Math-Net.Ru

Общероссийский математический портал

В. И. Арнольд, Динамическая система Ферма–Эйлера и статистика арифметики геометрических прогрессий, *Функц. анализ и его прил.*, 2003, том 37, выпуск 1, 1–18

DOI: <https://doi.org/10.4213/faa132>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.166.219.16

26 апреля 2023 г., 13:18:43

УДК 511.3+517.938+519.21

Динамическая система Ферма–Эйлера и статистика арифметики геометрических прогрессий

© 2003. В. И. Арнольд

§1. Орбиты и диаграммы Юнга динамических систем Ферма–Эйлера

ОПРЕДЕЛЕНИЕ 1. Динамическая система Ферма–Эйлера действует (на множестве вычетов по модулю n) по формуле $x \mapsto ax$, где число a взаимно просто с n . Ниже мы будем рассматривать случай $a = 2$, когда n — нечетное натуральное число.

Множество $\Gamma(n)$ вычетов, взаимно простых с n , инвариантно относительно системы Ферма–Эйлера.

ОПРЕДЕЛЕНИЕ 2. Число взаимно простых с n вычетов (считая и единицу) обозначается через $\varphi(n)$, и функция φ называется *функцией Эйлера* (обозначение введено Гауссом).

ПРИМЕР. Начальные значения: $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$, $\varphi(9) = 6$, $\varphi(15) = 8$.

«В среднем» φ растет при больших n как $(6/\pi^2)n$ (так как вероятность несократимости дроби p/q в среднем равна $1/\zeta(2)$). Здесь и дальше словами «в среднем» предваряются «слабые асимптотики», определенные в [2].

Для числа $n = \prod p_i^{a_i}$ (где p_i — разные простые) $\varphi(n) = \prod [(p_i - 1)p_i^{a_i - 1}]$, так как 1°) $\varphi(p) = p - 1$; 2°) $\varphi(p^a) = p^a - p^{a-1}$; 3°) делимости n на разные простые — независимые события.

Отображение Ферма–Эйлера переставляет между собой $\varphi(n)$ элементов множества $\Gamma(n)$.

ТЕОРЕМА 1. Все циклы этой перестановки Ферма–Эйлера имеют одинаковую длину (период) T , связанную поэтому с числом циклов соотношением $\varphi(n) = NT$, так что и $T(n)$, и $N(n)$ — делители числа $\varphi(n)$, причем выполняется следующее сравнение Ферма–Эйлера:

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

Иными словами, диаграмма Юнга перестановки Ферма–Эйлера — прямоугольник из N строк длины T каждая.

ДОКАЗАТЕЛЬСТВО. Если $a^T x = x$ и $z = xy$, то $a^T z = a^T(xy) = (a^T x)y = xy = z$. Но каждый элемент z из Γ представляется через любой другой (x) в виде $z = xy$, так как x и n взаимно просты (по определению Γ).

СЛЕДСТВИЕ. Имеет место сравнение Ферма–Эйлера

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

ДОКАЗАТЕЛЬСТВО. Число $\varphi(n)$, как и любое целое кратное периода T перестановки Ферма–Эйлера, тоже является ее периодом.

История этой теоремы Ферма–Эйлера и ее обобщений, с дискуссией вкладов Ферма, Эйлера, Гаусса, Якоби и других изложена подробно в книгах [3, 4].

ОПРЕДЕЛЕНИЕ. Мы будем говорить, что число n принадлежит классу $(N+)$, если имеет место сравнение (1) (в дальнейшем мы рассматриваем случай $a = 2$ и нечетные числа n , хотя перенесение большинства результатов на другие основания a несложно).

Нашей задачей будет исследование числа орбит $N(n)$, т.е. наибольшего решения N сравнения (1) (или, что то же, наименьшего периода $T(n)$ перестановки Ферма–Эйлера). Разумеется, делители N' числа N тоже доставляют решения сравнения (1), так что из принадлежности числа n классу $(N+)$ следует и его принадлежность каждому из классов $(N'+)$, где N' — делитель числа N .

Кроме сравнения (1), мы рассмотрим также сравнение

$$a^{\varphi(n)/M} \equiv -1 \pmod{n}. \quad (2)$$

Если оно имеет место, то мы будем говорить, что целое число n принадлежит классу $(M-)$. Мы будем рассматривать ниже случай $a = 2$ и нечетные n . Например, $43 \in (2-)$, $43 \in (6-)$, так как $128 + 1 = 43 \cdot 3$.

Число $M(n)$ определяется как наибольшее решение сравнения (2). Например, $M(43) = 6$. Отношение $\varphi(n)/M(n)$ — это наименьший период изменения знака периодической последовательности вычетов $\{a^i\}$. Разумеется, класс $(2N-)$ лежит в классе $(N+)$, так как

$$a^{\varphi(n)/N} = (a^{\varphi(n)/2N})^2 \equiv 1 \pmod{n},$$

если (2) выполнено при $M = 2N$. Точно так же класс $((2m+1)M-)$ содержит класс $(M-)$, поскольку $(-1)^{2m+1} = -1$.

Таблицы чисел $N(n)$ и $M(n)$ для нечетных n , меньших 512, приведены ниже, в §9. Эти таблицы подсказывают множество свойств классов $(N+)$ и $(N-)$. Некоторые из этих свойств доказаны ниже, а некоторые остаются пока загадочными экспериментальными наблюдениями (см. также статьи [5] и [6]).

§2. Идеал $(N+)$ в мультипликативной полугруппе нечетных натуральных чисел

Пусть нечетное число n лежит в классе $(N+)$, т.е. удовлетворяет сравнению (1), где $a = 2$:

$$2^{\varphi(n)/N} \equiv 1 + nA.$$

ТЕОРЕМА 2. Произведение числа n из класса $(N+)$ на нечетное натуральное число k также лежит в классе $(N+)$, т.е. имеет место сравнение вида (1)

$$2^{\varphi(kn)/N} \equiv 1 + knC$$

(с целым C).

ДОКАЗАТЕЛЬСТВО. Обозначим через D наибольший общий делитель чисел n и k , так что

$$n = PD, \quad k = QD, \quad (P, Q) = 1.$$

Функция Эйлера обладает (очевидным) мультипликативным свойством

$$\varphi(kn) = \varphi(k)\varphi(n)(D/\varphi(D)). \quad (3)$$

Из свойства (3) следует, что

$$2^{\varphi(kn)/N} = (2^{\varphi(n)/N})^{BD} = (1 + nA)^{BD}, \quad (4)$$

где целое число B дается формулой

$$B = \varphi(k)/\varphi(D) = \prod_{b_i > 0} p_i^{a_i - b_i} \prod_{b_i = 0} (p_i - 1)p_i^{a_i - 1},$$

если $D = \prod p_i^{b_i}$, $k = \prod p_i^{a_i}$ ($a_i \geq b_i$).

Для доказательства искомого сравнения вида (1) вычислим остаток от деления числа $(1 + nA)^{BD}$ на степени каждого из простых чисел, на которые делятся n или k . Пусть p — одно из этих простых чисел. Введем обозначения

$$D = p^d D', \quad P = p^u P', \quad Q = p^v Q',$$

где штрихованные множители на p уже не делятся. Из условия $(P, Q) = 1$ следует, что либо u , либо v равно нулю. Соответственно, мы находим кратности вхождения p в числа n , k и в BD :

$$\begin{aligned} n &= p^{u+d} n', & k &= p^d k', & BD &= p^d C, & \text{если } v = 0; \\ n &= p^d n', & k &= p^{v+d} k', & BD &= p^{d+v} C, & \text{если } u = 0 \end{aligned}$$

(во втором случае B делится на p^v из-за возможно большей кратности p в k , чем в D).

В предыдущих формулах штрихованные множители не делятся на p , а коэффициент C делиться на p может.

