MAS 4203 Number Theory Name:______________________________

Spring 2009 CODE-Name:______________________________

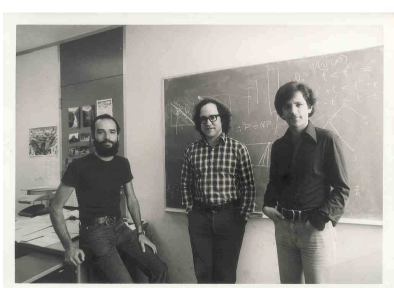
FINAL EXAM

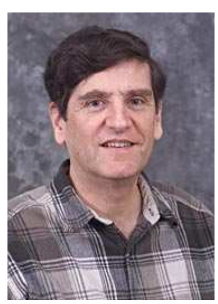
Instructions:

- There are 8 questions. Do only **SIX** questions.
- With SIX complete problems there are 120 total points. Full marks will be given for 120 points.
- Write on **ONE** side of the paper.
- Show all necessary working and reasoning to receive full credit.
- Your work needs to be written in a proper and coherent fashion.
- When giving proofs your reasoning should be clear.
- Only scientific calculators are allowed.
- A table of primes is supplied.

PLEASE GRADE THE FOLLOWING SIX QUESTIONS:

For 4 bonus points who are the people in the photos below and what is their connection with Question 8?





1. [$10 + 10 = 20$ points] Let a, m, n be positive integers with $a > 1$ and $n > 1$.

(i) Prove that if $m \mid n$ then $a^m - 1 \mid a^n - 1$.

HINT: $(x^b - 1) = (x - 1)(x^{b-1} + x^{b-2} + \cdots + x + 1)$.

(ii) Prove that if $a^n - 1$ is prime then $a = 2$ and n is prime.

2. [$5 + 15 = 20$ points]

(i) Let a, $b \in \mathbb{Z}$. Prove that if a and b are expressible in the form $6n + 1$ where n is an integer, then ab is also expressible in that form.

(ii) Prove that there are infinitely many primes of the form $6n + 5$ where n is an integer.

3. [$4 + 6 + 6 + 4 = 20$ points] Let a, b, c, d, $m \in \mathbb{Z}$ with $m > 0$.

(i) Define what it means to write

$$a \equiv b \pmod{m}.$$

(ii) Prove that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies that $ac \equiv bd \pmod{m}$.

(iii) Let p be prime. Prove that $a^2 \equiv b^2 \pmod{p}$ implies that $a \equiv \pm b \pmod{p}$.

(iv) Is (iii) still true if p is not prime? If not, give an example.

4. [$4 + 2 + 6 + 8 = 20$ points]

(i) State Fermat's Little Theorem.

(ii) Define what it means for a positive integer n to be a pseudo-prime.

(iii) Prove that $645 = (3)(5)(43)$ is a pseudoprime.

(iv) Let p and q be distinct primes, and suppose that $a \in \mathbb{Z}$. Prove that

$$a^{pq} + a \equiv a^p + a^q \pmod{pq}.$$

5. [$2+4+4+4+6=20$ points]

(i) Define what it means for an arithmetic function to be *multiplicative.*

(ii) Prove that if f is a multiplicative function then $f(1)=0$ or 1.

(iii) Prove that if $f(n)$ and $g(n)$ are multiplicative functions then $h(n)=f(n)\,g(n)$ is multiplicative.

(iv) Define the Möbius function $\mu(n)$ and state one important theorem (or proposition) for the Möbius function.

(v) Suppose $n \in \mathbb{Z}$, $n>1$ and $n=p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}$ is the prime factorization of n, f is multiplicative and $f(1)=1$. Prove that

$$\sum_{d|n} \mu(d)\,f(d) = \prod_{i=1}^{m}(1-f(p_i)).$$

6. [$4+6+4+6=20$ points]

(i) Define the arithmetic functions $\phi(n)$, $\nu(n)$ and $\sigma(n)$.

(ii) Explain why $\nu(n)$ and $\sigma(n)$ are multiplicative.

(iii) Suppose $n \in \mathbb{Z}$, $n>1$ and $n=p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}$ is the prime factorization of n. State formulas for $\phi(n)$, $\nu(n)$ and $\sigma(n)$.

(iv) Prove that $\nu(n)$ is odd if and only if n is a perfect square.

7. [$2+4+4+4+6=20$ points]

(i) Suppose a, $m \in \mathbb{Z}$ with $m>0$. Define what it means for a to be a *quadratic residue modulo m.*

(ii) Find the quadratic residues modulo 17.

(iii) Define the Legendre symbol $\left(\frac{a}{p}\right)$, and state three properties of the Legendre symbol.

(iv) State the Law of Quadratic Reciprocity.

(v) Find the Legendre symbol $\left(\frac{425}{149}\right)$.

8. [20 points] Do either (A) or (B) but NOT BOTH.

(A) Explain what the RSA algorithm is and give a proof of the decoding procedure.

(B) State the a-test for primality and prove that p passes the a-test for any given a, for all primes p.