Eliptičke krivulje u kriptografiji

Andrej Dujella

PMF – MO, Sveučilište u Zagrebu, 2013.

Sadržaj

Poglavlje 1

Eliptičke krivulje nad poljem racionalnih brojeva

1.1 Uvod u eliptičke krivulje

Neka je $\mathbb{K}$ polje. *Eliptička krivulja* nad $\mathbb{K}$ je nesingularna projektivna kubna krivulja nad $\mathbb{K}$ s barem jednom ($\mathbb{K}$-racionalnom) točkom. Ona ima (afinu) jednadžbu oblika

$$F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0,$$

gdje su koeficijenti $a, b, c, \dots, j \in \mathbb{K}$, a nesingularnost znači da je u svakoj točki na krivulji, promatranoj u projektivnoj ravnini $\mathbb{P}^2(\overline{\mathbb{K}})$ nad algebarskim zatvorenjem od $\mathbb{K}$, barem jedna parcijalna derivacija funkcije F različita od 0. Svaka takva jednadžba može se biracionalnim transformacijama (racionalnim transformacijama čiji je inverz također racionalna transformacija) svesti na oblik

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

koji nazivamo *Weierstrassova forma*.

Nadalje, ako je karakteristika polja $\mathbb{K}$ različita od 2 i 3 (pa smijemo nadopunjavati na potpun kvadrat i potpun kub, dijeleći s 2 i 3 ako je potrebno), onda se ova jednadžba može transformirati u oblik

$$y^2 = x^3 + ax + b,$$

koji nazivamo *kratka Weierstrassova forma*. Uvjet nesingularnosti je sada da kubni polinom $f(x) = x^3+ax+b$ nema višestrukih nultočaka (u algebarskom zatvorenju $\overline{\mathbb{K}}$), a to je pak ekvivalentno uvjetu da je *diskriminanta* $D = -4a^3 - 27b^2$ različita od 0.

Mi ćemo često pod eliptičkom krivuljom nad poljem $\mathbb{K}$ (karakteristike različite od 2 i 3) podrazumijevati skup svih točaka $(x, y) \in \mathbb{K} \times \mathbb{K}$ koji zadovoljavaju jednadžbu

$$E: \quad y^2 = x^3 + ax + b,$$

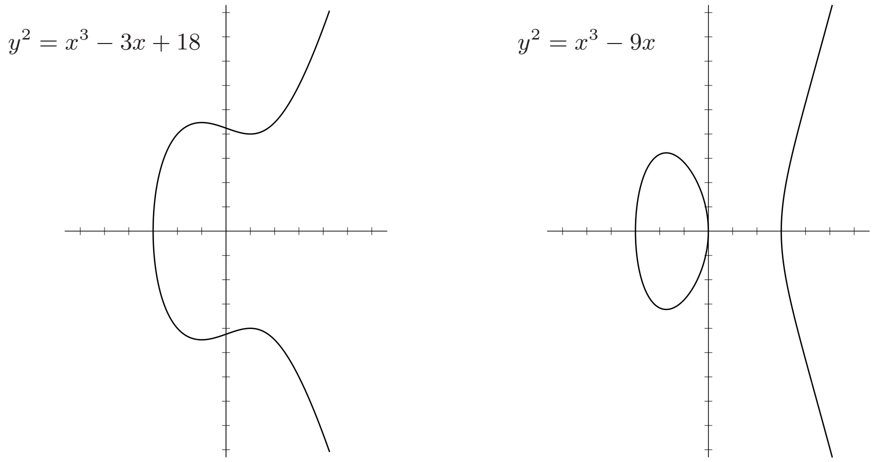
gdje su $a, b \in \mathbb{K}$ i $4a^3 + 27b^2 \neq 0$, zajedno s "točkom u beskonačnosti" $\mathcal{O}$. Taj skup ćemo označavati s $E(\mathbb{K})$.

Točka u beskonačnosti se pojavljuje prirodno ukoliko eliptičku krivulju prikažemo u projektivnoj ravnini. *Projektivnu ravninu* $\mathbb{P}^2(\mathbb{K})$ dobijemo tako da na skupu $\mathbb{K}^3 \setminus \{(0,0,0)\}$ uvedemo relaciju ekvivalencije $(X,Y,Z) \sim (kX,kY,kZ)$, $k \in \mathbb{K}$, $k \neq 0$. Ako u (afinoj) jednadžbi eliptičke krivulje uvedemo supstituciju $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, dobivamo projektivnu jednadžbu

$$Y^2 Z = X^3 + aXZ^2 + bZ^3.$$

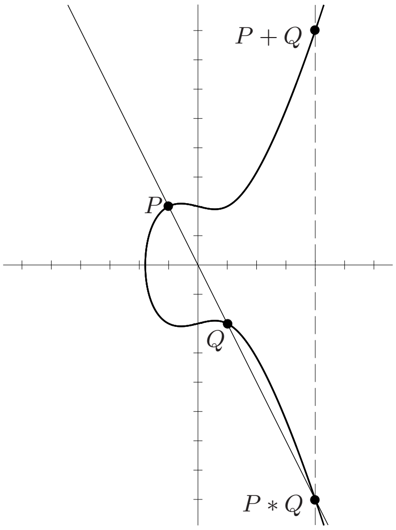
Ako je $Z \neq 0$, onda klasa ekvivalencije od (X,Y,Z) ima reprezentant $(x,y,1)$, pa tu klasu možemo identificirati s (x,y). Međutim, postoji i jedna klasa ekvivalencije koja sadrži točke za koje je $Z = 0$. Ona ima reprezentant $(0,1,0)$ i tu klasu identificiramo s točkom u beskonačnosti $\mathcal{O}$.

Jedno od najvažnijih svojstava eliptičkih krivulja jest da se na njima može, na prirodan način, uvesti operacija uz koju one postaju Abelove grupe. Da bismo to objasnili, uzmimo da je $\mathbb{K} = \mathbb{R}$ polje realnih brojeva. Tada eliptičku krivulju $E(\mathbb{R})$ (bez točke u beskonačnosti) možemo prikazati kao podskup ravnine. Polinom $f(x)$ može imati ili 1 ili 3 realna korijena. U ovisnosti o tome, graf pripadne eliptičke krivulje ima jednu ili dvije komponente, kao što je prikazano na sljedećim slikama.

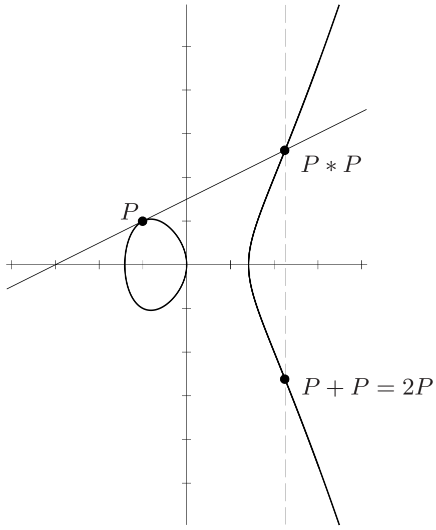


1 komponenta **2 komponente**

Definirat ćemo operaciju zbrajanja na $E(\mathbb{R})$. Neka su $P, Q \in E(\mathbb{R})$. Povucimo pravac kroz točke P i Q. On siječe krivulju E u tri točke. Treću točku označimo s $P * Q$. Sada definiramo da je $P + Q$ osnosimetrična točka točki $P * Q$ obzirom na os x. Ako je $P = Q$, onda umjesto sekante povlačimo tangentu kroz točku P. Po definiciji stavljamo da je $P + \mathcal{O} = \mathcal{O} + P = P$ za svaki $P \in E(\mathbb{R})$.



sekanta



tangenta

Dakle, operacija (zbrajanje) na skupu $E(\mathbb{R})$ se uvodi "geometrijski", tako da su tri točke na krivulji E kolinearne ako i samo ako im je suma jednaka neutralnom elementu $\mathcal{O}$. Naravno da se ovaj geometrijski zakon može opisati i eksplicitnim formulama za koordinate zbroja točaka. Tako dobivene formule onda mogu poslužiti za definiciju zbrajanja točaka na eliptičkoj krivulji nad proizvoljnim poljem (uz malu modifikaciju ako je karakteristika polja 2 ili 3). Navedimo sada te formule.

Neka je $P = (x_1, y_1)$, $Q = (x_2, y_2)$. Tada je

1) $-\mathcal{O} = \mathcal{O}$;

2) $-P = (x_1, -y_1)$;

3) $\mathcal{O} + P = P$;

4) ako je $Q = -P$, onda je $P + Q = \mathcal{O}$;

5) ako je $Q \neq -P$, onda je $P + Q = (x_3, y_3)$, gdje je

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = -y_1 + \lambda(x_1 - x_3),$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{ako je } x_2 \neq x_1, \\ \frac{3x_1^2 + a}{2y_1}, & \text{ako je } x_2 = x_1. \end{cases}$$

Broj λ je koeficijent smjera pravca kroz P i Q, odnosno tangente u točki P u slučaju $P = Q$. Uvršavanjem jednadžbe pravca kroz točku P, tj. $y = \lambda(x - x_1) + y_1$ u jednadžbu eliptičke krivulje, te izjednačavanjem koeficienata uz x^2 (Vièteove formule) u $x^3 + ax + b - (\lambda(x - x_1) + y_1)^2 = (x - x_1)(x - x_2)(x - x_3)$, dobivamo navedenu formulu za koordinatu x_3.

Pokazuje se da je $(E(\mathbb{K}), +)$ Abelova grupa. Sva svojstva Abelove grupe su evidentna, osim asocijativnosti čiji je dokaz nešto kompliciraniji.

Za primjene u kriptografiji, najvažniji je slučaj kada je $\mathbb{K}$ konačno polje $\mathbb{F}_q$. Posebno su važni slučajevi $q = p$ (prost broj) i $q = 2^k$. S druge strane, u teoriji brojeva najvažniju ulogu imaju eliptičke krivulje nad poljem racionalnih brojeva $\mathbb{Q}$.

Možemo se pitati od kud dolazi naziv eliptička krivulja. Veza između eliptičkih krivulja i elipse dolazi preko problema računanja opsega elipse. Neka je elipsa zadana jednadžbom $q^2x^2 + p^2y^2 = p^2q^2$. Tada je njezin opseg jednak vrijednosti integrala

$$4p \int_0^1 \frac{1 - (p^2 - q^2)t^2}{\sqrt{(1 - t^2)(1 - (p^2 - q^2)t^2)}}\, dt.$$

Pomoću racionalne supstitucije, ovaj se integral može svesti na sličan integral u kojem se pod korijenom nalazi kubna funkcija. Općenito se integrali u kojima je javljaju drugi korijeni polinoma trećeg ili četvrtog stupnja nazivaju *eliptički integrali*. Oni se ne mogu izraziti pomoću elementarnih funkcija. Međutim, moguće ih je izraziti pomoću *Weierstrassove* $\wp$*-funkcije*. Ova funkcija zadovoljava diferencijalnu jednadžbu oblika

$$\left(\frac{\wp'}{2}\right)^2 = \wp^3 + a\wp + b.$$

Ovdje je njena uloga analogna ulozi funkcije sinus (ili kosinus) u računanju integrala kod kojih se ispod korijena javljaju kvadratne funkcije. Naime, funkcija $y = \sin x$ zadovoljava diferencijalnu jednadžbu $y^2+(y')^2 = 1$. Slično kao što jediničnu kružnicu možemo parametrizirati pomoću $(\cos t, \sin t)$, tako se kompleksne točke na eliptičkoj krivulji $y^2 = x^3 + ax + b$ mogu parametrizirati pomoću $(\wp(t), \frac{1}{2}\wp'(t))$. Štoviše, pokazuje se da ako je $P = (\wp(t), \frac{1}{2}\wp'(t))$ i $Q = (\wp(u), \frac{1}{2}\wp'(u))$, onda je $P + Q = (\wp(t + u), \frac{1}{2}\wp'(t + u))$. Dakle, zbrajanje točaka na $E(\mathbb{C})$ odgovara zbrajanju kompleksnih brojeva. Poznavanje te činjenice daje elegantni dokaz asocijativnosti zbrajanja točaka na eliptičkoj krivulji.

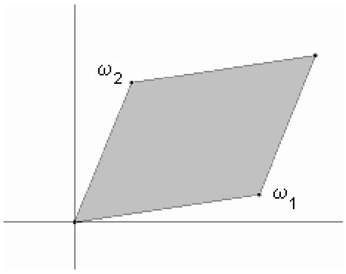
Kad se promatra nad poljem $\mathbb{R}$, eliptička krivulja je stvarno "krivulja", tj. 1-dimenzionalni objekt. No, promatrana nad $\mathbb{C}$ ona postaje 2-dimenzionalni objekt ("ploha") u 4-dimenzionalnom prostoru. Pokušajmo vizualizirati tu plohu.

Tu nam može pomoći funkcija $\wp$. Ona posjeduje mnoga važna svojstva. Jedno njih jest da je dvostruko periodična, tj. postoje kompleksni brojevi ω_1 i ω_2 (takvi da $\omega_1/\omega_2 \notin \mathbb{R}$) sa svojstvom $\wp(z + m\omega_1 + n\omega_2) = \wp(z)$ za sve cijele brojeve m, n. Označimo s L "rešetku" svih točaka oblika $m\omega_1 + n\omega_2$. Funkcija $\wp$ je analitička u svim točkama kompleksne ravnine, osim u točkama iz rešetke L u kojima ima pol drugog reda (tj. $\wp$ je meromorfna funkcija). Naime, vrijedi da je

$$\wp(z) = \frac{1}{z^2} + \sum_{w\in L,\, w\neq 0} \left(\frac{1}{(z - w)^2} - \frac{1}{w^2}\right).$$

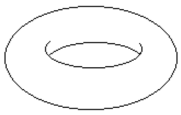
Općenito se meromorfne, dvostruko periodične funkcije nazivaju *eliptičke funkcije*.

Gore navedena parametrizacija točaka na eliptičkoj krivulji pomoću funkcije $\wp$ predstavlja zapravo izomorfizam grupa $E(\mathbb{C})$ i $\mathbb{C}/L$. Funkcija $\wp$ je u potpunosti određena svojim vrijednostima u "fundamentalnom paralelogramu" koji se sastoji od svih kompleksnih brojeva oblika $\alpha\omega_1 + \beta\omega_2$, $0 \leq \alpha, \beta < 1$.



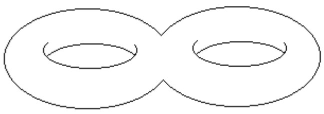
fundamentalni paralelogram

Razlika točaka koje se nalaze nasuprot jedna drugoj na paralelnim stranicama tog paralelograma je element iz L. Stoga su te točke poistovjećene u skupu $\mathbb{C}/L$. Da bi vizualizirali taj skup, možemo zamisliti da smo najprije "slijepili" dvije suprotne stranice paralelograma. Tako dobivamo valjak. Nakon toga "slijepimo" baze toga valjka. Tako dobivamo torus:



torus

Torus možemo zamisliti i kao sferu s "rupom". Pokazuje se da se svaka algebarska krivulja može prikazati u trodimenzionalnom prostoru kao sfera s konačno mnogo rupa.



2-torus

Taj broj rupa se naziva *genus* ili *rod* krivulje. Alternativna (šira) definicija eliptičke krivulje je da je to algebarska krivulja genusa jednakog 1. Ova definicija uključuje ne samo nesingularne kubne krivulje, već i sve one krivulje koje su im biracionalnog ekvivalentne. Biracionalne transformacije čuvaju genus krivulje, ali ne čuvaju njezin stupanj.

Ako krivulja ima stupanj n, onda je njezin genus $\leq (n-1)(n-2)/2$, s time da ako je krivulja nesingularna, onda joj je genus upravo jednak $(n-1)(n-$

$2)/2$. Poznato je da tzv. hipereliptičke krivulje čija je jednadžba $y^2 = f(x)$, gdje je $f(x)$ polinom stupnja $n \geq 3$ bez višestrukih korijena, imaju genus $\lfloor (n-1)/2 \rfloor$. To posebno znači da, pored slučaja kada je $n = 3$, i u slučaju kad je $n = 4$ (i krivulja ima barem jednu racionalnu točku) također imamo eliptičku krivulju. Uvjerimo se u to na jednom primjeru. Neka je C krivulja zadana jednadžbom

$$y^2 = x^4 + 3x^2 + 2x.$$

Ona ima očitu racionalnu točku $(0,0)$. Supstitucijama $x = \frac{2}{v}$, $y = \frac{2t}{v^2}$ dobivamo krivulju $t^2 = v^3 + 3v^2 + 4$, te konačno supstitucijom $v + 1 = s$ dobivamo eliptičku krivulju E u kratkoj Weiestrassovoj formi

$$t^2 = s^3 - 3s + 6.$$

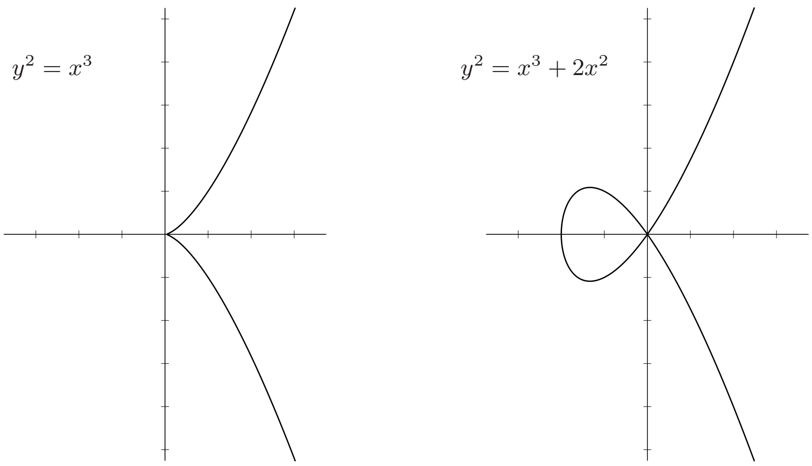
Dakle, transformacija koja prevodi C u E je $x = \frac{2}{s-1}$, $y = \frac{2t}{(s-1)^2}$. Inverzna transformacija je $s = \frac{x+2}{x}$, $t = \frac{2y}{x^2}$. Stoga je ovo biracionalna transformacija.

Genus krivulje igra važnu ulogu kod klasifikacije diofantskih jednadžbi. Naime, o njemu ovisi broj cjelobrojnih, odnosno racionalnih rješenja jednadžbe, te struktura skupa tih rješenja.

Krivulje genusa 0 su upravo one koje posjeduju parametrizaciju pomoću racionalnih funkcija. Svaka krivulja drugog stupnja (konika) ima genus 0. Npr. krivulja $x^2 + y^2 = 1$ ima racionalnu parametrizaciju

$$x = \frac{2t}{t^2+1}, \quad y = \frac{t^2-1}{t^2+1}.$$

Kubne singularne krivulje također imaju genus 0. Npr. krivulja $y^2 = x^3$ ima singularnu točku $(0,0)$ (šiljak - *cusp*). Stoga ova kubna krivulja nije eliptička. Njezina racionalna parametrizacija je $x = t^2$, $y = t^3$. Kao drugi primjer navedimo krivulju $y^2 = x^3 + 2x^2$. Ona također ima singularnu točku $(0,0)$ (čvor - *node*) i ima racionalnu parametrizaciju $x = t^2 - 2$, $y = t^3 - 2t$.



sing. krivulja - šiljak **sing. krivulja - čvor**

Očito je da ove dvije kubne krivulje imaju beskonačno mnogo cjelobrojnih točaka. Pellova jednadžba $x^2 - dy^2 = 1$ (d prirodan broj koji nije potpun kvadrat) je primjer krivulje drugog stupnja koja ima beskonačno mnogo cjelobrojnih točaka. Krivulja genusa 1 može imati samo konačno mnogo cjelobrojnih točaka. Racionalnih točaka može biti beskonačno mnogo, ali su "konačno generirane" (sve se mogu dobiti iz konačno točaka primjenom grupovne operacije na eliptičkoj krivulji). Krivulja genusa većeg od 1 može imati samo konačno mnogo racionalnih točaka. Ova tvrdnja je poznata Mordellova slutnja koju je 1983. godine dokazao Faltings.

1.2 Jednadžbe eliptičke krivulje

Često se eliptičke krivulje prikazuju u dugoj Weierstrassovoj formi

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Ta je forma "dobra" nad svakim poljem (bez obzira na karakteristiku), a vrlo je prikladna za opis eliptičkih krivulja nad $\mathbb{Q}$ s točakama zadanog konačnog reda. Pokažimo kao se od nje (u karakteristici različitoj od 2 i 3) dobiva kratka Weierstrassova forma. Supstitucijom $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ eliminiramo sve članove koji sadrže y, osim y^2 (ovo možemo napraviti ako karakteristika nije 2, pa smijemo dijeliti s 2). Dobivamo

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

gdje je

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6. \end{aligned}$$

Još se definira i $b_8 = \frac{1}{4}(b_2b_6 - b_4^2) = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2$. Uočimo da ako svakom a_i pridijelimo "težinu" i, onda je svaki od b_i-ova homogeni izraz težine i.

Ako je karakteristika različita i od 3, onda možemo uvesti supstitucije $x \mapsto \frac{x-3b_2}{36}$, $y \mapsto \frac{y}{108}$, te dobiti jednadžbu u kratkoj Weirstrassovoj formi

$$y^2 = x^3 - 27c_4x - 54c_6,$$

gdje je

$$\begin{aligned} c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

Formula za zbrajanje dvaju točaka na eliptičkoj krivulji u kratkoj Weierstrassovoj formi zahtjeva dva množenja, jedno kvadriranje i jedno dijeljenje u polju. Budući da je dijeljenje obično znatno sporije od množenja, od interesa su alternativne jednadžbe (koordinate) u kojima dijeljenje ne bi bilo nužno. I zaista, dijeljenje se može izbjeći korištenjem projektivnih koordinata.

Za tu svrhu mogu se iskoristiti već i standarne projektivne koordinate, tj. one u kojima projektivnoj točki (X, Y, Z) odgovara afina točka $(\frac{X}{Z}, \frac{Y}{Z})$. No, pokazuje se da jedna modifikacija projektivnih koordinata vodi do efikasnijih formula za zbrajanje, a naročito za dupliciranje točaka. To su *Jacobijeve* ili *težinske projektivne koordinate* u kojima projektivnoj točki (X, Y, Z) odgovara afina točka $(\frac{X}{Z^2}, \frac{Y}{Z^3})$ (prvoj koordinati smo dali težinu 2, a drugoj 3). Tada jednadžba eliptičke krivulje postaje

$$Y^2 = X^3 + aXZ^4 + bZ^6. \tag{1.1}$$

Točka u beskonačnosti sada ima koordinate $(1, 1, 0)$.

U ovim novim koordinatama se kod računanja zbroja točaka uopće ne pojavljuje dijeljenje. Neka su $P = (X_1, Y_1, Z_1)$, $Q = (X_2, Y_2, Z_2)$ točke za krivulji (1.1). Tada se koordinate točke $P+Q = (X_3, Y_3, Z_3)$ mogu izračunati pomoću:

$$r = X_1Z_2^2, \quad s = X_2Z_1^2, \quad t = Y_1Z_2^3, \quad u = Y_2Z_1^3, \quad v = s - r, \quad w = u - t,$$
$$X_3 = -v^3 - 2rv^2 + w^2, \quad Y_3 = -tv^3 + (rv^2 - X_3)w, \quad Z_3 = vZ_1Z_2.$$

dok se koordinate točke $P + P = (X_4, Y_4, Z_4)$ dobivaju na sljedeći način:

$$v = 4X_1Y_1^2, \quad w = 3X_1^2 + aZ_1^4,$$
$$X_4 = -2v + w^2, \quad Y_4 = -8Y_1^4 + (v - X_3)w, \quad Z_4 = 2Y_1Z_1.$$

Zbroj $P + Q$ se može izračunati uz 16 množenja (preciznije: 12 množenja i 4 kvadriranja), a zbroj $P + P$ uz 10 množenja (preciznije: 4 množenja i 6 kvadriranja). U primjenama se ponekad izabire parametar $a = -3$. Razlog je taj da se kod $P + P$ u računanju veličine w može uštediti jedno množenje zbog

$$w = 3(X_1^2 - Z_1^4) = 3(X_1 + Z_1^2)(X_1 - Z_1^2).$$

Vratimo se sada na Weierstrassovu jednadžbu

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Pomoću njenih koeficijenata a_1, a_2, a_3, a_4, a_6, definirali smo veličine $b_2, b_4, b_6, b_8, c_4, c_6$. Pomoću njih možemo definirati još dvije važne veličine:

- *diskriminantu* $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = \frac{c_4^3 - c_6^2}{1728}$,
- j*-invarijantu* $j = \frac{c_4^3}{\Delta}$.

Krivulja je nesingularna ako i samo ako je $\Delta \neq 0$. Ovako definirana diskriminanta je jednaka $1/16 \times$ (diskriminanta polinoma $4x^3 + b_2x^2 + 2b_4x + b_6$). Općenito se diskriminanta polinoma f stupnja n s vodećim koeficijentom a_n i korijenima $x_1, \ldots, x_n$ (iz $\overline{\mathbb{K}}$) definira kao

$$\mathrm{Dis}(f) = a_n^{2n-2} \prod_{i<j}^{n} (x_i - x_j)^2$$

i jednaka je 0 ako i samo ako f ima višestrukih korijena. Ako je eliptička krivulja dana jednadžbom $y^2 = x^3 + ax + b$, onda je $\Delta = -16(4a^3 + 27b^2)$. Za krivulje definirane nad $\mathbb{R}$, predznak diskriminante nam govori koliko komponenti ima graf krivulje: ako je $\Delta < 0$, onda imamo jednu komponentu, a ako je $\Delta > 0$, onda imamo dvije komponente.

Naziv j-invarijanta dolazi od toga što izomorfne krivulje imaju iste j-invarijante. Najopćenitiji oblik izomorfizma između dvaju eliptičkih krivulja danih općom Weierstrassovom formom je

$$\begin{aligned} x &= u^2x' + r, \\ y &= u^3y' + su^2x' + t, \end{aligned}$$

gdje je $r, s, t \in \mathbb{Q}$ i $u \in \mathbb{Q}^*$. Efekt ovih supstitucija na koeficijente a_i je

$$\begin{aligned} ua_1' &= a_1 + 2s, \\ u^2a_2' &= a_2 - sa_1 + 3r - s^2, \\ u^3a_3' &= a_3 + ra_1 + 2t, \\ u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st, \\ u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1, \end{aligned}$$

odakle se dobiva da vrijedi

$$u^4c_4' = c_4, \quad u^6c_6' = c_6, \quad u^{12}\Delta' = \Delta, \quad j' = j.$$

U slučaju kratkih Weierstrassovih formi jedine dopustive supstitucije su

$$x = u^2x', \quad y = u^3y', \quad u \in \mathbb{Q}^*.$$

Vrijedi i svojevrstan obrat ovog svojstva j-invarijanti. Naime, dvije eliptičke krivulje su izomorfne nad algebarskim proširenjem $\overline{\mathbb{Q}}$ ako i samo ako imaju istu j-invarijantu.

Ako promatramo krivulje nad algebarski zatvorenim poljem, onda nam j-invarijanta govori jesu li krivulje izomorfne. No, ako polje nije algebarski zatvoreno, primjerice ako promatramo krivulje nad $\mathbb{Q}$, onda dvije krivulje mogu imati jednake j-invarijante, ali da se ne mogu transformirati jedna u drugu pomoću racionalnih funkcija s koeficijentima iz $\mathbb{Q}$. Na primjer, krivulje $y^2 = x^3 - 4x$ i $y^2 = x^3 - 25x$ obje imaju $j = 1728$. Prva od njih ima konačno mnogo racionalnih točaka, dok ih druga ima beskonačno mnogo (točka $(-4, 6)$ je beskonačnog reda). Dakle, ove krivulje nisu izomorfne nad $\mathbb{Q}$, ali jesu nad $\mathbb{Q}(\sqrt{10})$ (supstitucije su $(x, y) \mapsto (u^2x, u^3y)$, $u = \frac{\sqrt{10}}{2}$).

Za $j \neq 0, 1728$, krivulja

$$y^2 = x^3 + \frac{3j}{j - 1728}x + \frac{2j}{j - 1728}$$

ima j-invarijantu upravo jednaku j. Krivulje oblika $y^2 = x^3 + b$ imaju j-invarijantu jednaku 0, dok krivulje oblika $y^2 = x^3 + ax$ imaju j invarijantu jednaku $1728 = 12^3$.

Neka je E eliptička krivulja definirana nad $\mathbb{Q}$. Promjenom varijabli, ako je potrebno, možemo pretpostaviti da je E dana jednadžbom

$$y^2 = x^3 + ax + b, \tag{1.2}$$

gdje su $a, b \in \mathbb{Z}$. Za prost broj $p > 3$, možemo promatrati jednadžbu $y^2 = x^3 + ax + b \pmod p$. Ako je ovom jednadžbom definirana eliptička krivulja nad poljem $\mathbb{F}_p$ ($\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ uz operacije zbrajanja i množenja modulo p), onda kažemo da E ima *dobru redukciju* modulo p. Kod prostih brojeva s lošom redukcijom, kubni polinom $x^3 + ax + b$ ima višestruki korijen modulo p. Ako polinom ima trostruki korijen, kažemo da E ima *aditivnu redukciju*, a ako polinom ima dvostruki korijen, onda kažemo da E ima *multiplikativnu redukciju*. Dodatno se razlikuje rascjepiva i nerascjepiva multiplikativna redukcija. Rascjepiva je ako su koeficijenti smjera tangenata u singularnoj točki iz $\mathbb{F}_p$, a nerascjepiva inače. Ovo posljednje se može odrediti tako da se jednadžba krivulje napiše u obliku $y^2 = x^2(x + c)$. Jednadžbe tangenti u singularnoj točki $(0, 0)$ su $y = \pm\sqrt{c}x$, pa vidimo da ćemo imati rascjepivu multiplikativnu redukciju ako i samo ako je c kvadrat u $\mathbb{F}_p$.

Uočimo da za krivulju E postoji više izbora za $a, b \in \mathbb{Z}$ u prikazu (1.2). U gornjim (neformalnim) definicijama pretpostavljamo da su a, b izabrani tako da E ima "najbolja moguća" svojstva. Dakle, za svaki p tražimo a, b sa svojstvom da kubni polinom $x^3 + ax + b$ ima što više različitih korijena modulo p, te da je diskriminanta $-16(4a^3 + 27b^2)$ djeljiva sa što manjom potencijom broja p. Kažemo da je takva jednadžba minimalna za p. Pokazuje se da je moguće izabrati takve a, b koji imaju ovo svojstvo da sve p. Pripadna jednadžba se naziva (globalna) *minimalna Weirstrassova jednadžba* od E.

Da bi se analogni pojmovi definirali za $p = 2$ i $p = 3$, trebamo gledati opću (dugu) Weierstrassovu formu.

Primjer 1.1. *Promotrimo eliptičku krivulju nad $\mathbb{Q}$ zadanu jednadžbom*

$$y^2 = x^3 - 270000x + 128250000.$$

Njezina diskriminanta je $\Delta = -2^{12}3^{12}5^{12}11$. Zaključujemo da E ima dobru redukciju svugdje, osim možda u $2, 3, 5, 11$. Također, odmah vidimo da se loša redukcija u $p = 11$ neće moći ukloniti (jer se diskriminante izomorfnih krivulja razlikuju za faktor u^{12}), dok je za $2, 3, 5$ to možda moguće. Supstitucijama

$$x = 25x_1, \quad y = 125y_1$$

dobivamo jednadžbu

$$y_1^2 = x_1^3 - 432x_1 + 8208,$$

čija je diskriminanta $-2^{12}3^{12}11$, pa E ima dobru redukciju u 5.

Kod razmatranja redukcije u 2 i 3 morat ćemo odustati od kratke Weierstrassove forme. Supstitucijama

$$x_1 = 9x_2 - 12, \quad y_1 = 27y_2$$

dobivamo jednadžbu

$$y_2^2 = x_2^3 - 4x_2^2 + 16, \tag{1.3}$$

čija je diskriminanta $-2^{12}11$, pa E ima dobru redukciju i u 3.

Konačno, supstitucijom

$$x_2 = 4x_3, \quad y_2 = 8y_3 + 4$$

dobivamo jednadžbu

$$y_3^2 + y_3 = x_3^3 - x_3^2. \tag{1.4}$$

Ova krivulja je nesingularna za $p = 2$, jer joj je diskriminanta jednaka -11 (drugi način da se to vidi je iz parcijalne derivacije po y, tj. $2y + 1 = 1$, koja je uvijek različita od nule). Stoga E ima dobru redukciju u 2.

Zaključujemo da E ima dobru redukciju u svim prostim brojevima, osim u $p = 11$, gdje ima lošu redukciju. Jednadžba (1.4) je minimalna Weierstrassova jednadžba od E.

Promotrimo još malo situaciju za $p = 11$, i to preko jednadžbe (1.3). U $\mathbb{F}_{11}$ imamo:

$$x_2^3 - 4x_2^2 + 16 = (x_2 + 1)^2(x_2 + 5),$$

pa vidimo da E ima multiplikativnu redukciju u $p = 11$. Tangente u singularnoj točki $(x_2, y_2) = (-1, 0)$ imaju koeficijente smjera $\pm 2 \in \mathbb{F}_{11}$ (jer jednadžba $\alpha^2 = 4$ ima rješenja u $\mathbb{F}_{11}$), pa E ima rascjepivu multiplikativnu redukciju u $p = 11$. $\diamondsuit$

Globalna minimalna jednadžba od E ima svojstvo da joj je $|\Delta|$ minimalno među svim cjelobrojnim modelima od E. U izomorfizmu između dvije minimalne jednadžbe mora biti $u = \pm 1$, dok su $r, s, t \in \mathbb{Z}$. Izborom parametara r, s, t uvijek se može postići da je $a_1, a_3 \in \{0, 1\}$, $a_2 \in \{-1, 0, 1\}$. Jednadžba koja zadovoljava ove uvjete zove se *reducirana*. Nije teško za vidjeti da je jedina transformacija (osim identitete) koja jednu reduciranu jednadžbu preslikava u drugu reduciranu jednadžbu transformacija $(r, s, t, u) = (0, -a_1, -a_3, -1)$; to je transformacija koja točki (x, y) pridružuje njezin inverz $-(x, y) = (x, -y - a_1x - a_3)$ i ne mijenja jednadžbu.

