1.

$$f(X) = 15\,X^3 + 12\,X^2 + A2\cdot X + 00$$

$$g(X) = 15\,X^3 + 0F\cdot X^2 + 00\cdot X + 13$$

Označimo
$$f(X) = a_3 X^3 + a_2 X^2 + a_1 X + a_0$$
$$g(X) = b_3 X^3 + b_2 X^2 + b_1 X + b_0 .$$

Treba naći produkt $h = f \otimes g = d_3 X^3 + d_2 X^2 + d_1 X + d_0$.

Određujemo ga iz matrične jednadžbe:

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} .$$

$$\Rightarrow \begin{cases} d_0 = a_0 b_0 + a_3 b_1 + a_2 b_2 + a_1 b_3 \\ d_1 = a_1 b_0 + a_0 b_1 + a_3 b_2 + a_2 b_3 \\ d_2 = a_2 b_0 + a_1 b_1 + a_0 b_2 + a_3 b_3 \\ d_3 = a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3 \end{cases}$$

$$d_0 = \cancel{00\cdot 13} + \cancel{15\cdot 00} + 12\cdot 0F + A2\cdot 15 = 12\cdot 0F + A2\cdot 15$$

$$d_1 = A2\cdot 13 + \cancel{00\cdot 00} + 15\cdot 0F + 12\cdot 15 = A2\cdot 13 + 15\cdot 0F + 12\cdot 15$$

$$d_2 = 12\cdot 13 + \cancel{A2\cdot 00} + \cancel{00\cdot 0F} + 15\cdot 15 = 12\cdot 13 + 15\cdot 15$$

$$d_3 = 15\cdot 13 + \cancel{12\cdot 00} + A2\cdot 0F + \cancel{00\cdot 15} = 15\cdot 13 + A2\cdot 0F$$

Produkt računamo u $GF(2^8)$:

d_0

$$12\cdot 0F = \overset{7654}{0001}|\overset{3210}{0010} \cdot \overset{7654}{0000}|\overset{3210}{1111} =$$ ← potencije polinoma

$$= (x^4 + x)\cdot(x^3 + x^2 + x + 1) =$$

$$= x^7 + x^6 + x^5 + \cancel{x^4} + \cancel{x^4} + x^3 + x^2 + x =$$

$$= x^7 + x^6 + x^5 + x^3 + x^2 + x = 1110|1110$$

Ovdje ne „reduciramo" dobiveni polinom modulo $x^8 + x^4 + x^3 + x + 1$ jer je već nižeg stupnja od 8.

$A2 \cdot 15 = 1010|0010 \cdot 0001|0101 =$

$= (x^7+x^5+x)\cdot(x^4+x^2+1) =$

$= x^{11} + x^9 + \cancel{x^7} + \cancel{x^9} + \cancel{x^7} + \cancel{x^5} + \cancel{x^5} + x^3 + x =$

$= \underline{\underline{x^{11}}} + x^3 + x \quad (\mathrm{mod}\ x^8+x^4+x^3+x+1)$

Ovaj je moramo „reducirati" dobiveni polinom :

$(x^{11}+x^3+x) : (x^8+x^4+x^3+x+1) = x^3$

$x^{11}+x^7+x^6+x^4+x^3$ ← predznak nije promijenjen jer su koeficijenti u $\mathbb{Z}_2$ gdje je $-x = x$.

$x^7+x^6+x^4+x$

$x^7+x^6+x^4+x = 1101|0010 = D2$

$\Rightarrow A2 \cdot 15 = x^7+x^6+x^4+x$

$\Rightarrow d_0 = 1110\,1110 + 1101\,0010 = 0011|1100 = 39$

XOR:

11101110
$\oplus\ 11010010$

00111100

d1) $A2 \cdot 13 = 1010|0010 \cdot 0001|0011 =$

$= (x^7+x^5+x)\cdot(x^4+x+1) =$

$= x^{11} + x^8 + x^7 + x^9 + x^6 + \cancel{x^5} + \cancel{x^5} + x^2 + x =$

$= x^{11} + x^9 + x^8 + x^7 + x^6 + x^2 + x \quad (\mathrm{mod}\ x^8+x^4+x^3+x+1)$

