Малая теорема Ферма

В.СЕНДЕРОВ, А.СПИВАК

Мы расскажем о периодичности остатков (заново доказав малую теорему Ферма и теорему Эйлера в формулировках, которые позволят решить многие интересные задачи), о первообразных корнях, функции Кармайкла, числах Мерсенна и о многом другом.

Статья насыщена интересными задачами. Вряд ли возможно при первом чтении решить их все. Но мы уверены: многие из них настолько заинтригуют вас, что рано или поздно все они будут решены – самостоятельно или с помощью раздела «Ответы, указания, решения».

Напоминание

Как помнит читатель первой части статьи, числа a и b сравнимы по модулю n, если $a - b$ кратно n, т.е. $a - b = kn$, где k – целое число.

Продолжение. Начало см. в «Кванте» №1

Малая теорема Ферма гласит: $a^p \equiv a \pmod p$ для любого целого числа a и простого числа p. В частности, если a не кратно p, то $a^{p-1} \equiv 1 \pmod p$.

Функция Эйлера $\varphi(n)$ – это количество взаимно простых с числом n и не превосходящих n натуральных чисел. Например, $\varphi(p) = p - 1$ для любого простого p. В первой части для $n = p_1^{m_1} p_2^{m_2} \cdot \ldots \cdot p_s^{m_s}$, где $p_1, p_2, \ldots, p_s$ – различные простые числа, $m_1, m_2, \ldots, m_s$ – натуральные числа, доказана общая формула

$$\varphi(n) = \varphi\left(p_1^{m_1}\right)\varphi\left(p_2^{m_2}\right)\cdot\ldots\cdot\varphi\left(p_s^{m_s}\right) =$$

$$= \left(p_1^{m_1} - p_1^{m_1-1}\right)\left(p_2^{m_2} - p_2^{m_2-1}\right)\cdot\ldots\cdot\left(p_s^{m_s} - p_s^{m_s-1}\right).$$

Теорема Эйлера – это обобщение малой теоремы Ферма на случай составного модуля: $a^{\varphi(n)} \equiv 1 \pmod n$, где a – целое число, взаимно простое с натуральным числом n.

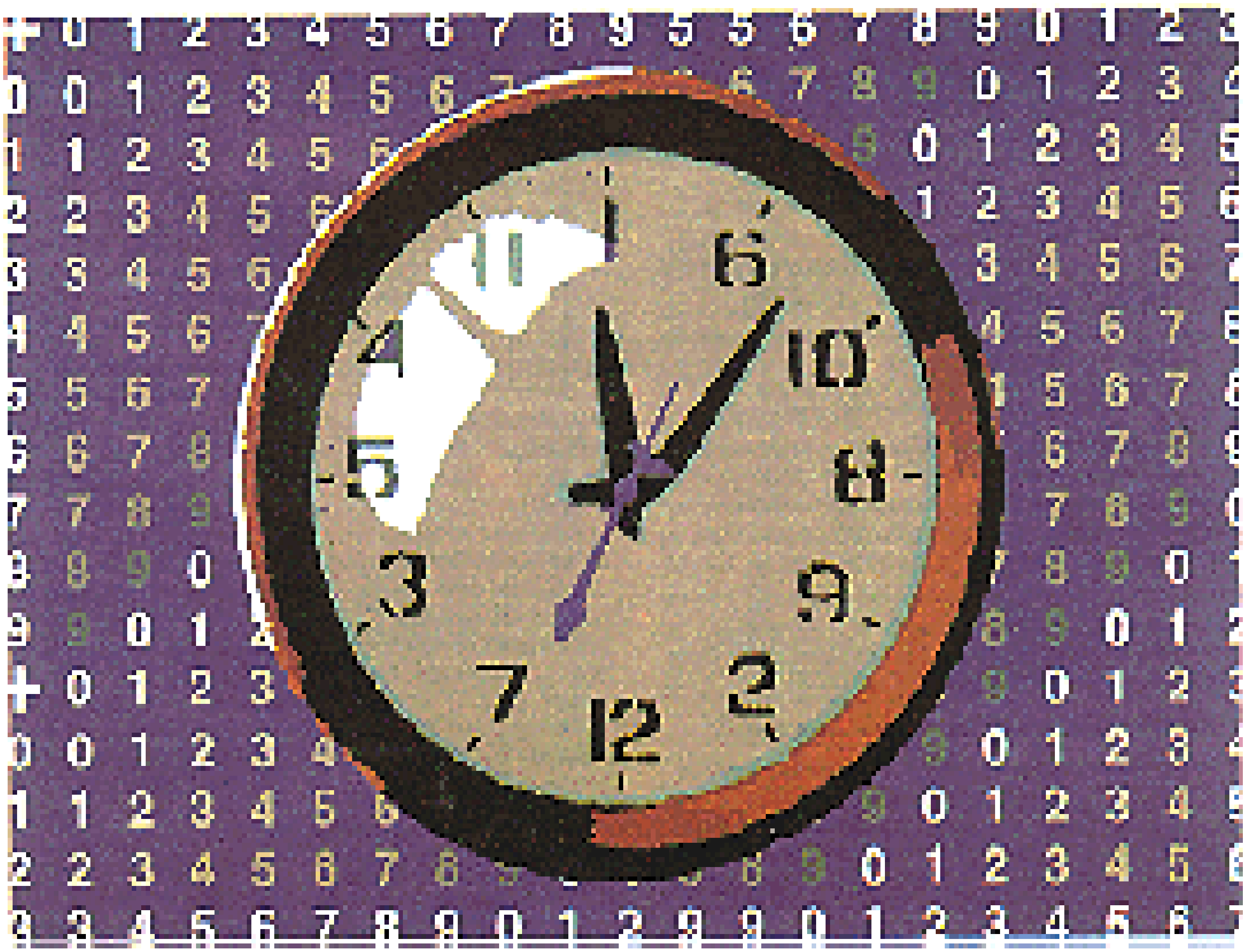

Иллюстрация М.Сумниной

Периодичность остатков

Мы заняты делом,
отвлечься не можем:
мы числа в тетради
все множим и множим.
А.Котова

