Algorithm for finding the nth root of modulo p

Takamasa Noguchi

2022/05/31

Description of the algorithm for finding the nth root of modulo p.

1 Introduction

First, this sentence is created by machine translation.[1],[2] There may be some strange sentences.

For $\{p-1=q^L\times m\ \ (\nmid q^x\ \vee\ \mid q^x\ (x\geqq L))\}$, it is the deterministic algorithm.

Last time, the calculation method I created was a prime number, a simple substance, but I added a method to calculate multiple prime numbers. The original calculation method has also been partially modified.

To find the nth root, we need to factoer n into prime factors. In some case, primitive roots are needed. If you don't know these, use the Tonelli-Shanks algorithm.

2 Prerequisites and definitions

$$g = primitive\ root$$
$$p = odd\ prime$$
$$q = prime$$

$$\begin{aligned} p-1=q^L\times m\ &= q_1^{L_1}\times q_2^{L_2}\times\dots q_n^{L_n} \\ F_E &= q_c^{X_c}\times\dots q_n^{X_n}\qquad (X_n=L_n) \\ F_S &= q_c^{X_c}\times\dots q_n^{X_n}\qquad (X_n<L_n) \\ p-1=q^L\times m\ &\nmid\ q_\alpha^{L_\alpha}\times q_\beta^{L_\beta}\times\dots q_\omega^{L_\omega} \\ F_N &= q_\alpha^{L_\alpha}\times q_\beta^{L_\beta}\times\dots q_\omega^{L_\omega} \end{aligned}$$

$$N=\begin{cases} q_\alpha^{L_\alpha}\times q_\beta^{L_\beta}\times\dots q_\omega^{L_\omega} & F_N \\ q_c^{X_c}\times\dots q_n^{X_n}\quad (X_n\geqq L_n) & F_E \\ q_c^{X_c}\times\dots q_n^{X_n}\quad (X_n\geqq L_n\ \wedge\ X_n<L_n) & F_E\times F_S \\ q_\alpha^{L_\alpha}\times q_\beta^{L_\beta}\times\dots q_\omega^{L_\omega}\times q_c^{X_c}\times\dots q_n^{X_n}\quad (X_n\geqq L_n) & F_N\times F_E \\ q_\alpha^{L_\alpha}\times q_\beta^{L_\beta}\times\dots q_\omega^{L_\omega}\times q_c^{X_c}\times\dots q_n^{X_n}\quad (X_n\geqq L_n\ \wedge\ X_n<L_n) & F_N\times F_E\times F_S \end{cases}$$

$$g^n\equiv a\pmod p$$

$$t_k = \frac{(p-1)}{q^k} \quad (q^k < q^L) \qquad t_L = \frac{(p-1)}{q^L} = m$$

$$d = q^{(xL)} - n \quad (n < q^{(xL)} < n + q^L)$$

2.1 Number of ($\mathbf{q^k}$ and $\mathbf{N^k}$)-th roots

2.2 Number of $\mathbf{q^k}$-th roots

$$(p-1) = q^L \times m \quad \{ (\mid q^k \ \vee \ \nmid q^k) \wedge (q^k < p) \}$$

$$(p-1) \equiv x \pmod{q} \begin{cases} \not\equiv \quad 0 \quad nth\ roots = 1 \\ \equiv \quad 0 \quad \begin{cases} (k < L) \quad a^{(t_k)} \equiv x \pmod{p} \begin{cases} \equiv 1 & nth\ roots = q^k \\ \not\equiv 1 & nth\ roots = 0 \end{cases} \\ (k \geqq L) \quad a^{(t_L)} \equiv x \pmod{p} \begin{cases} \equiv 1 & nth\ roots = q^L \\ \not\equiv 1 & nth\ roots = 0 \end{cases} \end{cases} \end{cases}$$

2.3 Number of $\mathbf{N^k}$-th roots

$$N^k \quad (N^k < p) \ \vee \ N \quad (N < p)$$

$$F = F_N \times F_E \times F_S \ \ (L_\omega = L_\omega \ \ \wedge \ \ X_n \leqq L_n)$$

