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.

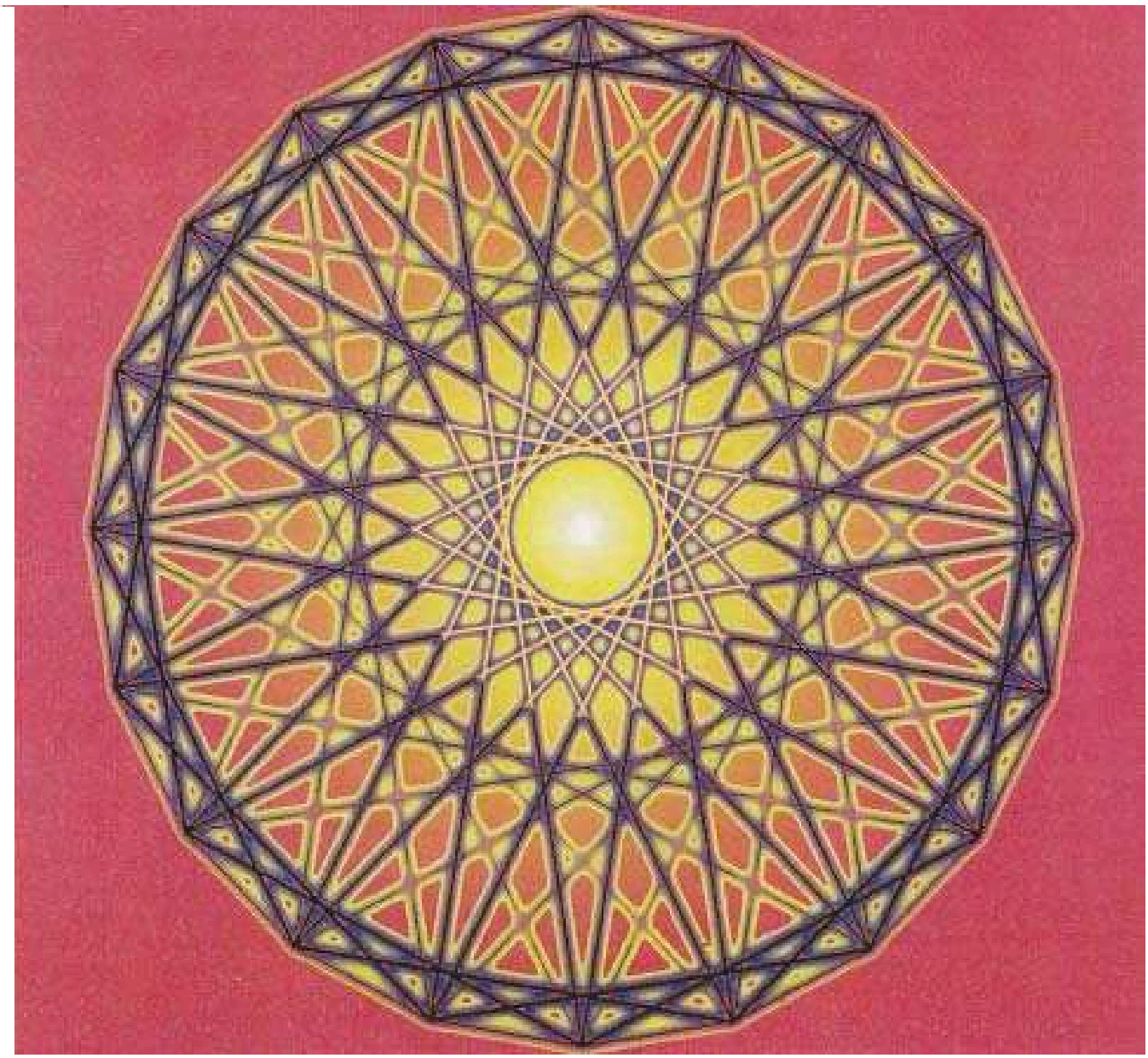

Иллюстрация В.Хлебниковой

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 $a = \pm 1$ и при $a = 0$ получаем ноль. Смотрим дальше: $2^5 - 2 = 30$, $3^5 - 3 = 240$, $4^5 - 4 = 1020$, $5^5 - 5 = 3120$, $6^5 - 6 = 7770$,... Все эти значения кратны числу 30.

Поскольку $30 = 2 \cdot 3 \cdot 5$, 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:

$$6 \equiv 36 \pmod{10},$$

но

$$1 \not\equiv 6 \pmod{10}.$$

Упражнения

2. Решите сравнение $3x \equiv 11 \pmod{101}$.

