Izboljšanje množenja s skalarjem na eliptičnih krivuljah

Jernej Tonejc

9. april 2001

Povzetek

V projektu predstavimo izboljšanje množenja na anomalnih eliptičnih krivuljah s kompleksnim množenjem nad $\mathbb{F}_2$ oz. nad razširitvami $\mathbb{F}_{2^n}$. Konkretno se bomo osredotočili na krivuljo $E : y^2 + xy = x^3 + x^2 + 1$, definirano nad $\mathbb{F}_2$. Z novo metodo porabimo v splošnem trikrat manj časa kot z metodo seštej in podvoji, v nekaterih primerih pa celo 4.5 krat manj časa, pri tem pa ne potrebujemo dodatnega prostora.

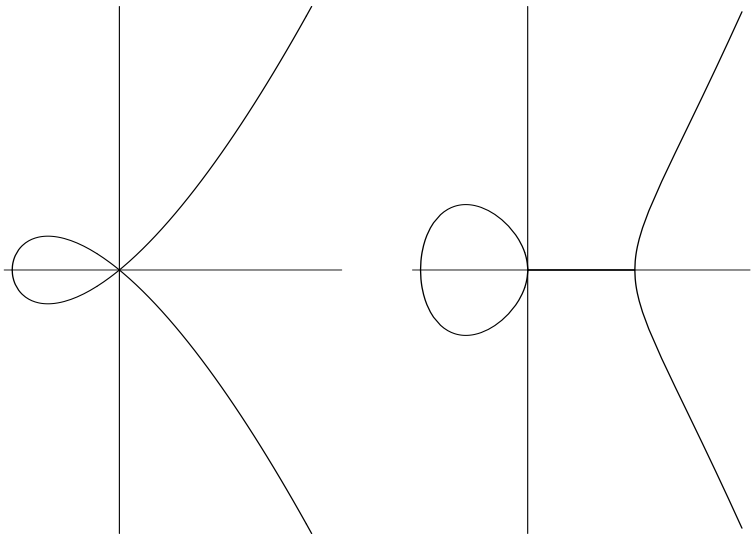
1 Uvod

1.1 Osnovne definicije in izreki

Naj bo $\mathbb{K}$ obseg in naj $\overline{\mathbb{K}}$ označuje algebraično zaprtje obsega $\mathbb{K}$. *Afina Weierstraßova enačba* nad $\mathbb{K}$ je enačba oblike

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{1}$$

kjer so $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$. Enačba (1) je *nesingularna*, če je v vsaki točki, ki je rešitev enačbe, vsaj eden od parcialnih odvodov neničelni. V tem primeru je z njo definirana *eliptična krivulja*. Slika 1 prikazuje dve krivulji nad $\mathbb{R}$. Leva je singularna v (0,0), desna pa je nesingularna in zato eliptična.



Slika 1: Krivulji $Y^2 = X^3 + X^2$ in $Y^2 = X^3 - X$ nad $\mathbb{R}$.

Točke na eliptični krivulji so urejeni pari $P = (X, Y)$, kjer $X, Y \in \overline{\mathbb{K}}$ rešita enačbo (1), skupaj s točko v neskončnosti $\mathcal{O}$. Na točkah eliptične krivulje definiramo *konjugiranje*, tako da točki $P = (x, y) \neq \mathcal{O}$ priredimo točko $\overline{P} = (x, -y - a_1x - a_3)$. Definiramo tudi vsoto točk, za katero

velja: $P+\mathcal{O}=\mathcal{O}+P=P$, $P+\overline{P}=\mathcal{O}$, vsota točk $P=(x_1,y_1)\neq\mathcal{O}$ in $Q=(x_2,y_2)\neq\mathcal{O}$, $Q\neq\overline{P}$ pa je točka $R=(x_3,y_3)$, podana z

$$\begin{aligned} x_3 &= \begin{cases} \left(\frac{y_2-y_1}{x_2-x_1}\right)^2+a_1\left(\frac{y_2-y_1}{x_2-x_1}\right)-a_2-x_1-x_2, & P\neq Q \\ \left(\frac{3x_1^2+2a_2x_1^2+a_4-a_1y_1}{2y_1+a_1x_1+a_3}\right)^2+a_1\left(\frac{3x_1^2+2a_2x_1^2+a_4-a_1y_1}{2y_1+a_1x_1+a_3}\right)-a_2-2x_1, & P=Q \end{cases} \\ y_3 &= \begin{cases} \frac{y_2-y_1}{x_2-x_1}(x_1-x_3)-y_1-(a_1x_3+a_3), & P\neq Q \\ \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}(x_1-x_3)-y_1-(a_1x_3+a_3), & P=Q \end{cases} \end{aligned} \tag{2}$$

V primeru, da je karakteristika obsega $\mathbb{K}$ 2 in je enačba krivulje $Y^2+XY=X^3+a_2X^2+a_6$, pa se formula za seštevanje poenostavi v

$$\begin{aligned} x_3 &= \begin{cases} \left(\frac{y_1+y_2}{x_1+x_2}\right)^2+\left(\frac{y_1+y_2}{x_1+x_2}\right)+a_2+x_1+x_2, & P\neq Q \\ x_1^2+\frac{a_6}{x_1^2}, & P=Q \end{cases} \\ y_3 &= \begin{cases} \frac{y_1+y_2}{x_1+x_2}(x_1+x_3)+y_1+x_3, & P\neq Q \\ \frac{x_1^2+y_1}{x_1}x_3+x_1^2+x_3, & P=Q \end{cases} \end{aligned} \tag{3}$$

Množica točk na eliptični krivulji tvori Abelovo grupo za to operacijo seštevanja. Operacijo konjugiranja lahko razširimo na endomorfizme grupe točk $\mathrm{End}(E)$ s predpisom $\overline{f}(P)=f(\overline{P})$, kjer je $f\in\mathrm{End}(E)$ poljuben. Sled endomorfizma f definiramo s $\mathrm{Tr}(f)=f+\overline{f}$.
Komutativni kolobar R z enico imenujemo *celostno polje*, če nima deliteljev niča. Kolobar R imenujemo *evklidski*, če obstaja funkcija $\psi: R\setminus\{0\}\to\mathbb{N}$, ki zadošča pogojema

(i) če $a,b\in R$ in $ab\neq 0$, potem je $\psi(a)\leqslant\psi(ab)$

(ii) če $a,b\in R$ in $b\neq 0$, potem obstajata $q,r\in R$, tako da je $a=qb+r$, kjer je bodisi $r=0$ bodisi $r\neq 0$ in $\psi(r)<\psi(b)$.

Funkcijo ψ imenujemo *norma*. Evklidski kolobar, ki je hkrati celostno polje, imenujemo *evklidsko polje*.
Za poljuben $n\in\mathbb{Z}$ je preslikava $\mu_n: P\mapsto nP$ endomorfizem. Pravimo, da ima eliptična krivulja *kompleksno množenje*, če obstaja kak endomorfizem grupe točk, ki je različen od množenja s celim številom.
Naj bo p praštevilo in $q=p^m$ za nek $m\in\mathbb{N}$. V primeru, da je $\mathbb{K}=\mathbb{F}_q$, definiramo Frobeniusovo preslikavo φ s predpisom

$$\varphi:(x,y)\mapsto(x^q,y^q).$$

Potem je φ endomorfizem grupe točk na eliptični krivulji, različen od množenja s celim številom (tu upoštevamo, da so koeficienti krivulje iz obsega $\mathbb{F}_q$, t.j. da je $a_i^q=a_i$). Torej imajo vse krivulje nad končnimi obsegi kompleksno množenje.
Z $\#E_q$ bomo označili število $\mathbb{F}_q$-točk na E (t.j. točk s koordinatami v $\mathbb{F}_q$).
V nadaljevanju bomo potrebovali še naslednja dva izrek iz teorije eliptičnih krivulj.

Izrek 1 (Hasse). *Naj bo $\mathbb{K}=\mathbb{F}_q$ in $t=q+1-\#E_q$. Potem za Frobeniusov endomorfizem φ velja*

1. $\varphi^2-t\varphi+q=0$
2. $|t|\leqslant 2\sqrt{q}$

(t je sled Frobeniusovega endomorfizma)

Izrek 2 (Weil). *Naj bo E definirana nad $\mathbb{F}_q$, $\#E_q = q + 1 - t$ in naj bo $m \in \mathbb{N}$. Nadalje naj bosta α in β kompleksni ničli enačbe $x^2 - tx + q = 0$. Potem je*

$$\#E_{q^m} = q^m + 1 - (\alpha^m + \beta^m).$$

Dokaza obeh izrekov lahko najdemo v [1, str. 95 – 98].
Če je sled Frobeniusovega endomorfizma enaka 1, pravimo, da je krivulja *anomalna.* V tem primeru φ zadošča enačbi

$$\varphi^2 - \varphi + q = 0. \tag{4}$$

1.2

Eliptične krivulje nad končnimi obsegi so primerne za kriptografske sisteme, ki temeljijo na problemu diskretnega logaritma. Privlačne so predvsem zato, ker so za enako stopnjo varnosti velikosti ključev občutno manjše kot pri ostalih sistemih. Prvič so bile predlagane v [2].
V [3] je Koblitz opisal anomalne eliptične krivulje, ki imajo nad obsegi s karakteristiko 2 naslednji zanimivi lastnosti:

1. Niso supersingularne, tako da ne moremo uporabiti Menezes - Okamoto - Vanstonove redukcije diskretnega logaritma z eliptične krivulje na končni obseg [4].

