В. И. АРНОЛЬД

ГРУППЫ ЭЙЛЕРА И АРИФМЕТИКА ГЕОМЕТРИЧЕСКИХ ПРОГРЕССИЙ

Москва
Издательство МЦНМО
2003

УДК 511
ББК 22.13
А84

Арнольд В. И.

А84 Группы Эйлера и арифметика геометрических прогрессий.— М.: МЦНМО, 2003.— 44 с.

ISBN 5-94057-141-7

ББК 22.13

ISBN 5-94057-141-7

§ 1. Основные определения

Для любого натурального числа n в группе вычетов $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ по модулю n лежит мультипликативная подгруппа $\Gamma(n) \subset \mathbb{Z}_n$, образованная вычетами, взаимно простыми с n.

Число $\varphi(n)$ элементов группы $\Gamma(n)$ Гаусс назвал значением в точке n *функции Эйлера* φ.

Определение. *Группой Эйлера* $\Gamma(n)$ называется мультипликативная группа взаимно простых с n вычетов по модулю n.

Таким образом, группа Эйлера является коммутативной группой порядка $\varphi(n)$. В то время как функция Эйлера много исследовалась (Ферма, Эйлером, Гауссом, Лежандром, Якоби и другими), группа Эйлера настолько же интереснее, чем числа $\varphi(n)$, доставляемые функцией Эйлера, насколько группы гомологий интереснее чисел Бетти.

Приведение по модулю a определяет естественный гомоморфизм $\Gamma(ab) \to \Gamma(a)$. Настоящая работа посвящена описанию групп Эйлера и этих естественных гомоморфизмов.

Замечание. Я не стал выискивать, кто первым открыл тот или иной сообщаемый ниже факт, но в литературе (ср. [4]—[8]) можно найти, в иных терминах, описания типа: «этот результат был известен Ферма, был сформулирован Эйлером и был доказан Гауссом (доказательства которого были позже усовершенствованы NN)». Я предпочитаю считать последующее изложением достойной войти в элементарные учебники «теории Эйлера», не заботясь об отсутствии в его публикациях как формулировок, так и доказательств.

§ 2. Отступление о функции Эйлера

Значение функции Эйлера легко вычисляется по разложению аргумента на простые множители, $n = p_1^{a_1} \cdots p_k^{a_k}$, а именно

$$\varphi(n) = (p_1 - 1)\, p_1^{a_1 - 1} \cdots (p_k - 1)\, p_k^{a_k - 1}.$$

Например, $\varphi(p) = p - 1$, $\varphi(9) = 6$, $\varphi(15) = 8$ (причем, по определению, $\varphi(1) = 1$).

Действительно, все вычеты по модулю простого числа p, кроме нуля, взаимно просты с ним, так что $\varphi(p) = p - 1$.

Из p^a вычетов по модулю $n = p^a$ не взаимно просты с n в точности делящиеся на p вычеты, число которых равно p^{a-1}, так что $\varphi(p^a) = p^a - p^{a-1}$.

Наконец, если простых делителей p_i у числа n имеется k, то взаимно простой с n остаток по модулю n имеет взаимно простой с p_i остаток r_i по модулю $p_i^{a_i}$ и определяется этими остатками r_i однозначно (формальное доказательство см. в § 6, где это следует из теоремы 1).

При больших значениях аргумента n значение $\varphi(n)$ растет, в среднем, как cn, где $c = 6/\pi^2$ близко к $2/3$ (ср. [3]). «Рост в среднем», введенный в [3], означает равенство единице предела при $n \to \infty$ отношения сумм n первых значений,

$$\lim_{n\to\infty} \frac{\varphi(1)+\varphi(2)+\ldots+\varphi(n)}{c\cdot 1 + c\cdot 2 + \ldots + cn} = 1.$$

Он не исключает довольно больших отличий некоторых значений $\varphi(n)$ от cn, означая только, что они редки.

Постоянная c — это вероятность несократимости дроби x/y с целыми x и y, определяемая как предел при $R \to \infty$ отношения числа несократимых пар (x, y) в круге $x^2 + y^2 \leqslant R^2$ к числу всех таких пар (растущему с R как πR^2).

Эта вероятность вычислена Гауссом и опубликована Дирихле [13]. Для аналогичной задачи о векторах из $\mathbb{Z}^m$ вероятность несократимости равна $c = 1/\zeta(m)$, где *дзета-функция Эйлера* определяется как сумма ряда

$$\zeta(m) = \frac{1}{1^m} + \frac{1}{2^m} + \frac{1}{3^m} + \ldots \ .$$

Доказательство формулы для c таково. Вероятность сократимости на 2 равна $1/2^m$ (так как на 2 должна делиться каждая из m компонент вектора). Вероятность сократимости на простое число p есть $1/p^m$, а вероятность несократимости на p есть $1 - 1/p^m$.

Поскольку сократимости на разные простые числа p очевидно независимы, вероятность полной несократимости равна $c = \prod \frac{1}{1-\frac{1}{p^m}}$ (произведение по всем простым). Но из единственности разложения числа n на простые множители вытекает заложившая начало теории градуированных алгебр формула Эйлера

$$\prod_p \frac{1}{1-\frac{1}{p^m}} = \sum_n \frac{1}{n^m}$$

(суммирование по всем натуральным значениям n). Формула Эйлера вытекает из выражения для суммы геометрической прогрессии

$$\frac{1}{1-\frac{1}{p^m}} = 1 + \frac{1}{p^m} + \frac{1}{p^{2m}} + \ldots$$

вследствие единственности разложения числа n на простые множители.

Наконец, формула $\zeta(2)=\pi^2/6$ для значения дзета-функции следует из теории рядов Фурье. А именно, рассмотрим 2π-периодическое продолжение f функции $|t|-\pi/2$, заданной на отрезке $|t|\leqslant\pi$. Коэффициенты Фурье легко вычисляются (и убывают как $1/n^2$), и выражение $f(0)=-\pi/2$ через эти коэффициенты доставляет для $\sum 1/n^2$ значение $\pi^2/6$.

Таким образом, исследование роста функции Эйлера φ включает всю математику, от рядов Фурье до теории вероятностей и теории градуированных алгебр.

Функция f, встретившаяся при вычислении значения $\zeta(2)$, является одним из членов знаменитой последовательности периодических функций Колмогорова, начинающейся с функции $F_0=\operatorname{sign}\cos t$ и продолжающейся по правилу $F'_{n+1}=F_n$.

Колмогоров изобрел эти функции (аппроксимирующие синусы и косинусы кусочно-полиномиальными функциями растущих степеней, от ступенчатой F_0 и пилообразной F_1 до параболически аппроксимирующей непрерывно дифференцируемой F_2 и n раз непрерывно дифференцируемой F_{n+1}) ради решения замечательной экстремальной задачи: найти наибольшее значение промежуточной k-й производной у 2π-периодической функции с заданными ограничениями сверху модулей самой функции и старшей (m-й) производной.

Его оценка подсказана теорией размерности или принципом автомодельности Леонардо да Винчи, учитывающим отраженную в обозначениях Лейбница размерность производной,

$$\dim\frac{d^r y}{(dx)^r}=\frac{\dim y}{(\dim x)^r}.$$

Оценка Колмогорова имеет вид

$$\left\|\frac{d^k y}{(dx)^k}\right\|\leqslant C\|y\|^a\left\|\frac{d^m y}{(dx)^m}\right\|^b,$$

где рациональные показатели a и b равны $b=k/m$, $a=1-b$ по принципу автомодельности. Постоянная C достигается на подходящей функции серии Колмогорова (причем, если период T отличен от 2π, то соображения подобия диктуют и вид зависимости постоянной C от T).

Например, первая производная оценивается корнем квадратным из произведения максимумов модулей функции и второй производной. Этот частный случай теоремы Колмогорова был ранее установлен (независимо друг от друга) Адамаром и Литтлвудом.

Общее неравенство Колмогорова явилось, по существу, первым результатом современной теории управляемых динамических систем (сделавшейся широко известной много позже, когда Понтрягин опубликовал

свой «принцип максимума»). Доказательство Колмогорова, опирающееся на общий геометрический принцип Гюйгенса теории распространения волн (вариантом которого является и «принцип максимума»), применимо, с небольшими изменениями, и в общей теории управляемых систем (подобно тому, как решение задачи о брахистохроне содержит, в сущности, все вариационное исчисление). Главной идеей является здесь переход от принципа огибающих волновых фронтов Гюйгенса к его инфинитезимальному варианту, являющемуся системой канонических уравнений Гамильтона в фазовом пространстве.

Практический вывод из этих общих соображений состоит в том, что в задачах управления с ограничениями для оптимизации нужно все время давать управлению (в задаче Колмогорова — высшей производной) экстремальное значение. Например, вторая производная в ситуации Адамара и Литтлвуда должна принимать все время то максимальное, то минимальное значение, что сразу и приводит (при учете периодичности) к пропорциональной F_2 экстремали в этой задаче. Так Колмогоров и пришел к своей последовательности функций F_n.

Что касается ряда Фурье четной функции $f = F_1$, нужного для вычисления $\zeta(2) = \pi^2/6$, то из формулы, представляющей f этим рядом, $f(t) = \sum a_k \cos(kt)$, мы находим, что $a_k = 0$ при четных k, тогда как для нечетного k коэффициент Фурье находится интегрированием по частям:

$$\pi a_k = \int_{-\pi}^{\pi} f(t)\cos(kt)\,dt = 2\int_0^{\pi} t\cos(kt)\,dt =$$

$$= 2\left[\left(\frac{kt}{k^2}\sin(kt)\right)\Big|_0^{\pi} - \frac{1}{k^2}\int_0^{\pi}\sin(kt)\,d(kt)\right] = \frac{2}{k^2}\left(\cos(kt)\right)\Big|_0^{\pi} = -\frac{4}{k^2}.$$

Итак, мы вычислили коэффициенты Фурье с нечетными номерами: они суть

$$a_k = \left(-\frac{4}{\pi}\right)\frac{1}{k^2}.$$

Стало быть, значение $f(0) = -\dfrac{\pi}{2}$ равно сумме ряда Фурье

$$f(0) = \left(\sum_{m=0}^{\infty}\frac{1}{(2m+1)^2}\right)\left(-\frac{4}{\pi}\right),$$

и мы вычислили сумму ряда обратных квадратов нечетных чисел

$$A = \sum_{m=0}^{\infty}\frac{1}{(2m+1)^2} = \frac{\pi^2}{8}.$$

Введем обозначение B для искомой суммы ряда обратных квадратов всех натуральных чисел

$$\sum_{k=1}^{\infty}\frac{1}{k^2}=\sum_{m=0}^{\infty}\frac{1}{(2m+1)^2}+\sum_{m=1}^{\infty}\frac{1}{(2m)^2}.$$

Тогда, поскольку каждое натуральное число либо нечетно, либо четно, мы представим искомую сумму в виде $B=A+B/4$. Следовательно (поскольку мы уже знаем нечетную часть, $A=\pi^2/8$, из ряда Фурье),

$$\zeta(2)=B=\frac{4}{3}A=\frac{\pi^2}{6}.$$

§ 3. Таблица групп Эйлера

Прямые вычисления дают для первых значений n группы Эйлера $\Gamma(n)$, приведенные в следующей таблице. Обозначение вроде $2^a.3^b.4^c$ в этой таблице означает коммутативную группу, изоморфную группе $(\mathbb{Z}_2)^a\times(\mathbb{Z}_3)^b\times(\mathbb{Z}_4)^c$ (порядок которой равен произведению $\varphi=2^a3^b4^c$).

Разумеется, группа $2^a.3^a$ есть та же группа, что и группа 6^a, но группа $2^a.4^a$ отличается от группы 8^a и группа 2^{2a} отличается от группы 4^a.

