• Our goal in the next two lectures is to prove the following theorem.

\textbf{Thm} Any integer can be written (essentially uniquely) as a product of "irreducible" integers, where \( p \in \mathbb{Z} \) is irreducible if any factorization \( p = m \cdot n \) has either \( m \) or \( n \) a unit.

• Shockingly tricky to prove! I invite you to try, but don't be surprised if you get stuck.

• Let's use the theory of rings to help.

• We should investigate ideals in \( \mathbb{Z} \).

• For example, \( 2\mathbb{Z} = \langle 2 \rangle \subset \mathbb{Z} \) forms an ideal called "the even numbers." Indeed:
  \[ \rightarrow 0 \text{ is even} \]
  \[ \rightarrow \text{even} + \text{even} = \text{even} \]
  \[ \rightarrow \text{even} \cdot (\text{anything}) = \text{even} \]
• More generally, we've seen \( k\mathbb{Z} = (k) \subseteq \mathbb{Z} \)
  the multiples of \( k \) form ideals. These are called
  "principal ideals," since each has a single generator.

• What about something like \( 30\mathbb{Z} + 8\mathbb{Z} = (30,8)\mathbb{Z} \)
  numbers of the form \( 30a + 8b \) \( a,b \in \mathbb{Z} \) ?

• Hmm... maybe these are the even numbers again.

\[ \text{Define} \quad \textbf{A PID} \quad \text{is a domain in which} \]
\[ \text{every ideal is principal.} \]

\[ \text{Conjecture} \quad \mathbb{Z} \quad \text{is a PID.} \]

• What about a crazy ideal like
  \( (96, 966, 9666, 96666, \ldots) \)

Could we somehow rewrite this ideal using
  a single generator?

Maybe the conjecture is a little optimistic.
Before we tackle the conjecture, let's solve an easier problem.

**Calculation**

\[ 3 \cdot 36 + 30 = 138 \]

**Consequence**

\[(138, 36) = (36, 30) \]

\[ \leq : \quad 138 = 3 \cdot 36 + 1 \cdot 30 \]
\[ 36 = 1 \cdot 36 + 0 \cdot 30 \]

\[ \geq : \quad 36 = 0 \cdot 138 + 1 \cdot 36 \]
\[ 30 = 1 \cdot 138 + (-3) \cdot 36 \]

- The calculation allowed us to simplify the ideal \((138, 36) \subseteq \mathbb{Z}\) a little bit.

- How do we come up with an equation

\[
\square \cdot 36 + \square = 138
\]

\(\uparrow\) don't care \quad \text{Want as small as possible}
\(\uparrow\) so the answer is simpler.
**Integer Division Theorem (for the number 36)**

Every number in \( \mathbb{Z} \) is of the form \( 36q + r \) where \( q \in \mathbb{Z} \) and \( r \in \{0, 1, 2, \ldots, 35\} \).

**Proof (Pf)**

By induction, \( 0 = 36 \cdot 0 + 0 \).

Assume the result for \( n \in \mathbb{N} \), \( n = 36q + r \).

So \( n + 1 = 36q + r + 1 \).

If \( r + 1 \in \{0, 1, \ldots, 35\} \), we're done.

Otherwise, \( r = 35 \).

\[
\begin{align*}
n + 1 &= 36q + 35 + 1 \\
       &= 36q + 36 \\
       &= 36(q + 1) + 0.
\end{align*}
\]

This establishes the claim for \( n \in \mathbb{N} \). But suppose \( n < 0 \), then \( (35) \cdot n > 0 \) and so \( (35) \cdot n = 36q + r \).

\[
36n + (35) \cdot n = 36n + 36q + r \\
\]

has the required form.
Now we're really in business!

\[(138, 36) = (36, 30) = (30, 6) = (6, 0) = (6)\].

Iterating the integer division theorem gives

"Euclid's algorithm."

How do we know the algorithm always ends

\[\ldots = (k, 0) = (k)\]

for some \(k\)? The remainders keep getting smaller.

**Defn** A domain \(R\) is a **Euclidean Domain**

if there exists a function

\[|\cdot| : R \rightarrow \mathbb{N}\]

\[\nu \mapsto |\nu|\]

so that \(\forall a, b \in R, b \neq 0, \exists q, r \in R\)

with \(a = bq + r\)

and either \(r = 0\) or \(|r| < |b|\).

*Thm* Euclid's algorithm terminates in a Euclidean domain

*Cor* Any ideal \((x, y) \subseteq R\) in a Euclidean domain

is principal (in spite of the way we wrote it).

Of course, \(\mathbb{Z}\) is a Euclidean Domain \(|\cdot|\) is abs. value.
⑤ Maybe we should try to generalize Euclid's algorithm to ideals of the form \((x, y, z)\) and so on to all finitely generated ideals, and then develop some sort of infinite version of the algorithm.

In fact, NO! We have the following incredibly slick thin and proof:

**Theorem:** Any Euclidean Domain is a PID.

**Proof:** Let \(I \subseteq R\) be an ideal in a Euclidean Domain. Choose \(k \in I\) of minimal norm, i.e.,
\[
|k| \leq |i| \quad \text{for any } i \in I - \{0\}.
\]
Given any \(a \in I\), \(3q, r\) so
\[
a = k \cdot q + r
\]
and either \(r = 0\) or \(|r| < |k|\).

By minimality, \(r = 0\) and any \(a = q \cdot k\) is a multiple of \(k\).