Графики зависимости ψ от φ для углов с нечётным и чётным числом m (при $\beta \neq 0$) представлены соответственно на рис. 8 и 9. На графиках стрелочками отмечено, что точки $\varphi = 0$ и $\varphi = \beta$ отделены от интервала $0 < \varphi < \beta$. Для интервала $0 < \varphi < \beta$ $n = m+1$, для значений $\varphi = 0$ и $\varphi = \beta$ имеем $n = m$.

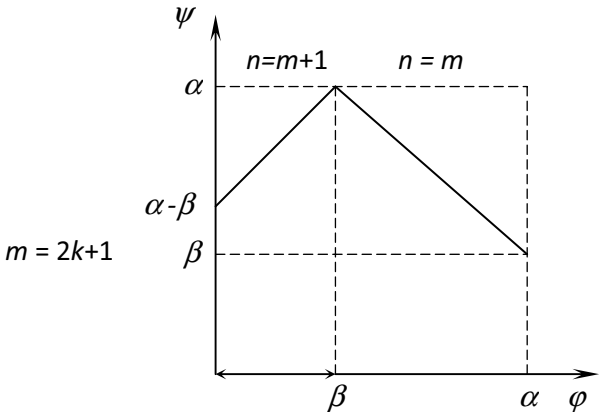

Рис.8

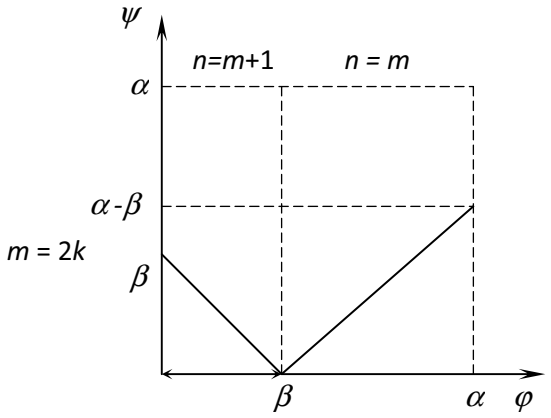

Рис.9

СПИСОК ЛИТЕРАТУРЫ

1. Гальперин Г. А., Земляков А. Н. Математические бильярды. – М.: Наука, 1990.
2. Дынкин Е. Б., Молчанов С. А., Розенталь А. П., Толпыго А. К., Математические задачи (библиотека физико-математической школы) – М.: Наука, 1966.
3. Шарыгин И. Ф. Задачи по геометрии. Планиметрия. М.: Наука, 1982.
4. Гольдфарб Н. И. Сборник вопросов и задач по физике. – М.: Высшая школа, 1982.

ЭЛЕМЕНТЫ СТРАТЕГИИ «СЛУЧАЙНОГО ВЫБОРА» ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

ELEMENTS OF THE STRATEGY OF "RANDOM SELECTION" OF THE ELLIPTIC CURVE

Кудубаева С.А. ,Фатеев Д.Г.

Костанайский государственный университет им. А. Байтурсынова, г.Костанай, Казахстан

Как показано в работе [1], стратегия «случайного выбора» эллиптической кривой (ЭК) опирается на использование алгоритма SEA для вычисления количества точек ЭК и порядка циклической группы точек для случайно выбранной ЭК. Данный алгоритм является результатом усовершенствования алгоритма Чуфа [2] с учетом модификаций, предложенных Элкисом (N. Elkies) и Аткином (A. Atkin). Теоретические основания данных алгоритмов приведены в работе [3].

Алгоритм расчета точек ЭК имеет следующий вид. Пусть $\overline{F_q}$ есть алгебраическое замыкание поля F_q. Эндоморфизм Фробениуса есть отображение $\varphi : E(\overline{F_q}) \to E(\overline{F_q})$, которое определяется соотношениями $\varphi(x, y) = (x^q, y^q)$, $\varphi(O) = O$ и удовлетворяют уравнению

$$\varphi^2 - T\varphi + q = 0 \quad \text{или} \quad \varphi(\varphi(P)) - T\varphi(P) + qP = O, \qquad (1)$$

где T *– след эндоморфизма Фробениуса*, и $|E(F_q)| = N = q + 1 - T$.

