MATH 573 — SECOND MIDTERM EXAM
(TAKE HOME PORTION)

May 17, 2007

NAME: Solutions

1. This exam is due Monday, May 21 before the bell rings for class. After the bell rings I will NOT accept the exam.
2. This exam has 5 pages including this cover. There are 4 problems.
3. Do not separate the pages of the exam.
4. Your proofs should be neat and legible. You may and should use the back of pages for scrap work.
5. 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	10	
2	14	
3	16	
4	10	
TOTAL	50	

1.(10 points) Let p and q be odd primes. Define $\epsilon_p = (-1)^{(p-1)/2}$. Prove that $\epsilon_p p$ is a square modulo q if and only if q is a square modulo p.

Proof: Observe that if one shows that $\left(\frac{\epsilon_p p}{q}\right)\left(\frac{q}{p}\right) = 1$ this is the same as showing that $\epsilon_p p$ is a square modulo q if and only if q is a square modulo p. We have

$$\begin{aligned}
\left(\frac{\epsilon_p p}{q}\right)\left(\frac{q}{p}\right) &= \left(\frac{\epsilon_p}{q}\right)\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \\
&= \left(\frac{-1}{q}\right)^{(p-1)/2}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \\
&= (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \\
&= (-1)^{(p-1)(q-1)/4}(-1)^{(p-1)(q-1)/4} \qquad \text{by quadratic reciprocity} \\
&= 1.
\end{aligned}$$

Thus, we have the result. ■

2. (2+2+5+5 points each) Consider the elliptic curve $E_{161} : y^2 = x^3 - 161^2 x$.

(a) What is the rank of E_{161}?

Using SAGE we have

$$\text{sage} : \text{E} = \text{EllipticCurve}([-161^2, 0]); \text{E.rank}()$$
$$\text{sage} : 2$$

Thus the rank of the elliptic curve is 2.

(b) What are the elements of $E_{161}(\mathbb{Q})_{\text{tors}}$?

As computed in class, we have $E_{161}(\mathbb{Q})_{\text{tors}} = \{0_{E_{161}}, (0,0), (\pm 161, 0)\}$.

(c) Compute $a_{E_{161},n}$ for $1 \leq n \leq 25$. (This does not have to be done by hand!) Use these values to estimate $L(E_{161}, 1)$.

We use SAGE to compute the values of $a_{E_{161},n}$ for $0 \leq n \leq 25$:

$$\text{sage} : \text{E.anlist}(25)$$
$$\text{sage} : [0, 1, 0, 0, 0, -2, 0, 0, 0, -3, 0, 0, 0, -6, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, -1]$$

We see the only nonzero terms correspond to $n = 1, 5, 9, 13, 17, 25$ with corresponding values $1, -2, -3, -6, 2, -1$. Thus, our approximation for $L(E_{161}, 1)$ is given by

$$\begin{aligned} L(E_{161}, 1) &\approx 1 \cdot 1^{-1} + (-2)5^{-1} + (-3)9^{-1} + (-6)13^{-1} + 2 \cdot 17^{-1} + (-1)25^{-1} \\ &= -\frac{1943}{16575} \\ &\approx -0.117. \end{aligned}$$

(d) Is 161 a congruent number? If so, find a triangle with rational sides and area 161.

One has from part (a) that the rank is 2, thus 161 is a congruent number. To find a triangle with area 161 we need a rational point on the curve. We use SAGE and the command E.point_search(10) to find the point $(x, y) = (289, 4080)$. We now plug this into the bijection established in the most recent homework assignment to get the triangle with sides (X, Y, Z) where

$$X = \frac{2737}{120}$$
$$Y = \frac{240}{17}$$
$$Z = \frac{54721}{2040}$$

where we have used that if (x, y) is a point on the curve, then $(x, -y)$ is also on the curve. Thus, when we use the homework problem and the point (x, y) we get a triple (X, Y, Z) with $X < 0$ and $Y < 0$, not real useful for a triangle! But if we use $(x, -y)$ instead we get the sides listed above.

3. (4 points each) In this problem you show that $\frac{x^2-2}{2y^2+3}$ is not an integer for any integers x, y. Suppose that there exists $x, y \in \mathbb{Z}$ so that $\frac{x^2-2}{2y^2+3} \in \mathbb{Z}$.

(a) Show that if p is a prime with $p \mid 2y^2+3$, then necessarily $p \equiv \pm 1 (\mathrm{mod}\, 8)$.

Proof: By assumption we have that $\frac{x^2-2}{2y^2+3} \in \mathbb{Z}$ and so if $p \mid 2y^2+3$ we must have $p \mid x^2-2$ as well. Thus, 2 is a square modulo p, i.e., $\left(\frac{2}{p}\right) = 1$. However, we know this is the case if and only if $p \equiv \pm 1 (\mathrm{mod}\, 8)$. ■

(b) Show that $2y^2+3 \equiv \pm 1 (\mathrm{mod}\, 8)$.

