Problem Set #2

1 Order on \( \mathbb{Z} \)

Exercise 1:
Prove that in any unitary commutative ordered ring \( R \), for any \( x, y \in R \):
1. \( x > y \Rightarrow x + c > y + c \), for all \( c \in R \).
2. \( x \neq 0 \Rightarrow x^2 > 0 \).
3. If \( a > 0 \) and \( b > 0 \) then \( a > b \Leftrightarrow a^2 > b^2 \). (Hint : \( (b^2 - a^2) = (b - a)(b + a) \). Use Rule of Sings).

2 Equivalence relation on sets

Exercise 2:
For \( n > 1 \) define \( a \equiv b(\text{mod} \ n) \) to mean
\[ b - a \text{ is an integer multiple of } n \]
Verify that this is an RST relation on \( X = \mathbb{Z} \).

3 Induction

Exercise 3:
Prove \( n^2 = (\text{sum of first } n \text{ odd integers}) = \sum_{k=1}^{n}(2k - 1) = 1 + 3 + \cdots + (2n - 1) \).

4 Integers

4.1 Absolute value

Exercise 4:
Prove
\[ |x + y| \leq |x| + |y| \]
in any commutative ordered ring \( R \).
4.2 Divisibility in the system of integers

4.2.1 GCD

Exercise 5:
1. Prove \( \gcd(a, b) = \gcd(b, a) \) for \( a, b \neq 0 \).
2. If \( k \in \mathbb{Z} \) is fixed and \( a, b \neq 0 \) prove that \( \gcd(a, b) = \gcd(a + kb, b) \).
3. If \( a, b > 0 \) and \( a \) divides \( b \), show that \( \gcd(a, b) = a \).

Exercise 6:
Taking \( a = 955, b = 11422 \), use the extended GCD extended to find first \( \gcd(955, 11422) \) and find \( r, s \in \mathbb{Z} \) such that \( ra + sb = \gcd(955, 11422) \).

Exercise 7:
Generalize the definition of \( \gcd \) to define \( \gcd(a_1, \ldots, a_r) \), where \( a_i \) are nonzero. Make the obvious changes in the definition of \( \gcd(a, b) \) and
1. Prove \( c = \gcd(a_1, \ldots, a_r) \) exits by considering the set of integer linear combinations
   \[
   \Gamma = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_r = \{ \sum_{i=1}^{r} k_i a_i : k_i \in \mathbb{Z} \}
   \]
   Show that \( \Gamma \cap \mathbb{N} \neq \emptyset \) and verify that the smallest element \( c \in \Gamma \cap \mathbb{N} \) (which exists by the Minimum principle) has a properties required of \( \gcd(a_1, \ldots, a_r) \).
2. Show that \( \Gamma = \mathbb{Z}c \) all integer multiples of \( \gcd(a_1, \ldots, a_r) \).

Exercise 8:
If \( a, b \neq 0 \) and \( u_1, u_2 \) are units in \( \mathbb{Z} \), prove that \( c = \gcd(a, b) \) is equal to \( c' = \gcd(u_1 a_1, u_2 b) \).

4.2.2 Prime factorization

Exercise 9:
Prove that \( p|a \leftrightarrow p^2|a^2 \) for any prime \( p > 1 \).

Exercise 10:
If \( n = \prod_{i=1}^{r} q_i \) with each \( q_i > 1 \) prime (repeats allowed), and with \( r \geq 2 \), so \( n \) is not already a prime. Show \( \exists \) index \( i \) such that \( q_i \leq \sqrt{n} \).

Exercise 11:
If \( p > 1 \) a prime and \( n \neq 0 \) prove that \( \gcd(p, n) > 1 \leftrightarrow p \) divides \( n \).