ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

Ш. Т. Ишмухаметов

1. Введение

Эллиптической кривой над конечным полем F_p называется множество точек (x, y) вместе с особой бесконечно удаленной точкой $\mathbf{O}$, удоветворяющих уравнению

$$y^2 = x^3 + ax + b \pmod{p}. \tag{1}$$

Каждая эллиптическая кривая такого вида определяется тройкой чисел (a, b, p). Одной из важных задач для эллиптических кривых является задача нахождения количества точек кривой. Обозначеним его через $\#EC$. Согласно неравенству Хассе число точек ЭК удовлетворяет неравенству:

$$p + 1 - 2\sqrt{p} < \#EC < p + 1 + 2\sqrt{p}, \tag{2}$$

причем может принимать любое значение из этого интервала.

2. Число точек кривой $y^2 = x^3 + b \pmod{p}$

Докажем следующую теорему.

Теорема 2.1. *Отображение $F_p^* \to F_p^*$, задаваемое функцией $T_p(x) = x^3$, $1 \leq x < p\}$ является перестановкой F_p^* тогда и только тогда, когда $p-3$ является квадратичным невычетом по модулю p.*

Доказательство. Если $T_p(x)$ не является перестановкой, найдутся два элемента $a \neq b$, $a^3 - b^3 \mod p = 0$, откуда $a^2 + ab + b^2 \equiv 0 \pmod{p}$. Отсюда, получим уравнение $x^2 + x + 1 \equiv 0 \pmod{p}$, где $x = a/b \pmod{p}$. Дискриминант $D = -3$ уравнения $x^2 + x + 1 = 0$ равен -3. Для того, что уравнение имело решение, дискриминант D должен быть квадратичным вычетом в поле F_p. В противном случае, $x^2 + x + 1 = 0$ не имеет решения в F_p, и отображение $T_p(x)$ является перестановкой. Теорема доказана.

Следствие 2.1. *Пусть коэффициенты кривой (1) a и b равны 0. Если $p - 3$ является квадратичным невычетом по модулю p, $p \geq 5$, кривая (1) содержит $p+1$ точку. В противном случае, кривая (1) содержит $6k+2$ точки, где $k \geq 1$ – мощность пересечения множеств $D(y) = \{y^2 \mod p : 1 \leq y < p\}$ и $E(x) = \{x^3 \mod p : 1 \leq x < p\}$.*

Действительно, если $p-3$ – невычет по модулю p, тогда T_p -перестановка F_p^*, и для каждого значения y, $0 \leq y < p$ найдется единственное x, при котором выполняется (1). Добавляя бесконечно удаленную точку, получим $\#EC = p+1$.

В противном случае, для каждой точки (x', y'), $x' > 0$, лежащей на кривой (1), найдутся еще 5 точек (x, y), удовлетворяющих соотношениям $x^3 \equiv (x')^3 \pmod{p}$, $y^3 \equiv (y')^2 \pmod{p}$ и лежащих на кривой. Число $k \geq 1$, поскольку оба множества обязательно содержат 1.

Например при $p = 7$ имеем $D(y) = \{1, 2, 4\}$, $E(x) = \{1\}$, $k = 2$, и кривая (3) содержит 6 точек.

Лемма 2.1. *Пусть $p > 3$ - простое число. Элемент $p-3$ является квадратичнм вычетом по модулю p тогда и только тогда, когда $p \equiv 1 \pmod 3$.*

Доказательство. Вычислим символ Лежандра $L(-3, p) = \left(\frac{-3}{p}\right)$. В силу мультипликативности символа Лежандра

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right)$$

Поскольку p - простое число, выполняется закон квадратичной взаимности Гаусса

$$L(-3, p) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p \bmod 3}{3}\right) = \left(\frac{p \bmod 3}{3}\right).$$

Лемма доказана.