Proof: We know that every prime that divides $2y^2+3$ is congruent to $\pm 1 (\mathrm{mod}\, 8)$. Thus, when we reduce $2y^2+3$ modulo 8 we obtain a product of 1's and -1's. This gives the result. ■

(c) Show $2 \nmid y$.

Proof: Suppose $2 \mid y$. Then $2y^2+3 \equiv 3 (\mathrm{mod}\, 8)$ since $8 \mid 2y^2$ if $2 \mid y$. However, we know that $2y^2+3 \equiv \pm 1 (\mathrm{mod}\, 8)$. Thus, $2 \nmid y$. ■

(d) Use the previous results in this problem to reach a contradiction, showing that $\frac{x^2-2}{2y^2+3} \notin \mathbb{Z}$ for any $x, y \in \mathbb{Z}$. (Using (c), what form must y be? Use this!)

Proof: Since $2 \nmid y$, y is necessarily odd. We can write $y = 2k+1$ for some $k \in \mathbb{Z}$. Thus we have

$$\begin{aligned} 2y^2+3 &= 2(2k+1)^2+3 \\ &= 2(4k^2+4k+1)+3 \\ &\equiv 5 (\mathrm{mod}\, 8). \end{aligned}$$

However, this again contradicts part (b). Thus, it must be that $\frac{x^2-2}{2y^2+3} \notin \mathbb{Z}$. ■

4. (5+5 points) **(a)** Let p be a prime and let a be an integer so that $\text{ord}_p(a) = 3$. Prove that $1 + a + a^2 \equiv 0 (\text{mod}\, p)$.

Proof: Observe that $(1 - a)(1 + a + a^2) = 1 - a^3$ (finite geometric series). Thus, we have

$$a^3 - 1 \equiv (a - 1)(1 + a + a^2) (\text{mod}\, p).$$

However, since $\text{ord}_p(a) = 3$ we have that the left hand side of the equation is 0. Thus, $p \mid (a-1)(1+a+a^2)$. Since $\text{ord}_p(a) = 3$, it can't be that $p \mid (a-1)$ and so $p \mid (1+a+a^2)$ as desired. ■

(b) Prove that $\text{ord}_p(1 + a) = 6$.

Proof: To show this we must establish the two facts that $(1+a)^6 \equiv 1 (\text{mod}\, p)$ and that $(1+a)^h \not\equiv 1 (\text{mod}\, p)$ for any $h \mid 6$, i.e., for $h = 1, 2, 3$. Observe that $(1+a)^6 = a^6 + 6a^5 + 15a^4 + 20a^3 + 15a^2 + 6a + 1$. We now use that $a^3 \equiv 1 (\text{mod}\, p)$ to get that

$$\begin{aligned}(1 + a)^6 &\equiv 22 + 21a + 21a^2 (\text{mod}\, p) \\ &\equiv 1 + 21(1 + a + a^2) (\text{mod}\, p) \\ &\equiv 1 (\text{mod}\, p)\end{aligned}$$

where we used part (a) for the last congruence. Thus, we at least have that $\text{ord}_p(1 + a) \mid 6$.
If $1 + a \equiv 1 (\text{mod}\, p)$ then we have $p \mid a$ which would contradict $\text{ord}_p(a) = 3$.
Suppose $(1+a)^2 \equiv 1 (\text{mod}\, p)$. Then $1 + 2a + a^2 \equiv 1 (\text{mod}\, p)$, i.e., $(a^2 + a + 1) + (a - 1) \equiv 0 (\text{mod}\, p)$. Using part (a) we obtain that $a \equiv 1 (\text{mod}\, p)$, contradicting that $\text{ord}_p(a) = 3$.
Suppose $(a+1)^3 \equiv 1 (\text{mod}\, p)$. Then $a^3 + 3a^2 + 3a + 1 \equiv 1 (\text{mod}\, p)$, i.e., $a(a^2 + 3a + 3) \equiv 0 (\text{mod}\, p)$. Again, $p \nmid a$ so we must have $a^2 + 3a + 3 \equiv 0 (\text{mod}\, p)$. Using part (a) again we obtain $2(a + 1) \equiv 0 (\text{mod}\, p)$. Since by assumption we have an element of order 3, $p \neq 2$. Thus $p \mid a+1$ which implies $a \equiv -1 (\text{mod}\, p)$, i.e., $\text{ord}_p(a) = 2$. Thus, the order of $1 + a$ cannot be 3.
Thus, 6 is the smallest positive integer gives 1 when we raise $1 + a$ and look modulo p, so $\text{ord}_p(1 + a) = 6$ as desired. ■