How to Find the Surplus Root (Prime Number) in Power Surplus of Prime Numbers

Takamasa Nguchi

2021/04/27

Explanation of how to find the root of the remainder (prime number) in power remainder of prime numbers.

1 Introduction

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

There are already various formulas for calculating power remainders and roots of remainders. Based on these, I have created a simple and quick way to calculate it. However, there is no theoretical proof.

2 $x^2 \equiv a \pmod{p}$

2.1 Definition of value

$$p = odd\ prime \quad g = primitive\ root \quad g^x \equiv a \pmod{p}$$
$$Quadratic\ residue = g^{2n} \equiv a^{(\frac{p-1}{2})} \equiv 1 \pmod{p} \quad [4]$$
$$Quadratic\ nonresidue = g^{2n+1} \equiv a^{(\frac{p-1}{2})} \equiv -1 \pmod{p} \quad [4]$$

2.2 Function to find the root of a square remainder

$$(p-1) = q^k \times n$$

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

$$\left(g^{(q^k \times n)}\right)^r \equiv a \pmod{p} \qquad g^{(q^k \times n)} \equiv (\pm a)^2 \pmod{p}$$

However, in the case of { $g^x \equiv 1 \pmod{p}$ }, the root of the square surplus cannot be calculated.

2.3 How to find $x^2 \equiv a \pmod p$

"x" assumes that there is a quadratic residue.

$$g^{2n} \equiv \pm x^2 \pmod p$$

$$(p-1) = 2^k \times n \qquad r = \frac{(p-1)+2^k}{2^{(k+1)}} \qquad j = \frac{(p-1)}{2^k}$$

$$\left(g^{(2^k \times n)}\right)^r \equiv a \pmod p \qquad g^{(2^k \times n)} \equiv (\pm a)^2 \pmod p$$

Correction method

$$\left(g^{(2^k \times n)}\right)^r \equiv a \pmod p$$

$$m = (p-1) - (moving\ distance) \times \frac{1}{2} \qquad g^{(\frac{x}{2})} = moving\ distance \times \frac{1}{2}$$

$$g^m \equiv f \pmod p \qquad f \times a \equiv y \pmod p \qquad \pm y = Quadratic\ residue\ root$$

First check the value of (k).
↓
Then calculate (r) from (k).
↓
Go from { g^{2n} } to the nearest { $g^{(2^k \times n)}$ } and calculate the root of the square surplus.
↓
Corrects the root of the square surplus according to the distance traveled.

However, in the case of { $g^x \equiv 1 \pmod p$ }, the root of the square surplus cannot be calculated.

2.4 Flowchart

$$(p-1) = 2^k \times n \qquad r = \frac{(p-1)+2^k}{2^{(k+1)}} \qquad j = \frac{(p-1)}{2^k}$$

$g^{2n} \equiv a \pmod p$

↓

$$k = 1 \begin{cases} r = \frac{(p-1)+2^k}{2^{(k+1)}} = \frac{p+1}{4} \qquad \left(g^{(2^k \times n)}\right)^r = \left(g^{(2n)}\right)^r \\ a^r \equiv b \pmod p \qquad a \equiv (\pm b)^2 \pmod p \\ fin. \end{cases}$$

↓

$$a^j \equiv -1 \pmod p \quad j = \frac{(p-1)}{2^t} \quad t = 2$$

↓

$$a \times g^m \equiv b_1 \pmod p \qquad m = 2^{(t-1)} \qquad (Move\ +2)$$

↓

$$b_1^j \equiv 1 \pmod p \quad j = \frac{(p-1)}{2^t} \quad t = 2 \quad \rightarrow \quad t = 3$$

$$b_1^j \equiv -1 \pmod p \quad j = \frac{(p-1)}{2^t} \quad t = 3$$

$\downarrow$
$b_1 \times g^m \equiv b_2 \pmod p \quad m = 2^{(t-1)} \quad (Move\ +4)$
$\downarrow$
$b_2^j \equiv -1 \pmod p \quad j = \frac{(p-1)}{2^t} \quad t = 3$
$\downarrow$
$b_2 \times g^m \equiv b_3 \equiv 1 \pmod p \quad NG \quad m = 2^{(t-1)} \quad (Move\ +4)$
$\downarrow$
$b_3 \times g^m \equiv b_4 \pmod p \quad m = 2^{(t-1)} \quad (Move\ +4)$
$\downarrow$
$\downarrow$

