Осень 2019

Лекция 1 — 06.09.2019

Лектор: Елена Киршанова *Оформил Филипп Максимов*

Литература.

1. A. Menezes "Elliptic curve public key cryptosystems"
2. D. Hankerson, A. Menezes, S. Vanstone "Guide to elliptic curve cryptography"
3. J. Silverman "Arithmetic of Elliptic Curves"

1 Введение

$\mathbb{F}_q$ — конечное поле, $|\mathbb{F}_q| = q = p^k$, p — простое, K — поле, $\overline{K}$ — алгебраическое замыкание.

1.1 Определения

Определение 1 (Уравнение Вейерштрасса)**.** Уравнение Вейерштрасса в проективных координатах — уравнение степени 3 вида

$$F : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1}$$

где $a_i \in K$. Уравнение Вейерштрасса **гладкое** (или несингулярное), если для любых проективных точек $P = (X : Y : Z) \in \mathbb{P}^2(K)$ [1], удовлетворяющих условию (1), хотя бы одна из частных производных $\frac{dF}{dX}, \frac{dF}{dY}, \frac{dF}{dZ}$ не обращается в 0 на P. Если все три частных производные обращаются в 0 хотя бы на одной точке P (точке сингулярности), (1) — сингулярное уравнение.

Определение 2. **Эллиптическая кривая** E (алгебраическая кривая рода 1) — множество всех точек в $\mathbb{P}^2(K)$, удовлетворяющих гладкой кривой (1).

Существует всего одна точка в E с координатой $Z = 0 : (0 : 1 : 0)$. Обозначаем эту точку $\mathcal{O}$, называем точкой в бесконечности.

Определение 3. Уравнение Вейерштрасса в аффинных координатах ($x = X/Z, y = Y/Z$):

$$f : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2}$$

[1] проективная плоскость над K — множество классов эквивалентности на $K^3 \setminus \{0, 0, 0\}$, т.е. $\overrightarrow{X} \sim \overrightarrow{Y}$, если $x_1 = u * y_1, x_2 = u * y_2, x_3 = u * y_3$

Тогда $F(K) = \{(x,y) \in K \times K : f(x,y) = 0\} \cup \{\mathcal{O}\}$.

Если $a_i \in K\ \forall i$, то будем говорить, что кривая E определена над K.

Определение 4. Обозначим

$$\begin{aligned} d_2 &= a_1^2 + 4a_2 \qquad (3)\\ d_4 &= 2a_4 + a_1a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= d_2^2 - 24d_4 \\ \text{Для проверки: } 4d_8 &= d_2d_6 - d_4^2 \end{aligned}$$

Тогда **дискриминант** уравнения (2) определяется как

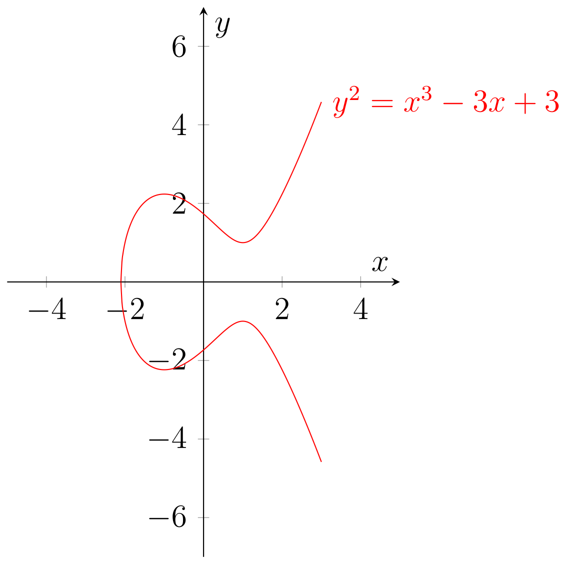
$$\Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6,$$

А j-инвариант эллиптической кривой E, $j(E)$, определяется как

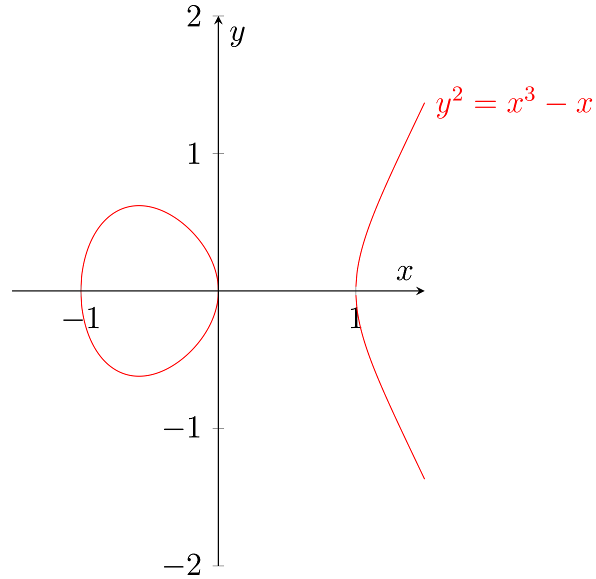
$$j(E) = \frac{c_4^2}{\Delta}$$

Теорема 5 (Sil, Thm. 1.4)**.** *Кривая, заданная уравнением Вейерштрасса, может быть классифицирована как:*