Остатки от деления на 11

Какие остатки дают степени двойки при делении на 11? Посмотрите на таблицу 1.

Таблица 1

n	1	2	3	4	5	6	7	8	9	10	11	12
2^n	2	4	8	16	32	64	128	256	512	1024	2048	4096
2^n(mod11)	2	4	8	5	10	9	7	3	6	1	2	4

Дальше можно не продолжать: $2^{10+n} = 2^{10} \cdot 2^n \equiv 1 \cdot 2^n = 2^n \pmod{11}$, остатки будут повторяться с периодом 10. Между прочим, средняя строка таблицы излишняя: в нижней строке каждое следующее число – это остаток от деления на 11 удвоенного предыдущего числа.

Как бы то ни было, $2^{10} \equiv 1 \pmod{11}$. Ничего удивительного в этом нет, это всего лишь частный случай малой теоремы Ферма. Интереснее другое: в нижней строке таблицы 1 присутствуют все ненулевые остатки от деления на 11. Например, $3 \equiv 2^8$, $5 \equiv 2^4$, $7 \equiv 2^7$, $10 \equiv 2^5 \pmod{11}$.

Другими словами, для любого целого числа a, не кратного 11, существует такое s, что

$$a \equiv 2^s \pmod{11}.$$

А сейчас – внимание:

$$a^{10} \equiv \left(2^s\right)^{10} = \left(2^{10}\right)^s \equiv 1^s = 1 \pmod{11}.$$

Таким образом, при $p = 11$ мы проверили малую теорему Ферма не только для $a = 2$, но для любого ненулевого остатка a. Красиво и неожиданно, не правда ли?

Упражнение 1. Рассматривая степени двойки, докажите малую теорему Ферма для а) $p = 13$; б) $p = 19$.

Что такое первообразный корень?

Число g называют *первообразным корнем* по простому модулю p, если числа g, g^2, ..., g^{p-1} дают разные (ненулевые) остатки при делении на p. Другими словами, g – первообразный корень, если для любого целого числа a, не кратного числу p, существует такое s, что $a \equiv g^s \pmod{p}$.

Упражнение 2. а) Какие из чисел 1, 2, 3, 4 являются первообразными корнями по модулю 5? б) Какие целые числа являются первообразными корнями по модулю 7?

Число 2 – первообразный корень по модулю 11

В разделе «Таблицы умножения» первой части статьи, как помните, мы составили таблицу умножения по модулю 11. Тот факт, что 2 – первообразный корень, позволяет нам так переставить ее столбцы и строки, что таблица приобретет гораздо более внятный вид (табл.2).

Если $a \equiv g^s$ и $b \equiv g^t$, то $ab \equiv g^s g^t = g^{s+t} \pmod{11}$. Это

Таблица 2

×	1	2	4	8	5	10	9	7	3	6
1	1	2	4	8	5	10	9	7	3	6
2	2	4	8	5	10	9	7	3	6	1
4	4	8	5	10	9	7	3	6	1	2
8	8	5	10	9	7	3	6	1	2	4
5	5	10	9	7	3	6	1	2	4	8
10	10	9	7	3	6	1	2	4	8	5
9	9	7	3	6	1	2	4	8	5	10
7	7	3	6	1	2	4	8	5	10	9
3	3	6	1	2	4	8	5	10	9	7
6	6	1	2	4	8	5	10	9	7	3

Таблица 3

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

сводит умножение по модулю 11 к сложению по модулю 10 (именно по этому модулю рассматриваются числа s и t). Давайте рассмотрим таблицу сложения по модулю 10 (табл.3).

Таблицы 2 и 3 очень похожи! Математик сказал бы, что мультипликативная [1] группа вычетов $\boldsymbol{Z}_{11}^*$ (ее элементы – ненулевые классы вычетов по модулю 11) *изоморфна* аддитивной [2] группе $\boldsymbol{Z}_{10}$ вычетов по модулю 10. Наивно говоря, изоморфизм – это взаимно однозначное отображение, сохраняющее операцию.[3] Например, изоморфизм между $\boldsymbol{Z}_{10}$ и $\boldsymbol{Z}_{11}^*$ можно установить, сопоставив каждому из чисел $s = 0, 1, \ldots, 9$ число 2^s. При этом сумме $s + t \pmod{10}$ будет, как мы уже говорили, сопоставлено произведение $2^s \cdot 2^t \pmod{11}$.

