**Арифметика**

**Функция Эйлера** \phi (n) (иногда обозначаемая \varphi(n) или {\it phi}(n)) — это количество чисел от 1 до n, взаимно простых с n. Иными словами, это количество таких чисел в отрезке [1; n], [наибольший общий делитель](http://e-maxx.ru/algo/export_euclid_algorithm) которых с n равен единице.

int phi (int n) {

int result = n;

for (int i=2; i\*i<=n; ++i)

if (n % i == 0) {

while (n % i == 0)

n /= i;

result -= result / i;

}

if (n > 1)

result -= result / n;

return result;

}

**Бин возведение в степень**

int binpow (int a, int n) {

int res = 1;

while (n) {

if (n & 1)

res \*= a;

a \*= a;

n >>= 1;

}

return res;

}

Пусть задан некоторый натуральный модуль m, и рассмотрим кольцо, образуемое этим модулем (т.е. состоящее из чисел от 0 до m-1). Тогда для некоторых элементов этого кольца можно найти **обратный элемент**.

r[1] = 1;

for (int i=2; i<m; ++i)

r[i] = (m - (m/i) \* r[m%i] % m) % m;

**Нахождение степени делителя факториала**

Даны два числа: n и k. Требуется посчитать, с какой степенью делитель k входит в число n!, т.е. найти наибольшее x такое, что n! делится на k^x.

int fact\_pow (int n, int k) {

int res = 0;

while (n) {

n /= k;

res += n;

}

return res;

}

# Вычисление факториала по модулю

int factmod (int n, int p) {

int res = 1;

while (n > 1) {

res = (res \* ((n/p) % 2 ? p-1 : 1)) % p;

for (int i=2; i<=n%p; ++i)

res = (res \* i) % p;

n /= p;

}

return res % p;

}