Math 3H03 (Number Theory)
Due: March 13, 2020

Homework Assignment 7

All of the questions from Part A will be graded. For Part B, do questions 3 and 4, one of which will be graded completely and the other for completion. Assignments will be submitted via *Crowdmark*.

Part A. [Short Questions; 4pts]

Exercise 1. Find all the units of $\mathbb{Z}_{30}$.

Exercise 2. Prove that $a^{37} \equiv a \pmod{1729}$ for all integers a. [HINT: $1729 = 7 \cdot 13 \cdot 19$.]

Part B. [Proof Questions; 6pts]

Exercise 3. Prove that if $\gcd(m, n) = 1$, then $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$.

Exercise 4. Suppose that $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ with all the primes p_i distinct. Show that $\phi(n) \geq n/2^r$.

Bonus. Consider the elliptic curve E given by $y^2 = x^3 + 1$. Show that the only *integer* pairs (a, b) that satisfy this equation are $(-1, 0), (0, \pm 1)$, and $(2, \pm 3)$. [HINT: you will need Catalan's conjecture (now a theorem) to prove this!]