**Definition:** Let $p$ be an integer such that $p \neq 0, \pm 1$, then $p$ is **prime** means:

Given $b, c \in \mathbb{Z}$, if $p \mid bc$ then $p \mid b$ or $p \mid c$

**Definition:** Let $p$ be an integer such that $p \neq 0, \pm 1$, then $p$ is **irreducible** means the only divisors of $p$ are $\pm 1$ and $\pm p$

**Theorem 21:** An integer $p$ be an integer such that $p \neq 0, \pm 1$ is prime if and only of it is irreducible.

**Part 1: if $p$ is prime, then it is irreducible**

**Proof:**

Let $p$ be prime.

Suppose that $a \mid p$. for some $a \in \mathbb{Z}$

Then $p = ab$ for some integer $b$.

So $p \mid ab$

by definition of prime, $p \mid a$ or $p \mid b$

| | |
|---|---|
| case 1: $p \mid a$<br>Then $p \mid a$ and $a \mid p$ so $a = \pm p$ | case 2: $p \mid b$<br>But because $p = ab$ we also know $b \mid p$<br>Because $p \mid b$ and $b \mid p$, we know $b = \pm p$<br>And $p = a(\pm p)$ so $a = \pm 1$ |

Thus if $a$ is a divisor of $p$ then $a = \pm p$ or $a = \pm 1$ so $p$ is irreducible.

---

**Part 2: if $p$ is irreducible, then it is prime**

**Proof:**

Let $p$ be irreducible, and let $a, b \in \mathbb{Z}$

Suppose $p \mid ab$

Further suppose that $p \nmid a$

Then let $d = \gcd(a, p)$

So $d \mid a$, $d \mid p$ and $d = au + pv$ for some $u, v \in \mathbb{Z}$

Because $p$ is irreducible, and $d \mid p$, then $d = 1$ or $d = \pm p$ (note that the gcd is always positive, but $p$ does not have to be positive).

| | |
|---|---|
| case 1: $d = 1$<br>Then $1 = au + pv$<br>So $b = abu + pbv$<br>Recall $p \mid ab$, so $ab = pk$ for some $k \in \mathbb{Z}$<br>Substituting in, we have:<br>$b = pku + pbv$<br>so $b = p(ku + bv)$ and thus<br>$p \mid b$ | case 2: $d = (\pm 1)p$<br>and $d \mid a$ so $a = di$ for some $i \in \mathbb{Z}$<br>so $a = (\pm 1)p \cdot i = p(\pm i)$<br>Thus $p \mid a$ |

Therefore, if $p \mid ab$ then $p \mid b$ or $p \mid a$

so $p$ is prime.