ЛЕММА. Целое число

$$(1 + p^a A)^{p^b E} - 1$$

делится на p^{a+b} , если $a \geq 1$.

ДОКАЗАТЕЛЬСТВО. По биномиальной формуле имеем

$$(1 + x)^m = 1 + mx + rx^2$$

с целым (при целых x и m) коэффициентом r . Поэтому при $a \geq 1$ мы получаем представление

$$(1 + p^a A)^p = 1 + p^{a+1} A + rp^{2a} A^2 = 1 + p^{a+1} A_1$$

с целым коэффициентом A_1 (поскольку $2a \geq a + 1$ при $a \geq 1$). Из этого, поскольку $a + 1 \geq 1$, вытекает, что

$$(1 + p^a A)^{p^2} = (1 + p^{a+1} A_1)^p = 1 + p^{a+2} A_2,$$

и, продолжая возводить результаты в степень p , после b возведений мы получим представление

$$(1 + p^a A)^{p^b} = 1 + p^{a+b} A_b$$

с целым коэффициентом A_b .

Доказываемая лемма получается из этого тождества возведением в степень E левой и правой частей.

Теперь для доказательства теоремы 2 мы применим лемму к соотношению (4) (учитывая уже подсчитанные выше кратности вхождения p в n , k и в BD):

$$\text{при } v = 0 \quad (1 + nA)^{BD} = (1 + p^{u+d}R)^{p^d C} = 1 + p^{u+2d}S,$$

$$\text{при } u = 0 \quad (1 + nA)^{BD} = (1 + p^d R)^{p^{d+v}C} = 1 + p^{v+2d}S.$$

Множитель перед целым числом S в обоих случаях делится на нужную для делимости на kn степень p (ведь $kn = p^{u+2d}k'n'$ при $v = 0$ или $p^{v+2d}k'n'$ при $u = 0$ соответственно, причем $k'n'$ на p уже не делится).

Итак, для каждого простого множителя p_i мы получили разложение (с целым коэффициентом C_i)

$$2^{\varphi(kn)/N} = 1 + C_i p_i^{a_i}, \quad \text{где } kn = \prod p_i^{a_i}.$$

Из полученного равенства

$$C_i p_i^{a_i} = C_j p_j^{a_j}$$

следует, ввиду различия простых чисел p_i и p_j , делимость коэффициента C_i на $p_j^{a_j}$ для всякого j , не равного i , так что, окончательно, мы доказали представление

$$2^{\varphi(kn)/N} = 1 + Ckn \quad (\text{с целым } C),$$

и теорема 2 доказана.

ПРИМЕР. Из приведенных ниже в §9 таблиц следует явный список чисел идеала (3+), меньших 512. Из этого списка вытекает перечень (меньших 512) образующих идеала (3+). Их 27, в том числе 15 простых (набранных ниже жирным шрифтом).

Образующие идеала (3+), меньшие 512:

31, 43, 63, 91, 109, 117, 127, 133, 157, 171, 223, 229, 247, 259,
277, 283, 307, 333, 397, 427, 433, 439, 457, 469, 481, 499, 511.

Я не знаю, *существуют ли образующие, кратные любому нечетному простому числу*: пока найдены кратные простым числам 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 109, 127 (это число 3 и простые вида $6s + 1$), а, например, образующие, кратные 5, мне неизвестны.

Все выписанные образующие дают при делении на $3^2 = 9$ остатки 0, 1, 4 или 7, являющиеся *квадратичными вычетами* по модулю 9. Поэтому я вычислил остатки при делении на 25 образующих идеала (5+), из которых меньше 512 следующие 7 образующих из таблицы §9:

151, 241, 251, 275, 341, 431, 451.

Остатки от деления этих чисел на 25 суть 1, 16, 1, 0, 16, 6, 1. Все эти остатки входят в число квадратичных вычетов по модулю 25 (которые суть $\{0, 1, 4, 9, 16, 0, 11, 24, 14, 6, 0, 21, 19\}$).

ЗАМЕЧАНИЕ. Из серии чисел $2^k - 1$ класс (3+) содержит числа (31, 63, 127, 511), но выпадают числа $n = 15$ и 255, для которых $\varphi(n) = 8$ и 128 даже не делятся на 3. Часто ли это происходит?

Число $\varphi(n)$, где $n = 2^{(2^m)} - 1$, не делится на 3 ($\varphi(n) = 2^t$, где $t = 2^m - 1$), пока суммы $2^{(2^s)} + 1 = 3, 5, 17, 257, \dots$ просты при $s < m$. В этом случае n не лежит в классе (3+). Ферма предполагал, что простота сохраняется и при больших s .

Число $2^{16} + 1 = 65537$ еще простое, но Эйлер опроверг гипотезу Ферма при $s = 5$: $2^{(2^5)} + 1 = 641 \cdot 6700417$. Второй простой множитель здесь вида $6s + 1$, поэтому $\varphi(n)$ делится на 6 при $m \geq 6$. Но лежат ли эти числа n в $(3+)$, неясно.

§3. Пересечения классов

Если числа K и N взаимно просты, то классы $(K+)$ и $(N+)$ очевидно пересекаются в точности по классу $(KN+)$. Докажем немного более общий факт.

ТЕОРЕМА 3. *Пересечение классов $(K+)$ и $(N+)$ есть класс $(X+)$, где число X — наименьшее общее кратное чисел K и N .*

ДОКАЗАТЕЛЬСТВО. Во-первых, $(KZ+) \subset (K+)$, так как из условия

$$2^{\varphi(n)/KZ} = 1 + An, \quad A \text{ целое,}$$

по формуле бинома следует (с целым A') равенство

$$2^{\varphi(n)/K} = (1 + An)^Z = 1 + A'n.$$

В частности, классы *монотонны по отношению делимости*: $(X+) \subset (K+)$, $(X+) \subset (N+)$.

Во-вторых, *предположим, что $n \in (K+) \cap (N+)$, и докажем, что $n \in (X+)$.*

Обозначим через D наибольший общий делитель чисел K и N , так что

$$K = PD, \quad N = QD, \quad (P, Q) = 1, \quad X = PQD.$$

Число $\varphi(n)$ делится и на K , и на N , а потому и на их наименьшее общее кратное X , так что $\varphi(n) = PQDT$, где T целое.

По условию вхождения n в пересечение классов для некоторых целых A и B имеем

$$2^{\varphi(n)/K} = 2^{QT} = 1 + nA, \quad 2^{\varphi(n)/N} = 2^{PT} = 1 + nB.$$

Обозначим через (U, V) решение в натуральных числах уравнения $PU - QV = 1$ (например, доставляемое цепной дробью числа P/Q).

Тогда $PUT = T + QVT$. Из уже известных нам соотношений (с целыми B' и A')

$$2^{PUT} = (1 + nB)^U = 1 + nB', \quad 2^{QVT} = (1 + nA)^V = 1 + nA'$$

мы находим тождество $1 + nB' = 2^T(1 + nA')$, откуда

$$2^{\varphi(n)/X} = 2^T = 1 + n(B' - 2^T A'),$$

так что n принадлежит классу $(X+)$. Теорема 3 доказана.

ТЕОРЕМА 4. *Класс $(M-)$, где M — нечетное натуральное число, пуст (например, пусты классы $(3-)$ и $(5-)$).*

ДОКАЗАТЕЛЬСТВО. Если (для целого числа A)

$$2^{\varphi(n)/M} = -1 + nA,$$

то, ввиду нечетности числа M , по формуле бинома для некоторого целого числа A' имеет место соотношение (с целым A')

$$2^{\varphi(n)} = (-1 + nA)^M = -1 + nA',$$

вопреки теореме Эйлера (следствию теоремы 1 выше). Теорема 4 доказана.

