НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

ДКР
Варіант №3

Роботу виконав:
Юрчук Олексій, ФІ-52мн

6 грудня 2025 р.
м. Київ

Завдання № 1

Умова:

1. Перевірити, що набір публічних параметрів $(N, p, q, d) = (7, 3, 41, 2)$ криптосистеми NTRUCrypt є коректним;
2. Використовуючи публічний ключ:

$$pk = 18x^6 + 6x^5 - 11x^4 + 3x^3 - 15x^2 - 2x - 2 = h(x)$$

зашифрувати повідомлення $m = -x^5 - x^4 - x^2 - x + 1$.

Розв'язання:

Спершу перевіримо, що набір параметрів є коректним. Це робиться дуже просто. Треба усього лиш перевірити, що виконується наступна рівність: $q > (6d + 1)p$.
У нас задано:

- $N = 7$;
- $p = 3$;
- $q = 41$;
- $d = 2$.

Маємо: $41 > (6 \cdot 2 + 1) \cdot 3 = 39$. Справді, $41 > 39$, то ж система NTRUCrypt є коректною.

Далі займемося зашифруванням повідомлення. Для цього нам необхідно спершу обчислити центральне підняття m. В нашому випадку саме повідомлення $m = -x^5 - x^4 - x^2 - x + 1$ і буде центральним підняттям, оскільки коефіцієнти вже лежать у напівінтервалі $(-41/2, 41/2]$, тобто в проміжку $(-20, 20]$.

Наступним нашим кроком є обрання випадкового многочлена $\mathbf{r}$ з множини тернарних многочленів $\mathcal{T}(d, d)$. В нас це $\mathcal{T}(2, 2)$ – де перша двійка вказує на кількість коефіцієнтів 1, а друга відповідно коефіцієнтів -1.

Нехай це буде многочлен $\mathbf{r} = x^6 - x^5 + x - 1$. Щоб отримати шифротекст $\mathbf{e}(x)$ необхідно обчислити:

$$\mathbf{e}(x) = p \cdot \mathbf{r}(x) \star \mathbf{h}(x) + \mathbf{m}(x)$$

Зробимо покроково. Спершу обчислимо добуток a.k.a. згортковий многочлен:

$$\mathbf{r}(x) \star \mathbf{h}(x) = (x^6 - x^5 + x - 1) \star (18x^6 + 6x^5 - 11x^4 + 3x^3 - 15x^2 - 2x - 2)$$

Для цього необхідно обчислити результуючі коефіцієнти. Скористаємось формулою:

$$c_k = \sum_{i+j \equiv k \pmod N} a_i \cdot b_j, \quad 0 \le k \le N-1$$

Для нашої задачі $N = 7$, тому формула матиме вигляд:

$$c_k = \sum_{i+j \equiv k \pmod 7} a_i \cdot b_j, \quad 0 \le k \le 6$$

Обчислимо коефіцієнти $c_0, \dots, c_6$, маючи

$$a_0 = -1,\ a_1 = 1,\ a_2 = 0,\ a_3 = 0,\ a_4 = 0,\ a_5 = -1,\ a_6 = 1$$
$$b_0 = -2,\ b_1 = -2,\ b_2 = -15,\ b_3 = 3,\ b_4 = -11,\ b_5 = 6,\ b_6 = 18$$