2. Množenje točk s celim številom lahko izvedemo skoraj tako učinkovito kot na supersingularnih krivuljah.

Osredotočili se bomo na krivulje nad obsegi s karakteristiko 2 oziroma konkretno na krivuljo

$$E: \ y^2 + xy = x^3 + x^2 + 1, \tag{5}$$

definirano nad $\mathbb{F}_2$. Ogledali si bomo tudi njen *zvin* $\tilde{E}$ nad $\mathbb{F}_2$, podan z enačbo

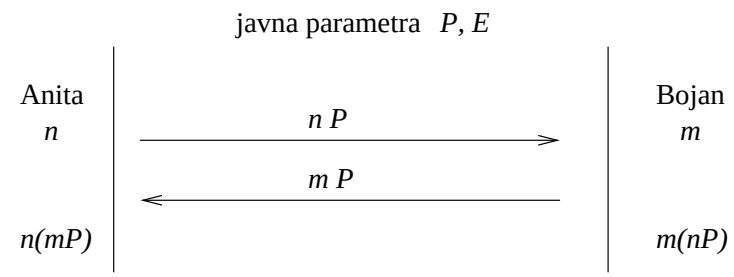
$$\tilde{E}: \ y^2 + xy = x^3 + 1. \tag{6}$$

Kasneje si bomo ti dve krivulji ogledali nad razširitvenimi obsegi $\mathbb{F}_{2^n}$. Pri tem bomo uporabljali oznaki E_n za $\mathbb{F}_{2^n}$-točke krivulje E, $\tilde{E}_n$ pa za $\mathbb{F}_{2^n}$-točke njenega zvina.
V naslednjem razdelku sestavimo algoritem za računanje razvojev celih števil po potencah α, nato pa prikažemo še nekaj izboljšav tega algoritma.

2 Izboljšanje množenja na anomalnih eliptičnih krivuljah

2.1 Osnovna ideja

Na sliki 2 je predstavljena Diffie-Hellmanova izmenjava ključev, izvedena na eliptični krivulji.



Slika 2: Diffie-Hellmanova izmenjava ključev.

Vidimo, da moramo računati večkratnike točk na krivulji E_n. S standardnim algoritmom podvoji in seštej prevedemo računanje večkratnikov na seštevanje točk na krivulji E_n. Iz formule za vsoto (2) oz. (3) je jasno razvidno, da je to računsko precej zahtevna operacija. Ker večino časa porabimo za seštevanje točk, je smiselno imeti algoritem, ki opravi čim manj seštevanj. Ideja je, da množenje z m nadomestimo z linearno kombinacijo potenc Frobeniusovega endomorfizma, saj lahko tega izračunamo z navadnim kvadriranjem v $\mathbb{F}_{2^n}$, kar lahko v normalni bazi dosežemo zgolj s pomikom (shift). Ogledali si bomo torej razvoje oblike

$$m = \sum_i c_i \varphi^i, \tag{7}$$

kjer so $c_i \in \{0, \pm 1\}$. Računanje mP prevedemo na $\ell - 1$ seštevanj, kjer je ℓ število neničelnih členov v (7). Naš cilj je poiskati čim krajše razvoje oziroma razvoje s čimmanj neničelnimi členi.

2.2 Glavna podgrupa

Na anomalni eliptični krivulji $E_1 (= E_{\mathbb{F}_2})$ Frobeniusov endomorfizem zadošča enačbi

$$\varphi^2 - \varphi + 2 = 0, \tag{8}$$

na $\tilde{E}_1$ pa

$$\varphi^2 + \varphi + 2 = 0. \tag{9}$$

S kratkim računom ugotovimo, da velja

$$\begin{aligned} E_1 &= \{\mathcal{O}, (0,1)\}, \\ \tilde{E}_1 &= \{\mathcal{O}, (0,1), (1,0), (1,1)\}. \end{aligned} \tag{10}$$

S pomočjo Weilovega izreka lahko izračunamo število točk na E_n po naslednji formuli:

$$\#E_n = |\alpha^n - 1|^2 = |\beta^n - 1|^2 = 1 + 2^n - \alpha^n - \beta^n, \tag{11}$$

pri čemer sta α in β (kompleksni) ničli karakteristične enačbe (8). Število točk na $\tilde{E}_n$ pa je podano z

$$\#\tilde{E}_n = |\alpha^n + 1|^2 = 1 + 2^n + \alpha^n + \beta^n. \tag{12}$$

Števili $\#E_n$ in $\#\tilde{E}_n$ lahko tudi izračunamo iz formul

$$\begin{aligned} \#E_n &= 2^n + 1 - a_n, \\ \#\tilde{E}_n &= 2^n + 1 + a_n, \end{aligned}$$

kjer a_n za $n \geqslant 2$ zadoščajo rekurziji $a_n = a_{n-1} - 2a_{n-2}$, $a_0 = 2$, $a_1 = 1$, kar sledi iz

$$\alpha^n + \beta^n = (\alpha + \beta)\alpha^{n-1} - 2\alpha^{n-2} + (\alpha + \beta)\beta^{n-1} - 2\beta^{n-2} = \alpha^{n-1} + \beta^{n-1} - 2(\alpha^{n-2} + \beta^{n-2}),$$

saj je $\alpha + \beta = 1$ in $\alpha\beta = 2$.
Ker izvajamo protokole za javno kriptografijo v grupi E_n oz. $\tilde{E}_n$, hočemo, da je problem diskretnega logaritma težek problem, zato mora biti moč grupe deljiva z velikim praštevilom. Idealno bi bilo, če bi bila moč grupe kar enaka praštevilu. Toda velja, da je E_1 podgrupa v E_n, zato iz (10) sledi, da 2 vedno deli $\#E_n$. Podobno za $\tilde{E}_n$ dobimo, da 4 vedno deli $\#\tilde{E}_n$. Če n ni praštevilo, dobimo še dodatne faktorje zaradi deliteljev n. Zato mora biti n praštevilo, če hočemo upati,

da je moč grupe enaka $2p$ oz. $4p$ za neko praštevilo p. Izkaže se, da takšni n obstajajo, in sicer je za $n \leqslant 512$ število $\#E_n$ dvakratnik praštevila za

$$n = 3, 5, 7, 11, 19, 23, 101, 107, 109, 113, 163, 283, 311, 331, 347, 359,$$

$\#\tilde{E}_n$ pa štirikratnik praštevila za

$$n = 5, 7, 13, 19, 23, 41, 83, 97, 103, 107, 131, 233, 239, 277, 283, 349, 409.$$

V nadaljevanju se bomo osredotočili samo na zgoraj navedene vrednosti n. Naj bo $\#E_n = 2 \cdot p_1$, $\#\tilde{E}_m = 4 \cdot p_2$, kjer sta p_1 in p_2 praštevili. Pogosto izvajamo kriptografske protokole v *glavni podgrupi*, t.j. podgrupi moči p_i $(i = 1, 2)$ in ne v celi grupi. Kako poiskati točke iz glavne podgrupe, nam pove naslednja lema.

Lema 1. *Naj bosta $\#E_n$ in $\#\tilde{E}_m$ kot zgoraj. Če je $P \in E_n$, potem je P v glavni podgrupi natanko tedaj, ko je $P = 2Q$ za nek $Q \in E_n$. Podobno je $P \in \tilde{E}_m$ v glavni podgrupi natanko tedaj, ko velja $P = 4Q$ za nek $Q \in \tilde{E}_m$.*

Dokaz. Iz (10) vidimo, da sta tako E_1 kot $\tilde{E}_1$ ciklični grupi. Od tod takoj sledi, da sta E_n oz $\tilde{E}_m$ ciklični, čim sta njuni moči oblike $2p_1$ oz. $4p_2$. Lema sedaj sledi iz lastnosti končnih cikličnih grup. □

Naslednji izrek podaja računski kriterij za ugotavljanje pripadnosti glavni podgrupi.

Izrek 3. *1. Naj bo $(x_1, y_1) \in E_n$. Potem je $(x_1, y_1) = 2(u, v)$ za nek $(u, v) \in E_n$ natanko tedaj, ko je $\mathrm{Tr}(x_1) = 1$.*

2. Naj bo $(x_2, y_2) \in \tilde{E}_n$. Potem je $(x_2, y_2) = 4(w, z)$ za nek $(w, z) \in \tilde{E}_n$ natanko tedaj, ko je $\mathrm{Tr}(x_2) = 0$ in $\mathrm{Tr}(y_2) = \mathrm{Tr}(\lambda x_2)$, kjer λ zadošča enačbi $\lambda^2 + \lambda = x_2$.

OPOMBA. Tukaj Tr označuje sled v obsegu $\mathbb{F}_{2^n}$, ki je definirana s

$$\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i}, \quad x \in \mathbb{F}_{2^n}.$$

Velja še, da je Tr $\mathbb{F}_2$-linearna in da je $\mathrm{Tr}(x^2) = \mathrm{Tr}(x)$. Nadalje velja, da je $\mathrm{Tr}(x) = 0$ natanko tedaj, ko obstaja $\lambda \in \mathbb{F}_{2^n}$, da je $x = \lambda^2 + \lambda$.

