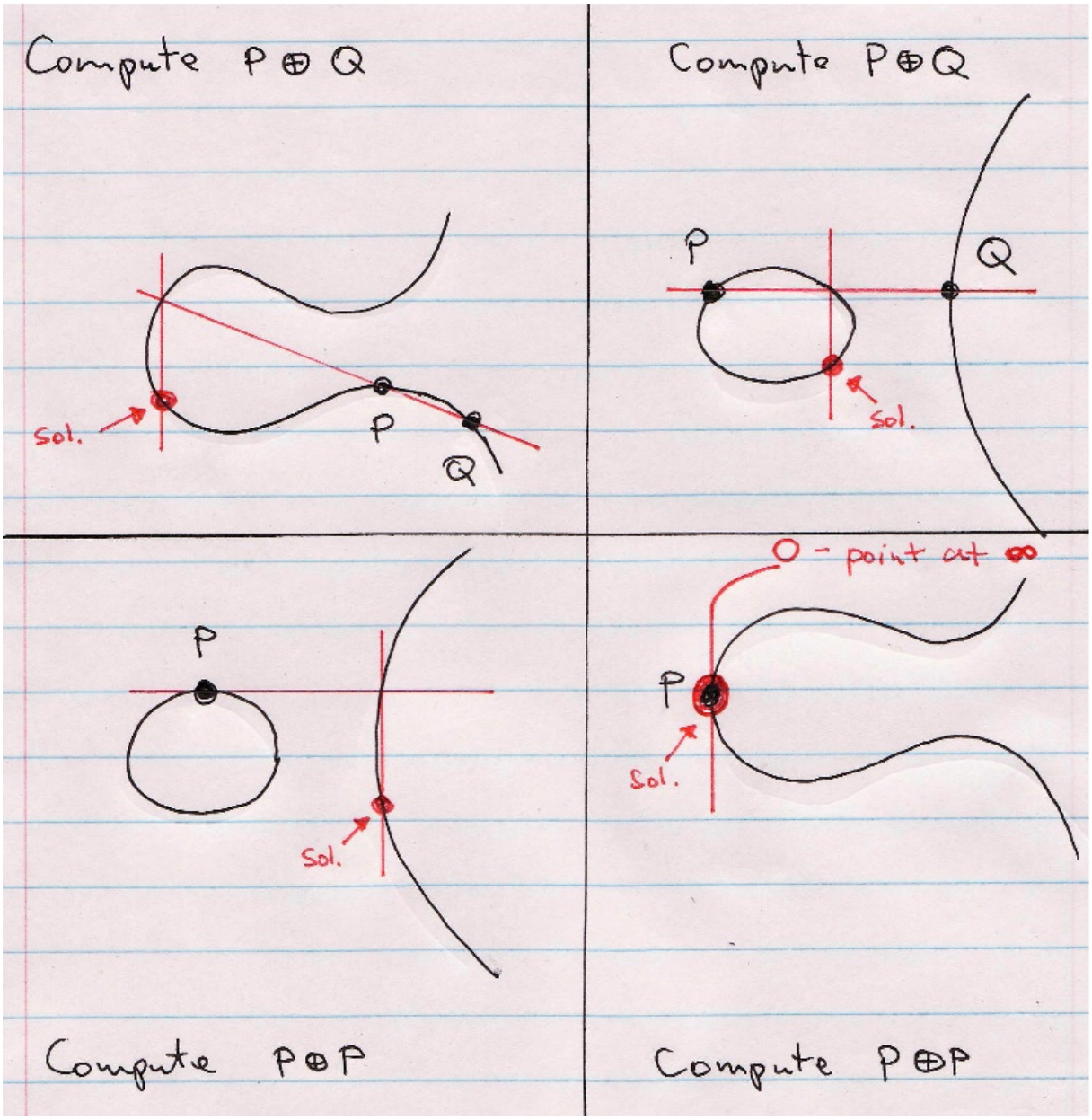
Math 4440 Michael Soltys Test 4 Spring 2008

Name _____ Student No. _____

No aids allowed. Answer all questions on test paper. Use backs of sheets for scratch work. ***Show all your work; there will be no credit for answers without a justification.***

Total Marks 100: four questions, each worth 25.

1. Compute geometrically the addition of the given points.



2. List the elements of $E(\mathbb{Z}_5)$ where the elliptic curve is given by $Y^2 = X^3 + 3X + 3$.
   SOLUTION: $\{\mathcal{O}\} \cup \{(3,2),(3,3)\}$.

3. Describe the ECDLP (Elliptic Curve Discrete Log Problem) and explain briefly why it seems to be a computationally infeasible problem.

   SOLUTION: Given $E, \mathbb{Z}_p, P, Q$, where $P, Q \in E(\mathbb{Z}_p)$, find an n (if it exists) such that $Q = n \cdot P$, where $n \cdot P = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n}$. This problem appears to be infeasible since the n may be very large and a brute-force search would take too long.

4. Suppose that $\mathbb{F}$ is a field and $p, q \in \mathbb{F}[x]$. Show that there exist $k, r \in \mathbb{F}[x]$ such that $p = q \cdot k + r$ where r is either the zero polynomial, or the degree of r is less than the degree of q (i.e., $\deg(r) < \deg(q)$). (Point out where in your proof you use the fact that $\mathbb{F}$ is a field, and not just a ring.)

SOLUTION: We show that this is the case by providing an algorithm that computes k and r. First, set $k = 0$ `&` $r = a$. Clearly, $a = b \cdot k + r$. If the degree of r is less than the degree of b, we are done. Otherwise,

$$b = b_0 + b_1 x + \cdots + b_d x^d$$
$$r = r_0 + r_1 x + \cdots + r_e x^e$$

where $b_d, r_e \neq 0, e \geq d$. Now,

$$a = b \cdot \underbrace{\left(k + \frac{r_e}{b_d} x^{e-d}\right)}_{k'} + \underbrace{\left(r - \frac{r_e}{b_d} x^{e-d} \cdot b\right)}_{r'}$$

and note that the degree of r' is less than the degree of r. If now the degree of r' is less than the degree of b, we are done. Otherwise, we continue. The algorithm terminates by the LNP. We need a field since we must divide by b_d.