Opće stvari:

Zbrajanje točaka na eliptičkoj krivulji:

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

Neka je $P = (x_1, x_2), Q = (y_1, y_2)$ onda je:

$$-\mathcal{O} = \mathcal{O}$$

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

$$\mathcal{O} + P = P$$

$$P + (-P) = \mathcal{O}$$

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

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = -y_1 + \lambda(x_1 - x_3)$$

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

Formula za računanje reda grupe $E(\mathbb{F}_p)$ gdje je $E : y^2 = x^3 + ax + b$:

$$|E(\mathbb{F}_p)| = p + 1 +$$

$$\sum_{x \in F_p} \left(\frac{x^3 + ax + b}{p} \right)$$

Legendreov simbol: $\left(\frac{x^3+ax+b}{p} \right)$ se računa prema:

Neka je p neparan prost broj, $\left(\frac{a}{p} \right)$ je jednak 1 ako je a kvadratni ostatak modulo p, -1 ako je a kvadratni neostatak modulo p, a 0 ako $p|a$.

Prema Eulerovom kriteriju vrijedi:

$$\left(\frac{a}{p} \right) \equiv a^{\frac{p-1}{2}} \pmod p$$

Ako kongruencija $x^2 \equiv a \pmod m$ ima rješenja, kažemo da je a **kvadratni ostatak** modulo m, u protivnom kažemo da je a kvadratni neostatak modulo m. Kažemo da je a **kvadratno slobodan** ako je 1 najveći kvadrat koji dijei a.

Prva DZ: 1) Neka je $E\ :\ y^2 = x^3 + ax + b$ eliptička krivulja kojoj trebamo odrediti sve proste brojeve u kojima ima lošu redukciju te njen minimalni model. Najprije izračunamo diskriminantu te rastavimo ju na proste faktore:

$$\begin{aligned} \Delta &= -16(4a^3 + 27b^2) && (1) \\ &= p_0^{\alpha_0} ... p_k^{\alpha_k} && (2) \end{aligned}$$

E ima dobru redukciju svugdje osim u $p_0, ..., p_k$, ta se redukcija da popraviti ako postoji $j \in \{0, .., k\}$ takvi da $12|\alpha_j$. Ukoliko ne postoji takav j loša redukcija se neće moći ukloniti, ipak ako postoji l td $\alpha_l \geq 12$ i $p_l \neq 2, 3$ možemo doći do minimalnog modela $E'\ :\ y'^2 = x'^3 + a'x' + b'$ uvodeći supstituciju: $x = p_l^2 x'$ i $y = p_l^3 y'$. **Za određivanje tipa redukcije** tražimo $x_1, x_2, x_3 \in \mathbb{F}_{p_l}$ takav da je

$$f(x) = x^3 + a'x + b' \equiv 0 (\bmod p_l)$$

U slučaju da se radi o trostukom korijenu radi se o aditivnoj redukciji, inače je redukcija multiplikativna i jedan je korijen dvostruki ($x_1 = x_2$ ili $x_2 = x_3$). Zapišemo $f_1(x) = (x - x_1)^2 (x - x_3)$ te $f_2(x) = (x - x_1)(x - x_3)^2$ i pogledamo koja se od f_1 ili f_2 poklapa $x \in \mathbb{F}_{p_l}$ sa f. Pretpostavimo da je to f_1, uvodi se supstitucija $x' = x'' + x_1$ i $y' = y''$ te uvrstimo to u minimalan model iz čega dobivamo novu eliptičku krivulju $E'' : y^2(x) = g(x)$, a za pripadnu funkciju $g(x)$ vrijedi: $g(x) = x^2(x - x_3 + x_1)$. Ako jednadžba $\alpha^2 = -x_3 + x_1$ ima rješenje u $\mathbb{F}_{p_l}$ tangente u singularnoj točki $(x_1, 0)$ imaju koeficijente smjera koji su riješenja jednadžbe $\alpha^2 = -x_3 + x_1$ pa govorimo o podijeljenoj multiplikativnoj redukciji u $p = p_l$, inače govorimo o nepodijeljenoj multiplikativnoj redukciji. **Dvije eliptičke krivulje su ekvivalnetne** nad algebarski zatvorenim poljem akko im se j-invarijante poklapaju. $\mathbb{Q}$ nije algebarski zatvoreno pa je potrebno vidjeti je li za supstituciju $(x, y) \rightarrow (u^2 x, u^3 y)$ $u \in \mathbb{Q}$.