[1] *От латинского «умножать».*
[2] *От латинского «складывать».*
[3] *Точное определение изоморфизма можно найти, например, в «Алгебре» Ван дер Вардена (М.: Наука, 1976).*

Числа на окружности

Для любых трех стоящих подряд чисел a, b, c рисунка 1 разность $b^2 - ac$ кратна 11. И это не случайный курьез, а частный случай общей конструкции: взяв первообразный корень g по простому модулю p, рассмотрим геометрическую прогрессию g, g^2, … …, g^{p-2}, g^{p-1} и выпишем вдоль окружности остатки от деления ее членов на p. (Рисунок 1 иллюстрирует случай $g = 2$ и $p = 11$, заставка к статье – случай $g = 6$ и $p = 13$.)

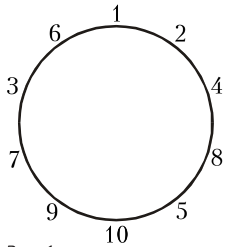

Рис.1

Дело вот в чем: если числа a, b, c образуют геометрическую прогрессию, то выполнено равенство $b^2 = ac$. (А поскольку мы заменяли числа на их остатки от деления на p, то вместо равенств получаем сравнения по модулю p.)

Итак, когда мы докажем, что по простому модулю p существует первообразный корень [4], то одновременно докажем и возможность такого расположения чисел 1, 2, …, $p - 1$ вдоль окружности, при котором для любых трех стоящих подряд чисел a, b, c разность $b^2 - ac$ кратна p.

Упражнение 3. Пусть n – составное. Можно ли так расположить числа 1, 2, …, $n - 1$ вдоль окружности, чтобы для любых трех стоящих подряд чисел a, b, c разность $b^2 - ac$ была кратна n?

Степени двойки по модулю 17

Рассмотрим остатки от деления степеней двойки на 17 (табл.4).

Таблица 4

n	1	2	3	4	5	6	7	8
$2^n \pmod{17}$	2	4	8	16	15	13	9	1

Зацикливание произошло слишком рано: $2^8 \equiv 1 \pmod{17}$. Поэтому не все ненулевые остатки от деления на 17 – остатки от деления степеней двойки. Например, в нижней строке таблицы 4 нет числа 5, так что разность $2^n - 5$ не кратна 17 ни при каком натуральном n.

Упражнения

4. Докажите, что ни при каком натуральном n число $1719^n - 3$ не кратно 17.

5. Среди чисел вида $2^n - 3$ бесконечно много чисел, кратных 5, и бесконечно много чисел, кратных 13, но нет ни одного числа, кратного 65 (= 5 · 13). Докажите это.

Степени тройки по модулю 17

Давайте начнем не с двойки, а с тройки и, не забывая переходить к остатку от деления на 17, будем умножать, умножать и умножать на три: 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1. Мы получили все 16 возможных ненулевых остатков от деления на 17. Значит, 3 – первообразный корень по модулю 17.

Не для каждого простого числа p в качестве первообразного корня годятся 2 или 3. Например, легко проверить, что

$$2^{11} \equiv 1 \equiv 3^{11} \pmod{23},$$

так что ни 2, ни 3 не являются первообразными корнями по модулю 23. (А вот –2 и –3, как можно убедиться, являются.)

Упражнение 6. Найдите наименьшее простое число p, для которого существует a, не сравнимое по модулю p ни с одним из чисел –1, 0, 1 и такое, что ни a, ни $-a$ не являются первообразными корнями по модулю p.

Когда $a^m - 1$ делится на $a^k - 1$?

От числовых примеров перейдем к более абстрактным рассуждениям. Прежде всего напомним формулы сокращенного умножения:

$$a^2 - 1 = (a-1)(a+1),$$

$$a^3 - 1 = (a-1)(a^2 + a + 1),$$

и вообще,

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1).$$

Теорема 1. *Если a, k, m – натуральные числа, $a > 1$, то $a^m - 1$ делится на $a^k - 1$ в том и только том случае, когда m делится на k.*

Доказательство. Если $m = kn$, то

$$a^m - 1 = (a^k - 1)(a^{k(n-1)} + a^{k(n-2)} + \ldots + a^k + 1).$$

Обратно, если m не делится на k, то разделим m на k с остатком:

$$m = kn + r,$$

где $0 < r < k$, и рассмотрим равенство

$$a^{kn+r} - 1 = a^{kn+r} - a^r + a^r - 1 = a^r(a^{kn} - 1) + (a^r - 1).$$

Число $a^r - 1$ не делится на $a^k - 1$, поскольку $0 < a^r - 1 < a^k - 1$. Теорема доказана.

Упражнения

7. Если число $a^n - 1$ простое, $a > 1$ и $n > 1$, то $a = 2$ и n – простое. Докажите это. (Не при всяком простом p число $2^p - 1$ простое: например, $2^{11} - 1 = 2047 = 23 \cdot 89$. Простые числа вида $2^p - 1$ называют *числами Мерсенна* [5]. В настоящий момент известно 38 чисел Мерсенна и неизвестно, конечно или бесконечно их множество. В 1997 году было найдено число Мерсенна $2^{2976221} - 1$, а 1 июня 1999 года нашли наибольшее из известных на сегодняшний день: $2^{26972593} - 1$.)

8. Если $a^n + 1$ – простое число, a, n – натуральные числа, $a > 1$, то a четно и n – степень числа 2. Докажите это. (Простые числа вида $2^{2^n} + 1$ называют *числами Ферма*. Их известно всего пять: $2^{2^0} + 1 = 3$, $2^{2^1} + 1 = 5$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$ и $2^{2^4} + 1 = 65537$. Существуют ли другие, неизвестно. Неизвестно и то, конечно или бесконечно множество простых чисел вида $p = a^2 + 1$.)

