Math-Net.Ru

Общероссийский математический портал

М. В. Николаев, Д. В. Матюхин, О сложности двумерной задачи дискретного логарифмирования в конечной циклической группе с эффективным автоморфизмом порядка 6, *Дискрет. матем.*, 2013, том 25, выпуск 4, 54–65

DOI: <https://doi.org/10.4213/dm1257>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 35.173.219.12

26 апреля 2023 г., 16:47:31

О сложности двумерной задачи дискретного логарифмирования в конечной циклической группе с эффективным автоморфизмом порядка 6

© 2013 г. М. В. Николаев, Д. В. Матюхин

Двумерная задача дискретного логарифмирования в конечной группе G (с аддитивной записью операции) заключается в поиске для заданных $P_1, P_2, Q \in G$, $0 < N_1, N_2 < \sqrt{|G|}$ таких значений n_1, n_2 , что $Q = n_1 P_1 + n_2 P_2$, $-N_1 \leq n_1 \leq N_1$, $-N_2 \leq n_2 \leq N_2$, в предположении, что эти значения существуют. В 2004 году Годри и Шост предложили алгоритм решения этой задачи, средняя трудоемкость которого при стандартных эвристических предположениях равна $(c + o(1))\sqrt{N}$ групповых операций в G , где $c \approx 2.43$, $N = 4N_1N_2$, $o(1) \rightarrow 0$ при $N \rightarrow \infty$. В 2009 году Гэлбрэйт и Рупрай усовершенствовали алгоритм Годри-Шоста, получив $c \approx 2.36$.

В настоящей работе показано, что для группы точек эллиптической кривой над конечным простым полем, имеющей эффективный автоморфизм φ порядка 6, средняя трудоемкость алгоритма Годри-Шоста решения двумерной задачи дискретного логарифмирования при $P_2 = \varphi(P_1)$ и $N_1 = N_2$ не превосходит $(c + o(1))\sqrt{N}$, где $c \approx 0.9781$.

1. Введение

Определение 1. Задача дискретного логарифмирования.

Дано: группа $G = \langle P \rangle$, $Q \in G$.

Найти: $n \in \{0, \dots, |G| - 1\}$ такое, что $Q = nP$.

Определение 2. Двумерная задача дискретного логарифмирования.

Дано: группа G ; $P_1, P_2, Q \in G$, $N_1, N_2 \in \mathbb{N}$, $Q = n_1 P_1 + n_2 P_2$ для некоторых (неизвестных) $n_1 \in \{-N_1, \dots, N_1\}$, $n_2 \in \{-N_2, \dots, N_2\}$.

Найти: такие $n'_1, n'_2 \in \mathbb{Z}$, что $Q = n'_1 P_1 + n'_2 P_2$.

В настоящее время в общем случае наиболее эффективным алгоритмом решения двумерной задачи дискретного логарифмирования является алгоритм Годри-Шоста, предложенный в 2004 году в работе [4]. Основная идея алгоритма может быть сформулирована следующим образом. Сначала выбираются так называемые «домашнее» (tame) и «дикое» (wild) множества:

$$T = \{-N_1, \dots, N_1\} \times \{-N_2, \dots, N_2\},$$

$$W = \{-N_1 + n_1, \dots, N_1 + n_1\} \times \{-N_2 + n_2, \dots, N_2 + n_2\}.$$

Затем параллельно вычисляются псевдослучайные последовательности

$$x_i P_1 + y_i P_2, \quad (x_i, y_i) \in T, \quad i = 1, 2, \dots, \quad (1)$$

$$Q + z_j P_1 + w_j P_2, \quad (z_j, w_j) \in T, \quad (n_1 + z_j, n_2 + w_j) \in W, \quad j = 1, 2, \dots, \quad (2)$$

до тех пор, пока в них не найдутся два одинаковых элемента:

$$x_k P_1 + y_k P_2 = Q + z_l P_1 + w_l P_2, \quad (3)$$

откуда находим $n'_1 = x_k - z_l, n'_2 = y_k - w_l$.

Средняя трудоемкость алгоритма Годри-Шоста и его различных модификаций, измеряемая количеством групповых операций в G , равна по порядку величины среднему значению количества элементов последовательностей, вычисляемых до появления совпадающих элементов, в предположении, что значения (n_1, n_2) , (x_i, y_i) и (z_j, w_j) выбираются случайно, равновероятно и независимо из соответствующих множеств. Это среднее значение определяется с использованием следующего результата Гэлбрэйта и Холмса, являющегося обобщением парадокса дней рождения.

