A. Student

Math 124 Problem Set 9

I chose problems 2-5;

2. The first step is to transform the elliptic curve into the form $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Z}$. The first problem of the previous problem set describes a method to transform the curve into the desired form, with rational coefficients. Clearing denominators gives the following curve:

$$Y^2 = X^3 + 27(48a_4 - 1)X + 27(12^3 a_6 - 144a_4 + 2),$$

where $a_4 = -8369487776175$ and $a_6 = 9319575518172005625$. The discriminant Δ is

$$1009310191436363411578571211896385085440000000 = 2^{18} \cdot 3^{18} \cdot 5^6 \cdot 13^6 \cdot 23^6 \cdot 61^2 \cdot 67^2 \cdot 73^2.$$

Therefore for Lutz-Nagell we must try over 50000 values of Y, since $Y^2 | \Delta$. (Even after we find the element of order 2 corresponding to $Y = 0$ we must go through these computations until perhaps the group attains maximal size for Mazur's theorem). For each Y we check if there is an integer X such that $[X, Y]$ is on the elliptic curve. If it is, we must check that the point indeed has finite order. Once we have the elements of the torsion subgroup, we must deduce its structure using Mazur's theorem. PARI's elltors function computes the torsion subgroup quickly using Doud's algorithm. For the above it finds that the torsion subgroup is isomorphic to $\mathcal{C}_{\not{x}}\mathcal{C}_{\in}$, with $[83058483, 326936156040]$ generating the cyclic subgroup of order 6, and $[60091419, 0]$ having order two.

3i. We write a PARI program to count the number of points in each group (including the point at infinity):

$ecount(p) = c = 0; (for(x = 0, p - 1, for(y = 0, p - 1, if((y^2 - (x^3 + 1))\%p == 0, c + +))));$

$write(\text{“}9 - 2ans.txt\text{”}, p\text{“”}c + +);$

$ecount2(n) = for(x = 3, n, ecount(prime(x)));$

Then $ecount2(10)$ yields (29 is the tenth prime):

p	5	7	11	13	17	19	23	29
N_p	6	12	12	12	18	12	24	30

3ii. It seems that if $p \equiv 2(mod\ 3)$, $N_p = p + 1$.

3iii. *Claim.* If p is a prime such that $p \equiv 2(mod\ 3)$, then $\phi(x) = x^3$ defines an automorphism on $(\mathbb{Z}/p\mathbb{Z})^*$.

Proof. Clearly ϕ is a homomorphism. We just need to check that $ker\ \phi$ is trivial. If not, then by Lagrange 3 divides $|(\mathbb{Z}/p\mathbb{Z})^*|$. However, since $p \equiv 2(mod\ 3)$ and $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$ this is impossible.

In particular, the claim shows that x^3 gives a bijection on $\mathbb{Z}/p\mathbb{Z}$; it follows that for every x in the field there is a y such that $y = x^3 + 1$. Adding the point of infinity gives $p + 1$ points, proving the conjecture.

4. We use Lutz-Nagell to find the torsion subgroup of the elliptic curve defined by $y^2 = x^3 + px$, where p is prime. The discriminant $\Delta = -64p^3$ in this case. Therefore either $y = 0$, in which case x must also be 0, and $(0, 0)$ has order two, or $y^2 = x^3 + px| - 64p^3$, where $x, y \in \mathbb{Z}$.
Write $y^2 = x(x^2 + p)$, and note that the only nontrivial factors of $-64p^3$ are 2 and p. If $p = 2$ then $x(x^2 + 2)$ contains an odd factor for $x \neq 0$, so $y^2 \nmid -512$. Therefore suppose that $p \neq 2$.
If $p \nmid x$ then x must be a power of 2. If $x = 1$ then $p = y^2 - 1$, so p must be 3, and we have points $[1, \pm 2]$, which PARI easily verifies are not in the torsion subgroup. Otherwise $x \geq 2$, but since $p \nmid x^2 + p$ and it is odd, $x^2 + p \nmid \Delta$. Therefore suppose that $p|x$.
Write $x = \alpha p$. Then $y^2 = \alpha p^2(\alpha^2 p + 1)|64p^3 \Rightarrow \alpha(\alpha^2 p + 1)|64p$, from which we deduce that $\alpha = p$. At this point we easily verify there are no solutions to $p^3 + 1|64$. Therefore the torsion subgroup contains two elements, the point of infinity and $[0, 0]$.

5i. Any finite set of points generates a countable set (since coefficients are over $\mathbb{Z}$). Therefore, since $E(\mathbb{R})$ is uncountable, it cannot be a finitely generated abelian group.
5ii. The cardinality of $E(k)$ is finite; automatically this means it is finitely generated.