$$c_0 = \sum_{i+j \equiv 0 \pmod 7} a_i \cdot b_j = a_0 \cdot b_0 + a_1 \cdot b_6 + a_2 \cdot b_5 + a_3 \cdot b_4 + a_4 \cdot b_3 + a_5 \cdot b_2 + a_6 \cdot b_1 =$$
$$= a_0 \cdot b_0 + a_1 \cdot b_6 + a_5 \cdot b_2 + a_6 \cdot b_1 = (-1) \cdot (-2) + 1 \cdot 18 + (-1) \cdot (-15) + 1 \cdot (-2) =$$
$$= 33 \pmod{41}$$
$$c_1 = \sum_{i+j \equiv 1 \pmod 7} a_i \cdot b_j = a_0 \cdot b_1 + a_1 \cdot b_0 + a_2 \cdot b_6 + a_3 \cdot b_5 + a_4 \cdot b_4 + a_5 \cdot b_3 + a_6 \cdot b_2 =$$
$$= a_0 \cdot b_1 + a_1 \cdot b_0 + a_5 \cdot b_3 + a_6 \cdot b_2 = (-1) \cdot (-2) + 1 \cdot (-2) + (-1) \cdot 3 + 1 \cdot (-15) = -18 =$$
$$= 23 \pmod{41}$$
$$c_2 = \sum_{i+j \equiv 2 \pmod 7} a_i \cdot b_j = a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0 + a_3 \cdot b_6 + a_4 \cdot b_5 + a_5 \cdot b_4 + a_6 \cdot b_3 =$$
$$= a_0 \cdot b_2 + a_1 \cdot b_1 + a_5 \cdot b_4 + a_6 \cdot b_3 = (-1) \cdot (-15) + 1 \cdot (-2) + (-1) \cdot (-11) + 1 \cdot 3 =$$
$$= 27 \pmod{41}$$
$$c_3 = \sum_{i+j \equiv 3 \pmod 7} a_i \cdot b_j = a_0 \cdot b_3 + a_1 \cdot b_2 + a_2 \cdot b_1 + a_3 \cdot b_0 + a_4 \cdot b_6 + a_5 \cdot b_5 + a_6 \cdot b_4 =$$
$$= a_0 \cdot b_3 + a_1 \cdot b_2 + a_5 \cdot b_5 + a_6 \cdot b_4 = (-1) \cdot 3 + 1 \cdot (-15) + (-1) \cdot 6 + 1 \cdot (-11) = -35 =$$
$$= 6 \pmod{41}$$
$$c_4 = \sum_{i+j \equiv 4 \pmod 7} a_i \cdot b_j = a_0 \cdot b_4 + a_1 \cdot b_3 + a_2 \cdot b_2 + a_3 \cdot b_1 + a_4 \cdot b_0 + a_5 \cdot b_6 + a_6 \cdot b_5 =$$
$$= a_0 \cdot b_4 + a_1 \cdot b_3 + a_5 \cdot b_6 + a_6 \cdot b_5 = (-1) \cdot (-11) + 1 \cdot 3 + (-1) \cdot 18 + 1 \cdot 6 =$$
$$= 2 \pmod{41}$$
$$c_5 = \sum_{i+j \equiv 5 \pmod 7} a_i \cdot b_j = a_0 \cdot b_5 + a_1 \cdot b_4 + a_2 \cdot b_3 + a_3 \cdot b_2 + a_4 \cdot b_1 + a_5 \cdot b_0 + a_6 \cdot b_6 =$$
$$= a_0 \cdot b_5 + a_1 \cdot b_4 + a_5 \cdot b_0 + a_6 \cdot b_6 = (-1) \cdot 6 + 1 \cdot (-11) + (-1) \cdot (-2) + 1 \cdot 18 =$$
$$= 3 \pmod{41}$$
$$c_6 = \sum_{i+j \equiv 6 \pmod 7} a_i \cdot b_j = a_0 \cdot b_6 + a_1 \cdot b_5 + a_2 \cdot b_4 + a_3 \cdot b_3 + a_4 \cdot b_2 + a_5 \cdot b_1 + a_6 \cdot b_0 =$$
$$= a_0 \cdot b_6 + a_1 \cdot b_5 + a_5 \cdot b_1 + a_6 \cdot b_0 = (-1) \cdot 18 + 1 \cdot 6 + (-1) \cdot (-2) + 1 \cdot (-2) = -12 =$$
$$= 29 \pmod{41}$$