Напротив, класс $(2-)$ довольно велик, например, в него входят числа **3, 5, 9, 11, 13, 19, 25, 27, ...** (подробное описание дано в следующем параграфе).

ТЕОРЕМА 5. *Классы $(2-)$ и $(N+)$, где число N нечетно, пересекаются в точности по классу $(2N-)$, а если $N > 2$ четно — то не пересекаются.*

ДОКАЗАТЕЛЬСТВО. Если $n \in (2N-)$, то (для некоторого целого A) $2^{\varphi(n)/2N} = -1 + nA$, поэтому $2^{\varphi(n)/2} = (-1 + nA)^N = (-1)^N + nA'$, так что $(2N-) \subset (2-)$, если число N нечетно, $(2N-) \subset (2+)$, если N четно; кроме того, $2^{\varphi(n)/N} = (-1 + nA)^2 = 1 + nA''$ (где A' и A'' целые), так что $(2N-) \subset (N+)$ в обоих случаях.

Обратно, если N нечетно и $n \in (2-) \cap (N+)$, то для некоторых целых чисел A и B верны равенства

$$2^{\varphi(n)/2} = -1 + nA, \quad 2^{\varphi(n)/N} = 1 + nB.$$

Число $\varphi(n)$ делится на произведение $2N$, так что $\varphi(n) = 2Nt$, и мы получаем из этих равенств

$$2^{Nt} = -1 + nA, \quad 2^{2t} = 1 + nB.$$

Если $N = 2U + 1$, то мы выводим, что

$$(2^{2t})^U 2^t = -1 + nA, \quad (1 + nB)^U 2^t = -1 + nA, \\ (1 + nB')2^t = -1 + nA, \quad 2^t = -1 + n(A - 2^t B'),$$

т. е. $2^{\varphi(n)/2N} = -1 + nB''$ с целым коэффициентом B'' . Мы доказали, что n входит в класс $(2N-)$.

Наконец, если число N четно, то класс $(N+)$ лежит в $(2+)$ по теореме 3, а потому не пересекается с классом $(2-)$, чем и заканчивается доказательство теоремы 5.

§4. Статистики периодов n чисел орбит

Для экспериментального изучения *среднего* роста чисел $N(n)$ и $T(n)$ обозначим через $[N] \approx 12N$ сумму двенадцати чисел орбит $N(n)$, соответствующих двенадцати последовательным нечетным значениям n (из интервала от $24c$ до $24(c+1)$).

Обозначим через $[T] \approx 12T$ такую же сумму длин 12 периодов $T(n)$.

Мы обсудим ниже поведение наблюдаемых при $0 \leq c \leq 20$ значений $[N]$ и $[T]$ в зависимости от c , имея в виду исследование среднего асимптотического распределения *форм N прямоугольников Юнга* с основанием $T(n)$ и высотой $N(n)$ при росте n . Из таблицы получаются следующие *наблюдаемые значения*:

$$[N] = 16, 25, 28, 48, 37, 47, 43, 26, 38, 58, 70, 62, 32, 57, 79, 49, 52, 44, 95, 50, 52;$$

$$[T] = 84, 210, 378, 339, 527, 682, 679, 1071, 1037, 804, 823, 891, 1375, 1165, 1411, \\ 2026, 1474, 1927, 1333, 2088, 1849.$$

ПРИМЕР. Наибольшему из рассмотренных в этих вычислениях значению $n = 511$ соответствует $[T] = 1849$, т. е. эмпирическое «среднее значение» $[T]/12 \approx 150$ гораздо больше истинного периода, $T(511) = 9$. Грубо говоря, «в среднем» наблюдаемые значения T порядка $n/3$. Поскольку $\varphi \approx 6n/\pi^2$, из слабой асимптотики «в среднем $T \approx n/3$ » следует слабая асимптотика «в среднем $N \approx 18/\pi^2 \approx 2$ », так что прямоугольник Юнга «в среднем» (в смысле слабой асимптотики [2])

длинный, с малым числом строк и с отношением $N/T \approx 6/n$, «в среднем» слабо асимптотически малым при больших значениях n .

В таблице встречаются изредка и специальные числа n с высокими прямоугольниками Юнга, например, $n = 2^T - 1$ (как для 511). В этом случае $N \approx (6/\pi^2)n/T \approx (6/\pi^2)n/\log n$, откуда $N/T \approx (6/\pi^2)n/\log^2 n \rightarrow \infty$ с n .

Но значения $N = 1$ и 2 (мало орбит) встречаются чаще и понижают «среднее» число орбит до слабой асимптотики $N \approx 2 \ll n/\log^2 n$.

Кроме этих двух крайних случаев очень длинных и очень высоких прямоугольников, в таблице §9 много и таких значений n , для которых стороны прямоугольника Юнга по длинам «соизмеримы», т.е. $N \approx T$ (как для квадрата). В этом предположении $N^2 \approx 6n/\pi^2$, т.е. *оба числа N и T слабо асимптотически растут с ростом n как квадратный корень из n* .

Это явление наводит на мысль о *хаотичности* последовательности вычетов чисел геометрической прогрессии $\{2^i\}$ среди всех взаимно простых с числом n вычетов.

Действительно, рассмотрим *случайную последовательность из T независимых выборов одного из m элементов заданного множества*. Ясно, что при достаточно малых T (по сравнению с большим числом m) все T выбранных элементов с подавляющей вероятностью различны, а при достаточно больших T совпадения с подавляющей вероятностью имеют место (и при $T > m$ неизбежны).

Простой подсчет показывает, что критическое значение T , разделяющее эти два случая, растет с числом элементов m как $c\sqrt{m}$ (причем постоянную c можно явно указать, так же как и асимптотическое erf -поведение вероятности совпадений, меняющейся от 0 до 1 в окрестности критического значения T).

Не останавливаясь на деталях этого подсчета («задачи о совпадении дней рождения T товарищей»), заметим, что число последовательных выборов T из m элементов без повторений есть $m(m-1)(m-2)\dots(m-T+1)$, а полное число всех исходов последовательностей T выборов есть m^T , так что изучаемая вероятность отсутствия повторений есть их отношение, равное

$$p(T) = \prod_{i=0}^{T-1} \left(1 - \frac{i}{m}\right).$$

Переходя к логарифмам (и считая дробь T/m , а значит, и дробь i/m , малыми), мы получаем (не останавливаясь на обоснованиях) приближенную формулу

$$\ln p \approx - \sum_{i=0}^{T-1} \frac{i}{m} = - \frac{T(T-1)}{2m}.$$

Это показывает, что вероятность отсутствия повторений, p , велика (близка к 1), пока $T^2 < am$, и мала, как только $T^2 > bm$ (с легко вычислимой по a и b асимптотикой «малости» и «близости»).

В случае орбиты системы Ферма–Эйлера число значений есть $m = \varphi(n) \approx (6/\pi^2)n$, а число совпадений значений точно равно нулю в пределах периода длины T (иначе период был бы меньше). Поэтому, *если бы динамика динамической системы, $x \mapsto 2^t x$, была вполне хаотической* (на что, по-видимому,

указывает большой показатель Ляпунова, $2 > 1$), то следовало бы ожидать периода $T(n)$ порядка $\sqrt{n}$.

Стало быть, наблюдаемые средние $[T/12]$ порядка $n/3$ указывают на нарушение хаотичности, проявляющееся в своеобразном расталкивании значений вычетов $2^t \pmod{n}$ в разные моменты времени t .

Это явление расталкивания вычетов членов геометрической прогрессии заслуживает специального изучения в эргодической теории чисел.

§5. Описание классов $(2+)$, $(2-)$

Это описание (открытое, видимо, Эйлером) состоит в следующем.

