Эллиптические кривые

Уравнение Вейерштрасса $y^2 + a_1 \cdot x \cdot y + a_3 \cdot y = x^3 + a_2 \cdot x^2 + a_4 \cdot x + a_6$ (1)

$a \in F$ – числовое поле. E/F – элл. кривая над полем F, включает точку $O = (x, \infty)$.

Условие невырожденности точки $P=(x_o, y_o)$: $\frac{\partial g}{\partial x}(x_o, y_o) \neq 0$ или $\frac{\partial g}{\partial y}(x_o, y_o) \neq 0$,

где $g = y^2 + a_1 \cdot x \cdot y + a_3 \cdot y - (x^3 + a_2 \cdot x^2 + a_4 \cdot x + a_6)$.

Любая E/F при $\mathrm{char}(F) > 3$ изоморфна кривой $y^2 = x^3\ a \cdot x + b$ (2)

Необходимое и достаточное условия невырожденности кривой:

дискриминант полинома $f(x) = x^3\ a \cdot x + b$ $\Delta f(x) \neq 0$.

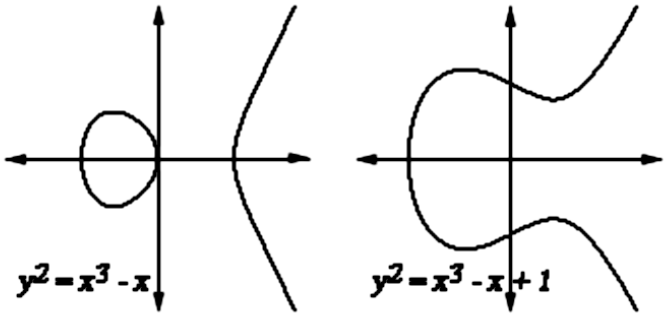
Дискриминант полинома $f(x) = a_0 + a_1 \cdot x \ \ldots\ a \cdot x^n$ равен $\Delta f(x) = a_n^{2n-2} \prod_{i-j} (\alpha_i - \alpha_j)$.

$\Delta f(x) = -4a^3 - 27b^2 \neq 0$

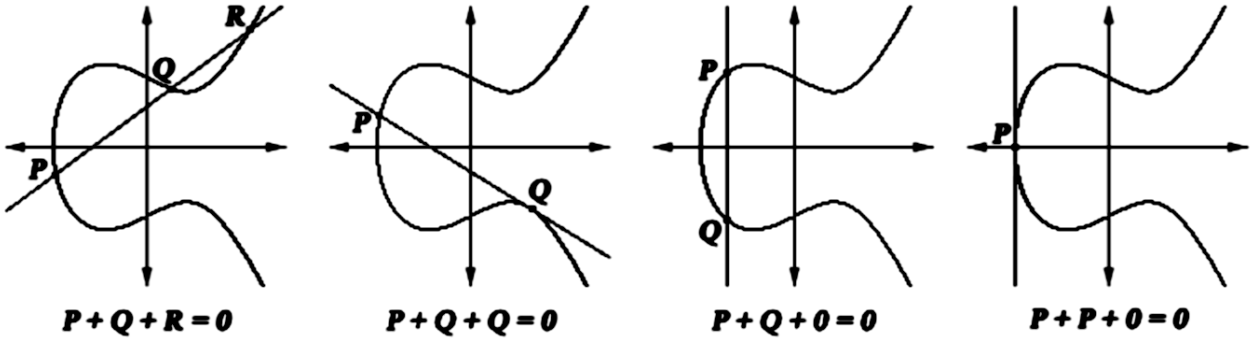
иногда

$\Delta' = -16(4a^3 + 27b^2) \neq 0$

$\Delta > 0$ $\Delta < 0$



Сложение точек эллиптической кривой



Уравнение прямой l : $y - y_1 = \lambda \cdot (x - x_1)$.

Если $P \neq Q$, то $y - y_2 = \lambda \cdot (x - x_2)$ и $\lambda = (y_1 - y_2) / (x_1 - x_2)$.

Если $P = Q$, то $\lambda = (3x_1^2 + a)/2y_1$

$P + Q = -R = \left[\lambda^2 - x_1 - x_2, \quad -y_1 + \lambda \cdot (2x_1 - \lambda^2 + x_2)\right]$