循環節の長さと冪剰余

黒木 亮汰

1　はじめに

この記事は一昨年の私の記事の誤植の訂正をしたものです．p は奇素数とします．ここでは $\frac{1}{p}$ の循環節長と $x^n \equiv a \bmod p$ という形の合同方程式の解の個数 (いわゆる冪剰余) の関係について述べます．

2　準備

証明は [1] 参照.

定義 1
a と m の最大公約数を (a,m) で表す.言いかえると,(a,m) は a と m を割り切る最大の整数.

定義 2
$a \equiv b \bmod c$ とは $a-b$ が c で割り切れる事である.

定義 3 (循環節長)
$a>1,(a,p)=1$ とする. $a^f \equiv 1 \bmod p$ を満たす最小の $0<f<p$ を$\frac{1}{p}$の a 進法においての循環節長という (本来なら循環節の長さと言うべきだがここでは省略する).

以後, 循環節長について述べるときは $(a,p)=1$ を仮定する.

定理 4 (Fermat の定理)
$a>1,(a,p)=1 \Rightarrow a^{p-1} \equiv 1 \bmod p$

定理 5 (原始根)
$\frac{1}{p}$ の r 進法においての循環節長が $p-1$ である自然数 r が存在する. r を p の原始根という.

原始根の一意性は保証されない.以後はこれを固定して議論する.

定理 6
r を原始根とすると $0<a<p$ と一対一に対応する $0<\mathrm{Ind}a<p$ があって $r^{\mathrm{Ind}a} \equiv a \bmod p$

定理 7
合同方程式の解の個数は $1 \leq x \leq p$ について言うと約束する.
$ax \equiv b \bmod m$ が解を (a,m) 個持つ $\iff (a,m)|b$
$ax \equiv b \bmod m$ が解をもたない $\iff (a,m) \not| b$

3　本題

$$x^n \equiv a \bmod p$$

の解 x の個数を考えたい. r を p の原始根とすれば,

$$r^{n\mathrm{Ind}x} \equiv r^{\mathrm{Ind}a} \bmod p$$

と変形できる. 元の式は指数があるので扱いにくいが, 定理 4,5 より

$$n\mathrm{Ind}x \equiv \mathrm{Ind}a \bmod p-1.$$

定理 6 より x と $\mathrm{Ind}x$ が一対一に対応するので, 最初の式の解 x の個数はこの式の解 $\mathrm{Ind}x$ の個数と一致する.
定理 7 よりその個数は

$$\begin{cases}(n,p-1) & ((n,p-1)|\mathrm{Ind}a)\\ 0 & ((n,p-1)\not|\mathrm{Ind}a)\end{cases}$$

条件分岐の式は Ind を含んでおり分かりづらいのでより簡単に表したい. そこで $\frac{1}{p}$ の a 進法においての循環節長 f を使って表そうと思う. まず,

$$r^{f\mathrm{Ind}a} = a^f \equiv 1 \bmod p$$

となり, $0<f<p$ なので, 定理 4 より $f|p-1$. 定理 5 より, $p-1|f\mathrm{Ind}a$ なので,

$$\frac{p-1}{f}|\mathrm{Ind}a$$

となる. よって
$f|\frac{p-1}{(n,p-1)}$ となる自然数 n について, $(n,p-1)|\mathrm{Ind}a$.
逆に $(n,p-1)|\mathrm{Ind}a$ となる自然数 n について, $q=\frac{\mathrm{Ind}a}{(n,p-1)}$ と置けば,

$$a^{\frac{p-1}{(n,p-1)}} \equiv r^{\frac{p-1}{(n,p-1)}\mathrm{Ind}a} = r^{(p-1)q} \equiv 1 \bmod p$$

なので, 定義 3 より $f|\frac{p-1}{(n,p-1)}$.

4 結論

以上より解の有無は $f|\frac{p-1}{(n,p-1)}$ (つまり $(n,p-1)|\frac{p-1}{f}$) かどうか, 解の数は $(n,p-1)$ で決まる.

定理 8
$\frac{1}{p}$の a 進法においての循環節長を $f, x^n \equiv a \bmod p$ の解の数を e とすると,

$$e = \chi(n)(n,p-1)$$

但し,

$$\chi(x) = \begin{cases}1 & ((n,p-1)|\frac{p-1}{f})\\ 0 & ((n,p-1)\not|\frac{p-1}{f})\end{cases}$$

系 9
$e=0 \Rightarrow f\not|\frac{p-1}{(n,p-1)}$.
$e\neq 0 \Rightarrow f|\frac{p-1}{(n,p-1)}$.

系 10
$n=2$ のとき,
$e=0 \Rightarrow f\not|\frac{p-1}{2}$.
$e\neq 0 \Rightarrow f|\frac{p-1}{2}$.

例 11
メルセンヌ素数 $M=2^{74207281}-1$ について, $\frac{1}{M}$の循環節長 f は奇数か偶数か

$x^2 \equiv 10 \bmod M$ の解の有無を考える. 平方剰余の相互法則より,

$$(\frac{2}{p}) = \begin{cases} 1 & (p \equiv \pm 1 \bmod 8) \\ -1 & (p \equiv \pm 3 \bmod 8) \end{cases}$$

$$(\frac{5}{p}) = \begin{cases} 1 & (p \equiv \pm 1 \bmod 5) \\ -1 & (p \equiv \pm 2 \bmod 5) \end{cases}$$

が得られて, $M \equiv -1 \bmod 8$, $M \equiv 1 \bmod 5$ なので

$$\begin{aligned}(\frac{10}{M}) &= (\frac{2}{M})(\frac{5}{M}) \\ &= 1 \cdot 1 = 1.\end{aligned}$$

よって $e \neq 0$. $M - 1 \equiv 2 \bmod 4$. なので系 10 より $\frac{1}{M}$ の循環節長 f は奇数.

5 終わりに

読んでいただきありがとうございました. $\frac{1}{p}$ の循環節長が $p-1$ の約数になることは定理 4 より容易に示せますが, 循環節長が偶数か奇数か求める方法を知らなかったので, OEIS などを参考に考察して, $4n+3$ 型素数の場合に法則性があることに気づいたので計算しました.

参考文献

[1] 雪江明彦：整数論 1