Взаимное отталкивание примитивных вычетов

В. И. Арнольд

Исследование распределения остатков от деления на натуральное число n, которые взаимно просты с n, среди всех n остатков $\{0, 1, \ldots, n-1\}$, показывает, что взаимно простые с n остатки распределены вдоль конечной окружности $\mathbb{Z}_n$ длины n совсем не так, как были бы распределены независимые случайные точки, расположенные на этой окружности в таком же количестве. А именно, взаимно простые с n остатки отталкивают своих соседей.

Ключевые слова: Стохастичность, число Рейнольдса, распределение Колмогорова, равномерная распределенность, дзета-функция Эйлера, группы Эйлера.

Примитивными вычетами по модулю n я называю взаимно простые с натуральным числом n остатки от деления на n. Например, при $n = 100$ имеется $k = 40$ примитивных вычетов, а именно:

$x = 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49,$
$51, 53, 57, 59, 61, 63, 67, 69, 71, 73, 77, 79, 81, 83, 87, 89, 91, 93, 97, 99.$

Ниже обсуждается вопрос, *случайно ли распределены среди n точек конечной окружности длины n, $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, состоящей из всех остатков от деления на n, эти $k(n)$ примитивных вычетов (взаимно простых с n)*.

Примеры показывают, что, хотя примитивные вычеты расположены среди всех вычетов довольно равномерно, их распределение статистически сильно отличается от распределения такого же числа $k(n)$ независимых случайных точек на целочисленной окружности $\mathbb{Z}_n$ длины n.

А именно, примитивные вычеты *взаимно отталкиваются*, малые расстояния между соседними примитивными вычетами встречаются гораздо реже, чем они встречаются для случайных выборок такого же числа $k(n)$ независимых точек в $\mathbb{Z}_n$.

Рукопись В. И. Арнольда отредактирована С. В. Конягиным. Редколлегия сборника «Математическое просвещение» выражает глубокую благодарность С. В. Конягину за помощь в подготовке к печати этой работы.

§ 1. Вычисление безразмерного параметра случайности β

Для k точек на целочисленной окружности длины n обозначим через $(a_1, a_2, \ldots, a_k)$ длины дуг, на которые эти точки делят окружность, т. е. расстояния между соседними точками. Таким образом

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

Пример. Для сорока примитивных вычетов по модулю $n = 100$ предыдущий список доставляет сорок последовательных дуг с длинами

2, 4, 2, 2, 2, 4, 2, 2, 2, 4, 2, 2, 2, 4, 2, 2, 2, 4, 2, 2, 2,
4, 2, 2, 2, 4, 2, 2, 2, 4, 2, 2, 2, 4, 2, 2, 2, 4, 2, 2

(расстояние между остатками 99 и 1 на окружности $\mathbb{Z}_{100}$ равно 2).

Рассмотрим сумму квадратов длин всех этих k дуг, на которые делят целочисленную окружность длины n примитивные вычеты по модулю n:

$$B = a_1^2 + a_2^2 + \ldots + a_k^2.$$

Эта сумма квадратов сильно зависит от распределения изучаемых k точек на окружности $\mathbb{Z}_n$.

В предыдущем примере (где $n = 100$) мы замечаем десять троек последовательных дуг длины 2, дающие в сумму квадратов длин дуг вклад

$$10(4 + 4 + 4) = 120,$$

и еще десять дуг длины 4, дающие вклад

$$10 \cdot 16 = 160.$$

Таким образом, при $n = 100$ мы вычислили значение

$$B(100) = 120 + 160 = 280.$$

Можно доказать (см., например, [1]), что значение B всегда заключено между наименьшим значением

$$B_0 = \frac{n^2}{k}$$

и наибольшим значением (превосходящим наименьшее в k раз),

$$B_1 = n^2.$$

Чтобы определить безразмерный аналог «числа Рейнольдса» (позволяющий сравнивать распределения k точек на окружностях $\mathbb{Z}_n$ разных длин n), я предложил в [1] рассматривать «безразмерный параметр стохастичности»

$$\beta = B/B_0 = B/(n^2/k).$$

В рассмотренном выше примере ($n = 100$, $k = 40$) получаются такие значения:

$$B_0 = \frac{100^2}{40} = 250, \quad \beta = \frac{B}{250} = 1{,}120.$$

Для случайных k точек, независимо набросанных на окружность длины n, в [1] вычислены средние значения параметров стохастичности,

$$\widehat{B} = \hat{\beta} B_0$$

(оказалось, что $\hat{\beta} \approx 2$ при больших k).

А именно, там доказано, что математическое ожидание значения безразмерного параметра стохастичности составляет

$$\hat{\beta} = \frac{2k}{k+1}\,.$$

В приведенном выше примере значение параметра $\beta = 1{,}12$ гораздо меньше среднего значения $\hat{\beta} \approx 1{,}951$ (из-за того, что примитивные вычеты далеко не независимы, а «отталкиваются» от своих соседей).

Если для набора k точек в $\mathbb{Z}_n$ наблюдается значительно меньшее, чем $\hat{\beta}$ (т. е. чем 2) значение безразмерного параметра стохастичности β, то это свидетельствует об отталкивании соседних точек. А если наблюдается значительно большее, чем $\hat{\beta}$ (т. е. чем 2) значение β, то это свидетельствует об их взаимном притяжении.

Мы увидим сейчас, что для примитивных вычетов получаются значительно меньшее, чем 2, значения безразмерного параметра стохастичности β.