2.1. **Частные случаи кривых $a = 0$.** Далее будем рассматривать кривые (1) при $p \equiv 1 \pmod 3$, $a = 0$, $1 \le b < p$:

$$y^2 = x^3 + b \pmod p, \quad p \equiv 1 \pmod 3, \ 1 \le b < p. \tag{3}$$

Лемма 2.2. *Пусть k - мощность множества $D(x) \cap E(y)$. Кривые, задаваемые уравнением (3), содержат $6k + c + d + 1$ точек, где $c = 2$, если b является квадратичным вычетом в F_p, и 0, иначе; $d = 3$, если $p-b$ является кубическим вычетом в F_p, и 0, иначе.*

Действительно, для каждого значения $t \in D(x) \cap E(y)$ множество

$$M(x, y) = (x, y) : \ x^3 \bmod p = t, \ y^3 \bmod p = t,$$

состоящее из 6 точек, принадлежащих (3). Если b является квадратичным вычетом в F_p, то имеем два значения $y = \pm\sqrt{b}$, при которых $(0, y) \in EC$. Если $p-b$ является кубическим вычетом в F_p, то найдется три значения $x : \ x^3 + b \bmod p = 0$, и соответствующие точки $(x, 0) \in EC$.

Пример. Пусть $p = 7, \ b = 1$. Пересечение $D(x) \cap E(y)$ содержит один элемент 1, $b = 1$ является квадратичным вычетом в F_7, $p - b = 6$ является кубическим вычетом в F_7. Число точек равно $\#EC = 6 \cdot 1 + 2 + 3 = 12$.

3. Нахождение точек на ЭК (3) порядков 2,3 и 4

Приведем формулы удвоения и сложения точек на эллиптической кривой. Пусть точка $P(x, y) \in EC$. Тогда 2P имеет координаты:

$$\begin{cases} x_2 = k^2 - 2x_1 \\ y_2 = k(x_1 - x_2) - y_1. \end{cases} \tag{4}$$

где $k = (3x_1^2 + a)/2y_1 \pmod p$.

$$\begin{cases} x_3 = k^2 - x_1 - x_2 \\ y_3 = k(x_1 - x_3) - y_1. \end{cases} \tag{5}$$

где $k = (y_2 - y_1)/(x_2 - x_1) \pmod p$.

Обозначим через $ord(P)$ порядок точки P.

Лемма 3.1. *Пусть точка $P(x, y) \in EC$. Для того, чтобы ее порядок был равен 2, необходимо и достаточно, чтобы координата y равнялась 0.*

Доказательство. Если $ord(P) = 2$, касательная в этой точке – вертикальна, и координата y равно 0.

Лемма 3.2. *Порядок точки $P(x, y) \in EC$, $x \neq 0$, вида (3) равен 3 тогда и только тогда, когда выполняется соотношение* $3x^3 \equiv 4y^2 \pmod p$.

Доказательство. Обозначим через (x_2, y_2) координаты т.2P. Если $ord(P) = 3$, тогда угловой коэффициент прямой, проходящей через т.P и 2P, равен ∞, значит, $x \equiv x_2 \pmod p$, или $x \equiv k^2 - 2x \pmod p$, откуда $k^2 \equiv 3x \pmod p$. Подставляя $k = (3x^2 + a)/2y$, получим

$$\frac{(3x^2 + a)^2}{(2y)^2} \equiv 3x \pmod p \ \rightarrow \ (3x^2 + a)^2 \equiv 12xy^2 \pmod p.$$

При $a = 0$ учитывая $x \neq 0$, получим требуемое соотношение.

Следствие 3.1. *Если кривая $y^2 = x^3 + b \pmod p$ содержит точку $P(x, y)$ порядка 3, тогда $(x, y) = (\sqrt[3]{-4b}, \pm\sqrt{-3b})$.*

Доказательство. Пусть $ord(P) = 3$. Тогда, $3x^3 \equiv 4y^2 \pmod p$. Подставляя $3x^3 = 4y^2$ в уравнение кривой $3y^2 = 3x^3 + 3b$, получим, $y^2 + 3b \equiv 0 \pmod p$, откуда $y \equiv \pm\sqrt{-3b} \pmod p$. Из уравнения (3) найдем x^3: $x^3 = y^2 - b = -4b$, и точка $(\sqrt[3]{-4b}, \pm\sqrt{-3b})$ принадлежит кривой.

