УДК 681.3

АНАЛИЗ МЕТОДА ПОСТРОЕНИЯ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ С ЗАДАННЫМ ПОРЯДКОМ

Н.И. ЧЕРВЯКОВ
М. Г. БАБЕНКО

Ставропольский государственный университет

e-mail: whbear@yandex.ru

В статье рассмотрен метод построения эллиптической кривой с заданным порядком. Предложена модификация метода деления пополам для нахождения корней многочленов над F_p.

Ключевые слова: криптосистемы на эллиптической кривой, методы нахождения корней многочленов над конечным полем.

Введение. Постановка задачи

Современные информационные системы требуют особого подхода к передаче электронных документов по открытым каналам связи. При этом возникает задача сохранения секретной информации в документе от сторонних глаз, которая решается с использованием ассиметричных алгоритмов.

Эллиптические кривые – один из самых перспективных инструментов для построения криптографических алгоритмов [2]. Это обусловлено тем, что они обеспечивают максимально возможную для криптосистемы с открытым ключом стойкость на один бит размера задачи [4]. Эллиптическая кривая E, заданная уравнением в форме Вейерштрассе:

$$E(F_p): y^2 = x^3 + ax + b, \quad (1)$$

где p — простое число.

Одним из основных требований, предъявляемых к эллиптической кривой (1) является, содержание большого простого числа в порядке группы точек. Французский математик Ф. Морейн предложил метод построения эллиптической кривой E над простым полем с заданным количеством точек.

Постановка задачи. Провести анализ метода Ф. Морейна и разработать метод нахождения корней многочлена заданного над F_p.

Основная часть.

Морейн обратил внимание на тот факт, что всегда можно найти кривую, если знать её инвариант $j(E)$ и $j(E) \neq 1728$ по следующим формулам:

$$a = 3k,\ b = 2k, \text{ где } k = \frac{j(E)}{1728 - j(E)} \bmod p. \quad (2)$$

Между порядком эллиптической кривой и инвариантом существует функциональная зависимость. Рассмотрим метод предложенный Ф. Морейном в работе [3].

1. По заданному порядку $\#E(F_p) = hn$, где n большое простое число $n > 2^{254}$ используя формулу $t = p + 1 - \#E(F_p)$ вычисляем значение дивизора: $D = 4p - t^2$.

2. Вычисляем многочлен Гильберта $H_D(X)$ (алгоритм вычисления многочлена Гильберта описан в работе [1])

3. Находим корни многочлена Гильберта $H_D(X)$ (одним из корней многочлена Гильберта, является искомое значение $j(E)$).

4. Для каждого из корней многочлена Гильберта $H_D(X)$ вычисляем значение коэффициентов a, b по формуле (2). Выбираем случайную точку

$P(x,y)\in E(F_p)\colon y^2=x^3+ax+b$ и проверяем на выполнение условия $\#E(F_p)P=O$. При выполнении условия кривая найдена.

5. Пусть $\#E(F_p)P\neq O$ переходим к кривой кручения $a'=ac^2$, $b'=bc^3$, $\left(\frac{c}{p}\right)=-1$. Выбираем случайную точку $P'(x,y)\in E(F_p)\colon y^2=x^3+a'x+b'$ и проверяем на выполнение условия $\#E(F_p)P'=O$. При выполнение условия процедура завершена, иначе возвращаемся на пункт 4 и рассматриваем следующий корень многочлена Гильберта в качестве $j(E)$.

Приведем примеры модулярных многочленов Гильберта:

$H_{163}(x)=x+640320;$

$H_{403}(x)=x^2-1088442034024910558330880000000\,x$

$+24528113892293313919795200000;$

$H_{883}(x)=x^3+167990285381627318187575520800123387904000000000\,x^2$

$-151960111125245282033875619529124478976000000\,x$

$+34903934341011819039224295011933392896000$

Для нахождения корней многочлена Гильберта в F_p, модифицируем численный метод деления отрезка пополам.

