COMPREHENSIVE EXAM

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 rational prime, and any reference to R refers to the algebraic integers in $\mathbb{Q}(\alpha)$, where some description of α is given in the problem.

(1) Calculate the remainder when $123456789101112\dots 100$ is divided by 180?

(2) An integer a is called a cubic residue modulo a prime p if there is an integer b for which $a \equiv b^3 \pmod{p}$.

(a) Prove that if $p \not\equiv 1 \mod 3$, then the number of incongruent cubic residues modulo p is p.

(b) Prove that 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 r be a positive integer, and let $f_1(x), \dots, f_r(x)$ be r polynomials with integer coefficients each of degree ≥ 1. Prove that there is an integer m such that $f_1(m), \dots, f_r(m)$ are all composite.

(6) Let $T = \{p_1, p_2, \dots\}$ be an infinite set of primes for which $\sum_{j=1}^{\infty} 1/p_j$ converges. Define $T(x) = |\{p \le x : p \in T\}|$.

(a) Prove that $\liminf_{x\to\infty} T(x)/\pi(x) = 0$.

(b) Prove, by example, that it is possible to have $\limsup_{x\to\infty} T(x)/\pi(x) = 1$.

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

(a) If $N(\beta)$ is a rational prime, then β is irreducible 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 $\mathbb{Q}(\alpha)$.

(8) Let n denote a positive integer. Prove that $\frac{1}{\pi}\cos^{-1}\left(\frac{1}{\sqrt{n}}\right)$ is rational if and only if $n \in \{1,2,4\}$.

(9) Consider the integers $n \geq 2$ such that $\binom{n}{2}$ is a square. The first such integer is 2 since $\binom{2}{2} = 1^2$. The second such integer is 9 and $\binom{9}{2} = 6^2$. Find the third, fourth, and fifth such integers.

(10) Prove the following theorem from class:

Theorem. *Let R be the ring of algebraic integers in $\mathbb{Q}(\sqrt{N})$. Then R is a Euclidean domain for $N = -1$, -2, -3, -7, and -11.*

(11) Consider all the pairs of integers satisfying $y^2 + 11 = x^3$.
 (a) Prove that there are no solutions with y odd.
 (b) Prove that there are ≤ 100 pairs of integers (x,y) with $y^2 + 11 = x^3$.

(12) Determine the odd primes p which can be expressed in the form $a^2 + 3b^2$ for some integers a and b. For example, 7 is such a prime since $7 = 2^2 + 3 \times 1^2$. Your final answer should be written as "$p = a^2 + 3b^2$ for some integers a and b if and only if $p \equiv L \pmod{N}$" where N is some positive integer and where L is a list of congruence classes modulo N. You may wish to combine material from Elementary and Algebraic Number Theory.