Comprehensive Exam, Summer 2003

for

MATH 780 & MATH 784

1. Let $p \equiv 1 \pmod 4$ be a prime number. Define $\mathcal{R}$ to be the set of integers in $\{1, 2, \ldots, p-1\}$ which are quadratic residues modulo p, and $\mathcal{N}$ to be the set of integers in $\{1, 2, \ldots, p-1\}$ which are quadratic nonresidues modulo p. (For example, if $p = 5$, then $\mathcal{R} = \{1, 4\}$, and $\mathcal{N} = \{2, 3\}$.) Prove that

$$\sum_{n \in \mathcal{R}} n = \sum_{n \in \mathcal{N}} n.$$

(In other words, show that the sum of the elements of the set $\mathcal{R}$ equals the sum of the elements of the set $\mathcal{N}$.)

2. Let $a \geq 2$ and $b \geq 2$ be relatively prime integers. Let $\mathcal{S}$ be the set of positive integers which can be represented in the form $ak + bl$ with k and l **nonnegative** integers. (For example, it is not difficult to show that if $a = 2$ and $b = 3$, then $\mathcal{S} = \{2, 3, 4, 5, \ldots\}$.) Prove that the largest positive integer which is not in $\mathcal{S}$ is $ab - a - b$. (Hint: If n is an integer, then at least one of the numbers $n, n-a, \ldots, n-(b-1)a$ is divisible by b.)

3. Let n be a positive integer.

(a) Find the order of 2 modulo $2^{2^n} + 1$.

(b) Let p be a prime divisor of $2^{2^n} + 1$. Prove that $p \equiv 1 \pmod{2^{n+1}}$.

(c) Let k be a positive integer. Using (b), prove that there exist infinitely many primes which are congruent to 1 modulo 2^{k+1}.

4. Let p be a prime number.

(a) Suppose that p is odd and is not of the form $8k + 5$ with k an integer. Prove that the congruence $a^4 \equiv 4 \pmod p$ has an integer solution.

(b) Suppose that p is of the form $8k + 5$ with k an integer. Prove that the congruence $a^4 \equiv -4 \pmod p$ has an integer solution.

(c) Prove that for any prime p the congruence $a^8 \equiv 16 \pmod p$ has an integer solution.

5. Let (x_n, y_n) denote the nth positive integral pair (x, y) satisfying $x^2 - 2y^2 = 1$ (ordered so that $x_1 < x_2 < \cdots$). Thus, for example, $(x_1, y_1) = (3, 2)$ and $(x_2, y_2) = (17, 12)$. Let p be a prime. Prove that

$$x_p \equiv x_1 \pmod p \quad \text{and} \quad y_p \equiv y_1 \pmod p \quad \Longleftrightarrow \quad p \equiv \pm 1 \pmod 8.$$

(Comment: This is meant to test your knowledge of both Math 780 and Math 784.)

6. Prove the following theorem from class, giving as many details as you can.

Theorem *Let α be an algebraic number with minimal polynomial $f(x) = x^n + \sum_{j=0}^{n-1} a_j x^j \in \mathbb{Q}[x]$. Every element of $\mathbb{Q}(\alpha)$ can be expressed uniquely in the form $g(\alpha)$ where $g(x) \in \mathbb{Q}[x]$ with $g(x) \equiv 0$ or $\deg g(x) \leq n - 1$.*

7. Let R be the ring of algebraic integers in $\mathbb{Q}(\sqrt{-47})$. Let I be the ideal in R generated by $(3+\sqrt{-47})/2$ and 2. Thus,

$$I = \left(\frac{3+\sqrt{-47}}{2}, 2\right).$$

   (a) Is I principal? (In other words, does there exist an $\alpha \in R$ such that $I = (\alpha)$?)

   (b) Let

$$J = \left(\frac{3-\sqrt{-47}}{2}, 2\right).$$

   The product of the ideals I and J is a principal ideal (β) for some $\beta \in R$. Find such a β.

   (c) Compute the norm of the ideal I (in the ring R).

8. The following concerns the Diophantine equation $x^2 + 13 = y^3$. The class number (the size of the class group) associated with the field $\mathbb{Q}(\sqrt{-13})$ is 2. In particular, the ring of integers R in $\mathbb{Q}(\sqrt{-13})$ is *not* a PID.

   (a) Suppose A is an ideal in R and A^3 is principal. Justify that A is necessarily a principal ideal in R. (Use that the class number is 2. You do not have to prove that the class number is 2.)

   (b) Suppose x_0 and y_0 are rational integers for which $x_0^2 + 13 = y_0^3$. Justify that $\gcd(y_0, 26) = 1$.

   (c) With the notation in part (b), justify that the ideals $\left(x_0 + \sqrt{-13}\right)$ and $\left(x_0 - \sqrt{-13}\right)$ are relatively prime.

   (d) Explain why there is a principal ideal $\left(a + b\sqrt{-13}\right)$ in R such that $\left(x_0 + \sqrt{-13}\right) = \left(a + b\sqrt{-13}\right)^3$.

   (e) Solve the Diophantine equation $x^2 + 13 = y^3$ (i.e., find with proof all integer pairs (x_0, y_0) such that $x_0^2 + 13 = y_0^3$.)