Теорема 1. [1, Theorem 1] *Предположим, что выполнены следующие условия.*

- (1) *В случайной последовательности шаров каждый шар имеет один из C цветов; k -й шар независимо от остальных имеет цвет $s \in \{1, \dots, C\}$ с вероятностью $r_{k,s}$, $k = 1, 2, \dots$. Для любого $s \in \{1, \dots, C\}$, существует $p_s = \lim_{n \rightarrow \infty} n^{-1} \sum_{k=1}^n r_{k,s}$ и $p_1 \geq p_2 \geq \dots \geq p_C > 0$. Пусть $b_{n,s} = p_s - n^{-1} \sum_{k=1}^n r_{k,s}$ и существует такая константа K , что для любых $s \in \{1, \dots, C\}$, $n > 1$ выполняется неравенство $|b_{n,s}| \leq K/n$.*
- (2) *Имеется $N' \in \mathbb{N}$ различных урн. Если k -й шар имеет цвет s , то он попадает в урну с номером i с вероятностью $q_{c,i}(N')$ независимо от цветов и размещений остальных шаров. Существует такое $d > 0$, не зависящее от N' и s , что для любых $s = 1, \dots, C$ и $i = 1, \dots, N'$*

$$0 \leq q_{c,i} \leq d/N'.$$

Существуют такие константы $\alpha, \mu > 0$, что $|\{i \in \{1, \dots, N'\} : q_{1,i}, q_{2,i} \geq \mu/N'\}| \geq \alpha N'$.

Тогда математическое ожидание числа $Z_{N'}$ шаров, размещенных до первого появления двух шаров разных цветов в одной урне, равно

$$\mathbf{M}(Z_{N'}) = \sqrt{\frac{\pi}{2A_{N'}}} + O(N'^{1/4}),$$

где

$$A_{N'} = \sum_{c=1}^C p_c \left(\sum_{c'=1, c \neq c'}^C p_{c'} \left(\sum_{i=1}^{N'} q_{c,i} q_{c',i} \right) \right)$$

и константа в O зависит от $C, p_c, d, K, \alpha, \mu$, но не зависит от N' и $q_{c,i}$.

Средняя трудоемкость алгоритма Годри-Шоста вычислена Гэлбрэйтом и Рупрай в работе [2] и составляет $(2.43 + o(1))\sqrt{N}$, где $N = 4N_1N_2$, $o(1) \rightarrow 0$ при $N_1, N_2 \rightarrow \infty$. В той же работе предложена усовершенствованная версия алгоритма с трудоемкостью $(2.36 + o(1))\sqrt{N}$.

Предположим теперь, что группа G — циклическая простого порядка n и обладает автоморфизмом φ , который можно вычислить за время, существенно меньшее необходимого для выполнения групповой операции, и для которого легко вычислить такое $\lambda \in \{1, \dots, n-1\}$, что φ действует в группе G как умножение на λ . Тогда группа G распадается на непересекающиеся классы эквивалентности (орбиты) относительно действия группы $\langle \varphi \rangle$, и подобно тому, как это делается в работе [6] для классической задачи дискретного логарифмирования, можно ускорить алгоритм, если искать не совпадающие элементы последовательностей (1) и (2), а совпадающие классы эквивалентности этих элементов. Действительно, в этом случае вместо равенства (3) имеем равенство