Итак, вот таблица первых групп Эйлера.

n	3	4	5	6	7	8	9	10	11	12	13	14	15
$\Gamma(n)$	2	2	4	2	6	2^2	6	4	10	2^2	12	6	4.2
g_i	2	3	2 3	5	3 5	(3, 5)	2 5	3 7	2,7 6,8	(5, 7)	2,6 7,11	3 5	(2, 11)

n	16	17	18	19	20	21	22	23	24
$\Gamma(n)$	4.2	16	6	18	4.2	6.2	10	22	2^3
g_i	(3, 7)	3,5,10,11 6,7,12,14	5 11	2,3,14 10,13,15	(3, 11)	(2, 5)	7,13 19,17	5,7,11,15,17 14,10,21,20,19	(5, 7, 13)

n	25	26	27	28	29
$\Gamma(n)$	20	12	18	$6.2=2^2.3$	28
g_i	2,3,8,12 13,17,22,23	7,11 15,19	2,5,20 14,11,23	(3, 13), (13, 27, 9)	2,3,4,5,7,8,9,12,14,16,18,19,23 15,10,22,6,25,11,13,17,27,20,21,26,24

n	30	31	32	33	34	35
$\Gamma(n)$	4.2	30	8.2	$10.2=2^2.5$	16	12.2
g_i	(7, 11)	3,11,12,22 21,17,13,24	(3, 15)	(2, 10), (10, 32, 4)	3,5,11,27 23,7,31,29	(2, 6)

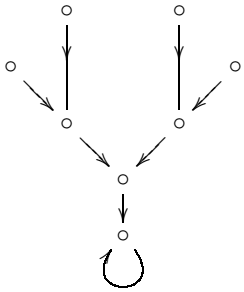
Числа g_i, указанные в третьей строке таблицы (для циклических групп $\Gamma(n)\subset\mathbb{Z}_n$) — это циклические образующие указанных циклических групп,

так что вычеты чисел g^k $(0 \leqslant k < \varphi(n))$ составляют группу $\Gamma(n)$. При этом под каждой образующей g указана обратная ей образующая h (так что $gh \equiv 1 \pmod{n}$). Циклические образующие группы $\Gamma(n)$ называются также *первообразными корнями по модулю n*.

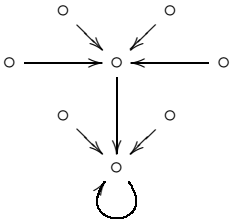
Для нециклических групп в строке образующих указан в скобках возможный набор циклических образующих групп-сомножителей (другие такие наборы легко получаются заменой этих образующих их степенями и произведениями).

Доказательство приведенной в таблице теоремы получается прямыми вычислениями геометрических прогрессий $a^k \pmod{n}$. Для опознания нециклических групп Эйлера удобно составлять ориентированный граф, вершинами которого являются элементы группы, а стрелки ведут к квадрату элемента (в аддитивной записи — от x к $2x$).

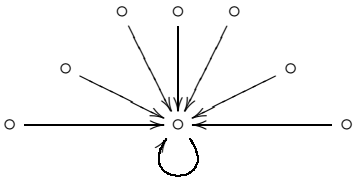
Пример. Графы групп порядка 8 таковы:



$8 = \mathbb{Z}_8$



$4.2 = \mathbb{Z}_4 \times \mathbb{Z}_2$



$2^3 = \mathbb{Z}_2^3$

Полезно также составлять таблицу количества элементов различных порядков в группе. В предыдущем примере эти таблицы такие:

группа \ порядок	1	2	4	8
$\mathbb{Z}_8$	1	1	2	4
$\mathbb{Z}_4 \times \mathbb{Z}_2$	1	3	4	0
$\mathbb{Z}_2^3$	1	7	0	0

§ 4. Группы Эйлера произведений

Анализ таблицы § 3 сразу приводит к следующим выводам (доказательства обсуждаются ниже, см. § 6).

Теорема 1. *Если числа a и b взаимно просты, то группа Эйлера их произведения — прямое произведение их групп Эйлера*: $\Gamma(ab) = \Gamma(a) \times \Gamma(b)$.

Теорема 2. *Если число $n = p$ простое, то группа Эйлера* $\Gamma(p) = \mathbb{Z}_{p-1}$ *— циклическая группа.*

Теорема 3. *Если число $n = p^a$ — степень нечетного простого числа, то его группа Эйлера — циклическая группа,*

$$\Gamma(p^a) = \mathbb{Z}_{\varphi(p^a)} = \mathbb{Z}_{(p-1)p^{a-1}}.$$

Теорема 4. *Если число $n = 2^a$, $a > 2$, — степень двойки, то его группа Эйлера есть произведение циклических групп порядков 2 и 2^{a-2}:*

$$\Gamma(2^a) = \mathbb{Z}_2 \times \mathbb{Z}_{2^{a-2}}.$$

Эти четыре теоремы доставляют все группы Эйлера, так как любое натуральное число можно разложить на простые множители.

Следствие. *Группа Эйлера* $\Gamma(n)$ *является циклической если и только если число n равно либо* 2, *либо* 4, *либо степени нечетного простого числа, либо удвоенной степени нечетного простого числа.*

Теорема 2 — это просто «малая теорема» Ферма, дополненная Эйлером (первообразность) и Гауссом.

§ 5. Гомоморфизм приведения по модулю a, $\Gamma(ab) \to \Gamma(a)$

Будем обозначать приведение по модулю a вычетов по модулю ab через $\pi\colon \mathbb{Z}_{ab} \to \mathbb{Z}_a$ (обозначая иногда тем же символом также ограничение этого приведения до $\Gamma(ab) \to \Gamma(a)$ или его действие на $\mathbb{Z}$).

Замечание. $\pi(\Gamma(ab)) \subset \Gamma(a)$ по следующей причине: если бы вычет $x \pmod a$ не был взаимно прост с a, то вычет $x \pmod{ab}$ не был бы взаимно прост с ab.

Как мы сейчас докажем, $\pi(\Gamma(ab)) = \Gamma(a)$ (хотя это и не совсем очевидно).

Пусть число x взаимно просто с a, т. е. $(x, a) = 1$. Отыщем вычет по модулю ab, проектирующийся в вычет $x \pmod a$. Мы должны исследовать все прообразы вычета $x \pmod a$ в $\mathbb{Z}_{ab}$ и среди них найти взаимно простой с ab элемент группы $\Gamma(ab)$. Докажем чуть более общий вариант «китайской теоремы об остатках».

Теорема $T_{D,B}$. *В арифметической прогрессии* $\{x + nD\}$ $(n = 0, 1, \ldots)$ *с взаимно простыми членом x и разностью D (так что $(x, D) = 1$)*

есть взаимно простой с B член:

$$\forall B\ \exists n\colon (x+nD, B)=1.$$

Доказательство. Теорема $T_{1,B}$ очевидна. Теперь мы будем предполагать верными теоремы $T_{d,b}$ с $d<D$ и выведем из них теорему $T_{D,B}$. Итак, пусть $(x, D)=1$.

Обозначим через δ наибольший общий делитель чисел B и D, так что

$$B=\beta\delta, \quad D=\gamma\delta, \quad (\beta,\gamma)=1.$$

Первый случай. $\gamma=1$, $D=\delta$.

В этом случае $B=\beta D>2$ или же $\beta=1$, $B=D$. Если $B=D$, то $(x, B)=1$ по условию, так что теорему $T_{D,D}$ доказывает выбор $n=0$.

В случае же $\beta>1$, когда $D<B$, мы приходим при $D>1$ (когда $\beta<B$) к импликации

$$T_{D,\beta}\Rightarrow T_{D,B},$$

поскольку из взаимной простоты числа $x+nD$ с β вытекает его взаимная простота с $B=\beta\delta$ (с δ это число, как и x, взаимно просто по условию доказываемой теоремы $T_{D,B}$ (где $D=\delta$)).

Итак, теорема $T_{D,B}$ сведена к теоремам с таким же D, но с меньшими B (причем, как только $B<D$, условие $\gamma=1$ больше выполняться не будет).

Второй случай. $\gamma>1$, $\delta<D$.

В этом случае мы выведем теорему $T_{D,B}$ из теоремы $T_{\delta,\beta}$, где $D=\gamma\delta$, $B=\beta\delta$, $(\beta,\gamma)=1$.

Из условия $(x, D)=1$ следует взаимная простота числа x с делителем δ числа D. По теореме $T_{\delta,\beta}$, существует целое число m такое, что число $r=x+m\delta$ взаимно просто с β.

Из взаимной простоты β и γ следует возможность представления $1=p\beta+q\gamma$ (с целыми p и q). Теперь мы можем представить r в виде

$$r=x+\delta(mp\beta+mq\gamma)=x+mpB+nD,$$

где $n=mq$.

Рассмотрим доказывающее теорему число

$$R=x+nD=r-mpB.$$

Это число взаимно просто с β, так как r взаимно просто с β (по теореме $T_{\delta,\beta}$ и выбору числа m). Кроме того, R взаимно просто с числом δ, так как $(x,\delta)=1$ по условию доказываемой теоремы $T_{D,B}$, а число $D=\gamma\delta$ делится на δ.

Стало быть, число R взаимно просто и с произведением $\beta\delta = B$, что и доказывает теорему $T_{D,B}$ (причем в качестве n выбирается число mq).

Теоремы $T_{D,B}$ доказаны теперь при любых D и B.

Из них следует соотношение $\pi(\Gamma(ab)) = \Gamma(a)$, так как по теореме $T_{a,b}$ среди вычетов чисел $x + na$, $n = 0, 1, 2, \ldots \pmod b$ имеется взаимно простой с b вычет (если $(x, a) = 1$, т. е. когда $x \in \Gamma(a)$).

Разумеется, число n можно здесь брать из интервала $[0, 1, \ldots, b-1]$, так как при увеличении n на b вычет числа $x + na \pmod{ab}$ не меняется.

Следствие. *Число прообразов каждой точки $x \in \Gamma(a)$ при отображении $\pi\colon \Gamma(ab) \to \Gamma(a)$ одинаково.*

Доказательство. Это отображение π — гомоморфизм группы $\Gamma(ab)$ *на группу* $\Gamma(a)$, как мы только что доказали. Так что указанное число прообразов равно порядку ядра этого гомоморфизма, $|\operatorname{Ker}\pi| = \varphi(ab)/\varphi(a)$.

§ 6. Доказательства теорем о группах Эйлера

Доказательство теоремы 1. Сравним оба гомоморфизма приведения по модулям a и b:

$$\pi\colon \Gamma(ab) \to \Gamma(a), \quad \rho\colon \Gamma(ab) \to \Gamma(b).$$

Пусть $x \in \Gamma(a)$, $\pi^{-1}(x) = \{X + na\}$, $0 \leqslant n < b$.

Все b вычетов чисел $X + na \pmod b$ различны, иначе число $n_1 a - n_2 a$ делилось бы на b при $|n_1 - n_2| < b$, вопреки предполагаемой в теореме 1 взаимной простоте чисел a и b.

Значит, в $\mathbb{Z}_{ab}$ найдется элемент с вычетом $x \pmod a$ и с любым вычетом $\pmod b$. Из этого следует также, что отображение

$$\pi \times \rho\colon \Gamma(ab) \to \Gamma(a) \times \Gamma(b)$$

покрывает все произведение (тот элемент z из $\mathbb{Z}_{ab}$, который сравним с $x \in \Gamma(a) \pmod a$ и с $y \in \Gamma(b) \pmod b$, обязательно лежит в $\Gamma(ab)$, так как из взаимной простоты числа z с сомножителями a и b следует его взаимная простота с произведением ab).

С другой стороны, *ядро отображения $\pi \times \rho$ тривиально*, так как его элементы сравнимы с 1 и по модулю a, и по модулю b, а значит, их разность в $\mathbb{Z}_{ab}$ делится на произведение ab, т. е. равна нулю (поскольку a и b взаимно просты в теореме 1).

Теорема 2 — это малая теорема Ферма, пополненная существованием первообразных корней по модулю простого числа (доказанным ниже в § 12). Существование первообразного корня нужно для того, чтобы порядок группы не оказался меньшим, чем $p - 1$.

Доказательство теоремы 3. Представим число p^{a+1}, где p — нечетное простое число, в виде произведения $p \cdot p^a$, и рассмотрим соответствующий приведению π (по модулю p) гомоморфизм групп

$$\pi\colon \Gamma(p^{a+1}) \to \Gamma(p).$$

Образом является вся группа $\Gamma(p)$, которая является циклической группой порядка $p-1$ (по теореме 2). Изучим ядро гомоморфизма π.

Лемма. *Ядро гомоморфизма π является циклической группой порядка p^a.*

Доказательство. Образующей ядра является, например, элемент $1+p$ (рассматриваемый как входящий в группу $\Gamma(p^{a+1})$ вычет по модулю p^{a+1}).

