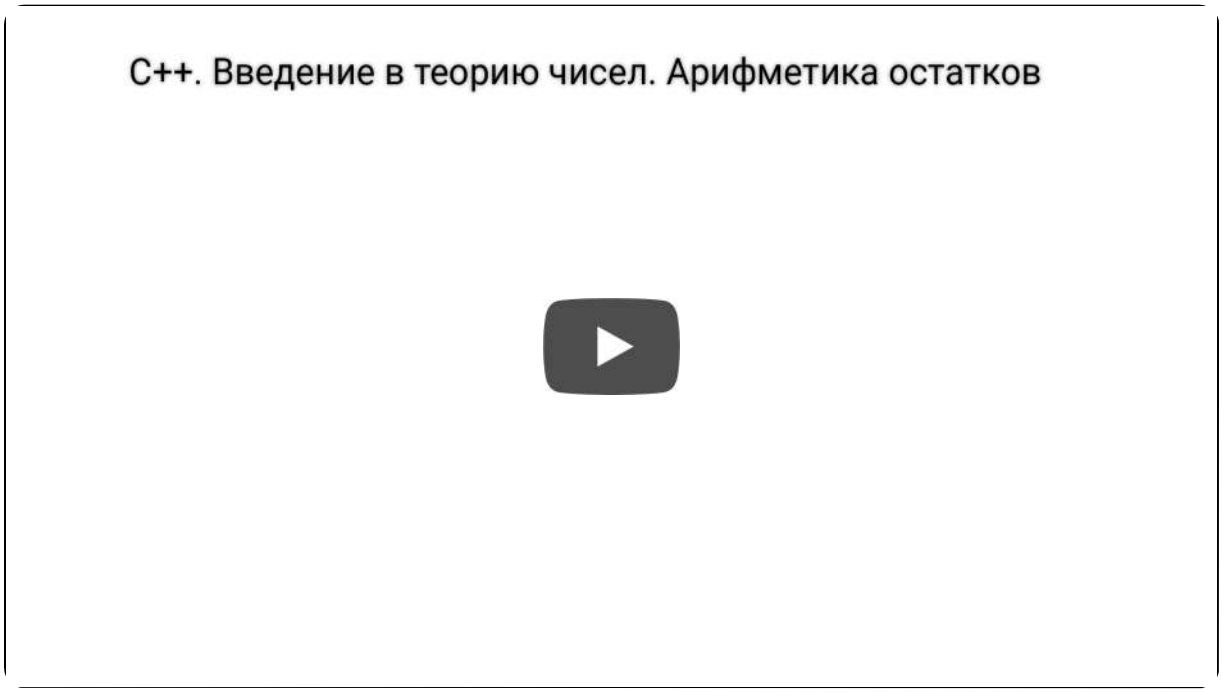
Арифметика остатков



Арифметика остатков

Деление целого числа a на целое число b ($b > 0$) с остатком — это представление a в виде $b \cdot q + r$, где r и q — целые числа, $0 \leq r < b$. Число q называется неполным частным при делении a на b, а r — остатком при делении a на b.

Например:

a	b	$a = b * q + r$
37	5	$37 = 5 * 7 + 2$
-12	5	$-12 = 5 * (-3) + 3$

В языках программирования операция взятия остатка при делении a на b, как правило, обозначается знаком $\%$. Операция нахождения неполного частного при делении a на b — это целочисленное деление, оно может обозначаться по-разному для различных языков. Используя эти две операции, мы можем выполнять деление с остатком при написании программ.

Важно отметить, что если для целого числа $a \geq 0$ операции деления с остатком на целое число $b > 0$ в языках программирования выполняются в

точности с данным выше определением, то в случае когда $a < 0$, ситуация сложнее. Например, в языке Python эти операции выполняются в соответствии с нашим определением, а в языке C++ нет. В Python выражение $-12\%5$ равно числу 3, а в C++ это же выражение будет равно числу -2. Чтобы остаток от деления всегда соответствовал данному выше определению, можно отдельно разбирать случай при $a < 0$ или писать выражение для нахождения остатка в виде $(a\%b + b)\%b$. А чтобы найти неполное частное, можно вычитать найденный остаток из числа a и после этого результат делить на b.

При этом, в языках программирования разрешено выполнять операции деления с остатком и для $b < 0$. Но мы не рекомендуем производить деление с остатком на отрицательное число. Всегда можно преобразовать формулы в решении задачи таким образом, чтобы использовать деление с остатком только на положительное целое число.

Пусть дано целое число $m > 1$. Говорят, что a сравнимо с b по модулю m, и пишут $a \equiv b \pmod{m}$, если $(a - b) \vdots m$ ($a - b$ делится нацело на m).

Например:

- $37 \equiv 2 \pmod{5}$
- $37 \equiv 7 \pmod{5}$
- $37 \equiv -3 \pmod{5}$

Для сравнений верны следующие свойства:

- $a \equiv a \pmod{m}$ (рефлексивность)
- $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ (симметричность)
- $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$ (транзитивность)

Пусть $a_1 \equiv b_1 \pmod{m}$ и $a_2 \equiv b_2 \pmod{m}$, тогда верны следующие сравнения:

- $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$
- $a_1 a_2 \equiv b_1 b_2 \pmod{m}$
- $a_1^n \equiv b_1^n \pmod{m}$, где n – натуральное число

Рассмотрим некоторое целое число $m > 1$. Любое целое число даёт какой-то остаток при делении на m. В рамках данного подхода будем считать, что числа,

которые дают одинаковый остаток при делении на m, — одинаковы. Тогда получается, что есть лишь конечное число различных чисел. Например, в качестве такого конечного набора остатков можно выбрать целые числа от 0 до $m-1$. Множество остатков по модулю m в математике принято обозначать через $\mathbb{Z}_m$. Так как остатков по модулю m конечное число, можно постороить таблицу сложения и умножения для всех возможных пар чисел из $\mathbb{Z}_m$.

Например, таблица сложения для $\mathbb{Z}_4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Или таблица умножения для $\mathbb{Z}_5$:

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Из данных таблиц можно сделать вывод о существовании в $\mathbb{Z}_m$ некоторых особых чисел:

- 0 — такой элемент, что при прибавлении к нему любого числа результат равен этому числу $0 + x \equiv x \pmod{m}$
- 1 — такой элемент, что при умножении его на любое число результат равен этому числу $1 \cdot x \equiv x \pmod{m}$

Обратное число в $\mathbb{Z}_m$ для числа a — такое число a^{-1}, что $a \cdot a^{-1} \equiv 1 \pmod{m}$.

Например:

- $1^{-1} \equiv 1 \pmod 5$
- $2^{-1} \equiv 3 \pmod 5$
- $3^{-1} \equiv 2 \pmod 5$
- $4^{-1} \equiv 4 \pmod 5$

Если m — простое число, то у любого числа в $\mathbb{Z}_m$, кроме числа 0, существует обратное.