Due Wednesday, September 29 at the beginning of class. All chapter and exercise numbers refer to Silverman's *A Friendly Introduction to Number Theory*, 4th edition.

(1) Let p be a prime. Recall that $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ when $0 \le k \le n$.

(a) Show $\binom{p-1}{k} \equiv (-1)^k \bmod p$ when $0 \le k \le p-1$.

(b) Show $\binom{p}{k} \equiv 0 \bmod p$ when $1 \le k \le p-1$.

(c) Prove that if $a^p \equiv b^p \bmod p$, then $a^p \equiv b^p \bmod p^2$.

(2) Let p be an odd prime.

(a) Show that $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \bmod p$. (Hint: apply the result of Ex. 9.2 from Problem Set 2.)

(b) Show that $x^2 \equiv -1 \bmod p$ has a solution if $p \equiv 1 \bmod 4$.

(c) Prove the converse: if $x^2 \equiv -1 \bmod p$ has a solution, then $p \equiv 1 \bmod 4$. (Hint: raise both sides to a power and apply Fermat's Little Theorem.)

(3) If $\gcd(a, n) = 1$, we define the *order* of the number $a \bmod n$ to be the least natural number k such that $a^k \equiv 1 \bmod n$. For example, the order of $3 \bmod 8$ is 2 since $3^2 \equiv 1 \bmod 8$.

(a) Determine the orders of the following numbers.

(i) $2 \bmod 27$

(ii) $14 \bmod 31$

(b) Show that the order of $a \bmod n$ divides $\varphi(n)$.

(c) Explain why order is not defined if $\gcd(a, m) > 1$.

(4) Ex. 11.2

(5) Ex. 11.3. Additionally, prove that if $d \mid n$, then $\varphi(d) \mid \varphi(n)$.

(6) Ex. 11.13