Zaključujemo da svaka eliptička krivulja ima jedinstvenu reduciranu minimalnu Weierstrassovu jednadžbu. Ova činjenica omogućava vrlo lako razlikovanje krivulja. Tako da se u različitim tablicama s podacima o konkretnim eliptičkim krivuljama najčešće nalaze samo podaci za reducirane minimalne jednadžbe.

Neka je eliptička krivulja dana jednadžbom s cjelobrojnim koeficijentima. Za prost broj p i cijeli broj n, označimo s $\mathrm{ord}_p(n)$ najveću potenciju od

p koja dijeli n. Ako je $\text{ord}_p(\Delta) < 12$ ili $\text{ord}_p(c_4) < 4$ ili $\text{ord}_p(c_6) < 6$, onda je ta jednadžba minimalna za prost broj p. Ako je $p \neq 2, 3$, onda vrijedi i obrat: ako je $\text{ord}_p(\Delta) \geq 12$ i $\text{ord}_p(c_4) \geq 4$, onda jednadžba nije minimalna za p. Situacija s $p = 2$ i $p = 3$ je kompliciranija. Tu se minimalna jednadžba za p može izračunati Tateovim algoritmom. To je algoritam koji računa minimalne jednadžbe za svaki p, globalnu minimalnu jednadžbu, konduktor, Kodairine simbole, te lokalne indekse c_p.

Za krivulju definiranu nad $\mathbb{Q}$ se definira veličina povezana s diskriminantom koja se naziva *konduktor*:

$$N = \prod_p p^{f_p}.$$

Ako je $p \neq 2, 3$, onda se f_p može lako odrediti iz minimalnog Weierstrassovog modela za E:

- $f_p = 0$ ako $p \nmid \Delta$;
- $f_p = 1$ ako $p | \Delta$ i $p \nmid c_4$;
- $f_p \geq 2$ ako $p | \Delta$ i $p | c_4$; ako je $p \neq 2, 3$, onda je $f_p = 2$.

U tablicama eliptičkih krivulja, od kojih su najpoznatije one Cremonine (`http://www.warwick.ac.uk/~masgaj/book/fulltext/index.html`, `http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html`, `http://www.math.utexas.edu/users/tornaria/cnt/cremona.html`), uglavnom se navode samo minimalne Weierstrassove jednadžbe krivulje, dok su krivulje obično sortirane prema svom konduktoru. Najmanji N za kojeg postoje krivulje s konduktorom jednakim N je $N = 11$. Sljedeće krivulje imaju konduktor 11:

$$y^2 + y = x^3 - x^2,$$

$$y^2 + y = x^3 - x^2 - 10x - 20,$$

$$y^2 + y = x^3 - x^2 - 7820x - 263580.$$

Diskriminante su im redom: -11, -11^5, -11. Prve dvije imaju točke reda 5, dok zadnja nema netrivijalnih racionalnih točaka. Treća krivulja je zanimljiva i po tome što predstavlja jedini poznati primjer krivulje čija minimalna jednadžba zadovoljava $|a_4| > \Delta^3$.

Sljedeće mogućnosti za konduktor su $N = 14, 15, 17, 20, 21, 24, 26, \ldots$. Sve krivulje s konduktorom manjim od 37 imaju samo konačno mnogo racionalnih točaka (imaju rang jednak 0). Jedna od krivulja s konduktorom 37,

$$y^2 + y = x^3 - x,$$

ima točku beskonačnog reda $(0, 0)$ (i rang jednak 1).

1.3 Eliptičke krivulje u programskom paketu PARI/GP

U programskom paketu PARI/GP (`http://pari.math.u-bordeaux.fr/`) implementiran je veći broj važnijih funkcija vezanih uz eliptičke krivulje. Sada ćemo navesti samo neke, dok ćemo ostale spomenuti onda kada se prirodno pojave u gradivu koje ćemo obrađivati (popis svih funkcija vezanih uz eliptičke krivulje može se dobiti sa `?5`).

Pretpostavljamo da je krivulja dana u Weierstrassovoj formi

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

te ju u PARI-ju reprezentiramo kao pet-komponentni vektor

$$e = [a_1, a_2, a_3, a_4, a_6].$$

Točke na E su reprezentirane kao dvo-komponentni vektori $[x, y]$, osim točke u beskonačnosti koja je reprezentirana kao jedno-komponentni vektor $[0]$.

Prije primjene bilo koje od ostalih funkcija, eliptičku krivulje "inicijaliziramo" pomoću funkcije `ellinit`.

$E =$ `ellinit`(e): računa sljedeće podatke za eliptičku krivulju nad $\mathbb{Q}$:

$$a_1,\ a_2,\ a_3,\ a_4,\ a_6,\ b_2,\ b_4,\ b_6,\ b_8,\ c_4,\ c_6,\ \Delta,\ j.$$

Npr. diskriminanta od E se može dobiti kao $E[12]$ ili E.`disc`, dok je j-invarijanta $E[13]$ ili E.`j`. Koeficijenti c_4 i c_6 se dobivaju kao E.`c4` i E.`c6`.

Sljedećih 6 podataka je opcionalno (i ovise nad kojim poljem je definirana krivulja, a ako ih ne trebamo, onda možemo koristiti `ellinit`$(E, 1)$):

- $E[14]$ ili E.`roots` je vektor čije su komponente korijeni polinoma na desnoj strani pridružene Weierstrassove jednadžbe

$$(y + a_1x/2 + a_3/2)^2 = g(x).$$

- $E[15]$ ili E.`omega`$[1]$ je realni, a $E[16]$ ili E.`omega`$[2]$ je kompleksni period od E. Drugim riječima, $\omega_1 = E[15]$ i $\omega_2 = E[16]$ čine bazu kompleksne rešetke od E.
- $E[17]$ i $E[18]$ (ili E.`eta`) su vrijednosti η_1 i η_2 za koje vrijedi $\eta_1\omega_2 - \eta_2\omega_2 = i\pi$.
- $E[19]$ ili E.`area` je površina fundamentalnog paralelograma od E.

`elladd`$(E, P1, P2)$: zbroj točaka $P1$ i $P2$ na eliptičkoj krivulji E.

`ellsub`$(E, P1, P2)$: razlika $P1 - P2$ točaka na eliptičkoj krivulji E.

`ellpow`(E, P, n): višekratnik nP točke P na eliptičkoj krivulji E.

`ellordinate`(E, x): daje vektor koji sadrži y-koordinate točka na eliptičkoj krivulji E čija je x-koordinata jednaka x.

`ellisoncurve`(E, P): daje 1 (tj. "istina") ako je P točka na E, a 0 (tj. "laž") inače.

`ellchangecurve`(E, v): daje eliptičku krivulju koja se iz E dobije pomoću supstitucija koje su određene vektorom $v = [u, r, s, t]$, tj. veza starih koordinata x, y i novih x', y' je dana sa $x = u^2x' + r$, $y = u^3y' + su^2x' + t$.

`ellminimalmodel`$(E, \&v)$: daje reducirani minimalni model za eliptičku krivulju nad $\mathbb{Q}$. Opcionalnoj varijabli v pridružuje se vektor $[u, r, s, t]$ koji daje odgovarajuću promjenu varijabli, tako da je krivulja koja se dobije pomoću ove funkcije upravo `ellchangecurve`(E, v).

`ellglobalred`(E): računa konduktor, globalni minimalni model od E i globalni Tamagawin broj c. Rezultat ove funkcije je tro-komponentni vektor $[N, v, c]$, gdje je N konduktor, v daje promjenu varijabli pomoću koje se iz E dobiva minimalni integralni model (`ellminimalmodel`), dok je c produkt lokalnih Tamagawinih brojeva c_p, što je veličina koja se pojavljuje u eksplicitnoj verziji Birch i Swinnerton-Dyerove slutnje.

`ellwp`$(E, \{z = x\})$: računa vrijednost u z Weierstrassove $\wp$ funkcije pridružene eliptičkoj krivulji E (zadanoj sa `ellinit` ili kao rešetka $[\omega_1, \omega_2]$).

`ellpointtoz`(E, P): računa kompleksan broj z (modulo rešetka određena sa E) koji odgovara točki P (njezin parametar), tj. $\wp(z) = P[1]$, $\wp'(z)/2 = P[2]$.

`ellztopoint`(E, z): računa koordinate $[x, y]$ točke na eliptičkoj krivulji E koja odgovara kompleksnom broju z. Dakle, ovo je inverzna funkcija od `ellpointtoz`. Točka $[x, y]$ prikazuje vrijednost Weierstrassove $\wp$ funkcije i njezine derivacije u točki z. Ako je z točka rešetke koja definira E nad $\mathbb{C}$, onda je rezultat ove funkcije točka u beskonačnosti $[0]$.

Primjer 1.2. *Ilustrirat ćemo korištenje nekih funkcija iz PARI-ja na primjeru eliptičke krivulje iz Primjera 1.1.*

```
? E=ellinit([0,0,0,-270000,128250000],1)
%1 = [0, 0, 0, -270000, 128250000, 0, -540000, 513000000,
-72900000000, 12960000, -110808000000, -5845851000000000000,
-4096/11]
? factor(E.disc)
%2 = [-1 1] [2 12] [3 12] [5 12] [11 1]
? F=ellminimalmodel(E, &v);
? [F.a1,F.a2,F.a3,F.a4,F.a6]
%3 = [0, -1, 1, 0, 0]
? v
%4 = [30, -300, 0, 13500]
```

```
? ellordinate(F,0)
%5 = [0, -1]
? P = [0, 0]; for(n=2,5,print(ellpow(F,P,n)))
[1, -1] [1, 0] [0, -1] [0]
```
$\diamondsuit$

Primjer 1.3. *U ovom primjeru ćemo uzeti krivulju*

$$y^2 + y = x^3 - x,$$

za koju smo rekli da je krivulja s najmanjim konduktorom koja ima beskonačno mnogo cjelobrojnih točaka.

```
? E=ellinit([0,0,1,-1,0],1)
%1 = [0, 0, 1, -1, 0, 0, -2, 1, -1, 48, -216, 37, 110592/37]
? P = [0,0]
%2 = [0,0]
? ellisoncurve(E,P)
%3 = 1
? for(n=2,8,print(ellpow(E,P,n)))
[1, 0] [-1, -1] [2, -3] [1/4, -5/8] [6, 14] [-5/9, 8/27]
[21/25, -69/125]
? E=ellinit([0,0,1,-1,0]);
? t1 = ellpointtoz(E,P)
%4 = 0.9295927152853956744051993444589580060б +
1.225694690993395030427112415933262б127*I
? t2 = ellpointtoz(E,[2, -3])
%5 = 0.7249122149096230677887873983833238464б +
1.5930919111324522771 E-58*I
? t2 - 4*t1
%6 = -2.9934586462319596298320099794525081778 -
4.902778763973580121708449663733050450 7*I
? E.omega[1]
%7 = 2.993458646231959629832009979452508177 8
? 2*E.omega[2]
4.902778763973580121708449663733050450 7*I
? G=ellglobalred(E)
%8 = [37, [1, 0, 0, 0], 1]
? cond = G[1]
%9 = 37
```
$\diamondsuit$

1.4 Računanje torzijske grupe

Najvažnija činjenica o eliptičkim krivuljama nad $\mathbb{Q}$ jest Mordell-Weilov teorem.

Teorem 1.1 (Mordell-Weil)**.** *Grupa $E(\mathbb{Q})$ je konačno generirana Abelova grupa.*

Mordell-Weilov teorem nam, drugim riječima, kaže da postoji konačan skup racionalnih točaka $P_1, \dots, P_k$ na E iz kojih se sve ostale racionalne točke na E mogu dobiti povlačeći sekante i tangente. Kako je svaka konačno generirana abelova grupa izomorfna produktu cikličkih grupa (preciznije, produktu oblika $\mathbb{Z}^n \times \mathbb{Z}_{k_1} \times \cdots \times \mathbb{Z}_{k_m}$ tako da $k_1 \mid k_2 \mid \cdots \mid k_m$, gdje je $\mathbb{Z}_k = \mathbb{Z}/k\mathbb{Z}$), dobivamo sljedeću neposrednu posljedicu Mordell-Weilovog teorema.

Korolar 1.1.
$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

Podgrupa $E(\mathbb{Q})_{\text{tors}}$ od $E(\mathbb{Q})$ koja se sastoji od svih točaka konačnog reda naziva se *torzijska grupa* od E, a nenegativni cijeli broj r se naziva *rang* od E i označava se s rank(E) (preciznije rank$(E(\mathbb{Q}))$). Korolar nam kaže da postoji r racionalnih točaka $P_1, \dots, P_r$ beskonačnog reda na krivulji E sa svojstvom da se svaka racionalna točka P na E može prikazati u obliku

$$P = T + m_1 P_1 + \cdots + m_r P_r,$$

gdje je T neka točka konačnog reda, a $m_1, \dots, m_r$ cijeli brojevi. Ovdje $m_1 P_1$ označava sumu $P_1 + \cdots + P_1$ od m_1 pribrojnika, koja se često označava i sa $[m_1]P_1$.

Postavlja se pitanje koje sve vrijednosti mogu poprimiti $E(\mathbb{Q})_{\text{tors}}$ i rank(E). Nadalje, pitanje je kako ih izračunati za konkretnu krivulju E. Pokazuje se da je puno lakše dati odgovore na ova pitanja za torzijsku grupu, nego za rang.

Promotrimo na trenutak točke konačnog reda nad $\mathbb{C}$ i $\mathbb{R}$. Rekli smo da se eliptička krivulja nad $\mathbb{C}$ može poistovijetiti s kvocijentnom grupom $\mathbb{C}/L$, gdje je $L = \{m_1\omega_1 + m_2\omega_2 \,:\, m_1, m_2 \in \mathbb{Z}\}$. Stoga je $nP = \mathcal{O}$ ako i samo ako je parametar od P oblika $\frac{m_1}{n}\omega_1 + \frac{m_2}{n}\omega_2$, $0 \le m_1, m_2 < n$. Dakle, rješenja jednadžbe $nP = \mathcal{O}$ čine grupu izomorfnu sa $\mathbb{Z}_n \times \mathbb{Z}_n$.

Općenito se za krivulju E nad poljem $\mathbb{K}$ i prirodan broj n definira

$$E[n] = \{P \in E(\overline{\mathbb{K}}) \,:\, nP = \mathcal{O}\}.$$

Može se pokazati da vrijedi:

- ako karakteristika od $\mathbb{K}$ ne dijeli n ili je jednaka 0, onda je $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$;

- ako karakteristika p od $\mathbb{K}$ dijeli n i $n = p^r n'$ uz $p \nmid n'$, onda je $E[n] \cong \mathbb{Z}_{n'} \times \mathbb{Z}_{n'}$ ili $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_{n'}$.

U slučaju krivulje s realnim koeficijentima, jedan od perioda, recimo ω_1, je realan, dok je drugi, ω_2, čisto imaginaran. Točkama iz $E(\mathbb{R})$ odgovaraju parametri $t \in [0, \omega_1\rangle$, te u slučaju kad graf od E ima dvije komponente još i $t - \frac{1}{2}\omega_2 \in [0, \omega_1\rangle$. Dakle, grupa $E(\mathbb{R})$ je izomorfna ili grupi kružnice S^1 (kada je $\Delta < 0$) ili $\mathbb{Z}_2 \times S^1$ (kada je $\Delta > 0$). Rješenja jednadžbe $nP = \mathcal{O}$ čine grupu izomorfnu sa $\mathbb{Z}_n$ ili $\mathbb{Z}_2 \times \mathbb{Z}_n$.

Vratimo se sada na krivulje nad $\mathbb{Q}$. Iz onoga što smo do sada pokazali, slijedi da bi grupa $E(\mathbb{Q})_{\text{tors}}$ trebala biti konačna podgrupa od S^1 ili $\mathbb{Z}_2 \times S^1$. No, poznato je da su sve konačne podgrupe od S^1 cikličke. Stoga je $E(\mathbb{Q})_{\text{tors}}$ izomorfno jednoj od grupa oblika $\mathbb{Z}_k$ ili $\mathbb{Z}_2 \times \mathbb{Z}_{2k}$ (ako je k neparan onda je $\mathbb{Z}_2 \times \mathbb{Z}_k \cong \mathbb{Z}_{2k}$).

Mazur je 1978. godine dokazao da postoji točno 15 mogućih torzijskih grupa za eliptičke krivulje nad $\mathbb{Q}$. To su grupe:

$$\begin{aligned} \mathbb{Z}_k, &\quad \text{za } k = 1,2,3,4,5,6,7,8,9,10,12 \\ \mathbb{Z}_2 \times \mathbb{Z}_k, &\quad \text{za } k = 2,4,6,8. \end{aligned}$$

Točke reda 2 na krivulji $y^2 = x^3 + ax^2 + bx + c$, su upravo točke s y-koordinatom jednakom 0. Možemo imati 0, 1 ili 3 takve točke, što ovisi o broju racionalnih nultočaka polinoma $x^3 + ax^2 + bx + c$. Te točke, zajedno s točkom $\mathcal{O}$, čine podgrupu od $E(\mathbb{Q})_{\text{tors}}$ koja je ili trivijalna ili jednaka $\mathbb{Z}_2$ ili jednaka $\mathbb{Z}_2 \times \mathbb{Z}_2$. Ostale točke konačnog reda možemo naći pomoću Lutz-Nagellovog teorema. Ideja je naći model krivulje u kome će sve torzijske točke biti cjelobrojne. To je upravo model s jednadžbom $y^2 = x^3+ax^2+bx+c$ kojeg dobijemo s opće Weierstrassove jednadžbe eliminirajući članove uz xy i y (supstitucijama s $u = 2$ ako je potrebno). Ako je $a_1 = a_3 = 0$, onda već Weierstrassova jednadžba ima željeni oblik; inače stavimo $a = b_2$, $b = 8b_4$, $c = 16b_6$. Potom se za torzijsku točku $P = (x, y)$ iskoristi činjenica da i P i $2P$ imaju cjelobrojne koordinate da bi se dobila ocjena za y. Često se Lutz-Nagellov teorem navodi na jednadžbu oblika $y^2 = x^3+ax+b$, što nije gubitak općenitosti budući da se član uz x^2 može eliminirati nadopunjavanjem na potpun kub, međutim, to eliminiraniranje uključuje dodatno skaliranje koordinata, te za rezultat ima (nepotrebno) veću ocjenu za y. Primijetimo da kod krivulje s općom Weierstrassovom jednadžbom za točku konačnog reda $P(x, y)$ vrijedi da su $4x$ i $8y$ cijeli brojevi.

Teorem 1.2 (Lutz-Nagell). *Neka je E eliptička krivulja zadana jednadžbom*

$$y^2 = f(x) = x^3 + ax^2 + bx + c, \tag{1.5}$$

gdje su $a, b, c \in \mathbb{Z}$. Ako je $P = (x_1, y_1)$ točka konačnog reda u $E(\mathbb{Q})$, tada su $x_1, y_1 \in \mathbb{Z}$.

Propozicija 1.1. *Neka je E eliptička krivulja zadana jednadžbom (1.5), gdje su $a, b, c \in \mathbb{Z}$. Ako je $P = (x_1, y_1)$ točka konačnog reda u $E(\mathbb{Q})$, tada je ili $y_1 = 0$ ili $y_1^2 | \Delta_0$, gdje je $\Delta_0 = -\Delta/16 = 27c^2 + 4a^3c + 4b^3 - a^2b^2 - 18abc$. .*

Dokaz: Ako je $2P = \mathcal{O}$, onda je $P = -P = (x_1, -y_1)$, pa je $y_1 = 0$. U protivnom je $2P = (x_2, y_2)$, gdje je po Lutz-Nagellovom teoremu $x_2, y_2 \in \mathbb{Z}$. Iz formule za zbrajanje na E imamo $2x_1 + x_2 = \lambda^2 - a$, gdje je $\lambda = \frac{f'(x_1)}{2y_1}$ koeficijent smjera tangente na E u točki P. Vidimo da je $\lambda \in \mathbb{Z}$, što povlači da je $y_1 | f'(x_1)$. Sada iz formule

$$\Delta_0 = (-27f(x) + 54c + 4a^3 - 18ab)f(x) + (f'(x) + 3b - a^2)f'(x)^2 \quad (1.6)$$

i $y_1^2 = f(x_1)$ slijedi da $y_1^2 | \Delta_0$. Formula (1.6) se dobije primjenom (proširenog) Euklidovog algoritma na polinome $f(x)$ i $(f'(x))^2$ (u PARI-ju, funkcija `bezout`(f, g) daje 3-komponentni vektor $[u, v, d]$ tako da je $d = \mathrm{nzd}(f, g)$, te $u \cdot f + v \cdot g = d$). □

Lutz-Nagellov teorem nam daje konačnu listu kandidata za torzijske točke. Točnije, daje nam kandidate za y-koordinate točaka. No, da dani y, nije teško naći cjelobrojna rješenja jednadžbe $x^3 + ax^2 + bx + c - y^2 = 0$ (ili ispitivanjem faktora od $y^2 - c$ ili preko Cardanovih formula za rješenja kubne jednadžbe). Ako je P torzijska točka, onda za svaki prirodan broj n, točka nP mora biti ili $\mathcal{O}$ ili jedna od točaka s liste. Budući je lista konačna, ili ćemo dobiti da je $nP = mP$ za neke $m \neq n$, u kojem je slučaju $(n - m)P = \mathcal{O}$ i točka P torzijska, ili će neki višekratnik nP biti izvan liste pa P nije torzijska. Alternativno, možemo koristiti i Mazurov teorem, po kojem je red svake torzijske točke ≤ 12. Stoga, ako je $nP \neq \mathcal{O}$ za $n \leq 12$, onda P nije torzijska.

Pretpostavimo da smo našli sve torzijske točke, te da nakon toga želimo odrediti strukturu torzijske grupe. Prema Mazurovom teoremu jedini slučajevi kada red grupe ne određuje u potpunosti strukturu grupe su slučajevi $|E(\mathbb{Q})_{\text{tors}}| = 4$, 8 i 12, kada imamo dvije mogućnosti: $\mathbb{Z}_{4k}$ ili $\mathbb{Z}_2 \times \mathbb{Z}_{2k}$. Ako imamo jednu točku reda 2, onda je $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_{4k}$, a ako imamo tri točke reda dva, onda je $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}_2 \times \mathbb{Z}_{2k}$.

Primjer 1.4. *Odredimo torzijsku grupu eliptičke krivulje*

$$E : \quad y^2 = x^3 + x.$$

Rješenje: Imamo $\Delta_0 = 4$. Stoga svaka torzijska točka $P = (x, y)$ mora zadovoljavati ili $y = 0$, ili $y | 2$. Dakle, $y \in \{0, 1, -1, 2, -2\}$. Lako se vidi da jednadžbe $x^3 + x = 1$ i $x^3 + x = 4$ nemaju cjelobrojnih rješenja, dok je $x = 0$ jedino cjelobrojno rješenje jednadžbe $x^3 + x = 0$. To znači da je $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0, 0)\} \cong \mathbb{Z}_2$. ♢

Primjer 1.5. *Odredimo torzijsku grupu eliptičke krivulje*

$$E : \quad y^2 = x^3 + 8.$$

Rješenje: Ovdje je $\Delta_0 = 1728$. Ako je $y = 0$, onda je $x = -2$, pa imamo točku $(0, -2)$ reda 2. Ako je $y \neq 0$, onda $y^2|1728$, tj. $y|24$. Testiranjem svih mogućnosti, nalazimo sljedeće točke s cjelobrojnim koordinatama: $P_1 = (1, 3)$, $P_2 = (2, 4)$, $-P_1 = (1, -3)$, $-P_2 = (2, -4)$. Računajući višekratnike dobivamo

$$2P_1 = \left(-\frac{7}{4}, -\frac{13}{8}\right), \quad 2P_2 = \left(-\frac{7}{4}, \frac{13}{8}\right).$$

Budući da koordinate točaka $2P_1$ i $2P_2$ nisu cjelobrojne, zaključujemo da su točke P_1 i P_2 beskonačnog reda. Dakle, $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0, -2)\} \cong \mathbb{Z}_2$. $\diamondsuit$

Problem s primjenom Lutz-Nagellovog teorem može se javiti ukoliko je teško faktorizirati diskriminantu Δ, ili ukoliko ona ima jako puno kvadratnih faktora.

Tada nam može pomoći sljedeća činjenica

Propozicija 1.2. *Neka je E eliptička krivulja zadana jednadžbom*

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

gdje su $a, b, c \in \mathbb{Z}$. Neka je p neparan prost broj takav da $p \nmid \Delta_0$, te neka je

$$\rho_p : E(\mathbb{Q}) \to E(\mathbb{F}_p)$$

redukcija modulo p. Ako je točka $P \in E(\mathbb{Q})$ konačnog reda i $\rho_p(P) = \mathcal{O}$, onda je $P = \mathcal{O}$.

Dokaz: Po Lutz-Nagellovom teoremu sve torzijske točke (osim $\mathcal{O}$) imaju cjelobrojne koordinate, pa se kod redukcije modulo p ne reduciraju u $\mathcal{O}$. $\square$

Po Propoziciji 1.2, jezgra restrikcije preslikavanja ρ_p na $E(\mathbb{Q})_{\text{tors}}$ je trivijalna. Slika te restrikcije je podgrupa od $E(\mathbb{F}_p)$, pa kako red podrupe dijeli red grupe, zaključujemo da $|E(\mathbb{Q})_{\text{tors}}|$ dijeli $|E(\mathbb{F}_p)|$. Ako uzmemo nekoliko vrijednosti od p, tada najveći zajednički dijelitelj g pripadnih vrijednosti od $|E(\mathbb{F}_p)|$ mora biti višekratnik od $|E(\mathbb{Q})_{\text{tors}}|$.

Kasnije ćemo govoriti detaljnije o efikasnim metoda za računanje reda od $E(\mathbb{F}_p)$ za velike p-ove. No, u primjenama na računanje torzijske grupe p-ovi su u pravilu vrlo mali (biramo najmanje neparne p-ove koji ne dijele diskriminantu), tako da je tu za računanje $|E(\mathbb{F}_p)|$ sasvim zadovoljavajuća sljedeća formula pomoću Legendreovog simbola:

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right).$$

U PARI-ju se $|E(\mathbb{F}_p)|$ može dobiti kao $p + 1 -$ `ellap`(E, p). Verzija `ellap`$(E, p, 1)$ koristi upravo navedenu formulu pomoću Legendreovih simbola, dok `ellap`$(E, p, 0)$ ili `ellap`(E, p) koristi Shanks-Mestreovu metodu koja je efikasnija za $p > 100$.

Primjer 1.6. *Odredimo torzijsku grupu eliptičke krivulje*

$$E\ :\ \ y^2 = x^3 + 18x + 72.$$

Rješenje: Ovdje je $\Delta_0 = 4\cdot 18^3 + 27\cdot 72^2 = 163296 = 2^5\cdot 3^6\cdot 7$. Koristeći Lutz-Nagellov teorem trebali bismo testirati sve djelitelje $y|108$. Umjesto toga, možemo provjeriti da je $|E(\mathbb{F}_5)| = 5$ i $|E(\mathbb{F}_{11})| = 8$, odakle, budući da je $\mathrm{nzd}(5,8) = 1$, direktno slijedi da je torzijska grupa od $E(\mathbb{Q})$ trivijalna. $\diamondsuit$

U prethodnom primjeru je bilo $g = 1$, pa nismo trebali tražiti torzijske točke. Postavlja se pitanje, ukoliko postoje netrivijalne torzijske točke, možemo li ih naći bez korištenja Lutz-Nagellovog teorema (i pripadne faktorizacije). Promatramo djelitelje n od g, krenuvši od najvećeg prema najmanjem, i tražimo točku reda n na E (uzimajući u obzir koji n-ovi su mogući prema Mazurovom teoremu).

Koristit ćemo vezu s kompleksnim, odnosno realnim točkama od E. Već smo rekli da točke u fundamentalnom paralelogramu koje odgovaraju realnim, pa onda i racionalnim, točkama leže na segmentu $[0,\omega_1\rangle$, te u slučaju kad graf od E ima dvije komponente još i na segmentu $\frac{1}{2}\omega_2 + [0,\omega_1\rangle$. Dupliciranjem točke iz drugog segmenta, dobiva se točka iz prvog segmenta. Dakle, ako je n neparan, sve točke P reda n dolaze od parametara sa segmenta $[0,\omega_1\rangle$. Preciznije, parametar im je oblika $\frac{m}{n}\omega_1$, gdje je $\mathrm{nzd}(m,n) = 1$. Neka je $mm' \equiv 1 \pmod{n}$. Onda je i $m'P$ točka reda n, a njezin parametar je $\frac{1}{n}\omega_1$. Stoga vrijednost $\wp(\frac{1}{n}\omega_1)$ mora biti cijeli broj.

Ako je n paran, onda slično kao gore dobivamo da jedan od brojeva $\wp(\frac{1}{n}\omega_1)$, $\wp(\frac{1}{n}\omega_1 + \frac{1}{2}\omega_2)$ ili $\wp(\frac{1}{n}\omega_1 + \frac{1}{2}\omega_1 + \frac{1}{2}\omega_2)$ mora biti cijeli.

Dakle, algoritam (*Doudov algoritam* iz 1998. godine) je sljedeći: računamo

- $\wp(\frac{1}{n}\omega_1)$ ako je n neparan ili ako je $\Delta < 0$;
- $\wp(\frac{1}{n}\omega_1)$, $\wp(\frac{1}{n}\omega_1 + \frac{1}{2}\omega_2)$, $\wp(\frac{1}{n}\omega_1 + \frac{1}{2}\omega_1 + \frac{1}{2}\omega_2)$ ako je n paran i $\Delta > 0$

za svaki djelitelj od g. Naravno, vrijednost funkcije $\wp$ ne možemo izračunati egzaktno, već s određenom preciznošću. Ako nađemo da je neka od vrijednosti $\wp$-funkcije vrlo blizu cijelog broja, onda testiramo hoće li taj cijeli broj x dati cjelobrojnu vrijednost y koja zadovoljava jednadžbu eliptičke krivulje. Za tako dobivenu točku $P = (x,y)$, računamo nP da provjerimo je li stvarno P točka reda n. Ako je tako, onda smo dobili najveću cikličku podgrupu torzijske grupe, te još samo trebamo vidjeti postoji li neka točka reda 2 koja nije sadržana u toj cikličkoj podgrupi. Ako dobijemo da je $nP \neq \mathcal{O}$, onda nastavljamo s manjim djeliteljima od g. Ovim postupkom dobivamo sve torzijske točke od $E(\mathbb{Q})$.

Primjer 1.7. *Odredimo torzijsku grupu eliptičke krivulje*

$$E\ :\ \ y^2 = x^3 - 58347x + 3954150.$$

Rješenje: Imamo da je $4a^3 + 27b^2 = -372386507784192 = -2^{18} \cdot 3^{17} \cdot 11$. Primijetimo da u našem rješenju nećemo koristiti ovu faktorizaciju. Možemo najprije uzeti $p = 5$. Dobivamo da je $|E(\mathbb{F}_5)| = 10$. Zatim dobivamo $|E(\mathbb{F}_7)| = 10$. I bez poznavanja potpune faktorizacije, lako bismo provjeriti da 11 dijeli diskriminantu. Stoga nastavljamo s $p = 13$. Dobivamo da je $|E(\mathbb{F}_{13})| = 10$. Zatim uzimamo $p = 17$ i dobivamo da je $|E(\mathbb{F}_{17})| = 20$. Zaključujemo da red torzijske grupe dijeli broj 10. Periodi su

$$\omega_1 = 0.198602\ldots \quad \omega_2 = 0.156713\ldots i.$$

Računamo (koristeći PARI)

$$\wp(\frac{1}{10}\omega_1) = 2539.825532\ldots,$$

što vidimo da nije blizu cijelog broja. Međutim,

$$\wp(\frac{1}{10}\omega_1 + \frac{1}{2}\omega_2) = -213.000000\ldots$$

ima traženo svojstvo i daje nam racionalnu točku

$$(x, y) = (-213, 2592)$$

na krivulji E (za $\wp(\frac{1}{10}\omega_1 + \frac{1}{2}\omega_1 + \frac{1}{2}\omega_2)$ se dobije $58.174468\ldots$). Sada se lako provjeri da ova točka ima red 10.

Budući da smo već prije zaključili da red torzijske grupe dijeli 10, dobivamo da je torzijska grupa izomorfna sa $\mathbb{Z}_{10}$ s generatorom $(-213, 2592)$. Konačno računamo višekratnike ove točke i dobivamo

$$\begin{aligned} E(\mathbb{Q})_{\text{tors}} = \{&\mathcal{O}, (-213, 2592), (651, -15552), (3, 1944), (219, -1296), (75, 0), \\ &(219, 1296), (3, -1944), (641, 15552), (-213, -2592)\}. \end{aligned}$$

$\diamondsuit$

Metode za određivanje torzijske grupe eliptičke krivulje nad $\mathbb{Q}$ koje smo opisali u ovom poglavlju implementirane su u programskom paketu PARI/GP preko funkcije `elltors`. Verzija `elltors`$(E, 1)$ koristi Lutz-Nagellov teorem, dok `elltors`$(E, 0)$ ili `elltors`(E) koristi Doudov algoritam. Rezultat je 3-komponentni vektor $[t, v1, v2]$, gdje je t red torzijske grupe, $v1$ daje strukturu torzijske grupe kao produkta cikličkih grupa, dok $v2$ daje generatore tih cikličkih grupa.

