# MATH 573 — FINAL EXAM

May 30, 2007

NAME: Solutions

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 12 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 $m_1 m_2$ to the system of equations

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

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

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

if and only if $a_1 \equiv a_2 (\mathrm{mod}\, d)$. Show that this solution $x$ is unique modulo $m_1 m_2 / d$.

**Proof:** We know that $x = a_1 + m_1 t$ is a solution to $x \equiv a_1 (\mathrm{mod}\, m_1)$ for any $t \in \mathbb{Z}$. We now want to determine when we can choose $t \in \mathbb{Z}$ so that $x = a_1 + m_1 t$ is also a solution to the congruence $x \equiv a_2 (\mathrm{mod}\, m_2)$. We have that $x$ is a solution to this second congruence if and only if $a_1 + m_1 t \equiv a_2 (\mathrm{mod}\, m_2)$, which is equivalent to $m_1 t = a_2 - a_1 (\mathrm{mod}\, m_2)$. This is now a linear congruence and we know this has a solution if and only if $\gcd(m_1, m_2) \mid (a_2 - a_1)$, as desired. Suppose now that $x$ and $y$ are both solutions to the system of congruences. Then $x \equiv y (\mathrm{mod}\, m_1)$ and $x \equiv y (\mathrm{mod}\, m_2)$. Thus, we must have the least common multiple of $m_1$ and $m_2$ divides $x - y$, i.e., $m_1 m_2 / d$ divides $x - y$. This is precisely what it means for the solution to be unique modulo $m_1 m_2 / d$. ■

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

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

From part (a) we see that we need to find a solution to

$$65t \equiv 42 - 17 (\mathrm{mod}\, 20),$$

i.e., a solution to

$$5t \equiv 5 (\mathrm{mod}\, 20).$$

This is obvious though with $t = 1$. Thus, our simultaneous solution is $x = 17 + 65 = 82$.

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

**Proof:** Suppose $x_0, y_0$ is an integer solution to the equation, i.e., $x_0, y_0 \in \mathbb{Z}$ and

$$x_0^2 - dy_0^2 = -1.$$

Looking at this equation modulo $p$ we obtain

$$x_0^2 \equiv -1 (\mathrm{mod}\, p).$$

This implies that $-1$ is a quadratic residue modulo $p$. Since $p \equiv 3 (\mathrm{mod}\, 4)$ this cannot be the case. Thus, there are no integer solutions to this equation. ■

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

Set $x = [\overline{1, 2}]$. Then we have $x = [1, 2, \overline{1, 2}]$. From this we have

$$\begin{aligned} x &= 1 + \frac{1}{2 + \frac{1}{x}} \\ &= 1 + \frac{x}{2x + 1} \\ &= \frac{3x + 1}{2x + 1}. \end{aligned}$$

This leads to the quadratic equation

$$2x^2 - 2x - 1 = 0.$$

We can use the quadratic equation to solve for $x$, noting that $x > 0$ to discard one of the solutions:

$$x = \frac{1}{2} + \frac{\sqrt{3}}{2}.$$

So we have

$$\begin{aligned} [2 : \overline{1, 2}] &= 2 + \frac{1}{x} \\ &= 2 + \frac{2}{1 + \sqrt{3}} \\ &= 2 + \frac{2 - 2\sqrt{3}}{1 - 3} \\ &= 1 + \sqrt{3}. \end{aligned}$$

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

We use the Euclidean algorithm to accomplish this:

$$\begin{aligned} 71 &= 55(1) + 16 \\ 55 &= 16(3) + 7 \\ 16 &= 7(2) + 2 \\ 7 &= 2(3) + 1 \\ 2 &= 1(2) + 0. \end{aligned}$$

We now convert these equations into the form we need:

$$\begin{aligned} \frac{71}{55} &= 1 + \frac{16}{55} \\ \frac{55}{16} &= 3 + \frac{7}{16} \\ \frac{16}{7} &= 2 + \frac{2}{7} \\ \frac{7}{2} &= 3 + \frac{1}{2} \\ 2 &= 2 + 0. \end{aligned}$$

Combining these equations we obtain the following continued fraction:

$$\begin{aligned} \frac{71}{55} &= 1 + \frac{16}{55} \\ &= 1 + \frac{1}{\frac{55}{16}} \\ &= 1 + \frac{1}{3 + \frac{7}{16}} \\ &= 1 + \frac{1}{3 + \frac{1}{\frac{16}{7}}} \\ &= 1 + \frac{1}{3 + \frac{1}{2 + \frac{2}{7}}} \\ &= 1 + \frac{1}{3 + \frac{1}{2 + \frac{1}{3 + \frac{1}{2}}}}. \end{aligned}$$

Thus, the continued fraction expansion of $\frac{71}{55}$ is $[1; 3, 2, 3, 2]$.

