有限と無限の間隙　(平成２０年)

1. フェルマーの小定理と巡回群

補助定理　p:素数　$a,\ b$ ：p で割り切れない数のとき

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

証明　$$(a+b)^p = a^p + b^p + \sum_{r=1}^{p-1} \binom{p}{r} a^r b^{p-r}$$

$$\binom{p}{r} = \frac{p!}{(p-1)!\ r!}$$

$$\therefore \quad \binom{p}{r} \equiv 0 \pmod{p} \qquad (0 < r < p)$$

$$\therefore \quad (a+b)^p \equiv a^p + b^p \pmod{p}$$

定理（Fermat）

p: 素数　a ：p で割り切れない数のとき $a^p \equiv a \pmod{p}$

証明　$a^p \equiv a \pmod{p}$ を $p(a)$ とおく

$p(0)$ と $p(1)$ は明らか

a に $a+1$ を代入すると

$$(a+1)^p \equiv a + 1 \pmod{p} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (1)$$

補助定理から

$$(a+1)^p \equiv a^p + 1 \pmod{p} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (1)$$

(1), (2) より

$$a^p + 1 \equiv a + 1 \pmod{p}$$

$$\therefore \quad a^p \equiv a \pmod{p}$$

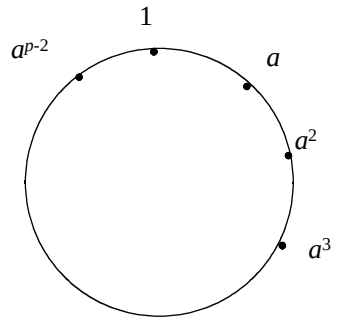
例　10^n を素数 7 で割るとき, その余りは次のように巡回する.

10の累乗	1	10	10^2	10^3	10^4	10^5	10^6	10^7	10^8	……
7で割った余り	1	3	2	6	4	5	1	3	2	……

繰り返し

このように 10 の累乗を 7 で割った余りは, 1, 3, 2, 6, 4, 5 の繰り返しで, 10 の累乗が 6 個ごとに巡回する.

注　p が素数で (a　p) = 1 のとき, 集 { 1, a, a^2, ……, a^{p-2} } 合 は巡回群をなす.



2.　有限体 F_p

Z を整数全体の集合とし, p を素数とすると, つぎの剰余類 Z / p は有限体をなし, F_p と記す.

$$F_p = Z / p = \{0\ (mod\ p),\ 1\ (mod\ p),\ \cdots,\ (p\ -1)\ (mod\ p)\}$$

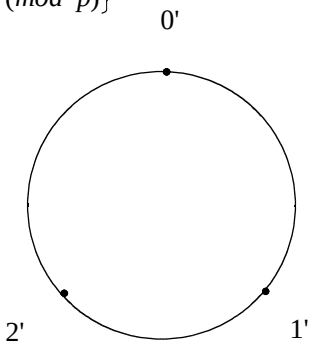
例　表記を略記するために　$p\ -1\ (mod\ p)$ を$(p\ -1)'$　と記す.

$F_3 = \{0',\ 1',\ 2'\}$

$0' = \{\cdots,\ -3,\ 0,\ 3,\ 6,\ \cdots\}$

$1' = \{\cdots,\ -2,\ 1,\ 4,\ 7,\ \cdots\}$

$2' = \{\cdots,\ -1,\ 2,\ 5,\ 8,\ \cdots\}$



素数 p を法とする剰余類は, 四則演算が可能である.

F_3 の加法と乗法は, つぎの表のようになる.

+	0	1'	2'
0'	0'	1'	2'
1'	1'	2'	0'
2'	2'	0'	1'

(表　1)

×	0'	1'	2'
0'	0'	0'	0'
1'	0'	1'	2'
2'	0'	2'	1'

(表　2)

注　(1) 加法と乗法は整数と同じ計算であるが, 計算結果が p を超えるときは, 計算結果を p で割った余りを答えとする.

(2)　減法は逆数を加えると考える. 即ち, $x + y = 0'$ のとき　y　を　x　の逆数といい, $-y$ と 記　$x - y = x + (-y)$ し, と計算する.

F_p では, $x + (p - x)\ (mod\ p) = p\ (mod\ p) = 0'$ だから $x\ (mod\ p)$ らの逆数は $(p - x)\ (mod\ p)$ である.

(3) 除法は逆数を乗ずると考える. 即ち, x ・y = 1' のとき, を y　の　x　逆数といい,　x^{-1} と記し,　$x \div y = x \cdot y^{-1}$　と計算する.

(4) F_p は有限体である.

引用文献

1. Olympia E. Nicodemi, Melissa A. Sutherland, Gary W. Towsley, Abstract Algebra, Upper Saddle River, 2007
2. Saunders Mac Lane, Garrett Birkhoff, Algebra, AMS Chelsea, 1999
3. ガロワと方程式 2002 草場公邦著朝倉書店