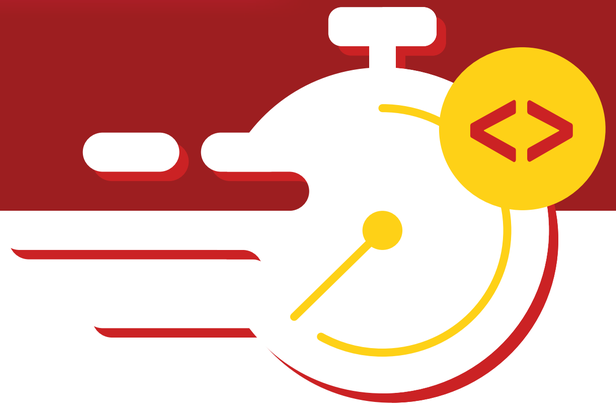
Бинарные операции по модулю

Урок 2.2



МФТИ
Московский физико-технический институт

При поддержке Фонда президентских грантов

RUCODE festival

Фонд развития Физтех-школ

В этом видео_

- Работа с остатками
- Основные свойства деления с остатком

Остатки: определения и возможный диапазон_

- r — остаток от деления a на $b>0$,
  если $a = qb + r$, $r \geq 0$, r — наименьшее возможное
- $r = 0$ тогда и только тогда,
  когда a делится на $b(a = qb + 0)$
- Если $r > b$, то $r = b + r_1$, то есть $0 < r_1 < r$;
  $a - r_1 = a - (r - b) = (a - r) + b$; $a - r$ делится на b,
  так как r — остаток. То есть $a - r_1$ делится на b
  и $r_1 < r$ — противоречит минимальности r

Тем самым $0 \leq r < b$

Единственность остатка_

- Если $a = by + k$, где $0 \le k < b$, то k — остаток от деления a на b
- Пусть это не так, и $a = bx + r$, где $r \ne k$, $0 \le k < b$
- Тогда $a - bx = r$ и $a - by = k$. Вычитаем из первого второе, получаем: $by - bx = r - k$
- $b(y - x) = r - k$; из ограничений на k и r видим, что $-b < r - k < b$. Так как $r \ne k$, то правая часть не делится на b, в то время как левая делится. Противоречие. Значит, остаток является единственным

Периодичность остатков_

$a = bq + r$, тогда $a + 1 = bq + (r + 1)$

- Если $0 \le r < b - 1$, то $0 \le (r + 1) < b$,
  значит, $(r + 1)$ — остаток
- Если $r = b - 1$, то $a + 1 = bq + (b - 1) + 1 = b(q + 1) + 0$,
  то есть 0 — остаток

Аналогично, $a - 1 = bq + (r - 1)$

- Если $0 < r < b - 1$, то $0 \le (r - 1) < b$,
  значит, $(r - 1)$ — остаток
- Если $r = 0$, то $a - 1 = bq - 1 = b(q - 1) + (b - 1)$,
  то есть $(b - 1)$ — остаток

То есть после каждых b последовательных увеличений/уменьшений остатки повторяются

Понятие сравнимости по модулю_

- Из периодичности остатков следует, что все числа вида $a + kb$ имеют такой же остаток при делении на b, что и a, то есть эквивалентны с точки зрения взятия остатка от деления на b
- Если x и y дают одинаковый остаток при делении на b, то говорят, что они сравнимы (или равны) по модулю b
- Запись: $x \equiv y \pmod b$ или даже $x = y \pmod b$
- Остаток от деления a на b обозначается $a \bmod b$

Оператор взятия остатка: проблемы и решение_

- Оператор взятия остатка — %: a % b.
  Но с отрицательными числами он работает **не так**
- -a % b = -(a % b); например, -7 % 5 = -2
  — не в том диапазоне!
- На самом деле -a = -qb – r = -q(b - q) + (b – r),
  то есть остаток равен b-r (-7 mod 5 = 3). Как исправить?

