Review

$S = \{0, 1, 2, \ldots, N\}$

① last time we introduced two groups on the set of integers 0 to N.

	$\mathbb{Z}_N$	$\mathbb{Z}_N^*$
Identity:	0	1
Operation:	$+$	$*$
Order:	N	$\phi(N)$
elements:	$\{0, 1, \ldots, N\}$	Invertible elements of S $\longleftrightarrow$ $(e, N) = 1$

② It's important to note that even though these groups are acting on many of the same elements they are not related to each other on a group level.

I.E. $\mathbb{Z}_N^* \not< \mathbb{Z}_N$

① Finish grading
② Make puzzle
③ Final Matter
④ Video's

Thm. Let $N = \prod_i p_i^{e_i}$ where $\{p_i\}$ are distinct primes and $e_i \geq 1$. Then $\phi(N) = \prod_i p_i^{e_i - 1}(p_i - 1)$ Homework!

$$\phi(p^2) = |\{1, p, 2p, \dots, (p-1)p\}^c| = p^2 - \phi(p-1) = p^2 \cancel{\ } + p + 1$$

$$= p^2 - p + 1$$

..

$(p-1)(p$

$p^2 - p = p(p-1)$

$\phi(p^3)$ $\{1, p, \dots, p-1, p^2\}$

$\underbrace{\quad p-1 \cdot p}_{p^2}$ $\underbrace{1 \cdot p^2 \quad \dots \quad p-1 \cdot p^2}_{p-1}$

$p^3 - p^2$

$p^2(p-1)$

$p^3 - p^2 + p - \cancel{1}$

Last time we stated the following Thm.

- This allows us to compute the order of $\mathbb{Z}_n$ with the multiplicative operation

Here is a rewording of the previous corollaries.

Corollary

1. Let $N>1$ and $a \in \mathbb{Z}_N^*$. Then $a^{\phi(N)} = 1 \bmod N$.
2. If N is prime and $a \in \{1, \dots, p-1\}$ then $a^{p-1} = 1 \bmod p$

FLT

Note. If $\mathbb{Z}_p^*$, where p is prime, then $|\mathbb{Z}_p^*| = p-1$.

3. Fix $N>1$. If $(e, \phi(N))=1$ then f_e is a permutation.
4. If $d = [e^{-1} \bmod \phi(N)]$ then f_d is the inverse of f_e.

Permutation

- We would like to understand the group structure of $\mathbb{Z}_n$ and $\mathbb{Z}_n^*$. To do this we need to introduce the CRT.
- Let's define the cross product of groups and review isomorphisms

Def. Let $(G, *)$, $(H, \circ)$ be groups. A function $f: G \to H$ is an isomorphism if

1. f is a bijection (injection + surjection)
2. $f(g_1 * g_2) = f(g_1) \circ f(g_2)$

More or less the groups are the same group if they are isomorphic. If we prove something about one, we learn about the other.

• Classic structure that you have seen in Calc III and Linear Algebra.

Def. Let $(G,*)$ $(H,\circ)$ be groups. Then $G \times H$ is the cross product of G, H. $G \times H$ is a group where

1. $a \in (G \times H)$ s.t. $a = (g, h)$ where $g, \in G$, $h \in H$
2. $(g,h) \bar{\circ} (g',h') = (g * g', h \circ h')$
3. If G, H is finite then $|G \times H| = |G|\,|H|$
4. $e \in G \times H \mapsto (e_G, e_H)$

Thm. Chinese Remainder Thm.

Let $N = pq$ where $(p,q) = 1$. Then

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q \quad \text{and} \quad \mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

The modular group is isomorphic to the cross product of the modular groups determined by the factors of N.

Continued

Note.

$\mathbb{Z}_N^*$ need not be cyclic - $\mathbb{Z}_6^* \simeq \mathbb{Z}_2^* \times \mathbb{Z}_3^*$

$\mathbb{Z}_N$ is always cyclic

$\mathbb{Z}_N^* \simeq C_{\varphi(N)}$ iff $\mathbb{Z}_N^*$ is cyclic

Let f map $x \in \{0, \ldots, N-1\}$ to (x_p, x_q) with $x_p \in \{0, \ldots, p-1\}$ and $x_q \in \{0, \ldots, q-1\}$ is defined by

$$f(x) = \left([x \bmod p], [x \bmod q] \right)$$

Second part.

