Writing Assignment 3

Christian Johnson Aidan Andersen

April 7, 2024

Contents

1 Division Algorithm

1.1 Showing the Form of Square of Odd Integers

Using the Division Algorithm, we can express any odd integer as $2k + 1$ for some integer k. The square of any odd integer can be represented as $(2k+1)^2$. Expanding this expression, we get: $(2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$. Since $k^2 + k$ is an integer, we can denote it as m, where $m \in \mathbb{Z}$. Therefore, the square of any odd integer is of the form $8m + 1$ for some $m \in \mathbb{Z}$.

1.2 Definition of Greatest Common Divisor (gcd)

According to the textbook (section 4.2), the greatest common divisor $\gcd(a, b)$ for any pair of positive integers a and b is defined as:

g, iff g is the largest common divisor of a and b; that is, iff:

1. $g|a, g|b$, and
2. if c is any integer such that $c|a$ and $c|b$, then $c \leq g$.

1.3 Finding gcd(345, 92)

$\gcd(345, 92) = 345m + 92n$
Step 1: Apply the Division Algorithm to find quotients and remainders:

- $345 = 92 \times 3 + 69$
- $92 = 69 \times 1 + 23$
- $69 = 23 \times 3 + 0$

Step 2: Identify the last non-zero remainder, which is 23.
Step 3: Express each remainder as a linear combination of the original numbers:

- $23 = 92 - 69 \times 1$
- $69 = 345 - 92 \times 3$

Step 4: Substitute the expressions for remainders into each other:

- $23 = 92 - (345 - 92 \times 3) \times 1$

- Simplify: $23 = 92 - 345 + 92 \times 3$
- Simplify further: $23 = 345 \times (-1) + 92 \times 4$

Step 5: Hence, $\gcd(345, 92) = 23 = 345 \times (-1) + 92 \times 4$, where $m = -1$ and $n = 4$.

2 Exploration of Congruence Classes

2.1 Interpretation of Congruence Statement

For $n > 1, n \in \mathbb{Z}$, the statement $a \equiv b \mod n$ means that a and b have the same remainder when divided by n.

2.2 Verification of Congruence and Finding Other Members

We verify $4 \equiv -7 \mod 11$ by observing that $4-(-7) = 11$, which is divisible by 11. Other positive members of the congruence class 4 can be found by adding multiples of 11, such as 15 and 26.

2.3 Partitioning Z into Congruence Classes

The relation "congruence mod n" for $n > 1, n \in \mathbb{Z}$ partitions $\mathbb{Z}$ into n classes, each containing integers with the same remainder when divided by n. Thus, it is an equivalence relation on $\mathbb{Z}$.

Explanation:

- Consider any integer a in $\mathbb{Z}$.
- When a is divided by n, it yields a remainder $r \mid 0 \leq r < n$.
- There are n possible remainders: $0, 1, 2, ..., n-1$.
- Each integer a belongs to the congruence class represented by its remainder r.
- Therefore, $\mathbb{Z}$ is partitioned into n congruence classes, each containing integers congruent to each other modulo n.
- **Example**:
  - For $n = 4$, the congruence classes are:
    * Class 0: $\{..., -8, -4, 0, 4, 8, ...\}$
    * Class 1: $\{..., -7, -3, 1, 5, 9, ...\}$
    * Class 2: $\{..., -6, -2, 2, 6, 10, ...\}$
    * Class 3: $\{..., -5, -1, 3, 7, 11, ...\}$

2.4 Explanation of Remainder Classes

For any $n > 1, n \in \mathbb{Z}$, there are exactly n remainder classes. This is because when dividing any integer a by n, we obtain a remainder r where $0 \leq r < n$. Thus, there are n possible remainders, forming n remainder classes. Remainder classes for an arbitrary n are: $0, 1, 2, ..., n-1$.