Изучение эллиптических кривых с помощью системы компьютерной алгебры Wolfram Mathematica

Лабораторная работа

Ревизия: 0.2

Последняя модификация: Vlad Kovtun

Дата последней модификации: 26.08.2012 20:45:00

История изменений

17.11.2011 – Версия 0.1. Первичный документ. Владислав Ковтун

26.07.2012 – Версия 0.2. Добавлены алгоритмы операций над элементами двоичного и простого полей. Добавлены алгоритмы операций над точками эллиптической кривой в различных формах и в различных представлениях. Владислав Ковтун. Анна Шаповал.

Содержание

Лабораторная работа 4. Изучение эллиптических кривых с использованием системы компьютерной алгебры Wolfram Mathematica

Вопросы

1. Общие положения.

2. Постановка задачи.

3. Методические рекомендации.

Постановка задачи

Цель

Разработать программу для системы компьютерной алгебры Wolfram Mathematica, которая реализует над точками эллиптической кривой:

- над различными полями: $\mathbf{GF}(p)$ и $\mathbf{GF}(2^m)$.
- в различных представлениях кривых: аффинное, стандартное проективное, расширенное стандартное проективное, проективное Якоби, модифицированное проективное Якоби, расширенное модифицированное проективное Якоби, проективное Лопеса-Дахаба, расширенное проективное Лопеса Дахаба, инвертированное проективное.
- в различных формах кривых: Вейерштрасса, Хессе, Эдвардса, скрученной Хессе, скрученной Эдвардса, Монтгомери, Якоби четвертой степени (кваритика).

Следующие арифметические операции в аффинном представлении для формы кривой Вейерштрасса:

- найти случайную точку принадлежащую ЭК,
- проверить принадлежит ли заданная точка указанной ЭК,
- сложить точки ЭК,
- удвоить точку ЭК,
- вычесть точки ЭК,
- вычислить отрицательную точку ЭК,
- скалярно умножить точку ЭК,
- найти случайную точку ЭК большого простого порядка,
- преобразование ЭК в форме Вейерштрасса в форму Эдвардса и Хессе и наоборот,

Отдельно следует изучить преобразования точек в заданном представлении:

- сложить точки ЭК,
- удвоить точки ЭК,
- скалярно умножить точку ЭК.

Задачи

1. Ознакомиться с основными теоретическими положениями теории групп, теории полей, теории алгебраических кривых (эллиптических кривых) в форме Вейерштрасса, Хессе, Хаффа, Эдвардса и их модификациями.

2. Ознакомиться с основными возможностями системы компьютерной алгебры Wolfram Mathematica по работе с конечными полями (полями Галуа).

3. Ознакомиться с основными алгоритмами по реализации арифметических операций над точками ЭК для поля $\mathbf{GF}(p)$ и $\mathbf{GF}(2^m)$.

4. Разработать набор функций и процедур для полей $\mathbf{GF}(p)$ и $\mathbf{GF}(2^m)$ и кривой форме Вейерштрасса в Аффинном представлении:

- Генерации случайной точки ЭК.
- Генерация случайной точки ЭК большого простого порядка.
- Проверка принадлежности точки ЭК.
- Сложение точек ЭК.
- Вычитание точек ЭК.
- Удвоение точек ЭК.
- Скалярное умножение точек ЭК.

5. Разработать набор функций и процедур для полей $\mathbf{GF}(p)$ и $\mathbf{GF}(2^m)$, которые:

- По заданному представлению ЭК в форме Вейерштрасса смогут получить кривую в форме Эдвардса, в форме Хессе и наоборот.
- Арифметические операции над точками ЭК для различных форм ЭК и представлений точек ЭК.

6. Подготовить и оформить отчет о проведенной лабораторной работе.

Задание на лабораторную работу

В качестве входных данных, см. таблицу 1, используется:

- Базовое поле.
- Параметры ЭК в форме Вейерштрасса.
- Большой простой порядок – большое простое число.

Таблица 1. Исходные данные для выполнения лабораторной работы

№	Базовое поле	Параметры кривой в форме Вейерштрасса a и b	Большой простой порядок
1	$\mathbf{GF}(p_{192})$, 6277101735386680763835789423207666416083908700390324961279	a=-3 b=64210519 e59c80e7 0fa7e9ab 72243049 feb8deec c146b9b1	$\mathbf{GF}(p_{192})$, 6277101735386680763835789423176059013767194773182842284081
2	$\mathbf{GF}(p_{224})$, 26959946667150639794667015087019630673557916260026308143510066298881	a=-3 b=b4050a85 0c04b3ab f5413256 5044b0b7 d7bfd8ba 270b3943 2355ffb4	$\mathbf{GF}(p_{224})$, 26959946667150639794670150870196259404578077144243917216827223680 61
3	$\mathbf{GF}(p_{256})$, 1157920892103562487626974469494075735300861434152903141955336313088670978539951	a=-3 b=5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b	$\mathbf{GF}(p_{256})$, 1157920892103562487626974469494075735299969552241357603424222590610685120443 69
4	$\mathbf{GF}(p_{384})$, 3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311 2319	a=-3 b=b3312fa7 e23ee7e4 988e056b e3f82d19 181d9c6e fe814112 0314088f 5013875a c656398d 8a2ed19d 2a85c8ed d3ec2aef	$\mathbf{GF}(p_{384})$, 3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
5	$\mathbf{GF}(p_{521})$, 6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151	a=-3 b=051 953eb961 8e1c9a1f 929a21a0 b68540ee a2da725b 99b315f3 b8b48991 8ef109e1 56193951 ec7e937b 1652c0bd 3bb1bf07 3573df88 3d2c34f1 ef451fd4 6b503f00	$\mathbf{GF}(p_{521})$, 6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
6	$\mathbf{GF}(2^{163})$, $p(t)=t^{163}+t^7+t^6+t^3+1$	a=1 b=2 0a601907 b8c953ca 1481eb10 512f7874 4a3205fd	$\mathbf{GF}(p_{163})$, 5846006549323611672814742442876390689256843201587
7	$\mathbf{GF}(2^{233})$, $p(t)=t^{233}+t^4+1$	a=0 b=066 647ede6c 332c7f8c 0923bb58 213b333b 20e9ce42 81fe115f 7d8f90ad	$\mathbf{GF}(p_{233})$, 6901746346790563787434755862277025555839812737345013555379383634485463
8	$\mathbf{GF}(2^{283})$, $p(t)=t^{283}+t^{12}+t^7+t^5+1$	a=0 b=27b680a c8b8596d a5a4af8a 19a0303f ca97fd76 45309fa2 a581485a f6263e31 3b79a2f5	$\mathbf{GF}(p_{283})$, 7770675568902916283677847627294075626569625924376904889109196526770044277787378692871
9	$\mathbf{GF}(2^{409})$, $p(t)=t^{409}+t^{87}+1$	a=0 b=021a5c2 c8ee9feb 5c4b9a75 3b7b476b 7fd6422e f1f3dd67 4761fa99 d6ac27c8 a9a197b2 72822f6c d57a55aa 4f50ae31 7b13545f	$\mathbf{GF}(p_{409})$, 6610559687902485989519153080327710398284046829642812192846487983041577748273748052081437237621791109659798672883665675267 71

10	$\mathbf{GF}(2^{571})$, $p(t)=t^{571}+t^{10}+t^5+t^2+1$	a=0 b=2f40e7e 2221f295 de297117 b7f3d62f 5c6a97ff cb8ceff1 cd6ba8ce 4a9a18ad 84ffabbd 8efa5933 2be7ad67 56a66e29 4afd185a 78ff12aa 520e4de7 39baca0c 7ffeff7f 2955727a	3864537523017258344695351890931987344298927329706434998657235251451519142289560424536143999389415773083133881121926944486246872462816813070234528288303332411393191105285703

В качестве входных данных, см. таблицу 2, используется:

- Базовое поле.
- Параметры ЭК в форме Хессе.
- Большой простой порядок – большое простое число.

Таблица 2. Исходные данные для выполнения лабораторной работы

№	Базовое поле	Параметр кривой в форме Хессе D	Большой простой порядок
1	$\mathbf{GF}(p_{160})$, $p=2^{160}-2933$	D=945639186043697550302587435415597619883075636292	$\mathbf{GF}(p_{160})$, 620595175087432237029165529381611169224913337 $\#E_H(p_{160})$=3*5*157*6205951750874322370291655293816111692249133337
2	$\mathbf{GF}(p_{224})$, $p=2^{224}-2^{10}-1$	D=25840187014857916932759133078916563544400020237401312879815735566345	$\mathbf{GF}(p_{224})$, 620595175087432237029165529381611169224913337 $\#E_H(p_{160})$=3*23*390723864741313620212565436043762777712823516673432244734573782061

Для каждой кривой, приведенной в таблице 1 и 2, согласно таблице 3, где указано какие представления, и формы кривых следует исследовать.

