Comprehensive Exam: Math 780 & 784

1. Find the smallest three positive integers n for which $3^n \equiv 27 \pmod{10800}$.

2. Let k be a positive integer. Prove that there exists a positive integer n such that all the numbers $n^2+1, (n+1)^2+1, (n+2)^2+1, \cdots, (n+k)^2+1$ are composite.

3. An integer a is called cubic residue modulo a prime p if there is an integer b for which $a \equiv b^3 \pmod{p}$.
   (a) Prove that if $p \equiv 1 \pmod{3}$, then the number of incongruent cubic residues modulo p is $(p+2)/3$.
   (b) Prove that if $p \equiv 2 \pmod{3}$, then the number of incongruent cubic residues modulo p is p.
   (c) Suppose $p \equiv 2 \pmod{3}$ and A and B are integers with A not divisible by p. Let N_p be the number of distinct pairs of integers (x, y) such that $0 \leq x < p$, $0 \leq y < p$, and $y^2 \equiv Ax^3 + B \pmod{p}$. Prove that $N_p = p$. (Hint: What are the residues of $Ax^3 + B$ modulo p when x runs from 0 to $p-1$.)

4. (a) Let a be a positive integer. Prove that there exist infinitely many primes p such that $\left(\frac{a}{p}\right) = 1$.
   (b) Let a be a positive integer, and let b be a positive integer which is not a perfect square. Assume that $\gcd(a, b) = 1$. Prove that there exist infinitely many primes p such that $\left(\frac{a}{p}\right) = 1$ while $\left(\frac{b}{p}\right) = -1$.
   (c) Let a and b be as in (b). Prove that there exist infinitely many primes p such that p does not divide *each* number in the sequence $a-b, a^2-b, a^3-b, \ldots, a^n-b, \ldots$.

5. Let α be an algebraic number, and let R be the ring of algebraic integers in $\mathbb{Q}(\alpha)$. Decide whether each of the following is true or false and give an appropriate justification for your answer. Note that an answer of "true" indicates that you believe the statement holds for every ring R as above.
   (a) If β and γ are in R, then $\beta^2 - \beta\gamma^3 + 5 \in R$.
   (b) The ideal (2) is a prime ideal in R.
   (c) The greatest common divisor of the ideals (4) and (6) is the ideal (2).
   (d) If $\beta \in R$ with $\beta \neq 0$, then $N(\beta)/\beta \in R$.
   (e) If $\beta \in \mathbb{Q}(\alpha)$ with $\beta \neq 0$, then $N(\beta)/\beta \in R$.

6. The polynomial $f(x) = x^4 - x^3 + 1$ is irreducible over the rationals (you do not need to justify this). Let α denote a root of $f(x)$.
   (a) Show that $\Delta(1, \alpha, \alpha^2, \alpha^3) = 4^4 f(3/4)$.
   (b) Explain why $\{1, \alpha, \alpha^2, \alpha^3\}$ is an integral basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

7. For the following, you may (but don't need to) assume that 2^u where u is rational refers to a real number. Each part after the first is intended to have something to do with the previous part. The basic goal is to find all rational solutions to $2^x + 2^y = 1$.

   (a) Let a, b, and d be positive integers. By taking norms in the appropriate number field (clarify which one) explain why the equation

   $$2^{a/d}\big(2^{b/d} - 1\big) = 1$$

   is impossible.

   (b) Explain why there are no positive rational numbers x and y such that $2^x - 2^y = 1$.

   (c) Explain why the only rational pairs (x, y) such that $2^x + 2^y = 1$ are given by $(x, y) = (-1, -1)$.

8. Let N be a squarefree rational integer $\equiv 3 \pmod 4$ such that the ring R of algebraic integers in $\mathbb{Q}(\sqrt{N})$ is a UFD. Let p be an odd rational prime not dividing N. Further suppose that N is a square modulo p.

   (a) Prove that if $p \equiv 1 \pmod 4$, then there exist integers x and y satisfying $p = x^2 - Ny^2$ but there do not exist integers x and y satisfying $-p = x^2 - Ny^2$.

   (b) Prove that if $p \equiv 3 \pmod 4$, then there exist integers x and y satisfying $-p = x^2 - Ny^2$ but there do not exist integers x and y satisfying $p = x^2 - Ny^2$.

   (c) Observe that $13 \equiv 1 \pmod 4$, 13 is a square modulo 3, and $13 = 5^2 - 3 \times 2^2$. Prove that there are infinitely many distinct pairs (x, y) of rational integers such that $13 = x^2 - 3y^2$.