Отже маємо:

$$c(x) = \mathbf{r}(x) \star \mathbf{h}(x) = 29x^6 + 3x^5 + 2x^4 + 6x^3 + 27x^2 + 23x + 33$$

Далі помножимо на p:

$$p \cdot c(x) = 3 \cdot (29x^6 + 3x^5 + 2x^4 + 6x^3 + 27x^2 + 23x + 33) =$$
$$= 5x^6 + 9x^5 + 6x^4 + 18x^3 + 40x^2 + 28x + 17 \pmod{41}$$

Далі додамо $\mathbf{m}(x)$ і отримаємо зашифроване повідомлення:

$$p \cdot c(x) + \mathbf{m}(x) = 5x^6 + 9x^5 + 6x^4 + 18x^3 + 40x^2 + 28x + 17 - x^5 - x^4 - x^2 - x + 1 =$$
$$= 5x^6 + 8x^5 + 5x^4 + 18x^3 + 39x^2 + 27x + 18 \pmod{41}$$

Отриманий криптотекст має вигляд:

$$\mathbf{e}(x) = p \cdot \mathbf{r}(x) \star \mathbf{h}(x) + \mathbf{m}(x) = 5x^6 + 8x^5 + 5x^4 + 18x^3 + 39x^2 + 27x + 18$$

Завдання № 2

Умова:

Еліптична крива E над полем $\mathbb{F}_{631}$ задана рівнянням:

$$y^2 = x^3 + 30x + 34$$

1. Перевірити, що точки $P = (36, 571)$ та $Q = (420, 48)$ належать ЕК;
2. Перевірити, що обидві точки мають порядок 5 і породжують підгрупу точок експоненти 5
3. Обчислити значення спарювання Вейля $w_5(P, Q)$ та перевірити, що отримане значення є коренем 5 степеня з 1.

Розв'язання:

Перевірку, чи точки справді лежать на кривій ми можемо звичайною підстановкою у рівняння ЕК.
Для точки P:

$$\begin{aligned} &P(36, 571) \leftarrow y^2 = x^3 + 30x + 34 \\ &571^2 = 36^3 + 30 \cdot 36 + 34 \pmod{631} \\ &445 = 445 \pmod{631} \end{aligned}$$

та точки Q:

$$\begin{aligned} &Q(420, 48) \leftarrow y^2 = x^3 + 30x + 34 \\ &48^2 = 420^3 + 30 \cdot 420 + 34 \pmod{631} \\ &441 = 441 \pmod{631} \end{aligned}$$

Як бачимо, точки належать еліптичній кривій. Для перевірки порядку 5 цих точок, треба обчислити точки $2P$, $3P$, $4P$, $5P$ та $2Q$, $3Q$, $4Q$, $5Q$ відповідно і переконатися що $5P = 5Q = \mathcal{O}$. Для зручності обчислень покладемо точку на нескінченності рівною $(0, 0)$: $\mathcal{O} = (0, 0)$. Це нам ніщо не забороняє зробити, оскільки $(0, 0)$ не належить заданій ЕК.

Суму точок обчислюємо за формулою:

$$\begin{cases} x_{P+Q} = \left(\dfrac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_3 \\ y_{P+Q} = \left(\dfrac{y_1 - y_2}{x_1 - x_2}\right) \cdot (x_1 - x_3) - y_1 \end{cases}$$

Подвоєння точки:

$$\begin{cases} x_{2P} = \left(\dfrac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ y_{2P} = \left(\dfrac{3x_1^2 + a}{2y_1}\right) \cdot (x_1 - x_3) - y_1 \end{cases}$$

Мінус точка:

$$x_{-P} = x_P \quad y_{-P} = -y_P$$

Маємо:

$P(36, 571)$	$Q(420, 48)$
$2P(617, 5)$	$2Q(121, 387)$
$3P(617, 626)$	$3Q(121, 244)$
$4P(36, 60)$	$4Q(420, 583)$
$5P(0, 0)$	$5Q(0, 0)$