ТЕОРЕМА 6. *Всякое нечетное число, делящееся на несколько разных простых, лежит в классе $(2+)$. Степень простого числа лежит в классе $(2+)$, если оно дает остаток 1 или -1 при делении на 8, и в классе $(2-)$, если оно дает остаток 3 или -3 при делении на 8.*

ПРИМЕРЫ. Числа 3, 5, 9, 27 принадлежат классу $(2-)$, а числа 7, 15, 17, 21, 23 — классу $(2+)$. Например, $\varphi(17) = 16$ и $2^8 - 1 = (2^4 - 1)(2^4 + 1)$ делится на 17, поэтому 17 лежит в классе $(2+)$. В то же время $\varphi(27) = 18$ и $2^9 + 1 = 513 = 27 \cdot 19$, поэтому 27 лежит в классе $(2-)$.

ЗАМЕЧАНИЕ. Из теоремы 6 следует, что *каждое нечетное число лежит либо в $(2+)$, либо в $(2-)$* (что для простых нечетных чисел p следует уже из теоремы Ферма, согласно сравнению $2^{\varphi(n)} - 1 = (2^{\varphi/2} - 1)(2^{\varphi/2} + 1) \equiv 0 \pmod{n}$).

ДОКАЗАТЕЛЬСТВО. 1°. Пусть $n = p$ простое. Разделим вычеты $\pmod{p}$, не равные нулю, на две группы по $(p-1)/2$ элементов: $(0 < x < p/2)$ и $(-p/2 < x < 0)$. Умножение вычетов на -1 переводит эти группы друг в друга. Умножение вычетов на 2 переводит из первой группы вычетов во вторую в точности те вычеты x , для которых $p/4 < x < p/2$. Если $p = 8c + r$, то, в зависимости от остатка $r = 1, 3, 5, 7$, эти интервалы имеют вид $[2c + 1, 4c]$, $[2c + 1, 4c + 1]$, $[2c + 2, 4c + 2]$, $[2c + 2, 4c + 3]$ соответственно. Поэтому число H таких вычетов x , переходящих из первой группы во вторую при своем удвоении, равно соответственно $2c$, $2c + 1$, $2c + 1$, $2c + 2$. Оно четно при $p \equiv \pm 1 \pmod{8}$ и нечетно при $p \equiv \pm 3 \pmod{8}$.

Каждый вычет $\pmod{p}$, рассматриваемый с точностью до знака, встречается среди $\varphi/2$ вычетов $2x$, где $0 < x < p/2$, ровно один раз. Действительно, если бы $2x$ был бы сравним с $2y$ или с $-2y \pmod{p}$, то либо $2(x - y) = Ap$, либо $2(x + y) = Ap$, т. е. $x - y$ или $x + y$ было бы кратно p , вопреки определяющим группой условиям $0 < x < p/2$, $0 < y < p/2$, $x \neq y$. Итак, произведение удвоенных вычетов отличается от произведения Π исходных вычетов первой группы лишь знаком $(-1)^H$, так что, по модулю p , имеет место равенство

$$\Pi \cdot 2^{\varphi(p)/2} \equiv (-1)^H \cdot \Pi,$$

что и доказывает (ввиду описанной зависимости от остатка r четности числа H) утверждение теоремы о классах простых чисел.

2°. Пусть $n_a = p^a$, $a > 1$. Тогда $\varphi(n_a) = (p - 1)p^{a-1} = p\varphi(n_{a-1})$, поэтому

$$2^{\varphi(n_a)/2} = (2^{\varphi(n_{a-1})})^p.$$

Если известно представление (с целым коэффициентом A)

$$2^{\varphi(n_{a-1})/2} = \pm 1 + An_{a-1},$$

то (с целым коэффициентом B) имеет место представление

$$2^{\varphi(n_a)/2} = (\pm 1 + An_{a-1})^p = \pm 1 + Bp^a$$

(по биному, так как $pn_{a-1} = p^a$ и n_{a-1}^2 делится на p^a , поскольку $2a - 2 \geq a$ при $a > 1$). Знак $\pm$ остался прежним, так как показатель степени p нечетен.

Мы убедились, что все числа n_a — в том же классе $(2\pm)$, что p .

Теорема 6 доказана (в 1° и 2°) для всех степеней простых чисел.

3°. Пусть теперь $n = p^a Q$, где $Q \neq 1$ взаимно просто с простым нечетным числом p , так что $\varphi(n) = \varphi(p^a)\varphi(Q)$. Проведем индукцию по числу разных простых сомножителей числа n . Если для Q утверждение теоремы уже доказано, так что известно представление

$$2^{\varphi(Q)/2} = \pm 1 + AQ, \quad \text{где } A \text{ целое,}$$

то мы получаем (ввиду четности числа $\varphi(p^a)$) представление улучшенной формы по модулю старого числа Q ,

$$2^{\varphi(n)/2} = (\pm 1 + AQ)^{\varphi(p^a)} = 1 + BQ, \quad \text{где } B \text{ целое.}$$

Точно так же из уже доказанного соотношения

$$2^{\varphi(p^a)/2} = \pm 1 + Cp^a, \quad \text{где } C \text{ целое,}$$

вытекает (ввиду четности числа $\varphi(Q)$) представление по модулю p^a ,

$$2^{\varphi(n)/2} = (\pm 1 + Cp^a)^{\varphi(Q)} = 1 + Up^a, \quad \text{где } U \text{ целое.}$$

Наконец, из доказанного совпадения обоих представлений

$$2^{\varphi(n)/2} = 1 + BQ = 1 + Up^a$$

следует делимость коэффициента B на взаимно простое с Q число p^a , так что $p^a Q \in (2+)$, если $Q \in (2+) \cup (2-)$.

Добавляя степени простых множителей по одному, мы убеждаемся, что *любое их произведение лежит в классе $(2+)$* , и теорема 6 доказана полностью.

§6. Описание классов $(4+)$ и $(4-)$

Разобьем это описание на восемь теорем 7–14.

ТЕОРЕМА 7. *Всякое нечетное число, имеющее более двух разных простых делителей, принадлежит классу $(4+)$.*

ТЕОРЕМА 8. *Для числа $n = p^a q^b$ (где p и q разные нечетные простые) вычет числа $2^{\varphi(n)/4}$ по модулю n дается следующей таблицей:*

$q \pmod 8 \backslash p \pmod 8$	+3	-3	-1	+1
+3	—	0	0	+
-3	0	+	0	+
-1	0	0	+	+
+1	+	+	+	+

Здесь ответ «+» означает « $\equiv +1 \pmod{n}$ », т. е. « $n \in (4+)$ ». Ответ «-» означает « $\equiv -1 \pmod{n}$ », т. е. « $n \in (4-)$ ». Ответ «0» означает « $\not\equiv \pm 1 \pmod{n}$ », т. е. « $n \notin (4+) \cup (4-)$ ».

ТЕОРЕМА 9. Если $n = PQ$ с взаимно простыми сомножителями P и Q класса $(2-)$, для которых четности чисел $\varphi(P)/2$ и $\varphi(Q)/2$ разные, то n не лежит ни в классе $(4+)$, ни в классе $(4-)$. Присутствие сомножителя с четным $\varphi(P)/2$ исключает класс $(4-)$ и без предположения о вхождении в $(2-)$.

ТЕОРЕМА 10. Если $n = p^f Q$, где простое число p сравнимо с 1 или с -1 по модулю 8, а $Q \neq 1$ не делится на p , то

$$2^{\varphi(n)/4} \equiv +1 \pmod{t^f}, \quad n \notin (4-).$$

ТЕОРЕМА 11. Если у n есть неединственный простой делитель, сравнимый с 1 по модулю 8, то $n \in (4+)$.

ТЕОРЕМА 12. Если $n = p^a$ принадлежит объединению классов $(4+) \cup (4-)$, то $p \equiv 1 \pmod{8}$.