1.5 Konstrukcija krivulja sa zadanom torzijskom grupom

Već smo spomenuli da je 1978. godine Mazur dokazao sljedeći teorem

Teorem 1.3. *Postoji točno 15 mogućih torzijskih grupa za eliptičke krivulje nad $\mathbb{Q}$. To su grupe:*

$$\begin{aligned} \mathbb{Z}_k, &\quad \textit{za } k = 1,2,3,4,5,6,7,8,9,10,12 \\ \mathbb{Z}_2 \times \mathbb{Z}_k, &\quad \textit{za } k = 2,4,6,8. \end{aligned}$$

Težina ovog rezultata leži u dokazivanju da se grupe koje nisu navedene u teoremu ne mogu pojaviti kao torzijske grupe eliptičke krivulje nad $\mathbb{Q}$.

Mi ćemo sada pokazati kako se za svaku od 15 grupa navedenih u Mazurovom teoremu može konstruirati beskonačno mnogo eliptičkih krivulja s tom torzijskom (pod)grupom. Najprije ćemo promotriti ciklički slučaj, tj. torzijske grupe oblika $\mathbb{Z}_k$.

Eliptičke krivulje ćemo tražiti u (dugoj) Weierstrassovoj formi

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.7}$$

Stoga navedimo formule za zbrajanje točaka na krivulji danoj sa (1.7): ako je $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, onda je $P_1 + P_2 = (x_3, y_3)$, gdje je

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

$$y_3 = -(\lambda + a_1)x_3 - \mu - a_3,$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{ako je } x_2 \neq x_1, \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & \text{ako je } P_2 = P_1, \end{cases}$$

$$\mu = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, & \text{ako je } x_2 \neq x_1, \\ \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}, & \text{ako je } P_2 = P_1. \end{cases}$$

Nadalje, $-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$.

Neka je P točka iz $E(\mathbb{Q})$ reda k. Bez smanjenja općenitosti možemo pretpostaviti da je $P = (0,0)$ (supstitucijom, tj. translacijom, $(x, y) \mapsto (x - x_P, y - y_p)$). Tada je u jednadžbi (1.7) $a_6 = 0$, a zbog nesingularnosti je jedan od brojeva a_3 i a_4 različit od nule.

Pretpostavimo najprije da je P točka reda 2. To znači da je $P = -P = (0, -a_3)$, pa je $a_3 = 0$. Dakle, za krivulje s jednadžbom

$$y^2 + a_1xy = x^3 + a_2x^2 + a_4x$$

je točka $P = (0,0)$ drugog reda.

Ako točka P nije točka drugog reda, onda možemo pretpostaviti da je $a_4 = 0$ (pa mora biti $a_3 \neq 0$) (linearnom supstitucijom $(x, y) \mapsto (x, y + a_3^{-1}a_4x)$ koja čuva točku $(0,0)$). Dakle, ubuduće ćemo promatrati krivulje oblika

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2.$$

Pretpostavimo da je P točka na toj krivulji reda 3. Tada je $-P = 2P$, pa iz $-P = (0, -a_3)$ i $2P = (-a_2, a_1a_2 - a_3)$, zaključujemo da je $3P = \mathcal{O}$ ako i samo ako je $a_2 = 0$. Dakle, krivulje s jednadžbom

$$y^2 + a_1xy + a_3y = x^3$$

imaju torzijsku podgrupu izomorfnu sa $\mathbb{Z}_3$.

U preostalim slučajevima možemo pretpostaviti da su a_2 i a_3 različiti od nule. Stavimo $u = a_3^{-1}a_2$. Supstitucija $(x, y) \mapsto \left(\frac{x}{u^2}, \frac{y}{u^3}\right)$ čuva točku $P = (0, 0)$, dok jednadžba krivulje postaje

$$y^2 + a_3^{-1}a_1a_2xy + a_3^{-2}a_2^3y = x^3 + a_3^{-2}a_2^3x^2.$$

Uvodimo oznake $b = -a_3^{-2}a_2^3$, $c = 1 - a_3^{-1}a_1a_2$, te dobivamo jednadžbu krivulje u *Tateovoj normalnoj formi*

$$y^2 + (1 - c)xy - by = x^3 - bx^2 \tag{1.8}$$

(primijetimo da su koeficijenti b i c težine 0). U ovim jednadžbama, prvih nekoliko višekratnika točke P ima vrlo jednostavne koordinate. Nama će trebati koordinate točaka $\pm P, \pm 2P, \ldots \pm 6P$ (da bismo preko njih izrazili uvjete $kP = \mathcal{O}$ za $k = 4, 5, \ldots, 10, 12$). Dobivamo:

$$-P = (0, b),\ \ 2P = (b, bc),\ \ -2P = (b, 0),\ \ 3P = (c, b - c),\ \ -3P = (c, c^2),$$

$$4P = \left(\frac{b(b-c)}{c^2}, \frac{-b^2(b-c-c^2)}{c^3}\right), \quad -4P = \left(\frac{b(b-c)}{c^2}, \frac{b(b-c)^2}{c^3}\right),$$

$$5P = \left(\frac{-bc(b-c-c^2)}{(b-c)^2}, \frac{bc^2(b^2-bc-c^3)}{(b-c)^3}\right),$$

$$-5P = \left(\frac{-bc(b-c-c^2)}{(b-c)^2}, \frac{b^2(b-c-c^2)^2}{(b-c)^3}\right),$$

$$6P = \left(\frac{(c-b)(c^3+bc-b^2)}{(c-b+c^2)^2}, \frac{c(c-b)^2(bc^2-c^2+3bc-2b^2)}{(c-b+c^2)^3}\right),$$

$$-6P = \left(\frac{(c-b)(c^3+bc-b^2)}{(c-b+c^2)^2}, \frac{c(c^3+bc-b^2)^2}{(c-b+c^2)^3}\right).$$

Iz koordinata ovih točaka zaključujemo redom:

- Točka P je reda 4, tj. $2P = -2P$ ako i samo ako je $c = 0$. Dakle, opći oblik krivulje s torzijskom podgrupom $\mathbb{Z}_4$ je

$$y^2 + xy - by = x^3 - bx^2, \quad b \in \mathbb{Q}.$$

- Točka P je reda 5, tj. $3P = -2P$ ako i samo ako je $b = c$. Dakle, opći oblik krivulje s torzijskom grupom $\mathbb{Z}_5$ je

$$y^2 + (1 - b)xy - by = x^3 - bx^2, \quad b \in \mathbb{Q}.$$

- Točka P je reda 6, tj. $3P = -3P$ ako i samo ako je $b = c + c^2$. Dakle, opći oblik krivulje s torzijskom podgrupom $\mathbb{Z}_6$ je

$$y^2 + (1-c)xy - (c+c^2)y = x^3 - (c+c^2)x^2, \quad c \in \mathbb{Q}.$$

- Točka P je reda 7, tj. $4P = -3P$ ako i samo ako je $b(b-c) = c^3$. Jednadžbu $b^2 - bc = c^3$ možemo shvatiti kao jednadžbu singularne kubike, sa singularitetom u $(b,c) = (0,0)$. Uvrstimo $b = cd$ u jednadžbu, pa dobivamo parametrizaciju $c = d^2 - d$, $b = d^3 - d^2$. Dakle, opći oblik krivulje s torzijskom grupom $\mathbb{Z}_7$ je

$$y^2 + (1-c)xy - by = x^3 - bx^2, \quad b = d^3 - d^2,\ \ c = d^2 - d,\ \ d \in \mathbb{Q}.$$

- Točka P je reda 8, tj. $4P = -4P$ ako i samo ako je $-b(b-c-c^2) = (b-c)^2$. Ponovo smo dobili singularnu jednadžbu sa singularitetom u $(b,c) = (0,0)$. Uvrštavanjem $b = cd$, dobivamo $cd = 2d^2 - 3d + 1 = (2d-1)(d-1)$, pa je $c = \frac{(2d-1)(d-1)}{d}$, $b = (2d-1)(d-1)$. Dakle, opći oblik krivulje s torzijskom grupom $\mathbb{Z}_8$ je

$$\begin{gathered} y^2 + (1-c)xy - by = x^3 - bx^2, \\ b = (2d-1)(d-1),\ \ c = \tfrac{(2d-1)(d-1)}{d},\ \ d \in \mathbb{Q}. \end{gathered}$$

- Točka P je reda 9, tj. $5P = -4P$ ako i samo ako je $-c^3(b-c-c^2) = (b-c)^3$. Uvrštavanjem $b = cd$, dobivamo $c^2 - (d-1)c = (d-1)^3$. Ovo je singularna kubika sa singularitetom u $(c,d) = (0,1)$. Stavimo $c = (d-1)f$, te uvrstimo u zadnju jednadžbu. Dobivamo da je $d = f^2 - f + 1$. Dakle, opći oblik krivulje s torzijskom grupom $\mathbb{Z}_9$ je

$$\begin{gathered} y^2 + (1-c)xy - by = x^3 - bx^2, \\ b = cd,\ \ c = (d-1)f,\ \ d = f^2 - f + 1,\ \ f \in \mathbb{Q}. \end{gathered}$$

- Točka P je reda 10, tj. $5P = -5P$ ako i samo ako je $bc^2(b^2 - bc - c^3) = b^2(b-c-c^2)^2$. Ponovo uvodimo supstitucije $b = cd$ i $c = (d-1)f$, te tako dobivamo da je $d = \frac{-f^2}{f^2-3f+1}$. Dakle, opći oblik krivulje s torzijskom grupom $\mathbb{Z}_{10}$ je

$$\begin{gathered} y^2 + (1-c)xy - by = x^3 - bx^2, \\ b = cd,\ \ c = (d-1)f,\ \ d = \tfrac{-f^2}{f^2-3f+1},\ \ f \in \mathbb{Q}. \end{gathered}$$

- Konačno, točka P je reda 12, tj. $6P = -6P$ ako i samo ako je $(c-b)^2(bc^2 - c^2 + 3bc - 2b^2) = (c^3 + bc - b^2)^2$. Nakon uvrštanja supstitucija $b = cd$ i $c = (d-1)f$ u ovu jednadžbu, dobivamo $3d^2 - fd^2 - 3d - fd + f^2 + 1 = 0$. Diskriminanta ove kvadratne jednadžbe $(4f-3)(f-1)^2$

mora biti kvadrat. Dakle, opet nam se kao uvjet pojavila singularna kubika. Odavde je $f = \frac{t^2+3}{4}$, pa uvrštavanjem dobivamo $d = \frac{t^2+2t+5}{2(t+3)}$. Zaključujemo da je opći oblik krivulje s torzijskom grupom $\mathbb{Z}_{12}$

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$
$$b = cd, \quad c = (d-1)f, \quad d = \frac{t^2+2t+5}{2(t+3)}, \quad f = \frac{t^2+3}{4}, \quad t \in \mathbb{Q}.$$

Razmotrit ćemo sada torzijske grupe $\mathbb{Z}_2 \times \mathbb{Z}_k$ za $k = 2, 4, 6, 8$. Sve takve krivulje imaju tri točke reda 2. Stoga ćemo ovdje promatrati krivulje s jednadžbom

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma), \quad \alpha, \beta, \gamma \in \mathbb{Q}. \tag{1.9}$$

Jednadžba (1.9) ima tri racionalne točke reda 2, pa stoga ima torzijsku podgrupu izomorfnu sa $\mathbb{Z}_2 \times \mathbb{Z}_2$.

U konstrukciji krivulja s torzijskom grupom $\mathbb{Z}_2 \times \mathbb{Z}_4$ koristimo sljedeću činjenicu

Teorem 1.4. *Neka je E eliptička krivulja nad poljem $\mathbb{K}$,* $\operatorname{char} \mathbb{K} \neq 2, 3$. *Neka je*

$$E\ :\ y^2 = (x-\alpha)(x-\beta)(x-\gamma), \quad \alpha, \beta, \gamma \in \mathbb{K}.$$

Za točku $Q = (x_2, y_2) \in E(\mathbb{K})$ postoji točka $P = (x_1, y_1) \in E(\mathbb{K})$ takva da je $2P = Q$ ako i samo ako su $x_2 - \alpha$, $x_2 - \beta$ i $x_2 - \gamma$ potpuni kvadrati u $\mathbb{K}$.

Dokaz: Dokazat ćemo jedan smjer ovog teorema i to onaj da ako postoji točka P takva da je $Q = 2P$, onda su $x_2 - \alpha$, $x_2 - \beta$ i $x_2 - \gamma$ kvadrati.

Neka je $P = (x_1, y_1)$ točka s traženim svojstvom, te neka je $y = \lambda x + \mu$ tangenta u P. Promotrimo jednadžbu

$$(x-\alpha)(x-\beta)(x-\gamma) - (\lambda x + \mu)^2 = 0.$$

Njezini korijeni su x_1 (korijen kratnosti 2) i x_2 (jer točka $-Q = (x_2, -y_2)$ leži na tangenti). Dakle,

$$(x-\alpha)(x-\beta)(x-\gamma) - (\lambda x + \mu)^2 = (x - x_1)^2 (x - x_2). \tag{1.10}$$

Uvrstimo $x = \alpha$ u (1.10), pa dobivamo

$$-(\lambda\alpha + \mu)^2 = (\alpha - x_1)^2(\alpha - x_2),$$

odakle zaključujemo da je $x_2 - \alpha$ kvadrat. Uvrštavanjem $x = \beta$, odnosno $x = \gamma$, dobivamo da i $x_2 - \beta$ i $x_2 - \gamma$ kvadrati. □

Vratimo se sada na konstrukciju krivulja s torzijskom grupom $\mathbb{Z}_2 \times \mathbb{Z}_4$. Bez smanjenja općenitosti možemo pretpostaviti da je točka $P = (0, 0)$ jedna od točaka reda 2 i to upravo ona točka za koju postoji $Q \in E(\mathbb{Q})$ takva da je $2Q = P$. To znači da krivulja ima jednadžbu

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

te da su brojevi $-\alpha$ i $-\beta$ kvadrati u $\mathbb{Q}$. Dakle, opći oblik krivulje s torzijskom podgrupom $\mathbb{Z}_2 \times \mathbb{Z}_4$ je

$$y^2 = x(x+r^2)(x+s^2), \quad r,s \in \mathbb{Q}. \tag{1.11}$$

Točka reda 4 na (1.11) je točka $Q = (rs, rs(r+s))$. Da bi dobili krivulju s torzijskom grupom $\mathbb{Z}_2 \times \mathbb{Z}_8$, trebala bi postojati točka R (reda 8) takva da je $2R = Q$. Prema Teoremu 1.4, nužan i dovoljan uvjet za postojanje takve točke jest da rs, $r(r+s)$ i $s(r+s)$ budu kvadrati racionalnih brojeva. Dakle, imamo: $rs = u^2$ i $r^2 + u^2 = v^2$. Odavde je $r = t^2 - 1$, $u = 2t$ za neki $\in \mathbb{Q}$. Stoga je opći oblik krivulje s torzijskom podgrupom $\mathbb{Z}_2 \times \mathbb{Z}_8$

$$y^2 = x(x+r^2)(x+s^2), \quad r = t^2-1, \ \ s = \frac{4t^2}{t^2-1}, \ \ t \in \mathbb{Q}.$$

Preostala nam je torzijska grupa $\mathbb{Z}_2 \times \mathbb{Z}_6$. Da bi nju dobili, trebali bi na njoj imati točku P reda 3 (bez smanjenja općenitosti možemo pretpostaviti da joj je prva koordinata jednaka 0) za koju postoji točka Q reda 6 takva da je $2Q = P$. Po Teoremu 1.4, tada u (1.9) moramo imati $\alpha = -r^2$, $\beta = -s^2$, $\gamma = -t^2$. Dakle, dobili smo krivulju

$$y^2 = (x+r^2)(x+s^2)(x+t^2), \tag{1.12}$$

koja pored triju točaka drugog reda, ima još jednu očitu racionalnu točku $P = (0, rst)$. Ako bi točka P bila reda 3, onda bismo dobili traženu torzijsku grupu. Dakle, moramo zadovoljiti uvjet $-P = 2P$, koji daje

$$\frac{(r^2s^2 + r^2t^2 + s^2t^2)^2}{4r^2s^2t^2} - r^2 - s^2 - t^2 = 0,$$

tj.

$$(sr+ts+tr)(-sr+ts+tr)(-sr+ts-tr)(sr+ts-tr) = 0.$$

Možemo uzeti da je $t = \frac{rs}{r-s}$, pa dobivamo da je opći oblik krivulje s torzijskom podgrupom $\mathbb{Z}_2 \times \mathbb{Z}_6$

$$y^2 = (x+r^2)(x+s^2)\left(x + \frac{r^2s^2}{(r-s)^2}\right), \quad r,s \in \mathbb{Q}.$$

1.6 Kanonska visina i Mordell-Weilov teorem

Dva osnovna koraka u dokazu Mordell-Weilovog teorema su

- dokaz da je indeks $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ konačan;
- svojstva *visine* h, definirane sa $h(P) = \ln H(x)$, gdje je $P = (x, y)$ i $H(\frac{m}{n}) = \max\{|m|, |n|\}$, dok je $h(\mathcal{O}) = 0$.

Funkcija H je ponekad naziva i "naivna" visina, a h logaritamska visina. Očito je da je za svaku konstantu C skup

$$\{P \in E(\mathbb{Q}) \,:\, h(P) \leq C\}$$

konačan (nema više od $2(2e^C + 1)$ elemenata).

Želimo vidjeti koja je veza između visina točaka P i $2P$ (ugrubo koliko se puta poveća broj znamenaka u prikazu točke $2P$ u odnosu na prikaz točke P). Neka je krivulja dana jednadžbom $y^2 = x^3 + ax + b$ i $P = (x, y) \in E(\mathbb{Q})$. Tada je x-koordinata točke $2P$

$$x(2P) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}.$$

Budući da se kvadriranjem broja, njegova visina udvostručuje, a najveća potencija od x koja se pojavljuje u izrazu od $x(2P)$ je x^4, zaključujemo da je $h(2P) \approx 4h(P)$.

Primjer 1.8. *Za krivulju*

$$E : \quad y^2 + y = x^3 - x$$

i točku $P = (0, 0)$ *imamo:*

$$2P = (1, 0), \;\; 4P = (2, -3), \;\; 8P = \left(\tfrac{21}{25}, -\tfrac{69}{125}\right), \;\; 16P = \left(\tfrac{480106}{4225}, \tfrac{332513754}{274625}\right),$$
$$32P = \left(\tfrac{5313922364481462429 0821}{1870098771536627436025}, \tfrac{122016683239503259568882191825132 56}{8087174560555986485289398018 6125}\right).$$

Slično bi iz formule za zbrajanje točaka zaključili da ako fiksiramo točku P_0, onda je $h(P + P_0) \approx h(2P)$. Ova razmatranja se mogu precizirati, kao što pokazuje sljedeća propozicija.

Propozicija 1.3.

a) *Postoji konstanta* c_0 *(koja ovisi samo o* E*) takva da za svaku točku* $P \in E(\mathbb{Q})$ *vrijedi*
$$|h(2P) - 4h(P)| \leq c_0.$$

b) *Postoji konstanta* c_1 *(koja ovisi samo o* E*) takva da za sve* $P_1, P_2 \in E(\mathbb{Q})$ *vrijedi*
$$h(P_1 + P_2) + h(P_1 - P_2) \leq 2h(P_1) + 2h(P_2) + c_1.$$

Već su ova svojstva visine h dovoljna za dovršetak dokaza Mordell-Weiovog teorema. No, još bolja i važnija svojstva ima *kanonska* ili *Néron-Tateova visina* $\hat{h}$ koju ćemo definirati u sljedećem teoremu. Za nju će nejednakosti iz Propozicije 1.3 postati jednakosti (uz $c_0 = c_1 = 0$).

Teorem 1.5. *Neka je E eliptička krivulja nad $\mathbb{Q}$. Postoji jedinstvena funkcija*

$$\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$$

sa svojstvima

1) *postoji konstanta c takva da je $|\hat{h}(P) - h(P)| \leq c$ za svaki $P \in E(\mathbb{Q})$;*
2) *$\hat{h}(2P) = 4\hat{h}(P)$,*

i ona je definirana s

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n}. \tag{1.13}$$

Nadalje, funkcija $\hat{h}$ ima još i sljedeća svojstva:

3) *Za sve $P \in E(\mathbb{Q})$ vrijedi $\hat{h}(P) \geq 0$.*
4) *Za svaku konstantu C je skup $\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq C\}$ konačan.*
5) *Jednakost $\hat{h}(P) = 0$ ako i samo ako je $P \in E(\mathbb{Q})_{tors}$.*
6) *Za sve $P, Q \in E(\mathbb{Q})$ vrijedi "relacija paralelograma"*

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q). \tag{1.14}$$

Dokaz: Pretpostavimo da $\hat{h}$ zadovoljava svojstva 1) i 2). Tada vrijedi

$$|4^n\hat{h}(P) - h(2^n P)| = |\hat{h}(2^n P) - h(2^n P)| \leq c.$$

Stoga je

$$\left|\hat{h}(P) - \frac{h(2^n P)}{4^n}\right| \leq \frac{c}{4^n},$$

pa $\hat{h}$ (ako postoji) mora zadovoljavati (1.13), čime smo dokazali jedinstvenost.

Da bi dokazali egzistenciju, moramo najprije pokazati da je niz $\frac{h(2^n P)}{4^n}$ konvergentan. To ćemo napraviti tako što ćemo dokazati da je ovaj niz Cauchyjev. Uzmimo $n \geq m \geq 0$ i $P \in E(\mathbb{Q})$. Koristeći Propoziciju 1.3a), imamo:

$$\left|\frac{h(2^n P)}{4^n} - \frac{h(2^m P)}{4^m}\right| = \left|\sum_{i=m}^{n-1}\left(\frac{h(2^{i+1}P)}{4^{i+1}} - \frac{h(2^i P)}{4^i}\right)\right|$$

$$\leq \sum_{i=m}^{n-1} \frac{1}{4^{i+1}}|h(2^{i+1}P) - 4h(2^i P)| \leq \sum_{i=m}^{n-1} \frac{c_0}{4^{i+1}} < \frac{c_0}{3\cdot 4^m}. \tag{1.15}$$

Pustimo li $m \to \infty$ u (1.15), vidimo da je niz $\frac{h(2^n P)}{4^n}$ Cauchyjev, pa je sa (1.13) dobro definirana funkcija $\hat{h}$. Dokazat ćemo da ona ima svojstva 1) – 6).

Stavimo li $m = 0$ i pustimo $n \to \infty$ u (1.15), dobivamo

$$|\hat{h}(P) - h(P)| \leq \frac{c_0}{3}, \tag{1.16}$$

što dokazuje 1).

Dokažimo 2):

$$\hat{h}(2P) = \lim_{n\to\infty} \frac{h(2^{n+1}P)}{4^n} = 4 \cdot \lim_{n\to\infty} \frac{h(2^{n+1}P)}{4^{n+1}} = 4\hat{h}(P).$$

Iz definicije je za sve $P \neq \mathcal{O}$, $H(x)$ prirodan broj, pa je $h(P) \geq 0$, te stoga i $\hat{h}(P) \geq 0$.

Ako je $\hat{h}(P) \leq C$, onda je, zbog (1.16), $h(P) \leq C + \frac{c_0}{3}$, pa postoji samo konačno mnogo točaka koji zadovoljavaju polaznu nejednakost.

Promotrimo skup $\mathcal{S} = \{2^n P \,:\, n \geq 0\}$. Ako je $P \in E(\mathbb{Q})_{\text{tors}}$, onda je skup $\mathcal{S}$ konačan, pa postoji konstanta c_2 takva da je $\hat{h}(P) \leq c_2$ za sve $R \in \mathcal{S}$. Koristeći svojstvo 2), dobivamo za svaki $n \geq 0$ vrijedi

$$\hat{h}(P) = \frac{\hat{h}(2^n P)}{4^n} \leq \frac{c_2}{4^n},$$

pa mora biti $\hat{h}(P) = 0$. Ako je P točka beskonačnog reda, onda je skup $\mathcal{S}$ beskonačan, pa zbog svojstva 4), mora postojati n sa svojstvom da je $\hat{h}(2^n P) > 1$. No, tada je $\hat{h}(P) = \frac{\hat{h}(2^n P)}{4^n} > \frac{1}{4^n} > 0$.

U dokazu svojstva 6), koristit ćemo Propoziciju 1.3b). Uzmimo da je $P_1 = 2^n P$, $P_2 = 2^n Q$, te podijelimo dobivenu nejednakost sa 4^n i nakon toga pustimo $n \to \infty$. Dobivamo da za sve $P, Q \in E(\mathbb{Q})$ vrijedi

$$\hat{h}(P+Q) + \hat{h}(P-Q) \leq 2\hat{h}(P) + 2\hat{h}(Q). \tag{1.17}$$

Uvrstimo sada u (1.17) da je $P = P' + Q'$ i $Q = P' - Q'$. Dobivamo da za sve $P', Q' \in E(\mathbb{Q})$ vrijedi

$$\hat{h}(2P') + \hat{h}(2Q') \leq 2\hat{h}(P'+Q') + 2\hat{h}(P'-Q').$$

Koristeći svojstvo 2), te dijeleći sa 2, dobivamo

$$2\hat{h}(P') + 2\hat{h}(Q') \leq \hat{h}(P'+Q') + \hat{h}(P'-Q'),$$

što je upravo obrnuta nejednakost od (1.17), te smo time dokazali relaciju paralelograma. □

Dokaz Mordell-Weilovog teorema (uz pretpostavku da je indeks $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ konačan):

Neka je $\{R_1, R_2, \ldots, R_n\}$ skup reprezentanata iz $E(\mathbb{Q})/2E(\mathbb{Q})$, tj.

$$E(\mathbb{Q}) = (R_1 + 2E(\mathbb{Q})) \cup (R_2 + 2E(\mathbb{Q})) \cup \cdots \cup (R_n + 2E(\mathbb{Q})), \tag{1.18}$$

te neka je $k = \max_i(\hat{h}(R_i))$. Neka su $Q_1, \ldots, Q_m$ sve točke iz $E(\mathbb{Q})$ za koje je $\hat{h}(Q_i) \leq k$ (pokazali smo u Teoremu 1.5 da je skup takvih točaka konačan). Neka je G podrupa od $E(\mathbb{Q})$ generirana točkama

$$R_1, \ldots, R_n, Q_1, \ldots, Q_m.$$

Tvrdimo da je $G = E(\mathbb{Q})$. Pretpostavimo suprotno, tj. da postoji $P \in E(\mathbb{Q})$ takav da $P \notin G$. Budući da postoji samo konačno mnogo točaka s kanonskom visinom manjom od $\hat{h}(P)$, bez smanjenja općenitosti možemo pretpostaviti da je P točka s najmanjom visinom za koju vrijedi $P \notin G$. Iz (1.18) imamo da za neki indeks i i točku $P_1 \in E(\mathbb{Q})$ vrijedi

$$P = R_i + 2P_1.$$

Po Teoremu 1.5, te zbog činjenice da je $\hat{h}(P) > k$ (zato što je $P \neq Q_i$), imamo:

$$\begin{aligned} 4\hat{h}(P_1) = \hat{h}(2P_1) = \hat{h}(P - R_i) &= 2\hat{h}(P) + 2\hat{h}(R_i) - \hat{h}(P + R_i) \\ &\leq 2\hat{h}(P) + 2k < 2\hat{h}(P) + 2\hat{h}(P) = 4\hat{h}(P). \end{aligned}$$

Dakle, $\hat{h}(P_1) < \hat{h}(P)$, pa budući da je P točka s najmanjom kanonskom visinom koja nije u G, to mora biti da je $P_1 \in G$. No, tada je i $P = R_i + 2P_1 \in G$, te smo dobili kontradikciju. Stoga je $G = E(\mathbb{Q})$, što dokazuje da je grupa $E(\mathbb{Q})$ konačno generirana. □

Recimo sada nešto o računanju kanonske visine. Jedna mogućnost je računanje $\hat{h}(P)$ po definiciji (preko limesa).

Primjer 1.9. *Neka je krivulja E zadana jednadžbom*

$$y^2 + y = x^3 + x,$$

te promotrimo na njoj točku $P = (0, 0)$ beskonačnog reda.

Računanjem redom vrijednosti $\frac{\hat{h}(2^n P)}{4^n}$, dobivamo sljedeće rezultate

n	$\hat{h}(2^n P)/4^n$
1	0
2	0
3	0.0433
4	0.05029
5	0.0511006
6	0.0511008
7	0.0511014
8	0.0511034
9	0.05111065
10	0.05111140815

Točna vrijednost od $\hat{h}(P)$ (na 11 decimala) je 0.05111140824. Konvergencija i ne izgleda jako spora, međutim, problem s ovakvim računanjem je da već brojnik i nazivnik od $x(2^{10}P)$ imaju više od 5800 znamenaka, a moramo ih egzaktno izračunati jer nam u idućem koraku trebaju vrijednosti brojnika i nazivnika nakon eventualnih kraćenja (a samo iz približnih vrijednosti ne možemo znati koja će kraćenja nastupiti. $\diamondsuit$

Silverman je 1988. godine dao efikasniji algoritam za računanje kanonske visine. Ideja je prikazati "globalnu visinu" $\hat{h}(P)$ kao sumu "lokalnih visina" $\hat{h}_p(P)$, gdje je p prost broj ili je $p = \infty$. U PARI-ju je taj algoritam implementiran u funkciji `ellheight`.

Relacija paralelograma (1.14) sugerira da ćemo, analogno kao u slučaju norme koja zadovoljava istoimenu relaciju, pomoću kanonske visine moći definirati neku varijantu "skalarnog produkta".

Definicija 1.1. Néron-Tateovo sparivanje visina *točaka* $P, Q \in E(\mathbb{Q})$ *je*

$$\begin{aligned} < P, Q > &= \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)) \\ &= \frac{1}{4}(\hat{h}(P+Q) - \hat{h}(P-Q)). \end{aligned}$$

Iz $\hat{h}(2P) = 4\hat{h}(P)$ slijedi da je $\hat{h}(P) =< P, P >$.

Propozicija 1.4. *Kanonska visina* $\hat{h}$ *je kvadratna forma na* $E(\mathbb{Q})$*, tj. vrijedi*

1) $\hat{h}$ *je parna, tj.* $\hat{h}(-P) = \hat{h}(P)$*,*

2) *Néron-Tateovo sparivanje visina je simetrično i bilinearno.*

Dokaz: Svojstvo 1) slijedi iz $x(-P) = x(P)$. Simetričnost je očita, pa ostaje još dokazati linearnost. Definiramo

$$\begin{aligned} T(P,Q,R) &= \ < P+Q, R > - < P, R > - < Q, R > \\ &= \hat{h}(P+Q+R) - \hat{h}(P+Q) - \hat{h}(P+R) - \hat{h}(Q+R) \\ &\quad + \hat{h}(P) + \hat{h}(Q) + \hat{h}(R). \end{aligned}$$

Trebamo dokazati da je $T(P,Q,R) = 0$. Svojstvo 1) povlači da je

$$T(-P,-Q,-R) = T(P,Q,R). \tag{1.19}$$

S druge strane, primjenom relacije paralelograma dobivamo

$$\begin{aligned} & T(P,Q,R) + T(P,Q,-R) \\ = \ & \hat{h}(P+Q+R) + \hat{h}(P+Q-R) - 2\hat{h}(P+Q) - \hat{h}(P+R) - \hat{h}(P-R) \\ & - \hat{h}(Q+R) - \hat{h}(Q-R) + 2\hat{h}(P) + 2\hat{h}(Q) + 2\hat{h}(R) \\ = \ & 2\hat{h}(P+Q) + 2\hat{h}(R) - 2\hat{h}(P+Q) - 2\hat{h}(P) - 2\hat{h}(R) - 2\hat{h}(Q) - 2\hat{h}(R) \\ & + 2\hat{h}(P) + 2\hat{h}(Q) + 2\hat{h}(R) = 0. \end{aligned}$$

Dakle, $T(P,Q,-R) = -T(P,Q,-R)$ pa, jer je T simetrična funkcija, dobivamo da je $T(-P,-Q,-R) = (-1)^3T(P,Q,R) = -T(P,Q,R)$. Usporedimo li ovo sa (1.19), zaključujemo da je $T(P,Q,R) = 0$. □

Iz prethodne propozicije dobivamo sljedeće poopćenje formule $\hat{h}(2P) = 4\hat{h}(P)$:

$$\hat{h}(mP) = < mP, mP >= m^2 < P, P >= m^2\hat{h}(P).$$

Odavde dobivamo da se umjesto niza 2^nP u definiciji kanonske visine može uzeti i jednostavno niz nP. Naime, vrijedi

$$\lim_{n\to\infty} \frac{h(nP)}{n^2} = \lim_{n\to\infty} \frac{\hat{nP} + O(1)}{n^2} = \lim_{n\to\infty} \left(\hat{h}(P) + \frac{O(1)}{n^2}\right) = \hat{h}(P).$$

Propozicija 1.5. *Ako je T torzijska točka, a P bilo koja točka na $E(\mathbb{Q})$, onda vrijedi*

$$\hat{h}(P+T) = \hat{h}(P) \ \ i \ \ < P, T >= 0.$$

Dokaz: Neka je T točka reda m. Tada je

$$\hat{h}(P+T) = \frac{\hat{h}(m(P+T))}{m^2} = \frac{\hat{h}(mP)}{m^2} = \hat{h}(P),$$

pa je

$$< P, T >= \frac{1}{2}(\hat{h}(P) - \hat{h}(P) - 0) = 0.$$

□

Otvoreno je pitanje vrijedi li obrat druge tvrdnje iz Propozicije 1.5, tj. ako je $< P, Q >= 0$, mora li barem jedna od točaka P, Q biti konačnog reda.

Definirat ćemo sada analogon Gramove determinante skalarnih produkata.

Definicija 1.2. Determinanta visina *točaka* $P_1, \dots, P_m$ *je* $\det(< P_i, P_j >)$.

U PARI-ju se determinanta visina može izračunati pomoću funkcije `ellheightmatrix`.

Vrijedi da je

$$\hat{h}(n_1P_1 + \cdots + n_mP_m) = N(< P_i, P_j >)N^\tau,$$

gdje je $N = (n_1, \dots, n_m)$.