Действительно, вычислим степени этого элемента в p-адической системе счисления. По формуле бинома Ньютона,

$$(1+p)^k = 1 + pk \pmod{p^2},$$

поэтому при $k = 0, 1, 2, \ldots, p-1$ мы получим (mod p^2) все p значений q (mod p) для числа

$$(1+p)^k - 1 = pq.$$

Из той же формулы бинома следует, что

$$(1+p)^p = 1 + p^2 \pmod{p^3}.$$

Возводя этот элемент в степени $k = 0, 1, 2, \ldots, p-1$, мы получаем точно так же начальные члены p-адического разложения

$$(1+p)^{kp} = 1 + kp^2 \pmod{p^3},$$
$$(1+p)^{p^2} = 1 + p^3 \pmod{p^4}.$$

Совершенно так же выводятся формулы

$$(1+p)^{kp^s} = 1 + kp^{s+1} \pmod{p^{s+2}},$$

доставляющие кратные высшим степеням p слагаемые,

$$k = 0, 1, 2, \ldots, p-1.$$

Перемножая формулы, соответствующие a членам p-адического разложения

$$k = k_0 + k_1 p + k_2 p^2 + \ldots + k_{a-1} p^{a-1} \pmod{p^a},$$

мы получаем удобное представление любого элемента циклической группы, порожденной образующей $1+p$:

$$(1+p)^k = (1+pk_0)(1+p^2k_1)\dots(1+p^ak_{a-1}) \pmod{p^{a+1}}.$$

Из этой формулы видно, что все полученные (при $0 \leqslant k < p^a$) p^a элементов группы $\Gamma(p^{a+1})$, входящие в ядро гомоморфизма π, различны[1]. Значит, это ядро (имеющее порядок $\varphi(p^{a+1})/\varphi(p) = (p-1)p^a/(p-1) = p^a$) — циклическая группа (порядка p^a).

Итак, абелева группа $\Gamma(p^{a+1})$ расслоена над $\mathbb{Z}_{p-1}$ со слоем $\mathbb{Z}_{p^a}$. Порядки ($p-1$ и p^a) этих циклических групп взаимно просты, поэтому расслоение π является прямым произведением (и циклической группой)

$$\Gamma(p^{a+1}) \approx \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^a} \approx \mathbb{Z}_{\varphi(p^a)},$$

что и доказывает теорему 3.

Доказательство теоремы 4. Рассмотрим гомоморфизм приведения по модулю 4, $\pi\colon \Gamma(2^a) \to \Gamma(4)$. Образ состоит из вычетов 1 и 3 (mod 4), и мы можем записать каждый элемент из группы $\Gamma(2^a)$ как вычет числа

$$x = 1 + 2\alpha + 4u, \quad 0 \leqslant \alpha, \quad u < 2^{a-2}.$$

В частности, имеется специальный элемент второго порядка

$$\omega = 2^{a-1} - 1, \quad \alpha(\omega) = 1 + 2 + 4 + \dots + 2^{a-3} = 2^{a-3} - 1, \quad u(\omega) = 0.$$

Для этого элемента $\omega^2 \equiv 1 \pmod{2^a}$, т. к. числа 2^{2a-2} и $2 \cdot 2^{a-1}$ делятся на 2^a при $a \geqslant 2$ (что $a \geqslant 2$, мы предполагали в теореме 4). Мы получаем подгруппу $\{1, \omega\}$.

Любой элемент x из $\Gamma(2^a)$ можно однозначно записать либо в виде $x = 1 + 4u$ (когда $\pi x = 1$), либо в виде $x = \omega(1+4z)$ (когда $\pi x = 3$, как и $\pi(\omega)$).

Это следует из соотношения $\pi(\omega x) = \pi(\omega)\pi(x) = 9 \equiv 1 \pmod 4$: искомый множитель $1+4z$ есть просто ωx.

Итак, мы представили группу $\Gamma(2^a)$ в виде прямого произведения непересекающихся подгрупп $\mathbb{Z}_2 = \{1, \omega\}$ и $\{1+4z\}$, где $0 \leqslant z < 2^{a-2}$. Теорема 4 вытекает из следующего факта.

Лемма. *Группа* $\{1+4z\}$ $(0 \leqslant z < 2^{a-2})$ *вычетов по модулю* 2^a — *циклическая*: $\{1+4z\} \approx \mathbb{Z}_{2^{a-2}}$.

[1] Произведение $(1+p)^K$, где $0 < K < p^a$, не может быть равным единице, так как первая из отличных от нуля компонент K_i разложения $K = \sum K_i p^i$ доставляет отличный от 0 остаток mod p^{i+1} отличия от 1 произведения.

Доказательство леммы. Докажем (подобно приведенному выше доказательству теоремы 3), что циклической образующей является элемент $1+4=5$, который мы запишем в виде

$$q_0 = 1 + 4A_0 + 8D_0, \quad A_0 = 1, \quad D_0 = 0.$$

Пусть теперь в $\Gamma(2^a)$ дан элемент $Q = 1 + 2^{2+i}A + 2^{3+i}D$.

Вычисление квадрата по формуле бинома дает ответ в виде биномиальной формулы

$$Q^2 = 1 + 2^{2+(i+1)}A' + 2^{3+(i+1)}D',$$

где $A' = A$ (число D' целое потому, что для не выписанных явно трех членов бинома степеней двоек больше: $2(2+i) \geqslant 3+(i+1)$, $2(3+i) > 3+(i+1)$, $1+(2+i)+(3+i) > 3+(i+1)$).

Применяя эту фильтрованую биномиальную формулу к случаю $Q = q_0$ (где $i=0$, $A = A_0$, $D = D_0$), мы получаем для $q_1 = Q^2 = q_0^2$ выражение

$$q_1 = 1 + 2^{2+1}A_1 + 2^{3+1}D_1 \quad (\text{где } A_1 = A_0).$$

Применяя нашу биномиальную форму к $Q = q_1$, мы находим для $q_2 = q_0^4 = q_1^2$ выражение

$$q_2 = 1 + 2^{2+2}A_2 + 2^{3+2}D_2, \quad A_2 = A_1.$$

Продолжая возведения в квадрат, находим последовательно

$$q_g = q_0^{2^g} = q_{g-1}^2 = 1 + 2^{2+g}A_g + 2^{3+g}D_g \quad (\text{где } A_g = A_{g-1})$$

для $g = 0, 1, 2, \ldots, a-3$. При $g = a-2$ мы получаем $q_{a-2} = q_0^{2^{a-2}} = 1 + 2^a A_{a-2} + 2^{a+1}D_{g-2} \equiv 1 \pmod{(2^a)}$, т. е. число $5^{2^{a-2}} \equiv 1 \pmod{2^g}$ доставляет единицу группы $\Gamma(2^a)$.

Напротив того, все предыдущие степени числа 5 отличны от единицы по модулю 2^a. Действительно, обозначим двоичное разложение числа N, меньшего, чем 2^{a-2}, через

$$N = N_0 + N_1 \cdot 2 + N_2 \cdot 2^2 + \ldots + N_{a-3} \cdot 2^{a-3},$$

где все N_i — нули или единицы.

Тогда для 5^N мы получаем выражение

$$q_0^N = q_0^{N_0} q_1^{N_1} q_2^{N_2} \ldots q_{a-3}^{N_{a-3}}.$$

Обозначим через i первый ненулевой из коэффициентов $N_0, N_1, \ldots, N_{a-3}$ двоичного разложения числа N. Из доказанных выше формул для q_g следует, что

$$q_0^N = 1 + 2^{2+i} \pmod{2^{3+i}},$$

так что $q_0^N \not\equiv 1$ в $\Gamma(2^a)$ (поскольку $i \leqslant a-3$).

Значит, все 2^{a-2} элементов группы $\{1+4z\} \pmod{2^a}$, которые мы построили в виде $5^N \pmod{2^a}$, различны, так что эта подгруппа $\{1+4z\}$, состоящая из всего 2^{a-2} элементов, исчерпана элементами вида 5^N и является циклической.

Лемма доказана, и это заканчивает доказательство теоремы 4.

§ 7. Динамическая система Ферма—Эйлера

Зафиксируем взаимно простое с n число a и рассмотрим умножение на a как преобразование A множества $\Gamma(n)$ взаимно простых с n вычетов по модулю n в себя: оно переводит вычет числа x в вычет числа ax (которое, как и x, взаимно просто с n). Мы определили перестановку $A\colon \Gamma(n) \to \Gamma(n)$, $x \mapsto ax$.

Преобразование A множества $\Gamma(n)$ в себя, как и любое взаимнооднозначное преобразование, разбивается на циклы этой перестановки $\varphi(n)$ элементов.

Теорема (Эйлера—Ферма). *Все циклы перестановки Ферма—Эйлера $A\colon \Gamma(n) \to \Gamma(n)$ имеют одинаковый период $T(n, a)$.*

Доказательство. Любой элемент y группы $\Gamma(n)$ получается из любого другого ее элемента x умножением справа на некоторый элемент z. Поэтому

$$A^T y = A^T(xz) = (A^T x)z = xz = y,$$

т. е. период T элемента x является периодом и для y.

Следствие. *Множество $\Gamma(n)$ взаимно простых с n вычетов по модулю n разбивается на $N(n, a) = \varphi(n)/T(n, a)$ непересекающихся орбит преобразования Ферма—Эйлера, так что число орбит N, как и период T, является делителем значения функции Эйлера, $\varphi(n) = NT$; и выполняется сравнение Ферма—Эйлера*

$$a^{\varphi(n)/N} \equiv 1 \pmod{n}.$$

Пример. Если число $n = p$ простое, то имеет место сравнение

$$a^{p-1} \equiv 1 \pmod{p}.$$

Это — исходная «малая теорема» Ферма, которую мы, таким образом, доказали.

Эйлер перенес эту теорему на составные числа n вместо p, заметив, что показатель $p - 1 = \varphi(p)$ нужно для этого заменить на $\varphi(n)$, откуда и произошла функция Эйлера φ.

Если преобразование Ферма—Эйлера имеет лишь одну орбиту ($N = 1$), то период есть $T = \varphi(n)$, так что сравнение Ферма—Эйлера сводится к его

простейшей форме

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

в которой оно верно и когда орбит больше.

Вопрос о поведении периода и числа орбит в зависимости от числа n весьма непрост. Ниже рассказано об (экспериментальных, в основном) данных, полученных путем вычисления значений функций $N(n)$ и $T(n)$ для простейшего случая $a = 2$ (в предположении нечетности числа n, т. е. взаимной его простоты с основанием a).

Значения числа орбит $N(n)$ и периода $T(n)$ операции A умножения на $a = 2$ для первых пяти десятков нечетных модулей n указаны в следующей таблице.

n	**3**	**5**	**7**	9	**11**	**13**	15	**17**	**19**	21	**23**	25	27	**29**	**31**	33	35	**37**	39
N	1	1	2	1	1	1	2	2	1	2	2	1	1	1	6	2	2	1	2
T	2	4	3	6	10	12	4	8	18	6	11	20	18	28	5	10	12	36	12

n	**41**	**43**	45	**47**	49	51	**53**	55	57	**59**	**61**	63	65	**67**	69	**71**	**73**	75	77
N	2	3	2	2	2	4	1	2	2	1	1	6	4	1	2	2	8	2	2
T	20	14	12	23	21	8	52	20	18	58	60	6	12	66	22	35	9	20	30

n	**79**	81	**83**	85	87	**89**	91	93	95	**97**	99
N	2	1	1	8	2	8	6	6	2	2	2
T	39	54	82	8	28	11	12	10	36	48	30

Простые числа n выделены здесь полужирным шрифтом. Для каждого из них $NT = n - 1$, в других случаях произведение $NT = \varphi(n)$ меньше.

Теорема Эйлера—Ферма означает, что диаграмма Юнга, описывающая разбиение множества $\Gamma(n)$ на орбиты преобразования Ферма—Эйлера A, всегда представляет собой прямоугольник площади $\varphi(n)$ с основанием длины $T(n)$ и $N(n)$ строками такой длины $T(n)$.

Каждая строка представляет собой орбиту действия преобразования A, и мы выписываем ее элементы в порядке $(x, Ax, A^2x, \ldots)$. Для $n = 15$ эта диаграмма Юнга такова:

7	14	13	11	$(11 \cdot 2 \equiv 7)$
1	2	4	8	$(8 \cdot 2 \equiv 1)$

§ 8. Статистика геометрических прогрессий

Рост функции $T(n)$ с ростом модуля n представляется довольно нерегулярным, так как среди диаграмм Юнга встречаются и высокие (с относительно большим отношением N/T, как для $n=511$, где $N=48$, $T=9$) и низкие (с малым отношением N/T, как $1/82$ для $n=83$).

Суммы десятков значений $1\leqslant n\leqslant 19$, $21\leqslant n\leqslant 39$, $41\leqslant n\leqslant 59$, $61\leqslant n\leqslant 79$, $81\leqslant n\leqslant 99$ и десятков соответствующих значений периодов T обнаруживают более регулярную зависимость:

$\sum n$	100	300	500	700	900
$\sum T$	68	158	246	299	329

Эти данные подсказывают линейный рост T с n (грубо говоря, в среднем порядка $T=Cn$, где $C\approx\frac{3}{7}$ при $n\sim 70$ медленно убывает с ростом n).

Никаких теорем на этот счет я не знаю. Вот, однако, некоторые соображения нематематического характера.

