Малая теорема Ферма

В.СЕНДЕРОВ, А.СПИВАК

Чем отличается ученик математического класса от ученика географического, экономического, политологического или коррекционного класса? Тем, что он больше размышляет над задачами? Да, и этим тоже. Но не только. Еще он знает малую теорему Ферма.

Программы обучения математике бывают разные: можно начать с подробного изучения геометрии, можно – с комбинаторики, кто-то начинает с теории множеств, все не перечесть. Но малая теорема Ферма прочно вошла в программу математических классов. Компьютерщики – авторы учебника «Конкретная математика» Р.Грэхем, Д.Кнут и О.Паташник – тоже включили ее в тот набор сведений, с которым они знакомят своих студентов.

Формулируется эта теорема, открытая советником парламента Тулузы (Франция) Пьером Ферма (1601–1665) в 1640 году, очень коротко: *если p – простое число, a – целое число, то $a^p - a$ кратно p*. Сразу и не видно, почему скромное с виду утверждение столь важно. Тем не менее, оно заслуживает величайшего внимания.

Мы начнем с материала, который доступен семикласснику, а закончим недавними открытиями в криптографии.

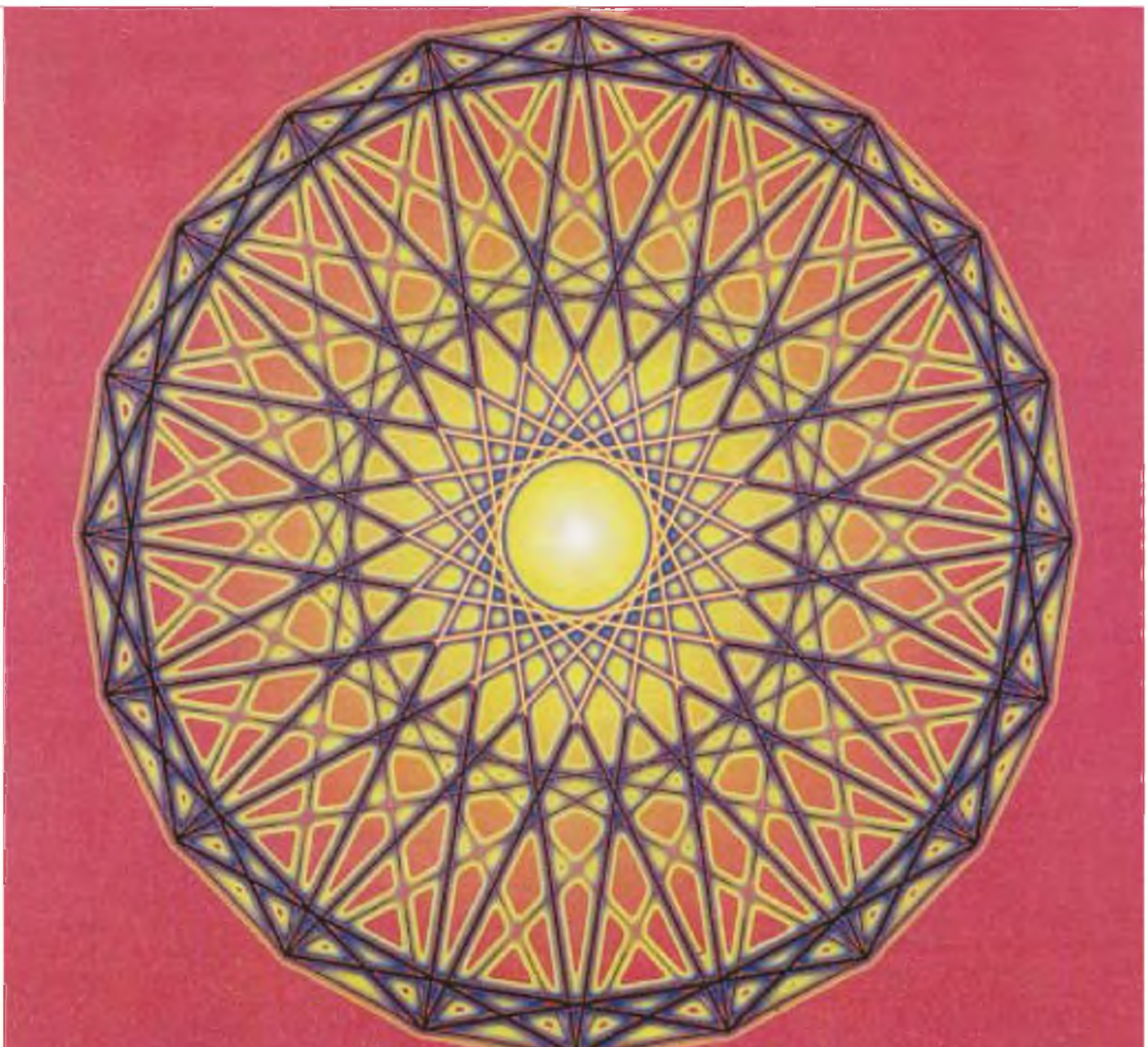


Иллюстрация В.Хлебниковой

Частные случаи

Если из книги вытекает какой-нибудь поучительный вывод, он должен получаться помимо воли автора, в силу самих изображенных фактов.

Ги де Мопассан

Из любых двух последовательных целых чисел a и $a+1$ одно четное, а другое нечетное. Поэтому произведение $a(a+1)=a^2+a$ четно при любом целом a.

Делимость числа a^2+a на 2 можно доказать и по-другому, разобрав два случая:

– если a четно, то a^2 тоже четно, а сумма двух четных чисел a и a^2 четна;

– если a нечетно, то a^2 тоже нечетно, а сумма двух нечетных чисел a и a^2 четна.

Вот так доказывают замечательное свойство многочлена a^2+a. Впрочем, при $\boldsymbol{p=2}$ в малой теореме Ферма фигурирует другой многочлен: $a^2-a=(a-1)a$. Все его значения в целых точках – четные числа (докажите!).

Теперь рассмотрим многочлен $\boldsymbol{a^3-a}$. Его легко разложить на множители:

$$a^3-a=a\left(a^2-1\right)=a(a-1)(a+1).$$

Получили произведение трех последовательных целых чисел: $a-1$, a и $a+1$. Как мы уже знаем, это произведение четно. Поскольку из любых трех последовательных чисел одно кратно 3, их произведение $(a-1)a(a+1)=a^3-a$ кратно 3 (и, значит, даже кратно 6).

Упражнение 1. При любом целом a сумма a^3+5a кратна 6. Докажите это.

Многочлен $\boldsymbol{a^4-a}$ при $a=2$ и $a=3$ принимает значения $2^4-2=14$ и $3^4-3=78$. Конечно, эти значения четны, но никакого общего делителя кроме 2 (и 1) у них нет. Не повезло! Впрочем, число 4 составное, а малая теорема Ферма говорит только о многочленах вида a^p-a, где p – простое число.

Пусть $\boldsymbol{p=5}$. Вычислим несколько значений многочлена a^5-a. При $a=\pm1$ и при $a=0$ получаем ноль. Смотрим дальше: $2^5-2=30$, $3^5-3=240$, $4^5-4=1020$, $5^5-5=3120$, $6^5-6=7770,\ldots$ Все эти значения кратны числу 30.

Поскольку $30=2\cdot3\cdot5$, доказательство делимости на 30 распадается на три части: во-первых, надо доказать, что a^5-a кратно 2; во-вторых, a^5-a кратно 3; в-третьих, a^5-a кратно 5.

Первая часть очевидна: числа a^5 и a либо оба четны, либо оба нечетны. Не вызывает затруднений и вторая часть:

$$a^5-a=a\left(a^4-1\right)=a\left(a^2-1\right)\left(a^2+1\right)=(a-1)a(a+1)\left(a^2+1\right),$$

произведение трех последовательных чисел всегда кратно 3.

Чуть сложнее третья часть. Нет, конечно, из пяти последовательных целых чисел обязательно одно кратно 5, так что произведение $(a-2)(a-1)a(a+1)(a+2)$ кратно 5. Но $a^2+1\neq(a-2)(a+2)$.

Как же быть? Самый бесхитростный способ – перебрать все подряд остатки от деления на 5: любое целое число при делении на 5 дает в остатке 0, 1, 2, 3 или 4. Если остаток равен 0, то кратен 5 второй множитель произведения $(a-1)a(a+1)(a^2+1)$. Если остаток равен 1 или 4, то кратен 5 первый или третий множитель. Если же остаток равен 2 или 3, то в дело вступает четвертый множитель. (Для тех, кто еще не привык работать с остатками, объясним: если $a=5b+2$, т. е. если a дает остаток 2 при делении на 5, то $a^2+1=(5b+2)^2+1=5\left(5b^2+4b+1\right)$. Аналогично можно рассмотреть случай $a=5b+3$.)

Есть и другой способ:

$$a^2+1=(a-2)(a+2)+5,$$

значит, если нас интересуют только остатки от деления на 5, то a^2+1 можно-таки заменить на $(a-2)(a+2)$. Формулой это записывают так:

$$a^2+1\equiv(a-2)(a+2)\pmod 5.$$

Предложенное в 1801 году К. Ф. Гауссом обозначение «$\equiv$» еще не раз будет использовано нами. По определению, a сравнимо с b по модулю n, если $a-b$ кратно n, т. е. $a-b=kn$, где k – целое число.

Обозначение

$$a\equiv b\pmod n$$

оказалось удачным потому, что свойства сравнений похожи на свойства обычных равенств. Сравнения можно складывать: если $a\equiv b\pmod n$ и $c\equiv d\pmod n$, то $a+c\equiv b+d\pmod n$. В самом деле, по определению, $a=b+kn$ и $c=d+ln$, где k, l – целые числа. Значит,

$$a+c=(b+kn)+(d+ln)=b+d+(k+l)n,$$

что и требовалось.

Аналогично, формулы

$$a-c=(b+kn)-(d+ln)=b-d+(k-l)n,$$

$$ac=(b+kn)(d+ln)=bd+knd+bln+kln^2=$$
$$=bd+(kd+bl+kln)n$$

позволяют утверждать, что сравнения можно вычитать и умножать. Коли можно умножать, то можно и возводить в степень: если $a\equiv b\pmod n$, то для любого натурального числа m верно сравнение $a^m\equiv b^m\pmod n$.

Сокращать сравнения надо с осторожностью:

$$6\equiv36\pmod{10},$$

но

$$1\not\equiv6\pmod{10}.$$

Упражнения

2. Решите сравнение $3x\equiv11\pmod{101}$.

3. Какие целые числа x удовлетворяют сравнению $14x\equiv0\pmod{12}$?