Пример. Пусть $p = 11$. При $b = 7$ $y \equiv \pm 1 \pmod{11}$, $x \equiv \sqrt[3]{5} \equiv 3 (\mathrm{mod}\ 11)$, и точка $(3, \pm 1)$ порядка 3 принадлежит кривой $y^2 = x^3 + 7 \pmod{11}$.

Лемма 3.3. *Порядок точки $P(x, y) \in EC$, $x \neq 0$, $y \neq 0$, вида (3) равен 4 тогда и только тогда, когда выполняется соотношение*

$$27x^3 - 36x^3y^2 + 8y^4 \equiv 0 \pmod p. \tag{6}$$

Доказательство. Пусть координаты т. $2P$ есть (x_2, y_2). Если $ord(P) = 4$, тогда $y_2 \equiv k(x - x_2) - y \equiv 0 \pmod p$. Поскольку, $x_2 = k^2 - 2x$, то

$$y_2 \equiv kx - k^3 + 2kx - y \equiv 0 (\mathrm{mod}\ p) \text{ или } k^3 - 3kx + y \equiv 0 \pmod p$$

Подставляя $k = 3x^2/2y$, получим

$$\frac{27x^3}{8y^3} - \frac{9x^3}{2y} + y \equiv 0 \pmod p,$$

откуда следует (6).

4. Тест простоты, основанный на эллиптических кривых

Будем рассматривать кривые вида $y^2 = x^3 + b \pmod p$ над полями F_p, $p \equiv 2 (\mathrm{mod}\ 3)$. Такие кривые всегда содержат $p+1$ точку. Определим значение $b = 1$. Построим некоторый алгоритм проверки чисел на простоту.

Пусть n- нечетное число вида $n \equiv 2 (\mathrm{mod}\ 3)$. Каждое такое число можно задать формулой $n = 6k + 5$, $k \in \mathbf{N}$. Найдем перебором на кривой $y^2 = x^3 + 1 \pmod n$ точку $P(x, y), x > 0$, $y > 0$, так чтобы $3x^3 \not\equiv 4y^2 \pmod p$. Порядок t точки $P(x, y)$ согласно лемме 3.2 больше 3 и является делителем числа точек на кривой. Если число n - простое, тогда число точек кривой $\#EC$ равно $n + 1$.

Это свойство можно использовать как тест простоты для нечетных чисел n, $n \equiv 2 (\mathrm{mod}\ 3)$. Для этого вычислим кратную точку $P_2 = (n + 1)P$, используя формулы (4) и (5). Если полученная точка равна $\mathbf{0}$ - бесконечно удаленной точке, то число n - простое, иначе - составное.

Такой тест может давать ошибки, определяя некоторые составные числа, как простые. Будем называть такие n ЭК-псевдопростыми. Для нахождения псевдопростых чисел можно проверять числа n, определяемые тестом на ЭК как простые, дополнительным тестом простототы, например, тестом Миллера-Рабина (см. [6]).

Упражнение. Напишите программу для проверки нечетных чисел тестом ЭК. Найдите все псевдопростые числа до 10^6.

Список литературы

[1] Washington, L. Elliptic curves : number theory and cryptography// .– 2nd ed. DISCRETE MATHEMATICS AND ITS APPLICATIONS Series, Editor KENNETH H. ROSEN. 524 p.

[2] Daniel Shanks. Five Number Theoretic Algorithms.// Proceedings of the Second Manitoba Conference on Numerical Mathematics. P. 51–70. 1973.

[3] Apostol T. *Introduction to Analytic Number Theory*/ Springer, 1976, 338 p.

[4] Crandall R. *The prime numbers: a computational perspertive* / R. Crandall, C. Pomerance.– sec.ed. Springer–Verlag, Berlin, 2005, 604 p.

[5] Чандрасекхаран К. *Введение в аналитическую теорию чисел.* – М: Мир, 1974. – 187 с.

[6] Ишмухаметов Ш.Т. *Методы факторизации натуральных чисел: учебное пособие.* – Казанский федеральный университет, Казань, 2011. – 190 с.

Казанский федеральный университет, Казань
Email address: Shamil.Ishmukhametov@ksu.ru, aphrodesia@mail.ru