Dokaz.

1. Predpostavimo najprej, da velja $(x_1, y_1) = 2(u, v)$ za nek $(u, v) \in E_n$. Iz formule za podvajanje točke na binarni krivulji dobimo $x_1 = \mu^2 + \mu + 1$, kjer je $\mu = u + \frac{v}{u}$. Zato je $\mathrm{Tr}(x_1) = \mathrm{Tr}(\mu^2) + \mathrm{Tr}(\mu) + \mathrm{Tr}(1) = 1$, saj je $\mathrm{Tr}(\mu^2) = \mathrm{Tr}(\mu)$ in $\mathrm{Tr}(1) = 1$.

   Obratno, naj velja $\mathrm{Tr}(x_1) = 1$. Potem ima $x_1 + 1$ sled 0 in zato obstaja $\lambda \in \mathbb{F}_{2^n}$, da je $x_1 + 1 = \lambda^2 + \lambda$. Poiščimo $u \in \mathbb{F}_{2^n}$, za katerega velja $y_1 = u^2 + (\lambda + 1)x_1$. Tak u je en sam, saj je kvadriranje v $\mathbb{F}_{2^n}$ bijektivna preslikava. Potem je $y_1^2 = u^4 + (\lambda^2 + 1)x_1^2$ in $x_1 y_1 = u^2 x_1 + (\lambda + 1)x_1^2$. Od tod sledi

   $$y_1^2 + x_1 y_1 = (\lambda^2 + \lambda)x_1^2 + u^4 + u^2 x_1 = (x_1 + 1)x_2^2 + u^4 + u^2 x_1.$$

   Ker (x_1, y_1) leži na krivulji, velja $y_1^2 + x_1 y_1 = x_1^3 + x_1^2 + 1$, torej je $u^4 + u^2 x_1 = 1$. Definirajmo $v = \lambda u + u^2$. Potem je

   $$\begin{aligned} v^2 + uv &= \lambda^2 u^2 + u^4 + \lambda u^2 + u^3 \\ &= (\lambda + x_1 + 1)u^2 + u^4 + \lambda u^2 + u^3 \\ &= x_1 u^2 + u^4 + u^3 + u^2 \\ &= u^3 + u^2 + 1, \end{aligned}$$

torej $(u,v) \in E_n$. Iz definicije v sledi, da velja $\lambda = u + \frac{v}{u}$, iz definicije u pa nato sledi $(x_1, y_1) = 2(u, v)$.

2. Predpostavimo najprej, da je $(x_2, y_2) = 4(w, z)$ za nek $(w, z) \in \tilde{E}_n$. Definirajmo $(x_3, y_3) = 2(w, z)$, tako da je $(x_2, y_2) = 2(x_3, y_3)$. Z majhnimi spremembami v dokazu točke (1) ($x_1 + 1$ zamenjamo z x_1, ostalo ostane enako) trditev sledi. Podobno dokažemo še obrat.

□

Posledica zgornje leme in izreka je, da je ugotavljanje pripadnosti glavni podgrupi zelo učinkovito, če uporabljamo normalno bazo, saj lahko v tem primeru računanje sledi izvedemo zelo učinkovito. Tako ne rabimo za E_n takorekoč nič, za $\tilde{E}_n$ pa samo eno množenje.

2.3 Razvoj množenja po potencah Frobeniusovega endomorfizma

Kot smo omenili že prej, se bomo osredotočili na konkretno krivuljo (5) in na njen zvin (6), obe definirani nad $\mathbb{F}_2$.
Množenje z m bomo poskusili zapisati kot kratko linearno kombinacijo potenc Frobeniusovega endomorfizma. V članku [3] so opisani razvoji oblike

$$m = \sum_j c_j \varphi^j, \quad c_j \in \{0, \pm 1\}.$$

Razvoji so povprečno dvakrat daljši od binarnega zapisa m-ja. Dokazali bomo, da lahko vedno konstruiramo razvoje dolžine n, kjer je n stopnja razširitve obsega.
Najprej opazimo, da obstaja naravni homomorfizem iz kolobarja

$$\mathbb{Z}[\alpha] = \{m + n\alpha \,|\, m, n \in \mathbb{Z}\} \subset \mathbb{C}$$

v kolobar endomorfizmov eliptične krivulje $\mathrm{End}(E)$, ki slika $\alpha = \frac{1+\sqrt{-7}}{2}$ v φ. α je tista rešitev enačbe $x^2 - x + 2 = 0$, ki ima pozitivni imaginarni del. Zato za vsak razvoj $m = \sum_j c_j \alpha^j$ v $\mathbb{Z}[\alpha]$ takoj dobimo ustrezen razvoj $m = \sum_j c_j \varphi^j$ v $\mathrm{End}(E)$, t.j. $mP = \sum_j c_j \varphi^j(P)$ za vsak $P \in E_n$. Pri iskanju razvojev v $\mathbb{Z}[\alpha]$ si bomo pomagali z algebraično strukturo kolobarja $\mathbb{Z}[\alpha]$.

Lema 2. *$\mathbb{Z}[\alpha]$ je evklidsko polje glede na normo*

$$\psi(a + b\alpha) = |a + b\alpha|^2 = a^2 + ab + 2b^2, \quad a, b \in \mathbb{Z}.$$

Dokaz. Dokažimo najprej, da $\mathbb{Z}[\alpha]$ nima deliteljev niča. Naj bo $x = a + b\alpha \neq 0$, $y = c + d\alpha \neq 0$ in naj bo $xy = 0$. Če je katerikoli izmed a, b, c in d enak 0, takoj sledi, da je vsaj eden izmed x in y enak 0. Torej je dovolj obravnavati primer, ko so vsi štirje neničelni. Brez škode za splošnost lahko predpostavimo, da je $a > 0$ in $c > 0$. Dobimo

$$0 = xy = (a + b\alpha)(c + d\alpha) = ac - 2bd + (ad + bc + bd)\alpha.$$

Torej mora veljati

$$ac = 2bd \tag{13}$$
$$ad + bc + bd = 0. \tag{14}$$

Če (14) prištejemo ac, dobimo $(a + b)(c + d) = ac$. Sedaj ločimo 4 možnosti:

1. $b > 0$, $d > 0$: V tem primeru je $a + b > a$ in $c + d > c$, torej $ac = (a + b)(c + d) > ac$, kar je očitno protislovje.

2. $b > 0$, $d < 0$: V tem primeru je $ac > 0$, $bd < 0$ in dobimo protislovje z $ac = 2bd$.

3. $b < 0$, $d > 0$: Tudi v tem primeru je $ac > 0$, $bd < 0$ in spet dobimo protislovje z $ac = 2bd$.

4. $b < 0$, $d < 0$: Iz (14) dobimo $(a+b)d = -bc$. Ker je desna stran pozitivna, d pa negativen, mora biti $a + b < 0$ in zato $a < -b$. Ker velja tudi $(c+d)b = -ad$, mora biti tudi $c < -d$. Toda potem je $2bd = ac < (-b)(-d) = bd$, kar je protislovje.

Torej smo ob predpostavki $x \neq 0$ in $y \neq 0$ prišli do protislovja. Od tod že sledi, da $\mathbb{Z}[\alpha]$ nima deliteljev niča.
Pokažimo še, da $\mathbb{Z}[\alpha]$ zadošča pogojema (i) in (ii) iz definicije evklidskega kolobarja! Naj bo $a = a_1 + a_2\alpha$ in $b = b_1 + b_2\alpha$, $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ ter $ab \neq 0$. Očitno za vsak $a \in \mathbb{Z}[\alpha]$, $a \neq 0$ velja $\psi(a) > 0$. Zato je

$$\begin{aligned}
\psi(ab) &= \psi((a_1 + a_2\alpha)(b_1 + b_2\alpha)) \\
&= (a_1b_1 - 2a_2b_2)^2 + (a_1b_1 - 2a_2b_2)(a_1b_2 + a_2b_1 + a_2b_2) + 2(a_1b_2 + a_2b_1 + a_2b_2)^2 \\
&= b_1^2(a_1^2 + a_1a_2 + 2a_2^2) + b_1b_2(-4a_1a_2 + a_1^2 + a_1a_2 - 2a_2^2 + 4a_1a_2 + 4a_2^2) + \\
&\quad b_2^2(4a_2^2 - 2a_1a_2 - 2a_2^2 + 2a_1^2 + 4a_1a_2 + 2a_2^2) \\
&= b_1^2(a_1^2 + a_1a_2 + 2a_2^2) + b_1b_2(a_1^2 + a_1a_2 + 2a_2^2) + 2b_2^2(a_1^2 + a_1a_2 + 2a_2^2) \\
&= (a_1^2 + a_1a_2 + 2a_2^2)(b_1^2 + b_1b_2 + 2b_2^2) \\
&= \psi(a)\psi(b) \geqslant \psi(a).
\end{aligned}$$

Torej je pogoj (i) izpolnjen. Za pogoj (ii) pa najprej postavimo $a = a_1 + a_2\alpha$ in $b > 0$. Potem lahko a_1 in a_2 zapišemo kot

$$\begin{aligned}
a_1 &= q_1b + r_1, \quad |r_1| \leqslant \frac{b}{2} \\
a_2 &= q_2b + r_2, \quad |r_2| \leqslant \frac{b}{2}.
\end{aligned}$$

