Занятие 6

Если не оговорено противное, в этой теме слово «число» означает целое число.

Целое число a *делится* на целое число b, если существует целое число k, т. ч. $a = bk$. Также в этом случае говорят, что a *кратно* b, b *делит* a и b есть *делитель* числа a. Пишут $b \mid a$. Отметим, что не всякое a, кратное b, можно поделить на b: 0 делится на любое целое число, в том числе на 0 (подойдет любое k), хотя деление на 0 не имеет смысла (именно потому, что «частное» определено не однозначно).

Задача 6.1. Известно, что a, b, c, d — положительные целые числа, $ab = cd$ и a делится на c. Докажите, что d делится на b.

Решение. Имеем $a = ck$ для некоторого k. Тогда $cd = ab = ckb$, откуда, с учетом $c \neq 0$, получаем $d = kb$, т. е. $b \mid d$. □

Теорема 1 (деление с остатком; разд. 4.3 Учебника)**.** *Для любых целых чисел a и $b \neq 0$ существует единственная пара целых чисел q и r, т. ч.*

$$a = bq + r \quad и \quad 0 \leqslant r < |b|.$$

Такое число q называется *(неполным) частным*, а r *остатком* при делении числа a на число b. Если $r = 0$, то говорят, что a *делится* на b *без остатка.*

Задача 6.2. При делении некоторого целого числа m на 13 и 15 получили одинаковые частные, но первое деление было с остатком 8, а второе без остатка. Найдите число m.

Решение. По условию, $m = 13q + 8$ и $m = 15q$ для некоторого q. Тогда, очевидно, $q = 4$ и $m = 60$. □

Пусть $m > 0$. Говорят, что числа a и b *сравнимы по модулю* m, если $m \mid (a - b)$. В этом случае пишут $a \equiv b \pmod{m}$. Очевидно, что сравнимость по данному модулю рефлексивна, симметрична и транзитивна: $a \equiv a \pmod{m}$; если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$; если $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.

Это делает осмысленными цепочки сравнений: запись $a_1 \equiv a_2 \equiv \ldots \equiv a_k \pmod{m}$ означает, что при любых $i, j \leqslant k$ числа a_i и a_j сравнимы по модулю m.

Лемма 2. *Для любых a, b и $m > 0$, $a \equiv b \pmod{m}$ тогда и только тогда, когда остатки при делении a и b на m одинаковы.*

Доказательство. Допустим, что $a - b = km$, $a = q_1 m + r_1$ и $b = q_2 m + r_2$, причем $0 \leqslant r_1 < m$ и $0 \leqslant r_2 < m$. Имеем

$$a = b + km = (q_2 + k)m + r_2$$

Однако остаток при делении a на m определен однозначно, так что $r_2 = r_1$. Обратно, пусть $a = q_1 m + r$ и $b = q_2 m + r$. Тогда $a - b = (q_1 - q_2)m$. □

Очевидно также, что любое число a сравнимо по модулю $m > 0$ с своим остатком при делении на m.

Лемма 3. *Пусть для некоторых чисел a, b, c, d и $m > 0$ верно $a \equiv b \pmod m$ и $c \equiv d \pmod m$. Тогда*

1. $a + c \equiv b + d \pmod m$;
2. $ac \equiv bd \pmod m$;
3. $a^n \equiv b^n \pmod m$ *для всех целых неотрицательных n.*

Доказательство. Проверим, например, второе утверждение (из которого легко следует третье). Итак, $a = b + km$ и $c = d + lm$ для каких-то k и l. Но тогда $ac - bd = bd + blm + kmd + klm^2 - bd = (bl + kd + klm)m$. □

Как видим, сравнения по данному модулю m, как и равенства, можно складывать и перемножать.

Число p *простое*, если $p > 1$ и для любого $d > 0$ из $d \mid p$ следует $d = 1$ или $d = p$. Числа a и b *взаимно просты*, если для любого $d > 0$ из $d \mid a$ и $d \mid b$ следует $d = 1$.

Теорема 4 (разд. 4.6 Учебника)**.** *Числа a и $m > 0$ тогда и только тогда взаимно просты, когда существует такое x, что $ax \equiv 1 \pmod m$.*

Эта теорема позволяет получить и сама легко получается из следующего утверждения.

Лемма 5 (соотношение Безу; разд. 4.7 Учебника)**.** *Если числа a и b взаимно просты, то найдутся числа u и v, т.ч. $au + bv = 1$.*

Доказательство. Число 0 не взаимно просто самое с собою, так что, без ограничения общности, $b \neq 0$. В зависимости от знака числа b, имеем, в силу теоремы 4, $au \equiv 1 \pmod{\pm b}$ для некоторого u. Но это значит, что $au \mp bv' = 1$ для некоторого v'. Далее берем $v = -v'$ или $v = v'$. □

Обычно именно соотношение Безу (получаемое с помощью *(расширенного) алгоритма Евклида* (разд. 4.9 Учебника)) используют для вывода теоремы 4.

