Осень 2020

Лекция 1 — 01.09.2020

Лектор: Семён Новосёлов

1 Введение

1.1 Мотивация

Эллиптические кривые в широко используются в сети Интернет в составе таких протоколов как HTTPS(TLS), SSH и IPSec. Основное применение – выработка общего ключа по протоколу Диффи-Хелмана (ECDH) и цифровые подписи (ECDSA). Используемые в настоящее время криптографические схемы основаны на задаче нахождения дискретного логарифма. В качестве альтернативы разрабатываются схемы (например, SIKE) основанные на сложности вычисления изогений – нетривиальных гомоморфизмов эллиптических кривых, которые отличаются стойкостью к атакам на квантовом компьютере.

С точки зрения математики, эллиптические кривые естественным образом появляются при попытке применить теорию групп к исследованию множеств решений систем полиномиальных уравнений, т.е. многообразий и алгебраических множеств. По определению эллиптическая кривая представляет собой групповое (абелево) многообразие размерности 1. Их изучению посвящено множество работ.

Данные лекции рассчитаны главным образом на изучение арифметических аспектов теории эллиптических кривых и их приложении к криптографии. Более основательное изложение можно найти в [Sil09].

1.2 Обозначения

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

1.3 Определения

Определение 1. *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 $P = (X : Y : Z) \in \mathbb{P}^2(K)$, удовлетворяющих уравнению (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), то (1) – сингулярное уравнение.

Определение 2. *Эллиптическая кривая* E – множество всех точек в $\mathbb{P}^2(K)$, удовлетворяющих гладкому уравнению (1).

Единственная точка $\mathcal{O}$ в E с координатами $(0 : 1 : 0)$, называется точкой в бесконечности.

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

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

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

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

Заметим, что использование проективных координат позволяет при выполнении арифметических операций на кривой избежать деления в поле за счёт увеличения количества умножений. Поэтому выбор подходящих координат для применения на практике зависит от скорости выполнения умножения по сравнению со скоростью выполнения деления.

Для определения является ли уравнение Вейерштрассе сингулярным/несингулярным используется понятие дискриминанта.

Определение 4. Обозначим

$$\begin{aligned} d_2 &= a_1^2 + 4a_2, \\ d_4 &= 2a_4 + a_1a_3, \\ d_6 &= a_3^2 + 4a_6, \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= d_2^2 - 24d_4. \end{aligned} \tag{3}$$

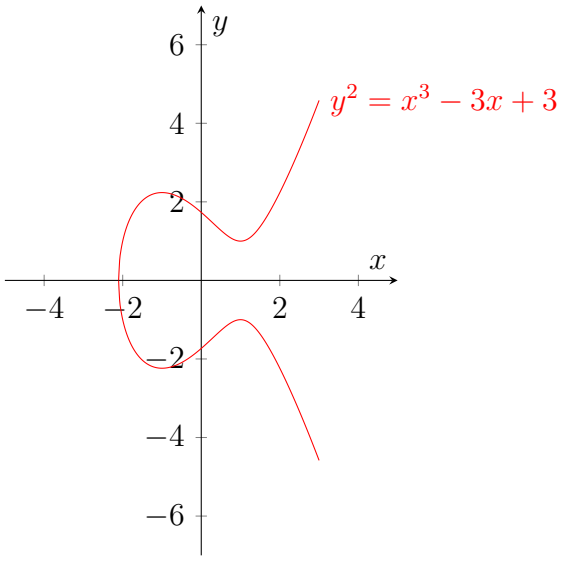
Тогда *дискриминант* уравнения (2) определяется как

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

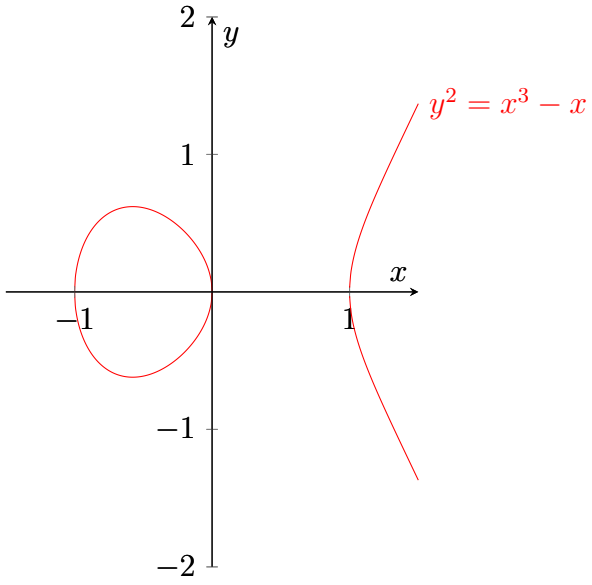
Теорема 5 ([Sil09], Thm. 1.4)**.** *Кривая, заданная уравнением Вейерштрасса, может быть классифицирована следующим образом.*

