LN IV a

This time first the project.

Hint: $G_5 = \{1,2,3,4\} \subset \mathbb{Z}_5$

multiplication table G_5

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Consider the powers of 2

2^k.

1	2	4	3	1
2^0	2^1	2^2	2^3	2^0

a	b	c	d

relable

Multiplication table of G_5 with new lables

	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

addition table $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Consider multiples/sums of 1

0	1	2	3	0
0·1	1·1	2·1	3·1	

4·1

a	b	c	d

relable

addition table of $\mathbb{Z}_4$ with new lables

	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

G_5 and $\mathbb{Z}_4$ are really indistinguishable. ☺

both sets can be represented as a cycle

G_5 : 1 2 4 3 1 $\quad 2^k$

$\mathbb{Z}_4$: 0 1 2 3 0 $\quad k \cdot 1$

This is not always the case.

$G_8 = \{1, 3, 5, 7\}$

1 3 1 $\quad 3^k$

3^0 3^1 3^2

only a cycle of length 2.

1 5 1 $\quad 5^4$

1 7 1 $\quad 7^k$

$G_5(\mathbb{Z}_4)$ is really different from G_8.

Conclusion: powers are useful.

§1.6 Euler's Theorem

$[a]_n$ has a finite multiplicative order if $\exists\ k \geq 1$ s.t. $[a]_n^k = [1]_n$

Ex) $[3]_{20}$: $3, 9, 27 = 7, 21 = 1$

$[3]_{20}^4 = [1]_{20}$. order $= 4$.

$[10]_{20}$: $10, 100 = 0, 0 \ldots\ldots$

If $[a]_n$ has a f.m.o. then the order of $[a]_n$ is the smallest positive k.

$$[a]_n^k = [1]_n$$

Thm $[a]_n$ has a fmo $\iff$ $(a,n)=1$

Pf) $\Rightarrow$) $[a]_n^k = [1]_n$

$$[a]_n^{k-1}[a]_n = [1]_n$$

So $[a]_n$ is invertible. Thm $(a,n)=1$

$\Leftarrow$) $(a,n)=1$

So $[a]_n$ has an inverse (and all its powers have inverses).

Consider

$$[a], [a]^2, [a]^3, \ldots, [a]^{n+1}$$

$\mathbb{Z}_n$ has only n elements. Thm $\exists$ k,t $k \neq t$.

$$[a]^k = [a]^t$$

$$[a]^k([1] - [a]^{t-k}) = [0]$$

multiply by $[a]^k$ inverse

$$[a]^{t-k} = [1]$$

□.

How do the powers repeat?

Thm $[a]_n$ has order k

$$[a]_n^r = [a]_n^s \iff r \equiv s \bmod k.$$

Pf $\Leftarrow$ $\quad r = s + k \cdot t$.

$$[a]^r = [a]^{s+kt} = [a]^s ([a]^k)^t = [a]^s \cdot [1] = [a]^s$$

$\Rightarrow$ Suppose $r \leq s$.

$[a]_n$ has order k. So $(a,n) = 1$

($[a]_n$ and) $[a]_n^r$ have an inverse.

$$[1]_n = [a]_n^{s-r}$$

Write $\quad s - r = qk + u \quad 0 \leq u < q$

$$[1] = [a]^{qk+u} = ([a]^k)^q \cdot [a]^u = [a]^u$$

$0 \leq u < q$. So $u = 0$.

$$s - r = kq$$

$\square$.

Ex) powers of $[4]_5$

$1 \quad 4 \quad 1$ order = 2 / 5-1

powers of $[4]_7$

~~1 4~~ $1 \quad 4 \quad 2 \quad 1$ order = 3 / 7-1

powers of $[5]_7$

$1 \quad 5 \quad 4 \quad 6 \quad 2 \quad 3 \quad 1$ order = 6 / 7-1

What are the possible orders?

Thm (Fermat) p prime

$$[a]_p^{p-1} = [1]_p \qquad ([a]_n \neq 0)$$

In particular

$$[a]_p^{p} = [a]_p$$

Cor all non-zero elmts of $\mathbb{Z}_p$ have finite order and the order divides $p-1$.

Pf) $G_p \subset \mathbb{Z}_p$ all invertible elents

$$G_p = \{[1], [2], \cdots, [p-1]\}.$$

because p is prime.

let $[a]G_p = \{[a][b] \mid [b] \in G_p\} \subset G_p$.

Claim: $\#[a]G_p = \#G_p$.