Чи породжують P і Q підгрупу експоненти порядку 5? Для цього візьмемо якусь умовну точку $S = \alpha P + \beta Q$ з цієї підгрупи, де $\alpha, \beta \in \mathbb{N}[0, 5)$. Знайдемо всі точки:

$P(36, 571), 2P(617, 5), 3P(617, 626), 4P(36, 60)$
$Q(420, 48), 2Q(121, 387), 3Q(121, 244), 4Q(420, 583)$
$5P = 5Q = \mathcal{O} = (0, 0)$ – точка на нескінченності
$P + Q = (36, 571) + (420, 48) = (575, 7)$
$P + 2Q = (36, 571) + (121, 387) = (531, 18)$
$P + 3Q = (36, 571) + (121, 244) = (595, 221)$
$P + 4Q = (36, 571) + (420, 583) = (289, 269)$
$2P + Q = (617, 5) + (420, 48) = (586, 584)$
$2P + 2Q = (617, 5) + (121, 387) = (428, 25)$
$2P + 3Q = (617, 5) + (121, 244) = (511, 608)$
$2P + 4Q = (617, 5) + (420, 583) = (339, 499)$
$3P + Q = (617, 626) + (420, 48) = (339, 132)$
$3P + 2Q = (617, 626) + (121, 387) = (511, 23)$
$3P + 3Q = (617, 626) + (121, 244) = (428, 606)$
$3P + 4Q = (617, 626) + (420, 583) = (586, 47)$
$4P + Q = (36, 60) + (420, 48) = (289, 362)$
$4P + 2Q = (36, 60) + (121, 387) = (595, 410)$
$4P + 3Q = (36, 60) + (121, 244) = (531, 613)$
$4P + 4Q = (36, 60) + (420, 583) = (575, 624)$

Усього можливих точок підгрупи експоненти 5 – 25 штук.
5, це мається на увазі, що кожен елемент з цієї множини матиме порядок кратний 5. Перевірити це легко, можна взяти точку $5S$ і переконатися чи вона рівна $\mathcal{O}$.

$$5S = 5 \cdot (\alpha P + \beta Q) = 5 \cdot \alpha P + 5 \cdot \beta Q = \left\{ \begin{matrix} \alpha, \beta, 5 \\ \text{звичайні числа} \end{matrix} \right\} = \alpha \cdot (5P) + \beta \cdot (5Q) = \alpha \cdot \mathcal{O} + \beta \cdot \mathcal{O} = \mathcal{O}.$$

Бачимо, що кожен елемент у підгрупі зануляється при множенні на 5, тобто ці точки породжують підгрупу точок експоненти 5.

Значення спарювання Вейля $w_5(P,Q)$ обчислюємо формулою:

$$w_5(P,Q) = \frac{f_{5,P}(Q+R)/f_{5,P}(R)}{f_{5,Q}(P-R)/f_{5,Q}(-R)}$$

Для цього зафіксуємо точку $R = (0, 36)$, що не лежить в підгрупі (з попереднього списку явно видно, що вона не знаходиться), і використавши алгоритм Міллера знайдемо ці чотири невідомі значення:

$$f_{5,P}(Q+R), \quad f_{5,P}(R), \quad f_{5,Q}(P-R), \quad f_{5,Q}(-R)$$

Algorithm 1 Алгоритм Міллера

Require: $n \in \mathbb{N}$, $P \in E$, D — дівізор, для якого $\text{supp}(D) \cap \{P, 0\} = \emptyset$.
Ensure: $f_{n,P}(D)$.

