Homework #11 Due Wednesday May 3 (last one!):

Below, $\mathbb{F}_p$ denotes the field with p-elements, e.g. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

1. Are there countable subgroups of S^1 which are not finitely generated? (In other words, can you prove Mordell's Theorem just by using that $C(\mathbb{Q})$ is a countable subgroup of $C(\mathbb{R}) = S^1$ or $S^1 \oplus \mathbb{Z}/2\mathbb{Z}$).

2. Let Λ be a lattice in $\mathbb{C}$.

   (a) Show that the series defining the Weierstrass function $\wp_\Lambda$ is absolutely convergent on $\mathbb{C} - \Lambda$.

   (b) Prove that $\wp$ is an even function, that is $\wp(-u) = \wp(u)$.

   (c) Prove that $\wp$ is a doubly periodic function; that is, show that

   $$\wp(u + \omega) = \wp(\omega) \quad \text{for every} \quad u \in \mathbb{C}, \omega \in \Lambda.$$

   Hint: First prove that $\wp'$ is periodic, then integrate. If you don't know any complex analysis, you may skip part (c).

3. Let C be the elliptic curve defined by $y^2 = x^3 + 1$.

   (a) For each prime $5 \leq p < 30$, describe the group of points on the curve $C(\mathbb{F}_p)$.

   (b) For each prime in (a), let M_p be the number of points in the group (don't forget the point at infinity). For the set of primes $p \equiv 2 \mod 3$, can you see a pattern for the values of M_p? Make and prove a general conjecture for the value of M_p witn $p \equiv 2 \mod 3$.

   (c) Generalize your result in part (b) to curves of the form

   $$y^2 = x^3 + c$$

   and primes $p \equiv 2 \mod 3$ where $c \not\equiv 0 \mod p$.

4. This exercise is a special case of a result of Eichler and Shimura. It proves a special case of the Taniyama-Shimura-Weil conjecture.

   (a) Let C be the elliptic curve given by

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

   As usual, $M_p = \#C(\mathbb{F}_p)$ be the number of points on C over the field F_p. Calculate M_p for all primes $3 \leq p \leq 13$. If you love your (or someone else's) computer, you can go farther.

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

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

Let N_n be the coefficient of q^n in $F(q)$,

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

Calculate N_n for $n \leq 13$.

(c) For each p in part (a) compute the sum $M_p + N_p$. Formulate a general conjecture of what this sum should be. If you like, you can try to prove your conjecture (this is difficult).

Remarks: Replacing q by $e^{2\pi iz}$ we get a function

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

This is a homomorphic function on the upper-half plane $\mathbb{H}^2$. In fact, its a modular form of weight 2 associated to the congruence subgroup $\Gamma_0(11)$.

It turns out that N_p is encoded in Φ, that is

$$N_p\Phi(z) = \Phi(pz) + \sum_{j=0}^{p} \Phi\left(\frac{z+j}{p}\right).$$

Thus, assuming your conjecture in part (c), this modular form encodes M_p!