The Division Algorithm and Integers mod p

The Division Algorithm

Theorem The Division Algorithm  Let \( n \) be an integer and \( d \) a positive integer, then there are unique integers \( q \) and \( r \), with \( 0 \leq r < d \) such that \( n = dq + r \).

Definition The integer \( d \) above is called the divisor and \( n \) is called the dividend, \( q \) is called the quotient, and \( r \) is called the remainder. We denote these as \( q = n \text{ DIV } d \) and \( r = n \text{ MOD } d \).

Examples
Find the quotient and remainder if 101 is divided by 11: \[ 101 = 11 \cdot (9) + 2 \]
Find the quotient and remainder if -11 is divided by 3: \[ -11 = 3(-4) + 1 \]

\[ q = n \text{ DIV } d = \text{floor}(n/d) \text{ and } r = n \text{ MOD } d = n - d \cdot q \]

The values of \( n \text{ MOD } d \) are in the set \{0, 1, 2, 3, \ldots , d-1\} which set is called \( \mathbb{Z}(d) \)

Congruence modulo \( p \)
The relation, defined by \( m \equiv n \text{ (mod } p) \) if and only if \( (m-n) = p \cdot q \), is an equivalence relation. The respective remainders on division by \( p \) represent the equivalence classes.

Example Find the equivalence classes for modulo 3:
[0]_3 = \{ . . . , -6, -3, 0, 3, 6, . . . \}
[1]_3 = \{ . . . , -5, -2, 1, 4, 7, . . . \}
[2]_3 = \{ . . . , -4, -1, 2, 5, 8, . . . \}

Note the remainder on division of \( n \) by \( p \) \([n \text{ MOD } p]\) is congruent to \( n \) modulo \( p \) \([n \text{ (mod } p)]\).

Arithmetic on \( \mathbb{Z}(p) \) is done by reducing the corresponding sums and products modulo \( p \). Hence the commutative, associative, and distributive properties of addition and multiplication still hold in the arithmetic of \( \mathbb{Z}(p) \).

Addition and multiplication tables mod 4:

\[
\begin{array}{cccc}
+ & 0 & 1 & 2 & 3 \\
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}
\quad
\begin{array}{cccc}
\times & 0 & 1 & 2 & 3 \\
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 \\
2 & 0 & 2 & 0 & 2 \\
3 & 0 & 3 & 2 & 1 \\
\end{array}
\]

However the cancellation property and the zero products principle may not hold when the modulus \( p \) is not prime.

Examples:
\[ 3 \times_6 1 = 3 \text{ and } 3 \times_6 5 = 3 \text{ but } 1 \neq 5; \text{ also } 3 \times_6 2 = 0, \text{ but } 3 \neq 0 \text{ and } 2 \neq 0. \]