Algorithm for finding q^k-th root of a $[\ q = Prime \qquad a \equiv x^{(q^k)} \pmod p\ ]$

Takamasa Noguchi

2021/10/19

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.

Primitive roots are not required for $\{(p-1) = q^L \times m \quad (L = 0)\}$ and $\{k = L\}$, but are required for the other cases.

If the calculation requires a primitive root and the primitive root is not known, use the Tonelli-Shanks algorithm.

2 Prerequisites

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

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

$$g^{(q^k \times n)} \equiv a \pmod p \qquad (\ k \leqq L\ )$$

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

$$a^{\left(\frac{p-1}{q^k}\right)} \equiv 1 \pmod p \qquad (\ L > 0\ )$$

3 Function to find the q^k-th root

3.1 k ≧ 1 L = 0

$$q < p$$

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

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

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

$$p \equiv x_1 \pmod q$$

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

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

$$r^k \equiv c \pmod{p-1}$$
$$a^c \equiv y \pmod{p} \qquad a \equiv y^{(q^k)} \pmod{p}$$

3.2 k ≦ L

$$(p-1) = q^L \times m \qquad (k \leqq L)$$
$$g^{(q^k \times n)} \equiv a \pmod{p} \quad a^{\left(\frac{p-1}{q^k}\right)} \equiv 1 \pmod{p}$$

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

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

Moving method

$$w = \frac{(p-1)}{q^t} \quad t = 1 \qquad mv = 0 \quad (\ moving\ distance\ )$$

$$a^w \equiv x \pmod{p} \begin{cases} \equiv \quad 1 \quad t = t+1 \quad w = \frac{(p-1)}{q^t} \\ \not\equiv \quad 1 \begin{cases} qm = q^{(t-1)} \quad a \times g^{(qm)} \equiv a \pmod{p} \\ mv = mv + q^{(t-1)} \quad (Move\ \ + q^{(t-1)}) \end{cases} \end{cases}$$

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

$$a = x \begin{cases} = 1 & mv = mv + q^L \\ \neq 1 & mv = mv \end{cases}$$

$$mv = (\ moving\ distance\ )$$

Correction method

$$g^{(q^k \times n)} \equiv a \pmod p$$

$$a \times g^{mv} \equiv a_1 \pmod p$$

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

$$a_1^c \equiv a_2 \pmod p$$

$$m = mv \times \frac{1}{q^k}$$

$$g^{(p-2)} \equiv h_f \pmod p$$

$$a_2 \times h_f^m \equiv y_1 \pmod p$$

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

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

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

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

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

3.3 k = L

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

$$g^{(q^L \times n)} \equiv a \pmod p \qquad a^{\left(\frac{p-1}{q^L}\right)} \equiv 1 \pmod p$$

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

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

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

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

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

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

4 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