$$\varphi^s(x_k P_1 + y_k P_2) = Q + z_l P_1 + w_l P_2, \quad (4)$$

для некоторого s , откуда

$$Q = (\lambda^s x_k - z_l) P_1 + (\lambda^s y_k - w_l) P_2,$$

т. е. $n'_1 = \lambda^s x_k - z_l, n'_2 = \lambda^s y_k - w_l$. Примерами таких групп с *эффективными автоморфизмами* являются подгруппы группы точек эллиптических кривых над конечным простым полем $GF(p)$. В частности, операция вычисления обратного элемента является эффективным автоморфизмом порядка 2 для любой такой кривой, а кривая, заданная уравнением $y^2 = x^3 + Ax$, при $p \equiv 1 \pmod{4}$ обладает эффективным автоморфизмом порядка 4. В работе Лиу [5] для этих случаев и $P_2 = \varphi(P_1)$ предложены соответствующие модификации алгоритма Годри-Шоста, имеющие при $N \rightarrow \infty$ трудоемкость при $(1.45 + o(1))\sqrt{N}$ и (при $N_1 = N_2$) $(1.0255 + o(1))\sqrt{N}$ соответственно. В настоящей работе рассматривается эллиптическая кривая E , заданная над $GF(p)$ уравнением $y^2 = x^3 + B$ при $p \equiv 1 \pmod{3}$, обладающая эффективным автоморфизмом φ порядка 6, $\varphi(x, y) = (\beta x, -y)$, где $\beta \neq 1$ — кубический корень из 1 по модулю p , λ — корень уравнения $\lambda^2 - \lambda + 1 \equiv 0 \pmod{n}$. Если $P_2 = \varphi(P_1)$, то

$$\varphi(aP_1 + bP_2) = a(\lambda P_1) + b(\lambda - 1)P_1 = -bP_1 + (a + b)P_2,$$

откуда

$$\begin{aligned} \varphi^2(aP_1 + bP_2) &= -(a + b)P_1 + aP_2, \\ \varphi^3(aP_1 + bP_2) &= -aP_1 - bP_2, \\ \varphi^4(aP_1 + bP_2) &= bP_1 - (a + b)P_2, \\ \varphi^5(aP_1 + bP_2) &= (a + b)P_1 - aP_2, \end{aligned}$$

т. е. класс эквивалентности точки $aP_1 + bP_2$ относительно действия группы $\langle \varphi \rangle$ включает также указанные пять точек. Каждому такому классу эквивалентности соответствует множество (класс) пар

$$C(a, b) = \{(a, b), (-b, a + b), (-(a + b), a), (-a, -b), (b, -(a + b)), (a + b, -a)\}.$$

2. Трудоемкость решения двумерной задачи дискретного логарифмирования с использованием автоморфизма порядка 6

Теорема 2. Пусть G — подгруппа простого порядка n группы точек эллиптической кривой E , заданной над конечным простым полем $GF(p)$ уравнением $y^2 = x^3 + B$ при $p \equiv 1 \pmod{3}$; φ — автоморфизм группы G , $\varphi(x, y) = (\beta x, -y)$, где $\beta \neq 1$ — кубический корень из 1 по модулю p ; λ — такой корень уравнения $\lambda^2 - \lambda + 1 \equiv 0 \pmod{n}$, что $\varphi(x, y) = \lambda(x, y)$. Тогда средняя трудоемкость решения двумерной задачи дискретного логарифмирования в группе G при $N_1 = N_2$, $P_2 = \varphi(\underline{P}_1)$ и случайном равновероятном выборе (n_1, n_2) не превосходит $(0.97811 + o(1))\sqrt{N}$ групповых операций, где $N = 4N_1N_2$, $N \rightarrow \infty$.

Доказательство. В качестве «домашнего» множества T возьмем

$$T = \{C(a, b) : -N_1 \leq a \leq N_1, -N_1 \leq b \leq N_1\}.$$

Заметим, что элементы множества T находятся во взаимно однозначном соответствии с элементами множества представителей классов

$$\tilde{T} = \{0, \dots, N_1\} \times \{0, \dots, N_1\}$$

(в работах [3, 5] такое множество называется фундаментальной областью «домашнего» множества). На рис. 1 изображено объединение классов из множества T (обозначим его T_0), множество $\tilde{T}$ — это часть изображения, ограниченная первым квадрантом плоскости.

Рис. 1

Рис. 2

Определим «дикое» множество

$$W = \left\{ C(n_1 + a, n_2 + b) : -\frac{N_1}{2} \leq a \leq \frac{N_1}{2}, -\frac{N_1}{2} \leq b \leq \frac{N_1}{2} \right\}$$

и множество

$$\widetilde{W} = \left\{ -\frac{N_1}{2} + n_1, \dots, \frac{N_1}{2} + n_1 \right\} \times \left\{ -\frac{N_1}{2} + n_2, \dots, \frac{N_1}{2} + n_2 \right\}$$

(при $n_1 = n_2 = 0$ множество $\widetilde{W}$ изображено на рис. 2 — выделено темно серым цветом).

