Rmk: Recall that $x \in R$ is called irreducible if $x$ is not a unit, and

$$x = u \cdot v \implies u \text{ or } v \text{ is a unit in } R.$$ 

$x$ is called prime if $(x)$ is a prime ideal—i.e.,

$$x = u \cdot v \implies u \text{ or } v \text{ is a multiple of } x.$$ 

In a domain, every prime is irreducible. What about converse?

Let $R$ be a Noetherian domain. Then TFAE:

1. Every irreducible is prime.
2. $R$ is a UFD.

It's an open problem in H.W to show that $R$ UFD $\implies \mathbb{Z}[x]$ UFD. This is why looking for primes in $\mathbb{Z}[x]$ is the same as looking for irreducibles in $\mathbb{Z}[x].$

Rmk: There's an obvious obstruction to $f(x) \in \mathbb{Z}[x]$ being irreducible—$\gcd(\text{coefficients of } f) \geq 2$. For then

$$f = \gcd(\text{coefficients of } f) \cdot f_0$$

where $\gcd$ is not a unit. This is also an obstruction to testing irreducibility of $f(x) \in \mathbb{Z}[x]$ by passing to $\mathbb{Q}(x)$—obviously, $\gcd$ is a unit in $\mathbb{Q}(x)$. The Gauss lemma says $\gcd$ is only obstruction.
Then (Gauss Lemma)

let \( g, h \in \mathbb{Z}[x] \), monic. If
\[
g, h \in \mathbb{Z}[x]
\]
then
\[
gh \in \mathbb{Z}[x]
\]

More generally, if \( R \) is a UFD and \( K = \text{Quot}(R) \),
then any factorization of \( f \in \mathbb{Z}[x] \) by \( g, h \in \mathbb{K}[x] \)
induces a factorization of \( f \) in \( \mathbb{K}[x] \).

**Gauss Lemma** If \( f \in \mathbb{Z}[x] \) is irreducible, then either
- \( f \) is a prime integer (constant poly, prime), or
- \( \gcd(\text{coeffs of } f) = 1 \), and \( f \in \mathbb{Q}[x] \) is irreducible.

Let \( R \) be a UFD — then "gcd" has a meaning. Given \( f \in \mathbb{K}[x] \), let \( c(f) \in K \) be the least sat
\[
f(x) = c(f) \cdot f_0(x)
\]
c is the "content" of \( f \).

where \( f_0(x) \in \mathbb{K}[x] \) is a polynomial w/ \( \gcd(\text{coeffs of } f_0) \) a unit.
\( c(f) \) is well-defined up to units in \( R \) — if \( R = \mathbb{Z} \), one can take \( c(f) \)
to be \( \left( \text{denominator of coeffs of } f \right)^{-1} \).

Note \( c(f) \in R \iff f \in \mathbb{R}[x] \).
Now, if \( g = c(g)g_0 \) \( h = c(h)h_0 \), we have

\[ gh = (c(g)c(h))g_0 h_0. \]

Thus \( gh \in \mathbb{R}[x] \iff c(g)c(h) \in \mathbb{R} \). We conclude that if \( f(x) = gh \), then

\[ f(x) = (c(g)c(h))g_0 h_0 \]

is a factorization of \( f \) in \( \mathbb{R}[x] \).

When \( g, h \) are monic, the leading coefficient of \( f = gh \) is equal to \( c(g)c(h) \). Moreover, if \( g \) monic, \( c(g) \) is a function \( \mathbb{Q} \to \mathbb{Q} \). Hence \( gh \in \mathbb{Z}[x] \implies gh \in \mathbb{Z}[x] \) because \( c(g)c(h) = \text{something} \). \( \Box \)

If \( f \) \text{ is an integer, obviously irreducible.} 
\text{If } \gcd(\text{coeffs}) \neq 1, \text{ obviously reducible.}
\text{If } \gcd(\text{coeffs}) = 1 \text{ and } f \in \mathbb{Z}[x] \text{ reducible, have}

\[ f = gh = c(g)h_0 g_0 h_0. \]

\( c(g)h_0 \) is an integer — divide all \( \text{coeffs} \) of 1, so \( c(g)h_0 \) \( = 1 \). This gives factorization of \( f \). \( \Box \)
Studying curves over \( \mathbb{Z} \): When is \( f \in \mathbb{Z}[x] \) irreducible? Some tools:

Let \( f(x) = a_n x^n + \cdots + a_0 \). Suppose \( p \mid a_n \) and that \( f \) is reducible in \( \mathbb{Z}[x] \). Then \( f \) is reducible in \( \mathbb{F}_p[x] \).

