1. A polynomial \( f(x) \in \mathbb{Z}[x] \) is \textit{primitive} if the greatest common divisor of its coefficients is 1. Prove Gauss’s Lemma: If \( f(x), g(x) \in \mathbb{Z}[x] \) are primitive, then \( f(x)g(x) \) is primitive.

[Hint: Fill in all the details for the following idea: Write \( f(x) = \sum_{i=0}^{n} a_i x^{n-i} \) and \( g(x) = \sum_{j=0}^{m} b_j x^{m-j} \). Suppose \( p \) is a prime and \( i, j \) are the smallest indices satisfying \( p \nmid a_i \) and \( p \nmid b_j \). Consider the coefficient \( x^{i+j} \) in \( f(x)g(x) \).]

2. Recall that if \( K \) is a field containing \( \mathbb{Q} \), an element \( \alpha \in K \) is called an \textit{algebraic number} if and only if there exists \( g(x) \in \mathbb{Q}[x] \) such that \( g(\alpha) = 0 \). If \( \alpha \) is an algebraic number, we let \( \text{Irr}_\alpha(x; \mathbb{Q}) = \text{Irr}_\alpha(x) \) be the monic polynomial in \( \mathbb{Q}[x] \) of least degree having \( \alpha \) as a root. An algebraic number \( \alpha \) is called an \textit{algebraic integer} if there exists a monic polynomial in \( \mathbb{Z}[x] \) having \( \alpha \) as a root.

(a) Use Gauss’ Lemma to prove that if \( \alpha \) is an algebraic integer, then \( \text{Irr}_\alpha(x; \mathbb{Q}) \in \mathbb{Z}[x] \).

(b) Prove that an algebraic number \( \alpha \) is an algebraic integer if and only if \( \text{Irr}_\alpha(x) \in \mathbb{Z}[x] \).

3. (a) Suppose all roots in \( \mathbb{C} \) of a monic polynomial

\[
f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Q}[x]
\]

have absolute value 1. Show that \( |a_r| \leq \binom{n}{r} \) for \( 0 \leq r \leq n-1 \).

(b) Show that for a fixed positive integer \( n \), there are only finitely many algebraic integers of degree \( n \) whose minimal polynomial has all of its roots in \( \mathbb{C} \) on the unit circle. [Hint: think about Problem 2.]

(c) Show that if the minimal polynomial of an algebraic integer \( \alpha \) has all its roots on the unit circle, then \( \alpha^k = 1 \) for some integer \( k \). This is a famous theorem of Leopold Kronecker. [Hint: can the sequence of powers of \( \alpha \) be non-repeating?]

4. Let \( \alpha = \sqrt{5} + \sqrt{13} \). Show that \( \alpha \) is an algebraic integer. Show that \( 2|\alpha \) in the sense that \( \alpha/2 \) is also an algebraic integer. Show that \( 4 \nmid \alpha \).

5. Let \( \alpha \) be an algebraic number. Show that there exists an integer \( m \) such that \( m\alpha \) is an algebraic integer.

6. Suppose \( \alpha, \beta, \gamma \in K \) where \( K \) is an algebraic number field. Suppose \( \alpha, \beta \) are algebraic integers and \( \gamma \) satisfies \( x^2 + \alpha x + \beta = 0 \). Show that \( \gamma \) is an algebraic integer. Can you generalize this result?

For the due date, check the course web page; check the website periodically for hints, updates, additions, and or corrections.
7. Suppose \( f(x) = x^2 + mx + n \in \mathbb{Z}[x] \) is irreducible. Suppose \( K \) is a field of degree 2 over \( \mathbb{Q} \) and containing an element \( \alpha \) such that \( f(\alpha) = 0 \). (For instance \( K = \mathbb{Q}[x]/(f) \) and \( \alpha = x + (f) \) or \( K = \mathbb{Q}(\alpha) \) and \( \alpha \) is given by the quadratic formula, but no matter). Let \( \mathbb{Q}[\alpha] = \{g(\alpha) \mid g(x) \in \mathbb{Q}[x]\} \) be the set consisting of all \( \mathbb{Q} \)-polynomial expressions in \( \alpha \). Let \( \mathbb{Q}(\alpha) \) be the fraction field of \( \mathbb{Q}[\alpha] \), i.e. the smallest subfield of \( K \) that contains \( \mathbb{Q}[\alpha] \). Let \( d_f = m^2 - 4n \) be the discriminant of \( f \) and suppose \( d_f = dk^2 \) where \( d \) is square-free, meaning the only square that divides it is 1. Show that
   (i) \( \mathbb{Q}[\alpha] \) is a subring of \( K \);
   (ii) \( \mathbb{Q}[\alpha] = \mathbb{Q}(\alpha) \);
   (iii) \( \mathbb{Q}[\alpha] = \mathbb{Q}[\beta] \), where \( \beta = (2\alpha + m)/k \) satisfies \( \beta^2 = d \).

8. Staying with the situation of the preceding problem, let us assume \( \alpha = (-m + \sqrt{d_f})/2 \in \mathbb{C} \) so that \( \beta = \sqrt{d} \). Let \( \mathcal{O}_K \subseteq \mathbb{Q}(\alpha) \) be the set of algebraic integers in \( K = \mathbb{Q}(\alpha) \).
   (i) Suppose \( d \equiv 2, 3 \mod 4 \). Show that \( \mathcal{O}_K = [1, \sqrt{d}]_\mathbb{Z} \).
   **Notation:** Whenever \( \gamma_1, \ldots, \gamma_t \) are elements of a field \( F \) and \( R \) is a subring of \( F \), we let \( [\gamma_1, \ldots, \gamma_t]_R \) be the set of all \( \mathbb{R} \)-linear combinations \( \sum_{i=1}^t r_i \gamma_i \).
   (ii) if \( d \equiv 1 \mod 4 \), show that \( \mathcal{O}_K = [1, 1+\sqrt{d}]_\mathbb{Z} \). [Hint: don’t forget the useful criterion of problem 2].
   (iii) Show that in either case, \( \mathcal{O}_K = [1, \frac{D+\sqrt{D}}{2}]_\mathbb{Z} \), where \( D = d \) if \( d \equiv 1 \mod 4 \) and \( D = 4d \) if \( d \equiv 2, 3 \mod 4 \).

9. Let \( \omega = e^{2\pi i/3} \). What is the quickest way to show that \( \omega \) is an algebraic integer? Now determine \( \text{Irr}_\omega(x) \).

10. Prove or disprove: if \( \alpha \) is an algebraic number, with minimal polynomial \( \text{Irr}_\alpha(x) \), then \( \text{Irr}_\alpha(x) \) does not have repeated roots (in \( \mathbb{C} \)).

11. Let \( \alpha \) be an algebraic number of degree \( n \) over \( \mathbb{Q} \), i.e. \( \text{Irr}_\alpha(x; \mathbb{Q}) \) has degree \( n \). Suppose \( f, g \in \mathbb{Q}[x] \) are polynomials of degree strictly less than \( n \) such that \( f(\alpha) = g(\alpha) \). Show that \( f = g \).