Таблица 3. Варианты заданий для индивидуальных заданий

№	Базовое поле	Форма кривой	Представление
1	$\mathbf{GF}(p)$	Вейерштрасса	Стандартное проективное
2	$\mathbf{GF}(p)$	Вейерштрасса	Проективное Якоби
3	$\mathbf{GF}(p)$	Вейерштрасса	Проективное Лопеса-Дахаба
4	$\mathbf{GF}(p)$	Хессе	Аффинное
5	$\mathbf{GF}(p)$	Хессе	Стандартное проективное
6	$\mathbf{GF}(p)$	Хессе	Расширенное проективное
7	$\mathbf{GF}(p)$	Скрученное Хессе	Стандартное проективное
8	$\mathbf{GF}(p)$	Скрученное Хессе	Расширенное проективное
9	$\mathbf{GF}(p)$	Эдвардса	Аффинное
10	$\mathbf{GF}(p)$	Эдвардса	Стандартное проективное
11	$\mathbf{GF}(p)$	Скрученная Эдвардса	Аффинное

12	$\mathbf{GF}(p)$	Скрученная Эдвардса	Стандартное проективное
13	$\mathbf{GF}(p)$	Скрученная Эдвардса	Инвертированное проективное
14	$\mathbf{GF}(p)$	Скрученная Эдвардса	Расширенное стандартное проективное
15	$\mathbf{GF}(p)$	Якоби четвертой степени	Аффинное
16	$\mathbf{GF}(p)$	Якоби четвертой степени	Проективное Лопеса-Дахаба
17	$\mathbf{GF}(p)$	Якоби четвертой степени	Модифицированное проективное Лопеса-Дахаба
18	$\mathbf{GF}(p)$	Монтгомери	Аффинное
19	$\mathbf{GF}(p)$	Монтгомери	Стандартное проективное
20	$\mathbf{GF}(2^m)$	Вейерштрасса	Стандартное проективное
21	$\mathbf{GF}(2^m)$	Вейерштрасса	Проективное Лопеса-Дахаба
22	$\mathbf{GF}(2^m)$	Эдвардса	Аффинное
23	$\mathbf{GF}(2^m)$	Эдвардса	Стандартное проективное
24	$\mathbf{GF}(2^m)$	Хессе	Аффинное
25	$\mathbf{GF}(2^m)$	Хессе	Проективное

В таблице 3 приведены варианты, для выполнения лабораторной работы согласно номеру по списку в журнале.

Таблица 4. Индивидуальные задания по использованию кривых.

№	Номер кривой из таблицы 1	Представления точек и формы кривых из таблицы 2
1	3, 6, 9	8, 16, 24
2	4, 7, 10	9, 17, 25
3	5, 8, 1	10, 18, 1
4	6, 9, 2	11, 19, 2
5	7, 10, 3	12, 20, 3
6	8, 1, 4	13, 21, 4
7	9, 2, 5	14, 22, 5
8	10, 3, 6	15, 23, 6
9	1, 4, 7	16, 24, 7
10	2, 5, 8	17, 25, 8

Выход

В результате выполнения лабораторной работы, каждый студен обязан обладать:

- Исходным кодом программы в Wolfram Mathematica.
- Грамотно оформленным отчетом, который содержит, как исходные данные, так и результаты работы программы.

Для каждой кривой из задания следует выполнить базовое задание – реализовать основные алгоритмы для работы с элементами поля и точками ЭК в Аффинном представлении, и представлении, указанном в задании:

- Сформировать 5 случайных точек. Как правило формирование случайных точек происходит в аффинном представлении с последующим переводом в необходимое представление.
- Вычислить сумму (различных точек) 5 различных пар сформированных точек. Проверить на принадлежность кривой точки-суммы. Формулы следует брать из раздела Теоретические сведения и [3].
- Вычислить сумму (одинаковых точек - удвоить) 5 различных сформированных точек. Проверить на принадлежность кривой точки-суммы. Формулы следует брать из раздела Теоретические сведения и [3].
- Вычислить отрицательную точку для 5 различных сформированных точек. Проверить на принадлежность кривой точки-отрицания. Формулы следует брать из раздела Теоретические сведения и [3].
- Вычислить скалярное произведение 5 сформированных точек для случайных скалярных множителей, принадлежащих полю порядка. Проверить на принадлежность кривой точек. Алгоритмы следует брать из раздела Теоретические сведения.
- Сформировать 5 случайных точек большого простого порядка. Проверить на принадлежность кривой точек. Алгоритмы следует брать из раздела Теоретические сведения.

После выполнения базового задания, следует выполнить расширенное задание:

- Преобразовать (при соответствии базовых полей) кривые, заданные в форме Вейерштрасса в изоморфные им и наоборот, согласно задания, см. таблицу 3. Основной теоретический материал представлен в разделе Теоретические сведения.
- Для каждой полученной кривой в заданной форме и представлении точек (результат проверить посредством вычислений в Аффинных координатах в форме Вейерштрасса):
    - Реализовать преобразование точек из Аффинного в заданное, и наоборот.
    - Сложить.
    - Удвоить.
    - Вычислить отрицательную точку.
    - Скалярно умножить.

Требования

Исходный код следует грамотно структурировать используя процедуры и функции, а также хорошо документировать, используя возможности среды программирования Wolfram Mathematica.

Теоретические сведения

Во время выполнения лабораторной работы, следует ознакомиться с приведенным ниже теоретическим материалом, а также формулами для сложения и удвоения точек ЭК, приведенных в [3].

Алгоритмы операций в полях

При разработке программы, потребуются различные алгоритмы для операций над элементами полей. Ниже приведем наиболее необходимые.

Программу следует разбить на 2 части:

- Работа с полями $\mathbf{GF}(p)$.
- Работа с полями $\mathbf{GF}(2^m)$.

Операции над элементами поля $\mathbf{GF}(p)$

Вычисление последовательности Лукаса

Пусть P и Q отличные от нуля целые. Последовательность Лукаса U_k и V_k для P и Q задается следующим образом:

$U_0 = 0$, $U_1 = 1$ и $U_k = PU_{k-1} - QU_{k-2}$ для $k \geq 2$,

$V_0 = 2$, $V_1 = P$ и $V_k = PV_{k-1} - QV_{k-2}$ для $k \geq 2$.

Данная рекурсия является приемлемой для вычисления U_k и V_k для небольших значений k. Для больших значений k, для вычисления U_k и V_k следует использовать следующий алгоритм.

Алгоритм. Вычисление последовательности Лукаса.

Вход: нечетное простое число p, отличные от нуля целые P и Q, и положительное число k.

Выход: $U_k \bmod p$ и $V_k \bmod p$.

1. Установить $\Delta \leftarrow P^2 - 4Q$.

2. Пусть $k = k_r k_{r-1} \ldots k_1 k_0$ является двоичным представлением числа k, где старший бит k_r числа k равен 1.

3. Установить $U \leftarrow 1$, $V \leftarrow P$.

4. For i from $r-1$ downto 0 do

4.1. Установить $(U,V) \leftarrow (UV \bmod p, (V^2 + \Delta U^2)/2 \bmod p)$.

4.2. If $k_r = 1$ then set $(U,V) \leftarrow ((PU+V)/2 \bmod p, (PV + \Delta U)/2 \bmod p)$.

5. Return (U,V).

Приведенное в алгоритме деление на 2 может быть эффективно реализовано посредством сдвига вправо двоичного представления.

Вычисление квадратного корня

Следующий алгоритм реализует эффективный метод решения квадратного уравнения вида $\beta^2 \equiv \alpha \pmod p$ относительно β над полем $\mathbf{GF}(p)$, либо доказать, что решение не существует.

Алгоритм. Вычисление квадратного корня целого числа α по модулю p относительно $\beta \neq 0$.

Вход: нечетное простое число p и целое число α, такое что $0 < \alpha < p$.

Выход: число β принадлежащее полю $\mathbf{GF}(p)$, если существует квадратный корень.

Switch (p)

Case I. $p \equiv 3 \pmod 4$, $p = 4k+3$.