9. а) Число $2^n - 1$ делится на $2^m + 1$ тогда и только тогда, когда n делится на $2m$. Докажите это. б) Для каких натуральных чисел m существует такое натуральное n, что $2^n + 1$ делится на $2^m - 1$?

[4] *А мы это докажем, хотя и не в этом номере журнала.*

[5] *Марен Мерсенн (1588–1648) занимался математикой, теорией музыки, физикой и философией. Он был товарищем Р. Декарта по учебе в иезуитском колледже и членом монашеского ордена минимов. Мерсенн сыграл выдающуюся роль как организатор науки. Он состоял в переписке с Р. Декартом, Ж. Робервалем, Б. Паскалем, Х. Гюйгенсом, Б. Кавальери, Б. Френиклем де Бесси, Дж. Валлисом и др. Вокруг него образовался кружок ученых, который стал основой для создания Парижской Академии наук (1666 год).*

10. Натуральные числа a, b, n таковы, что $a - k^n$ кратно $k - b$ для любого натурального числа $k \neq b$. Докажите, что $a = b^n$.

Степени числа *a* по модулю *p*

Для любого целого числа a, не кратного простому p, рассмотрим числа 1, a, a^2, ..., a^{p-1}. Ни одно из них не кратно p. Поскольку ненулевых остатков от деления на p существует всего $p - 1$ штук, а мы рассматриваем p чисел, то какие-то два из них дают один и тот же остаток:

$$a^r \equiv a^s \pmod p,$$

где $0 \le r < s < p$. Сокращая на a^r, получаем:

$$a^{s-r} \equiv 1 \pmod p,$$

т. е. остаток от деления числа a^{s-r} на p равен 1. Значит, последовательность остатков от деления степеней числа a на p – периодическая.

Упражнения

11. а) Пусть число n нечетно и не кратно 5. Докажите, что существует кратное n число, записываемое одними единицами. б) Если целое число a и натуральное n взаимно просты, то существует такое k, что сумма $1 + a + a^2 + \ldots + a^k$ кратна n. Докажите это.

12. а) Докажите, что для любого натурального n числа $8^n + 1$ и $5 \cdot 4^n + 1$ – составные. б) Существует бесконечно много составных чисел вида $10^n + 3$. Докажите это. (Неизвестно, существует ли бесконечно много простых чисел вида $10^n + 3$.) в) Пусть a, b, c – натуральные числа, $b > 1$. Докажите, что среди чисел вида $ab^n + c$ бесконечно много составных.

Что такое порядок?

Наименьшее натуральное число k, для которого $a^k \equiv 1 \pmod p$, называют *порядком* (не кратного p) числа a по модулю p.

Очевидно, числа a, a^2, ..., $a^k (\equiv 1)$ дают при делении на p разные остатки, а дальше последовательность периодична: $a^{k+1} \equiv a$, $a^{k+2} \equiv a^2$, ... При этом

$$a^k \equiv a^{2k} \equiv a^{3k} \equiv \ldots \equiv 1 \pmod p,$$

а другие степени числа a не сравнимы с 1 по модулю p.

Если вместо простого числа p вы рассмотрите любое натуральное число n, то аналогичным образом сможете доказать следующую важную теорему.

Теорема 2. *Если целое число a взаимно просто с натуральным числом n, то существует бесконечно много таких натуральных m, что $a^m - 1$ кратно n. Все они являются кратными наименьшего из них (которое называют порядком числа a по модулю n).*

Упражнения

13. Если целое число a взаимно просто с натуральным n и если $a^r \equiv a^s \equiv 1 \pmod n$, то $a^{\text{НОД}(r,s)} \equiv 1 \pmod n$. Докажите это.

14. Зная, что порядок числа $a = 10$ по модулю $p = 19$ равен 18, выясните, при каких k число $\underbrace{11\ldots1}_{k}$ кратно 19.

15. Если число 1000...01 кратно 19, то оно кратно 13. Докажите это.

Разбиение на циклы

Пусть целое число a не кратно простому p и пусть k – порядок числа a по модулю p. Как при помощи k сформулировать малую теорему Ферма? А вот как: $p - 1$ кратно k. (Т.е. $p - 1 = km$ для некоторого натурального m; сравнение $a^{p-1} \equiv 1$ получается из сравнения $a^k \equiv 1$ возведением в m-ю степень.)

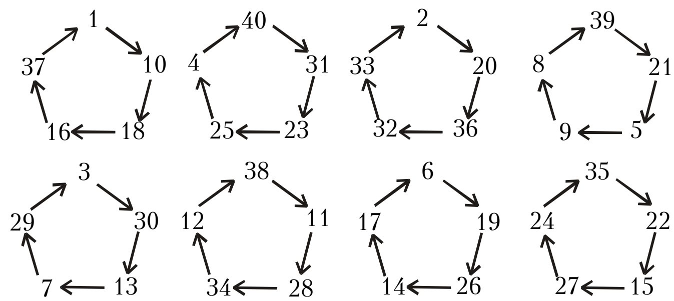

Рис.2

Теорема 3. *Порядок k не кратного простому p целого числа a является делителем числа p – 1.*

Доказательство. Идея в том, что все $p - 1$ ненулевых остатков от деления на p мы разобьем на циклы вида $\{x, ax, \ldots, a^{k-1}x\}$. Каждый такой цикл состоит из k остатков. Например, при $p = 41$ и $a = 10$ разбиение изображено на рисунке 2, на котором стрелочкой показано действие операции умножения на 10 («по модулю 41», т.е. мы каждый раз не только умножаем на 10, но и берем остаток от деления на 41).[6]

В общем случае, проведя от каждого ненулевого остатка x стрелочку к остатку от деления на p числа ax, мы получим рисунок, на котором из каждого ненулевого остатка выходит одна стрелочка и к каждому ненулевому остатку ведет тоже одна стрелочка (если бы к какому-то остатку y вели стрелочки от x_1 и x_2, то выполнялись бы сравнения $ax_1 \equiv y \equiv ax_2 \pmod p$, откуда $x_1 \equiv x_2 \pmod p$, так что $x_1 = x_2$).

