

Полиномы Гильберта и j -инварианты эллиптических кривых

В стандартах электронной цифровой подписи ГОСТ Р 34.10–2001 и ECDSA не определен этап генерации параметров подписи. В статье предлагается алгоритм и программа в среде MATHEMATICA для генерации эллиптической кривой с использованием полиномов Гильберта. Приведены j -инварианты эллиптических кривых для всех квадратичных порядков с числом классов 1 и 2 и полиномы Гильберта для всех мнимых квадратичных порядков с числом классов 3.

Rostovtsev A.G. and Makhovenko E.B.,
SPbSPU

Hilbert polynomials and elliptic curve j -invariants

Digital signature standards ГОСТ Р 34.10–2001, ECDSA do not determine the method of elliptic curve generation. The method and program in MATHEMATICA for elliptic curve generation are suggested, based on computing Hilbert polynomials. Elliptic curve j -invariants for all imaginary quadratic orders with class numbers 1 and 2 and Hilbert polynomials for all imaginary quadratic orders with class number 3 are given.

Введение

Эллиптические кривые над конечными полями являются основной математической структурой для реализации протоколов электронной цифровой подписи ГОСТ Р 34.10–2001 и ECDSA. Однако эти стандарты подписи не предусматривают алгоритмов выбора эллиптических кривых.

В работе [1] предложены эллиптические кривые, j -инварианты которых являются целыми числами. В работе [2] предложен более общий подход к генерации эллиптических кривых, который, однако, неудобен для реализации. Целью данной статьи является создание общего алгоритма генерации эллиптических кривых для указанных стандартов.

1. Теоретические сведения

Мероморфная функция f над полем \mathbb{C} комплексных чисел называется *эллиптической*, если существуют комплексные числа ω_1 и ω_2 такие, что $\omega_1/\omega_2 \notin \mathbb{R}$ и для любых целых чисел m, n выполняется равенство $f(z + m\omega_1 + n\omega_2) = f(z)$ [3, 4].

Назовем *решеткой* L свободный \mathbb{Z} -модуль ранга 2: $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$; решетка задает факторгруппу \mathbb{C}/L .

Эллиптические функции для заданной решетки образуют поле, которое порождается функцией Вейерштрасса $\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$ и ее

производной (суммирование ведется по всем ненулевым элементам ω решетки L). Функция Вейерштрасса удовлетворяет уравнению

$$\wp'(z)^2 = 4\wp^3(z) - g_2\wp(z) - g_3,$$

где $g_2(L) = 60 \sum_{\omega \in L \setminus \{0\}} \omega^{-4}$, $g_3(L) = 140 \sum_{\omega \in L \setminus \{0\}} \omega^{-6}$. Таким образом, функция Вей-

ерштрасса параметризует эллиптическую кривую. Имеет место изоморфизм $\mathbb{C}/L \cong E(\mathbb{C})$.

Решетки L и M называются *гомоморфными* (соответственно *изоморфными*), если существует такой элемент $\alpha \in \mathbb{C}^*$, что $\alpha L \subseteq M$ (соответственно $\alpha L = M$). Изоморфизм решеток индуцирует изоморфизм соответствующих эллиптических кривых, а гомоморфизм решеток — изогении эллиптических кривых. Необходимое и достаточное условие изоморфизма решеток L и M

задается равенством $j(L) = j(M)$, где $j = \frac{1728g_2^3}{g_2^3 - 27g_3^2}$.

Решетка не меняется, если вектор ее периодов умножить на произвольную матрицу $A \in \text{SL}_2(\mathbb{Z})$. Если положить $\omega_1/\omega_2 = \tau$ и рассматривать $j = j(\tau)$ как функцию комплексной переменной τ , то $j(\tau') = j(A(\tau))$. Инвариант решетки как функция совпадает с j -инвариантом эллиптической кривой $E(\mathbb{C})$.

Если $k \subset \mathbb{C}$ — числовое поле, $p \in \mathbb{Z}$ — простое число, \mathfrak{P} — простой идеал кольца целых над \mathbb{Z} элементов поля k и O_k — локальное кольцо элементов относительно \mathfrak{P} -адического нормирования, то существует гомоморфизм $E(k) \rightarrow E(\mathbb{F}_p)$, заданный редукцией по модулю p . При этом точки с координатами из O_k переходят в аффинные точки. Тогда j -инвариант эллиптической кривой $E(\mathbb{F}_p)$ является продолжением функции $j(\tau)$ на O_k и, следовательно, на поле \mathbb{C} .