$\downarrow$
$b_n^j \equiv 1 \pmod p \quad j = \frac{(p-1)}{2^t} \quad t = k$
$\left(g^{(2^k \times n)}\right)^r \equiv h \pmod p \quad r = \frac{(p-1)+2^k}{2^{(k+1)}} \quad \pm h = Quadratic\ residue\ root$
$\downarrow$
$d = (p-1) - ((\ moving\ distance\ ) \times \frac{1}{2})$
$g^d \equiv f \pmod p$
$\downarrow$
$f \times h \equiv y \pmod p$
$\downarrow$
$a \equiv (\pm y)^2 \pmod p$

3 $x^3 \equiv a \pmod p$

3.1 Definition of value

$p \geqq 13 \qquad g = primitive\ root \quad (g = 2, 3, 5, 7, \ldots P_n)$
$g^x \equiv a \pmod p$

3.2 Judgment by type

$$p \geqq 13 \qquad (p-1) = q^k \times n$$

1. $p \equiv 2 \pmod 3$
2. $p \not\equiv 2 \ \wedge \ n \equiv 1 \pmod 3$
3. $p \not\equiv 2 \ \wedge \ n \equiv 2 \pmod 3$

3.3 Function to find the cubic surplus root

$$(p-1) = q^k \times n$$

type1. type2. s = 2 type 3. s = 1

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

$$\left(g^{(q^k \times n)}\right)^r \equiv a \pmod{p} \qquad g^{(q^k \times n)} \equiv a^3 \pmod{p}$$

However, in the case of $\{\ g^x \equiv 1 \pmod{p}\ \}$, the cubic surplus root cannot be calculated.

3.4 How to find 1 type 1. $p \equiv 2 \pmod{3}$

$$g^n \equiv a \pmod{p} \qquad (p-1) = q^k \times n \qquad s = 2$$

$$q = 3 \qquad k = 0 \qquad (p-1) = n$$

$$r = \frac{(p-1) \times s + q^k}{q^{(k+1)}} = \frac{(p-1) \times 2 + 3^k}{3^{(k+1)}} = \frac{(p-1) \times 2 + 1}{3}$$

$$a^r \equiv b \pmod{p} \qquad a \equiv b^3 \pmod{p} \qquad = \textit{Cubic surplus root}$$

3.5 How to find 2 type 2. type 3. $(k = 1)$

"a" assumes that there is a cubic surplus.

$$g^{3n} \equiv a \pmod{p} \qquad a^{(\frac{p-1}{3})} \equiv 1 \pmod{p} \qquad (p-1) = q^k \times n$$

$$q = 3 \qquad k = 1 \qquad (p-1) = 3 \times n \qquad type2.\ \ s = 2 \qquad type3.\ \ s = 1$$

$$type\ 2 \qquad r = \frac{(p-1) \times s + 3^k}{3^{(k+1)}} = \frac{(p-1) \times 2 + 3}{3^2}$$

$$type\ 3 \qquad r = \frac{(p-1) \times s + 3^k}{3^{(k+1)}} = \frac{(p-1) + 3}{3^2}$$

$$a^r \equiv b \pmod{p}$$

$$g^j \equiv h \pmod{p} \qquad j = \frac{(p-1)}{3}$$

$$h \times b \equiv c \pmod{p} \qquad h \times c \equiv d \pmod{p}$$

$$a \equiv b^3 \equiv c^3 \equiv d^3 \pmod{p} \qquad = \textit{Cubic surplus root}$$

3.6 How to find 3 type 2. type 3. $(k \geqq 2)$

"a" assumes that there is a cubic surplus.