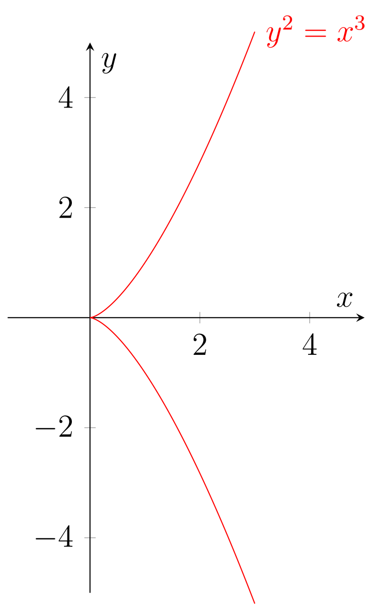
1. *Несингулярная* $\iff \Delta \neq 0$ *(*$\implies$ *задаёт эллиптическую кривую)*
2. *Кривая, обладающая узлом (node)* $\iff \Delta = 0, c_4 \neq 0$
3. *Кривая, обладающая точкой перегиба (cusp)* $\iff \Delta = c_4 = 0$



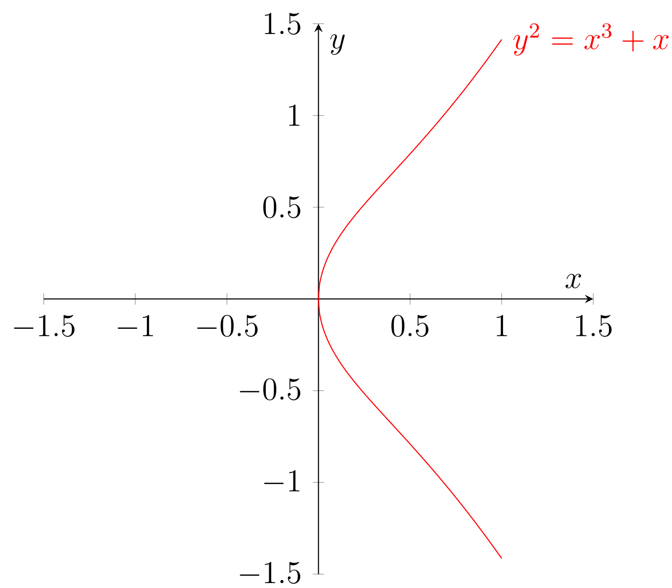
(a) $\Delta < 0$



(b) $\Delta > 0$



(c) Одна касательная



(d) $\Delta < 0$

Рис. 1: Эллиптические кривые над $\mathbb{R}$

1.2 Особые формы уравнения (2)

$charK \neq 2$**:**

$$f : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2}$$

$$\text{Дополним до полного квадрата: } y^2 + 2y(a_1x + a_3) + (a_1x + a_3))^2 - \frac{1}{4}(a_1x + a_3)^2$$

$$\implies 4(2y + \frac{a_1x + a_3}{2})^2 = 4 + \frac{1}{4}(a_1x + a_3)^2 + (a_2x^2 + a_4x + a_6) \quad | \cdot 4$$

$$\implies (2y + a_1x + a_3)^2 = 4x^3 + (a_1^2 + 4a_3)x^2 + (2a_1a_3 + 4a_2)x^2 + a_3^2 + 4a_6$$

$$\implies y = \frac{1}{2}(y' - a_1x - a_3)$$

$$\implies y^2 = 4x^3 + d_2x^2 + 2d_4 + d_6$$

Вывод: $(x, y) \mapsto (x, \frac{1}{2}(y - a_1x - a_3))$ для $E/K, charK \neq 2$, преобразует кривую вида (2) к кривой

$$E/K : y^2 = 4x^3 + d_2x^2 + 2d_4 + d_6. \tag{4}$$

$charK \neq 2, 3$**:** Дополним правую часть (4) до полного куба. Замена переменных

$$(x, y) \mapsto (\frac{x - 3d_2}{36}, \frac{y}{216})$$

Преобразует (4) в

$$E/K : y^2 = x^3 + ax + b \tag{5}$$

$$a = -27c_4$$

$$b = -56(d_2^3 + 36d_2d_4 - 216d_6)$$

В этом случае,

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

$$j(E) = -1728\frac{4a^3}{\Delta}.$$

$charK = 2$**:**

$$j(E) \neq 0\,(a_1 \neq 0) \implies (x, y) \mapsto (a_1^2x + \frac{a_3}{a_1}; a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3})$$

$$E/K : y^2 + xy = x^3 + a_2'x^2 + a_6' \tag{6}$$

$$j(E) \neq 0\,(a_1 \neq 0) \implies (x, y) \mapsto (x + a_2, y)$$

$$E/K : y^2 + a_3y = x^3 + a_4x + a_6 \tag{7}$$

1.3 Изоморфизм эллиптических кривых

Определение 6. $E_1/K, E_2/K$ изоморфны, если они изоморфны как проективные многообразия, т.е. $\exists$ морфизмы $\phi : E_1/K \to E_2/K, \psi : E_2/K \to E_1/K$ (определённые над K), такие что $\psi \circ \phi = id_{E_1}, \phi \circ \psi = id_{E_2}$.

