Экспериментальное исследование гипотезы о порядке случайного элемента матричной модулярной группы

С. К. РОСОШЕК
Томский государственный университет
e-mail: rososhek@list.ru

Е. С. ГОРБУНОВ
Томский государственный университет
e-mail: ghostman23@mail.ru

УДК 512.5+00326.09

Ключевые слова: матричная группа, кольцо вычетов, матричные модулярные криптосистемы, порядок элемента группы.

Аннотация

Гипотеза о порядке случайного элемента матричной модулярной группы формулируется следующим образом: случайный элемент матричной группы над кольцом вычетов по модулю n с высокой вероятностью имеет порядок, больший или равный значению функции Эйлера от n. Если эта гипотеза верна, то можно будет существенно ускорить генерацию ключей в матричных модулярных криптосистемах, что повысит эффективность и безопасность этих криптосистем. Эксперименты проводились в пяти матричных модулярных группах по однотипной схеме: сначала формировалась большая выборка случайных элементов группы, а затем вычислялись порядки элементов этой выборки. Результаты экспериментов показывают, что для всех рассмотренных групп порядки случайных элементов удовлетворяют одному и тому же вероятностному распределению. Более того, вероятность того, что случайный элемент группы имеет «большой порядок» (т. е. порядок больше или равен значению функции Эйлера от n), оказалась примерно одинаковой во всех рассмотренных группах, а именно около 0,85.

Abstract

S. K. Rososhek, E. S. Gorbunov, Experimental study of the hypothesis on the order of a random element of the matrix modular group, Fundamentalnaya i prikladnaya matematika, vol. 20 (2015), no. 1, pp. 231—239.

The hypothesis on the order of a random element of the matrix modular group is formulated as follows: a random element of a matrix group over the ring of residues modulo n with high probability has order greater than or equal to the value of the Euler function of n. If this hypothesis is correct, then it will be possible to significantly speed up the generation of the keys in the matrix modular cryptosystems, which will improve both efficiency and security of these cryptosystems. Experiments were carried out in five matrix modular groups by the scheme of the same type: first, a large sample of random elements of the group was formed, and then the orders of the elements of the sample were computed. Experimental results show that for all considered groups the orders of

Фундаментальная и прикладная математика, 2015, том 20, № 1, с. 231—239.
© 2015 *Национальный Открытый Университет «ИНТУИТ»*

random elements satisfy the same probability distribution. Moreover, the probability that a random element of the group has "large order" (i.e., the order is greater than or equal to the value of the Euler function of n) was approximately the same in all considered groups, namely, about 0.85.

1. Введение

Безопасность современных используемых на практике криптосистем с открытым ключом основана преимущественно на двух вычислительно сложных задачах теории чисел: целочисленной факторизации и дискретного логарифмирования. Чаще всего применяются криптосистемы RSA и Эль-Гамаля. Они встраиваются во многие коммерческие продукты, число которых постоянно растёт. Они также используются в операционных системах фирм Apple, Microsoft, Novell, Sun. В аппаратном исполнении эти криптосистемы применяются в защищённых телефонах, на сетевых платах Ethernet, на смарт-картах, широко используются в криптографическом оборудовании. Кроме того, они входят в состав всех основных протоколов для защищённых коммуникаций Internet, в том числе S/MIME, SSL и S/WAN.

Однако при создании достаточно мощного квантового компьютера безопасность этих криптосистем окажется под угрозой, так как в настоящее время существуют квантовые алгоритмы, решающие эти задачи за полиномиальное время [2]. В данный момент создан квантовый компьютер с маленьким количеством кубит, который пока не способен составить реальную угрозу безопасности этих криптосистем. Но, возможно, в скором времени мощность квантового компьютера сильно возрастёт. Квантовые полиномиальные алгоритмы работают в коммутативных алгебраических структурах, так как важная составная часть этих алгоритмов — преобразование Фурье. Преобразование Фурье работает только в коммутативном случае, поэтому для некоммутативного случая необходимы принципиально новые квантовые алгоритмы. Существуют ли такие алгоритмы, неизвестно, во всяком случае, пока опасности со стороны квантового компьютера для некоммутативных алгебраических структур нет.

