Prop 7.1 For any a, b $\exists!\, q, r$ s.t. $a = qb + r$ $\quad 0 \le r < b$

$b \mid a$ b divides a

Prop 7.2 Let $a, b \in \mathbb{Z}$. Then $\exists\, X, Y$ s.t. $aX + bY = \gcd(a, b)$

gcd is minimal such linear combination

Prop 7.4 $p \mid N$, $q \mid N$ and $(p, q) = 1$ then $pq \mid N$.

divisibility

7.7 a is invertible mod N iff $\gcd(a, N) = 1$

$\boxed{ac = 1 \bmod N}$

modulo

Thm 7.14 $m = |G|$. Then $\forall g \in G$ $\quad g^m = 1$

corollary $m = |G|$. Then $\forall g \in G$ $\quad g^i = g^{[i \bmod m]}$

corollary $m = |G|$. $f_e = cg^e$ is permutation if $(e, m) = 1$

groups

7.1.4

- $\mathbb{Z}_n^+$, $|\mathbb{Z}_n^+| = n$ (Always cyclic)
- $\mathbb{Z}_n^*$, $|\mathbb{Z}_n^*| = \phi(n)$ (need not be cyclic) $\cancel{\mathbb{Z}_n^* \cong \mathbb{Z}_K}$ $\boxed{n < K}$
- $\phi(n)$ = # of elements $\{1, \dots, p-1\}$ coprime with n.
- $|\mathbb{Z}_p^*| = p - 1$ - prime is always cyclic but $\mathbb{Z}_8^+$ is not

Proof.

$\Rightarrow$ assume a is invertible, let b be the inverse

$ab = 1 \bmod N$ $\quad\quad ab = qN + r \quad\quad 1 = q'N + r$

$$ab - 1 = (q - q')N$$

$$\boxed{ab - 1 = cN}$$

$$\boxed{ab - cN = 1}$$

$$\boxed{\gcd(a, N) = b\underline{a} - c\underline{N} = 1}$$ by Previous Thm

---

$\Leftarrow$ If $\gcd(a, N) = 1$ then $\exists X, Y$ s.t. $Xa + YN = 1$ Thm

$$Xa - 1 = -YN \quad \text{Solve}$$

unique $\Downarrow$ $r = r'$ $\quad \rightarrow \quad \boxed{\begin{aligned} Xa &= qN + r \\ 1 &= q'N + r \end{aligned}}$ where $\cancel{m} = -YN$ $\quad (q - q') = -Y$

$Xa \equiv 1 \bmod N \Rightarrow X$ is inverse of a

Groups

Def. A group G is a set with a binary operation $*$ such that;

1. Closure: For all $g, h \in G$, $g * h \in G$
2. Existence of an identity: There $\exists\, e \in G$ s.t. $\forall g \in G$, $e * g = g * e = g$
3. Existence of an inverse: $\forall g \in G$, $\exists\, h \in G$ s.t. $g * h = h * g = e$
4. Associativity: $\forall g_1, g_2, g_3 \in G$ $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$

Def. A group G is abelian if $\forall g, h \in G$, $gh = hg$.
(Commutativity)

Def. G is a finite group if the set G has a finite amount of elements. The order of a group is denoted $|G|$.

In this course we will only consider finite abelian groups.

Def. H is a subgroup of G if H is a subset of G that is a group under the same operation.

Unwritten Notes

1. Associativity implies order of group operation does not matter
2. The identity is unique.
3. The inverse of an element is unique. Meaning a group element has only 1 inverse.

Notation: Group operations

	Symbol	identity	inverse	exponentiation
Additive notation	$+$	0	$-a$	$m \cdot a$
Multiplicative notation	$*$	1	a^{-1}	a^{m}

1. Group operations do not represent integer addition and multiplication!
2. They are merely used as notation which is reflected in the indentity and inverses
3. A useful application of the notation is exponentiation
4. Which is just the application of a group operation of an element to itself numerous times.

Example. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with operation $+$ under modulo N.

Identity element: 0

Inverse of g : $[-g \bmod N]$

Associativity : Follows from formal definition of equivalence classes of $\mathbb{Z}$ and $\mathbb{Z}_n$

Commutativity: $[a] + [b] \bmod n = [b] + [a] \bmod n$

Order: n

Example 2 $(\mathbb{Z}_{15}, +)$ has 15 elements

Lemma. Let G be group and $a, b, c \in G$. If $ac = bc$ then $a = b$.
Furthermore if $ac = c$ then a is the identity element.

Proof. $ac = bc \mapsto acc^{-1} = bcc^{-1} \mapsto a = b$

(multiplicative operation)

Example 3 $(\mathbb{Z}_{15}, *) \neq (\mathbb{Z}_{15}, +)$

$3 * b = 1$ where $b = 0, \ldots, 14$ $\boxed{3 * b = 15K + 1}$.

But a is invertible iff $\gcd(a, 15) = 1$. This implies $3 \notin (\mathbb{Z}_{15}, *)$.

In fact $\mathbb{Z}_{15}, *$ does not form a group if we use all elements of the set!

- Invertible elements form a group under multiplication modulo N but it is different than the group under addition

Group exponentiation.

Apply group operation m times to a fixed element g.