Теорема 3 доказана.

Теорема Эйлера

Рассмотрев вместо простого p любое натуральное число n, аналогичным образом можно доказать, что порядок (по модулю n) взаимно простого с n целого числа a – делитель числа $\varphi(n)$. При этом $a^{\varphi(n)} \equiv 1 \pmod n$. Последнее утверждение, как вы помните, носит имя Леонарда Эйлера.

Упражнения

16. Существует ли такое натуральное число k, что сто последних цифр десятичной записи числа 3^k совпадают со ста последними цифрами числа 7^k?

17. Если a и b – взаимно простые натуральные числа, то $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$. Докажите это.

18. Существует бесконечно много натуральных чисел n, для которых $2^n + n^2$ кратно 100. Докажите это.

19. Для любого простого числа p существует бесконечно много чисел вида $2^n - n$, кратных p. Докажите это.

20. а) Последние две цифры квадрата любого натурального числа и его 22-й степени совпадают: $n^2 \equiv n^{22} \pmod{100}$. Докажите это. б) Докажите, что $n^{103} \equiv n^3 \pmod{1000}$ для любого целого числа n.

21. Докажите, что последние цифры чисел вида а) n^n; б) n^{n^n} (n – натуральное) образуют периодическую последовательность, и найдите длину ее наименьшего периода.

22. Найдите четыре последние цифры числа а) 3^{1999}; б) 2^{1999}; в) $2^{3^{2000}}$.

---

[6] *Эти циклы тесно связаны с разложениями обыкновенных дробей со знаменателем 41 в периодические десятичные дроби (см. статью Л. Семеновой «Периодические дроби» в «Кванте» №2).*

23*. Докажите, что уравнение $x^7 + y^7 = 1998^z$ не имеет решений в натуральных числах.

24*. Для любого целого числа $k \neq 1$ существует бесконечно много натуральных чисел n, для которых число $2^{2^n} + k$ – составное. Докажите это. (Аналогичное утверждение для $k = 1$ мы доказать не умеем: существует или нет бесконечно много составных чисел вида $2^{2^n} + 1$, неизвестно.)

Усиление теоремы Эйлера

Рассмотрим утверждение теоремы Эйлера при $n = 360$. Очевидно, $\varphi(360) = \varphi(2^3 \cdot 5 \cdot 9) = 4 \cdot 4 \cdot 6 = 96$. Значит, для любого целого числа a, взаимно простого с 360, выполнено сравнение

$$a^{96} \equiv 1 \pmod{360}.$$

А на самом деле верно даже сравнение

$$a^{12} \equiv 1 \pmod{360}.$$

Для доказательства достаточно применить теорему Эйлера к каждому из модулей 8, 5 и 9:

$$a^4 \equiv 1 \pmod 8,$$

$$a^4 \equiv 1 \pmod 5,$$

$$a^6 \equiv 1 \pmod 9,$$

и заключить, что $a^{12} \equiv 1$ по каждому из модулей 8, 5 и 9, а значит, и по модулю 360.

В общем виде это можно сформулировать следующим образом. Рассмотрим разложение

$$n = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s}$$

числа n в произведение степеней различных простых множителей. Обозначим через $f(n)$ наименьшее общее кратное чисел $\varphi\left(p_i^{m_i}\right)$, где $i = 1, 2, \dots, s$. (Например, $f(360)=\text{НОК}\left[\varphi(2^3), \varphi(3^2), \varphi(5)\right] = \text{НОК}[4, 6, 4] = 12$.) Тогда при любом целом a, взаимно простом с n, справедливы сравнения

$$a^{f(n)} \equiv 1 \left(\operatorname{mod} p_i^{m_i}\right),$$

где $i = 1, 2, \dots, s$; следовательно,

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

Упражнение 25. а) Для каких натуральных n верно равенство $f(n) = \varphi(n)$?

б) Пусть $n > 4$ и n не представимо ни в виде p^m, ни в виде $2p^m$, где p – нечетное простое, m – натуральное. Докажите, что невозможно так расположить все $\varphi(n)$ меньших n и взаимно простых с ним натуральных чисел вдоль окружности, чтобы для любых трех стоящих подряд чисел a, b, c разность $b^2 - ac$ делилась на n. (Другими словами, для этих n нет первообразного корня, т.е. нет числа g, порядок которого по модулю n равен $\varphi(n)$.)

Сравнения по модулю 2^m

Пусть m – натуральное число, $m \geq 3$. Теорема Эйлера утверждает, что $a^{2^{m-1}} \equiv 1 \left(\operatorname{mod} 2^m\right)$ для любого нечетного числа a. На самом деле верно более сильное утверждение:

$$a^{2^{m-2}} \equiv 1 \left(\operatorname{mod} 2^m\right).$$

Его легко доказать по индукции.