$$g^{3n} \equiv a \pmod{p} \qquad a^{(\frac{p-1}{3})} \equiv 1 \pmod{p} \qquad (p-1) = q^k \times n$$

$$q = 3 \qquad (p-1) = 3^k \times n \qquad type2.\ \ s = 2 \qquad type3.\ \ s = 1$$

$$type\ 2 \qquad r = \frac{(p-1) \times s + q^k}{q^{(k+1)}} = \frac{(p-1) \times 2 + 3^k}{3^{(k+1)}}$$

$$type\ 3 \qquad r = \frac{(p-1) \times s + q^k}{q^{(k+1)}} = \frac{(p-1) + 3^k}{3^{(k+1)}}$$

$$\left(g^{(3^k \times n)}\right)^r \equiv b \pmod{p} \qquad g^{(3^k \times n)} \equiv b^3 \pmod{p}$$

$$g^j \equiv h \pmod{p} \qquad j = \frac{(p-1)}{3}$$

$$h \times b \equiv c \pmod{p} \qquad h \times c \equiv d \pmod{p}$$

$$g^{(3^k \times n)} \equiv b^3 \equiv c^3 \equiv d^3 \pmod{p} \qquad = \mathit{Cubic\ surplus\ root}$$

Moving method

$$(p-1) = 3^k \times n \qquad j = \frac{(p-1)}{3^t} \quad t_1 = 1$$

$$a^j \equiv x \pmod{p} \begin{cases} \equiv \quad 1 \quad t_n + 1 = t_{(n+1)} \quad a^j \equiv x \pmod{p} \\ \not\equiv \quad 1 \quad a_n \times g^s \equiv a_{(n+1)} \pmod{p} \quad s = 3^{t_n} \qquad (\mathit{Move}\ +3^s) \end{cases}$$

$$\mathit{Repeat\ until}\ \{\ t_n = k \quad a^j \equiv 1 \pmod{p}\ \}$$

$$a \times g^{(\ \mathit{moving\ distance}\ )} \equiv g^{(3^k \times n)} \pmod{p}$$

Correction method

$$g^{(3^k \times n)} \equiv b^3 \equiv c^3 \equiv d^3 \pmod{p} \qquad = \mathit{Cubic\ surplus\ root}$$

$$g^m \equiv f \pmod{p} \qquad m = (p-1) - (\mathit{moving\ distance}) \times \frac{1}{3}$$

$$f \times b \equiv b_2 \pmod{p} \qquad f \times c \equiv c_2 \pmod{p} \qquad f \times d \equiv d_2 \pmod{p}$$

$$a \equiv b_2^3 \equiv c_2^3 \equiv d_2^3 \qquad = \mathit{cubic\ surplus\ root}$$

First check the value of (k).
↓
Then calculate (r) from (k).
↓
Go from { g^{3n} } to the nearest { $g^{(3^k \times n)}$ } and calculate the root of the cubic remainder.
↓
Corrects to cubic surplus root according to the distance traveled.

However, in the case of { $g^x \equiv 1 \pmod{p}$ }, the cubic surplus root cannot be calculated.

4 $x^q \equiv a \pmod p$

$$g^n \equiv a \pmod p \quad g = primitive\ root \quad (g = 2, 3, 5, 7, \dots P_n)$$

4.1 Function to find the surplus root

$$(p-1) = q^k \times n \quad (q = 2, 3, 5, 7, 11, \dots p_n)$$
$$r = \frac{(p-1) \times s + q^k}{q^{(k+1)}}$$
$$\left(g^{(q^k \times n)}\right)^r \equiv b \pmod p \qquad g^{(q^k \times n)} \equiv b^q \pmod p$$

4.2 k = 0

$$(p-1) = q^k \times n = n \quad k = 0 \quad (q = 2, 3, 5, 7, 11, \dots p_n)$$
$$g^n \equiv a \pmod p$$
$$r = \frac{(p-1) \times s + q^k}{q^{(k+1)}} = \frac{(p-1) \times s + 1}{q}$$
$$a^r \equiv b \pmod p \qquad a \equiv b^q \pmod p$$

I think the function to find "s" is as follows.

$$p \equiv x_1 \pmod q$$

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

4.3 k $\geqq$ 1

"a" assumes that there is a surplus root.