$(x^{11}+x^9+x^8+\cancel{x^7}+\cancel{x^6}+x^2+x) : (x^8+x^4+x^3+x+1) = x^3+x+1$

$x^{11}+\cancel{x^7}+\cancel{x^6}+x^4+x^3$

$\cancel{x^9}+x^8+\cancel{x^4}+x^3+\cancel{x^2}+\cancel{x}$

$\cancel{x^9}+x^5+\cancel{x^4}+\cancel{x^2}+\cancel{x}$

$\cancel{x^8}+x^5+\cancel{x^3}$

$\cancel{x^8}+x^4+\cancel{x^3}+x+1$

$x^5+x^4+x+1 \quad \Rightarrow \quad A2 \cdot 13 = 0011|0011 = 33$

$15 \cdot 0F = 0001|0101 \cdot 0000|1111 =$

$= (x^4+x^2+1)\cdot(x^3+x^2+x+1) =$

$= x^7+x^6+\cancel{x^5}+\cancel{x^4}+\cancel{x^5}+\cancel{x^4}+\cancel{x^3}+\cancel{x^2}+\cancel{x^3}+\cancel{x^2}+x+1 =$

$= x^7+x^6+x+1 = 1100|0011 = C3$

$12 \cdot 15 = 0001|0010 \cdot 0001|0101 =$

$= (x^4+x)\cdot(x^4+x^2+1) =$

$= x^8+x^6+x^5+x^4+x^3+x \pmod{x^8+x^4+x^3+x+1}$

$(x^8+x^6+x^5+x^4+x^3+x) : (x^8+x^4+x^3+x+1) = 1$

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

$\overline{x^6+x^5+1} \quad \Rightarrow \quad 12\cdot 15 = 0110|0001$

$\Rightarrow d_1 = A2\cdot 13 + 15\cdot 0F + 12\cdot 15 = 91$

XOR:

0011 0011
11000011
⊕ 01100001
10010001

d_2 $\quad 12\cdot 13 = 0001|0010 \cdot 0001|0011 =$

$= (x^4+x)\cdot(x^4+x+1) =$

$= x^8+\cancel{x^5}+x^4+\cancel{x^5}+x^2+x \pmod{x^8+x^4+x^3+x+1}$

$(x^8+x^4+x^2+x) : (x^8+x^4+x^3+x+1) = 1$

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

$\overline{x^3+x^2+1} \quad \Rightarrow \quad 12\cdot 13 = 0000|1101$

$15\cdot 15 = 0001|0101 \cdot 0001|0101 =$

$= (x^4+x^2+1)\cdot(x^4+x^2+1) =$

$= x^8+\cancel{x^6}+\cancel{x^4}+\cancel{x^6}+\cancel{x^4}+\cancel{x^2}+x^4+\cancel{x^2}+1 =$

$= x^8+x^4+1 \pmod{x^8+x^4+x^3+x+1}$

$(x^8 + x^4 + 1) : (x^8 + x^4 + x^3 + x + 1) = 1$

$\cancel{x^8} + \cancel{x^4} + x^3 + x + \cancel{1}$

$x^3 + x \Rightarrow 15 \cdot 15 = 0000|1010$

XOR:
$$\begin{array}{r} 00001101 \\ \oplus\ 00001010 \\ \hline 0000|0111 \end{array} \Rightarrow d2 = 12 \cdot 13 + 15 \cdot 15 = 07$$

d3

$15 \cdot 13 = 0001|0101 \cdot 0001|0011 =$

$= (x^4 + x^2 + 1) \cdot (x^4 + x + 1) =$

$= x^8 + x^5 + \cancel{x^4} + x^6 + x^3 + x^2 + \cancel{x^4} + x + 1 =$

$= x^8 + x^6 + x^5 + x^3 + x^2 + x + 1 \pmod{x^8 + x^4 + x^3 + x + 1}$

$(x^8 + x^6 + x^5 + x^3 + x^2 + x + 1) : (x^8 + x^4 + x^3 + x + 1) = 1$

$\cancel{x^8} + x^4 + \cancel{x^3} + \cancel{x} + \cancel{1}$

$x^6 + x^5 + x^4 + x^2 \Rightarrow 15 \cdot 13 = 0111|0100$

$A2 \cdot 0F = 1010|0010 \cdot 0000|1111 =$

$= (x^7 + x^5 + x) \cdot (x^3 + x^2 + x + 1) = x^4 + x^3 + x^2 + x =$

$= x^{10} + x^9 + \cancel{x^8} + \cancel{x^7} + \cancel{x^8} + \cancel{x^7} + x^6 + x^5 + x^4 + x^3 + x^2 + x \pmod{x^8 + x^4 + x^3 + x + 1}$