Согласно ГОСТ Р 34.10–2001 необходимо знать j -инвариант эллиптической кривой, который связан с числом точек $\#E(\mathbb{F}_p)$. Для вычислимости j -инварианта кривой $E(\mathbb{F}_p)$ функция j должна быть алгебраической, а значение $j(\tau)$ — алгебраическим числом. Справедливо следующее утверждение [3].

Теорема 1. Число $j(\tau)$ является алгебраическим тогда и только тогда, когда τ — элемент мнимого квадратичного поля.

Определим мнимое квадратичное поле $K = \mathbb{Q}[\sqrt{-D}]$ и O_D — квадратичный порядок поля K . Пусть $\xi = \sqrt{-D}$ при $D \not\equiv 1 \pmod{4}$ и $\xi = \frac{1 + \sqrt{-D}}{2}$ при

$|D| \equiv 3 \pmod{4}$. Тогда $O_D = \mathbb{Z} + \mathbb{Z}\xi$. Поле K обладает множеством квадратичных порядков. Дискриминант квадратичного порядка равен f^2D , где D свободно от квадратов или является учетверенным свободным от квадратов числом. В случае $f=1$ порядок называется максимальным.

В общем случае кольцо O_D не является кольцом главных идеалов, и идеал имеет базис из двух элементов. Нормой $N(\mathfrak{A})$ идеала \mathfrak{A} квадратичного порядка O_D является число классов вычетов аддитивных групп O_D/\mathfrak{A} . Идеалы квадратичного порядка имеют простое описание [5].

Теорема 2. Любой идеал \mathfrak{A} квадратичного порядка O_D может быть задан в виде $\mathfrak{A} = a\mathbb{Z} + \mathbb{Z}(b + \xi)$, где $a, b \in \mathbb{Z}$.

Отношение эквивалентности для идеалов $\mathfrak{A}, \mathfrak{B} \in O_D$ (идеалы \mathfrak{A} и \mathfrak{B} эквивалентны тогда и только тогда, когда существуют такие элементы $\alpha, \beta \in O_D$, что $\alpha\mathfrak{A} = \beta\mathfrak{B}$) разбивает их множество на классы. Класс, содержащий идеал \mathfrak{A} , будем обозначать \mathbf{A} .

Определим произведение классов идеалов $\mathbf{C} = \mathbf{A}\mathbf{B}$ как класс, содержащий идеал $\mathfrak{C} = \mathfrak{A}\mathfrak{B}$. Умножение классов идеалов квадратичных порядков коммутативно и ассоциативно: $\mathbf{A}\mathbf{B} = \mathbf{B}\mathbf{A}$, $\mathbf{A}(\mathbf{B}\mathbf{C}) = (\mathbf{A}\mathbf{B})\mathbf{C}$. Единичным классом является класс, содержащий главный идеал. Пусть идеал \mathfrak{A} соответствует классу \mathbf{A} и $\mathfrak{A}\mathfrak{B}$ — главный идеал. Тогда класс \mathbf{B} , содержащий идеал \mathfrak{B} , является обратным к классу \mathbf{A} . Таким образом, классы идеалов квадратичного порядка O_D образуют абелеву группу классов, и эта группа конечна, поскольку каждый класс \mathbf{A} содержит идеал с нормой, меньшей чем $\sqrt{|D|}$ [5]. Обозначим h_D — число классов порядка O_D .

Идеалы квадратичных порядков связаны с квадратичными формами над \mathbb{Z} , что следует из выражения для нормы идеалов. Если $\mathfrak{A} = (\alpha, \beta) = (\alpha x + \beta y)$ для $x, y \in \mathbb{Z}$ и $\alpha, \beta \in O_D$, то

$$N(\mathfrak{A}) = (\alpha x + \beta y)(\overline{\alpha x + \beta y}) = ax^2 + bxy + cy^2,$$

где $a, b, c \in \mathbb{Z}$. Квадратичную форму $f = ax^2 + bxy + cy^2$ можно задать симметрической матрицей $M_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ с определителем $-D/4$. Определим

эквивалентные квадратичные формы как орбиты относительно группы $SL_2(\mathbb{Z})$. Эквивалентные идеалы биективно соответствуют эквивалентным квадратичным формам.

