A Bridge between Finite and Infinite (2008)

1. Fermat's Little theorem and Cyclic group

Lemma

If p is a prime and a and b are integers, then

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

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

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

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

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

Theorem（Fermat）

If p is a prime, then $a^p \equiv a \pmod{p}$

Proof Let $p(a)$ be the proposition that $a^p \equiv a \pmod{p}$

The $p(0)$ and $p(1)$ are of obvious.

The proposition $p(a + 1)$ implies

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

Using Lemma, we find

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

By（1）and（2）, we find

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

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

Example

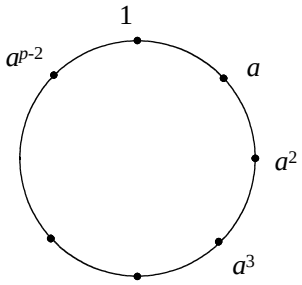
$$\begin{array}{r} 142857 \\ 7\overline{)\,1000000} \end{array} \quad \cdots\cdots\cdots\cdots\ 10^{7-1} = 10^6$$

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

The remainders of the successive powers of 10 (mod 7) are 1, 3, 2, 6, 4, 5, 1. This shows that 10 belongs to the exponent 6 (mod 7) and the period is 6.

power of 10	1	10	10^2	10^3	10^4	10^5	10^6	10^7	10^8	·····
remainder (mod 7)	1	3	2	6	4	5	1	3	2	·····
							repeats			

Remark If p is a prime and $(a, p) = 1$, then the set $\{1, a, a^2, \cdots\cdots, a^{p-2}\}$ is called a cyclic group.



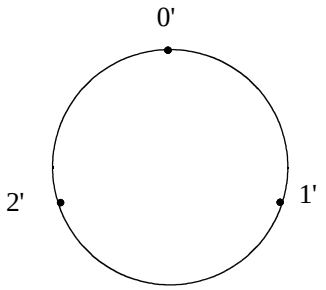
2. Finite fields F_p

Let Z be a set of all integers and let p be a prime, then the following residue class Z/p consists a finite field. We generally denote Z/p as F_p.

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

Example If we denote $p-1\ (mod\ p)$ as $(p-1)'$ for short,

$$F_3 = \{0', 1', 2'\}$$
$$0' = \{\cdots, -3, 0, 3, 6, \cdots\}$$
$$1' = \{\cdots, -2, 1\ 4, 7, \cdots\}$$
$$2' = \{\cdots, -1, 2, 5, 8, \cdots\}$$



These remainders modulo p can be added and multiplied. Take the usual sum or product; if the result exceeds p, replace by its remainder on division by p.

For the F_3, this sum + and the product $\times$ are those given by the following tables:

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

(Table 1)

$\times$	0'	1'	2'
0'	0'	0'	
1'	1'	2'	
2'	2'	1'	

(Table 2)

Remark

(1) For each x there is a y such that $x + y = 0'$. We call y the additive inverse of x and denote it by the symbol $-x$. For instance, 2' is the additive inverse of 1' because $2' + 1' = 0'$. So $2' = -1'$. More generally, the additive inverse of any x in F_p

is $(p-x) \pmod p$ since $\{x + (p-x)\} \pmod p = p \pmod p = 0'$,

(2) If $x \cdot y = 1'$, the element y is called the multiplicative inverse of x. We denote y by the symbol x^{-1}. In F_3 every nonzero element has a multiplicative inverse. For instance, $1' \times 1' = 1'$ and so $1'^{-1} = 1'$. (Also $2'^{-1} = 2'$). Thus F_p forms a finite field.

References

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. Toshikuni Kusaba, Galois and Equations, Asakura Shoten, 2002