УДК 511

Случайны ли квадратичные вычеты?

В. И. Арнольд

Получено 28 декабря 2009 г.

От редакции: Последняя опубликованная статья Владимира Игоревича Арнольда. Английский перевод напечатан в журнале Regular and Chaotic Dynamics *(2010, vol. 15, no. 4–5, pp. 425–430.). Результаты этой работы были изложены в одноименном докладе В. И. Арнольда, прочитанном 11 января 2010 г. в Москве на Научной конференции «Избранные проблемы современной математики», посвященной 60-летию В. В. Козлова. Видеозапись доклада доступна на Общероссийском математическом портале* Math-Net.Ru.

Ключевые слова: арифметическая динамика, квадратичные вычеты

V. I. Arnol'd
Are quadratic residues random?

Keywords: arithmetical dynamics, quadratic residue, randomness
MSC 2010: 11A07, 1N69

1. Статистика различных квадратичных вычетов

Множество $\mathbb{Z}_n$ (всех n остатков от деления на целое число n, т. е. конечная окружность длины n) содержит подмножество из k квадратичных вычетов по модулю n (т. е. остатков от деления на n всех элементов вида x^2, $x \in \mathbb{Z}_n$, кольца $\mathbb{Z}_n$).

Пример. Число k всех (различных) квадратичных вычетов по модулю $n = 100$ равно 22.

Эти k точек делят конечную окружность длины n на k дуг длин a_j:

$$a_1 + a_2 + \ldots + a_k = n.$$

В предыдущем примере ($n = 100$, $k = 22$) значения $a_j = m$ встречаются $q(m)$ раз, где кратности $q(m)$ таковы:

m	1	2	3	4	5	6	7
q	2	0	5	2	8	0	5

Общее число дуг, $\sum q(m)$, равно 22.

Вопрос о том, случайны ли $k = 22$ точки $\{x^2\}$ на окружности длины $n = 100$, мы исследуем, сравнив распределение $\{q(m)\}$ длин m дуг, на которые эти 22 точки делят окружность длины n, с распределением длин тех $k = 22$ дуг, на которые делят конечную окружность длины $n = 100$ независимые k случайных точек той же окружности.

Ответ оказывается отрицательным: все статистические характеристики наборов квадратичных вычетов резко отличаются от таких же характеристик случайных вычетов.

Легко доказывается (ср. [1, 2]) комбинаторная

Теорема 1. *Числа $\sharp(m)$ дуг длин m, на которые разбивают окружность $\mathbb{Z}_n$ длины n все различные распределения k точек вдоль этой целочисленной окружности, доставляются биномиальными коэффициентами*

$$\sharp(m) = nC_{n-m-1}^{k-2}, \qquad 1 \leqslant m \leqslant n - (k-1).$$

Здесь два распределения не считаются различными, если одно из них переводится в другое поворотом конечной окружности $\mathbb{Z}_n$ (так что общее число дуг различных распределений k точек составляет nC_{n-1}^{k-1}).

Следствие 1. *Доля, $p(m)$, дуг длины m среди всех дуг различных распределений k точек на окружности $\mathbb{Z}_n$ длины n составляет дробь*

$$p(m) = \frac{C_{n-m-1}^{k-2}}{C_{n-1}^{k-1}}.$$

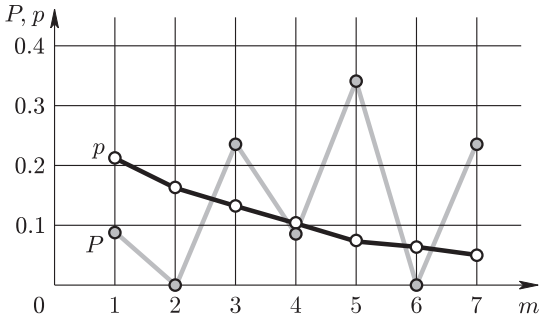
Пример. Для $k = 22$ точек деления окружности длины $n = 100$ доля дуг длины m есть

$$p(m) = \frac{C_{99-m}^{20}}{C_{99}^{21}} :$$

m	1	2	3	4	5	6	7
p	0.212	0.169	0.132	0.105	0.086	0.069	0.052
P	0.09	0	0.23	0.09	0.36	0	0.23

В последней строке таблицы выписаны наблюденные для 22 квадратичных вычетов по модулю 100 доли $P(m) = q(m)/22$ дуг длины m.