Форма (a, b, c) называется нормальной, если $-a < b \leq a$. Нормальная форма называется приведенной, если $a \leq c$ и $b \geq 0$ при $a = c$. Каждый класс идеалов задается приведенной квадратичной формой.

Для группы классов справедливо следующее утверждение [3].

Теорема 3. Для квадратичного порядка O_D существует приведенный полином Гильберта $H_D(X) \in \mathbb{Z}[X]$ степени h_D , для которого $j(\tau)$ является корнем. Если порядок O_D максимальный, то $K[j(\tau)]$ — гильбертово поле классов.

Имеет место равенство

$$H_D(X) = \prod \left(X - j \left(\frac{b + \sqrt{-D}}{2a} \right) \right),$$

где произведение берется по всем классам идеалов, представленным тройками целых чисел (a, b, c) , то есть целочисленными квадратичными формами вида $au^2 + buv + cv^2$ дискриминанта $-D$.

Значение j для квадратичного аргумента вычисляется приближенно, с использованием методов математического анализа. Для этого положим $q = e^{2\pi i \tau}$ — преобразование Фурье. Тогда

$$j(\tau) = q \left(1 + \sum_{k \geq 1} (-1)^k \left(q^{\frac{k(3k-1)}{2}} + q^{\frac{k(3k+1)}{2}} \right) \right)^{24}.$$

Расчетные значения $j(\tau)$ — это комплексные числа, представленные с некоторым округлением (как правило, точность вычислений должна быть не хуже нескольких десятков десятичных знаков). Найти, какое именно алгебраическое число представляет приближенное значение $j(\tau)$, сложно. Поэтому на практике действуют наоборот: сначала по приближенным значениям составляют полином Гильберта $H_D(X)$, затем коэффициенты полинома округляют до целых чисел и находят алгебраические числа, являющиеся корнями $H_D(X)$, то есть алгебраические j -инварианты.

Число $j(\tau)$ является целым только тогда, когда квадратичный порядок обладает числом классов 1, то есть для 11 эллиптических кривых: $|D| = 2, j = 20^3$; $|D| = 4, j = 66^3$; $|D| = 7, j = -15^3$; $|D| = 11, j = -32^3$; $|D| = 12, j = 2 \cdot 30^3$; $|D| = 19, j = -96^3$; $|D| = 27, j = -3 \cdot 160^3$; $|D| = 28, j = 255^3$; $|D| = 43, j = -960^3$; $|D| = 67, j = -5280^3$; $|D| = 163, j = -640320^3$.

Существуют квадратичные порядки с числом классов больше 1. Для них тоже можно вычислить j -инвариант и определить число точек.

Корни полинома Гильберта в общем случае являются вычислимыми над полем алгебраических чисел лишь в том случае, если степень полинома не превосходит 4. Если степень полинома более 4, то необходимо решать уравнение $H_D(X) = 0$ в конечном поле \mathbb{F}_p .

Скрученные эллиптические кривые, заданные уравнениями $E(\mathbb{F}_p): y^2 = x^3 + Ax + B$ и $E'(\mathbb{F}_p): y^2 = x^3 + Au^2x + Bu^3$, где u — квадратичный невычет

по модулю p , обладают одинаковыми j -инвариантами: $j = \frac{6912A^3}{4A^3 + 27B^2}$. Инва-

риант определяет эллиптическую кривую над квадратичным расширением исходного поля с точностью до изоморфизма: $A = \frac{3j}{1728-j}$, $B = \frac{2j}{1728-j}$.

Если характеристика поля может быть представлена в мнимом квадратичном порядке O_D в виде $p = a^2 + Db^2$, то число точек на скрученных кривых равно $p + 1 \pm 2a$. Если характеристика поля может быть представлена в виде $p = \frac{D+1}{4}a^2 + Dab + Db^2$, то число точек на скрученных кривых равно $p + 1 \pm a$.

Таким образом, генерация эллиптической кривой сводится к нахождению полинома Гильберта.

2. Вычисление полинома Гильберта и j -инварианта

Приведем метод генерации эллиптической кривой с использованием пакета MATHEMATICA версии 5.0.

