mod p 上の 1 の n 乗根　出典：https://twitter.com/kirika_comp/status/1203603433455927297

1 の n 乗根 a を求めたい。$a^n = 1 \bmod p$ かつ $a^{p-1} = 1 \bmod p$ だから $p-1 = 0 \bmod n$ が必要。このとき原始根 g を用いて n 乗根が $g^{(p-1)/n}$ と書ける。よって $p-1 = 0 \bmod n$ が 1 の n 乗根が存在するための必要十分条件。b をランダムに取ってくる。b が原始根 g を用いて $b = g^k$ と書けるとする。$(k\frac{p-1}{n}x = 0 \bmod p-1 \Leftrightarrow x = n \bmod p-1)$ は $k \mod n$ が n と互いに素であることと同値。このような k は $1, 2, \ldots, p-1$ のうち $\frac{p-1}{n}\phi(n)$ 個ある。したがって $\frac{\phi(n)}{n}$ の確率で $b^{(p-1)/n}$ が 1 の n 乗根になる。

体係数 1 変数多項式環 $K[X]$ ユークリッド整域だから拡張ユーグリッドの互除法により互いに素な f, g に対して $f^{-1} \bmod g$ が求められる。従って Garner のアルゴリズムが適用できる。

1 形式的冪級数

出典：http://sugarknri.hatenablog.com/entry/2019/10/08/001359 R を可換環とする。$n-1$ 次で打ち切った形式的冪級数 $P = R[[X]]/\langle X^n \rangle$ の成す環の演算を考える。

1.1 等比級数による逆元の計算

等比級数の和の公式より

$$1/f = (f_0)^{-1} \sum_{i=0}^{n} (1-f)^i$$

である。$g := (1-f), h(k) := 1 + g + g^2 + ... + g^{2^k - 1}$ と置くと、$h(k) = h(k-1)(1 + g^{2^{k-1}})$ という漸化式が成り立ち $O(n \log^2(n))$ で計算できる。

1.2 Newton 法による逆元の計算

1.3 Newton 法による平方根の計算

$g^2 = f$ なる g を求めたい。$F(X) = X^2 - f$ に対して $F(X) = 0$ の解をニュートン法で求めると

$$g_{n+1} = \frac{g_n}{2} + \frac{f}{2g_n}$$

となる。このとき

$$g_{n+1}^2 - f = (\frac{g_n}{2} + \frac{f}{2g_n})^2 - f \tag{1}$$

$$= \frac{1}{4g_n^2}(g_n^2 - f)^2 \tag{2}$$

$$\tag{3}$$

だから二次収束する。計算量は $O(\sum_{k=1,2,4,8,\ldots,n} k \log k) = O(n \log n)$ となる。

1.4 Newton 法による対数の計算

$\exp(g) = f$ なる g を求めたい。$[x^0]f = 1$ とする。

$$\exp(g) = f \tag{4}$$
$$\Rightarrow g'f = f' \tag{5}$$
$$\Rightarrow g = \int \frac{f'}{f} dX' \tag{6}$$
$$\tag{7}$$

ただし $[x^0]g = 0$ である。よって g は $O(n \log n)$ で求まる。

1.5 Newton 法による指数の計算

$f = \exp(g)$ を求めたい。$[X^0]g = 0$ とする。$F(X) = \log(X) - f$ として $F(X) = 0 \bmod X^{n+1}$ の解をニュートン法で求めると

$$g_{n+1} = g_n(1 - F(g_n))$$

となる。$\log(1 + X) = X - \frac{X^2}{2} + O(X^3)$ を用いて、

$$F(g_{n+1}) = \log(g_{n+1}) - f \tag{8}$$
$$= \log(g_n) + \log(1 - F(g_n)) - f \tag{9}$$
$$= \log(g_n) - F(g_n) + \frac{g_n^2}{2} - f + O(g_n^3) \tag{10}$$
$$= \frac{g_n^2}{2} + O(g_n^3) \tag{11}$$
$$\tag{12}$$

よって二次収束する。

1.6 初等関数による合成関数

$1, 2, \ldots, n$ が逆元を持つとする。このとき積分が計算できる。よって $\log, \arctan$ に対する合成関数は $\log(f) = \int \frac{f'}{f}$, $\arctan(f) = \int \frac{f'}{1+f^2}$ によって計算できる。$\sin, \cos, \sinh, \cosh$ の合成関数は $\exp$ の線形結合に変形することで計算できる。$\sin, \cos$ については虚数単位 $\sqrt{-1}$ が必要になるので $R = \mathbb{F}_p(\sqrt{-1})$ で計算する。ただし平方剰余の相互法則の第一補充法則より $p \in 4\mathbb{Z} + 1$ のとき $\sqrt{-1} \in \mathbb{F}_p$ であることに注意する。

1.7 一般的な合成関数: Brent-Kung algorithm

参考：http://fredrikj.net/math/rev.pdf
ホーナー法により

$$f(g) = \sum_{k=0} f_k(g)^k \tag{13}$$
$$= f_0 + g(f_1 + g(f_2 + \ldots)) \tag{14}$$
$$\tag{15}$$

とできて $O(n^2 \log n)$ で計算できる。

平方分割により高速化できる。$m = [\sqrt{n}]$ として $h_k := \sum_{i=0}^{m-1} f_{mk+i} g^i$ とすると $f = \sum_{i=0}^{m} h_i g^{mi}$ とできる。g^i の列挙は $O(n^{3/2} \log n)$ で行える。愚直にやっても h_k の列挙は $O(n^2)$ で行える。よって全体で $O(n^2)$ で計算できる。