MATH 573 — SECOND MIDTERM EXAM
(IN CLASS PORTION)

May 17, 2007

NAME: Solutions

1. Do not open this exam until you are told to begin.
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. If you are unsure whether you can quote a result from class or the book, please ask.
6. Please turn **off** all cell phones.

PROBLEM	POINTS	SCORE
1	12	
2	16	
3	10	
4	12	
TOTAL	50	

1. (3 points each) In this problem we will work with the elliptic curve $E_{21} : y^2 = x^3 - 441x$.

(a) If we reduce this curve modulo 5 is the resulting curve nonsingular? If so, prove it. If not, give a singular point.

Let $\overline{E}_{21}$ be the curve after reducing modulo 5. Let $f(x,y) = y^2 + \overline{4}x^3 + x$. Then a point $(x_0, y_0) \in (\mathbb{Z}/5\mathbb{Z})^2$ is on the curve $\overline{E}_{21}$ if and only if $f(x_0, y_0) = \overline{0}$. To see if points are singular, we look at partial derivatives:

$$\frac{\partial f}{\partial y} = \overline{2}y$$
$$\frac{\partial f}{\partial x} = \overline{2}x^2 + \overline{1}.$$

The curve is singular if and only if there is a point with both partial derivatives vanishing. Observe that $\frac{\partial f}{\partial x} = \overline{0}$ if and only if $2x^2 + 1 \equiv 0 \pmod 5$. However, this is equivalent to $2x^2 \equiv 4 \pmod 5$, i.e, $x^2 \equiv 2 \pmod 5$. Thus, we have that the partial derivative with respect to x vanishes if and only if $\left(\frac{2}{5}\right) = 1$. However, we know that 2 is not a quadratic residue modulo 5 (as $5 \not\equiv \pm 1 \pmod 8$). Thus, there are no singular points when we reduce modulo 5.

(b) Though we only defined $a_{E_N,p}$ for primes where $\overline{E}_N$ is an elliptic curve, we can use the exact same definition to define $a_{E_N,p}$ for primes where $\overline{E}_N$ is not an elliptic curve. Keeping this in mind, compute $a_{E_{21},5}$.

This amounts to checking whether each point (i,j) satisfies $f(i,j) = \overline{0}$ for $0 \leq i, j \leq 4$. The points that satisfy this are $\{(0,0), (1,0), (2,1), (2,4), (3,2), (3,3), (4,0)\}$. Thus, (throwing in the point at infinity) we have $\#\overline{E}_{21}(\mathbb{Z}/5\mathbb{Z}) = 8$. So we have $a_{E_{21},5} = 5 + 1 - 8 = -2$.

(c) Show that the point $(-3, 36)$ is on the curve E_N.

This amounts to showing $36^2 = (-3)^3 - 441(-3)$, which is easily confirmed.

(d) Prove that the number 21 is a congruent number.

Proof: Part (c) showed that $P = (-3, 36) \in E_{21}(\mathbb{Q})$. We know that the torsion subgroup is given by $E_{21}(\mathbb{Q})_{\text{tors}} = \{0_{E_{21}}, (0,0), (\pm 21, 0)\}$ as was shown in class. Thus, we have a non-torsion point on the curve which implies the rank is positive. Thus, 21 is a congruent number (as was shown in the last homework set!). ∎

2. (4 points each) Let $n > 1$ and $a \in \mathbb{Z}$ so that $\gcd(a, n) = 1$.

(a) Define $\mathrm{ord}_n(a)$.

It is the smallest positive integer so that $a^{\mathrm{ord}_n(a)} \equiv 1 (\bmod n)$.

(b) Prove that $a^h \equiv 1 (\bmod n)$ if and only if $\mathrm{ord}_n(a) \mid h$.

Proof: Suppose that $a^h \equiv 1 (\bmod n)$. Write $h = \mathrm{ord}_n(a)q + r$ for $q, r \in \mathbb{Z}$ with $0 \leq r < \mathrm{ord}_n(a)$. We have

$$\begin{aligned} a^r &\equiv a^{\mathrm{ord}_n(a)q} a^r (\bmod n) \\ &\equiv a^{\mathrm{ord}_n(a)q+r} (\bmod n) \\ &\equiv a^h (\bmod n) \\ &\equiv 1 (\bmod n). \end{aligned}$$

However, since $r < \mathrm{ord}_n(a)$ and $r \geq 0$, the definition of $\mathrm{ord}_n(a)$ implies that we must have $r = 0$ and so $\mathrm{ord}_n(a) \mid h$.
Suppose now that $\mathrm{ord}_n(a) \mid h$. There exists $k \in \mathbb{Z}$ so that $h = k\,\mathrm{ord}_n(a)$. Thus,

$$\begin{aligned} a^h &\equiv a^{k\,\mathrm{ord}_n(a)} (\bmod n) \\ &\equiv 1^k (\bmod n) \\ &\equiv 1 (\bmod n) \end{aligned}$$

as desired. ■

(c) Prove that $a^i \equiv a^j (\bmod n)$ if and only if $i \equiv j (\bmod \mathrm{ord}_n(a))$.

