

## 有限と無限の間隙 (2008)

### 1. フェルマーの小定理と巡回群

補助定理

$p$ : 素数      $a$ :  $p$  で割り切れ数  
 $(a + b)^p \equiv a^p + b^p \pmod{p}$

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

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

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

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

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  $p(a)$  と置くと

$p(0)$  と  $p(1)$  は明らかに成り立つ

$a$  に  $a + 1$  を代入すると

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

補助定理から

$$(a + 1)^p \equiv a^p + 1 \pmod{p} \dots\dots\dots(2)$$

(1)と(2)より

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

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

例

$$7) \frac{142857}{1000000} \dots\dots\dots 10^{7-1} = 10^6$$

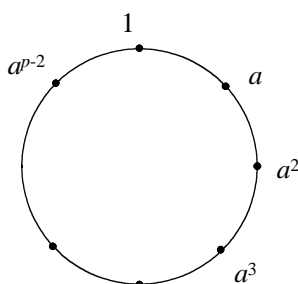
$$\begin{array}{r} 7 \\ \hline 30 \\ 28 \\ \hline 20 \\ 14 \\ \hline 60 \\ 56 \\ \hline 40 \\ 35 \\ \hline 50 \\ 49 \\ \hline 1 \end{array}$$

10の累乗	1	10	10 <sup>2</sup>	10 <sup>3</sup>	10 <sup>4</sup>	10 <sup>5</sup>	10 <sup>6</sup>	10 <sup>7</sup>	10 <sup>8</sup>	.....
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, 集合  $\{1, a, a^2, \dots, a^{p-2}\}$  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。

$$F_p = Z/p = \{0 \pmod p, 1 \pmod p, \dots, (p-1) \pmod p\}$$

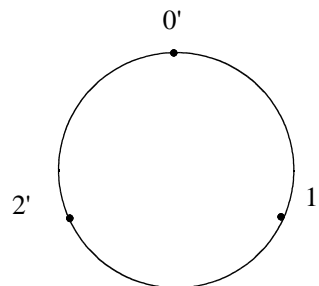
例 表記を略記するために  $p-1 \pmod p$  を  $(p-1)'$  と記すと,

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

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

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

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



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  $p$  を越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える。即ち,  $x + y = 0'$  のとき,  $y$  を  $x$  の逆数といい,  $-y$  と記し,  $x - y = x + (-y)$  と計算する。

$F_p$  では,  $\{x + (p - x)\} \pmod{p} = p \pmod{p} = 0$ , だから  $x \pmod{p}$  の逆数は  $(p - x) \pmod{p}$  である.

(3) 除法は逆数を乗ずると考える. 即ち,  $x \cdot y = 1$ , のとき,  $y$  を  $x$  の逆数といい,  $x^{-1}$  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