Возрастание погрешностей в значении x при умножении x на большое при больших временах t число a^t, осуществляемое за время t динамической системой Ферма—Эйлера $A\colon \Gamma(n)\to\Gamma(n)$, наводит на мысль, что орбита $\{a^t x,\ t=1,\dots,T\}$ должна быть разбросана внутри $\Gamma(n)$ (и даже внутри $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$) хаотическим образом.

Длина или период T этой орбиты определяется тем условием, что все T «случайных точек» $a^t x$ должны занимать разные положения среди $m=\varphi(n)$ точек множества $\Gamma(n)$ (или среди всех $m=n$ точек множества $\mathbb{Z}_n$). Поэтому возникает идея сравнить $T(n)$ с длиной типичной случайной последовательности независимых выборов одной из m точек какого-либо множества, в которой все элементы этой случайной последовательности оказались различными.

Эта задача теории вероятностей обычно называется задачей о днях рождения (T — число студентов в группе, $m=365$ — число вариантов дня рождения). Спрашивается, какова вероятность того, что дни рождения всех T студентов в группе различны?

Ясно, что эта вероятность тем меньше, чем больше число студентов T, и совсем мала, начиная с некоторого их числа (и даже равна нулю при $T>m$). Напротив, если число студентов T мало, то мала вероятность наличия совпадений.

Критический размер группы T_*, где вероятность совпадений мала при $T<T_*$ и велика при $T>T_*$, растет с m как квадратный корень из m.

В этом проще всего убедиться, разделив число наборов непересекающихся последовательных выборов T элементов из m (равное произведению

T множителей $m(m-1)\dots(m-T+1)$) на число всевозможных наборов (равное m^T):

$$p = 1\left(1-\frac{1}{m}\right)\left(1-\frac{2}{m}\right)\dots\left(1-\frac{T-1}{m}\right).$$

Предполагая число T небольшим по сравнению с m (например, устремляя m к бесконечности при фиксированном T), мы получаем (не останавливаясь на деталях оценки ошибки) $\ln p \approx -\sum\limits_{j=1}^{T-1} j/m$.

Таким образом, приближенная формула для вероятности несовпадения есть

$$p \approx e^{-\frac{T(T-1)}{2m}}.$$

Это число мало, когда $T \gg \sqrt{2m}$, и близко к 1, когда $T \ll \sqrt{2m}$, так что длина отрезка m-значной случайной последовательности без совпадений растет с числом значений как квадратный корень из этого числа.

Замечание. Я думаю, что переход от малых значений p к большим при переходе T через критическое значение порядка $\sqrt{m}$ описывается универсальной функцией erf (интегралом от гауссовой плотности) при соответствующих (зависящих от m) единицах измерения отклонения значения T от критического. Но, к сожалению, я не видел в литературе доказательства соответствующей теоремы, несмотря на ее явный интерес для многих приложений: этот вопрос, видимо, слишком прост, чтобы его рассматривать вероятностникам.

Сравнивая указанный факт теории вероятностей с нашей таблицей чисел $T(n)$, мы приходим к выводу, что наблюденные периоды $T(n)$ геометрических прогрессий 2^t растут с числом выборов n быстрее, чем при полной независимости T значений (будем ли мы считать их принадлежащими множеству $\mathbb{Z}_n$ из $m=n$ элементов или же его подмножеству $\Gamma(n)$ из $m=\varphi(n)$ элементов, поскольку m растет «в среднем» как cn).

А именно, можно сформулировать это наблюдение как указание на присутствие какого-то (не изученного еще) *отталкивания* членами геометрической прогрессии $\{2^t \pmod n\}$ друг от друга. Из-за этого расталкивания орбита далеко не случайна и совпадений (или даже близких приближений) точек $2^t \pmod n$ друг к другу оказывается меньше, чем если бы последовательные точки ($t=1,2,\dots,T$) выбирались независимо друг от друга в m-элементном множестве ($\mathbb{Z}_n$ или $\Gamma(n)$).

§ 9. Измерение степени случайности подмножества

Для того, чтобы исследовать, насколько случайно расположены точки орбиты $\{a^t\}$ преобразования Ферма—Эйлера среди всех вычетов, входящих в $\mathbb{Z}_n$ (или среди $m=\varphi(n)$ взаимно простых с n вычетов, составляющих

группу Эйлера $\Gamma(n)$), я решил измерять «расталкивание» элементов T-элементного множества точек отрезка друг другом при помощи следующей величины.

Обозначим через $\{x_1, \ldots, x_T\}$ последовательность расстояний между соседними точками.

Имея в виду приложения к вычетам, я склеил концы отрезка в окружность, так что сумма положительных чисел x_i равна длине L этого отрезка или окружности.

Для измерения присутствия или отсутствия близких сближений точек множества я использовал «*параметр стохастичности*» (randomness)

$$R = x_1^2 + \ldots + x_T^2.$$

Чтобы сделать параметр безразмерным (не зависящим от единиц измерения, т. е. от длины L), я нормировал его, подобно преобразовав отрезок, к случаю $L = 1$: *нормализованный параметр стохастичности T точек есть*

$$r = R/L^2.$$

Эту нормализацию нужно делать, применяя теорию к вычетам из $\mathbb{Z}_n$ (где $L = n$) или к элементам группы Эйлера $\Gamma(n)$ (где $L = m$ и «расстояния» x_i — это число свободных от элементов группы $\Gamma(n)$ дуг между двумя элементами этой группы, расстояние между которыми измеряет целое число x_i).

Всевозможные конфигурации T точек окружности длины 1 описываются $(T-1)$-мерным симплексом

$$\{x = (x_1, \ldots, x_T),\ 0 \leqslant x_i \leqslant 1,\ \sum x_i = 1\}$$

(с точностью до поворота окружности).

Параметр стохастичности r является моментом инерции точки x относительно начала координат (квадратом расстояния от x до 0). Поэтому его наименьшее значение соответствует центру симплекса: $x_i = 1/T$, $r_{\min} = T(1/T)^2 = 1/T$, а наибольшее значение — вершине ($x_1 = 1$, остальные нули): $r_{\max} = 1$.

Для сравнения множеств с разным числами элементов T естественно ввести *бинормализованный параметр стохастичности*

$$s = r/r_{\min} = T \sum (x_i/L)^2.$$

Интервал изменения этого параметра при различных выборах подмножеств окружности из T элементов есть

$$(s_{\min} = 1) \leqslant s \leqslant (s_{\max} = T).$$

Минимальное значение, $s = 1$, достигается на правильном, казарменном расположении (арифметической прогрессии) вершин правильного T-угольника $x_i = 1/T$ (считая $L = 1$). В этом случае можно говорить о «сильном расталкивании», не допускающем сближения точек.

Максимальное значение, $s = T$, достигается на скученном кластере из T слившихся точек, для которого все расстояния x_i равны нулю, кроме одного, равного единице.

В этом случае можно говорить о «сильном притяжении», собравшем все точки в одно место.

Обсудим теперь истинно случайные расположения T независимо расположенных на окружности точек. Оказывается, бинормализованный параметр стохастичности таких расположений имеет вполне определенное значение s_1, близкое (при большом числе точек T) к значению $s = 2$. Сейчас мы вычислим это «указывающее на хаотичность множества» значение s_1. Его можно назвать «*свободолюбивым значением*», указывающим на отсутствие как отталкивания, так и притяжения точки исследуемого множества ее соседями. Меньшие значения параметра, вплоть до значения $s_{\min} = 1$, соответствующего казарменному регулярному строю равноотстоящих точек, указывают на расталкивание.

Большие, чем свободолюбивое значение $s \approx 2$, значения бинормализованного параметра стохастичности указывают на взаимное притяжение точек множества, крайним проявлением которого является соответствующее полному скучиванию максимальное (при фиксированном числе элементов множества) значение T.

§ 10. Среднее значение параметра стохастичности

Рассмотрим случайное распределение точки x в симплексе размерности $T - 1$

$$\{0 \leqslant x_i \leqslant 1,\ \sum_{i=1}^{T} x_i = 1\},$$

с постоянной относительно лебеговой меры плотностью (что соответствует и расстояниям между T точками, независимо случайно набросанными на окружность длины 1).

Теорема. *Среднее значение параметра стохастичности* $s = T \sum_{i=1}^{T} x_i^2$ *равно «свободолюбивому значению»*

$$s_1 = \frac{2T}{T+1}.$$

Доказательство. Вычислим среднее значение для каждого слагаемого x_i^2 и сложим эти средние (пользуясь их независимостью).

Объем слоя нашего симплекса между $x_i = u$ и $x_i = u + \varepsilon$ равен в первом приближении по ε произведению $C\varepsilon(1-u)^{T-2}$ (так как этот $(T-1)$-мерный слой толщины ε опирается на $(T-2)$-мерный симплекс $\{0 \leqslant x_j \leqslant 1-u,\ \sum x_j = 1-u,$ где $j \neq i\}$ объема $C(1-u)^{T-2}$).

Стало быть интеграл от x_i^2 по всему $(T-1)$-мерному симплексу есть

$$I = \int x_i^2\, dx^{T-1} = \int_{u=0}^{u=1} Cu^2(1-u)^{T-2}\, du = \int_0^1 Cv^{T-2}(1-v)^2\, dv.$$

Последний интеграл вычисляется уже легко (переход к автомодельной переменной v обязателен) и равен $I = C\left(\frac{1}{T-1} - \frac{2}{T} + \frac{1}{T+1}\right)$, в то время как объем всего нашего $T-1$-мерного симплекса равен аналогичному интегралу без множителя u^2, т. е. без $(1-v)^2$,

$$M = \frac{C}{T-1}.$$

Итак, среднее значение суммы T слагаемых Tx_i^2 есть $s_1 = T^2 I/M = T^2\left(1 - \frac{2(T-1)}{T} + \frac{T-1}{T+1}\right) = \frac{T^3(T+1) - 2T^2(T^2-1) + T^3(T-1)}{T(T+1)} = \frac{2T}{T+1}$, что и доказывает теорему.

Сравнивая наблюденные для геометрических прогрессий значения параметра стохастичности s со свободолюбивым значением s_1, я обнаружил, в большинстве прогрессий $\{2^t \bmod n\}$, меньшие свободолюбивого значения, $1{,}4 \leqslant s \leqslant s_1$, близкие обычно к 1,6, что указывает на заметное расталкивание вычетов членов геометрических прогрессий.

Но никаких теорем об асимптотике величины $s(n)$ при больших n я не доказал.

Замечание. Было бы интересно рассмотреть не только среднее значение s_1, но и другие характеристики истинно случайных множеств — например, функцию распределения величины x_i, или ее моменты, или распределение вероятностей различных разбиений суммы L на T целочисленных слагаемых x_i (в случае целочисленных значений переменных x_i)[2].

[2]Упомяну лишь, что в [1] доказано, что вероятности p_k встретить дуги длины k среди T дуг, на которые делят конечную окружность $\mathbb{Z}_m$ T разных случайно выбранных точек, пропорциональны биномиальным коэффициентам, стоящим на параллельной стороне прямой на расстоянии $T-2$ от стороны треугольника Паскаля:

$$p_k = C_{m-1-k}^{T-2} / C_{m-1}^{T-1} \quad (1 \leqslant k \leqslant m-T-1).$$

Например, для $T = 4$ случайных точек вероятности длин дуг соотносятся как

$$1:3:6:10:15\ldots$$

(наименьшую вероятность имеет наибольшая длина дуги, равная $m-T-1$).

Все эти интегралы явно вычислимы и задают кусочно-полиномиальные распределения (например, для величины s, зависящей от пробегающего симплекс случайного параметра x).

Вероятно, эти распределения (и особенно их универсальные асимптотики вблизи свободолюбивого среднего значения s_1 при больших T) заслуживают специального изучения в теории вероятностей или в стохастической геометрии.

Что же касается статистики геометрических прогрессий вычетов, то здесь распределения окажутся другими, и их изучение, даже экспериментальное, может привести к новым открытиям в этой эргодической теории чисел.

Я попытался исследовать, кроме геометрических прогрессий, также арифметические прогрессии вычетов $\{dt \pmod n,\ t = 1, 2, 3, \dots, T\}$ и множества взаимно простых с n вычетов, $\Gamma(n) \subset \mathbb{Z}_n$.

В обоих случаях наблюдаются заключенные между 1 и 2 значения параметра стохастичности s, т. е. расталкивание соседей друг другом. Вероятно, для случая арифметических прогрессий эти результаты можно доказать при помощи цепных дробей (и надлежащих обобщений теоремы Кузьмина).

§ 11. Дополнительные замечания о динамике Ферма—Эйлера

Экспериментальное исследование функций T и N переменной n привело меня к сотням наблюдений, некоторые из которых стали сегодня теоремами. Вот простейший пример.

