メモ (整数論)

hos

2019 年 9 月 12 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，$a \times (3a \operatorname{xor} 2) \equiv 1 \pmod{2^5}$ (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，$|s_2| < |s_3| < \cdots < |s_{k-1}| < |s_k| = \dfrac{|b|}{\gcd(a,b)}$, $|t_2| < |t_3| < \cdots < |t_{k-1}| < |t_k| = \dfrac{|a|}{\gcd(a,b)}$.

3　mod 平方根 (素数)

p を奇素数とする．平方剰余 $a \in \mathbb{F}_p^\times$ に対し，$b^2 - a$ が平方非剰余となる $b \in \mathbb{F}_p$ は $\dfrac{p-1}{2}$ 個ある ($b^2 - a = c^2$ の解は $(b+c)(b-c) = a$ より $(b, c) = \left(\dfrac{t + at^{-1}}{2}, \dfrac{t - at^{-1}}{2}\right)$ と書ける $p-1$ 個で，c を $-c$ にしても同じ b が対応して，$c = 0$ は解でないので)．よってそのような b は期待値約 2 回の乱択で見つかる．

2 次拡大 $\mathbb{F}_p(\sqrt{b^2-a})$ を考えて，$x = \left(b + \sqrt{b^2-a}\right)^{\frac{p+1}{2}}$ とすると，Frobenius 準同型の性質より $x^2 = \left(b + \sqrt{b^2-a}\right)\left(b + \sqrt{b^2-a}\right)^p = \left(b + \sqrt{b^2-a}\right)\left(b - \sqrt{b^2-a}\right) = a$ となる．$x^2 = a$ の解は $\mathbb{F}_p(\sqrt{b^2-a})$ においても 2 個しかないので，$x \in \mathbb{F}_p$ である．

4　有限体上の多項式の因数分解

p を素数，$q = p^e$ とする．以下の 3 ステップを行う．

4.1　square-free factorization

$f \in \mathbb{F}_q[T]$ を $f = f_1^1 f_2^2 \cdots$ (f_i は square-free) の形にする．

$\gcd(f, f') = \prod_{p \nmid i} f_i^{i-1} \prod_{p \mid i} f_i^i$ なので，除算と gcd で f_1 から順に f_i $(p \nmid i)$ が求まる．残りは p 乗根をとって (指数を p で割って係数に Frobenius 準同型の逆をかける) 再帰的に処理.

4.2 distinct-degree factorization

$f \in \mathbb{F}_q[T]$ を $f = f_1 f_2 \cdots$ (f_j は j 次既約多項式の積) の形にする．

$T^{q^j} - T$ は $\mathbb{F}_q$ 上の次数が j の約数の既約多項式すべての積である ($T^{q^j} - T$ は微分が -1 なので square-free．最小分解体は $\mathbb{F}_{q^j}$ で，部分拡大は $\mathbb{F}_{q^{(j\text{ の約数})}}$)．よって $T^{q^j} - T$ $(j = 1, 2, \ldots)$ との gcd をとって割っていけば f_1 から順に求まる．

$\gcd((f\text{ の約数}), T^{q^j} - T)$ を求めるために，$(T^{q^j} - T) \bmod f$ を計算する．$\mathbb{F}_q[T]/(f)$ を $\deg f$ 次線型空間とみて，q 乗は線型写像なので先に行列を求めておけば，$O((\deg f)^2 \log q + (\deg f)^3)$ 回の計算でできる．

4.3 Cantor–Zassenhaus algorithm

$f \in \mathbb{F}_q[T]$ が j 次既約多項式の積のとき，f を因数分解する．

$f = f_1 \cdots f_l$ (f_k は既約) とする．中国剰余定理より $\mathbb{F}_q[T]/(f) \cong \mathbb{F}_q[T]/(f_1) \times \cdots \times \mathbb{F}_q[T]/(f_l)$ なので，$r \in \mathbb{F}_q[T]/(f)$ を一様ランダムにとるとその $\mathbb{F}_q[T]/(f_k)$ $(k = 1, \ldots, l)$ での像は独立に一様ランダムに分布する．

$p = 2$ のとき，$\mathrm{tr}_{(\mathbb{F}_{2^e}/(f_k))/\mathbb{F}_2}(r) = r + r^2 + r^4 + \cdots + r^{2^{e-1}} \in \mathbb{F}_2$ は確率 $\dfrac{1}{2}$ ずつで $0, 1$ になる (恒等 0 ではない線型写像なので)．

$p \neq 2$ のとき，$r^{(q^e-1)/2} \in \{0, \pm 1\}$ は $f_k \mid r$ のときのみ 0，確率 $\dfrac{(q^e-1)/2}{q^e}$ ずつで ± 1 になる (有限体 $\mathbb{F}_q[T]/(f_k)$ の乗法群が巡回群だから)．

よって $\mathrm{tr}_{(\mathbb{F}_{2^e}/(f_k))/\mathbb{F}_2}(r)$ あるいは $r^{(q^e-1)/2} - 1$ と f の gcd をとれば $f_1, \ldots, f_l$ のうち半分ほどが入る．

(TODO: ちゃんと解析する)

5 連立合同式

$t \equiv B \pmod{M}$ かつ $at \equiv b \pmod{m}$ なる t を求める．$t = B + Mz$ として，$aMz \equiv b - aB \pmod{m}$ が条件．$g = \gcd(aM, m)$ とおいて，$g \nmid b - aB$ なら解なし．そうでないとき，$x \equiv \left(\dfrac{aM}{g}\right)^{-1} \pmod{\dfrac{m}{g}}$ として (互除法で $aMx + my = g$ なる (x, y) も求まっている)，$z \equiv x\dfrac{b - aB}{g} \pmod{\dfrac{m}{g}}$．$t$ は $\bmod \dfrac{Mm}{g}$ で一意.

6 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，$2^{-k}a \equiv \dfrac{a + (aM' \bmod 2^k)M}{2^k}$ である (分子が $\equiv 0 \pmod{2^k}$ かつ $\equiv a \pmod{M}$ なので)．$0 \leq a < 2^k M$ 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．

7　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．