# Эллиптические кривые

Аметов Имиль, гр. M07-903

28 мая 2020 г.

*Задача:*
Приведите пример эллиптической кривой над $GF(p)$, где $p = 71$.
*Решение:*
Я выбрал эллиптическую кривую $y^2 = x^3 + 3x + 7$. Здесь

$$4 \cdot 3^3 + 27 \cdot 7^2 = 11 \mod 71.$$

Это удовлетворяет условию $4a^3 + 27b^2 \not\equiv 0(\mod p)$.
У меня получились следующие точки :

$$P_1 = O, P_2 = (3; 16), P_3 = (3; 55), P_4 = (4; 15),$$
$$P_5 = (4; 56), P_6 = (5; 17), P_7 = (5; 54), P_8 = (7; 4),$$
$$P_9 = (7; 67), P_{10} = (10, 16), P_{11} = (10; 55), P_{12} = (14; 33),$$
$$P_{13} = (14; 38), P_{14} = (15; 27), P_{15} = (15; 44), P_{16} = (17; 1),$$
$$P_{17} = (17; 70), P_{18} = (18; 0), P_{19} = (19; 6), P_{20} = (19; 65),$$
$$P_{21} = (21; 32), P_{22} = (21; 39), P_{23} = (22; 0), P_{24} = (24; 22),$$
$$P_{25} = (24; 49), P_{26} = (25; 4), P_{27} = (25; 67), P_{28} = (31; 0),$$
$$P_{29} = (34; 24), P_{30} = (34; 47), P_{31} = (35; 23), P_{32} = (35; 48),$$
$$P_{33} = (37; 19), P_{34} = (37; 52), P_{35} = (39; 4), P_{36} = (39; 67),$$
$$P_{37} = (45; 23), P_{38} = (45; 48), P_{39} = (47; 13), P_{40} = (47; 58),$$
$$P_{41} = (48; 14), P_{42} = (48; 57), P_{43} = (52; 7), P_{44} = (52; 64),$$
$$P_{45} = (58; 16), P_{46} = (58; 55), P_{47} = (59; 35), P_{48} = (59; 36),$$
$$P_{49} = (62; 23), P_{50} = (62; 48), P_{51} = (65; 25), P_{52} = (65; 46),$$
$$P_{53} = (66; 3), P_{54} = (66; 68), P_{55} = (67; 12), P_{56} = (67; 59),$$
$$P_{57} = (69; 8), P_{58} = (69; 63), P_{59} = (70; 28), P_{60} = (70; 43).$$

Порядок эллиптической кривой оказался равен 60. Этот порядок также подтверждается теоремой Хассе:

$$(\sqrt{71}-1)^2 \leq |E(GF(71))| \leq (\sqrt{71}+1)^2,$$

или

$$55 \leq |E(GF(71))| \leq 88.$$

Делители 60 следующие: 1, 2, 3, 4, 5, 6, 10, 15, 30, 60. Среди всех точек я нашёл точку $P_8 = (7;4)$ с рангом 30.

Доказательство:

$$2P_8 = (58;16), 3P_8 = (66;3), 4P_8 = (34;47), 5P_8 = (4;56),$$
$$6P_8 = (37;19), 7P_8 = (45;48), 8P_8 = (5;17), 9P_8 = (48;14),$$
$$10P_8 = (24;49), 11P_8 = (19;6), 12P_8 = (47;13), 13P_8 = (21;39),$$
$$14P_8 = (67;59), 15P_8 = (22;0), 16P_8 = (67;12), 17P_8 = (21;32),$$
$$18P_8 = (47;58), 19P_8 = (19;65), 20P_8 = (24;22), 21P_8 = (48;57),$$
$$22P_8 = (5;54), 23P_8 = (45;23), 24P_8 = (37;52), 25P_8 = (4;15),$$
$$26P_8 = (34;24), 27P_8 = (66,68), 28P_8 = (58;55), 29P_8 = (7;67),$$
$$30P_8 = O.$$

Теперь выбираю закрытый ключ $d$, который больше нуля и меньше ранга выбранной точки (т.е., меньше 30 в моём случае). Я выбрал $d = 23$.

Находим точку $Q = dP = 23 \cdot (7;4) = (45;23)$.

В результате, получен открытый ключ

$$[(a,b), P, p, Q] = [(3,7), (7;4), 71, (45;23)].$$

*Зашифровывание сообщения.* Пусть надо зашифровать сообщение

$$m = 50.$$

Выбирается случайное число $k (0 < k < p)$. Я выбрал $k = 11$. Вычисляется точка $P_k = k \cdot P = 11 \cdot (7;4) = (19;6)$. После этого вычисляется точка $Q_k(x_{q_k}, y_{q_k}) = k \cdot Q = 11 \cdot (45;23) = (21;39)$. Вычисляется

$$c = m \cdot x_{qk} \mod p = 50 \cdot 21 \mod 71 = 56.$$

Получен зашифрованный текст $[P_k, c]$. В моём случае, это $[(19;6), 56]$.

*Расшифровывание сообщения.* Вычисляется точка

$$D(x_d; y_d) = d \cdot P_k = 23 \cdot (19;6) = (21;39).$$

Теперь вычисляем сообщение

$$m = c \cdot x_d^{-1} \mod p = 56 \cdot 21^{-1} \mod 71 = 56 \cdot 44 \mod 71 =$$
$$= 50 \mod 71.$$

Окончательно получил $m = 50$.