V primeru, da v kateri od neenakosti velja enačaj, lahko r_1 in r_2 izberemo tako, da sta različno predznačena, zato vedno velja $r_1r_2 < \frac{b^2}{4}$. Definiramo $q = q_1 + q_2\alpha$ in $r = r_1 + r_2\alpha$. Sledi $a_1 + a_2\alpha = q_1y + r_1 + q_2y\alpha + r_2\alpha = (q_1 + q_2\alpha)y + (r_1 + r_2\alpha) = qy + r$. Velja še, da je bodisi $r = 0$ bodisi

$$\psi(r) = r_1^2 + r_1r_2 + 2r_2^2 < r_1^2 + \frac{b^2}{4} + 2r_2^2 \leqslant \frac{b^2}{4} + \frac{b^2}{4} + \frac{b^2}{2} = b^2 = \psi(b).$$

Naj bo sedaj $a = a_1 + a_2\alpha$ in $b = b_1 + b_2\alpha \neq 0$. Definirajmo $\tilde{b} = b_1 + b_2\overline{\alpha}$. Potem je

$$b\tilde{b} = b_1^2 + 2\mathrm{Re}(\alpha)b_1b_2 + b_2^2\alpha\overline{\alpha} = b_1^2 + b_1b_2 + 2b_2^2 \geqslant 0.$$

Zato po že dokazanem obstajata $q, r_0 \in \mathbb{Z}[\alpha]$, da velja $a\tilde{b} = qb\tilde{b} + r_0$, kjer je bodisi $r_0 = 0$ bodisi $\psi(r_0) < \psi(b\tilde{b})$. Definiramo $r = a - qb$. Sledi $a = qb + r$ in $r_0 = r\tilde{b}$. Iz dokaza pogoja (i) sledi $\psi(r_0) = \psi(r\tilde{b}) = \psi(r)\psi(\tilde{b})$. Ker je $\psi(\tilde{b}) \neq 0$, velja bodisi $r = 0$ bodisi

$$\psi(r) = \frac{\psi(r_0)}{\psi(\tilde{b})} < \frac{\psi(b\tilde{b})}{\psi(\tilde{b})} = \psi(b).$$

S tem je lema dokazana. □

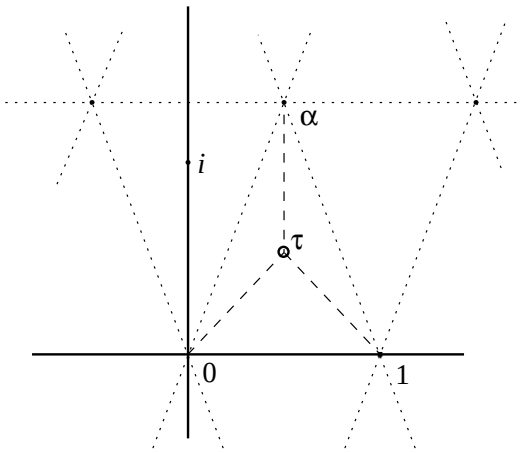
OPOMBA. Lemo bi lahko dokazali precej krajše, če bi upoštevali, da je ψ definirana z absolutno vrednostjo kompleksnega števila. Vendar pa je prednost zgornjega dokaza v tem, da se da posplošiti na primere, ko ψ ni porojena iz absolutne vrednosti.

Sedaj pa dokažimo, da $\mathbb{Z}[\alpha]$ zadošča močnejšemu pogoju kot je pogoj (ii) iz definicije evklidskega kolobarja.

Lema 3. *Za poljubna $a, b \in \mathbb{Z}[\alpha]$, $b \neq 0$, obstajata $q, r \in \mathbb{Z}[\alpha]$, da velja $a = qb + r$ in*

$$\psi(r) \leqslant \frac{4}{7}\psi(b).$$

Dokaz. Elementi kolobarja $\mathbb{Z}[\alpha]$ tvorijo mrežo v $\mathbb{C}$. Zato lahko celo kompleksno ravnino pokrijemo s trikotniki z oglišči v $\mathbb{Z}[\alpha]$, kot to prikazuje slika 3.



Slika 3: Kolobar $\mathbb{Z}[\alpha]$ kot podmnožica $\mathbb{C}$

Oglejmo si trikotnik z oglišči 0,1 in α. Točka $\tau = \frac{1}{2} + \frac{3\sqrt{7}}{14}i$ je središče trikotniku očrtane krožnice, saj je $|\tau - 0| = |\tau - 1| = |\tau - \alpha| = \frac{2}{\sqrt{7}}$. Torej je vsaka točka v tem trikotniku od najbližjega oglišča oddaljena kvečjemu za $\frac{2}{\sqrt{7}}$. Ker je vsaka točka v ravnini v nekem trikotniku, od tod sledi, da za poljuben $z \in \mathbb{C}$ obstaja $a \in \mathbb{Z}[\alpha]$, da je

$$\psi(z - a) \leqslant \left(\frac{2}{\sqrt{7}}\right)^2 = \frac{4}{7}.$$

Naj bosta sedaj $a, b \in \mathbb{Z}[\alpha]$ poljubna in $b \neq 0$. Oglejmo si kvocient $z = a/b$, izračunan v obsegu $\mathbb{Q}(\alpha) = \{a + b\alpha \,|\, a, b \in \mathbb{Q}\} \subset \mathbb{C}$. Potem obstaja $q \in \mathbb{Z}[\alpha]$, za katerega velja $\psi(q - z) \leqslant \frac{4}{7}$, $r = a - qb = (z - q)b$ pa ima normo $\psi(r) = \psi(z - q)\psi(b) \leqslant \frac{4}{7}\psi(b)$, od koder sledi, da imata q in r zahtevano lastnost. □

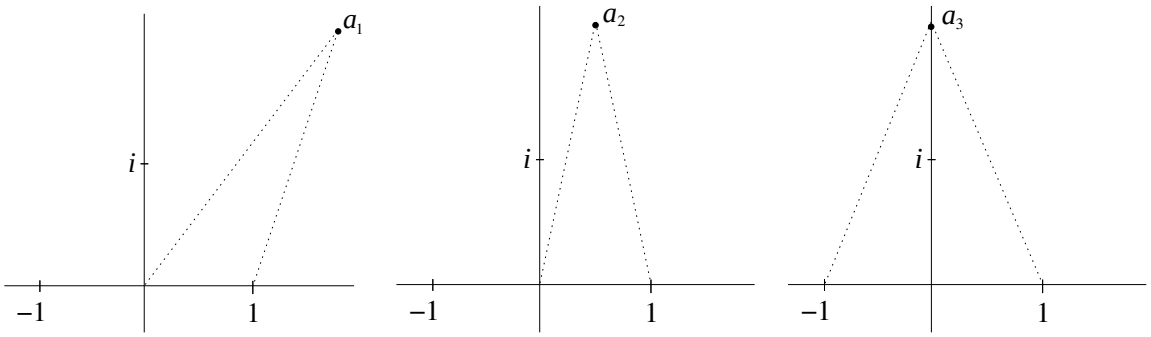
Lema 4. *Za poljuben $a \in \mathbb{Z}[\alpha]$ z normo $\psi(a) < 2^n$, $n \in \mathbb{N}$, obstaja razvoj*

$$a = \sum_{j=0}^{n-1} c_j \alpha^j \tag{15}$$

dolžine n, kjer so $c_j \in \{0, \pm 1\}$.

Dokaz. Lemo bomo dokazali s pomočjo indukcije. Za $n = 1, 2$ si oglejmo vse elemente v $\mathbb{Z}[\alpha]$ z normo manjšo od 4. To so

- 0 z normo 0,
- ± 1 z normo 1,
- $\pm\alpha, \pm(1 - \alpha)$ z normo 2.



(a) Nekritičen primer. (b) Mejni primer. (c) Kritičen primer.

Slika 4: Trije primeri.

Za te elemente trditev v lemi očitno drži.
Naj bo sedaj $a \in \mathbb{Z}[\alpha]$ s $\psi(a) < 2^n$, $n > 2$. Ker je $\mathbb{Z}[\alpha]$ evklidsko polje, lahko a izrazimo kot

$$a = a'\alpha + c, \tag{16}$$

kjer je $\psi(c) < \psi(\alpha) = 2$, t.j. $c \in \{0, \pm 1\}$. Če je $c = 0$ (t.j. če α deli a), potem je redukcija (16) enolična. V nasprotnem primeru pa imamo zaradi dejstva, da α deli 2, vedno redukcijo s $c = 1$ in redukcijo s $c = -1$. Če bi lahko redukcijo izvedli tako, da bi veljalo $\psi(a') \leqslant \frac{\psi(a)}{2} < 2^{n-1}$, bi bil dokaz s pomočjo indukcije končan. Toda obstajajo primeri, ko ne obstaja redukcija s $\psi(a') \leqslant \frac{\psi(a)}{2}$. Ločimo naslednje tri primere:

1. *Nekritičen primer:* Obstaja redukcija (16) s $\psi(a') < \frac{\psi(a)}{2}$.

2. *Mejni primer:* Obstaja redukcija (16) s $\psi(a') = \frac{\psi(a)}{2}$.

3. *Kritičen primer:* Obstajajo samo redukcije (16) s $\psi(a') > \frac{\psi(a)}{2}$.