1. Return $(\beta = \alpha^{k+1} \pmod p)$.

Case II. $p \equiv 5 \pmod 8$, $p = 8k+5$.

1. Compute $\gamma = (2\alpha)^k \bmod p$.

2. Compute $i = 2\alpha\gamma^2 \bmod p$.

3. Return $(\beta = \alpha\gamma(i-1) \bmod p)$.

Case III. $p \equiv 1 (\mathrm{mod}\, 4)$, $p = 4k+1$.

1. Set $Q \leftarrow \alpha$.

2. Generate random P, $0 < P < p$.

3. Compute the Lucas sequence elements with indexes $2k+1$: $U = U_{2k+1} (\mathrm{mod}\, p)$, $V = V_{2k+1} (\mathrm{mod}\, p)$.

4. If $U = 0$ then Return $(\beta = V/2)$.

5. If $V = 0$ then Return ("no square roots exist").

6. Go to Step 2.

Операции над элементами поля $\mathbf{GF}(2^m)$

Решение квадратного уравнения

Следующий алгоритм реализует эффективный метод решения квадратного уравнения вида $z^2 + z \equiv \beta$ относительно z над полем $\mathbf{GF}(2^m)$, либо доказать, что решение не существует.

Если β является элементом поля $\mathbf{GF}(2^m)$, тога уравнение:

$$z^2 + z \equiv \beta$$

имеет $2 - 2T$ решений над полем $\mathbf{GF}(2^m)$, где $T = Tr(\beta)$. Таким образом, может существовать либо 0 либо 2 решения. Если z является первым решением, тогда другое решение является $z+1$. В случае $\beta = 0$, решениями являются 0 и 1.

Алгоритм. Алгоритм решения квадратного уравнения $z^2 + z \equiv \beta$ в поле.

Вход: элемент $\beta \neq 0$ поля $\mathbf{GF}(2^m)$ в полиномиальном представлении.

Выход: элемент z поля $\mathbf{GF}(2^m)$, такой что $z^2 + z \equiv \beta$, если такой элемент существует.

Switch (m)

I. Число m является нечетным.

1. Return $(z = half - Tr(\beta))$.

II. Число m является четным.

1. Choose random $\rho \in \mathbf{GF}(2^m)$.

2. Set $z \leftarrow 0$, $w \leftarrow \rho$.

3. For i from 1 to $m-1$ do

3.1. Set $z \leftarrow z^2 + w^2 \beta$.

3.2. Set $w \leftarrow w^2 + \rho$.

4. If $w = 0$ then go to Step 1

5. Return z.

Если предполагается, что алгоритм будет выполняться несколько раз для одного и того же поля, и имеется свободная память, то тогда можно предвычислить ρ и значения w.

Trace (след)

Если α является элементом $\mathbf{GF}(2^m)$, тог следом элемента поля α является:

$Tr(\alpha) = \alpha + \alpha^2 + \alpha^{2^2} + \cdots + \alpha^{2^{m-1}}$.

Значение $Tr(\alpha)$ является 0 для половины элементов поля $\mathbf{GF}(2^m)$ и равно 1 для остальной половины.

Алгоритм. Вычисления следа элемента α поля $\mathbf{GF}(2^m)$.

Вход: элемент α поля $\mathbf{GF}(2^m)$ в полиномиальном представлении.

Выход: след $Tr(\alpha)$ элемент α поля $\mathbf{GF}(2^m)$.

1. Set $T \leftarrow \alpha$.

2. For i from 1 to $m-1$ do

2.1. $T \leftarrow T^2 + \alpha$.

3. Return (T).

Half-Trace (полуслед)

Если m является нечетным, тогда полуслед элемента α поля $\mathbf{GF}(2^m)$ является:

$HfTr(\alpha) = \alpha + \alpha^{2^2} + \cdots + \alpha^{2^{m-1}}$.

Алгоритм. Вычисления полуследа элемента α поля $\mathbf{GF}(2^m)$.

Вход: элемент α поля $\mathbf{GF}(2^m)$ в полиномиальном представлении.

Выход: полуслед $HfTr(\alpha)$ элемент α поля $\mathbf{GF}(2^m)$.

1. Set $H \leftarrow \alpha$.

2. For i from 1 to $(m-1)/2$ do

2.1. $H \leftarrow H^2$.

2.2. $H \leftarrow H^2 + \alpha$.

3. Return (H).

Вычисление квадратного корня

Для вычисления квадратного корня α над полем $\mathbf{GF}(2^m)$ для $\alpha^2 \equiv \beta$:

$\alpha = \alpha_{m-1} t^{m-1} + \cdots + \alpha_2 t^2 + \alpha_1 t + \alpha_0$,

тогда

$\beta \equiv \alpha^2 = \alpha_{m-1} t^{2m-2} + \cdots + \alpha_2 t^4 + \alpha_1 t^2 + \alpha_0 \bmod p(t)$.

для вычисления $\sqrt{\beta} \equiv \alpha$, необходимо для β выполнить возведение в квадрат $m-1$ раз.

Алгоритмы операций в группе точек ЭК

При разработке программы, потребуются различные алгоритмы для операций над точками ЭК. Ниже приведем наиболее необходимые.

Программу следует разбить на 2 части:

- Работа с полями $\mathbf{GF}(p)$.
- Работа с полями $\mathbf{GF}(2^m)$.

Операции над точками ЭК над полем $\mathbf{GF}(p)$

Поиск случайной точки

Следующий алгоритм реализует эффективный метод поиска случайной точки, отличной от точки на бесконечности, для ЭК над полем $\mathbf{GF}(p)$.

Вход: простое число $p>3$ и параметры кривой a и b в форме Вейерштрасса E над полем $\mathbf{GF}(p)$.

Выход: случайно сформированная точка $\mathbf{P}$, отличная от O на кривой E.

1. Выбор случайного x, такого, что $0 \le x < p$.

2. Вычислить $\alpha \leftarrow x^3 + ax + b \bmod p$.

3. Если $\alpha = 0$ тогда $\mathbf{P} = (x, 0)$ и переход к п.8.

4. Решить квадратное уравнение $\beta^2 \equiv \alpha (\bmod p)$ относительно β, либо доказать, что решение не существует.

5. Если решение не существует, то переход к п.1.

6. Решением уравнения $\beta^2 \equiv \alpha (\bmod p)$ будет $0 \le \beta < p$.

7. Генерация случайного бита μ и установка $y \leftarrow (-1)^{\mu} \beta$.

8. Return $\mathbf{P} = (x, y)$.

Сложение точек

Следующий алгоритм реализует эффективный метод сложения точек $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$ в аффинных координатах, отличных друг от друга, для ЭК в форме Эдвардса $x^2 + y^2 = c^2(1 + dx^2y^2)$ над полем $\mathbf{GF}(p)$:

$$x_3 = (x_1y_2 + y_1x_2)/c(1 + dx_1x_2y_1y_2),$$
$$y_3 = (y_1y_2 - x_1x_2)/c(1 - dx_1x_2y_1y_2).$$

Следующий алгоритм реализует эффективный метод сложения точек $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$ в аффинных координатах, отличных друг от друга, для ЭК в форме Хессе $x^3 + y^3 + 1 = 3dxy$ над полем $\mathbf{GF}(p)$:

$$x_3 = (y_1^2x_2 - y_2^2x_1)/(x_2y_2 - x_1y_1),$$
$$y_3 = (x_1^2y_2 - x_2^2y_1)/(x_2y_2 - x_1y_1).$$

Следующий алгоритм реализует эффективный метод сложения точек $P_1 = (s_1, c_1, d_1)$ и $P_2 = (s_2, c_2, d_2)$ в аффинных координатах, отличных друг от друга, для ЭК в форме Якоби $s^2 + c^2 = 1$, $as^2 + d^2 = 1$ над полем $\mathbf{GF}(p)$.

$$s_3 = (c_2s_1d_2 + d_1s_2c_1)/(c_2^2 + (d_1s_1)^2),$$
$$c_3 = (c_2c_1 - d_1s_2s_1d_2)/(c_2^2 + (d_1s_1)^2),$$
$$d_3 = (d_1d_2 - as_1s_2c_1c_2)/(c_2^2 + (d_1s_1)^2).$$