Теорема 7. *Пусть $E_1/K, E_2/K$ — две эллиптические кривые, заданные уравнениями*

$$\begin{aligned} E_1 &: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \\ E_2 &: y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6' \end{aligned} \tag{8}$$

$$E_1 \cong E_2 \iff \exists u, r, s, t \in K, u \neq 0, \text{такие что замена}$$

$$(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t) \tag{9}$$

преобразует уравнение кривой E_1 в уравнение кривой E_2. Изоморфизм кривых задаёт отношение эквивалентности.

$$\begin{aligned} &\phi : (x, y) \mapsto (u^{-2}(x - r),\ u^{-3}(y - sx - t + rs)) - \text{точки } E_1 \text{ в } E_2 \\ &\psi : (x, y) \mapsto (u^2x + r,\ u^3y + u^2sx + t)) - \text{точки } E_2 \text{ в } E_1 \\ &\phi \circ \psi = id_{E_2}, \psi \circ \phi = id_{E_1}. \end{aligned}$$

Примеры 8.
Кривая E из (4) $\cong$ (2), если $charK \neq 2$.
(5) $\cong$ (4) $\cong$ (2), если $charK \neq 2, 3$.
(6) $\cong$ (2), если $charK = 2, j(E_1) \neq 0$.
(7) $\cong$ (2), если $charK = 2, j(E_1) = 0$

Следствие 9. *Если E_1, E_2 определены над K с $char(K) \neq 2, 3$, то (9) можно упростить:*

$$(x, y) \mapsto (u^2x, u^3y), u \neq 0$$

С помощью преобразования (9), можно вывести коэффициенты кривой E_2:

$$\begin{aligned} a_1' &= \frac{1}{u}(a_1 + 2s) \\ a_2' &= \frac{1}{u^2}(a_2 - sa_1 + 3r - s^2) \\ a_3' &= \frac{1}{u^3}(a_3 + ra_1 + 2t) \\ a_4' &= \frac{1}{u^4}(a_4 = sa_3 + 2ra_2 = (t + rs)a_1 + 3r^2 - 2st) \\ a_6' &= \frac{1}{u^6}(a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1) \end{aligned} \tag{10}$$

Аналогично, можно получить уравнения для d_i, j:

$$\Delta' = \frac{1}{u^{12}}\Delta$$
$$j' = j$$

Теорема 10. *$E_1 \cong E_2$ над $\bar{K}$ $\iff$ $j(E_1) = j(E_2)$*

Доказательство. Докажем для случая $char(K) \neq 2, 3$ (см. Silverman для общего случая).

$\implies$ следует из формул (10).

$\Longleftarrow$ Рассмотрим

$$E_1 : y^2 = x^3 + ax + b$$
$$E_2 = (y')^2 = (x')^3 + a'x' + b'$$

Тогда из $j(E_1) = j(E_2) \Rightarrow$

$$\frac{(4a)^3}{4a^3 + 27b^2} = \frac{(4a')^3}{4(a')^3 + 27(b')^2}$$
$$4^4a^3(a')^3 + 4^3a^3 27(b')^2 = 4^4a'^3a^3 + 4^3(a')^3 27b^2$$
$$a^3b^{12} = a^{13}b^2 \tag{*}$$

Нас интересуют только изоморфизмы вида $(x, y) \mapsto (u^2x', u^3y')$ (следствие 3).

Рассмотрим 3 случая:
Случай 1. $a = 0\,(\Rightarrow j = 0)$. Тогда $b \neq 0$ (т.к. $\Delta \neq 0$), $a' = 0$;

$$y^2 = x^3 + b, \qquad y^{12} = x'^3 + b', \qquad u = (\frac{b}{b'})^{\frac{1}{6}}$$

Случай 2. $b = 0$ (Тогда $a \neq 0, b' = 0$).

$$u = (\frac{a}{a'})^{\frac{1}{4}}$$

Случай 3. $b \neq 0 \implies a'b' \neq 0$

$$u = (\frac{a}{a'})^{\frac{1}{4}} = (\frac{b}{b'})^{\frac{1}{6}}$$

$\square$

Результаты

1. Получить уравнение изоморфных для E кривых над K, надо взять $(u, r, s, t) \in K$ и получить коэффициенты изоморфной кривой из (10).
   Сложность: $\mathcal{O}$ операций деления/умножения в K.

2. Проверить, являются ли две кривые $E_1/K, E_2/K$ изоморфными: решить (10) для неизвестных (u, r, s, t). Если решение в K существует, значит $E_1 \cong E_2$.
   Сложность: полиномиальная – решение системы уравнений в K.

3. Определить, над каким полем $L \subseteq K$ изоморфны кривые E_1, E_2: в каком расширении K лежат решения системы (10).