MATH 104C: REVIEW EXERCISES FOR EXAM

The following exercises need not be turned in. But you are strongly recommended to do these problems in preparation for the midterm. Moreover, look at old homework problems, and related problems in the book.

The following exercise deals with reduction mod p for rational points on an elliptic curve $E : y^2 = x^3 + ax^2 + bx + c$. We use projective coordinates $[X, Y, Z]$ for points in $\mathbf{P}^2(\mathbf{Q})$, where $[aX, aY, aZ] = [X, Y, Z]$ for any nonzero scalar a. As usual, we identify $\mathbf{Q}^2$ with the subset $[X, Y, 1]$, $X, Y \in Q$ of $\mathbf{P}^2(\mathbf{Q})$. One defines $\mathbf{P}^2(\mathbf{F}_p)$ similarly, where we now consider elements in the finite field $\mathbf{F}_p$ of p elements, i.e. we consider the numbers mod p. Finally, recall that we define reduction mod p for a point $P = (\frac{A}{B^2}, \frac{C}{B^3})$, where $gcd(A, B, C) = 1$, by identifying it with $[AB, C, B^3]$ in $\mathbf{P}^2(\mathbf{Q})$, and doing the usual reduction mod p there.

1. In the following, we always assume that the prime p does not divide the discriminant Δ of the given elliptic curve.
   (a) Show that if $p \not| B$, then the reduction mod p of the point P as above is given by (AB^{-2}, CB^{-3}) mod p, where B^{-1} is the inverse of B mod p.
   (b) Show that if $p|B$ then the reduction of P mod p is $[0, 1, 0]$ in projective coordinates, which corresponds to our point ∞.
2. Let P be a rational point on an elliptic curve which is not a torsion point, i.e. $kP \neq \infty$ for all k. Show that for a given prime number p which does not divide the discriminat there exists a number k such that $p|B_k$, where $kP = (\frac{A_k}{B_k^2}, \frac{C_k}{B_k^3})$, with $gcd(A_k, B_k, C_k) = 1$. You may assume that kP can always be written in such a way.
3. (a) Find the inverse map of $a \mapsto a^7$ mod 77, where $a \in \mathbf{Z}_{77}^*$, i.e. $gcd(a, 77) = 1$. *Hint* : The inverse map is of the form $a \mapsto a^f$ for some suitable number f. We have considered a similar problem before for numbers mod p.
   (b) Explain why it is difficult to find the inverse of the map $a \mapsto a^e$ for $a \in \mathbf{Z}_n^*$ if one only knows n, but not its factorization if $n = pq$ is the product of two large primes. This is the principle by which the RSA public key system works.
   (c) See also problems 3.6 and 3.7 on page 177 in the electronic book by Hoffstein, Pipher and Silverman, chapter 3, mentioned on the course web page. You can download it from our library at roger@ucsd.edu (search for one of the authors).
3. Is the point $(2, 1)$ a torsion point of $E : y^2 = x^3 - 2x + 5$?
4. Do Problem 41.5 in Silverman's Friendly Introduction.

You can use results of previous sections for solving later sections regardless whether you could do the problem or not. Please ask if you are confused about anything. I should be able to read email while I am away.