Лемма 6 (разд. 4.10 Учебника)**.** *Если число p простое и $p \mid ab$, то $p \mid a$ или $p \mid b$.*

Доказательство. Пусть $p \mid ab$ и $p \nmid a$. Тогда, очевидно, числа a и p взаимно просты. В силу соотношения Безу, $au + pv = 1$ для некоторых u и v. Тогда $abu + pbv = b$, откуда видно, что b кратно p. □

Простым следствием этой леммы является единственность разложения каждого ненулевого числа в произведение простых.

Теорема 7 («основная теорема арифметики»; разд. 4.10 Учебника)**.** *Для любого $a \neq 0$ существует единственное множество $\{\varepsilon, (i_1, \alpha_{i_1}), \ldots, (i_k, \alpha_{i_k})\}$, где $\varepsilon = \pm 1$, а числа i_j и α_{i_j} натуральные, такое что*

$$a = \varepsilon p_{i_i}^{\alpha_{i_1}} \cdot \ldots \cdot p_{i_k}^{\alpha_{i_k}},$$

где p_{i_j} есть i_j-ое (например, по возрастанию — так что $p_1 = 2$, $p_2 = 3$ и т. д.) просто число.

Иначе говоря, набор простых делителей и максимальная степень каждого, на которую делится a, определены однозначно.

Доказательство. Все легко сводится к случаю $a > 0$. Индукцией по a докажем существование. Если a простое, то все ясно. Иначе его можно поделить на некоторое меньшее число так, что тоже получится число, меньшее a. К обоим применим предположение индукции и попарно сложим степени имеющихся в их разложениях простых.

Установим единственность. Если есть два разложения одного числа, то сократим их на все простые числа, фигурирующие в том и в другом (с учетом степени). Если получились единицы, то все доказано. Иначе возьмем любой простой делитель из первого разложения. Он является делителем и второго разложения, а значит, по лемме 6, делит какой-либо из его простых множителей, т. е. совпадает с ним. Значит, некое простое число встречается (в положительной степени) в обоих разложениях после сокращения. Противоречие. □

Задача 6.3. Найдите остаток при делении

a) 100^{100} на 99;

b) $\binom{15}{8}$ на 13;

c) $20^2 + 21^2 + 22^2$ на 23;

d) $\binom{32}{3}$ на 33;

e) $8^{8^{8^8}}$ на 13.

Решение. **a)** Ясно, что $100 \equiv 1 \pmod{99}$. Значит, $100^{100} \equiv 1^{99} \equiv 1 \pmod{99}$. По лемме 2, числа 100^{100} и 1 делятся на 99 с одинаковым остатком — единицей.

b) Как мы знаем, $\binom{15}{8} \cdot 8! = 15 \cdot 14 \cdot 13 \cdot \ldots \cdot 8$. Значит, $13 \mid \binom{15}{8} \cdot 8!$. Применяя лемму 6, видим, что $13 \mid \binom{15}{8}$ (так как $13 \nmid 8, 13 \nmid 7, \ldots$). Поэтому искомый остаток 0.

c) Имеем $20 \equiv -3 \pmod{23}$, $21 \equiv -2 \pmod{23}$ и $22 \equiv -1 \pmod{23}$. Возведя эти сравнения в квадрат и затем сложив, получаем

$$20^2 + 21^2 + 22^2 \equiv 9 + 4 + 1 \equiv 14 \pmod{23}.$$

Значит, остаток данного выражения тот же, что у числа 14 — четырнадцать.

d) Имеем $\binom{32}{3} = \frac{32 \cdot 31 \cdot 30}{3!} = 32 \cdot 31 \cdot 5$. Однако

$$32 \cdot 31 \cdot 5 \equiv (-1) \cdot (-2) \cdot 5 \equiv 10 \pmod{33}.$$

e) Число 8 возводится в степень $8^{8^8} = 2^{3 \cdot 8^8} = 2^{2+N} = 4 \cdot 2^N$ для подходящего натурального N. Имеем тогда,

$$8^{8^{8^8}} \equiv 8^{4 \cdot 2^N} \equiv ((8^2)^2)^{2^N} \equiv ((-1)^2)^{2^N} \equiv 1^{2^N} \equiv 1 \pmod{13}.$$

□

Задача 6.4. Сформулируйте и докажите признак делимости **a)** на 9; **b)** на 11. (В десятичной системе счисления.)

