ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 31 МАТЕМАТИКИ Выпуск 1
2024

С. А. Орлова, В. В. Маркова (Москва, НИУ ВШЭ). **О вероятности нахождения системы образующих группы $Z_n \oplus Z_n$.**

УДК 512.541.82, 512.542.1, 512.543.14, 519.212.2
DOI https://doi.org/10.52513/08698325_2024_31_1_1

Резюме: Вычислена вероятность того, что два случайных различных элемента группы будут являться системой образующих в группе $\mathbb{Z}_n \oplus \mathbb{Z}_n$, где n является числом свободным от квадратов.

Ключевые слова: Вероятность, системы образующих, конечные абелевы группы.

Для группы $G \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$, где $n = \prod_{i=1}^{k} p_i$ и $\forall i, j,\ i \neq j : p_i \neq p_j$, под системой образующих будем понимать пару таких элементов $g_1, g_2 \in G$, для которых выполняется следующее условие:

$$\forall g \in G,\ \exists! a, b \in \mathbb{Z}_n : a \cdot g_1 + b \cdot g_2 = g.$$

Если g_1 и g_2 являются системой образующих, будем указывать, что $\langle g_1, g_2 \rangle = G$.

Любой элемент G можно представить в виде пары чисел $(a, b) :\ a, b \in \mathbb{Z}_n$. Обозначим за $g_1 = (a_1, b_1)$ и $g_2 = (a_2, b_2)$ элементы, рассматриваемые в данной работе. Вероятность того, что различные элементы g_1, g_2 будут являться системой образующих, вычисляется с помощью методов классической вероятности. Число искомых пар элементов g_1, g_2 находится через последующие теоремы.

Теорема 1. *Всего существует* $\phi(n) \cdot \prod_{i=1}^{k}(1+p_i)$ *элементов* $g_1 = (a_1, b_1)$ *для которых* $\exists g_2 :\ \langle g_1, g_2 \rangle = G$.

Доказательство. Упорядочим простые числа в разложении n так, что если элемент a_1 имеет порядок d, то $d = \prod_{i=1}^{t} p_i$. Тогда существует $\phi(d) = d \cdot \prod_{i=1}^{t}(1 - \frac{1}{p_i})$ элементов, имеющих данный порядок в группе $\mathbb{Z}_n$. Так как НОК $(\operatorname{ord} a_1, \operatorname{ord} b_1)$ обязан быть равным n, $q = \prod_{i=t+1}^{k} p_i$, НОД $(q, b_1) = 1$ в силу того, что для $x \in \mathbb{Z}_n$, порядок x вычисляется как ord $x = \frac{n}{\text{НОД}(x,n)}$ и $q \mid \operatorname{ord} \mathrm{b}_1$.

Число возможных значений, которые принимает элемент b_1 рассчитывается путем решения обратной задачи. Вычтем из n число элементов, которые не взаимопросты с q. Их количество легко найти через формулу включений исключений. Тогда:

$$n - \left(\frac{n}{p_{t+1}} + \frac{n}{p_{t+2}} + \cdots + \frac{n}{p_k} - \frac{n}{p_{t+1} \cdot p_{t+2}} - \cdots - \frac{n}{p_{k-1} \cdot p_k} + \cdots + (-1)^{(k-t-1)} \cdot \frac{n}{q} \right)$$

$$n \cdot \left(1 - \frac{1}{p_{t+1}} - \frac{1}{p_{t+2}} - \cdots - \frac{1}{p_k} + \frac{1}{p_{t+1} \cdot p_{t+2}} + \cdots + \frac{1}{p_{k-1} \cdot p_k} - \cdots + (-1)^{k-t} \cdot \frac{1}{q} \right)$$

$$n \cdot \left(1 - \frac{1}{p_{t+1}}\right) \cdot \left(1 - \frac{1}{p_{t+2}}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$$

Объединяя оба результата, получаем число возможных пар (a_1, b_1), при условии, что ord $a_1 = d$:

$$d \cdot \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right) \cdot n \cdot \prod_{i=t+1}^{k} \left(1 - \frac{1}{p_i}\right) = d \cdot n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = d \cdot \phi(n).$$

Так как $a_1 \in \mathbb{Z}_n$, то порядки элементов принимают значения всех возможных делителей n, а значит полученная ранее формула суммируется по всем возможным d. Сумма всех делителей числа $n = \prod_{i=1}^{k}(1+p_i)$, итоговый результат равен $\phi(n) \cdot \prod_{i=1}^{k}(1+p_i)$.