Соответственно, для нахождения порядка ЭК $E(F_q)$ необходимо найти значение T.

Для этого достаточно найти $T(mod\, l_i)$, где l_i – малые попарно взаимные простые числа, произведение которых не превышает $4\sqrt{q}$ (так как нужно рассмотреть случаи $N > q$ и $N < q$). При этом само значение T вычисляется по китайской теореме об остатках.

Вначале необходимо рассмотреть случай $l = 2$. Тогда в $E(F_q)$ найдется ненулевая точка $P = (x,0)$ второго порядка тогда и только тогда, когда выполнено условие:

$$\text{НОД}(x^q - x, x^3 + ax + b) \neq 1, \qquad (2)$$

в этом случае $t = 0(mod\ 2)$, иначе $t = 1(mod\ 2)$. Для рассмотрения $l > 2$ необходимо ввести ряд дополнительных определений.

Для каждого натурального числа n обозначим через $E[n]$ подгруппу $E(\overline{F_q})$, состоящую из точек, порядок которых делит n:

$$E[n] = \{P \in E(\overline{F_q}) \mid nP = O\},$$

при этом очевидно, что $\varphi(E[n]) \in E[n]$. Обозначим $\varphi(E[n])$ как φ_l для удобства.

Основная идея алгоритма Чуфа состоит в рассмотрении равенства (1) для ЭК $E(F_q)$ как сравнения по модулю малых простых l. При этом подбором находится такое значение $T(mod\, l)$, что

$$\varphi_l^2 + k \equiv \tau\varphi_l (mod\, l), \qquad (3)$$

где $k = q(mod\, l)$, $\tau = T(mod\, l)$.

Определим многочлены $\psi_n(x,y) \in F_q[x,y]$, $n = -1,0,1,2,\ldots$, следующими соотношениями:

$$\psi_{-1}(x,y) = -1,\ \psi_0(x,y) = 0,\ \psi_1(x,y) = 1,\ \psi_2(x,y) = 2y,$$
$$\psi_3(x,y) = 3x^4 + 6ax^2 + 12bx - a^2,$$
$$\psi_4(x,y) = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3);$$

далее, при $n \geq 3$:

$$\psi_{2n}(x,y) = \psi_n(x,y)(\psi_{n+2}(x,y)\psi_{n-1}(x,y)^2 - \psi_{n-2}(x,y)\psi_{n+1}(x,y)^2)/(2y),$$

и при $n \geq 2$:

$$\psi_{2n+1}(x,y) = \psi_{n+2}(x,y)\psi_n(x,y)^3 - \psi_{n+1}(x,y)^3\psi_{n-1}(x,y).$$

Многочлены $\psi_n(x,y)$ называются *многочленами деления***.** Заменим y^2 на $x^3 + ax + b$ и обозначим полученные полиномы через ψ'_n, тогда полиномы деления будут лежать в $F_q[x]$ или в $yF_q[x]$. Пусть $f_n(x) = \psi'_n(x,y)$, если n нечетное, и $f_n(x) = \psi'_n(x,y)/y$, если n четное. Кроме того, если n – нечетно, q не делит n, то $\deg f_n(x) = (n^2 - 1)/2$ и $\deg f_n(x) = (n^2 - 4)/2$ при четном n.

Полиномы деления позволяют умножать точку ЭК $E(\overline{F_q})$ на целое n:

$$n \cdot (x,y) = \left(x - \frac{\psi_{n-1}(x,y)\psi_{n+1}(x,y)}{\psi_n(x,y)^2}, \frac{\psi_{n+2}(x,y)\psi_{n-1}(x,y)^2 - \psi_{n-2}(x,y)\psi_{n+1}(x,y)^2}{4y\psi_n(x,y)^3} \right) \qquad (4)$$

Кроме того, справедлива следующая теорема: если для ЭК $E(\overline{F_q})$ точка $P = (x_P, y_P)$, то равенство $kP = P_\infty$ выполняется тогда и только тогда, когда $f_k(x_P) = 0$.

