NUMBER THEORY COMPREHENSIVE EXAM
FOR MATH 780 AND MATH 784

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) A squarefree number is a positive integer which is not divisible by the square of a prime. Using the Chinese Remainder Theorem, explain why there exist arbitrary long sequences of consecutive non-squarefree numbers. In other words, show that for every positive integer k, there is a non-negative integer n such that each of $n+1, n+2, \dots, n+k$ is not squarefree.

(2) An integer a is called a cubic residue modulo a prime p if there is an integer b for which $a \equiv b^3 \pmod{p}$. Prove that (i) if $p \not\equiv 1 \mod 3$, then the number of incongruent cubic residues modulo p is p, and (ii) if $p \equiv 1 \mod 3$, then the number of incongruent cubic residues modulo p is $(p+2)/3$.

(3) Prove that if $19m$ is a pseudoprime where m is a positive integer, then $m \equiv 1 \pmod{18}$. (For example, $1729 = 7 \times 13 \times 19 = 19 \times 91$ is a pseudoprime and $91 \equiv 1 \pmod{18}$.)

(4) Prove that if q is a prime $\equiv 1 \pmod 4$ and $p = 2q+1$ is prime, then 2 is a primitive root modulo p. (Hint: Think quadratic residues and Euler's criterion.)

(5) Let $\omega(n)$ denote the number of distinct prime divisors of n. Suppose that $f(x) \in \mathbb{Z}[x]$ is of degree ≥ 1. Recall that we showed that $f(m)$ cannot be prime for every integer m.

(a) Prove the stronger result that

$$\limsup_{m\to\infty} \omega(f(m)) = \infty.$$

(b) Show that there is a prime p such that for any positive integer k, there is an integer m for which p^k divides $f(m)$.

(6) (a) Using Riemann-Stieltjes' integrals, show that $\sum_{p\le x} \log p \sim x$ is a consequence of the Prime Number Theorem.

(b) Prove that there is an x_0 such that if $x \ge x_0$ and $n = \prod_{p \le (\log x)/2} p$, then $n \le x$.

(c) Prove that $\sum_{p\le(\log x)/2} \log\left(1 - \frac{1}{p}\right) = -\log\log\log x + O(1)$. (You may use that $\sum_{p\le z}(1/p) = \log\log z + O(1)$.)

(d) Prove that there is an absolute constant $c > 0$ and arbitrary large integers n such that

$$\phi(n) \le \frac{cn}{\log\log n}$$

where ϕ is Euler's ϕ-function. (Hint: This is the fourth part of a four part question.)

(7) 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 $C \subseteq B$.

(8) (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.

(9) 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 $I = R$.

(10) (a) Suppose that u and v are positive integers and that the simple continued fraction for u/v is $[a_0, a_1, \ldots, a_{r+2}]$ for some positive integers $a_1, \ldots, a_{r+2}$. Explain why α also has $a_0, a_1, \ldots, a_r$ (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 $a_1, a_2, \ldots, a_n$. 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 $a_0, a_1, \ldots, a_n$ in that order. In other words, show that there is a positive integer N and a positive integer a_0 such that $\sqrt{N} = [a_0, a_1, \ldots, a_n, a_{n+1}, \ldots]$ for some positive integers $a_{n+1}, a_{n+2}, \ldots$. (Hint: $\sqrt{N+1}$ is mighty close to $\sqrt{N}$).

(11) 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.

(12) 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 $\leq m$ 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 $\leq 2d(n)^2$.