$$(p-1) \equiv x \pmod{F} \begin{cases} \not\equiv \quad 0 \quad \begin{cases} F_N \qquad nth\ roots = 1 \\ F_N \times F_E \quad a^{\left(\frac{p-1}{F_E}\right)} \equiv x \pmod{p} \begin{cases} \equiv 1 & nth\ roots = F_E \\ \not\equiv 1 & nth\ roots = 0 \end{cases} \\ F_N \times F_S \quad a^{\left(\frac{p-1}{F_S}\right)} \equiv x \pmod{p} \begin{cases} \equiv 1 & nth\ roots = F_S \\ \not\equiv 1 & nth\ roots = 0 \end{cases} \\ F_N \times F_E \times F_S \\ \qquad a^{\left(\frac{p-1}{F_E \times F_S}\right)} \equiv x \pmod{p} \begin{cases} \equiv 1 & nth\ roots = F_E F_S \\ \not\equiv 1 & nth\ roots = 0 \end{cases} \end{cases} \\ \equiv \quad 0 \quad \begin{cases} F_E \qquad a^{\left(\frac{p-1}{F_E}\right)} \equiv x \pmod{p} \begin{cases} \equiv 1 & nth\ roots = F_E \\ \not\equiv 1 & nth\ roots = 0 \end{cases} \\ F_S \qquad a^{\left(\frac{p-1}{F_S}\right)} \equiv x \pmod{p} \begin{cases} \equiv 1 & nth\ roots = F_S \\ \not\equiv 1 & nth\ roots = 0 \end{cases} \\ F_E \times F_S \quad a^{\left(\frac{p-1}{F_E \times F_S}\right)} \equiv x \pmod{p} \begin{cases} \equiv 1 & nth\ roots = F_E F_S \\ \not\equiv 1 & nth\ roots = 0 \end{cases} \end{cases} \end{cases}$$

3 Function to find the $\mathbf{q^k}$-th root

3.1 (p - 1 $\nmid$ $\mathbf{q^k}$) $\wedge$ $\mathbf{q^k < p}$

$$(p-1) = q^L \times m \quad \nmid q^k$$

$$s - function \tag{1}$$

$$p \equiv x_1 \pmod{q}$$
$$x_1 \times (q-1) \equiv x_2 \pmod{q}$$
$$(x_2+1)^{(q-2)} \equiv s \pmod{q}$$

$$r = \frac{(p-1) \times s + q^L}{q^{(L+1)}} = \frac{(p-1) \times s + 1}{q}$$
$$r^k \equiv c \pmod{p-1}$$
$$a^c \equiv y \pmod{p}$$
$$a \equiv y^{(q)^k} \pmod{p}$$

3.2 $\mathbf{q^k < q^L}$

3.2.1 If the primitive root is not known

Tonelli-Shanks, Use Algorithm.

3.2.2 When the primitive root is known

$$a^{(t_k)} \equiv 1 \pmod{p}$$
$$s - function \tag{2}$$
$$m \equiv x_1 \pmod{q}$$
$$x_1 \times (q-1) \equiv x_2 \pmod{q}$$
$$x_2^{(q-2)} \equiv s \pmod{q}$$

$$r = \frac{(p-1) \times s + q^L}{q^{(L+1)}}$$
$$r^k \equiv c \pmod{t_k}$$

Phase shift correction method

$$\text{initial value} \quad d = 0 \quad t = 1 \quad w = \frac{(p-1)}{q^t}$$

$$a_n^w \equiv x \pmod{p} \begin{cases} \equiv \quad 1 \quad t = t+1 \quad w = \frac{(p-1)}{q^t} \\ \not\equiv \quad 1 \begin{cases} a_n \times g^{(q^t)} \equiv a_{(n+1)} \pmod{p} \\ d_n + q^t = d_{(n+1)} \quad (distance \ + q^t) \end{cases} \end{cases}$$

$$Repeat\ until \ \{ \ q^t = q^L \ \wedge \ a^w \equiv 1 \pmod{p} \ \}$$

$$\text{roop max } = (q-1) \times (L-k)$$

$$f(x) = \frac{m \times d \times (q-1) \times (q-s)}{q^k}$$

$$a^c \times g^{f(x)} \equiv y_1 \pmod{p}$$

$$(q^k th\ root) - function \qquad (3)$$

$$a \equiv y_1^{(q)^k} \pmod{p}$$

If you don't know the primitive root $\quad p_n^{(t_k)} \equiv h_k \pmod{p} \quad (p_n < p \quad \wedge \quad h_k \not\equiv 1)$

If you know the primitive root $\quad g^{(t_k)} \equiv h_k \pmod{p}$

$$h_k \times y_1 \equiv y_2 \pmod{p} \quad \ldots \quad h_k \times y_{(q^k-1)} \equiv y_{q^k} \pmod{p}$$

$$a \equiv y_1^{(q)^k} \equiv y_2^{(q)^k} \quad \ldots \quad \equiv y_{q^k}^{(q)^k} \pmod{p} \quad = q^k th\ root$$