ТЕОРЕМА 13. Если $n \equiv 5 \pmod{8}$, то n не принадлежит классу $(4-)$.

ТЕОРЕМА 14. Если $n \equiv 7 \pmod{8}$, то n не принадлежит классу $(4-)$.

ПРИМЕРЫ. В классе $(4-)$ лежат простые числа

$$n = 17, 41, 97, 113, 137, 193, 241, 313, 401, 409, 433, 457, 499.$$

В классе $(4+)$ лежат простые числа

$$n = 73 \in (8+), 89 \in (8+), 233 \in (8+), 257 \in (32-, 16+, 8+), 353 \in (8-).$$

Как заранее узнать, лежит ли простое число $n = 8s + 1$ в классе $(4-)$ или $(4+)$, я не знаю, приведенные ответы — результат эксперимента.

Не простые числа $(4-)$ бывают сравнимыми с $3 \pmod{8}$, хотя и не часто: в моей таблице $n = 99, 363, 387$ (много ли их вообще — не знаю).

Простые $(4+)$ и $(4-)$ с остатком 1 $\pmod{8}$ многочисленны, но асимптотика мне неизвестна (думаю, что чисел $(4-)$ больше). Простые с остатком 1 $\pmod{8}$ принадлежат либо $(4+)$, либо $(4-)$.

Из меньших 100 чисел класса $(2+)$ не попадают ни в $(4+)$, ни $(4-)$ в точности следующие 3 серии:

I. $p^a q^b$, $p \equiv 3 \pmod{8}$, $q \equiv 7 \pmod{8}$: $n = 21, 35, 63, 69, 77, 91, 93$;

II. $p^a q^b$, $p \equiv 3 \pmod{8}$, $q \equiv 5 \pmod{8}$: $n = 15, 39, 45, 55, 75, 87$;

III. $\varphi(n) \not\equiv 0 \pmod{4}$: $n = 7, 23, 31, 47, 49, 71, 79$.

§7. Доказательства теорем о классах $(4\pm)$

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 7. Запишем число n в виде $n = p^a q^b R$ (с взаимно простым с простыми числами p и q множителем R). По теореме 6 числа $p^a R$ и $q^b R$ принадлежат классу $(2+)$, т. е. существуют представления (с целыми A и B)

$$2^{\varphi(q^b R)/2} = 1 + Aq^b R, \quad 2^{\varphi(p^a R)/2} = 1 + Bp^a R.$$

Согласно мультипликативному свойству функции Эйлера,

$$\varphi(n) = \varphi(p^a) \varphi(q^b R) = \varphi(q^b) \varphi(p^a R).$$

Поэтому

$$2^{\varphi(n)/4} = (2^u)^v = (2^w)^z,$$

где

$$u = \varphi(q^b R)/2, \quad v = \varphi(p^a)/2, \quad w = \varphi(p^a R)/2, \quad z = \varphi(q^b)/2$$

(все эти 4 числа целые вследствие нечетности простых чисел p и q). Итак, мы получаем представления (с целыми A' и B')

$$2^{\varphi(n)/4} = (1 + Aq^b R)^v = 1 + A'q^b R, \quad 2^{\varphi(n)/4} = (1 + Bp^a R)^z = 1 + B'p^a R.$$

Из равенства представляемых чисел и взаимной простоты p с $q^b R$ следует делимость коэффициента A' на p^a , так что (с целым коэффициентом C)

$$A' = p^a C, \quad 2^{\varphi(n)/4} = 1 + A'q^b R = 1 + nC,$$

что и доказывает вхождение n в класс $(4+)$. Теорема 7 доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 8. Введем обозначения

$$u = \varphi(p^a)/2, \quad v = \varphi(q^b)/2.$$

Согласно теореме 6, известны представления (с целыми коэффициентами A и B)

$$2^u = \alpha(p) + Ap^a, \quad 2^v = \alpha(q) + Bq^b,$$

где $\alpha = \pm 1$ и четность числа u , заданная как $\xi(p) = (-1)^u$, даются, в зависимости от остатка r от деления простого числа p на 8, таблицей

r	1	3	5	7
$\alpha(p)$	+1	-1	-1	+1
$\xi(p)$	+1	-1	+1	-1

Эта таблица позволяет исследовать два представления интересующего нас числа $2^{\varphi(n)/4}$:

$$2^{\varphi(n)/4} = (2^u)^v = (2^v)^u$$

(поскольку $\varphi(n)/4 = uv$ ввиду мультипликативного свойства функции Эйлера). Из предположенных выше сравнений мы получаем (с целыми коэффициентами A' и B') представления

$$2^{\varphi(n)/4} = (\alpha(p) + Ap^a)^v = (\alpha(p))^{u(q)} + A'p^a,$$

$$2^{\varphi(n)/4} = (\alpha(q) + Bq^b)^u = (\alpha(q))^{u(p)} + B'q^b.$$

Приведенная выше таблица значений α и ξ доставляет матрицу значений $(\alpha(p))^{u(q)}$ в зависимости от остатков от деления p и q на 8:

$r(q) \backslash r(p)$	1	3	5	7
1	+1	+1	+1	+1
3	+1	-1	-1	+1
5	+1	+1	+1	+1
7	+1	-1	-1	+1

Теперь разберем три представляющихся случая:

$$\alpha(p)^{u(q)} = \alpha(q)^{u(p)} = +1,$$

$$\alpha(p)^{u(q)} = \alpha(q)^{u(p)} = -1,$$

$$\alpha(p)^{u(q)} \neq \alpha(q)^{u(p)}.$$

В первом случае мы докажем, что $n \in (4+)$, во втором $n \in (4-)$, а в третьем n заведомо не лежит ни в $(4+)$, ни в $(4-)$.

Действительно, в первых двух случаях

$$2^{\varphi(n)/4} = \varepsilon + A'p^a = \varepsilon + B'q^b,$$

поэтому A' делится на q^b и, значит, $A' = Cq^b$, $2^{\varphi(n)/4} = \varepsilon + Cp^aq^b$, т. е. $n \in (4+)$ при $\varepsilon = 1$ (в первом случае), $n \in (4-)$ при $\varepsilon = -1$ (во втором).

В третьем случае мы получаем противоречие с принадлежностью n к классу (4ε) , т. е. к представлению (с целым C) вида

$$2^{\varphi(n)/4} = \varepsilon + Cp^aq^b,$$

выбрав из двух различных по знаку первого члена представлений, выписанных выше, то, для которого этот знак противоположен знаку ε , для определенности —

$$2^{\varphi(n)/4} = -\varepsilon + A'p^a.$$

Из двух выписанных только что представлений следует, что

$$2\varepsilon = (A' - Cq^b)p^a,$$

т. е. что нечетное простое число p является делителем двойки, невозможность чего оканчивает доказательство теоремы 8.

ЗАМЕЧАНИЕ. Последняя часть рассуждения, доказывающая, что n не лежит ни в классе $(4+)$, ни в классе $(4-)$, применима и к более общему случаю чисел $n = PQ$, где $(P, Q) = 1$ и

$$2^{\varphi(P)/2} = \alpha(P) + AP, \quad 2^{\varphi(Q)/2} = \alpha(Q) + BQ, \quad \alpha = \pm 1,$$

когда нарушается условие симметрии, т. е. когда $\alpha(P)^{\varphi(Q)/2} \neq \alpha(Q)^{\varphi(P)/2}$.