Следующий алгоритм реализует эффективный метод сложения точек $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$ в аффинных координатах, отличных друг от друга, для ЭК в форме Якоби квартик $y^2 = x^4 + 2ax^2 + 1$ над полем $\mathbf{GF}(p)$:

$$x_3 = (x_1y_2 + y_1x_2)/(1 - (x_1x_2)^2),$$

$$y_3 = \left(\left(1+(x_1x_2)^2\right)(y_1y_2+2ax_1x_2)+2x_1x_2\left(x_1^2+x_2^2\right)\right)/\left(1-(x_1x_2)^2\right)^2.$$

Следующий алгоритм реализует эффективный метод сложения точек $P_1=(x_1,y_1)$ и $P_2=(x_2,y_2)$ в аффинных координатах, отличных друг от друга, для ЭК в форме Монтгомери $by^2=x^3+ax^2+x$ над полем $\mathbf{GF}(p)$:

$$x_3 = b(y_2-y_1)^2/(x_2-x_1)^2-a-x_1-x_2,$$

$$y_3 = (2x_1+x_2+a)(y_2-y_1)/(x_2-x_1)-b(y_2-y_1)^3/(x_2-x_1)^3-y_1.$$

Следующий алгоритм реализует эффективный метод сложения точек $P_1=(x_1,y_1)$ и $P_2=(x_2,y_2)$ в аффинных координатах, отличных друг от друга, для ЭК в форме Монтгомери $by^2=x^3+ax^2+x$ над полем $\mathbf{GF}(p)$:

$$x_3 = b(y_2-y_1)^2/(x_2-x_1)^2-a-x_1-x_2;$$

$$y_3 = (2x_1+x_2+a)(y_2-y_1)/(x_2-x_1)-b(y_2-y_1)^3/(x_2-x_1)^3-y_1.$$

Следующий алгоритм реализует эффективный метод сложения точек $P_1=(x_1,y_1)$ и $P_2=(x_2,y_2)$ в аффинных координатах, отличных друг от друга, для ЭК в сокращенной форме Вейерштрасса $y^2=x^3+ax^2+b$ над полем $\mathbf{GF}(p)$:

$$x_3 = (y_2-y_1)^2/(x_2-x_1)^2-x_1-x_2,$$

$$y_3 = (2x_1+x_2)(y_2-y_1)/(x_2-x_1)-(y_2-y_1)^3/(x_2-x_1)^3-y_1.$$

Следующий алгоритм реализует эффективный метод сложения точек $P_1=(x_1,y_1)$ и $P_2=(x_2,y_2)$ в аффинных координатах, отличных друг от друга, для ЭК в свернутой форме Эдвардса $ax^2+y^2=1+dx^2y^2$ над полем $\mathbf{GF}(p)$:

$$x_3 = (x_1y_2+y_1x_2)/(1+dx_1x_2y_1y_2),$$

$$y_3 = (y_1y_2-ax_1x_2)/(1-dx_1x_2y_1y_2).$$

Следующий алгоритм реализует эффективный метод сложения точек $P_1=(x_1,y_1)$ и $P_2=(x_2,y_2)$ в аффинных координатах, отличных друг от друга, для ЭК в свернутой форме Хессе $ax^3+y^3+1=dxy$ над полем $\mathbf{GF}(p)$:

$$x_3 = \left(x_1-y_1^2x_2y_2\right)/\left(ax_1y_1x_2^2-y_2\right),$$

$$y_3 = \left(y_1y_2^2-ax_1^2x_2\right)/\left(ax_1y_1x_2^2-y_2\right).$$

Следующий алгоритм реализует эффективный метод сложения точек $P_1=(x_1,y_1)$ и $P_2=(x_2,y_2)$ в аффинных координатах, отличных друг от друга, для ЭК в форме Доче-Икарт-Кохеля $y^2=x^3+ax^2+16ax$, ориентированной на удвоение над полем $\mathbf{GF}(p)$:

$$x_3 = \left(-x_1^3+(x_2-3a)x_1^2+\left(x_2^2+6ax_2\right)x_1+\left(y_1^2-2y_2y_1+\left(-x_2^3-3ax_2^2+y_2^2\right)\right)\right)/\left(x_1^2-2x_2x_1+x_2^2\right),$$

$$y_3 = \frac{\begin{array}{c}\left(-y_1+2y_2\right)x_1^3+\left(-3ay_1+\left(-3y_2x_2+3ay_2\right)\right)x_1^2+\left(\left(3x_2^2+6ax_2\right)y_1-6ay_2x_2\right)x_1+\\ \left(y_1^3-3y_2y_1^2+\left(-2x_2^3-3ax_2^2+3y_2^2\right)y_1+\left(y_2x_2^3+3ay_2x_2^2-y_2^3\right)\right)\end{array}}{\left(-x_1^3+3x_2x_1^2-3x_2^2x_1+x_2^3\right)}.$$

Следующий алгоритм реализует эффективный метод сложения точек $P_1=(x_1,y_1)$ и $P_2=(x_2,y_2)$ в аффинных координатах, отличных друг от друга, для ЭК в форме Доче-Икарт-Кохеля $y^2=x^3+3a(x+1)^2$, ориентированной на утроение над полем $\mathbf{GF}(p)$:

$$x_3 = \left(-x_1^3+(x_2-a)x_1^2+\left(x_2^2+2ax_2\right)x_1+\left(y_1^2-2y_2y_1+\left(-x_2^3-ax_2^2+y_2^2\right)\right)\right)/\left(x_1^2-2x_2x_1+x_2^2\right);$$

$$y_3 = \frac{\begin{array}{c}(-y_1+2y_2)x_1^3+(-ay_1+(-3y_2x_2+ay_2))x_1^2+((3x_2^2+2ax_2)y_1-2ay_2x_2)x_1+\\ (y_1^3-3y_2y_1^2+(-2x_2^3-ax_2^2+3y_2^2)y_1+(y_2x_2^3+ay_2x_2^2-y_2^3))\end{array}}{(-x_1^3+3x_2x_1^2-3x_2^2x_1+x_2^3)}.$$

Вычитание точек

Вычитание точек $P_1=(x_1,y_1)$ и $P_2=(x_2,y_2)$ в аффинных координатах производится посредством вычисления точки $-P_2$ с последующим ее сложением $P_1+(-P_2)$. Данный подход применим для всех форм кривых и видов представлений точек.

Ниже приведем формулы для отрицания точек.

Для ЭК в форме Эдвардса $x^2+y^2=c^2(1+dx^2y^2)$ в аффинных координатах:

$$-(x_1,y_1)=(-x_1,y_1).$$

Для ЭК в форме Хессе $x^3+y^3+1=3dxy$ в аффинных координатах:

$$-(x_1,y_1)=(y_1,x_1).$$

Для ЭК в форме Якоби $s^2+c^2=1$, $as^2+d^2=1$ в аффинных координатах:

$$-(s_1;c_1;d_1)=(-s_1;c_1;d_1).$$

Для ЭК в форме Якоби квартик $y^2=x^4+2ax^2+1$ в аффинных координатах:

$$-(x_1;y_1)=(-x_1;y_1).$$

Для ЭК в форме Монтгомери $by^2=x^3+ax^2+x$ в аффинных координатах:

$$-(x_1;y_1)=(x_1;-y_1).$$

Для ЭК в сокращенной форме Вейерштрасса $y^2=x^3+ax^2+b$ в аффинных координатах:

$$-(x_1;y_1)=(x_1;-y_1).$$

Для ЭК в свернутой форме Эдвардса $ax^2+y^2=1+dx^2y^2$ в аффинных координатах:

$$-(x_1;y_1)=(-x_1;y_1).$$

Для ЭК в свернутой форме Хессе $ax^3+y^3+1=dxy$ в аффинных координатах:

$$-(x_1;y_1)=(x_1/y_1,1/y_1).$$

Для ЭК в форме ориентированной на удвоения Доче-Икарт-Кохеля $y^2=x^3+ax^2+16ax$ в аффинных координатах:

$$-(x_1,y_1)=(x_1,-y_1).$$

Для ЭК в форме ориентированной на утроения Доче-Икарт-Кохеля $y^2=x^3+3a(x+1)^2$ в аффинных координатах:

$$-(x_1,y_1)=(x_1,-y_1).$$

Удвоение точек

Следующий алгоритм реализует эффективный метод удвоения $P_3=2P_1$ точек $P_1=(x_1,y_1)$ аффинных координатах, для ЭК в форме Эдвардса $x^2+y^2=c^2(1+dx^2y^2)$ над полем $\mathbf{GF}(p)$:

$$x_3=(x_1y_1+y_1x_1)/(c(1+dx_1x_1y_1y_1)),$$
$$y_3=(y_1y_1-x_1x_1)/(c(1-dx_1x_1y_1y_1)).$$