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

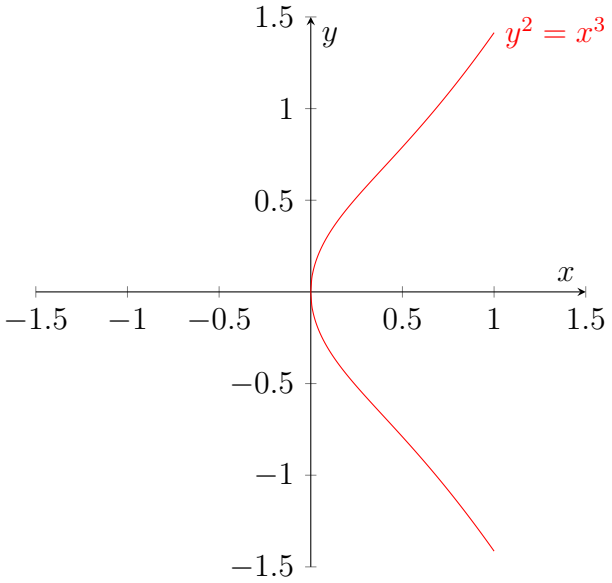
[0]проективная плоскость над K — множество классов эквивалентности на $K^3 \setminus \{0, 0, 0\}$, т.е. $\overrightarrow{X} \sim \overrightarrow{Y}$, если $x_1 = u * y_1, x_2 = u * y_2, x_3 = u * y_3$



(a) $\Delta < 0$



(b) $\Delta > 0$

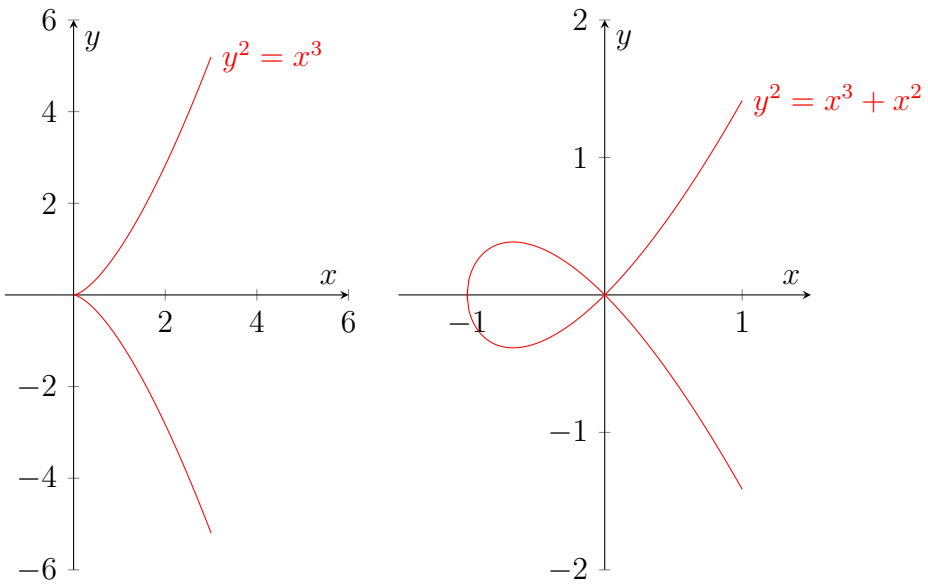


(c) $\Delta < 0$

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

1.4 Изоморфизмы эллиптических кривых

Если существует взаимнооднозначное отображение между двумя эллиптическими кривыми, задаваемое полиномиальными функциями (морфизмами), то кривые называются изоморфными. Такие кривые эквивалентны и в принципе нету разницы с какой изоморфной кривой работать. Это свойство достаточно широко используется на практике. Например, для приведения кривой в более простую краткую форму (см. ниже),



(a) Касп: одна касательная, $\Delta = 0$

(b) Нода: две касательных, $\Delta = 0$

Рис. 2: Сингулярные кубические кривые над $\mathbb{R}$

которая имеет меньше коэффициентов и соответственно арифметика на кривой более эффективная. Также существуют различные модели кривых с ещё более оптимизированной арифметикой (например, кривые Монтгомери) или имеющие другие интересные свойства (например, кривые в форме Шолтена[JV12] уязвимы к атакам на дискретный логарифм методом спуска Вейля). Однако, не всегда существуют изоморфизмы приводящие кривую в нужную форму.