1: Знаходимо бінарний розклад числа n:

$$n = \sum_{j=0}^{L} n_j \cdot 2^j, \quad n_j \in \{0,1\}, \quad n_L = 1$$

2: **Ініціалізація:**
$T = P$
$f = 1$
3: **for** $(j = L-1; j \geq 0; j--)$ **do**
4: $f = f^2 \cdot \frac{I_{T,T}(D)}{v_{[2]T}(D)}$
5: $T = [2]T$
6: **if** $n_j = 1$ **then**
7: $f = f \cdot \frac{I_{T,P}(D)}{v_{T+P}(D)}$
8: $T = T + P$
9: **end if**
10: **end for**
11: **return** f

- $I_{P,P}$ – пряма, яка є дотичною до ЕК в точці P.
- $I_{P,Q}$ – пряма, що проходить через точки P, Q, $P \neq Q$.
- v_P – вертикальна пряма через точку P

Спершу зрозуміємо, як обраховувати кожну з прямих:

1. $I_{P,P}(D)$
   Рівняння дотичної до ЕК має вигляд: $y - y_P = \lambda \cdot (x - x_P)$ Це схоже на формулу для y-координати $2P$, але є один нюанс: точка $2P$, на еліптичній кривій – це відбиття точки перетину дотичної з кривою відносно вісі X, тобто $(x_{2P}, -y_{2P}) \to (x_{2P}, y_{2P})$. Якщо підставити точку $2P$ в це рівняння, то можна отримати відому формулу для y_{2P}:
   $$-y_{2P} - y_P = \lambda \cdot (x_{2P} - x_P) \Rightarrow y_{2P} = \lambda \cdot (x_P - x_{2P}) - y_P,$$
   де $\lambda = \frac{3x_P^2 + a}{2y_P}$.
   Повертаючись до того, з чого починали, замінимо P на T, перенесемо все в одну сторону і перегруповуємо: $y - y_T - \lambda x + \lambda x_T = y - \lambda x + (\lambda x_T - y_T)$
   Остаточно маємо:
   $$I_{T,T}(D) = y - y_T - \lambda x + \lambda x_T = y_D - \lambda x_D + (\lambda x_T - y_T)$$

2. $I_{P,Q}(D)$
   Тут аналогічна ситуація. Рівняння січної до ЕК має вигляд $y - y_P = \lambda \cdot (x - x_P)$ Це схоже на формулу для y-координати $P + Q$, але такий самий нюанс: точка перетину вже січною еліптичної кривої має відбитися відносно вісі X, тобто $(x_{P+Q}, -y_{P+Q}) \to (x_{P+Q}, y_{P+Q})$ – будуть справжніми координатами $P + Q$. В цьому можна переконатися, якщо підставити точку $P + Q$ в це рівняння, то можна отримати вже формулу для y_{P+Q}:
   $$-y_{P+Q} - y_P = \lambda \cdot (x_{P+Q} - x_P) \Rightarrow y_{P+Q} = \lambda \cdot (x_P - x_{P+Q}) - y_P,$$
   де $\lambda = \frac{y_P - y_Q}{x_P - y_Q}$.
   Повернемось до рівняння січної. Перенесемо все в одну сторону і перегрупуємо: $y - y_{T+P} - \lambda x + \lambda x_{T+P} = 0 \Rightarrow y - \lambda x + (\lambda x_{T+P} - y_{T+P})$
   Остаточно маємо:
   $$I_{T,P}(D) = y_D - \lambda x_D + (\lambda x_{T+P} - y_{T+P})$$

3. $v_P(D)$ Рівняння вертикальної прямої це: $x - x_P = 0$. У нас в алгоритмі є два випадки $v_{2T}(D)$ і $v_{T+P}(D)$:
   - Якщо $v_{2T}(D)$, то відповідно пряма $x - x_{2T} = 0$, $x_{2T} = \underbrace{\left(\frac{3x_T^2 + a}{2y_T}\right)^2}_{\lambda^2} - 2x_T = \lambda^2 - 2x_T$, підставляючи одне в інше, маємо: $v_{2T}(D) = x_D - (\lambda^2 - 2x_T)$
   - Якщо $v_{T+P}(D)$, то пряма має вигляд: $x - x_{T+P} = 0$, $x_{T+P} = \underbrace{\left(\frac{y_T - y_P}{x_T - x_P}\right)^2}_{\lambda^2} - x_T - x_P = \lambda^2 - x_T - x_P$. підставляючи одне в інше, маємо: $v_{T+P}(D) = x_D - (\lambda^2 - x_T - x_P)$

