wektorem w L. Algorytm opiera sią na następującym fakcie: jeśli ω_1', ω_2' jest bazą dla L, taką że $|\omega_2' + m\omega_1'| \geq |\omega_1'|$ dla każdego $m \in \mathbb{Z}$, to ω_1' jest najkrótszym wektorem w L. Niech $v = a\omega_1' + b\omega_2'$ dla $a, b \in \mathbb{Z}$ będzie niezerowym wektorem w L. Jeśli $b = 0$, to oczywiście $|v| \geq |\omega_1'|$. Jeśli $b \neq 0$,

to dzieląc z resztą $a = bq + r, 0 \leq r < |b|$, mamy $|v| = |(bq+r)\omega_1' + b\omega_2'| = |b(\omega_2' + q\omega_1') + r\omega_1'| \geq \big||b|(\omega_2' + q\omega_1')| - r|\omega_1'|\big| \geq |b||\omega_1'| - r|\omega_1'| \geq |\omega_1'|$.

Aby otrzymać bazę ω_1', ω_2' wykonujemy następujące redukcje bazy ω_1, ω_2. Załóżmy, że $|\omega_2| \geq |\omega_1|$. Wówczas dla $m_0 = \lfloor -\frac{<\omega_1,\omega_2>}{|\omega_1|^2} \rceil$ funkcja $|\omega_2 + m\omega_1|$ przyjmuje minimum dla $m \in \mathbb{Z}$. Liczba m_0 jest najbliższą liczbą całkowitą pierwszej współrzędnej wierzchołka paraboli $|\omega_2 + m\omega_1|^2 = m^2|\omega_1|^2 + 2m < \omega_1, \omega_2 > +|\omega_2|^2$. Jeśli $|\omega_2 + m_0\omega_1| \geq |\omega_1|$, to ω_1 jest najkrótszym wektorem. Jeśli $|\omega_1| > |\omega_2 + m_0\omega_1|$, to przyjmujemy $\omega_2 := \omega_1$, $\omega_1 := \omega_2 + m_0\omega_1$ i powtarzamy redukcję. W ten sposób otrzymujemy bazy, w których długości wektorów maleją, więc po skończonej liczbie kroków otrzymamy bazę z najkrótszym wektorem. Podobnie jak w algorymie Euklidesa, można pokazać, że koszt tego algorytmu jest $O(\log^2 \max\{|\omega_1|, |\omega_2|\})$.

Algorytm 4.1. ([5, Alg. 1.3.14])
Input: Krata dyskretna $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$.
Output: Baza ω_1', ω_2' kraty L, taka że ω_1' jest najkrótszym wektorem w L.

(1) Jeśli $|\omega_1| > |\omega_2|$ przestaw ω_1, ω_2.
(2) Połóż $m_0 = \lfloor -\frac{<\omega_1,\omega_2>}{|\omega_1|^2} \rceil$.
(3) Jeśli $|\omega_2 + m_0\omega_1| \geq |\omega_1|$, zwróć ω_1, ω_2 i zakończ algorytm.
(4) Jeśli $|\omega_2 + m_0\omega_1| < |\omega_1|$, połóż $\omega := \omega_2 + m_0\omega_1$, $\omega_2 := \omega_1$, $\omega_1 := \omega$ i wróć do kroku 2.

Jeśli $\alpha \in I$ jest generatorem ideału I, to pozostałe generatory I są postaci $u\alpha$ dla $u \in \mathcal{O}_K^*$. Następujący algorytm wyznacza rozwiązania równania $N(\alpha) = n$.

Algorytm 4.2. Input: Ciało urojone kwadratowe $K = \mathbb{Q}(\sqrt{-d})$ oraz liczba $n = \prod_{i=1}^{k} p_i^{n_i}$ o znanej faktoryzacji.
Output: Zbiór $S = \{\alpha \in \mathcal{O}_K : N(\alpha) = n\}$.