4. Пусть $k\neq0$. Докажите, что а) если $ka\equiv kb\pmod{kn}$, то $a\equiv b\pmod n$;

б) если $ka\equiv kb\pmod n$ и числа k, n взаимно просты, то $a\equiv b\pmod n$.

Продолжим изучение многочленов вида a^p-a: докажем, что при любом целом a число $\boldsymbol{a^7-a}$ кратно 7. Как всегда, можно рассмотреть все 7 остатков от деления на 7: $0^7-0=0$, $1^7-1=0$, $2^7-2=126=7\cdot18,\ldots$, $6^7-6=279930=7\cdot39990$. (Можно и чуточку сэкономить: поскольку любое целое число представимо в виде $a=7b$, $7b\pm1$, $7b\pm2$ или $7b\pm3$, очевидно, при проверке малой теоремы Ферма для $p=7$ можно ограничиться рассмотрением случаев $a=0$, 1, 2 и 3.)

Но бездумная проверка не может научить нас ничему интересному. Лучше рассмотрим разложение на множители:

$$a^7 - a = a\left(a^6 - 1\right) = a\left(a^3 - 1\right)\left(a^3 + 1\right) =$$
$$= a(a-1)\left(a^2 + a + 1\right)(a+1)\left(a^2 - a + 1\right).$$

Поскольку

$$a^2 + a + 1 = \left(a^2 + a - 6\right) + 7 \equiv a^2 + a - 6 =$$
$$= (a-2)(a+3) \pmod 7$$

и

$$a^2 - a + 1 \equiv a^2 - a - 6 = (a+2)(a-3) \pmod 7,$$

имеем:

$$a^7 - a \equiv a(a-1)(a-2)(a+3)(a+1)(a+2)(a-3) \pmod 7.$$

Произведение семи последовательных целых чисел кратно 7.

Упражнение 5. Докажите, что а) наибольший общий делитель чисел вида $\boldsymbol{a^7 - a}$ равен 42; б) наибольший общий делитель чисел вида $\boldsymbol{a^9 - a}$ равен 30. (Заметьте: 30 не кратно 9. Это находится в согласии с тем, что число 9 не простое, а составное.)

Теперь рассмотрим число $\boldsymbol{p = 11}$. Очевидно,

$$a^{11} - a = a\left(a^{10} - 1\right) = a\left(a^5 - 1\right)\left(a^5 + 1\right) =$$
$$= a(a-1)\left(a^4 + a^3 + a^2 + a + 1\right)(a+1)\left(a^4 - a^3 + a^2 - a + 1\right).$$

Тут не так-то просто догадаться, как быть дальше. Но полный перебор всех 11 остатков все еще возможен. И когда мы его выполним, окажется, что значения многочлена $a^4 + a^3 + a^2 + a + 1$ кратны 11 при $a \equiv 3$, 4, 5 или 9 $\pmod{11}$, а значения многочлена $a^4 - a^3 + a^2 - a + 1$ кратны 11 при $a \equiv 2$, 6, 7 или 8.

Между прочим, если мы раскроем скобки в произведении $(a-3)(a-4)(a-5)(a-9)$, получим

$$\left(a^2 - 7a + 12\right)\left(a^2 - 14a + 45\right) \equiv \left(a^2 + 4a + 1\right)\left(a^2 - 3a + 1\right) =$$
$$= a^4 + a^3 - 10a^2 + a + 1 \equiv a^4 + a^3 + a^2 + a + 1 \pmod{11}.$$

Аналогично можно проверить, что $(a-2)(a-6)(a-7)(a-8) \equiv a^4 - a^3 + a^2 - a + 1 \pmod{11}$.

Что дальше? При $\boldsymbol{p = 13}$, если действовать нашим способом, придется возводить в двенадцатую степень числа от 1 до 12 или раскрывать скобки в произведении тринадцати множителей: $a - 6$, $a - 5, \ldots, a + 5$, $a + 6$. Заниматься этим не хочется, даже если ограничиться возведением в степень чисел 1, 2, 3, 4, 5, 6 или перемножать «всего лишь» шесть скобок: $(a^2 - 1)(a^2 - 4)(a^2 - 9)(a^2 - 16)(a^2 - 25)(a^2 - 36)$.

Чем больше p, тем больше вариантов надо перебирать. Поэтому мы прекратим разбор частных случаев и перейдем к доказательству малой теоремы Ферма, которое охватывает сразу все простые числа p.

Упражнения

6. а) Произведение любых четырех последовательных целых чисел кратно 24. Докажите это. б) Произведение любых пяти последовательных целых чисел кратно 120. Докажите это. в) Докажите, что $a^5 - 5a^3 + 4a$ при всяком целом a кратно 120.

7. Для любого натурального a число a^5 оканчивается на ту же цифру, что и a. Докажите это.

8. Докажите, что $m^5 n - mn^5$ кратно 30 при любых целых m и n.

9. Если число k не кратно ни 2, ни 3, ни 5, то $k^4 - 1$ кратно 240. Докажите это.

10. а) Докажите, что $2222^{5555} + 5555^{2222}$ кратно 7. б) Найдите остаток от деления числа $\left(13^{14} + 15^{16}\right)^{17} + 18^{19^{20}}$ на 7.

11. Докажите, что число $11^{10} - 1$ оканчивается на два нуля (т.е. кратно 100).

12. а) Найдите все целые числа a, для которых $a^{10} + 1$ оканчивается цифрой ноль. б) Докажите, что ни при каком целом a число $a^{100} + 1$ не оканчивается цифрой ноль.

13. Пусть n – четное число. Найдите наибольший общий делитель чисел вида $\boldsymbol{a^n - a}$, где a – целое число.

14. Пусть n – натуральное число, $n > 1$. Докажите, что наибольший общий делитель чисел вида $a^n - a$, где a пробегает множество всех целых чисел, совпадает с наибольшим общим делителем чисел вида $a^n - a$, где $a = 1, 2, 3, \ldots, 2^n$. (Заметьте: из этого следует, что наибольший общий делитель чисел вида $a^n - a$, где a – целое, совпадает с наибольшим общим делителем чисел такого вида, где a – натуральное.)

Общий случай

И каждого в свою уложат яму.
Эжен Гильвик

Выпишем в строчку числа 1, 2, 3, ..., $p - 1$, домножим каждое из них на k, где k не кратно p, и рассмотрим остатки от деления на p. Например, при $p = 19$ и $k = 4$ получим таблицу 1. В нижней строке таблицы – те же самые числа, что и в верхней, только они расположены в другом порядке! Оказывается, это общий закон: не только при $p = 19$ и $k = 4$, но *при любом простом p и не кратном p целом числе k всегда получатся те же самые числа 1, 2, 3, ..., $p - 1$, возможно, записанные в некотором другом порядке.*

Таблица 1

a	1	2	3	4	5	6	7	8	9
4a	4	8	12	16	20	24	28	32	36
4$a$mod19	4	8	12	16	1	5	9	13	17
a	10	11	12	13	14	15	16	17	18
4a	40	44	48	52	56	60	64	68	72
4$a$mod19	2	6	10	14	18	3	7	11	15

Почему? Ну, во-первых, в нижней строке не может появиться 0, ибо произведение не кратных простому числу p чисел a и k не может быть кратно p. Во-вторых, все числа нижней строки разные (это легко доказать «от противного»: если бы числа ak и bk давали при делении на p одинаковые остатки, то разность $ak - bk = (a - b)k$ была бы кратна p, что невозможно, поскольку $a - b$ не кратно p). Этих двух замечаний достаточно: ненулевых остатков от деления на p существует $p - 1$ штук, все они вынуждены по одному разу появиться в нижней строке таблицы.

Упражнения

15. Существует ли такое натуральное n, что число $1999n$ оканчивается на цифры 987654321?

16. Если целое число k взаимно просто с натуральным числом n, то существует такое натуральное число x, что $kx - 1$ кратно n. Докажите это.

17. Если целые числа a и b взаимно просты, то любое целое число c представимо в виде $c = ax + by$, где x, y – целые числа. Докажите это.

Как вы помните, малая теорема Ферма утверждает, что при любом целом k и простом p число $k^p - k = k\left(k^{p-1} - 1\right)$

кратно p. Значит, для чисел k, не кратных p, теорему можно формулировать следующим образом:

Теорема 1. *Если целое число k не кратно простому числу p, то k^{p-1} дает остаток 1 при делении на p.*

Доказательство. Поскольку остатки от деления на p чисел k, $2k$, $3k$, …, $(p-1)k$ – это (с точностью до перестановки) числа 1, 2, 3, …, $p-1$, то

$$k \cdot 2k \cdot 3k \cdot \ldots \cdot (p-1)k \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p},$$

откуда

$$k^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Сократив на $(p-1)!$, получим желаемое:

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

А тот, кто не решил упражнение 4 б) и не знает, почему сравнения можно сокращать (на число, взаимно простое с модулем), пусть рассуждает следующим образом: поскольку произведение $\left(k^{p-1}-1\right)\cdot(p-1)!$ кратно p, а число $(p-1)!$ не кратно p, то число $k^{p-1}-1$ кратно простому числу p.

Упражнения

18. Найдите остаток от деления числа 3^{2000} на 43.

19. Если целое число a не кратно 17, то a^8-1 или a^8+1 кратно 17. Докажите это.

20. Докажите, что $m^{61}n - mn^{61}$ кратно 56786730 при любых целых m и n.

21. Найдите все такие простые числа p, что $5^{p^2}+1$ кратно p.

22. Пусть p – простое число, $p \neq 2$. Докажите, что число $7^p - 5^p - 2$ кратно $6p$.

23. Если p – простое число, то сумма $1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1}$ при делении на p дает остаток $p-1$. Докажите это.

24. Шестизначное число кратно 7. Его первую цифру стерли и затем записали ее позади последней цифры числа. Докажите, что полученное число тоже кратно 7. (Например, из кратных 7 чисел 632387 и 200004 таким образом получаем числа 323876 и 42, которые тоже кратны 7.)

25. Пусть p – простое число, отличное от 2, 3 и 5. Докажите, что число, записанное $p-1$ единицей, кратно p. (Например, 111111 кратно 7.)

26*. Докажите, что для любого простого p число 11…1122…22…99…99, состоящее из $9p$ цифр (сначала p единиц, потом p двоек, p троек, …, наконец, p девяток), при делении на p дает такой же остаток, как и число 123456789.

Таблицы умножения

Назло ей я все-таки помножил землекопов. Правда, ничего хорошего про них не узнал, но зато теперь можно было переходить к другому вопросу.
Л.Гераскина

Рассмотрим все $n-1$ разных ненулевых остатков от деления на n. Составим таблицу умножения, написав на пересечении a-го столбца и b-й строки остаток от деления на n произведения ab. Например, при $n = 5$ получим таблицу 2, при $n = 11$ — таблицу 3.