Nadalje, točke $P_1, \dots, P_m$ su zavisne mod $E(\mathbb{Q})_{\text{tors}}$, tj. postoje cijeli brojevi $n_1, \dots, n_m$ koji nisu svi jednaki 0 tako da je $n_1P_1 + \cdots n_mP_m \in E(\mathbb{Q})_{\text{tors}}$, ako i samo ako je $\det(< P_i, P_j >) = 0$.

Posebno važan slučaj nezavisnih točaka je Mordell-Weilova baza. *Mordell-Weilova baza* $Q_1, \dots, Q_r$ za $E(\mathbb{Q})$ je $\mathbb{Z}$-baza za $E(\mathbb{Q})$ mod $E(\mathbb{Q})_{\text{tors}}$, tj. svaki $P \in E(\mathbb{Q})$ se na jedinstven način može prikazati kao

$$P = n_1Q_1 + \cdots + n_rQ_r + T, \ \ n_i \in \mathbb{Z}, \ \ T \in E(\mathbb{Q})_{\text{tors}}.$$

Regulator od E je $\mathrm{Reg}(E) = \det(< Q_i, Q_j >)$, gdje je $Q_1, \ldots, Q_r$ Mordell-Weilova baza. Ako je $r = 0$, onda se po definiciji stavlja da je $\mathrm{Reg}(E) = 1$. Iz nezavisnosti točaka u bazi slijedi da je $\mathrm{Reg}(E) \neq 0$, no može se pokazati da uvijek vrijedi $\mathrm{Reg}(E) > 0$.

Ako su $P_1, \ldots, P_r$ r nezavisnih točaka mod $E(\mathbb{Q})_{\mathrm{tors}}$, te pretpostavimo da $\{P_1, \ldots, P_r\} \cup E(\mathbb{Q})_{\mathrm{tors}}$ generira podgrupu G od $E(\mathbb{Q})$ indeksa q. Tada je

$$\det(< P_i, P_j >) = q^2 \, \mathrm{Reg}(E).$$

Dakle, $\mathrm{Reg}(E)$ je najmanja determinanta visina od r nezavisnih točaka na $E(\mathbb{Q})$. Nadalje, r nezavisnih točaka čini bazu ako i samo ako im je determinanta visina jednaka regulatoru.

1.7 Računanje ranga - krivulje s točkom reda 2

Pitanja koja se tiču ranga su puno teža od pitanja vezanih uz torzijske grupe, a zadovoljavajući odgovori još uvijek nisu poznati. Vjeruje se da rang može biti proizvoljno velik, tj. da za svaki $M \in \mathbb{N}$ postoji eliptička krivulja E nad $\mathbb{Q}$ takva da je rank$(E) \geq M$. No, danas se tek zna da postoji eliptička krivulja ranga ≥ 28. Tu je krivulju 2006. godine pronašao Noam Elkies. Jednadžba (minimalna) joj je:

$$y^2 + xy + y = x^3 - x^2 -$$

$$20067762415575526585033208209338542750930230312178956502x+$$

$$3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

a 28 nezavisnih točaka beskonačnog reda (krivulja nema netrivijalnih torzijskih točaka):

$$P_1 = [-2124150091254381073292137463, 259854492051899599030515511070780628911531]$$

$$P_2 = [2334509866034701756884754537, 18872004195494469180868316552803627931531]$$

$$P_3 = [-1671736054062369063879038663, 251709377261144287808506947241319126049131]$$

$$P_4 = [2139130260139156666492982137, 36639509171439729202421459692941297527531]$$

$$P_5 = [1534706764467120723885477337, 85429585346017694289021032862781072799531]$$

$$P_6 = [-2731079487875677033341575063, 262521815484332191641284072623902143387531]$$

$$P_7 = [2775726266844571649705458537, 12845755474014060248869487699082640369931]$$

$$P_8 = [1494385729327188957541833817, 88486605527733405986116494514049233411451]$$

$$P_9 = [1868438228620887358509065257, 59237403214437708712725140393059358589131]$$

$$P_{10} = [2008945108825743774866542537, 47690677880125552882151750781541424711531]$$

$$P_{11} = [2348360540918025169651632937, 17492930006200557857340332476448804363531]$$

$$P_{12} = [-1472084007090481174470008663, 246643450653503714199947441549759798469131]$$

$$P_{13} = [2924128607708061213363288937, 28350264431488878501488356474767375899531]$$

$$P_{14} = [5374993891066061893293934537, 286188908427263386451175031916479893731531]$$

$$P_{15} = [1709690768233354523334008557, 71898834974686089466159700529215980921631]$$

$$P_{16} = [2450954011353593144072595187, 4445228173532634357049262550610714736531]$$

$$P_{17} = [2969254709273559167464674937, 32766893075366270801333682543160469687531]$$

$$P_{18} = [2711914934941692601332882937, 2068436612778381698650413981506590613531]$$

$$P_{19} = [20078586077996854528778328937, 2779608541137806604656051725624624030091531]$$

$$P_{20} = [2158082450240734774317810697, 34994373401964026809969662241800901254731]$$

$$P_{21} = [2004645458247059022403224937, 48049329780704645522439866999888475467531]$$

P_{22}=[2975749450947996264947091337,33398989826075322320208934410104857869131]

P_{23}=[−2102490467686285150147347863,259576391459875789571677393171687203227531]

P_{24}=[311583179915063034902194537,168104385229980603540109472915660153473931]

P_{25}=[2773931008341865231443771817,12632162834649921002414116273769275813451]

P_{26}=[2156581188143768409363461387,35125092964022908897004150516375178087331]

P_{27}=[3866330499872412508815659137,121197755655944226293036926715025847322531]

P_{28}=[2230868289773576023778678737,28558760030597485663387020600768640028531]

Pregled pronalazaka rekordnih krivulja dan je u sljedećoj tablici (detalji o rekordnim krivuljama mogu se naći na web stranici `http://web.math.hr/~duje/tors/rankhist.html`):

rank $\geq$	year	Author(s)
3	1938	Billing
4	1945	Wiman
6	1974	Penney & Pomerance
7	1975	Penney & Pomerance
8	1977	Grunewald & Zimmert
9	1977	Brumer - Kramer
12	1982	Mestre
14	1986	Mestre
15	1992	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao & Kouya
22	1997	Fermigier
23	1998	Martin & McMillen
24	2000	Martin & McMillen
28	2006	Elkies

Striktno govoreći, nije poznat niti jedan algoritam za računanje ranga. Naime, za "algoritme" (uobičajeno ih je ipak tako nazivati) koji se koriste za računanje, od kojih ćemo neke sada i prikazati, nema garancije da će dati rezultat u svim slučajevima. Važan dio tih algoritama uključuje odluku ima li racionalnih točaka na izvjesnoj krivulji genusa 1 za koju je poznato da ima točaka svugdje lokalno (tj. nad $\mathbb{R}$, te na p-adskim poljem $\mathbb{Q}_p$ za sve proste brojeve p). No, nije poznat algoritam koji bi dao odgovor na to pitanje. Nadalje, čak i ako zanemarimo ovaj problem (jer nam se možda neće pojaviti za konkretnu krivulju koju promatramo), kod krivulja koje nemaju racionalnih točaka reda 2 i imaju velike koeficijente, poznati algoritmi nisu dovoljno efikasni za praktičnu primjenu.

Pretpostavimo da E ima točku reda 2. U tom slučaju je računanje ranga obično lakše nego u općem slučaju. Opisat ćemo metodu za računanje ranga koja se naziva "silazak pomoću 2-izogenije". Promjenom koordinata možemo pretpostaviti da je točka reda 2 upravo točka $(0,0)$, te da E ima jednadžbu

$$y^2 = x^3 + ax^2 + bx, \tag{1.20}$$

gdje su $a, b \in \mathbb{Z}$. Ako je polazna krivulja bila dana jednadžbom $y^2 = x^3 + a_2x^2 + a_4x + a_6$, te ako je x_0 nultočka polinoma $x^3 + a_2x^2 + a_4x + a_6$, onda stavimo $a = 3x_0 + a_2$, $b = (a+a_2)x_0 + a_4$. A ako je polazna krivulja bila dana pomoću Weierstrassove jednadžbe, onda za x_0 uzimamo korijen kubnog polinoma $x^3 + b_2x^2 + 8b_4x + 16b_6$ i stavimo $a = 3x_0 + b_2$, $b = (a+b_2)x_0 + 8b_4$. Uvjet nesingularnosti za krivulju E je $\Delta = 16b^2(a^2 - 4b) \neq 0$.

Za krivulju E' koja ima jednadžbu

$$y^2 = x^3 + a'x^2 + b'x, \tag{1.21}$$

gdje je $a' = -2a$ i $b' = a^2 - 4b$, kažemo da je 2-izogena krivulji E. Uvjet nesingularnosti za obje krivulje E i E' je isti i može se iskazati u obliku $bb' \neq 0$. Općenito, izogenijom zovemo homomorfizam između dvije eliptičke krivulje koji je dan pomoću racionalnih funkcija. U našem slučaju, radi se o preslikavanju $\varphi : E \to E'$, $\varphi(P) = (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2})$ za $P = (x,y) \neq \mathcal{O}, (0,0)$, a $\varphi(P) = \mathcal{O}$ inače. Analogno se definira $\psi : E' \to E$ sa $\psi(P') = (\frac{y'^2}{4x'^2}, \frac{y'(x'^2-b')}{8x'^2})$ za $P' = (x', y') \neq \mathcal{O}, (0,0)$, a $\psi(P') = \mathcal{O}$ inače. . Vrijedi $(\psi \circ \varphi)(P) = 2P$ za sve $P \in E$ i $(\varphi \circ \psi)(P') = 2P'$ za sve $P' \in E'$.

Definirajmo još i preslikavanja $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$, $\beta : E'(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$, sa $\alpha(\mathcal{O}) = 1 \cdot \mathbb{Q}^{*2}$, $\alpha(0,0) = b \cdot \mathbb{Q}^{*2}$, $\alpha(x,y) = x \cdot \mathbb{Q}^{*2}$ za $P = (x,y) \neq \mathcal{O}, (0,0)$, te sasvim analogno za β. Jasno je da je $\mathrm{Ker}(\varphi) = \{\mathcal{O}, (0,0)\}$, $\mathrm{Ker}(\psi) = \{\mathcal{O}, (0,0)\}$, a pokazuje se da vrijedi $\mathrm{Im}(\varphi) = \mathrm{Ker}(\beta)$ i $\mathrm{Im}(\psi) = \mathrm{Ker}(\alpha)$. Broj 2 u nazivu 2-izogenija dolazi od toga što su jezgre od φ i ψ dvočlane.

Ova preslikavanja se koriste u prvom koraku dokaza Mordell-Weilovog teorema, tj. u dokazu da podgrupa $2E(\mathbb{Q})$ ima konačan indeks u grupi $E(\mathbb{Q})$. Naime, lako se vidi da ta tvrdnja slijedi iz konačnosti indeksa $[E(\mathbb{Q}) : \psi(E'(\mathbb{Q})]$ i $[E'(\mathbb{Q}) : \varphi(E(\mathbb{Q})]$, a to pak, po teoremu o izomorfizmu grupa, slijedi iz konačnosti grupa $\mathrm{Im}(\alpha)$ i $\mathrm{Im}(\beta)$. Zapravo je veza ovih preslikavanja s rangom još eksplicitnija. Naime, vrijedi

$$2^r = \frac{[E(\mathbb{Q}) : \psi(E'(\mathbb{Q})] \cdot [E'(\mathbb{Q}) : \varphi(E(\mathbb{Q})]}{4} = \frac{|\mathrm{Im}(\alpha)| \cdot |\mathrm{Im}(\beta)|}{4},$$

gdje je $r = \mathrm{rank}(E(\mathbb{Q}))$. Vrijedi i da je $r = \mathrm{rank}(E'(\mathbb{Q}))$, no torzijske grupe od E i E' općenito ne moraju biti izomorfne, već vrijedi $|E(\mathbb{Q})_{\mathrm{tors}}| = 2^i |E'(\mathbb{Q})_{\mathrm{tors}}|$, gdje je $i \in \{-1, 0, 1\}$.

Želimo dobiti opis elementa iz $\mathrm{Im}(\alpha)$. Sa $\tilde{x}$ ćemo označiti klasu od x u $\mathbb{Q}/\mathbb{Q}^{*2}$.

Neka je $(x,y) \in E(\mathbb{Q})$. Ako je $x = 0$, onda je $(x,y) = (0,0)$ i $\alpha(x,y) = \tilde{b}$. Ako je $x \neq 0$, zapišimo x i y u obliku $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$, $\mathrm{nzd}(m,e) = \mathrm{nzd}(n,e) = 1$, te ih uvrstimo u jednadžbu od E. Dobivamo:

$$n^2 = m(m^2 + ame^2 + be^4).$$

Stavimo $b_1 = \pm\,\mathrm{nzd}(m,b)$, gdje je predznak odabran tako da je $mb_1 > 0$. Tada je $m = b_1 m_1$, $b = b_1 b_2$, $n = b_1 n_1$, pa dobivamo

$$n_1^2 = m_1(b_1 m_1^2 + am_1 e^2 + b_2 e^4).$$

Budući da su faktori na desnoj strani posljednje jednadžbe relativno prosti, te $m_1 > 0$, zaključujemo da postoje cijeli brojevi M i N tako da vrijedi $m_1 = M^2$, $b_1 m_1^2 + am_1 e^2 + b_2 e^4 = N^2$, te tako konačno dobivamo jednadžbu

$$N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4 \tag{1.22}$$

u kojoj su nepoznanice M, e i N. Sada je $\alpha(x,y) = (\frac{b_1 M^2}{e^2}) \cdot \mathbb{Q}^{*2} = \tilde{b_1}$.

Zaključujemo da se $\mathrm{Im}(\alpha)$ sastoji od $\tilde{1}$, $\tilde{b}$, te od svih $\tilde{b_1}$ gdje je b_1 djelitelj broja b za kojeg jednadžba

$$N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4,$$

gdje je $b_1 b_2 = b$, ima rješenja $N, M, e \in \mathbb{Z}$, $e \neq 0$. Tada je $(\frac{b_1 M^2}{e^2}, \frac{b_1 MN}{e^3}) \in E(\mathbb{Q})$. Uočimo da jednadžba (1.22) uvijek ima rješenja za $b_1 = 1$, a to je $(M,e,N) = (1,0,1)$ i za $b_1 = b$, a to je $(M,e,N) = (0,1,1)$.

Pri ispitivanju rješivosti jednadžbe (1.22) možemo pretpostaviti da je $\mathrm{nzd}(M,e) = 1$. Također, nije gubitak općenitosti ako se gledaju samo oni djelitelji b_1 koji su kvadratno slobodni. Alternativno, ako se gledaju svi djelitelji b_1, onda se može tražiti samo rješenja koja zadovoljavaju $\mathrm{nzd}(N,e) = \mathrm{nzd}(M,N) = 1$.

Imamo sljedeći algoritam za računanje ranga eliptičke krivulje E koja ima racionalnu točku reda 2, tj. ima jednadžbu oblika (1.20). Za svaku faktorizaciju $b = b_1 b_2$, gdje je b_1 kvadratno slobodan cijeli broj, napišemo jednadžbu (1.22). Pokušamo odrediti ima li ta jednadžba netrivijalnih cjelobrojnih rješenja (uočimo da za ovakve jednadžbe ne mora vrijediti lokalno-globalni princip Hassea i Minkowskog, što znači da zapravo nemamo algoritam koji bi sa sigurnošću odgovorio na ovo pitanje). Svako rješenje (M,e,N) jednadžbe (1.22) inducira točku na krivulji E s koordinatama $x = \frac{b_1 M^2}{e^2}$, $y = \frac{b_1 MN}{e^3}$. Neka je r_1 broj faktorizacija za koje pripadna jednadžba (1.22) ima rješenja, te neka je r_2 broj definiran na isti način za krivulju E'. Tada postoje nenegativni cijeli brojevi e_1 i e_2 takvi da je $r_1 = 2^{e_1}$, $r_2 = 2^{e_2}$ i pritom vrijedi da je

$$\mathrm{rank}\,(E) = e_1 + e_2 - 2.$$

Primjer 1.10. *Izračunajmo rang eliptičke krivulje*

$$E\,:\,y^2 = x^3 - 5x.$$

Rješenje: Ovdje je pripadna 2-izogena krivulja

$$E'\,:\,y^2 = x^3 + 20x.$$

Za krivulju E, mogućnosti za broj b_1 su ± 1, ± 5. Za $b_1 = 1$ i $b_1 = -5$ ne trebamo gledati jer znamo su pripadne jednadžbe sigurno rješive. Preostaju $b_1 = -1$, $b_1 = 5$ i pripadne diofantske jednadžbe $N^2 = -M^4 + 5e^4$, $N^2 = 5M^4 - e^4$, Budući da je $2^2 = -1^4 + 5 \cdot 1^4$, zaključujemo da je $r_1 = 4$ i $e_1 = 2$.

Za E' je $b_1' \in \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20\}$. Međutim, ako uzmemo da je b_1' je kvadratno slobodan, te uvažimo da očito b_1' i b_2' ne mogu oba biti negativni, dobijemo da je $b_1' \in \{1, 2, 5, 10\}$. Za 1 i 5 ne trebamo gledati jer je $\tilde{5} = \tilde{20}$, pa moramo još samo odrediti ima li jednadžba

$$N^2 = 2M^4 + 10e^4$$

rješenja. Budući da su M i e relativno prosti, možemo pretpostaviti da je $\mathrm{nzd}(M, 5) = 1$. Tada je po Malom Fermatovom teoremu $M^4 \equiv 1 \pmod 5$ i $N^2 \equiv 2 \pmod 5$. No, to je nemoguće jer kvadrati cijelih brojeva pri djeljenju s 5 daju ostatke 0, 1 ili 4. Zaključujemo da je $r_2 = 2$ i $e_2 = 1$. Konačno je $\mathrm{rank}\,(E) = 2 + 1 - 2 = 1$. $\diamondsuit$

Uočimo da smo u prethodnom primjeru kod eliminiranja b_1'-ova za koje pripadna diofantska jednadžba nema rješenja koristili činjenice da negativan broj ne može biti kvadrat u $\mathbb{R}$, te da broj 2 nije kvadrat u $\mathbb{Z}/5\mathbb{Z}$. No, kod diofantskih jednadžbi stupnja većeg od 2 može se dogoditi da one imaju rješenja u $\mathbb{R}$, te da imaju rješenja u $\mathbb{Z}/m\mathbb{Z}$ za svaki cijeli broj m, ali da ipak nemaju netrivijalnih rješenja u $\mathbb{Q}$. Jedan takav primjer je jednadžba

$$N^2 = 17M^4 - 4e^4$$

koja se pojavljuje kod računanja ranga eliptičke krivulje $y^2 = x^3 + 17x$. U takvim slučajevima je određivanje ranga znatno teže.

Označimo sa $\omega(b)$ broj različitih prostih faktora od b. Tada b ima $2^{\omega(b)+1}$ (pozitivnih i negativnih) kvadratno slobodnih faktora. Sada iz formule $2^r = \frac{|\mathrm{Im}(\alpha)| \cdot |\mathrm{Im}(\beta)|}{4}$, slijedi direktno da je $r \le \omega(b) + \omega(b')$. No, iz jednadžbe (1.22) slijedi da ako je $a \le 0$ i $b > 0$, onda b_1 mora biti pozitivan. Analogno, ako je $a' \le 0$ i $b' > 0$, onda b_1' mora biti pozitivan. Isto tako iz

$$N^2 = b_1(M^2 + \frac{ae^2}{2b_1})^2 - \frac{b'e^4}{4b_1}$$

slijedi da ako je $b' < 0$, onda b_1 mora biti pozitivan, te analogno ako je $b < 0$, onda b_1' mora biti pozitivan. Uočimo da b i b' ne mogu biti istovremeno negativni, jer je $4b + b' = a^2$. Očito je $a \le 0$ ili $a' \le 0$. Stoga se negativni djelitelji ne mogu pojaviti u barem jednom od skupova $\mathrm{Im}(\alpha)$, $\mathrm{Im}(\beta)$. Zaključujemo da je

$$r \leq \omega(b) + \omega(b') - 1.$$

U slučaju kada je rang jednak 0 (i mi to uspijemo dokazati), pomoću Lutz-Nagellovog teorema mogu se naći sve racionalne, pa onda i sve cjelobrojne točke na toj eliptičkoj krivulji.

Primjer 1.11. *Promotrimo skup $\{1,2,5\}$. On je tzv. $D(-1)$-trojka. Naime, $1 \cdot 2 - 1$, $1 \cdot 5 - 1$ i $2 \cdot 5 - 1$ su potpuni kvadrati. Postavlja se pitanje, može li se ovaj skup proširiti do četvorke s istim svojstvom, tj. postoji li $x \in \mathbb{Z}$ takav da su*

$$1 \cdot x - 1, \quad 2 \cdot x - 1, \quad 5 \cdot x - 1$$

kvadrati cijelih brojeva. Pokazat ćemo da je jedino rješenje $x = 1$, pa jer je $1 \in \{1,2,5\}$, to će značiti da se skup $\{1,2,5\}$ ne može proširiti $D(-1)$-četvorke. Ova se tvrdnja može dokazati transformacijom problema na rješavanje sustava pellovskih jednadžbi Bakerovom metodom. No, mi ćemo ovdje riješiti i nešto općenitiji problem nalaženja svih cjelobrojnih (čak svih racionalnih) točaka na eliptičkoj krivulji

$$y^2 = (x-1)(2x-1)(5x-1). \tag{1.23}$$

Rješenje: Dovedimo najprije krivulju u Weierstrassov oblik, množenjem obje strane jednadžbe s 10^2 i supstitucijom $10y \mapsto y$, $10x \mapsto x$. Dobivamo

$$y^2 = x^3 - 17x^2 + 80x - 100.$$

Translacijom $x \mapsto x+5$, dovedimo krivulju u oblik prikladan za računanje ranga:

$$E: \quad y^2 = x^3 - 2x^2 - 15x.$$

Njezina 2-izogena krivulja je

$$E': \quad y^2 = x^3 + 4x^2 + 64x.$$

Za krivulju E, mogućnosti za broj b_1 su ± 1, ± 3, ± 5, ± 15. Pripadne diofantske jednadžbe su $N^2 = M^4 - 2M^2e^2 - 15e^4$, $N^2 = -M^4 - 2M^2e^2 + 15e^4$, $N^2 = 3M^4 - 2M^2e^2 - 5e^4$, $N^2 = -3M^4 - 2M^2e^2 + 5e^4$, $N^2 = 5M^4 - 2M^2e^2 - 3e^4$, $N^2 = -5M^4 - 2M^2e^2 + 3e^4$, $N^2 = 15M^4 - 2M^2e^2 - e^4$, $N^2 = -15M^4 - 2M^2e^2 + e^4$. Zbog simetričnosti, dovoljno je ispitati rješivost prve četiri jednadžbe. Za prvu jednadžbu već znamo da ima rješenje $(M,e,N) = (1,0,1)$, dok četvrta ima rješenje $(M,e,N) = (1,1,0)$. Druga jednadžba je ekvivalentna sa $N^2 = (3e^2 - M^2)(5e^2 + M^2)$. Lako se vidi da je $\mathrm{nzd}(3e^2 - M^2, 5e^2 + M^2) \in \{1,2\}$, pa imamo dvije mogućnosti: ili su oba faktora kvadrati ili su oba dvostruki kvadrati. No, $3e^2 - M^2 = s^2$ je nemoguće modulo 3, jer je $(\frac{-1}{3}) = -1$, dok je $5e^2 + M^2 = 2t^2$ nemoguće modulo 5, jer je $(\frac{2}{5}) = -1$. Treća jednadžba je ekvivalentna sa $N^2 = (M^2+e^2)(3M^2-5e^2)$. Ponovo imamo iste dvije mogućnosti za faktore u zadnjem izrazu, i ponovo obje mogućnosti otpadaju: $3M^2 - 5e^2 = t^2$ je nemoguće modulo 5, jer je $(\frac{3}{5}) = -1$, dok je $3M^2 - 5e^2 = 2t^2$ nemoguće modulo 8, jer je $3M^2 - 5e^2 \equiv 6 \pmod 8$, a $2t^2 \equiv 2 \pmod 8$ (kvadrat neparnog broja daje ostatak 1 pri dijeljenju s 8). Dakle, $e_1 = 2$.

Za E' je $b_1' \in \{\pm 1, \pm 2\}$, pa su pripadne diofantske jednadžbe $N^2 = M^4+4M^2e^2+64e^4$, $N^2 = -M^4+4M^2e^2-64e^4$, $N^2 = 2M^4+4M^2e^2+32e^4$ i $N^2 = -2M^4+4M^2e^2-32e^4$. Za prvu jednadžbu znamo da ima rješenje $(M, e, N) = (1, 0, 1)$. Primijetimo da je ovdje $\tilde{b'} = \tilde{64} = \tilde{1}$. Druga i četvrta jednadžba su ekvivalentna s $N^2 = -(M^2-2e^2)^2 - 60e^4$, odnosno $N^2 = -2(M^2-e^2)^2 - 30N^2$, te očito nemaju netrivijalnih rješenja. Treća jednadžba je ekvivalentna sa $2 \cdot (N/2)^2 = (M^2+e^2)^2 + 15e^4$, te nema rješenja modulo 5, jer je $(\frac{2}{5}) = -1$. Dakle, $e_2 = 0$.

Zaključak: $\operatorname{rank}(E) = 2 + 0 - 2 = 0$.

Dakle, treba još samo naći torzijske točke na E. Ona ima tri točke reda 2: $(0,0)$, $(-3,0)$, $(5,0)$. Za ostale torzijske točke (x, y) bi trebalo vrijediti $y^2 | D = 14400$, tj. $y|120$. Možemo provjeriti da jednadžbe $x(x-3)(x+5) = 1, 4, 9, \ldots, 144000$ nemaju cjelobrojnih rješenja. Alternativno, možemo uočiti da je $|E(\mathbb{F}_7)| = 4$. Dakle, jedine racionalne točke na E su $\mathcal{O}$, $(0,0)$, $(-3,0)$, $(5,0)$, pa su jedine racionalne točke na krivulji (1.23): $\mathcal{O}$, $(1,0)$, $(\frac{1}{2}, 0)$, $(\frac{1}{5}, 0)$. Stoga je jedini cijeli broj x sa svojstvom da su $1 \cdot x - 1$, $2 \cdot x - 1$ i $5 \cdot x - 1$ potpuni kvadrati, broj $x = 1$. $\diamondsuit$

Recimo sada nešto u provjeravanju lokalne rješivosti jednadžbe

$$N^2 = b_1 M^4 + aM^2e^2 + b_2 e^4, \tag{1.24}$$

odnosno njoj pridružene (afine) jednadžbe

$$u^2 = b_1 v^4 + av^2 + b_2. \tag{1.25}$$

Općenito, kriterij za rješivost nad $\mathbb{R}$ (tj. za $p = \infty$) jednadžbe $Y^2 = g(X)$ je vrlo jednostavan: polinom g mora u nekoj točki x poprimiti pozitivnu vrijednost. To će sigurno biti zadovoljeno ako ako g ima realnih korijena, a ako g nema realnih korijena, onda vodeći koeficijent od g mora biti pozitivan.

Što se tiče rješivosti jednadžbe (1.25) u $\mathbb{Q}_p$ (odnosno jednadžbe (1.24) modulo p^k za svaki $k \geq 1$), dovoljno je promatrati samo one proste brojeve p za koje vrijedi $p | 2\Delta$. Naime, pokazuje se da su za sve ostale p-ove jednadžbe sigurno rješive.

Jednadžbu (1.24) možemo zapisati i u obliku

$$N^2 = b_1 \left(M^2 + \frac{ae^2}{2b_1} \right)^2 - \frac{b'e^4}{4b_1},$$

odakle dobivamo uvjet da za svaki neparni prosti djelitelj p od b' mora za Legendreov simbol vrijediti $(\frac{b_1}{p}) = 1$. Naravno, ovo daje samo nužni, a ne i dovoljni uvjet za rješivost u $\mathbb{Q}_p$. Opći algoritam koristi Henselovu lemu, tako da za dano rješenje modulo p^k provjerava može li se to rješenje "podići" do rješenja modulo p^{k+1}. Čim je k dovoljno velik ($k > \mathrm{ord}_p(\Delta)$), algoritam sigurno daje odgovor na to pitanje, te tako rješava pitanje rješivosti u $\mathbb{Q}_p$.

Skup svih b_1 za koje je jednadžba (1.22) svugdje lokalno rješiva također čini grupu (i analogno za b_1'). Ako su pripadni redovi 2^{f_1} i 2^{f_2}, onda se broj $s = f_1 + f_2 - 2$ naziva Selmerov rang od E. Jasno je da je $r \leq s$. Vidjeli smo na primjerima da može biti $r = s$, ali i $r < s$. Slutnja je da je $r \equiv s \pmod 2$.

Program MWRANK autora Johna Cremone predstavlja danas najbolju slobodno dostupnu implementaciju algoritama navedenih u ovom poglavlju. Uključen je u programski paket SAGE.

Primjerice za krivulju

$$y^2 + xy + y = x^3 + 34318214642441646362435632562579908747x$$
$$+ 3184376895814127197244886284686214848599453811643486936756$$

(Dujella, 2002) za manje od 10 sekundi dobijemo rezultat da je rang jednak 15. Uz opcije `mwrank -v 0 -o` dobivamo output u obliku prikladnom za interakciju s PARI-jem:

$$\begin{gathered}
[[15],\\
[[1932582037583921429525068139/20052484, 85266017462824901833206386641046403974733/89795023352],\\
[-13070363183130396895, 22426720593885250315808361822],\\
[9078914752207548334164879/3724900, 411883550391942617366531307703144678657/7189057000],\\
[7007445993440694361372245/34969, 18561410601719170080618893537906456866/6539203],\\
[-13355269496967217795, 18546130994061497511090240822],\\
[149870247957012331948105845/5678689, 2028605859078953898287470255223606071114/13532315887],\\
[733136262557597968336021008/3052009, 19858937569077402700127984270443452206044/5331859723],\\
[-64477624322529690869079745/31427236, 9817780211323241387273625449736313512927/176181085016],\\
[400403178044680851773070/29929, 402332496020048427677508364465518374/5177717],\\
[644032321294427950393722414045/23860363024, -568304660161464498684456724621287778818542621/3685662555591232],\\
[77907613083308505969942914720/10871607289, 69861217834666589660130540792904754692492236/1133549877202163],\\
[2336794052323119040528950866670/2250838249, 3572219934150181057098017887493794635552612154/106786519047307],\\
[-17800941052090028988748755/1281424, -7527801861977928071320713933862221929/1450571968],\\
[4221484502164642865015109720/2199289, 274283649415183707195607637459232322865764/3261545587],\\
[-4800885649600334123495970/516961, -16889638094480540858475491871421774702/371694959]]]
\end{gathered}$$

Ova je krivulja 2002. bila krivulja s najvećim rangom za koju je rang egzaktno izračunat (a ne samo donja ograda za rang). Danas je takva rekordna krivulja, krivulja ranga 18 koju je pronašao Elkies 2006. godine:

$$y^2 + xy = x^3 - 26175960092705884096311701787701203903556438969515x$$
$$+ 51069381476131486489742177100373772089779103253890567848326775119094885041.$$

I za ovu krivulju MWRANK vrlo brzo (za oko 45 sekundi) daje odgovor. Primijetimo da je u oba navedena primjera s krivuljama velikog ranga, Selmerov rang jednak pravom rangu, tj. sve pripadne kvartike koje su svugdje lokalno rješive su i globalno rješive.

1.8 Konstrukcija eliptičkih krivulja velikog ranga

Izaberemo li eliptičku krivulju na “slučajan” način, ona će najvjerojatnije imati trivijalnu torzijsku grupu i vrlo mali rang (0 ili 1). Ranije smo vidjeli kako možemo osigurati da krivulja ima unaprijed zadanu torzijsku podgrupu. Sada ćemo razmotriti metode za nalaženje eliptičkih krivulja relativno velikog ranga (jako velik rang ne možemo očekivati imajući u vidu da trenutno nije poznata niti jedna eliptička krivulja s rangom većim od 28). Ako što smo već spomenuli, iako nam nisu poznati primjeri krivulja s vrlo velikim ranga, slutnja je da ipak rang može biti proizvoljno velik. Jedan teoretski rezultat koji daje izvjesnu potporu toj slutnji je rezultat Tatea i Šafarevića koji kaže da rang eliptičkih krivulja nad poljem $\mathbb{F}_q(t)$ (polje funkcija od jedne varijable nad konačnim poljem) neograničen.

Opća metoda za nalaženje krivulja s velikim rangom se sastoji od sljedeće tri faze:

- Konstrukcija: Generiramo familiju eliptičkih krivulja nad $\mathbb{Q}$ (npr. krivulju nad $\mathbb{Q}(t)$) za koju vjerujemo (ili znamo) da sadrži eliptičke krivulje velikog ranga (npr. zato što je “generički” rang krivulje nad $\mathbb{Q}(t)$ relativno velik).

- Sito: Za svaku krivulju u promatranoj familiji izračunamo neke podatke koje nam daju izvjesne informacije o rangu (npr. donju i gornju ogradu za rang - moguće pretpostavljajući da vrijedi neka od opće prihvaćenih slutnji). Ovdje je bitno za se te, (premda možda dosta neprecizne) informacije o rangu mogu izračunati puno brže od samog ranga. Na osnovu tih informacija, izabiremo u promatranoj familiji mali podskup najboljih kandidata za veliki rang.

- Računanje: Za svaku krivulju iz (malog) skupa najboljih kandidata pokušavamo egzaktno izračunati rang ili barem što bolju donju ogradu za rang, da bi potvrdili da ta krivulja stvarno ima velik rang.

Većinu metoda koje se i danas koriste u prve dvije faze uveo je Jean-Francois Mestre između 1982. i 1992. godine.