Следующий алгоритм реализует эффективный метод удвоения $P_3 = 2P_1$ точек $P_1 = (x_1, y_1)$ аффинных координатах, для ЭК в форме Хессе $x^3 + y^3 + 1 = 3dxy$ над полем $\mathbf{GF}(p)$:

$$x_3 = y_1(1 - x_1^3)/(x_1^3 - y_1^3);$$
$$y_3 = x_1(y_1^3 - 1)/(x_1^3 - y_1^3).$$

Следующий алгоритм реализует эффективный метод удвоения $P_3 = 2P_1$ точек $P_1 = (s_1, c_1, d_1)$ аффинных координатах, для ЭК в форме Якоби $s^2 + c^2 = 1$, $as^2 + d^2 = 1$ над полем $\mathbf{GF}(p)$:

$$s_3 = (c_1 s_1 d_1 + d_1 s_1 c_1)/(c_1^2 + (d_1 s_1)^2),$$
$$c_3 = (c_1 c_1 - d_1 s_1 s_1 d_1)/(c_1^2 + (d_1 s_1)^2),$$
$$d_3 = (d_1 d_1 - a s_1 s_1 c_1 c_1)/(c_1^2 + (d_1 s_1)^2).$$

Следующий алгоритм реализует эффективный метод удвоения $P_3 = 2P_1$ точек $P_1 = (x_1, y_1)$ аффинных координатах, для ЭК в форме Якоби квартик $y^2 = x^4 + 2ax^2 + 1$ над полем $\mathbf{GF}(p)$:

$$x_3 = (x_1 y_1 + y_1 x_1)/(1 - (x_1 x_1)^2),$$
$$y_3 = ((1 + (x_1 x_1)^2)(y_1 y_1 + 2a x_1 x_1) + 2x_1 x_1 (x_1^2 + x_1^2))/(1 - (x_1 x_1)^2)^2.$$

Следующий алгоритм реализует эффективный метод удвоения $P_3 = 2P_1$ точек $P_1 = (x_1, y_1)$ аффинных координатах, для ЭК в форме Монтгомери $by^2 = x^3 + ax^2 + x$ над полем $\mathbf{GF}(p)$:

$$x_3 = b(3x_1^2 + 2ax_1 + 1)^2 / (2by_1)^2 - a - x_1 - x_2,$$
$$y_3 = (2x_1 + x_1 + a)(3x_1^2 + 2ax_1 + 1)/(2by_1) - b(3x_1^2 + 2ax_1 + 1)^3 / (2by_1)^3 - y_1.$$

Следующий алгоритм реализует эффективный метод удвоения $P_3 = 2P_1$ точек $P_1 = (x_1, y_1)$ аффинных координатах, для ЭК в краткой форме Вейерштрасса $y^2 = x^3 + ax^2 + b$ над полем $\mathbf{GF}(p)$:

$$x_3 = (3x_1^2 + a)^2 / (2y_1)^2 - x_1 - x_1,$$
$$y_3 = (2x_1 + x_1)(3x_1^2 + a)/(2y_1) - (3x_1^2 + a)^3 / (2y_1)^3 - y_1.$$

Следующий алгоритм реализует эффективный метод удвоения $P_3 = 2P_1$ точек $P_1 = (x_1, y_1)$ аффинных координатах, для ЭК в форме Эдвардса $ax^2 + y^2 = 1 + dx^2 y^2$ над полем $\mathbf{GF}(p)$:

$$x_3 = (x_1 y_1 + y_1 x_1)/(1 + d x_1 x_1 y_1 y_1),$$
$$y_3 = (y_1 y_1 - a x_1 x_1)/(1 - d x_1 x_1 y_1 y_1).$$

Следующий алгоритм реализует эффективный метод удвоения $P_3 = 2P_1$ точек $P_1 = (x_1, y_1)$ аффинных координатах, для ЭК в свернутом виде Хессе $ax^3 + y^3 + 1 = dxy$ над полем $\mathbf{GF}(p)$:

$$x_3 = (x_1 - y_1^3 x_1)/(a y_1 x_1^3 - y_1),$$
$$y_3 = (y_1^3 - a x_1^3)/(a y_1 x_1^3 - y_1).$$

Следующий алгоритм реализует эффективный метод удвоения $P_3 = 2P_1$ точек $P_1 = (x_1, y_1)$ аффинных координатах, для ЭК в форме Доче-Икарт-Кохеля ориентированной на удвоение $y^2 = x^3 + ax^2 + 16ax$ над полем $\mathbf{GF}(p)$:

$$x_3 = x_1^4 / (4y_1^2) - 8a/(y_1^2 x_1^2) + 64a^2 / y_1^2 ;$$

$$y_3 = x_1^6 / (8y_1^3) + x_1^4 (-a^2 + 40a) / (4y_1^3) + x_1^2 (ay_1^2 + (16a^3 - 640a^2)) / (4y_1^3) + (-4a^2 y_1^2 - 512a^3) / y_1^3$$

Следующий алгоритм реализует эффективный метод удвоения $P_3 = 2P_1$ точек $P_1 = (x_1, y_1)$ аффинных координатах, для ЭК в форме Доче-Икарт-Кохеля ориентированной на утроения $y^2 = x^3 + 3a(x+1)^2$ над полем $\mathbf{GF}(p)$:

$$x_3 = 9x_1^4 / 4y_1^2 + 9ax_1^3 / y_1^2 + (9a^2 / y_1^2 + 9a / y_1^2) x_1^2 + (18a^2 / y_1^2 - 2) x_1 + (9a^2 / y_1^2 - 3a);$$

$$y_3 = -27x_1^6 / 8y_1^3 - 81ax_1^5 / 4y_1^3 + x_1^4 (-81a^2 / 2y_1^3 - 81a / 4y_1^3) + x_1^3 (-27 / y_1^3 a^3 - 81 / y_1^3 a^2 + 9 / 2y_1) + x_1^2 (-81 / y_1^3 a^3 - 81a^2 / 2y_1^3 + 27a / 2y_1) + x_1 (-81a^3 / y_1^3 + 9a^2 / y_1 + 9a / y_1) + (-27a^3 / y_1^3 + 9a^2 / y_1 - y_1)$$

Операции над точками над полем $\mathbf{GF}(2^m)$

Поиск случайной точки

Следующий алгоритм реализует эффективный метод поиска случайной точки, отличной от точки на бесконечности, для ЭК над полем $\mathbf{GF}(2^m)$.

Алгоритм. Поиск случайно точки ЭК в форме Вейерштрасса над полем $\mathbf{GF}(2^m)$.

Вход: простое число $p > 3$ и параметры кривой a и b в форме Вейерштрасса E над полем $\mathbf{GF}(2^m)$.

Выход: случайно сформированная точка $\mathbf{P}$, отличная от O на кривой E.

1. Выбор случайного x из $\mathbf{GF}(2^m)$.

2. Если $x = 0$ тогда $\mathbf{P} = (0, b^{2^{m-1}})$ и переход к п.9.

3. Вычислить $\alpha \leftarrow x^3 + ax^2 + b$.

4. Если $\alpha = 0$ тогда $\mathbf{P} = (x, 0)$ и переход к п.10.

5. Вычислить $\beta \leftarrow x^{-2}\alpha$.

6. Решить квадратное уравнение $z^2 + z \equiv \beta$ относительно z, либо доказать, что решение не существует.

7. Если решение не существует, то переход к п.1.

8. Решение уравнения $z^2 + z \equiv \beta$ составит $z \in \mathbf{GF}(2^m)$.

9. Генерация случайного бита μ и установить $y \leftarrow (z + \mu)x$.