В следующих таблицах приведены значения параметров (n, k, B, β) для примитивных остатков от деления на n целых чисел, $2 \leqslant n \leqslant 31$.

Число α_a в этих таблицах означает число дуг длины a (при $n = 100$ вышеприведенный список доставляет

$$\alpha_2 = 30, \quad \alpha_4 = 10.)$$

Всегда выполняются соотношения

$$\sum \alpha_a = k, \quad \sum a\alpha_a = n, \quad \sum a^2\alpha_a = B.$$

Еще Эйлер заметил (в своей работе о дзета-функции), что в среднем

$$\frac{k}{n} \approx \frac{6}{\pi^2} = \frac{1}{\zeta(2)} \approx 0{,}608$$

(при больших n), а также, что для простого $n = p$ выполнены соотношения

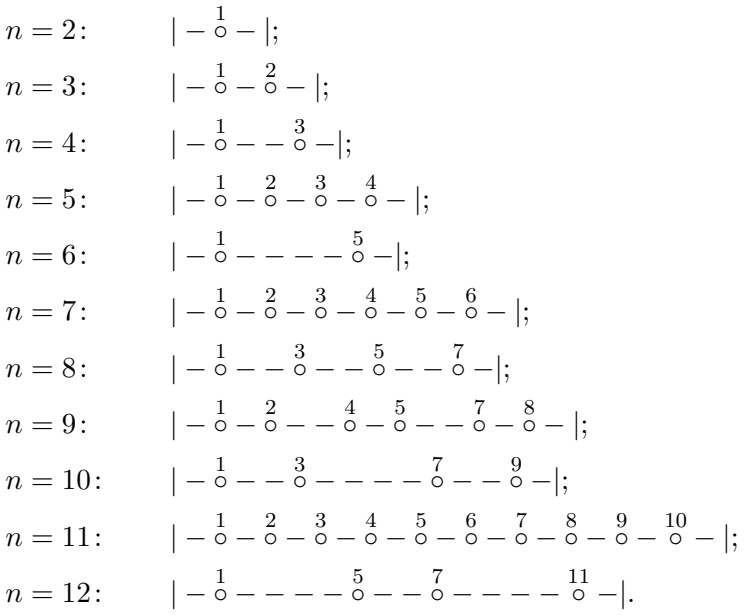
$$k(p) = p - 1, \quad k(p^\omega) = (p-1)p^{\omega-1},$$

и что «φ-функция» $k = k(n)$ мультипликативна:

$$k(uv) = k(u)k(v),$$

если u и v взаимно просты (обычное в теории чисел обозначение этой мультипликативной функции k аргумента n есть $\varphi(n)$).

Вычисление указанных в таблицах значений повторяет приведенное выше в случае $n = 100$ прямое перечисление примитивных вычетов, но оно проще, так как значения k меньше. Например, примитивные вычеты по модулям $n = 2, \dots, 12$ образуют такие картинки



Подобные рисунки доставляют следующие значения параметров стохастичности систем примитивных вычетов:

n	2	3	4	5	6	7	8	9	10	11
k	1	2	2	4	2	6	4	6	4	10
B	4	5	8	7	20	9	16	15	28	13
B_0	4	4,5	8	6,25	18	8,167	16	13,5	25	12,1
β	1	1,111	1	1,120	1,111	1,102	1	1,111	1,120	1,074
α_1	0	1	0	3	0	5	0	3	0	9
α_2	1	1	2	1	1	1	4	3	3	1
α_3	0	0	0	0	0	0	0	0	0	0
α_4	0	0	0	0	1	0	0	0	1	0
Δ	2	2	2	2	4	2	2	2	4	2

Величина Δ в этой таблице — длина наиболее длинной из дуг, на которые примитивные вычеты делят окружность $\mathbb{Z}_n$.

При бóльших значениях n встречаются и более длинные дуги.

n	12	13	14	15	16	17	18	19	20	21
k	4	12	6	8	8	16	6	18	8	12
B	40	15	36	33	32	19	60	21	56	43
B_0	36	14,1	32,67	28,125	32	18,06	54	20,05	50	36,75
β	1,111	1,065	1,102	1,173	1	1,052	1,111	1,047	1,12	1,17
α_1	0	11	0	3	0	15	0	17	0	5
α_2	2	1	5	3	8	1	3	1	6	5
α_3	0	0	0	2	0	0	0	0	0	2
α_4	0	0	1	0	0	0	3	0	2	0
Δ	4	2	4	3	2	2	4	2	4	3

Третий десяток значений n приводит к следующим значениям параметров стохастичности:

n	22	23	24	25	26	27	28	29	30	31
k	10	22	8	20	12	18	12	28	8	30
B	52	25	80	35	60	45	72	31	132	33
B_0	48,4	24,04	72	31,25	56,333	40,5	65,333	30,036	112,5	32,033
β	1,074	1,059	1,111	1,12	1,065	1,111	1,102	1,032	1,173	1,030
α_1	0	21	0	15	0	9	0	27	0	29
α_2	9	1	4	5	11	9	10	1	3	1
α_3	0	0	0	0	0	0	0	0	0	0
α_4	1	0	4	0	1	0	2	0	3	0
α_5	0	0	0	0	0	0	0	0	0	0
α_6	0	0	0	0	0	0	0	0	2	0
Δ	4	2	4	2	4	2	4	2	6	2

Сопоставляя найденные выше значения безразмерного параметра стохастичности β, мы замечаем, что, хотя все они гораздо меньше критического значения 2, они заметно осциллируют при изменении числа n.