Определение. Нечетное число n принадлежит классу N, если удовлетворяется сравнение Ферма—Эйлера

$$2^{\frac{\varphi(n)}{N}} \equiv 1 \pmod n.$$

Теорема. *Класс N представляет собой идеал в коммутативной мультипликативной группе нечетных чисел: если n принадлежит классу N, то и произведение n на любое нечетное натуральное число тоже ему принадлежит.*

Пример. Классу (3+) принадлежат числа **31**, **43**, 63, 91, 93, 117, 129, 133, 155, **157**, 171, 189, 215, 217, **223**, **229**, 247, 259, 273, 279, **283**, 301 (полужирным выделены простые числа).

Образующими полугруппы являются те из них, которые не кратны другим: это все простые элементы и еще 63, 91, 117, 133, 171, 247, 259.

Странное наблюдение, для которого не видно пока никаких оснований, состоит в том, что вычеты всех этих образующих по модулю 9 являются квадратичными (принадлежат четверке $\{0, 1, 4, 7\}$).

Аналогичный результат (так же как и этот, являющийся только наблюдением в пределах имеющихся таблиц, простирающихся, впрочем, довольно далеко) верен для класса (5+) и вычетов по модулю 25.

Для некоторых других N квадратичными оказываются вычеты по модулю N^2 не всех, а *простых* образующих идеала N.

Класс $(N-)$ определяется сравнением

$$2^{\varphi(n)/N} \equiv -1 \pmod{n}$$

для его элементов n.

Если число $\varphi(n)$ делится на 4 и нечетное число n принадлежит классу (2+), то n лежит либо в (4+), либо в (4−): по модулю n

$$(2^{\varphi(n)/4} - 1)(2^{\varphi(n)/4} + 1) = (2^{\varphi(n)/2} - 1) \equiv 0$$

по теореме Эйлера.

Но указать явно, какие из элементов класса (2+) лежат в (4+), а какие в (4−) не удается (как и не удается пока различить подклассы (8+) и (8−) внутри класса (4+)).

Условия принадлежности к разного рода классам иногда бывают довольно явными. Например, в статье [1] доказана

Теорема. *Если нечетное число n имеет k или больше разных простых делителей, то оно принадлежит классу* (2^k+).

Значительную информацию о классе числа-произведения дает иногда описание классов сомножителей. Например, в статьях [1] и [2] имеется (восходящая, вероятно, к Эйлеру, если не к Ферма)

Теорема. *Нечетное число p^a лежит в классе* (2+), *если простое число p дает при делении на* 8 *остаток* 1 *или* -1, *и в классе* (2−), *если оно дает остаток* 3 *или* -3.

Так что распознать принадлежность любого нечетного числа классам (2+) или (2−) легко. Но уже для классов (4+) и (4−) (и даже для простых чисел этих классов) положение сложнее и критерий неясен.

Например, числа

17, **41**, 57, **97**,

принадлежат классу (4−), а числа

65, **73**, **89**, **113**

— классу (4+), но причины этого неясны.

Таблицы подсказывают десятки разнообразных гипотез, часть из которых уже стала теоремами.

Например, в [1] доказано, что *если простое число $p = 8c + 1$* (вроде $p = 73$) *принадлежит классу* (4+), *то все произведения $p^a q^b$, где q — другое нечетное и простое число, принадлежат классу* (8+).

§ 12. Первообразные корни простого модуля

Здесь мы докажем теорему 2 из § 4, из которой выше доказана только половина: то, что $a^{p-1} \equiv 1 \pmod{p}$ для простого модуля p.

Остается доказать цикличность группы $\Gamma(n)$, т. е. существование такой геометрической прогрессии $\{a^t\} \bmod p$, все $p-1$ членов которой (с $1 \leqslant t \leqslant p-1$) различны (так что $a^t \not\equiv 1 \pmod{p}$ при $0 < t < p-1$).

Такое основание $a \in \Gamma(p)$ называется *первообразным корнем*. Оказывается, число таких корней равно $\varphi(p-1)$.

Доказательство существования первообразного корня основано на замечательном тождестве Эйлера: *сумма значений функции Эйлера во всех делителях d числа n равна самому этому числу n*:

$$\varphi(1) + \ldots + \varphi(d) + \ldots + \varphi(n) = n.$$

Например, делителями числа 6 являются $d = 1, 2, 3, 6$, и тождество сводится к соотношению

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + 2 = 6.$$

Доказательство тождества Эйлера получается из разбиения всех вычетов по модулю n в зависимости от их наибольших общих делителей.

Наибольший общий делитель d с числом n имеет вычет вида kd, причем число k должно быть взаимно простым с n/d (иначе общий делитель d вычетов с числом n не был бы наибольшим).

Итак, число вычетов, наибольший общий делитель каждого из которых с n есть d, равно $\varphi(n/d)$.

Все n вычетов $\bmod n$ разбиваются по делителям d числа n на классы (вычетов, наибольший общий делитель членов каждого из которых с n есть d) из $\varphi(n/d)$ элементов.

Поэтому общее число вычетов представлено в виде суммы по всем делителям d числа n,

$$n = \sum_d \varphi(n/d).$$

А так как число $k = n/d$ также является делителем числа n, и дополнительные делители d и k взаимно определяют друг друга, то последняя сумма может быть переписана и в виде

$$n = \sum_k \varphi(k),$$

где суммирование опять распространено на все делители числа n. Тождество Эйлера доказано.

Пример. Для $n = 6$ наибольшее общие делители $d = (1, 2, 3, 6)$ с числом $n = 6$ имеют вычеты $(1, 5)$, $(2, 4)$, (3), (6) соответственно. Числа

вычетов, имеющих такие наибольшие общие делители с $n=6$, равны $k=\varphi(6/1)=2$, $\varphi(6/2)=2$, $\varphi(6/3)=1$, $\varphi(6/6)=1$, соответственно, так что общее число вычетов ($n=6$) представлено указанным их разбиением на классы с разными наибольшими общими делителями d с числом n в виде

$$6=\varphi(6/1)+\varphi(6/2)+\varphi(6/3)+\varphi(6/6)=\varphi(6)+\varphi(3)+\varphi(2)+\varphi(1).$$

Рассмотрим теперь геометрические прогрессии вида $\{a^t \bmod p\}$, где p — нечетное простое число и где a взаимно просто с p. По теореме Ферма $a^{p-1}\equiv 1 \pmod p$, но для некоторых оснований a минимальный период прогрессии может оказаться равным не $p-1$, а одному из делителей T числа $p-1$:

$$a^T \equiv 1 \pmod p.$$

В этой прогрессии имеется тогда ровно $\varphi(T)$ членов $b=a^t$ (где $0<t<T$ взаимно просто с T), имеющих тот же минимальный период T прогрессии $\{b^t\} \pmod p$.

Действительно, $b^T=a^{tT}=(a^T)^t\equiv 1(p)$, а меньшим, чем T, период быть не может, так как $b^r=a^{tr}=a^u$, где u — меньший T остаток от деления tr на T; так что, если бы b^r было единицей по модулю p, то период T не был бы минимальным и для основания a.

Других решений сравнения $a^T\equiv 1(p)$, кроме T членов прогрессии $\{a^t\}$, по модулю p нет, так как сравнение степени T по простому модулю p со старшим коэффициентом 1 не может иметь больше T решений (по теореме Виета). Значит, $\varphi(T)$ — это полное число всех решений указанного сравнения.

Таким образом, распределение всех $p-1$ чисел $0<a<p$ (которые все взаимно просты с p) по их минимальным периодам T прогрессий $\{a^t \pmod p\}$ (являющимися притом делителями числа $p-1$) имеет вид

$$p-1=\sum \varphi(T), \qquad (*)$$

где суммирование идет по тем делителям T числа $p-1$, для которых одна из прогрессий $\{a^t\}$ имеет наименьший период T.

По тождеству Эйлера число $n=p-1$ равно сумме значений $\varphi(d)$ по *всем* делителям d числа $p-1$. Значит, и в сумме $(*)$ ни один делитель d не может отсутствовать. Доказана

Теорема. *Число остатков $0<a<p$ с наименьшим периодом d у прогрессии $\{a^t \pmod p\}$ равно $\varphi(d)$ для любого делителя d числа $p-1$.*

В частности, делителем является и число $d=p-1$.

Следствие. *Число первообразных корней по модулю p равно $\varphi(p-1)$ (и, в частности, такие корни всегда есть).*

Пример. Для модуля $p=7$ число первообразных корней есть $\varphi(6)=2$. Прогрессии $\{a^t \pmod 7\}$ $(t=1,2,\dots)$ (где $a=1,2,\dots,6$) и их наименьшие периоды $T(a)$ суть:

$$\{1,1,\dots\},\ T=1;$$
$$\{2,4,(8\equiv 1);2,\dots\},\ T=3;$$
$$\{3,(9\equiv 2),6,(18\equiv 4),(12\equiv 5),(15\equiv 1);3,\dots\},\ T=6;$$
$$\{4,(16\equiv 2),(8\equiv 1);4,\dots\},\ T=3;$$
$$\{5,(25\equiv 4),(20\equiv 6),(30\equiv 2),(10\equiv 3),(15\equiv 1);5,\dots\},\ T=6;$$
$$\{6,(36\equiv 1);6,\dots\},\ T=2;$$

Первообразные корни — это $a=3$ и $a=5$. Число корней периода $T=3$ также равно $\varphi(3)=2$.

§ 13. Узор координат квадратичных вычетов

Используем доказанные выше факты о геометрических прогрессиях для описания геометрии квадратичных вычетов по нечетным простым модулям p.

Обозначим через A какой-нибудь первообразный вычет $\bmod p$, $0<A<p$. Геометрическая прогрессия $\{A^t\}$, $0\leqslant t<p-1$, содержит (по разу) все ненулевые вычеты по модулю p. Квадратичные ненулевые вычеты соответствуют четным значениям t.

Обозначим через T наименьший период геометрической прогрессии $\{2^t\}$, $2^T\equiv 1 \pmod p$, и обозначим через N число строк диаграммы Юнга перестановки «умножение вычета на 2» множества всех $\varphi(p)=p-1$ ненулевых вычетов по модулю p (так что $TN=p-1$).

Основное предложение. *Все TN вычетов* $\pmod p$ *чисел*

$$A^r 2^s \quad (0\leqslant s<T,\ 0\leqslant r<N)$$

различны.

Доказательство. В случае совпадения двух вычетов мы получили бы равенство единице одного из таких же вычетов (а именно, равного отношению двух совпадающих),

$$A^u 2^v \equiv 1 (p) \quad (0\leqslant u<T,\ 0\leqslant v<N).$$

Если u и v не оба нули, то, возведя это сравнение в степень T, мы получили бы сравнение

$$A^{Tu}2^{Tv}\equiv A^{Tu}\equiv 1 \pmod p, \quad \text{где } 0<Tu<TN=\varphi(p),$$

т. е. вычет A не был бы первообразным по модулю p.

Итак, основное предложение доказано. Мы будем использовать вычеты $s \pmod T$ и $r \pmod N$ в качестве *координат* точек диаграммы Юнга или вычетов $A^t \equiv A^r 2^s \pmod p$.

Опишем *места, занимаемые в этих координатах квадратичными вычетами*. Они образуют замечательные узоры на плоскости (r, s). По самому определению, все вычеты с четными r и s квадратичны. Но их число составляет всего около четверти общего числа $p-1$ ненулевых вычетов, в то время как число квадратичных вычетов равно их половине, т. е. $(p-1)/2$ [3].

Значит, существуют и другие квадратичные вычеты, происходящие из квадратов вычетов $A^i 2^j$. Они равны $A^{2i} 2^{2j} \equiv A^r 2^s \pmod p$, где $r \neq 2i$.

Места (r, s) этих квадратов расположены на диаграмме Юнга поразному, в зависимости от остатка при делении простого модуля p на восемь.

Теорема. *Если* $p = 8c \pm 1$, *то квадратичными являются все вычеты четных строк,* $A^{2r} 2^s$ *и только они. При этом число строк* N *всегда четно.*

Если $p = 8c \pm 3$, *то квадратичные вычеты составляют половину каждой строки, а именно, квадратичны вычеты* $A^{2r} 2^{2s}$, $A^{2m-1} 2^{2m-1}$ *и только они.*

При этом число строк N *всегда нечетно, а длины* T *строк четны* (*делятся на* 4 *при* $p = 8c-3$ *и не делятся на* 4 *при* $p = 8c+3$).

