MATH 573 — FINAL EXAM

May 30, 2007

NAME: ____

1. This exam is due Wednesday, June 6 before the 1:30 pm. After 1:30 pm I will NOT accept the exam.
2. This exam has 13 pages including this cover. There are 10 problems.
3. Your proofs should be neat and legible. You may and should use the back of pages for scrap work.
4. You are welcome to use any non-human sources you choose. (Note, talking to someone on the phone, over the internet, etc. falls under getting human help.) Be sure to cite your sources as unacknowledged sources constitute plagarism and will receive 0 points.

PROBLEM	POINTS	SCORE
1	11	
2	10	
3	12	
4	10	
5	10	
6	10	
7	15	
8	10	
9	12	
TOTAL	100	

1.(6+5 points) We proved in class that given integers a_1, a_2, m_1, m_2 with $\gcd(m_1, m_2) = 1$, then there is a unique simultaneous solution x modulo m_1m_2 to the system of equations

$$x \equiv a_1 (\operatorname{mod} m_1)$$
$$x \equiv a_2 (\operatorname{mod} m_2).$$

(a) If $\gcd(m_1, m_2) = d$, prove that there is a simultaneous solution x to the system of equations

$$x \equiv a_1 (\operatorname{mod} m_1)$$
$$x \equiv a_2 (\operatorname{mod} m_2)$$

if and only if $a_1 \equiv a_2 (\operatorname{mod} d)$. Show that this solution x is unique modulo m_1m_2/d.

(b) Find the smallest positive simultaneous solution to the system of equations:

$$x \equiv 17 (\operatorname{mod} 65)$$
$$x \equiv 42 (\operatorname{mod} 20).$$

2. (10 points) Let D be a positive integer and suppose there exists a prime p dividing D so that $p \equiv 3 \pmod 4$. Prove that $x^2 - Dy^2 = -1$ has no integer solutions.

3. (6+6 points) **(a)** Evaluate the continued fraction $[2 : \overline{1, 2}]$.

(b) Express $\frac{71}{55}$ as a finite simple continued fraction. Do this by hand!

4. (10 points) Is 137 a congruent number? Be sure to justify your answer. If it is a congruent number, find a triangle with rational sides and area 137.

5. (10 points) Prove that 3 is a primitive root of all integers of the form 7^k and $2 \cdot 7^k$ for $k \geq 1$.

6. (10 points) Find 6 different positive values of n so that $n+1$ and $\frac{n}{2}+1$ are both perfect squares. Are there infinitely many different values for n so that $n+1$ and $\frac{n}{2}+1$ are both perfect squares? Prove your answer is true. (You may use any theorems proven in class to prove your result.)

7. (5 points each) Let a and $b > 1$ be relatively prime integers with b odd. Write $b = p_1 \cdots p_r$ with the p_i odd, define the Jacobi symbol $\left(\frac{a}{b}\right)$ by

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right).$$

(a) Prove that if a is a quadratic residue of b then $\left(\frac{a}{b}\right) = 1$. Is the converse true? Prove it or give a counterexample.

(b) Prove that $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$ and $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$.

(c) Prove that if a and b are relatively prime positive odd integers each greater then 1, then

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}.$$

It may be helpful to note that if u, v are odd integers, then $(u-1)/2+(v-1)/2 \equiv (uv-1)/2 \pmod 2$.

8. (10 points) Prove that $\phi(p!) = (p-1)\phi((p-1)!)$ for p a prime.

Choose either version of problem 9 to do. You may receive extra credit for doing the other one though!

9. (12 points) Consider the equation

$$a^2 + b^2 = p(c^2 + d^2).$$

Show that if $p \equiv 3 \pmod 4$ that this equation has no solutions. (You may want to use descent here!)

9. (6+6 points) Let m be a positive square-free integer.

(a) Show that the elements $a + b\sqrt{m}$ with $a, b \in \mathbb{Z}$ are all algebraic integers in $\mathbb{Q}(\sqrt{m})$.

(b) Prove there are infinitely many units in $\mathbb{Q}(\sqrt{m})$.