卒業研究

$X^Q = 1$ の m を法としたときの解の個数について

発表者　高島　雄

この研究では

$X^Q \equiv 1 \bmod M$ の解と解の個数を調べ、M が素数 P での解の個数 N との関係。また、**N の周期の長さを調べる。**

$X^Q \equiv 1 \bmod M$ の解の個数Nの考察。

実行結果より次のことが予測できた。　実行結果をご覧ください。

Mが素数Pのとき解の個数をNとする。

(1) $Q = P - 1$であれば　$N = P - 1$
(2) $Q = P - 2$であれば　$N = 1$
(3) $Q = P - 3$であれば　$N = 2$
(4) $Q = P - 4$であれば　$N = 3$または1

以上を証明する。

1.　Xが素数Pの倍数でないならば（互いに素のとき）

フェルマーの小定理により。

$$\boxed{X^{P-1} \equiv 1 \bmod P}$$

は成立している。

よってX=1,2, $\cdots$, $P-1$がすべて解なので　$N = P-1$。

2.　$Q = P - 2$　により　$X^{P-2} \equiv 1 \bmod P$

この両辺にXをかけると

$$X \cdot X^{P-2} \equiv X \bmod P$$

$$X^{P-1} \equiv X$$

フェルマーの小定理より。

$$X^{P-1} \equiv 1$$

$$1 \equiv X^{P-1} \equiv X$$

ゆえに$X \equiv 1$なので、$N = 1$。

3.　以上の証明と同様に、

$$X^2 \cdot X^{P-3} \equiv X^2 \bmod P$$

$$X^{P-1} \equiv X^2$$

フェルマーの小定理より。

$$1 \equiv X^{P-1} \equiv X^2 \bmod P$$

ゆえに$X \equiv \pm 1$、よって$N = 2$。

4　以上の証明と同様にしてフェルマーの小定理より、

$$1 \equiv X^{P-1} \equiv X^3 \bmod P$$

次に　$\boxed{X^3 \equiv 1 \bmod P}$　の解を調べる。

$X^3 \equiv 1 \bmod P$　の解を因数分解をして

$$X^3 - 1 = (X - 1)(X^2 + X + 1)$$

X は1を解にもつので

$$X \neq 1$$

ならば

$$X^2 + X + 1 = 0$$

この解があれば解は2個あるので、　　$N = 3$

解がなければ　　$N = 1$

次にどんなとき　　$\boxed{X^2 + X + 1 = 0}$　　は解をもつかを調べる。

実行結果より。

$$P = 7, 13, 19, 31, 37, 43, 61, 67 \cdots$$

この数列を**階差数列**で考えると、

$$13-7=6,\ 19-13=6,\ 31-19=12\cdots$$

$$6,6,12,6,6,18,6,12\cdots$$

以上より、$P=7+6n$　のとき $X^2+X+1=0$　は解をもち、$N=3$　になると予想できる。

次に、　$Q = M - 6$,　$Q = M - 9$のときの解の個数を調べる。
次のような予想がたつ。

5.　$Q = M - 6$のとき解の個数$N = 1$または5
6.　$Q = M - 9$のとき解の個数$N = 1$または7

同様にする。

$$X^5 = (X-1)(X^4 + X^3 + X^2 + X + 1)$$

$$(X^4 + X^3 + X^2 + X + 1) = 0$$

が解をもてば$N = 5$　解をもたなければ$N = 1$

実行結果より

$$P = 11, 31, 41, 61, 71, 101, 131, , ,$$

この数列を階差数列で考えると

$$10, 10, 20, 10, 30, 30 \cdots$$

$M = 11 + 10n$　$P \equiv 1 \bmod 10$　をみたしている。

予想　このとき　$X^5 \equiv 1 \bmod P$　は$N = 5$

同様にする。

$$X^7 = (X-1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)$$

$$(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1) = 0$$

が解をもてばN=7　解をもたなければN=1

実行結果より

$$P = 29, 43, 71, 113, 127, , ,$$

