Лабораторная работа №5

Деревянченко
Владислав
Павлович
ВКБ-41

$y = x^3 + x + 2 \mod 29 \quad P(1;27)$

1) $R = P = (1;27)$

2) $\lambda = \frac{3x^2+a}{2y} (\mod p) = \frac{3 \cdot 1^2 + 1}{2 \cdot 27} = \frac{4}{54} \equiv 22 (\mod 29)$

$x_3 = \lambda^2 - 2x = 22^2 - 2 = 28 (\mod 29)$

$y_3 = \lambda(x - x_3) - y = 28(1 - 28) - 27 = 0$

$\underline{2P(28,0)}$

3) $3P = P + 2P = (1;27) + (28,0)$

$\lambda = \frac{0-27}{28-1} \mod 29 \equiv 28 \mod 29$

$x_3 = 28^2 - 1 - 28 \equiv 1 (\mod 29)$

$y_3 = 28(1-1) - 27 \equiv 0 \mod 29$

$\underline{3P = (1,2)}$

4) $4P = 2 \cdot 2P = (28;0)$

$\lambda = \frac{3 \cdot 28^2 + 1}{2 \cdot 0} \mod 29 \underline{= 0}$

5) $5P = 2P + 3P = (28;0) + (1;2)$

$\lambda = \frac{2-0}{1-28} = \frac{2}{-27} = \frac{2 \cdot 28}{2} \equiv 1 (\mod 29)$

$x_3 = \lambda^2 - x_1 - x_2 = 1^2 - 28 - 1 \equiv 1 \mod 29$

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

$\underline{5P = (1;27)}$

6) $6P = 2 \cdot 3P = (1;2) + (1;2)$

$\lambda = \frac{3 \cdot 1^2 + 1}{2 \cdot 2} = \frac{4}{4} = 1 \mod 29$

$x_3 = 1^2 - 2 \cdot 1 \equiv 1 - 2 \equiv -1 \equiv 28 \mod 29$

$y_3 = \lambda(x_1 - x_3) - y_1 = 1(1-28) - 2 \equiv -27 - 2 \equiv -29 \equiv 0 \pmod{29}$

$\underline{6P = (28;0)}$

7) $7P = 3P + 4P = (1;2) + O = \underline{(1;2)}$

04.04.25

Для непар

$nP = \left(\frac{n-1}{2}\right)P + \left(\frac{n+1}{2}\right)P$

Для пар

$nP = \left(\frac{n}{2}\right)P \cdot 2$