HOMEWORK 7

DUE 5 JUNE 2015

SHOW ALL YOUR WORK.

1. (a) Find the projection of the affine part with $Z \neq 0$ of the projective point

$$A = [2 : 3 : 5].$$

(b) Write the projective equation for the curve

$$y^2 = x^3 + 5.$$

(c) Write down all three affine equations for the projective curve

$$X^3 + Y^3 + XZ^2 = 5Z^3.$$

In each case, specify the point at infinity.

2. (a) Find the intersection of the lines

$$2x - 3y = 7 \quad \text{and} \quad 2x + 5y = 15.$$

(b) Find the intersection of the lines from (a) in the projective plane.

(c) Find the intersection of the line

$$2x - 4y = 7 \quad \text{and} \quad x - 2y = 3.$$

(d) Find the intersection of the lines from (c) in the projective plane.

(e) Find the intersection of the curves

$$x^2 + y^2 = 1 \quad \text{and} \quad x + y = 1.$$

(f) Find the intersection of the curves from (e) in the projective plane.

3. Consider the elliptic curve

$$y^2 = x^3 + ax + b.$$

Take two distinct points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ on the curve.

(a) Compute the slope of the line through P and Q. What happens if $x_P = x_Q$? How many are there? Do you get the same number of points no matter what P and Q are?

(b) Find all the points where the line through P and Q intersects the curve.

(c) Find the slope of the tangent to the curve at P.

(d) Find all the points where the tangent at P intersects the curve. How many are there? Do you get the same number of points for all P?

4. Take the curve from the previous problem and write it projectively. Now answer the same 4 questions as before.

5. (a) Prove that the line through two rational points is rational.

(b) Prove that the intersection of two rational lines is a rational point (in projective plane).

6. Consider the elliptic curve

$$y^2 = x^3 + 17.$$

(a) Find the point at infinity.

(b) Show that $P_1 = (-2, 3), P_2 = (-1, 4), P_3 = (2, 5), P_4 = (4, 9), P_5 = (8, 23)$ are points on the curve.

(c) Compute the points

$$P_6 = -P_1 + 2P_3 \quad \text{and} \quad P_7 = 3P_1 - P_3.$$

(d) (**Extra credit**) The points $P_1, \ldots, P_7$ have integer coordinates. There is exactly one other point P on this curve with integer coordinates and $y_p > 0$. Find P. (You will probably need a computer, or else a lot of patience.)

7. Suppose $P = (x, y)$ is a point on the elliptic curve

$$y^2 = x^3 + ax + b.$$

(a) Show that the x-coordinate of $2P$ is

$$x(2P) = \frac{x^4 - 2ax - 8bx + a^2}{4y^2}.$$

(b) Derive a similar formula for $y(2P)$.

Hint: Problems 3 and 4 will be useful.

8. Consider the elliptic curve

$$y^2 = x^3 - 43x + 166.$$

(a) Show that the point $P = (3, 8)$ is on the curve.

(b) Compute $2P, 3P, 4P$ and $8P$.

(c) Comparing $8P$ and P, what can you conclude?