База – случай $m = 3$. Число $a^2 - 1 = (a-1)(a+1)$ кратно 8, поскольку одно из соседних четных чисел $a - 1$ и $a + 1$ кратно 4.

Переход. Пусть утверждение верно для некоторого $m \geq 3$. Рассмотрим разложение на множители:

$$a^{2^{m-1}} - 1 = \left(a^{2^{m-2}} - 1\right)\left(a^{2^{m-2}} + 1\right).$$

Поскольку первый множитель правой части делится на 2^m, а второй множитель четен, произведение делится на 2^{m+1}, что и требовалось доказать.

Упражнение 26. Пусть a нечетно, $m \geq 3$. а) Решите сравнение $x^2 \equiv a^2 \left(\operatorname{mod} 2^m\right)$. б) Докажите, что сравнение $x^2 \equiv a \left(\operatorname{mod} 2^m\right)$ разрешимо для тех и только тех a, для которых $a \equiv 1 \pmod 8$.

Функция Кармайкла

Через $\lambda(n)$ обозначим такое наименьшее натуральное число k, что $a^k - 1$ кратно n для любого числа a, взаимно простого с n. Функцию λ называют *функцией Кармайкла*.

Легко понять, что для любого натурального числа l, не кратного $\lambda(n)$, существует такое взаимно простое с n целое число a, что $a^l \not\equiv 1 \pmod n$. Чтобы это доказать, разделим с остатком l на $\lambda(n)$. Имеем:

$$l = \lambda(n)q + r,$$

где q – целое неотрицательное, $0 < r < \lambda(n)$. При этом

$$a^l = \left(a^{\lambda(n)}\right)^q \cdot a^r.$$

Поскольку $r < \lambda(n)$, хотя бы для одного взаимно простого с n числа a сравнение $a^r \equiv 1 \pmod n$ не выполнено. Это и требовалось доказать.

Функция Кармайкла обладает еще одним интересным свойством: $\lambda(mn) = \text{НОК}\left[\lambda(m), \lambda(n)\right]$ *для любых взаимно простых натуральных чисел m и n*. В самом деле, если целое число a взаимно просто с числами m и n, то по определению

$$a^{\lambda(m)} \equiv 1 \pmod m,$$

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

откуда для числа $k = \text{НОК}\left[\lambda(m), \lambda(n)\right]$ имеем

$$a^k \equiv 1 \pmod m,$$

$$a^k \equiv 1 \pmod n,$$

так что $a^k \equiv 1 \pmod{mn}$. Таким образом, $\lambda(mn) \leq k$.

Осталось доказать, что $\lambda(mn)$ делится как на $\lambda(m)$, так и на $\lambda(n)$. Сделаем это «от противного». Пусть, например, $l = \lambda(mn)$ не делится на $\lambda(m)$. Тогда существует такое число b, взаимно простое с m, что $b^l \not\equiv 1 \pmod m$.

Рассмотрим число a, для которого $a \equiv b \pmod m$ и a взаимно просто с n.[7] Очевидно, $a^l \equiv b^l \not\equiv 1 \pmod m$, что и требовалось доказать.

[7] *Почему такое a существует? Например, можно рассмотреть числа вида b + mx, где x = 1, 2, …, n. Они дают разные остатки при делении на n. Поскольку этих чисел n – столько же, сколько классов вычетов по модулю n, – то среди них найдется и нужное нам a.*

Функция Кармайкла от степеней простых чисел такова: $\lambda(2) = 1$, $\lambda(4) = 2$, $\lambda(2^m) = 2^{m-2}$ при $m \ge 3$, $\lambda(p^m) = p^{m-1}(p-1)$ для любых нечетного простого p и натурального m.

Упражнение 27*. Докажите это, считая известным, что если p – нечетное простое, то для любого $k < p-1$ существует такое не кратное p число g, что $g^k \not\equiv 1 \pmod{p}$.

Следствия из малой теоремы Ферма

Теорема 3 позволяет легко решать многие задачи, которые без нее или очень трудны, или вообще недоступны. Рассмотрим букет таких задач, начав с одной из тех пяти, которые сформулированы в конце первой части статьи.

Простые делители чисел вида $a^4 + a^3 + a^2 + a + 1$

Если сумма $a^4 + a^3 + a^2 + a + 1$ кратна простому числу p, то число

$$a^5 - 1 = (a-1)(a^4 + a^3 + a^2 + a + 1)$$

тоже кратно p. Рассмотрим два случая.

Пусть $a \equiv 1 \pmod{p}$. Тогда $a^4 + a^3 + a^2 + a + 1 \equiv 1^4 + 1^3 + 1^2 + 1 + 1 = 5 \pmod{p}$, так что число p должно быть делителем числа 5. Попросту говоря, $p = 5$.

Пусть теперь $a \not\equiv 1 \pmod{p}$. Тогда порядок числа a по модулю p равен 5. Поскольку порядок является делителем числа $p-1$, то $p-1$ делится на 5.

Итак, *если простое число p является делителем числа вида $a^4 + a^3 + a^2 + a + 1$*, то *$p = 5$ или $p \equiv 1 \pmod{5}$.*

Когда мы докажем теорему о существовании первообразного корня, то поймем, что верно и обратное утверждение. А именно, для $p = 5$ годится $a = 1$, а для простого числа $p = 5k + 1$ годится $a = g^k$, где g – первообразный корень по модулю p. В самом деле, $g^{5k} = g^{p-1} \equiv 1 \pmod{p}$. Следовательно, произведение $(a-1)(a^4 + a^3 + a^2 + a + 1) = a^5 - 1$ кратно p. Поскольку первый множитель не делится на p, второй должен делиться, что и требовалось доказать.