Вот несколько примеров значений чисел строк N и их длин T:

$p = 8c+1$:

c	p	T	N
2	17	8	2
9	73	9	8
14	113	28	4
29	233	29	8

; $p = 8c+3$:

c	p	T	N
0	3	2	1
1	11	10	1
5	43	14	3
31	251	50	5

;

$p = 8c+5$:

c	p	T	N
0	5	4	1
1	13	12	1
4	37	36	1
13	109	36	3

; $p = 8c+7$:

c	p	T	N
0	7	3	2
3	31	5	6
15	127	7	18
53	431	43	10

.

Интересный вопрос о росте чисел T и N с ростом числа p изучен лишь эмпирически, и эксперимент подсказывает чаще гораздо меньшие, чем T,

[3] Операция возведения вычета в квадрат складывает множество ненулевых вычетов пополам потому, что квадрат 1 имеют только вычеты 1 и -1, поэтому каждый ненулевой квадрат является квадратом в точности двух вычетов, $\pm x$.

значения N (которые в среднем, быть может, даже остаются ограниченными).

Квадратичные вычеты (mod p) набраны полужирным шрифтом в следующих четырех диаграммах Юнга, строки каждой из которых — вычеты чисел $A^r 2^s$ с фиксированным r (координата $s = 0, 1, \ldots, T-1$ растет здесь слева направо, а координата $r = 0, 1, \ldots, N-1$ — сверху вниз, как это и обычно для матриц).

Мы рассмотрим четыре примера (с остатками 1, 3, 5 и 7 числа p по модулю 8).

$p = 17$: $N = 2$, $T = 8$,

1	**2**	**4**	**8**	**16**	**15**	**13**	**9**	$(18 \equiv 1)$
3	6	12	7	14	11	5	10	$(20 \equiv 3)$

;

$p = 43$: $N = 3$, $T = 14$,

1	2	**4**	8	**16**	32	**21**	42	**41**	39	**35**	27	**11**	22	$(44 \equiv 1)$
3	**6**	12	**24**	5	**10**	20	**40**	37	**31**	19	**38**	33	**23**	$(46 \equiv 3)$
9	18	**36**	29	**15**	30	**17**	34	**25**	7	**14**	28	**13**	26	$(52 \equiv 9)$

;

$p = 13$: $N = 1$, $T = 12$,

1	2	**4**	8	**3**	6	**12**	11	**9**	5	**10**	7	$(14 \equiv 1)$

;

$p = 31$: $N = 6$, $T = 5$,

1	**2**	**4**	**8**	**16**	$(32 \equiv 1)$
3	6	12	24	17	$(34 \equiv 3)$
9	**18**	**5**	**10**	**20**	$(40 \equiv 9)$
27	23	15	30	29	$(58 \equiv 27)$
19	**7**	**14**	**28**	**25**	$(50 \equiv 9)$
26	21	11	22	13	$(26 \cdot 3 \equiv 16)$

.

Легко увидеть из этих таблиц, что число $A = 3$ — первообразный вычет для модулей $p = 17$, 43 и 31. Предыдущая теорема утверждает, что узоры, образованные квадратичными вычетами на этих диаграммах, не случайны: приведенное ниже доказательство показывает, что именно такое расположение квадратичных вычетов (разное в зависимости от остатка при делении модуля p на 8) неизбежно.

Доказательство теоремы. Заметим прежде всего, что если число N четное, то в строках $A^r 2^s$ с нечетными r квадратов нет, поэтому в строках с четными r квадраты не только те (очевидные) вычеты, у которых s четно.

Если какой-либо вычет $A^{2r}2^{2n-1}$ является квадратичным, то квадратичными будут и все остальные вычеты вида такой же четности,

$$A^{2u}2^{2v-1} = A^{2r}A^{2n-1}(A^{u-r}2^{v-n})^2.$$

Итак, *при четном N квадратичные вычеты — это все вычеты четных строк*, $\{A^{2u}2^s\}$, *и только они*.

Если же число строк N нечетно, то, как мы сейчас докажем, *квадратичные вычеты составляют половину каждой строки*: *это вычеты* $\{A^r 2^s\}$, *где r и s одной четности*.

Для доказательства обозначим нечетное число N через $2r-1$ (и заметим, что период T при нечетном N четен, так как произведение $NT = p-1$ — четное число).

Квадрат элемента A^r есть $A^{N+1} = A^N A$.

Лемма 1. *Имеет место сравнение элементов N-й и нулевой строк*,

$$A^N \equiv 2^i \pmod{p},$$

где i — некоторое целое число, $0 < i < T$.

Доказательство. Произведения вида

$$A^u 2^v \quad (\text{где } 0 \leqslant u < N,\ 0 \leqslant v < T)$$

исчерпывают все $NT = \varphi(p)$ вычетов по модулю p по доказанному выше основному предложению. Поэтому вычет A^{N+1} совпадает с одним из них.

Он не может совпасть с вычетом элемента $A^w 2^i$ какой-либо промежуточной строки (для которой $0 < w < N$) по тому же основному предложению. Значит, $w = 0$ и лемма доказана.

Представляя теперь вычет квадрата элемента A^r в виде стоящего в первой строке вычета $A2^i$, мы заключаем, что квадратичными являются также все вычеты элементов всех строк $A^u 2^{iu}$, а, следовательно, и всех элементов вида $A^u 2^j$, где j имеет такую же четность, как iu.

Таким образом мы получили в каждой из N строк по $T/2$ квадратичных вычетов, т. е. всего $\varphi(p)/2$ квадратичных ненулевых вычетов, а значит, мы получили все квадратичные вычеты.

Кроме того, мы заключаем, что число i нечетно, так как иначе сам вычет A оказался бы квадратическим, так что $A \equiv A^{2s} \pmod{p}$, $A^{2s-1} \equiv 1 \pmod{p}$, и нечетное число $2s-1$ должно было бы делиться на четный период $\varphi(p)$ операции умножения вычетов на первообразный вычет A.

Из нечетности числа i вытекает одинаковость четностей обоих показателей u, v квадратичных вычетов $A^u 2^v$ в случае нечетности числа строк N.

Чтобы закончить теперь доказательство теоремы, исследуем четность числа строк N (в зависимости от остатка при делении простого модуля p на 8).

Лемма 2. *Если* $p = 8c \pm 3$, *то число строк* N *нечетно.*

Доказательство. Если бы число строк N было бы четным, то мы нашли бы, для указанных простых чисел p, соответственно,

$$\begin{array}{cc} \varphi = 8c + 2 = 2(4c+1); & \varphi = 8c - 4 = 4(2c-1); \\ N = 2m; & N = 2m \text{ или } N = 4m; \\ 4c + 1 = mk; & 2c - 1 = mk; \\ T = k & T = 2k \text{ или } T = k; \end{array}$$

(где число k везде нечетно как делитель нечетного числа $\varphi/2$ или $\varphi/4$ соответственно, равного mk).

Из указанных формул мы получаем сравнение

$$2^{\varphi/2} = 2^{mk} \equiv (2^T)^m \equiv +1 \quad \text{при} \quad p \equiv 3 \pmod 8.$$

Если же $p = 8c - 3$, то имеет место либо сравнение

$$2^{\varphi/2} = 2^{2mk} \equiv (2^T)^m \equiv +1$$

в первом указанном выше случае (когда $N = 2m$), либо же сравнение

$$2^{\varphi/2} = 2^{mk} \equiv (2^T)^{2m} \equiv +1$$

во втором, когда $N = 4m$. Это во всех трех случаях противоречит свойству $p \in (2-)$ простых чисел $p = 8c \pm 3$, т. е. выполняющемуся для них сравнению Ферма—Эйлера (имеющемуся в статье [2])

$$2^{\varphi(p)/2} \equiv -1 \pmod p.$$

Лемма 2 доказана.

Лемма 3. *Если* $p = 8c \pm 1$, *то число* N *четно.*

Доказательство. Пусть $p = 8c - 1$. Тогда $\varphi = 8c - 2 = 2(4c-1)$, и, если бы число N было нечетным, то мы нашли бы четный период $T = 2m$, $4c - 1 = mk$, $N = k$.

Мы получили бы тогда для последовательности вычетов $\{2^t \pmod p\}$ период $T = 2m$ (по теореме Эйлера или Ферма, что $p \in (2+)$) и $\varphi(p)/2 = mk$. Из нечетности последнего числа следует, что период T не минимален, вопреки своему определению. Значит, предположение о нечетности числа строк N неверно, и лемма доказана в случае $p = 8c - 1$.

Доказательство в случае $p = 8c + 1$ сложнее, и мы рассмотрим сперва некоторые вспомогательные конструкции.

По теореме Ферма—Эйлера, имеет место сравнение (доказанное, например, в [2])

$$2^{\varphi(p)} - 1 \equiv 0 \pmod{p}.$$

Представим число $\varphi(p) = 8c$ в виде произведения $\varphi(p) = 2^a n$, где число n нечетно ($a \geqslant 3$). Разлагая разности квадратов на множители, мы перепишем сравнение Ферма—Эйлера в виде

$$(2^{t_1} + 1) \ldots (2^{t_i} + 1) \ldots (2^n + 1)(2^n - 1) \equiv 0 \pmod{p},$$

где $t_i = 2^{a-i} n$, $1 \leqslant i \leqslant a$.

Одна из этих скобок — нулевой вычет, и мы разберем по очереди два случая.

Случай I. Имеет место сравнение

$$2^n \equiv 1 \pmod{p}.$$

Утверждение. *В этом случае период T — нечетный делитель числа $n = Tm$, а число строк четно, $N = 2^a m$.*

Действительно, нечетное число n является (по условию I) одним из периодов умножения вычетов на 2, а значит, кратно наименьшему периоду, который, следовательно, нечетен. Значит, число строк N четно, так как $TN = \varphi(p)$ — четное число.

Случай II. Имеет место сравнение

$$2^{t_i} \equiv -1 \pmod{p}.$$

Утверждение. *В этом случае число N четно.*

Действительно, возведя сравнение II в квадрат, мы убедимся, что число $2t_i = 2^{a-i+1} n$ является одним из периодов операции умножения вычетов на 2, и, следовательно, кратно наименьшему периоду T.

С другой стороны, знак минус в сравнении II показывает, что само число $t_i = 2^{a-i} n$ этому периоду T не кратно. Значит, число T делится на 2^{a-i+1} и имеет поэтому вид

$$T = 2^{a-i+1} m,$$

где m — нечетный делитель нечетного числа $n = mk$.

Стало быть, число $N = \varphi(p)/T = 2^a mk/(2^{a-i+1} m) = 2^{i-1} k$ четно, если $i > 1$.

Если бы число i равнялось 1, то мы имели бы

$$2^{\varphi(p)/2} \equiv -1 \pmod{p}$$

вопреки теореме Эйлера—Ферма ($8c+1 \in (2+)$), согласно которой (см., например, статью [2])

$$2^{\varphi(p)/2} \equiv +1 \pmod{p}.$$

Итак, мы проверили, что N нечетно, и закончили доказательство леммы 3.

Соединяя полученную информацию о четности чисел T и N с проведенным в начале доказательства теоремы анализом координат u и v квадратичных вычетов $A^u 2^v$ в зависимости от четности чисел T и N, мы заканчиваем доказательство теоремы.

§ 14. Приложения к квадратичным сравнениям

Из доказанного в предыдущем параграфе описания узора координат квадратичных вычетов сразу следуют удивительные результаты о представлении чисел квадратичными формами (описание этой теории и ее связей с релятивистским миром де Ситтера имеется в статье [9]).

Теорема 1. *Если число x^2+y^2 делится на простое число $p=4c+3$, то и x и y делятся на него.*

Иными словами:

Теорема 1′. *Сравнение $x^2+y^2 \equiv 0 \pmod{p}$ не имеет ненулевых решений $x \pmod{p}$, $y \pmod{p}$, если p дает при делении на 4 остаток 3.*

Следствие. *Если уравнение $x^2+y^2=n$ имеет целочисленное решение, и $n=\prod p_i^{a_i} \prod q_j^{b_j}$ — разложение правой части n на простые множители, где $p_i \equiv 3 \pmod 4$ для всякого i, то имеет целочисленное решение уже и уравнение без множителей p_i в правой части, т. е.*

$$x^2+y^2=m,$$

где $m=\prod q_j^{b_j}$.

Замечание 1. В частности, ни одно из чисел $n=3, 27, 21, 63$ не представимо в виде x^2+y^2 с целыми x и y.

Замечание 2. В действительности все простые числа $q \equiv 1 \pmod 4$ (и следовательно, согласно статье [9], все произведения их степеней) представимы в виде x^2+y^2.

Разрешимость этих уравнений для ненулевых вычетов следует из результатов предыдущего параграфа, но саму представимость $q=x^2+y^2$ (например, $5=4+1$, $13=9+4$, $17=16+1$) мы доказывать не будем, ограничиваясь исследованием сравнений.

