Problem Set 3 (two pages)

Cyclotomic number fields
1) Let \( \mathbb{Q}_n = \mathbb{Q}[\mu_n] \) be the \( n^{th} \) cyclotomic number field. Prove the following assertions from the class:
   a) Set \( n_0 = \varphi(n) = [\mathbb{Q}_n : \mathbb{Q}] \), \( \pi = 1 - \zeta \) with \( \zeta \) primitive. Then \( 1, \ldots, \pi^{n_0-1} \) is a basis of \( \mathbb{Q}_n \) over \( \mathbb{Q} \).
   b) Prove or disprove: \( \pi = 1 - \zeta \) is a unit in \( \mathbb{Z}[\zeta] \) if and only if \( n \) is not a power of a prime number.
   c) Give the precise formula for the discriminant \( \Delta_{\mathbb{Q}_n} \) including the sign.
2) Let \( \chi_n : \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \to (\mathbb{Z}/n)^\times \) be the the cyclotomic character.
   a) Describe the decomposition/inertia/ramification groups of the primes in \( \mathbb{Z}[\mu_n] \mid \mathbb{Z} \).
   b) Give the relation between existence of primes in arithmetic progressions and decomposition of primes in cyclotomic number fields.

Quadratic residues
3) Let \( p \) be an odd prime number, \( \zeta \) a primitive \( p^{th} \) root of unity. Let \( S = \sum_{m=1}^{p-1} \left( \frac{n}{p} \right) \zeta^m \) be the Gauß sum attached to the Legendre symbol.
   a) Show that \( S^2 = (\frac{-1}{p})p \).
   b) In particular, if \( p' = (\frac{-1}{p})p \), then \( \sqrt{p'} \in \mathbb{Z}[\mu_p] \).
   c) Complete the proof of the Gauß Reciprocity Law for odd primes by using the decomposition of primes in cyclotomic extensions.
4) Prove the special cases “left to the reader” of the Gauß Reciprocity Law:
   \[ \left( \frac{-1}{p} \right) = (-1)^{(p-1)/2} \quad \text{and} \quad \left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8}. \]
   Hint. Compute in \( \mathbb{Z}[i] \): \( (1 + i)^2 = 2i \Rightarrow (1 + i)^{(p-1)} = i^{(p-1)/2} 2^{(p-1)/2} \). Now view everything \( \pmod{p} \), etc.
5) One defines the Jacobi Symbol as follows: Let \( m = p_0p_1 \ldots p_r \) and \( n = q_1 \ldots q_s \) be integers such that \( p_i, q_j \) are prime numbers, \( n \) being odd. Suppose that \( m \) and \( n \) are relatively prime. Define the Jacobi symbol by \( \left( \frac{m}{n} \right)' = \prod_{i,j} \left( \frac{p_i}{q_j} \right) \), where \( \left( \frac{p_i}{q_j} \right) \) is the usual Legendre symbol. Prove the following:
   a) If \( m_1 \equiv m_2 \pmod{n} \), then \( \left( \frac{m_1}{n} \right)' = \left( \frac{m_2}{n} \right)' \).
   b) \( \left( \frac{m_1}{n} \right)' \) is multiplicative in both variables \( m \) and \( n \).
   c) One has \( \left( \frac{1}{n} \right)' = (-1)^{(n-1)/2} \). Prove or disprove: \( \left( \frac{2}{n} \right)' = (-1)^{(n^2-1)/4} \).
   d) If \( m \) is odd too, then \( \left( \frac{m}{n} \right)' = \left( \frac{m}{n} \right)'(-1)^{(m-1)(n-1)/4} \).
   e) Prove or disprove: \( m \pmod{n} \) is a square in \( \mathbb{Z}/n \) iff \( \left( \frac{m}{n} \right)' = 1 \).
6) Using the properties of the Jacobi symbol try to estimate the number of multiplications needed for checking whether \( x \pmod{p} \) is a square in \( \mathbb{F}_p \). How does this compare with making a list of all the squares in \( \mathbb{F}_p \)?

Minkowski’s Method
7) Prove or disprove the following:
   a) Every non-trivial finitely generated subgroup \( \Gamma \subset \mathbb{Q} \subset \mathbb{R} \) is a lattice in \( (\mathbb{R},+) \).
   b) Same question for non-trivial finitely generated subgroups \( \Gamma \subset K \subset \mathbb{C} \), where \( K|\mathbb{Q} \) is an imaginary quadratic number field.
   c) Same question for non-trivial finitely generated subgroups \( \Gamma \subset K \subset \mathbb{C} \), where \( K|\mathbb{Q} \) is a real quadratic number field.

Due: Wed, Nov 21, 2007
8) Prove the following assertions made in the class:
   a) If \( \Gamma_1 \subseteq \Gamma_2 \subseteq \mathbb{R}^n \) are additive subgroups with \( \Gamma_2 / \Gamma_1 \) finite, then \( \Gamma_1 \) is a (complete) lattice if and only if \( \Gamma_2 \) is so.
   b) Compute the volumes of the convex symmetric bodies \( X_\bullet, X_M, X_0 \) as given in the class/notes.
   c) Show that for every positive real constant \( c > 0 \), there exist at most finitely many ideals \( \mathfrak{a} \subset \mathcal{O}_K \) such that \( \|\mathfrak{a}\| \leq c \).
      Give rough estimates for the number of such ideals.
   d) Prove the functoriality properties of the map content map \( || \) \, and show that \( ||f_{\mathcal{O}_K}|| = |N_{K/\mathbb{Q}}(f)| \).

9) Prove or disprove: The quadratic fields with discriminants \( -11, -8, -7, -4, -3, 5, 8, 13 \) are PID. Find the square free \( d \in \mathbb{Z} \) defining these quadratic fields.

10) Describe the ideal class group of the following number fields:
   a) \( K = \mathbb{Q}(\sqrt{d}) \), with \( d = 33, 37, 93 \).
   b) \( K = \mathbb{Q}(\alpha) \), with \( \alpha^3 = 2 \).