Eliptičke krivulje

Andrej Dujella

e-mail: duje@math.hr
URL: http://web.math.hr/~duje/

Sažetak:

Cilj ovog kolegija je upoznati studente s osnovnim pojmovima, činjenicama i algoritmima vezanim uz eliptičke krivulje nad poljem racionalnih brojeva i konačnim poljima, te njihovim primjenama u kriptografiji.

Opisat će se grupovni zakon za eliptičke krivulje. Potom će se obraditi osnovna svojstva eliptičkih krivulja nad poljem racionalnih brojeva. Opisat će se algoritmi za računanje torzijske grupe i ranga eliptičke krivulje.

Kod eliptičkih krivulja nad konačnim poljima, bit će riječi o efikasnoj implementaciji zbrajanja i multipliciranja točaka. Prikazat će se algoritmi za efikasno brojenje točaka, te algoritmi za problem diskretnog logaritma na eliptičkoj krivulji.

Objasnit će se primjena eliptičkih krivulja u kriptografiji, te dati usporedba kripotosustava zasnovanih na eliptičkim krivuljama s ostalim najvažnijim kriptosustavima s javnim ključem. Također će se prikazati primjena eliptičkih krivulja u faktorizaciji i dokazivanju prostosti velikih prirodnih brojeva.

Od studenata se očekuje poznavanje osnovnih pojmova i činjenica iz teorije brojeva. Ispit će se sastojati od rješavanja domaćih zadaća, te pisanja seminarskog rada.

Literatura:

[1] I. Blake, G. Seroussi, N. Smart: *Elliptic Curves in Cryptography*, Cambridge University Press, 1999.

[2] I. Connell: *Elliptic Curve Handbook*, McGill University, 1999.
`http://www.math.mcgill.ca/connell/public/ECH1/`

[3] J. E. Cremona: *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1997.
`http://www.warwick.ac.uk/~masgaj/book/amec.html`

[4] A. Dujella, M. Maretić: *Kriptografija*, Element, 2007.

[5] D. Hankerson, A. Menezes, S. Vanstone: *Guide to Elliptic Curve Cryptography*, Springer-Verlag, 2004.

[6] N. Koblitz: A Course in Number Theory and Cryptography, Springer-Verlag, 1994.

[7] J. S. Milne: Elliptic Curves, BookSurge Publishers, 2006.
`http://www.jmilne.org/math/Books/ectext.html`

[8] J. H. Silverman: The Arithmetic of Elliptic Curves, Springer-Verlag, 1996.

[9] J. H. Silverman, J. Tate: *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.

[10] L. C. Washington: *Elliptic Curves: Number Theory and Cryptography*, CRC Press, 2008.

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 $a, b, c, \ldots, j \in \mathbb{K}$, 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*

$$\Delta = -4a^3 - 27b^2$$

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

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

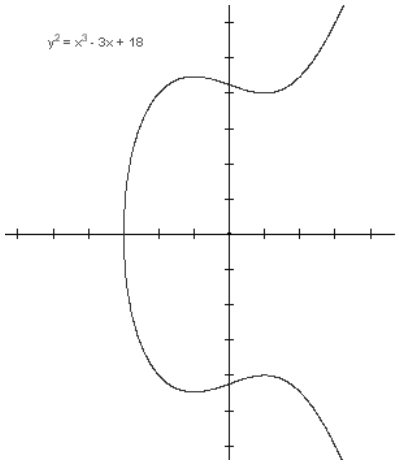
gdje su $a, b \in \mathbb{K}$ i $4a^3 + 27b^2 \neq 0$, zajedno s "točkom u beskonačnosti" $\mathcal{O}$. Taj skup ćemo označavati s $E(\mathbb{K})$.

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

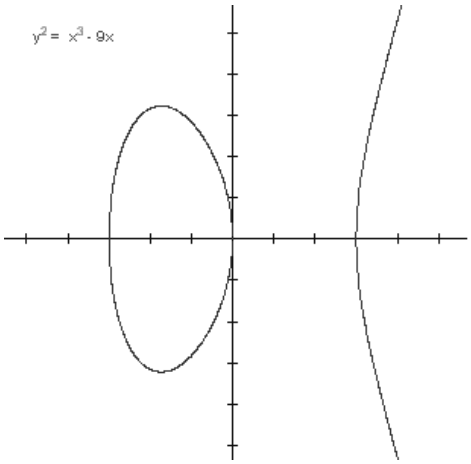
$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

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.

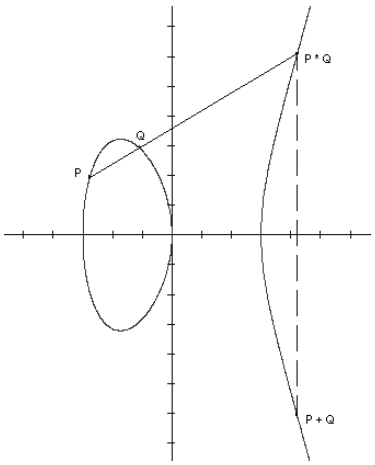


1 komponenta

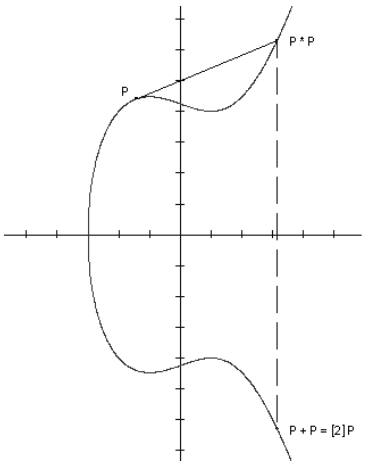


2 komponente

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 $P = Q$.