У нас $n = 5_{10} = 101_2 \Rightarrow L = 2$ (індекс старшого біту), тобто $L-1 = 1$. Алгоритм матиме 2 кроки, оскільки ініціалізацією $T = P$ ми враховуємо старший біт $n_L = 1$.

Ітерація №1

$$I_{T,T}(D) = y_D - \lambda x_D + (\lambda x_T - y_T) \pmod{631}, \quad \lambda = \frac{3x_T^2 + a}{2y_T}$$

$$v_{2T}(D) = x_D - (\lambda^2 - 2x_T) \pmod{631}, \quad \lambda = \frac{3x_T^2 + a}{2y_T}$$

$$f = f^2 \cdot \frac{I_{T,T}(D)}{V_{[2]T}(D)} \pmod{631}$$

$$T = [2]T, \quad n_1 = 0, \text{ тому continue}$$

Ітерація №2

$$I_{T,T}(D) = y_D - \lambda x_D + (\lambda x_T - y_T) \pmod{631}, \quad \lambda = \frac{3x_T^2 + a}{2y_T}$$

$$v_{2T}(D) = x_D - (\lambda^2 - 2x_T) \pmod{631}, \quad \lambda = \frac{3x_T^2 + a}{2y_T}$$

$$f = f^2 \cdot \frac{I_{T,T}(D)}{V_{[2]T}(D)} \pmod{631}$$

$$T = [2]T, \quad n_0 = 1, \text{ тому :}$$

$$I_{T,P}(D) = y_D - \lambda x_D + (\lambda x_{T+P} - y_{T+P}) \pmod{631}, \quad \lambda = \frac{y_T - y_P}{x_T - y_P}$$

$$v_{T+P}(D) = x_D - (\lambda^2 - x_T - x_P) \pmod{631}, \quad \lambda = \frac{y_T - y_P}{x_T - x_P}$$

$$f = f \cdot \frac{I_{T,P}(D)}{v_{T+P}(D)} \pmod{631}$$

$$T = T + P$$

Return: $f_{5,P}(D)$

Обчислимо $f_{5,P}(Q+R)$

Вхідні дані:

Вхідні дані: $Q(420,48)$, $R(0,36)$, $D=Q+R=(535,129)$, $a=30$, $\mathrm{mod}=631$;

Ініціалізація: $T=P=(36,571)$, $f=1$

Ітерація №1. $j=1$, $n_1=0$

$$\lambda=\frac{3\cdot 36^2+30}{2\cdot 571}=\frac{3918}{1142}=132\cdot 511^{-1}=62 \pmod{631}$$

$$I_{T,T}(Q+R)=129-62\cdot 535+(62\cdot 36-571)=170 \pmod{631}$$

$$V_{[2]T}(Q+R)=535-(62^2-2\cdot 36)=549 \pmod{631}$$

$$f=1^2\cdot\frac{170}{549}=170\cdot 549^{-1}=198 \pmod{631}$$

$$[2]T=(617,5)$$

$T=(617,5)$, $\quad n_1=0$, тому continue

Ітерація №2. $j=0$, $n_0=1$

$$\lambda=\frac{3\cdot 617^2+30}{2\cdot 5}=\frac{1142097}{10}=618\cdot 10^{-1}=188 \pmod{631}$$

$$I_{T,T}(Q+R)=129-188\cdot 535+(188\cdot 617-5)=396 \pmod{631}$$

$$V_{[2]T}(Q+R)=535-(188^2-2\cdot 617)=499 \pmod{631}$$

$$f=198^2\cdot\frac{396}{499}=82\cdot 396\cdot 499^{-1}=291\cdot 435=385 \pmod{631}$$

$$[2]T=(36,60)=-P$$

$T=(36,60)$, $\quad n_0=1$, тому:

