Last time: Every field is (also) an integral domain.

Examples: Zero divisors in \( \mathbb{Z}_n, n > 1 \)

- \( a \in \mathbb{Z}_n \) is a zero divisor \( \Leftrightarrow \) \( a \neq 0 \) and \( \gcd(\text{a,n}) 
eq 1 \).

Proof: Let \( a \in \mathbb{Z}_n \). Assume \( a \neq 0 \).

If \( \gcd(\text{a,n}) = 1 \) then it's a unit, so it's not a zero divisor.

If \( \gcd(\text{a,n}) \neq 1 \) then let \( b = \frac{\text{n}}{\gcd(\text{a,n})} \). Then \( b \in \mathbb{Z}_n \) and \( b \neq 0 \), hence \( ab \) is a multiple of \( n \), because

\[
\frac{ab}{n} = \frac{a(n/\gcd(\text{a,n}))}{n} = \frac{a}{\gcd(\text{a,n})} \in \mathbb{Z}
\]

\[ \therefore \text{Elements of } \mathbb{Z}_n \ (n > 1) \text{ are either 0, zero divisors, or units.} \]

**Thm:** In a finite ring \( R \) with \( 1 \neq 0 \), every element is either a unit, a zero divisor, or \( 0 \).

Proof: \( 0 \) is not a unit and not a zero divisor.

Let \( a \in R \) with \( a \neq 0 \).

The map \( f: R \to R \) given by \( f(x) = ax \) is either one-to-one or not one-to-one.

If it is one-to-one, then it's onto, so its image contains \( 1 \), \( \therefore f(b) = 1 \) for some \( b \in R \), so \( ab = 1 \) for some \( b \in R \).

This is a right multiplicative inverse of \( a \).

Conversely, if \( a \) has a right mult. inv. \( b \), then \( ab = 1 \), so \( y \in R \), \( f(by) = a(by) = (ab)y = y \cdot y = y \), so \( f \text{ is onto} \).

\[ \therefore f \text{ is one-to-one} \Leftrightarrow a \text{ has a right multiplicative inverse.} \]
If \( f \) is not 1-1, then \( \exists b \neq c \in \mathbb{R} \) such that \( b + c = a \) and \( f(b) = f(c) \). So \( ab = ac \), \( \therefore a(b-c) = 0 \). Since \( a \neq 0 \), \( a \) is a zero divisor. (We say that \( a \) is a left zero divisor.)

Conversely, if \( a \) is a left zero divisor, then \( ab = 0 \) for some \( b \neq 0 \), \( \therefore f(b) = ab = 0 = a0 = f(a0) \), \( \therefore f \) is not one-to-one. So \( f \) is not 1-1 if and only if \( a \) is a left zero divisor.

\[ \therefore a \text{ has a right inverse } \iff f \text{ is 1-1 } \iff a \text{ is not a left zero divisor.} \]

Similarly, using the map \( g : v \mapsto ax + b \), we have:

\[ a \text{ has a left inverse } \iff g \text{ is 1-1 } \iff a \text{ is not a right zero divisor.} \]

If \( a \) has a (two-sided) inverse, then it has both a left inverse and a right inverse.

Conversely, suppose \( a \) has a left inverse \( b \) and a right inverse \( c \).

Then \( b = c \) because
\[ a \text{ has a multiplicative inverse, so it is a unit.} \]

So \( a \) is a unit \( \iff \) it has both a left and a right inverse
\( \iff \) it is neither a left zero divisor nor a right zero divisor.
\( \iff \) it is not a zero divisor.

(Recall \( \mathbb{Z}/n\mathbb{Z} \).) \( \text{(n>1)} \)

**Thm:** Every finite integral domain is a field.

**Proof:** Let \( R \) be a finite integral domain. Then every nonzero element is a unit, because there are no zero divisors in \( R \).
\( \therefore R \) is a field.

Also, \( R \) is commutative and \( R \) has 1 to because there are part of the definition of integral domain, too.
Characteristic of a Ring

Def: Let \( R \) be a ring.