$$(p-1) = q^k \times n \quad (k \geqq 1) \quad (q = 2, 3, 5, 7, 11, \dots p_n)$$
$$g^{(qn)} \equiv a \pmod p \quad a^{\left(\frac{p-1}{q}\right)} \equiv 1 \pmod p$$
$$r = \frac{(p-1) \times s + q^k}{q^{(k+1)}}$$
$$\left(g^{(q^k \times n)}\right)^r \equiv b \pmod p \qquad g^{(q^k \times n)} \equiv b^q \pmod p$$

$$q = 5 \quad n \equiv x \pmod 5 \begin{cases} \equiv 1 & s = 4 \\ \equiv 2 & s = 2 \\ \equiv 3 & s = 3 \\ \equiv 4 & s = 1 \end{cases} \qquad q = 7 \quad n \equiv x \pmod 7 \begin{cases} \equiv 1 & s = 6 \\ \equiv 2 & s = 3 \\ \equiv 3 & s = 2 \\ \equiv 4 & s = 5 \\ \equiv 5 & s = 4 \\ \equiv 6 & s = 1 \end{cases}$$

Based on the above calculations, I believe that the function to find "s" should be as follows.

$$n \equiv x_1 \pmod q$$

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

$$\left(g^{(q^k \times n)}\right)^r \equiv b \pmod p \qquad g^{(q^k \times n)} \equiv b^q \pmod p$$

$$g^j \equiv h \pmod p \qquad j = \frac{(p-1)}{q}$$

$$h \times b \equiv b_1 \pmod p \quad \dots \quad h \times b_{q-2} \equiv b_{q-1} \pmod p$$

$$g^{(q^k \times n)} \equiv b^q \equiv \quad \dots \quad \equiv b_{q-1}^q \pmod p \quad = \textit{surplus root}$$

Moving method

$$(p-1) = q^k \times n \qquad j = \frac{(p-1)}{q^t} \quad t_1 = 1$$

$$a^j \equiv x \pmod p \begin{cases} \equiv & 1 \quad t_n + 1 = t_{(n+1)} \quad a^j \equiv x \pmod p \\ \not\equiv & 1 \quad a_n \times g^s \equiv a_{(n+1)} \pmod p \quad s = q^{t_n} \quad (Move\ + q^s) \end{cases}$$

$$Repeat\ until\ \{\ t_n = k \quad a^j \equiv 1 \pmod p\ \}$$

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

Correction method

$$g^{(q^k \times n)} \equiv b^q \equiv \quad \dots \quad \equiv b_{q-1}^q \pmod p \quad = \textit{surplus root}$$

$$g^m \equiv f \pmod p \qquad m = (p-1) - (moving\ distance) \times \frac{1}{q}$$

$$f \times b \equiv c_1 \pmod p \quad \dots \quad f \times b_{q-1} \equiv c_q \pmod p$$

$$a \equiv c_1^q \equiv \quad \dots \quad \equiv c_q^q \pmod p \quad = \textit{surplus root}$$

However, in the case of $\{\ g^x \equiv 1 \pmod p\ \}$, the surplus root cannot be calculated.

5 Conclusion

We have created a calculation method, but unfortunately we do not have a theoretical proof. So, if it is a huge prime number or special prime number, may be wrong.

6 Example

$$-- \quad (p = 37) \quad --$$

$$(p-1) = 2^2 \times 3^2 \quad q = 3 \quad k = 2 \quad g = 2 \quad 2^2 \equiv 1 \pmod{3}$$

$$\frac{p-1}{3} = 12 \quad \frac{p-1}{3^2} = 4 \quad r = \frac{(36 \times 2 + 3^2)}{3^3} = 3$$

$$-- \quad (\bmod 37) \quad --$$

$$g^x \equiv 2^{24} \equiv 10$$

$$\frac{p-1}{3} = 12 \quad 10^{12} \equiv 1 \quad 10^4 \equiv 10$$

$$10 \times 2^3 \equiv 6$$

$$\frac{p-1}{3^2} = 4 \quad 6^4 \equiv 1$$

$$r = \frac{(36 \times 2 + 3^2)}{3^3} = 3 \quad 6^3 \equiv 31$$

$$\frac{p-1}{3} = 12 \quad 2^{12} \equiv 26$$

$$26 \times 31 \equiv 29 \quad 26 \times 29 \equiv 14$$

$$(p-1) - \frac{3}{3} = 35 \quad 2^{35} \equiv 19$$

$$19 \times 31 \equiv 34 \quad 19 \times 29 \equiv 33 \quad 19 \times 14 \equiv 7$$