Это доказывает теорему 9, где $\alpha = -1$, а числа $\varphi(P)/2$ и $\varphi(Q)/2$ разной четности. Точно так же вхождение n в класс $(4-)$ противоречило бы четности числа $\varphi(P)/2$, делающей число $\alpha(Q)^{\varphi(P)/2}$ равным $+1$.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 10. По условию взаимной простоты p и Q

$$\varphi(n)/4 = (\varphi(p^f)/2)(\varphi(Q)/2).$$

По теореме 6, ввиду того что $p \equiv \pm 1(8)$,

$$2^{\varphi(p^f)/2} = 1 + p^f A, \quad \text{где } A \text{ целое.}$$

По формуле бинома

$$2^{\varphi(n)/4} = (1 + p^f A)^{\varphi(Q)/2} = 1 + p^f A'$$

с целым коэффициентом A' , что и утверждалось в теореме 10.

Полученное сравнение исключает вхождение n в класс $(4-)$, которое заставляло бы нечетное простое число p быть делителем двойки.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 11. Если разных простых делителей больше двух, то это теорема 7, а если два — то теорема 8. С одним делителем утверждение неверно, так как число $n = 17$ лежит в $(4-)$, а не в $(4+)$.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 12. Оба класса $(4+)$ и $(4-)$ составляют часть класса $(2+)$, поэтому по теореме 6 остаток от деления p на 8 равен либо $+1$, либо -1 . Если $p = 8c - 1$, то $\varphi(p^a) = (p-1)p^{a-1}$ не делится на 4, так что число $n = p^a$ не может принадлежать ни классу $(4+)$, ни классу $(4-)$.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 13. Запишем разложение числа n на множители p_i, q_j, r_k, s_l с остатками 3, 5, 7 и 1 при делении на 8 соответственно,

$$n = \prod p_i^{a_i} q_j^{b_j} r_k^{c_k} s_l^{d_l}.$$

Остаток от деления n на 8 можно выразить через их кратности,

$$n \equiv 3^{A+B}(-1)^{B+C} \pmod{8},$$

где $A = \sum a_i$ и т. д. (поскольку $5 \equiv -3$ и $7 \equiv -1 \pmod{8}$).

По условию $n \equiv 5 \pmod{8}$ числа $A+B$ и $B+C$ нечетны. Значит, хотя бы одно из простых чисел p_i и q_j имеет нечетную кратность. Если B нечетно и это число q , а эта кратность $b_j = 2b+1$, то

$$n = PQ, \quad Q = q^{2b+1}, \quad (P, Q) = 1, \quad P \equiv 1 \pmod{8}, \quad Q \equiv 5 \pmod{8}.$$

Если B четно, то A и C нечетны, значит, нечетны кратность $a_i = 2a+1$ одного из простых чисел $p_i = p$ и кратность $c_k = 2c+1$ одного из простых чисел $r_k = r$.

В этом случае мы положим $Q = p^{2a+1}r^{2c+1}$ и опять получим разложение $n = PQ$, где P и Q взаимно просты и дают при делении на 8 остатки 1 и 5.

Из $(P, Q) = 1$ следует, что $\varphi(n) = \varphi(P)\varphi(Q)$, поэтому

$$2^{\varphi(n)/4} = (2^{\varphi(P)})^m, \quad \text{где } m = \varphi(Q)/4.$$

Число m целое, так как, соответственно двум указанным выше возможностям,

$$\varphi(Q) = (q-1)q^{2b} \quad \text{или} \quad (p-1)p^{2a}(r-1)r^{2c},$$

$q \equiv 5 \pmod{8}$, $p \equiv 3 \pmod{8}$, $r \equiv 7 \pmod{8}$, так что и $q-1$, и произведение $(p-1)(r-1)$ делятся на 4.

По сравнению Ферма–Эйлера (теорема 1 выше) имеем представление (с целым A)

$$2^{\varphi(P)} = 1 + AP.$$

Следовательно, мы получаем сравнение

$$2^{\varphi(n)/4} = (1 + AP)^m \equiv 1 \pmod{P},$$

которое противоречит принадлежности n классу $(4-)$, из которой вытекает сравнение с -1 , а не с 1 , и по модулю P . Мы заключаем, что для принадлежности числа n к классу $(4-)$ необходимо сравнение $1 \equiv -1$ по модулю P , т. е. необходимо, чтобы $P = 1$.

Итак, все числа $n \equiv 5 \pmod{8}$ класса $(4-)$, если они есть, имеют один из двух видов:

$$(I) \quad n = q^{2b+1}, \quad q \equiv 5 \pmod{8},$$

$$(II) \quad n = p^{2a+1}r^{2c+1}, \quad p \equiv 3 \pmod{8}, \quad r \equiv 7 \pmod{8}.$$

Из теоремы 10 следует, что числа типа II не принадлежат классу $(4-)$.

Числа вида I тоже ему не принадлежат, так как они принадлежат классу (2−) (по теореме 6), а весь класс (4−) лежит внутри класса (2+) (см. §1).

Тем самым теорема 13 доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 14. Запишем число n в виде произведения взаимно простых множителей P и Q , где P содержит все простые множители, дающие при делении на 8 остатки +3 и −3, а Q — остатки +1 и −1.

Поскольку функция Эйлера мультипликативна, $\varphi(n) = \varphi(P)\varphi(Q)$, поэтому

$$2^{\varphi(n)/4} = (2^{\varphi(Q)/2})^m, \quad \text{где } m = \varphi(P)/2.$$

По теореме 6 имеем представление (с целым A)

$$2^{\varphi(Q)/2} = 1 + AQ.$$

Действительно, Q лежит в (2+), если разных простых множителей в Q больше одного. Если же он один, то Q тоже принадлежит классу (2+), поскольку он сравним с ± 1 по модулю 8.

Теперь мы получаем представление (с целым A')

$$2^{\varphi(n)/4} = (1 + AQ)^m = 1 + A'Q.$$

Если $Q \neq 1$, то это представление противоречит принадлежности числа n классу (4−), доставляющей остаток −1, а не 1, при делении на $n = PQ$.

Если же $Q = 1$, то мы получаем представление

$$n = \prod p_i^{a_i} q_j^{b_j}, \quad p_i \equiv 3 \pmod{8}, \quad q_j \equiv -3 \pmod{8}.$$

Представим это число n в виде произведения взаимно простых множителей, $n = PQ$, которое приведет нас к противоречию с принадлежностью числа n к классу (4−). Мы находим

$$2^{\varphi(n)/4} = (2^{\varphi(P)/2})^m, \quad \text{где } m = \varphi(Q)/2.$$

Противоречие получится, если

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

По теореме 6 это сравнение всегда имеет место, если m четно, а если m нечетно, то если число P имеет больше одного простого делителя. Поэтому принадлежность n классу (4−) невозможна, если число разных простых множителей числа n больше двух (в этом случае мы выбрали бы в качестве P произведение максимальных степеней двух простых множителей и пришли бы к противоречию с принадлежностью n к классу (4−)).

Если разных простых множителей два, то для выполнения условия $n \equiv -1 \pmod{8}$ их кратности должны удовлетворять условиям

$$\sum b_j \text{ — нечетное число, } \sum a_i + \sum b_j \text{ — четное число.}$$

Поэтому число $\sum a_i$ нечетно. Значит, отличны от нуля ровно одно из чисел a_i и ровно одно из чисел b_j , так что $n = p^{2a+1}q^{2b+1}$.

Теперь мы получаем представление

$$2^{\varphi(n)/4} = (2^{\varphi(p^{2a+1})/2})^m, \quad \text{где } m = \varphi(q^{2b+1})/2.$$

В этом случае $\varphi(q^{2b+1}) = (q-1)q^{2b}$, где $q = 8u - 3$. Поэтому $q - 1 = 8u - 4$, так что $m = (4u - 2)q^{2b}$ — четное число. Стало быть, число $2^{\varphi(n)/4}$ сравнимо с $+1$ по модулю p^{2a+1} , что несовместно с принадлежностью числа n к классу $(4-)$.

Остается только случай, когда n есть степень одного простого числа: $n = p^a$ либо q^b .