Prikazat ćemo jednu njegovu konstrukciju kojom je 1991. godine dobio beskonačno mnogo eliptičkih krivulja ranga ≥ 11. Ta konstrukcija se obično naziva *Mestreova polinomijalna metoda*. Polazište u konstrukciji je sljedeća činjenica.

Lema 1.1. *Neka je $p(x) \in \mathbb{Q}[x]$ normiran polinom i deg $p = 2n$. Tada postoje jedinstveni polinomi $q(x), r(x) \in \mathbb{Q}[x]$ takvi da je $p = q^2 - r$ i deg $r \leq n - 1$.*

Polinom q možemo naći sukcesivnim računanjem koeficijenata ili iz asimptotskog razvoja od $\sqrt{p}$.

Pretpostavimo sada da je $p(x) = \prod_{i=1}^{2n}(x-a_i)$, gdje su $a_1, \dots, a_{2n}$ različiti racionalni brojevi. Tada na krivulji

$$C: \quad y^2 = r(x)$$

leže točke $(a_i, \pm q(a_i))$, $i = 1, \dots, 2n$. Ako je $\deg r = 3$ ili 4, te $r(x)$ nema višestrukih korijena, onda C predstavlja eliptičku krivulju. Za $\deg r = 3$ to je sasvim jasno. Ako je $\deg r = 4$, onda izaberemo jednu racionalnu točku na C (npr. $(a_1, q(a_1))$) za točku u beskonačnosti i transformiramo C u eliptičku krivulju.

Za $n = 5$ skoro svi izbori a_i-ova daju $\deg r = 4$. Tada C ima 10 racionalnih točaka oblika $(a_i, q(a_i))$ i možemo očekivati da ćemo dobiti eliptičku krivulju ranga ≥ 9. Mestre je konstruirao familiju eliptičkih krivulja (tj. eliptičku krivulju nad poljem racionalnih funkcija $\mathbb{Q}(t)$) ranga ≥ 11, tako da je uzeo $n = 6$ i $a_i = b_i + t$, $i = 1, \dots 6$; $a_i = b_{i-6} - t$, $i = 7, \dots, 12$. Sada polinom $r(x)$ općenito ima stupanj 5. Zato možemo pokušati izabrati brojeve $b_1, \dots, b_6$ tako da koeficijent uz x^5 bude jednak 0. U prvom Mestreovom primjeru iz 1991. godine bilo je $b_1 = -17$, $b_2 = -16$, $b_3 = 10$, $b_4 = 11$, $b_5 = 14$, $b_6 = 17$.

Kasnije su Mestre, Nagao i Kihara, koristeći slične konstrukcije, poboljšali ovaj rezultat, te konstruirali krivulje nad $\mathbb{Q}(t)$ ranga 14. Nedavno je, koristeći bitno drugačije metode, koje svoje izvorište imaju u algebarskoj geometriji, Elkies uspio konstruirati krivulju nad $\mathbb{Q}(t)$ ranga 18. Sve ove krivulje imaju trivijalnu torzijsku grupu. Fermigier, Kulesz i Lecacheux su modificirali Mestreovu metodu, te dobili familije krivulja s (relativno) velikim rangom i netrivijalnom torzijskom grupom.

U drugoj fazi, "sijanju", gruba ideja je da je izglednije da će krivulja imati "puno" racionalnih točaka (tj. veliki rang) ako ima puno točaka pri redukciji modulo p (tj. ako je broj $N_p = |E(\mathbb{F}_p)|$ velik) za "većinu" p-ova. Napomenimo da po Hasseovom teoremu vrijedi:

$$p + 1 - 2\sqrt{p} \leq N_p \leq p + 1 + 2\sqrt{p},$$

pa to da je broj N_p velik, zapravo znači da je blizu gornje ograde iz Hasseovog teorema.

Puno preciznija verzija ove grube ideje je čuvena *Birch i Swinnerton-Dyerova (BSD) slutnja*:

$$\prod_{p \leq X,\, p \nmid 2\Delta} \frac{N_p}{p} \sim const \cdot (\log X)^r,$$

gdje je $r = \text{rank}(E)$. BSD slutnja se obično iskazuje pomoću L-funkcije, koja je definirana sa

$$L(E, s) = \prod_{p \nmid \Delta} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} \cdot \prod_{p \mid \Delta} \left(1 - a_p p^{-s}\right)^{-1},$$

gdje je $a_p = p + 1 - N_p$ za p-ove u kojima E ima dobru redukciju, $a_p = 0$ u slučaju aditivne redukcije, $a_p = 1$ u slučaju multiplikativne rascjepive, a $a_p = -1$ u slučaju multiplikativne nerascjepive redukcije. Ovu funkciju možemo shvatiti kao analogon Riemannove ζ funkcije, ako se prisjetimo Eulerove formule $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1}$. Funkcija $L(E, s)$ ima analitičko produljenje na cijelu kompleksnu ravninu $\mathbb{C}$, te zadovoljava funkcionalnu jednadžbu

$$\Lambda(s) = w_E \cdot \Lambda(2 - s),$$

gdje je $w_E \in \{1, -1\}$, dok je

$$\Lambda(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E, s),$$

a N označava konduktor od E.

Sada se BSD slutnja može iskazati tako da je red izčezavanja od $L(E, s)$ u $s = 1$ (tzv. analitički rang od E) jednak rangu r, tj. da je

$$L(E, s) = const \cdot (s - 1)^r + \text{članovi višeg reda.}$$

Poznato je da slutnja vrijedi ako je analitički rang jednak 0 ili 1 (Kolyvagin (1990)).

Slutnja je da vrijednost w_E određuje parnost ranga: $w_E = (-1)^r$, tj. ako je $w_E = 1$, onda je rank paran, a ako je $w_E = -1$, onda je rank neparan (to je naziva "Parity Conjecture" i omogućava nam da uvjetno odredimo rang u slučajevima kad ostalim metodama dobijemo zaključak da je $r \in \{r', r' + 1\}$ za neki r'. Vrijednost w_E se može izračunati u PARI-ju pomoću funkcije `ellrootno`. Vrijedi: $w_E = -\prod_{p|\Delta} \varepsilon_p$, gdje su ε_p lokalni faktori. Ako je p prost broj s multiplikativnom redukcijom, onda je $\varepsilon_p = -1$ ako je redukcija rascjepiva, a $\varepsilon_p = 1$ ako je nerascjepiva. Ako E u p ima aditivnu redukciju i $\nu_p(j) < 0$, onda je $\varepsilon_p = (\frac{-1}{p})$ za p neparan, a $\varepsilon_2 = -\bar{b}$, gdje je $\bar{b} \in \{-1, 1\}$, $\bar{b} \equiv b \pmod 4$, $c_6 = 2^a b$.

Iako je sama Birch i Swinnerton-Dyerova slutnja izuzetno važna za razumjevanje ranga eliptičkih krivulja, ona nije prikladna za direktno računanje (makar uvjetno) ranga. Zato se u fazi "sijanja" obično koriste neke druge varijacije gore spomenute grube ideje.

Možemo fiksirati konačan skup prostih brojeva $\mathcal{P}$, pa za svaki $p \in \mathcal{P}$ naći sve vrijednosti parametara $\mathrm{mod} p$ koje maksimiziraju N_p. (Ako promatramo krivulju oblika $y^2 = x^3 + ax + b$, parametri ći biti $(a, b) \in \mathbb{F}_p^2$, a maksimalni N_p je $p + 1 + \lfloor 2\sqrt{p} \rfloor$. Ako tražimo krivulje velikog ranga sa zadanom torzijskom grupom, onda koristimo odgovaraćuje prije navedene parametrizacije, a maksimalni N_p je $|E(\mathbb{Q})_{\text{tors}}| \cdot \left\lfloor \frac{p+1+\lfloor 2\sqrt{p} \rfloor}{|E(\mathbb{Q})_{\text{tors}}|} \right\rfloor$.) Nakon toga, pomoću Kineskog teorema o ostacima, konstruiramo listu s parametrima koji maksimiziraju N_p za sve $p \in \mathcal{P}$. Ovo se naziva metoda konačnog polja.

Mestre i Nagao su dali heurističke argumente (motivirane BSD slutnjom) koji sugeriraju da bi za krivulje velikom ranga izvjesne sume trebale poprimati velike vrijednosti (najveće u promatranoj familiji). Neke od tih suma su

$$S_1(X) = \sum_{p \le X} \frac{N_p + 1 - p}{N_p} \log p,$$

$$S_2(X) = \sum_{p \le X} \frac{N_p + 1 - p}{N_p},$$

$$S_3(X) = \sum_{p \le X} (N_p - p - 1) \log p.$$

U primjenama ove ideje izabere se nekoliko prirodnih brojeva $X_1 < X_2 < \cdots < X_k$, te se računa $S_i(X_1)$, $S_i(X_2)$, $\ldots$, ali tako da se u svakom koraku odbaci recimo 80% "najlošijih" krivulja, tj. onih s najmanjom vrijednošću pripadne sume. Uočimo da za efikasnu implementaciju ove metode X_k ne bi smio biti prevelik (recimo $X_k < 100000$) jer nemamo vrlo efikasan algoritam za računanje N_p za vrlo velike p-ove. O metodama za računje broja N_p za velike p-ove će biti više riječi kasnije. U PARI-ju se broj a_p može izračunati pomoću funkcije `ellap`(E, p), pa se N_p dobije kao $N_p = p + 1 - a_p$.

Pogledajmo koji heuristički argument povezuje sumu $S_1(N)$ i BSD slutnju. BSD slutnja povlači da je $L(E, s) = L(s) = (s-1)^r \cdot g(s)$, gdje je $g(1) \neq 0$. (U stvari, preciznija verzija BSD slutnje točno predviđa čemu je jednako $g(1)$. U opisu, se pored ostalih veličina, pojavljuju redovi torzijske i Tate-Šafarevićeve grupe, te regulator.) Logaritamska derivacija daje

$$\frac{L'(s)}{L(s)} = \frac{r}{s-1} + \frac{g'(s)}{g(s)},$$

Dakle, očekujemo da za logaritamska derivacije od L kad s teži u 1 brže teži u beskonačno što je rang veći. Sada ćemo promotriti produkt

$$L(s, N) = \prod_{p \le N} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

koji se od $L(s)$ razlikuje po tome što smo produkt "prerezali" u N, te što smo ignorirali razliku u faktorima između prostih brojeva s dobrom i lošom redukcijom. Stavimo $f(s, N) = \log L(s, N)$. Tada je

$$f'(s, N) = -\sum_{p \le N} \frac{a_p p^{-s} - 2p^{1-2s}}{1 - a_p p^{-s} + p^{1-2s}} \log p.$$

Čini se da je razumno uzeti da je $\lim_{N\to\infty} f'(s, N)$ dobra aproksimacija za $\frac{L'(s)}{L(s)}$. Stoga brzina divergencije limesa

$$\lim_{s\to 1} \lim_{N\to\infty} f'(s, N) \tag{1.26}$$

može biti indikator veličine ranga. Kad bismo smjeli zamijeniti poredak limesa u (1.26), dobili bismo upravo

$$\lim_{N\to\infty} f'(1,N) = \lim_{N\to\infty} -\frac{a_p - 2}{p+1-a_p}\log p = \lim_{N\to\infty} S_1(N),$$

čime smo pokazali najavljenu vezu izmeđ BSD slutnje i sume $S_1(N)$.

Vidjeli smo ranije da u slučaju kada E ima racionalnu točku reda 2, imamo vrlo jednostavnu gornju ogradu za rang: $r \leq \omega(b) + \omega(b') - 1$, a također i $r \leq s$, gdje je s Selmerov rang. Općenito, u slučaju kada E ima točku konačnog reda, moguće je dati jednostavnu gornju ogradu za rang. Ukoliko imamo toliko sreće da se ta gornja ograda podudara s donjom ogradom koju dobijemo pretragom za točkama s malom visinom, na taj način možemo dobiti egzaktnu vrijednost za rang bez primjene metode općeg 2-silaska. Spomenuta gornja ograda se naziva *Mazurova ograda*. Neka je E eliptička krivulja nad $\mathbb{Q}$ zadana sa svojom minimalnom Weierstrassovom jednadžbom, te neka je E ima racionalnu točku neparnog prostog reda p. Tada vrijedi

$$r \leq m_p = b + a - m - 1,$$

gdje je

- b broj prostih brojeva s lošom redukcijom;
- a prostih brojeva s aditivnom redukcijom;
- m broj prostih brojeva q s multiplikativnom redukcijom za koje dodatno vrijedi da p ne dijeli eksponent od q u Δ i da je $q \not\equiv 1 \pmod p$.

Primjer 1.12. *Izračunajmo rang krivulje*

$$E\ :\ y^2+y = x^3+x^2-17123710160751178600x+885787957535691389512940164$$

(Dujella-Lecacheux (2001)).

Rješenje: Imamo:

$$\begin{gathered} E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, [888689186, 8116714362487], \\ [-139719349, -33500922231893], [-139719349, 33500922231892], \\ [888689186, -8116714362488]\} \cong \mathbb{Z}_5. \end{gathered}$$

Zato možemo izračunati Mazurovu ogradu m_5. Diskriminanta je

$$\Delta = -3^{15}\cdot 5^5\cdot 7^5\cdot 11^5\cdot 19^5\cdot 41^5\cdot 127^5\cdot 1409\cdot 10864429,$$

pa imamo: $b = 9$, $a = 0$, $m = 2$, te dobivamo da je $r \leq m_5 = 6$.

Pretragom za točkama $P = (x, y)$ na E s cjelobrojnim koordinatama i $|x| < 10^9$, nalazimo sljedećih 6 nezavisnih točaka modulo $E(\mathbb{Q})_{\text{tors}}$:

$$[624069446, 7758948474007], [763273511, 4842863582287]$$
$$[680848091, 5960986525147], [294497588, 20175238652299]$$
$$[-206499124, 35079702960532], [676477901, 6080971505482],$$

čime smo dokazali da je rank$(E) = 6$. $\diamondsuit$

Neka je G jedna od 15 mogućih torzijskih grupa za eliptičku krivulju nad $\mathbb{Q}$ (prema Mazurovom teoremu). Definiramo

$$B(G) = \sup\{\text{rank}\,(E(\mathbb{Q}))\ :\ E(\mathbb{Q})_{\text{tors}} = G\}.$$

Slutnja je da je $B(G)$ neogranično za sve G. Međutim, danas znamo tek da je $B(G) \geq 3$ za sve G. U sljedećoj tablici su dani trenutno najbolje poznate donje ograde za $B(G)$. Većina rezultata iz ove tablice je dobivena nekom kombinacijom metoda opisanih u ovom poglavlju. Detalji o rekordnim krivuljama se mogu naći na web stranici `http://web.math.hr/~duje/tors/tors.html`.

G	$B(G) \geq$	Author(s)
0	28	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	19	Elkies (2009)
$\mathbb{Z}/3\mathbb{Z}$	13	Eroshkin (2007,2008,2009)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies (2006)
$\mathbb{Z}/5\mathbb{Z}$	8	Dujella & Lecacheux (2009), Eroshkin (2009)
$\mathbb{Z}/6\mathbb{Z}$	8	Eroshkin (2008), Dujella & Eroshkin (2008), Elkies (2008), Dujella (2008), Dujella & Peral (2012)
$\mathbb{Z}/7\mathbb{Z}$	5	Dujella & Kulesz (2001), Elkies (2006), Eroshkin (2009,2011), Dujella & Lecacheux (2009), Dujella & Eroshkin (2009)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (2006)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (2009)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (2005,2008), Elkies (2006)
$\mathbb{Z}/12\mathbb{Z}$	4	Fisher (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	15	Elkies (2009)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	9	Dujella & Peral (2012)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (2000), Dujella (2000,2001,2006, 2008), Campbell & Goins (2003), Rathbun (2003,2006), Dujella - Rathbun (2006), Flores - Jones - Rollick - Weigandt - Rathbun (2007), Fisher (2009)

1.9 Mordell-Weilova baza

Pretpostavimo da smo uspjeli izračunati rang r eliptičke krivulje E nekom od metoda iz prethodnih poglavlja. Te metode će nam uglavnom dati i r

točaka $P_1, \ldots, P_r$ na E koje su nezavisne modulo $E(\mathbb{Q})_{\text{tors}}$. No, to ne znači da će nužno $\{P_1, \ldots, P_r\} \cup E(\mathbb{Q})_{\text{tors}}$ generirati cijelu grupu $E(\mathbb{Q})$, već možda samo neku njezinu podgrupu konačnog indeksa. Tu podgrupu ćemo označiti s H. Željeli bismo, ako je moguće, naći generatore cijele Mordell-Weilove grupe, tj. Mordell-Weilovu bazu $Q_1, \ldots, Q_r$ (tako da se svaka točka $P \in E(\mathbb{Q})$ može, na jedinstven način, prikazati u obliku $P = n_1Q_1 + \cdots + n_rQ_r + T$, $n_i \in \mathbb{Z}$, $T \in E(\mathbb{Q})_{\text{tors}}$).

Pogledat ćemo samo jedan jednostavan slučaj kada je $r = 1$ (pa se Mordell-Weilova grupa sastoji od jedne točke, koja se zove slobodni generator) i $\Delta > 0$. Tada E ima jednadžbu oblika $y^2 = (x - e_1)(x - e_2)(x - e_3)$, gdje su $e_i \in \mathbb{R}$. Neka je $e_1 < e_2 < e_3$. Tada je $E^0(\mathbb{Q}) = \{(x, y) \in E(\mathbb{Q}) : x \geq e_3\} \cup \{\mathcal{O}\}$ podgrupa od $E(\mathbb{Q})$ koja se zove parna ili neutralna komponentna, dok se $E^{gg}(\mathbb{Q}) = \{(x, y) \in E(\mathbb{Q}) : e_1 \leq x \leq e_2\}$ zove neparna komponenta ("jaje"). Neparna komponenta može biti prazna, a ako je neprazna, onda $E^0(\mathbb{Q})$ ima indeks 2 u $E(\mathbb{Q})$. Primijetimo da u rešetki $\mathbb{C}/L$ točke na $E^0(\mathbb{R})$ odgovaraju parametrima $z \in \mathbb{R}$, dok točke na $E^{gg}(\mathbb{R})$ odgovaraju parametrima z (iz fundametalnog pravokutnika) za koje je $z - \omega_2/2 \in \mathbb{R}$.

Propozicija 1.6. *Neka eliptička krivulja E s cjelobrojnim koeficijentima zadovoljava sljedeće uvjete:*

(i) *rank*$(E(\mathbb{Q})) = 1$*;*

(ii) $E(\mathbb{Q})$ *ima točku P beskonačnog reda takvu da $P + T$ ima cjelobrojne koordinate za sve $T \in E(\mathbb{Q})_{tors}$;*

(iii) $\Delta > 0$*;*

(iv) *neparna komponenta je neprazna.*

Tada se jedan slobodni generator Q neka od konačno mnogo točaka s cjelobrojnim koordinatama na neparnoj komponenti.

Dokaz: Neka je Q slobodni generator. Tada je $nQ = P + T$ za neki $n \in \mathbb{Z}$ i neku torzijsku točku T. Po pretpostavci (ii), točka nQ ima cjelobrojne koordinate. No, tada i točka $Q = (x, y)$ ima cjelobrojne koordinate.

To slijedi iz činjenice koja se koristi i u dokazu Lutz-Nagellovog teorema. Naime, pretpostavimo da je $\nu_p(x) < 0$ za neki prost broj p. Tada je $\nu_p(x) = -2k$, $\nu_p(y) = -3k$ za neki $k \in \mathbb{N}$. Činjenica koja ovdje trebamo jest da je

$$E(p^k) := \{(x, y) \in E(\mathbb{Q}) : \nu_p(x) \leq -2k\} \cup \{\mathcal{O}\}$$

podgrupa od $E(\mathbb{Q})$. Stoga iz $Q \in E(p^k)$ slijedi $nQ \in E(p^k)$, što je u suprotnosti i time na nQ ima cjelobrojne koordinate.

Za svaki $T' \in E(\mathbb{Q})_{\text{tors}}$ je točka $Q + T'$ slobodni generator, pa po upravo dokazanom ima cjelobrojne koordinate. Tvrdimo da se barem jedna od tih točaka nalazi u neparnoj komponenti. Pretpostavimo suprotno. Tada je Q u parnoj komponenti, a također i svi $T' \in E(\mathbb{Q})_{\text{tors}}$ su u parnoj komponeneti. Ali $E(\mathbb{Q})$ je generiran s Q i $E(\mathbb{Q})_{\text{tors}}$, pa bi tada bio sadržan u svojoj parnoj komponenti, što je u suprotnosti s pretpostavkom (iv).

Točaka s cjelobrojnim koordinatama u neparnoj komponenti očito ima samo konačno mnogo, jer im se x-koordinate nalaze u segmentu $[e_1, e_2]$. □

Primjer 1.13. *Nađimo slobodni generator krivulje*

$$E\,:\; y^2 = x^3 - 5x.$$

Rješenje: U Primjeru 1.10 vidjeli smo da je rang od E jednak 1. Algoritam nam je dao i jednu točku $P = (-1, 2)$ beskonačnog reda. Ta točka se nalazi u neparnoj komponenti. Jedina netrivijalna torzijska točka je $T = (0, 0)$. Imamo: $P + T = (5, 10)$. Stoga su zadovoljeni svi uvjeti Propozicije 1.6. Lako se vidi da su jedine točke s cjelobrojnim koordinatama čija je x-koordinata iz segmenta $[-\sqrt{5}, 0]$ upravo točke $\pm P = (-1, \pm 2)$ i T. Zaključujemo da P slobodni generator od $E(\mathbb{Q})$ (ostali slobodni generatori su $-P$, $P + T$ i $-P + T$). ♢

Poglavlje 2

Eliptičke krivulje nad konačnim poljima

2.1 Konačna polja

Konačno polje s q elemenata označavat ćemo s $\mathbb{F}_q$ (koristi se još i oznaka $GF(q)$ koja dolazi od “Galoisovog polja”). Konačno polje ne može biti karakteristike 0, stoga neka je p karakteristika od $\mathbb{F}_q$. Tada $\mathbb{F}_q$ sadrži prosto polje $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Nadalje, $\mathbb{F}_q$ je konačno dimenzionalan vektorski prostor nad $\mathbb{F}_p$. Neka je k njegova dimenzija, a $\{e_1, \ldots, e_k\}$ baza. Tada se svaki element $a \in \mathbb{F}_q$ može na jednoznačan način prikazati u obliku linearne kombinacije

$$a = \lambda_1 e_1 + \cdots \lambda_k e_k,$$

gdje su $\lambda_i \in \mathbb{Z}_p$. Na taj način svakom $a \in \mathbb{F}_q$ možemo bijektivno pridružiti uređenu k-torku $(\lambda_1, \ldots, \lambda_k) \in (\mathbb{Z}_p)^k$. Stoga je $q = p^k$.

Vrijedi i obrat: za svaku potenciju prostog broja $q = p^k$ postoji polje od q elemenata, i ono je jedinstveno do na izomorfizam.

Elementi polja $\mathbb{F}_q$ različiti od nule tvore abelovu grupu s obzirom na množenje. Tu grupu označavamo sa $\mathbb{F}_q^*$. Iz Lagrangeovog teorema slijedi da red svakog elementa $a \in \mathbb{F}_q^*$ dijeli $q-1$. Grupa $\mathbb{F}_q^*$ je ciklička. Ako je g generator od $\mathbb{F}_q^*$, onda je g^j također generator ako i samo ako je $\mathrm{nzd}(j, q-1) = 1$. Stoga postoji točno $\varphi(q-1)$ generatora grupe $\mathbb{F}_q^*$.

Postavlja se pitanje kako efektivno realizirati konačno polje s p^k elemenata (ako je $k > 1$), te operacije na njemu. Polje $\mathbb{F}_q$ za $q = p^k$ možemo realizirati kao kvocijentni prsten $\mathbb{Z}_p[t]/(g(t))$, gdje je $g(t)$ neki normirani ireducibilni polinom stupnja n u $\mathbb{Z}_p[t]$, a $(g(t))$ označava glavni ideal generiran s $g(t)$ (ovaj prsten je polje zbog toga što je $g(t)$ ireducibilan). Elemente ovog polja se može prikazati kao polinome nad $\mathbb{Z}_p$ stupnja $\leq k-1$, dok su pripadne operacije zbrajanje i množenje polinoma u $\mathbb{Z}_p[t]$, s time da se nakon množenja računa ostatak pri dijeljenju s polinomom $g(t)$.

Uočimo da su $\mathbb{F}_{p^k}$ i $\mathbb{Z}_{p^k}$ za $k \geq 2$ bitno različite strukture. U $\mathbb{F}_{p^k}$ su svi nenul elementi invertibilni, dok u $\mathbb{Z}_{p^k}$ ima točno $\varphi(p^k) = p^k - p^{k-1}$ invertibilnih elemenata.

Na ovom mjestu se možemo pitati kako naći ireducibilni polinom stupnja k nad $\mathbb{Z}_p$ (i imali li uopće takvih polinoma). Pokazuje se da normiranih ireducibilnih polinoma stupnja k nad $\mathbb{Z}_p$ ima približno p^k/k, tj. otprilike svaki k-ti normirani polinom stupnja k nad $\mathbb{Z}_p$ je ireducibilan. Npr. ako je k prost broj, onda postoji točno $\frac{p^k-p}{k}$ različitih normiranih ireducibilnih polinoma stupnja k u $\mathbb{Z}_p[t]$. Testiranje je li konkretni polinom ireducibilan zasniva se na činjenici da je polinom $g(t)$ stupnja k nad $\mathbb{Z}_p$ ireducibilan ako i samo ako je $\mathrm{nzd}(g(t), t^{p^j} - t) = 1$ za $j = 1, 2, \ldots \lfloor k/2 \rfloor$. Posljednji uvjet se provjerava Euklidovim algoritmom za polinome. Da bi operacije u polju $\mathbb{F}_q$ bile što efikasnije, obično se polinom $g(t)$ bira tako da ima što manju težinu W (broj koeficijenata različitih od 0). U slučaju $q = 2^k$, koji je najzanimljiviji za primjene u kriptografiji, čini se da je uvijek moguće postići da je $W = 3$ ili $W = 5$. Primjerice, u šifriranju pomoću Advanced Encryption Standarda (AES) koristi se polje $\mathbb{F}_{2^8}$, definirano pomoću ireducibilnog polinoma $x^8 + x^4 + x^3 + x + 1$.

Kako smo već rekli, polje $\mathbb{F}_{2^k}$ jest vektorski prostor nad $\mathbb{F}_2$ dimenzije k. Postoji mnogo različitih baza tog vektorskog prostora. Mi ćemo spomeniti dva tipa takvih baza: trinomijalne baze i normalne baze.

Ako je $g(x)$ ireducibilni polinom stupnja k nad $\mathbb{F}_2$, tada se polje F_{2^k} može reprezentirati kao skup svih polinoma nad $\mathbb{F}_2$ stupnja manjeg od k, s operacijama modulo $g(x)$. To se naziva reprezentacija pomoću *polinomijalne baze*. Reprezentacija pomoću *trinomijalne baze* je specijalni slučaj reprezentacije pomoću polinomijalne baze u kojem polinom $g(x)$ ima oblik $g(x) = x^k + x^m + 1$, tj. $W = 3$. Prednost takve reprezentacije jest efikasnost provođenja redukcije modulo $g(x)$. Za neke k-ove (npr. za $k \equiv 0 \pmod 8$), trinomijalna baza ne postoji. Eksperimentalno je pokazano da trinomijalna baza postoji za nešto više od pola k-ova manjih od 1000.

Sljedeći algoritam računa ostatak pri dijeljenju polinoma $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{2k-2}x^{2k-2} \in \mathbb{F}_2[X]$ s polinomom $g(x) = x^k + x^m + 1$ $(0 < m < k)$.

Redukcija modulo $g(x) = x^k + x^m + 1$**:**

for $i = 2k - 2$ to k by -1 do
  $a_{i-k} = a_{i-k} + a_i$
  $a_{i-k+m} = a_{i-k+m} + a_i$

Normalna baza od $\mathbb{F}_{2^k}$ nad $\mathbb{F}_2$ je baza oblika

$$\{b, b^2, b^{2^2}, \ldots, b^{2^{k-1}}\},$$

gdje je $b \in \mathbb{F}_{2^k}$. Takva baza uvijek postoji. U reprezentaciji pomoću normalne baze, kvadriranje u polju postaje trivijalno: ako je $a = (a_0, a_1, \dots, a_{k-1})$, onda je $a^2 = (a_{k-1}, a_0, a_1, \dots, a_{k-2})$. Dakle, kvadriranje nije ništa drugo nego ciklički pomak udesno. Međutim, za općenitu normalnu bazu, množenje u polju je znatno kompliciranije. Stoga su od interesa one normalne baze kod kojih je množenje što jednostavnije. Takve baze se nazivaju *optimalne normalne baze* (ONB). Alternativna karakterizacija kaže da b generira ONB ako i samo ako za sve i_1, i_2, $0 \le i_1 < i_2 \le k-1$, postoje cijeli brojevi j_1, j_2 takvi da vrijedi

$$b^{2^{i_1}+2^{i_2}} = b^{2^{j_1}} + b^{2^{j_2}}.$$

Optimalna normalna baza ne mora postojati. Jedan od nužnih uvjeta za postojanje ONB je da je barem jedan od brojeva $k+1$ i $2k+1$ prost. Primjerice, ako je $k+1$ prost i 2 primitivni korijen modulo $k+1$, tada k netrivijalnih $(k+1)$-vih korijena iz jedinice tvore ONB od $\mathbb{F}_{2^k}$ nad $\mathbb{F}_2$.

2.2 Grupa $E(\mathbb{F}_q)$

Eliptičke krivulje nad konačnim poljima vrlo su važne za primjene u kriptografiji, a imaju primjene i na probleme faktorizacije i dokazivanja prostosti.

Neka je E eliptička krivulja nad konačnim poljem $\mathbb{F}_q$, $q = p^k$. Kao što smo već vidjeli, ako je $p > 3$, onda E ima jednadžbu oblika

$$y^2 = x^3 + ax + b.$$

Ako je $p = 3$, onda E ima jednadžbu oblika

$$y^2 = x^3 + ax^2 + bx + c,$$

a ako je $p = 2$, onda se E može transformirati u jedan od sljedeća dva oblika

$$y^2 + cy = x^3 + ax + b \quad \text{ili} \quad y^2 + xy = x^3 + ax^2 + b.$$

Sada ćemo reći nešto o najvažnijim svojstvima eliptičkih krivulja definiranih nad konačnim poljima. Krenimo s jednim primjerom.

Primjer 2.1. *Promotrimo eliptičku krivulju*

$$E : \quad y^2 = x^3 + x + 3$$

nad poljem $\mathbb{F}_7$. Odredimo elemente i strukturu grupe $E(\mathbb{F}_7)$.

Rješenje: Uočimo da su 0, 1, 2 i 4 svi kvadrati u polju $\mathbb{F}_7$. Uvrštavamo $x = 0$, 1, 2, 3, 4, 5, 6 u jednadžbu krivulje E, te dobivamo redom jednadžbe $y^2 = 3, 5, 6, 5, 1, 0, 1$ u $\mathbb{F}_7$. Zaključujemo da samo za $x = 4, 5$ i 6 pripadne jednadžbe imaju rješenja. Konačno dobivamo da je

$$E(\mathbb{F}_7) = \{\mathcal{O}, (4, 1), (4, 6), (5, 0), (6, 1), (6, 6)\}.$$

Odredimo sada strukturu grupe $E(\mathbb{F}_7)$. Uzmimo točku $P = (4, 1)$ i izračunajmo njezine višekratnike. Imamo:

$$[2]P = (6, 6), \quad [3]P = (5, 0), \quad [4]P = (6, 1), \quad [5]P = (4, 6), \quad [6]P = \mathcal{O}.$$

Dakle, $E(\mathbb{F}_7)$ je ciklička grupa reda 6, a točka P joj je generator. $\diamondsuit$

Postavlja se pitanje, što se može reći općenito o grupi $E(\mathbb{F}_q)$, tj. o njezinom redu $|E(\mathbb{F}_q)|$ i strukturi. Lako je zaključiti da je $|E(\mathbb{F}_q)| \in [1, 2q + 1]$. Naime, na E imamo točku $\mathcal{O}$, a pored toga svakom od q mogućih x-eva odgovaraju najviše dva y-a. No, samo pola elemenata od $\mathbb{F}_q$ imaju kvadratni korijen (to su elementi oblika g^{2n}, gdje je g generator (cikličke) grupe $\mathbb{F}_q^*$), pa možemo očekivati da je $|E(\mathbb{F}_q)| \approx q + 1$. Preciznu informaciju o redu grupe $E(\mathbb{F}_q)$ daje čuveni Hasseov teorem.

Teorem 2.1 (Hasse)**.**

$$q + 1 - 2\sqrt{q} \le |E(\mathbb{F}_q)| \le q + 1 + 2\sqrt{q}$$

Veličina $t = q+1-|E(\mathbb{F}_q)|$ naziva se *Frobeniusov trag*. Prema Hasseovom teoremu je $|t| \le 2\sqrt{q}$.

Vrijedi i svojevrstan obrat Hasseovog teorema (Deuringov teorem) koji kaže da za svaki prirodan broj

$$m \in \langle p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p} \rangle$$

postoji eliptička krivulja nad $\mathbb{F}_p$ takva da je $|E(\mathbb{F}_p)| = m$.

U primjenama eliptičkih krivulja, često biramo eliptičke krivulje čiji red ima neko zadano aritmetičko svojstvo (prost je, ima samo male proste faktore, i sl.). Pritom je jako važna činjenica, koju je dokazao H. W. Lenstra, a koja kaže da su redovi $|E(\mathbb{F}_p)|$, za $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p$, “skoro uniformno” distribuirani unutar intervala $\langle p + 1 - \sqrt{p}, p + 1 + \sqrt{p} \rangle$ (centralne polovice Hasseovog intervala). To znači da će red slučajno odabrane eliptičke krivulje nad $\mathbb{F}_p$ imati zadano svojstvo s približno istom vjerojatnošću kao i slučajno odabran prirodan broj reda veličine kao p.

