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。

形式的冪級数　出典：http://sugarknri.hatenablog.com/entry/2019/10/08/001359

$g^2 = f \bmod X^{n+1}$ 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

$$\begin{aligned} g_{n+1}^2 - f =& (\frac{g_n}{2} + \frac{f}{2g_n})^2 - f && (1) \\ =& \frac{1}{4g_n^2}(g_n^2 - f)^2 && (2) \\ & && (3) \end{aligned}$$

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。

$\exp(g) = f \bmod X^{n+1}$ なる g を求めたい。$[x^0]f = 1$ とする。

$$\begin{aligned} & \exp(g) = f && (4) \\ \Rightarrow & g'f = f' && (5) \\ \Leftrightarrow & g = \int \frac{f'}{f} dX' && (6) \\ & && (7) \end{aligned}$$

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

$f = \exp(g) \bmod x^{n+1}$ 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、

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

よって二次収束する。