В строгой и явной форме изоморфизм задаётся следующим образом.

Определение 6. Две эллиптические кривые E_1/K и E_2/K изоморфны, если они изоморфны как проективные многообразия, т.е. $\exists$ морфизмы $\phi : E_1/K \to E_2/K$ и $\psi : E_2/K \to E_1/K$ (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*

$$\begin{aligned} E_1 &: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \\ E_2 &: y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6. \end{aligned} \tag{4}$$

Тогда

$$\begin{aligned} E_1 \simeq E_2 \iff \exists u, r, s, t \in K, u \neq 0, \text{такие что замена} \\ (x, y) \mapsto (u^2x + r, u^3y + u^2sx + t) \end{aligned} \tag{5}$$

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

отношение эквивалентности.

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

С помощью преобразования (5), можно вывести коэффициенты кривой E_2:

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

Аналогично, можно получить уравнения для дискриминанта:

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

Определить являются ли кривые изоморфными можно решением системы уравнений относительно (u, r, s, t) составленной из (6).

Вместо решения системы уравнений удобней было бы определить и использовать функцию от коэффициентов кривой, которая имеет одинаковые значения на изоморфных кривых, или другими словами была бы инвариантна относительно изоморфизмов. Такая функция существует для кривых с точками над замыканием поля, называется j-инвариантом. Определяется следующим образом.

Пусть $c_4 = d_2^2 - 24d_4$ тогда j-инвариант эллиптической кривой E, $j(E)$, определяется как

$$j(E) = \frac{c_4^3}{\Delta}.$$

Теорема 8. *$E_1 \simeq E_2$ над $\bar{K} \iff j(E_1) = j(E_2)$.*

Доказательство теоремы можно найти в [Sil09, с. 46].

Кривые, изоморфные над замыканием называются *кручениями*[1]. Так как кривые изоморфные над базовым полем K, также должны быть изоморфными и над замыканием, то для определения изоморфности над K следует сначала сравнить j-инварианты, а затем уже решать систему уравнений.

[1] *анг.* twists

1.5 Краткие формы уравнения Вейерштрасса

С помощью изоморфных преобразований и дополнительных ограничений можно существенно упросить общее уравнение кривой.

Пусть эллиптическая кривая задана в полной форме:

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

Случай $\operatorname{char} K \neq 2$. Дополним до полного квадрата:

$$y^2 + 2y(a_1x + a_3) + (a_1x + a_3))^2 - \frac{1}{4}(a_1x + a_3)^2$$

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

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

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

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

Получаем, что отображение $(x, y) \mapsto (x, \frac{1}{2}(y - a_1x - a_3))$ для $E/K, \operatorname{char} K \neq 2$, преобразует кривую вида (2) к кривой

$$E/K : y^2 = 4x^3 + d_2x^2 + 2d_4 + d_6. \tag{7}$$

Случай $\operatorname{char} K \neq 2, 3$. Дополним правую часть (7) до полного куба. Замена переменных

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

преобразует (7) в

$$E/K : y^2 = x^3 + ax + b, \tag{8}$$

$$a = -27c_4,$$

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

В этом случае,

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

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

Случай $\operatorname{char} K = 2$**.**

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

$$E/K : y^2 + xy = x^3 + a_2'x^2 + a_6' \tag{9}$$

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

$$E/K : y^2 + a_3 y = x^3 + a_4 x + a_6 \tag{10}$$

Для кривых в краткой форме изоморфизмы имеют более простой вид.

Следствие 9 (из Теоремы 7)**.** *Если* E_1, E_2 *определены над* K *и* $\operatorname{char} K \neq 2, 3$*, то* (5) *можно упростить до преобразования*

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

Список литературы

[Bla+99] Ian Blake и др. *Elliptic curves in cryptography*. 1999.

[HMV06] Darrel Hankerson, Alfred J Menezes и Scott Vanstone. *Guide to elliptic curve cryptography*. 2006.

[JV12] Antoine Joux и Vanessa Vitse. "Cover and decomposition index calculus on elliptic curves made practical". в: 2012 (цит. на с. 4).

[Men93] Alfred J Menezes. *Elliptic Curve Public Key Cryptosystems*. 1993.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*. 2009 (цит. на с. 1, 2, 5).

[Was08] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. 2008.