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

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

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).

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

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