Due Wednesday, September 22 at the beginning of class. All chapter and exercise numbers refer to Silverman's *A Friendly Introduction to Number Theory*, 4th edition.

(1) Suppose $a, m, n \in \mathbb{N}$. Use the Euclidean algorithm to prove $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$.

(2) The *Riemann zeta function* $\zeta(s)$ is given by the formula

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

when $s > 1$. Use the fundamental theorem of arithmetic to prove $\zeta(s)$ can also be written as

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

when $s > 1$. (Note: $\prod$ is an *infinite product.* Hint: Expand each term in the product using the formula for the sum of a geometric series.)

(3) Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients and $a_n \neq 0$. Suppose $p(r/s) = 0$, where r and s are integers such that $\gcd(r, s) = 1$. The *rational root theorem* states that $r \mid a_0$ and $s \mid a_n$.

(a) Prove the rational root theorem. (Hint: set $p(r/s) = 0$ and clear denominators.)

(b) Use the rational root theorem to prove $\sqrt{2}$ and $\sqrt[5]{9}$ are irrational.

(c) Suppose $m, n \in \mathbb{N}$ and $\sqrt[n]{m}$ is rational. Prove that $\sqrt[n]{m}$ is in fact an integer.

(4) Show that every odd prime p may be written uniquely as a difference of squares, i.e. there exists a unique pair $(a, b) \in \mathbb{N}^2$ with $a > b$ such that $p = a^2 - b^2$.

(5) Ex. 8.2

(6) Ex. 8.4(d)–(e)

(7) Ex. 9.2

(8) Ex. 9.3. Additionally, prove a formula for the value of $(m-1)! \bmod m$ when m is composite.

(9) Find the last digits in the ordinary decimal representations of 2^{400} and 3^{400}.

(10) Suppose p is a prime other than 2 or 5. Prove that p divides infinitely many of the integers 1, 11, 111, 1111, ...