Особливий випадок: $T+P=\mathcal{O}$ (точка на нескінченності)

$I_{T,P}(Q+R)=x_{Q+R}-x_T=535-36=499 \pmod{631}$ (вертикальна лінія)

$V_{T+P}(Q+R)=1$ (для точки $\mathcal{O}$ покладають таке)

$$f=385\cdot\frac{499}{1}=385\cdot 499=291 \pmod{631}$$

Результат: $f_{5,P}(Q+R)=291$

Обчислимо $f_{5,P}(R)$

Вхідні дані: $D = R = (0, 36)$, $a = 30$, mod $= 631$;
Ініціалізація: $T = P = (36, 571)$, $f = 1$

Ітерація №1. $j = 1$, $n_1 = 0$

$$\lambda = \frac{3 \cdot 36^2 + 30}{2 \cdot 571} = \frac{3918}{1142} = 132 \cdot 511^{-1} = 62 \pmod{631}$$

$$I_{T,T}(R) = 36 - 62 \cdot 0 + (62 \cdot 36 - 571) = 435 \pmod{631}$$

$$V_{[2]T}(R) = 0 - (62^2 - 72) = 14 \pmod{631}$$

$$f = 1^2 \cdot \frac{435}{14} = 435 \cdot 14^{-1} = 617 \pmod{631}$$

$$[2]T = (617, 5)$$

$$T = (617, 5), \quad n_1 = 0, \text{ тому continue}$$

Ітерація №2. $j = 0$, $n_0 = 1$

$$\lambda = \frac{3 \cdot 617^2 + 30}{2 \cdot 5} = \frac{1142097}{10} = 618 \cdot 10^{-1} = 188 \pmod{631}$$

$$I_{T,T}(R) = 36 - 188 \cdot 0 + (188 \cdot 617 - 5) = 554 \pmod{631}$$

$$V_{[2]T}(R) = 0 - (188^2 - 2 \cdot 617) = 595 \pmod{631}$$

$$f = 617^2 \cdot \frac{554}{595} = 196 \cdot 554 \cdot 595^{-1} = 52 \cdot 333 = 279 \pmod{631}$$

$$[2]T = (36, 60) = -P$$

$$T = (36, 60), \quad n_0 = 1, \text{ тому:}$$

Особливий випадок: $T + P = \mathcal{O}$

$$I_{T,P}(R) = x_R - x_T = 0 - 36 = 595 \pmod{631}$$

$$V_{T+P}(R) = 1$$

$$f = 279 \cdot \frac{595}{1} = 52 \pmod{631}$$

Результат: $f_{5,P}(R) = 52$

Обчислимо $f_{5,Q}(P-R)$

Вхідні дані: $P(36,571)$, $R(0,36)$, $D = P - R = P + (-R) = (315,246)$, $a = 30$, $\mathrm{mod} = 631$;
Ініціалізація: $T = Q = (420,48)$, $f = 1$

Ітерація №1. $j = 1$, $n_1 = 0$

$$\lambda = \frac{3 \cdot 420^2 + 30}{2 \cdot 48} = \frac{529230}{96} = 452 \cdot 96^{-1} = 31 \pmod{631}$$

$$I_{T,T}(P-R) = 246 - 31 \cdot 315 + (31 \cdot 420 - 48) = 298 \pmod{631}$$

$$V_{[2]T}(P-R) = 315 - (31^2 - 840) = 194 \pmod{631}$$

$$f = 1^2 \cdot \frac{298}{194} = 298 \cdot 194^{-1} = 587 \pmod{631}$$

$$[2]T = (121,387)$$

$$T = (121,387), \quad n_1 = 0, \text{ тому continue}$$

Ітерація №2. $j = 0$, $n_0 = 1$

$$\lambda = \frac{3 \cdot 121^2 + 30}{2 \cdot 387} = \frac{43953}{774} = 414 \cdot 143^{-1} = 250 \pmod{631}$$