Используем следующие формулы

$$x^p-x=\prod_{i=0}^{p-1}(x-i)$$

Метод деления отрезка пополам для нахождения корней многочлена $g(x)$ над F_p.

Пусть $f(x)=x^p-x$ и $v\in F_p^*$ образующий элемент в F_p^*.

Вначале определим количество различных корней многочлена $g(x)$, для этого вычислим $НОД(f(x),g(x))=g_1(x)$, тогда количество различных корней многочлена $g(x)$ равно $\deg g_1(x)=n$.

На втором этапе вычислим $НОД(f(x),g(x^2))=g_{1,1}(x)$, если $\deg g_{1,1}(x)>0$, то количество корней многочлена $g_1(x)$, являющихся квадратичными вычетами в F_p^* равно $\frac{\deg g_{1,1}(x)}{2}$, а количество корней многочлена $g_1(x)$, являющихся квадратичными невычетами в F_p^* равно $\frac{\deg g_{1,2}(x)}{2}$, где $g_{1,2}(x)=НОД(g(v\cdot x^2),f(x))$.

На третьем этапе рассмотрим два случая:

1. Если $\deg g_{1,1}(x)>2$, то вычисляем $НОД(f(x),g(x^4))=g_{1,1,1}(x)$, если $\deg g_{1,1,1}(x)=2\cdot\deg g_{1,1}(x)$, то переходим на шаг 4, иначе вычисляем $НОД(f(x),g(v^2\cdot x^4))=g_{1,1,2}(x)$.

2. Если $\deg g_{1,2}(x)>2$, то вычисляем $НОД(f(x),g(v\cdot x^4))=g_{1,2,1}(x)$, если $\deg g_{1,2,1}(x)=2\cdot\deg g_{1,2}(x)$, то переходим на шаг 4, иначе вычисляем $НОД(f(x),g(v^3\cdot x^4))=g_{1,2,2}(x)$.

Шаг четвертый разбивается на четыре случая:

1. Если $\deg g_{1,1,1}(x) > 4$, то вычисляем $НОД\left(f(x), g\left(x^8\right)\right) = g_{1,1,1,1}(x)$ если $\deg g_{1,1,1,1}(x) = 2 \cdot \deg g_{1,1,1}(x)$, то переходим на шаг 5 иначе вычисляем $НОД\left(f(x), g\left(v^4 \cdot x^8\right)\right) = g_{1,1,1,2}(x)$.

2. Если $\deg g_{1,1,2}(x) > 4$, то вычисляем $НОД\left(f(x), g\left(v^2 \cdot x^8\right)\right) = g_{1,1,2,1}(x)$ если $\deg g_{1,1,2,1}(x) = 2 \cdot \deg g_{1,1,2}(x)$, то переходим на шаг 5, иначе вычисляем $НОД\left(f(x), g\left(v^6 \cdot x^8\right)\right) = g_{1,1,2,2}(x)$.

3. Если $\deg g_{1,2,1}(x) > 4$, то вычисляем $НОД\left(f(x), g\left(v \cdot x^8\right)\right) = g_{1,2,1,1}(x)$, если $\deg g_{1,2,1,1}(x) = 2 \cdot \deg g_{1,2,1}(x)$, то переходим на шаг 5, иначе вычисляем $НОД\left(f(x), g\left(v^5 \cdot x^8\right)\right) = g_{1,2,1,2}(x)$.

4. Если $\deg g_{1,2,2}(x) > 4$, то вычисляем $НОД\left(f(x), g\left(v^3 \cdot x^8\right)\right) = g_{1,2,2,1}(x)$, если $\deg g_{1,2,2,2}(x) = 2 \cdot \deg g_{1,2,2}(x)$, то переходим на шаг 5, иначе вычисляем $НОД\left(f(x), g\left(v^7 \cdot x^8\right)\right) = g_{1,2,2,2}(x)$. и т. д.

Процесс останавливается когда выполняется условие $\deg g_{1,i_1,\ldots,i_k}(x) = 2^k$.