Теорема 2. *Если число x^2+2y^2 делится на простое число $p=8c+5$ или $8c+7$, то и целые числа x и y делятся на него.*

Подобно теореме $1'$ и ее следствию, теорема 2 сводит решение уравнения $x^2+2y^2=n$ к случаю, когда каждый простой множитель p числа n дает при делении на 8 в остатке 1 или 3. В этом случае уравнение $x^2+2y^2=p$ имеет на самом деле целочисленное решение (откуда следует, согласно статье [9], и разрешимость уравнения с любой правой частью n, делящейся лишь на такие простые числа). Но мы не будем этого доказывать, ограничившись лишь легко вытекающим из предыдущего параграфа анализом сравнений (теоремой 2).

Пример. Для $p=5$ всевозможные значения вычетов x, y и формы $x^2+2y^2 \pmod 5$ составляют матрицу.

y \ x	0	1	2	3	4
0	0	1	4	4	1
1	2	3	1	1	3
2	3	4	2	2	4
3	3	4	2	2	4
4	2	3	1	1	3

Нулевая по модулю 5 *сумма* x^2+2y^2 *встречается только в одном случае*, $x\equiv 0\equiv y \pmod 5$.

Теорема 2 обобщает это наблюдение на случай произвольного простого числа p вместо 5, но при условии, что оно дает при делении на 8 остаток 5 или 7: в матрице будет тогда только один нуль.

Для $p\equiv 1$ или $3 \pmod 8$ положение совершенно иное, решения есть (для сравнений вместо уравнений, можно было бы получить полное решение из результатов предыдущего параграфа). Это уравнение было изучено Якоби, Эйлером и Ферма.

Пример. Формой x^2+2y^2 представимы простые числа

$$17=3^2+2\cdot 2^2\equiv 1 \pmod 8,$$
$$19=1^2+2\cdot 3^2\equiv 3 \pmod 8$$

и вообще *все простые числа*, *сравнимые с* 1 *или с* 3 *по модулю* 8, *а также все их произведения* (утверждение о произведениях следует из статьи [9]).

Для вопроса о представлении целого числа целочисленной квадратичной формой доказана его принципиальная сводимость к сравнениям: *если как сравнение по достаточно многим модулям уравнение степени два разрешимо*, *то оно имеет и настоящее целочисленное решение* («принцип Хассе»).

Напротив, для диофантовых уравнений более высоких степеней встречается случай разрешимости по любому модулю при отсутствии настоящего целочисленного решения (не знаю, насколько часто это бывает).

Вопрос здесь сходен с проблемой сходимости формальных степенных рядов для решения задач анализа. Из существования такого формального ряда следует разрешимость уравнения по модулю сколь угодно высоких степеней переменных, но не следует, вообще говоря, существование аналитического решения: ряд может расходиться.

Доказательство теоремы 1. Пусть сначала $p = 8c + 3$. Воспользуемся описанием узора координат остатков от деления на p квадратов ненулевых вычетов

$$x^2 \equiv A^{2r} 2^{2s} \quad \text{или} \quad A^{2r-1} 2^{2s-1} \quad \text{при } p = 8c + 3.$$

По теореме Эйлера—Ферма, $p \in (2-)$, т. е. имеет место сравнение

$$(2^{\varphi/2} = 2^{4c+1}) \equiv -1 \pmod{p}.$$

Из этого сравнения мы заключаем, что противоположные квадратам вычеты образуют дополнительный узор,

$$-y^2 \equiv A^{2r-1} 2^{2s} \quad \text{или} \quad A^{2r} 2^{2s-1}.$$

Поэтому сравнение $x^2 + y^2 \equiv 0$, т. е. $x^2 \equiv -y^2 \pmod{p}$, не имеет ненулевых решений, и *теорема* 1 *доказана в случае* $p \equiv 3 \pmod 8$.

При $p = 8c + 7$ ненулевые квадраты вычетов имеют вид $x^2 \equiv A^{2r} 2^s$ (по теореме о координатах квадратичных вычетов).

Из сравнения $x^2 + y^2 \equiv 0 \pmod{p}$ при $y^2 \equiv A^{2u} 2^v$ мы получили бы

$$A^{2u} 2^v (1 + A^{2(r-u)} 2^{s-v}) \equiv 0 \pmod{p},$$

что, как мы сейчас увидим, невозможно.

Действительно, вычет -1 по модулю p может иметь только одна степень первообразного вычета A, а именно $A^{\varphi/2} = A^{4c+3}$ (ведь квадрат этой величины должен быть вычетом 1, так что удвоенный показатель степени должен делиться на период $\varphi(p)$ прогрессии $\{A^t\}$).

Итак, при $x^2 + y^2 \equiv 0 \pmod{p}$ мы получили бы сравнение

$$A^{2(r-u)} 2^{s-v} \equiv A^{4c+3} \pmod{p}.$$

Используя сравнение $2^T \equiv 1 \pmod{p}$ и определение числа строк N, мы приводим его к сравнению вида

$$A^d 2^e \equiv 1 \quad (0 \leqslant d < N,\ 0 \leqslant e < T)$$

с нечетным показателем d. Это последнее сравнение противоречит доказанному в предыдущем параграфе основному предложению о различии всех NT вычетов такого вида.

Стало быть, *сравнение* $x^2+y^2\equiv 0 \pmod p$ *не имеет ненулевых решений вида* $p=8c+7$.

Теорема 1 доказана (открыл ли ее первым Ферма или только Эйлер, я не сумел понять).

Доказательство теоремы 2. Пусть опять $p=8+7$, так что узор квадратов имеет вид

$$x^2\equiv A^{2r}2^s,\quad y^2\equiv A^{2u}2^v \pmod p.$$

В этом случае имеет место сравнение

$$x^2+2y^2\equiv A^{2r}2^s+A^{2u}2^{v+1} \pmod p.$$

Неразрешимость этого сравнения относительно не нулевых вместе вычетов x, y уже доказана (при разборе случая $p=8+7$) в доказательстве теоремы 1. Значит, *не нулевых вместе решений сравнение* $x^2+2y^2\equiv 0 \pmod p$ *не имеет*.

Пусть теперь $p=8+5$. В этом случае из теоремы о координатах квадратичных вычетов мы находим сравнения для узора ненулевых квадратов

$$x^2\equiv A^r2^{2i}\quad (0\leqslant r<N,\ 0\leqslant 2i<T),$$
$$y^2=A^u2^{2v}\quad (0\leqslant u<N,\ 0\leqslant 2v<T).$$

Следовательно, из сравнения $x^2+2y^2\equiv 0 \pmod p$ (с не нулевыми вместе вычетами x и y) вытекает сравнение

$$A^r2^{2i}+A^u2^{(2v+1)}\equiv 0 \pmod p.$$

С другой стороны, по теореме Ферма—Эйлера «$p\in(2-)$» из [2] имеет место сравнение

$$(2^{\varphi(p)/2}=2^{4c+2})\equiv -1 \pmod p,$$

так что мы можем привести предыдущее сравнение к виду

$$A^r2^{2i+4c+2}\equiv A^u2^{2v+1} \pmod p.$$

Это сравнение опять противоречит неразрешимости сравнений вида

$$A^d2^e\equiv 1\quad (0\leqslant d<N,\ 0\leqslant e<T)$$

(где $(d,e)\neq(0,0)$), доказанному в основном предложении предыдущего параграфа (о различии всех NT вычетов такого вида).

Теорема 2 доказана.

Все эти примеры применения геометрии узоров, образуемых квадратичными вычетами $A^d 2^e$ на плоскости с координатами d и e, подсказывают возможность использования наших результатов и их естественных обобщений на прогрессии $\{a^t\}$ для исследования мультипликативной полугруппы целых чисел, образованной всеми значениями бинарной квадратичной формы $mx^2 + ny^2 + kxy$. Полугруппу значения формы образуют, например, если форма представляет единицу (как ее представляет всякая форма вида $x^2 + ny^2$). Другой пример полугруппы образуют значения $\{Nf\}$, где N — одно из значений формы f (скажем, значения формы $4x^2 + 2ny^2 = 2(2x^2 + ny^2)$). Много других примеров описано в статье [9].

Все эти мультипликативные полугруппы было бы интересно исследовать в геометрических терминах многогранников Ньютона, образованных векторными показателями степеней входящих в элементы полугруппы простых множителей:

$$n = 2^a 3^b 5^c 7^d \ldots.$$

Векторы бесконечномерного пространства с компонентами $(a, b, c, d, \ldots)$, соответствующие входящим в полугруппу значений числам n, образуют уже аддитивную полугруппу, и интересно было бы узнать, допускает ли она столь простое описание, как полугруппа значений формы Гаусса квадрата нормы комплексных чисел $x^2 + y^2$, где это описание таково: *показатели* $(b, d, \ldots)$ *простых чисел, дающих при делении на* 4 *в остатке* 3, *должны быть четными*.

В случае формы $x^2 + 2y^2$ описание полугруппы значений тоже просто: *четными должны быть показатели простых чисел, дающих при делении на* 8 *в остатке* 5 *или* 7.

Но вообще, говоря, аддитивные полугруппы целочисленных векторов могут иметь куда более сложную структуру (например, для полугрупп векторов на плоскости или в трехмерном пространстве).

Было бы интересно узнать, встречаются ли такие сложности в полугруппах теории чисел, или же, может быть, полугруппа значений квадратичной формы всегда допускает простое описание, подобное приведенным выше примерам (или конечности базиса полиномиального идеала).

В обоих наших примерах, ограничения накладывались только на векторную оболочку аддитивной полугруппы (условия четности некоторых координат), тогда как в общей аддитивной полугруппе возможны еще ограничения типа неравенств. Можно взять, например, в качестве аддитивной полугруппы множество тех целых точек некоторой решетки, которые лежат внутри какого-либо выпуклого конуса (или многогранника Ньютона).

Ни одного примера полугрупп значений квадратичных форм с такими нетривиальными многогранниками Ньютона я не знаю.

В самой геометрии аддитивных полугрупп, даже состоящих просто из натуральных чисел, тоже много открытых вопросов. Например, полугруппа $\{mx+ny\}$, порожденная двумя взаимно простыми натуральными числами x и y (и состоящая из их линейных комбинаций с неотрицательными целыми коэффициентами), содержит все целые числа, начиная с указанного Сильвестром предела $K=(m-1)(n-1)$, а от нуля до этого предела полугруппа содержит ровно половину целых чисел (а именно, если число c входит, то $K-1-c$ не входит в полугруппу). Пример: $x=3$, $y=5$, $K=8$, входят $\{0,3,5,6\}$; не входят — $\{7,4,2,1\}$.

Обобщения этих результатов Сильвестра на случай бóльшего двух числа образующих остаются пока гипотезами, даже если ограничиваться (как это и разумно здесь делать) усредненными асимптотиками величин вроде $K(x,y,z)$ для большинства больших векторов (x,y,z), пренебрегая редко встречающимися большим отклонениями (подробнее об этом написано в статье [3]).

Интересно также исследовать число представлений большего элемента полугруппы суммами образующих: здесь тоже имеются, видимо, красивые ответы, если не гнаться за точными формулами, а ограничиваться средними асимптотиками, описывающими кратности проекций множества целых точек соответствующего выпуклого многогранника на типичные целочисленные прямые (и пренебрегая редко встречающимися большими уклонениями от средних).

Переход к подобным усредненным асимптотикам является самым многообещающим подходом ко многим задачам диофантовой геометрии, включая и задачи о целочисленных квадратичных формах и о целочисленных геометрических прогрессиях, рассматривавшиеся Ферма и Эйлером и описанные выше (см. также [3]).

Эта программа применима, например, к исследованию асимптотики наименьшего периода $T(a,n)$ геометрической прогрессии $\{a^t \pmod n,\ t=1,2,\dots\}$ при больших значениях модуля n: верно ли, что период $T(2,n)$ растет (в среднем) как степенная функция от n (или, во всяком случае, быстрее, чем $n^{1-\alpha}$, или чем $n/\ln n$)? Как растет период $T(3,n)$? Что происходит с периодом при одновременном росте и a, и n (при значениях a порядка cn)?

Здесь были бы интересны даже просто численные эксперименты: именно так Ферма открыл свою «малую теорему», а Лежандр — закон распределения простых чисел (со средней плотностью $1/\ln n$).