3.2.3 Example

$$p = 271 \qquad p - 1 = 2 \times 3^3 \times 5 = q^L \times m = 3^3 \times 10 \qquad primitive\ root\ = g = 6$$

$$q^k = 3^1 \qquad g^n = 6^{30} \equiv a \equiv 258 \pmod{p}$$

$$q^k th\ root \begin{cases} a \equiv 114, 217, 211 \\ n \equiv \ 10, 100, 190 \end{cases}$$

$$d = 24$$

$$10 \equiv 1 \pmod{3}$$

$$1 \times (3-1) \equiv 2 \pmod{3}$$

$$2^{(3-2)} \equiv 2 \pmod{3}$$

$$s = 2$$

$$r = \frac{(p-1) \times s + q^L}{q^{(L+1)}} = \frac{270 \times 2 + 3^3}{3^4} = 7$$

$$r^k \equiv c \pmod{t_k} \qquad 7 \equiv 7 \pmod{90}$$

$$f(x) = \frac{m \times d \times (q-1) \times (q-s)}{q^k}$$

$$a^c \times g^{f(x)} \equiv y_1 \pmod{p}$$

$$n_a \times c + \frac{m \times d \times (q-1) \times (q-s)}{q^k} \equiv n \pmod{(p-1)}$$

$$30 \times 7 + \frac{10 \times 24 \times (3-1) \times (3-2)}{3} \equiv 100 \pmod{(p-1)}$$

$$t_k = \frac{(p-1)}{q^k} = \frac{270}{3} = 90$$

$$100 + 90 \equiv 190 \qquad 190 + 90 \equiv 10 \pmod{(p-1)}$$

$$q^k th\ root \qquad n \equiv 10 \equiv 100 \equiv 190$$

$$p = 271 \qquad p - 1 = 2 \times 3^3 \times 5 = q^L \times m = 3^3 \times 10 \qquad primitive\ root\ = g = 6$$

$$q^k = 3^2 \qquad g^n = 6^9 \equiv a \equiv 19 \pmod{p}$$

$$q^k th\ root \begin{cases} a \equiv 6, 193, 201, 97, 94, 133, 168, 255, 208 \\ n \equiv 1, 31, 61, 91, 121, 151, 181, 211, 241 \end{cases}$$

$$d = 18 \qquad s = 2$$

$$r = 7 \qquad r^k \equiv c \equiv 7^2 \equiv 19 \pmod{t_k}$$

$$f(x) = \frac{m \times d \times (q-1) \times (q-s)}{q^k}$$

$$a^c \times g^{f(x)} \equiv y_1 \pmod{p}$$

$$n_a \times c + \frac{m \times d \times (q-1) \times (q-s)}{q^k} \equiv n \pmod{(p-1)}$$

$$9 \times 19 + \frac{10 \times 18 \times (3-1) \times (3-2)}{3^2} \equiv 211 \pmod{(p-1)}$$

$$t_k = \frac{(p-1)}{q^k} = \frac{270}{3^2} = 30$$

$$211 + 30 \equiv 241 \qquad 241 + 30 \equiv 1 \qquad 1 + 30 \equiv 31 \pmod{(p-1)}$$

$$31 + 30 \equiv 61 \qquad 61 + 30 \equiv 91 \qquad 91 + 30 \equiv 121 \pmod{(p-1)}$$

$$121 + 30 \equiv 151 \qquad 151 + 30 \equiv 181 \pmod{(p-1)}$$

$$q^k th\ root \qquad n \equiv 1 \equiv 31 \equiv 61 \equiv 91 \equiv 121 \equiv 151 \equiv 181 \equiv 211 \equiv 241$$

3.3 $\mathbf{q^k \geqq q^L \ \wedge \ q^k < \ p}$

$$a^{(t_L)} \equiv 1 \pmod{p}$$

$$s - function \qquad (2)$$

$$r = \frac{(p-1) \times s + q^L}{q^{(L+1)}}$$

$$r^k \equiv c \pmod{t_L}$$

$$a^c \equiv y_1 \pmod{p}$$

$$(q^k th\ root) - function \tag{4}$$

$$a \equiv y_1^{(q)^k} \pmod{p}$$

If you don't know the primitive root $\quad p_n^{(t_L)} \equiv h_L \pmod{p} \quad (p_n < p \ \wedge \ h_L \not\equiv 1)$