$= x^{10} + x^9 + x^6 + x^5 + x^4 + x^3 + x^2 + x \; (x^{10} + x^9 + x^6 + x^5 + x^4 + x^3 + x^2 + x) : (x^8 + x^4 + x^3 + x + 1) = x^2 + x$

$\cancel{x^{10}} + x^6 + \cancel{x^5} + \cancel{x^3} + \cancel{x^2}$

$x^9 + x^4 + x$

$\cancel{x^9} + x^5 + \cancel{x^4} + x^2 + \cancel{x}$

$x^5 + x^2 \Rightarrow A2 \cdot 0F = 0010|0100$

XOR:
$$\begin{array}{r} 01110100 \\ \oplus\ 00100100 \\ \hline 01010000 \end{array} \Rightarrow d3 = 15 \cdot 13 + A2 \cdot 0F = 50$$

konačno, imamo:

$$f(x) \otimes g(x) = h(x) = d_3 x^3 + d_2 x^2 + d_1 x + d_0 =$$

$$= 50 x^3 + 07 x^2 + 91 x + 39$$

2.

Kako n_1 i n_3 nisu relativno prosti, faktorizirat ćemo sve n_i, $i=1,2,3$ i uzet ćemo relativno proste faktore.

Imamo:
$$706969 = 761 \cdot 929$$
$$222119 = 389 \cdot 571$$
$$200143 = 263 \cdot 761.$$

Za nove vrijednosti n_i uzimamo faktore iz svakog izraza:

$$\boxed{\begin{array}{ll} n_1 = 761 & c_1 = 634305 \\ n_2 = 389 & c_2 = 17418 \\ n_3 = 263 & c_3 = 153353 \end{array}}$$

Iz toga dobivamo sljedeći sustav kongruencija:

$$\begin{cases} c_1 \equiv m^3 \pmod{n_1} \\ c_2 \equiv m^3 \pmod{n_2} \\ c_3 \equiv m^3 \pmod{n_3} \end{cases}$$

$$634305 \equiv m^3 \pmod{761}$$
$$17418 \equiv m^3 \pmod{389}$$
$$153353 \equiv m^3 \pmod{263}$$

Sustav rješavamo pomoću kineskog teorema o ostacima.

$$x \equiv \underbrace{634305}_{A_1} \pmod{\underbrace{761}_{M_1}}$$

$$x \equiv \underbrace{17418}_{A_2} \pmod{\underbrace{389}_{M_2}}$$

$$x \equiv \underbrace{153353}_{A_3} \pmod{\underbrace{263}_{M_3}}$$

Definiramo brojeve $N_1 = M_2 \cdot M_3$

$N_2 = M_1 \cdot M_3$

$N_3 = M_1 \cdot M_2$

i zatim rješavamo kongruencije $N_j x \equiv A_j \pmod{M_j}$; $i = 1,2,3.$

$j=1$ $N_1 = M_2 \cdot M_3 = 389 \cdot 263 = 102307$

$$\underbrace{102307}_{N_1} x \equiv \underbrace{634305}_{A_1} \pmod{\underbrace{761}_{M_1}}$$

Pomoću Euklidovog algoritma određimo

$gcd(102307, 761)$:

1) $102307 = 761 \cdot 134 + 333$
2) $761 = 333 \cdot 2 + 95$
3) $333 = 95 \cdot 3 + 48$
4) $95 = 48 \cdot 1 + 47$
5) $48 = 47 \cdot 1 + 1$ $\Rightarrow gcd(102307, 761) = 1 = g$

$47 = 1 \cdot 47 + \underline{\underline{0}}$

Dalje koristimo rekurzivne relacije:
$$\begin{cases} x_i = x_{i-2} - q_i \cdot x_{i-1} \\ y_i = y_{i-2} - q_i \cdot y_{i-1} \end{cases}$$
$i = 1,2,3,4,5$

i	-1	0	1	2	3	4	5
q_i	/	/	134	2	3	1	1
x_i	1	0	1	-2	7	-9	16
y_i	0	1	-134	269	-941	1210	-2151

