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 $1, 2, 3, \ldots, p - 1$, 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

a	1	2	3	4	5	6	7	8	9
4a	4	8	12	16	20	24	28	32	36
4a 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
4a 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 $1, 2, 3, \ldots, p - 1$, 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 $k^p - k = k\left(k^{p-1} - 1\right)$