Таблица 2

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Таблица 3

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

Таблица 4

×	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Таблица 5

×	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	0	2	4	6	8	10
3	3	6	9	0	3	6	9	0	3	6	9
4	4	8	0	4	8	0	4	8	0	4	8
5	5	10	3	8	1	6	11	4	9	2	7
6	6	0	6	0	6	0	6	0	6	0	6
7	7	2	9	4	11	6	1	8	3	10	5
8	8	4	0	8	4	0	8	4	0	8	4
9	9	6	3	0	9	6	3	0	9	6	3
10	10	8	6	4	2	0	10	8	6	4	2
11	11	10	9	8	7	6	5	4	3	2	1

Поскольку в обоих примерах число n простое, в каждой строке, как и в каждом столбце, возникает некоторая перестановка чисел 1, 2, …, $n-1$. Если же рассмотреть составное число, то в таблице обязательно встретится нуль. Например, при $n = 4$ имеем $2 \cdot 2 \equiv 0$ (табл.4); не лучше ситуация и при $n = 12$ (табл.5): опять в некоторых строках есть нули! И вообще, при любом составном числе $n = ab$, где $1 < a$, $b < n$, на пересечении a-й строки и b-го столбца стоит остаток от деления ab на n, т.е. 0.

Итак, если n составное, то имеются *делители нуля* – ненулевые остатки a и b, произведение ab которых кратно n, иными словами, равно нулю по модулю n. Но даже при составном n в некоторых строках таблицы умножения нет нулей. В таблице 4 таковы первая и третья строки, а в таблице 5 – первая, пятая, седьмая и одиннадцатая. Подумав немного, можно понять, что нули присутствуют в тех и только тех строках, номера которых имеют с числом n общий делитель, отличный от 1 (докажите это!). Давайте же вычеркнем из таблицы все такие строки и столбцы. (Если n – простое число, то вычеркивать ничего не придется.) При $n = 4$ получим таблицу из двух строк и столбцов (табл.6), а при $n = 12$ останется таблица размером 4×4 (табл.7).

Таблица 6

×	1	3
1	1	3
3	3	1

Таблица 7

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Упражнение 27. Заметьте, что каждая из таблиц 2–7 симметрична относительно обеих своих диагоналей. Докажите, что это так для любого n.

Теорема Эйлера

Чтобы обобщить малую теорему Ферма на случай составного числа n, оставим в таблице умножения только те строки и столбцы, в которых нет нулей, т.е. рассмотрим взаимно простые с n остатки от деления на n. В новой таблице строки (и столбцы) отличаются друг от друга лишь порядком, в котором расположены числа. Другими словами, если мы для натурального числа n выпишем все остатки $a_1, a_2, \ldots, a_r$, взаимно простые с n, и домножим каждый из них на взаимно простое с n число k, то получим числа $ka_1, ka_2, \ldots, ka_r$, которые тоже взаимно просты с n и дают разные остатки при делении на n (докажите!).

Итак, строка остатков от деления на n чисел $ka_1, ka_2, \ldots$ $\ldots, ka_r$ может отличаться от строки $a_1, a_2, \ldots, a_r$ только порядком расположения чисел. Поэтому точно так же, как для простого p, для составного n имеем:

$$ka_1ka_2\ldots ka_r \equiv a_1a_2\ldots a_r \pmod{n},$$

откуда

$$\left(k^r - 1\right)a_1a_2\ldots a_r \equiv 0 \pmod{n}.$$

Значит, произведение $\left(k^r - 1\right)a_1a_2\ldots a_r$ кратно n. Поскольку числа $a_1, a_2, \ldots, a_r$ взаимно просты с n, то $k^r - 1$ кратно n. Если n – простое число, то $r = n - 1$ и получаем в точности утверждение малой теоремы Ферма. В общем же случае приходим к теореме Эйлера:

Теорема 2. *Если k – целое число, взаимно простое с натуральным числом n, то $k^r - 1$ кратно n, где r – количество взаимно простых с n натуральных чисел, не превосходящих n.*

Упражнения

28. Докажите, что если число k не кратно 3, то

а) k^3 при делении на 9 дает остаток 1 или 8;

б) k^{81} при делении на 243 дает остаток 1 или 242.

29. а) Если $a^3 + b^3 + c^3$ кратно 9, то хотя бы одно из целых чисел a, b, c кратно 3. Докажите это.

б) Сумма квадратов трех целых чисел кратна 7 в том и только том случае, когда сумма четвертых степеней этих чисел кратна 7. Докажите это.

30. Докажите, что число $7^{7^{7^{7^{7^{7}}}}} - 7^{7^{7^{7}}}$ кратно 10.

31. Каковы три последние цифры числа 7^{9999}?

32. Если целое число a взаимно просто с натуральным числом $n > 1$, то сравнение $ax \equiv b \pmod{n}$ равносильно сравнению $x \equiv a^{r-1}b \pmod{n}$. Докажите это.

33. Если n – нечетное натуральное число, то $2^{n!} - 1$ кратно n. Докажите это.

34*. Найдите все натуральные $n > 1$, для которых сумма $1^n + 2^n + \ldots + (n-1)^n$ кратна n.

35*. Для каждого натурального числа s существует кратное ему натуральное число n, сумма цифр которого равна s. Докажите это.

Функция Эйлера

В 1763 году Леонард Эйлер (1707–1783) ввел обозначение $\varphi(n)$ (читают: фи от эн) для количества r остатков, взаимно простых с n. Например, $\varphi(1) = 1$, $\varphi(4) = 2$, $\varphi(12) = 4$.

Если число p простое, то $\varphi(p) = p - 1$. Легко вычислить и $\varphi\left(p^m\right)$, где m – натуральное число. В самом деле, выпишем все p^m возможных остатков: $0, 1, 2, \ldots, p^m - 1$. Из них кратны p в точности остатки $0, p, 2p, \ldots, p^m - p$. Значит,

$$\varphi\left(p^m\right) = p^m - p^{m-1} = p^m\left(1 - \frac{1}{p}\right).$$

Давайте вычислим $\varphi(1000)$ – количество чисел первой тысячи, которые не кратны ни 2, ни 5. Для этого из 1000 вычтем сначала 500 – именно столько в первой тысяче четных чисел. Не забудем вычесть и 200 – столько в первой тысяче чисел, кратных 5. Что еще? Еще мы должны учесть, что некоторые числа (оканчивающиеся цифрой 0) кратны и 2, и 5. Таких чисел 100 штук; каждое из них мы учитывали оба раза, а надо было – только один раз! Поэтому правильный ответ дает формула

$$\varphi(1000) = 1000 - 500 - 200 + 100 = 400.$$

Упражнения

36. Найдите $\varphi\left(2^a5^b\right)$, где a, b – натуральные числа.

37. Пусть p, q – различные простые числа. Найдите а) $\varphi(pq)$, б) $\varphi\left(p^aq^b\right)$, где a, b – натуральные числа.

38. Решите уравнения: а) $\varphi\left(7^x\right) = 294$; б) $\varphi\left(3^x5^y\right) = 360$.

В принципе, примененный нами способ позволяет вычислить $\varphi(n)$ для любого натурального числа n. Например, чтобы вычислить $\varphi(300)$, мы можем выписать все числа от 1 до 300 и вычеркнуть 150 четных чисел, а также 100 чисел, кратных 3, и 60 чисел, кратных 5. Затем мы должны вспомнить, что некоторые числа вычеркнуты дважды (а иные даже трижды), и «восстановить справедливость», т.е. к числу 300 – 150 – 100 – 60 прибавить 50 чисел, кратных $2 \cdot 3 = 6$, а также 30 чисел, кратных $2 \cdot 5 = 10$, и 20 чисел, кратных $3 \cdot 5 = 15$. Но и этого недостаточно: каждое из десяти чисел, кратных $2 \cdot 3 \cdot 5 = 30$, было сначала трижды выброшено (как кратное 2, 3, 5) и затем трижды возвращено (как кратное 6, 10, 15). Но выбросить эти 10 чисел все-таки надо! Поэтому

$$\varphi(300) = 300 - 150 - 100 - 60 + 50 + 30 + 20 - 10 = 80.$$

Ничего сложного, как видите, нет. Но с ростом количества простых делителей числа n мы будем получать ответ, в котором все больше и больше слагаемых и вычитаемых. В статье Н. Васильева и В.Гутенмахера «Арифметика и принципы подсчета» (Приложение к журналу «Квант» №2 за 1994 год) это все подробно объяснено. А здесь мы изложим другой способ.

Теорема 3. *Функция Эйлера мультипликативна, т.е.*

$$\varphi(mn) = \varphi(m)\varphi(n)$$

для любых взаимно простых натуральных чисел m и n.

Следствие. *Если $n = p_1^{a_1} p_2^{a_2} \cdot \ldots \cdot p_s^{a_s}$, где $p_1, p_2, \ldots, p_s$ – различные простые числа, $a_1, a_2, \ldots, a_s$ – натуральные числа, то*

$$\varphi(n) = \varphi\left(p_1^{a_1}\right)\varphi\left(p_2^{a_2}\right) \cdot \ldots \cdot \varphi\left(p_s^{a_s}\right) =$$

$$= \left(p_1^{a_1} - p_1^{a_1 - 1}\right)\left(p_2^{a_2} - p_2^{a_2 - 1}\right) \cdot \ldots \cdot \left(p_s^{a_s} - p_s^{a_s - 1}\right).$$

Доказательство теоремы 3. Рассмотрим числа вида $mx + ny$, где $0 \le x < n$ и $0 \le y < m$. Запишем их в виде таблицы размером $n \times m$. Например, при $n = 5$ и $m = 8$ получаем таблицу 8.

Таблица 8

$x \backslash y$	0	1	2	3	4	5	6	7
0	0	5	10	15	20	25	30	35
1	8	13	18	23	28	33	38	43
2	16	21	26	31	36	41	46	51
3	24	29	34	39	44	49	54	59
4	32	37	42	47	52	57	62	67

Остатки от деления на mn всех чисел этой таблицы разные. В самом деле, если бы какие-то два остатка совпали, то было бы выполнено сравнение

$$mx_1 + ny_1 \equiv mx_2 + ny_2 \pmod{mn},$$

где $0 \le x_1, x_2 < n$ и $0 \le y_1, y_2 < m$. Отсюда следуют два сравнения:

$$mx_1 + ny_1 \equiv mx_2 + ny_2 \pmod{m}$$

и

$$mx_1 + ny_1 \equiv mx_2 + ny_2 \pmod{n}.$$

Первое приводит к сравнению

$$ny_1 \equiv ny_2 \pmod{m},$$

из которого вследствие взаимной простоты чисел m и n получаем

$$y_1 \equiv y_2 \pmod{m}.$$

Вспомнив, что $0 \le y_1, y_2 < m$, получаем: $y_1 = y_2$. Аналогично, сравнение по модулю n приводит к равенству $x_1 = x_2$.