Чтобы сгладить эти осцилляции и выявить систематическое поведение чисел $\beta(m)$, составим их чезаровские средние

$$\hat{\beta}(n) = \left(\sum_{m=2}^{n} \beta(m)\right) / \left(\sum_{m=2}^{n} 1\right) = \sum_{m=2}^{n} \beta(m)/(n-1).$$

В следующих таблицах приведены значения сумм

$$\Sigma(n) = \sum_{m=2}^{n} \beta(m)$$

и значения чезаровских средних

$$\hat{\beta}(n) = \Sigma(n)/(n-1) :$$

n	2	3	4	5	6	7	8	9	10	11
$\Sigma(n)$	1,00	2,111	3,111	4,231	5,342	6,444	7,444	8,565	9,675	10,749
$\hat{\beta}(n)$	1,00	1,056	1,037	1,058	1,068	1,074	1,063	1,069	1,075	1,075

Второй десяток значений n доставляет еще более медленный рост чезаровских средних $\hat{\beta}(n)$:

n	12	13	14	15	16	17	18	19	20	21
$\Sigma(n)$	11,860	12,925	14,027	15,20	16,20	17,252	18,363	19,5	20,62	21,79
$\hat{\beta}(n)$	1,075	1,077	1,079	1,086	1,080	1,078	1,080	1,083	1,085	1,089

Третий десяток значений n почти прекращает рост значений чезаровских средних $\hat{\beta}(n)$:

n	22	23	24	25	26	27	28	29	30	31
$\Sigma(n)$	22,864	23,929	25,034	26,154	27,219	28,33	29,432	30,464	31,537	32,567
$\hat{\beta}(n)$	1,089	1,087	1,088	1,089	1,089	1,090	1,090	1,088	1,089	1,086

В пределах первого десятка значений ($2 \leqslant n \leqslant 11$) величина чезаровского среднего $\hat{\beta}(n)$ возрастает от 1 до 1,075, т. е. на 0,075. В пределах второго десятка значений ($12 \leqslant n \leqslant 21$) величина чезаровского среднего $\hat{\beta}(n)$ возрастает на 0,011, т. е. примерно в семь раз меньше, чем в предыдущем десятке. При дальнейшем росте n (в пределах $22 \leqslant n \leqslant 31$) прирост значения чезаровского среднего $\hat{\beta}(n)$ мало заметен.

Все это позволяет предположить, что чезаровское среднее $\hat{\beta}(n)$ остается и при больших значениях n ограниченным (и даже недалеким от 1).

Чтобы эмпирически проверить эту гипотезу, я вычислил значения параметров стохастичности для $n = 100$ и для окрестности этого значения, $96 \leqslant n \leqslant 104$. Вот полученные 9 значений безразмерного параметра стохастичности β:

n	96	97	98	99	100	101	102	103	104
k	32	96	42	60	40	100	32	102	48
B	320	99	252	189	280	103	372	105	290
B_0	288	$96\frac{1}{96}$	$228\frac{2}{3}$	163,35	250	102,01	$325\frac{1}{8}$	104,09	$225\frac{1}{3}$
β	1,111	1,010	1,102	1,157	1,120	1,0097	1,144	1,0087	1,065
Δ	4	2	4	3	4	2	6	2	4
σ	1,111	2,121	3,223	4,380	5,500	6,510	7,654	8,663	9,728

Здесь $\sigma(n) = \sum\limits_{m=96}^{n} \beta(m)$. Поэтому среднее значение $\hat{\hat{\beta}}$ параметра β по указанной девятке значений n (вблизи $n = 100$) составляет

$$\hat{\hat{\beta}}(100) = \frac{\sigma(104)}{9} \approx 1{,}081.$$

Мы видим, что средние значения безразмерного показателя стохастичности $\beta(n)$ (системы примитивных вычетов по модулю n) мало отличаются друг от друга при $n \approx 20$ и при $n \approx 100$. Это подтверждает высказанную выше гипотезу о стабилизации $\hat{\beta}(n)$ при $n \to \infty$ (утверждающую, что значения $\hat{\beta}(n)$ не только остаются ограниченными при $n \to \infty$, но что они приближаются к стабильному значению $\beta^* \approx 1{,}08$).

Однако даже такая стабилизация чезаровских средних не означает еще стремления к пределу самих значений показателя стохастичности $\beta(n)$: они могут сильно отличаться от средних $\hat{\beta}(n)$ столь редко, что эти различия не разрушат стабилизации $\hat{\beta}(n) \to \beta^*$.

В [7] показано, что величины $\beta(n)$ ограничены и, более того, $\beta(n) \to 2$, где предел берется по любой подпоследовательности значений n, для которых $k(n)/n \to 0$. По-видимому, используя технику статьи [7], можно доказать, что $\beta(n) < 2$ и $\hat{\beta}(n)$ близко к 1 при всех n, но это потребует больших компьютерных вычислений.

§ 2. Параметр стохастичности Колмогорова λ

А. Н. Колмогоров [6] ввел свой параметр стохастичности λ в работе 1933 г., опубликованной по-итальянски в журнале страховой статистики. Он использовал этот параметр для решения практически важного вопроса, правдоподобно ли утверждение о случайном происхождении данной числовой последовательности $\{x_1, x_2, \ldots\}$.

