9. Introductory Number Theory

1. For a and b given below, find q and r such that $a = qb + r$ and $0 \leq r < b$.
   (a) $a = 10$, $b = 3$.
   (b) $a = -84$, $b = 5$.
   (c) $a = 75$, $b = 5$.
   (d) $a = -66$, $b = 11$.
2. The C programming language uses `%` for the mod operation. However if you calculate `-12 % 5` in C, it returns `-2`. Explain why this is a problem if you are a mathematician.
3. Prove that $a \equiv b \pmod{n}$ is an equivalence relation.
4. What are the equivalence classes of $a \equiv b \pmod{n}$?
5. Calculate $\gcd(a, b)$ for:
   (a) $a = 20$, $b = 25$.
   (b) $a = 203$, $b = 56$.
   (c) $a = -453$, $b = -36$.
   (d) $a = 17$, $b = 15$.
   (e) $a = 24$, $b = 0$.
6. For each of the above pairs of numbers, find x and y such that $ax + by = \gcd(a, b)$.
7. Let a and n be relatively prime. Prove that there is some b such that $ab \equiv 1 \pmod{()}n)$.
8. Disprove: If p is prime, then given any integer a, a and p are relatively prime.
9. Calculate the following:
   (a) $5 + 6 \pmod{8}$.
   (b) $7 - 16 \pmod{19}$.
   (c) $-3 \pmod{5}$.
   (d) $7 \times 5 \pmod{12}$.
   (e) $-(4 \times 2) \pmod{7}$.
   (f) $6 \times 8 \pmod{12}$.
10. Write out the addition and multiplication tables $\pmod{4}$.
11. Write out the multiplication table $\pmod{7}$.
12. Find the inverses of 1, 2, ..., 6 $\pmod{7}$.
13. Prove that if a is invertible $\pmod{n}$, then a^{-1} is invertible $\pmod{n}$ and $(a^{-1})^{-1} = a \pmod{n}$.
14. Find $27^{-1} \pmod{41}$.
15. Find all solutions of $x^2 = 1 \pmod{3}$.
16. A field is a mathematical object $\mathbb{F} = (F, +, \times, 0, 1)$, where F is a set, $+ : F \times F \to F$ and $\times : F \times F \to F$ are functions, and $0, 1 \in F$, which satisfies the following conditions:
    (a) for all x, $y \in F$, $x + y = y + x$.
    (b) for all x, y, $z \in F$, $x + (y + z) = (x + y) + z$.
    (c) for all $x \in F$, $x + 0 = x$.
    (d) for all $x \in F$, there is some $y \in F$ such that $x + y = 0$ (we usually write $y = -x$).
    (e) for all x, $y \in F$, $x \times y = y \times x$.
    (f) for all x, y, $z \in F$, $x \times (y \times z) = (x \times y) \times z$.
    (g) for all $x \in F$, $x \times 1 = x$.
    (h) for all $x \in F$ such that $x \neq 0$, there is some $y \in F$ such that $x \times y = 1$ (we usually write $y = x^{-1}$).
    (i) for all x, y, $z \in F$, $x \times (y + z) = x \times y + x \times z$.

    The real numbers, complex numbers, and rational numbers are all examples of fields. Prove that $\mathbb{Z}_n$ is a field if and only if n is prime.