Pf) Suppose $\left.\begin{matrix}[a][b] = [a][c] \\ [a] \text{ invertible}\end{matrix}\right\} \Rightarrow [b] = [c]$ □

So $[a]G_p = G_p$.

let $[N] = [1][2]\cdots[p-1] \in G_p$.

Because $[a]G_p = G_p$

$$[N] = [a][1]\ [a][2] \cdots [a][p-1]$$

So $\left.\begin{matrix}[N] = [a]^{p-1}[N] \\ [N] \text{ invertible}\end{matrix}\right\} \Rightarrow [1] = [a]^{p-1}$

□

Def: $\phi(n) = \#G_n$.

Generalization of Fermat Theorem for general moduli n.

Thm $n \geq 2$ (Euler)
$(a,n)=1$ (a has fmo).

$$[a]_n^{\phi(n)} = [1]_n.$$

Cor: order of $a \mid \phi(n)$.

This is only useful to determine order of $[a]_n$ if one knows $\phi(n)$.

The following Thm's allow to calculate all $\phi(n)$.

Thm p prime $n \geq 1$

$$\phi(p^n) = p^n - p^{n-1}$$

Proof] $\phi(p^n) = \#G_{p^n}$.

an elem $[a]_{p^n} \in G_{p^n}$ has $(a, p^n) = 1$.

So a has no factors p. The numbers which have a factor p are

$$p \cdot k \quad \text{with } 1 \le k < p^{n-1}$$

So $\#G(p^n) = p^n - p^{n-1}$ □.

Thm $(a,b) = 1$

$$\phi(a)\,\phi(b) = \phi(ab).$$

Pf] We will define

$$h: G_a \times G_b \longrightarrow G_{ab}$$

and show that h is a bijection.

This would mean.

$$\phi(ab) = \#G_{ab} = \#G_a \cdot \#G_b = \phi(a)\,\phi(b)$$

Done.

Definition h

$[r]_a \in G_a \qquad [s]_b \in G_b \qquad [x]_{ab} \in G_{ab}$

$h([r]_a, [s]_b) = [x]_{ab}.$

Solve

$$\begin{cases} x \equiv r \mod a \\ x \equiv s \mod b \end{cases}$$

$\exists!\ [x]_{ab}$ (Chinese Remainder Thm).

This defines h.

Claim: h is onto.

Choose $[x]_{ab} \in G_{ab}$ let $[r]_a = [x]_a$

and $[s]_b = [x]_b$.

Claim: h is injective (1-1)

If $h([r_1][s_1]) = [x]$ and

$h([r_2][s_2]) = [x]$ then

$$\left.\begin{array}{l} x \equiv r_1 \mod a \\ x \equiv r_2 \mod a \end{array}\right\} \Rightarrow r_1 = r_2$$

Similarly $s_1 = s_2$

Conclusion: $\exists\ h: G_a \times G_b \to G_{ab}$ bijection

□.

Examples

$$\phi(15) = \phi(3\cdot 5) \left.\begin{matrix} \\ (3,5)=1 \end{matrix}\right\} = \phi(3)\,\phi(5)$$

$$= (3^1 - 3^0)(5^1 - 5^0) = 2\cdot 4 = 8$$

$$\phi(72) = \phi(3^2 \cdot 2^3) \left.\begin{matrix} \\ (3^2, 2^3)=1 \end{matrix}\right\} = \phi(3^2)\,\phi(2^3)$$

$$= (3^2 - 3^1)(2^3 - 2^2) = 6\cdot 4 = 24.$$

Pf Euler | The proof is in essence the same as the given proof for the Fermat Thm.

Consider G_n. $\#G_n = \phi(n)$.

$(a,n)=1 \therefore [a]_n \in G_n$ is invertible.

let $[a]_n G_n = \{[a][b] \mid [b] \in G_n\}$.

The same proof as for Fermat Shows.

$$[a]_n G_n = G_n.$$

let $[N] = \prod_{[b]_n \in G_n} [b]$.

$$= \prod_{[a][b] \in [a]G_n} [a][b] = [a]^{\#G_n} [N]$$

So $[a]_n^{\phi(n)} = [1]_n$. □

Ex] What is the order of $[3]_{14}$?

$(3,14)=1$. So $[3]_{14}$ has finite order k.

$k \mid \phi(14)$.

$$\phi(14) = \phi(2\cdot 7) = \phi(2)\,\phi(7) = (2-1)(7-1) = 6$$

$(2,7)=1$

So $k \mid 6$: $k = \cancel{1}, \cancel{2}, \cancel{3}, 6$

$[3]_{14}^2 = [9]_{14} \neq 1$

$[3]_{14}^3 = [27]_{14} = [13]_{14} \neq 1$

order $[3]_{14} = 6$