**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.

Using SAGE one finds the rational point $\left(-\frac{3136}{25}, \frac{77112}{125}\right)$. This is clearly not in the set $E_{137}(\mathbb{Q})_{\text{tors}}$, so 137 is a congruent number. Previous homework allows one to turn this rational point into the triangle with side lengths: $\frac{1377}{280}, \frac{76720}{1377}, \frac{21565121}{385560}$, which one can easily check has 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 $k \geq 1$.

**Proof:** For this one needs to go back to how we proved primitive roots existed for prime powers. In fact, with the proper set-up one could just quote these results. It is elementary to check that 3 is a primitive root modulo 7. We can also check that $3^6 \not\equiv 1 (\text{mod}\, 49)$. Thus, 3 satisfies the hypotheses of Lemma 2 on page 160 of the textbook (we also covered this in class, but we didn't number it there.) Thus, we have $3^{7^{k-2}6} \not\equiv 1 (\text{mod}\, 7^k)$ for all $k \geq 2$. Now the proof of Theorem 8.9 of the text shows that 3 is a primitive root for $7^k$ with $k \geq 1$ and the Corollary to Theorem 8.9 shows 3 is a primitive root of $2 \cdot 7^k$ for all $k \geq 1$. ■

**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.)

**Proof:** Suppose $n+1$ and $\frac{n}{2}+1$ are both perfect squares, i.e., there exists $x, y \in \mathbb{Z}$ so that $n+1 = x^2$ and $\frac{n}{2}+1 = y^2$, i.e., $n+2 = 2y^2$. Subtracting these two equations gives that $n+1$ and $\frac{n}{2}+1$ are perfect squares if and only if there is an integer solution to the equation $x^2 - 2y^2 = -1$. We know from class that if we let $\frac{p_k}{q_k}$ be the convergents of the continued fraction expansion of $\sqrt{2}$, then

$$p_k^2 - 2q_k^2 = (-1)^{k+1} b_{k+1}$$

where $b_{k+1}$ is defined as in class. We saw that this equation has solutions if and only if the period of the continued fraction expansion of $\sqrt{2}$ is odd, which in this case it is with period $n = 1$. We found the solutions to be given by $p_{n(2t+1)-1}, q_{n(2t+1)-1}$ with $t \geq 1$, which in our case are given by $p_{2t}, q_{2t}$. This shows in fact that we have infinitely many $x, y \in \mathbb{Z}$ satisfying this equation and thus infinitely many such $n$. We now just need to find 6 of them. The first 6 solutions of the equation are: $(x, y) = (7, 5), (41, 29), (239, 169), (1393, 985), (8119, 5741), (47321, 33461)$. The corresponding values of $n$ are: $48, 1680, 57120, 1940448, 65918160, 2239277040$. ■

**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.

**Proof:** Let $b = p_1 \cdots p_r$ with $p_i$ odd primes. If $a$ is a quadratic residue modulo $b$ then there exists an integer $x$ so that $x^2 \equiv a (\mathrm{mod}\, b)$. Thus, $b \mid (x^2 - a)$. Since $p_i \mid b$, we have $x^2 \equiv a (\mathrm{mod}\, p_i)$ for each $i$. Namely, we have

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{n} \left(\frac{a}{p_i}\right) = \prod_{i=1}^{n} 1 = 1.$$

The converse is false. Consider $a = 3$ and $b = 35$. Then $a$ is not a quadratic residue modulo 35 (check by computation) but

$$\left(\frac{3}{35}\right) = \left(\frac{3}{5}\right)\left(\frac{3}{7}\right) = (-1)(-1) = 1. \blacksquare$$

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

**Proof:** Let $b = p_1 \cdots p_r$. We have

$$\left(\frac{aa'}{b}\right) = \prod_{i=1}^{n} \left(\frac{aa'}{p_i}\right)$$
$$= \prod_{i=1}^{n} \left(\frac{a}{p_i}\right)\left(\frac{a'}{p_i}\right) \qquad = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$$

where we have used the analogous property for the quadratic residue symbol. Let $b' = p_{r+1} \cdots p_s$ with $p_j$ $(r+1 \le j \le s)$ primes. We have

$$\left(\frac{a}{bb'}\right) = \prod_{i=1}^{s} \left(\frac{a}{p_i}\right)$$
$$= \prod_{i=1}^{r} \left(\frac{a}{p_i}\right) \prod_{j=r+1}^{s} \left(\frac{a}{p_j}\right)$$
$$= \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$$

