1. 18AE3 Show the converse of the lemma: if \( f(x) \) and \( g(x) \) are in \( \mathbb{Z}[x] \) and \( f(x)g(x) \) is primitive, then \( f(x) \) and \( g(x) \) are both primitive.

Let \( f(x) = a_nx^n + \cdots + a_0 \) and \( g(x) = b_mx^m + \cdots + b_0 \). If one of these polynomials, say \( f(x) \) fails to be primitive, then there exists a prime \( p \) such that \( p \mid a_i \) for \( i = 0, \ldots, n \). Thus \( \Phi_p(f(x)) = 0 \). This implies of course that \( \Phi_p(f(x)g(x)) = \Phi_p(f(x)) \cdot \Phi_p(g(x)) = 0 \cdot \Phi_p(g(x)) = 0 \), because \( \Phi_p \) is a homomorphism. Thus \( p \) divides every coefficient of \( f(x)g(x) \) and so \( fg \) must not be primitive. This is a contradiction. We conclude that both \( f \) and \( g \) are in fact primitive.

2. 18AE7 If \( f \) and \( g \) are monic polynomials in \( \mathbb{Z}[x] \), does their (monic) greatest common divisor in \( \mathbb{Q}[x] \) necessarily have coefficients in \( \mathbb{Z} \)?

The answer to this question is yes. The proof of this will rely heavily on the fact that there if two monic polynomials are associates, then they are equal. Suppose for instance that \( \lambda(x) \) and \( \gamma(x) \) are two monic associates in \( \mathbb{Q}[x] \), so that \( \lambda(x) = q\gamma(x) \) for some \( q \in \mathbb{Q} \). We write \( \lambda(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \), and \( \gamma(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0 \). Then \( x^n + a_{n-1}x^{n-1} + \cdots + a_0 = qx^n + qb_{n-1}x^{n-1} + \cdots + qb_0 \) whence it is clear that \( q = 1 \) and \( \lambda(x) = \gamma(x) \).

So suppose that \( h(x) = (f(x), g(x)) \) is the monic greatest common divisor of \( f(x) \) and \( g(x) \). The worry is that \( h(x) \) may have coefficients in \( \mathbb{Q} \), so that \( h(x) \in \mathbb{Q}[x] - \mathbb{Z}[x] \) (this is a concern, because using Euclid’s algorithm to find \( h \) must be done over a field ... we can use \( \mathbb{Q} \), but that may result in coefficients in \( \mathbb{Q} \)). Because \( h \) is the GCD, there exists a polynomial \( r(x) \in \mathbb{Q}[x] \) such that \( rh = f \). By Gauss’s lemma, we can also find polynomials \( r'(x) \) and \( h'(x) \) in \( \mathbb{Z}[x] \), associates of \( r(x) \) and \( h(x) \) respectively, such that \( r'(x)h'(x) = f(x) \). Write \( r'(x) = a_nx^n + \cdots + a_0 \), and \( h'(x) = b_mx^m + \cdots + b_0 \). Because \( rh = f \) we know that \( a_nb_m = 1 \) (recall that \( f \) is monic), and because \( a_n, b_m \in \mathbb{Z} \), we conclude that \( a_n = 1 \) or \( a_n = -1 \). If \( a_n = 1 \) then \( h' \) is monic. As above this implies that \( h' \) and its monic associate \( h \) are equal, that is, \( h = h' \in \mathbb{Z}[x] \) as required.

If on the other hand \( a_n = -1 \), then the polynomial \( h''(x) = -h'(x) \) is a monic polynomial in \( \mathbb{Z}[x] \). Because \( h \) and \( h'' \) are monic associates, we conclude that \( h = h'' \in \mathbb{Z}[x] \).

3. Prove that the Fundamental Theorem of Algebra is equivalent to the following theorem.

Theorem: Any \( f(z) \in \mathbb{C}[z] \), degree \( f > 0 \), is a product of linear polynomials in \( \mathbb{C}[z] \).

Proof:
In order to show that the two theorems are equivalent, we must show that assuming one, we may prove the other. Because we know that given \( f, g \in \mathbb{C}[z] \), \( \deg(fg) = \deg(f) + \deg(g) \), it is clear that a polynomial of degree \( n \) is the product of linears if and only if it is the product of \( n \) linears. Thus we will use the following statement of the Theorem:
Theorem: Any \( f(z) \in \mathbb{C}[z] \), degree \( f = n > 0 \), is a product of \( n \) linear polynomials in \( \mathbb{C}[z] \)

(a) First we assume the Fundamental Theorem of Algebra and prove the theorem.

We induct on the degree of \( f \). Let \( P(n) \) be the statement that a degree \( n \) polynomial \( f \) is a product of \( n \) linear polynomials in \( \mathbb{C}[z] \). \( P(1) \) is obviously true. So assume \( P(k) \) is true for some \( k \geq 1 \), and let \( f \) be an arbitrary degree \( k + 1 \) polynomial. By the Fundamental Theorem of Algebra, \( f(z) \in \mathbb{C}[z] \) has some root, say \( f(\alpha) = 0 \) for \( \alpha \in \mathbb{C} \). Then by the root theorem \( (z-\alpha) \mid f(z) \). Thus there exists \( g(z) \in \mathbb{C}[z] \) such that \( (z-\alpha)g(z) = f(z) \) where the degree of \( g \) is \( k \). By induction, \( g(z) \) is a product of \( k \) linear polynomials \( g(z) = (z-\alpha_1)(z-\alpha_2) \cdots (z-\alpha_k) \) for some \( \alpha_1, \ldots, \alpha_k \in \mathbb{C} \). This means of course that \( f(z) = (z-\alpha)(z-\alpha_1)(z-\alpha_2) \cdots (z-\alpha_k) \), that is, we have shown \( f \) is a product of \( k + 1 \) linear factors in \( \mathbb{C}[z] \). Therefore \( P(k + 1) \) must be true and we conclude by Induction (1) that \( P(n) \) must be true for all \( n \geq 1 \).

(b) Now we assume the theorem and prove the Fundamental Theorem of Algebra.

Let \( f(z) \) be a polynomial of degree \( n \geq 1 \) in \( \mathbb{C}[z] \). Then by the theorem, \( f(z) = (z-\alpha_1) \cdots (z-\alpha_n) \) for \( \alpha_1, \ldots, \alpha_n \in \mathbb{C} \). Thus \( f(\alpha_i) = 0 \) for all \( i = 1, \ldots, n \). Thus the Fundamental Theorem of Algebra is proved (we proved that \( f \) had a root in \( \mathbb{C} \)).