Теорема 2. *Пусть для $g_1 = (a_1, b_1)$ известно, что $\exists g_2 :$ $\langle g_1, g_2 \rangle = G$. Тогда таких элементов g_2 существует ровно $n \cdot \phi(n)$, где $\phi(n)$ — функция Эйлера.*

Доказательство. Заметим, что НОК(ord a_1, ord b_1) $= n$, так как в противном случае элемент (0,0) может быть получен несколькими способами. Аналогичное условие распространяется для НОК(ord a_1, ord a_2), НОК(ord b_1, ord b_2), так как в этом случае не все элементы из $\mathbb{Z}_n$ будут представлены на первой и второй позициях соответственно.

Пусть ord $a_1 = d = \prod_{i=1}^{t} p_i$, $d \neq n$. Из этого следует, что если $q = \prod_{i=t+1}^{k} p_i$, то $q \,|\, \text{ord}\, a_2$. Также известно, что для $x \in \mathbb{Z}_n$, порядок x вычисляется как ord $x = \frac{n}{\text{НОД}(x,n)}$.

Заметим, что по условию на роль числа a_2 подойдут только такие числа, для которых верно: $q \,|\, \text{ord}\ \ a_2 = \frac{n}{\text{НОД}(a_2,n)}$. Следовательно, НОД (a_2, q) $= 1$. В противном случае, множители входили бы в НОД и не выполнялось бы условие $q \,|\, \text{ord} a_2$.

Найдем числа от 0 до $n-1$, которые взаимопросты с q. Решим эту задачу через обратную: определим количество чисел из заданного интервала, которые не являются взаимно простыми с q. Это числа кратные $p_{t+1}, p_{t+2}, \ldots, p_k, p_{t+1} \cdot p_{t+2}, \ldots, p_{k-1 \cdot k}, \ldots, q$. Посчитать число таких элементов для чисел от 0 до $n-1$ можно с помощью формулы включений-исключений, которая примет итоговый вид:

$$\frac{n}{p_{t+1}} + \frac{n}{p_{t+2}} + \cdots + \frac{n}{p_k} - \frac{n}{p_{t+1} \cdot p_{t+2}} - \cdots - \frac{n}{p_{k-1} \cdot p_k} + \cdots + (-1)^{(k-t-1)} \cdot \frac{n}{q}.$$

Остается вычесть полученное значение из n (числа всех возможных элементов a_2) и получить формулу вида:

$$n - \left(\frac{n}{p_{t+1}} + \frac{n}{p_{t+2}} + \cdots + \frac{n}{p_k} - \frac{n}{p_{t+1} \cdot p_{t+2}} - \cdots - \frac{n}{p_{k-1} \cdot p_k} + \cdots + (-1)^{(k-t-1)} \cdot \frac{n}{q}\right)$$

$$n \cdot \left(1 - \frac{1}{p_{t+1}} - \frac{1}{p_{t+2}} - \cdots - \frac{1}{p_k} + \frac{1}{p_{t+1} \cdot p_{t+2}} + \cdots + \frac{1}{p_{k-1} \cdot p_k} - \cdots + (-1)^{k-t} \cdot \frac{1}{q}\right)$$

$$n \cdot \left(1 - \frac{1}{p_{t+1}}\right) \cdot \left(1 - \frac{1}{p_{t+2}}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$$

Таким образом, мы нашли возможное число значений для a_2. Далее будем считать, что a_1, b_1, a_2 зафиксированы. Заметим, что если $\exists k_1, k_2 (k_1 \neq 0, k_2 \neq 0$ вместе), и $k_1(a_1, b_1) + k_2(a_2, b_2) = (0, 0)$, то (a_1, b_1) и (a_2, b_2) не являются системой образующих согласно определению. Следовательно, в этом случае система уравнений

$$\begin{cases} a_1 \cdot k_1 + a_2 \cdot k_2 = 0 \text{ (mod n)} \\ b_1 \cdot k_1 + b_2 \cdot k_2 = 0 \text{ (mod n)} \end{cases} \tag{1}$$

имеет нетривиальное решение. Согласно китайской теореме об остатках и [1], данную систему уравнений можно решать по модулю каждого из множителей n. Заметим, что если существует хоть одно i, для которого найдется нетривиальное решение системы 1 по модулю p_i, то элементы не будут системой образующих, так как нетривиальное решение будет восстановлено по китайской теореме об остатках.

Согласно ранним утверждениям, ord $a_1 = d = \prod_{i=1}^{t} p_i$, $q = \prod_{i=t+1}^{k} p_i$, q $\mid$ ord a_2. В то же время q $\mid$ a_1, а следовательно для $t+1 \leqslant i \leqslant k$: $a_1 \equiv 0 \mod p_i$, $a_2 \not\equiv 0 \mod p_i$. Кроме того, $b_1 \not\equiv 0 \mod p_i$, иначе бы НОК$(a_1, b_1) \neq n$, из этого следует, что детерминант матрицы $\begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix} \in M_2(\mathbb{F}_{p_i})$ никогда не будет равен 0, а значит не будет существовать нетривиальных решений системы уравнений.