Сравнение строчки распределения p длин дуг, порожденных 22 точками, со строчкой P долей длин дуг, порожденных 22 квадратичными вычетами по модулю 100, показывает, что эти два распределения длин дуг имеют совершенно разные статистики:



Мы приходим к выводу, что распределение 22 квадратичных вычетов по модулю 100 совершенно не случайно.

2. Статистика квадратичных вычетов с повторениями

Поскольку $x^2 \equiv (-x)^2$, мы будем рассматривать $k = n/2 = 50$ квадратичных вычетов (с повторениями) по модулю 100.

Эти (не обязательно различные) точки конечной окружности $\mathbb{Z}_n$ делят ее на k «дуг» (считая повторяющиеся квадратичные вычеты)

$$\cdots y_0 < y_1 = y_2 = y_3 = \ldots = y_s < y_{s+1},$$

делящими конечную окружность на «дуги» длин

$$\ldots\ (y_1 - y_0),\ \underbrace{0,\ 0,\ \ldots,\ 0}_{s-1\ \text{раз}},\ (y_{s+1} - y_s),\ \ldots.$$

Это разбиение на k «дуг» мы сравним с аналогичным разбиением, порожденным на конечной окружности $\mathbb{Z}_n$ случайным набором k независимых (не обязательно различных) точек.

Легко доказывается (ср. [1, 2]) комбинаторная

Теорема 2. *Числа $\sharp'(m)$ «дуг» длины m, на которые разбивают окружность $\mathbb{Z}_n$ длины n все различные распределения k (не обязательно различных) точек вдоль этой целочисленной окружности, доставляются биномиальными коэффициентами*

$$\sharp'(m) = nC^{y}_{n+y-m}, \quad \textit{где } y = k-2,\ 0 \leqslant m \leqslant n.$$

Следствие 2. *Доля, $p'(m)$, «дуг» длин m (среди всех дуг различных распределений k не обязательно различных точек на окружности $\mathbb{Z}_n$ длины n) составляет дробь*

$$p'(m) = \frac{C^y_{n+y-m}}{C^{k-1}_{n+k-1}}, \quad \text{где } y = k-2.$$

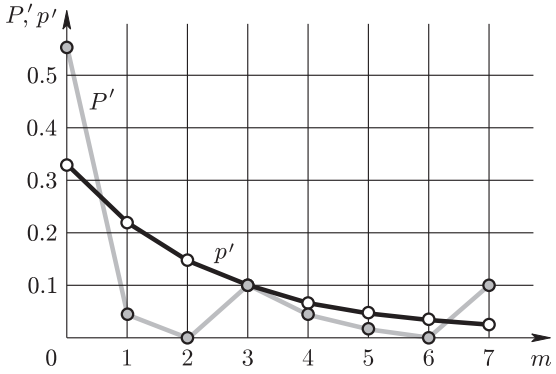
Пример. При $n = 100$, $k = 50$ эти доли таковы:

m	0	1	2	3	4	5	6	7
p'	0.32	0.22	0.15	0.10	0.067	0.044	0.029	0.019
$\sharp'$	28	2	0	5	2	8	0	5
P'	0.56	0.04	0	0.10	0.04	0.16	0	0.10

В строке $\sharp'$ этой таблицы выписаны количества «дуг» длин m, разделяемых пятьюдесятью (не обязательно различными) квадратичными вычетами на конечной окружности $\mathbb{Z}_{100}$ длины 100.

В строке $P'(m)$ указаны доли «дуг» длины $m \geqslant 0$ (среди общего числа 50 «дуг», на которые делят окружность $\mathbb{Z}_{100}$ $k = 50$ не обязательно различных квадратичных вычетов).

Сравнение «теоретической» строки p' (долей различных длин «дуг» m при $k = 50$ случайных точках деления) со строкой P' (долей различных длин «дуг» m при делении окружности $k = 50$ не обязательно различными точками деления) показывает, что их распределения совершенно различны:



Мы приходим к выводу, что распределение P' не обязательно различных квадратичных вычетов, столь же мало похоже на распределение p' такого же числа не обязательно различных случайных точек окружности вычетов, как различаются распределения различных вычетов (без учетов их повторений).

