Simple prime number determination method for natural numbers including Carmichael numbers

Takamasa Noguchi

2019/12/06

Explanation of effective prime number judgment method even for Carmichael number.[1]

1 introduction

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

This judgment method is based on case where ($a^{\frac{n-1}{2}} \equiv x \mod p$) becomes $p-1$. This method of judgment does not give a 100% correct answer. Care must be taken especially for ($n = p^k \quad p = Prime$) with primitive roots.[1]

2 Judgment criteria

$P = Prime$

2.1 $P \equiv 1 \pmod 4$

$a_1 + a_2 = p \qquad (a > 1)$
$a_1^{\frac{p-1}{2}} \equiv \alpha \pmod p \qquad a_2^{\frac{p-1}{2}} \equiv \beta \pmod p$
$\alpha = \beta$

$b_n = 2$
$\frac{p-1}{2} \equiv 2 \pmod 4 \quad \rightarrow \quad (p-b_n)^{\frac{p-1}{2}} \equiv p-1 \pmod p$
$\frac{p-1}{2} \equiv 0 \pmod 4 \quad \rightarrow \quad (p-b_n)^{\frac{p-1}{2}} \equiv 1 \pmod p$

$2 < b_n \leqq \frac{p-1}{2} \qquad (b_n = Odd\ prime)$
$p - b_n \equiv c \pmod{b_n} \quad \rightarrow \quad (p-b_n)^{\frac{p-1}{2}} \equiv p-1 \pmod p$
c = (b_n)Quadratic non-residue[3]

$p - b_n \equiv c \pmod{b_n} \quad \rightarrow \quad (p-b_n)^{\frac{p-1}{2}} \equiv 1 \pmod p$
c = (b_n) Quadratic residue[3]

$a^n \equiv x \pmod{13} \quad (p = 13)$

n/a	1	2	3	4	5	6	7	8	9	10	11	12
2	1	4	9	3	12	10	10	12	3	9	4	1
-												
$\frac{p-1}{2}$	1	12	1	1	12	12	12	12	1	1	12	1
-												
p-2	1	7	9	10	8	11	2	5	3	4	6	12
p-1	1	1	1	1	1	1	1	1	1	1	1	1

2.2 $P \equiv 3 \pmod 4$

$a_1 + a_2 = p \quad (a > 1)$
$a_1^{\frac{p-1}{2}} \equiv \alpha \pmod p \qquad a_2^{\frac{p-1}{2}} \equiv \beta \pmod p$
$\alpha + \beta = p$

$a^n \equiv x \pmod{11} \quad (p = 11)$

n/a	1	2	3	4	5	6	7	8	9	10
2	1	4	9	5	3	3	5	9	4	1
-										
$\frac{p-1}{2}$	1	10	1	1	1	10	10	10	1	10
-										
p-2	1	6	4	3	9	2	8	7	5	10
p-1	1	1	1	1	1	1	1	1	1	1

3 Judgment method

3.1 $n \equiv 3 \pmod 4 \quad (n > 17)$

(1) $a^{n-1} \equiv x \pmod n \qquad a = \{2, 3, 5, 7, 11, 13\}$

$\vdash - - - - \rightarrow \quad x \neq 1 \quad \rightarrow \quad non - Prime$

$\downarrow$

$x = 1 \quad \rightarrow \quad OK$

(2) $(n-k)^{\frac{n-1}{2}} \equiv x_1 \pmod n \qquad k = \{2, 3, 4, 5, 7\}$

$\vdash - - - - - - - \rightarrow \quad x \neq 1, n-1 \quad \rightarrow \quad non - Prime$

$\downarrow \qquad\qquad \downarrow$

$x_1 = n - 1 \qquad x_1 = 1$

$\downarrow$

$(n-k)^{n-2} \equiv x_2 \pmod n$

$$\downarrow$$

$$\begin{cases} x_2^{\frac{n-1}{2}} \not\equiv n-1 \pmod{n} & \rightarrow \quad non-Prime \\ x_2^{\frac{n-1}{2}} \equiv n-1 \pmod{n} & \rightarrow \quad OK \end{cases}$$

$x_1 = 1$

$k^{\frac{n-1}{2}} \equiv x_3 \pmod{n}$

$\vdash - - - - \rightarrow \quad x_3 \neq n-1 \quad \rightarrow \quad non-Prime$