Proof: If $i = j$ the statement is trivial. Without loss of generality we can assume $i > j$.
Assume $a^i \equiv a^j (\bmod n)$. Since $\gcd(a, n) = 1$, we can cancel j copies of a to achieve $a^{i-j} \equiv 1 (\bmod n)$. Part (b) then gives that $\mathrm{ord}_n(a) \mid (i - j)$, which is the desired result.
Assume $i \equiv j (\bmod \mathrm{ord}_n(a))$. Then $\mathrm{ord}_n(a) \mid (i - j)$ which implies $a^{i-j} \equiv 1 (\bmod n)$. Multiplying both sides by a^j gives the desired result. ■

(c) Prove that $\{a, a^2, \ldots, a^{\mathrm{ord}_n(a)}\}$ are all incongruent modulo n.

Proof: Suppose $a^i \equiv a^j (\bmod n)$ for some $1 \leq i < j \leq \mathrm{ord}_n(a)$. This implies by part (c) that $i \equiv j (\bmod \mathrm{ord}_n(a)$. However, this is clearly impossible. Thus $\{a, a^2, \ldots, a^{\mathrm{ord}_n(a)}\}$ must all be incongruent modulo n. ■

3. (10 points) Does the congruence $x^2 \equiv 60 (\bmod 83)$ have a solution? Be sure to justify your answer as a "yes" or "no" with no justification will receive 0!

We want to calculate $\left(\frac{60}{83}\right)$ since 83 is a prime. Note that $60 = 2^2 \cdot 3 \cdot 5$. Recalling from class that $\left(\frac{60}{83}\right) = \left(\frac{2^2}{83}\right)\left(\frac{3}{83}\right)\left(\frac{5}{83}\right)$ and applying problem 4 (a), we see that $\left(\frac{60}{83}\right) = \left(\frac{3}{83}\right)\left(\frac{5}{83}\right)$. We use quadratic reciprocity to calculate the second two:

$$\left(\frac{3}{83}\right)\left(\frac{83}{3}\right) = (-1)^{(83-1)(3-1)/4} = -1.$$

We have that $\left(\frac{83}{3}\right) = \left(\frac{2}{3}\right) = -1$. Thus, $\left(\frac{3}{83}\right) = 1$.

$$\left(\frac{5}{83}\right)\left(\frac{83}{5}\right) = (-1)^{(83-1)(5-1)/4} = 1.$$

We have $\left(\frac{83}{5}\right) = \left(\frac{3}{5}\right)$. One can now look at all the squares modulo 5 or apply quadratic reciprocity again to conclude that $\left(\frac{3}{5}\right) = -1$. Thus, $\left(\frac{5}{83}\right) = -1$ and so $\left(\frac{60}{83}\right) = -1$ and so there are no solutions to the given congruence.

4. (4+8 points) **(a)** Prove that $\left(\frac{a^2}{p}\right) = 1$ for all a with $p \nmid a$.

Proof: This is equivalent to showing there is a solution to the congruence $x^2 \equiv a^2 (\operatorname{mod} p)$ with $p \nmid a$. This is clear though, take $x = a$. ■

(b) If $p > 7$ is a prime, prove that there are at least 2 consecutive quadratic residues modulo p. (Hint: Consider 4 and 9. Look at the cases $\left(\frac{5}{p}\right) = 1$ and $\left(\frac{5}{p}\right) = -1$.)

Proof: By part (a) we have $\left(\frac{4}{p}\right) = 1$ and $\left(\frac{9}{p}\right) = 1$ for all primes p with $p > 7$. If $\left(\frac{5}{p}\right) = 1$ we are done with our consecutive quadratic residues being 4 and 5. Suppose $\left(\frac{5}{p}\right) = -1$. Then we have $\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = -\left(\frac{2}{p}\right)$. If $\left(\frac{2}{p}\right) = -1$ then $\left(\frac{10}{p}\right) = 1$ and our consecutive quadratic residues are 9 and 10. If $\left(\frac{2}{p}\right) = 1$, then $\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right) = 1$ and so 8 and 9 are our consecutive quadratic residues. Thus, in all cases we have consecutive quadratic residues. ■