O strukturi grupa $E(\mathbb{F}_q)$ govori sljedeći teorem.

Teorem 2.2. *Neka je E eliptička krivulja nad $\mathbb{F}_q$. Tada je*

$$E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2},$$

gdje su n_1 i n_2 prirodni brojevi i vrijedi $n_1 | n_2$ i $n_1 | q - 1$.

Ako je $n_1 = 1$, onda je grupa $E(\mathbb{F}_q)$ ciklička. Iz uvjeta da $n_1 | \operatorname{nzd}(n_2, q - 1)$, zaključujemo da se može očekivati da će općenito n_1 biti mali prirodan broj, a grupa $E(\mathbb{F}_q)$ "skoro ciklička".

2.3 Implementacija osnovnih operacija na eliptičkim krivuljama

Recimo nešto o implementaciji grupovne operacije na $E(\mathbb{F}_q)$, ponajprije za slučajeve $q = p$ ($p > 3$) i $q = 2^k$ koji su najzanimljiviji za primjene. Ako zbroj dvije točke $P + Q$ računamo po formuli za zbrajanje točaka na krivulji zadanoj afinom jednadžbom, vidimo da trebamo računati inverz. Inverz se može izračunati pomoću (proširenog) Euklidovog algoritma ("obična" verzija u slučaju $q = p$, a polinomijalna u slučaju $q = 2^k$). Iako je složenost Euklidovog algoritma teoretski istog reda veličine kao složenost množenja, u praksi je množenje ipak znatno brže od računanja inverza. Vidjeli smo već da se računanje inverza može izbjeći korištenjem Jacobijevih težinskih projektivnih koordinata u kojima projektivnoj točki (X, Y, Z) odgovara afina točka $(\frac{X}{Z^2}, \frac{Y}{Z^3})$. Tada jednadžba eliptičke krivulje (za $q = p$ gdje možemo koristiti kratku Weierstrassovu jednadžbu) postaje

$$Y^2 = X^3 + aXZ^4 + bZ^6.$$

U ovim novim koordinatama se kod računanja zbroja točaka uopće ne pojavljuje dijeljenje. Zbroj $P + Q$ se može izračunati uz 16 množenja, a zbroj $P + P$ uz 10 množenja. Dodatna ušteda se može dobiti ako se koriste "miješane" koordinate. Npr. ako je točka P zapiše u Jacobijevim koordinatama, točka Q u afininim, a rezultat $P + Q$ ponovo u Jacobijevim, za računanje koordinata točke $P + Q$ treba samo 11 množenja.

U slučaju $q = 2^k$, tj. krivulja u polju s karakteristikom 2, rekli smo već da možemo pretpostaviti da eliptička krivulja ima afinu jednadžbu jednog od ova dva oblika:

$$y^2 + cy = x^3 + ax + b, \tag{2.1}$$

$$y^2 + xy = x^3 + ax^2 + b. \tag{2.2}$$

Krivulje oblika (2.1) su tzv. supersingularne krivulje i nisu od većeg interesa za primjene u kriptografiji, pa ćemo mi govoriti uglavnom o krivuljama oblika (2.2). Ovdje se nadalje može uzeti da je $a \in \{0, \gamma\}$, gdje je $\gamma \in \mathbb{F}_{2^k}$ sa svojstvom da je $\operatorname{Tr}(\gamma) = \gamma + \gamma^2 + \gamma^{2^2} + \cdots + \gamma^{2^{k-1}} = 1$. Posebno, ako je k neparan, onda možemo uzeti da je $a \in \{0, 1\}$. I u ovom slučaju mogu se koristiti Jacobijeve koordinate. Jednadžba (2.2) poprima oblik

$$Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6.$$

U ovim koordinatama za računanje $P + Q$ treba 14 množenja (odnosno 10 miješanim koordinatama), dok za $P + P$ treba 5 množenja. U ovoj situaciji još nešto bolji efekt se dobije korištenjem druge verzije težinskih koordinata. To su tzv. López-Dahabove koordinate u kojima projektivnoj točki (X, Y, Z) odgovara afina točka $(\frac{X}{Z}, \frac{Y}{Z^2})$. Jednadžba (2.2) tada postaje

$$Y^2 + XYZ = X^3Z + aX^2Z^2 + bZ^4,$$

a broj operacija je za računanje $P + Q$ 14 množenja (8 u miješanim koordinatama), a za $P + P$ 4 množenja.

U primjenama eliptičkih krivulja često je potrebno izračunati višekratnik neke točke P, tj. točku

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ pribrojnika}}.$$

To se može napraviti pomoću općih algoritama za efikasno potenciranje u Abelovim grupama. Najjednostavniji i najstariji takav algoritam je algoritam "kvadriraj i množi" (u multiplikativnoj notaciji), odnosno "dupliciraj i zbrajaj" (u aditivnoj notaciji koju koristimo kod eliptičkih krivulja). Algoritam se još naziva i "binarne ljestve", jer koristi binarni zapis broja m. Recimo da želimo izračunati $13P$. Binarni zapis od 13 je $(1\,1\,0\,1)_2$. Sada $13P$ možemo izračunati kao

$$13P = P + 2(2P) + 2(2(2P)).$$

Mogli bi reći da smo binarni zapis čitali s desna na lijevo. Ako isti zapis pročitamo s lijeva na desno, onda imamo

$$13P = 2(2(P + 2P)) + P.$$

Dakle, imamo sljedeća dva algoritma za računanje $Q = mP$, gdje je $m = (m_d, \ldots, m_0)_2$.

Binarne ljestve (s desna na lijevo):

$Q = \mathcal{O}$; $R = P$
for $i = 0$ to $d - 1$
  if $(m_i = 1)$ then $Q = Q + R$
  $R = 2R$
$Q = Q + R$

Binarne ljestve (s lijeva na desno):

$Q = P$
for $i = d - 1$ to 0 by -1
  $Q = 2Q$
  if $(m_i = 1)$ then $Q = Q + P$

Obje varijante binarne metode imaju isti broj operacija: d dupliciranja, te množenja onoliko koliko ima jedinica u binarnom zapisu od m (što je $\leq d+1$, a u prosječnom slučaju je oko $d/2$). Prednost druge varijante (s lijeva na desno) je u tome da se u koraku $Q = Q + P$ dodaje uvijek ista točka P, što se može pokušati iskorisiti u implementaciji. Broj operacija za računanje mP za eliptičku krivulju nad poljem $\mathbb{F}_q$ je $O(\ln m \ln^2 q)$.

Postoje različita opća poboljšanja binarne metode, no mi ćemo spomenuti jednu koja je specifična za eliptičke krivulje. Naime, jedna od specifičnosti grupe točka na eliptičkoj krivulji je da u njoj inverzna operacija (oduzimanje) nije nimalo kompliciranija od originalne grupovne operacije (zbrajanja): $-(x, y) = (x, -y)$, odnosno u karakteristici 2, $-(x, y) = (x, x + y)$. Ova činjenica se može iskoristiti za efikasnije multipliciranje). Glavna ideja je zamjena binarnog zapisa sa zapisom u kojem su dopuštene znamenke -1, 0, 1. Prikaz broja m u obliku $m = \sum_{i=0}^{d} s_i 2^i$, $s_i \in \{-1, 0, 1\}$, zovemo *SD (signed digit) prikaz* od m. Jasno je da SD prikaz nije jedinstven. Naime, imamo 3^{d+1} kombinacija, a samo $2^{d+1} - 1$ brojeva koji se mogu prikazati s $d + 1$ znamenkom. Npr. $3 = (0\ 1\ 1) = (1\ 0\ \text{-}1)$. Ova višeznačnost nam sugerira da pokušamo izabrati prikaz koji će imati što više nula, a to će rezultirati efikasnijim multipliciranjem.

Reći ćemo da je SD prikaz *rijedak* ili *nesusjedan* (non-adjacent form, kraće: NAF prikaz) ako nema susjednih znamenaka različitih od 0, tj. ako je $s_i s_{i+1} = 0$ za svaki i. Može se pokazati da svaki prirodan broj n ima jedinstveni NAF prikaz. Nadalje, NAF ima najmanju težinu (broj znamenki različitih od 0) među svim SD prikazima od n, a najviše za jednu znamenku je dulji od najkraćeg SD prikaza od n. Očekivana (prosječna) težina NAF prikaza je $d/3$, za razliku od binarnog prikaza kod kojeg je očekivana težina $d/2$.

Sljedeći algoritam iz poznatog binarnog zapisa $(n_{d-1}, \ldots, n_0)_2$ broja n računa njegov NAF prikaz $(s_d, \ldots, s_0)$.

Algoritam za NAF prikaz

$c_0 = 0$
for $i = 0$ to d
    $c_{i+1} = \lfloor (n_i + n_{i+1} + c_i)/2 \rfloor$
    $s_i = n_i + c_i - 2c_{i+1}$

Umjesto formula iz ovog algoritma, možemo koristiti sljedeću tablicu koja za sve moguće vrijednosti ulaznih podataka u i-tom koraku (n_i, c_i, n_{i+1}) daje odgovarajuće vrijednosti izlaznih podataka (c_{i+1}, s_i).

n_i	0	0	0	0	1	1	1	1
c_i	0	0	1	1	0	0	1	1
n_{i+1}	0	1	0	1	0	1	0	1
c_{i+1}	0	0	0	1	0	1	1	1
s_i	0	0	1	-1	1	-1	0	0

Sve metode za potenciranje zasnovane na binarnom prikazu, mogu se jednostavno modificirati za NAF prikaz. Prikažimo to za binarnu metodu (s lijeva na desno).

Binarne ljestve s predznakom (aditivna verzija):

```
Q = P
for i = d − 1 to 0 by −1
    Q = 2Q
    if (m_i = 1) then Q = Q + P
    if (m_i = −1) then Q = Q − P
```

2.4 Određivanje reda grupe $E(\mathbb{F}_q)$

Hoće li konkretna eliptička krivulja biti prikladna za primjene u kriptografiji, ovisi prvenstveno o redu grupe $E(\mathbb{F}_q)$. Da bi problem diskretnog logaritma u toj grupi bio dovoljno težak, $|E(\mathbb{F}_q)|$ trebao bi imati barem jedan prosti faktor veći od 2^{160}. Nadalje, za krivulje specijalnog oblika poznati su efikasni algoritmi za problem diskretnog logaritma. To su *anomalne krivulje* kod kojih je $|E(\mathbb{F}_q)| = q$, te *supersingularne krivulje* kod kojih $p|t$, što za $p > 3$ znači da je $|E(\mathbb{F}_p)| = p + 1$ (a za $q = 2^k$ da je $j(E) = 0$). Stoga takve krivulje nisu prikladne za primjene u kriptografiji.

Reći ćemo sada nešto o metodama za određivanje reda $|E(\mathbb{F}_q)|$.

Prva metoda koju ćemo spomenuti koristi Legendreov simbol (odnosno njegovo poopćenje za $\mathbb{F}_q$), tj. formulu

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p} \right).$$

Složenost ovog algoritma je $O(p \ln^2 p)$, što možemo pisati i kao $O(p^{1+\varepsilon})$, gdje je ε proizvoljno mala pozitivna konstanta. Ovaj algoritam je efikasan samo za vrlo male p-ove, a praktički je neprimjenjiv za $p > 10000$.

Prikazat ćemo sada *Shanks-Mestreovu metodu*, čija je složenost $O(p^{1/4+\varepsilon})$ i koja je u praksi primjenjiva za $p < 10^{30}$.

Iz Hasseova teorema znamo da je $|E(\mathbb{F}_p)| = p + 1 - t$, $|t| \leq 2\sqrt{p}$. Izaberimo slučajnu točku $P \in E(\mathbb{F}_p)$. Želimo naći broj $N \in \langle p+1-2\sqrt{p}, p+1+2\sqrt{p} \rangle$ takav da je $[N]P = \mathcal{O}$. Takav broj N sigurno postoji jer, po Lagrangeovu teoremu, red od P dijeli $|E(\mathbb{F}_p)|$. Ako je red od P veći od $4\sqrt{p}$, onda je takav N jedinstven i jednak je $|E(\mathbb{F}_p)|$. Naivan način za pronalaženje broja N bio bi da ispitamo svih $\lfloor 4\sqrt{p} \rfloor$ mogućih brojeva. Bolji način se zasniva na Shanksovoj metodi "malih i velikih koraka" (engl. *baby step - giant step* (BSGS)). Neka je $Q = [p+1+\lfloor 2\sqrt{p} \rfloor]P$. Tada za broj $n = p+1+\lfloor 2\sqrt{p} \rfloor - N$ vrijedi da je $0 \leq n \leq 4\sqrt{p}$ i

$$[n]P = [p + 1 + \lfloor 2\sqrt{p} \rfloor - N]P = Q.$$

Dakle, zapravo trebamo riješiti problem diskretnog logaritma. Iako za taj problem nemamo jako efikasan algoritam, ipak ga BSGS metodom možemo riješiti efikasnije nego da redom uvrštavamo sve moguće n-ove. Neka je $m = \lceil 2p^{1/4} \rceil$. Tada je $n < m^2$, pa n možemo prikazati u obliku

$$n = im + j, \quad 0 \leq i \leq m-1, \quad 0 \leq j \leq m-1.$$

"Mali koraci" (engl. *baby steps*) se sastoje u računanju točaka $[j]P$, $0 \leq j \leq m-1$ (nova točka dobiva se iz stare dodavanjem P - mali korak). "Veliki koraci" (engl. *giant steps*) se sastoje u računanju točaka $Q - [i]([m]P)$, $0 \leq i \leq m-1$ (nova točka dobiva se iz stare oduzimanjem $[m]P$ - veliki korak). Za svaki i testiramo postoji li j takav da je

$$Q - [i]([m]P) = [j]P.$$

Kada takve i, j pronađemo, tada je traženi n jednak $im + j$. Dakle, imamo sljedeći algoritam:

Shanks-Mestreova metoda):

$m = \lceil 2p^{1/4} \rceil$
$P \in E(\mathbb{F}_p)$, $|P| > 4\sqrt{p}$
$Q = [p + 1 + \lfloor 2\sqrt{p} \rfloor]P$
for $j = 0$ to $m-1$
    izračunaj i spremi $[j]P$
for $i = 0$ to $m-1$
    if $(Q - [i]([m]P) = [j]P$ za neki $0 \leq j \leq m-1)$ then
        $t = im + j - \lfloor 2\sqrt{p} \rfloor$
return t

Primjer 2.2. *Zadana je krivulja*

$$E : y^2 = x^3 + 3x + 5$$

nad poljem $\mathbb{F}_{163}$. *Odrediti red grupe* $E(\mathbb{F}_{163})$.

Ovdje je $m = 8$. Uzmimo $P = (1, 3)$. Tada je $Q = [163 + 1 + 25]P = (106, 61)$. U sljedećoj tablici su prikazani "mali koraci":

j	0	1	2	3	4	5	6	7
$[j]P$	$\mathcal{O}$	$(1,3)$	$(162,162)$	$(4,154)$	$(11,37)$	$(143,101)$	$(77,80)$	$\mathbf{(118,5)}$

Izračunamo $R = [8]P = (97, 150)$. "Veliki koraci" su prikazani u sljedećoj tablici:

i	0	1	2	3	4	5	6	7
$Q - [i]R$	$(106,61)$	$(79,83)$	$(145,65)$	$\mathbf{(118,5)}$	$(1,160)$	$(142,61)$	$(7,83)$	$(124,8)$

Dakle, $n = 3 \cdot 8 + 7 = 31$, $t = 31 - 25 = 6$ i konačno $|E(\mathbb{F}_{163})| = 163 + 1 - 6 = 158$. $\diamondsuit$

Ako je red točke P manji od $4\sqrt{p}$, onda će nam ovaj algoritam dati više mogućih kandidata za red grupe $|E(\mathbb{F}_p)|$. Dakle, postavlja se pitanje postoji li točka $P \in E(\mathbb{F}_p)$ čiji je red P veći od $4\sqrt{p}$. Potvrdan odgovor na ovo pitanje dao je Mestre. Da bismo formulirali njegov rezultat, treba nam pojam "zakretanja" (engl. *twist*) eliptičke krivulje. Za eliptičku krivulju E nad poljem $\mathbb{K}$ danu jednadžbom $y^2 = x^3 + ax + b$ i $g \in \mathbb{K}^*$, (kvadratni) *twist* od E s g je eliptička krivulja čija je jednadžba $gy^2 = x^3 + ax + b$, odnosno (uz supstituciju $X = gx$, $Y = g^2y$) $Y^2 = X^3 + g^2aX + g^3b$. U slučaju kada je $\mathbb{K} = \mathbb{F}_p$, svi *twistovi* od E čine dvije klase izomorfnih krivulja. One kod kojih je g kvadratni ostatak modulo p izomorfne su s E, dok su sve one kod kojih je g kvadratni neostatak modulo p izomorfne jednoj drugoj krivulji koju ćemo označiti s E'. Iz formule za prikaz $|E(\mathbb{F}_p)|$ pomoću Legendreovih simbola, direktno slijedi da je

$$|E(\mathbb{F}_p)| + |E'(\mathbb{F}_p)| = 2p + 2.$$

To znači da ako znamo red $|E(\mathbb{F}_p)|$, onda znamo i red od $|E'(\mathbb{F}_p)|$, i obrnuto. Sada možemo navesti gore najavljeni Mestreov rezultat koji kaže da ako je $p > 457$, onda postoji točka reda većeg od $4\sqrt{p}$ na barem jednoj od krivulja E i E'. Štoviše, takvih točaka ima relativno mnogo (ima ih više od $c \ln p / \ln \ln p$ za neku konstantu c).

Prvi polinomijalni algoritam za računanje reda grupe $E(\mathbb{F}_q)$ dao je Schoof 1995. godine. Taj je algoritam imao složenost $O(\ln^8 q)$. Kasnije su Atkin i Elkies poboljšali Schoofov algoritam do složenosti $O(\ln^6 q)$, pa je danas moguće izračunati red grupe $E(\mathbb{F}_p)$ za proste brojeve $p < 10^{500}$. Vrlo kratko ćemo spomenuti neke od ideja koje se koriste u Schoofovom algoritmu. Polazna ideja je računanje broja t tako da se izračuna $t \bmod l$ za male proste brojeve l. Ako je l_{max} najmanji prost broj takav da je

$$\prod_{\substack{l \text{ prost} \\ l \le l_{max}}} l > 4\sqrt{q},$$

onda iz poznavanja $t \bmod l$ za $2 \le l \le l_{max}$, pomoću Kineskog teorema o ostatcima možemo izračunati t. Broj l_{max} je reda veličine $O(\ln q)$, pa je broj kongruencija u pripadnom sustavu $O(\frac{\ln q}{\ln \ln q})$. U određivanju $t \mod l$ koristi se tzv. *Frobeniousov endomorfizam*. To je preslikavanje $\varphi : E(\mathbb{F}_q) \to E(\mathbb{F}_q)$ zadano sa $\varphi(x, y) = (x^q, y^q)$, $\varphi(\mathcal{O}) = \mathcal{O}$. Frobeniusov endomorfizam φ i Frobeniusov trag t povezani su relacijom

$$\varphi^2 - [t]\varphi + [q] = [0],$$

tj. za svaku točku $P = (x, y) \in E(\mathbb{F}_q)$ vrijedi

$$(x^{q^2}, y^{q^2}) - [t](x^q, y^q) + [q](x, y) = \mathcal{O}.$$

Neka je točka $P \in E(\mathbb{F}_q)$ takva da je $[l]P = \mathcal{O}$, te neka je $q_l = q \bmod l$. Ako za $\tau \in \{0, 1, \dots, l-1\}$ vrijedi $\varphi^2(P) + [q_l]P = [\tau]\varphi(P)$, onda je $t \bmod l = \tau$.

Ako je E definirana nad $\mathbb{F}_q$, onda E možemo promatrati kao krivulju nad bilo kojim proširenjem $\mathbb{F}_{q^k}$ od $\mathbb{F}_q$. Ako znamo $|E(\mathbb{F}_q)|$, onda $|E(\mathbb{F}_{q^k})|$ možemo izračunati preko formule

$$|E(\mathbb{F}_{q^k})| = q^k + 1 - \alpha^k - \beta^k, \tag{2.3}$$

gdje su α i β kompleksni brojevi koji zadovoljavaju $1 - tT + qT^2 = (1 - \alpha T)(1 - \beta T)$.

Ova metoda se može promijeniti za konstukciju prikladnih krivulja nad $\mathbb{F}_{2^k}$, gdje je k djeljiv s malim prirodnim brojem l. Najprije izaberemo krivulju nad malim poljem $\mathbb{F}_{2^l}$, izračunamo $|E(\mathbb{F}_{2^l})|$, te onda iskoristimo formulu (2.3) za računanje $|E(\mathbb{F}_{2^k})|$.

Primjer 2.3. *Koblitzove krivulje* su krivulje oblika

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

za $a = 0$ ili 1. Dakle, one imaju koeficijente iz $\mathbb{F}_2$. Ali u primjenama možemo ih promatrati kao krivulje nad $\mathbb{F}_{2^k}$ za veliki k. Koristeći gore opisanu metodu dobivamo $(1 - \alpha T)(1 - \beta T) = 1 + \mu T + 2T^2$, gdje je $\mu = (-1)^a$, i stoga

$$\#E(\mathbb{F}_{2^k}) = 2^k + 1 - \left(\frac{-\mu + \sqrt{-7}}{2}\right)^k - \left(\frac{-\mu - \sqrt{-7}}{2}\right)^k.$$

Spomenimo da se na Koblitzovim krivuljama računanje $[m]P$ može efikasnije implementirati korištenje prikaza broja m pomoću potencija od $\tau = \frac{-\mu + \sqrt{-7}}{2}$, umjesto binarnog prikaza (dupliranje točaka se zamijeni primjenom Frobeniusovog endomorfizma).

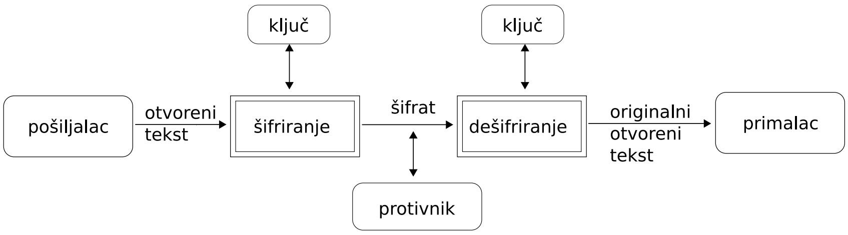
Poglavlje 3

Kriptografija javnog ključa

3.1 Ideja javnoj ključa

Kako uspostaviti sigurnu komunikaciju preko nesigurnog komunikacijskog kanala? Metode za rješavanje ovog problema pročava znanstvena disciplina koja se zove *kriptografija* (ili *tajnopis*). Osnovni zadatak kriptografije je omogućavanje komunikacije dvaju osoba (zovemo ih *pošiljalac* i *primalac* - u kriptografskoj literaturi za njih su rezervirana imena *Alice* i *Bob*) na takav način da treća osoba (njihov *protivnik* - u literaturi se najčešće zove *Eve* ili *Oskar*), koja može nadzirati komunikacijski kanal, ne može razumjeti njihove poruke.

Poruku koju pošiljalac želi poslati primaocu zovemo *otvoreni tekst*. Pošiljalac transformira otvoreni tekst koristeći unaprijed dogovoreni *ključ* K. Taj se postupak zove *šifriranje*, a dobiveni rezultat *šifrat*. Nakon toga pošiljalac pošalje šifrat preko nekog komunikacijskog kanala. Protivnik prisluškujući može saznati sadržaj šifrata, ali kako ne zna ključ, ne može odrediti otvoreni tekst. Za razliku od njega, primalac zna ključ kojim je šifrirana poruka, pa može *dešifrirati* šifrat i odrediti otvoreni tekst.



shema simetrične kriptografije

Ove pojmove ćemo formalizirati u sljedećoj definiciji.

Definicija 3.1. Kriptosustav *je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$*, gdje je* $\mathcal{P}$ *konačan skup svih otvorenih tekstova,* $\mathcal{C}$ *konačan skup svih šifrata,* $\mathcal{K}$ *konačan skup svih mogućih ključeva,* $\mathcal{E}$ *skup svih funkcija šifriranja i* $\mathcal{D}$ *skup svih* *funkcija dešifriranja. Za svaki* $K \in \mathcal{K}$ *postoji* $e_k \in \mathcal{E}$ *i odgovarajući* $d_K \in \mathcal{D}$. *Pritom su* $e_K : \mathcal{P} \to \mathcal{C}$ *i* $d_K : \mathcal{C} \to \mathcal{P}$ *funkcije sa svojstvom da je* $d_K(e_K(x)) = x$ *za svaki* $x \in \mathcal{P}$.

Shema koju smo u uvodu opisali predstavlja tzv. *simetrični ili konvencionalni kriptosustav*. Funkcije koje se koriste za šifriranje e_K i dešifriranje d_K ovise o ključu K kojeg Alice i Bob moraju tajno razmjeniti prije same komunikacije. Kako njima nije dostupan siguran komunikacijski kanal, ovo može biti veliki problem.

Godine 1976. Diffie i Hellman su ponudili jedno moguće rješenje problema razmjene ključeva, zasnovano na činjenici da je u nekim grupama potenciranje puno jednostavnije od logaritmiranja. O ovom algoritmu ćemo detaljnije govoriti u jednom od sljedećih poglavlja.

Diffie i Hellman se smatraju začetnicima *kriptografije javnog ključa*. Ideja javnog ključa se sastoji u tome da se konstruiraju kriptosustavi kod kojih bi iz poznavanja funkcije šifriranja e_K bilo praktički nemoguće (u nekom razumnom vremenu) izračunati funkciju dešifriranja d_K. Tada bi funkcija e_K mogla biti javna. Dakle, u kriptosustavu s javnim ključem svaki korisnik K ima dva ključa: javni e_K i tajni d_K. Ako Alice želji poslati Bobu poruku x, onda je ona šifrira pomoću Bobovog javnog ključa e_B, tj. pošalje Bobu šifrat $y = e_B(x)$. Bob dešifrira šifrat koristeći svoj tajni ključ d_B, $d_B(y) = d_B(e_B(x)) = x$. Uočimo da Bob mora posjedovati neku dodatnu informaciju (tzv. *trapdoor* - skriveni ulaz) o funkciji e_B, da bi samo on mogao izračunati njezin inverz d_B, dok je svima drugima (a posebno Eve) to nemoguće. Takve funkcije čiji je inverz teško izračunati bez poznavanja nekog dodatnog podatka zovu se *osobne jednosmjerne funkcije*.

Napomenimo da su kriptosustavi s javnim ključem puno sporiji od modernih simetričnih kriptosustava (DES, IDEA, AES), pa se stoga u praksi ne koriste za šifriranje poruka, već za šifriranje ključeva, koji se potom koriste u komunikaciji pomoću nekog simetričnog kriptosustava.

Druga važna primjena kriptosustava s javnim ključem dolazi od toga da oni omogućavaju da se poruka "*digitalno potpiše*". Naime, ako Alice pošalje Bobu šifrat $z = d_A(e_B(x))$, onda Bob može biti siguran da je poruku poslala Alice (jer samo ona zna funkciju d_A), a također jednakost $e_A(z) = e_B(x)$ predstavlja i dokaz da je poruku poslala Alice, pa ona to ne može kasnije zanijekati.

3.2 RSA kriptosustav

U konstrukciji kriptosustava s javnim ključem, tj. osobnih jednosmjernih funkcija, obično se koriste neki "teški" matematički problemi. Jedan od takvih problema je *problem faktorizacije* velikih prirodnih brojeva. O metodama faktorizacije ćemo detaljno govoriti kasnije. Za sada kažimo da je danas praktički nemoguće rastaviti na faktore pažljivo odabran broj s više od 200 znamenaka.

Najpoznatiji kriptosustav s javnim ključem je RSA kriptosustav iz 1977. godine, nazvan po svojim tvorcima Rivestu, Shamiru i Adlemanu. Njegova sigurnost je zasnovana upravo na teškoći faktorizacije velikih prirodnih brojeva. Slijedi precizna definicija RSA kriptosustava.

> **RSA kriptosustav:** Neka je $n = pq$, gdje su p i q prosti brojevi. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, te
>
> $$\mathcal{K} = \{(n, p, q, d, e) \,:\, n = pq,\ de \equiv 1 \pmod{\varphi(n)}\}.$$
>
> Za $K \in \mathcal{K}$ definiramo
>
> $$e_K(x) = x^e \bmod n, \qquad d_K(y) = y^d \bmod n, \quad x, y \in \mathbb{Z}_n.$$
>
> Vrijednosti n i e su javne, a vrijednosti p, q i d su tajne, tj. (n, e) je javni, a (p, q, d) je tajni ključ.

Ovdje je $\varphi(n)$ Eulerova funkcija. U našem slučaju je $\varphi(n) = \varphi(pq) = (p-1)(q-1) = n - p - q + 1$.

Da bi RSA kriptosustav bio siguran, nužno je da broj $n = pq$ bude dovoljno velik tako da bi njegova faktorizacija bila praktički nemoguća. Stoga se preporuča izbor prostih brojeva p i q s barem 100 znamenaka.

Postoje dva glavna tipa algoritama za faktorizaciju: specijalni (koji koriste specijalna svojstva broja n) i opći (efikasnost im ovisi samo o veličini broja n). Specijalni algoritmi nam sugeriraju kakve tipove brojeva n (tj. p i q) treba izbjegavati. Npr. ako su p i q jako blizu jedan drugome, onda ih se može pronaći testirajući brojeve koji su blizu $\sqrt{n}$ (Fermatova faktorizacija). Također, ako $p-1$ ili $q-1$ imaju samo male proste faktore (kaže se da su "glatki"), onda Pollardova $p-1$ metoda može biti uspješna u faktorizaciji broja n.

U slučaju RSA modula n, situacije u kojima su takvi specijalni algoritmi efikasni je lako izbjeći, pa su za ozbiljne napade na RSA relevantniji opći algoritmi. Danas su najbolji takvi algoritmi *kvadratno sito* (QS) i *sito polja brojeva* (NFS). Oni se zasnivaju na ideji korištenja faktorske baze prostih brojeva za nalaženje brojeva s i t koji zadovoljavaju $t^2 \equiv s^2 \pmod{n}$, a tada se netrivijalni faktor od n nalazi iz $\gcd(t \pm s, n)$.

Složenost oba spomenuta algoritma je subeksponencijalna. Preciznije, neka je

$$L_n[u, v] = e^{v(\log n)^u (\log\log n)^{1-u}}$$

(za $u = 0$ imamo $L_n[0, v] = (\log n)^v$, što je polinomijalna složenost; za $u = 1$ imamo $L_n[1, v] = n^v$, što je eksponencijalna složenost). Njihova složenost je:
za QS: $L_n[\frac{1}{2}, 1 + \varepsilon]$,
za NFS: $L_n[\frac{1}{3}, (\frac{32}{9})^{1/3} + \varepsilon)]$.

3.3 Kriptosustavi zasnovani na problemu diskretnog logaritma

Neka je G konačna abelova grupa. Da bi bila prikladna za primjene u kriptografiji javnog ključa, grupa G bi trebala imati svojstvo da su operacije množenja i potenciranja u njoj jednostavne, dok je logaritmiranje (inverzna operacija od potenciranja) vrlo teško. Također bi trebalo biti moguće generirati slučajne elemente grupe na gotovo uniforman način. Ipak, centralno pitanje jest koliko je težak tzv. *problem diskretnog logaritma* u grupi G.

Problem diskretnog logaritma: Neka je $(G, *)$ konačna grupa, $g \in G$, $H = \{g^i : i \geq 0\}$ podgrupa od G generirana s g, te $h \in H$. Treba naći najmanji nenegativni cijeli broj x takav da je $h = g^x$, gdje je $g^x = \underbrace{g * g * ... * g}_{x \text{ puta}}$. Taj broj x se zove *diskretni logaritam* i označava se s $\log_g h$.

Činjenicu da postoje grupe u kojima je problem diskretnog logaritma težak, iskoristili su Diffie i Hellman u svom rješenju problema razmjene ključeva.

Pretpostavimo da se Alice i Bob žele dogovoriti o jednom tajnom slučajnom elementu u grupi G, kojeg bi onda poslije mogli koristi kao ključ za šifriranje u nekom simetričnom kriptosustavu. Oni taj svoj dogovor moraju provesti preko nekog nesigurnog komunikacijskog kanala, bez da su prethodno razmjenili bilo kakvu informaciju. Jedina informacija koju imaju jest grupa G i njezin generator g (pretpostavimo zbog jednostavnosti da je grupa G ciklička).

Slijedi opis Diffie-Hellmanovog protokola. Sa $|G|$ ćemo označavati broj elemenata u grupi G.

Diffie-Hellmanov protokol za razmjenu ključeva:

1. Alice generira slučajan prirodan broj $a \in \{1, 2, ..., |G| - 1\}$. Ona pošalje Bobu element g^a.
2. Bob generira slučajan prirodan broj $b \in \{1, 2, ..., |G| - 1\}$, te pošalje Alice element g^b.
3. Alice izračuna $(g^b)^a = g^{ab}$.
4. Bob izračuna $(g^a)^b = g^{ab}$.

Sada je njihov tajni ključ $K = g^{ab}$.

Njihov protivnik (Eve), koji može prisluškivati njihovu komunikaciju preko nesigurnog komunikacijskog kanala, zna sljedeće podatke: G, g, g^a, g^b. Eve treba iz ovih podataka izračunati g^{ab} (kaže se da Eve treba riješiti *Diffie-Hellmanov problem* (DHP)). Ako Eve iz poznavanja g i g^a može izračunati a (tj. ako može riješiti problem diskretnog logaritma (DLP)), onda i ona može pomoću a i g^b izračunati g^{ab}. Vjeruje se da su za većinu grupa koje se koriste u kriptografiji ova dva problema, DHP i DLP, ekvivalentni (tj. da postoje polinomijalni algoritmi koji svode jedan problem na drugi).