Для k вещественных чисел x_i $(1 \leqslant i \leqslant k)$ Колмогоров определил значение своего параметра λ следующей конструкцией. Обозначим через f_k «эмпирическую считающую функцию» данного набора k точек, определенную условием

$$f_k(x) = (\text{число не превосходящих } \ x \ \text{ значений } \ x_i).$$

Колмогоров обсуждает вопрос о правдоподобности гипотезы, что $\{x_i\}$ суть k независимых значений случайной величины x, распределенной на вещественной оси с данной непрерывной функцией распределения F:

$$F(X) = (\text{вероятность события } \ x \leqslant X).$$

Составим «теоретическую считающую функцию»

$$F_k(X) = kF(X)$$

(это значение есть математическое ожидание числа меньших или равных X значений x_i в выборке из k независимых значений с данным распределением F).

Для вычисления своей характеристики λ множества k вещественных чисел x_i Колмогоров упорядочивает их (так, чтобы $x_1 \leqslant x_2 \leqslant \dots x_k$).

Если все k значений x_i различны, то ступенчатая считающая функция f_k равна 0 в точках $x < x_1$, 1 в точках полуинтервала $x_1 \leqslant x < x_2$, 2 в точках полуинтервала $x_2 \leqslant x < x_3$ и т. д., до значения k в точках $x \geqslant x_k$. Считающая функция f_k множества $k = 4$ взаимно простых с числом $n = 10$ вычетов по модулю 10 имеет график, изображенный на рис. 1.

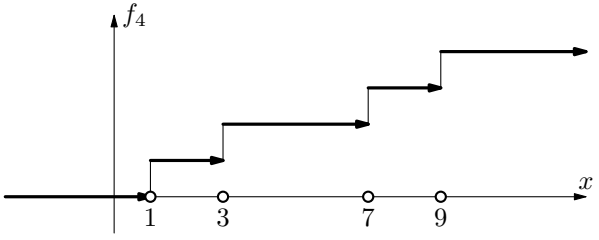


Рис. 1.

Если же в наборе $\{x_i\}$ есть повторения, то величина $f_k(z+0)-f_k(z-0)$ скачка в точке z равна числу совпавших с z точек изучаемого набора (т. е. числу тех i, для которых $x_i = z$).

Основной шаг в конструкции Колмогорова — исследование отличия эмпирической считающей функции f_k от теоретической считающей функции F_k.

Определение 1. *Отклонение Колмогорова* S_k определяется (для k точек $\{x_i\}$) как

$$S_k = \sup_{x\in\mathbb{R}} |f_k(x) - F_k(x)|.$$

Определение 2. *Параметр Колмогорова* λ_k имеет (для данного набора k точек $\{x_i\}$) значение

$$\lambda_k = S_k/\sqrt{k}.$$

Замечание. Деление на квадратный корень из k позволяет сравнивать между собою (по значению параметра стохастичности λ) наборы из разного числа точек $\{x_i\}$.

Дело в том, что разность $f_k - F_k$ можно представить как сумму k независимых слагаемых порядка 1 с математическим ожиданием ноль для

каждого слагаемого (считающих по 1 точке в каждом слагаемом). По закону больших чисел типичные значения этой суммы имеют порядок величины $\sqrt{k}$ (и они велики при больших k).

Деление на $\sqrt{k}$ уничтожает это масштабирующее влияние числа k изучаемых точек — велико или мало значение λ_k определяется не тем, велико или мало число k точек x_i, а тем, насколько они случайны.

Колмогоров в [6] доказал, что для k независимых случайных величин x_i с одинаковой непрерывной функцией распределения F получаемые из разных выборок k точек $\{x_i\}$ значения параметра стохастичности λ_k имеют (на положительной полуоси $\Lambda \geqslant 0$) универсальную функцию распределения Φ_k (не зависящую от F_k), а при $k \to \infty$ эти функции стремятся к универсальной функции распределения Колмогорова

$$\Phi(\Lambda) = \sum_{s=-\infty}^{+\infty} \Big((-1)^s e^{-2s^2\Lambda^2} \Big).$$

Здесь функции распределения Φ_k определяются условиями

$$\Phi_k(\Lambda) = (\text{вероятность события } \ \lambda_k \leqslant \Lambda).$$

Сходимость $\Phi_k \to \Phi$ (при $k \to \infty$) — равномерная (на полуоси $\Lambda \geqslant 0$).

Функция Φ монотонно растет от $\Phi(0) = 0$ (где равны нулю и все ее производные) до $\Phi(\infty) = 1$.

Среднее значение так распределенной величины Λ равно

$$\widehat{\Lambda} = \sqrt{\pi/2}\ln 2 \approx 0{,}869.$$

Вдали от среднего значения $\widehat{\Lambda}$ функция Φ быстро стремится к 0 (слева) и к 1 (справа). Например,

$$\Phi(0{,}4) \approx 0{,}003, \quad \Phi(1{,}8) \approx 0{,}997.$$

Поэтому как слишком малые значения параметра Колмогорова λ_k данного набора $\{x_i\}$, так и слишком большие значения указывают на малое правдоподобие стохастичности изучаемого набора k чисел $\{x_i\}$.

Вот значения функции Φ в некоторых точках Λ:

Λ	0,4	0,6	0,8	1,0	1,2	1,4	1,6	1,8	2,0
$10^4\Phi$	28	1357	4558	7300	8877	9603	9888	9969	9993

Медианное значение Λ^* параметра стохастичности Колмогорова (для которого как меньшие, так и большие его значения параметра стохастичности в распределении Колмогорова Φ имеют одинаковую вероятность $1/2$) составляет $\Lambda^* \approx 0{,}83$.

