How to find the quadratic residue for prime numbers

Takamasa Nguchi

2021/03/31

Explanation of how to find the quadratic residue.

1 Introduction

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

Great seniors are studying quadratic residues,and various formulas already exist. I tried to summarize based on these.

2 Definition of the required numerical value

$p = odd\ prime \qquad g = primitive\ root \quad g = 2, 3, 5, 7, \ldots P_n$

$g^x \equiv a \pmod p$

$Quadratic\ residue \quad = g^{2n} \equiv a^{(\frac{p-1}{2})} \equiv 1 \pmod p$ [3]

$Quadratic\ nonresidue = g^{2n+1} \equiv a^{(\frac{p-1}{2})} \equiv -1 \pmod p$ [3]

3 Formula for finding quadratic residue

$$(p-1) = 2^k \times n$$

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

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

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

4 How to find $\{g^{2n} \equiv \pm(x)^2 \pmod p\}$

"x" assumes that there is a quadratic residue.

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

4.1 $2^1 \times n$

$$(p-1) = 2^k \times n = 2^1 \times n$$

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

$$\left(g^{(2^k \times n)}\right)^r = \left(g^{(2n)}\right)^r$$

$$\left(g^{(2n)}\right)^r \equiv a \pmod p \qquad \pm a = \textit{Quadratic residue}$$

4.2 $2^k \times n$

$$(p-1) = 2^k \times n$$

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

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

First check the value of k.
↓
Next,increase the oder from the aaa formula $\{\frac{(p-1)}{2^k}\}$ move to the place where the value of "k" is reached.
↓
Find the quadratic residue from $\{\left(g^{(2^k \times n)}\right)^r \equiv a \pmod p\}$ and apply the correction according to the distance traveled.

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

4.3 Supplement

$(p-1) = 2^2 \times n \quad k=2 \quad r = \frac{(p+3)}{2^3} \quad m = \frac{(p-1)}{2^k} \quad \left(g^{(2^2 \times n)}\right)^r \equiv a \pmod p$

n	$f(x)$ $\pmod p$		n/2	$f(x)$ $\pmod p$
$4n$	Quadratic residue($\pm c$)	$(g^{4n})^r \equiv c$	$2n$	c
$4n+3$	Quadratic nonresidue		——	
$4n+2$	Quadratic residue($\pm b$)	$(g^{4n})^r \not\equiv b$	$2n+1$	$b \equiv c \times f(x)$
$4n+1$	Quadratic nonresidue		——	
$4n$	Quadratic residue($\pm a$)	$(g^{4n})^r \equiv a$	$2n$	a

$$g^{2x} \equiv g^{(4n+2)} \equiv b \pmod p$$
$\downarrow$
$$\left(g^{2x}\right)^m \equiv -1 \pmod p \quad m = \frac{(p-1)}{2^k} \quad k = 2$$
$\downarrow$
$$g^{2x} \times g^2 \equiv g^{4n} \pmod p \qquad n+2$$
$\downarrow$
$$\left(g^{4n}\right)^m \equiv 1 \pmod p \quad m = \frac{(p-1)}{2^k} \quad k = 2$$
$\downarrow$
$$\left(g^{4n}\right)^r \equiv a \pmod p$$
$\downarrow$
$$f(x) \begin{cases} d = (p-1) - (2 \times \frac{1}{2}) \\ g^d \equiv c \pmod p \end{cases}$$
$\downarrow$
$$a \times f(x) \equiv y \pmod p$$
$\downarrow$
$$b \equiv y \pmod p$$

$$(p-1) = 2^3 \times n \quad k = 3 \quad r = \frac{(p+7)}{2^4} \quad m = \frac{(p-1)}{2^k} \quad \left(g^{(2^3 \times n)}\right)^r \equiv a \pmod p$$

n	$f(x) \pmod p$		n/2	$f(x) \pmod p$
$8n+1$	Quadratic nonresidue		——	
$8n$	Quadratic residue($\pm e$)	$g^{(\frac{p-1}{8})} \equiv 1 \quad (g^{8n})^r \equiv e$	$4n$	e
$8n+7$	Quadratic nonresidue		——	
$8n+6$	Quadratic residue($\pm d$)	$g^{(\frac{p-1}{4})} \equiv -1$	$4n+3$	$d \equiv e \times f(x_1)$
$8n+5$	Quadratic nonresidue		——	
$8n+4$	Quadratic residue($\pm c$)	$g^{(\frac{p-1}{4})} \equiv 1 \quad (g^{8n})^r \not\equiv c$	$4n+2$	$c \equiv e \times f(x_2)$
$8n+3$	Quadratic nonresidue		——	
$8n+2$	Quadratic residue($\pm b$)	$g^{(\frac{p-1}{4})} \equiv -1$	$4n+1$	$b \equiv e \times f(x_3)$
$8n+1$	Quadratic nonresidue		——	
$8n$	Quadratic residue($\pm a$)	$g^{(\frac{p-1}{8})} \equiv 1 \quad (g^{8n})^r \equiv a$	$4n$	a

$$g^{2x} \equiv g^{(8n+2)} \equiv b \pmod p$$
$\downarrow$
$$\left(g^{2x}\right)^m \equiv -1 \pmod p \qquad m = \frac{(p-1)}{2^k} \qquad k = 2$$
$\downarrow$
$$g^{(8n+2)} \times g^2 \equiv g^{(8n+4)} \pmod p \qquad n+2$$
$\downarrow$
$$\left(g^{(8n+4)}\right)^m \equiv 1 \pmod p \qquad m = \frac{(p-1)}{2^k} \qquad k = 2$$
$$\left(g^{(8n+4)}\right)^m \equiv -1 \pmod p \qquad m = \frac{(p-1)}{2^k} \qquad k = 3$$
$\downarrow$
$$g^{(8n+4)} \times g^4 \equiv g^{(8n+8)} \pmod p \qquad n+4$$
$\downarrow$

$$\left(g^{(8n+8)}\right)^m \equiv 1 \pmod p \quad m = \frac{(p-1)}{2^k} \quad k = 3$$
$\downarrow$
$$\left(g^{8n}\right)^r \equiv e \pmod p$$
$\downarrow$
$$f(x) \begin{cases} d = (p-1) - ((2+4) \times \frac{1}{2}) \\ g^d \equiv h \pmod p \end{cases}$$
$\downarrow$
$$e \times f(x) \equiv y \pmod p$$
$\downarrow$
$$b \equiv y \pmod p$$