Итак, все mn чисел таблицы дают разные остатки при делении на mn. Но возможных остатков от деления на mn ровно столько же, сколько чисел в таблице! Значит, рассматриваемые числа дают все возможные остатки от деления на mn. Другими словами, *для любого числа $d = 0, 1, \ldots, mn - 1$ существует и единственна такая пара целых чисел x, y, что $0 \le x < n$, $0 \le y < m$ и $d \equiv mx + ny \pmod{mn}$.*

В таблице 8 четные числа образуют четыре столбца, а числа, кратные 5, образуют одну строку. Это не случайно:

$$\text{НОД}(mx + ny,\ m) = \text{НОД}(ny,\ m) = \text{НОД}(y,\ m);$$

аналогично, $\text{НОД}(mx + ny,\ n) = \text{НОД}(x,\ n)$. По этой причине в рассматриваемой таблице числа, взаимно простые с m, расположены в $\varphi(m)$ столбцах (тех, где y взаимно просто с m), а числа, взаимно простые с n, образуют $\varphi(n)$ строк.

Теперь доказательство теоремы 3 не составляет труда: чтобы d было взаимно просто с mn, необходимо и достаточно, чтобы d было взаимно просто с числами m и n. Такие числа d лежат на пересечении $\varphi(m)$ столбцов (состоящих из чисел, взаимно простых с m) с $\varphi(n)$ строками (состоящими из чисел, взаимно простых с n). Всего получаем «решетку» из $\varphi(m)\varphi(n)$ чисел, что и требовалось доказать.

Упражнения

39. Запишем числа от 0 до $mn - 1$ в таблицу из m строк и n столбцов (табл.9).

Таблица 9

0	1	2	...	$n-1$
n	$n+1$	$n+2$	...	$2n-1$
$2n$	$2n+1$	$2n+2$	...	$3n-1$
...	...	...	...	...
...	...	...	...	...
$(m-1)n$	$(m-1)n+1$	$(m-1)n+2$	...	$mn-1$

а) Составьте такую таблицу для $m = 3$ и $n = 4$. Зачеркните в ней сначала все четные числа, а затем – те из оставшихся чисел, которые кратны 3. Заметьте, что незачеркнутыми остались в

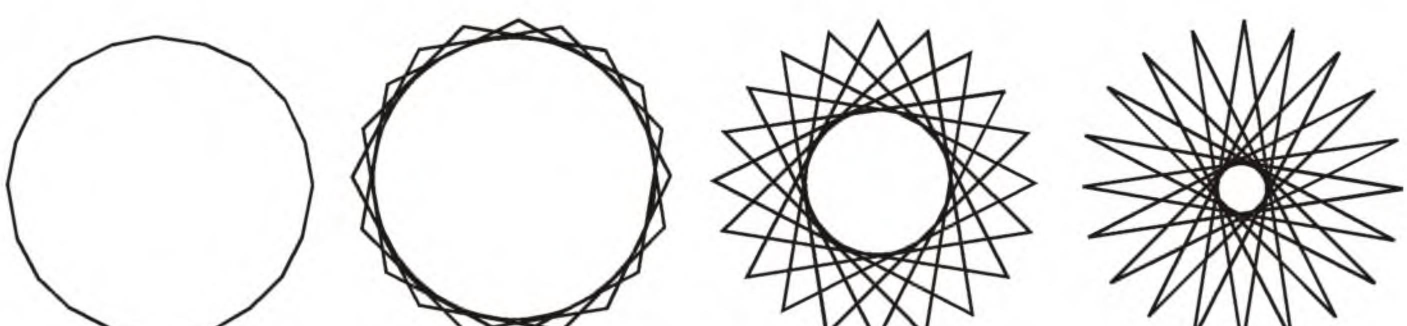


Рис.1

точности числа, взаимно простые с 12, и что незачеркнутые числа не образуют решетки.

б) Докажите теорему Эйлера по следующему плану:

1) числа, взаимно простые с n, заполняют собой $\varphi(n)$ столбцов таблицы 9;

2) остатки от деления на m всех m чисел любого столбца таблицы 9 различны;

3) в каждом столбце присутствует ровно $\varphi(m)$ чисел, взаимно простых с m;

4) число взаимно просто с mn тогда и только тогда, когда оно взаимно просто с n (такие числа лежат в $\varphi(n)$ столбцах) и взаимно просто с m (в каждом столбце таких чисел $\varphi(m)$).

40. Окружность разделили n точками на n равных частей. Сколько можно построить различных замкнутых ломаных из n равных звеньев с вершинами в этих точках? (Две ломаные, получающиеся одна из другой поворотом, считаем одинаковыми. На рисунке 1 изображены все такие ломаные при $n = 20$.)

41. Для любых натуральных чисел m и n докажите равенства:

а) $\varphi(m)\varphi(n) = \varphi(\text{НОК}(m,n))\varphi(\text{НОД}(m,n))$;

б) $\varphi(mn) = \varphi(\text{НОК}(m,n)) \cdot \text{НОД}(m,n)$;

в) $\varphi(m)\varphi(n)\text{НОД}(m,n) = \varphi(mn)\varphi(\text{НОД}(m,n))$.

г) Пусть m и n – натуральные числа, причем $\text{НОД}(m,n) > 1$. Докажите неравенство $\varphi(mn) > \varphi(m)\varphi(n)$.

42. Решите уравнения: а) $\varphi(x) = 18$; б) $\varphi(x) = 12$; в) $x - \varphi(x) = 12$; г*) $\varphi\left(x^2\right) = x^2 - x$; д) $\varphi(x) = x/2$; е) $\varphi(x) = x/3$; ж*) $\varphi(x) = x/n$, где n – натуральное число, $n > 3$; з) $\varphi(nx) = \varphi(x)$, где n – натуральное число, $n > 1$.

Шифры с открытым ключом

На вопрос, что он написал в шифровке, Штирлиц ответил: «Не помню. Теперь это знает только Центр.»

Вообразите, что вам нужно получить зашифрованное сообщение от вашего друга, но вы с ним не договорились заранее, каким шифром будете пользоваться. Как быть? Существует ли такой метод шифрования, что его можно сообщить всему миру (в том числе и вашему другу, и врагам), но это не даст врагам возможности расшифровать сообщение?

Это был бы замечательный шифр: в отличие от старых шифров, где главный секрет – ключ, знание которого позволяет и зашифровывать, и расшифровывать сообщения, новый шифр – «с открытым ключом»: каждый может зашифровывать, но только автор шифра может расшифровать получаемые сообщения.

Шифр RSA

...Так начались необычайные события, которые вовлекли в свой круговорот немало людей.

Е.Велтистов

Скорее всего, шифр с открытым ключом уже изобретен! В 1978 году три математика – Ривест, Шамир и Адлеман – зашифровали некоторую английскую фразу и пообещали награду в 100$ первому, кто расшифрует сообщение

$$y = 96869613754622061477140922254355882905759991124574319874695120930816298225145708356931476622883989628013391990551829945157815154.$$

Они подробно объяснили способ шифрования. Сначала фразу бесхитростно (a = 01, b = 02, c = 03,..., z = 26, пробел = 00) записали в виде последовательности цифр. Получилось некоторое 78-значное число x. Затем взяли 64-значное простое число p и 65-значное простое число q. Перемножили их (не вручную, разумеется, а на компьютере):

$$pq = 114381625757888867669325779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541.$$

Теперь – главное:

$$y \equiv x^{9007} \pmod{pq}.$$

Понимаете? Они опубликовали и произведение pq, и число 9007, и сам метод шифрования (и, разумеется, число y). Было даже сказано, что из чисел p и q одно 64-значное, а другое 65-значное. В секрете остались только сами числа p и q. Требовалось найти x.

Эта история завершилась в 1994 году, когда Аткинс, Крафт, Ленстра и Лейланд расшифровали эту фразу. Числа p и q оказались равны

$$p = 3490529510847650949147849619903898133417764638493387843990820577,$$

$$q = 32769132993266709549961988190834461413177642967992942539798288533.$$

В книге «Введение в криптографию» (М., МЦНМО, 1998 г.) сказано: «Этот замечательный результат (разложение на множители 129-значного числа) был достигнут благодаря использованию алгоритма разложения чисел на множители, называемого методом квадратичного решета. Выполнение вычислений потребовало колоссальных ресурсов. В работе, возглавлявшейся четырьмя авторами проекта и продолжавшейся после предварительной теоретической подготовки примерно 220 дней, на добровольных началах участвовало около 600 человек и примерно 1600 компьютеров, объединенных сетью Internet.»

К сожалению, рассказ о методе квадратичного решета увел бы нас далеко в сторону от основной темы. Потому оставим его до лучших времен, а здесь обсудим основную идею системы RSA (по первым буквам фамилий авторов: Rivest, Shamir, Adleman).

Идея очень красива. Во-первых, зная p и q, можно найти $\varphi(pq) = (p-1)(q-1)$. Во-вторых (и это главное!), если

$$ef = 1 + k\varphi(pq),$$

где e, f, k – натуральные числа, то для любого числа x, взаимно простого с pq, по теореме Эйлера имеем

$$x^{ef} = x \cdot \left(x^k\right)^{\varphi(pq)} \equiv x \cdot 1 = x \pmod{pq}.$$

Вы поняли, что такое e и f? В нашем примере $e = 9007$ (единственное обязательное математическое требование к числу e – его взаимная простота с числом $(p-1)(q-1)$; впрочем, брать $e = 1$ или $e = (p-1)(q-1) - 1$ вряд ли разумно, если хотите сохранить секреты). А число f, как уже было сказано, – решение сравнения

$$ef \equiv 1 \pmod{\varphi(pq)}.$$

(В *Приложении* рассказано, как алгоритм Евклида позволяет решать такие сравнения.)

Сравнения

$$y^f \equiv x^{ef} \equiv x \pmod{pq}$$

показывают, что для нахождения x достаточно найти остаток от деления y^f на pq. (Числа выбраны так, что $x < pq$. При этом x не кратно ни p, ни q. Не подумайте, что это всерьез нас ограничивает: если p и q – большие числа, то вероятность того, что x нацело разделится на p или q, пренебрежимо мала. Кроме того, можно предусмотреть в алгоритме, чтобы в случае чего сообщение x было автоматически как-то так чуть-чуть изменено, без изменения его смысла, что x и pq станут взаимно просты.)