If you know the primitive root $\quad g^{(t_L)} \equiv h_L \pmod{p}$

$$h_L \times y_1 \equiv y_2 \pmod{p} \quad \ldots \quad h_L \times y_{(q^L-1)} \equiv y_{q^L} \pmod{p}$$

$$a \equiv y_1^{(q)^k} \equiv y_2^{(q)^k} \quad \ldots \quad \equiv y_{q^L}^{(q)^k} \pmod{p} \quad = q^k th\ root$$

4 $\mathbf{N^k < p \;\vee\; N < p}$

$$a \equiv x^{(N)^k} \pmod{p} \;\vee\; a \equiv x^N \pmod{p}$$

4.1 $\mathbf{N = q_\alpha^{L_\alpha} \times q_\beta^{L_\beta} \times \dots q_\omega^{L_\omega}}$ $\quad$ $\mathbf{(F_N)^k}$ $\quad$ $\mathbf{((F_N)^k < p)}$

Refer to 3.1 (p - 1 $\nmid$ q^k) $\wedge$ $q^k < p$

$$r_n = \frac{(p-1) \times s + 1}{q_n}$$

$$r_n^{(L_n)} \equiv c_n \pmod{p-1}$$

$$(c_1 \times \dots c_n)^k \equiv R^k \pmod{p-1}$$

$$a^{(R)^k} \equiv y \pmod{p}$$

$$a \equiv y^{(N)^k} \pmod{p}$$

4.2 $\mathbf{N = q_c^{X_c} \times \dots q_n^{X_n}}$ $\mathbf{(X_n \geqq L_n)}$ $\quad$ $\mathbf{(F_E)^k}$ $\quad$ $\mathbf{((F_E)^k < p)}$

$$a^{\left(\frac{p-1}{F_E}\right)} \equiv 1 \pmod{p}$$

Refer to 3.3 $q^k \geqq q^L$ $\wedge$ $q^k < p$

$$r_n = \frac{(p-1) \times s + q_n^{L_n}}{q_n^{(L_n+1)}}$$

$$r_n^{(X_n)} \equiv c_n \pmod{t_L} \quad (X_n \geqq L_n)$$

$$(c_1 \times \dots c_n)^k \equiv R^k \left(\bmod \left(\frac{p-1}{F_E}\right)\right)$$

$$a^{(R)^k} \equiv y_1 \pmod{p}$$

$$(N^k th\ root) - function \tag{5}$$

$$a \equiv y_1^{(N)^K} \pmod{p}$$

If you don't know the primitive root $\quad p_n^{\left(\frac{p-1}{F_E}\right)} \equiv h_F \pmod{p} \quad (p_n < p \;\wedge\; h_F \not\equiv 1)$

If you know the primitive root $\quad g^{\left(\frac{p-1}{F_E}\right)} \equiv h_F \pmod{p}$

$$h_F \times y_1 \equiv y_2 \pmod{p} \;\dots\; h_F \times y_{(F_E-1)} \equiv y_{F_E} \pmod{p}$$

$$a \equiv y_1^{(N)^k} \equiv y_2^{(N)^k} \;\dots\; \equiv y_{F_E}^{(N)^k} \pmod{p} \quad = N^k th\ root$$

4.3 $\mathbf{N = q_c^{X_c} \times \ldots q_n^{X_n} \quad (X_n < L_n) \qquad F_S}$

If you don't know the primitive root, use Tonelli-Shanks Algorithm.

$$a^{\left(\frac{p-1}{F_S}\right)} \equiv 1 \pmod p$$

Refer to 3.2 $q^k < q^L$

$$f_q(x) \begin{cases} r_n = \frac{(p-1)\times s + q_n^{Ln}}{q_n^{(Ln+1)}} \\ r_n^{X_n} \equiv c_n \pmod{t_k} \quad (X_n < L_n) \\ f(x) = \frac{m \times d \times (q-1) \times (q-s)}{q^k} \\ a^{(c_n)} \times g^{f(x)} \equiv b_1 \pmod p \end{cases}$$

$$f_q(b_1) \equiv b_2 \quad f_q(b_2) \equiv b_3 \ldots \equiv b_n \pmod p$$

$$b_n \equiv y_1 \pmod p$$

$$(Nth\ root) - function \tag{6}$$

$$a \equiv y_1^N \pmod p$$

If you don't know the primitive root $\quad p_n^{\left(\frac{p-1}{F_S}\right)} \equiv h_S \pmod p \quad (p_n < p \ \wedge \ h_S \not\equiv 1)$