5 Example

$$-- \quad (p = 61) \quad --$$

$$(p-1) = 2^2 \times n \quad k = 2 \quad r = \frac{(p+3)}{2^3} = 8 \quad m = \frac{(p-1)}{2^k}$$

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

$$-- \quad (\bmod 61) \quad --$$

$$g^{2x} \equiv 2^{50} \equiv 14$$

$$\downarrow$$

$$14^{15} \equiv -1 \quad m = \frac{(p-1)}{2^k} \quad k = 2$$

$$\downarrow$$

$$14 \times 2^2 \equiv 56 \quad n + 2$$

$$\downarrow$$

$$56^{15} \equiv 1 \quad m = \frac{(p-1)}{2^k} \quad k = 2$$

$$56^8 \equiv 42$$

$$\downarrow$$

$$60 - (2 \times \frac{1}{2}) = 59$$

$$2^{59} \equiv 31$$

$$\downarrow$$

$$42 \times 31 \equiv 21$$

$$14 \equiv \pm(21)^2 \pmod{61}$$

$$\textit{Quadratic residue} = 21, 40$$

$$-- \pmod{61} --$$

$$g^{2x} \equiv 2^{58} \equiv 46$$

$$\downarrow$$

$$14^{15} \equiv -1 \quad m = \frac{(p-1)}{2^k} \quad k = 2$$

$$\downarrow$$

$$46 \times 2^2 \equiv 1 \quad n + 2 \quad g^x \equiv 1 \;\; NG$$

$$\downarrow$$

$$1 \times 2^2 \equiv 4 \quad n + 2$$

$$\downarrow$$

$$4^{15} \equiv -1 \quad m = \frac{(p-1)}{2^k} \quad k = 2$$

$$\downarrow$$

$$4 \times 2^2 \equiv 16 \quad n + 2$$

$$16^{15} \equiv 1 \quad m = \frac{(p-1)}{2^k} \quad k = 2$$

$$\downarrow$$

$$16^8 \equiv 57$$

$$\downarrow$$

$$60 - ((2 + 2 + 2) \times \frac{1}{2}) = 57$$

$$2^{57} \equiv 23$$

$$\downarrow$$

$$57 \times 23 \equiv 30$$

$$46 \equiv \pm(30)^2 \pmod{61}$$

$$Quadratic\ residue = 30, 31$$

$$-- \quad (p = 97) \quad --$$

$$(p-1) = 2^5 \times n \quad k = 5 \quad r = \frac{(p+31)}{2^6} = 2 \quad m = \frac{(p-1)}{2^k}$$

$$g = 5 \quad \left(g^{(2^5 \times n)}\right)^r \equiv a \pmod{p}$$

$$-- \pmod{97} --$$

$$g^{2x} \equiv 2^{70} \equiv 3$$

$$\downarrow$$

$$3^{24} \equiv -1 \quad m = \frac{(p-1)}{2^k} \quad k = 2$$

$$\downarrow$$
$$3 \times 5^2 \equiv 75 \quad n+2$$
$$\downarrow$$
$$75^{24} \equiv 1 \quad m = \frac{(p-1)}{2^k} \quad k = 2$$
$$75^{12} \equiv -1 \quad m = \frac{(p-1)}{2^k} \quad k = 3$$
$$\downarrow$$
$$75 \times 5^4 \equiv 24 \quad n+4$$
$$\downarrow$$
$$24^{12} \equiv -1 \quad m = \frac{(p-1)}{2^3} \quad k = 3$$
$$\downarrow$$
$$24 \times 5^4 \equiv 62 \quad n+4$$
$$\downarrow$$
$$62^{12} \equiv 1 \quad m = \frac{(p-1)}{2^k} \quad k = 3$$
$$62^{6} \equiv 1 \quad m = \frac{(p-1)}{2^k} \quad k = 4$$
$$62^{3} \equiv -1 \quad m = \frac{(p-1)}{2^k} \quad k = 5$$
$$\downarrow$$
$$62 \times 5^{16} \equiv 1 \quad n+16 \quad g^x \equiv 1 \;\; NG$$
$$1 \times 5^{16} \equiv 36 \quad n+16$$
$$\downarrow$$
$$36^{3} \equiv -1 \quad m = \frac{(p-1)}{2^k} \quad k = 5$$
$$\downarrow$$
$$36 \times 5^{16} \equiv 35 \quad n+16$$
$$35^{3} \equiv 1 \quad m = \frac{(p-1)}{2^k} \quad k = 5$$
$$\downarrow$$
$$35^2 \equiv 61$$
$$\downarrow$$
$$96 - ((2+4+4+16+16+16) \times \frac{1}{2}) = 67$$
$$5^{67} \equiv 59$$
$$\downarrow$$
$$61 \times 59 \equiv 10$$
$$3 \equiv \pm(10)^2 \pmod{97}$$
$$Quadratic\ residue = 10, 87$$

References

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

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

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

ehime-JAPAN