Почему многие надеются, что шифр RSA является шифром с открытым ключом? Да потому, что числа pq и e можно сделать общедоступными. Тогда зашифровать сообщение сможет любой, у кого есть компьютер (и какая-нибудь программа, позволяющая выполнять действия с многозначными числами). Расшифровать сообщение легко, если мы знаем число f. Но единственный известный ныне способ нахождения числа f требует нахождения чисел p и q, т.е. разложения произведения pq на множители. А эффективных алгоритмов решения этой задачи пока нет (удача 1994 года не в счет: если бы в числах p и q было не 64 и 65, а хотя бы по 300 цифр, то и ресурсов сети Internet не хватило бы!). Впрочем, нет сейчас и доказательства того, что никто никогда не научится быстро (математик сказал бы: «за время, полиномиальное от количества цифр») разлагать числа на простые множители.

Приложение

Как возводить в большую степень?

Чтобы возвести число x в 9007-ю степень, по определению, достаточно выполнить 9006 умножений. Но можно обойтись и меньшим числом операций: вычислить x^2, $\left(x^2\right)^2 = x^4$, $\left(x^4\right)^2 = x^8, \ldots, \left(x^{2048}\right)^2 = x^{4096}$, наконец, $\left(x^{4096}\right)^2 = x^{8192}$ и воспользоваться формулой

$$x^{9007} = x \cdot x^2 \cdot x^4 \cdot x^8 \cdot x^{32} \cdot x^{256} \cdot x^{512} \cdot x^{8192},$$

которая основана на том, что в двоичной системе счисления 9007 имеет вид

$$9007_{10} = 10001100101111_2 .$$

Понимаете? Мы разложили 9007 в сумму 1 + 2 + 4 + 8 + 32 + + 256 +512 + 8192 и смогли сильно сэкономить: обошлись 13-ю возведениями в квадрат на первом этапе вычислений и 7-ю умножениями на втором этапе. Всего 20 умножений вместо 9006. Огромная экономия! (Для придирчивого читателя отметим, что выше следовало бы говорить не об умножениях, а об умножениях по модулю pq: дабы количество цифр не росло катастрофически, мы всякий раз должны не только перемножать, но и брать остаток от деления на pq. Но сейчас разговор не об этом.)

Преимущества изложенного метода возведения в степень тем нагляднее, чем больше показатель степени. Например, если показатель степени состоит не из четырех цифр, как 9007, а из нескольких десятков или сотен цифр, то наивный способ не то что утомителен, а неосуществим ни на каких, даже самых мощных, компьютерах. А основанный на двоичной системе – работает и в такой ситуации!

Упражнение 43 (М1086). С числом разрешено производить две операции: «увеличить в 2 раза» и «увеличить на 1». За какое наименьшее число операций можно из числа 0 получить число а) 100; б) 9907; в) n, если в двоичной системе счисления n имеет вид $\overline{a_m a_{m-1} \ldots a_1 a_0}$?

Алгоритм Евклида

Алгоритм Евклида – это способ отыскания наибольшего общего делителя, основанный на формуле

$$\text{НОД}(a,b) = \text{НОД}(a - bq,\ b),$$

которая верна для любых целых чисел a, b, q. (Докажите эту формулу!) Подробно о нем рассказано в статье Н.Васильева «Алгоритм Евклида и основная теорема арифметики» (Приложение к журналу «Квант» № 6 за 1998 год). Собственно говоря, нам нужен даже не алгоритм Евклида, а основанный на нем способ решения линейных уравнений.

Итак, даны два взаимно простых числа e и m (в интересовавшем нас случае $m = \varphi(pq)$, но здесь это не важно). Нужно найти такие числа f и k, что

$$ef = 1 + km.$$

Если бы m было не очень большим, то можно было бы выполнить полный перебор всех m остатков. Но если m большое, то перебор нереален. Оказывается, алгоритм Евклида позволяет быстро решать эту задачу.

Чтобы объяснить, как он работает, рассмотрим пример: $e = 9007$, $m = 19876$. (Мы хотели взять сто-с-лишним-значное число m, но в последний момент струсили.) Уравнение

$$9007f = 1 + 19876k$$

можно записать в виде

$$9007f = 1 + 9007 \cdot 2k + 1862k,$$

т.е.

$$9007(f - 2k) = 1 + 1862k.$$

Обозначим $a = f - 2k$. Тогда

$$9007a = 1 + 1862k.$$

Заметьте: получилось уравнение того же типа, что и исходное, только коэффициенты стали меньше. Теперь следующий шаг:

$$1862 \cdot 4a + 1559a = 1 + 1862k,$$

т.е.

$$1559a = 1 + 1862(k - 4a).$$

Обозначим $k - 4a = b$, тогда

$$1559a = 1 + 1862b.$$

Далее,

$$1559(a - b) = 1 + 303b.$$

Обозначив $a - b = c$, получаем уравнение

$$1559c = 1 + 303b.$$

Дальше – так же:

$$44c = 1 + 303(b - 5c),\quad d = b - 5c,\quad 44c = 1 + 303d;$$

$$44(c - 6d) = 1 + 39d,\quad x = c - 6d,\quad 44x = 1 + 39d;$$

$$5x = 1 + 39(d - x),\quad y = d - x,\quad 5x = 1 + 39y.$$

Машина продолжила бы вычисления дальше, пока коэффициент при одной из неизвестных не стал бы равен 1. А мы остановимся уже здесь: очевидно, $x = 8$, $y = 1$ – одно из решений

(*Окончание см. на с. 37*)

Малая теорема Ферма

(Начало см. на с. 9)

последнего уравнения. Зная x и y, легко находим

$$d = x + y = 9,\ \ c = x + 6d = 62,\ \ b = d + 5c = 319,$$

$$a = b + c = 381,\ \ k = b + 4a = 1843,\ \ f = a + 2k = 4067.$$

Победа! Числа k и f найдены! (Проверка: $9007 \cdot 4067 = 36631469 = 1 + 19876 \cdot 1843$.)

Упражнение 44* (для тех, кто очень любит программировать). а) Найдите число f, которое нашли Аткинс, Крафт, Ленстра и Лейланд. б) Расшифруйте фразу, зашифрованную в 1978 году Ривестом, Шамиром и Адлеманом.

Что дальше?

Что остается от сказки потом,
После того, как ее рассказали?
В.Высоцкий

Подытожим. В первой части статьи мы доказали малую теорему Ферма и ее обобщение – теорему Эйлера. Рассказали о практическом применении теоремы Эйлера в криптографии. Правда, осталось тайной, откуда взялись числа p, q (точнее говоря, как можно конструировать большие – в несколько десятков или сотен цифр – простые числа).

Во второй части мы расскажем об основанных на малой теореме Ферма методах конструирования больших простых чисел. Расскажем и о числах Кармайкла, история которых началась в древности, а существование бесконечного множества которых доказано в 1994 году.

Малую теорему Ферма не обязательно доказывать именно так, как это сделано выше. Во второй части мы изложим другие способы. Один из них приведет к теореме о существовании первообразного корня по простому модулю и далее – к теореме о строении мультипликативной группы вычетов по (не обязательно простому) модулю n.

Чтобы вы лучше оценили силу результатов второй части статьи, подумайте над следующими задачами. Все они будут решены во второй части. Не огорчайтесь даже в том случае, если ни одна из них не получится: это не упражнения, а довольно трудные задачи!

Задачи

1. Существует ли такое составное число n (число Кармайкла), что для любого целого числа a разность $a^n - a$ кратна n?

2. Ни для какого натурального числа n число $2^n + 1$ не кратно $n + 1$. Докажите это.

3. Если $2^n + 1$ кратно n, то $n = 1$ или n кратно 3. Докажите это.

4. Для каких n числа 1, 2,… …, $n - 1$ можно расставить вдоль окружности так, чтобы для любых подряд идущих чисел a, b, c разность $b^2 - ac$ была кратна n? (На рисункае 2 изображен случай $n = 7$.)

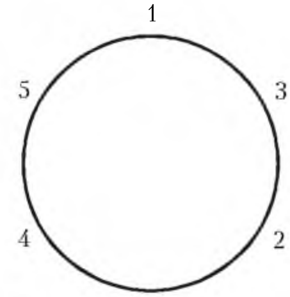


Рис. 2

5. Для каких простых чисел p существует такое целое число a, что $a^4 + a^3 + a^2 + a + 1$ кратно p?

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.