Описанная выше теорема Колмогорова [6] (об универсальном распределении Φ) доказана им в предположении непрерывности функции

распределения F независимых вещественных величин x_i (релятивистское соображение состоит в том, что величины с разными такими распределениями превращаются друг в друга заменами координат на оси x). Поэтому не зависящие от выбора координаты на оси x величины (вроде колмогоровского отклонения S и параметра Колмогорова λ) ведут себя для любого непрерывного распределения так же, как для равномерного распределения вдоль некоторого отрезка (где все вычисления сводятся к суммированию объемов симплексов, биномиальным коэффициентам и формуле Стирлинга для их асимптотик).

Я же собираюсь (незаконно) применить эту теорию к наборам точек на конечных окружностях $\mathbb{Z}_n$, к которым она формально не относится.

Прежде всего, вычеты образуют дискретное множество, так что функция распределения никак не может быть непрерывной. Я надеюсь, однако, что при больших n конечная окружность $\mathbb{Z}_n$ приближается к вещественной окружности S^1, и что естественно-научные факты, доказанные для предельного случая непрерывного множества значений x_i, дают хорошее приближение к положению дел для значений, принадлежащих к дискретным множествам значений, аппроксимирующим непрерывные.

Другая трудность состоит в том, что конечная окружность $\mathbb{Z}_n$ аппроксимирует не прямую $\mathbb{R}$, к которой относится теория Колмогорова, а гладкую окружность S^1. Беда здесь в топологическом различии: одномерная группа когомологий окружности нетривиальна и заданные на ней распределения обычно не имеют поэтому однозначных функций распределения.

Ведь функция распределения — это первообразная его плотности, так что это многозначная функция на накрывающей окружность прямой при полном обходе окружности получает приращение (равное массе изучаемого распределения на окружности).

Чтобы преодолеть эту топологическую трудность, я использовал следующую конструкцию.

Рассмотрим на окружности два распределения одинаковой суммарной массы (в нашем случае одно из распределений дискретное, сосредоточенное в точках x_i, а другое — непрерывное).

Рассматривая окружность $S^1 = \mathbb{R}/\mathbb{Z}$ при помощи ее универсальной накрывающей $\mathbb{R}$, мы поднимем оба распределения на окружности до $\mathbb{Z}$-периодических распределений на накрывающей прямой.

На прямой распределение с плотностью ρ уже имеет функцию распределения

$$f(X) = \int_{X_0}^{X} \rho(n)\, dx.$$

Выбор этой первообразной (зависящей от «начальной точки» X_0) неоднозначен — она определена лишь с точностью до «постоянной интегрирования», первообразными являются также и функции $f + C$ при любой постоянной c.

Чтобы определить аналог отклонения Колмогорова S для пары распределений одинаковой массы на окружности, я поступлю следующим образом.

Обозначим через $\tilde{f}_k$ и $\widetilde{F}_k$ функции распределения на накрывающей прямой, полученные поднятием исходного дискретного распределения k точек на окружности и «теоретического» непрерывного распределения такой же суммарной массы k (в нашем случае это будет равномерное распределение:

$$\widetilde{F}_k(y) = py \text{ на накрывающей прямой}).$$

Коэффициент p выбирается так, чтобы приращение величины $\widetilde{F}_k$ при увеличении y на длину рассматриваемой окружности составляло число k точек (массу) изучаемого распределения.

В нашем случае конечной окружности $\mathbb{Z}_n = \mathbb{Z}/(n\mathbb{Z})$ длины n мы получаем для коэффициента p значение k/n.

Чтобы определить отклонение S_k, остается лишь выбрать постоянные интегрирования (c и C) для интегралов f_k и F_k вдоль накрывающей прямой.

Определение 3. *Отклонение* S_k между эмпирическим распределением k точек на окружности длины n и непрерывным распределением массы k на ней определяется как

$$S_k = \inf_{c\in\mathbb{R}} \Big(\sup_{x\in\mathbb{R}} |\tilde{f}_k(x) - (\widetilde{F}_k(x) + c)| \Big),$$

где $\tilde{f}_k$ и $\widetilde{F}_k$ — какие угодно две первообразные функции поднятий на накрывающую прямую (для эмпирического распределения k точек на окружности и для непрерывного распределения массы k вдоль нее).

Замечание. Величина отклонения S_k не зависит от того, какие именно первообразные взяты: при взятии нижней грани по c вторая первообразная согласуется с первой.

Пример 1. Рассмотрим величины

$$M = \sup_x (\tilde{f} - \widetilde{F}), \quad m = \inf_x (\tilde{f} - \widetilde{F}).$$

Величина отклонения есть

$$S = \frac{M - m}{2},$$

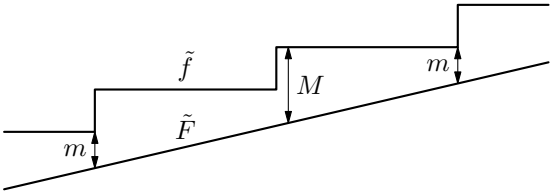


Рис. 2.

так как к $\widetilde F$ можно прибавить оптимизирующую постоянную $c = \dfrac{M+m}{2}$ (для которой отклонения верх и вниз одинаковы).

