Лабораторная работа 7

Деревенченко
Вадим
Павлович
ВКБ-41

$y^2 = x^3 + x + 2 \bmod 29$

$P_0 = (7, 2)$ $P = (7, 2)$ $c = 3$ $n = 4$

$X_0 = (7, 2)$

$i = 1$

$X_0^{-1} - ?$

$x = 7 \Rightarrow x^{-1} \bmod 29 = 25$ $y = 2$

$3 \cdot (25, 2)$ $\lambda = \frac{3 \cdot 25^2 + 1}{2 \cdot 2} = \frac{1876}{4} \bmod 29$

$1276 \bmod 29 = 20$

$4^{-1} \bmod 29 = 22$

$\lambda = 20 \cdot 22 = 440 \bmod 29 = 5$

$x_3 = 5^2 - 2 \cdot 25 \Rightarrow 5 - 50 = -25 \bmod 29 = 4$

$y_3 = 5 \cdot (25 - 4) - 2 = 105 - 2 = 103 \bmod 29 = 16$

$2P = (4, 16)$

$3 \cdot (25, 2) = (4, 16) + (25, 2)$ $\lambda = \frac{2 - 16}{25 - 4} = \frac{-14}{21} = 15 \cdot 21^{-1}$

$21^{-1} \bmod 29 = 24$

$\lambda = 15 \cdot 24 = 360 \bmod 29 = 12$

$x_3 = 12^2 - 4 - 25 = 144 - 29 = 115 \bmod 29 = \underline{28}$

$y_3 = 12(4 - 28) - 16 = 12 \cdot (-24) - 16 = -288 - 16 =$

$= -304 \bmod 29 = 27$

$X_1 = (28, 27) + (7, 2)$ $(28, 27)$

$\lambda = \frac{2 - 27}{7 - 28} = \frac{-25}{-21} = 4 \cdot 2 = 32 \bmod 29 = 3$

$\lambda = \frac{4}{5} \Rightarrow 5^{-1} = 11 \Rightarrow 4 \cdot 11 = 44 \bmod 29 = 15$

$x_3 = 15^2 - 28 - 7 = 190 \bmod 29 = \underline{16}$

$y_3 = 15(28 - 16) - 27 = 153 \bmod 29 = \underline{8}$

$X_1 = (16, 8)$

$i = 2$

$X_1 = (16, 2) \Rightarrow X^{-1} = 11$

$X_1^{-1} (11, 2)$

$3 \cdot (11, 2)$

$\lambda = \frac{3 \cdot 11^2 + 1}{2 \cdot 8} = \frac{365}{16}$ $365 \bmod 29 = 17$

$16^{-1} \bmod 29 = 20$ $\lambda = 17 \cdot 20 \bmod 29 = \underline{21}$

$3P = (13, 2) + (11, 2)$

$\lambda = \frac{2-2}{13-11} = 0$ $x_3 = -29 = 5$

$X_2 = (5, 21) + (7, 2)$ $y_3 = -2 = 21 \Rightarrow 3 \cdot (11, 2) = (5, 21)$

$\lambda = \frac{2-21}{7-5} = \frac{-19}{2} = 10 \cdot 2^{-1} \bmod 29 = 5$

$x_3 = 5^2 - 5 - 7 = 25 - 12 = 13$

$y_3 = 5(5 - 13) - 21 = -61 \bmod 29 = 26$

$X_2 = (13, 26)$

$i = 3$

$x = 13$ $x^{-1} = 9$ $X_2^{-1} = (9, 26)$

$3 \cdot (9, 26)$

$\lambda = \frac{3 \cdot 21 + 1}{2 \cdot 26} = \frac{244}{32} = 12 \cdot 52^{-1} \bmod 29 = 12$

$x_3 = 12^2 - 2 \cdot 9 = 4 \cdot 12 = -14 \bmod 29 = 15$

$y_3 = 21(9 - 15) - 26 = -12 - 26 = -32 = 20$

$2P = (15, 20)$

$3P = (15, 20) + (9, 26)$ $\lambda = \frac{26 - 20}{9 - 15} = \frac{6}{-6} = -1 = 28$

$x_3 = 22^2 - 15 - 9 = 760 \bmod 29 = 7$

$y_3 = 22(15 - 7) \cdot 20 = 204 \bmod 29 = 1$

$3 \cdot (9, 26) = (7, 1)$

$(7, 1) + (7, 2) = \underline{O}$

11.04.25