Exercises

1. Find a complete set of mutually in-congruent solutions of each of the following. If there is no solution, prove the solution does not exit.

   (1) $5x \equiv 4 \pmod{51}$.

   (2) $6x \equiv 8 \pmod{51}$.

   (3) $6x \equiv 3 \pmod{39}$.

2. If exists, find a^{-1}, the inverse of a modulo m. Otherwise, prove it does not exist.

   (1) $a = 2$ and $m = 5$;

   (2) $a = 4$ and $m = 9$;

   (2) $a = 6$ and $m = 9$;

3. Let $f(x)$ be a polynomial with integer coefficients. Prove that if $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$. (Hints: use properties of congruences.)
4. Prove that: if $a \equiv b \pmod{m}$, then $\gcd(a, m) = \gcd(b, m)$.
5. Prove that: if p is a prime and $a^2 \equiv b^2 \pmod{p}$, then $p \mid (a + b)$ or $p \mid (a - b)$.
6. Find a complete set of mutually in-congruent solutions to the equation $x^2 \equiv 1 \pmod{20011}$ where 20011 is a prime.
7. Prove that: if $x^2 \equiv x \pmod{p^e}$ for some positive integer e, then $x \equiv 0, 1 \pmod{p^e}$.
8. Let m be a positive modulus. Prove if the following statement is true. Otherwise find a counter-example.

$$ab \equiv 0 \pmod{m} \implies a \equiv 0 \pmod{m} \text{ or } b \equiv 0 \pmod{m}.$$

9. Prove that $n^2 - 1$ is divisible by 8 for all odd integers n.