Пример 2. Для четырех взаимно простых с $n = 10$ остатков $\{1, 3, 7, 9\}$ от деления на 10 получается такая оптимальная первообразная $\widetilde F_4 + c$:

$$p = \frac{k}{n} = \frac{2}{5}\,, \quad S_4 = \frac{4}{5}\,, \quad \lambda_4 = \frac{4}{5\sqrt{4}} = \frac{2}{5}\,.$$

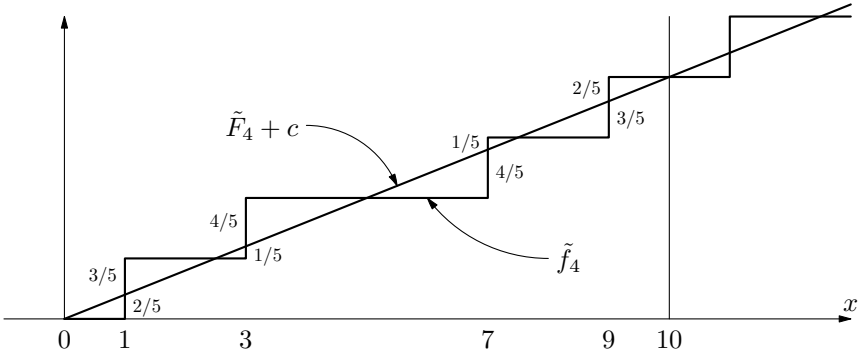


Рис. 3.

Приведенное выше определение 3 отклонения S_k позволяет определить значение $\lambda_k = S_k/\sqrt{k}$ параметра Колмогорова для распределения k точек на окружности. Теорема Колмогорова об универсальном распределении Φ обобщается и на этот вариант его теории (только универсальное предельное распределение Φ параметра Колмогорова λ в этом случае несколько изменится). Каждому распределению на окружности $S^1 = \mathbb{R}/\mathbb{Z}$ соответствует распределение на $[0, 1)$. Сопоставляя этому распределению случайные величины

$$S_k^+ = \sup_{x\in\mathbb{R}}(f_k(x) - F_k(x)),$$
$$S_k^- = \inf_{x\in\mathbb{R}}(f_k(x) - F_k(x)),$$

мы видим, что вышеопределенное отклонение S_k для распределения S^1 удовлетворяет соотношению

$$S_k = (S_k^+ - S_k^-)/2.$$

Поскольку предельное совместное распределение $(S_k^+/\sqrt{k}, S_k^-/\sqrt{k})$ известно ([4, с. 403]), то можно найти и предельное распределение для $S_k/\sqrt{k}$. Вычисления показывают, что для непрерывной функции распределения предел математических ожиданий величины $S_k/\sqrt{k}$ равен $\sqrt{\pi/8} \approx 0{,}63$.

Переход от точек на непрерывной окружности S^1 к точкам на конечных окружностях $\mathbb{Z}_n$ (с большими значениями n) строго не обоснован. Но это, я предполагаю, лишь временное техническое затруднение — асимптотика поведения ответов для $\mathbb{Z}_n$ при $n \to \infty$ согласуется, вероятно, с обобщением на случай случайных величин на окружности S^1 результатов Колмогорова о вещественных случайных величинах.

§ 3. Вычисление значений параметра стохастичности Колмогорова для групп Эйлера примитивных вычетов по модулю n

Приведенные в § 1 сведения о семействах примитивных вычетов позволяют легко нарисовать картинки типа примера 2 из § 2 выше для рассмотренных в § 1 значений n. Эти вычисления дают следующие значения величины отклонения S_k и параметра Колмогорова λ_k:

n	4	5	6	7	8	9	10	11	12	13
k	2	4	2	6	4	6	4	10	4	12
S_k	$\frac{1}{2}$	$\frac{4}{5}$	$\frac{2}{3}$	$\frac{11}{12}$	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{4}{5}$	$\frac{10}{11}$	$\frac{2}{3}$	$\frac{12}{13}$
λ_k	0,354	0,400	0,471	0,374	0,250	0,272	0,400	0,287	$\frac{1}{3}$	0,266

Второй десяток значений параметров λ_k делает столь же маловероятной гипотезу о случайности примитивных вычетов по этим модулям (при $\lambda \leqslant 0{,}4$ вероятность случайности меньше 3/1000 по таблице функции Колмогорова Φ, приведенной выше):

n	14	15	16	17	18	19	20	21	22	23	24
k	6	8	8	16	6	18	8	12	10	22	8
S_k	$\frac{6}{7}$	$\frac{14}{15}$	$\frac{1}{2}$	$\frac{16}{17}$	$\frac{2}{3}$	$\frac{18}{19}$	$\frac{4}{5}$	$\frac{8}{7}$	$\frac{10}{11}$	$\frac{22}{23}$	$\frac{2}{3}$
λ_k	0,350	0,330	0,177	0,235	0,272	0,223	0,283	0,330	0,287	0,204	0,236

Оставшиеся 7 значений ($25 \leqslant n \leqslant 31$) доставляют следующие значения параметров Колмогорова λ_k:

n	25	26	27	28	29	30	31
k	20	12	18	12	28	8	30
S_k	$\frac{4}{5}$	$\frac{12}{13}$	$\frac{2}{3}$	$\frac{6}{7}$	$\frac{28}{29}$	$\frac{14}{15}$	$\frac{30}{31}$
λ_k	0,179	0,289	0,157	0,247	0,182	0,330	0,177