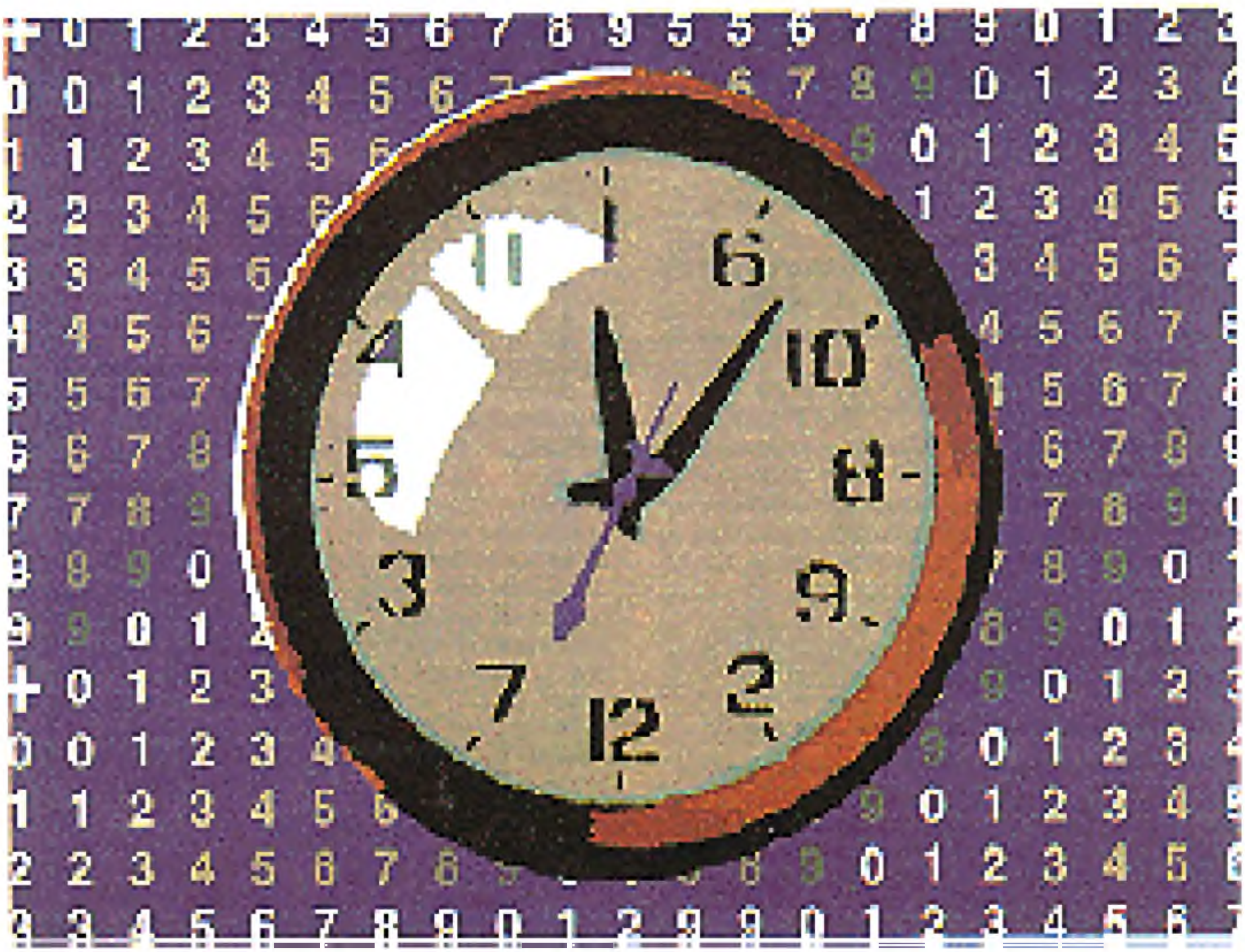


Иллюстрация М.Сумниной

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
$2^n(\mathrm{mod}\,11)$	2	4	8	5	10	9	7	3	6	1	2	4

Дальше можно не продолжать: $2^{10+n} = 2^{10} \cdot 2^n \equiv 1 \cdot 2^n = 2^n (\mathrm{mod}\,11)$, 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, $2^{10} \equiv 1 (\mathrm{mod}\,11)$. 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, $3 \equiv 2^8$, $5 \equiv 2^4$, $7 \equiv 2^7$, $10 \equiv 2^5 (\mathrm{mod}\,11)$.

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

$$a \equiv 2^s (\mathrm{mod}\,11).$$

А сейчас – внимание:

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

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 $a \equiv g^s (\mathrm{mod}\,p)$.

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).

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

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

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

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 $s + t (\mathrm{mod}\,10)$ будет, как мы уже говорили, сопоставлено произведение $2^s \cdot 2^t (\mathrm{mod}\,11)$.

[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 $p = 13$.)

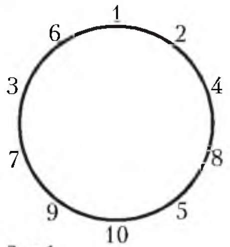


Рис.1

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(mod17)	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: $2^{6972593} - 1$.)

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 $1, a, a^2, \ldots, a^{p-1}$. 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 $a, a^2, \ldots, a^k (\equiv 1)$ 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.)

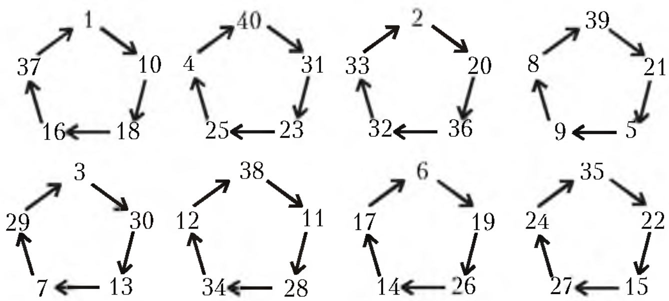


Рис.2

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

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

числа n в произведение степеней различных простых множителей. Обозначим через $f(n)$ наименьшее общее кратное чисел $\varphi\left(p_i^{m_i}\right)$, где $i = 1, 2, \ldots, s$. (Например, $f(360)$=НОК$\left[\varphi(2^3), \varphi(3^2), \varphi(5)\right]$ = 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 $i = 1, 2, \ldots, s$; 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: $\lambda(mn)$ = 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 = 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 $m \geq 3$, $\lambda(p^m) = p^{m-1}(p-1)$ 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, $p \neq 2$, 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 $2^n \equiv -1 \pmod{n}$ имеем $2^n \equiv$ $\equiv -1 \pmod{3}$, откуда $\left(2^n\right)^2-2^n+1 \equiv (-1)^2-(-1)+1 \equiv$ $\equiv 0 \pmod{3}$.)

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

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

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

Малая теорема Ферма

В. СЕНДЕРОВ, А. СПИВАК

Напоминание

Малая теорема Ферма гласит: *если a – целое число, не делящееся на простое число p, то $a^{p-1}-1$ делится на p.*

Функция Эйлера $\varphi(n)$ – это количество натуральных чисел от 1 до n, взаимно простых с n.

Функция Кармайкла $\lambda(n)$ – это такое наименьшее натуральное число k, что для всякого целого числа a, взаимно простого с натуральным числом n, разность a^k-1 делится на n.

Число g называют *первообразным корнем по модулю n*, если для всякого целого a, взаимно простого с n, существует такое натуральное число m, что $g^m \equiv a \pmod n$.

Подробно об этих и многих других понятиях и теоремах арифметики можно прочитать в предыдущих частях статьи. Там не было доказано существование первообразного корня по простому модулю. Пришла пора это сделать.

Первообразные корни

Первообразные корни по модулю 11

Число 2 – первообразный корень по модулю 11. Какие еще есть первообразные корни по этому модулю?

Для ответа не нужно перебирать все числа 3, 4, 5, …, 9, 10 и составлять для каждого из них таблицу. Некоторые степени двойки можно сразу отбросить:

$$\left(2^2\right)^5 = 2^{10} \equiv 1,$$

$$\left(2^4\right)^5 = 2^{20} \equiv 1,$$

$$\left(2^5\right)^2 \equiv 1,$$

$$\left(2^6\right)^5 \equiv 1,$$

$$\left(2^8\right)^5 \equiv 1 \pmod{11}.$$

А вот степени двойки $2^1 \equiv 2$, $2^3 \equiv 8$, $2^7 \equiv 7$ и $2^9 \equiv 6$, показатели которых взаимно просты с 10, являются первообразными корнями. (Обдумайте это!)

И вообще, если g – первообразный корень по простому модулю p, то g^s является первообразным корнем в том и только том случае, когда s и $p-1$ взаимно просты.

Упражнения

44. Докажите это.

45. Для того чтобы число a было первообразным корнем по простому модулю p, необходимо и достаточно, чтобы a не делилось на p и ни для какого простого делителя q числа $p-1$ разность $a^{(p-1)/q}-1$ не делилась бы на p. Докажите это.

46. Найдите наименьшее натуральное число, являющееся первообразным корнем по модулю а) 23; б) 41; в) 257.

47. а) Проверьте, что 2 не является первообразным корнем по модулю 263, а -2 является.

б) Пусть a^3-a не делится на 83. Докажите, что ровно одно из чисел a и $-a$ является первообразным корнем по модулю 83.

48. а) Пусть p – простое число, $p \equiv 1 \pmod 4$. Докажите, что число $-a$ является первообразным корнем по модулю p тогда и только тогда, когда само число a – первообразный корень по модулю p.

б) Пусть p – простое число, $p \equiv 3 \pmod 4$. Докажите, что число a является первообразным корнем по модулю p тогда и только тогда, когда порядок числа $-a$ по модулю p равен $(p-1)/2$.

Порядки классов вычетов

В таблице 5 для каждого ненулевого остатка $a \pmod{11}$ указан его порядок k.

Как и должно быть, порядки – делители числа 10. Давайте посчитаем, сколько раз в нижней строке таблицы 5 встречаются числа 1, 2, 5 и 10. Ответы запишем в виде таблицы 6.

Таблица 5

a	1	2	3	4	5	6	7	8	9	10
k	1	10	5	5	5	10	10	10	5	2

Таблица 6

Порядок	1	2	5	10
Встречается	1	1	4	4

Видна закономерность? Если нет, посмотрите на таблицу 7, составленную для $p = 13$.

Таблица 7

a	1	2	3	4	5	6
k	1	12	3	6	4	12
a	7	8	9	10	11	12
k	12	4	3	6	12	2

В ней порядки – делители числа 12. Посчитаем, сколько раз встречаются в нижней строке таблицы 7 числа 1, 2, 3, 4, 6 и 12 (табл.8).

Таблица 8

Порядок	1	2	3	4	6	12
Встречается	1	1	2	2	2	4

Если вы все еще не догадались, составьте такие таблицы для нескольких других простых чисел p, и рано или поздно увидите, что в нижних строках этих таблиц – значения функции Эйлера: $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$, $\varphi(10)=4$, $\varphi(12)=4$.

Великий немецкий математик К.Ф.Гаусс (1777 – 1855) в «Арифметических исследованиях», опубликованных в 1801 году, доказал, что это не случайность, а общий закон.

Теорема 4. *Среди $p-1$ ненулевых классов вычетов по простому модулю p порядок k, где k – делитель числа $p-1$, имеют ровно $\varphi(k)$ классов вычетов. (В частности, для любого простого числа p существует $\varphi(p-1)$ первообразных корней по модулю p.)*

Для доказательства теоремы 4 мы используем теорему Безу и одно интересное свойство функции Эйлера.

Теорема Безу

Для тех, кто знаком с делением многочленов с остатком, теорему Безу[1] можно сформулировать и до-

Окончание. Начало см. в «Кванте» №1, 3.

[1] *Этьен Безу (1730–1783) – французский математик.*

казать очень коротко. В равенство

$$f(x)=(x-a)g(x)+r,$$

где $g(x)$ – многочлен (неполное частное), а r – число (остаток), можно подставить вместо x число a. Получим

$$f(a)=(a-a)g(a)+r=r.$$

Значит, остаток r от деления $f(x)$ на $x-a$ равен $f(a)$. Это и есть теорема Безу.

А для остальных читателей теорему Безу можно сформулировать и доказать чуть более длинным, но не менее естественным способом.

Теорема 5. *Число a является корнем многочлена f(x) в том и только том случае, когда f(x) делится на x − a, т.е. когда*

$$f(x)=(x-a)g(x),$$

где g – некоторый многочлен.