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 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

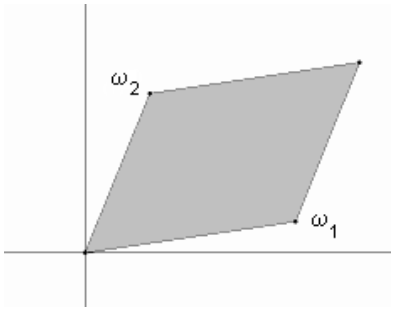
$$P + Q = (\wp(t+u), \frac{1}{2}\wp'(t+u)).$$

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

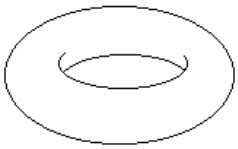
Gore navedena parametrizacija točaka na eliptičkoj krivulji pomoću funkcije $\wp$ predstavlja zapravo izomorfizam grupa $E(\mathbb{C})$ i $\mathbb{C}/L$. Funkcija $\wp$ je u potpunosti određena svojim vrijednostima u "fundamentalnom paralelogramu" koji se sastoji od svih kompleksnih brojeva oblika $m\omega_1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



fundamentalni paralelogram

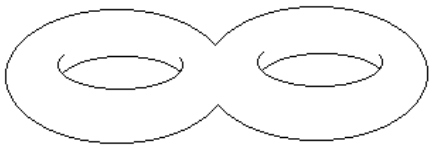
Razlika točaka koje se nalaze nasuprot jedna drugoj na paralelnim stranicama tog paralelograma je element iz L. Stoga su te točke poistovjećene u skupu $\mathbb{C}/L$. Da bi vizualizirali taj skup, možemo zamisliti da smo najprije "slijepili" dvije suprotne stranice paralelograma. Tako dobivamo valjak.

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 $n = 4$ također imamo eliptičku krivulju. Uvjerimo se u to na jednom primjeru. Neka je C krivulja zadana jednadžbom

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

Uvedimo suptituciju $x = \frac{2}{s-1}$, $y = \frac{2t}{(s-1)^2}$. Inverzna transformacija je $s = \frac{x+2}{x}$, $t = \frac{2y}{x^2}$. Stoga je ovo biracionalna transformacija. Ona prevodi krivulju C u eliptičku krivulju danu jednadžbom

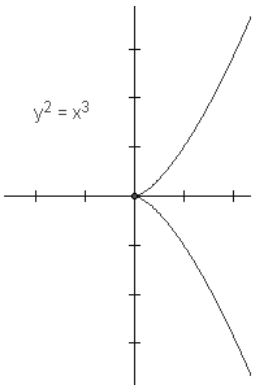
$$t^2 = s^3 - 3s + 6.$$

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

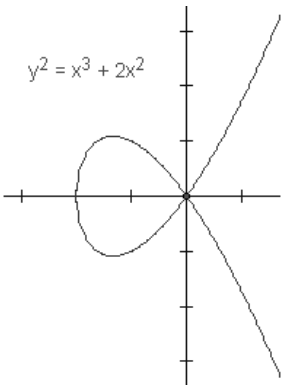
Krivulje genusa 0 su upravo one koje posjeduju parametrizaciju pomoću racionalnih funkcija. Svaka krivulja drugog stupnja (konika) ima genus 0. Npr. krivulja $x^2 + y^2 = 1$ ima racionalnu parametrizaciju

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

Kubne singularne krivulje također imaju genus 0. Npr. krivulja $y^2 = x^3$ ima singularnu točku $(0,0)$. 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 je također singularna i ima racionalnu parametrizaciju $x = t^2 - 2$, $y = t^3 - 2t$.



singularna krivulja



singularna krivulja

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.

2. Eliptičke krivulje nad $\mathbb{Q}$

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

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

Mordell-Weilov teorem nam, drugim riječima, kaže da postoji konačan skup racionalnih točaka $P_1, \ldots, P_k$ 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 $k_1 \,|\, k_2 \,|\, \cdots \,|\, k_m$, gdje je $\mathbb{Z}_k = \mathbb{Z}/k\mathbb{Z}$), dobivamo sljedeću neposrednu posljedicu Mordell-Weilovog teorema.

Korolar:

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

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 $P_1, \ldots, P_r$ 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 $m_1, \ldots, m_r$ 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 $\frac{m_1}{n}\omega_1 + \frac{m_2}{n}\omega_2$, $0 \leq m_1, m_2 < n$. Dakle, rješenja jednadžbe $nP = \mathcal{O}$ čine grupu izomorfnu sa $\mathbb{Z}_n \times \mathbb{Z}_n$.