Če α deli a, imamo redukcijo $a = a'\alpha$ s $c = 0$ in $\psi(a') = \frac{\psi(a)}{2}$, t.j. a je mejni primer. Če α ne deli a, potem α deli tako $a + 1$ kot $a - 1$. V tem primeru se izkaže, da je tip redukcije odvisen od absolutne vrednosti realnega dela a.
1. *Nekritičen primer:* $|\mathrm{Re}(a)| \geqslant 1$. Naj bo na primer $\mathrm{Re}(a) \geqslant 1$, kot prikazuje slika 4(a). Potem je $\psi(a-1) < \psi(a)$ in obstaja redukcija $a = a'\alpha + 1$ s $\psi(a') = \psi(a-1)/\psi(a) < \frac{\psi(a)}{2}$. Podobno, če je $\mathrm{Re}(a) \leqslant -1$, je $a = a'\alpha - 1$ in $\psi(a') < \frac{\psi(a)}{2}$.
2. *Mejni primer:* $|\mathrm{Re}(a)| = \frac{1}{2}$. Ta primer prikazuje slika 4(b). Velja $\psi(a-1) = \psi(a)$ in obstaja redukcija $a = a'\alpha + 1$, kjer je $\psi(a') = \psi(a-1)/\psi(\alpha) = \frac{\psi(a)}{2}$. Podobno imamo v primeru $\mathrm{Re}(a) = -\frac{1}{2}$ redukcijo $a = a'\alpha - 1$, kjer je $\psi(a') = \frac{\psi(a)}{2}$.
3. *Kritičen primer:* $\mathrm{Re}(a) = 0$. Ta primer prikazuje slika 4(c). Po pitagorovem izreku je $\psi(a-1) = \psi(a+1) = \psi(a) + 1$. Obstajata redukciji $a = a'\alpha + 1$ in $a = a''\alpha - 1$, kjer je $\psi(a') = \psi(a'') = \frac{\psi(a)+1}{2}$. Ker je $a'' - a' = \frac{2}{\alpha} = 1 - \alpha$, vsaj eden izmed a' in a'' ni deljiv z α. Recimo, da a' ni deljiv z α. Trdimo, da je a' v tem primeru nekritičen oz. da je $|\mathrm{Re}(a')| \geqslant 1$. Ker je $\mathrm{Re}(a) = 0$, velja $a = s\sqrt{-7}$ za neko število $s \in \mathbb{Z}$, $|s| \geqslant 1$. Potem lahko a' izračunamo v $\mathbb{Q}(\alpha)$:

$$a' = (a-1)\alpha^{-1} = (s\sqrt{-7} - 1)\frac{1}{4}(1 - \sqrt{-7}) = \frac{7s-1}{4} + \frac{s+1}{4}\sqrt{-7}.$$

Od tod pa že sledi $|\mathrm{Re}(a')| \geqslant \frac{3}{2}$.

Podobno vidimo, da je a'' nekritičen, če α ne deli a''.
Vrnimo se k dokazu leme. Če ima a nekritično oz. mejno redukcijo $a = a'\alpha + c$, velja $\psi(a') \leqslant \frac{\psi(a)}{2} < 2^{n-1}$. Po indukcijski predpostavki ima a' razvoj dolžine $n-1$, torej ima a razvoj dolžine n. Če ima pa a samo kritično redukcijo $a = a'\alpha + c$, potem je $\psi(a') = \frac{\psi(a)+1}{2} \leqslant 2^{n-1}$. Ker neenakost ni stroga, indukcijske predpostavke ne moremo uporabiti. Toda zgoraj smo videli, da ima v tem primeru a' nekritično redukcijo $a' = a''\alpha + c'$, kjer je $\psi(a'') < \frac{\psi(a')}{2} \leqslant 2^{n-2}$. Sledi $a = a''\alpha^2 + c'\alpha + c$ in po indukcijski predpostavki ima a'' razvoj dolžine $n-2$. Torej ima a razvoj dolžine n. S tem je lema dokazana. □

Dokažimo zdaj naslednji izrek.

Izrek 4. *Naj bo E_n kot prej. Potem lahko množenje z m na E_n zapišemo kot*

$$m = \sum_{j=0}^{n-1} c_j \varphi^j, \quad c_j \in \{0, \pm 1\}. \tag{17}$$

Dokaz. Ker gledamo krivuljo E_n nad razširitvenim obsegom $\mathbb{F}_{2^n}$, velja za Frobeniusovo preslikavo $\varphi^n(P) = \varphi^n(x,y) = (x^{2^n}, y^{2^n}) = (x,y) = P$, torej je $\varphi^n = 1$. Od tod sledi, da razvoja po potencah α, ki sta kongruentna po modulu $\alpha^n - 1$, porodita isti endomorfizem na E_n. Zato zadošča izračunati razvoj m' po potencah α, kjer je m' ostanek pri deljenju m z $\alpha^n - 1$, t.j. $m = q(\alpha^n - 1) + m'$. Po lemi 3 velja

$$\psi(m') \leqslant \frac{4}{7}\psi(\alpha^n - 1).$$

Da bomo lahko ocenili $\psi(m')$, moramo najprej izračunati $\psi(\alpha^n - 1)$, pri čemer upoštevamo (11) in definicijo ψ:

$$\psi(\alpha^n - 1) = |\alpha^n - 1|^2 = (\alpha^n - 1)(\beta^n - 1) = \alpha^n\beta^n - (\alpha^n + \beta^n) + 1 = 2^n + 1 - (\alpha^n + \beta^n) = \#E_n.$$

Po Hassejevem izreku (glej npr [1, str. 95]) je $\#E_n \leqslant 2^n + 1 + 2^{\frac{n}{2}+1}$, za $n \geqslant 4$ pa velja $\frac{4}{7}(2^n + 1 + 2^{\frac{n}{2}+1}) < 2^n$, torej je

$$\psi(m') < 2^n$$

in izrek velja po lemi 4. Za $n \leqslant 3$ pa preverimo izrek direktno. Spomnimo se, da je enačba krivulje E

$$y^2 + xy = x^3 + x^2 + 1.$$

Poiščimo točke iz E_n za vsak $n = 1, 2, 3$ posebej.

$n = 1$: V tem primeru je zraven točke v neskončnosti samo točka $P = (0,1)$, zato ni kaj dokazovati.

$n = 2$: Naj bo γ ničla enačbe $x^2 + x + 1 = 0$. Potem lahko pišemo $\mathbb{F}_4 = \{0, 1, \gamma, \gamma + 1\}$. Število točk na E_2 je $2^2 + 1 - \alpha^2 - \beta^2 = 8$, točke pa so

$$(0,1),\ (1,\gamma),\ (1,\gamma+1),\ (\gamma,1),\ (\gamma,\gamma+1),\ (\gamma+1,1),\ (\gamma+1,\gamma) \text{ in } \mathcal{O}.$$

Ker velja $8P = \mathcal{O}$ za vsak $P \in E_2$, moramo samo poiskati m' za $1 < m \leqslant 7$, kjer je $m' \equiv m \pmod{\alpha^2 - 1}$. S kratkim računom dobimo

$$\begin{aligned}
2 &= \alpha - \alpha^2 = -1(\alpha^2 - 1) + (\alpha - 1),\\
3 &= 2 + 1 = -(\alpha^2 - 1) + \alpha,\\
4 &= 3 + 1 = -(\alpha^2 - 1) + (\alpha + 1),\\
5 &= 3 + 2 = (-1 - \alpha)(\alpha^2 - 1) + (-\alpha),\\
6 &= 5 + 1 = (-1 - \alpha)(\alpha^2 - 1) + (-\alpha + 1),\\
7 &= 3 + 4 = (-2 - \alpha)(\alpha^2 - 1) + (-1).
\end{aligned}$$

V vseh primerih je m' dolžine največ dva, zato izrek velja.

$n = 3$: Naj bo γ ničla enačbe $x^3 + x + 1 = 0$. Potem je

$$\mathbb{F}_8 = \{0, 1, \gamma, \gamma + 1\, \gamma^2, \gamma^2 + 1, \gamma^2 + \gamma, \gamma^2 + \gamma + 1\}.$$

Število točk na E_3 je $2^3 + 1 - \alpha^3 - \beta^3 = 14$, točke pa so

$$\begin{gathered}(0,1),\ (\gamma, \gamma^2+1),\ (\gamma, \gamma^2+\gamma+1),\ (\gamma+1, 0),\ (\gamma+1, \gamma+1),\\ (\gamma^2, \gamma+1),\ (\gamma^2, \gamma^2+\gamma+1),\ (\gamma^2+1, 0),\ (\gamma^2+1, \gamma^2+1),\ (\gamma^2+\gamma, \gamma+1),\\ (\gamma^2+\gamma, \gamma^2+1),\ (\gamma^2+\gamma+1, 0),\ (\gamma^2+\gamma+1, \gamma^2+\gamma+1) \text{ in } \mathcal{O}.\end{gathered}$$

Tudi zdaj se z nekaj računanja prepričamo, da velja

$$\begin{aligned}2 &= \alpha - \alpha^2,\\ 3 &= 2 + 1 = 1 + \alpha - \alpha^2,\\ 4 &= 2 + 2 = -(\alpha^3 - 1) + (-\alpha^2 - 1),\\ 5 &= 4 + 1 = -(\alpha^3 - 1) + (-\alpha^2),\\ 6 &= 5 + 1 = -(\alpha^3 - 1) + (-\alpha^2 + 1),\\ 7 &= 5 + 2 = (\alpha - 2)(\alpha^3 - 1) + (\alpha^2 + \alpha + 1),\\ 8 &= 7 + 1 = (\alpha - 3)(\alpha^3 - 1) + (\alpha^2 - 1),\\ 9 &= 8 + 1 = (\alpha - 3)(\alpha^3 - 1) + \alpha^2,\\ 10 &= 9 + 1 = (\alpha - 3)(\alpha^3 - 1) + (\alpha^2 + 1),\\ 11 &= 10 + 1 = (\alpha - 3)(\alpha^3 - 1) + \alpha,\\ 12 &= 11 + 1 = (\alpha - 3)(\alpha^3 - 1) + (\alpha + 1),\\ 13 &= 12 + 1 = (\alpha - 4)(\alpha^3 - 1) + (-1).\end{aligned}$$

Tudi tukaj so ostanki pri deljenju z $\alpha^3 - 1$ take oblike kot trdimo v izreku, zato tudi v tem primeru izrek velja.