3. Взаимодействие квадратичных вычетов

Рассматривая k точек конечной окружности $\mathbb{Z}_n$ длины n, делящих ее на k дуг длин a_j,

$$a_1 + \ldots + a_k = n,$$

я исследовал (в статье [1]) величину

$$B = a_1^2 + \ldots + a_k^2.$$

Наименьшее возможное значение этой величины, очевидно, равно $B_0 = n^2/k$ (оно достигается на «воинском строе» равноудаленных от соседей точек: $a_j = n/k$). Среднее (по всевозможным расположениям k точек на окружности) значение величины B есть

$$B_1 = \frac{2k}{k+1}\, B_0 \approx 2B_0 \qquad \text{(см. статью [1])}.$$

Составим безразмерный «параметр случайности» $\beta = B/B_0$. Среднее значение этого параметра (для набора большого числа независимых точек деления) есть примерно $\beta = 2$.

Бóльшие среднего значения параметра ($\beta > 2$) указывают на взаимное притяжение точек деления (имеющих тенденцию скапливаться в одно место, вплоть до «полного коллапса» $a_1 = n$, когда $B = n^2$, $\beta = k$).

Меньшие среднего значения параметра ($\beta < 2$) также указывают на взаимодействие точек деления (имеющих тенденцию взаимно отталкиваться, чтобы выстроиться солдатским строем $a_j = n/k$, $B = n^2/k$, $\beta = 1$).

Для исследования степени случайности квадратичных вычетов я сосчитал значения параметра случайности β для набора $k = n/2$ квадратичных вычетов (не обязательно различных) по модулю n.

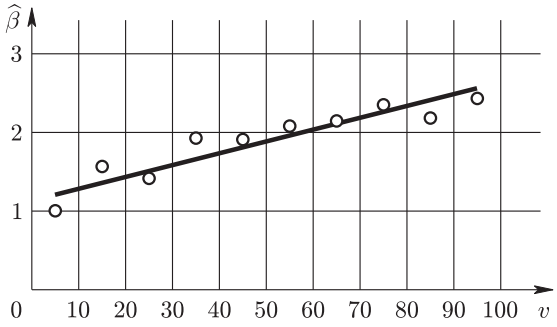
В этом случае $B_0 = n^2/k = 2n$. Чтобы получить бóльшую информацию о поведении параметра $\beta = B/B_0$ при изменении значения n, я усреднил значения $\beta(n)$ по десяткам соседних значений аргумента n:

$$\widehat{\beta}(10u) = \sum_{10(u-1)<n\leqslant 10u} \beta(n).$$

Это усреднение приводит к таким средним значениям параметра β:

u	1	2	3	4	5	6	7	8	9	10
$\widehat{\beta}(10u)$	1.01	1.60	1.44	1.90	1.88	2.10	2.13	2.36	2.20	2.43

График этих средних близок к прямой линии (непонятно почему):



Эта зависимость среднего значения $\widehat{\beta}$ параметра стохастичности от n неплохо аппроксимируется линейной функцией, $\widehat{\beta} \approx 1.22 + n/70$.

Значение $\widehat{\beta}$ равно 2 при $n/70 \approx 0.78$, т. е. при $n = 55$. Мы заключаем, что *$n/2$ квадратичных вычетов по модулю n в среднем отталкиваются друг от друга, пока $n < 50$, и в среднем притягиваются друг к другу, когда $n > 60$.*

Возникает даже гипотеза, что при $n \to \infty$ средние значения параметра стохастичности неограниченно растут: $\widehat{\beta} \to \infty$ (хотя бы для чезаровских средних).

Иными словами, средние *квадратичные вычеты по модулю большого числа, предположительно, притягивают друг друга.*

4. Взаимодействие случайных вычетов

Чтобы сравнить поведение квадратичных вычетов по модулю n с распределением по конечной окружности $\mathbb{Z}_n$ случайных точек, я построил шесть наборов I–VI «псевдослучайных» вычетов при помощи следующего алгоритма.