Externaly useful for Computations

Then f is an isomorphism from $\mathbb{Z}_N$ to $\mathbb{Z}_p \times \mathbb{Z}_q$ and from $\mathbb{Z}_N^*$ to $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

Note.

1. $\mathbb{Z}_n^*$ is not necessarily cyclic: $\mathbb{Z}_8^* \simeq \mathbb{Z}_2 \ast \mathbb{Z}_2$.
2. It is known when $\mathbb{Z}_n^*$ is cyclic not needed (yet.)
3. $\mathbb{Z}_n$ is always a cyclic group. Generator g are of the following form $(g, n) = \underline{1}$. 1 is a generator.
4. $\mathbb{Z}_p^*$ is cyclic if p is prime.

Proof.

If $x \in \mathbb{Z}_n$ then $x \longmapsto (x \bmod p, x \bmod q)$.

So $f(x) = (x_p, x_q)$.

(1.) f is 1-1.

$f(x) = f(x') \rightarrow$

p	q
$x = x \bmod p$	$x = x \bmod q$
$x' = x \bmod p$	$x' = x \bmod q$
$x - x' = 0 \bmod p$	$x - x' = 0 \bmod q$

$x - x'$ are divisible by p, q but $\gcd(p, q) = 1$ $\longrightarrow$ $x - x'$ is divisible by pq, $x - x' = 0 \bmod N$

$x = x' \bmod N \longrightarrow x = x' \in \mathbb{Z}_N$

$\longrightarrow$ f is 1-1

(2) Surjection

$|\mathbb{Z}_N| = N = pq$

$|\mathbb{Z}_p \times \mathbb{Z}_q| = |\mathbb{Z}_p| \, |\mathbb{Z}_q| = pq$

Since f is an injection and each element maps uniquely, this implies $\forall (x_p, x_q) \in \mathbb{Z}_p \times \mathbb{Z}_q$, $\exists\, g \in \mathbb{Z}_N$ s.t.

$$f(g) = \mathbb{Z}_p \times \mathbb{Z}_q$$

---

(3) $f(a+b) = f(a_p, a_q) + f(b_p, b_q)$

$$([a+b \bmod p], [a+b \bmod q])$$

$$= ([a \bmod p], [a \bmod q]) + ([b \bmod p], [b \bmod q])$$

$$= f(a) + f(b)$$

$\mathbb{Z}_N^*$

$x \in \mathbb{Z}_N^*$ then $(x_p, x_q) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

Suppose not. $x_p \notin \mathbb{Z}_p^*$ then $\gcd([x \bmod p], p) \neq 1$.

Then $(x, p) \neq 1 \Rightarrow (x, N) \neq 1$

$$f(a) + f(b) = ([a \bmod p], [a \bmod q]) + ([b \bmod p], [b \bmod q])$$

$$= ([[a \bmod p] + [b \bmod p]], [[a \bmod q] + [b \bmod q]])$$

$$= ([a \bmod p + b \bmod p], [a + b \bmod q])$$

$$[[a \bmod p] + [b \bmod p]] = [a + b \bmod p]$$

$$[a' + b']$$

$a + b = \underline{m}p + \underline{r}$

$a = m'p + r'$

$b = m''p + r''$

$$[[a \bmod p] + [b \bmod p]] = [a + b \bmod p]$$

$$[a\%p + b\%p] = [a + b\%p] = [a\%p + b\%p]$$

Lets use the CRT, to simplify elements

Example. Let's compute $11^4 \bmod 15$ where $11 \in \mathbb{Z}_{15}^*$

$$11^4 = (\underbrace{1 \bmod 5}_{\mathbb{Z}_5}, \underbrace{2 \bmod 3}_{\mathbb{Z}_3})^4 = (1^4 \bmod 5, 2^4 \bmod 3) = (1 \bmod 5, 1 \bmod 3)$$

Homomorphism

$$f(11 \cdot 11 \cdot 11 \cdot 11) = f(11) f(11) f(11) f(11) \qquad = (1,1) = 1 \bmod 15$$

---

(1) It is easy to map an element x modulo N to the corresponding representation modulo p, q.

$$x \in \mathbb{Z}_N^* \longmapsto (x \bmod p, x \bmod q) \in \mathbb{Z}_p^*, \mathbb{Z}_q^*$$

(2.) We can go in the reverse direction if we know the factorization of N.