В первом случае $n = 8u + 1$ при четном a и $8u + 3$ при нечетном. Во втором случае $n = 8u + 1$ при четном b и $8u - 3$ при нечетном. Поэтому сравнение $n \equiv 7 \pmod{8}$ не выполнено ни в одном из случаев. Теорема 14 доказана.

§8. Описание класса $(3+)$

Анализ таблиц §9 приводит к следующему выводу. Как мы уже знаем из §3 и §5, числа класса $(3+)$ разбиваются на два подкласса, $(6+) = (3+) \cap (2+)$ и $(6-) = (3+) \cap (2-)$.

ТЕОРЕМА 15. Числа класса $(6-)$ являются степенями простых чисел, дающих при делении на 8 остатки ± 3 .

Числа класса $(6+)$, являющиеся простыми, дают при делении на 8 остатки ± 1 (как 433, 457, 31, 127, 223, 439).

Простые числа классов $(6+)$ и $(6-)$ дают при делении на 6 остаток 1.

ЗАМЕЧАНИЕ. Некоторые простые числа не принадлежат ни классу $(6+)$, ни $(6-)$, например, $n = 11$ и 13 .

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 15. Число, имеющее несколько простых делителей, принадлежит классу $(2+)$ по теореме 6, а потому все числа класса $(6-)$, входящего в класс $(2-)$ (согласно §1) являются степенями простых чисел. Эти простые должны давать при делении на 8 остатки ± 3 , иначе степень принадлежала бы классу $(2+)$, а не $(2-)$ по теореме 6 и не входила бы в подкласс $(6-)$ класса $(2-)$.

Точно так же простые числа класса $(6+)$, чтобы входить в $(2+)$, должны по теореме 6 давать при делении на 8 остатки 1 или -1 , чем и доказана теорема 15 (остаток 1 при делении на 6 простого числа p класса $(6+)$ или $(6-)$ следует из нужной для этого делимости $\varphi(p)$ на 6).

ПРИМЕР. Все степени числа 43 принадлежат классу $(6-)$ (четные степени дают при делении на 8 остаток 1, а нечетные — остаток 3).

Действительно, $\varphi(43)/6 = 42/6 = 7$, поэтому

$$2^{\varphi(43)/6} = 128 = 43 \cdot 3 - 1 = -1 + 43 \cdot A.$$

Это позволяет по индукции убедиться в представлении

$$2^{\varphi(43^a)/6} = (-1 + 43^{a-1} A_{a-1})^{43} = -1 + 43^a A_a$$

с целым коэффициентом A_a . Доказанное сравнение означает принадлежность числа 43^a классу $(6-)$.

§9. Классификация нечетных чисел, меньших 512

В приведенной ниже таблице для каждого нечетного числа $n > 1$ указаны его классы $(N+)$ и $(M-)$ с наибольшими N и M , а также значения его наименьшего периода $T(n)$ и значение функции Эйлера $\varphi(n) = N(n)T(n)$. Расположена эта информация так:

$$n \quad (M-, N+) \quad (T(n), \varphi(n)).$$

Простые числа n набраны полужирным шрифтом: $\mathbf{n}$. Знак $(M-)$ указан, лишь когда число n принадлежит какому-либо классу $(K-)$, и в этом случае указывается в качестве M наибольшее из таких чисел K ; точно так же знак $(N+)$ указывается, лишь когда число n принадлежит какому-либо классу $(L+)$ с $L > 1$, и в этом случае указывается в качестве N наибольшее из таких чисел L .

В частности, знак $(2-)$ не сопровождается вытекающим из него знаком $(1+)$, который здесь подразумевается, но не пишется. В этом случае $T(n) = \varphi(n)$, $N(n) = 1$.

Поскольку класс $(N+)$ содержится во всех классах $(N'+)$, где N' — делитель числа N , то обозначение вроде $(10+)$ около числа n означает вхождение числа n в классы $(10+)$, $(5+)$ и $(2+)$ (и, конечно, в класс $(1+)$, содержащий все числа n по теореме Эйлера).

Точно так же обозначение $(M-)$ около числа n обозначает вхождение этого числа n не только в сам класс $(M-)$, но также и в классы $(M'-)$, где $M = M'F$ с нечетным F , а также в классы $(N+)$, где $M = NF$ с четным F . Например, обозначение $(12-)$ влечет вхождение n также в классы $(4-)$, $(6+)$, $(3+)$, $(2+)$. Из этих классов указывается явно в таблице только $(N+)$ с наибольшим значением N (т. е. в нашем примере $(6+)$).

Таблица классов нечетных чисел и их периодов

9 (2-) (6) 17 (4-, 2+) (8, 16)	3 (2-) (2) 11 (2-) (10) 19 (2-) (18)	5 (2-) (4) 13 (2-) (12) 21 (2+) (6, 12)	7 (2+) (3, 6) 15 (2+) (4, 8) 23 (2+) (11, 22)
25 (2-) (20) 33 (4-, 2+) (10, 20) 41 (4-, 2+) (20, 40)	27 (2-) (18) 35 (2+) (12, 24) 43 (6-) (14, 42)	29 (2-) (28) 37 (2-) (36) 45 (2+) (12, 24)	31 (6+) (5, 30) 39 (2+) (12, 24) 47 (2+) (23, 46)
49 (2+) (21, 42) 57 (4-, 2+) (18, 36) 65 (8-, 4+) (12, 48)	51 (4+) (8, 32) 59 (2-) (58) 67 (2-) (66)	53 (2-) (52) 61 (2-) (60) 69 (2+) (22, 44)	55 (2+) (20, 40) 63 (6+) (6, 36) 71 (2+) (35, 70)
73 (8+) (9, 72) 81 (2-) (54) 89 (8+) (11, 88)	75 (2+) (20, 40) 83 (2-) (82) 91 (6+) (12, 72)	77 (2+) (30, 60) 85 (8+) (8, 64) 93 (6+) (10, 60)	79 (2+) (39, 78) 87 (2+) (28, 56) 95 (2+) (36, 72)
97 (4-, 2+) (48, 96) 105 (4+) (12, 48) 113 (8-, 4+) (28, 112)	99 (4-, 2+) (30, 60) 107 (2-) (106) 115 (2+) (44, 88)	101 (2-) (100) 109 (6-, 3+) (36, 108) 117 (6+) (12, 72)	103 (2+) (51, 102) 111 (2+) (36, 72) 119 (4+) (24, 96)
121 (2-) (110) 129 (12-, 6+) (14, 84) 137 (4-, 2+) (68, 136)	123 (4+) (20, 80) 131 (2-) (130) 139 (2-) (138)	125 (2-) (100) 133 (6+) (18, 108) 141 (2+) (46, 92)	127 (18+) (7, 126) 135 (2+) (36, 72) 143 (2+) (60, 120)
145 (8-, 4+) (28, 112) 153 (4+) (24, 96) 161 (4+) (33, 132)	147 (2+) (42, 84) 155 (6+) (20, 120) 163 (2-) (162)	149 (2-) (148) 157 (6-, 3+) (52, 156) 165 (4+) (20, 80)	151 (10+) (15, 150) 159 (2+) (52, 104) 167 (2+) (83, 166)
169 (2-) (156) 177 (4-, 2+) (58, 116) 185 (8-, 4+) (36, 144)	171 (12-, 6+) (18, 108) 179 (2-) (178) 187 (4+) (40, 160)	173 (2-) (172) 181 (2-) (180) 189 (6+) (18, 108)	175 (2+) (60, 120) 183 (2+) (60, 120) 191 (2+) (95, 190)
193 (4-, 2+) (96, 192) 201 (4-, 2+) (66, 132) 209 (4-, 2+) (90, 180)	195 (8+) (12, 96) 203 (2+) (84, 168) 211 (2-) (210)	197 (2-) (196) 205 (16-, 8+) (20, 160) 213 (2+) (70, 140)	199 (2+) (99, 198) 207 (2+) (66, 132) 215 (6+) (28, 168)
217 (12+) (15, 180) 225 (2+) (60, 120) 233 (8+) (29, 232)	219 (8+) (18, 144) 227 (2-) (226) 235 (2+) (92, 184)	221 (8+) (24, 192) 229 (6-, 3+) (76, 228) 237 (2+) (78, 156)	223 (6+) (37, 222) 231 (4+) (30, 120) 239 (2+) (119, 238)