Упражнения

28 (М1324). Ни при каком целом a число $a^2 + a + 1$ не кратно а) 5; б) 11; в) 17; г) $6m - 1$, где m – натуральное число. Докажите это.

29. Докажите, что всякий положительный делитель числа $a^4 - a^2 + 1$ дает остаток 1 при делении на 12.

30. Докажите, что если порядок числа a по простому модулю p равен

а) 3, то число $a^2 + a + 1$;

б) 4, то число $a^2 + 1$;

в) 15, то число $a^8 - a^7 + a^5 - a^4 + a^3 - a + 1$

кратно p. (Тот, кто знаком с многочленами деления круга, скажет, что это упражнение – частный случай общего утверждения: число a имеет порядок k тогда и только тогда, когда k – делитель числа $p-1$ и $\Phi_k(a) \equiv 0 \pmod{p}$.)

31. Если по простому модулю p число a имеет порядок а) 3, то порядок числа $a + 1$ равен 6; б) 10, то порядок числа $a^3 - a^2 + a - 1$ равен 5. Докажите это.

32. а) Пусть a – натуральное число, $a > 1$, p – простое, $p > 2$. Докажите, что всякий простой делитель q числа $a^p \pm 1$ является делителем числа $a \pm 1$ или имеет вид $q = 2pm + 1$, где m – натуральное.

б) Пусть a, b – взаимно простые целые числа, n – натуральное, q – простое, $a^n - b^n$ делится на q, и пусть ни для одного отличного от n делителя m числа n разность $a^m - b^m$ не делится на q. Докажите, что $q \equiv 1 \pmod{n}$. (Биркгоф и Вандивер, используя свойства многочленов деления круга, доказали в 1902 году, что для любых (кроме одного исключительного случая, о котором сказано ниже) натуральных взаимно простых чисел a и b, где $a > b$, и для любого натурального числа $n > 2$ существует простой делитель q разности $a^n - b^n$, не являющийся делителем ни одной разности $a^m - b^m$, где $m < n$. Единственное исключение: $a = 2$, $b = 1$, $n = 6$.)

Простые делители чисел вида $a^{2^n} + 1$

Если $a^2 + 1$ делится на простое число p, $p \ne 2$, то

$$a^2 \equiv -1 \pmod{p},$$

откуда

$$a^4 = (a^2)^2 \equiv (-1)^2 = 1 \pmod{p}.$$

Значит, порядок числа a равен одному из чисел 1, 2 и 4.

Первый и второй случаи невозможны, поскольку сравнение $a^2 \equiv 1$ противоречит сравнению $a^2 \equiv -1 \pmod{p}$.

В третьем случае в силу теоремы 3 имеем: $p-1$ делится на 4. Мы доказали довольно общее и часто используемое утверждение: *любой нечетный простой делитель числа $a^2 + 1$ имеет вид $p = 4k + 1$ (а не $4k + 3$).*

Рассуждая аналогично, можно доказать, что если p – нечетный простой делитель числа $a^{2^n} + 1$, то $p-1$ делится на 2^{n+1}.

Верно и обратное: для любого простого числа $p = 2^{n+1}k + 1$ существует кратное ему число вида $a^{2^n} + 1$. Доказать это очень легко, если знать теорему о существовании первообразного корня g. В самом деле, пусть $a = g^k$. Тогда

$$a^{2^n} = g^{2^n k} = g^{(p-1)/2}.$$

Число $g^{(p-1)/2}$ не сравнимо с единицей по модулю p, но квадрат этого числа есть $g^{p-1} \equiv 1 \pmod{p}$. Поэтому

$$a^{2^n} = g^{(p-1)/2} \equiv -1 \pmod{p},$$

что и требовалось.

Упражнения

33. Если числа a и b взаимно просты, то всякий нечетный простой делитель p числа $a^{2^n} + b^{2^n}$ дает остаток 1 при делении на 2^{n+1}. Докажите это.

34. Пусть a, n – натуральные числа, причем a четно. Докажите, что числа n и $a^{2^n} + 1$ взаимно просты.

35. Пусть a, n – натуральные числа. Докажите, что

а) если $a^n + 1$ делится на $n + 1$, то a и n нечетны;

б) если a нечетно и $a > 1$, то существует бесконечно много натуральных n, для которых $a^n + 1$ делится на $n + 1$.

36. а) Пусть $n > 1$ и $2^n + 2$ делится на n. Докажите, что n четно.

б) Существует бесконечно много таких натуральных n, что $2^n + 2$ кратно n. Докажите это.

37 (Международная математическая олимпиада, 1996 г.). Пусть a, b – такие натуральные числа, что $15a + 16b$ и $16a - 15b$ – квадраты натуральных чисел. Найдите наименьшее возможное значение меньшего из этих квадратов.

Когда $2^n + 1$ делится на n?

Этот вопрос один из нас задал себе скорее в шутку, чем всерьез. И очень долго мы оба не понимали, что закономерности, обнаруживаемые в вычислениях, производимых следующей программой [8], имеют самое непосредственное отношение к малой теореме Ферма.