Оператор взятия остатка: проблемы и решение_

- Оператор взятия остатка — %: a % b.
  Но с отрицательными числами он работает **не так**
- -a % b = -(a % b); например, -7 % 5 = -2 — не в том диапазоне!
- На самом деле -a = -qb – r = -q(b - q) + (b – r),
  то есть остаток равен b-r (-7 mod 5 = 3). Как исправить?
- -b < a % b < b, прибавим b: 0 < (a % b) + b < 2b, снова берём остаток. То есть a mod b реализуется как ((a % b) + b) % b

Остаток суммы и разности_

- Пусть $a = bq + r_a$, $c = bk + r_c$, где $r_a = a \bmod b$, $r_c = c \bmod b$
- Тогда $a + c = bq + r_a + bk + r_c = b(q + k) + r_a + r_c$,
  то есть: **$(a + c) \bmod b = (a \bmod b + c \bmod b) \bmod b$**
- Аналогично, $a - c = b(q - k) + r_a - r_c$,
  то есть: $(a - c) \bmod b = (a \bmod b - c \bmod b) \bmod b$

Остатки и умножение_

1. Умножение по модулю

Пусть $a = bq + A$, $c = bk + C$, где $A = a \bmod b$, $C = c \bmod b$.
$ac = (bq + A)(bk + C) = b^2qk + b(kA + qC) + AC = b(bqk + kA + qC) + AC$

Отсюда **$ac \bmod b = (a \bmod b * c \bmod b) \bmod b$**

2. Масштабирование остатка

Умножим обе части равенства $a = bq + r_a$ на целое $k > 0$,
получим $ka = (kb)q + kr_a$; так как $0 \le r_a < b - 1$,
то $0 \le kr_a < (b - 1)k < bk - 1$, kr_a — остаток,
то есть **$ak \bmod bk = k (a \bmod b)$**

Реализация вычислений по модулю_

```
long long norm(long long d, long long MOD) {
return ((d % MOD) + MOD) % MOD; }

long long Madd (long long x, long long y, long long MOD) {
return norm (norm(x, MOD) + norm (y,MOD), MOD); }

long long Msub (long long x, long long y, long long MOD) {
return norm (norm(x, MOD) – norm (y,MOD), MOD);}

long long Mmul (long long x, long long y, long long MOD) {
return norm (norm(x, MOD) * norm (y,MOD), MOD); }
```

Задача про числа Фибоначчи_

- Числа Фибоначчи: $a0 = a1 = 1$, $ax = ax - 1 + ax - 2$ для $x > 1$.
  Найти N-е число Фибоначчи по заданному модулю

Задача про числа Фибоначчи: рекурсия?_

- Числа Фибоначчи: $a_0 = a_1 = 1$, $a_x = a_{x-1} + a_{x-2}$ для $x > 1$.
  Найти N-е число Фибоначчи по заданному модулю
- При рекурсивном вычислении по формуле $f(x) = f(x - 1) + f(x - 2)$ каждый шаг рекурсии порождает при раскрытии 2, то есть на втором шаге $(f(x - 2) + f(x - 3)) + (f(x - 3) + f(x - 4))$ — 4 слагаемых, далее 8, 16... $O(2n)$ операций — слишком много!

Задача про числа Фибоначчи: никакой рекурсии!_

- Числа Фибоначчи: $a_0 = a_1 = 1$, $a_x = a_{x-1} + a_{x-2}$ для $x > 1$.
  Найти N-е число Фибоначчи по заданному модулю
- При рекурсивном вычислении по формуле $f(x) = f(x - 1) + f(x - 2)$ каждый шаг рекурсии порождает при раскрытии 2, то есть на втором шаге $(f(x - 2) + f(x - 3)) + (f(x - 3) + f(x - 4))$ — 4 слагаемых, далее 8, 16... $O(2^n)$ операций — слишком много!
- Правильнее в цикле вычислять что-то наподобие
  fib3 = fib2 + fib1; fib1 = fib2; fib2 = fib3;
  Тогда всего $O(n)$ операций

Подведем итог_

- Сложенние, вычитание и умножение по модулю