Как и в алгоритме Годри-Шоста, будем параллельно вычислять последовательности точек

$$x_i P_1 + y_i P_2, \quad (x_i, y_i) \in \widetilde{T}, i = 1, 2, \dots, \quad (5)$$

$$Q + z_j P_1 + w_j P_2, \quad (z_j, w_j) \in \widetilde{W}, j = 1, 2, \dots \quad (6)$$

до тех пор, пока в них не найдутся две точки из одного класса эквивалентности, после чего находим решение задачи как в п. 1. (При этом предполагается, что значения (x_i, y_i) и (z_j, w_j) выбираются случайно, равновероятно и независимо из соответствующих множеств.)

Очевидно, что интересующая нас средняя трудоемкость, выраженная в количестве групповых операций, не превосходит математического ожидания суммарного числа $Z_{N'}$ значений (x_i, y_i) и $(n_1 + z_j, n_2 + w_j)$, выбираемых до появления таких значений (x_k, y_k) и $(n_1 + z_l, n_2 + w_l)$, что $C(x_k, y_k) = C(n_1 + z_l, n_2 + w_l)$.

Вычислим с помощью теоремы 1 условное математическое ожидание $\mathbf{M}(Z_{N'} | (n_1, n_2))$ случайной величины $Z_{N'}$ при фиксированных n_1, n_2 . В обозначениях теоремы в нашем случае $C = 2$: шары цвета 1 — это элементы множества $\widetilde{T}$, а шары цвета 2 — элементы множества $\widetilde{W}$. Так как вычисление последовательностей (5) и (6) происходит параллельно, мы можем считать, что $r_{k,1} = r_{k,2} = \frac{1}{2}$ для всех $k = 1, 2, \dots$, откуда $p_1 = p_2 = \frac{1}{2}$. Множество урн в нашем случае — это $T \cup W$, и шар (a, b) попадает в урну $C(a, b)$. Ясно, что $N' = O(N)$. Для записи далее величины $o(N)$ при $N \rightarrow \infty$ будут опускаться. Тогда имеем: $|T| = |\widetilde{T}| = |\widetilde{W}| = \frac{N}{4}$ и

$$q_{1,i} = \begin{cases} \frac{4}{N}, & \text{если } i \in T, \\ 0 & \text{в противном случае.} \end{cases}$$

С учетом последнего равенства и утверждения теоремы 1 нас интересуют значения $q_{2,i}$ лишь для $i \in T \cap W$. Поскольку каждый класс $C(a, b)$ содержит не более 6 элементов, то $T \cap W$ разбивается на 6 непересекающихся подмножеств $U_j, j = 1, \dots, 6$, так, что в каждый класс из U_j попадает ровно j элементов из $\widetilde{W}$, т.е.

$$q_{2,i} = \frac{4j}{N}, \quad i \in U_j.$$

Из двух последних равенств получаем:

$$A_{N'} = 2 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{4}{N} \cdot \frac{4}{N} \cdot \sum_{j=1}^6 j \cdot |U_j| = \frac{8}{N^2} |U|,$$

где $U = \widetilde{W} \cap T_0$, и по теореме 1 при $N \rightarrow \infty$

$$\mathbf{M}(Z_{N'} | (n_1, n_2)) \sim \sqrt{\frac{\pi}{2A_{N'}}} = \frac{N}{4} \sqrt{\frac{\pi}{|U|}}.$$

Следуя работам [3, 5], положим $n_1 = xN_1, n_2 = yN_1, |x|, |y| \leq 1$ и рассмотрим различные случаи расположения множества U в зависимости от значений x и y .

- 1) $(n_1, n_2) \in B_1 = \{(xN_1, yN_1) : y > \frac{1}{2}, |x| \leq \frac{1}{2}, x < 1 - y\}$. Множество значений (x, y) изображено на следующем рис. 3.

Рис. 3

Рис. 4

Вероятность события $(n_1, n_2) \in B_1$ равна $\frac{3}{32}$. Множества $\widetilde{W}$ и T_0 изображены на следующем рис. 4.

