COMPREHENSIVE EXAM FOR MATH 780 & 788M

(1) Find the smallest three positive integers n for which

$$2^n \equiv 6188 \pmod{12540}.$$

(2) (a) Determine the primes p for which the quadratic $x^2 + 3x + 1$ factors modulo p as a product of two linear polynomials. Your answer should be in the form $p \equiv L \pmod{N}$ where L is a list of numbers and N is a positive integer.

(b) Prove that the quartic $x^4 + 3x^2 + 1$ factors modulo p as a product of two (not necessarily irreducible) polynomials of degree ≥ 1 for every prime p.

(3) (a) Prove that if p is a prime and $p \equiv 13 \pmod{280}$, then $\left(\dfrac{10}{p}\right) = 1$ and $\left(\dfrac{7}{p}\right) = -1$.

(b) Using (a), prove that if p is a prime such that $p \equiv 13 \pmod{280}$, then p does *not* divide any number in the sequence $31, 331, 3331, 33331, \dots$.

(4) The following have to do with cubes modulo primes. You may wish to think in terms of primitive roots to resolve the problems (that's what I intended).

(a) Prove that 47 is a cube modulo 1997. (The number 1997 is a prime, and you do not need to verify that it's prime.)

(b) Prove that 47 is *not* a cube modulo 199. (The number 199 is prime, and you do not need to verify that it's prime.) Comment: This part may require a bit of tedious computations (which nevertheless may become easier than you might guess).

(5) (a) Let $f(x)$ and $g(x)$ be real valued functions such that $f(x) \geq 2$ for all $x \in \mathbb{R}$ and $g(x) \geq 2$ for all $x \in \mathbb{R}$. Suppose further that $f(x) \ll g(x)$. Prove that $\log f(x) \ll \log g(x)$.

(b) Let $f(x)$ and $g(x)$ be real valued functions such that $f(x) \geq 2$ for all $x \in \mathbb{R}$ and $g(x) > 1$ for all $x \in \mathbb{R}$. Give an example to show that there are such $f(x)$ and $g(x)$ for which $f(x) \ll g(x)$ holds but $\log f(x) \ll \log g(x)$ does not hold (both simultaneously; i.e., for the same $f(x)$ and $g(x)$).

(6) (a) Prove that 2465 is an absolute pseudoprime.

(b) Is 2465 a strong pseudoprime to the base 2? Justify your answer. (Hint: Work modulo the prime factors of 2465 rather than modulo 2465.)

(7) (a) State the Proth-Pocklington-Lehmer primality test.

(b) Prove the Proth-Pocklington-Lehmer primality test.

(8) Demonstrate what MAPLE's version of the Lucas-Lehmer test is doing by checking the primality of $n = 37$ using $P = 3$.

(9) Given $f(x) = \sum_{j=0}^{n} a_j \in \mathbb{Z}[x]$, define $\|f\| = \left(\sum_{j=0}^{n} a_j^2\right)^{1/2}$. Prove Mignotte's inequality:

Theorem. *If $f(x)$, $g(x)$, and $h(x)$ in $\mathbb{Z}[x]$ are such that $f(x) = g(x)h(x)$, then $\|g\| \le 2^{\deg g}\|f\|$.*

(10) Let $n = 1377989$. The quadratic sieve algorithm is used to factor n as follows. It is determined that $[\sqrt{n}] = 1173$, and $s(a) = a^2 \bmod n$ is computed for $1174 \le a \le 2000$. (We ignore here the possibility of $s(a)$ being negative and only use positive residues.) We factor each such $s(a)$ and discard $s(a)$ if it has a prime factor > 20. We obtain the following data:

Values for a	$a^2 \pmod{n}$
1192	$5^3 \times 7^3$
1679	$3^2 \times 7^2 \times 11 \times 13$
1688	$2 \times 3^3 \times 7 \times 13 \times 19$
1954	$2 \times 3 \times 7 \times 11^3 \times 19$

Continue the quadratic sieve algorithm by finding numbers A and B for which $\gcd(A, B)$ is reasonably a non-trivial divisor of n. You do not need to compute the $\gcd(A, B)$. Furthermore, you do not need to give A and B explicitly. Specifically, A may be left in the form $A = u \times v \times w \times x \times y \bmod n$ (the number of variables written here is not significant), and similarly for B.