Решение. **a)** Признак делимости на 9 хорошо известен: необходимо и достаточно, чтобы сумма цифр числа делилась на 9. В самом деле, имеем

$$\overline{a_n \dots a_1 a_0} = a_0 + a_1 10 + a_2 10^2 + \dots + a_n 10^n =$$
$$(a_0 + a_1 + a_2 + \dots + a_n) + a_1(10 - 1) + a_2(10^2 - 1) + \dots + a_n(10^n - 1) =$$
$$\sum_{k=0}^{n} a_k + \sum_{k=1}^{n} a_k(10^k - 1).$$

Покажем, что вторая сумма кратна девяти. Имеем $10 \equiv 1 \pmod{9}$, откуда $10^k - 1 \equiv 0 \pmod{9}$. Теперь ясно, что $\overline{a_n \dots a_1 a_0} \equiv \sum_{k=0}^{n} a_k \pmod{9}$.

b) Заметим, что $10 \equiv -1 \pmod{11}$, откуда $10^k - (-1)^k \equiv 0 \pmod{11}$. Следовательно, мы можем рассуждать как выше, взяв, однако, сумму цифр числа с перемежающимися знаками:

$$\overline{a_n \dots a_1 a_0} = a_0 + a_1 10 + a_2 10^2 + \dots + a_n 10^n =$$
$$(a_0 - a_1 + a_2 - \dots + (-1)^n a_n) + a_1(10 + 1) + a_2(10^2 - 1) + \dots + a_n(10^n - (-1)^n) =$$
$$\sum_{k=0}^{n} (-1)^k a_k + \sum_{k=1}^{n} a_k(10^k - (-1)^k).$$

Итак, $\overline{a_n \dots a_1 a_0} \equiv \sum_{k=0}^{n} (-1)^k a_k \pmod{11}$. Отметим, что в вопросе делимости безразлично, с какого знака начинать складывать цифры, ведь $0 \equiv -0 \pmod{11}$. □

Задача 6.5. **a)** Какой может быть последняя цифра степени тройки в десятичной записи? **b)** Докажите, что предпоследняя цифра степени тройки всегда четна.

Решение. **a)** Понятно (например, из рассуждений предыдущей задачи), что последняя цифра в десятичной записи числа равна остатку при делении этого числа на 10. Ясно, что $3^4 \equiv 81 \equiv 1 \pmod{10}$. Тогда $3^{4k+m} \equiv (3^4)^k \cdot 3^m \equiv 3^m \pmod{10}$.

Следовательно, последняя цифра числа 3^n определяется остатком от деления n на 4. Для всевозможных остатков получаем:

$$\begin{aligned} 3^{4k} &\equiv 1 \pmod{10} \\ 3^{4k+1} &\equiv 3 \pmod{10} \\ 3^{4k+2} &\equiv 9 \pmod{10} \\ 3^{4k+3} &\equiv 7 \pmod{10}. \end{aligned}$$

b) Можно считать, что в однозначном числе предпоследняя цифра 0. Предпоследняя цифра не изменится, если вычесть из числа его последнюю цифру.

С другой стороны, в числе $a = \overline{a_n \dots a_1 0}$, оканчивающемся нулем, предпоследняя цифра a_1 четна тогда и только тогда, когда число a делится на 4. В самом деле,

$$\overline{a_n \dots a_1 0} \equiv a_1 10 + 100(a_2 + \dots + a_n 10^{n-2}) \equiv 10a_1 \pmod{4}.$$

Ясно, что $10a_1$ кратно 4 тогда и только тогда, когда $2 \mid 5a_1$, т. е., согласно лемме 6, $2 \mid a_1$.

Имеем

$$\begin{aligned} 3^{4k} - 1 &\equiv (-1)^{4k} - 1 \equiv 0 \pmod{4} \\ 3^{4k+1} - 3 &\equiv (-1)^{4k+1} - (-1) \equiv 0 \pmod{4} \\ 3^{4k+2} - 9 &\equiv (-1)^{4k+2} - 1 \equiv 0 \pmod{4} \\ 3^{4k+3} - 7 &\equiv (-1)^{4k+3} - (-1) \equiv 0 \pmod{4}. \end{aligned}$$

С учетом предыдущего пункта, всякая степень тройки имеет четную предпоследнюю цифру. □

Теорема 8 (малая теорема Ферма; разд. 4.12)**.** *Пусть p простое и $p \nmid a$. Тогда*

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

Доказательство. Рассмотрим $p-1$ число $a, 2a, \dots, (p-1)a$, т. е. всевозможные числа ka при $0 < k < p$. При разных k эти числа попарно несравнимы про модулю p, так как из $ka \equiv ma \pmod{p}$ получается $p \mid (k-m)a$, что, вследствие леммы 6, дает $p \mid k - m$. Без ограничения общности $k \geqslant m$, но тогда $0 \leqslant k - m < p$, т. е. $0 \leqslant tp < p$, откуда $0 \leqslant t < 1$. Поскольку t целое, $t = 0$ и $k = m$.