Druga DZ: **Singularnost krivulje i supstitucije** $E'\ :\ y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$. Uvode se supstitucije: $b_2 = a_1^2 + 4a_2$, $b_4 = a_1 a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$, $b_8 = \frac{1}{4}(b_2 b_6 - b_4^2)$, $E'\ :\ y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$, zatim se dalje uvode supstitucije: $c_4 = b_2^2 - 24b_4$ i $c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6$ te se dobiva krivulja: $E\ :\ y^2 = x^3 - 27c_4 x - 54c_6$. Gledamo diskriminantu:

$$\Delta = \frac{c_4^3 - c_6^2}{1728}$$

Vrijedi: $\Delta = 0$ akko krivulja singularna.

$$\begin{aligned} f(x, y) = x^3 + a_2 x^2 + a_4 x + a_6 \\ -(y^2 + a_1 xy + a_3 y) \end{aligned}$$

Točka (x_0, y_0) je singularna akko $\partial_x f(x_0, y_0) = \partial_y f(x_0, y_0) = 0$. Provjeravamo je li (x_0, y_0) zadovoljava jdbu krivulje, ako da uvodimo supstituciju $t = \frac{y - y_0}{x - x_0}$, odnosno

$$y = t(x - x_0) + y_0 \qquad (3)$$

(nadajmo se da je $y_0 = 0$). Umjesto y u $f(x, y) = 0$ uvrstimo $t(x - x_0) + y_0$. Iz te jednadžbe dobijemo sređivanjem izraza (gdje je x^3 mi stavimo $((x - x_0) + x_0)^3$) $x - x_0 = g(t)$ i umjesto $x - x_0$ u 3 ubacimo $g(t)$ i dobijemo $y = tg(t) + y_0$. Pa je racionalna parametrizacija krivulje dana sa $\phi(t) = (g(t), tg(t) + y_0)$.

Određivanje reda i generatora grupe $E(\mathbb{F}_p)$ gdje je $E\ :\ y^2 = f(x)$. Pogledamo za koje $x_0 \in \mathbb{F}_p$ dana jdba ima rješenja i koja su to (za y možemo dobiti više riješenja jer riješavamo $y^2 \equiv \alpha\,(mod\, p)$) Označimo ih s $(x_1, y_1), (x_2, y_2), ..., (x_l, y_l)$ gdje se može dogoditi $x_i = x_j$, za $i \neq j$. Red grupe $|E(\mathbb{F}_p| = |\{(x_1, y_1), ..., (x_l, y_l), \mathcal{O}\}| = l + 1$. Uzmemo neku točku Q iz $E(\mathbb{F}_p)$, i pogledamo vrijedi li da je ta točka generator grupe, odnosno, vrijedi li da je $\forall P \in E(\mathbb{F}_p)$ postoji $l \in 1, ..., l$ takav da je

$$[l]Q = \underbrace{Q + Q + ... + Q}_{l} = P$$

Traženje torzijske grupe $E(\mathbb{Q})_{tors}$. Računamo $\Delta_0 = 4a^3 + 27b^2 = p_0^{\alpha_0} ... p_l^{\alpha_l}$. Sada za proste brojeve $q \notin \{p_0, ..., p_l\}$ promatramo $|E(\mathbb{F}_q|$ (obično se gleda do prvog prostog broja većeg od p_l. Neka su to $q_0, ..., q_k$. Promatramo

$$nzd(\{E(\mathbb{F}_q) : q \in \{q_0, ..., q_k\}\})$$

. Pretpostavi se da je to red grupe (to služi kao svojevrsna provjera). $y^2 | \Delta_0$ pa gledamo zapravo p_j takve da $\alpha_j \geq 2$. Promatramo polinome $f(x) = x^3 + ax + b - y_0^2$ gdje

$$y_0 \in \left\{ d : d | \prod_{\substack{j=0 \\ \alpha_j \geq 2}}^{l} p_j^{\alpha_j} \right\}$$

i gledamo postoje li njegove cjelobrojne nultočke. Neka je y_0 neki fiksan iz gornjeg skupa takav da je x_0 neka cjelobrojna nultočka polinoma $f(x)$. Tada je $P = (x_0, y_0)$ generator od $E(\mathbb{Q})_{tors}$, a red te grupe je $m \in \mathbb{N}$ takav da $[m]P = \mathcal{O}$, a $E(\mathbb{Q})_{tors} \cong \mathbb{Z}_m$ gdje je onda $m \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ ili $E(\mathbb{Q})_{tors} \cong \mathbb{Z}_2 \times \mathbb{Z}_{\frac{m}{2}}$ gdje je onda $m \in \{4, 8, 12, 16\}$.