as claimed. ■

**(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 $(u-1)/2+(v-1)/2 \equiv (uv-1)/2 (\mathrm{mod}\, 2)$.

**Proof:** Let $a = p_1 \cdots p_r$ and $b = q_1 \cdots q_s$. We have

$$\begin{aligned}
\left(\frac{a}{b}\right) &= \prod_{i=1}^{s}\left(\frac{a}{q_i}\right) \\
&= \prod_{i=1}^{s}\prod_{j=1}^{r}\left(\frac{p_j}{q_i}\right) \\
&= \prod_{i=1}^{s}\prod_{j=1}^{r}\left(\frac{q_i}{p_j}\right)(-1)^{\left(\frac{p_j-1}{2}\right)\left(\frac{q_i-1}{2}\right)} \qquad \text{(quadratic reciprocity)} \\
&= \left(\frac{b}{a}\right)\prod_{i=1}^{s}\prod_{j=1}^{r}(-1)^{\left(\frac{p_j-1}{2}\right)\left(\frac{q_i-1}{2}\right)} \\
&= \left(\frac{b}{a}\right)(-1)^{\sum_{i=1}^{s}\sum_{j=1}^{r}\left(\frac{p_j-1}{2}\right)\left(\frac{q_i-1}{2}\right)} \\
&= \left(\frac{b}{a}\right)(-1)^{\sum_{i=1}^{s}\left(\frac{q_i-1}{2}\right)}(-1)^{\sum_{j=1}^{r}\left(\frac{p_j-1}{2}\right)} \\
&= \left(\frac{b}{a}\right)(-1)^{\left(\frac{b-1}{2}\right)\left(\frac{a-1}{2}\right)}
\end{aligned}$$

where the last equality follows from the hint. Now we use that $\left(\frac{b}{a}\right) = \pm 1$ to move $\left(\frac{b}{a}\right)$ to the other side of the equation $\left(\left(\frac{b}{a}\right) = \left(\frac{b}{a}\right)^{-1}\right)$. ■

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

**Proof:** We can write $p! = p(p-1)!$. Since $p$ is a prime, $\gcd(p, (p-1)!) = 1$ and so $\phi(p(p-1)!) = \phi(p)\phi((p-1)!) = (p-1)\phi((p-1)!)$, as claimed. ■

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 $p \equiv 3 (\mathrm{mod}\, 4)$ that this equation has no solutions. (You may want to use descent here!)

**Proof:** Let $u_1, v_1, x_1, y_1 \in \mathbb{Z}_{>0}$ be a solution to the equation so that

$$u_1^2 + v_1^2 = p(x_1^2 + y_1^2). \tag{1}$$

This implies that $u_1^2 + v_1^2 \equiv 0 (\mathrm{mod}\, p)$, i.e., $u_1^2 \equiv -v_1^2 (\mathrm{mod}\, p)$. Suppose $p \nmid v_1$. Then we have that $\left(\frac{-v_1^2}{p}\right) = 1$. However, we know that $\left(\frac{v_1^2}{p}\right) = 1$ and so we must have $\left(\frac{-1}{p}\right) = 1$. This is impossible since $p \equiv 3 (\mathrm{mod}\, 4)$. Thus, we have $p \mid v_1$ and hence $p \mid u_1$ as well. Set $u_2 = u_1/p$ and $v_2 = v_1/p$. Then we have

$$(pu_2)^2 + (pv_2)^2 = p(x_1^2 + y_1^2)$$

i.e.,

$$x_1^2 + y_1^2 = p(u_2^2 + v_2^2).$$

Note that $u_2 < u_1$. We can now repeat the same argument to obtain that $p \mid x_1$ and $p \mid y_1$. Setting $x_2 = x_1/p$ and $y_2 = y_1/p$ and applying the same argument we obtain

$$u_2^2 + v_2^2 = p(x_2^2 + y_2^2).$$

However, this gives another solution $(u_2, v_2, x_2, y_2)$ with strictly smaller positive values then our original solution. Applying descent we see that we have a strictly decreasing sequence of positive integers, a contradiction. Thus there can be no solutions. ■

**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 $\mathbb{Q}(\sqrt{m})$.

**Proof:** Set $\alpha = a + b\sqrt{m}$ with $a, b \in \mathbb{Z}$. Observe that $\alpha + \overline{\alpha} = 2a \in \mathbb{Z}$ and $\alpha\overline{\alpha} = a^2 - mb^2 \in \mathbb{Z}$. Thus, the polynomial $f(x) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}$ is a monic polynomial with integer coefficients. Plugging in $\alpha$ we see that

$$f(\alpha) = \alpha^2 - (\alpha + \overline{\alpha})\alpha + \alpha\overline{\alpha} = 0.$$

Thus, we see that $\alpha$ is necessarily an algebraic integer in $\mathbb{Q}(\sqrt{m})$. ■

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

**Proof:** Recall that $\alpha = a + b\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ is a unit if and only if $\mathrm{N}(\alpha) = \alpha\overline{\alpha} = \pm 1$ and $\alpha$ is an algebraic integer. The statement about the norm is equivalent to the statement that $a^2 - mb^2 = \pm 1$. Consider the equation $x^2 - my^2 = 1$. This is Pell's equation and we know there are infinitely many solutions to this equation for $m$ positive and square-free. For any solution $x_n, y_n$ of the equation $x^2 - my^2 = 1$ we have that the element $x_n + y_n\sqrt{m}$ is then a unit in $\mathbb{Q}(\sqrt{m})$ by part (a) along with the fact that it has norm 1. Since there are infinitely many integer solutions to Pell's equation, there are infinitely many units in $\mathbb{Q}(\sqrt{m})$. ■