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. 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: (Lutz-Nagell) Neka je E eliptička krivulja zadana jednadžbom

$$y^2 = f(x) = x^3 + ax^2 + bx + c, \qquad (1)$$

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

Korolar: Neka je E eliptička krivulja zadana jednadžbom (1), 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 $y_1^2 | \Delta$, gdje je

$$\Delta = -27c^2 - 4a^3c - 4b^3 + a^2b^2 + 18abc.$$

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.

Primijetimo da je za krivulju oblika $y^2 = x^3 + ax + b$, $\Delta = -4a^3 - 27b^2$.

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: Odredimo torzijsku grupu eliptičke krivulje

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

Rješenje: Imamo $\Delta = -4$. 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: Odredimo torzijsku grupu eliptičke krivulje

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

Rješnje: Ovdje je $\Delta = -1728$. Ako je $y = 0$, onda je $x = -2$, pa imamo točku $(-2, 0)$ reda 2. Ako je $y \neq 0$, onda $y^2 | 1728$, tj. $y | 24$. Testiranjem svih mogućnosti, nalazimo sljedeće dvije 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,
$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (-2, 0)\} \cong \mathbb{Z}_2$.

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, koja je posljedica Lutz-Nagellovog teorema:

Propozicija: 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 $p \nmid \Delta$, 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 $P = \mathcal{O}$.

Po propoziciji, 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 metodama 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 $p + 1 - \texttt{ellap}(E, p)$. Verzija $\texttt{ellap}(E, p, 1)$ koristi upravo navedenu formulu pomoću Legendreovih simbola, dok $\texttt{ellap}(E, p, 0)$ ili $\texttt{ellap}(E, p)$ koristi Shanks-Mestreovu metodu koja je efikasnija za $p > 100$.

Primjer: Odredimo torzijsku grupu eliptičke krivulje

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

Rješenje: Ovdje je $\Delta = -4 \cdot 18^3 - 27 \cdot 72^2 = -16396 = -2^5 \cdot 3^6 \cdot 7$. 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 $\gcd(5, 8) = 1$, direktno slijedi da je torzijska grupa od $E(\mathbb{Q})$ trivijalna.

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 $\gcd(m, n) = 1$. 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 cijelobrojnu 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 $E(\mathbb{Q})$.

Za primjenu ovog algoritma, trebamo moći efikasno izračunati periode ω_1 i ω_2, a također i vrijednost funkcije $\wp$. Kao što smo već spominjali, u PARI-ju postoje gotove funkcije za njihovo računanje, koje koriste *aritmetičko-geometrijsku sredinu* (AGM). Aritmetičko-geometrijsku sredinu pozitivnih realnih brojeva a i b, uveo je Gauss, u svrhu računanja eliptičkih integrala. Definiramo dva niza brojeva (a_n) i (b_n) sa

$$a_0 = a, \;\; b_0 = b, \;\; a_n = \frac{1}{2}(a_{n-1} + b_{n-1}),$$

$$b_n = \sqrt{a_{n-1} b_{n-1}}.$$

Propozicija: Pretpostavimo da je $a \geq b > 0$. Tada vrijedi

$$b_{n-1} \leq b_n \leq a_n \leq a_{n-1}, \quad 0 \leq a_n - b_n \leq \frac{1}{2}(a_{n-1} - b_{n-1}).$$

Stoga limesi $\lim_{n\to\infty} a_n$ i $\lim_{n\to\infty} b_n$ postoje i jednaki su. Nadalje, ako je $b \geq 1$, onda vrijedi

$$\frac{a_n - b_n}{8} \leq \left(\frac{a_{n-1} - b_{n-1}}{8}\right)^2. \qquad (2)$$

Zajednički limes iz prethodne propozicije zove se aritmetičko-geometrijska sredina (AGM) brojeva a i b, te se označava s $M(a,b)$. Zbog $M(ca,cb) = cM(a,b)$ i $M(b,a) = M(a,b)$, možemo lako postići da je $b \geq 1$ i $a \geq b$. Nejednakost (2) nam pokazuje da kod aproksimacije $M(a,b)$ pomoću a_n i b_n, u svakoj sljedećoj iteracija broj točkih decimalnih mjesta se udvostručuje.

Weierstrassova funkcija $\wp$, koja odgovara rešetki Λ, definira se sa

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

Jedan od načina da se efikasno izračuna vrijednost funkcije $\wp$ je pomoću slijedeće formule:

$$\wp(z) = \left(\frac{2\pi i}{\omega_1}\right)^2 \left(\frac{1}{12} + \frac{u}{(1-u)^2} + \sum_{n=1}^{\infty} q^n \left(\frac{u}{(1-q^n u)^2} + \frac{u}{(q^n - u)^2} - \frac{2}{(1-q^n)^2} \right) \right),$$

gdje je $u = e^{2\pi i z/\omega_1}$, $\tau = \omega_2/\omega_1$ i $q = e^{2\pi i \tau}$.

