Math 4400
Week 4 - Thursday
More Lagrange, refined CRT, and fields.

Example (Like Exercise 2 - (3)).
Compute 3^{29} in $\mathbb{Z}/21\mathbb{Z}$.

⚠ 3 and 21 are not coprime, $\gcd(3,21) = 3 \neq 1$.
So $3 \notin (\mathbb{Z}/21\mathbb{Z})^\times$.

Note $21 = 7 \cdot 3$. We'll compute 3^{29} in $\mathbb{Z}/7\mathbb{Z}$ and 3^{29} in $\mathbb{Z}/3\mathbb{Z}$, then solve the congruence.

$3^{29} = 0$ in $\mathbb{Z}/3\mathbb{Z}$
because $3 \mid 3^{29}$
Know $3^{29} = 0 \bmod 3$

3^{29} in $\mathbb{Z}/7\mathbb{Z}$
$\gcd(3,7) = 1$ so
$3 \in (\mathbb{Z}/7\mathbb{Z})^\times$ and can use

$3^{29} = 5 \bmod 7$

Can find $3^{29} \bmod 21$ by solving $x \equiv 0 \bmod 3$, $x \equiv 5 \bmod 7$

$\boxed{3^{29} = 12 \bmod 21.}$

Lagrange, $|(\mathbb{Z}/7\mathbb{Z})^\times| = \phi(7) = 6$

$3^{29} = 3^{4\cdot 6 + 5}$ in $(\mathbb{Z}/7\mathbb{Z})^\times$

$= (3^6)^4 \cdot 3^5$ (by Lagrange $\Rightarrow 1$)

$= 3^5$ in $\mathbb{Z}/7\mathbb{Z}$

Can use $3^5 = 3^{-1} = 5$ in $\mathbb{Z}/7\mathbb{Z}$.

Chinese Remainder Theorem revisited!

Theorem: If $m_1, \ldots, m_K$ are pairwise coprime ($\gcd(m_i, m_j) = 1$ for all $i \neq j$), then the natural map

$$\mathbb{Z}/m_1 \cdots m_K \mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_K\mathbb{Z}$$

$$a \bmod m_1 \cdots m_K \longmapsto (a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_K)$$

i.e. take a, divide by m_i, take remainder.

Is a ring isomorphism (a bijection that respects multiplication and addition laws).

In particular, it restricts to a group isomorphism (a bijection that respects the group law)

$$(\mathbb{Z}/m_1 \cdots m_K \mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_K\mathbb{Z})^\times = (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_K\mathbb{Z})^\times.$$

i.e. a has a mult. inverse mod $m_1 \cdots m_K$ $\Leftrightarrow$ a has a mult. inverse mod m_i for each i.

Corollary: If $m_1, \ldots, m_K$ are pairwise coprime, $\phi(m_1 \cdot m_2 \cdots m_K) = \phi(m_1)\phi(m_2) \cdots \phi(m_K)$.

A useful reinterpretation of $\mathbb{Z}/n\mathbb{Z}$.

Before: $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$
with multiplication + addition defined
by taking remainders after dividing by n.

Note: Nothing special about $\{0, 1, \ldots, n-1\}$
EXCEPT that every integer is
congruent to exactly one of these mod n.

Sometimes useful to consider a different <u>set of representatives</u> for the congruence classes mod n.

Example: $\mathbb{Z}/12\mathbb{Z}$ and clock arithmetic.
$\{0, \ldots, 11\}$ is not the right set for telling time.
Instead use $\{1, \ldots, 12\}$ as representatives.

A better definition of $\mathbb{Z}/n\mathbb{Z}$:

$\mathbb{Z}/n\mathbb{Z}$ is the set of congruence classes mod n.

<u>Example</u>:

- $\mathbb{Z}/2\mathbb{Z}$ has 2 elements:
  0 mod 2 (even) 1 mod 2 (odd)

$\{\ldots,-4,-2,0,2,4,\ldots\}$ $\quad$ $\{\ldots,-3,-1,1,3,5,\ldots\}$.

- $\mathbb{Z}/3\mathbb{Z}$ has 3 elements:

$0 \bmod 3 = \{\ldots,-3,0,3,6,\ldots\}$ $\quad$ $1 \bmod 3 = \{\ldots,-2,1,4,7,\ldots\}$ $\quad$ $2 \bmod 3 = \{\ldots,-1,2,5,\ldots\}$.

Can compute in $\mathbb{Z}/n\mathbb{Z}$ using <u>any</u> set of representatives.

$\{0,1,\ldots,n-1\}$ – the <u>standard representatives</u>

Gear shift for last couple of minutes:

Definition: A <u>field</u> is a ring such that every non-zero element is invertible.
(i.e. a ring R is a field if $R^\times = R\setminus\{0\}$).

Example:

- $\mathbb{Z}$ is not a field – $\mathbb{Z}^\times = \{\pm 1\} \neq \mathbb{Z}\setminus\{0\}$
- $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields
- $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.

$\mathbb{Z}/n\mathbb{Z}$ is a field $\iff$

$(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$

$\iff |(\mathbb{Z}/n\mathbb{Z})^\times| = |\mathbb{Z}/n\mathbb{Z} \setminus \{0\}|$

$\iff \phi(n) = n-1$.

Holds if n is prime, simple exercise to check it never holds if n is not prime.