$g = x_5 \cdot 102307 + y_5 \cdot 761$

Jer su N_1 i M_1 relativno prosti, imamo da je

x_1 jedinstveno rješenje kongruencije:

$\underline{x_1} \equiv x_5 \cdot A_1 \equiv 16 \cdot 634305 \pmod{761} \equiv \underline{184 \pmod{761}}$

$j=2$

$$N_2 = M_1 \cdot M_3 = 761 \cdot 263 = 200143$$

$$\underbrace{200143}_{N_2} x \equiv \underbrace{17418}_{A_2} \pmod{\underbrace{389}_{M_2}}$$

Analognim postupkom kao za $j=1$ dobije se da je $\gcd(200143, 389) = 1$ pa kongruencija ima jedinstveno rješenje:

$$200143 \cdot \underbrace{156}_{u} + 389 \cdot (\underbrace{-80263}_{v}) = 1$$

$$\underline{x_2} \equiv u \cdot A_2 \equiv 156 \cdot 17418 \pmod{389} \equiv \underline{43 \pmod{389}}$$

$j=3$

$$N_3 = M_1 \cdot M_2 = 761 \cdot 389 = 296029$$

$$\underbrace{269029}_{N_3} \cdot x \equiv \underbrace{153353}_{A_3} \pmod{\underbrace{263}_{M_3}}.$$

Analognim postupkom: $\gcd(296029, 263) = 1$,

$$296029 \cdot (\underbrace{-111}_{u}) + 263 \cdot \underbrace{124940}_{v} = 1$$

$$\Rightarrow \quad \underline{x_3} \equiv u \cdot A_3 \equiv -111 \cdot 153353 \pmod{263} \equiv \underline{229 \pmod{263}}$$

Sada imamo jedinstveno rješenje sustava:

$$x_0 \equiv N_1 x_1 + N_2 x_2 + N_3 x_3 \pmod{M_1 M_2 M_3}$$

$$x_0 \equiv 102307 \cdot 184 + 200143 \cdot 43 + 296029 \cdot 229 \pmod{761 \cdot 389 \cdot 263}$$

$$\boxed{x_0 \equiv 17365651 \pmod{77855627}}$$

$$x_0 \equiv m^3 \pmod{77855627}$$

$\rightarrow$ m treba naći iz jednakosti: (odnosno tražimo $k \in \mathbb{N}_0$ za koji je m prirodan broj)

$$m = \sqrt[3]{x_0 + k \cdot 77855627} \in \mathbb{N}$$

* za $k = 0, 1, \dots, 20$ ne dobiva se $m \in \mathbb{N}$ pa zaključujemo da je $k > 20$ (pod pretpostavkom da je sustav dobro riješen...)

(3.) Prvo pokažimo da je 35 primitivni korijen modulo 571. To znači da je $k = \varphi(571) = 570$ najmanja potencija za koju vrijedi

$$35^k \equiv 1 \pmod{571}. \quad (\text{red od } 35 \pmod{571} \text{ je } 570)$$

Po Malom Fermatovom teoremu $(571 \nmid 35)$ slijedi

$$35^{571-1} \equiv 1 \pmod{571}.$$

Treba još pokazati da je to najmanji takav broj.

Pretpostavimo da je d red od $35 \pmod{571}$.

Tada $d \mid \underbrace{570}_{\varphi(571)} = 2 \cdot 3 \cdot 5 \cdot 19.$

Imamo da su mogućnosti za d:

$$d \in \{2, 3, 5, 19, 6, 10, 38, 15, 57, 95\}.$$

Tražena tvrdnja će slijediti ako se svaka od ovih opcija za d obori. To znači da treba pokazati $35^d \not\equiv 1 \pmod{571}$ za sve moguće d.

Kako postupak ide analogno za sve opcije, raspisat ćemo samo jednu za primjer. Npr. uzmimo $d = 95$.

$$\begin{aligned}
35^{95} &\equiv (35^5)^{19} \pmod{571} \equiv \\
&\equiv 153^{19} \pmod{571} \equiv \\
&\equiv 153 \cdot 153^{18} \pmod{571} \equiv \\
&\equiv 153 \cdot (153^3)^6 \pmod{571} \equiv \\
&\equiv 153 \cdot 265^6 \pmod{571} \equiv \\
&\equiv 153 \cdot (265^2)^3 \pmod{571} \equiv \\
&\equiv 153 \cdot 563^3 \pmod{571} \equiv \\
&\equiv 153 \cdot 59 \pmod{571} \equiv \\
&\equiv 9027 \pmod{571} \equiv 462 \pmod{571} \not\equiv 1 \pmod{571}
\end{aligned}$$

✓

Zaključujemo da d ne može biti netrivijalni djelitelj od $570 = \varphi(571)$ pa mora biti $d = 570$.

