Let’s recall the definitions of prime and irreducible integers:

Definition. 1) \( n \in \mathbb{Z}^* \) is called irreducible if
\[
\forall a, b \in \mathbb{Z}, \quad n = ab \implies (n = |a| \text{ or } n = |b|).
\]

2) \( p \in \mathbb{Z}^* \) is called prime if
\[
\forall a, b \in \mathbb{Z}, \quad p \mid ab \implies (p \mid a \text{ or } p \mid b).
\]

Recall that \( n \in \mathbb{Z}^* \) is irreducible if and only if the only positive divisors of \( n \) are 1 and \( n \).

Theorem. \( \forall n \in \mathbb{Z}^* \), \( n \) is irreducible \( \iff \) \( n \) is prime.

An alternative way to formulate the above theorem is

Suppose \( n \in \mathbb{Z}^* \). \( n \) has only two positive divisors
if and only if the following holds \( n \mid ab \implies n \mid a \text{ or } n \mid b \).

(\( \implies \)) side of the above statement is called Euclid’s lemma.

Proof of Theorem. (\( \implies \)) We assume \( n \) is irreducible, and we have to prove \( n \mid ab \implies (n \mid a \vee n \mid b) \). It is enough to prove
\[
(n \mid ab \land n \nmid a) \implies n \nmid b.
\]
\[ \gcd(a,n) \mid a \implies \gcd(a,n) \neq n \implies \gcd(a,n) = 1. \]
\[ n \nmid a \quad \text{the only positive divisors of } n \quad \text{are 1 and } n \]
\[ n \mid ab \implies n \mid b \] by Corollary 2.
\[ \gcd(n,a)=1 \]
\[ \iff n=ab. \text{ Since } n \neq 0, a \neq 0 \text{ and } b \neq 0; \text{ and } n \mid ab. \]
Since \( n \) is prime, \( n \mid a \) or \( n \mid b \).

**Case 1.** \( n \mid a \).

In this case, as \( a \neq 0 \), we have \( n \leq |a| \). So \( |a| |b| \leq |a| \).
Thus \( |b| \leq 1 \). Hence \( |b| = 1 \), which implies \( n = |a| \).

**Case 2.** \( n \mid b \).

By a similar argument, as in **Case 1**, we get \( n = |a| \).

This theorem is the key result in proving any integer \( > 1 \) can be written as a product of primes in a unique way. You will see this either in your algebra series or in your number theory series. We say \( \mathbb{Z} \) is a unique factorization domain (UFD).
We’d like to solve congruence equations.

**Q** Find all the solutions of $ax \equiv b \pmod{n}$. Does it have a solution?

**Ex.** For $n=2$ and $b=1$; there are two cases:

- If $a \equiv 0$, then, for any $x \in \mathbb{Z}$, $ax \equiv 0 \not\equiv 1$. So $ax \equiv 1$ has no solution.

- If $a \equiv 1$, then any odd $x$ is a solution of $x^2 \equiv 1$.

**Ex.** For $n=3$ and $b=1$; there are three cases:

- If $a \equiv 0$, $1$, or $2$.

As above $a^3 \equiv 0$ has no solution, and any integer of the form $3k+1$ is a solution of $x^3 \equiv 1$.

How about $a \equiv 2$? In rational numbers we write:

$$2x = 1 \Rightarrow \left(\frac{1}{2}\right)2x = \frac{1}{2} \Rightarrow x = \frac{1}{2}.$$

But here we are looking for integers $x$ such that $2x \equiv 1$. 

-
As in the rational case we look for an "inverse" of $2 \mod 3$.

Modulo 3 any number is congruent to 0, 1, or 2. So we can look for an inverse among these numbers:

\[
\begin{array}{c|ccc}
\times & 0 & 1 & 2 \\
\hline
0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 \\
2 & 0 & 2 & 1 \\
\end{array}
\]

Table of multiplication mod 3.

So 2 is an inverse of 2 mod 3. Hence

\[
2 \cdot 3 \equiv 1 \implies (2) (2x) \equiv (2)(1)
\]

\[
\implies x \equiv 2.
\]

So $x$ is a solution if and only if $x$ is of the form $3k+2$.

Ex. For $n=4, b=1$; there are four cases: $a \equiv 0, 1, 2, 3$. As before we can handle the cases of $a \equiv 0$ and 1.

Does $2x \equiv 1$ have a solution? (Since $2x-1$ is odd, $4+2x-1$; and so it does NOT have a solution.)

Next we will prove two lemmas that give alternative arguments...
for this case.

**Lemma.** For any $n \in \mathbb{Z}^+$, $a \equiv b \mod n \Rightarrow \gcd(a, n) = \gcd(b, n)$.

**Proof.** Let $d_1 = \gcd(a, n)$ and $d_2 = \gcd(b, n)$. To show $d_1 = d_2$, it is enough to show $d_1 | d_2$ and $d_2 | d_1$ (notice that $d_i \geq 1$).

By symmetry, it is enough to show $d_1 | d_2$.

$a \equiv b \mod n \Rightarrow \exists k \in \mathbb{Z}, b = nk + a$.

$d_1 | n \Rightarrow d_1 | nk + a$. So $d_1 | b$ and $d_1 | n$.

$d_1 | b \Rightarrow d_1 | \gcd(b, n) \Rightarrow d_1 | d_2$.

In the next lecture, we will use this lemma to prove Euclid's algorithm for finding $\gcd$ of two integers.

**Lemma.** If $ax \equiv b \mod n$ has a solution, then $\gcd(a, n) | b$.

(We have already proved this lemma, when we discussed
Lecture 28: Linear equations in congruence arithmetic

linear Diophantine equations.

Proof of lemma. For some integer $x$, we have $ax \equiv b \pmod{n}$.

So, by the previous lemma, $\gcd(ax, n) = \gcd(b, n)$.

Let $d = \gcd(a, n)$. Then $d \mid a \iff d \mid ax \iff d \mid \gcd(ax, n)$.

Hence $d \mid \gcd(b, n)$. On the other hand $\gcd(b, n) \mid b$.

Therefore $d \mid b$, which means $\gcd(a, n) \mid b$.

In the next lecture we will prove the converse.