Math 168A: FINAL

William Stein

Due: Friday, Dec 9, 2005, at 5pm

The problems have equal point value, and parts of multi-part problems are of the same value. **You may not talk to anybody about these problems.** *You* are *allowed to use your notes, computer software (show complete session logs), books and web pages. There are 8 problems. This exam is worth 25% of your grade.*

1. Find 13 pairs x, y of rational numbers such that $y^2 + xy = x^3 + 1$. You will only receive half credit if you only find 12 solutions.

2. Let E be an elliptic curve and $P \in E(\mathbb{Q})$ a point. Prove from the definition of the group law that $(P+P)+P = P+(P+P)$. (You may use either the geometric definition involving the chord and tangent procedure or the algebraic formula for the group law from class.)

3. The right triangle with side lengths 33, 56, and 65 has area 924. Find two more right triangles with positive rational sides and area 924.

4. Let a be a positive integer.

   (a) For any prime $p \nmid 6a$, prove that the (projective) curve E_a associated to the equation $y^2 = x^3 + a$ is an elliptic curve. (I.e. check that a certain discriminant is nonzero modulo p.)

   (b) Suppose $p \nmid 6a$ is a prime with $p \equiv 2 \pmod 3$. Prove that E_a has $p+1$ points modulo p, i.e., $\#E_a(\mathbb{F}_p) = p+1$.

5. Consider the following elliptic curve ElGamal cryptosystem (as in the textbook) over the finite field $\mathbb{F}_{97}$ of order 97:

$$\begin{aligned} &E : y^2 = x^3 + x + 3 \\ &B = (51, 3) \qquad \text{(base point)} \\ &n = 17 \qquad\quad \text{(secret)} \end{aligned}$$

   (a) Compute the public key (p, E, B, nB).

   (b) There is a point P on E whose x-coordinate encodes a very special day in December. For some random e, the point P encrypts as

$$(rB, P + r(nB)) = ((28, 62), (63, 85)).$$

   Show how to use knowledge of E, B, n to find P, then find P.

(c) Find a point $P \in E(\mathbb{F}_p)$ with x-coordinate equal to the day of the month when you were born. Then encrypt this point by computing $(rB, P + r(nB))$ for some random value of r.

6. (a) Compute the matrix of T_2 on the following (Victor Miller) basis for $M_{32}(\mathrm{SL}_2(\mathbb{Z}))$:

$$f_1 = 1 + 2611200q^3 + 19524758400q^4 + 19715347537920q^5 + 5615943999897600q^6 + \cdots,$$
$$f_2 = q + 50220q^3 + 87866368q^4 + 18647219790q^5 + 965671206912q^6 + \cdots,$$
$$f_3 = q^2 + 432q^3 + 39960q^4 - 1418560q^5 + 17312940q^6 + \cdots$$

(b) Factor the characteristic polynomial of the matrix of T_2.

(c) Let n be a positive integer. How many of the coefficients of f_1, f_2, and f_3 are needed in order for you to compute the matrix of T_n using the formula for the action of T_n on q-expansions.

7. Compute with $\boldsymbol{\mathcal{M}}_2(\Gamma_0(5))$ explicitly:

(a) Write down the 6 Manin symbols for $\Gamma_0(5)$.

(b) Write down a few 2 and 3 term relations.

(c) Using dimension formulas one can show that $\boldsymbol{\mathcal{M}}_2(\Gamma_0(5))$ has dimension 1 (you do not have to prove this). Find a Manin symbol (c, d) so that every other Manin symbol is a multiple of (c, d) modulo the 2-term and 3-term relations.

(d) Compute the 1×1 matrix of T_2 acting on $\boldsymbol{\mathcal{M}}_2(\Gamma_0(5))$.

(e) Compute the cuspidal subspace $\boldsymbol{\mathcal{S}}_2(\Gamma_0(5))$.

8. There is a basis for $\boldsymbol{\mathcal{S}}_2(\Gamma_0(23))$ such that the Hecke operators T_2 and T_3 with respect to this basis are given by the following matrices:

$$T_2 = \begin{pmatrix} 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & 1 \\ -1 & 2 & -2 & 1 \\ -1 & 1 & 0 & -1 \end{pmatrix}, \qquad T_3 = \begin{pmatrix} -1 & -2 & 2 & 0 \\ 0 & -3 & 2 & -2 \\ 2 & -4 & 3 & -2 \\ 2 & -2 & 0 & 1 \end{pmatrix}$$

Using this show how to write down a basis for $S_2(\Gamma_0(23))$. (Here each basis element should be a q-expansion of the form $a_1q + a_2q^2 + a_3q^3 + \cdots$. Also, I expect you to use the algorithm I described in class that relates $S_2(\Gamma_0(23))$ to homomorphisms $\mathbb{T} \to \mathbb{C}$.)