Math 7770 Spring 2011
Homework 8
Due: March 28, 2011

You are welcome to work together but everyone needs to write up **distinct** solutions. If you use any books outside of our textbook or other people, please make sure to give them credit. Make sure your solutions are complete. If your handwriting is atrocious, I am happy to give you a basic introduction to LaTeX.

Warmup

- §5.6 # 10. Show that the cubic curve $y^2 = 4x^3 + x^2 - 2x + 1$ is non-singular. Note that this curve contains the four rational points $(0, \pm 1)$, $(1, \pm 2)$. Apply the chord-and-tangent method to (a couple of) these points and note the results.
- Compute the group $E(\mathbb{F}_p)$ for the curve $E : y^2 = x^3 + x + 1$ and the primes $p = 3, 7, 11, 13$.
- The ring $\{0, 2, 4, 6, 8\}$ under addition and multiplication modulo 10 has a multiplicative identity. Find it.
- Find an integer n so that $\mathbb{Z}/n\mathbb{Z}$ does not have the following properties (which are all properties that $\mathbb{Z}$ *does* have).
  - $a^2 = a$ implies $a = 0$ or $a = 1$
  - $ab = 0$ implies $a = 0$ or $b = 0$
  - $ab = ac$ and $a \neq 0$ imply $b = c$
- Show that the three properties in the previous problem are *valid* for $\mathbb{Z}/p\mathbb{Z}$ when p is prime.

Challenge

In class last week I mentioned that part of the proof of Fermat's Last Theorem was an idea of Gerhard Frey in the early 1980s (which was completed in 1986 by the proof of a conjecture of Jean-Pierre Serre by Ken Ribet) that a solution to equations $x^n + y^n = z^n$ for $n \geq 3$ in integers would imply the existence of an elliptic curve so special it couldn't possibly exist. This idea that the elliptic curve couldn't exist is called the "Taniyama-Shimura-Weil" conjecture (or some subset of those three names depending on the reference). And this result is basically what Andrew Wiles proved in 1995. (He didn't really prove it for all elliptic curves, he proved it for a subset which was sufficient to imply Fermat's Last Theorem. The other cases have since been proven too.)

This exercise proves a very special case of this theorem. Again, some of these parts are particularly difficult and may require outside knowledge. Feel free to ask for clarification. The $\Phi(z)$ defined below is called *a modular form of weight* 2. Modular forms are a very active current research area in mathematics (and number theory in particular).

(a) Let E be the cubic curve given by the equation

$$E : y^2 = x^3 - 4x^2 + 16.$$

Let $M_p = \#E(\mathbb{F}_p)$ be the number of points on E over the field $\mathbb{F}_p$. Calculate M_p for all primes $3 \leq p \leq 13$. (If you have a way to compute this with computers, compute it up to $p \leq 100$.)

(b) Let $F(q)$ be the formal power series given by the infinite product

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

Let N_n be the coefficients of q^n in $F(q)$ where

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

Calculate N_n for $n \leq 13$. (Again, if you have a way to compute this with computers, compute it up to $n \leq 100$.)

(c) For each prime p, compute the sum $M_p + N_p$ of the quantities calculated in (a) and (b). Formulate a conjecture as to what this value should be in general.

(d) Prove your conjecture in (c) is correct. (This part is not necessary to continue.)

(e) If we replace the indeterminate q by the quantity $e^{2\pi iz}$ we obtain a function

$$\Phi(z) = F(e^{2\pi iz}) = e^{2\pi iz}\prod_{n=1}^{\infty}\left(1-e^{2\pi inz}\right)^2\left(1-e^{2\pi i11nz}\right)^2.$$

Prove that $\Phi(z)$ is a holomorphic function on the upper half plane $\mathfrak{h} = \{z = x + iy \in \mathbb{C} \mid y > 0\}$. Also prove that

$$\lim_{y\to\infty}\Phi(x+iy) = 0.$$

(f) Prove that for every prime p except $p = 11$, the function $\Phi(z)$ satisfies the relation

$$N_p\Phi(z) = \Phi(pz) + \sum_{j=0}^{p}\Phi\left(\frac{z+j}{p}\right) \quad \text{for all } z \in \mathfrak{h}.$$

Prove that if a, b, c, d are integers satisfying $ad - bc = 1$ and $c \equiv 0 \bmod 11$ then

$$\Phi\left(\frac{az+b}{cz+d}\right) = (cz+d)^2\Phi(z) \quad \text{for all } z \in \mathfrak{h}.$$