Primjer: Odredimo torzijsku grupu eliptičke krivulje

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

Rješenje: Imamo da je

$$\Delta = -4a^3 - 27b^2 = 372386507784192 = 2^{18} \cdot 3^{17} \cdot 11.$$

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. Koristeći AGM, računamo periode

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

Odavde dobivamo

$$\tau = 0.789080\ldots i, \quad q = 0.00702741\ldots.$$

Računamo

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

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

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

Metode za određivanje torzijske grupe eliptičke krivulje nad $\mathbb{Q}$ koje smo opisali 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.

U programskom paketu PARI/GP (`http://pari.math.u-bordeaux.fr/`) implementiran je veći broj važnijih funkcija vezanih uz eliptičke krivulje. Ovdje ćemo navesti samo neke (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`. (Koeficijenti b_i i c_i se javljaju kod prebacivanja krivulje u kratku Weierstrassovu formu.)

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 $x = u^2x' + r$, $y = u^3y' + su^2x' + t$.

`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 t (modulo rešetka određena sa E) koji odgovara točki P (njezin parametar), tj. $\wp(t) = P[1]$, $\wp'(t) = P[2]$.

`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].

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

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

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

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \quad (3)$$

Stoga navedimo formule za zbrajanje točaka na krivulji danoj sa (3): 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 (3) $a_6 = 0$, 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*

$$y^2 + (1 - c)xy - by = x^3 - bx^2. \qquad (4)$$

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:

$$-P = (0, b), \;\; 2P = (b, bc), \;\; -2P = (b, 0),$$

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

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

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

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

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

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

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

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

$$y^2 + (1-c)xy - by = x^3 - bx^2,$$

$$b = d^3 - d^2, \;\; c = d^2 - d, \;\; d \in \mathbb{Q}.$$

- 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

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

- 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

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

- 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

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

- 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 $\mathbb{Z}_{12}$

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

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

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma), \quad \alpha, \beta, \gamma \in \mathbb{Q}. \quad (5)$$

Jednadžba (5) 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: 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 $P = 2Q$, 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,

$$(x-\alpha)(x-\beta)(x-\gamma)-(\lambda x+\mu)^2 = (x-x_1)^2(x-x_2). \tag{6}$$

Uvrstimo $x = \alpha$ u (6), 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

$$y^2 = x(x + r^2)(x + s^2), \quad r, s \in \mathbb{Q}. \qquad (7)$$

Točka reda 4 na (7) 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 prethodnom teoremu, 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 $t \in \mathbb{Q}$. Stoga je opći oblik krivulje s torzijskom podgrupom $\mathbb{Z}_2 \times \mathbb{Z}_8$

$$y^2 = x(x + r^2)(x + s^2),$$

$$r = t^2 - 1, \;\; s = \frac{4t^2}{t^2 - 1}, \;\; t \in \mathbb{Q}.$$

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 $2Q = P$. Tada u (5) moramo imati $\alpha = -r^2$, $\beta = -s^2$, $\gamma = -t^2$. Dakle, dobili smo krivulju

$$y^2 = (x + r^2)(x + s^2)(x + t^2), \qquad (8)$$

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

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

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

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

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

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:

P_1=[−212415009125438107329213746 3,259854492051899599030515511070780628911531]

P_2=[233450986603470175688475453 7,188720041954944691808683165528036279315 31]

P_3=[−167173605406236906387903866 3,251709377261144287808506947241319126049131]

P_4=[213913026013915666649298213 7,366395091714397292024214596929412975275 31]

P_5=[153470676446712072388547733 7,854295853460176942890210328627810727995 31]

P_6=[−273107948787567703334157506 3,262521815484332191641284072623902143387531]

P_7=[277572626684457164970545853 7,128457554740140602488694876990826403699 31]

P_8=[149438572932718895754183381 7,884866055277334059861164945140492334114 51]

P_9=[186843822862088735850906525 7,592374032144377087127251403930593585891 31]

P_{10}=[200894510882574377486654253 7,476906778801255528821517507815414247115 31]

P_{11}=[234836054091802516965163293 7,174929300062005578573403324764488043635 31]

P_{12}=[−147208400709048117447000866 3,246643450653503714199947441549759798469131]

P_{13}=[292412860770806121336328893 7,283502644314888785014883564747673758995 31]

P_{14}=[537499389106606189329393453 7,286188908427263386451175031916479893731531]

P_{15}=[170969076823335452333400855 7,718988349746860894661597005292159809216 31]

P_{16}=[245095401135359314407259518 7,444522817353263435704926255061071473653 1]

P_{17}=[296925470927355916746467493 7,327668930753662708013336825431604696875 31]

P_{18}=[271191493494169260133288293 7,206843661277838169865041398150659061353 1]

P_{19}=[200785860779968545287783289 37,277960854113780660465605172562462403009 1531]

P_{20}=[215808245024073477431781069 7,349943734019640268099696622418009012547 31]

P_{21}=[200464545824705902240322493 7,480493297807046455224398669998884754675 31]

P_{22}=[297574945094799626494709133 7,333989898260753223202089344101048578691 31]

P_{23}=[−210249046768628515014734786 3,259576391459875789571677393171687203227531]

P_{24}=[311583179915063034902194537,168104385229980603540109472915660153473931]

P_{25}=[277393100834186523144377181 7,126321628346499210024141162737692758134 51]

P_{26}=[215658118814376840936346138 7,351250929640229088970041505163751780873 31]

P_{27}=[386633049987241250881565913 7,121197755655944226293036926715025847322531]

P_{28}=[223086828977357602377867873 7,285587600305974856633870206007686400285 31]

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, 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

$$y^2 = x^3 + ax^2 + bx, \tag{9}$$

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 $a = 3x_0 + a_2$, $b = (a + a_2)x_0 + a_4$.