If you know the primitive root $\quad g^{\left(\frac{p-1}{F_S}\right)} \equiv h_S \pmod p$

$$h_S \times y_1 \equiv y_2 \pmod p \ \ \ldots \ \ h_S \times y_{(F_S-1)} \equiv y_{F_S} \pmod p$$

$$a \equiv y_1^N \equiv y_2^N \ \ \ldots \ \ \equiv y_{F_S}^N \pmod p \quad = Nth\ root$$

4.4 $\mathbf{N = q_c^{X_c} \times \ldots q_n^{X_n} \quad (X_n \geqq L_n \ \wedge \ X_n < L_n) \qquad F_E \times F_S}$

If you don't know the primitive root, use Tonelli-Shanks Algorithm.

$$a^{\left(\frac{p-1}{F_E \times F_S}\right)} \equiv 1 \pmod p$$

F_E

Refer to 4.2 $N = q_c^{X_c} \times \ldots q_n^{X_n} \quad (X_n \geqq L_n)$

$(F_E)^k \quad ((F_E)^k < p)$

$$a^R \equiv y \equiv b_1 \pmod p$$

F_S

Refer to 4.3 $N = q_c^{X_c} \times \ldots q_n^{X_n} \quad (X_n < L_n) \qquad F_S$

$$f_q(b_1) \equiv b_2 \quad f_q(b_2) \equiv b_3 \ldots \equiv b_n \pmod p$$

$$b_n \equiv y_1 \pmod p$$

$$(Nth\ root) - function \quad (7)$$

$$a \equiv y_1^N \pmod{p}$$

If you don't know the primitive root $p_n^{\left(\frac{p-1}{F_E \times F_S}\right)} \equiv h_S \pmod{p} \quad (p_n < p \ \wedge \ h_S \not\equiv 1)$

If you know the primitive root $g^{\left(\frac{p-1}{F_E \times F_S}\right)} \equiv h_S \pmod{p}$

$$h_S \times y_1 \equiv y_2 \pmod{p} \ \ldots \ h_S \times y_{(F_E F_S - 1)} \equiv y_{F_E F_S} \pmod{p}$$

$$a \equiv y_1^N \equiv y_2^N \ \ldots \ \equiv y_{F_E F_S}^N \pmod{p} \quad = Nth\ root$$

4.5 $\mathbf{N = q_\alpha^{L_\alpha} \times q_\beta^{L_\beta} \times \ldots q_\omega^{L_\omega} \ \times \ q_c^{X_c} \times \ldots q_n^{X_n} \quad (X_n \geqq L_n) \quad F_N \times F_E}$

$$a^{\left(\frac{p-1}{F_E}\right)} \equiv 1 \pmod{p}$$

$$\mathrm{F_N}$$

Refer to 4.1 $\mathrm{N} = \mathrm{q}_\alpha^{L_\alpha} \times \mathrm{q}_\beta^{L_\beta} \times \ldots \mathrm{q}_\omega^{L_\omega} \qquad (\mathrm{F_N})^k \quad ((\mathrm{F_N})^k < \ p\ )$

$$r_n = r_\alpha \ , \ r_\beta \ldots r_\omega$$

$$\mathrm{F_E}$$

Refer to 4.2 $\mathrm{N} = \mathrm{q_c}^{X_c} \times \ldots \mathrm{q_n}^{X_n} \quad (X_n \geqq L_n) \qquad (\mathrm{F_E})^k \quad ((\mathrm{F_E})^k < \ p\ )$

$$r_n = r_b \ , \ r_c \ldots r_z$$

$$(r_\alpha^{L_\alpha} \times r_\beta^{L_\beta} \ldots r_\omega^{L_\omega}) \times (r_b^{X_b} \times r_c^{X_c} \ldots r_z^{X_z}) \equiv R \pmod{\left(\frac{p-1}{F_E}\right)} \qquad (X_n \geqq L_n)$$

$$a^R \equiv y_1 \pmod{p}$$

$$a \equiv y_1^N \pmod{p}$$

$$(Nth\ root) - function \quad (5)$$

$$a \equiv y_1^N \equiv y_2^N \ \ldots \ \equiv y_{F_E}^N \pmod{p} \quad = Nth\ root$$

4.6 $\mathbf{N = q_\alpha^{L_\alpha} \times q_\beta^{L_\beta} \times \ldots q_\omega^{L_\omega} \times q_c^{X_c} \times \ldots q_n^{X_n}}$ $\mathbf{(X_n < L_n)}$ $\mathbf{F_N \times F_S}$

