NUMBER THEORY COMPREHENSIVE EXAM
FOR MATH 784 AND MATH 788F

Do as many of the following problems as you can. You should not use a calculator during the exam. You should attempt all parts of all problems (since, in particular, the first part of a problem may not be the easiest part of that problem). Throughout the exam, the letter p denotes a prime. For the algebraic number theory questions below, any reference to R refers to the algebraic integers in $\mathbb{Q}(\alpha)$, where some description of α is given in the problem.

(1) Let B and C be ideals in the ring R of algebraic integers in an algebraic number field. Prove that $B|C$ if and only if $C \subseteq B$.

(2) (a) Prove that $\sqrt{2}$ and $\sqrt{3}$ are in $\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

(b) Are the principal ideals $(\sqrt{2})$ and $(\sqrt{3})$ equal in the ring of algebraic integers in $\mathbb{Q}(\sqrt{2}+\sqrt{3})$? Justify your answer.

(3) Let $\mathbb{Q}(\alpha)$ be an algebraic number field. Determine which of the following holds for all choices of α and all choices of β and γ in R. Justify each answer.

(a) If $N(\beta)$ is a rational prime, then β is a prime in R.

(b) If β is a prime in R, then β is irreducible in R.

(c) If $N(\beta) = N(\gamma)$, then $\beta = \epsilon\gamma$ for some unit ϵ in R.

(d) The field conjugates of β all lie in $\mathbb{Q}(\alpha)$.

(e) If I is an ideal in R and $N(I) = 1$, then $I = R$.

(4) (a) Suppose that u and v are positive integers and that the simple continued fraction for u/v is $[a_0, a_1, \dots, a_{r+2}]$ for some positive integers $a_1, \dots, a_{r+2}$. Explain why α also has $a_0, a_1, \dots, a_r$ (but maybe not a_{r+1} or a_{r+2}) as partial quotients if u/v is a convergent of the simple continued fraction for α. (Hint: The simple continued fraction for u/v is almost unique.)

(b) Let n be a fixed positive integer, and consider arbitrary positive integers $a_1, a_2, \dots, a_n$. Prove that there is a positive integer N and a positive integer a_0 such that the first $n+1$ partial quotients of the simple continued fraction for $\sqrt{N}$ are $a_0, a_1, \dots, a_n$ in that order. In other words, show that there is a positive integer N and a positive integer a_0 such that $\sqrt{N} = [a_0, a_1, \dots, a_n, a_{n+1}, \dots]$ for some positive integers $a_{n+1}, a_{n+2}, \dots$. (Hint: $\sqrt{N+1}$ is mighty close to $\sqrt{N}$).

(5) Suppose we wish to find integers x and y which satisfy $y^2 + 25 = 2x^3$. First, observe that y must be odd (this should be obvious). There are 2 cases one can consider, the case when 5 divides y and the case when 5 does not divide y. Do the second case. In other words, find all the solutions to $y^2 + 25 = 2x^3$ with $\gcd(10, y) = 1$. You should get one solution.

(6) Let α be an algebraic number with minimal polynomial $f(x)$ of degree m. Let $d(n)$ denote the number of divisors of a positive rational integer n.

(a) Prove that if p is a rational prime, then the ideal (p) is the product of $\le m$ prime ideals in R.

(b) For n a rational integer, prove that the number of ideal divisors of (n) is bounded by $d(n)^m$.

(c) Suppose that $\alpha = \sqrt{-D}$ for some positive squarefree integer $D > 3$. Prove that if β and γ are in R and $(\beta) = (\gamma)$, then $\gamma = \pm\beta$. Discuss what happens in the cases that $D = 2$ and $D = 3$.

(d) Fix positive integers n and D with D squarefree and > 3. Show that the number of integer pairs (x, y) satisfying $x^2 + Dy^2 = n$ is $\le 2d(n)^2$.

(7) Determine whether $f(x) = x^3 - x^2 + 4x + 2$ is Eisenstein.

(8) Prove that for each prime p, $\Phi_{200}(x)$ has at least 4 factors modulo p. (You should state any result you use as clearly as possible.)

(9) Prove that if $f(x) \in \mathbb{Z}[x]$ is monic, is irreducible, and has all of its roots in the set $\{z : |z| = 1\}$, then $f(x)$ is a cyclotomic polynomial.

(10) For n an integer ≥ 2, define $f_n(x) = ((x+1)^n - x^n - 1)/x$.

(a) Suppose α is a root of $f_n(x)$. Explain why $1/\alpha$ is a root of $f_n(x)$.

(b) Let $n = 2p$, where p is an odd prime. Consider the Newton polygon for $f_n(x)$ with respect to p and show that either $f_n(x)$ is irreducible or $f_n(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are irreducible polynomials of degree $p - 1$.

(c) Suppose $f_n(x) = g(x)h(x)$ in part (b) (so $n = 2p$ and $g(x)$ and $h(x)$ are irreducible polynomials of degree $p - 1$). One can obtain a little more information from the Newton polygons considered in part (b). Show that if α is a root of $g(x)$, then $1/\alpha$ is NOT a root of $g(x)$.

(d) Again, suppose $f_n(x) = g(x)h(x)$ in part (b). Show that $h(x) = x^{p-1}g(1/x)$.

(e) Show that if $n = 2p$ where p is an odd prime, then $f_n(x)$ is irreducible. In other words, show that the situation in part (d) cannot occur.

(Comment: A computer check showed me that $f_n(x)$ is irreducible over the rationals for n even and $n \le 150$. Maybe its true for all even n, but I haven't been able to show it.)

(11) Let $f(x) \in \mathbb{Z}[x]$. Prove that there is a B depending on $f(x)$ such that if $b \ge B$, then $f(x)(x-b)+1$ is irreducible. If you use a result (a lemma or theorem) from class other than Rouché's theorem, state the result and supply a proof. (Hint: Let $g(x) = -f(x)(x-b)$ and start by using Rouché's theorem to show that $f(x)(x-b)+1$ has at most one root with absolute value $\ge b/2$. In class, we only used Rouché's theorem to compare roots of polynomials in the circle $\{z : |z| = 1\}$; here, you want to use the circle $\{z : |z| = b/2\}$, or you can modify the polynomials you are dealing with - for example, consider $g(bx/2)$ instead of $g(x)$.)