Для вычисления полинома Гильберта нужно сначала выбрать дискриминант $-DD$ и точность toc , найти число классов cn , определяющее число сомножителей в полиноме Гильберта, найти представители классов (тройки cl , представляющие аргумент τ), вычислить приближенно функции $\text{tt}[[i]]$ как $j(\tau)$, вычислить приближенно коэффициенты $\text{aa}[[i]]$ полинома Гильберта и округлить их. Результатом является полином H . Соответствующая программа имеет вид:

```
<<NumberTheory`NumberTheoryFunctions`
DD = -*** «Ввести требуемое значение дискриминанта»;
cl = ClassList[DD];
cn = Length[cl];
tau = Table[0, {i, 1, cn}];
j = Table[0, {i, 1, cn}];
aa = Table[0, {i, 1, cn}];
toc = 250;
For[i = 1, i < cn + 1, i++,
  tau[[i]] = Simplify[(cl[[i, 2]] + Sqrt[DD])/(2cl[[i, 1]])];
  j[[i]] = N[1728*KleinInvariantJ[tau[[i]]], toc];
HD0 = N[Expand[Product[(X - j[[i]]), {i, 1, cn}], toc];
For[i = 1, i < cn + 1, i++,
  aa[[i]] = Round[Coefficient[HD0, X, i - 1]];
H = X^cn + Sum[aa[[i]]*X^(i - 1), {i, 1, cn}]
```

Критерием правильного выбора точности вычислений является то, что коэффициенты полинома H при увеличении точности не меняются, а подкоренное выражение для квадратных корней кратно дискриминанту $|DD|$ или является его делителем.

Инвариант эллиптической кривой может быть найден как корень полинома Гильберта. Отметим, что если $h_D < 5$, то корни полинома Гильберта могут быть найдены как целые алгебраические числа в явном виде. После этого j -

инвариант в конечном поле вычисляется просто редукцией по модулю p . При $h_D \geq 5$ явное выражение для инварианта в алгебраических числах отсутствует, корни полинома Гильберта можно найти только для конечного поля, например, разложив полином на множители.

Данный алгоритм позволяет находить j -инварианты эллиптических кривых для квадратичных порядков с большим числом классов. Например, для $D = -1039$ с числом классов 23 и характеристики поля длиной 256 бит полином Гильберта вычисляется и раскладывается на простые множители быстрее, чем за секунду.

Данный метод позволяет генерировать «хорошие» эллиптические кривые над полями произвольных характеристик. Для данной характеристики поля p нужно подобрать такой свободный от квадратов квадратичный вычет $-D$ по модулю p , что для разложения $p = a^2 + Db^2$ число точек $p + 1 \pm 2a$ или для разложения $p = \frac{D+1}{4}a^2 + Dab + Db^2$ число точек $p + 1 \pm a$ удовлетворяет криптографическим требованиям. При этом следует иметь в виду, что число классов легко вычислимо только для $|D| < 10^7$. Разложение характеристики поля можно выполнить алгоритмом, приведенным в работе [1].

3. j -инварианты для квадратичных порядков с числом классов 1 и 2

Число классов 1 имеют 13 порядков, из которых 11 допускаются стандартом ГОСТ Р 34.10–2001: $-D \in \{2, 4, 7, 11, 12, 19, 27, 28, 43, 67, 163\}$. Инварианты эллиптических кривых для дискриминантов с числом классов 1 указаны в таблице 1.

Таблица 1

Инварианты эллиптических кривых для дискриминантов с числом классов 1

$-D$	2	4	7	11	12	19	27	28	43	67	163
j	20^3	66^3	-15^3	-32^3	$2 \cdot 30^3$	-96^3	$-3 \cdot 160^3$	255^3	-960^3	-5280^3	-640320^3

Число классов 2 имеют 29 порядков, для которых $-D \in \{5, 6, 8, 10, 13, 15, 22, 35, 36, 37, 48, 51, 58, 64, 72, 75, 91, 99, 100, 112, 115, 123, 147, 148, 187, 235, 267, 403, 427\}$. Инварианты эллиптических кривых для дискриминантов с числом классов 2 указаны в таблице 2, при этом $j = b(b_0 + b_1\sqrt{d})$.

