MATH 844: HOMEWORK 4, DUE NOV 17.

1. Let E be the elliptic curve over $\mathbf{Q}$ with equation $y^2 = x^3 + 16$. Let $L_p(E, s)$ denote the Euler factor at the prime p of the L-series of E.

(a) Show that E has good reduction at every prime $p \neq 3$. What is $L_3(E, s)$?

Let ω be a primitive cube root of 1. If p is a rational prime $\neq 3$, then the ideal of $\mathbf{Z}[\omega]$ it generates either factors into a product of two prime, principal ideals (if $p \equiv 1 \pmod 3$) or is itself a prime ideal (if $p \equiv 2 \pmod 3$).

(b) Show that for $p = 2, 5, 7$,

$$(*) \quad L_p(E, s) = \prod_{\wp} (1 - \alpha_{\wp}^{\deg(\wp)} (N\wp)^{-s})^{-1},$$

where the product is over the (one or two) prime ideals above in the factorization of $p\mathbf{Z}[\omega]$, where $N\wp = |\mathbf{Z}[\omega]/\wp|$, and $\alpha_{\wp}^{\deg(\wp)}$ is the unique generator of $\wp$ such that $\alpha_{\wp}^{\deg(\wp)} \equiv 1 \pmod 3$.

(c) Prove that if p is an odd prime such that $p \equiv 2 \pmod 3$, then $|E(\mathbf{F}_p| = p+1$. Explain how if $(*)$ is true for all primes $p \neq 3$, then we get a formula for $|E(\mathbf{F}_p)|$.

2. (a) Show that $ab(a - b)(a + b)$ is a congruent number if $a > b$ are positive integers.

(b) Find the density of squarefree odd positive integers among all odd positive integers.

(c) Deduce that there are infinitely many triples of consecutive odd positive integers that are squarefree.

(d) Deduce that there are infinitely many squarefree congruent numbers.

(e) If E is the elliptic curve over $\mathbf{Q}$ given by the equation $y^2 = f(x)$, its quadratic twists are the curves $E_d : \ dy^2 = f(x)$. Show that E and E_d have the same j-invariant. Find an E of rank 0, which has infinitely many non-isomorphic quadratic twists of rank > 0.