Ovime je pokazano da je 35 primitivni korijen u $\mathbb{Z}^*_{571}$. ■

$\mathbb{Z}^*_p = \mathbb{Z}^*_{571}$ – $p = 571$, $g = 35$, baza: $\{2,3,5,7,11,13\}$.

Treba ouračiti $\log_{35} 270 \pmod{\varphi(571)} \equiv$

$\equiv \log_{35} 2 \cdot 3^3 \cdot 5 \pmod{570} \equiv$

$\equiv \underbrace{\log_{35} 2}_{?} + 3 \underbrace{\log_{35} 3}_{?} + \underbrace{\log_{35} 5}_{?} \pmod{570}$.

Za to nam treba (najviše) 6 relacija oblika $g^k \pmod{571}$, $k \in \{0,1,\dots,570\}$ proizvoljni, takvi da se g^k može prikazati preko faktorske baze (kao produkt elemenata faktorske baze).

(6 relacija jer je 6 elemenata faktorske baze)

Posebno su važni k-ovi koji daju prikaz g^k u faktorskoj bazi preko elemenata 2,3,5 koji su nama bitni.

$\rightarrow k=3$ $\quad 35^3 \equiv 50 \pmod{571} \equiv 2 \cdot 5^2 \pmod{571}$

$\rightarrow k=6$ $\quad 35^6 \equiv 216 \pmod{571} \equiv 2^3 \cdot 3^3 \pmod{571}$

$\rightarrow k=20$ $\quad 35^{20} \equiv 4 \pmod{571} \equiv 2^2 \pmod{571}$

samo 2,3,5 !

Ti k-ovi su bili 3, 6, 20.

Uz oznaku $\log_{35} = \text{ind}_{35}$ slijedi

$$\begin{cases} 3 \equiv \log_{35} 2 + 2\log_{35} 5 \pmod{570} & (*) \\ 6 \equiv 3\log_{35} 2 + 3\log_{35} 5 \pmod{570} & (**) \\ 20 \equiv 2\log_{35} 2 \pmod{570}. & (***) \end{cases}$$

(***)

$\log_{35} 2$ računamo iz zadnje relacije tako da riješimo linearnu kongruenciju $\underbrace{2}_{a}x \equiv \underbrace{20}_{b} \pmod{\underbrace{570}_{n}}$.

Kako je $\underbrace{\gcd(a,n)}_{g} = \gcd(2,570) = 2$, $2 \mid 20$,

ova kongruencija ima 2 rješenja.

Kao u teoremu o rješenju linearne kongruencije

definiramo: $a' = \frac{a}{g} = 1$, $b' = \frac{b}{g} = 10$, $n' = \frac{n}{g} = 285$

pa riješimo: $a'x \equiv b' \pmod{n'}$.

$1 \cdot x \equiv 10 \pmod{285}$.

ova kongruencija ima jedinstveno rješenje:

$\gcd(1,285) = 1 \Rightarrow (\exists u, v \in \mathbb{Z})\ 1 \cdot u + 285 \cdot v = 1$

i $x_0 \equiv u \cdot b' \pmod{n'}$.

naše rješenje

Imamo $u = 286$, $v = -1$ pa je

$x_0 \equiv 286 \cdot 10 \pmod{285} \equiv 10 \pmod{285}$.

$\Rightarrow$ sva rješenja početne kongruencije su:

$x \equiv x_0 + k \cdot n' \pmod{n}$; $k = 0, \ldots, \gcd(a,n)-1$

$\underline{x} \equiv 10 + 0 \cdot 285,\ 10 + 1 \cdot 285 \pmod{570} \equiv$

$\underline{\equiv 10, 295 \pmod{570}}$

Sada znamo da je $\log_{35} 2 \in \{10, 295\}$.