Za krivulju E' koja ima jednadžbu

$$y^2 = x^3 + a'x^2 + b'x, \tag{10}$$

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

Želimo dobiti opis elementa iz $\text{Im}(\alpha)$. 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 $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$, $\gcd(m, e) = \gcd(n, e) = 1$, te ih uvrstimo u jednadžbu od E. Dobivamo:

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

Stavimo $b_1 = \pm \gcd(m, b)$, 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 $m_1 = M^2$, $b_1 m_1^2 + a m_1 e^2 + b_2 e^4 = N^2$, te tako konačno dobivamo jednadžbu

$$N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4 \qquad (11)$$

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 Im(α) sastoji od $\tilde{1}$, $\tilde{b}$, te od svih $\tilde{b_1}$ gdje je b_1 djelitelj broja b za kojeg jednadžba

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

gdje je $b_1 b_2 = b$, ima rješenja $N, M, e \in \mathbb{Z}$, $e \neq 0$. Tada je $(\frac{b_1 M^2}{e^2}, \frac{b_1 M N}{e^3}) \in E(\mathbb{Q})$. Uočimo da jednadžba (11) 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 (11) možemo pretpostaviti da je $\gcd(M, e) = 1$. 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 $\gcd(N, e) = \gcd(M, N) = 1$.

Program MWRANK autora Johna Cremone predstavlja danas najbolju slobodno dostupnu implementaciju algoritma silaska pomoću 2-izogenije. Uključen je u programski paket SAGE.

Imamo sljedeći algoritam za računanje ranga eliptičke krivulje E koja ima racionalnu točku reda 2, tj. ima jednadžbu oblika (9). Za svaku faktorizaciju $b = b_1 b_2$, gdje je b_1 kvadratno slobodan cijeli broj, napišemo jednadžbu (11). 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 (11) inducira točku na krivulji E s koordinatama $x = \frac{b_1 M^2}{e^2}$, $y = \frac{b_1 M N}{e^3}$. Neka je r_1 broj faktorizacija za koje pripadna jednadžba (11) 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

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

Primjer: 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 $\gcd(M, 5) = 1$. 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 $\text{rank}\,(E) = 2 + 1 - 2 = 1$.

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 $\mathbb{Z}_5$. No, kod diofantskih jednadžbi stupnja većeg od 2 može se dogoditi da one imaju rješenja u $\mathbb{R}$, te da imaju rješenja u $\mathbb{Z}_m$ 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 $2^r = \frac{|\text{Im}(\alpha)|\cdot|\text{Im}(\beta)|}{4}$, slijedi direktno da je $r \leq \omega(b) + \omega(b')$. No, iz jednadžbe (11) slijedi da ako je $a \leq 0$ i $b > 0$, onda b_1 mora biti pozitivan. Analogno, ako je $a' \leq 0$ 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 $a \leq 0$ ili $a' \leq 0$. Stoga se negativni djelitelji ne mogu pojaviti u barem jednom od skupova Im(α), Im(β). 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: 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

$$y^2 = (x - 1)(2x - 1)(5x - 1). \tag{12}$$

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 $\gcd(3e^2 - M^2, 5e^2 + M^2) \in \{1, 2\}$, 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 (12): $\mathcal{O}$, $(1,0)$, $(\frac{1}{2},0)$, $(\frac{1}{5},0)$. 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 $x=1$.

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). 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: 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 $a_1, \ldots, a_{2n}$ različiti racionalni brojevi. Tada na krivulji

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

leže točke $(a_i, \pm q(a_i))$, $i = 1, \ldots, 2n$. 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 $a_i = b_i + t$, $i = 1, \ldots, 6$; $a_i = b_{i-6} - t$, $i = 7, \ldots, 12$. Sada polinom $r(x)$ općenito ima stupanj 5. Zato možemo pokušati izabrati brojeve $b_1, \ldots, b_6$ tako da koeficijent uz x^5 bude jednak 0. U prvom Mestreovom primjeru iz 1991. godine bilo je $b_1 = -17$, $b_2 = -16$, $b_3 = 10$, $b_4 = 11$, $b_5 = 14$, $b_6 = 17$.

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 $r = \text{rank}(E)$.