Пример. Найти корни многочлена $g(x) = x^3 + 10x^2 + 4x + 6$ над F_{17}

Решение

Так как $НОД\left(x^{17} - x, g(x)\right) = g_1(x) = g(x)$ и $\deg\left(g\ (x)\right) = 3$, то, многочлен $g(x)$ имеет три различных корня в F_{17} и $v = 6$.

Вычисления удобно оформить в виде схемы, представлены на рис. 1.

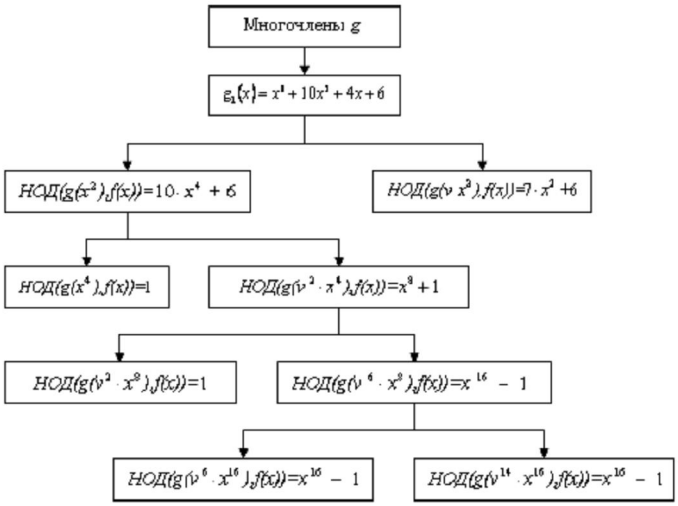

Рис 1. Схема работы метода деления отрезка пополам для нахождения корней многочлена $g(x)$ над F_p

Из $НОД(g(v^6 \cdot x^{16}),f(x))=x^{16} - 1$ следует, что корнем $g_1(x)$ является $x_1 = v^6 \bmod 17 = 8$. Из $НОД(g(v^{14} \cdot x^{16}),f(x))=x^{16} - 1$ следует, что корнем $g_1(x)$ является

$x_2 = v^{14} \bmod 17 = 9$, а из $НОД(g(v \cdot x^2), f(x)) = 7 \cdot x^2 + 6$ следует, что корнем $g_1(x)$ является $x_3 = -\frac{6}{7} \cdot v \bmod 17 = 4 \cdot 6 \bmod 17 = 7$.

Выводы.

В статье проведен анализ метода Ф. Морейна для построения эллиптической кривой E над простым полем с заданным количеством точек. Предложен метод нахождения корней многочлена заданного над F_p.

Литература

1. Lay G.J., Zimmer H., Constructing elliptic curves with given group order over large finite fields, in Algorithmic Number Theory-ANTS-I. Lecture Notes in Computer Science, vol. 877 (Springer, Berlin, 1994), pp. 250-263

2. Menezes A., van Oorchot P., Vanstone S. Handbook of applied cryptography. – CRC Press, 1997. – 816 p.

3. Morain F., Primality proving using elliptic curves: an update. In "Algorithmic Number Theory, Third International Symposium, ANTS-III," J. P. Buhler editor, Lecture Notes in Comput. Sci. Vol, 1423, Springer-Verlag, June 1998. pp. 111-127

4. Ростовцев А. Г. Маховенко Е. Б. Два подхода к логарифмированию на эллиптической кривой. http://www.ssl.stu.neva.ru/ssl/archieve/lift1.pdf

ANALYSIS METHOD OF CONSTRUCTION ELLIPTIC CURVES WITH A GIVEN ORDER

N.I. CHERVAYKOV
M.G. BABENKO

Stavropol State University

e-mail:
whbear@yandex.ru

The article represents the method of the elliptic curve construction with a given order. The modification of the bisection method for finding roots of polynomials over F_p is suggested.

Key words: cryptosystem on an elliptic curve, methods for finding roots of polynomials over finite fields.