Всего возможен $p-1$ остаток по модулю p, а значит, попарно несравнимые числа $a, 2a, \dots, (p-1)a$ дают все эти остатки ровно по разу. В частности, они дают ровно те же остатки, что и числа $1, 2, \dots, p-1$. Поэтому

$$a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Имеем $p \mid (a^{p-1} - 1)(p-1)!$, откуда, по лемме 6, $p \mid a^{p-1} - 1$. □

Задача 6.6. a) Пусть p простое число большее 3. Докажите, что p^2-1 делится на 24. **b)** Докажите, что при любом целом a число $a^{73}-a$ делится на 2, на 3, на 5, на 7, на 13, на 19, на 37, на 73.

Решение. **a)** Ясно, что $24 = 3 \cdot 2^3$. Поскольку $3 \nmid p$, в силу малой теоремы Ферма, $3 \mid p^2-1$. С другой стороны, $p^2-1 = (p-1)(p+1)$. Посмотрим, с чем сравнимы числа $p \pm 1$ по модулю 8 в зависимости от остатка, получающегося при делении p на 8. Поскольку p нечетно, этот остаток также нечетен.

$p-1$	0	2	4	6
p	1	3	5	7
$p+1$	2	4	6	0

Из таблицы видно, что всегда $(p-1)(p+1) \equiv 0 \pmod 8$. Итак, число p^2-1 кратно 8 и 3, а значит, кратно 24.

b) Имеем $x = a^{73}-a = a(a^{72}-1)$, поэтому a и $a^{72}-1$ суть делители числа x. Далее, $a^{72}-1 = (a^{36}-1)(a^{36}+1) = (a^{18}-1)(a^{18}+1)(a^{36}+1)$, откуда видно, что x кратно $a^{36}-1$ и $a^{18}-1$.

Из легко проверяемого тождества $u^3-1 = (u-1)(u^2+u+1)$ следует, что x делится на $a^{12}-1$ и на a^6-1, а стало быть, также на a^4-1 и на a^2-1. Последнее означает еще и делимость на $a-1$.

Итак, мы показали, что число $x = a^{73}-a$ имеет (среди прочих) следующие делители:

$$a, a^{72}-1, a^{36}-1, a^{18}-1, a^{12}-1, a^6-1, a^4-1, a^2-1, a-1.$$

Отсюда видно, что при любом a число x кратно каждому из данных нам простых. Например, рассмотрим число 7. Если $7 \mid a$, то $7 \mid x$. В противном случае $a^6 \equiv 1 \pmod 7$ по теореме 8. Но тогда $7 \mid a^6-1$, а значит, вновь $7 \mid x$. □

Задача 6.7. Докажите, что $(p-1)!$ сравнимо с -1 по модулю p для любого простого числа p.

Решение. Это утверждение известно как *теорема Вильсона*. Докажем его. Каждое k среди $p-1$ числа $1, 2, \ldots, p-1$ взаимно просто с p. В силу теоремы 4, для каждого k найдется x, т. ч. $kx \equiv 1 \pmod p$. Очевидно, x можно заменить его остатком по модулю p, лежащим среди чисел $1, 2, \ldots, p-1$ (поскольку, разумеется, $p \nmid x$).

Итак, каждое число k из $1, 2, \ldots, p-1$ лежит в этом множестве вместе с числом m, т. ч. $km \equiv 1 \pmod p$. Если m и m' два таких числа, то $p \mid k(m-m')$, откуда $p \mid (m-m')$ и $m = m'$. Обозначим единственное подходящее m символом k^{-1}. Ясно, что $(k^{-1})^{-1} = k$. Отсюда видно, что все числа $1, 2, \ldots, p-1$ разбиваются на попарно непересекающиеся пары $\{k, k^{-1}\}$.

Может ли быть $k = k^{-1}$? В этом случае имеем $k^2 \equiv 1 \pmod p$, т. е. $p \mid (k-1)(k+1)$, откуда $k = 0$ или $k = p-1$. Легко проверить, что такие k действительно совпадают с k^{-1}.

В произведении $1 \cdot 2 \cdot \ldots \cdot (p-1)$ все числа, кроме 1 и $p-1$, попарно сократятся со своими обратными:

$$(p-1)! \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

□

Задача 6.8. Докажите, что для любого целого положительного $n > 2$ между n и $n!$ есть простое число.

Решение. Предположим, что любое число m, для которого $n < m < n!$, не простое. При $n > 2$ имеем, как легко проверить, $1 < n < n! - 1 < n!$. Значит, любой простой делитель p числа $n! - 1$ (который найдется в силу теоремы 7) не больше n. Но тогда $p \mid n!$.

С другой стороны, если $d \mid a$ и $d \mid a + 1$, то $d \mid 1$. Значит, $p \mid 1$, что неверно. □