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 mod$p$ koje maksimiziraju N_p. (Ako promatramo krivulju oblika $y^2 = x^3+ax+b$, parametri će 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

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

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

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

U primjenama ove ideje izabere se nekoliko prirodnih brojeva $X_1 < X_2 < \cdots < X_k$, te se računa $S_i(X_1)$, $S_i(X_2)$, ..., 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 $N_p = p + 1 - a_p$.

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`.

T	$B(T) \geq$	Autori
0	28	Elkies (06)
$\mathbb{Z}/2\mathbb{Z}$	19	Elkies (09)
$\mathbb{Z}/3\mathbb{Z}$	13	Eroshkin (07,08,09)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies (06)
$\mathbb{Z}/5\mathbb{Z}$	8	Dujella & Lecacheux (09), Eroshkin (09)
$\mathbb{Z}/6\mathbb{Z}$	8	Eroshkin (08), Dujella & Eroshkin (08), Elkies (08), Dujella (08)
$\mathbb{Z}/7\mathbb{Z}$	5	Dujella & Kulesz (01), Elkies (06), Eroshkin (09), Dujella & Lecacheux (09), Dujella & Eroshkin (09)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (06)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (09)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (05,08), Elkies (06)
$\mathbb{Z}/12\mathbb{Z}$	4	Fisher (08)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	15	Elkies (09)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	8	Elkies (05), Eroshkin (08), Dujella & Eroshkin (08)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (06)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (00), Dujella (00,01,06,08), Campbell & Goins (03), Rathbun (03,06), Flores, Jones, Rollick & Weigandt (07), Fisher (09)

Pretpostavimo da smo uspjeli izračunati rang r eliptičke krivulje E nekom od opisanih metoda. 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 $P = n_1 Q_1 + \cdots + n_r Q_r + T$, $n_i \in \mathbb{Z}$, $T \in E(\mathbb{Q})_{\text{tors}}$).

Pogledat ćemo samo 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 fundamentalnog pravokutnika) za koje je $z - \omega_2/2 \in \mathbb{R}$.

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

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

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

(iii) $\Delta > 0$;

(iv) neparna komponenta je neprazna.

Tada je 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: Nađimo slobodni generator krivulje

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

Ranije smo vidjeli 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 prethodne propozicije. 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 je P jedan slobodni generator od $E(\mathbb{Q})$ (ostali slobodni generatori su $-P$, $P + T$ i $-P + T$).

3. Eliptičke krivulje nad konačnim poljima

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 $\mathbb{F}_q^*$. Grupa $\mathbb{F}_q^*$ je ciklička.

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 ne-nul elementi invertibilni, dok u $\mathbb{Z}_{p^k}$ ima točno $\varphi(p^k) = p^k - p^{k-1}$ invertibilnih elemenata.

Možemo se 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. 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 $\gcd(g(t), t^{p^j} - t) = 1$ 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

$$x^8 + x^4 + x^3 + x + 1.$$

Polje $\mathbb{F}_{2^k}$ je 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.

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 $a = (a_0, a_1, \ldots, a_{k-1})$, onda je

$$a^2 = (a_{k-1}, a_0, a_1, \ldots, a_{k-2}).$$

Dakle, kvadriranje nije ništa drugo nego cikličkі 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). Element b generira ONB ako i samo ako za sve i_1, i_2, $0 \leq i_1 < i_2 \leq k-1$, 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.

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: 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:

$$[2]P = (6,6),\ [3]P = (5,0),\ [4]P = (6,1),$$

$$[5]P = (4,6),\ [6]P = \mathcal{O}.$$

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

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: (Hasse)

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

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

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: 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 $E(\mathbb{F}_q)$ cikličk a. Iz uvjeta da $n_1 | \gcd(n_2, q-1)$, zaključujemo da se može očekivati da će općenito n_1 biti mali prirodan broj, a grupa $E(\mathbb{F}_q)$ "skoro cikličk a".

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.

Računanje inverza može izbjeći korištenjem *Jacobijevih težinskih projektivnih koordinata* u kojima projektivnoj točki (X, Y, Z) odgovara afina točka $(\frac{X}{Z^2}, \frac{Y}{Z^3})$ (prvoj koordinati smo dali težinu 2, a drugoj 3). Tada jednadžba eliptičke krivulje (za $q = p$ gdje možemo koristiti kratku Weierstrassovu jednadžbu) postaje

$$Y^2 = X^3 + aXZ^4 + bZ^6. \qquad (13)$$

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 (13). Tada se koordinate točke $P + Q = (X_3, Y_3, Z_3)$ mogu izračunati pomoću:

$$r = X_1 Z_2^2, \quad s = X_2 Z_1^2, \quad t = Y_1 Z_2^3,$$
$$u = Y_2 Z_1^3, \quad v = s - r, \quad w = u - t,$$
$$X_3 = -v^3 - 2rv^2 + w^2,$$
$$Y_3 = -tv^3 + (rv^2 - X_3)w, \quad Z_3 = vZ_1 Z_2.$$

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

$$v = 4X_1 Y_1^2, \quad w = 3X_1^2 + aZ_1^4,$$
$$X_4 = -2v + w^2,$$
$$Y_4 = -8Y_1^4 + (v - X_3)w, \quad Z_4 = 2Y_1 Z_1.$$