Доказательство. Если

$$f(x)=(x-a)g(x),$$

то

$$f(a)=(a-a)g(a)=0.$$

Обратно, пусть $f(a)=0$. Подставим в многочлен

$$f(x)=k_nx^n+k_{n-1}x^{n-1}+\ldots$$
$$\ldots+k_2x^2+k_1x+k_0$$

число a. Получим

$$0=f(a)=k_na^n+k_{n-1}a^{n-1}+\ldots$$
$$\ldots+k_2a^2+k_1a+k_0.$$

Следовательно,

$$f(x)=f(x)-f(a)=$$
$$=k_n\left(x^n-a^n\right)+k_{n-1}\left(x^{n-1}-a^{n-1}\right)+\ldots$$
$$\ldots+k_2\left(x^2-a^2\right)+k_1(x-a).$$

Каждая из разностей

$x-a$,

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

…

$x^n-a^n=$

$=(x-a)\left(x^{n-1}+x^{n-2}a+\ldots+xa^{n-2}+a^{n-1}\right)$

кратна $x-a$. Теорема доказана.

Переформулировка малой теоремы Ферма

Из теоремы Безу следует, что если $a_1, a_2, \ldots, a_m$ – различные корни многочлена $f(x)$, то $f(x)=(x-a_1)(x-a_2)\ldots(x-a_m)g(x)$, где g – некоторый многочлен.

Применив это соображение к многочлену $x^{p-1}-1$, получим замечательную переформулировку малой теоремы Ферма:

$$x^{p-1}-1\equiv(x-1)(x-2)\ldots(x-p+1),$$

где знак сравнения означает, что если раскрыть все скобки в правой части и вычесть из нее левую, то получим многочлен, коэффициенты которого кратны p. Как вы помните, для частных случаев $p = 2, 3, 5, 7$ и 11 это разложение на множители встречалось в первой части статьи.

Упражнение 49. Подставив $x = 0$, докажите теорему Вильсона: $(p-1)!\equiv-1 \pmod p$ для любого простого числа p.

Сравнение $x^k\equiv 1 \pmod p$

Если k – делитель числа $p-1$, т.е. $p-1=km$, то

$$x^{p-1}-1=$$
$$=\left(x^k-1\right)\left(x^{k(m-1)}+x^{k(m-2)}+\ldots+x^k+1\right).$$

Значит, многочлен x^k-1 является делителем многочлена $x^{p-1}-1$. Поскольку $x^{p-1}-1$ разлагается в произведение многочленов первой степени, то его делитель x^k-1 является произведением k многочленов первой степени.

Немного подумав, можно сообразить, что мы доказали следующее утверждение.

Теорема 6. *Если p – простое число, k – делитель числа p − 1, то сравнению $x^k\equiv 1 \pmod p$ удовлетворяют ровно k классов вычетов по модулю p.*

Упражнения

50. Решите сравнения

а) $x^4\equiv 1 \pmod{13}$; б) $x^{1604}\equiv 1 \pmod{17}$.

(*Указание.* 2 и 3 – первообразные корни, соответственно, по модулю 13 и по модулю 17.)

51. Зная, что 2 – первообразный корень по модулю 29, решите сравнение

$$x^6+x^5+x^4+x^3+x^2+x+1\equiv 0 \pmod{29}.$$

52. Пусть p – простое число. При каких k сумма $1^k+2^k+\ldots+(p-1)^k$ кратна p?

53. а) Сколько существует таких пар (a,b) натуральных чисел, что $a,b\le 1717$ и a^8+b^8 кратно 17?

б) Сколько существует таких троек (a,b,c) натуральных чисел, что $a,b,c\le 289$ и $a^{1000}+b^{3000}+c^{9000}$ кратно 17?

Сумма значений функции Эйлера

Рассмотрим 100 дробей: $1/100$, $2/100$, …, $100/100$. Если каждую из них привести к несократимому виду, то получим $\varphi(100)=40$ дробей со знаменателем 100, $\varphi(50)=20$ дробей со знаменателем 50, и так далее: для каждого делителя d числа 100 получим $\varphi(d)$ дробей со знаменателем d. (Почему? Потому что $\varphi(d)$ – это количество несократимых правильных дробей со знаменателем d.)

Мы получили замечательное равенство:

$$100=\varphi(100)+\varphi(50)+\varphi(25)+\varphi(20)+$$
$$+\varphi(10)+\varphi(5)+\varphi(4)+\varphi(2)+\varphi(1).$$ [2]

Если бы мы рассмотрели не дроби со знаменателем 100, а дроби со знаменателем n, то точно так же доказали бы следующее утверждение.

Теорема 7. *Для любого натурального числа n сумма значений функции Эйлера $\varphi(d)$ по всем делителям d числа n равна n.*

Упражнения

54. Если d – делитель числа n, то существует ровно $\varphi(n/d)$ таких натуральных чисел k, что $k\le n$ и НОД$(k,n)=d$. Докажите это.

55. Пусть $n>1$. Найдите сумму всех несократимых правильных дробей, знаменатели которых равны n.

Доказательство теоремы 4

Мы должны доказать, что если k – делитель числа $p-1$, то среди ненулевых классов вычетов по простому модулю p существует ровно $\varphi(k)$ классов порядка k.

Применим индукцию. *База.* Для $k = 1$ утверждение верно.

Переход. Рассмотрим некоторый делитель k числа $p-1$. Предположим, что для любого делителя d числа k, где $d<k$, существует ровно $\varphi(d)$ классов вычетов порядка d. Найдем количество классов вычетов порядка k.

В силу теоремы 6, сравнению $x^k\equiv 1 \pmod p$ удовлетворяют ровно k классов вычетов. Каждое решение x этого сравнения имеет некоторый

[2] *Для Фомы неверующего: 40 + 20 + + 20 + 8 + 4 + 4 + 2 + 1 + 1 = 100.*

порядок по модулю p, причем этот порядок – делитель числа k. Осталось вспомнить теорему 7 – и становится ясно, что классов порядка k существует ровно $\varphi(k)$ штук. Теорема 4 доказана.

Упражнения

56. Пусть p – простое число, $p > 3$. Найдите остаток от деления на p произведения тех из чисел 1, 2, ..., $p - 1$, которые являются первообразными корнями по модулю p.

57. а) Если порядки чисел a и b по модулю p равны m и n соответственно, то порядок произведения ab – делитель числа НОК$[m, n]$. Докажите это.

б) Покажите, что порядок числа ab равен mn, если числа m и n взаимно просты, и не обязательно равен числу НОК$[m, n]$, если m и n не взаимно просты.

58. а) Пусть p – простое число, $p > 2$, $p - 1 = q_1^{a_1} q_2^{a_2} \ldots q_s^{a_s}$ – разложение числа $p - 1$ в произведение степеней различных простых чисел. Пусть $g_1, g_2, \ldots, g_s$ – такие не кратные p числа, что $g_i^{(p-1)/q_i} \not\equiv 1 \pmod p$ при $i = 1, 2, \ldots, s$. Докажите, что число $g = g_1^{(p-1)/q_1^{a_1}} g_2^{(p-1)/q_2^{a_2}} \ldots g_s^{(p-1)/q_s^{a_s}}$ – первообразный корень по модулю p. (Заметьте: мы получили еще одно доказательство существования первообразного корня по простому модулю!)

б) Для любого натурального n существует взаимно простое с n целое число a, порядок которого по модулю n равен $\lambda(n)$. Докажите это.

в) Если $n = 2, 4, p^m$ или $2p^m$, где p – нечетное простое, m – натуральное, то существует первообразный корень по модулю n. Докажите это.

Гипотеза Артина

Как мы только что доказали, для каждого простого числа p существует первообразный корень по модулю p. Интересно: какие целые числа бывают первообразными корнями, а какие не бывают?

Очевидно, -1 является первообразным корнем только по модулю 2 или 3. Далее, из равенства $\left(a^2\right)^{(p-1)/2} = a^{p-1}$ следует, что точный квадрат не может быть первообразным корнем ни по какому нечетному простому модулю p.

Немецкий алгебраист Эмиль Артин (1898–1962) предположил, что для любого целого числа $g \neq -1$, не являющегося квадратом целого числа, существует бесконечно много таких простых p, что g – первообразный корень по модулю p.

Более того, некоторые вероятностные соображения привели Артина к следующему уточнению его гипотезы: если k есть наибольшее такое число, что g является k-й степенью, то отношение количества $\pi_g(n)$ простых чисел, не превосходящих n, по модулю которых g является первообразным корнем, к количеству $\pi(n)$ всех простых чисел, не превосходящих n, стремится при $n \to \infty$ к зависящему только от k пределу

$$\lim_{n\to\infty} \frac{\pi_g(n)}{\pi(n)} = \prod_{k:q}\left(1 - \frac{1}{q-1}\right) \cdot \prod_{k \text{ не } :q}\left(1 - \frac{1}{q(q-1)}\right),$$

где первое произведение распространено на все простые числа q, являющиеся делителями k, а второе – на все простые числа q, не являющиеся делителями k.

К настоящему времени гипотеза Артина не доказана, хотя некоторый ее аналог, относящийся к полю рациональных функций от одной переменной над конечным полем, доказать удалось.

Числа Кармайкла

В силу малой теоремы Ферма, $2^{p-1} \equiv 1 \pmod p$ для любого нечетного простого числа p. Существуют ли составные числа с тем же свойством? Да, существуют:

$$2^{340} \equiv 1 \pmod{341}.$$

В самом деле, $341 = 11 \cdot 31$, причем $2^{10} - 1 = 1023 = 3 \cdot 11 \cdot 31$. (Можно проверить, что число 341 – наименьшее составное число n со свойством $2^{n-1} \equiv 1 \pmod n$.)

Упражнение 59. а) Если $n = \left(4^p - 1\right)/3$, где p – простое число, $p > 3$, то $2^{n-1} \equiv 1 \pmod n$. Докажите это.

б) (М672) Пусть a – такое натуральное число, что $2^a - 2$ кратно a (например, $a = 3$). Определим последовательность $x_1, x_2, x_3, \ldots$ условиями $x_1 = a$, $x_{n+1} = 2^{x_n} - 1$. Докажите, что $2^{x_n} - 2$ кратно x_n при любом n.

Но почему мы заинтересовались именно случаем $a = 2$? Наверное, разумнее спросить: существуют ли такие составные числа n, что для любого a, взаимно простого с n, выполнено сравнение $a^{n-1} \equiv 1 \pmod n$? Такие числа тоже существуют! Их называют *числами Кармайкла*. Наименьшее число – это

$$561 = 3 \cdot 11 \cdot 17,$$

за ним идут

$$1105 = 5 \cdot 13 \cdot 17,\ 1729 = 7 \cdot 13 \cdot 19,$$
$$2465 = 5 \cdot 17 \cdot 29,\ 2821 = 7 \cdot 13 \cdot 31,$$
$$6601 = 7 \cdot 23 \cdot 41,\ 8911 = 7 \cdot 19 \cdot 67,$$
$$10585 = 5 \cdot 29 \cdot 73,\ 15841 = 7 \cdot 31 \cdot 73,$$
$$29341 = 13 \cdot 37 \cdot 61,$$
$$41041 = 7 \cdot 11 \cdot 13 \cdot 41, \ldots$$

В 1994 году в журнале Annals of Mathematics (т. 139, с. 703–722) три математика – Альфорд, Гренвилль и Померанц – опубликовали (абсолютно недоступное для школьника) доказательство бесконечности множества чисел Кармайкла.