Таблица 2

Инварианты эллиптических кривых для дискриминантов с числом классов 2

$-D$	b	b_0	b_1	d
5	320	1975	884	5
6	1728	1399	988	2
8	1000	26125	18473	2
10	8640	24635	11016	5
13	216000	15965	4428	13
15	135/2	-1415	637	5

22	216000	14571395	10303524	2
35	-163840	360	161	5
36	192	399849	230888	3
37	216000	91805981021	15092810460	37
48	40500	35010	20213	3
51	-442368	6263	1519	17
58	216000	1399837865393267	259943365786104	29
60	135/2	274207975	122629507	5
64	54	761354780	538359129	2
72	8000	23604673	9636536	6
75	-884736	369830	165393	5
91	-884736	5854330	1623699	13
99	-180224	104359189	18166603	33
100	1728	12740595841	5697769392	5
112	3375	40728492440	15393921	7
115	-4423680	48360710	21627567	5
123	-110592000	6122264	956137	41
147	-331776000	525181123	11460394	21
187	-940032000	2417649815	586366209	17
235	-5887918080	69903946375	31261995198	5
267	-55296000	177979346192125	18865772964857	89
403	-110592000	11089461214325319155	3075663155809161078	13
427	147197952000	53028779614147702	6789639488444631	61

Инварианты указанных эллиптических кривых являются целыми квадратичными числами дискриминанта $d \in \{2, 3, 5, 6, 7, 13, 17, 21, 29, 33, 37, 41, 61, 89\}$. Построение соответствующей эллиптической кривой требует вычисления \sqrt{d} в поле \mathbb{F}_p .

4. Полиномы Гильберта для квадратичных порядков с числом классов 3

Число классов 3 имеют 25 порядков, для которых $-D \in \{23, 31, 44, 59, 76, 83, 92, 107, 108, 124, 139, 172, 211, 243, 268, 283, 307, 331, 379, 499, 547, 643, 652, 883, 907\}$. Расчетные значения коэффициентов полинома Гильберта $H_D(X) = X^3 + a_2X^2 + a_1X + a_0$ приведены в таблице 3.

Таблица 3

Коэффициенты полинома Гильберта для дискриминантов с числом классов 3

D	Коэффициенты полинома Гильберта
-23	$a_2 = 3491750$ $a_1 = -5151296875$ $a_0 = 23375^3$
-31	$a_2 = 39491307$ $a_1 = -58682638134$ $a_0 = 1566028350940383$
-44	$a_2 = -1122662608$ $a_1 = 270413882112$ $a_0 = -653249011576832$
-59	$a_2 = 30197678080$ $a_1 = -140811576541184$

D	Коэффициенты полинома Гильберта
	$a_0 = 116127^3$
-76	$a_2 = -784074438864$ $a_1 = 1128678666363648$ $a_0 = -827237892283232256$
-83	$a_2 = 2691907584000$ $a_1 = -41490055168000000$ $a_0 = 8192000^3$
-92	$a_2 = -12207823849750$ $a_1 = -263033266852296875$ $a_0 = -18437375^3$
-107	$a_2 = 129783279616000$ $a_1 = -6764523159552000000$ $a_0 = 69632000^3$
-108	$a_2 = -151013228706000$ $a_1 = 224179462188000000$ $a_0 = -12342000^3$
-124	$a_2 = -1559739536377947$ $a_1 = -874125972104525910$ $a_0 = -8432127$
-139	$a_2 = 12183160834031616$ $a_1 = -53041786755137667072$ $a_0 = 40697856^3$
-172	$a_2 = -782759106183330000$ $a_1 = 1164707517403692000000$ $a_0 = -884790000^3$
-211	$a_2 = 65873587288630099968$ $a_1 = 277390576406111100862464$ $a_0 = 1744699392^3$
-243	$a_2 = 1855762905734664192000$ $a_1 = -3750657365033091072000000$ $a_0 = 1036288000^3$
-268	$a_2 = 21667237292024856738000$ $a_1 = -32240842762858236972000000$ $a_0 = 147198006000^3$
-283	$a_2 = 89611323386832801792000$ $a_1 = 90839236535446929408000000$ $a_0 = 5861376000^3$
-307	$a_2 = 805016812009981390848000$ $a_1 = -5083646425734146162688000000$ $a_0 = 20791296000^3$
-331	$a_2 = 6647404730173793386463232$ $a_1 = 368729929041040103875232661504$ $a_0 = 382987173888^3$
-379	$a_2 = 364395404104624239018246144$ $a_1 = -121567791009880876719538528321536$ $a_0 = 2490287652864^3$
-499	$a_2 = 3005101108071026200706725969920$ $a_1 = -6063717825494266394722392560011051008$ $a_0 = 167163228389376^3$
-547	$a_2 = 81297395539631654721637478400000$ $a_1 = -139712328431787827943469744128000000$ $a_0 = 4367388672000^3$
-643	$a_2 = 39545575162726134099492467011584000$ $a_1 = -6300378505047247876499651797450752000000$