$\downarrow$

$x_3 = n-1$

$k^{n-2} \equiv x_4 \pmod{n}$

$$\downarrow$$

$$\begin{cases} x_4^{\frac{n-1}{2}} \not\equiv n-1 \pmod{n} & \rightarrow \quad non-Prime \\ x_4^{\frac{n-1}{2}} \equiv n-1 \pmod{n} & \rightarrow \quad OK \end{cases}$$

ALL OK $\quad \rightarrow \quad$ *Prime*

3.2 $n \equiv 1 \pmod{4} \quad (n > 17)$

(1) $a^{n-1} \equiv x \pmod{n} \qquad a = \{2, 3, 5, 7, 11, 13\}$

$\vdash - - - - \rightarrow \quad x \neq 1 \quad \rightarrow \quad non-Prime$

$\downarrow$

$x = 1 \quad \rightarrow \quad OK$

(2) $b_n = 2$

$\frac{n-1}{2} \equiv x_1 \pmod{4}$

$\downarrow$

$x_1 = 2$

$(n - b_n)^{\frac{n-1}{2}} \equiv x_2 \pmod{n}$

$\vdash - - - - \rightarrow \quad x_2 \neq n-1 \quad \rightarrow \quad non-Prime$

$\downarrow$

$x_2 = n-1$

$(n - b_n)^{n-2} \equiv x_3 \pmod{n}$

$$\downarrow$$

$$\begin{cases} x_3^{\frac{n-1}{2}} \not\equiv n-1 \pmod{n} & \rightarrow \quad non-Prime \\ x_3^{\frac{n-1}{2}} \equiv n-1 \pmod{n} & \rightarrow \quad OK \end{cases}$$

(3) $2 < b_n \leqq \frac{n-1}{2} \qquad b_n = \;$ *Odd prime* $\; = \{3, 5, 7, \ldots\}$

$n - b_n \equiv c \pmod{b_n}$ $\leftarrow - - - - - - - - - - - - - - - - - -$ $b_{n+1} > b_n$

$\vdash - - - - - - - - - - - - - - - - -$

$\downarrow$ $\qquad\qquad\qquad\qquad$ $\downarrow$ $\qquad\qquad\qquad$ $\uparrow$

$c = \ (b_n) Quadratic\ non-residue$ $\qquad$ $c = \ (b_n) Quadratic\ residue$ $\ |$

$(n-b_n)^{\frac{n-1}{2}} \equiv x_1 \pmod{n}$ $\qquad\qquad |\qquad\qquad |$

$\vdash\rightarrow\ x_1 \neq n-1 \ \rightarrow\ non-Prime$ $\qquad - - - - - - - -$

$\downarrow$

$x_1 = n-1$

$(n-b_n)^{n-2} \equiv x_2 \pmod{n}$

$\downarrow$

$$\begin{cases} x_2^{\frac{n-1}{2}} \not\equiv n-1 \pmod{n} & \rightarrow \quad non-Prime \\ x_2^{\frac{n-1}{2}} \equiv n-1 \pmod{n} & \rightarrow \quad OK \end{cases}$$

$(1) \ \rightarrow ALL\ OK,\ \ (2)+(3)\ \rightarrow OK \geqq 2 \quad \rightarrow \quad Prime$

If $(n - b_n \equiv c \mod b_n)$ is all Quadratic residue, it is not a prime number.

If n is very large and the judgment times is limited, set b_n to $(b_n \leqq 101)$.
I think there are very few prime where $(n - b_n \equiv c \mod b_n)$ $(b_n \leqq 101)$ is all Quadratic residue.

4 Memo

$p \equiv 1 \pmod{4}$

$\frac{p-1}{2} \equiv 2 \pmod{4} \quad \rightarrow \quad (p-2)^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{2}} \equiv p-1 \pmod{p}$

$$p \equiv 1 \pmod{4} \quad \begin{cases} p \equiv 1 \pmod{8} & \rightarrow \quad \frac{p-1}{2} \equiv 2 \pmod{4} \\ p \equiv 5 \pmod{8} & \rightarrow \quad \frac{p-1}{2} \equiv 0 \pmod{4} \end{cases}$$

$p \equiv 3 \pmod{4} \quad \rightarrow \quad p \equiv 3,7 \pmod{8}$

I think $(p \equiv 1 \mod 8)$ is infinite.
However, $(2^{\frac{p-1}{2}} \equiv p-1 \mod p)$ is not necessarily primitive roots.

References

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

[2] S.Serizawa 『Prime Number Primer～Understand while calculating～』 Kodansha company 2002 (230-258)

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

ehime-JAPAN