If you don't know the primitive root, use Tonelli-Shanks Algorithm.

$$a^{\left(\frac{p-1}{F_S}\right)} \equiv 1 \pmod p$$

F_N

Refer to 4.1 $N = q_\alpha^{L_\alpha} \times q_\beta^{L_\beta} \times \ldots q_\omega^{L_\omega}$ $(F_N)^k$ $((F_N)^k < p)$

$$a^R \equiv y \equiv b_1 \pmod p$$

F_S

Refer to 4.3 $N = q_c^{X_c} \times \ldots q_n^{X_n}$ $(X_n < L_n)$ F_S

$$f_q(b_1) \equiv b_2 \quad f_q(b_2) \equiv b_3 \ldots \equiv b_n \pmod p$$
$$b_n \equiv y_1 \pmod p$$
$$a \equiv y_1^N \pmod p$$

$$(Nth\ root) - function \quad (6)$$

$$a \equiv y_1^N \equiv y_2^N \quad \ldots \quad \equiv y_{F_S}^N \pmod p \quad = Nth\ root$$

4.7 $\mathbf{N = q_\alpha^{L_\alpha} \times q_\beta^{L_\beta} \times \ldots q_\omega^{L_\omega} \times q_c^{X_c} \times \ldots q_n^{X_n}}$ $\mathbf{(X_n \geqq L_n \ \wedge \ X_n < L_n)}$ $\mathbf{F_N \times F_E \times F_S}$

If you don't know the primitive root, use Tonelli-Shanks Algorithm.

$$a^{\left(\frac{p-1}{F_S \times F_S}\right)} \equiv 1 \pmod p$$

$F_N \times F_E$

Refer to 4.5 $N = q_\alpha^{L_\alpha} \times q_\beta^{L_\beta} \times \ldots q_\omega^{L_\omega} \times q_c^{X_c} \times \ldots q_n^{X_n}$ $(X_n \geqq L_n)$ $F_N \times F_E$

$$(r_\alpha^{L_\alpha} \times r_\beta^{L_\beta} \ldots r_\omega^{L_\omega}) \times (r_b^{X_b} \times r_c^{X_c} \ldots r_z^{X_z}) \equiv R \pmod{\left(\frac{p-1}{F_E}\right)} \qquad (X_n \geqq L_n)$$

$$a^R \equiv y \equiv b_1 \pmod p$$

F_S

Refer to 4.3 $N = q_c^{X_c} \times \ldots q_n^{X_n}$ $(X_n < L_n)$ F_S

$$f_q(b_1) \equiv b_2 \quad f_q(b_2) \equiv b_3 \ldots \equiv b_n \pmod{p}$$
$$b_n \equiv y_1 \pmod{p}$$
$$a \equiv y_1^N \pmod{p}$$

$$(Nth\ root) - function \quad (7)$$

$$a \equiv y_1^N \equiv y_2^N \quad \ldots \quad \equiv y_{F_E F_S}^N \pmod{p} \quad = Nth\ root$$

5 Memo

$$f(x) = x + \frac{1}{n} \qquad a^{f(x)} \equiv b \pmod{p}$$
$$a^{\left(\frac{p-1}{n}\right)} \equiv 1 \pmod{p}$$
$$a^x \equiv b_1 \pmod{p}$$
$$a \equiv y_1^{(n)} \pmod{p} \quad = nth\ root$$
$$a \equiv y_1^{(n)} \equiv y_2^{(n)} \quad \ldots \quad \equiv y_n^{(n)} \pmod{p} \quad = nth\ root$$
$$(b_1 \times y_\omega)^n \equiv b^{\left\{(x+\frac{1}{n})\times n\right\}} \pmod{p}$$
$$b_1 \times y_\omega \equiv b \equiv a^{f(x)} \pmod{p}$$

6 Conclusion

We have created a calculation method, but unfortunately we do not have a theoretical proof. So, in the case of huge prime numbers or special prime numbers, it may be wrong.

References

[1] https://translate.google.com google translation

[2] https://www.deepl.com DeepL translation

[3] S.Serizawa 『Introduction to Number Theory
-You can learn while understanding the proof』
Kodansha company 2008 (140-175)

[4] Y.Yasufuku『Accumulating discioveries and anticipation
-That is Number Theory』 Ohmsha company 2016 (64-102)

ehime-JAPAN