[8] *Программу для нас написал В.Иофик – тогда абитуриент, а сейчас – студент мехмата МГУ.*

Программа

```
#include<stdio.h>
#include<conio.h>
#include<stdlib.h>

unsigned long mult(unsigned long a, unsigned long b, unsigned long n)
{unsigned long c=0;
 for(;b;b>>=1){if(b&1)c=(a+c)%n;a=a*2%n;}
 return c;}

int power(unsigned long b, unsigned long p, unsigned long m)
{unsigned long a=1;
 while(p){if(p&1)a=mult(b,a,m); b=mult(b,b,m); p>>=1;}
 return !((a+1)%m);}

main(int argc, char *argv[])
{if(argc<3){cprintf("\n\rВведите командную строку:\n\r");
cprintf("%s <файл> <основание> [начальный показатель (по умолчанию 1)]\n",argv[0]);
   return 1;}
 unsigned long b=atol(argv[2]), k;
 if(argc>3)k=atol(argv[3]); else k=1;
 if(!(b&&k))
 {cprintf("\n\n\n\rОснование степени и начальное число должны быть отличны от 0");
 return 1;}
 FILE *f=fopen(argv[1],"wt");
 cprintf("\n\n\n\r%10lu",k);
 fprintf(f,"%s^n+1 делится на n при следующих значениях:",argv[2]);
      for(unsigned long i=k;!kbhit()&&i<2147483648;i++)
      {cprintf("\b\b\b\b\b\b\b\b\b\b%10lu",i);
      if(power(b,i,i)){fprintf(f,"\n%10lu  ",i); cprintf("\n\r");}}
 fclose(f);
 while(kbhit())getch();
 return 0;}
```

Результаты работы этой программы таковы: 2^n+1 делится на n при $n = 1, 3, 9, 27, 81, 171$[9], 243, 513, 729, 1539, 2187, 3249, 4617, 6561, 9747, 13203[10], 13851, 19683, 29241, 39609, 41553, 59049, 61731, 87723, 97641, 118827, 124659, …

Все эти числа (кроме единицы, но она не в счет) делятся на 3. И среди них присутствуют все степени тройки. Как это объяснить?

Со степенями тройки мы разобрались мгновенно: по индукции легко доказать, что $2^{3^k}+1$ делится на 3^{k+1}.

И мы сразу сообразили, что верно следующее утверждение: *если n кратно 3 и 2^n+1 кратно n, то $2^{3n}+1$ кратно $3n$.* В самом деле,

$$2^{3n}+1=\left(2^n+1\right)\left(\left(2^n\right)^2-2^n+1\right);$$

первый множитель кратен n, а второй кратен 3. (Почему? Потому что из условия $2^n \equiv -1\ (\mathrm{mod}\, n)$ имеем $2^n \equiv$ $\equiv -1\ (\mathrm{mod}\, 3)$, откуда $\left(2^n\right)^2-2^n+1 \equiv (-1)^2-(-1)+1 \equiv$ $\equiv 0\ (\mathrm{mod}\, 3)$.)

Но это все не отвечало на самый наивный и самый интересный вопрос: почему числа n, для которых 2^n+1 кратно n и $n > 1$, поголовно делятся на 3?

Подумав несколько недель, мы поняли: надо рассмотреть *наименьший простой делитель p числа n.* Тогда

$$2^n \equiv -1\ (\mathrm{mod}\, p).$$

Значит, $2^{2n} \equiv 1\ (\mathrm{mod}\, p)$, и поэтому порядок числа 2 по модулю p является делителем числа $2n$. Поскольку он не превосходит $p-1$ и поскольку число n не имеет простых делителей, меньших p, есть единственная возможность: порядок числа 2 по модулю p равен 2. Это значит, что $2^2 \equiv 1\ (\mathrm{mod}\, p)$, т. е. $p = 3$, что и требовалось доказать.

Упражнения

38. Пусть a, n – натуральные числа, $n > 1$. Докажите, что если a^n+1 делится на n, то наименьший простой делитель числа n является делителем числа $a+1$.

39. Пусть n – натуральное число, $n > 3$ и 2^n+1 кратно n. Докажите, что

а) n кратно 9;

б) если $n > 9$, то n кратно 27 или 19;

в) если n делится на простое число $p \neq 3$, то $p \geq 19$;

г*) если n делится на простое число p, причем $p \neq 3$ и $p \neq 19$, то $p \geq 163$.

40. Если 2^a+1 кратно b и 2^b+1 кратно a, где $a > 1$ и $b > 1$, то a и b кратны 3. Докажите это.

41 (М1260*). Найдите все такие натуральные n, для которых 2^n+1 кратно n^2.

42. а) Если 2^n-1 кратно n, то $n = 1$. Докажите это.

б) Докажите, что существует бесконечно много натуральных чисел n, для которых $\text{НОД}\left(2^n-1, n\right) > 1$.

в) Пусть a – натуральное число, $a > 2$. Докажите, что множество натуральных чисел n, для которых a^n-1 кратно n, бесконечно.

43. Пусть a – натуральное число, $a > 1$.

а) Существует бесконечно много n таких, что a^n+1 делится на n. Докажите это.

б) При каких a существует число $n > 1$ такое, что a^n+1 делится на n^2?

(Окончание следует)

---

[9] *Заметьте: предыдущие числа – степени тройки, а 171 = = 19 · 9.*

[10] *Впервые возник отличный от 3 и 19 простой множитель: 13203 = 163 · 81.*