1) Быстрое возв. в степень.

$a^n = (a^2)^{n/2}$, если $n : 2$

$a^n = (a^2)^{[n/2]} a$, если $n \not: 2$

$a^0 = 1$.

$a^{10^{18}}$:

Линейно: 10^{18}

Быстро: $\log 10^{18} = \log 1000^6 = 6 \log 1000 \approx 60$

Решето Эратосфена

Найти все простые числа, меньше n.

2 3 4 5 6 7 8 9 10 11 ... n

p

$i = 17$

$2 \cdot 17, 3 \cdot 17, 4 \cdot 17, \ldots, 16 \cdot 17, 17 \cdot 17$

$O(n \log\log n)$

$\log\log 10^{18} \approx \log 60 \approx 8$

НОД

greatest common divizor

$GCD(a,b) \overset{a>b}{=} GCD(a-b,b)$

$GCD(12,15) = GCD(3,12) = GCD(9,3) =$
$= GCD(6,3) = GCD(3,3) = GCD(0,3) = 3$

1) Не использовать вычитание

$GCD(10000,2) = GCD(9998,2) = GCD(9996,2) = \dots$

-2
$-2 \cdot 2$
$-2 \cdot 3$
$\vdots$
$-2 \cdot n$

$GCD(a,b) \overset{a>b}{=} GCD(a\%b, b)$
$= GCD(b, a\%b)$

1	0
2	1
3	2
5	3
8	5

Худший случай

Последовательность Фибоначчи

$O(\log_{\frac{1+\sqrt{5}}{2}} n)$

$f(n) \sim \left(\frac{1+\sqrt{5}}{2}\right)^n$

↑ золотое сечение

Модульная арифметика.

$a \bmod n = r$ — взять остаток от деления

$r \in [0; n-1]$

$-10 \bmod 3 = -1 \bmod 3 = 2$

```
int Mod(int a, int b){
    if(b<0){
        a*=-1;
        b*=-1;
    }
    a%=b;
    if(a<0)
        a+=b;
    return a;
}
```

Def $a \equiv b \pmod n \Leftrightarrow a \bmod n = b \bmod n$

$a \equiv b \pmod n \Leftrightarrow (a-b) \vdots n$

$\Rightarrow$

$a = n \cdot k_a + r$

$b = n \cdot k_b + r$

$a - b = n(k_a - k_b) \vdots n$

$\Leftarrow$

$a = n k_a + r_a$

$b = n k_b + r_b$

$a - b = n(k_a - k_b) + (r_a - r_b)$, $(r_a - r_b) \in [-(n-1); n-1]$

$n \vdots n$, $(r_a - r_b) = 0 \vdots n$

□

$a \equiv b \pmod n$

$c \equiv d \pmod n$

$a + c \equiv b + d \pmod n$ $\quad (a+c) - (b+d) = (a-b) + (c-d) \vdots n$

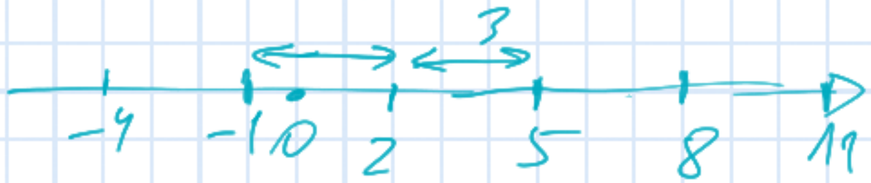
$a - c \equiv b - d \pmod n$

$a c \equiv b d \pmod n$ $\quad ac - bd = ac - cb + cb - bd = c(a-b) + b(c-d) \vdots n$

$(a+b)\%n = (a\%n + b\%n)\%n$

$ab\%n = (a\%n)(b\%n)\%n$

$-10 \bmod 3 = -1 \bmod 3 = 2$



$a = kn + r$

$k = \left\lfloor \frac{a}{n} \right\rfloor$ $\quad r = a\%n$

$\frac{-10}{3} = -3,333\ldots$

$\left\lfloor \frac{-10}{3} \right\rfloor = -4$

$-10 = -4 \cdot 3 + 2$

Th (малая теорема Ферма)

n – простое; $a \nmid n$, тогда:

$$a^{n-1} \equiv 1 \pmod{n}$$

$\frac{a}{b} \to a \cdot b^{-1}$ $\quad b^{-1}: b \cdot b^{-1} \equiv 1 \pmod{n}$

$a \cdot \underbrace{a^{n-2}}_{a^{-1}} \equiv 1$ $\quad \frac{a}{b} = a \cdot b^{-1}$

$a = a \cdot \underbrace{b^{-1} \cdot b}_{1}$

$$\frac{a}{b} \equiv a \cdot b^{n-2} \pmod{n}$$

$20 * 10 = 200 \equiv 4 \pmod 7$

$20 \equiv 6 \pmod 7$

$20 \equiv 27 \equiv 13$

$\frac{4}{6} \equiv x \pmod 7$

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$20 \equiv 6 \pmod 7$

$20 * k \equiv 4 \pmod 7$

$k \bmod 7 - ?$

$4^5 = (16)^2 4 \equiv (2)^2 \cdot 4 = 4^2 = 16 \equiv 2 \pmod 7$

$4 \cdot (6)^{9-2} \equiv 4 \cdot 6^5 \equiv 4 \cdot (-1)^5 \equiv -4 \equiv 3 \pmod 7$

$6 \equiv -1 \pmod 7$