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

$$y^2 + cy = x^3 + ax + b, \tag{14}$$
$$y^2 + xy = x^3 + ax^2 + b. \tag{15}$$

Krivulje oblika (14) su tzv. supersingularne krivulje i nisu od većeg interesa za primjene u kriptografiji, pa ćemo mi govoriti uglavnom o krivuljama oblika (15). Ovdje se nadalje može uzeti da je $a \in \{0, \gamma\}$, gdje je $\gamma \in \mathbb{F}_{2^k}$ sa svojstvom da je

$$\mathrm{Tr}(\gamma) = \gamma + \gamma^2 + \gamma^{2^2} + \cdots + \gamma^{2^{k-1}} = 1.$$

Posebno, ako je k neparan, onda možemo uzeti da je $a \in \{0, 1\}$. I u ovom slučaju mogu se koristiti Jacobijeve koordinate. Jednadžba (15) poprima oblik

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

U ovim koordinatama za računanje $P+Q$ treba 14 množenja, dok za $P + P$ treba 5 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 -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 $(s_d, \ldots, s_0)$ (uzimamo da je $n_i = 0$ za $i \geq d$).

Algoritam za NAF prikaz

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

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 $Q = Q - P$

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 $|E(\mathbb{F}_p)| = p+1$. 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: Zadana je krivulja

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

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

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

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

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

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

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

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

onda iz poznavanja $t \bmod l$ za $2 \leq l \leq l_{max}$, 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 $q_l = q \mod l$. Ako za $t' \in \{0, 1, \ldots, l-1\}$ vrijedi $\varphi^2(P) + [q_l]P = [t']\varphi(P)$, onda je $t \mod l = t'$.

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

$$|E(\mathbb{F}_{q^k})| = q^k + 1 - \alpha^k - \beta^k, \qquad (16)$$

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 (16) za računanje $|E(\mathbb{F}_{2^k})|$.

Primjer: *Koblitzove krivulje* su krivulje oblika

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

za $a = 0$ or 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

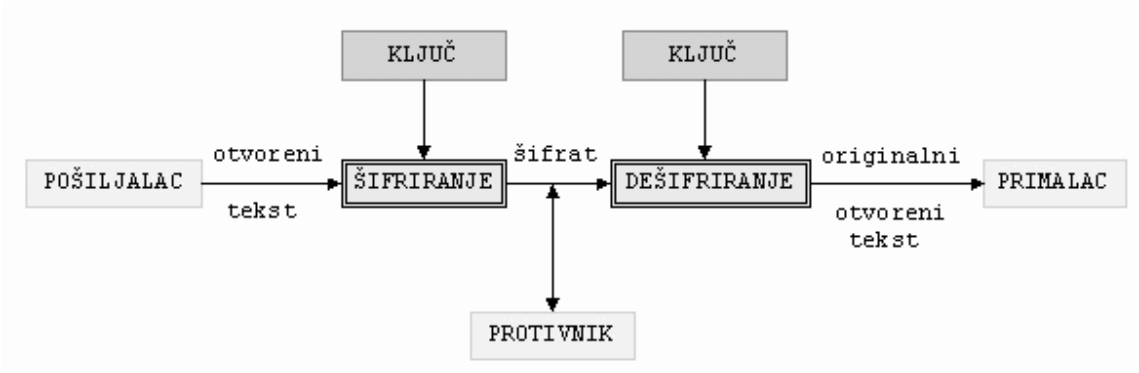
$$\#E(\mathbb{F}_{2^k}) = 2^k + 1 - \left(\frac{-\mu + \sqrt{-7}}{2}\right)^k - \left(\frac{-\mu - \sqrt{-7}}{2}\right)^k.$$

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).

4. Primjena eliptičkih krivulja u kriptografiji

Kako uspostaviti sigurnu komunikaciju preko nesigurnog komunikacijskog kanala? Metode za rješavanje ovog problema pročava znanstvena disciplina koja se zove *kriptografija*. 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 *Eva*), 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.



Ove pojmove ćemo formalizirati u sljedećoj definiciji.

Definicija: *Kriptosustav* je uređena petorka $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, gdje je $\mathcal{P}$ konačan skup svih otvoqrenih 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 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.

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 Evi) 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.

U konstrukciji kriptosustava s javnim ključem, tj. osobnih jednosmjernih funkcija, obično se koriste neki "teški" matematički problemi. Najpoznatiji kriptosustav s javnim ključem je RSA kriptosustav iz 1977. godine, nazvan po svojim tvorcima Rivestu, Shamiru i Adlemanu. Njegova sigurnost je zasnovana na teškoći faktorizacije velikih prirodnih brojeva.

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

$$e_K(x) = x^e \bmod n,\ d_K(y) = y^d \bmod n,\ x, y \in \mathbb{Z}_n.$$

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; $\varphi(n) = \varphi(pq) = (p-1)(q-1) = n - p - q + 1$.

Da bi RSA kriptosustav bio siguran, nužno je da broj $n = pq$ bude dovoljno velik tako da bi njegova faktozacija 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 $p-1$ 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 korisštenja 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: $L_n[\frac{1}{3}, (\frac{32}{9})^{1/3} + \varepsilon)]$.