Još treba provjeriti (po definiciji indeksa ind_{35}):

$35^{10} \equiv 569 \pmod{571} \not\equiv 2 \pmod{571}$ ✗

$35^{295} \equiv 2 \pmod{571}$ ✓

$\Rightarrow \boxed{\log_{35} 2 = 295}$

(kk)

Iz druge relacije sada imamo (za naći $\log_{35} 3$):

$$3\log_{35} 3 \equiv 6 - 3\cdot 295 \pmod{570} \equiv$$
$$\equiv -879 \pmod{570} \equiv$$
$$\equiv -879 + 2\cdot 570 \pmod{570} \equiv 261 \pmod{570}$$

pa rješavamo linearnu kongruenciju

$$3x \equiv 261 \pmod{570}.$$

Analogno prethodnom postupku dobije se rješenja:

$$x \equiv 87, 277, 467 \pmod{570}.$$

Jer je samo za 467 ispunjeno $35^{467} \equiv 3 \pmod{571}$

slijedi $\boxed{\underbrace{\log_{35} 3}_{= \operatorname{ind}_{35} 3} = 467}$.

Iz prve relacije (k) imamo da je:

$$2\log_{35} 5 \equiv 3 - \log_{35} 2 \pmod{570} \equiv$$
$$\equiv 3 - 295 \pmod{570} \equiv$$
$$\equiv 278 \pmod{570}$$

Rješavanjem linearne kongruencije dobijemo:

$$x \equiv 139, 424 \pmod{570}$$

i vidimo $35^{424} \equiv 5 \pmod{571}$

pa je $\boxed{\log_{35} 5 = 424}$.

Konačno, vidimo da je:

$$\log_{35} 270 \equiv \log_{35} 2 + 3\cdot \log_{35} 3 + \log_{35} 5 \pmod{570} \equiv$$
$$\equiv 295 + 3\cdot 467 + 424 \pmod{570} \equiv$$
$$\equiv 410 \pmod{570} \Rightarrow \boxed{\log_{35} 270 = 410}$$ //

4. $E(\mathbb{F}_{13})$ - $q=13$

$y^2 = x^3 + Ax + 1$ s barem 5 točaka

Prema Hasseovom teoremu:

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

$$|14-\#E(\mathbb{F}_{13})| \leq 2\sqrt{13}$$

$$\Rightarrow \underbrace{14-2\sqrt{13}}_{\approx 6,7} \leq \#E(\mathbb{F}_{13}) \leq \underbrace{14+2\sqrt{13}}_{\approx 21,2}$$

$$\Rightarrow 7 \leq \#E(\mathbb{F}_{13}) \leq 21.$$

$\rightarrow$ npr. za $A=3$ $\Rightarrow$ $D = -4\cdot 3^3 - 27\cdot 1^2 \equiv$

$\equiv -5\cdot 27 \pmod{13} \equiv$

$\equiv -135 \pmod{13} \equiv$

$\equiv 8 \pmod{13} \not\equiv 0 \pmod{13}$

je dobro definirana eliptička krivulja $E = E(\mathbb{F}_{13})$.

$A = 3 \Rightarrow E(\mathbb{F}_{13}) \ldots\ldots y^2 = x^3 + 3x + 1.$

Nađimo točke:

za dani $x \in \mathbb{F}_{13} = \{0, \ldots, 12\}$ treba naći sve

$y \in \mathbb{F}_{13}$ takve da je ispunjeno:

$$y^2 \equiv x^3 + 3x + 1 \pmod{13}.$$

$x=0$ $\quad y^2 \equiv 1 \pmod{13}$.

Izračunom Legendreovog simbola $\left(\frac{1}{13}\right)$ vidimo

da gornja kongruencija ima rješenja.

$$\left(\left(\frac{1}{13}\right) = \left(\frac{1^2}{13}\right) = 1 \right)$$

Provjerimo za koje $y \in \mathbb{F}_{13}$ je relacija zadovoljena.

