4 Fermat の小定理

入学年度		学部	学 科		組		番　号			検	フリガナ	
2	3	B		1							氏 名	

前回に引き続き，素数 p を固定し，p を法として合同という関係でグループに分けて得られる合同類の全体の集合 $\{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ について考える．この集合を $\mathbf{F}_p$ はと表され，p **元体**と呼ばれる．混同の恐れがないときは，- をとってさらに簡単に表すので，

$$\mathbf{F}_p = \{0, 1, 2, \ldots, p-1\}$$

である．$\mathbf{F}_p$ は加法・減法について閉じている．さらに，$\mathbf{F}_p$ から $\overline{0} = 0$ を除いた集合

$$\mathbf{F}_p^{\times} = \{1, 2, \ldots, p-1\}$$

を考えると，$\mathbf{F}_p^{\times}$ は p が素数であることにより乗法・除法について閉じていることが示される．前回見たのは，$\mathbf{F}_p^{\times}$ の乗法の表は，$\mathbf{F}_p$ の加法の表とは異なり，一見してわかる単純なパターンは見当たらないということであった．しかし，$\mathbf{F}_p^{\times}$ の元 a は必ず逆数 a^{-1} をもつことがわかる．また，$\mathbf{F}_p$ の元を係数とする多項式（$\mathbf{F}_p$ 上の多項式と呼ぶ）については因数定理も成り立つ．

1　$x^2 - 1$ を $\mathbf{F}_p$ 上の多項式とみる．明らかに $x^2 - 1 \equiv (x-1)(x+1) \pmod{p}$ が成り立つ．このことを用いて，次のことを示せ．ただし，p は 2 以外の素数とする．

a)　$\mathbf{F}_p^{\times}$ の元 a で，$a^2 = 1$ となるものは $a = 1$ または $a = p-1$ に限る．

b)　$\mathbf{F}_p^{\times}$ の元 a で，$a = a^{-1}$ となるものは $a = 1$ または $a = p-1$ に限る．

c)　$\mathbf{F}_p^{\times}$ の元は，$\{1\}, \{p-1\}$ と $\dfrac{p-3}{2}$ 個の $\{a, a^{-1}\}$ という形の集合に分割される．$p = 19$ の場合に $\mathbf{F}_{19}^{\times}$ を実際にこのように分割してみよ．

$p = 5$ として，$\mathbf{F}_5^{\times}$ 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	…

2　$p = 7$ として，$\mathbf{F}_7^{\times}$ の各元 a について上と同じような表を作れ．

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

3　Excel を用いて $p = 11, 17, 19, \ldots$ の場合に上と同じ表を作り，1 の現れ方を観察せよ．

［Excel の各セルで直接 a^k を計算し，p で割った余りを計算しようとするとたちまち桁数オーバーになってしまう．そこで，$a^k = a^{k-1} \times a$ であることを用い，すぐ左隣のセルに a をかけて p で割った余りを求めるという方法をとるとよい。］

実は，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，

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

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．

4　Excel を用いて，$m = 12, 15, 16, \ldots$ の場合に上と同様の $a^k \pmod{m}$ の表を作り，素数の場合との違いをみよ．

【裏に続く】

5 p を法とする合同類から 0 の類を除いて作ったのかけ算の表の各行には 1 から $p-1$ までの数が各 1 回ずつ現れる.

a) 1 の行をすべてかけ合わせるとき，問題 1 c) を利用してかけ算の順序を変えてかけ合わせることにより

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

であることを示せ.

b) a の行には，$1, 2, \ldots, p-1$ がそれぞれ 1 回ずつ現れることを用いて,

$$a \times 2a \times 3 \times \cdots \times (p-1)a \equiv (p-1)! \pmod{p}$$

であることを示せ.

c) フェルマーの小定理を証明せよ.

a を p と互いに素な整数とすると，フェルマーの小定理により $a^k \equiv 1 \pmod{p}$ であるが，$k = 1, 2, \ldots, p-2$ については $a^k \not\equiv 1 \pmod{p}$ であるとき，a は**原始元** (primitiviv element) であると呼ばれる.

6 問題 3 で作った $a^k \bmod p$ の表を用いて，$p = 17$ のとき原始元をすべて求めよ.

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)