この数列を階差数列で考えると

$$14, 28, 42, 14 \cdots$$

$P = 29 + 14n$　$P = 29 + 14n$　$P \equiv 1 \bmod 14$　をみたしている。

予想　このとき　$X^7 \equiv 1 \bmod P$　なら$N = 7$

周期性を調べるため。　$1 < Q < M < 150$　ではなく
$M, Q < 150$　としたプログラムに変更する。

実行結果 をご覧ください。

観察結果

1　Mが奇素数Pのとき Nの周期は$N = 1, 2, \cdots, P - 1$.
$Q = \frac{P-1}{2}$のとき$N = \frac{P-1}{2}$。

2　Mが合成数のとき、周期の長さと解の個数はともにM
のEuler関数$\varphi(M)$の約数。
Nの最大値は$\varphi(M)$。

$\boxed{2-1}$

$M = p \cdot q$ (p, qは異なる素数)

$\varphi(M) = (p-1) \cdot (q-1)$　であり

$\varphi'(M)$=lcm$(p-1, q-1)$　とおく、

周期は$\varphi'(M)$。　$\varphi'(M)$は$\frac{1}{2} \cdot \varphi(M)$　の約数。

（例）　$p = 3, q = 5$

$(p-1) \cdot (q-1) = 2 \cdot 4 = 8$　Euler数

$\varphi'(15)$=lcm$(4, 2) = 4$　周期

$\boxed{2-2}$

$M = p \cdot q \cdot r$

p, q, r(異なる奇素数)

$$\varphi(M) = (p-1) \cdot (q-1) \cdot (r-1)$$

$$\varphi'(M) = \mathrm{lcm}(p-1, q-1, r-1)$$

$p-1, q-1, r-1$の最小公倍数が周期で$\varphi'(M)$。周期は$\varphi(M) \cdot \frac{1}{4}$の約数。

（例）$p = 3, q = 5, r = 7$ (p, q, rは異なる素数なら)

$(p-1) \cdot (q-1) \cdot (r-1) = 2 \cdot 4 \cdot 6 = 48$　Euler数

$\varphi'(105) = \mathrm{lcm}(2, 4, 6) = 12$　周期

$\boxed{2-3}$

$M = p \cdot 2^r$ (pは素数)

$\varphi(M) = (p-1) \cdot 2^{r-1}$

（例）$3 \cdot 2^2 = 12$

$\varphi(12) = (2) \cdot 2^1 = 4$

$\varphi'(12) = 2$

euler数の$\frac{1}{2} = \varphi'(12) = 2$　周期

M が合成数の場合、素数のときと周期にずれがある。しかしEuler 関数$\varphi(M)$を少し変えて$\varphi'(M)$で考えると周期が一般化できることが予測できた。

Mを因数分解。($p_1, p_2 \cdots p_r$が奇素数のとき)

$$M = p_1^{e1} \cdot p_2^{e2} \cdots p_r^{e_r}$$

とするとき、因数分解のeuler数の最小公倍数を

$$\varphi'(M) = \mathrm{lcm}\ (\varphi(p_1^{e1}) \cdot \varphi(p_2^{e2}) \cdots \varphi(p_r^{e_r}))$$

とおく。

$M = 2^e$ の場合

$e = 1, 2$ のとき $\varphi'(M) = 2^{e-1}$ を周期の長さ。

$e \geq 3$ のとき $\varphi'(M) = 2^{e-2}$ を周期の長さ。

また、$M = 2^e \cdot M_1$(M_1 は奇数) のときは、

$$\varphi'(M) = \mathrm{lcm}(\varphi(2^e), \varphi'(M_1))$$

(例)　　$M = 8 \cdot 17 \cdot 29$　のとき

$\varphi(M) = 4 \cdot 16 \cdot 28 = 1536$

$M_1 = 17 \cdot 29$ とし、
$\varphi'(M_1)=\mathrm{lcm}((17-1),(29-1))=64$

$\varphi'(M)=\mathrm{lcm}(\varphi(2^3),\varphi'(64))=64$

ゆえに周期 $\varphi'(M) = 64$。

終幕。