(1) Any element $(x_p, x_q) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ can be rewritten as

$$(x_p, x_q) = x_p(1,0) + x_q(0,1)$$

(2) If we find $I_p, I_q \in \{0, \ldots, N-1\}$ s.t. $I_p \to (1,0)$ and $I_q \mapsto (0,1)$ then

$$(x_p, x_q) = x_p(1,0) + x_q(0,1) \xrightarrow{f^{-1}} [x_p \cdot I_p + x_q \cdot I_q \bmod N]$$

Since p, q are distinct primes.

(3) Claim $I_p = [Y_q \bmod N]$ and $I_q = [X_p \bmod N]$ if

$X(p) + Y(q) = 1$. (exists and is true since p, q are primes)

☆ $[[Y_q \bmod N] \bmod p] = [Y_q \bmod p] = [(1 - \cancel{X}p) \bmod p] = 1$

By Lemma $\exists$ unique X, Y s.t.

$$Xp + Yq = 1.$$

Claim $1_p = [Yq \bmod N]$ (I.e. $Yq \bmod N \to (1,0)$)

$$\left[\{ Yq \bmod N \} \bmod p \right] = [Yq \bmod p] = [(1-Xp) \bmod p] = 1 \bmod p$$

b/c $\{Yq \bmod N\} \le N-1$ and not divisible by p

$$\left[[Yq \bmod N] \bmod q \right] = [Yq \bmod q] = 0 \bmod q$$

$$1_p = [Yq \bmod N] \longrightarrow (1,0)$$

by Symmetry

$$1_q = [Xp \bmod N] \longrightarrow (0,1)$$

Summary $(x_p, x_q) \longmapsto x_N$

① Compute X, Y s.t. $Xp + Yq = 1$ (By Extended Euclidean algorithm) Use calculator

② Set $1_p = [Yq \bmod N]$ and $1_q = [Xp \bmod N]$

③ Compute $x = [(x_p \cdot 1_p + x_q \cdot 1_q) \bmod N]$

Compute $2021^{2020} \bmod 35$.

$35 = 7 \cdot 5$

$$\mathbb{Z}_5^* \qquad \mathbb{Z}_7^*$$

$$2021 \longmapsto (2021 \bmod 5,\ 2021 \bmod 7) = (1 \bmod 5,\ 5 \bmod 7)$$

$$2021^{2020} \longmapsto (1 \bmod 5,\ 5 \bmod 7)^{2020} = (\underbrace{1^{2020} \bmod 5}_{\mathbb{Z}_5^*},\ 5^{2020} \bmod 7)$$

$$\mathbb{Z}_7^*$$

$$= (1^{2020} \bmod 5,\ 5^4 \bmod 7) = (1 \bmod 5,\ 2 \bmod 7)$$

$$= [51 \bmod 35] = 16 \bmod 35$$

$X \cdot 5 + Y 7 = 1 \qquad X = 3,\ Y = -2$

$[14 \bmod N] = -14 \qquad + 3 \cdot 5 \bmod 35 = 1$

$1_p = 21 \qquad 1_q = 15.$

7.30

Compute $18^{25} \bmod 35$.

$$18 \xrightarrow[\text{crt}]{} ([18 \bmod 5],\ 18 \bmod 7) = (3, 4)$$

$$18^{25} \longrightarrow (3^{25} \bmod 5,\ 4^{25} \bmod 7) = (3^{25 \bmod 4} \bmod 5,\ 4^{25 \bmod 6} \bmod 7)$$

$\mathbb{Z}_5^*$ $\mathbb{Z}_7^*$

$\boxed{3 \in \mathbb{Z}_5^*}$ $3^{25} \bmod 5$

$$= (3^1 \bmod 5,\ 4 \bmod 7)$$

1. compute X, Y for $Xp + Yq = 1$

$X = 3$ $Y = -2$

2. $1_p = -2 \cdot 7 \bmod 35 = 21 \bmod 35$

$1_q = 3 \cdot 5 \bmod 35 = 15 \bmod 35$

3. $1_p\, 3 + 1_q\, 4 \bmod 35$

$63 + 45 \bmod 35$

$108 \bmod 35 = 18$