Рассмотрим p_i, где $1 \leqslant i \leqslant t$. В этом случае $a_1 \not\equiv 0 \mod p_i$, а значит существует b_2, при котором $\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = 0 \pmod{p_i}$. Это произойдет при $b_2 = a_1^{-1} \cdot a_2 \cdot b_1 = T$ (все числа являются элементами поля $\mathbb{F}_{p_i}, a_1 \neq 0 \to \exists a_1^{-1}$). Пусть это условие выполняется при: $\begin{cases} b_1 \equiv T_1 \pmod{p_1} \\ b_2 \equiv T_2 \pmod{p_2} \\ \ldots \\ b_t \equiv T_t \pmod{p_t} \end{cases}$

Чисел от 0 до $n-1$, для которых выполняется условие $b_i \equiv T_i \mod p_i$ будет $\frac{n}{p_i}$. С помощью формулы включений-исключений можно найти число элементов, для которых не выполняется ни одно из условий сравнения (что эквивалентно тому, что не существует нетривиального решения изначальной системы):

$$n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \cdots + \frac{n}{p_k} - \frac{n}{p_1 \cdot p_2} - \cdots - \frac{n}{p_{t-1} \cdot p_t} + \cdots + (-1)^{(t-1)} \cdot \frac{n}{d} \right)$$

$$n \cdot \left(1 - \frac{1}{p_1} - \frac{1}{p_2} - \cdots - \frac{1}{p_k} + \frac{1}{p_1 \cdot p_2} + \cdots + \frac{1}{p_{t-1} \cdot p_t} - \cdots + (-1)^t \cdot \frac{1}{d} \right)$$

$$n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_t}\right).$$

Комбинируя число возможных выборов a_2, и значений b_2 при фиксированном a_2, получаем, что способов выбрать пару (a_2, b_2) будет:

$$n \cdot \left(1 - \frac{1}{p_{t+1}}\right) \cdot \left(1 - \frac{1}{p_{t+2}}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) \cdot n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_t}\right)$$

$$= n^2 \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = n \cdot \phi(n).$$

Из теорем [1] и [2] формула искомой вероятности выражается следующим образом:

Утверждение 3. *Два случайных различных элемента группы* $\mathbb{Z}_n \oplus \mathbb{Z}_n$, *где n является числом свободным от квадратов, являются системой образующих с вероятностью* $\frac{\phi^2(n)\cdot\prod_{i=1}^{k}(p_i+1)}{n\cdot(n^2-1)}$.

Доказательство. Число способов выбрать два случайных элемента в группе $\mathbb{Z}_n \oplus \mathbb{Z}_n = \frac{n^2\cdot(n^2-1)}{2}$. Из теорем [1] и [2] следует, что $g_1 = (a_1, b_1)$ можно выбрать $\phi(n)\cdot\prod_{i=1}^{k}(1+p_i)$ способами, а для каждого g_1 есть $n\cdot\phi(n)$ подходящих g_2. Очевидно, что если g_1, g_2 — система образующих, то g_2, g_1 — тоже система образующих. Поэтому пар элементов g_1, g_2, которые образуют систему — $\frac{n\cdot\phi^2(n)\cdot\prod_{i=1}^{k}(1+p_i)}{2}$ Используя формулу классической вероятности, получаем результат:

$$\frac{\frac{n\cdot\phi^2(n)\cdot\prod_{i=1}^{k}(1+p_i)}{2}}{\frac{n^2\cdot(n^2-1)}{2}}$$

$$\frac{\phi^2(n)\cdot\prod_{i=1}^{k}(1+p_i)}{n\cdot(n^2-1)}$$

СПИСОК ЛИТЕРАТУРЫ

1. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. Изд. 2-е, доп. М.: Изд-во МЦНМО, 2006, 333 с.

Поступила в редакцию
04.X.2024

UDC 512.541.82, 512.542.1, 512.543.14, 519.212.2
DOI https://doi.org/10.52513/08698325_2024_31_1_1

Orlova S. A., ***Markova V. V.*** (Moscow, National Research University Higher School of Economics)**. About the probability of finding a generating set of the group** $Z_n \oplus Z_n$.

Abstract: The probability that two different, randomly selected elements of the group $G = \mathbb{Z}_n \oplus \mathbb{Z}_n$ will form a generating set of the group G has been calculated for a square-free integer n.

Keywords: Probability, generating set, finite Abelian groups.