$$10 \equiv 34^3 \equiv 33^3 \equiv 7^3$$

$$-- \quad (p = 43) \quad --$$

$$(p-1) = 2 \times 3 \times 7 \quad q = 7 \quad k = 1 \quad g = 3$$

$$\frac{p-1}{7} = 6 \quad r = \frac{(42 \times 1 + 7)}{7^2} = 1$$

$$-- \quad (\bmod 43) \quad --$$

$$g^x \equiv 3^{28} \equiv 6$$

$$\frac{p-1}{7} = 6 \quad 6^6 \equiv 1$$

$$6 \equiv 6 \pmod{7} \quad 6 \times 6 \equiv 1 \pmod{7} \quad 1^5 \equiv 1 \pmod{7} \quad s = 1$$

$$r = \frac{(42 \times 1 + 7)}{7^2} = 1 \quad 6^1 \equiv 6$$

$$\frac{p-1}{7} = 6 \quad 3^6 \equiv 41$$

$$41 \times 6 \equiv 31 \quad 41 \times 31 \equiv 24 \quad 41 \times 24 \equiv 38$$

$$41 \times 38 \equiv 10 \quad 41 \times 10 \equiv 23 \quad 41 \times 23 \equiv 40$$

$$6 \equiv 6^7 \equiv 31^7 \equiv 24^7 \equiv 38^7 \equiv 10^7 \equiv 23^7 \equiv 40^7$$

$$-- \quad (p = 97) \quad --$$
$$(p-1) = 2^5 \times 3 \qquad g = 5$$

$$-- \quad (\bmod 97) \quad --$$
$$q = 19 \qquad k = 0$$
$$g^x \equiv 5^{57} \equiv 67$$
$$97 \equiv 2 \pmod{19} \qquad 2 \times 18 \equiv 17 \pmod{19} \qquad 18^{17} \equiv 18 \pmod{19} \qquad s = 18$$
$$r = \frac{((p-1) \times 18 + 1)}{19} = 91 \qquad 67^{91} \equiv 28$$
$$67 \equiv 28^{19}$$

$$-- \quad (\bmod 97) \quad --$$
$$q = 2 \qquad k = 5 \qquad r = \frac{(p+31)}{2^6} = 2 \qquad m = \frac{(p-1)}{2^k}$$
$$g^{2x} \equiv 2^{70} \equiv 3$$
$$\downarrow$$
$$3^{24} \equiv -1 \qquad m = \frac{(p-1)}{2^k} \qquad k = 2$$
$$\downarrow$$
$$3 \times 5^2 \equiv 75 \qquad n + 2$$
$$\downarrow$$
$$75^{24} \equiv 1 \qquad m = \frac{(p-1)}{2^k} \qquad k = 2$$
$$75^{12} \equiv -1 \qquad m = \frac{(p-1)}{2^k} \qquad k = 3$$
$$\downarrow$$
$$75 \times 5^4 \equiv 24 \qquad n + 4$$
$$\downarrow$$
$$24^{12} \equiv -1 \qquad m = \frac{(p-1)}{2^3} \qquad k = 3$$
$$\downarrow$$
$$24 \times 5^4 \equiv 62 \qquad n + 4$$
$$\downarrow$$
$$62^{12} \equiv 1 \qquad m = \frac{(p-1)}{2^k} \qquad k = 3$$
$$62^6 \equiv 1 \qquad m = \frac{(p-1)}{2^k} \qquad k = 4$$
$$62^3 \equiv -1 \qquad m = \frac{(p-1)}{2^k} \qquad k = 5$$

$$\downarrow$$

$$62 \times 5^{16} \equiv 1 \quad n+16 \quad g^x \equiv 1 \;\; NG$$

$$1 \times 5^{16} \equiv 36 \quad n+16$$

$$\downarrow$$

$$36^3 \equiv -1 \quad m = \frac{(p-1)}{2^k} \quad k=5$$

$$\downarrow$$

$$36 \times 5^{16} \equiv 35 \quad n+16$$

$$35^3 \equiv 1 \quad m = \frac{(p-1)}{2^k} \quad k=5$$

$$\downarrow$$

$$35^2 \equiv 61$$

$$\downarrow$$

$$96 - ((2+4+4+16+16+16) \times \frac{1}{2}) = 67$$

$$5^{67} \equiv 59$$

$$\downarrow$$

$$61 \times 59 \equiv 10$$

$$3 \equiv (\pm 10)^2 \pmod{97}$$

$$Quadratic\ residue\ root = 10, 87$$

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