5 Fermat の小定理

前回の最後に，p 元体 $\mathbb{F}_p$ の可逆元全体の集合 $\mathbb{F}_p^\times$ は，a とその逆元 a^{-1} をペアにすることにより，

$$\{1\},\quad \{2,2^{-1}\},\quad \{3,3^{-1}\},\ \ldots,\ \{p-1\}$$

と $\frac{p+1}{2}$ 個の集合に分割されることを見た．たとえば，$p=11$ とすると，

$$\{1\},\quad \{2,6\},\quad \{3,4\},\quad \{5,9\},\quad \{7,8\},\quad \{10\}$$

と $\frac{11+1}{2}=6$ 個に分割される．ポイントは，1 と $p-1=-1$ 以外は，自身とその逆数が等しくなることはないということである．

1 $p=17$ として，$\mathbb{F}_{17}^\times=\{1,2,3,\ldots,16\}$ を上のように分割してみよ．

2 $(p-1)!$ を順序を変えて計算することにより，Wilson の定理と呼ばれる次の式を証明せよ．

$$(p-1)!\equiv -1 \pmod{p}$$

普通の整数では，任意の a について $a,a^2,a^3,\ldots,a^k,\ldots$ と計算していくと，その絶対値はどんどん大きくなり発散していく．しかし，有限個の元しか持たない p 元体 $\mathbb{F}_p$ では，$a,a^2,a^3,\ldots,a^k,\ldots$ のすべてが閉じた $\mathbb{F}_p$ に納まるので，「鳩の巣原理」あるいは「部屋割り論法」により，$k\neq l$ であって $a^k=a^l$ となることが起きないわけにはいかない．そこで，$\mathbb{F}_p$ でのべき乗 a^k の様子を見るために，まず $p=5$ として，$\mathbb{F}_5^\times$ の各元 a について a^k $(k=1,2,\ldots)$ を計算してみると次のような表が出来る．

a \ k	1	2	3	4	5	6	…
1	1	1	1	1	1	1	…
2	2	4	3	1	2	4	…
3	3	4	2	1	3	4	…
4	4	1	4	1	4	1	…

入学年度		学部	学 科		組		番　号			検	フリガナ	
		B		1							氏 名	

3 a) $p=7$ として，$\mathbb{F}_7^\times$ の各元 a について上と同じような表を作れ．

［ $a^k \pmod 7$ を直接けいさんするのではなく，すぐ左にある $a^{k-1} \pmod 7$ に a をかければよい．］

a \ k	1	2	3	4	5	6	7	8	9	…
1										…
2										…
3										…
4										…
5										…
6										…

b) 上の表の $k=6$ の列と $k=3$ の列に注目してその特徴を述べよ．

4 $p=11$ とし，$\mathbb{F}_{11}^\times=\{\pm1,\pm2,\pm3,\pm4,\pm5\}$ と表して，a^k の表を作れ．

［ $k=1$ から 5 まで計算すると，$a^6=a^5a^1$，$a^7=a^5a^2$ などとして，$k\geqq 6$ については $k=1$ から 5 までの結果を用いてすぐ計算できる．また，$(-a)^k=-a^k$ (k は奇数)，$(-a)^k=a^k$ (k は偶数) を用いるとよい．］

a \ k	1	2	3	4	5	6	7	8	9	10
1										
2										
3										
4										
5										
−5										
−4										
−3										
−2										
−1										

【裏に続く】

一般に次の性質が成り立つ.

Fermat の小定理

p を素数とし，a を p と互いに素な整数とする．このとき，

(1) $$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ.

ここで，p が素数であることが重要で，素数でない整数 m を法とし場合は同様の性質は成り立たない.

5 $2^{9-1} \pmod 9$，$2^{12-1} \pmod{12}$，$2^{13-1} \pmod{13}$，$2^{15-1} \pmod{15}$ をそれぞれ計算せよ.

6 以前，$\mathbb{F}_p^\times$ のかけ算の表の各行には 1 から $p-1$ までの数がちょうど 1 回ずつ現れることを見た.

a) a の行に現れる数は $a, 2a, 3a, \ldots$ であるを用いて，a の行に現れる数の積を求めよ.

b) 一方，a の行には，順序はばらばらであるが，$1, 2, \ldots, p-1$ がそれぞれ 1 回ずつ現れることを用いて，a の行に現れる数の積を求めよ.

c) Wilson の定理 $(p-1)! \equiv -1 \pmod{p}$ を用いてフェルマーの小定理を証明せよ.

フェルマーの小定理により任意の $\mathbb{F}_p^\times$ の元 a について，$a^{p-1} \equiv 1 \pmod{p}$ であるが，$2^3 \equiv 1 \pmod 7$ のように，$k < p-1$ であっても $a^k \equiv 1 \pmod{p}$ となることもある．$a \in \mathbb{F}_p^\times$ について，$k = 1, 2, \ldots, p-2$ に対しては $a^k \not\equiv 1 \pmod{p}$ であるとき，a は $\mathbb{F}_p$ の**原始元** (primitiviv element) であると呼ばれる.

7 これまでに作った $a^k \bmod p$ の表を用いて，$p = 5, 7, 11$ について $\mathbb{F}_p$ の原始元をすべて求めよ.

8 $p = 17, 19, 23$ の場合，それぞれについて 2 が原始元であるかどうかを判定せよ.

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)