Jedini taki y su $y = 1, 12$ pa su dobivene točke za slučaj $x=0$: $\boxed{(0,1), (0,12)}$

$x=2$ Za ovaj slučaj nema točaka na E.

$$y^2 \equiv 2^3 + 3 \cdot 2 + 1 \pmod{13} \equiv$$
$$\equiv 8+6+1 \pmod{13} \equiv 15 \pmod{13}$$

Nema rješenja u $\mathbb{F}_{13}$ jer je Legendreov simbol:

$$\left(\frac{15}{13}\right) = \left(\frac{3 \cdot 5}{13}\right) \equiv 3^{\frac{13-1}{2}} \cdot 5^{\frac{13-1}{2}} \pmod{13} \equiv 3^6 \cdot 5^6 \pmod{13} \equiv$$
$$\equiv 12 \pmod{13} \equiv -1 \pmod{13}.$$

Računajući ovako za sve ostale $x \in \mathbb{F}_{13}$ dobivamo sve točke krivulje:

$E = \{ (0,1), (0,12), (4,5), (4,8), (6,1), (6,12), (9,4), (9,9), (7,1), (7,12), (8,2), (8,11), (10,2), (10,11), (11,0), (12,6), (12,7) \}$

Odredimo cikličku podgrupu $\langle (7,12) \rangle$ grupe E.

Za to nam trebaju sve „potencije" elementa $(7,12)$ u E:

$$2 \cdot (7,12) = \underset{x_1\ y_1}{(7,12)} + \underset{x_2\ y_2}{(7,12)} = (x_3, y_3)$$

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = -y_1 + \lambda(x_1 - x_3)$$
$$x_2 = x_1 \Rightarrow \underline{\lambda} = \frac{3 \cdot x_1^2 + a}{2y_1} = (3x_1^2 + a) \cdot (2y_1)^{-1} =$$
$$= (3 \cdot_{13} 7^2 +_{13} 3) \cdot (2 \cdot_{13} 12)^{-1} =$$
$$= (3 \cdot 10 + 3) \cdot (11)^{-1} = (4+3) \cdot (11)^{-1} = 7 \cdot (11)^{-1} =$$
$$= 7 \cdot 6 = \underline{3}$$

$\ulcorner (11)^{-1}$ dobivamo iz $\quad 11 \cdot x \equiv 1 \pmod{13}$.

$x = 6$ jer je $\quad 66 - 1 = 65 = 13 \cdot 5 \equiv 0 \pmod{13} \lrcorner$

$\Rightarrow \quad x_3 = 3^2 - 7 - 7 = 9 + 6 + 6 = 8$

$y_3 = -12 + 3 \cdot (7 - 8) = 1 + 3 \cdot (7 + 5) = 1 + 3 \cdot 12 = 1 + 10 = 11$

$\Rightarrow \quad \underline{2 \cdot (7,12) = (8,11)}$

$\vdots$

Nastavljajući ovaj postupak nalazimo čitavu cikličku podgrupu generiranu s $(7,12)$:

$$\langle (7,12) \rangle = \{ (7,12), (8,11), (12,6), (10,2), (10,11), (12,17), (8,2), (7,1) \}.$$

Ove podatke ćemo sada iskoristiti na primjeru Menezes-Vanstoneovog kriptosustava.

$\alpha = (7,12)$ – generator cikličke podgrupe (određene gore).

Uzmimo $a = 6$.

Imamo: $\beta = [a] \alpha = 6 \cdot (7,12) = (12,17)$

Uzmimo $k = 8$, $x = (4,5)$.

$e_k(x,k) = e_k((4,5),8) = (y_0, y_1, y_2)$;

$y_0 = [k] \cdot \alpha = 8 \cdot (7,12) = (7,1)$

$(c_1, c_2) = [k] \cdot \beta = 8 \cdot (12,17) = (8,6)$

$$\langle (12,17) \rangle = \{ \overset{1}{(12,17)}, \overset{2}{(5,11)}, \overset{3}{(10,7)}, \overset{4}{(3,2)}, \overset{5}{(8,7)}, \overset{6}{(9,10)}, \overset{7}{(9,3)}, \underline{\overset{8}{(8,6)}}, (3,11), (10,6), (5,2), (12,9) \}$$

$y_1 \equiv c_1 x_1 \pmod p \equiv 8 \cdot 4 \pmod{13} \Rightarrow y_1 = 6$

$y_2 \equiv c_2 x_2 \pmod p \equiv 6 \cdot 5 \pmod{13} \Rightarrow y_2 = 4$

$e_k(x, k) = ((7,1), 6, 4) = y$

$d_k(y) = d_k(y_0, y_1, y_2) =$

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

$= (6 \cdot (8)^{-1} \pmod{13}),\ 4 \cdot (6)^{-1} \pmod{13})) =$

$= 6 \cdot 5 \pmod{13}),\ 4 \cdot 11 \pmod{13}) = \underline{(4, 5)} = x$

$(8)^{-1}$ in $\mathbb{Z}$: $8x \equiv 1 \pmod{13} \Rightarrow x = 5$

$(6)^{-1}$ in $\mathbb{Z}$: $6x \equiv 1 \pmod{13} \Rightarrow x = 11$

5. $\mathbb{Z}^*_{571}$. $- \; p = 571$

$\alpha = 35$

Uzimamo $a = 505$, $k = 444$, $x = 201$.