U originalnoj definiciji Diffie-Hellmanovog protokola za grupu G se uzima multiplikativna grupa $\mathbb{F}_p^*$ svih ne-nul ostataka modulo p, gdje je p dovoljno velik prost broj. Poznato je da je grupa $\mathbb{F}_p^*$ ciklička. Generator ove grupe se naziva *primitivni korijen* modulo p. Broj $g \in \{1, 2, ..., p-1\}$ je primitivni korijen modulo p ako je g^{p-1} najmanja potencija broja g koja daje ostatak 1 pri djeljenju s p.

Sada ćemo opisati *ElGamalov kriptosustav* iz 1985. godine, koji zasnovan na teškoći računanja diskretnog logaritma u u grupi $(\mathbb{F}_p^*, \cdot_p)$.

Pokazuje se da je ovaj problem približno iste težine kao problem faktorizacije složenog broja n (ako su p i n istog reda veličine), a i neke od metoda koje koriste u najboljim poznatim algoritmima za rješavanje tih problema su vrlo slične.

ElGamalov kriptosustav: Neka je p prost broj i $\alpha \in \mathbb{F}_p^*$ primitivni korijen modulo p. Neka je $\mathcal{P} = \mathbb{F}_p^*$, $\mathcal{C} = \mathbb{F}_p^* \times \mathbb{F}_p^*$ i

$$\mathcal{K} = \{(p, \alpha, a, \beta) \,:\, \beta \equiv \alpha^a \pmod{p}\}.$$

Vrijednosti p, α, β su javne, a vrijednost a je tajna.

Za $K \in \mathcal{K}$ i tajni slučajni broj $k \in \{0, 1, \dots, p-1\}$ definiramo

$$e_K(x, k) = (\alpha^k \bmod p,\ x\beta^k \bmod p).$$

Za $y_1, y_2 \in \mathbb{Z}_p^*$ definiramo

$$d_K(y_1, y_2) = y_2(y_1^a)^{-1} \bmod p.$$

Mogli bismo reći da se otvoreni tekst x "zamaskira" množeći s β^k. Onaj tko poznaje tajni eksponent a može iz α^k izračunati β^k i "ukloniti masku".

Da bi eksponent a stvarno bio tajan, prost broj p mora biti dovoljno velik da bi u $\mathbb{Z}_p^*$ problem diskretnog logaritma bio praktički nerješiv. Stoga se danas preporuča korištenje prostih brojeva od oko 1024 bita. Također bi, zbog razloga koje ćemo kasnije objasniti, red grupe, tj. broj $p-1$, trebao imati barem jedan veliki prosti faktor (od barem 160 bitova).

Poglavlje 4

Kriptosustavi koji koriste eliptičke krivulje

4.1 Menezes-Vanstoneov kriptosustav

Nije $\mathbb{F}_p^*$ jedina grupa kod koje je potenciranje puno lakše od logaritmiranja. Dapače, ima grupa, poput grupe eliptičke krivulje nad konačnim poljem, kod kojih je razlika u težini ova dva problema (potenciranja i logaritmiranja) još veća.

Ideju o tome da bi eliptičke krivulje mogle biti korisne u konstrukciji kriptosustava s javnim ključem prvi su javno iznijeli Koblitz i Miller 1985. godine.

Svi kriptosustavi koji u svojoj originalnoj definiciji koriste grupu $\mathbb{F}_p^*$, kao što je npr. ElGamalov, mogu se vrlo lako modificirati tako da koriste grupu $E(\mathbb{F}_p)$. No, doslovno prevođenje ElGamalovog kriptosustava u eliptičke krivulje ima nekoliko nedostataka.

Prvi je da prije šifriranja moramo elemente otvorenog teksta prebaciti u točke na eliptičkoj krivulji. Za to ne postoji zadovoljavajući deterministički algoritam. No, postoji vjerojatnosni algoritam, koji koristi činjenicu da kvadrati u konačnom polju predstavljaju 50% svih elemenata. To znači da s približnom vjerojatnošću $1 - \frac{1}{2^k}$ možemo očekivati da ćemo iz k pokušaja pronaći broj x takav da je $x^3 + ax + b$ kvadrat u $\mathbb{Z}_p$. Za $k = 30$ to je sasvim zadovoljavajuća vjerojatnost. Pretpostavimo sada da su nam osnovne jedinice otvorenog teksta cijeli brojevi između 0 i M. Pretpostavimo nadalje da je $p > Mk$. Sada otvorenom tekstu m pridružujemo točku na eliptičkoj krivulji $E(\mathbb{F}_p)$ na sljedeći način. Za brojeve x oblika $mk + j$, $j = 1, 2, \ldots, k$ provjeravamo da li je $x^3 + ax + b$ kvadrat u $\mathbb{F}_p$. Kad nađemo takav broj, izračunamo y koji zadovoljava da je $y^2 \equiv x^3 + ax + b \pmod{p}$, te broju m pridružimo točku (x, y) na $E(\mathbb{F}_p)$. Obrnuto, iz točke (x, y) pripadni otvoreni tekst m možemo dobiti po formuli

$$m = \left\lfloor \frac{x-1}{k} \right\rfloor.$$

Drugi problem je da se šifrat jednog elementa otvorenog teksta kod ove varijante ElGamalovog kriptosustava sastoji od uređenog para točaka na eliptičkoj krivulji. To znači da, prilikom šifriranja, poruka postane otprilike 4 puta dulja.

Navest ćemo jednu varijantu ElGamalovog kriptosustava koja koristi eliptičke krivulje. Zove se *Menezes-Vanstoneov kriptosustav*. U njemu se eliptičke krivulje koriste samo za "maskiranje", dok su otvoreni tekstovi i šifrati proizvoljni uređeni parovi elemenata iz polja (a ne nužno parovi koji odgovaraju točkama na eliptičkoj krivulji). Kod ovog kriptosustava, šifrirana poruka je (samo) 2 puta dulja od originalne poruke.

Menezes-Vanstoneov kriptosustav: Neka je E eliptička krivulja nad $\mathbb{F}_p$ ($p > 3$ prost), te H ciklička podgrupa od E generirana s α. Neka je $\mathcal{P} = \mathbb{F}_p^* \times \mathbb{F}_p^*$, $\mathcal{C} = E \times \mathbb{F}_p^* \times \mathbb{F}_p^*$ i

$$\mathcal{K} = \{(E, \alpha, a, \beta) \,:\, \beta = a\alpha\},$$

gdje $a\alpha$ označava $\alpha + \alpha + \cdots + \alpha$ (a puta), a $+$ je zbrajanje točaka na eliptičkoj krivulji.

Vrijednosti E, α, β su javne, a vrijednost a je tajna.

Za $K \in \mathcal{K}$ i tajni slučajni broj $k \in \{0, 1, \ldots, |H| - 1\}$, te za $x = (x_1, x_2) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$ definiramo

$$e_K(x, k) = (y_0, y_1, y_2),$$

gdje je $y_0 = k\alpha$, $(c_1, c_2) = k\beta$, $y_1 = c_1 x_1 \bmod p$, $y_2 = c_2 x_2 \bmod p$.

Za šifrat $y = (y_0, y_1, y_2)$ definiramo

$$d_K(y) = (y_1 (c_1)^{-1} \bmod p,\ y_2 (c_2)^{-1} \bmod p),$$

gdje je $a y_0 = (c_1, c_2)$.

Primjer 4.1. Neka je E eliptička krivulja nad $\mathbb{F}_{13}$ zadana jednadžbom

$$y^2 = x^3 + 4x + 4.$$

Grupa $E(\mathbb{F}_{13})$ je ciklička grupa reda 15 s generatorom $\alpha = (1, 3)$. Pretpostavimo da Alice želi poslati poruku $(x_1, x_2) = (12, 7)$ Bobu, čiji je tajni ključ $a = 2$, a javni ključ $\beta = a\alpha = [2](1,3) = (12,8)$. Pretpostavimo da je Alice izabrala tajni broj $k = 5$. Tada ona računa:

$$\begin{aligned}(c1, c2) &= [k]\beta = [5](12,8) = (10,11),\\ y_0 &= [k]\alpha = [5](1,3) = (10,2),\\ y_1 &= c_1x_1 = 120 = 3 \bmod 13,\\ y_2 &= c_2x_2 = 77 = 12 \bmod 13.\end{aligned}$$

Sada Alice šalje Bobu šifrat $(y_0, y_1, y_2) = ((10,2), 3, 12)$. Nakon primitka šifrata, Bob računa:

$$\begin{gathered}[a]y_0 = [2](10,2) = (10,11) = (c1, c2),\\ (3 \cdot 10^{-1} \bmod 13, 12 \cdot 11^{-1} \bmod 13) = (12,7) = (x_1, x_2).\end{gathered}$$

$\diamondsuit$

4.2 Elliptic Curve Digital Signature Algorithm

Najpoznatiji algoritmi za digitalne potpise su Digital Signature Algorithm (DSA/DSS) i Elliptic Curve Digital Signature Algorithm (ECDSA). DSA se zasniva na problemu diskretnog logaritma u multiplikativnoj grupi konačnog polja, dok ECDSA koristi eliptičke krivulje nad konačnim poljima. U siječnju 1999. ECDSA je prihvaćen kao ANSI standard.

Opisat ćemo tri etape ECDSA-a.

ECDSA: generiranje ključeva

E je eliptička krivulja nad $\mathbb{F}_p$, a P je točka prostog reda n na $E(\mathbb{F}_p)$. Svaki korisnik napravi sljedeće:

a) izabere slučajan broj d iz skupa $\{1, 2, \ldots, n-1\}$;

b) izračuna $Q = [d]P$;

c) Q je javni, a d tajni ključ.

ECDSA: generiranje potpisa

Kad želi potpisati poruku m, Alice radi sljedeće:

a) izabere slučajan broj k iz skupa $\{1, 2, \ldots, n-1\}$;

b) izračuna $[k]P = (x_1, y_1)$ i $r = x_1 \bmod n$. Ako je $r = 0$, onda se vrati na korak a);

c) izračuna $k^{-1} \bmod n$;

d) izračuna $s = k^{-1}(H(m) + dr) \bmod n$, gdje je H hash funkcija (npr. SHA-1, koja daje 160-bitni *sažetak poruke*). Ako je $s = 0$, onda se vrati na korak a);

e) Potpis poruke m je uređeni par prirodnih brojeva (r, s).

ECDSA: provjera potpisa
Da bi verificirao Alicein potpis (r, s) poruke m, Bob treba napraviti sljedeće:

a) dobiti Alicein javni ključ Q;

b) provjeriti da su r i s cijeli brojevi iz skupa $\{1, ..., n-1\}$;

c) izračunati $w = s^{-1} \bmod n$ i $H(m)$;

d) izračunati $u_1 = H(m)w \bmod n$ i $u_2 = rw \bmod n$;

e) izračunati $[u_1]P + [u_2]Q = (x_0, y_0)$ i $v = x_0 \bmod n$;

f) prihvatiti potpis kao vjerodostojan ako i samo ako je $v = r$.

Zaista, imamo

$$[u_1]P + [u_2]Q = [H(m)w + rdw]P = [sks^{-1}]P = [k]P.$$

Uvjet $r \neq 0$ osigurava da se u potpisivanju stvarno koristi Alicein tajni ključ d, dok se uvjet $s \neq 0$ pojavljuje zbog c) koraka u algoritmu provjere potpisa.

4.3 Problem diskretnog logaritma za eliptičke krivulje

Kao što smo već spomenuli, glavni razlog za uvođenje eliptičkih krivulja u kriptografiju javnog ključa jest taj da je problem diskretnog logaritma u grupi $E(\mathbb{F}_p)$ još teži od problema diskretnog logaritma u grupi $\mathbb{F}_p^*$.

To pak znači da se ista sigurnost može postići s manjim ključem. Tako je npr. umjesto ključa duljine duljine 1024 bita, dovoljan ključ duljine 160 bitova. To je osobito važno kod onih primjena (kao što su npr. čip-kartice) kod kojih je prostor za pohranu ključeva vrlo ograničen.

4.3.1 Index calculus metoda

Najefikasniji poznati algoritmi za problem diskretnog algoritma u grupi $\mathbb{F}_p^*$ zasnovani su na tzv. *index calculus metodi*. Sama metoda se može definirati za proizvoljnu grupu G, no njezina efikasnost bitno ovisi o svojstvima te grupe. Ponajprije, moramo biti u stanju izabrati relativno mali podskup $\mathcal{B}$

grupe G (tzv. *faktorsku bazu*) koji ima svojstvo da se velik broj elemenata iz G može efikasno prikazati kao produkt elemenata iz $\mathcal{B}$.

Za efikasnost ove metode u grupi $\mathbb{F}_p^*$ presudna su svojstva distribucije prostih brojeva, ponajprije činjenica da ih ima beskonačno mnogo. Preciznije, broj prostih brojeva, koji su manji od realnog broja x, asimptotski je jednak $\frac{x}{\ln x}$. Vidjet ćemo da teškoća nalaženja eliptičkih krivulja velikog ranga, predstavlja najvažniji ograničavajući faktor za primjenu ove metode na grupe eliptičkih krivulja nad konačnim poljem. Ovo je upravo i predstavljalo motivaciju za uvođenje eliptičkih krivulja u kriptografiju.

Opisat ćemo sada algoritam koji za cikličku grupu G reda n s generatorom g, računa diskretni logaritam $\log_g h$ proizvoljnog elementa h grupe G (diskretni logaritam se još naziva i *indeks*, pa odatle dolazi naziv metode).

***Index calculus* algoritam:**

1. IZBOR FAKTORSKE BAZE

   Izaberemo podskup $\mathcal{B} = \{p_1, p_2, \ldots, p_m\}$ od G sa svojstvom da se relativno velik broj elemenata iz G može prikazati kao produkt elemenata iz $\mathcal{B}$.

2. LINEARNE RELACIJE U LOGARITMIMA

   Za slučajan broj k, $0 \leq k \leq n-1$, izračunamo g^k, te ga pokušamo prikazati kao produkt elemenata iz $\mathcal{B}$:

   $$g^k = \prod_{i=1}^{m} p_i^{c_i}, \quad c_i \geq 0.$$

   Ukoliko smo u tome uspjeli, logaritmiramo dobivenu relaciju, te tako prikažemo $k \bmod n$ kao linearnu kombinaciju logaritama:

   $$k \equiv \sum_{i=1}^{m} c_i \log_g p_i \pmod{n}.$$

   Ponavljamo ovaj postupak sve dok ne dobijemo barem m takvih relacija. Obično se zadovoljavamo s $m+10$ relacija, jer tada s velikom vjerojatnošću pripadni sustav od $m+10$ jednadžbi s m nepoznanica ima jedinstveno rješenje.

3. RJEŠAVANJE SUSTAVA

   Riješimo linearni sustav od, recimo, $m+10$ jednadžbi s m nepoznanica, te tako dobijemo vrijednosti $\log_g p_i$.

4. RAČUNANJE $x = \log_g h$

   Za slučajan broj k, $0 \leq k \leq n-1$, izračunamo $h \cdot g^k$, te ga pokušamo prikazati kao produkt elemenata iz $\mathcal{B}$:

   $$h \cdot g^k = \prod_{i=1}^{m} p_i^{d_i}, \quad d_i \geq 0.$$

Ukoliko nismo u tome uspjeli, izaberemo novi k, a ukoliko smo uspjeli, logaritmiramo dobivenu relaciju, te tako dobijemo da je

$$x = \log_g h = \left(\sum_{i=1}^{m} d_i \log_g p_i - k\right) \bmod n.$$

U primjeni *index calculus* metode na grupu $\mathbb{F}_p^*$, koja je ciklička grupa reda $n = p - 1$, za faktorsku bazu $\mathcal{B}$ uzimamo prvih m prostih brojeva. Potom pokušavamo brojeve oblika $r = g^k \bmod p$ prikazati kao produkt potencija prvih m prostih brojeva. Jasno je da što veći m izaberemo, to je veća vjerojatnost da će se r moći rastaviti kao produkt potencija prvih m prostih brojeva. S druge strane, veći m znači da će rješavanje sustava u 3. koraku algoritma biti teže. Pokazuje se da je optimalan izbor ako odaberemo da je najveći element faktorske baze p_m približno jednak

$$L(p) = e^{\sqrt{\ln p \ln\ln p}}.$$

Na taj način, algoritam *index calculus* postaje subeksponencijalni algoritam za računanje diskretnog logaritma u grupi $\mathbb{F}_p^*$.

4.3.2 ECDLP

Recimo sada nešto o poznatim algoritmima za rješavanje problema diskretnog logaritma u grupi eliptičke krivulje nad konačnim poljem (ECDLP).

Opisat ćemo najprije *Pohlig-Hellmanov algoritam redukcije* koji se temelji na tome da se određivanje broja m svodi na određivanje vrijednosti od m modulo svaki prosti faktor od n. Direktna posljedica postojanja ovog algoritma jest da ako želimo da kriptosustav zasnovan na ECDLP bude siguran, onda n mora imati veliki prosti faktor.

Pohlig-Hellmanov algoritam se može primijeniti u bilo kojoj Abelovoj grupi G. Neka je red n od G djeljiv s prostim brojem p, te pretpostavimo da želimo riješiti problem diskretnog logaritma $Q = mP$. Neka je je $n' = n/p$, $m \equiv m_0 \pmod{p}$, te $Q' = n'Q$ i $P' = n'P$. Tada je P' točka reda p, pa je $mP' = m_0P'$. Sada se problem diskretnog logaritma $Q = mP$ u G reducira na podgrupu od G reda p, tako što se rješava problem

$$Q' = n'Q = n'mP = m_0P'.$$

Rješenjem ovog novog problema određujemo vrijednost m_0, tj. određujemo m modulo p.

Vrijednosti od m modulo $p^2, p^3, \ldots, p^c$ (gdje je p^c najveća potencija od p koja dijeli n) određuju se na sljedeći način. Pretpostavimo da je poznato da je $m \equiv m_{i-1} \pmod{p^i}$. Tada je $m = m_{i-1} + kp^i$, za neki cijeli broj k. Tako dobivamo problem

$$R = Q - m_{i-1}P = k(p^iP) = kS,$$

gdje su R i S poznati i S ima red $s = n/p^i$. Vrijednost od $k_{i-1} = k \bmod p$ određuje se na isti način kao što je gore određena vrijednost od m modulo p, pa dobivamo da je $m \equiv m_i \pmod{p^{i+1}}$, gdje je $m_i = m_{i-1} + k_{i-1}p^i$.

Nastavljajući ovaj postupak, rješavanjem problema diskretnog logaritma u podgrupama reda p, mi na kraju određujemo vrijednost m modulo p^c. Nakon što izračunamo ovu vrijednost za sve proste djelitelje od n, sam broj m, tj. rješenje originalnog problema diskretnog logaritma, nalazimo primjenom Kineskog teorema o ostatcima.

Primjer 4.2. *Neka je dana eliptička krivulja*

$$E\,:\,y^2 = x^3 + 71x + 602$$

nad $\mathbb{F}_{1009}$*. Red grupe* $E(\mathbb{F}_{1009})$ *je* $1060 = 2^2 \cdot 5 \cdot 53$*. Zadane su točke* $P = (1, 237)$*,* $Q = (190, 271)$*. Treba riješiti problem eliptičkog diskretnog logaritma* $Q = [m]P$*.*

Rješenje: Točka P ima red $530 = 2 \cdot 5 \cdot 53$ u grupi $E(\mathbb{F}_{1009})$. Dakle, kod nas je $n = 530$ i pomoću Pohlig-Hellmanovog algoritma računanje broja m se reducira na računanje od m modulo 2, 5 i 53.

Modulo 2: Množeći točke P i Q s $530/2 = 265$, dobivamo točke $P_2 = [265]P = (50, 0)$ i $Q_2 = [265]Q = (50, 0)$. Dobivamo problem

$$Q_2 = (m \bmod 2)P_2,$$

otkud očito slijedi da je $m \equiv 1 \pmod 2$.

Modulo 5: Množeći točke P i Q s $530/5 = 106$, dobivamo točke $P_5 = [106]P = (639, 160)$ i $Q_5 = [106]Q = (639, 849)$. Očito je $Q_5 = -P_5$, što povlači $m \equiv -1 \equiv 4 \pmod 5$.

Modulo 53: Sada se točke množe s $530/53 = 10$. Tako se dobivaju točke $P_{53} = [10]P = (32, 737)$ i $Q_{53} = [10]Q = (592, 97)$. Dobili smo problem diskretnog logaritma u grupi reda 53, koji ćemo riješiti malo kasnije kao ilustraciju BSGS metode. Rezultat je $m \equiv 48 \pmod{53}$.

Rješenje originalnog problema $Q = [m]P$, za $P = (1, 237)$, $Q = (190, 271)$, dobivamo rješavanjem sustava kongruencija

$$m \equiv 1 \pmod 2, \quad m \equiv 4 \pmod 5, \quad m \equiv 48 \pmod{53},$$

čije je rješenje, po Kineskom teoremu o ostacima, $m = 419$. $\diamondsuit$

Poznato je nekoliko metoda za rješavanje ECDLP koje imaju složenost $O(\sqrt{n})$. Danas se najboljom smatra *Pollardova ρ-metoda*, kod koje je za određivanje diskretnog logaritma potrebno približno $\frac{\sqrt{\pi n}}{2}$ zbrajanja točaka na eliptičkoj krivulji. Mi ćemo ovdje opisati Shanksovu "baby step - giant step" (BSGS) metodu. Ova metoda je primjenjiva na problem diskretnog logaritma u proizvoljnoj Abelovoj grupi G. Njezina kompleksnost je također

$O(\sqrt{n})$, gdje je n red grupe G, a pripadna konstanta je čak i nešto bolja nego kod ρ-metode. No, za razliku od ρ-metode, BSGS metoda zahtjeva i pohranjivanje u memoriju $O(\sqrt{n})$ elemenata grupe.

Slijedi opis BSGS metode. Neka su P, Q elementi grupe G, te neka je $Q = mP$. Po teoremu o dijeljenju s ostatkom, znamo da se m može zapisati u obliku

$$m = \lceil \sqrt{n} \rceil a + b, \quad \text{gdje je } 0 \leq a, b < \sqrt{n}.$$

Trebamo odrediti vrijednosti od a i b. Jednadžbu $Q = mP$ možemo sada zapisati u obliku

$$(Q - bP) = a(\lceil \sqrt{n} \rceil P).$$

Na prvi pogled se može činiti da smo samo dodatno zakomplicirali problem, međutim ovakav prikaz jednadžbe nam omogućava rješavanje problema balansiranjem zahtjeva za "prostor i vrijeme". Najprije izračunamo tablicu "baby stepova". Ta se tablica sastoji od svih vrijednosti

$$R_b = Q - bP, \quad \text{za } b = 0, 1, \ldots, \lceil \sqrt{n} \rceil - 1.$$

Tablica se sortira, te spremi u memoriju tako da može biti efikasno pretraživana. Nakon toga računamo redom "giant stepove":

$$S_a = a(\lceil \sqrt{n} \rceil P), \quad \text{za } a = 0, 1, \ldots, \lceil \sqrt{n} \rceil - 1.$$

Nakon svakog računanja "giant stepa", provjerimo pojavljuje li se S_a u tablici. Ako se pojavljuje, onda smo otkrili vrijednosti od a i b. Ovaj postupak mora završiti prije nego što a dosegne vrijednost $\lceil \sqrt{n} \rceil$.

Primjer 4.3. *Nastavak primjera 4.2: U gornjem primjeru, promatrali smo eliptičku krivulju*

$$E \, : \, y^2 = x^3 + 71x + 602$$

nad $\mathbb{F}_{1009}$. *Nakon primjene Pohlig-Hellmanovog algoritma, originalni problem smo sveli na određivanje broja* m_0 *za kojeg vrijedi* $Q' = [m_0]P'$, *gdje je* $Q' = (592, 97), P' = (32, 737)$.

Rješenje: Znamo da je red od P' jednak 53. Kako je $\lceil \sqrt{53} \rceil = 8$, trebamo napraviti osam "baby stepova". Dobivamo sljedeću tablicu:

b	$R_b = Q' - [b]P'$
0	$(592, 97)$
1	$(728, 450)$
2	$(537, 344)$
3	$(996, 154)$
4	$(817, 136)$
5	$(365, 715)$
6	$(627, 606)$
7	$(150, 413)$

Sada računamo "giant stepove":

a	$S_a = [a]([8]P')$
1	$(996, 855)$
2	$(200, 652)$
3	$(378, 304)$
4	$(609, 357)$
5	$(304, 583)$
6	$(592, 97)$

Primjećujemo poklapanje za $a = 6$ i $b = 0$, što povlači $m_0 = 8a + b = 48$. (Već iz $a = 1$ smo mogli zaključiti da je $S_1 = -R_3$, otkud je $[8]P' = -Q + [3]P'$, što ponovo povlači da je $m \equiv -5 \equiv 48 \pmod{53}$.) $\diamondsuit$

Napomenimo da za eliptičke krivulje specijalnih oblika postoje i efikasniji algoritmi za ECDLP od gore navedenih. Poznavanje tih algoritama je važno jer nam oni pokazuju koje eliptičke krivulje trebamo izbjegavati u kriptografskim primjenama.

4.4 Izbor parametara u ECC

Dva su osnovna koraka kod izbora parametara za kriptosustav zasnovan na eliptičkim krivuljama:

- izbor konačnog polja $\mathbb{F}_q$;
- izbor eliptičke krivulje E nad $\mathbb{F}_q$.

Kod izbora polja, dvije su osnovne mogućnosti: ili je $q = p$ prost broj ili $q = 2^k$ potencija broja 2. Ako su p i 2^k približno iste veličine, ova dva izbora pružaju istu razinu sigurnosti.

Među poljima $\mathbb{F}_p$, da bi se minimiziralo vrijeme potrebno za modularno množenje, preporuča se da p ima oblik $2^k \pm c$ za neki mali prirodni broj c (npr. Mersenneovi prosti brojevi oblika $2^k - 1$, brojevi $2^{160} + 7$, $2^{255} + 95$, i sl.).

Kod polja karakteristike 2, osim broja elemenata, moramo odabrati i način reprezentacije elemenata. Najčešće se koriste trinomijalne i optimalne normalne baze. Izbor takvih baza omogućuje efikasniju implementaciju. No, takve baze ne postoje za svako konačno polje karakteristike 2, pa i to utječe na izbor polja. Neki popularni izbori su npr. 2^{163}, 2^{191}, 2^{239} i 2^{431}.

Kod izbora eliptičke krivulje trebamo paziti da problem diskretnog logaritma bude težak. Kako smo već napomenuli, ECDLP je, prema svemu što nam je danas poznato, vrlo težak problem. Međutim, postoje tipovi eliptičkih krivulja kod kojih je taj problem nešto (ali čak puno) lakši. Zato takve krivulje treba izbjegavati. Situacija je vrlo slična kao kod kriptosustava koji svoju sigurnost zasnivaju na teškoći faktorizacije velikih prirodnih brojeva (npr. RSA ili Rabinov). I tamo je tvrdnja da je broj oblika pq, gdje su p i q veliki prosti brojevi, teško rastaviti na faktore točna samo ako se p i q odaberu pažljivo (npr. p i q ne smiju biti jako bliski; brojevi $p-1$ i $q-1$ moraju imati barem jedan veliki prosti faktor).

Navest ćemo sada tipove eliptičkih krivulja koje treba izbjegavati:

- Pohlig-Hellmanov algoritam implicira da trebamo izbjegavati eliptičke krivulje kod kojih red grupe $E(\mathbb{F}_q)$ nema niti jedan veliki prosti faktor. Preciznije, $|E(\mathbb{F}_q)|$ bi trebao imati barem jedan prosti faktor n veći od 2^{160}, jer bismo u protivnom ECDLP mogli riješiti, npr. Pollardovom metodom. Obično se krivulja E odabire tako da broj $|E(\mathbb{F}_q)|$ bude oblika $h \cdot r$, gdje je r prost broj, a $h = 1, 2$ ili 4.

- Eliptička krivulja naziva se *anomalna* ako joj je Frobeniusov trag $t = q+1-|E(\mathbb{F}_q)|$ jednak 1, tj. ako je $|E(\mathbb{F}_q)| = q$. Za takve krivulje postoji polinomijalni algoritam za ECDLP koji su otkrili Smart, Satoh, Araki i Semaev. Stoga se analomalne krivulje nikako ne bi smjele koristiti u ovom kontekstu.

- Za eliptičku krivulju E nad $\mathbb{F}_q$, gdje je $q = p^k$, kažemo da je *supersingularna* ako p dijeli t. Za krivulje nad $\mathbb{F}_p$ za $p \geq 5$ to znači da je $t = 0$, tj. $|E(\mathbb{F}_p)| = p + 1$. Za takve krivulje postoji *MOV-napad* (Menezes, Okamoto, Vanstone) koji u polinomijalnom vremenu reducira ECDLP u polju $E(\mathbb{F}_q)$ na (običan) DLP u polju $\mathbb{F}_{q^2}$. Zbog toga bi supersingularne krivulje trebalo izbjegavati. Nadalje, trebalo bi izbjegavati sve krivulje za koje postoji mali prirodni broj k (recimo $k \leq 20$) takav da je $q^k \equiv 1 \pmod{|E(\mathbb{F}_q)|}$, zato što u tom slučaju MOV-napad reducira ECDLP na DLP u polju $\mathbb{F}_{q^k}$.

Vidimo da je lako odlučiti je li konkretna eliptička krivulja dobra za primjenu u kriptografiji ukoliko znamo red grupe $E(\mathbb{F}_q)$.

Primjer 4.4. Navest ćemo jedan primjer koji zadovoljava sve gore navedene savjete i zahtjeve za izbor polja i eliptičke krivulje. Neka je krivulja E zadana jednadžbom

$$y^2 = x^3 + x + 1010685925500572430206879608558642904226772615919$$

nad poljem $\mathbb{F}_p$, gdje je $p = 2^{160} + 7$. Tada je

$$|E(\mathbb{F}_p)| = 1461501637330902918203683038630093524408650319587.$$

Može se dokazati (npr. metodom dokazivanja prostosti pomoću eliptičkih krivulja) da su brojevi p i $\#E(\mathbb{F}_p)$ prosti. $\diamondsuit$

4.5 Usporedba kriptosustava s javnim ključem

Osnovna motivacija za korištenje eliptičkih krivulja dolazi iz nepostojanja subeksponencijalnog algoritma za rješavanje problema diskretnog logaritma za eliptičke krivulje, dok se problem diskretnog logaritma u multiplikativnoj grupi konačnog polja može se riješiti u subeksponencijalnom vremenu korištenjem *index calculus* metode. Glavni razlozi zašto je *index calculus* metoda neprimjenjiva na eliptičke krivulje leže u tome što

- teško je naći eliptičku krivulju nad $\mathbb{Q}$ velikog ranga;
- teško je naći eliptičku krivulju generiranu točkama s malim brojnicima i nazivnicima;
- teško je "podići" točke iz $E(\mathbb{F}_p)$ do točaka iz $E(\mathbb{Q})$.

Kad bi bilo moguće riješiti ove teške probleme, onda bi mogli primijeniti analogon *index calculus* metode u kojem bi skup prostih brojeva zamijenili s generatorima neke eliptičke krivulje nad $\mathbb{Q}$ velikog ranga. Spomenimo da je procijenjeno da bi za primjenu ove ideje za p približno jednak 2^{160} trebali koristiti krivulju ranga većeg od 180. Budući da danas nije poznata niti jedna krivulja ranga većeg od 28, jasno je da ova ideja vrlo nerealistična.

Zbog toga možemo očekivati da ćemo kod kriptosustava zasnovanih na eliptičkim krivuljama postići zadovoljavajuću sigurnost s (puno) kraćim ključem nego kod kriptosustava zasnovanih na faktorizaciji ili običnom problemu diskretnog logaritma. Sada ćemo pokušati malo precizirati ovo razmatranje.

Pretpostavimo da imamo jedan kriptosustav zasnovan na DLP u grupi $\mathbb{F}_p^*$, te drugi zasnovan na ECDLP u grupi $E(\mathbb{F}_q)$. Ovdje su p i q prosti brojevi. Neka je M broj bitova od p, a N broj bitova od q. Brojeve M i N možemo interpretirati kao duljine ključeva u pripadnim kriptosustavima. Stoga želimo naći odnos između M i N, uz pretpostavku da su pripadni kriptosustavi podjednako sigurni, tj. da su pripadni problemi diskretnog logaritma podjednako teški.

Najbolji poznati algoritmi za problem eliptičkog diskretnog logaritma trebaju $O(\sqrt{n})$ operacija, gdje je n red grupe $E(\mathbb{F}_q)$. Kako je n vrlo blizu q, zaključujemo da je složenost promatranog ECDLP proporcionalna s $2^{N/2}$. S druge strane, složenost najboljeg poznatog algoritma za problem običnog DLP je približno

$$e^{1.92M^{1/3}(\ln(M\ln 2))^{2/3}}.$$

Primijetimo da najbolji poznati algoritmi za faktorizaciju velikih brojeva imaju vrlo sličnu složenost. Stoga će zaključci, koje ćemo dobiti, biti primjenjivi i na usporedbu kriptosustava zasnovanih na eliptičkim krivuljama s onima zasnovanima na faktorizaciji (kao što je npr. RSA).

Usporedbom gore navedenih složenosti (zanemarujući konstante), dobivamo sljedeći odnos između M i N:

$$N \approx 4.91 M^{1/3} (\ln(M \ln 2))^{2/3}.$$

Dakle, uz današnja saznanja o najboljim algoritmima za problem diskretnog logaritma, za istu razinu sigurnosti, duljina ključa N je ugrubo treći korijen duljine ključa M. Naravno, naša komparacija nije bila sasvim precizna, prvenstveno zbog toga što je implementacija grupovnih operacija kompleksnija u slučaju eliptičkih krivulja. Ali ona svakako pokazuje prednost kriptosustava zasnovanih na eliptičkim krivuljama (ECC kriptosustava) u odnosu na RSA ili ElGamalov kriptosustav. No, više nego za asimptotski odnos između M i N, zainteresirani smo za njihovu usporedbu kod standarnih vrijednosti, koje odgovaraju današnjim potrebama za sigurnošću. Tako za postizanje iste razine sigurnosti kao kod RSA kriptosustava (a za ElGamalov vrijedi isto) s duljinom ključa od 1024 (a to je standardna vrijednost), kod eliptičkih krivulja je dovoljno uzeti ključ duljine 160 bitova (što je standardna vrijednost za ECC).