10. Return $\mathbf{P} = (x, y)$.

Сложение точек

Следующий алгоритм реализует эффективный метод сложения точек $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$ в аффинных координатах, отличных друг от друга, для ЭК в двоичной форме Эдвардса $d_1(x+y) + d_2(x^2 + y^2) = (x + x^2)(y + y^2)$ над полем $\mathbf{GF}(2^m)$:

$$x_3 = (d_1(x_1 + x_2) + d_2(x_1 + y_1)(x_1 + y_2) + (x_1 + x_1^2)(x_2(y_1 + y_2 + 1) + y_1 y_2)) / (d_1 + (x_1 + x_1^2)(x_2 + y_2)),$$

$$y_3 = \left(d_1(y_1+y_2)+d_2(x_1+y_1)(x_1+y_2)+\left(y_1+y_1^2\right)\left(y_2(x_1+x_2+1)+x_1x_2\right)\right)/\left(d_1+\left(y_1+y_1^2\right)(x_2+y_2)\right).$$

Следующий алгоритм реализует эффективный метод сложения точек $P_1=(x_1,y_1)$ и $P_2=(x_2,y_2)$ в аффинных координатах, отличных друг от друга, для ЭК в форме Хессе $x^3+y^3+1=3dxy$ над полем $\mathbf{GF}(2^m)$:

$$x_3 = \left(y_1^2x_2-y_2^2x_1\right)/(x_2y_2-x_1y_1),$$
$$y_3 = \left(x_1^2y_2-x_2^2y_1\right)/(x_2y_2-x_1y_1).$$

Следующий алгоритм реализует эффективный метод сложения точек $P_1=(x_1,y_1)$ и $P_2=(x_2,y_2)$ в аффинных координатах, отличных друг от друга, для ЭК в сокращенной форме Вейерштрасса $y^2+xy=x^3+a_2x^2+a_6$ над полем $\mathbf{GF}(2^m)$:

$$x_3 = ((y_1+y_2)/(x_1+x_2))^2+(y_1+y_2)/(x_1+x_2)+x_1+x_2+a_2,$$
$$y_3 = ((y_1+y_2)/(x_1+x_2))^3+(x_2+a_2+1)(y_1+y_2)/(x_1+x_2)+x_1+x_2+a_2+y_1.$$

Вычитание точек

Вычитание точек $P_1=(x_1,y_1)$ и $P_2=(x_2,y_2)$ в аффинных координатах производится посредством вычисления точки $-P_2$ с последующим ее сложением $P_1+(-P_2)$. Данный подход применим для всех форм кривых и видов представлений точек.

Ниже приведем формулы для отрицания точек.

Для ЭК в двоичной форме Эдвардса $d_1(x+y)+d_2(x^2+y^2)=(x+x^2)(y+y^2)$ в аффинных координатах:

$$-(x_1,y_1)=(y_1,x_1).$$

Для ЭК в форме Хессе $x^3+y^3+1=3dxy$ в аффинных координатах:

$$-(x_1,y_1)=(y_1,x_1).$$

Для ЭК в краткой форме Вейерштрасса $y^2+xy=x^3+a_2x^2+a_6$ в аффинных координатах:

$$-(x_1,y_1)=(x_1,x_1+y_1).$$

Удвоение точек

Следующий алгоритм реализует эффективный метод удвоения $P_3=2P_1$ точек $P_1=(x_1,y_1)$ аффинных координатах, для ЭК в двоичной форме Эдвардса $d_1(x+y)+d_2(x^2+y^2)=(x+x^2)(y+y^2)$ над полем $\mathbf{GF}(2^m)$:

$$x_3 = \left(d_1(x_1+x_1)+d_2(x_1+y_1)(x_1+y_1)+\left(x_1+x_1^2\right)\left(x_1(y_1+y_1+1)+y_1y_1\right)\right)/\left(d_1+\left(x_1+x_1^2\right)(x_1+y_1)\right),$$
$$y_3 = \left(d_1(y_1+y_1)+d_2(x_1+y_1)(x_1+y_1)+\left(y_1+y_1^2\right)\left(y_1(x_1+x_1+1)+x_1x_1\right)\right)/\left(d_1+\left(y_1+y_1^2\right)(x_1+y_1)\right).$$

Следующий алгоритм реализует эффективный метод удвоения $P_3=2P_1$ точек $P_1=(x_1,y_1)$ аффинных координатах, для ЭК в форме Хессе $x^3+y^3+1=3dxy$ над полем $\mathbf{GF}(2^m)$:

$$x_3 = y_1\left(1-x_1^3\right)/\left(x_1^3-y_1^3\right),$$
$$y_3 = x_1\left(y_1^3-1\right)/\left(x_1^3-y_1^3\right).$$

Следующий алгоритм реализует эффективный метод удвоения $P_3 = 2P_1$ точек $P_1 = (x_1, y_1)$ аффинных координатах, для ЭК в краткой форме Вейерштрасса $y^2 + xy = x^3 + a_2 x^2 + a_6$ над полем $\mathbf{GF}(2^m)$:

$$x_3 = (x_1 + y_1/x_1)^2 + (x_1 + y_1/x_1) + a_2,$$

$$y_3 = (x_1 + y_1/x_1)^3 + (x_1 + a_2 + 1)(x_1 + y_1/x_1) + a_2 + y_1.$$

Проверка на принадлежность точки кривой

Проверка на принадлежность точки ЭК осуществляется посредством подстановки соответствующих координат точки в уравнение ЭК.

Скалярное умножение точек

Можно выделить класс универсальных алгоритмов скалярного умножения, которые не зависят от формы кривой и представления точек. Одним из таких, является распространенный алгоритм, основанный на сложении и удвоении точек.

Следующий алгоритм реализует эффективный метод скалярного умножения точек в различных координатах (как правило в смешанных), для ЭК над полем $\mathbf{GF}(q)$.

Алгоритм. Скалярное умножение методом сложения-удвоения слева-направо.

Вход: целое число $k = (k_{m-1}, \ldots, k_1, k_0)_2$ и точка ЭК P.

Выход: точка ЭК kP.

1. $Q \leftarrow \mathrm{O}$.

2. For i from $m-1$ downto 0 do

2.1. $Q \leftarrow 2Q$.

2.2. If $k_i = 1$ then $Q \leftarrow Q + P$

3. Return (Q).

Поиск точки большого простого порядка

Следующий алгоритм реализует эффективный метод поиска случайной точки большого простого порядка в аффинных координатах, для ЭК над полем $\mathbf{GF}(q)$.

Если порядок $\#E(\mathbf{GF}(q)) = u$ ЭК E является близким к простому, тогда ниже приведенный алгоритм позволит эффективно вычислить случайную точку на E, чей порядок будет является большим простым делителем r для $u = kr$.

Алгоритм. Поиск точки ЭК большого простого порядка

Вход: простое r, целое положительное k, не делящееся на r и ЭК E над полем $\mathbf{GF}(q)$.

Выход: если $\#E(\mathbf{GF}(q)) = kr$, точка G на ЭК E порядка r, в противном случае "wrong order."

1. Формирование случайной точки $P \neq \mathrm{O}$ на ЭК E.

2. Set $G \leftarrow kP$.

3. If $G = \mathrm{O}$ then go to Step 1.

4. Set $Q \leftarrow rG$.

5. If $Q \neq \mathrm{O}$ then Return ("wrong order").

6. Return (G).

Эквивалентность ЭК в форме Вейерштрасса

Уравнение ЭК в общей форме Вейерштрасса имеет вид [9]:

$$E_W(F_q): y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Для случая $\mathrm{char}(q) > 3$, уравнение может быть упрощено посредством замены переменных [9]:

1. $(x, y) \leftarrow \left(x, y - \frac{a_1}{2}x - \frac{a_3}{2}\right)$, в результате подстановки может быть получено уравнение $E_W(F_q): y^2 = x^3 + b_2x^2 + b_4x + b_6$. Дальнейшая замена переменных может еще более упростить уравнение.

2. $(x, y) \leftarrow \left(\frac{x - 3b_2}{36}, \frac{y}{216}\right)$, в результате подстановки может быть получено уравнение $E_W(F_q): y^2 = x^3 + ax + b$.

Эквивалентность между ЭК в форме Вейерштрасса и форме Якоби

Форма Якоби является еще одной параметризацией ЭК для $\mathrm{char}(q) > 3$. Представим ЭК как пересечение двух квартик в $\mathbf{P}^3$: $\left\{S^2 + C^2 = T^2, k^2S^2 + D^2 = T^2\right\}$, где точка представляется в виде (S, C, D, T). Пусть ЭК в форме Вейерштрасса представлена в виде $E_W(F_q): y^2 = x^3 + ax + b$, причем $\#E_W(F_q) \bmod 4 \equiv 0$. Применив стандартное преобразование Мебиуса, можем переместить три точки порядка 2 в $(0, 0)$, $(-1, 0)$ и $(-\lambda, 0)$, мы получим изоморфную кривую $E'_W(F_q): y^2 = x(x+1)(x+\lambda)$. Пусть $\lambda = 1 - k^2$, представим полученную ЭК в проективном виде: $E''_W(F_q): Y^2Z = X(X+Z)(X+\lambda Z)$, которая эквивалентна пересечению двух квартик:

$$E_W(F_q) \to E_{JQ}(F_q) \qquad E_{JQ}(F_q) \to E_W(F_q)$$

$$S = -2(X+Z)Y \qquad X = (D-T)\lambda$$

$$C = \lambda(-X^2 - Z^2 - 2XZ) + Y^2 \qquad Y = S\lambda k^2$$

$$T = \lambda(X^2 + Z^2 + 2XZ) + Y^2 \qquad Z = Ck^2 - D + T\lambda$$

$$D = \lambda Z^2 + Y^2 + 2XZ + (2-\lambda)X^2$$

Эквивалентность между ЭК в форме Вейерштрасса и форме Хессе

Проведенные в публикации [4] рассуждения показали существование линейной эквивалентности между представления ЭК в сокращенной форме Вейерштрасса и формой Хессе. Ниже приведем, часть рассуждений [4, 5].