(1) Uporządkuj liczby pierwsze p_i, tak że p_i rozpadają się w $\mathcal{O}_K$ dla $1 \leq i \leq k_1$, p_i pozostają pierwsze w $\mathcal{O}_K$ dla $k_1 < i \leq k_2$, p_i rozgałęziają się w $\mathcal{O}_K$ dla $k_2 < i \leq k$.
(2) Niech $S := \emptyset$. Jeśli $n_i \equiv 1 \bmod 2$ dla pewnego $k_1 < i \leq k_2$, zwróć S i zakończ algorytm.
(3) Wyznacz ideały pierwsze $P_i, \overline{P}_i$ leżące nad p_i dla $1 \leq i \leq k_1$ oraz ideały pierwsze P_i leżące nad p_i dla $k_2 < i \leq k$.
(4) Połóż $c_0 := \prod_{k_1 < i \leq k_2} p_i^{n_i/2}$ i utwórz ideał $J = \prod_{k_2 < i \leq k} P_i^{n_i}$.
(5) Dla liczb całkowitych $(u_1, \ldots, u_{k_1}) \in [0, \ldots, \lfloor \frac{n_1}{2} \rfloor] \times \cdots \times [0, \ldots, \lfloor \frac{n_{k_1}}{2} \rfloor]$ wykonuj:

(6) Połóż $c_1 = \prod_{1\le i\le k_1} p_i^{u_i}$.
(7) Dla $(Q_1, \dots, Q_{k_1}) \in \{P_1, \overline{P}_1\} \times \cdots \times \{P_{k_1}, \overline{P}_{k_1}\}$ wykonuj:
(8) Utwórz ideał $I = \prod_{1\le i\le k_1} Q_i^{n_i - 2u_i} J$
(9) Znajdź bazę I nad $\mathbb{Z}$.
(10) Zastosuj Algorytm 4.1 aby znaleźć liczbę $\alpha' \in I \setminus 0$ o najmniejszej normie.
(11) Jeśli $(c_0c_1)^2 \mathrm{N}(\alpha') = n$, połóż $\alpha := c_0c_1\alpha'$.
(12) Jeśli $d \neq 1, 3$, połóż $S := S \cup \{\pm\alpha\}$.
(13) Jeśli $d = 1$, połóż $S := S \cup \{\pm\alpha, \pm i\ \alpha\}$.
(14) Jeśli $d = 3$, połóż $S := S \cup \{\pm\alpha, \pm\zeta_3\alpha, \pm\zeta_3^2\alpha\}$.
(15) Zwróć S.

Alternatywną metodę wyznaczania ideałów o normie n można znaleźć w [4].

5. Algorytm Rozwiązujący Problem 1.1

Niech $K = \mathbb{Q}(\sqrt{-d})$ będzie ciałem urojonym kwadratowym oraz r liczbą pierwszą. Aby skonstruować krzywą eliptyczną E nad pewnym ciałem prostym $\mathbb{F}_p$, taką że $r \mid \#E(\mathbb{F}_p)$ i $\mathrm{End}(E) = \mathcal{O}_K$ będziemy dla kolejnych $h = 1, 2, \dots$ wyznaczać rozwiązania $\alpha \in \mathcal{O}_K$ równania $\mathrm{N}(\alpha) = hr$ dopóki nie znajdziemy takiego rozwiązania, że $p = \mathrm{N}(\alpha + 1)$ jest liczbą pierwszą. Wówczas istnieje krzywa eliptyczna $E/\mathbb{F}_p$ rzędu hr z $\mathrm{End}(E) = \mathcal{O}_K$, którą można skonstruować za pomocą CM metody dla odpowiednio małego d. Jeśli równanie $\mathrm{N}(\alpha) = hr$ ma rozwiązanie dla $h < r$, to z (4.5) r musi rozpadać się w K.

Stwierdzenie 5.1. *Jeśli liczba pierwsza r rozpada się w K, to przy poniższych heurystycznch założeniach można oczekiwać znalezienia rozwiązania Problemu 1.1 dla $h \le O(\sqrt{d}\ln^{1+\varepsilon}(\sqrt{d}r))$, gdzie $\varepsilon > 0$.*

Dowód. Z twierdzeń o liczbach pierwszych i Chebotareva o gęstości wynika, że dla dużych liczb B prawdopodobieństwo, że $p \le B$ jest liczbą pierwszą rozpadającą się w K jest bliskie $1/2 \ln B$. Prawdopodobieństwo, że losowy ideał w $\mathcal{O}_K$ jest główny jest równe $1/h_K$, gdzie h_K jest liczbą klas ciała K. Naturalne jest założenie, że takie samo jest prawdopodobieństwo otrzymania ideału głównego w zbiorze ideałów RP, gdzie R jest ideałem pierwszym w $\mathcal{O}_K$ leżącym nad r oraz P jest ideałem pierwszym leżącym nad liczbą pierwszą $p \le B$ rozpadającą się w K. Stąd dla $h \le B$ równanie $\mathrm{N}(\alpha) = hr$ ma rozwiązanie z prawdopodobieństwem przynajmniej $1/2h_K \ln B$.