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 (Eva), 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 $k \in \{0, 1, \ldots, p-1\}$ 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 $\mathbb{F}_p^*$ 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).

No, 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 $\mathbb{F}_p$. Za $k=30$ to je sasvim zadovoljavajuća vjerojatnost. Pretpostavimo sada da su nam osnovne jedinice otvorenog teksta cijeli brojevi između 0 i M, te neka 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 je li 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 $E(\mathbb{Z}_p)$. Obrnuto, iz točke (x,y) pripadni otvoreni tekst m možemo dobiti po formuli $m=\lfloor\frac{x-1}{k}\rfloor$.

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 eliptikoj 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 $x = (x_1, x_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ 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 $a y_0 = (c_1, c_2)$.

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 konačog 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 q 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 $v = r$.

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.

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.

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 $\frac{x}{\ln x}$. 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:

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 $\mathcal{B}$.

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.

Rješavanje sustava

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

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 $\mathbb{F}_p^*$.

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: 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

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

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

Poznato je nekoliko metoda za rješavanje ECDLP koje imaju složenost $O(\sqrt{n})$. Danas se najboljima smatraju *Pollardova ρ-metoda* i Shanksova "baby step - giant step" (BSGS) metoda, koju ćemo sada opisati.

Ova metoda je primjenjiva na problem diskretnog logaritma u proizvoljnoj Abelovoj grupi G. Njezina složenost je $O(\sqrt{n})$, 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 izraunamo 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: U prethodnom 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 $m_0 = 8a + b = 48$.

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.

Navest ćemo sada tipove eliptičkih krivulja koje treba izbjegavati:

1. 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 ili Shanksovom 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.

2. 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.

3. 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 $E(\mathbb{F}_q)$.

5. Primjena eliptički krivulja u dokazivanju prostosti i faktorizaciji

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: (Pocklington) Neka je s djelitelj od $n-1$ koji je veći od $\sqrt{n}$. Pretpostavimo da postoji prirodan broj a takav da vrijedi

$$a^{n-1} \equiv 1 \pmod{n},$$

$(a^{(n-1)/q}-1, n) = 1$ za svaki prosti djelitelj q od s.

Tada je n prost.

Dokaz: Pretpostavimo suprotno, tj. da je n složen. Tada on ima prosti faktor $p \leq \sqrt{n}$. 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: 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 $2^{n-1} \equiv 1 \pmod{n}$, $(2^{(n-1)/2} - 1, n) = 1$, $(2^{(n-1)/137} - 1, n) = 1$. 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 $(2^8 - 1, 137) = 1$ 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, kao što smo već više puta napomenuli, 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 $n-1$.

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: Neka je E eliptička krivulja nad $\mathbb{Z}_n$, gdje je $(6, n) = 1$ 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

$$[m]P = \mathcal{O} \quad \text{i} \quad [m/q]P \neq \mathcal{O},$$

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 $(m', q) = 1$, 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.

Primjer: 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 prije navedene algoritme za mP; 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).

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 intevalu 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.

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.

Pollardova $p-1$ *metoda* iz 1974. godine spada u specijalne metode faktorizacije. Njezino polazište je 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 $\gcd(a, p) = 1$. Štoviše, vrijedi $a^m \equiv 1 \pmod{p}$ za svaki višekratnik od $p-1$. Ako nađemo m, onda nam $\gcd(a^m - 1, n)$ 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 $1, 2, \ldots, B$. U najgorem slučaju, a to je kada je broj $\frac{p-1}{2}$ prost, ova metoda nije ništa bolja od običnog dijeljenja.

Primjer: 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 $\gcd(346904, n) = 421$. Zaista, $n = 421 \cdot 2011$.

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 $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$, 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 $\gcd(n,6)=1$, te ćemo promatrati eliptičke krivulje oblika

$$E_{a,b}: \quad y^2 = x^3 + ax + b,$$

gdje je $\gcd(4a^3+27b^2, n) = 1$. 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 $g = \gcd(4a^3 + 27b^2, n)$. 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 $g = \gcd(d, n)$. 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: 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 $[2]P = (163, 169)$. Zatim računamo $[3]P = P + [2]P$. Pripadni λ je $166 \cdot 163^{-1} = 60 \bmod 209$, 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 $\gcd(77, 209) = 11$. Odavde zaključujemo da je 11 faktor od 209. Zaista, $209 = 11 \cdot 19$.

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 $|E(\mathbb{Z}_p)|$, 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 $E(\mathbb{Z}_p)$ će vrijediti da je $[k]P = \mathcal{O}$.

Kod ocjene složenosti ovog algoritma ključno je pitanje kako optimalno odabrati granicu B. Pokazuje se da se minimum postiže za

$$B = e^{(\sqrt{2}/2+\varepsilon)\sqrt{\ln p \ln\ln p}},$$

dok je složenost algoritma

$$e^{(\sqrt{2}+\varepsilon)\sqrt{\ln p \ln\ln p}}.$$

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.).