Algorithm for finding q^k-th root of a [2]

Takamasa Noguchi

2022/04/11

Description of the algorithm for finding the q^k-th root of a.

1 Introduction

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

There is no basic difference in the calculation method created in the previous version. Some additions and changes have been made.

In some cases, a primal root may be required for the calculation. If the calculation requires a primitive root and the primitive root is not known, use the Tonelli-Shanks algorithm.

2 Prerequisites and definitions

$$g = primitive\ root$$

$$p = odd\ prime$$

$$q = prime$$

$$p - 1 = q^L \times m$$

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

$$a \equiv x^{(q^k)} \pmod{p} \qquad (q^k < p)$$

$$(\ L > 0\ ) \qquad a^{\left(\frac{p-1}{x_1}\right)} \equiv 1 \pmod{p} \begin{cases} k < L & x_1 = q^k \\ k \geqq L & x_1 = q^L \end{cases}$$

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

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

3 Number of q^k-th roots

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

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

4 Function to find the q^k-th root

4.1 $q^L = 1 \ \wedge\ q^k < p$

$$(p-1) = q^L \times m = m \qquad (\ L = 0\ )$$

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

$$p \equiv x_1 \pmod{q}$$

$$x_1 \times (q-1) \equiv x_2 \pmod{q}$$

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

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

$$r^k \equiv c \pmod{p-1}$$

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

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

4.2 $q^k < q^L$

4.2.1 If the primitive root is not known

Tonelli-Shanks, Use Algorithm.

4.2.2 When the primitive root is known

$$s - function \tag{2}$$

$$m \equiv x_1 \pmod{q}$$

$$x_1 \times (q-1) \equiv x_2 \pmod{q}$$

$$x_2^{(q-2)} \equiv s \pmod{q}$$

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

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

Phase shift correction method

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

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

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

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

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

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

$$(q^k th\ root) - function \tag{3}$$

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

$$g^{(t_k)} \equiv h_k \pmod{p}$$

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

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

4.2.3 Example

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

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

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

$$d = 24$$

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

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

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

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

$$r^k \equiv c \pmod{t_L} \qquad 7 \equiv 7 \pmod{10}$$

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

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

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

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

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

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

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

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

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

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

$$d = 18$$

$$r = 7 \qquad r^k \equiv c \equiv 7^2 \equiv 9 \pmod{t_L}$$

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

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

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

$$9 \times 9 + 18 \times 10 \times \left(\frac{2}{3^2}\right) \equiv 121 \pmod{(p-1)}$$

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

$$121 + 30 \equiv 151 \qquad 151 + 30 \equiv 181 \qquad 181 + 30 \equiv 211 \pmod{(p-1)}$$

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

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

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

4.3 $\mathbf{q^k \geqq q^L \ \wedge \ q^k < \ p}$

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

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

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

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

$$(q^k th\ root) - function \quad (4)$$

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

$$g^{(t_L)} \equiv h_L \pmod{p}$$

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

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

5 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