Lab 2 – Elliptic Curves in Sage

Problem 1: After a change of variables, an elliptic curve over a field k is a curve defined by the equation

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

where $a, b \in k$ and $-16(4a^3 + 27b^2) \neq 0$ this is called the Weierstrass form). In general an elliptic curve is of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and is constructed in Sage via the command

```
EllipticCurve([a1,a2,a3,a4,a6])
```

In the space below, sketch the elliptic curve $y^2 = x^3 - 5x + 4$ by typing the following into Sage (if the elliptic curve is in Weierstrass form, you can construct it via `E = EllipticCurve[(a,b)]`.

```
E = EllipticCurve([-5,4])
P = E.plot()
```

Also sketch an example where $-16(4a^3 + 27b^2) = 0$ (you can't use the same code as above to do this, you'll need to plot using the regular plot command).

Problem 2: By default, Sage makes an elliptic curve over $\mathbf{Q}$. In Sage, the field $\mathbf{Z}/p\mathbf{Z}$ is denoted $GF(p)$. In the space below, sketch the elliptic curve $y^2 = x^3 + x$ over $\mathbf{Z}/37\mathbf{Z}$.

Problem 3: For each prime $5 \leq p < 50$ let M_p be the number of points on the elliptic curve $y^2 = x^3 + 1$ over $\mathbf{Z}/p\mathbf{Z}$ (don't forget the point at infinity!). For the set of primes $p \equiv 2 \pmod 3$, what is the value of M_p? Try to prove your conjecture (this might be hard).

Problem 4: In this problem you will verify the Taniyama Shimura Theorem (this is what Wiles proved to prove Fermat's Last Theorem) for a particular curve. Let E be the elliptic curve $y^2 = x^3 - 4x^2 + 16$. Compute M_p for primes up to 100. Also, let

$$F(q) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + \cdots$$

and write

$$F(q) = \sum_{n=1}^{\infty} N_n q^n..$$

For primes up to 13, compute $N_p + M_p$. Make a conjecture as to what the value should be. Here's the best way to compute $F(q)$: Construct the elliptic curve E over $\mathbf{Q}$. Then enter

```
f = E.modular_form()
f.qexp(100)
```

will give you N_n for n up to 100.