Распределение получившихся 28 значений параметров Колмогорова λ_k совершенно непохоже на распределение Колмогорова Ф. Разделим ось значений λ на 6 частей:

$$\lambda \leqslant 0{,}2; \quad 0{,}2 < \lambda \leqslant 0{,}25; \quad 0{,}25 < \lambda \leqslant 0{,}3;$$
$$0{,}3 < \lambda \leqslant 0{,}35; \quad 0{,}35 < \lambda \leqslant 0{,}4; \quad \lambda > 0{,}4$$

мы получим в этих частях, соответственно,

$$5,\ 6,\ 7,\ 5,\ 4,\ 1$$

значений. Суммы этих значений составляют, соответственно,

$$0{,}872;\ 1{,}385;\ 1{,}956;\ 1{,}673;\ 1{,}528;\ 0{,}471.$$

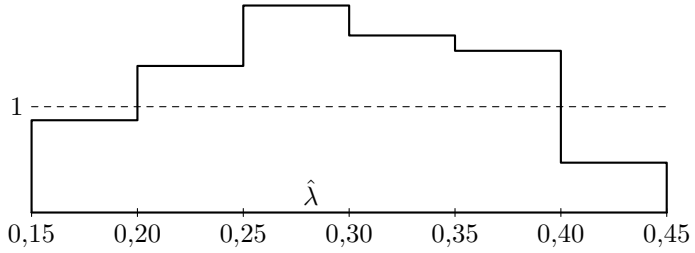


Рис. 4.

Среднее значение $\hat{\lambda}$ по всем 28 значениям параметра λ составляют примерно 0,282. В распределении Колмогорова суммарная вероятность всех 28 таких значений составляет менее $1/300$, так они малы.

Мы заключаем, что изучаемые распределения k примитивных вычетов на окружности $\mathbb{Z}_n$ весьма сильно отличаются от случайных распределений k независимых точек. Это еще одно подтверждение вывода § 1 о зависимости между примитивными вычетами (которые ведь отталкиваются от своих соседей).

Ясно также, что вычисленные значения $\lambda_k(n)$ имеют тенденцию убывать с ростом n. Это можно было бы объяснить ростом с n знаменателя в формуле $\lambda_k = S_k/\sqrt{k}$, если бы отклонения S_k не слишком росли с ростом n (и, следовательно, с ростом $k \sim (6/\pi^2)n$).

Приведенные выше значения наводят на мысль, что величины отклонений S_k остаются ограниченными (и даже величинами порядка 1) при росте k.

Однако, в действительности дело обстоит иначе: при некоторых натуральных значениях n отклонения S_k сколь угодно велики.

А именно, возьмем в качестве n произведение всех j простых чисел, меньших некоторого p_{j+1}:

$$n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots \cdot p_j.$$

Лемма 1. *Ни одно из целых чисел x в интервале $2 \leqslant x \leqslant p_{j+1}$ не взаимно просто с n.*

Действительно, все простые множители числа x, меньшего p_{j+1}, являются делителями числа n, а значит — его общими делителями с x.

Лемма 2. *Имеет место следующее неравенство для отклонения D, построенного по $k(n)$ примитивным вычетам по модулю n:*

$$D \geqslant \frac{k}{n} \, \frac{p_{j+1} - 1}{2} \, .$$

Доказательство. График ступенчатой считающей функции f примитивных вычетов по модулю n содержит горизонтальный участок $\{1, \ldots, p_{j+1}\}$ длины $p_{j+1} - 1$. Функция распределения для равномерного распределения массы k вдоль окружности длины n (определенная на накрывающей окружность прямой) линейна с наклоном $p = k/n$.

Отклонение никакой линейной функции наклона p от функции, постоянной на отрезке длины L, не может быть меньшим половины произведения pL. Это и доставляет утверждение леммы 2 (при $p = k/n$, $L = p_{j+1} - 1$). □

Лемма 3. *Произведение*

$$\frac{k(n)}{n} \, \frac{p_{j+1} - 1}{2}$$

принимает сколь угодно большие значения для чисел n, являющихся произведениями достаточно большого числа j последовательных простых чисел

$$n = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p_j.$$

Запишем число $k(n)$ взаимно простых с n остатков от деления на n по формуле мультипликативности Эйлера

$$k = \prod_{i=1}^{j} (p_i - 1).$$

Мы получим тогда

$$\frac{k}{n} = \prod_{i=1}^{j} \frac{p_i - 1}{p_i} = \prod_{i=1}^{j} \Big(1 - \frac{1}{p_i}\Big).$$

Следовательно, в силу известных оценок для последнего произведения [2, с. 94] справедливо асимптотическое равенство

$$\frac{k}{n} = \frac{e^{-\gamma}}{\ln L}(1 + o(1))$$

при $j \to \infty$, $L = p_{j+1} - 1$, где γ — постоянная Эйлера. Таким образом, утверждение леммы 3 вытекает из леммы 2.

Заметим, что для больших j утверждение леммы 2, основанное на том, что существует L последовательных чисел, не взаимно простых с n, можно усилить. Теорема Эрдеша и Ранкина показывает, что при $L > 20$ найдется не менее

$$\frac{cL \ln L \ln\ln\ln L}{(\ln\ln L)^2}$$

последовательных чисел с таким свойством, где $c > 0$ — некоторая константа. Более того, в [8] показано, что при $L \to \infty$ можно взять $c = 2e^{\gamma} + o(1)$.

Пример. Рассмотрим значение

$$n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 43 \cdot 47$$

(соответствующее $j = 15$). В этом случае $p_{j+1} = 53$,

$$n = 1 \cdot 2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 \cdot 16 \cdot 18 \cdot 22 \cdot 28 \cdot 30 \cdot 36 \cdot 40 \cdot 42 \cdot 46.$$

Значение k/n можно сосчитать, умножая выписанные сомножители, но проще заменить это умножение сомножителей сложением их логарифмов.