S tem je dokaz izreka končan. □

Izrek velja tudi v primeru, ko namesto E_n vzamemo $\tilde{E}_n$.
Razvoj po potencah α za poljuben element $a + b\alpha \in \mathbb{Z}[\alpha]$ ni težko izračunati. Iz dokaza leme 4 lahko izpeljemo enostaven algoritem, ki po vrsti izpiše koeficiente $c_0, c_1, \ldots, c_{n-1}$.

Algoritem 1.

```
Dokler (a ≠ 0 ali b ≠ 0) ponavljaj
    Če je a sod, potem
        c ← 0;
    sicer
        Če 2a + b ≠ 0, potem
            c ← sgn(2a + b);
        sicer
            c ← (a mod 4) − 2;
    x ← (a − c)/2;
    a ← x + b;
    b ← −x;
    Izpiši c;
```

2.4 Pretvarjanje razvoja po potencah α v nesosedno obliko

Definicija. *Predznačen binarni zapis (t.j. zaporedje števil* $0, 1$ *in* -1*) je v* **nesosedni** *obliki (NSO), če velja, da je izmed poljubnih dveh zaporednih elementov vsaj en enak nič.*

Na primer: $\mathrm{NSO}(49) = \langle 1, 0, -1, 0, 0, 0, 1\rangle$, saj je $49 = 64 - 16 + 1$. Enostavno je videti, da ima vsako naravno število enolično NSO. Velja še, da je NSO največ za en bit daljši od binarnega zapisa. Za naravno število a lahko $\mathrm{NSO}(a)$ preprosto izračunamo z naslednjim algoritmom:

Algoritem 2 (računanje NSO).

```
Dokler a > 0 ponavljaj
    Če je a sod, potem
        c ← 0;
    sicer
        c ← 2 − (a mod 4);
        a ← a − c;
    Izpiši c;
    a ← a/2;
```

Algoritem 2 izpiše elemente NSO od zadaj naprej, torej bi v primeru $a = 49$ izpisal po vrsti $1, 0, 0, 0, -1, 0$ in 1.
Poskusimo razviti podoben algoritem za računanje nesosednih oblik razvojev po potencah α. Tak razvoj bomo imenovali α-NSO. Potrebovali bomo naslednjo lemo.

Lema 5. *Element* $s = a + b\alpha \in \mathbb{Z}[\alpha]$ *je deljiv z* α *natanko tedaj, ko je* a *sod in je deljiv z* α^2 *natanko tedaj, ko je*

$$a \equiv 2b \pmod 4. \qquad (\star)$$

Dokaz. Velja

$$(c + d\alpha)\alpha = -2d + (c + d)\alpha,$$

od koder takoj sledi, da če α deli $a + b\alpha$, potem je a sod. Obratno, če je a sod, potem je

$$\frac{a + b\alpha}{\alpha} = b + \frac{a}{2}\cdot\frac{2}{\alpha} = b + \frac{a}{2}\cdot\frac{\alpha(1-\alpha)}{\alpha} = \frac{a+2b}{2} - \frac{a}{2}\alpha \in \mathbb{Z}[\alpha].$$

Da dokažemo še drugi del leme, najprej pišimo $\alpha^2 = \alpha - 2$. Od tod sledi, da ima vsak večkratnik α^2 obliko

$$(c + d\alpha)(\alpha - 2) = -2(c + d) + (c - d)\alpha.$$

Hitro vidimo, da vrednosti $a = -2(c+d)$ in $b = c-d$ zadoščata $(\star)$. Obratno, če je $(\star)$ izpolnjena, velja

$$\frac{a + b\alpha}{\alpha^2} = \frac{-a + 2b}{4} + \frac{-a - 2b}{4}\alpha \in \mathbb{Z}[\alpha].$$

□

S pomočjo leme v duhu algoritma 2 dobimo naslednji algoritem, ki izračuna α-NSO za $a + b\alpha \in \mathbb{Z}[\alpha]$.

Algoritem 3 (računanje α-NSO).

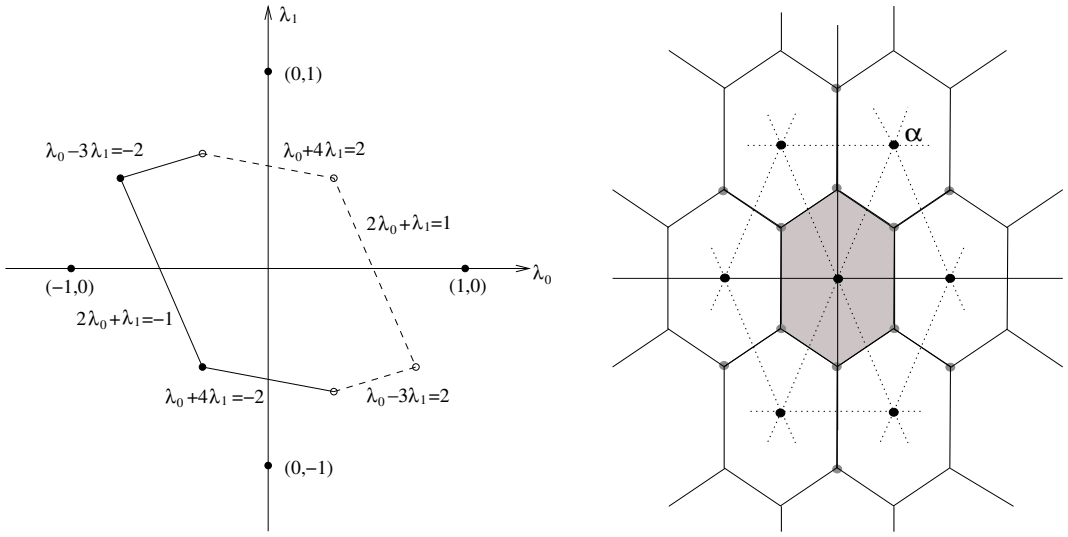
```
Dokler (a ≠ 0 ali b ≠ 0) ponavljaj
    Če je a sod, potem
        c ← 0;
    sicer
```

$c \leftarrow 2 - (a - 2b) \bmod 4$;
$x \leftarrow \frac{a-c}{2}$;
$a \leftarrow x + b$;
$b \leftarrow -x$;
`Izpiši` c;

Dá se dokazati, da je α-NSO enolična. Opazimo tudi, da sta si algoritma 1 in 3 precej podobna. Ker na vsakem koraku delimo z α, ki ima normo 2, lahko približno ocenimo dolžino α-NSO na $\log_2(\psi(a + b\alpha))$ (točnejša ocena je izpeljana v [5]). Ker je za $n \in \mathbb{Z}$ $\psi(n) = n^2$, je torej dolžina α-NSO(n) približno dvakrat večja od binarnega zapisa n. Zato bo naš naslednji korak združitev algoritma 3 z redukcijo, opisano v dokazu izreka 4. Ker še nismo opisali, kako redukcijo učinkovito izvedemo, se bomo najprej lotili tega problema. Za to moramo razviti metode za modularno redukcijo v $\mathbb{Z}[\alpha]$.
Za poljuben $\lambda \in \mathbb{C}$ pišimo $\lambda = \lambda_0 + \lambda_1\alpha$. Naj bo območje $\mathcal{U}$ v (λ_0, λ_1)-ravnini podano z

$$-1 \leqslant 2\lambda_0 + \lambda_1 < 1, \tag{18}$$
$$-2 \leqslant \lambda_0 + 4\lambda_1 < 2, \tag{19}$$
$$-2 \leqslant \lambda_0 - 3\lambda_1 < 2, \tag{20}$$

kot prikazuje slika 5(a). Kopije $\mathcal{U}$-ja pokrivajo ravnino, v središču vsake kopije pa je element $\mathbb{Z}[\alpha]$.



(a) Območje $\mathcal{U}$ v (λ_0, λ_1) ravnini (b) Povezava med $\mathcal{U}$ in mrežo $\mathbb{Z}[\alpha]$.