Возникает необходимость в некоммутативных криптосистемах, которые были бы устойчивы к нападению на квантовом компьютере. Как раз такой криптосистемой является базовая матричная модулярная криптосистема(BMMC) [4], которая построена на некоммутативной группе $\mathrm{GL}_2(\mathbb{Z}_n)$. Также разработана модификация протокола Диффи—Хеллмана обмена ключами, основанная на BMMC [5], которая позволяет устранить не только угрозу со стороны квантового компьютера, но также атаку «человека посередине». Для ускорения шифрования были разработаны различные модификации BMMC. Кроме того, генерация ключей может быть значительно ускорена, если окажется справедливой следующая гипотеза о порядке случайного элемента матричной модулярной группы.

Пусть g — случайный элемент матричной группы над кольцом вычетов по модулю n. Тогда с высокой вероятностью порядок элемента g больше или равен значению функции Эйлера от n.

Будем говорить, что элемент группы $\mathrm{GL}_2(\mathbb{Z}_n)$ имеет «большой порядок», если его порядок больше или равен $\phi(n)$ — значения функции Эйлера от n. Эта статья описывает экспериментальное исследование справедливости этой гипотезы и уточняет её формулировку относительно термина «с высокой вероятностью». Справедливость этой гипотезы (для сокращения назовём её основной гипотезой) проверяется для пяти матричных модулярных групп посредством формирования больших выборок случайных элементов и вычисления их порядков.

2. Алгоритм вычисления порядка элемента

Алгоритм является модификацией известного алгоритма из [3] (алгоритм 4.79), программная реализация которого не всегда давала правильный ответ.

Даны конечная мультипликативная матричная группа G порядка $f(n)$ над кольцом вычетов по модулю n и элемент g группы G.

Функция нахождения порядка.

Вход: модуль n, элемент g, порядок $f(n)$ группы G.

Выход: порядок t элемента g.

1. Присвоить $t \leftarrow f(n)$.
2. Представить t как $t = p_1^{l_1} \cdots p_k^{l_k}$.
3. Для i от 1 до k выполнить следующее:
   1) присвоить $d \leftarrow \frac{t}{p_i}$;
   2) вычислить $g_1 \leftarrow g^d$;
   3) Если $g_1 = 1$, то
      а) опять вызвать функцию $t \leftarrow$ функция нахождения порядка, где на входе $f(n) \leftarrow d$;
      б) выход из цикла.
4. Возврат t.

Замечание. Для вычисления степеней элементов используется алгоритм матричной модулярной экспоненциации. Алгоритм матричной модулярной экспоненциации в $\mathrm{GL}_2(\mathbb{Z}_n)$ получается из алгоритма модулярной экспоненциации в $\mathbb{Z}_n$ (см. [3, алгоритм 2.143]) заменой вычетов из $\mathbb{Z}_n$ матрицами из $\mathrm{GL}_2(\mathbb{Z}_n)$ и заменой модулярного умножения чисел на модулярное умножение матриц.

3. Описание исследования

Исследование проводилось в матричной группе $\mathrm{GL}_2(\mathbb{Z}_n)$ над кольцом вычетов по модулю n для пяти различных значений модуля n следующим образом.

1. Вычислялись определители для всех матриц, построенных из заданного количества случайных элементов a_{11}, a_{12}, a_{21}, a_{22}.
2. С помощью расширенного алгоритма Евклида отсеивались матрицы с необратимым определителем над кольцом вычетов по модулю n.
3. Находился определитель, при котором было минимальное число матриц, и при всех остальных определителях количество матриц сокращалось до такого же числа, т. е. при всех определителях оставалось одинаковое количество матриц.
4. По вышеописанному алгоритму находились порядки для всех полученных матриц.
5. Строилась общая диаграмма для всей выборки и диаграммы для выборок каждого определителя отдельно, рассчитывалась вероятность получения случайной матрицы «большого порядка».

Замечание. Мощность группы $\mathrm{GL}_2(\mathbb{Z}_n)$ в случае $n = p^i$, p — простое число, i — натуральное число, равна

$$f(p^i) = |\mathrm{GL}_2(\mathbb{Z}_{p^i})| = p^{4i-3}(p^2-1)(p-1)$$

(см. [1]). Как следствие, в случае $n = pq$, p, q — простые числа, имеем

$$f(pq) = |\mathrm{GL}_2(\mathbb{Z}_{pq})| = p(p^2-1)(p-1)q(q^2-1)(q-1).$$

4. Результаты исследования

4.1. Исследование для $n = 25$

Берутся матрицы вида

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

где элементы изменяются следующим образом:

— a_{11} пробегает все целые числа от 0 до 24;
— для каждого a_{11} выбирается a_{12}, который пробегает восемь случайных целых чисел в промежутке от 0 до 24;
— для каждого a_{12} выбирается a_{21}, который пробегает восемь случайных целых чисел в промежутке от 0 до 24, и для каждого a_{21} выбирается a_{22}, который пробегает все целые числа от 0 до 24.