Opći oblik jednadžbi krivulja sa torzijskim grupama:

$\mathbb{Z}_2 \times \mathbb{Z}_4$:

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

$$\alpha, \beta, \gamma \in \mathbb{Q}$$

$\mathbb{Z}_2 \times \mathbb{Z}_4$:

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

Za $\mathbb{Z}_2 \times \mathbb{Z}_8$:

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

gdje su $rs, r(r+s), s(r+s)$ kvadrati racionalnih brojeva.

$\mathbb{Z}_2 \times \mathbb{Z}_4$:

$$y^2 = (x+r^2)(x+s^2)\left(x + \frac{r^2s^2}{(r-s)^2}\right),$$

$$r, s \in \mathbb{Q}$$

Rang krivulje

$$E : y^2 = x^3 + ax^2 + bx$$

Uvjet nesingularnosti: $\Delta = 16b^2(a^2 - 4b) \neq 0$. Njoj pripadna 2-izogena krivulja ima jednadžbu:

$$\begin{aligned} E' : y^2 &= x^3 - 2ax^2 + (a^2-4b)x \\ &= x^3 + a'x^2 + b'x \end{aligned}$$

Za računanje ranga krivulje E promatramo odgovarajuća preslikavanja α i β te određujemo $|Im(\alpha)|$ i $|Im(\beta)|$. Za $|Im(\alpha)|$ tražimo (M, e, N) takve da jdba:

$$b_1M^4 + aM^2e^2 + b_2e^4 = N^2$$

ima riješenja gdje:

- b_1 djelitelj od b koji je kvadratno slobodan
- $b_1b_2 = b$
- $(M, e) = 1$

Pripadne jednadžbe uvijek promatramo u parovima jer je jednadžba simetrična. Dakle riješenja za (b_1, b_2) su simetrična riješenjima za (b_2, b_1) (onda riješenje (b_1, b_2) brojimo 2 puta, a ovo drugo uopće ne promatramo). Broj takvih (M, e, N) gdje pripadna jednadžba ima riješenja je $|Im(\alpha)|$. Analogan postupak je za b_1', b_2' gdje vrijede isti uvjeti, a broj rješenja pripadnih jednadžbi je $|Im(\beta)|$. U konačnici vrijedi da je

$$2^{rank(E) = \frac{|Im(\alpha)||Im(\beta)|}{4}}$$

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 $0 \le j \le m-1)$ then
        $t = im + j - \lfloor 2\sqrt{p} \rfloor$
return t

E(F_p)=p+1-t

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 $Q = Q + P$

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 $Q = Q - P$

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

Algoritam za NAF prikaz

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

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 eliptičkcj krivulji.

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

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

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

gdje je $y_0 = k\alpha$, $(c_1, c_2) = k\beta$, $y_1 = c_1x_1 \bmod p$, $y_2 = c_2x_2 \bmod p$.

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 $ay_0 = (c_1, c_2)$.

Pollardova $p-1$ *metoda* iz 1974. godine spada u specijalne metode faktorizacije. Njezino polazište je ponovno Mali Fermatov teorem. Neka je n složen broj koji želimo faktorizirati, te neka je p neki njegov prosti faktor. Tada je $a^{p-1} \equiv 1 \pmod{p}$ za nzd$(a,p) = 1$. Štoviše, vrijedi $a^m \equiv 1 \pmod{p}$ za svaki višekratnik m od $p-1$. Ako nađemo m, onda nam nzd$(a^m - 1, n)$ daje faktor (nadamo se netrivijalni) od n. No, pitanje je kako naći višekratnik od $p-1$ kad ne znamo p. To možemo efikasno napraviti u slučaju kada broj $p-1$ ima samo male proste faktore. Za prirodan broj kažemo da je *B-gladak* ako su mu svi prosti faktori $\le B$. Pretpostavimo dodatno da su sve potencije prostih brojeva, koje dijele $p-1$, manje ili jednake B. Tada za m možemo uzeti najmanji zajednički višekratnik brojeva $1, 2, \ldots, B$. Za ovako odabrani m, broj operacija za računanje $a^m \bmod n$ je $O(B \ln B \ln^2 n + \ln^3 n)$. U naj-