Slika 5:

V kolobarju $\mathbb{Z}[\alpha]$ definiramo naslednji operaciji. Dani $\lambda = \lambda_0 + \lambda_1\alpha \in \mathbb{Q}(\alpha)$ *zaokrožimo* tako, da izberemo središče tiste kopije $\mathcal{U}$, ki vsebuje λ. To operacijo označimo z

$$(q_0, q_1) = \mathrm{Round}(\lambda_0, \lambda_1)$$

oziroma z

$$q_0 + q_1\alpha = \mathrm{Round}(\lambda_0 + \lambda_1\alpha).$$

Definiramo še

$$(\!(\lambda)\!) = \lambda - \mathrm{Round}(\lambda).$$

Iz slike 5(b) vidimo, da točko dejansko zaokrožimo tako, da izberemo najbližje oglišče trikotnika, v katerem se nahaja točka. Zato iz leme 3 takoj dobimo

Lema 6. *Naj bo λ v notranjosti $\mathcal{U}$. Potem je*

$$\psi(\lambda) < \frac{4}{7}.$$

Dokaz. Sledi neposredno iz leme 3. □

Dokažimo še naslednjo lemo.

Lema 7. *Naj bo $\lambda \in \mathcal{U}$. Potem za vsak $a \in \mathbb{Z}[\alpha]$, $a \neq 0$ velja*

$$\psi(\lambda) < \psi(\lambda + a).$$

Dokaz. Kratek račun pokaže, da velja

$$\begin{aligned}
\psi(\lambda) < \psi(\lambda \pm 1) &\text{ natanko tedaj, ko } |2\lambda_0 + \lambda_1| < 1,\\
\psi(\lambda) < \psi(\lambda \pm \alpha) &\text{ natanko tedaj, ko } |\lambda_0 + 4\lambda_1| < 2,\\
\psi(\lambda) < \psi(\lambda \pm (1-\alpha)) &\text{ natanko tedaj, ko } |\lambda_0 - 3\lambda_1| < 2.
\end{aligned}$$

Iz definicije $\mathcal{U}$ sledi, da λ izpolnjuje vse tri pogoje. Torej je lema dokazana za $a = \pm 1, \pm\alpha$, $\pm(1-\alpha)$. Naj bo zdaj $b \in \mathbb{Z}[\alpha]$ poljuben, različen od prej naštetih. Potem je $\psi(b) \geqslant 4$ in ker je po lemi 6 $\psi(\lambda) < \frac{4}{7}$, rezultat sledi iz trikotniške neenakosti za $\sqrt{\psi}$. □

Naslednji algoritem nam izračuna q_0 in q_1, kjer je $q_0 + q_1\alpha = \mathrm{Round}(\lambda)$, $\lambda = \lambda_0 + \lambda_1\alpha$.

Algoritem 4.

$f_0 \leftarrow \mathrm{Round}(\lambda_0)$, $f_1 \leftarrow \mathrm{Round}(\lambda_1)$;
$g_0 \leftarrow \lambda_0 - f_0$, $g_1 \leftarrow \lambda_1 - f_1$;
$h_0 \leftarrow 0$, $h_1 \leftarrow 0$;
$\eta \leftarrow 2g_0 + g_1$;
`Če je` $\eta \geqslant 1$, `potem`
    `Če je` $g_0 - 3g_1 < -1$, `potem`
        $h_1 \leftarrow 1$;
    `sicer`
        $h_0 \leftarrow 1$;
`sicer`
    `Če je` $g_0 + 4g_1 \geqslant 2$, `potem`
        $h_1 \leftarrow 1$;
`Če je` $\eta < -1$, `potem`
    `Če je` $g_0 - 3g_1 \geqslant 1$, `potem`
        $h_1 \leftarrow -1$;
    `sicer`
        $h_0 \leftarrow -1$;
`sicer`
    `Če je` $g_0 + 4g_1 < -2$, `potem`
        $h_1 \leftarrow -1$;
$q_0 \leftarrow f_0 + h_0$;
$q_1 \leftarrow f_1 + h_1$;
`Izpiši` q_0 `in` q_1.

S pomočjo zaokroževanja bomo sedaj razvili algoritma za deljenje in modularno redukcijo v $\mathbb{Z}[\alpha]$. Če imamo dan deljenec $\gamma = a + b\alpha$ in delitelj $\delta = c + d\alpha$, želimo najti količnik $\eta = q_0 + q_1\alpha$ in ostanek $\rho = r_0 + r_1\alpha$, da bo veljalo

$$\gamma = \eta\delta + \rho,$$

pri čemer bomo želeli, da ima ρ čim manjšo normo. To bomo dosegli tako, da bomo zaokrožili γ/δ, pri čemer bomo dobili η, nato pa bomo izračunali ρ. Konkretno, če je

$$\lambda = \frac{\gamma}{\delta} = \frac{\gamma\overline{\delta}}{\psi(\delta)} = \frac{g_0 + g_1\alpha}{\psi(\delta)},$$

definiramo $\eta = \mathrm{Round}(\lambda)$ in $\rho = \gamma - \eta\delta$. Naslednji algoritem podrobneje opisuje ta postopek.

Algoritem 5 (deljenje v $\mathbb{Z}[\alpha]$).

$g_0 \leftarrow ac + ad + 2bd$;
$g_1 \leftarrow bc - ad$;
$N \leftarrow c^2 + cd + 2d^2$;
$\lambda_0 \leftarrow g_0/N$;
$\lambda_1 \leftarrow g_1/N$;
$(q_0, q_1) \leftarrow \mathrm{Round}(\lambda_0, \lambda_1)$;
$r_0 \leftarrow a - cq_0 + 2dq_1$;
$r_1 \leftarrow b - dq_0 - bq_1 - dq_1$;
`Izpiši` q_0, q_1, r_0, r_1.

Če v zgornjem algoritmu izpišemo samo ostanek, dobimo algoritem za modularno redukcijo. V tem primeru pišemo

$$\rho = \gamma \bmod \delta,$$

in velja

$$\rho = \delta\left(\left(\frac{\gamma}{\delta}\right)\right).$$

Zdaj smo v položaju, ko lahko združimo redukcijo in α-NSO. Kot smo omenili že v razdelku 2.2 si izberemo tak n, za katerega je $\#E_n = 2p$, kjer je p praštevilo. Naj bo P točka v glavni podgrupi. Definirajmo

$$\delta = \frac{\alpha^n - 1}{\alpha - 1}.$$

Iz dokaza izreka 4 sledi, da je $\psi(\delta) \leqslant 2^{n-1} + O(2^{n/2})$. Denimo, da želimo izračunati mP za neko naravno število m. Brez škode za splošnost lahko predpostavimo, da je $m < p/2$, saj velja $mP = -(p-m)P$, kjer smo upoštevali, da je $pP = \mathcal{O}$, saj je P v glavni podgrupi. Definirajmo $\rho = m \bmod \delta$. Iz leme 1 in dokaza izreka 4 sledi, da je $\delta P = \mathcal{O}$, zato sta si α-NSO(m) in α-NSO(ρ) ekvivalentna glede na glavno podgrupo. Po lemi 3 sledi, da je $\psi(\rho) \leqslant \frac{2^{n+1}}{7} + O(2^{n/2})$, zato je dolžina α-NSO(ρ) približno $n+1$. Ker ima α-NSO približno $1/3$ neničelnih elementov, smo torej računanje mP prevedli na samo $n/3$ seštevanj brez podvajanj na eliptični krivulji. To je za faktor $9/2$ boljše od navadne metode seštej in podvoji.
Zapišimo še algoritem, ki nam izračuna mP po tej metodi.

Algoritem 6 (računanje mP z redukcijo in α-NSO).

`Izračunaj` r_0, r_1 `s pomočjo Algoritma 5 za` $c + d\alpha = \delta$;
$Q \leftarrow \mathcal{O}$;
$P_0 \leftarrow P$;
`Dokler (`$r_0 \neq 0$ `ali` $r_1 \neq 0$`) ponavljaj`
    `Če je` r_0 `lih, potem`

$c \leftarrow 2 - (r_0 - 2r_1) \bmod 4$;
$Q \leftarrow Q + cP_0$; // $c = \pm 1$
$P_0 \leftarrow \varphi(P_0)$;
$x \leftarrow \frac{r_0 - c}{2}$;
$r_0 \leftarrow x + r_1$;
$r_1 \leftarrow -x$;
`Izpiši` Q.