Имеем:

$$|S_1| = \left(\frac{1}{2} + y - 1\right) \left(\frac{1}{2} + x\right) \frac{N}{4} = \left(y - \frac{1}{2}\right) \left(x + \frac{1}{2}\right) \frac{N}{4},$$

$$|S_2| = \left(y - \frac{1}{2}\right) \left(y - \frac{1}{2}\right) \cdot \frac{1}{2} \cdot \frac{N}{4},$$

$$|U| = |\widetilde{W}| - |S_1| - |S_2| = \frac{N}{4} - \left(y - \frac{1}{2}\right) \left(\frac{y}{2} + x + \frac{1}{4}\right) \frac{N}{4} = \frac{N}{8} \left(\frac{9}{4} + x - y^2 - 2xy\right).$$

Тогда условное математическое ожидание величины $Z_{N'}$ при условии $(n_1, n_2) \in B_1$ и $N \rightarrow \infty$ имеет вид

$$\begin{aligned} \mathbf{M}(Z_{N'} | (n_1, n_2) \in B_1) &= \frac{1}{|B_1|} \sum_{(n_1, n_2) \in B_1} \mathbf{M}(Z_{N'} | (n_1, n_2)) \\ &\sim \frac{32}{3N} \sum_{(xN_1, yN_1) \in B_1 \cap \mathbb{Z}^2} \frac{N}{4} \sqrt{\frac{\pi}{\frac{N}{8} \left(\frac{9}{4} + x - y^2 - 2xy\right)}} \\ &\sim \frac{16}{3} \sqrt{\frac{2\pi}{N}} \int_{\frac{N_1}{2}}^{N_1} \int_{-\frac{N_1}{2}}^{(1-y)N_1} \frac{d(xN_1)d(yN_1)}{\sqrt{\left(\frac{9}{4} + x - y^2 - 2xy\right)}} \\ &= \frac{16}{3} \sqrt{\frac{2\pi}{N}} \cdot \frac{N}{4} \int_{\frac{1}{2}}^1 \int_{-\frac{1}{2}}^{(1-y)} \frac{dxdy}{\sqrt{\left(\frac{9}{4} + x - y^2 - 2xy\right)}} \approx \frac{8}{3} \cdot 0.28232 \cdot \sqrt{\frac{\pi N}{2}}. \end{aligned}$$

Осталось заметить, что, в силу симметричности отображения φ есть еще 3 случая с таким же значением условного математического ожидания, т. е. общее количество аналогичных случаев здесь $K_1 = 4$.

- 2) $(n_1, n_2) \in B_2 = \{(xN_1, yN_1) : y > \frac{1}{2}, |x| \leq \frac{1}{2}, x \geq 1 - y\}$. Множество значений (x, y) изображено на рис. 5.

Рис. 5

Рис. 6

Вероятность события $(n_1, n_2) \in B_2$ равна $\frac{1}{32}$. Множества $\widetilde{W}$ и T_0 изображены на рис. 6.

Имеем:

$$\begin{aligned}
 |S_1| &= \left(y - \frac{1}{2}\right) \left(x + \frac{1}{2}\right) \cdot \frac{N}{4}, \\
 |S_2| &= \frac{\frac{1}{2} + y - 1 + \frac{1}{2} + y - 1 - \frac{1}{2} + x}{2} \cdot \left(\frac{1}{2} - x\right) \cdot \frac{N}{4} = \left(\frac{1}{2} - x\right) \left(\frac{x}{2} + y - \frac{3}{4}\right) \cdot \frac{N}{4}, \\
 |U| &= |\widetilde{W}| - |S_1| - |S_2| = \frac{N}{4} - \left(\left(y - \frac{1}{2}\right) \left(x + \frac{1}{2}\right) + \left(\frac{1}{2} - x\right) \left(\frac{x}{2} + y - \frac{3}{4}\right) \right) \cdot \frac{N}{4} = \\
 &= \frac{N}{8} \cdot \left(x^2 - x - 2y + \frac{13}{4}\right).
 \end{aligned}$$

Тогда условное математическое ожидание величины $Z_{N'}$ при условии $(n_1, n_2) \in B_2$ и $N \rightarrow \infty$ имеет вид

$$\begin{aligned}
 \mathbf{M}(Z_{N'} | (n_1, n_2) \in B_2) &= \frac{1}{|B_2|} \sum_{(n_1, n_2) \in B_2} \mathbf{M}(Z_{N'} | (n_1, n_2)) \\
 &\sim \frac{32}{N} \sum_{(xN_1, yN_1) \in B_2 \cap \mathbb{Z}^2} \frac{N}{4} \sqrt{\frac{\pi}{\frac{N}{8} \cdot (x^2 - x - 2y + \frac{13}{4})}} \\
 &\sim 16 \sqrt{\frac{2\pi}{N}} \int_{\frac{N_1}{2}}^{N_1} \int_{(1-y)N_1}^{\frac{N_1}{2}} \frac{d(xN_1)d(yN_1)}{\sqrt{(x^2 - x - 2y + \frac{13}{4})}} \\
 &= 16 \sqrt{\frac{2\pi}{N}} \cdot \frac{N}{4} \int_{\frac{1}{2}}^1 \int_{(1-y)}^{\frac{1}{2}} \frac{dxdy}{\sqrt{(x^2 - x - 2y + \frac{13}{4})}} \approx 8 \cdot 0.1075 \cdot \sqrt{\frac{\pi N}{2}}.
 \end{aligned}$$