Возвращаясь к сравнению (3), в алгоритме Чуфа рассматриваются два случая: $\tau = 0$ и $\tau \neq 0$. Случай $\tau = 0$ рассмотрен ниже в рамках описания алгоритма, а для случая $\tau \neq 0$ уравнение (1) с учетом формулы (4) будет иметь вид:

$$(x^{q^2}, y^{q^2}) \otimes \left(x - \frac{\psi_{k-1}(x,y)\psi_{k+1}(x,y)}{\psi_k(x,y)^2}, \frac{\psi_{k+2}(x,y)\psi_{k-1}(x,y)^2 - \psi_{k-2}(x,y)\psi_{k+1}(x,y)^2}{4y\psi_k(x,y)^3} \right) =$$

$$\left(x^q - (\frac{\psi_{\tau-1}(x,y)\psi_{\tau+1}(x,y)}{\psi_\tau(x,y)^2})^q, (\frac{\psi_{\tau+2}(x,y)\psi_{\tau-1}(x,y)^2 - \psi_{\tau-2}(x,y)\psi_{\tau+1}(x,y)^2}{4y\psi_\tau(x,y)^3})^p \right),$$

где $\otimes$ – операция сложения точек на кривой. Последнее равенство приводится к виду:

$$\begin{cases} H_1(x) \equiv 0 (mod\ f_l(x)), \\ H_2(x) \equiv 0 (mod\ f_l(x)), \end{cases}$$

где $H_1(x)$, $H_2(x) \in F_q[x]$. В результате перебора $\tau = 0,1,\ldots,l-1$ можно найти значение $\tau = T(mod\ l)$.

Исходя из данного теоретического обоснования, общая типизированная схема алгоритма Чуфа для расчёта точек ЭК над конечным полем простого порядка $(q = p)$ может быть представлен следующим образом:

Вход: ЭК $E(F_p)$.

Выход: N – число точек $E(F_p)$.

1.Вычислить набор простых $l_i > 2$ таких, что их произведение $l_1 l_2 \ldots l_n \geq 4\sqrt{p}$;

2. $t =$, $i = 0$, $L = 1$;

3. Если уравнение $x^3 + ax + b = 0$ имеет решение в F_p, то $t = \{0,2\}$, иначе $t = \{1,2\}$;

4. $i = i + 1$, $L = L \cdot l_i$;

5. Если $L \geq 4\sqrt{p}$, перейти к шагу 13;

6. $l = l_i$, $k = p(mod\ l)$;

7.Определить, существует ли точка $P \in E(\overline{F_q})$ такая, что $\varphi_l^2(P) = \pm kP$;

A) если существует P, где $\varphi_l^2(P) = kP$, тогда перейти к шагу 8;

B) если существует P, где $\varphi_l^2(P) = -kP$, тогда $t = t \cup \{0, l\}$ и вернуться к шагу 4;

C) если точки не существует, то перейти к шагу 10.

8. Если $(\frac{k}{l}) = -1$, то $t = t \cup \{0, l\}$ и вернуться к шагу 4, иначе $\omega = \sqrt{k}(mod\ l)$;

9. Если $\pm\omega$ не является собственным значением эндоморфизма φ_l, то $t = t \cup \{0, l\}$ и вернуться к шагу 4, иначе определить знак для ω и в соответствии с этим $t = t \cup \{\pm 2\omega, l\}$ и вернуться к шагу 4;

10. Перебором найти τ, $1 \leq \tau \leq \frac{l-1}{2}$, для которого соотношение $(\varphi_l^2 + k)(P) = \pm\tau\varphi_l(P)$, выполняется на $E[l]$ тождественно;

11. $t = t \cup \{\tau, l\}$;

12. Вернуться к шагу 4;

13. Используя китайскую теорему об остатках, вычислить T;

14. Вернуть $N = p + 1 - T$.

