Directions: Solve the following 6 problems. For computer problems, complete solutions include source code, an **English language overview** of your code, and the final answer. The overview should be sufficiently complete that an intelligent reader with no prior access to your code will understand how it works. See the course syllabus and the Homework Webpage on the course website for general directions and guidelines.

1. [NT 5-2.{9,10}]

   (a) Prove that if p is a prime and $p \equiv 1 \pmod 4$, then $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p$.

   (b) Use the above to find a solution for each of the following.

      i. $x^2 \equiv -1 \pmod{13}$

      ii. $x^2 \equiv -1 \pmod{17}$

2. [NT 5-3.4]

   (a) Prove that for each n, there are n consecutive integers, each of which is divisible by a perfect square larger than 1.

   (b) Using your proof above, explicitly find 3 consecutive integers, each of which is divisible by a perfect square larger than 1. In your answer, give the integers as well as the corresponding perfect squares.

3. [NT 6-4.2] Prove that if $f(n)$ is multiplicative, then $\sum_{d|n} \mu(d)f(d) = \prod_{p|n} 1 - f(p)$.

4. Primitive Roots.

   (a) [NT 7-1.1] Find all primitive roots modulo 5, modulo 9, modulo 11, modulo 13, and modulo 15.

   (b) Let a and m be positive, relatively prime integers. Let S be the set of primes dividing $\phi(m)$. Prove that if $a^{\phi(m)/p} \not\equiv 1 \pmod m$ for each $p \in S$, then a is a primitive root of m.

5. [NT 8-1.4] Modify the proof of Theorem 8–1 to prove that there exist infinitely many primes congruent to $5 \pmod 6$.

6. The prime number counting function.

   (a) In class, we proved that $\pi(2n) \leq \ln(4) \cdot \frac{n}{\ln n} + \pi(n)$ for $n \geq 2$. Prove by induction that $\pi(2^t) \leq 6\frac{2^t}{t}$ for $t \geq 1$. *Hint:* establish the base cases $t = 1$ and $t = 2$ directly, and the case $t \geq 3$ in the inductive step. *Note:* using additional base cases, we could reduce the constant 6.

   (b) Prove that $\pi(n) \leq C\frac{n}{\ln n}$ for some constant C.