Additive exponentiation notation: $mg = \underbrace{g + g + \cdots g}_{m \text{ times}}$

This notation not multiplication

Multiplicative exponentiation notation $g^m = \underbrace{g \cdot g \cdots g}_{m \text{ times}}$

Multiplicative exponentiation rules hold

$$g^m \cdot g^{m'} = g^{m+m'}$$

$$(g^m)^{m'} = g^{mm'}$$

$$g^1 = g$$

$$g^{-m} \underset{\text{def}}{=} (g^{-1})^m$$

Lets go back to the question, what is the group of some modulo group under multiplication?

<u>Def.</u> $(\mathbb{Z}_n, *) = \mathbb{Z}_n^*$ is the group of invertible elements under multiplication

<u>Question.</u> What are the invertible elements?

$$\gcd(a,n) = 1 \longleftrightarrow a \text{ is invertible}$$

<u>Example</u> $(\mathbb{Z}_{15}^*) = \{1,2,4,7,8,11,13,14\}$, order $|\mathbb{Z}_{15}^*| = 8$

order $|\mathbb{Z}_{15}| = 15$

These groups share elements but structurally they are very different since there orders are of different magnitudes!

Let's see some more properties.

<u>Thm.</u> Let G be a finite group with $m = |G|$. Then $\forall g \in G$

$$g^m = 1$$

<u>Proof.</u> Note this is a famous Thm called Fermat's little Thm.

We will prove a special case where G is abelian

(1) Let G be abelian. Fix $g \in G$ and let $g_1, \ldots, g_m$ be elements of G.

(2) $gg_i = gg_j$ implies $g_i = g_j$

(3) Then $g_1 \cdots g_m = (gg_1) \cdots (gg_m)$

(4) Since G is abelian $g_1 \cdots g_m = g^m (g_1 \cdots g_m)$

(5) $1 = g^m$

<u>Nonabelian case is a bit harder</u>

Corollary. Let G be a finite group with $m' = |G| > 1$. Then for any $g \in G$ and any m, $g^m = g^{[m \bmod m']}$

Proof. Suppose $m > m'$ then

$m = qm' + r$ and $[m \bmod m'] = r$ Then

$$g^m = g^{qm'+r} = g^{qm'} g^r = (g^{m'})^q g^r = 1 g^r$$

$$= g^{[m \bmod m']}$$

Example. What is $[3^{12002} \bmod 77]$? (Assume elements are in $\mathbb{Z}^*_{77}$)

↑ has order 60

$$3^{12002} \bmod 77 = 3^{12002 \bmod 77} \bmod 77$$

Since we are working in exponentials

$$= 3^{67} \bmod 77$$

$3^{67} = g$ is invertible mod 77 since

Example Find $[3^{12002} \bmod 77]$ when $g \in \mathbb{Z}_{77}^*$.

① Order $|\mathbb{Z}_{77}^*| = 60$

② $3^{12002} = 3^{12002 \bmod 60} = 3^2 = 9$

③ $[9 \bmod 77] = 9$

Corollary 7.17

Let G be a finite group with $m = |G| > 1$. Let $e > 0$ be an integer, and define $f_e : G \to G$ by $f_e(g) = g^e$. If $\gcd(e, m) = 1$ then f_e is a permutation:

If $d = [e^{-1} \bmod m]$ then f_d is the inverse of f_e.

Proof. If $(e, m) = 1$ then e is invertible modulo m. So $e^{-1} \bmod m$ exists. Then $\forall g$

$$f_d(f_e(g)) = f_d(g^e) = (g^e)^d = g^{ed \bmod m} = g^1 = g$$

Therefore f_d is a permutation and f_e is the inverse.

7.1.4 - The group $\mathbb{Z}_n^*$ and CRT

Def. The group $\mathbb{Z}_n^* = \{ a \in \{1, \dots, N-1\} \mid \gcd(a, N) = 1 \}$

- Exercise show this is a group!

The euler totient function is directly related to $\mathbb{Z}_n^*$.

Def. $\Phi(N) =$ # of integers $0 < i < N$ s.t $\gcd(N, i) = 1$

$\Phi(N) = |\mathbb{Z}_n^*|$

Examples.

Let $N = p$ be prime.

$\Phi(P) = p - 1$ since $\gcd(P, i) = 1$ then for $1 \leq i < p$

Let $N = pq$ s.t p, q are unique primes.

Compute $\Phi(N)$

If $a \in \{1, \dots, N-1\}$ and $(a, N) \neq 1$ then either

$(a, p) \neq 1$ or $(a, q) \neq 1$.

Note: $p | a$ or $q | a$ but $p | a$ and $q | a$ is not true since

then $pq | a$ but $a < N = pq$

- The elements in $\{1, \dots, N-1\}$ which are divisible by p are

$\{p, 2p, 3p, \dots, (q-1)p\} = \alpha$ $\quad |\alpha| = q-1$

- By symmetry, divisible elements by q are $\{q, 2q, \dots, (p-1)q\} = \beta$

$|\beta| = p-1$

- Remaining elements $N - 1 - |\alpha| - |\beta|$

$$= N - 1 - (p-1) - (q-1)$$

$$= pq - 1 - p + 1 - q + 1$$

$$= pq - p - q + 1$$

$$\Phi(N) = (p-1)(q-1)$$