Общее число матриц равно 40 000.

После удаления необратимых остаётся 15 528 матриц. После уравнивания числа матриц при каждом определителе остаётся 14 560 матриц. Таким образом, для каждого из 20 обратимых определителей имеется по 728 матриц. Значение функции Эйлера в этом случае равно 20.

Вероятность матриц «большого порядка» (т. е. матриц порядка, большего или равного значению функции Эйлера) равна 0,875068. Вероятность матриц

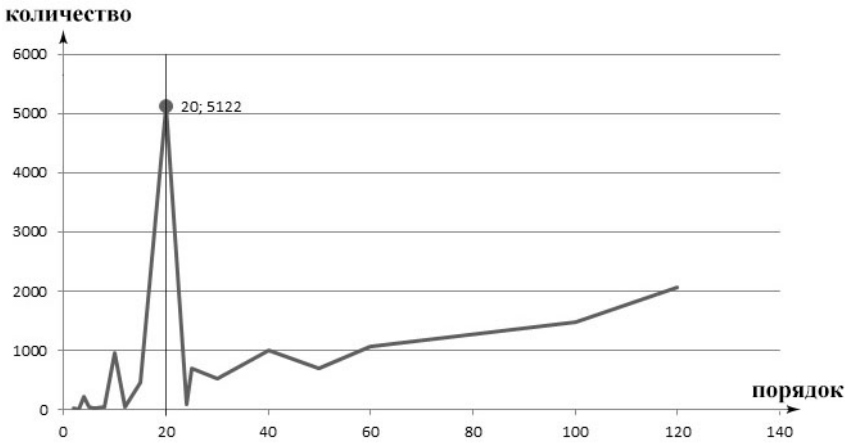

Рис. 1. Диаграмма при $n = 25$

«большого порядка» для каждого определителя отдельно колеблется от 0,699175 до 1.

4.2. Исследование для $n = 121$

Берутся матрицы вида

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

где элементы изменяются следующим образом:

— a_{11} пробегает все целые числа от 0 до 120;
— для каждого a_{11} выбирается a_{12}, который пробегает три случайных целых числа в промежутке от 0 до 120;
— для каждого a_{12} выбирается a_{21}, который пробегает три случайных целых числа в промежутке от 0 до 120, и для каждого a_{21} выбирается a_{22}, который пробегает все целые числа от 0 до 120.

Общее число матриц равно 131 769.

После удаления необратимых остаётся 60 150 матриц. После уравнивания числа матриц при каждом определителе остаётся 55 220 матриц. Таким образом, для каждого из 110 обратимых определителей имеется по 502 матрицы. Значение функции Эйлера в этом случае равно 110.

Вероятность матриц «большого порядка» во всей выборке равна 0,839061. Вероятность матриц «большого порядка» для каждого определителя отдельно колеблется от 0,511952 до 1.

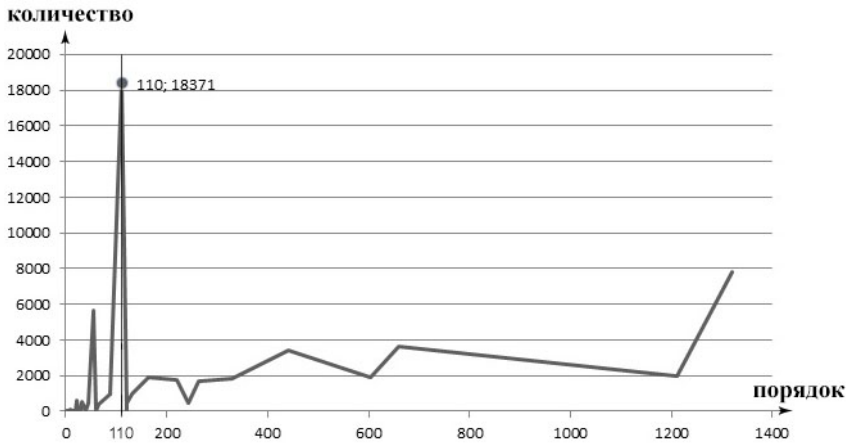

Рис. 2. Диаграмма при $n = 121$

4.3. Исследование для $n = 361$

Берутся матрицы вида

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

где элементы изменяются следующим образом:

