COMPREHENSIVE EXAM

Math 780 and Math 788M

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). You should give as many details as possible without relying on results from class; in other words, avoid using a result that is equivalent to or more general than a problem you are doing.

(1) Let $n = pq$ where p and q are distinct odd primes. Show that among the integers $a \in [1, pq]$ with $\gcd(a, pq) = 1$ exactly $1/4$ of them are squares modulo pq.

(2) 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 $91 \equiv 1 \pmod{18}$.)

(3) 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.

(4) Lattice points are points (a, b) where both a and b are integers. A lattice point (a, b) is said to be visible from the origin if a small particle sitting at $(0, 0)$ would be able to see it without its view being obstructed by another lattice point. A lattice point (a, b) is visible from the origin if and only if $\gcd(a, b) = 1$. Find integers x_0 and y_0, such that the circle centered at (x_0, y_0) of radius 2 contains only lattice points not visible from the origin. Show your work.

(5) (a) Evaluate $\left(\dfrac{15}{107}\right)$.

(b) Using Euler's Criterion and (a), deduce that $15^{53} \equiv -1 \pmod{107}$.

(c) Using (b), prove that 15 is a primitive root modulo 107.

(6) Let k be an integer ≥ 2 and p a prime satisfying $p \equiv 1 \pmod{k}$ and $p > k + 1$. Then $G = \{a^k \bmod p : a \in \mathbb{Z} \cap [1, p-1]\}$ forms a group under multiplication modulo p. In fact, G is a subgroup of the group consisting of the reduced residue system under multiplication modulo p. The cosets of G are therefore $bG = \{a^k b \bmod p : a \in \mathbb{Z} \cap [1, p-1]\}$ where b ranges over the integers in $[1, p-1]$. Answer each of the following. (Hint: you may want to consider a primitive root modulo p.)

(a) Prove that the sum of all the elements in any coset of G is divisible by p.

(b) Prove that the sum in part (a) for every coset is exactly $\dfrac{p(p-1)}{2k}$ if and only if $p \equiv 1 \pmod{2k}$.

(7) Define a strong pseudoprime to the base b and prove that no integer $n > 1$ is a strong pseudoprime to every base b with $1 \le b \le n$ and $\gcd(b, n) = 1$.

(8) State and prove the Proth, Pocklington, Lehmer Test for primality.

(9) Show that

$$\lim_{N\to\infty} \frac{|\{(a,b) \in \mathbb{Z}^2 : 1 \le a \le N, 1 \le b \le N, \gcd(a,b) > \log\log\log N\}|}{N^2} = 0.$$

(10) Prove that most positive integers n have a prime factor $> \sqrt{n}$. More specifically, show that

$$\liminf_{x\to\infty} \frac{|\{n \le x : \exists \text{ a prime } p > \sqrt{n} \text{ such that } p|n\}|}{x} > \frac{1}{2}.$$

(11) (a) For $f(x) \in \mathbb{R}[x]$, prove $M(f) \le \|f\|$.

(b) For $f(x) \in \mathbb{R}[x]$, prove $\|f\| \le 2^{\deg f} M(f)$.

(c) Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{Z}[x]$ such that $g(x)|f(x)$. Prove Mignotte's Inequality that $\|g\| \le 2^{\deg g}\|f\|$.

(12) Given $n = 12371$, describe precisely how to use Dixon's Factoring Algorithm and the following information to find a nontrivial factor of n. You do not need to come up with a factor of n, but use Dixon's Factoring Algorithm to reduce coming up with a factor of n to the computation of $\gcd(a, n)$ where you tell me rather precisely what the value of a is (it should involve multiplication and addition of specific numbers). It is possible that the a you choose will not produce a factorization of n; in the algorithm one might need to try more than one value of a. You need only give me one reasonable choice for a. Use the following information where all congruences shown are modulo n:

$$116^2 \equiv 5 \times 7 \times 31, \quad 136^2 \equiv 5^3 \times 7^2, \quad 159^2 \equiv 7^2 \times 11,$$

$$170^2 \equiv 2 \times 3^3 \times 7 \times 11, \quad 173^2 \equiv 3 \times 7 \times 13 \times 19, \quad 184^2 \equiv 2 \times 3 \times 7^2 \times 31.$$