241 (20–, 10+) (24, 240) 249 (4–, 2+) (82, 164) 257 (32–, 16+) (16, 256)	243 (2–) (162) 251 (10–, 5+) (50, 250) 259 (6+) (36, 216)	245 (2+) (84, 168) 253 (2+) (110, 220) 261 (2+) (84, 168)	247 (6+) (36, 216) 255 (16+) (8, 128) 263 (2+) (131, 262)
265 (8–, 4+) (52, 208) 273 (12+) (12, 144) 281 (8–, 4+) (70, 280)	267 (8+) (22, 176) 275 (10+) (20, 200) 283 (6–, 3+) (94, 282)	269 (2–) (268) 277 (6–, 3+) (92, 276) 285 (4+) (36, 144)	271 (2+) (135, 270) 279 (6+) (30, 180) 287 (4+) (60, 240)
289 (4–, 2+) (136, 272) 297 (4–, 2+) (90, 180) 305 (8–, 4+) (60, 240)	291 (4+) (48, 192) 299 (2+) (132, 264) 307 (6–, 3+) (102, 306)	293 (2–) (292) 301 (6+) (42, 252) 309 (2+) (102, 204)	295 (2+) (116, 232) 303 (2+) (100, 200) 311 (2+) (155, 310)
313 (4–, 2+) (156, 312) 321 (4–, 2+) (106, 212) 329 (4+) (69, 276)	315 (12+) (12, 144) 323 (4+) (72, 288) 331 (22–, 11+) (30, 330)	317 (2–) (316) 325 (8–, 4+) (60, 240) 333 (6+) (36, 216)	319 (2+) (140, 280) 327 (6+) (36, 216) 335 (2+) (132, 264)
337 (16+) (21, 336) 345 (4+) (44, 176) 353 (8–, 4+) (88, 352)	339 (8+) (28, 224) 347 (2–) (346) 355 (2+) (140, 280)	341 (30+) (10, 300) 349 (2–) (348) 357 (8+) (24, 192)	343 (2+) (147, 294) 351 (6+) (36, 216) 359 (2+) (179, 358)
361 (2–) (342) 369 (4+) (60, 240) 377 (8–, 4+) (84, 336)	363 (4–, 2+) (110, 220) 371 (2+) (156, 312) 379 (2–) (378)	365 (8+) (36, 288) 373 (2–) (372) 381 (18+) (14, 252)	367 (2+) (183, 366) 375 (2+) (100, 200) 383 (2+) (191, 382)
385 (4+) (60, 240) 393 (4–, 2+) (130, 260) 401 (4–, 2+) (200, 400)	387 (12–, 6+) (42, 252) 395 (2+) (156, 312) 403 (6+) (60, 360)	389 (2–) (388) 397 (18–, 9+) (44, 396) 405 (2+) (108, 216)	391 (4+) (88, 352) 399 (12+) (18, 216) 407 (2+) (180, 360)
409 (4–, 2+) (204, 408) 417 (4–, 2+) (138, 276) 425 (8+) (40, 320)	411 (4+) (68, 272) 419 (2–) (418) 427 (6+) (60, 360)	413 (2+) (174, 348) 421 (2–) (420) 429 (4+) (60, 240)	415 (2+) (164, 328) 423 (2+) (138, 276) 431 (10+) (43, 430)
433 (12–, 6+) (72, 432) 441 (6+) (42, 252) 449 (4–, 2+) (224, 448)	435 (8+) (28, 224) 443 (2–) (442) 451 (20+) (20, 400)	437 (2+) (198, 396) 445 (8+) (44, 352) 453 (10+) (30, 300)	439 (6+) (73, 438) 447 (2+) (148, 296) 455 (24+) (12, 288)
457 (12–, 6+) (76, 456) 465 (12+) (20, 240) 473 (12–, 6+) (70, 420)	459 (4+) (72, 288) 467 (2–) (466) 475 (2+) (180, 360)	461 (2–) (460) 469 (6+) (66, 396) 477 (2+) (156, 312)	463 (2+) (231, 462) 471 (6+) (52, 312) 479 (2+) (239, 478)
481 (24–, 12+) (36, 432) 489 (4–, 2+) (162, 324) 497 (4+) (105, 420)	483 (4+) (66, 264) 491 (2–) (490) 499 (6–, 3+) (166, 498)	485 (8+) (48, 384) 493 (8+) (56, 448) 501 (2+) (166, 332)	487 (2+) (243, 486) 495 (4+) (60, 240) 503 (2+) (251, 502)
505 (8–, 4+) (100, 400)	507 (2+) (156, 312)	509 (2–) (508)	511 (48+) (9, 432)

Все теоремы, доказанные выше, были обнаружены как экспериментальные факты при разглядывании этой таблицы. Еще больше экспериментальных фактов, бросающихся в глаза, остается недоказанными гипотезами, из которых выше сформулирована лишь малая часть (другие обсуждаются в статьях [5] и [6]).

Все эти гипотезы и теоремы были обнаружены при попытках [1] явного описания полугруппы значений совершенных бинарных квадратичных форм, вроде $x^2 + 2y^2$ (форма называется совершенной, если произведение любых двух ее значений в целых точках также достигается в целой точке).

Для совершенной формы $x^2 + y^2$ полугруппа значений (т. е. квадратов норм гауссовых комплексных чисел) была известна уже Ферма: кратности простых чисел вида $4s + 3$ (как 3, 7, 11, ...) в разложении значения формы на простые множители должны быть четными: $n = 3^{2a}5^{b7^{2c}} \dots$, так как

$$3 \neq x^2 + y^2, \quad 9 = 3^2 + 0^2, \quad 27 \neq x^2 + y^2 \quad \text{и т. д.}$$

Совершенными оказывается, по-видимому, около четверти всех форм, но описание соответствующих им полугрупп в терминах простых делителей, подобное приведенному выше описанию квадратов норм гауссовых комплексных чисел,

неизвестно и упирается в необходимость исследования описанных выше классов чисел n и периодов $T(n)$ определенных ими динамических систем Ферма–Эйлера, которыми я из-за этого и занялся. Для значений формы $x^2 + 2y^2$ четны кратности простых чисел, дающих при делении на 8 остатки 5 и 7.

ЛИТЕРАТУРА

1. *Arnold V. I.* Arithmetics of binary quadratic forms, symmetry of their continued fractions, and geometry of their de Sitter world. Moscow, Dubna, МСНМО, 2002, pp. 1–40. (Bol. Soc. Brasil. Mat., 2003.)
2. *Арнольд В. И.* Слабые асимптотики числа разложений диофантовых задач. Функци. анализ и его прил., **33**, вып. 4, 65–66 (1999).
3. *Арнольд И. В.* Теория чисел. Учпедгиз, 1933.
4. *Венков Б. А.* Элементарная теория чисел. ОНТИ НКТП, 1937.
5. *Арнольд В. И.* Группы Эйлера и арифметика геометрических прогрессий. МЦНМО, 2003.
6. *Arnold V.* Ergodic and arithmetic properties of geometrical progression's dynamics and of its orbits. Moscow Mathematical Journal, **3**, 1–20 (2003).

Математический институт им. В. А. Стеклова,
CEREMADE, Université Paris-Dauphine

Поступило в редакцию
23 октября 2002 г.