

# メモ (整数論)

hos

2019 年 1 月 26 日

$\div$  は整数除算 (剰余の符号を被除数に合わせる).

## 1 mod 逆元 (2 冪)

奇数  $a$  に対し,  $a \times (3a \text{ xor } 2) \equiv 1 \pmod{2^5}$  (黒魔術).

$ab \equiv 1 \pmod{2^k}$  のとき,  $a \times b(2 - ab) \equiv 1 \pmod{2^{2k}}$  ( $1 - ab(2 - ab) = (1 - ab)^2$  より).

$ab \equiv -1 \pmod{2^k}$  のとき,  $a \times b(2 + ab) \equiv -1 \pmod{2^{2k}}$  ( $1 + ab(2 + ab) = (1 + ab)^2$  より).

## 2 mod 逆元 (一般)

$(r_0, s_0, t_0) = (a, 1, 0)$ ,  $(r_1, s_1, t_1) = (b, 0, 1)$ ,  $(r_i, s_i, t_i) = (r_{i-2}, s_{i-2}, t_{i-2}) - (r_{i-2} \div r_{i-1})(r_{i-1}, s_{i-1}, t_{i-1})$  とすると,  $r_i = as_i + bt_i$ ,  $\gcd(s_i, t_i) = 1$  が不変.  $r_k = 0$  になったとき,  $|r_{k-1}| = \gcd(a, b)$  なので, 特に  $as_{i-1} \equiv \pm 1 \pmod{b}$ .

$k \geq 3$  なら,  $|s_2| < |s_3| < \dots < |s_{k-1}| < |s_k| = \frac{|b|}{\gcd(a, b)}$ ,  $|t_2| < |t_3| < \dots < |t_{k-1}| < |t_k| = \frac{|a|}{\gcd(a, b)}$ .

## 3 Montgomery reduction

正の奇数  $M$  に対し,  $M < 2^k$  として,  $M' \equiv -M^{-1} \pmod{2^k}$  をとっておく.

整数  $a$  に対し,  $2^{-k}a \equiv \frac{a + (aM' \bmod 2^k)M}{2^k}$  である (分子が  $\equiv 0 \pmod{2^k}$  かつ  $\equiv a \pmod{M}$  なの).  $0 \leq a < 2^k M$  なら右辺は 0 以上  $2M$  未満.

$\bmod M$  で加減乗をたくさん行うとき,  $f(a) = 2^k a \bmod M$  で変換してから行う.  $f(ab) \equiv 2^{-k} f(a) f(b) \pmod{M}$ . 2 冪以外での除算は  $f$  の適用時のみになる.

## 4 多項式除算

除算  $e(t) = f(t)q(t) + r(t)$  ( $\deg e = m$ ,  $\deg f = n$ ,  $m \geq n$ ,  $\deg q = m - n$ ,  $\deg r < n$ ) の両辺を  $t^m$  で割って  $T = t^{-1}$  とすると,  $E(T) = F(T)Q(T) + T^{m-n+1}R(T)$ . ここで  $E, F, Q, R$  はそれぞれ  $e, f, q, r$  を係数逆順にした多項式 ( $r$  は  $n$  項まで 0 埋め).

$f$  が monic なら  $F(0) \neq 0$  なので  $F(T)F'(T) \equiv 1 \pmod{T^{m-n+1}}$  なる  $F'$  がとれて,  $Q(T) = E(T)F'(T) \bmod T^{m-n+1}$  として  $Q$  が求まる.

$\bmod f(t)$  を常にとりながら加減乗を行うとき, 被除数は次数  $2n - 2$  以下なので,  $F'$  は  $\bmod T^{n-1}$  で 1

回求めておけばよい.  $F'$  は  $F'(T) = 1$  から  $F' \mapsto F'(2 - FF')$  を  $\lceil \log_2(n-1) \rceil$  回繰り返せば求まる.  $O(n(\log n)^2)$  時間だが, FFT の配列の長さをちゃんとやると  $O(n \log n)$  時間にできる.