Более подробное описание общего алгоритма Чуфа с теоретическими выкладками и обоснованием можно найти в [1,4,5].

Как указано выше, алгоритм SEA представляет собой алгоритм Чуфа, усовершенствованный с помощью идей Аткина и Элкиса. Общий принцип алгоритма остается без изменения, однако при вычислении значения $T(mod\ l_i)$, где l_i – малые попарно взаимные простые числа, произведение которых не превышает $4\sqrt{q}$, простые числа l_i разбиваются на два типа. Они называются *«простое l Аткина»* и «простое l *Элкиса»*. В том случае, если l_i является «простым Аткина», то вычисление $T(mod\ l_i)$ производится, следуя алгоритму

Аткина, рассмотренному в работе [5]. В случае, если же l_i является «простым Элкиса», то вычисление $T(mod\ l_i)$ производится, следуя алгоритму Элкиса, также показанному в [5]. Для разделения простых l_i на две указанные группы используется механизм «*модульных полиномов*» [6]. Подробные теоретические выкладки представлены в работах [2,6].

Общая структура алгоритма SEA имеет следующий вид.

Вход: ЭК E над конечным полем (F_q).

Выход: N – число точек $E(F_q)$.

1. $M = 1$, $l = 2$, $A = \{\}$, $E[l] = \{\}$;
2. Если $M > 4\sqrt{q}$, перейти к шагу 15;
3. Если степень $(НОД(x^q - x, \Phi_l(x, j))) \neq 0$, тогда перейти к шагу 9;
4. Вычислить степень r для случая несупервырожденной ЭК [6];
5. Вычислить образующий g группы $F_{l^2}^*$;
6. $S = \{\gamma_r = g^{i(l^2-1)/r} \mid НОД(i,r) = 1\}$;
7. Для каждого $\gamma_r \in S$:
   - решить систему уравнений:

$$\begin{cases} \lambda/\mu = \gamma_r \\ t = \lambda + \mu (mod\ l) \\ q = \lambda\mu (mod\ l) \end{cases}$$

   - $A = A \cup (t,l)$.
8. Перейти к шагу 12;
9. Вычислить полином $F_l(x)$ вида 10;
10. Вычислить λ такое, что $НОД(\psi_\lambda^2(x^p - x) + \psi_{\lambda-1}\psi_{\lambda+1}, F_l) \neq 1$;
11. $t = \lambda + q/\lambda (mod\ l)$, $E[l] = E[l] \cup (t,l)$;
12. $M = M \cdot l$;
13. Сгенерировать следующее простое число l;
14. Перейти к шагу 2;
15. Вычислить T – след эндоморфизма с помощью китайской теоремы об остатках и алгоритма «больших и малых шагов» Шенкса [7];
16. Вернуть $N = q + 1 - T$.

Стоит заметить, что используемые в алгоритме SEA для расчёта числа точек ЭК полиномы деления могут быть вычислены заранее, так как зависят только от числа q. Данное обстоятельство позволяет уменьшить количество промежуточных вычислений в алгоритме. В целом, критерии получения параметров ЭК методом «случайного выбора» в настоящее время полностью основываются на вышеприведенных алгоритмах. Исследования в данной области показывают [8,9], что применение указанной стратегии позволяет эффективно решать актуальную задачу получения криптографически стойких параметров ЭК.

СПИСОК ЛИТЕРАТУРЫ

1. Lencier, R. Finding good random elliptic curves for cryptosystems defined F2n [Текст] / Lencier R.; Lecture Notes in Computer Science, 1997, Vol.1233, P. 379–392.

2. Schoof, R. Elliptic curves over finite fields and the computation of square roots mod p [Текст] / Schoof R.; Math. Comp., 1985, Vol. 44, P. 483–494.