3. Какие целые числа x удовлетворяют сравнению $14x \equiv 0 \pmod{12}$?

4. Пусть $k \neq 0$. 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: $0^7 - 0 = 0$, $1^7 - 1 = 0$, $2^7 - 2 = 126 = 7 \cdot 18$,..., $6^7 - 6 = 279930 = 7 \cdot 39990$. (Можно и чуточку сэкономить: поскольку любое целое число представимо в виде $a = 7b$, $7b \pm 1$, $7b \pm 2$ или $7b \pm 3$, 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 $a^7 - a$ равен 42; б) наибольший общий делитель чисел вида $a^9 - a$ равен 30. (Заметьте: 30 не кратно 9. Это находится в согласии с тем, что число 9 не простое, а составное.)

Теперь рассмотрим число $p = 11$. 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 $p = 13$, если действовать нашим способом, придется возводить в двенадцатую степень числа от 1 до 12 или раскрывать скобки в произведении тринадцати множителей: $a-6$, $a-5$,..., $a+5$, $a+6$. 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 $m^5n - mn^5$ 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 $a^n - a$, 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

Таблица 1

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

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.*

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 $ka_1, ka_2, \ldots, ka_r$ 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 $7^{7^{7^{7}}} - 7^{7^{7}}$ 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, …, $p^m - 1$. Из них кратны p в точности остатки 0, p, $2p$,…, $p^m - p$. 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 $2\cdot3 = 6$, а также 30 чисел, кратных $2\cdot5 = 10$, и 20 чисел, кратных $3\cdot5 = 15$. Но и этого недостаточно: каждое из десяти чисел, кратных $2\cdot3\cdot5 = 30$, 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,..., p_s – различные простые числа, a_1, a_2,..., 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

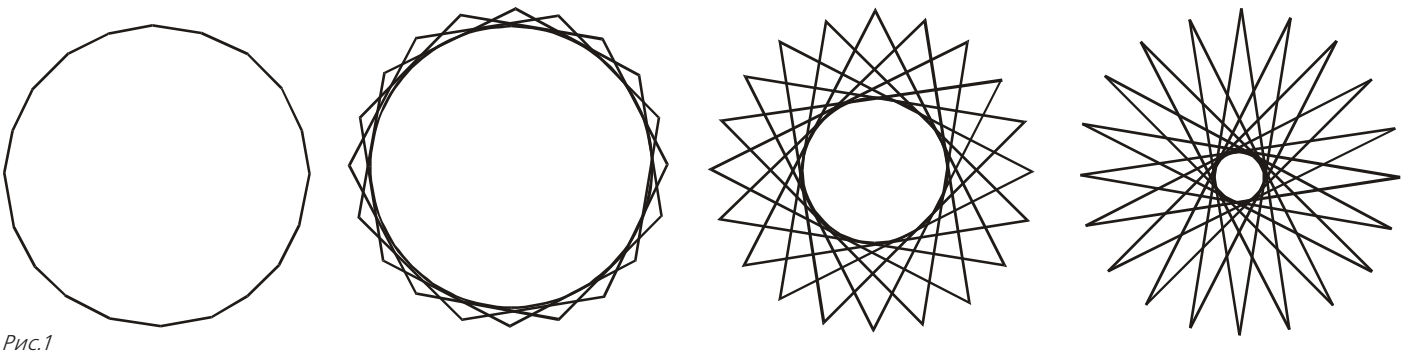

Рис.1

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

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

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

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

$$y = 9686961375462206147714092225435588290575999112457431987469512093081629822514570835693147662288398962801339199055182994515781515 4.$$

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

$$p = 3490529510847650949147849619903898133417764638493387843990820577,$$

$$q = 3276913299326670954996198819083446141317764296799294253979828853 3.$$

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, $\left(x^2\right)^2 = x^4$, $\left(x^4\right)^2 = x^8$,..., $\left(x^{2048}\right)^2 = x^{4096}$, 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:

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

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

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

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

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

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

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 $1, 2, \ldots, n-1$ можно расставить вдоль окружности так, чтобы для любых подряд идущих чисел a, b, c разность $b^2 - ac$ была кратна n? (На рисунке 2 изображен случай $n = 7$.)

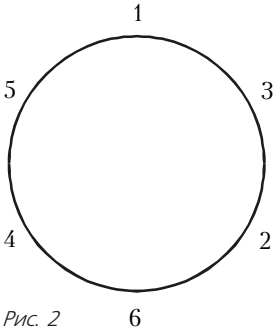

Рис. 2

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