U članku iz 2001. godine, Lenstra i Verheul su dali preporuke za duljine ključeva koje bi trebalo koristiti da bi se postigla zadovoljavajuća sigurnost. Također su dali predviđanja o tome kako bi se te duljine ključeva trebale kretati u budućnosti. U svojim preporukama su uzeli u obzir više varijabilnih parametara. Jedan od osnovnih parametara uzima u obzir razumnu pretpostavku da najbolji *javno objavljeni* rezultati u razbijanju pojedinih kriptosustava ne predstavljaju garanciju da ne postoje i bolji (neobjavljeni) rezultati. Za parametar koji uzima ovu pretpostavku u obzir, uzeli su zadnju godinu u kojoj se smatra da je najpopularniji simetrični kriptosustav DES bio siguran. DES je kao standard prihvaćen 1976. godine. Kod njega je duljina ključa 56 bitova. Već su tada neki kriptografi smatrali da je ta duljina ključa premala, međutim do javnog razbijanja DES-a došlo je tek 1997. godine. U podatcima u sljedećoj tablici koristi se pretpostavka da je zadnja godina u kojoj je DES bio siguran bila 1982. godina. Napomenimo da njihova predviđanja ne uzimaju u obzir moguću konstrukciju kvantnih računala, koja bi skoro sve kriptosustave javnog ključa koji su danas u uporabi učinila nesigurnima.

U tablici su dane preporučene duljine ključa u bitovima za simetrične kriptosustave (DES, AES), kriptosustave zasnovane na faktorizaciji ili diskretnom logaritmu u konačnom polju (RSA, ElGamal), te kriptosustave zasnovane na eliptičkim krivuljama. Uz to, dana je procjena kompjuterskog vremena potrebnog za razbijanje šifre u *MIPS godinama*. Jedna MIPS (engl. million-instructions-per-second) godina se definira kao količina računanja koje se može provesti u godinu dana na računalu sposobnom provesti milijun naredbi u sekundi.

Godina	DES duljina ključa	RSA duljina ključa	ECC duljina ključa	MIPS godina
1990	63	622	117	$3.51 \cdot 10^7$
2000	70	952	132	$7.13 \cdot 10^9$
2010	78	1369	146	$1.45 \cdot 10^{12}$
2020	86	1881	161	$2.94 \cdot 10^{14}$
2030	93	2493	176	$5.98 \cdot 10^{16}$
2040	101	3214	191	$1.22 \cdot 10^{19}$

Možemo zaključiti da kriposustavi zasnovani na eliptičkim krivuljama, trenutno, uz 7 puta manju duljinu ključa pružaju istu sigurnost kao RSA kriptosustav, a u budućnosti se može očekivati da će taj omjer biti još povoljniji za ECC. To je osobito važno kod onih primjena (kao što su "pametne kartice") kod kojih je prostor za pohranu ključeva vrlo ograničen. Jasno je da su zbog toga eliptičke krivulje u posljednje vrijeme od velikog interesa za kriptografe. Njihovim intenzivnijim proučavanjem može se očekivati da će nestati i jedan od rijetkih argumenata protiv njihove uporabe u kriptografiji, a to je da su problemi na kojima je zasnovana uporaba eliptičkih krivulja u kriptografiji slabije istraženi, i puno kraće u žarištu interesa kriptografa, od recimo, problema faktorizacije.

Multiplikativna grupa konačnog polja i grupa točaka na eliptičkoj krivulji nad konačnim poljem su dva najvažija tipa grûpa koje se koriste u kriptografiji javnog ključa. Pored njih, još su dva tipa grupa proučavana u ovom kontekstu. Prvi tip su grupe klasa ideala u imaginarnim kvadratnim poljima (ili, što je ekvivalentno, grupe klása pozitivno definitnih kvadratnih formi). No, nakon što je McCurley 1989. godine pronašao efikasan algoritam za problem diskretnog logaritma u njima, interes za primjenu ovih grupa u kriptografiji je znatno smanjen.

Drugi tip su tzv. Jacobijani hipereliptičkih krivulja, čija je moguća primjena u kriptografiji predmet intenzivnog istraživanja posljednjih godina.

Poglavlje 5

Ostale primjene eliptičkih krivulja

5.1 Dokazivanje prostosti pomoću eliptičkih krivulja

Ukoliko broj n prođe nekoliko dobrih testova prostosti (npr. Miller-Rabinov test za nekoliko različitih baza), onda možemo biti prilično sigurni da je n prost. Međutim, ti testovi nam ne daju *dokaz* da je n prost. Što se tiče relevantnosti ovog problema za primjene u kriptografiji, treba razlikovati dva različita načina na koje se pojavljuje potreba za velikim prostim brojevima. Npr. kod izbora tajnih prostih brojeva p i q za RSA kriptosustav, želimo što brže generirati takve brojeve i tu se zadovoljavamo s time da je vrlo velika vjerojatnost da su prosti. S druge strane, kod izbora polja koje će se koristiti za šifriranje u npr. ElGamalovom kriptosustavu, radi se o prostom broju koji će se preporučiti kao standard za uporabu možda i na nekoliko godina, pa tu želimo biti sigurni (imati dokaz) da je broj stvarno prost. Sada ćemo reći nešto o metodama kojima se može dokazati da je dani broj prost.

Teorem 5.1 (Pocklington). *Neka je s djelitelj od $n-1$ koji je veći od $\sqrt{n}$. Pretpostavimo da postoji prirodan broj a takav da vrijedi*

$$a^{n-1} \equiv 1 \pmod{n},$$

$$\mathrm{nzd}(a^{(n-1)/q} - 1, n) = 1 \quad \textit{za svaki prosti djelitelj } q \textit{ od } s.$$

Tada je n prost.

Dokaz: Pretpostavimo suprotno, tj. da je n složen. Tada on ima prosti faktor $p \le \sqrt{n}$. Stavimo $b = a^{(n-1)/s}$. Tada je

$$b^s \equiv a^{n-1} \equiv 1 \pmod{n},$$

pa je i $b^s \equiv 1 \pmod{p}$. Tvrdimo da je s red od b modulo p. Zaista, pretpostavimo da za neki djelitelj q od s vrijedi $b^{s/q} \equiv 1 \pmod{p}$. Tada bi p

dijelio n i $b^{s/q} - 1$, tj. $a^{(n-1)/q} - 1$, što je u suprotnosti s pretpostavkom da su n i $a^{(n-1)/q} - 1$ relativno prosti. Kako je iz Malog Fermatova teorema $b^{p-1} \equiv 1 \pmod{p}$, zaključujemo da s dijeli $p-1$. No, to je nemoguće budući da je $s > \sqrt{n}$, a $p \leq \sqrt{n}$. □

Primjer 5.1. *Dokažimo da je broj $n = 213173$ prost.*

Rješenje: Imamo $n - 1 = 2^2 \cdot 137 \cdot 389$, pa možemo uzeti $s = 4 \cdot 137$. Prosti djelitelji od s su 2 i 137. Možemo uzeti $a = 2$ jer je $2^{n-1} \equiv 1 \pmod{n}$, $\mathrm{nzd}(2^{(n-1)/2} - 1, n) = 1$, $\mathrm{nzd}(2^{(n-1)/137} - 1, n) = 1$. Stoga Pocklingtonov teorem povlači da je n prost. Ovdje smo implicitno koristili da je 137 prost. Da bismo dokazali prostost od 137, možemo postupiti na isti način. Imamo $137 - 1 = 136 = 2^3 \cdot 17$, pa uzmimo $s = 17$. Tada iz $2^{136} \equiv 1 \pmod{137}$ i $\mathrm{nzd}(2^8 - 1, 137) = 1$ slijedi da je 137 prost (uz pretpostavku da je broj 17 prost). ♢

U prethodnom smo primjeru vidjeli da primjenom Pocklingtonova teorema pitanje o prostosti jednog broja svodimo na isto pitanje za jedan ili više manjih brojeva, i taj postupak nastavljamo sve dok brojevi ne postanu dovoljno mali.

Da bismo dokazali prostost broja n pomoću Pocklingtova teorema, moramo poznavati barem djelomičnu faktorizaciju broja $n - 1$. No, faktorizacija velikih brojeva je općenito težak problem. Ipak, ova metoda je vrlo prikladna u slučaju brojeva specijalnog oblika, kod kojih je poznata faktorizacija dovoljno velikog faktora od $n - 1$.

Teorem 5.2 (Proth). *Neka je $l \geq 2$, $k \geq 1$, $k \not\equiv 0 \pmod{3}$ i $k \leq 2^l - 1$. Tada je broj $n = k \cdot 2^l + 1$ prost ako i samo ako je $3^{k \cdot 2^{l-1}} \equiv -1 \pmod{n}$.*

Dokaz: Pretpostavimo da je $3^{k \cdot 2^{l-1}} \equiv -1 \pmod{n}$. Stavimo $s = 2^l$, $a = 3$, $n = k \cdot 2^l + 1$. Tada je $a^{n-1} = 3^{k \cdot 2^l} \equiv (-1)^2 \equiv 1 \pmod{n}$ i $a^{(n-1)/2} \equiv -1 \pmod{n}$. Budući da n dijeli $a^{(n-1)/2} + 1$, on je relativno prost s $a^{(n-1)/2} - 1$. Po Pocklingtonovu teoremu zaključujemo da je broj n prost.

Dokažimo sada obrat. Neka je n prost. Tada je, zato što 3 ne dijeli k, $n \equiv 2 \pmod{3}$, pa imamo

$$3^{k \cdot 2^{l-1}} = 3^{(n-1)/2} \equiv \left(\frac{3}{n}\right) \equiv \left(\frac{n}{3}\right) \equiv \left(\frac{2}{3}\right) \equiv -1 \pmod{n}.$$

□

Postoje metode za dokazivanje prostosti koje se zasnivaju na faktorizaciji od $n + 1$, umjesto od $n - 1$. Spomenimo samo *Lucas-Lehmerovu metodu* za dokazivanje prostosti Mersenneovih brojeva. Brojevi $M_p = 2^p - 1$, gdje je p prost, nazivaju se *Mersenneovi brojevi*. Neki Mersennovi brojevi su prosti, kao npr. $M_7 = 127$, a neki su složeni, kao npr. $M_{11} = 2047 = 23 \cdot 89$. Slutnja je da prostih Mersennovih brojeva ima beskonačno mnogo.

Teorem 5.3 (Lucas-Lehmer). *Neka je niz (v_k) zadan sa*

$$v_0 = 4, \quad v_{k+1} = v_k^2 - 2.$$

Neka je p neparan prost broj. Tada je $M_p = 2^p - 1$ prost ako i samo ako M_p dijeli v_{p-2}.

Najveći poznati prosti Mersennov broj je $M_{57885161}$. To je ujedno i najveći danas poznati prosti broj (ima 17425170 znamenaka; otkrio ga je 25.1.2013. Curtis Cooper u okviru *Great Internet Mersenne Prime Search* (GIMPS)).

Kao što smo već napomenuli, problem s primjenom Pocklingtonova teorema je u tome što zahtjeva (djelomičnu) faktorizaciju broja $n-1$. Ovaj broj $n-1$ se može shvatiti kao red grupe $\mathbb{Z}_n^*$ (ako je n prost). Jedna od ideja kako riješiti ovaj problem je zamjena grupe $\mathbb{Z}_n^*$ s grupom $E(\mathbb{Z}_n)$, gdje je E neka eliptička krivulja nad $\mathbb{Z}_n$. Naime, kod mogućih redova grupe $E(\mathbb{Z}_n)$ imamo veću fleksibilnost, pa se možemo nadati da ćemo naći eliptičku krivulju čiji će red biti lako faktorizirati. Ideju o korištenju eliptičkih krivulja za dokazivanje prostosti su uveli Goldwasser i Killian 1986. godine.

Dakle, promatrat ćemo eliptičke krivulje nad prstenom $\mathbb{Z}_n$. Budući da n ne mora biti prost, može se dogoditi da neke točke na $E(\mathbb{Z}_n)$ nećemo moći zbrojiti jer će se u formuli za zbrajanje točaka u nazivniku pojaviti broj koji nije invertibilan modulo n. No, to nam neće biti problem jer će to značiti da je n složen. Štoviše, moći ćemo mu naći netrivijalni faktor tako da izračunamo najveći zajednički djelitelj tog nazivnika i broja n.

Teorem 5.4. *Neka je E eliptička krivulja nad $\mathbb{Z}_n$, gdje je $\mathrm{nzd}(6, n) = 1$ i $n > 1$, dana jednadžbom $y^2 = x^3 + ax + b$. Neka je m prirodan broj koji ima prosti faktor $q > (n^{1/4} + 1)^2$. Ako postoji točka $P \in E(\mathbb{Z}_n)$ takva da je*

$$[m]P = \mathcal{O} \quad i \quad [m/q]P \neq \mathcal{O},$$

onda je broj n prost.

Dokaz: Ako je n složen, onda ima prosti faktor $p \leq \sqrt{n}$. Promotrimo eliptičku krivulju E' nad $\mathbb{Z}_p$ danu istom jednadžbom kao i E. Neka je m' red grupe $E'(\mathbb{Z}_p)$. Po Hasseovu teoremu je

$$m' \leq p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2 \leq (n^{1/4} + 1)^2 < q.$$

Stoga je $\mathrm{nzd}(m', q) = 1$, pa postoji $u \in \mathbb{Z}$ takav da je $uq \equiv 1 \pmod{m'}$. Neka je $P' \in E'(\mathbb{Z}_p)$ točka dobivena iz P redukcijom koordinata modulo p. Budući da je po uvjetu teorema $[m/q]P$ definirano i različito od $\mathcal{O}$ modulo n, sasvim istim postupkom modulo p dobivamo da je $[m/q]P' \neq \mathcal{O}$. No, s druge strane imamo

$$[m/q]P' = [uq \cdot \frac{m}{q}]P' = [um]P' = [u]([m]P') = \mathcal{O},$$

pa smo dobili kontradikciju. $\square$

Primjer 5.2. *Dokažimo da je broj $n = 907$ prost.*

Rješenje: Neka je E eliptička krivulja zadana jednadžbom $y^2 = x^3 + 10x - 2$ nad $\mathbb{Z}_n$. Red od $E(\mathbb{Z}_n)$ je $m = 923 = 71 \cdot 13$. Uzmimo $P = (56, 62)$ i $q = 71$. Tada je $[13]P = (338, 305) \neq \mathcal{O}$ i $[923]P = [71]([13]P) = \mathcal{O}$ (za računanje možemo koristiti algoritme iz Poglavlja 2.2; primijetimo da su NAF prikazi $13 = (1, 0, -1, 0, 1)$, $71 = (1, 0, 0, 1, 0, 0, -1)$). Budući da je $71 > (907^{1/4} + 1)^2$, odavde slijedi da je broj 907 prost (ako je poznato da je broj 71 prost). $\diamondsuit$

U praksi je kod velikih brojeva n najproblematičiji dio algoritma pronalaženje eliptičke krivulje za koju će red grupe $E(\mathbb{Z}_n)$, a to će biti broj m iz teorema, imati dovoljno veliki prosti faktor. Jedna je mogućnost biranje krivulja na slučajan način, pa računanje njihovih redova Schoofovim algoritmom. Da bismo ocijenili kolika je vjerojatnost uspjeha pronalaženja odgovarajuće krivulje, trebali bismo znati nešto o distribuciji prostih brojeva u intervalu oblika $[x+1-2\sqrt{x}, x+1+2\sqrt{x}]$. Nažalost, o tome postoje samo (nedokazane) slutnje. Ako bi vrijedilo

$$\pi(x + 1 + 2\sqrt{x}) - \pi(x + 1 - 2\sqrt{x}) > A\frac{\sqrt{x}}{\ln x},$$

za neku konstantu A (što je slutnja za koju se vjeruje da bi trebala vrijediti, a motivirana je teoremom o prostim brojevima), onda bi očekivani broj operacija u Goldwasser-Killianovu algoritmu bio $O(\ln^{10} n)$. Mogli bismo reći da je interval iz Hasseova teorema dovoljno velik za praksu, ali ne i za trenutno stanje teorije. Adleman i Huang su 1992. godine predložili algoritam koji umjesto eliptičkih krivulja koristi Jacobijane hipereliptičkih krivulja, a za koji se korištenjem poznatih rezultata o distribuciji prostih brojeva u intervalu oblika $[x, x + x^{3/4}]$ može dokazati da mu je očekivani broj operacija polinomijan.

Atkin i Morain su 1993. godine predložili jednu varijantu dokazivanja prostosti pomoću eliptičkih krivulja, za koju se danas smatra da je najefikasnija u praksi. Pomoću te se metode danas može efikasno dokazati prostost brojeva s oko 1000 znamenaka. Metoda koristi eliptičke krivulje s *kompleksnim množenjem*, s pripadnim imaginarnim kvadratnim poljem $\mathbb{Q}(\sqrt{-d})$. Za takve krivulje E vrijedi da ako je $4p = x^2 + dy^2$, onda su mogući redovi od E nad $\mathbb{Z}_p$ brojevi $p + 1 \pm x$. Dakle, ove brojeve možemo efikasno izračunati, te vidjeti imaju li dovoljno veliki prosti faktor. Kad pronađemo red koji nas zadovoljava, samu krivulju konstruiramo koristeći teoriju kompleksnog množenja, posebno j-*invarijante*.

Spomenimo još da su 2002. godine Agrawal, Kayal i Saxena pronašli prvi polinomijalni algoritam za dokazivanje prostosti, po njima nazvan *AKS algoritam* (članak su objavili 2004. godine u jednom od najprestižnijih matematičkih časopisa "Annals of Mathematics"). Kao i većina algoritama za testiranje ili dokazivanje prostosti, i AKS algoritam se zasniva na jednoj varijanti

Malog Fermatovog teorema. Točnije, polazište mu je sljedeći rezultat. Neka su a i n cijeli brojevi, $n \geq 2$ i $\mathrm{nzd}(a,n) = 1$. Tada je broj n prost ako i samo ako vrijedi

$$(X+a)^n \equiv X^n + a \pmod{n}, \tag{5.1}$$

tj. ako i samo ako su odgovarajući koeficijenti polinoma na lijevoj i desnoj strani kongruencije (5.1) kongruentni modulo n.

5.2 Faktorizacija pomoću eliptičkih krivulja

Ako prirodan broj n ne prođe neki od testova prostosti, onda znamo da je n sigurno složen. Međutim, ti nam testovi uglavnom ne daju niti jedan netrivijalni faktor od n. Stoga se postavlja pitanje kako naći netrivijalni faktor velikog složenog broja. To se smatra teškim problemom i na njegovoj su težini zasnovani neki od najvažnijih kriptosustava s javnim ključem.

Metode faktorizacije možemo podijeliti na opće i specijalne. Kod općih metoda očekivani broj operacija ovisi samo o veličini broja n, dok kod specijalnih ovisi također i o svojstvima faktora od n.

Naivna metoda faktorizacije broja n jest dijeljenje broja n sa svim prostim brojevima $\leq \sqrt{n}$. Broj potrebnih dijeljenja je u najlošijem slučaju oko $\frac{2\sqrt{n}}{\ln n}$, pa je složenost ove metode $O(\sqrt{n}\ln n)$. Kod ove smo ocjene pretpostavili da nam je dostupna tablica svih prostih brojeva $\leq \sqrt{n}$. U protivnom, dijelili bismo s 2, te sa svim neparnim brojevima, ili samo s neparnim brojevima koji zadovoljavaju određene kongruencije (npr. $\equiv 1, 5 \pmod{6}$ ili $\equiv 1, 7, 11, 13, 17, 19, 23, 29 \pmod{30}$). U svakom slučaju, ova metoda je vrlo neefikasna za velike n-ove. Međutim, dobro ju je koristiti u kombinaciji s boljim metodama faktorizacije, za uklanjanje eventualnih malih faktora od n.

Pollardova $p-1$ metoda iz 1974. godine spada u specijalne metode faktorizacije. Njezino polazište je ponovno Mali Fermatov teorem. Neka je n složen broj koji želimo faktorizirati, te neka je p neki njegov prosti faktor. Tada je $a^{p-1} \equiv 1 \pmod{p}$ za $\mathrm{nzd}(a,p) = 1$. Štoviše, vrijedi $a^m \equiv 1 \pmod{p}$ za svaki višekratnik m od $p-1$. Ako nađemo m, onda nam $\mathrm{nzd}(a^m-1, n)$ daje faktor (nadamo se netrivijalni) od n. No, pitanje je kako naći višekratnik od $p-1$ kad ne znamo p. To možemo efikasno napraviti u slučaju kada broj $p-1$ ima samo male proste faktore. Za prirodan broj kažemo da je *B-gladak* ako su mu svi prosti faktori $\leq B$. Pretpostavimo dodatno da su sve potencije prostih brojeva, koje dijele $p-1$, manje ili jednake B. Tada za m možemo uzeti najmanji zajednički višekratnik brojeva $1, 2, \ldots, B$. Za ovako odabrani m, broj operacija za računanje $a^m \bmod n$ je $O(B \ln B \ln^2 n + \ln^3 n)$. U najgorem slučaju, a to je kada je broj $\frac{p-1}{2}$ prost, ova metoda nije ništa bolja od običnog dijeljenja.

Primjer 5.3. Neka je $n = 846631$. Izaberimo $B = 8$ i $a = 2$. Tada je $m = 2^3 \cdot 3 \cdot 5 \cdot 7 = 840$. Imamo da je $2^{840} \bmod n = 346905$ i $\mathrm{nzd}(346904, n) = 421$. Zaista, $n = 421 \cdot 2011$. $\diamondsuit$

Pomoću $p-1$ metode je Baillie 1980. godine našao 25-znamenkasti faktor Mersenneovog broja $2^{257} - 1$.

Uspjeh $p-1$ metode direktno ovisi o glatkoći broja $p-1$. Postoje varijante ove metode koje koriste glatkoću brojeva $p+1$, p^2+p+1, p^2+1 ili p^2-p+1. No, najvažnija modifikacija $p-1$ metode je Lenstrina metoda faktorizacije pomoću eliptičkih krivulja. U njoj se, ponovo, grupa $\mathbb{F}_p^*$ reda $p-1$ zamjenjuje grupom $E(\mathbb{F}_p)$, čiji red varira unutar intervala $\langle p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}\,\rangle$, pa se možemo nadati da ćemo pronaći eliptičku krivulju nad $\mathbb{F}_p$ dovoljno glatkog reda.

Godine 1987. H. W. Lenstra je predložio modifikaciju Pollardove $p-1$ metode koja koristi eliptičke krivulje. Kao rezultat je dobio subeksponencijalni algoritam koji i danas predstavlja jedan od najefikasnijih poznatih algoritama za faktorizaciju.

Slično kao kod metode dokazivanja prostosti pomoću eliptičkih krivulja, i ovdje ćemo raditi s eliptičkim krivuljama nad prstenom $\mathbb{Z}_n$. Dok je kod dokazivanja prostosti postojala (mala) mogućnosti da je n složen (tj. da $\mathbb{Z}_n$ nije polje), ovdje ćemo od početka biti sigurni da je n složen. Pretpostavit ćemo da je $\mathrm{nzd}(n, 6) = 1$, te ćemo promatrati eliptičke krivulje oblika

$$E_{a,b} : \quad y^2 = x^3 + ax + b,$$

gdje je $\mathrm{nzd}(4a^3 + 27b^2, n) = 1$. Kada je n prost, onda na eliptičkoj krivulji postoji samo jedna projektivna točka koja ne odgovara nekoj afinoj točki (točka u beskonačnosti). U slučaju kada je n složen, takvih točaka može biti više.

Opišimo sada osnovne korake u *Lenstrinom algoritmu za faktorizaciju* (Elliptic Curve Method - ECM).

1. Izbor eliptičke krivulje.

   Postoji više načina za izbor odgovarajuće eliptičke krivulje. Na primjer, možemo slučajno izabrati elemente $a, x, y \in \mathbb{Z}_n$, pa izračunati $b = (y^2 - x^3 - ax) \bmod n$. Neka je $g = \mathrm{nzd}(4a^3 + 27b^2, n)$. Ako je $1 < g < n$, onda smo našli netrivijalni faktor od n. Ako je $g = n$, onda biramo nove a, x, y. Ako je $g = 1$, onda smo našli eliptičku krivulju $E_{a,b}$ nad $\mathbb{Z}_n$ i točku $P = (x, y)$ na njoj.

2. Neka je k najmanji zajednički višekratnik brojeva $1, 2, \ldots, B$, za prikladno odabranu granicu B. U praksi se obično uzima najprije $B = 10000$, a potom se granica po potrebi povećava.

3. Računamo $[k]P \in E_{a,b}(\mathbb{Z}_n)$ koristeći formule za zbrajanje točaka:

$$(x_3, y_3) = (\lambda^2 - x_1 - x_2 \bmod n,\ \lambda(x_1 - x_3) - y_1 \bmod n),$$

   gdje je $\lambda = (3x_1^2 + a) \cdot (2y_1)^{-1} \bmod n$ ako su točke jednake, a $\lambda = (y_1 - y_2)(x_1 - x_2)^{-1} \bmod n$, inače.

4. Ako se u računanju $[k]P$ dogodi da neki zbroj točaka ne možemo izračunati zato što ne možemo izračunati d^{-1} jer d nema inverz modulo n, onda izračunamo $g = \mathrm{nzd}(d, n)$. Ako je $g \neq n$, onda smo našli netrivijalni faktor od n.

5. U slučaju neuspjeha, možemo izabrati novu eliptičku krivulju ili povećati granicu B.

Primjer 5.4. *Faktorizirati broj* $n = 209$.

Rješenje: Neka je $B = 3$, pa je $k = 6$. Izaberimo eliptičku krivulju $y^2 = x^3 + 4x + 9$ i očitu točku na njoj $P = (0, 3)$. Računamo $[6]P = [2](P + [2]P)$. Najprije računamo $[2]P$. Pripadni λ je $4 \cdot 6^{-1} = 140 \bmod 209$, pa dobivamo $[2]P = (163, 167)$. Zatim računamo $[3]P = P + [2]P$. Pripadni λ je $164 \cdot 163^{-1} = 160 \bmod 209$, pa je $[3]P = (148, 143)$. Konačno, računamo $[6]P = [2]([3]P)$. Pripadni λ je $90 \cdot 77^{-1}$. Kod računanja inverza od 77 modulo 209, dobivamo da taj inverz ne postoji jer je $\mathrm{nzd}(77, 209) = 11$. Odavde zaključujemo da je 11 faktor od 209. Zaista, $209 = 11 \cdot 19$. $\diamondsuit$

O čemu ovisi uspjeh ovog algoritma? Slično kao kod $p-1$ metode, i ovdje bi k trebao biti višekratnik reda pripadne grupe. U ovom bi slučaju k trebao biti višekratnik od $|E(\mathbb{F}_p)|$, gdje je p neki prosti faktor od n. Zaista, u tom slučaju će kod računanja $[k]P$ pripadni nazivnik biti djeljiv s p, pa neće biti invertibilan modulo n. Naime, u $E(\mathbb{F}_p)$ će vrijediti da je $[k]P = \mathcal{O}$.

Kod ocjene složenosti ovog algoritma ključno je pitanje kako optimalno odabrati granicu B. Uvedimo oznaku

$$\psi(x, y) = \#\{1 \leq n \leq x \,:\, n \text{ je } y\text{-gladak}\}.$$

Koristeći činjenicu da su redovi $|E(\mathbb{F}_p)|$ skoro uniformno distribuirani unutar Hasseova intervala, dolazimo do sljedeće ocjene za vjerojatnost uspjeha algoritma:

$$prob(B) > c \cdot \frac{\psi(p + 1 + 2\sqrt{p}, B) - \psi(p + 1 - 2\sqrt{p}, B)}{\sqrt{p} \ln p}.$$

Kako je, s druge strane, broj operacija potrebnih za pokušaj faktorizacije pomoću jedne krivulje proporcionalan s B, željeli bismo minimizirati vrijednost $B/prob(B)$. Pokazuje se da se minimum postiže za

$$B = e^{(\sqrt{2}/2 + o(1))\sqrt{\ln p \ln \ln p}},$$

dok je složenost algoritma

$$e^{(\sqrt{2}+o(1))\sqrt{\ln p \ln\ln p}}.$$

U najlošijem slučaju (kada je $p = O(\sqrt{n})$), složenost metode faktorizacije pomoću eliptičkih krivulja je $e^{O(\sqrt{\ln n \ln\ln n})}$. Dakle, to je subeksponencijalni algoritam.

Iako postoje algoritmi bolje složenosti (algoritam sita polja brojeva), važno svojstvo ECM je da njezina složenost ovisi o najmanjem prostom faktoru od n. Zato ona nije najprikladnija za faktorizaciju RSA modula, tj. brojeva oblika $n = pq$, gdje su p i q bliski prosti brojevi. Međutim, kod faktorizacije "slučajnih" brojeva, ECM često daje bolje rezultate od ostalih metoda, jer takvi brojevi obično imaju neki prosti faktor koji je znatno manji od $\sqrt{n}$. Čak i kod primjene asimptotski boljih metoda, unutar tih algoritama potrebno je faktorizirati neke pomoćne brojeve, za koje možemo očekivati da se ponašaju kao slučajni brojevi, pa se tu ECM može koristiti kao pomoćna metoda.

Među faktorizacijama dobivenim pomoću ECM, spomenimo nalaženje 33-znamenkastog faktora Fermatovog broja $2^{2^{15}}+1$ (Crandall, van Halewyn, 1997.), te nalaženje 49-znamenkastog faktora Mersenneovog broja $2^{2071}-1$ (Zimmermann, 1998.).

Bibliografija

[1] A. ASH, R. GROSS, *Elliptic Tales: Curves, Counting and Number Theory*, Princeton University Press, 2012.

[2] A. K. BHANDARI, D.D. NAGRAJ, R. RAMAKRISHNAN, T.N. VENKATARAMANA (EDS.), *Elliptic Curves, Modular Forms and Cryptography*, Hindustan Book Agency, 2003.

[3] I. BLAKE, G. SEROUSSI, N. SMART, *Elliptic Curves in Cryptography*, Cambridge University Press, 1999.

[4] I. BLAKE, G. SEROUSSI, N. SMART (EDS), *Advances in Elliptic Curve Cryptography*, Cambridge University Press, 2005.

[5] J. S. CHAHAL, *Topics in Number Theory*, Plenum Press, 1988.

[6] H. COHEN, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.

[7] H. COHEN, G. FREY (EDS), *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall/CRC, 2005.

[8] I. CONNELL, *Elliptic Curve Handbook*, `http://www.math.mcgill.ca/connell/public/ECH1/`

[9] J. B. CONREY, D. W. FARMER, F. MEZZADRI, N. C. SNAITH (EDS), *Ranks of Elliptic Curves and Random Matrix Theory*, Cambridge University Press, 2007.

[10] J. E. CREMONA, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1997.

[11] H. DARMON, *Rational Points on Modular Elliptic Curves*, American Mathematical Society, 2004.

[12] F. DIAMOND, J. SHURMAN, *A First Course in Modular Forms*, Springer-Verlag, 2005.

[13] A. DUJELLA, M. MARETIĆ, *Kriptografija*, Element, Zagreb, 2007.

[14] T. EKEDAHL, *One Semester of Elliptic Curves*, European Mathematical Society, 2006.

[15] P. GARRETT, D. LIEMAN (EDS.), *Public-Key Cryptography*, American Mathematical Society, 2005.

[16] D. HANKERSON, A. MENEZES, S. VANSTONE, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, 2004.

[17] J. HOFFSTEIN, J. PIPHER, J. H. SILVERMAN, *An Introduction to Mathematical Cryptography*, Springer, 2008.

[18] H. KISILEVSKY, M. R. MURTY (EDS.), *Elliptic Curves and Related Topics*, American Mathematical Society, 1994.

[19] A. W. KNAPP, *Elliptic Curves*, Princeton University Press, 1992.

[20] N. KOBLITZ, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, 1993.

[21] N. KOBLITZ, *A Course in Number Theory and Cryptography*, Springer-Verlag, 1994.

[22] N. KOBLITZ, *Algebraic Aspects of Cryptography*, Spinger-Verlag, 1999.

[23] N. KOBLITZ, A. MENEZES, S.A. VANSTONE, *The State of Elliptic Curve Cryptography*, Designs, Codes and Cryptography 19 (2000), pp. 173–193.

[24] S. LANG, *Elliptic Curves: Diophantine Analysis*, Springer-Verlag, 1978.

[25] A. K. LENSTRA, E. R. VERHEUL, *Selecting cryptographic key sizes*, Journal of Cryptology 14 (2001), 255-293.

[26] R. A. MOLLIN, *An Introduction to Cryptography*, Chapman & Hall/CRC Press, 2001.

[27] M. ROSING, *Implementing Elliptic Curve Cryptography*, Manning, 1999.

[28] S. SCHMITT, H. G. ZIMMER, *Elliptic Curves. A Computational Approach*, de Gruyter, 2003.

[29] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1996, 2009.

[30] J. H. SILVERMAN, J. TATE, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.

[31] N. SMART, *Cryptography. An Introduction*, McGraw-Hill, New York, 2002.

[32] D. R. STINSON, *Cryptography. Theory and Practice*, CRC Press, 1996, 2002, 2005.

[33] W. TRAPPE, L. C. WASHINGTON, *Introduction to Cryptography with Coding Theory*, Prentice Hall, 2002.

[34] L. C. WASHINGTON, *Elliptic Curves: Number Theory and Cryptography*, CRC Press, 2003, 2008.

[35] S. Y. YAN, *Number Theory for Computing*, Springer-Verlag, 2002.