12. フェルマの定理と応用

代数Ⅱ

逆元と正則

- 法mの完全剰余系

$$Z_m = \{0,1,2,\cdots,m-1\}$$

合同式

$$ax \equiv 1(mod\ m)$$

xを法mに関するaの逆元，aが法mに関する逆元を持つとき，aは法mに関して，正則である

$(a,m) = 1$ならば，各元をa倍した

$$\{0,a,2a,\cdots,(m-1)a\}$$

も完全剰余系である.

法pの剰余体

- 法p（素数）の完全剰余系

$$Z_p = \{0,1,2,\cdots,p-1\}$$

は法pの演算に関して体となる.

法mの剰余環Z_mにおいて
$a \neq 0, b \neq 0 (mod\ m)$ではあるが，$ab \equiv 0 (mod\ m)$
このようなa, bを零因子とよぶ

フェルマーの(小)定理

- pが素数，$(a,p) = 1$ならば

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

$$a \cdot a^{p-2} \equiv 1 (mod\ p)$$

すなわち，aの逆元はa^{p-2}である

pが素数ならば，$a^p \equiv a (mod\ p)$

定理

- ウィルソンの定理

  pが素数ならば，

  $$(p-1)! \equiv p-1 (mod\ p)$$

- ライプニッツの定理

  pが素数ならば，

  $$(p-2)! \equiv 1 (mod\ p)$$

1次合同式の解法

- $ax \equiv c (mod\ m)$

を満たす整数解xを求めることを解くという

$(a, m) = 1$ならば，簡単に解ける

法mに関するaの逆元a'を掛けると

$$x \equiv a'c (mod\ m)$$