Treba odrediti $\beta \equiv \alpha^a \pmod{p}$:

$$\beta \equiv 35^{505} \pmod{571} \equiv$$

$$\equiv 35^{5 \cdot 101} \pmod{571} \equiv$$

$35^5 \equiv 153 \pmod{571}$,

$101 = 2^2 \cdot 5 \cdot 5$

$$\equiv (35^5)^{101} \pmod{571} \equiv$$

$$\equiv 153 \cdot 153^{2^2 \cdot 5 \cdot 5} \pmod{571} \equiv$$

$153^5 \equiv 41 \pmod{571}$

$$\equiv 153 \cdot (153^5)^{4 \cdot 5} \pmod{571} \equiv$$

$$\equiv 153 \cdot 41^{4 \cdot 5} \pmod{571} \equiv$$

$301 \equiv 41^5$

$$\equiv 153 \cdot (41^5)^4 \pmod{571} \equiv$$

$$\equiv 153 \cdot 301^4 \pmod{571} \equiv$$

$301^4 \equiv 513 \pmod{571}$

$$\equiv 153 \cdot 513 \pmod{571} \equiv$$

$$\equiv 78489 \pmod{571} \equiv 262 \pmod{571}$$

Sada treba odrediti $\alpha^k \pmod{p}$ i $x\beta^k \pmod{p}$:

$$\alpha^k \pmod{p} \equiv 35^{444} \pmod{571} \equiv$$

$$\equiv 35^{4 \cdot 111} \pmod{571} \equiv$$

$35^4 \equiv 37 \pmod{571}$

$$\equiv (35^4)^{111} \pmod{571} \equiv$$

$$\equiv 37^{111} \pmod{571} \equiv$$

$$\equiv 37 \cdot 37^{110} \pmod{571} \equiv$$

$$\equiv 37 \cdot 37^{2 \cdot 5 \cdot 11} \pmod{571} \equiv \ldots \equiv$$

$$\equiv 20 \pmod{571}$$

$\underline{x\beta^k \pmod p} \equiv 201 \cdot 262^{444} \pmod{571} \equiv$ (analogno)

$\equiv \underline{65 \pmod{571}}$

$\Rightarrow \underline{e_k(x,k)} = e_k(201, 444) = \underline{(20, 65)} \in \mathbb{Z}_{571}^* \times \mathbb{Z}_{571}^*$

Još treba izračunati $d_k(20, 65)$.

Imamo formulu: $d_k(y_1, y_2) = y_2 \cdot (y_1^a)^{-1} \pmod p$.

$d_k(y_1, y_2) = d_k(20, 65) \equiv$

$\equiv 65 \cdot \underbrace{(20^{505})^{-1}} \pmod{571} \equiv$

$20^{505} \equiv 131 \pmod{571}$ (analogno postupku s početka zadatka)

$\equiv 65 \cdot 131^{-1} \pmod{571} \equiv$

$\equiv 65 \cdot 170 \pmod{571} \equiv 201 \pmod{571}$

$\underbrace{(131)^{-1}}$ Rješavamo $\underbrace{131}_{a} \cdot x \equiv \underbrace{1}_{b} \pmod{\underbrace{571}_{n}}$ — $\underbrace{571}$ prost broj

$131 < 571 \Rightarrow \gcd(131, 571) = 1$

Euklidovim algoritmom uz rekurzivne relacije

dobije se:

$1 = \gcd(131, 571) = 131 \cdot \underbrace{170}_{u} + 571 \cdot \underbrace{(-39)}_{v}$

$x_0 \equiv u \cdot b \equiv 170 \cdot 1 \equiv 170 \pmod{571}$

Dakle, $131^{-1} = 170$ u grupi $\mathbb{Z}_{571}^*$.