Лабораторная работа №4

Деревянченко
Владислав
Павлович
ВКБ-41

$y = x^3 + x + 2 \mod(29)$

x	$x^3+x+2 \pmod{29}$
0	2
1	4
2	12
3	3
4	12
5	16
6	21
7	4
8	0
9	15
10	26
11	10
12	2
13	8
14	5
15	22
16	25
17	2
18	23
19	7
20	18
21	4
22	0
23	12
24	17
25	21
26	1
27	21
28	0

y	$y^2 \mod 29$
0	0
1	1
2	4
3	9
4	16
5	25
6	7
7	20
8	6
9	23
10	13
11	5
12	28
13	24
14	22
15	27
16	24
17	28
18	5
19	13
20	23
21	6
22	20
23	7
24	25
25	16
26	9
27	4
28	1

(0): (1;2), (1;27), (5;4), (5;25), (7;2), (7;27), (8;0), (14;11), (14;18), (15;12), (15;17), (16;5), (16;24), (18;9), (18;20), (19;6), (19;23), (21;2), (21;27), (22;0), (26;1), (26;28), (28;0). ПЭК: 24

$P = (1;2) \quad Q = (5;4)$

$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{4-2}{5-1} = 2 \cdot 4^{-1} \pmod{29} = 2 \cdot 22 \mod 29 = 15$

$x_3 = \lambda^2 - x_1 - x_2 = 15^2 - 1 - 5 = 225 - 6 = 219 \mod 29 = 16$

$y_3 = \lambda \cdot (x_1 - x_3) - y_1 = 15(1-16) - 2 = 15 \cdot (-15) - 2 = -225 - 2 = -227 \mod 29 = 5$

$P + Q = (16, 5)$

$2P$

$\lambda = \frac{3x_1^2 + a}{2y_1} \bmod p = \frac{3 \cdot 1^2 + 1}{2 \cdot 2} \bmod 29 = 7$

$x_3 = \lambda^2 - 2x_1 = 1^2 - 2 = -1 \bmod 29 = 28 \bmod 29$

$y_3 = \lambda(x_1 - x_3) - y_1 = 1(1 - 28) - 2 = -27 - 2 = -29 \bmod 29 = 0$

$2P = (28, 0)$

04.04.25