Упражнение 60. а) Докажите, что $a^{561} - a$ кратно числу 561 при любом целом a.

б) Докажите при $n = 1105$ сравнения $2^{n-1} \equiv 1 \equiv 3^{n-1} \pmod n$. (Можно доказать, что число 1105 – наименьшее составное число с таким свойством.)

Очевидно, составное число n является числом Кармайкла тогда и только тогда, когда $n - 1$ делится на $\lambda(n)$.

Теорема 8. *Составное число* $n = p_1^{m_1} p_2^{m_2} \cdot \ldots \cdot p_s^{m_s}$, *где* $p_1, p_2, \ldots, p_s$ – *различные простые числа,* $m_1, m_2, \ldots, m_s$ – *натуральные числа, является числом Кармайкла в том и только том случае, когда* $m_1 = m_2 = \ldots = m_s = 1$ *и* $n - 1$ *кратно каждому из чисел* $p_1 - 1$, $p_2 - 1$, ..., $p_s - 1$.

Следствие. *Если* n – *число Кармайкла, то для любого целого числа* a *верно сравнение* $a^n \equiv a \pmod n$.

Доказательство теоремы 8. Пусть n – число Кармайкла. Поскольку при $n > 2$ значение функции Кармайкла $\lambda(n)$ четно, то $n - 1$ должно быть четным. Следовательно, n нечетно.

Поскольку $\lambda(n)$ делится на $\lambda\left(p_i^{m_i}\right) = p_i^{m_i - 1}\left(p_i - 1\right)$, а $n - 1$ не делится на p_i, то в случае $m_i > 1$ получаем противоречие. Следовательно, $m_1 = m_2 = \ldots = m_s = 1$. Завершение доказательства теоремы 8 предоставляем читателю.

Упражнения

61. а) Докажите, что $2^{161038} \equiv 2 \pmod{161038}$. (При помощи компьютера легко проверить, что $n = 161038 = 2 \cdot 73 \cdot 1103$ – наименьшее четное составное число, для которого $2^n \equiv 2 \pmod n$. Следующее такое четное число $215326 = 2 \cdot 23 \cdot 31 \cdot 151$.)

б) Для любого целого числа $a \neq -1$ существует такое четное число $n > 2$, что $a^n \equiv a \pmod n$. Докажите это.

в*) Для любого натурального числа a существует бесконечно много таких четных чисел n, что $a^n \equiv a \pmod n$. Докажите это. (*Указание.* Используйте теорему Биркгофа–Вандивера, сформулированную в упражнении 32.)

62. а) Пусть $n = 3^m - 2^m$. Докажите, что если $n - 1$ кратно m, то число $3^{n-1} - 2^{n-1}$ кратно n.

б) Существует ли составное число n, для которого $3^{n-1} - 2^{n-1}$ кратно n?

в) (М1510) Докажите, что существует бесконечно много таких составных чисел n, что $3^{n-1}-2^{n-1}$ кратно n.

63. Докажите, что если n – составное число и $1^{n-1}+2^{n-1}+\ldots+(n-1)^{n-1}\equiv -1\pmod n$, то n – число Кармайкла. (Воспользовавшись списком чисел Кармайкла, не превосходящих 10^{16}, можно при помощи компьютера проверить, что не существует ни одного удовлетворяющего этому сравнению числа, не превосходящего 10^{16}. Существуют ли такие числа, большие 10^{16}, мы не знаем.)

Приложения

Бином Ньютона

Малую теорему Ферма легко доказать по индукции, если использовать формулу бинома Ньютона. Мы сделаем это для натуральных чисел a, оставив случай отрицательных чисел читателю.

Пусть сначала $p=3$. *База индукции*: $1^3-1=0$ делится на 3. *Переход*: если для некоторого числа a уже доказали, что a^3-a кратно 3, то

$$(a+1)^3-(a+1)=$$
$$=a^3+3a^2+3a+1-(a+1)\equiv$$
$$\equiv a^3+1-a-1=a^3-a\equiv 0\pmod 3.$$

Аналогично для $p=5$: база очевидна $\left(1^5-1\equiv 0\pmod 5\right)$, а для перехода используем формулу

$$(a+1)^5=a^5+5a^4+10a^3+10a^2+5a+1.$$

Видите, коэффициенты при a^4, a^3, a^2 и a кратны 5. Поэтому

$$(a+1)^5\equiv a^5+1\pmod 5,$$

откуда и следует возможность индукционного перехода:

$$(a+1)^5-(a+1)\equiv$$
$$\equiv a^5+1-a-1=a^5-a\pmod 5.$$

Упражнение 64. Докажите индукцией по a малую теорему Ферма для а) $p=2$; б) $p=7$.

Займемся общим случаем. Формула бинома имеет вид

$$(a+1)^p=a^p+pa^{p-1}+\frac{p(p-1)}{2}a^{p-2}+$$
$$+\frac{p(p-1)(p-2)}{3!}a^{p-3}+\ldots$$
$$\ldots+\frac{p(p-1)}{2}a^2+pa+1.$$

Коэффициенты

$$C_p^1=p,\ C_p^2=p(p-1)/2,\ \ldots$$
$$\ldots C_p^k=p(p-1)\ldots(p-k+1)/k!,\ldots$$
$$\ldots C_p^{p-1}=p$$

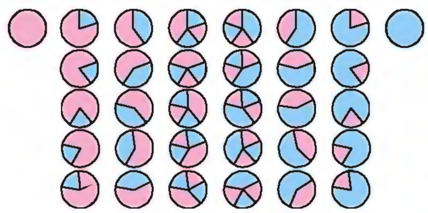
кратны простому числу p. Поэтому $(a+1)^p\equiv a^p+1\pmod p$, что и требовалось:

$$(a+1)^p-(a+1)\equiv$$
$$\equiv a^p+1-a-1=a^p-a\pmod p.$$

Упражнение 65. Если n составное, то хотя бы один из биномиальных коэффициентов C_n^{n-2}, C_n^2, …, C_n^k, …, C_n^{n-1} не кратен n. Докажите это.

Комбинаторное доказательство

На рисунке изображены все 32 способа раскраски в два цвета круга, который разделен на 5 равных секторов. Среди



них выделяются два способа – когда весь круг синий и когда он весь красный. А остальные разбиты на 6 групп по 5 раскрасок, получающихся одна из другой поворотом.

Задача. Сколькими способами можно раскрасить a разными красками круг, разбитый на p одинаковых секторов, где p – простое число? (Каждый сектор окрашивается одной краской; не обязательно использовать все краски; две раскраски, совпадающие при повороте круга, считаются одинаковыми.)

Решение. Очевидно, можно все секторы покрасить одной краской. Таких способов столько же, сколько красок, т.е. a способов.

А вот из любой другой раскраски поворотами можно получить p разных раскрасок (считая и саму эту раскраску: она получается поворотом на 0°). Значит, ответ таков:

$$a+\frac{a^p-a}{p}.$$

Поскольку количество способов не бывает дробным, число a^p-a обязано нацело делиться на p.

Упражнение 66. Сколькими способами можно раскрасить a разными красками круг, разбитый а) на p^2 секторов, где p – простое число? б) на pq секторов, где p, q – простые числа, $p\neq q$? (Каждый сектор окрашиваем одной краской; не обязательно использовать все краски; две раскраски, совпадающие при повороте круга, считаем одинаковыми.)

Как строят большие простые числа?

Как помнит читатель первой части статьи, для криптографической системы RSA нужны большие (лучше всего – длиной в несколько сот цифр) простые числа. Наиболее эффективным средством построения таких чисел сейчас является метод, основанный на следующей лемме.

Лемма. *Пусть q – нечетное простое число, r – четное натуральное, $n=qr+1$. Если существует такое целое число a, что $a^{n-1}\equiv 1\pmod n$ и НОД$\left(a^r-1,n\right)=1$, то каждый простой делитель p числа n удовлетворяет сравнению $p\equiv 1\pmod{2q}$.*

Доказательство. Обозначим порядок числа a по модулю p буквой k. Поскольку $a^{n-1}\equiv 1\pmod p$ и $a^{(n-1)/q}\not\equiv 1\pmod p$, то k делится на q. В силу теоремы 3, $p-1$ делится на k. Следовательно, $p-1$ делится на q. Кроме того, $p-1$ четно. Лемма доказана.

Следствие. *Если выполнены условия леммы и $r\le 4q+2$, то n – простое число.*

Доказательство. Пусть n равняется произведению не менее чем двух простых чисел. Поскольку каждое из них не меньше $2q+1$, получаем противоречие:

$$(2q+1)^2\le n=qr+1\le 4q^2+2q+1.$$

Покажем теперь, как, имея большое простое число q, можно пытаться строить существенно большее простое число n. Выберем случайным образом четное число r на промежутке $q<r\le 4q+2$ и положим $n=qr+1$. Затем проверим n на отсутствие малых простых делителей, перепробовав малые простые числа.[3] Если при этом выяснится, что n – составное, то следует выбрать новое значение r и повторить вычисления.

Если же есть надежда, что n простое, то можно случайным образом выбрать число a и проверить, выполнены ли для него соотношения $a^{n-1}\equiv 1\pmod n$ и НОД$\left(a^r-1,n\right)=1$. Если выполнены, то можно утверждать, что n простое (заметьте: $n>q^2$, так что число n записывается примерно вдвое большим количеством цифр, чем q). Если же нет, то можно взять другое значение a, и так далее.

В настоящий момент нет доказательства того, что этот алгоритм сработает и тем более – что он сработает достаточно быстро. Однако на практике он позволяет строить большие (порядка 10^{300}) простые числа.

[3] *В этом месте мы чуть лукавим: следует не только делить на малые простые числа, но и применять более хитрые методы проверки на простоту. Хотя эти методы основаны на малой теореме Ферма и по сути сводятся к тому, что если для некоторого a, взаимно простого с n, число a^{n-1} не сравнимо с 1 по модулю n, то n составное, подробное обсуждение завело бы нас слишком далеко в бурно развивающуюся область теории чисел и вычислительной математики.*