D	Коэффициенты полинома Гильберта
	$a_0 = 675369750528000^3$
-652	$a_2 = -68925893036109279891085639286946000$ $a_1 = -102561728837719322645921325412908000000$ $a_0 = 262537412640822000^3$
-883	$a_2 = 34903934341011819039224295011933392896000$ $a_1 = -151960111125245282033875619529124478976000000$ $a_0 = 5517741993984000^3$
-907	$a_2 = 123072080721198402394477590506838687744000$ $a_1 = 39181594208014819617565811575376314368000000$ $a_0 = 5303371235328000^3$

5. Полиномы Гильберта для квадратичных порядков с числом классов 4 и более

Число мнимых квадратичных порядков с числами классов 4–14, а также соответствующие максимальный и минимальный дискриминанты приведены в таблице 4.

Таблица 4

Число мнимых квадратичных порядков с числами классов 4–14

h_D	4	5	6	7	8	9	10	11	12	13	14
$\#\{D\}$	84	29	101	38	108	55	123	46	379	43	134
$ D _{\min}$	39	47	87	71	95	199	119	167	231	191	215
$ D _{\max}$	1555	2683	4075	5923	7987	10627	13843	15667	19723	20563	27547

Рассмотрим в качестве примера генерацию эллиптической кривой для мнимого квадратичного порядка с дискриминантом $D = -1039$.

Выбираем простое число p длиной 256 бит такое, что для разложения $p = a^2 + Db^2$ одно из чисел $p + 1 \pm 2a$ является учетверенным простым. Находим

$$p = 57896044618658097711785492504343975927078785129037869149539333871902348253493;$$

$$r = 14474011154664524427946373126085993981769696282259467287384833467975587064067.$$

Число классов равно 23; соответствующие классы идеалов: $(1, 1, 260)$, $(2, -1, 130)$, $(2, 1, 130)$, $(4, -1, 65)$, $(4, 1, 65)$, $(5, -1, 52)$, $(5, 1, 52)$, $(7, -5, 38)$, $(7, 5, 38)$, $(8, -7, 34)$, $(8, 7, 34)$, $(10, -9, 28)$, $(10, -1, 26)$, $(10, 1, 26)$, $(10, 9, 28)$, $(13, -1, 20)$, $(13, 1, 20)$, $(14, -9, 20)$, $(14, -5, 19)$, $(14, 5, 19)$, $(14, 9, 20)$, $(16, -7, 17)$, $(16, 7, 17)$.

Вычисляем полином Гильберта для квадратичного порядка с дискриминантом -1039 и для точности вычислений в 250 десятичных знаков и раскладываем его на множители над полем \mathbb{F}_p . Полином раскладывается на линейные множители. Наименьшее значение инварианта равно

$$j = 678910437114801175942679754952258276822355881159902280896781257166832287771.$$

Библиографический список

1. **Ростовцев А.Г., Маховенко Е.Б.** Введение в криптографию с открытым ключом. СПб.: Мир и Семья, Интерлайн, 2001.
2. **Atkin A.O., Morain F.** Elliptic curves and primality proving // Mathematics of Computation. 1993. Vol. 61. P. 29–68.
3. **Milne J.S.** Elliptic curves // <http://www.jmilne.org/math/CourseNotes/math679.pdf>.
4. **Ленг С.** Эллиптические функции / Пер. с англ. С.А. Степанова. Новокузнецкий физико-математический институт, 2000.
5. **Buchmann J.** Algorithms for binary quadratic forms // www.cdc.informatik.todarmstadt.de/~buchmann/AlgorithmsForQuadraticForms.ps.