Таблица периодов $T(a,n)$ геометрических прогрессий $\{a^t \pmod n,\ t=1,2,\dots\}$ начинается со следующих значений наименьших периодов:

a																					
20																					
19																				2	
18																		2			
17																2		9		4	
16																	2		9		
15															2		8		18		
14														2			16		18		
13													2	4	4	4	4	3	18	4	
12												2					16		6		
11											2	12	3	2	4	16	6	3	2		
10										2		6				16		18			
9									2	5		3	3		2	8		9	2		
8								2		10		4		4		8		6			
7							2	3	4	10	2	12		4	2	16	3	3	4		
6						2				10		12				16		9			
5					2	6	2	6		5	2	4	6		4	16	6	9			
4				2		3		3		5		6		2		4		9			
3			2	4		6	2		4	5		3	6		4	16		18	4		
2		2		4		3		6		10		12		4		8		18			
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	n	
S	1	4	7	18	21	43	50	71	82	145	152	227	248	271	294	465	486	669	694		
M	1	1,5	1,5	2,75	1,5	3,5	1,75	3,5	2,75	6,3	1,75	6,25	3,5	2,9	2,9	10,7	3,5	10,2	3,1		

В графе S внизу таблицы указана для каждого модуля n сумма всех периодов, $S = \sum T(a, m)$, для $1 \leqslant a < m$ (взаимно простых с m) для предыдущих модулей, включая n (для $m \leqslant n$). Суммирование облегчает анализ асимптотик, играя роль усреднения.

В графе M указан средний (по a) период для каждого модуля n. Значения a берутся только взаимно простые с n.

Ориентировочные выводы о поведении в среднем подсказывают, что S растет подобно $cn^2/2$ (с коэффициентом c порядка $1/5$), а средний период M — подобно qn (с коэффициентом q порядка $1/3$).

Эти наблюдения интересно сравнить с тем обстоятельством, что для простого n максимальное значение периода, $T(a, n) = \varphi(n)$, достигается на $\varphi(\varphi(n))$ первообразных вычетах a по модулю n. Если учесть, что функция Эйлера φ в среднем растет как $(6/\pi^2)n$, и если (незаконно) воспользоваться предыдущим обстоятельством для не простых n тоже, то получился бы вклад этих наибольших периодов в их сумму порядка $(6/\pi^2)^3 n$, а в сумму S по предыдущим модулям — порядка $(6/\pi^2)^3 n^2/2 \approx n^2/7$.

В качестве оправдания незаконного перехода от простых n к произвольным, замечу, что для $\varphi(n)$ переход от $\varphi(p) = p - 1$ к среднему росту $\varphi(n)$ как $(6/\pi^2)n$ лишь меняет в асимптотике коэффициент 1 на $6/\pi^2 \approx 2/3$.

Для среднего периода такое же (незаконное) рассуждение дает линейный рост с модулем, n: доля максимальных значений периодов составляет в среднем порядка $2/3$ от всех периодов $T(a,n)$ (при фиксированном модуле n), так что можно грубо оценивать средний период как две трети максимального, равного $\varphi(n)$. Предполагая последний растущим как $(2/3)n$, получаем грубую оценку среднего по a периода порядка $(4/9)n$. Но, конечно, простые значения n составляют лишь малую долю всех, (да и $\varphi(n)$ для них порядка n, а не $(2/3)n$), так что распространение формул, имеющих место для простого модуля, на средние по n значения надлежит сопроводить надлежащими изменениями (хотя бы значений коэффициентов), для осуществления которых предыдущую таблицу периодов нужно было бы продолжить гораздо дальше.

Для геометрических прогрессий с фиксированным основанием a таблица тоже приводит к эмпирическим данным об усредненном по n росте периода $T(a,n)$ с ростом модуля n (взаимно простого с a).

В переделах приведенной выше таблицы приближение имеет линейный вид $T(2,n)\approx un$, $u\approx 0{,}38$, а для основания $a=3$ — вид $T(3,n)\approx vn$, $v\approx 0{,}31$. Но это — только усреднение, отклонения от них довольно велики ($T(2,15)=4$, но $T(2,19)=18$). Проведенные мною при бóльших модулях n, вплоть до $n=511$, вычисления периода $T(2,n)$ показывают в среднем линейный по n рост с несколько меньшим при бóльших n коэффициентом u и не исключают возможности убывания этого «коэффициента» с ростом n (скажем, как $1/\ln n$).

Например, $T(2,511)=9$, но соседние модули дают гораздо бóльшие периоды: $T(2,499)=166$, $T(2,503)=251$, $T(2,509)=508$, а среднее периодов $T(2,n)$ по десятку нечетных модулей от $n=493$ до $n=511$ равно примерно 158, что соответствовало бы коэффициенту $u\approx 1/3$.

Проведенные по моей просьбе Ф. Аикарди вычисления значений периодов $T(n)$ и чисел орбит $N(n)$ при модулях $n\leqslant 2001$ приводят к следующим (удивительным) приближенным эмпирическим формулам, удовлетворительно описывающим рост этих функций в среднем:

$$N\sim 0{,}67n^{2/5},\quad T\sim 1{,}41n^{4/5}.$$

Эти «слабые асимптотики» получаются из линейной (неоднородной) аппроксимации наблюденной зависимости логарифмов сумм значений

$$\lg\left(\sum_{k-1}^{n}N(k)\right),\quad \lg\left(\sum_{k-1}^{n}T(k)\right)$$

от логарифма аргумента, $\lg n$ (где суммирование распространено на нечетные значения k, если исследуются период T и число орбит N системы

Ферма—Эйлера, определяющей геометрическую прогрессию вычетов $\{2^t \pmod k\}$).

Таблицы Аикарди доставляют, например, следующие значения сумм:

n	9	109	509	1009	1509	2009
$\sum^n N$	5	132	1017	2625	4651	6921
$\sum^n T$	15	1409	23607	82761	176016	302277

(для $2001 < k \leqslant 2009$ данные экстраполированы).

Если бы число орбит и период имели асимптотики степенного вида,

$$N(n) \sim an^{\alpha}, \quad T(n) \sim bn^{\beta},$$

то для сумм получились бы (интегральные) асимптотики тоже степенного вида,

$$\sum_{k=1}^{n} N(k) \sim \tilde{a} n^{\alpha+1}, \quad \sum_{k=1}^{n} T(k) \sim \tilde{b} n^{\beta+1}.$$

Поэтому эмпирические данные о поведении $\sum N$ и $\sum T$ (сумм, которые ведут себя гораздо менее хаотически, чем сами сильно осциллирующие слагаемые N и T) доставляют приближенные значения коэффициентов $(a, \alpha; b, \beta)$, которые и указаны выше.

Замечание. Полученные из наблюдений значения $\alpha \approx 2/5$ и $\beta \approx 4/5$ могут удивлять, так как произведение $\varphi(n) = N(n)T(n)$ растет в среднем как cn (где $c = 6/\pi^2 \approx 2/3$).

Казалось бы, сумма показателей асимптотик, α и β, должна бы быть поэтому равной единице (показателю слабой асимптотики произведения φ).

Но слабая асимптотика произведения может сильно отличаться от произведения слабых асимптотик сомножителей, так как среднее значение произведения может сильно отличаться от произведения средних значений сомножителей, особенно если большие и малые значения сомножителя перемежаются.

Пример. Предположим, что значения сомножителя $N(n)$ перемежаются в окрестности значения n своего аргумента так: N принимает два значения

$$(N_1 = n^u) \gg (N_2 = 1) \quad (0 < u < 1),$$

причем первое в n^w раз чаще, чем второе ($w > 0$).

Для сохранения значения произведения $NT = n$ предположим, что второй сомножитель принимает, соответственно, значения

$$(T_1 = n^{1-u}) \ll (T_2 = n).$$

В этой ситуации вклады указанной окрестности в $\sum N$ и в $\sum T$ определяются, соответственно, в основном первой и в основном второй частью: они пропорциональны, соответственно, n^{u+w} и n^1 (если $1-u+w<1$, чтобы вклад $\sum T_1$ был меньше вклада $\sum T_2$).

Таким образом, наблюдаемые эмпирически слабые асимптотики сомножителей были бы степенными, с показателями

$$\alpha = u + w, \quad \beta = 1,$$

сумма которых больше 1.

Для этого нужно только, как указано выше, чтобы показатель перемежаемости, w, превосходил величину показателя u.

Анализ наблюденных значений $T(n)$ и $N(n)$ показывает их значительную перемежаемость. Например, значения числа $N(n)$ изменяются при небольшом изменении аргумента n в десятки раз:

$$N(1969) = 2, \quad N(1971) = 72, \quad N(1973) = 1.$$

Неплохую в среднем аппроксимацию частот p_N значений величины $N(n)$ при изменении аргумента в окрестности данного значения модуля n дают (для $n \leqslant 2001$) следующие эмпирические приближенные слабые асимптотические формулы (где $N = 1, 2, 4, 8$ и $N \geqslant 10$):

$$p_1 \sim C_1 n^{-7/18}, \ p_2 \sim C_2 n^{-1/9}, \ p_4 \sim C_4 n^{1/3}, \ p_8 \sim C_8 n^{1/9}, \ p_{\geqslant 10} \sim C_{10} n^1.$$

Из этих формул видно, что отношения частот встречаемости больших и малых значений N ведут себя как степенные (в среднем) функции от n (подобные величине n частоты перемежаемости в разобранном выше примере).

Все эти, не подтвержденные никакими теоремами, эмпирические данные можно рассматривать как математические гипотезы. В их пользу говорит удивительно точное расположение графиков соответствующих функций#сумм f и g, нарисованных на двойной логарифмической бумаге в окрестностях соответствующих прямых линий.

Речь идет о функциях (определенных значениями $N(k) = y$ и $T(k) = z$, встречаемость которых изучается):

$$f_y(n) = (\#k\colon N(k) = y, \ 1 \leqslant k \leqslant n);$$
$$g_z(n) = (\#k\colon T(k) = z, \ 1 \leqslant k \leqslant n).$$

Прямолинейность или почти прямолинейность их графиков на двойной логарифмической бумаге означает приближенные формулы

$$\lg f_y(n) \approx A_y \lg n + B_y, \ \lg g_z(n) \approx C_z \lg n + D_z \quad (A_y = 1 + \alpha_y, C_z = 1 + \beta_z).$$

Указанные выше показатели α_y, β_z степенных асимптотик ($\alpha_1 = -7/18$, ...) найдены именно путем рисования этих прямых, априорных оснований для рациональности этих показателей я не знаю (кроме, разве, теории турбулентности).

Список литературы

[1] Arnold V. Ergodic and arithmetical properties of geometric progression dynamics. To appear in Moscow Mathematical Journal.

[2] Арнольд В. И. Динамическая система Ферма—Эйлера и статистика арифметики геометрических прогрессий // Функциональный анализ и его приложения. 2003. Т. 37, вып. 1. С. 1—18.

[3] Арнольд В. И. Слабая асимптотика чисел решений диофантовых задач // Функциональный анализ и его приложения. 1999. Т. 33, вып. 3. С. 65—66.

[4] Арнольд И. В. Теория чисел. М.: Учпедгиз, 1939. 288 с.

[5] Fermat P. Œuvres de Fermat, T. I—IV. Paris, 1894—1912.

[6] Euler L. Commentationes arithmeticae collectae, T. 1. Санкт-Петербург, 1849. 584 с.; T. 2. Санкт-Петербург, 1849. 651 с.

[7] Jacobi C. G. J. Canon Arithmeticus. Berolini, 1839. 248 pp.

[8] Венков Б. А. Элементарная теория чисел. М.—Л.: ОНТИ, 1937. 218 с.

[9] Arnold V. I. Arithmetics of binary quadratic forms, symmetry of their continued fractions and geometry of their de Sitter world // Bull. Brasil Math. Soc. 2003. Vol. 3, №. 1. P. 1—41.

[10] Арнольд В. И. Топология и статистика формул арифметики // Успехи матем. наук. 2003. Т. 58, вып. 4. С. 3–28.

[11] Арнольд В. И. Топология алгебры: комбинаторика операции возведения в квадрат // Функциональный анализ и его приложения. 2003. Т. 37, вып. 3. С. 20–35.

[12] Летняя школа «Современная математика» (Москва—Дубна, 2002). МЦНМО, 2002. 40 с.

[13] Dirichlet L., Abhandlungen Akad. Wiss. Berlin (Math.). 1849. P. 78—81 (Werke, Vol. 2. P. 60—64.)

Оглавление

Владимир Игоревич Арнольд
ГРУППЫ ЭЙЛЕРА И АРИФМЕТИКА ГЕОМЕТРИЧЕСКИХ ПРОГРЕССИЙ

Лицензия ИД №01335 от 24.03.2000 г. Формат 60 × 90/16. Печать офсетная. Объем 2,75 печ. л. Тираж 1000 экз. Заказ № .

Издательство Московского центра непрерывного математического образования. 119002, Москва, Большой Власьевский пер., 11. Тел. 241—72—85.

Отпечатано с готовых диапозитивов в ФГУП «Полиграфические ресурсы».