Math 168A: MIDTERM

William Stein

Due: Wednesday, Oct 26, 2005

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, books and web pages.*

1. Make a conjecture about the set of primes p such that $y^2 = x^3 + x$ has exactly $p + 1$ points modulo p. You do not have to prove your conjecture. You might find the following table helpful:

p	2	3	5	7	11	13	17	19	23	29	31	37	41
N_p	3	4	4	8	12	20	16	20	24	20	32	36	32

p	43	47	53	59	61	67	71	73	79	83	89	97
N_p	44	48	68	60	52	68	72	80	80	84	80	80

2. The point $(1, 1)$ is a solution to the equation

$$3 + 2y + y^2 = x^2 + 2x + 3x^3. \qquad (1)$$

Find three other solutions as follows:

(a) Multiply both sides of the equation by 9 and let $X = 3x$, $Y = 3y$ to obtain an equation of the form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6. \qquad (2)$$

(b) Find the point P on (2) corresponding to the point $(1, 1)$ on (1).

(c) Use the group operation on (2), e.g., via SAGE, to compute several multiples of P.

(d) Use the multiples of P to recover points on (1).

3. The right triangle with rational side lengths $a = 24/5$, $b = 35/12$, $c = 337/60$ has area 7. Find another right triangle with rational side lengths and area 7 as follows (note that none of the sides lengths of this second triangle are allowed to be the same as the side lengths of the above triangle):

(a) Find the point P on $y^2 = x^3 - 49x$ corresponding to the triangle $(24/5, 35/12, 337/60)$ under the bijection from class (see notes from 2005-10-17).

(b) Compute $Q = P + P$ using the elliptic curve group law.

(c) Find the triangle corresponding to Q under the bijection from class.