Пусть представление ЭК в сокращенной форме Вейерштрасса в стандартных проективных координатах имеет вид: $E_W(F_q): Y^2Z = X^3 - aXZ^2 - bZ^3$ для $p \geq 5$. Точка на бесконечности $P_\infty = (0, 1, 0)$. Преобразование координат ЭК из проективного в аффинное представление имеет вид $\left(\frac{X}{Z}; \frac{Y}{Z}\right) \to (x; y)$.

ЭК в форме Хессе имеет вид: $E_H(F_q)$: $U^3 = V^3 + W^3 - 3mUVW$, $p \neq 3$, $m^3 \neq 1$. Точка на бесконечности $P_\infty = (1, -1, 0)$ и еще точки $P_\infty = (1, -\rho, 0)$, $P_\infty = (1, -\rho^2, 0)$, где $\rho = \frac{-1+\sqrt{-3}}{2}$ если существует корень из -3 в этом поле. Преобразование координат ЭК из проективного в аффинное представление имеет вид $\left(\frac{U}{W}; \frac{V}{W}\right) \to (u; v)$

Тогда, параметрически заданная ЭК в сокращенной форме Вейрештрасса в проективном виде может быть преобразована в кривую в форме Хессе в проективном виде посредством отображения $(X, Y, Z, a, b) \to (u^2 X, u^3 Y, Z, u^4 a, U^6 b)$.

Отображения могут существовать в случае $q \equiv 5 (\mathrm{mod}\, 6)$ и ЭК в сокращенной форме Вейерштрасса $E_W(F_q)$ имеет след Фробениуса эндоморфизма $T \equiv 0 (\mathrm{mod}\, 3)$.

$$E_W(F_q) \to E_H(F_q) \qquad E_H(F_q) \to E_W(F_q)$$

$$U = u^2 mX + u^3 Y + \frac{4 - m^3}{3} Z \qquad X = u^{-2} m^2 (U + V) + \frac{4 - m^3}{3} W$$

$$V = u^2 mX - u^3 Y + \frac{4 - m^3}{3} Z \qquad Y = u^{-3} \frac{4 - m^3}{3} (-U + V)$$

$$W = -2u^2 X - 2m^2 Z \qquad Z = -U - V - mW$$

Значения $(m, \pm u)$ являются корнями системы уравнений:

$$\begin{cases} u^4 a = -\dfrac{m(8 + m^3)}{3} \\ u^6 b = \dfrac{2(-8 - 20m^3 + m^6)}{27} \end{cases}$$

Отметим, что указанная система имеет решения, лишь в случае существования решений системы, для случая $E_W(F_q) \to E_H(F_q)$:

$$\begin{cases} a = -\dfrac{m(8 + m^3)}{3} \\ b = \dfrac{2(-8 - 20m^3 + m^6)}{27} \end{cases}$$

Согласно результатам, полученным в работе [9], бирациональное отображение ЭК в сокращенной форме Вейерштрасса $E_W(F_q): Y^2 = X^3 + aX + b$ может быть получено из уравнения ЭК в форме Хессе $E_H(F_q): x^3 + y^3 + 1 = dxy$ следующим образом.

$$E_W(F_q) \to E_H(F_q) \qquad E_H(F_q) \to E_W(F_q)$$

$$a = -\alpha d (d^3 + 216),$$

$$b = 2\alpha^3 (d^6 - 540 d^3 - 5832),$$

$$\alpha = \tfrac{1}{3},\ \alpha \in F_q.$$

Тогда, параметрически заданная ЭК в сокращенной форме Вейрештрасса в аффинных координатах, может быть получена из кривой в форме Хессе посредством отображения $\phi_1 : (x, y) \to \lambda_3 (X + d^2, \alpha^2 \lambda_1 \lambda_3)$.

Обратное отображение ЭК из сокращенной формы Вейерштраса в форму Хессе имеет вид: $\phi_1^{-1} : (X, Y) \to (\lambda_4 x - d^2, 3\lambda_4 (y - 1))$.

Значения

$\lambda_1 = d^3 - 3dX - 108$, $\lambda_2 = d^3 - 27$, $\lambda_3 = 54 \dfrac{\lambda_2 (3Y + \lambda_1)}{729 (X + d^2)^3 + \lambda_1^3}$, $\lambda_4 = \dfrac{4\lambda_2}{3(dx + dy + 3)}$

Эквивалентность между ЭК в форме Вейерштрасса и форме Эдвардса

Проведенные в публикации [6, 7] рассуждения показали существование линейной эквивалентности между представления ЭК в сокращенной форме Вейерштрасса и формой Эдвардса. Ниже приведем, часть рассуждений [6, 7].

Пусть представление ЭК в сокращенной форме Вейерштрасса в стандартных аффинных координатах имеет вид: $E_W(F_q): y^2 = x^3 + a_2x^2 + a_4x$ для $p \geq 5$.

ЭК в форме Эдвардса имеет вид: $E_E(F_q): x^2 + y^2 = 1 + dx^2y^2$.

ЭК в скрученной форме Эдвардса имеет вид: $E_E(F_q): ax^2 + y^2 = 1 + dx^2y^2$.

Тогда, параметрически заданная ЭК в не сокращенной форме Вейрештрасса в аффинных координатах, может быть получена из кривой в скрученной форме Эдвардса посредством отображения $\phi_1 : (x, y) \to \left((a-d)\frac{1+y}{1-y}, (a-d)\frac{2(1+y)}{x(1-y)} \right)$.

Обратное отображение ЭК из не сокращенной формы Вейерштраса в скрученную форму Эдвардса имеет вид: $\phi_1^{-1} : (x, y) \to \left(\frac{2x}{y}, \frac{x-(a-d)}{x+(a-d)} \right)$.

Ниже приведем коэффициенты бирациональных кривых в скрученной форме Эдвардса и не сокращенной форме Вейерштрасса.

$E_W(F_q) \to E_E(F_q)$ $\qquad$ $E_E(F_q) \to E_W(F_q)$

$a_2 = 2\frac{(a+d)}{(a-d)^2}$ $\qquad$ $a_2 = 2(a+d)$

$a_4 = \frac{1}{(a-d)^2}$ $\qquad$ $a_4 = (a-d)^2$

Тогда, параметрически заданная ЭК в сокращенной форме Вейрештрасса в аффинных координатах, может быть получена из кривой в форме Эдвардса посредством отображения $\phi_1 : (x, y) \to \left((1-d)\frac{1+y}{1-y}, (1-d)\frac{2(1+y)}{x(1-y)} \right)$.

Обратное отображение ЭК из сокращенной формы Вейерштраса в форму Эдвардса имеет вид: $\phi_1^{-1} : (x, y) \to \left(\frac{2x}{y}, \frac{x-(1-d)}{x+(1-d)} \right)$.

Ниже приведем коэффициенты бирациональных кривых в форме Эдвардса и сокращенной форме Вейерштрасса.

$E_W(F_q) \to E_E(F_q)$ $\qquad$ $E_E(F_q) \to E_W(F_q)$

$a_2 = 2\frac{(1+d)}{(1-d)^2}$

$a_4 = \frac{1}{(1-d)^2}$

Пусть представление ЭК в сокращенной форме Вейерштрасса в стандартных аффинных координатах имеет вид: $E_W(F_q): y^2 = x^3 + a_2x^2 + a_6$ для $p \geq 5$.

Тогда, параметрически заданная ЭК в сокращенной форме Вейрештрасса в аффинных координатах, может быть получена из кривой в скрученной форме Эдвардса посредством отображения $\phi_1 : (x, y) \to \left(\frac{(5a-d)+(a-5d)y}{12(1-y)}, \frac{(a-d)(1+y)}{4x(1-y)} \right)$.

