
$p, q \in \mathbb{Z}$ について次を満たすとする。

$$^{\exists}x \in \mathbb{Z} \text{ s.t. } x^2 \equiv q \pmod p \tag{1}$$

この時、q を p を法とする**平方剰余**という。平方剰余でない数を**平方非剰余**という。

---

p: 奇素数、a:p と互いに素な整数

a が p を法として**平方非剰余**であれば次の式が成り立つ。(オイラーの規準)

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p \tag{2}$$

. . . .

この性質を利用し整数の素因子を探すことが出来る。

n を正の奇数とし、$\frac{p-1}{2}$ の奇数倍であるとする。この時、整数 a が p を法として平方非剰余であれば $a^n + 1 \equiv 0 \pmod p$ である。

$$a^{k \times \frac{p-1}{2}} \equiv -1 \pmod p \tag{3}$$

問

$5^{4851} + 1$ の素因子をこの方法でできるだけ多く見つけよ。但し、$4851 = 3^2 \cdot 7^2 \cdot 11$ である。

. . . .

$4851 = k \times \frac{p-1}{2}$ となるような p を探す。つまり、4851 の因数となる $\frac{p-1}{2}$ を探す。

4851 の因数は次の通りである。

$$
\begin{align}
&1 \tag{4}\\
&3,\ 7,\ 11 \tag{5}\\
&3^2,\ 3 \cdot 7,\ 3 \cdot 11,\ 7^2,\ 7 \cdot 11 \tag{6}\\
&3^2 \cdot 7,\ 3^2 \cdot 11,\ 3 \cdot 7^2,\ 3 \cdot 7 \cdot 11,\ 7^2 \cdot 11 \tag{7}\\
&3^2 \cdot 7^2,\ 3^2 \cdot 7 \cdot 11,\ 3 \cdot 7^2 \cdot 11 \tag{8}\\
&3^2 \cdot 7^2 \cdot 11 \tag{9}
\end{align}
$$

因数は 18 個ある。素因数は全て奇数 $3, 7, 11$ なので、因数も全て奇数である。

$\frac{p-1}{2} = 1$ の時、つまり $p = 3$ を考える。3 と 5 は互いに素である。そこで次のように式を変形できる。

$$5^{4851} + 1 = 5^{4851 \times \frac{3-1}{2}} + 1 \equiv 0 \pmod 3 \tag{10}$$

よって、素因数 3 を持つことがわかる。

これを残り 17 個の因数に対して考える。つまり、$\frac{p-1}{2}$ が因数と等しくなるような奇素数 $p(\neq 5)$ を探せばよい。

$$
\begin{aligned}
\frac{p-1}{2} &= 3 \ \Rightarrow & p &= 7 \ [\mathrm{p}] & (11)\\
\frac{p-1}{2} &= 7 \ \Rightarrow & p &= 15 = 3 \cdot 5 & (12)\\
\frac{p-1}{2} &= 11 \ \Rightarrow & p &= 23 \ [\mathrm{p}] & (13)\\
\frac{p-1}{2} &= 3^2 \ \Rightarrow & p &= 19 \ [\mathrm{p}] & (14)\\
\frac{p-1}{2} &= 3 \cdot 7 \ \Rightarrow & p &= 43 \ [\mathrm{p}] & (15)\\
\frac{p-1}{2} &= 3 \cdot 11 \ \Rightarrow & p &= 67 \ [\mathrm{p}] & (16)\\
\frac{p-1}{2} &= 7^2 \ \Rightarrow & p &= 99 = 3 \cdot 11 & (17)\\
\frac{p-1}{2} &= 7 \cdot 11 \ \Rightarrow & p &= 155 = 5 \cdot 31 & (18)\\
\frac{p-1}{2} &= 3^2 \cdot 7 \ \Rightarrow & p &= 127 \ [\mathrm{p}] & (19)\\
\frac{p-1}{2} &= 3^2 \cdot 11 \ \Rightarrow & p &= 199 \ [\mathrm{p}] & (20)\\
\frac{p-1}{2} &= 3 \cdot 7^2 \ \Rightarrow & p &= 295 = 5 \cdot 59 & (21)\\
\frac{p-1}{2} &= 3 \cdot 7 \cdot 11 \ \Rightarrow & p &= 463 \ [\mathrm{p}] & (22)\\
\frac{p-1}{2} &= 7^2 \cdot 11 \ \Rightarrow & p &= 1079 = 13 \cdot 83 & (23)\\
\frac{p-1}{2} &= 3^2 \cdot 7^2 \ \Rightarrow & p &= 883 \ [\mathrm{p}] & (24)\\
\frac{p-1}{2} &= 3^2 \cdot 7 \cdot 11 \ \Rightarrow & p &= 1387 = 19 \cdot 73 & (25)\\
\frac{p-1}{2} &= 3 \cdot 7^2 \cdot 11 \ \Rightarrow & p &= 3235 = 5 \cdot 647 & (26)\\
\frac{p-1}{2} &= 3^2 \cdot 7^2 \cdot 11 \ \Rightarrow & p &= 9703 = 31 \cdot 313 & (27)
\end{aligned}
$$

18 個の因数から 10 個の素数 $p = 3, 7, 23, 19, 43, 67, 127, 199, 463, 883$ が見つかる。p がこれらの素数の時、$\frac{p-1}{2}$ は 4851 の因数であり、$5^{4851} + 1 = 5^{k \times \frac{p-1}{2}} + 1$ となる。このとき k は奇数である。

これらの素数は奇素数であり、5 と互いに素である。$5^{k \times \frac{p-1}{2}} + 1$ は p を法として 0 であるので、次の素数が $5^{4851} + 1$ の素因数として見つかる。

$$p = 3, 7, 23, 19, 43, 67, 127, 199, 463, 883 \tag{28}$$