Начнем с десятичных цифр (u_j, v_j) квадратов всех вычетов

$$j^2 = 10u_j + v_j, \qquad 0 \leqslant j < 100.$$

Из последовательности $n = 100$ десятичных цифр квадратов,

$$(*_{\mathrm{I}}) = \{u_0, v_0, u_1, v_1, \ldots, u_{49}, v_{49}\},$$

составим сто «случайных» двузначных вычетов по модулю 100 следующим образом:

$$(\mathrm{I}) = (10u_0 + v_0, 10v_0 + u_1, 10u_1 + v_1, \ldots)$$

(т. е. читая цифры последовательности $(*_{\mathrm{I}})$ подряд, не обращая внимания на разницу между u и v).

«Псевдослучайную» последовательность $k = 100$ точек (I) в $\mathbb{Z}_n$ можно считать линейным образом системы квадратичных вычетов, и мы будем применять к ней описанную выше теорию параметров стохастичности B и $\beta = B/B_0$, $B_0 = n^2/k$.

Вычисления показывают, что число разных вычетов в последовательности I составляет $l_{\mathrm{I}} = 51$, а сумма квадратов расстояний между ними (на конечной окружности $\mathbb{Z}_n$) есть, при $n = 100$,

$$B_{\mathrm{I}} = 300, \qquad B_{0\,\mathrm{I}} = 100,$$

так что безразмерный параметр стохастичности принимает в этом случае значение

$$\beta_{\mathrm{I}} = 3.00.$$

Для остальных пяти случаев построение «псевдослучайной» последовательности получается из последовательности цифр совершенно таким же образом, только вместо последовательности $(*_{\mathrm{I}})$ берутся ее простые модификации:

$$(*_{\mathrm{II}}) = \{v_0, u_0, v_1, u_1, \ldots, v_{49}, u_{49}\}.$$

Затем последовательность $(*_{\mathrm{I}})$ можно заменить ее левой или правой половиной:

$$(*_{\mathrm{III}}) = (*_{\mathrm{I}'}) = (u_0, v_0, \ldots, u_{24}, v_{24}),$$
$$(*_{\mathrm{IV}}) = (*_{\mathrm{I}>>}) = (u_{25}, v_{25}, \ldots, u_{49}, v_{49}).$$

Аналогичным образом из последовательности $(*_{\mathrm{II}})$ строятся последовательности

$$(*_{\mathrm{V}}) = (*_{\mathrm{II}'}) = (v_0, u_0, \ldots, v_{24}, u_{24}),$$
$$(*_{\mathrm{VI}}) = (*_{\mathrm{II}>>}) = (v_{25}, u_{25}, \ldots, v_{49}, u_{49}).$$

Проделав эти вычисления, я получил следующие ответы:

	I	II	III	IV	V	VI
B_0	100	100	200	200	200	200
B	300	202	366	374	484	394
l	51	47	39	40	37	38
β	3.00	2.02	1.83	1.87	2.42	1.97
n	100	100	100	100	100	100
k	100	100	50	50	50	50

Полученные значения показателя стохастичности β оказались для наших псевдослучайных последовательностей не слишком далекими от среднего значения $\beta \approx 2$ для истинно случайных последовательностей. Среднее арифметическое наших значений

$$\beta_* = \frac{\beta_{\mathrm{I}} + \beta_{\mathrm{II}} + \ldots + \beta_{\mathrm{VI}}}{6} = 2.185$$

незначительно отличается от $\beta = 2$.

Последовательности II–VI уже более или менее забывают свое происхождение из исходной последовательности квадратичных вычетов, I.

Найденные выше для исходных квадратичных вычетов значения усредненного параметра стохастичности

$$\widehat{\beta} \approx 1.22 + \frac{u}{70}$$

(доставляющие сильно бóльшие 2 значения параметра стохастичности при $n > 60$) свидетельствуют о серьезном взаимодействии (притяжении) квадратичных вычетов по большому модулю, отсутствующем у независимо выбранных случайных вычетов по тому же модулю (выбранных в таком же числе).

Список литературы

[1] Арнольд В. И. Группы Эйлера и арифметика геометрических прогрессий. М.: МЦНМО, 2003. С. 18–22.

[2] Arnold V. I. Ergodic and arithmetical properties of geometric progression's dynamics // Mosc. Math. J., 2005, vol. 5, no. 1, pp. 5–22.