— a_{11} пробегает 110 случайных целых чисел от 0 до 360;

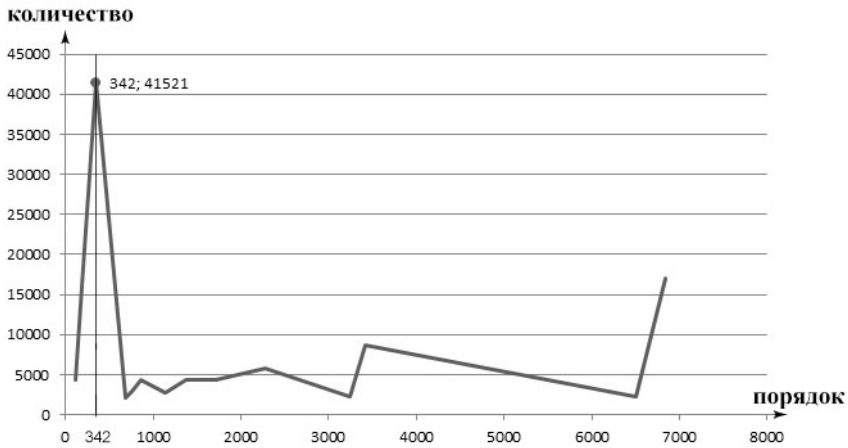

Рис. 3. Диаграмма при $n = 361$

— для каждого a_{11} выбирается a_{12}, который пробегает пять случайных целых чисел в промежутке от 0 до 360;
— для каждого a_{12} выбирается a_{21}, который пробегает пять случайных целых чисел в промежутке от 0 до 360, и для каждого a_{21} выбирается a_{22}, который пробегает 110 случайных целых чисел от 0 до 360.

Общее число матриц равно 302 500.

После удаления необратимых остаётся 150 338 матриц. После уравнивания числа матриц при каждом определителе остаётся 129 276 матриц. Таким образом, для каждого из 342 обратимых определителей имеется по 378 матриц. Значение функции Эйлера в этом случае равно 342.

Вероятность матриц «большого порядка» во всей выборке равна 0,843931. Вероятность матриц «большого порядка» для каждого определителя отдельно колеблется от 0,404761 до 1.

4.4. Исследование для $n = 961$

Берутся матрицы вида

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

где элементы изменяются следующим образом:

— a_{11} пробегает 90 случайных целых чисел от 0 до 960;
— для каждого a_{11} выбирается a_{12}, который пробегает восемь случайных целых чисел в промежутке от 0 до 960;

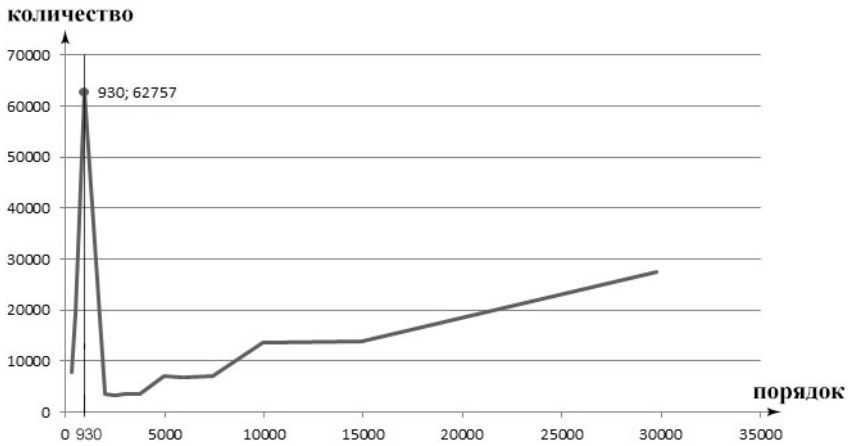

Рис. 4. Диаграмма при $n = 961$

— для каждого a_{12} выбирается a_{21}, который пробегает восемь случайных целых числа в промежутке от 0 до 960, и для каждого a_{21} выбирается a_{22}, который пробегает 90 случайных целых чисел от 0 до 960.