(a). For all \( n \in \mathbb{Z}^+ \) and all \( a \in R \), \( n \cdot a = a + a + \ldots + a \) \( (n \) times) \( \)
(a) for the additive group of \( R \).

(b). The characteristic of \( R \) is the smallest element of
the set \( \{ n \in \mathbb{Z}^+ : n \cdot a = 0 \ \forall a \in R \} \),
or \( 0 \) if this set is empty.

Note: If \( R \) has a unity element \( 1 \), then this set is equal to
\( \{ n \in \mathbb{Z}^+ : n \cdot 1 = 0 \} \).

Proof: "\( \forall \) \( n \in \mathbb{Z}^+ \) if \( n \cdot 1 = 0 \) then
\( n \cdot a = a + a + \ldots + a \) \( (n \) times) \[ = \left( \underbrace{1 + 1 + \ldots + 1}_{n \text{ times}} \right) a = n \cdot a = 0 \Rightarrow a = 0. \]

" \( \exists \)": If \( n \cdot 0 = 0 \ \forall a \in R \), then we can take \( a = 1 \)
to get \( n \cdot 1 = 0. \)

Examples: \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C} \) all have characteristic 0.
\( \mathbb{Z}_n \) has characteristic \( n. \)

Turning *\( \mathbb{Z}/n\mathbb{Z} \) into a ring:

Define a binary operation on \( \mathbb{Z}/n\mathbb{Z} \) by letting
\[ (a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = ab + n\mathbb{Z}. \]
This is well defined because if \( a + n\mathbb{Z} = a' + n\mathbb{Z} \) and \( b + n\mathbb{Z} = b' + n\mathbb{Z} \),
then \( a' = a + rn \) and \( b' = b + sn \) for some integers \( r \) and \( s \),
and \[ a' \cdot b' = (a + rn)(b + sn) = ab + (as + br + ms)n, \]
so
\[ a' \cdot b' + n\mathbb{Z} = ab + n\mathbb{Z}. \]
This multiplication is associative, because
\[ ((a + n\mathbb{Z})(b + n\mathbb{Z}))c + n\mathbb{Z} = ab + n\mathbb{Z} = a(b + n\mathbb{Z})(c + n\mathbb{Z}). \]
For distributivity:
\[ (a + n\mathbb{Z})(b + n\mathbb{Z} + c + n\mathbb{Z}) = a(b + c + n\mathbb{Z}) + n\mathbb{Z} + a(n\mathbb{Z} + c + n\mathbb{Z}). \]
\( \mathbb{Z}/n\mathbb{Z} \) is a ring, and the canonical map (from group theory) is a ring homomorphism.
As we did with quotient groups, we can use the bijection $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}_n$ to define a multiplication operation on $\mathbb{Z}_n$, so that $\mathbb{Z}_n$ becomes a ring isomorphic to $\mathbb{Z}/n\mathbb{Z}$, via the group isomorphism $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}_n$.

This is the same as the multiplication operation we defined earlier, because if $a, b \in \mathbb{Z}_n$ and $\psi : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}_n$ is the isomorphism, then $a = \psi(a + n\mathbb{Z})$ and $b = \psi(b + n\mathbb{Z})$.

And by our definition $a \cdot b = \psi(ab + n\mathbb{Z})$ in $\mathbb{Z}_n$.

So $ab \equiv ab \pmod{n}$.

In $\mathbb{Z}_n$ by the new def.

In $\mathbb{Z}$ by the old def.

Remember when you divide $ab$ by $n$.

It is in $\mathbb{Z}_n$ by the old def.

---

The midterm will cover up to here ---

Fermat's "little theorem" is a consequence of the following fact:

If $p$ is prime, then $\mathbb{Z}_p^*$ is a group.

Since $\mathbb{Z}_p$ is a field, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, so $\mathbb{Z}_p^*$ has order $p-1$.

$a^{p-1} \equiv 1 \pmod{p}$ for all $a \in \mathbb{Z}_p^*$.

Pull that back to $\mathbb{Z}$ by the ring homomorphism $\mathbb{Z} \rightarrow \mathbb{Z}_p$ (reduction mod $p$).