Таблица логарифмов дает (десятичные) логарифмы

$$\lg n \approx 17{,}78879, \quad \lg k \approx 16{,}93088.$$

Поэтому $\lg(n/k) \approx 0{,}85791$, так что

$$\frac{n}{k} \approx 7{,}21 \quad \text{и} \quad \frac{k}{n} \approx 0{,}139.$$

Зная длину $L = 52$ горизонтального участка $[1, 53]$ графика эмпирической функции распределения, мы получаем (лемма 2) для отклонения S оценку снизу

$$S \geqslant \frac{k}{n}\frac{L}{2} \approx 0{,}139 \cdot 26 \approx 3{,}61.$$

Этот пример показывает, что предположение $S \leqslant 2$, доставляемое приведенными выше таблицами (где $n \leqslant 31$) ошибочно: отклонения S бывают сколь угодно большими.

Правда, нужные для этого значения n очень велики (так что величина показателя стохастичности Колмогорова $\lambda = S/\sqrt{k}$ в приведенном выше примере и других, подобных ему, мала). Можно было предположить, что большие отклонения $S_{k(m)}$ встречаются столь редко, что чезаровские средние

$$\hat{S}_n = \frac{\sum\limits_{m=1}^{n} S_{k(m)}}{n}$$

остаются при $n \to \infty$ ограниченными (или даже имеют конечный предел). Оказывается, однако, что это не так! В [3] доказано, что

$$S_{k(m)} \geqslant c2^{\omega(m)/2}/\omega(m),$$

где $c > 0$ — абсолютная константа, а $\omega(m)$ — число различных простых делителей m. Далее, известно, что для почти всех натуральных m величина $\omega(m)$ близка к $\ln\ln m$. Точнее, для любого $b \in (1/2, 1)$ справедливо асимптотическое соотношение

$$\sum_{m=1}^{n}{}' 1 = o(n) \quad (n \to \infty),$$

где $\sum'$ означает, что суммирование проводится по тем $m \leqslant n$, для которых $|\omega(m) - \ln\ln m| > (\ln\ln m)^b$ ([2, задача 20 к главе 1]). Если теперь через $\sum''$ обозначить суммирование по тем $m \leqslant n$, для которых $|\omega(m) - \ln\ln m| \leqslant (\ln\ln m)^b$, то мы получим

$$\sum_{m=1}^{n}{}'' S_{k(m)} \geqslant n(\ln n)^{(\ln 2/2)+o(1)} \quad (n \to \infty).$$

Следовательно,

$$\hat{S}_n \geqslant (\ln n)^{(\ln 2/2)+o(1)} \quad (n \to \infty).$$

Неслучайность распределения примитивных вычетов по модулю n может быть продемонстрирована следующим фактом: соответствующие значения показателей стохастичности Колмогорова $\lambda_{k(n)} = \dfrac{S_{k(n)}}{\sqrt{k(n)}}$ сходятся к нулю при $n \to \infty$, причем довольно быстро. В [5] показано, что

$$S_{k(n)} \leqslant 2^{\omega(n)}.$$

Далее, поскольку при $k = k(n)$

$$\frac{k}{n} \geqslant \prod_{i=1}^{\omega(n)} \frac{p_i - 1}{p_i} \geqslant \prod_{i=1}^{\omega(n)} \frac{i}{i+1} = \frac{1}{\omega(n)+1},$$

из вышеприведенной оценки для произведения в последнем неравенстве

следует, что

$$\frac{S_k}{\sqrt{k}} \leqslant \frac{2^{\omega(n)}(\sqrt{\omega(n)+1})}{\sqrt{n}}\,.$$

Так как $2^{\omega(n)} \leqslant d(n)$, где $d(n)$ — количество делителей числа n, то из известной оценки для $d(n)$ (см. [2, с. 32]) следует, что

$$\frac{S_k}{\sqrt{k}} \leqslant \frac{\exp((\ln 2 + o(1))\ln n)/\ln\ln n)}{\sqrt{n}} \to 0$$

при $n \to \infty$.

Список литературы

[1] Арнольд В. И. *Группы Эйлера и арифметика геометрических прогрессий*. — М.: МЦНМО, 2003. — 43 с.

[2] Прахар К. *Распределение простых чисел*. — М.: Мир, 1967. — 512 с.

[3] Bell J. P., Bober J. W. *Bounded step functions and factorial ratio sequences* // Intern. J. Number Theory — 2009. — V. 5 — P. 1419–1431.

[4] Doob J. L. *Heuristic approach to the Kolmogorov – Smirnov theorems* // Ann. Math. Statist. — 1949. — V. 20. — P. 393–403.

[5] Friedlander J. B., Shparlinski I. E. *On the distribution of the power generator* // Math. Comp. — 2001. — V. 70 — P. 1575–1589.

[6] Kolmogorov A. N. *Sulla determinazione empirica di una legge di distribuzione* // Giorn. Ist. Ital. Attuari. — 1933. — V. 4, № 1. — P. 83–91.

[7] Montgomery H. L., Vaughan R. C. *On the distribution of reduced residues* // Ann. Math. — 1986. — V. 123. — P. 311–333.

[8] Pintz J. *Very large gaps between consecutive primes* // J. Number Theory. — 1997. — V. 63. — P. 286–301.