$E_W(F_q) \to E_E(F_q)$ $\quad$ $E_E(F_q) \to E_W(F_q)$

$$a_2 = -\frac{a^2 + 14ad + d^2}{48}$$

$$a_6 = -\frac{a^3 - 33a^2 d - 33ad^2 + d^3}{864}$$

Эквивалентность между ЭК в форме Вейерштрасса и форме Монтгомери

Проведенные в публикации [8] рассуждения показали существование линейной эквивалентности между представления ЭК в сокращенной форме Вейерштрасса и формой Монтгомери. Ниже приведем, часть рассуждений [8].

Пусть представление ЭК в сокращенной форме Вейерштрасса в стандартных аффинных координатах имеет вид: $E_W(F_q): y^2 = x^3 + a_4 x + a_6$ для $p \geq 5$.

ЭК в форме Монтгомери $b = 1$ (все кривые изоморфны кривой с $b = 1$) имеет вид: $E_M(F_q): by^2 = x^3 + ax^2 + x$.

Тогда, параметрически заданная ЭК в сокращенной форме Вейрештрасса в аффинных координатах, может быть получена из кривой в форме Монтгомери посредством отображения $\phi_1 : (x, y) \to (x - \alpha, y)$ для случая, когда $b = 1$. Если $b = 1$, тогда α является корнем полинома $f(x) = x^3 + a_4 x + a_6$, т.е. $f(\alpha) = 0$.

Обратное отображение ЭК из сокращенной формы Вейерштраса в форму Монтгомери лишь в случае, если ЭК в сокращенной форме Вейерштрасса имеет точки порядка 4, имеет вид: $\phi_1^{-1} : (x, y) \to (x + \alpha, y)$ для случая, когда $b = 1$ и $a = 3\alpha$.

Ниже приведем коэффициенты бирациональных кривых в форме Монтгомери и сокращенной форме Вейерштрасса.

$E_W(F_q) \to E_M(F_q)$

$b = 1,$

$a = 3\alpha$

$f(\alpha) = 0$, для $f(x) = x^3 + a_4 x + a_6$

$E_M(F_q) \to E_W(F_q)$

$a_4 = 1 - 3\alpha^2,$

$a_6 = 2\alpha^3 - \alpha,$

$\alpha = a/3$

Рассмотрим аналогичные рассуждения, приведенные в [9]. Предположим, что $f(x) = x^3 + a_4 x + a_6$ имеет корни в поле F_q, пусть α является корнем $f(\alpha) = 0$. Предположим, что $3\alpha^2 + a_4$ является квадратичным вычетом в поле F_q. Тогда предположим, что существует такое s, что $s^{-2} = 3\alpha^2 + a_4$. Исходя из выше приведенных рассуждений, каждая точка ЭК в форме Вейерштрасса отобразится в форму Монтгомери $\phi_1^{-1} : (x, y) \to (s(x - \alpha), sy)$ и ЭК в форме Монтгомери будет иметь вид: $sy^2 = x^3 + 3\alpha s x^2 + x$, т.е. $b = s$, $a = 3\alpha s$.

Переход от ЭК в форме Монтгомери к форме Вейерштрасса происходит следующим образом. Точка $(0, 0)$ на ЭК в форме Монтгомери $E_M(F_q)$ является точкой второго порядка и ей соответствует некая точка на ЭК в форме Вейерштрасса $E_W(F_q)$, значит $\#E_W(F_q) \bmod 2 \equiv 0$. Исходя из рассуждений относительно отображения токе ЭК $E_W(F_q)$ в ЭК $E_M(F_q)$, видим, что точка $(0, 0)$ на $E_M(F_q)$ отображается в $(\alpha, 0)$. Таким образом, отображение $E_M(F_q) \to E_W(F_q)$ будет иметь вид: $a_4 = b^{-2} - 3\alpha^2$, $a_6 = -\alpha^3 - a\alpha$, $\alpha = a/(3b)$.

Эквивалентность между ЭК в форме Эдвардса и форме Монтгомери

Проведенные в публикации [8] рассуждения показали существование линейной эквивалентности между представления ЭК в форме Эдвардса и формой Монтгомери. Ниже приведем, часть рассуждений [8].

Пусть представление ЭК в скрученной форме Эдвардса в стандартных аффинных координатах имеет вид: $E_E(F_q): ax^2 + y^2 = 1 + dx^2y^2$ для $p \geq 5$.

ЭК в форме Монтгомери $B \neq 0$ (все кривые изоморфны кривой с $B = 1$) имеет вид: $E_M(F_q): By^2 = x^3 + Ax^2 + x$.

Тогда, параметрически заданная ЭК в скрученной форме Эдвардса в аффинных координатах, может быть получена из кривой в форме Монтгомери посредством отображения $\phi_1 : (x, y) \to (x - \alpha, y)$ для случая, когда $b = 1$. Если $b = 1$, тогда α является корнем полинома $f(x) = x^3 + a_4x + a_6$, т.е. $f(\alpha) = 0$.

Обратное отображение ЭК из скрученной формы Эдвардса в форму Монтгомери лишь в случае, если ЭК в скрученной форме Эдвардса имеет точки порядка 4, имеет вид: $\phi_1^{-1} : (x, y) \to (x + \alpha, y)$ для случая, когда $b = 1$ и $a = 3\alpha$.

Ниже приведем коэффициенты бирациональных кривых в форме Монтгомери и сокращенной форме Вейерштрасса.

$$E_E(F_q) \to E_M(F_q) \qquad E_M(F_q) \to E_E(F_q)$$

$$A = \frac{2(a+d)}{(a-d)}, \qquad a = \frac{A+2}{B},$$

$$B = \frac{4}{(a-d)}. \qquad d = \frac{(A-2)}{B}.$$

Эквивалентность между ЭК в форме Хаффа и форме Вейерштрасса

Проведенные в публикации [8] рассуждения показали существование линейной эквивалентности между представления ЭК в форме Хаффа и формой Вейрштрасса. Ниже приведем, часть рассуждений [8].

Пусть представление ЭК в скрученной форме Хаффа в стандартных аффинных координатах имеет вид: $E_{Hu}(F_q): x(ay^2 - 1) = y(bx^2 - 1)$ для $ab(a - b) \neq 0$.

ЭК в форме Вейрштрасса в стандартных аффинных координатах имеет вид: $E_W(F_q): y^2 = x^3 + a_2x^2 + a_4x$.

Тогда, параметрически заданная ЭК в форме Вейерштрасса в аффинных координатах, может быть получена из кривой в форме Хаффа посредством отображения $\phi_1 : (x, y) \to \left(\frac{bx + ay}{y - x}, \frac{b - a}{y - x}\right)$

Обратное отображение ЭК из формы Хаффа в форму Вейрштрасса, имеет вид: $\phi_1^{-1} : (x, y) \to \left(\frac{x + a}{y}, \frac{x + b}{y}\right)$.

Ниже приведем коэффициенты бирациональных кривых в форме Хаффа и форме Вейерштрасса.

$$E_W(F_q) \to E_{Hu}(F_q) \qquad E_{Hu}(F_q) \to E_W(F_q)$$

$$a_2 = a + b,$$

$$a_4 = ab.$$

Литература

1. Официальный web-сайт Wolfram Mathematica.URL:

2. Теоретические материалы и программное обеспечение доступны по адресу: www.nrjetix.com/r-and-d/lectures

3. Таня Ланге. Бернштейн. База формул операций над точками эллиптической кривой в различных формах и представлениях. http://hyperelliptic.org/EFD/

4. Alexander Rostovtsev. Linear equivalence between elliptic curves in Weierstrass and Hesse form.

5. Преобразование эллиптической кривой из формы Вейерштрасса в форму Хессе и обратно. URL: http://en.wikipedia.org/wiki/Hessian_form_of_an_elliptic_curve

6. Dustin Moody, Daniel Shumow. Isogenies on Edwards and Huff Curves.

7. Hamish Ivey-Law and Robert Rolland. Finding cryptographically strong elliptic cures: a technical report.

8. Richard Moloney, Gary McGuire, Michael Markowitz. Elliptic Curves in Montgomery Form with B=1 and Their Low Order Torsion. -7 p.

9. Mathieu Ciet, Gilles Piret, Jean-Jacques Quisquater. Several Optimizations for Elliptic Cures Implementation on Smart Card. –24 p.