3 Zaključek

V projektu smo prikazali, kako učinkovito računati večkratnike točk na anomalnih eliptičnih krivuljah nad binarnim obsegom. S pomočjo izreka 4 smo dosegli faktor izboljšanja 3 za anomalno krivuljo nad $\mathbb{F}_{2^n}$ za poljuben n in poljubno točko $P \in E_n$, s pomočjo algoritma 6 pa celo faktor 4.5 za tiste n, ki so našteti v razdelku 2.2, ter za P iz glavne podgrupe. Ker se za kriptografske namene v glavnem uporabljajo samo točke iz glavne podgrupe, lahko v večini primerov izberemo ustrezno velikost n in uporabljamo samo algoritem 6. Pri tem je potrebno poudariti, da ne potrebujemo dodatnega prostora za predizračun, kot pri nekaterih drugih metodah.
Možne so še dodatne izboljšave algoritma 6, vendar bi to preseglo okvir tega projekta. Omenimo samo, da se da prirediti metodo računanja α-NSO tako, da je med poljubnimi w zaporednimi elementi kvečjemu 1 neničelni. To je posplošitev metod z oknom širine w (angl. window-w methods). Pri računanju naključnih večkratnikov točk na krivulji (to na primer potrebujemo pri ECDSA in pri Diffie-Hellmanovi izmenjavi ključev) lahko dodatno izboljšavo dosežemo še tako, da namesto redukcije, ki je prvi korak v algoritmu 6, namesto naključnega števila m izberemo naključno reducirano α-NSO na naslednji način: Prvi bit v razvoju α-NSO generiramo s slučajnostno porazdelitvijo

$$\begin{pmatrix} 0 & 1 & -1 \\ 1/2 & 1/4 & 1/4 \end{pmatrix}, \tag{21}$$

za nadaljnje bite pa za vsakim neničelnim generiramo 0, za vsako 0 pa spet generiramo bit s porazdelitvijo (21). Ta metoda nam da naključna zaporedja, v katerih se biti pojavljajo s pravo verjetnostjo, toda ni znano, ali so zaporedja porazdeljena enakomerno. Še ena izboljšava je ta, da namesto algoritma 5 za redukcijo uporabljamo algoritem, ki redukcijo izračuna samo približno. Podrobnosti so opisane v [5].
Še ena možnost posplošitve je, da metode v razdelku 2.3 prenesemo na splošne eliptične krivulje nad majhnimi obsegi karakteristike 2, t.j. na krivulje, definirane nad $\mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_{16}$ in $\mathbb{F}_{32}$, ki niso anomalne. Kako to naredimo, je opisano v [6].

4 Odprti problemi

Omenimo dva odprta problema na področju anomalnih eliptičnih krivulj nad obsegi $\mathbb{F}_{2^m}$:

- Ni znano, ali je problem diskretnega logaritma na anomalnih binarnih krivuljah bistveno lažji od problema diskretnega logaritma na splošnih krivuljah iste velikosti, kot je to v primeru supersingularnih. Znano je, da se da najboljši korenski napad na splošne eliptične krivulje v primeru anomalnih modificirati, tako da da dobljeni algoritem potrebuje manj korakov kot v splošnem primeru, vendar je vsak korak nekoliko dražji. Znano je tudi, da je problem diskretnega logaritma na anomalnih krivuljah nad $\mathbb{F}_p$ rešljiv celo v linearnem času.

- Kot je že omenjeno v zaključku, ni znano, ali je naključno izbiranje reduciranih α-NSO ekvivalentno naključnemu izbiranju m. Da se videti, da je povprečno število zaporedij, ki dajo za rezultat isto točko na krivulji, 16/3, ni pa znano, kakšno je odstopanje od tega povprečja.

Literatura

[1] Andreas Enge. *Elliptic curves and their application to cryptography; an introduction.* Kluwer Academic Publisher, Norwell, MA, USA, and Dordrecht, The Netherlands, first edition, 1999.

[2] V. S. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology - Crypto '85*, pages 417–426, 1986.

[3] Neal Koblitz. CM-curves with good cryptographic properties. *Lecture Notes in Computer Science*, 576:279–287, 1991.

[4] S.A. Vanstone A. Menezes, T. Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. *Proceedings of the 23rd ACM Symp. Theory of Computing*, 1991.

[5] J. A. Solinas. An improved algorithm for arithmetic on a family of elliptic curves. *Lecture Notes in Computer Science*, 1294:357–371, 1997.

[6] V. Müller. Fast multiplication on elliptic curves over small fields of characteristic two. *Journal of Cryptology*, 11(4):219–234, 1998.

[7] Neal Koblitz. *A Course in Number Theory and Cryptography*, volume 114 of *Graduate texts in mathematics*. Springer-Verlag, second edition, 1994.

[8] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate texts in mathematics*. Springer-Verlag, first edition, 1986.

[9] NIST. Recommended elliptic curves for federal government use. 1999.

[10] Neal Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1(3):139–150, 1989.

[11] N. P. Smart. The discrete logarithm problem on elliptic curves of trace one. *Journal of Cryptology*, 12(3):193–196, 1999.

[12] W. Meier and O. Staffelbach. Efficient multiplication on certain nonsupersingular elliptic curves. *Lecture Notes in Computer Science*, 740:333–344, 1993.

[13] I. A. Semaev. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Math. Comp*, 67(221):353–356, 1998.

[14] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, January 1987.

Dodatek

Med naslednjimi anomalnimi krivuljami jih je pet opisanih v dokumentu [9], ki je dosegljiv na naslovu

`http://csrc.nist.gov/encryption`,

dve pa sta izračunani doma (za velikost 131 in ena za velikost 283). Oznaka K pomeni, da je krivulja dobljena iz (5), $\tilde{K}$ pa, da gre za zvin (6).
Vsaka od teh krivulj ima velikost oblike $2p$ ali $4p$. Pri vsaki je tudi podana točka v glavni podgrupi, zapisana v polinomski bazi.

$\tilde{K} - 131$:

Enačba:	$y^2 + xy = x^3 + 1$
Št. točk:	$4 * 680564733841876926932320129493409985129$
Nerazcepen polinom:	$t^{131} + t^8 + t^3 + t^2 + 1$
P_x:	`3 1844C908 BF59E34F 0F02F294 0E20E9DE`
P_y:	`0 C8D40C31 5FB7DDC8 E53A4825 6058F8EC`

$K - 163$:

Enačba:	$y^2 + xy = x^3 + x^2 + 1$
Št. točk:	$2 * 5846006549323611672814741753598448348329118574063$
Nerazcepen polinom:	$t^{163} + t^7 + t^6 + t^3 + 1$
P_x:	`2 FE13C053 7BBC11AC AA07D793 DE4E6D5E 5C94EEE8`
P_y:	`2 89070FB0 5D38FF58 321F2E80 0536D538 CCDAA3D9`

$\tilde{K} - 233$:

Enačba:	$y^2 + xy = x^3 + 1$
Št. točk:	$4 * 3450873173395281893717377931138512760570940988862252126328$0
Nerazcepen polinom:	$t^{233} + t^{74} + 1$
P_x:	`172 32BA853A 7E731AF1 29F22FF4 149563A4 19C26BF5 0A4C9D6E EFAD6126`
P_y:	`1DB 537DECE8 19B7F70F 555A67C4 27A8CD9B F18AEB9B 56E0C110 56FAE6A3`

$\tilde{K} - 283$:

Enačba:	$y^2 + xy = x^3 + 1$
Št. točk:	$4 * 3885337784451458141838923813647037813284811733793061324295$8\ 749975298158297044226038 73
Nerazcepen polinom:	$t^{283} + t^{12} + t^7 + t^5 + 1$
P_x:	`503213F 78CA4488 3F1A3B81 62F188E5 53CD265F 23C1567A 16876913 B0C2AC24 58492836`
P_y:	`1CCDA38 0F1C9E31 8D90F95D 08E5426F E87E45C0 E8184698 E4596236 4E341161 77DD2259`

$K - 283$:

Enačba:	$y^2 + xy = x^3 + x^2 + 1$
Št. točk:	$2 * 7770675568902916283677847627294075626569631244830993521422$\ 749282851602622232822777663

Nerazcepen polinom: $t^{283} + t^{12} + t^7 + t^5 + 1$

P_x:
```
 521CD3A 6B3993BB 5EFDDFD6 B69A09B7 1CB97313 A2236842
323762E9 F35A62EE 3205CCDC
```

P_y:
```
 3B17F17 83AFEEF6 62A66AA9 032E73B3 4DC37FC7 9E9417BE
2C456BF6 F25FA1AB 61B92E75
```

$\tilde{K} - 409$:

Enačba: $y^2 + xy = x^3 + 1$

Št. točk:
```
4*330527984395124299475957654016385519914202341482140609642 32\
  439502288071128924919105067325845777745801409636659061773 13\
  58671
```

Nerazcepen polinom: $t^{409} + t^{87} + 1$

P_x:
```
 060F05F 658F49C1 AD3AB189 0F718421 0EFD0987 E307C84C
27ACCFB8 F9F67CC2 C460189E B5AAAA62 EE222EBA B35540CF
E9023746
```

P_y:
```
 1E36905 0B7C4E42 ACBA1DAC BF04299C 3460782F 918EA427
E6325165 E9EA10E3 DA5F6C42 E9C55215 AA9CA27A 5863EC48
D8E0286B
```

$\tilde{K} - 571$:

Enačba: $y^2 + xy = x^3 + 1$

Št. točk:
```
4*193226876150862917234767594546599367214946366485321749932 86\
  176257257595711447802122681339785227067118347067128008253 51\
  461273674974066617311929682421617092503555733685276673
```

Nerazcepen polinom: $t^{571} + t^{10} + t^5 + t^2 + 1$

P_x:
```
 26EB7A8 59923FBC 82189631 F8103FE4 AC9CA297 0012D5D4
60248048 01841CA4 43709584 93B205E6 47DA304D B4CEB08C
BBD1BA39 494776FB 988B4717 4DCA88C7 E2945283 A01C8972
```

P_y:
```
 349DC80 7F4FBF37 4F4AEADE 3BCA9531 4DD58CEC 9F307A54
FFC61EFC 006D8A2C 9D4979C0 AC44AEA7 4FBEBBB9 F772AEDC
B620B01A 7BA7AF1B 320430C8 591984F6 01CD4C14 3EF1C7A3
```