Jeśli $\alpha \in \mathcal{O}_K$ jest rozwiązaniem równania $\mathrm{N}(\alpha) = hr$ dla $h \le B$, to liczba $p = \mathrm{N}(\alpha + 1)$ jest wielkości Br. Załóżmy również, że p jest liczbą

pierwszą z takim samym prawdopodobieństwem jak losowa liczba $< Br$, tj. $1/(\ln B + \ln r)$. Zatem liczbę pierwszą p powinniśmy średnio otrzymać dla $\ln B + \ln r$ rozwiązań równania $\mathrm{N}(\alpha) = hr$. Przynajmniej tyle rozwiązań α powinniśmy otrzymać jeśli B spełnia nierówność

$$\frac{B}{2h_K \ln B} \geq \ln B + \ln r,$$

skąd $B > 2h_K \ln B(\ln B + \ln r)$. Stąd łatwo widać, że wystarczy wziąć $B = O(h_K \ln^{1+\varepsilon}(h_K r))$ dla dowolnego $\varepsilon > 0$. Ponieważ $h_K = O(\sqrt{d})$, mamy $B = O(\sqrt{d} \ln^{1+\varepsilon}(\sqrt{d} r))$. □

Następujący algorytm znajduje rozwiązanie Problemu 1.1.

Algorytm 5.2. Input: Ciało urojone kwadratowe $K = \mathbb{Q}(\sqrt{-d})$ oraz liczba pierwsza r, taka że $(\frac{-d}{r}) = 1$.
Output: Liczba pierwsza p oraz krzywa eliptyczna $E/\mathbb{F}_p$, taka że $\#E(\mathbb{F}_p) = hr$ oraz $\mathrm{End}(E) = \mathcal{O}_K$.

(1) Dla $h = 1, 2, \ldots$ wykonuj:
(2) Zastosuj Algorytm 4.2 aby znaleźć wszystkie rozwiązania $\alpha \in \mathcal{O}_K$ równania $\mathrm{N}(\alpha) = hr$.
(3) Dla każdego rozwiązania α sprawdź czy $p = \mathrm{N}(\alpha+1)$ jest liczbą pierwszą.
(4) Jeśli p jest liczbą pierwszą, zastosuj Algorytm 3.2 aby skonstruować krzywą eliptyczną $E/\mathbb{F}_p$ rzędu hr.
(5) Zwróć E i zakończ algorytm.

Przykład 5.3. Niech $K = \mathbb{Q}(\sqrt{-2014})$ oraz r będzie najmniejszą liczbą pierwszą $> 2^{240}$, taką że $(\frac{-2014}{r}) = 1$, tj. $r = 2^{240} + 897$. Dla $h = 5678$ znajdujemy krzywą eliptyczną E rzędu hr nad ciałem $\mathbb{F}_p$, gdzie

$$p{=}1003215763381166622337396320921829133306832089485807550601321181770945792607 1.$$

Stosując Algorytm 3.2 znajdujemy równanie E,

$$\begin{aligned} E{:}y^2{=}x^3{+}&48732382754611589005411440430067845033589 \\ &47143591836524675846606793111533020x \\ {+}&31424919117828326452084263552519455898 5 \\ &46926844184270232767046453555834603 41. \end{aligned}$$

W tym przypadku liczba klas $h_K = 36$. Powyższe obliczenia z wykorzystaniem Magmy zajęły kilka sekund.

Jeśli $\mathcal{O}_K$ jest dziedziną ideałów głównych, to możemy podać prostszy algorytm, który nie wymaga rozwiązywania równania $\mathrm{N}(\alpha) = hr$. Dowodzi się, że $\mathcal{O}_K$ jest d.i.g dla $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$. Jeśli $R = (\gamma)$ jest ideałem pierwszym leżącym nad r, to wystarczy dla kolejnych $x, y = 1, 2, \ldots$ sprawdzać czy dla $\beta = x + y\omega$ otrzymamy liczbę pierwszą $p = \mathrm{N}(\beta\gamma + 1)$.

Algorytm 5.4. Input: Ciało kwadratowe urojone $K = \mathbb{Q}(\sqrt{-d})$, takie że $\mathcal{O}_K$ jest d.i.g. oraz liczba pierwsza r, taka że $(\frac{-d}{r}) = 1$.
Output: Krzywa eliptyczna $E/\mathbb{F}_p$, taka że $\#E(\mathbb{F}_p) = hr$ oraz $\mathrm{End}(E) = \mathcal{O}_K$.

