Theorem 17.2: Over $\mathbb{Q}$ implies over $\mathbb{Z}$.
Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

(1) Show by counterexample that the converse of Theorem 17.2 is false. Refer carefully to the definition of reducibility (what are the units of $\mathbb{Z}$)?

Corollary: Irreducibility of pth Cyclotomic Polynomial.
For any prime p, the pth cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$.

(2) Why does the corollary fail if p is a positive even number? (It also fails for $p = 9$ since $1 + x + x^2$ is a factor. Can you prove it fails for an odd composite p?)

Theorem 17.5: $\langle p(x) \rangle$ is Maximal iff $p(x)$ is Irreducible.
Let F be a field and let $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $F[x]$ iff $p(x)$ is irreducible over F.

Corollary 1: $F[x]/\langle p(x) \rangle$ is a Field.
Let F be a field and $p(x)$ an irreducible polynomial over F. Then $F[x]/\langle p(x) \rangle$ is a field.

Corollary 2: $p(x)|a(x)b(x)$ Implies $p(x)|a(x)$ or $p(x)|b(x)$.
Let F be a field and let $p(x)$, $a(x)$, $b(x) \in F[x]$. If $p(x)$ is irreducible over F and $p(x)|a(x)b(x)$, then $p(x)|a(x)$ or $p(x)|b(x)$.

Dynamic Programming Classification of Irreducible Polynomials in $\mathbb{Z}_p$.
Given a prime p, the polynomials in $\mathbb{Z}_p$ can be classified as reducible or irreducible by exhaustively considering all polynomials of degree n, where n successively equals 0, 1, 2, etc.

Initialization. Fix p prime and set $n = 1$. All degree 1 polynomials are irreducible.
1. Replace $n \leftarrow n + 1$.
2. For all i from 1 to $n - 1$, multiply all polynomials of degree i by all polynomials of degree $n - i$.
3. Label the results of step 2 reducible, and the rest of the degree n polynomials irreducible.
4. Go to step 1.

(3) Use the dynamic programming method to find all irreducible degree 3 polynomials in $\mathbb{Z}_2$.

(4)(a) Show that in $\mathbb{Z}_2$, $x^4 + \langle x^3 + x^2 + 1 \rangle = x^2 + x + 1 + \langle x^3 + x^2 + 1 \rangle$.
(b) Construct the multiplication table for the field $\mathbb{Z}_2[x]/\langle x^3 + x^2 + 1 \rangle$.

Unique Factorization in $\mathbb{Z}[x]$.
Every polynomial in $\mathbb{Z}[x]$ that is not the zero polynomial or a unit in $\mathbb{Z}[x]$ can be written in the form $b_1 b_2 \cdots b_s p_1(x) p_2(x) \cdots p_m(x)$, where the b_i's are irreducible polynomials of degree 0, and the $p_i(x)$'s are irreducible polynomials of positive degree. Furthermore, if

$$b_1 b_2 \cdots b_s p_1(x) p_2(x) \cdots p_m(x) = c_1 c_2 \cdots c_t q_1(x) q_2(x) \cdots q_m n(x),$$

where the b's and c's are irreducible polynomials of degree 0, and the $p(x)$'s and $q(x)$'s are irreducible polynomials of positive degree, then $s = t$, $m = n$, and, after renumbering the c's and $q(x)$'s, we have $b_i = \pm c_i$ for $i = 1, \ldots, s$; and $p_i(x) = \pm q_i(x)$ for $i = 1, \ldots, m$.

(5) (Rational Root Theorem) Let $f(x) = a_n x^n + \cdots + a_1 x^1 + a_0 \in \mathbb{Z}[x]$, and $a_n \neq 0$. Let r, s be relatively prime integers with $f(r/s) = 0$.
(a) Simplify the form of $f(r/s)s^n$.
(b) Inspect the result of (a) to prove that $r | a_0$ and $s | a_n$.
(c) Let $f(x) = 4x^3 + 8x^2 + x - 3$. Given that $f(x)$ factors over $\mathbb{Q}$, what is the set of possible roots according to (b)?
(d) Give the factorization of $f(x)$; try to ignore the quadratic formula and reverse foil.