$$I_{T,T}(P-R) = 246 - 250 \cdot 315 + (250 \cdot 121 - 387) = 577 \pmod{631}$$

$$V_{[2]T}(P-R) = 315 - (250^2 - 242) = 526 \pmod{631}$$

$$f = 587^2 \cdot \frac{577}{526} = 43 \cdot 577 \cdot 526^{-1} = 202 \cdot 6 = 581 \pmod{631}$$

$$[2]T = (420,583) = -Q$$

$$T = (420,583), \quad n_0 = 1, \text{ тому:}$$

Особливий випадок: $T + Q = \mathcal{O}$

$$I_{T,Q}(P-R) = x_{P-R} - x_T = 315 - 420 = 526 \pmod{631}$$

$$V_{T+Q}(P-R) = 1$$

$$f = 581 \cdot \frac{526}{1} = 202 \pmod{631}$$

Результат: $f_{5,Q}(P-R) = 202$

Обчислимо $f_{5,Q}(-R)$

Вхідні дані: $D = -R = (0, 595)$, $a = 30$, mod $= 631$;

Ініціалізація: $T = Q = (420, 48)$, $f = 1$

Ітерація №1. $j = 1$, $n_1 = 0$

$$\lambda = \frac{3 \cdot 420^2 + 30}{2 \cdot 48} = \frac{529230}{96} = 452 \cdot 96^{-1} = 31 \pmod{631}$$

$$I_{T,T}(-R) = 595 - 31 \cdot 0 + (31 \cdot 420 - 48) = 316 \pmod{631}$$

$$V_{[2]T}(-R) = 0 - (31^2 - 840) = 510 \pmod{631}$$

$$f = 1^2 \cdot \frac{316}{510} = 316 \cdot 510^{-1} = 352 \pmod{631}$$

$$[2]T = (121, 387)$$

$T = (121, 387), \quad n_1 = 0,$ тому continue

Ітерація №2. $j = 0$, $n_0 = 1$

$$\lambda = \frac{3 \cdot 121^2 + 30}{2 \cdot 387} = \frac{43953}{774} = 414 \cdot 143^{-1} = 250 \pmod{631}$$

$$I_{T,T}(-R) = 595 - 250 \cdot 0 + (250 \cdot 121 - 387) = 170 \pmod{631}$$

$$V_{[2]T}(-R) = 0 - (250^2 - 774) = 211 \pmod{631}$$

$$f = 352^2 \cdot \frac{170}{211} = 228 \cdot 170 \cdot 211^{-1} = 269 \cdot 317 = 88 \pmod{631}$$

$$[2]T = (420, 583) = -Q$$

$T = (420, 583), \quad n_0 = 1,$ тому:

Особливий випадок: $T + Q = \mathcal{O}$

$$I_{T,Q}(-R) = x_D - x_T = 0 - 420 = 211 \pmod{631}$$

$$V_{T+Q}(-R) = 1$$

$$f = 88 \cdot \frac{211}{1} = 269 \pmod{631}$$

Результат: $f_{5,Q}(-R) = 269$

Обчислюємо спарювання Вейля

Спираючись на попередні обчислення:

$$w_5(P, Q) = \frac{f_{5,P}(Q + R)/f_{5,P}(R)}{f_{5,Q}(P - R)/f_{5,Q}(-R)} = \frac{291/52}{202/269} = \frac{291 \cdot 449}{202 \cdot 441} = \frac{42}{111} = 42 \cdot 523 = 512 \pmod{631}$$

Перевірка: $512^5 \pmod{631} = 1 \Rightarrow$ є коренем 5 степеня з 1.