3. Schoof, R. Counting points on elliptic curves over finite fields. [Текст] / Schoof R.; Journal de Théorie des Nombres des Bordeaux, 1995, Vol. 7, P. 219–254.

4. Пылин, В.В. Генерация параметров асимметричной криптосистемы на эллиптических кривых [Текст] /В.В Пылин; //Новые информационные технологии в научных исследованиях и в образовании (НИТ-2006): тезисы докладов XI Всерос. науч.-техн. конф. студентов, молодых ученых и специалистов, Фед. агентство по образованию, науки и молодеж. политики, Адм. Рязан. обл., Рязан. гос. радиотехн., университет. Рязань: Рязан. гос. радиотехн. университет, 2006, С. 149–150.

5. Пылин, В.В. Условия эффективной реализации алгоритма Чуфа для расчета числа точек эллиптической кривой над конечным полем [Текст] / В.В. Пылин; Труды международных научно-технических конференций «Интеллектуальные системы» (AIS'06) и «Интеллектуальные САПР» (CAD–2006): в 3 т., М.: Физматлит, 2006, Т.2, С. 163–167.

6. Dewaghe, L. Remarks on the Schoof–Elkies–Atkin algorithm [Текст] / Dewaghe. L; Mathematics of Computation, 1998, Vol. 67(223), P. 1247–1252.

7. Shanks, D. Class number, a theory of factorization and genera [Текст] / Shanks. D.; Proc. Symp. Pure Math, 1971, Vol.20, P. 415–440.

8. Csirik, J. A. An exposition of the SEA algorithm, preprint [Текст] / Csirik. J. A; t, 2000

9. Mueller, V. On the generation of Cryptographically Strong Elliptic Curves [Текст] /Mueller, V. //Technical Report, Technical University of Darmstadt, 1997.

ФУНКЦИИ МОЛИНА ДЛЯ ПРЕДСТАВЛЕНИЙ ЧЕТЫРЕХМЕРНЫХ ТОЧЕЧНЫХ ГРУПП

MOLIN FUNCTIONS FOR REPRESENTATIONS OF FOUR-DIMENSIONAL POINT GROUPS

Кужукеев Ж.М.

Костанайский инженерно-экономический университет им.М.Дулатова, г.Костанай, Казахстан

Построены функции Молина для представлений 4-мерной точечной группы K_{384} и для некоторых магнитных точечных групп.

Функции Молина или производящие функции полиномиальных инвариантов для 3-мерных точечных групп приводятся в работах [1,2]. Разработана теория построения функций Молина для 3-мерных пространственных групп [3]. Непосредственное приложение к физическим проблемам прослеживается в [4,5].

Целью настоящей работы было: 1) вычислить функции Молина для представлений 4-мерной точечной группы K_{384} из списка [6]; 2) используя редукционные соотношения между представлениями группы K_{384} и ее подгруппами [7], построить функции Молина для магнитных точечных групп.

Показано, что информация, содержащаяся в них, облегчает процедуру построения целых рациональных базисов тензорных инвариантов. Так как полезность ЦРБИ для конструирования термодинамического потенциала в теории фазовых переходов несомненна, то можно надеяться на дальнейшее физическое приложение полученных результатов.

I. Степени главных инвариантов группы K_{384}

Опираясь на теорему Шевалле [8], найдем главные инварианты группы K_{384}, так как степени главных инвариантов входят составной частью в формулу функции Молина.

Теорема. Пусть G – конечная, порожденная отражениями, группа в ***n*** – мерном пространстве V над полем K характеристики нуль. Тогда K – алгебра I инвариантов группы G генерируется ***n*** алгебраически независимыми однородными элементами $I_1, I_2, \ldots, I_n$ со степенями $m_1+1, m_2+1, \ldots, m_n+1$, такими, что

$$\prod_{i=1}^{n}(m_l+1)=|G|, \qquad (1)$$

где $|G|$ - порядок группы.