**Remark:** \( \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \).

**Proposition:** \( f \) reducible in \( \mathbb{Z}[x] \) if and only if \( f = gh \), where \( g, h \in \mathbb{Z}[x] \) and \( \deg(g) \geq 1, \deg(h) \geq 1 \).

Then \( f = gh \) in \( \mathbb{F}_p[x] \), since \( \mathbb{Z}[x] \to \mathbb{F}_p[x] \), \( \mathbb{Z}[x^2] \to \mathbb{F}_p[x^2] \) is a ring homomorphism.

If \( g(x) = b_n x^n + \cdots + b_0 \), \( h(x) = c_n x^n + \cdots + c_0 \), the hypothesis \( p \mid a_n \Rightarrow p \mid b_n, p \mid c_0 \) implies \( \deg(g) = \deg(h) \).

Note that if \( f = gh \) over \( \mathbb{Q} \), we can assume \( g, h \in \mathbb{Z}[x] \), because

\[
f = (c_1 g)(c_2 h) g_0 h_0.
\]

So the method of proof above shows:
Can let \( f \in \mathbb{Z}[x] \) be leading coefficient of \( f \). If \( \exists \) prime \( p \) s.t.

\[
p \nmid a_n
\]

\[
f \text{ is irreducible mod } p
\]

then \( f \) is irreducible over \( \mathbb{Q} \).

For this reason, it's good to have an arsenal of irreducible polynomials mod \( p \). The sieve method (of Eratosthenes) is an efficient way to list them.

**Ex.** If \( f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \) and each \( a_i \) is odd, \( f \) is irreducible. You can actually see this easily: if \( x \) is even, \( f(x) \) is odd. If \( x \) is odd, so is \( f(x) \). Equivalently, reduce mod \( p = 2 \), and observe that \( x^2 + x + 1 \) has no roots mod 2.

**Remark:** A lot of lectures skip checks of irreducibility at \( \deg f \leq 3 \) polynomials — since if \( \deg f \leq 3 \) and \( f \) has no roots, \( f \) is irreducible. Of course, if \( \deg f > 4 \), even if \( f \) has no roots, \( f \) may still be reducible. (Ex: \( f = (\text{quadratic}) \times (\text{quadratic}) \).)
Here's another good (often used) way to conclude whether a polynomial is irreducible. It's a very special case, when \( f(x) \) equals \( a_n x^n \mod p \), (with special constant term in \( \mathbb{Z} \)):

**Rabin's Irreducibility Criterion**

Let

\[ f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x] \]

and suppose \( p \) prime \( p \) s.t.

\[ \cdot \quad f(x) = a_n x^n \mod p, \quad a_n \neq 0 \]

\[ \cdot \quad p^2 \nmid a_0. \]

Then \( f \) is irreducible over \( \mathbb{Z} \).

**Note:** This differs from other techniques, which need an arsenal of irreducible polynomials mod \( p \). On the other hand, very few satisfy these criteria — how often are all the lesser coefficients multiples of \( p \)? Not often.
Example let \( \Phi_p(x) = x^{p-1} - \cdots - x + 1 \) be the \( p \)-th cyclotomic polynomial. The reason \( \Phi_p(x) \) is important:

\[
(x-1) \Phi_p(x) = x^p - 1
\]

so (along with \( x = 1 \)) the roots of \( \Phi_p(x) \) are \( p \)-th roots of unity.

Consider the translation automorphism \( x \mapsto y+1 \). Then

\[
(x-1) \Phi_p(x) = y \Phi_p(y+1)
\]

\[
= (y+1)^p - 1
\]

\[
= y^p + \sum_{k=1}^{p-1} \binom{p}{k} y^k + 1 - 1
\]

\[
= y \left( y^{p-1} + \sum_{k=2}^{p-2} \binom{p}{k} y^{k-1} + \binom{p}{p-1} \right)
\]

Here \( \Phi_p(y+1) = y^{p-1} + \sum_{k=2}^{p-2} \binom{p}{k} y^{k-1} + \frac{\binom{p}{p-1}}{y} \) is not divisible by \( p \).

By Eisenstein, \( \Phi_p(y+1) \) is irreducible over \( \mathbb{Q} \). Since \( \Phi_p(y+1) \) is monic, it is irreducible over \( \mathbb{Z} \) (since gcd(coefs) ≠ ±1).

Since \( x \mapsto y+1 \) is an automorphism of \( \mathbb{Z}[x] \), \( \Phi_p(x) \) is irreducible over \( \mathbb{Z} \).