Суммирование точек на эллиптической кривой

Плотников Антон. А4101.

16 декабря 2016 г.

Определение

Определение 1. Рассмотрим конечное поле $F_q, q = p^k$ с характеристикой $p \geq 2$.

Тогда эллиптической кривой над полем F_q называется множество точек $(x, y) \in F_q \oplus F_q$, удовлетворяющих уравнению Вейерштрасса:

$$y^2 + ay + b = x^3 + cx^2 + dx + e, \tag{1}$$

вместе со специальной точкой, обозначающейся символом ∞ и называемая точкой в бесконечности.

Если $p \geq 3$, то уравнение 1 может быть преобразовано в сокращенное уравнение Вейерштрасса:

$$y^2 = x^3 + ax + b,$$

где $a, b \in F_q$.

Важными характеристиками эллиптической кривой являются её дискриминант Δ и инвариант j:

$$\Delta = -16(4a^3 + 27b^2) \qquad j = \frac{1728(4a)^3}{\delta}$$

На множестве точек E *неособой* эллиптической кривой (детерминант Δ, которой не равен нулю) можно определить групповую операцию суммирования $+$. Нулем будет этой группы является точка ∞, а обратным элементом по сложению к точке $P = (x, y) \in E$ будет являться точка $-P = (x, -y)$.

Суммирование точек на эллиптической кривой

Проведем прямую через пару произвольных точек P и Q прямую L до пересечения с третьей точкой R, такая точка обязательно найдется, т.к. пересечение произвольной прямой с эллиптической кривой имеет либо одну либо 3 точки пересечения.

Определим сумму трех точек $P(x_p, y_p)$, $Q(x_q, y_q)$ и $R(x_r, y_r)$ равной нулю:

$$P + Q + R = \infty,$$

тогда $P + Q = -R$.

Для вычисления координаты точки $S(x_s, y_s) = P + Q$ найдем параметры прямой L: $y = \lambda x + d$:

$$y = \frac{y_q - y_p}{x_q - x_p}, d = y_p - \lambda x_p.$$

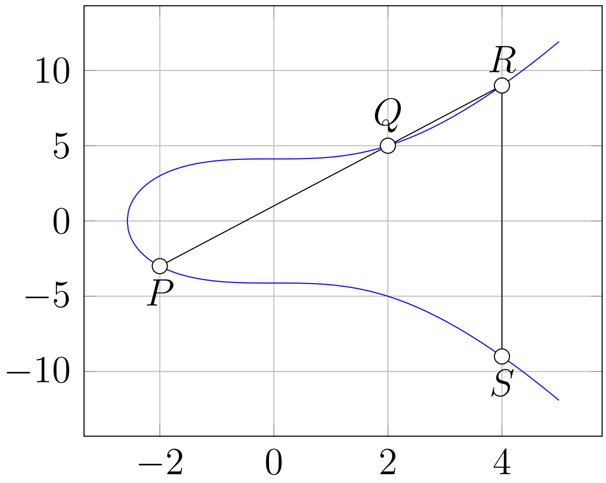

Рис. 1: Геометрическая интерпретация операции суммирования

Подставляя выражение для L в уравнение 1 получим:

$$x^3 + cx^2 + ax + b - (\lambda x + d)^2 = 0.$$

Сумма координат $x_p + x_q + x_s$ должна быть равна коэффициенту при x^2, взятому с противоположным знаком:

$$x_p + x_q + x_s = \lambda^2 - c = \left(\frac{y_q - y_p}{x_q - x_r}\right)^2 - c,$$

отсюда получим формулу для координат суммы:

$$\begin{cases} x_s = \lambda^2 - x_p - x_q - c \\ y_s = \lambda(x_p - x_q) - y_p = \lambda(2x_p + x_q - \lambda^2 + c) - y_p \end{cases}.$$

Если точки P и Q совпадают, то угловой коэффициент прямой L можно найти дифференцируя уравнение 1 по x.