(1) Zastosuj Algorytm 4.1 aby znaleźć generator γ ideału pierwszego $R \subset \mathcal{O}_K$ leżącego nad r.
(2) Dla $z := 1, 2, \ldots$ wykonuj:
(3) Dla $x := z$ i $y := 1, \ldots, z - 1$ lub $y := z$ i $x := 1, \ldots, z - 1$ wykonuj:
(4) Połóż $\alpha := (x + y\omega)\gamma$, gdzie ω jest dana (4.1).
(5) Jeśli $d = 1$, sprawdź czy $p = \mathrm{N}(u\alpha + 1)$ jest liczbą pierwszą dla $u = \pm 1, \pm i$.
(6) Jeśli $d = 3$, sprawdź czy $p = \mathrm{N}(u\alpha + 1)$ jest liczbą pierwszą dla $u = \pm 1, \pm\zeta_3, \pm\zeta_3^2$.
(7) Jeśli $d \neq 1, 3$, sprawdź czy $p = \mathrm{N}(u\alpha + 1)$ jest liczbą pierwszą dla $u = \pm 1$.
(8) Jeśli p jest liczbą pierwszą, zastosuj Algorytm 3.2 aby skonstruować krzywą eliptyczną $E/\mathbb{F}_p$ rzędu $\mathrm{N}(\alpha)$.
(9) Zwróć E i zakończ algorytm.

Przykład 5.5. Niech $K = \mathbb{Q}(\sqrt{-3})$ oraz r będzie najmniejszą liczbą pierwszą $> 2^{240}$, taką że $(\frac{-3}{r}) = 1$, tj. $r := 2^{240} + 897$. Dla $h = 28$ znajdujemy krzywą eliptyczną E rzędu hr nad ciałem $\mathbb{F}_p$, gdzie

p=4947171781379476122833233002080171845668411057622508415836034166689176350 3.

Stosując metodę z Uwagi 3.3 znajdujemy równanie $E : y^2 = x^3 + 5$.

Literatura

[1] A. O. L. Atkin, F. Morain, *Elliptic curves and primality proving*, Math. Comp. 61 (1993), 29-68.
[2] J. Belding, R. Bröker, A. Enge, and 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.

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

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

[5] H. Cohen, *A course in computational algebraic number theory*, Springer Graduate Texts in Mathematics, vol. 138, 1993.

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

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

[8] R. Gallant, R. Lambert, S. Vanstone, *Faster point multiplication on elliptic curves with efficient endomorphisms*, In: Kilian, J. (ed.) CRYPTO. LNCS, vol. 2139, pp. 190–200. Springer (2001).

[9] S. D. Galbraith, X. Lin, M. Scott, *Endomorphisms for faster elliptic curve cryptography on a large class of curves*, J. Cryptology, 24(3):446–469, 2011.

[10] N. Koblitz, *CM-curves with good cryptographic properties*, Proc. Crypto'91, Springer-Verlag (1992) pp. 279–287.

[11] S. Lang, *Elliptic functions* Springer, 1987.

[12] G. Lay, H. Zimmer, *Constructing elliptic curves with given group order over large finite fields*, Algorithmic Number theory Symposium I, Springer Lecture Notes in Computer Science, 1994. MR1322728 (96a:11054).

[13] R. Schoof, *Elliptic curves over finite fields and the computation of square roots* mod p. Math. Comp. 44, (1985), 483–494.

[14] R. Schoof, *Counting points on elliptic curves over finite fields*, J. Théorie des Nombres de Bordeaux 7 (1995). 219–254.

[15] J. Silverman, *The Arithmetic of Elliptic Curves* Springer, 1986.

[16] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, GTM 151, 1995.

[17] A. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Math. Comp. 80 (2011), 501–538.

CONSTRUCTING ELLIPTIC CURVES WITH A SUBGROUP OF A GIVEN ORDER AND WITH A GIVEN ENDOMORPHISM RING

Abstract. The complex multiplication (CM) method allows one to construct an elliptic curve over a finite field, whose endomorphism ring is the maximal order in an imaginary quadratic field with a suitably small discriminant. Using CM method Lay-Zimmer and Bröker-Stevenhagen gave a method to construct an elliptic curve of a given order n over some prime field. Their method has a heuristic polynomial time if n has not too many prime factors. In this paper we show that in an analogous way one can construct an elliptic curve, which contains a subgroup of a given order r and has a given endomorphism ring with a suitably small discriminant. We give heuristic arguments, which show that the method works in a polynomial time if r is prime.

Keywords: elliptic curves with a given order, CM method, Cornacchia's algorithm, endomorphism ring.