Общее число матриц равно 518 400.

После удаления необратимых остаётся 251 831 матриц. После уравнивания числа матриц при каждом определителе остаётся 201 810 матриц. Таким образом, для каждого из 930 обратимых определителей имеется по 217 матриц. Значение функции Эйлера в этом случае равно 930.

Вероятность матриц «большого порядка» во всей выборке равна 0,848852. Вероятность матриц «большого порядка» для каждого определителя отдельно колеблется от 0,387096 до 1.

4.5. Исследование для $n = 3\,721$

Берутся матрицы вида

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

где элементы изменяются следующим образом:

— a_{11} пробегает 100 случайных целых чисел от 0 до 3 720;
— для каждого a_{11} выбирается a_{12}, который пробегает десять случайных целых чисел в промежутке от 0 до 3 720;
— для каждого a_{12} выбирается a_{21}, который пробегает десять случайных целых чисел в промежутке от 0 до 3 720, и для каждого a_{21} выбирается a_{22}, который пробегает сто случайных целых чисел от 0 до 3 720.

Общее число матриц равно 1 000 000.

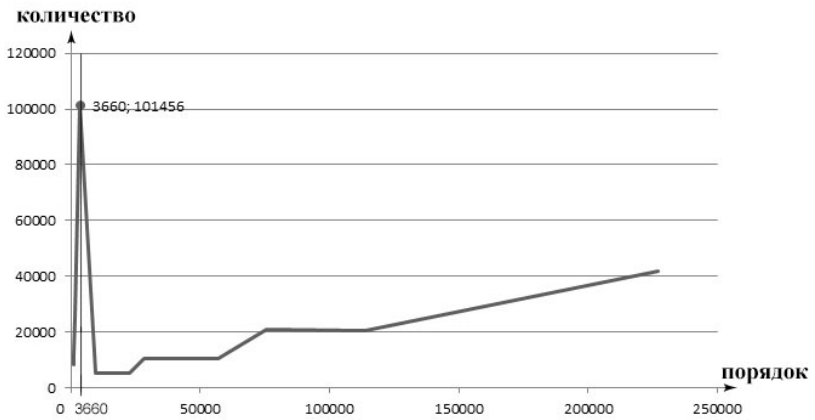

Рис. 5. Диаграмма при $n = 3\,721$

После удаления необратимых остаётся 457 695 матриц. После уравнивания числа матриц при каждом определителе остаётся 322 080 матриц. Таким образом, для каждого из 3 660 обратимых определителей имеется по 88 матриц. Значение функции Эйлера в этом случае равно 3 660.

Вероятность матриц «большого порядка» во всей выборке равна 0,843952. Вероятность матриц «большого порядка» для каждого определителя отдельно колеблется от 0,284090 до 1.

5. Заключение

Для пяти рассмотренных в данной статье матричных модулярных групп случайные элементы больших выборок в этих группах, как видно из соответствующих диаграмм, удовлетворяют одному и тому же вероятностному распределению по отношению к порядкам этих элементов.

Для пяти рассмотренных в данной статье матричных модулярных групп случайный элемент большой выборки в этих группах имеет «большой порядок» с вероятностью около 0,85.

Необходимы дальнейшие экспериментальные и теоретические исследования гипотезы о порядке случайного элемента матричной группы над кольцом вычетов, желательно различными исследователями независимо друг от друга.

Литература

[1] Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. — М.: Наука, 1977.

[2] Квантовый компьютер и квантовые вычисления: Сб. науч. тр. в 2-х тт. Т. 1 / В. А. Садовничий, гл. ред. — Ижевск, 1999.

[3] Menezes A., van Ooshot P., Vanstone S. Handbook of Applied Cryptography. — CRC Press, 1996.

[4] Rososhek S. K. New practical algebraic public key cryptosystem and some related algebraic and computational aspects // Applied Math. — 2013. — Vol. 4, no. 7. — P. 1043—1049.

[5] Rososhek S. K., Gorbunov E. S. Noncommutative analogue of Diffie—Hellman protocol in matrix ring over the residue ring // Int. J. Computers Technology. — 2013. — Vol. 11, no. 10. — P. 3051—3059.