Осталось заметить, что, в силу симметричности отображения φ есть еще 3 случая с таким же значением условного математического ожидания, т. е. общее количество аналогичных случаев здесь $K_2 = 4$.

- 3) $(n_1, n_2) \in B_3 = \{(xN_1, yN_1) : y > \frac{1}{2}, x < -\frac{1}{2}, x > -y\}$. Множество значений (x, y) изображено на рис. 7.

Рис. 7

Рис. 8

Вероятность события $(n_1, n_2) \in B_3$ равна $\frac{1}{32}$. Множества $\widetilde{W}$ и T_0 изображены на рис. 8.

Имеем:

$$\begin{aligned}
 |S_1| &= \frac{1}{2} \cdot (x+y)^2 \cdot \frac{N}{4}, \\
 |S_2| &= \left(\frac{1}{2} + x\right) \left(\frac{1}{2} - y\right) \cdot \frac{N}{4}, \\
 |U| &= |\widetilde{W}| - |S_1| - |S_2| = \frac{N}{4} - \left(\frac{1}{2} \cdot (x+y)^2 + \left(\frac{1}{2} + x\right) \left(\frac{1}{2} - y\right)\right) \cdot \frac{N}{4} = \\
 &= \frac{N}{8} \left(\frac{3}{2} - x^2 - y^2 - x + y\right).
 \end{aligned}$$

Тогда условное математическое ожидание величины $Z_{N'}$ при условии $(n_1, n_2) \in$

B_3 и $N \rightarrow \infty$ имеет вид

$$\begin{aligned}
 \mathbf{M}(Z_{N'} | (n_1, n_2) \in B_3) &= \frac{1}{|B_3|} \sum_{(n_1, n_2) \in B_3} \mathbf{M}(Z_{N'} | (n_1, n_2)) \\
 &\sim \frac{32}{N} \sum_{(xN_1, yN_1) \in B_3 \cap \mathbb{Z}^2} \frac{N}{4} \sqrt{\frac{\pi}{\frac{N}{8} \cdot \left(\frac{3}{2} - x^2 - y^2 - x + y\right)}} \\
 &\sim 16 \sqrt{\frac{2\pi}{N}} \int_{\frac{N_1}{2} - yN_1}^{N_1} \int_{-\frac{N_1}{2}}^{-\frac{N_1}{2}} \frac{d(xN_1)d(yN_1)}{\sqrt{\left(\frac{3}{2} - x^2 - y^2 - x + y\right)}} \\
 &= 16 \sqrt{\frac{2\pi}{N}} \cdot \frac{N}{4} \int_{\frac{1}{2}}^1 \int_{-y}^{-\frac{1}{2}} \frac{dxdy}{\sqrt{\left(\frac{3}{2} - x^2 - y^2 - x + y\right)}} \approx 8 \cdot 0.092436 \cdot \sqrt{\frac{\pi N}{2}}.
 \end{aligned}$$

Осталось заметить, что, в силу симметричности отображения φ , есть еще 3 случая с таким же значением условного математического ожидания, т. е. общее количество аналогичных случаев здесь $K_3 = 4$.

- 4) $(n_1, n_2) \in B_4 = \{(xN_1, yN_1) : |y| \leq \frac{1}{2}, |x| \leq \frac{1}{2}\}$. Множество значений (x, y) изображено на рис. 9.

Рис. 9

Рис. 10

Вероятность события $(n_1, n_2) \in B_4$ равна $\frac{1}{4}$. Множества $\widetilde{W}$ и T_0 изображены на рис. 10.

