Math 122 Monday, October 3

$\mathbb{Z}, +$ recall all nonzero subgroups have the form $n\mathbb{Z}$, $n \geq 1$

quotient group $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} : a = 0, 1, 2, \ldots, n-1\}$ finite of order n
cyclic, generated by $1 + n\mathbb{Z}$

Can also multiply cosets $(a+n\mathbb{Z})(b+n\mathbb{Z}) = ab + n\mathbb{Z}$
well defined because $(a+nk)(b+nl) = ab + anl + bnk + n^2kl$
$= ab + n(\cdots)$

elements $a' \in a + n\mathbb{Z}$ write $a' \equiv a \pmod{n}$ or $a' \equiv a\ (n)$ if you are lazy
e.g. $2 \equiv 3 + 7 \pmod{8}$
$5 \equiv 3 \times 7 \pmod{8}$

arithmetic mod n $n \geq 2$ (so that the additive identity $n\mathbb{Z} \neq$ mult. identity $1 + n\mathbb{Z}$)

note: multiplication mod n is associative
multiplication has an identity $1 \pmod{n}$ $a \cdot 1 \equiv a \pmod{n}$

The coset $0 \pmod{n}$ has no inverse. $0 \cdot a \equiv 0 \pmod{n}$
an inverse to $a \pmod{n}$ is a coset $b \pmod{n}$ with $ab \equiv 1 \pmod{n}$

But some cosets have no inverse (e.g. $2 \pmod{6}$).
We can still find a group by restricting to the invertible elements
(e.g. $GL_n(\mathbb{R}) \subset M_n(\mathbb{R})$ the set of matrices w/ $\det \neq 0$)

Write $(\mathbb{Z}/n\mathbb{Z})^* \subset (\mathbb{Z}/n\mathbb{Z})$ the set of cosets $a \pmod{n}$ with a multiplicative inverse. This is an abelian group, containing $1 + n\mathbb{Z}$ but not $0 + n\mathbb{Z}$, closed under multiplication but not addition.

Know $\mathbb{Z}^* = \{\pm 1\} \subset \mathbb{Z}$ but what is the structure of $(\mathbb{Z}/n\mathbb{Z})^*$?

Recall Euclid's greatest common divisor:

defn $d = \gcd(a, n)$ if d divides both a and n and is the largest integer to do so.
If $\gcd(a, n) = 1$ then say a and n are relatively prime.

e.g. $\gcd(15, 21) = 3$

Goal Show that $(\mathbb{Z}/n\mathbb{Z})^* = \{a \pmod{n} : \gcd(a, n) = 1\}$.

Suppose $a, b \geq 1$. Then b divides $a \iff b\mathbb{Z} \supset a\mathbb{Z}$.
If $a = bk$ then $na = nbk = (nk)b$ so $a\mathbb{Z} \subset b\mathbb{Z}$.
Conversely if $a\mathbb{Z} \subset b\mathbb{Z}$ then $a = bk$.

Take $a, n \geq 1$. Consider the subgroup $H \subset \mathbb{Z}$ generated by a and n.
$H = a\mathbb{Z} + n\mathbb{Z} = \{xa + yn : x, y \in \mathbb{Z}\}$.

But H is a subgroup of $\mathbb{Z}$ so $H = d\mathbb{Z}$ for some $d \geq 1$.

Claim If $a\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ then $d = \gcd(a, n)$.
Pf: Note $a\mathbb{Z} \subset d\mathbb{Z}$, $n\mathbb{Z} \subset d\mathbb{Z}$ so d divides a and n. If e divides a and n then $e\mathbb{Z} \supset a\mathbb{Z}$ and $e\mathbb{Z} \supset n\mathbb{Z} \Rightarrow e\mathbb{Z} \supset a\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z} \Rightarrow e$ divides d.

Corollary $\exists$ integers x and y: $\gcd(a, n) = d = xa + yn$. Pf: $d \in d\mathbb{Z} = a\mathbb{Z} + n\mathbb{Z}$.

So suppose $\gcd(a, n) = 1$
$xa + yn = 1 \Rightarrow xa \equiv 1 \pmod{n} \Rightarrow a^{-1} \equiv x \pmod{n}$
If a^{-1} exists then $xa \equiv 1 \pmod{n} \Rightarrow xa = ynx + 1 \Rightarrow \gcd(a, n) = 1$.

defn $\varphi(n) =$ order of $(\mathbb{Z}/n\mathbb{Z})^*$ the Euler phi function.

Say $n = p$ a prime. Then $\{1, 2, \ldots, p-1\}$ relatively prime and $\varphi(p) = p - 1$.

Say $n = pq$, a product of primes. Here $\varphi(n) = pq - \#\text{div. by } q - \#\text{div. by } p + 1$
(note divisible by p and q $\Rightarrow$ divisible by n or 0 so add back 1)

$\#$ div. by $q = p$ and $\#$ div. by $p = q$ so $\varphi(n) = pq - p - q + 1 = (p-1)(q-1)$

Note: if you know n and $\varphi(n)$ you can easily find p and q, good for cryptanalysts
But it is not easy to find $\varphi(n)$ given n if you don't know the prime factorization!

More examples: $\mathbb{Z}/8\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$ a group of order 4

We know 2 group of order 4: $\mathbb{Z}/4\mathbb{Z}$ and the klein-4 group $\left\{\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}\right\}$, which has 3 elements of order 2.

Note $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$
$\Rightarrow (\mathbb{Z}/8\mathbb{Z})^* \simeq$ klein 4-group.

In particular $(\mathbb{Z}/n\mathbb{Z})^*$ is not always cyclic though $\mathbb{Z}/n\mathbb{Z}$ is.

Euler (very difficult Thm) When n is a prime p, $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$.

This is very hard because there is no natural way to find a generator like there is for $\mathbb{Z}/n\mathbb{Z}$. We'll prove this later when we get to fields.

If $\gcd(a,n)=1$, there is an efficient algorithm to determine $a^{-1} \pmod n$.

$n=p=389$ $\quad a \equiv 37 \pmod{389}$ Use the Euclidean algorithm:

on 389 and 37: $389 = 10\cdot 37 + 19$

on 37 and 19: $37 = 1\cdot 19 + 18$

on 19 and 18: $19 = 1\cdot 18 + 1$

Working backwards this says $1 = 19 - 18$

$= 19 - (37 - 1\cdot 19) = 2\cdot 19 - 37$

$= 2(389 - 10\cdot 37) - 37$

$= 2\cdot 389 - 21\cdot 37$

So $(-21)\cdot 37 \equiv 1 \pmod{389} \implies a^{-1} \equiv -21 \equiv 368 \pmod{389}$.

Check $37\times(-21) = -777 = 1 + 2\cdot 389$ ✓

Gauss Can we solve $x^2 \equiv a \pmod n$? $\quad x^2 \equiv -1 \pmod n$?