Short Homework Assignment 8: Elliptic Curves II
Due **Monday** November 25

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2002**

There are only two problems.

1. (2 points) Prove that $\mathbb{R}/\mathbb{Z}$ is not finitely generated.

2. If $a, b \in \mathbb{Z}/p$ and $4a^3 + 27b^2 \neq 0$, then MAGMA can easily compute the group $E(\mathbb{Z}/p)$ associated to the elliptic curve defined by $y^2 = x^3 + ax + b$. Here's an example:

```
> AbelianGroup(EllipticCurve([GF(7)|1,3]));
Abelian Group isomorphic to Z/6
Defined on 1 generator
Relations:
6*$.1 = 0
```

   (a) (2 points) Find a prime p and $a, b \in \mathbb{Z}/p$, so that the group $E(\mathbb{Z}/p)$ associated to $y^2 = x^3 + ax + b$ is not a cyclic group. (Hint: Just try a, b, p at random...)

   (b) (5 points) Let Φ be the set of the fifteen possible torsion subgroups of elliptic curves over $\mathbb{Q}$. For each group $G \in \Phi$, find a prime p and $a, b \in \mathbb{Z}/p$ such that $G \cong E(\mathbb{Z}/p)$. Hint: Systematically list the groups that occur. You might find the MAGMA commands illustrated below useful:

```
> IsEllipticCurve([GF(3)|0,1]);
false
> Invariants(AbelianGroup(EllipticCurve([GF(3)|1,0])));
[ 4 ]
```

   (c) (2 points) Suppose $n > 1$ is an integer. Make a guess about whether or not $\mathbb{Z}/n$ must be isomorphic to a group $E(\mathbb{Z}/p)$ for some elliptic curve over some finite field $\mathbb{Z}/p$. Support your guess with evidence.