Имеем:

$$|U| = \frac{N}{4}.$$

Тогда условное математическое ожидание величины $Z_{N'}$ при условии $(n_1, n_2) \in B_4$ и $N \rightarrow \infty$ имеет вид

$$\begin{aligned} \mathbf{M}(Z_{N'} | (n_1, n_2) \in B_4) &= \frac{1}{|B_4|} \sum_{(n_1, n_2) \in B_4} \mathbf{M}(Z_{N'} | (n_1, n_2)) \\ &\sim \frac{4}{N} \sum_{(xN_1, yN_1) \in B_4 \cap \mathbb{Z}^2} \frac{N}{4} \sqrt{\frac{\pi}{\frac{N}{4}}} = \frac{N}{4} \sqrt{\frac{\pi}{\frac{N}{4}}} \approx \sqrt{\frac{\pi N}{2}} \cdot 0.7071. \end{aligned}$$

Общее количество аналогичных случаев здесь $K_4 = 1$.

5) $(n_1, n_2) \in B_5 = \{(xN_1, yN_1) : y > \frac{1}{2}, x > \frac{1}{2}\}$. Множество значений (x, y) изображено на рис. 11.

Рис. 11

Рис. 12

Вероятность события $(n_1, n_2) \in B_5$ равна $\frac{1}{16}$. Множества $\widetilde{W}$ и T_0 изображены на рис. 12.

Имеем:

$$|U| = \frac{N}{4} \cdot \left(\frac{3}{2} - x\right) \left(\frac{3}{2} - y\right).$$

Тогда условное математическое ожидание величины $Z_{N'}$ при условии $(n_1, n_2) \in B_5$ и $N \rightarrow \infty$ имеет вид

$$\begin{aligned}
& \mathbf{M}(Z_{N'} | (n_1, n_2) \in B_5) \\
&= \frac{1}{|B_5|} \sum_{(n_1, n_2) \in B_5} \mathbf{M}(Z_{N'} | (n_1, n_2)) \\
&\sim \frac{16}{N} \sum_{(xN_1, yN_1) \in B_5 \cap \mathbb{Z}^2} \frac{N}{4} \sqrt{\frac{\pi}{\frac{N}{4} \cdot \left(\frac{3}{2} - x\right) \left(\frac{3}{2} - y\right)}} \\
&\sim 8 \sqrt{\frac{\pi}{N}} \int_{\frac{N_1}{2}}^{N_1} \int_{\frac{N_1}{2}}^{N_1} \frac{d(xN_1)d(yN_1)}{\sqrt{\left(\frac{3}{2} - x\right) \left(\frac{3}{2} - y\right)}} \\
&= 8 \sqrt{\frac{\pi}{N}} \cdot \frac{N}{4} \int_{\frac{1}{2}}^1 \int_{\frac{1}{2}}^1 \frac{dxdy}{\sqrt{\left(\frac{3}{2} - x\right) \left(\frac{3}{2} - y\right)}} \\
&\approx 4 \cdot \sqrt{\frac{\pi N}{2}} \cdot 0.24264.
\end{aligned}$$

Осталось заметить, что, в силу симметричности отображения φ есть еще 1 случай с таким же значением условного математического ожидания, т. е. общее количество аналогичных случаев здесь $K_5 = 2$.

В итоге получаем

$$\mathbf{M}(Z_{N'}) = \sum_{i=1}^5 \mathbf{P}((n_1, n_2) \in B_i) \cdot M(Z_{N'} | (n_1, n_2) \in B_i) \cdot K_i \approx 0.97811 \cdot \sqrt{N}.$$

Теорема доказана.

Список литературы

1. Galbraith S. D., Holmes M., A non-uniform birthday problem with applications to discrete logarithms.. *Discrete Applied Mathematics* (2012) **160**, №10–11, 1547–1560.
2. Galbraith S. D., Ruprai R. S., An improvement to the Gaudry-Schost algorithm for multidimensional discrete logarithm problems. *Lect. Notes Comput. Sci.* (2009) **5921**, 368–382.
3. Galbraith S. D., Ruprai R. S., Using equivalence classes to accelerate solving the discrete logarithm problem in a short interval. Public key cryptography. *Lect. Notes Comput. Sci.* (2010) **6056**, 368–383.
4. Gaudry P. , Schost E., A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm. *Lect. Notes Comput. Sci.* (2004) **3076**, 208–222.
5. Liu W., *Improved algorithms for the 2-dimensional discrete logarithm problem with equivalence classes*, MSc Thesis, Univ. Auckland, 2010.

6. Wiener M. J., Zuccherato R. J., Faster attacks on elliptic curve cryptosystems. *Lect. Notes Comput. Sci.* (1999) **1556/1999**, 190–200.

Статья поступила 20.11.2012.