MAT251 The Division Algorithm and Integers mod p

The Division Algorithm

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

Definition The integer d above is called the divisor and a is called the dividend, q is called the quotient, and r is called the remainder. We denote these as \( q = a \div d \) and \( r = a \mod d \)

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: \( -11 = 3 \cdot (-4) + 1 \)

\( q = a \div d = \text{floor}(a/d) \) and \( r = a \mod d = a - d \cdot q \)

The values of \( a \mod d \) are in the set \{0, 1, 2, 3, . . ., d−1\} which set is called \( \mathbb{Z}(d) \)

Theorem 1 on page 121 establishes that the relation, defined by \( m = n \pmod{p} \) if and only if \( (m−n) = p \cdot q \), is an equivalence relation. The respective remainders on division by p represent the equivalence classes.

Theorem 2 on page 122, Theorem 3 on page 123, and Theorem 4 on page 124 show the connection between arithmetic on \( \mathbb{Z} \) and arithmetic on \( \mathbb{Z}(p) \).

The commutative, associative, and distributive properties of addition and multiplication still hold in the arithmetic of \( \mathbb{Z}(p) \).

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

Examples: \( 3 \cdot_6 5 = 3 \cdot_6 1 \) but \( 5 \neq 1 \) and \( 3 \cdot_6 2 = 0 \), but \( 3 \neq 0 \) and \( 2 \neq 0 \).
1. Find q and r as in the division algorithm: \( n = m \cdot q + r \), where \( 0 \leq r < m \).

Note that the letter \( m \) is used here rather than the letter \( p \).

a) \( n = 20 \), \( m = 3 \): \( q = \lfloor \frac{20}{3} \rfloor = 6 \) and \( r = 20 - 3(6) = 2 \); so \( 20 = 3(6) + 2 \).

b) \( n = 20 \), \( m = 4 \): \( q = \lfloor \frac{20}{4} \rfloor = 5 \) and \( r = 20 - 4(5) = 0 \); so \( 20 = 4(5) + 0 \).

c) \( n = -20 \), \( m = 3 \): \( q = \lfloor \frac{-20}{3} \rfloor = -7 \) and \( r = -20 - 3(-7) = 1 \); so \( -20 = 3(-7) + 1 \).

d) \( n = -20 \), \( m = 4 \): \( q = \lfloor \frac{-20}{4} \rfloor = -5 \) and \( r = -20 - 4(-5) = 0 \); so \( -20 = 4(-5) + 0 \).

e) \( n = 371246 \), \( m = 65 \): \( q = \lfloor \frac{371246}{65} \rfloor = 5711 \) and \( r = 371246 - 65(5711) = 31 \).

f) \( n = -371246 \), \( m = 65 \): \( q = \lfloor \frac{-371246}{65} \rfloor = -5712 \) and \( r = -371246 - 65(-5712) = 34 \).

2. Find \( n \) DIV \( m \) and \( n \) MOD \( m \) for the values of \( n \) and \( m \) given as in exercise 1. Answers are the same, where \( q = n \) DIV \( m \) and \( r = n \) MOD \( m \).

3. List three integers that are congruent mod 4 to each of the following.

a) \([0]_4 = \{0, 4, -4, ...\} \)
b) \([1]_4 = \{1, 5, -3, ...\} \)
c) \([2]_4 = \{2, 6, -2, ...\} \)
d) \([3]_4 = \{3, 7, -1, ...\} \)
e) \([4]_4 = \{4, 8, 0, ...\} = [0]_4 \).

4. If we let the smallest non-negative element in an equivalence class represent that class, then

a) \( \mathbb{Z}(4) = \{0, 1, 2, 3\} \) and b) \( \mathbb{Z}(73) = \{0, 1, 2, 3, ..., 72\} \).

5. For the following integers \( m \) find the unique integer \( r \) in \( \{0, 1, 2, 3\} \) such that \( m \equiv r \) (mod 4).

a) \( m = 17 \equiv r \) (mod 4) \( \Rightarrow r = 1 \).

b) \( m = 7 \equiv r \) (mod 4) \( \Rightarrow r = 3 \).

c) \( m = -7 \equiv r \) (mod 4) \( \Rightarrow r = 1 \).

d) \( m = 2 \equiv r \) (mod 4) \( \Rightarrow r = 2 \).

6. Calculate the following modular sums and products.

a) \( 4 +_7 4 = 8 - 7 = 1 \)

b) \( 5 +_7 6 = 11 - 7 = 4 \)

c) \( 4 *_7 4 = 16 - 7(2) = 2 \)

d) \( 0 +_7 k = k \) for any \( k \) in \( \mathbb{Z}(7) \).

e) \( 1 *_7 k = k \) for any \( k \) in \( \mathbb{Z}(7) \).

7. a) Calculate: \( 6 +_{10} 7 = 13 - 10 = 3 \); \( 6 *_{10} 7 = 42 - 4(10) = 2 \).

b) \( m +_{10} k \) is the units digit of \( (m + k) \).

c) \( m *_{10} k \) is the units digit of \( (m * k) \).

8. For \( A_k = \{m \in \mathbb{Z} : -10 \leq m \leq 10 \text{ and } m \equiv k \) (mod 3)\},

a) \( A_0 = \{-9, -6, -3, 0, 3, 6, 9\} \), \( A_1 = \{-8, -5, -2, 1, 4, 7, 10\} \), \( A_2 = \{-10, -7, -4, -1, 2, 5, 8\} \).

b) \( A_3 = A_0 \), \( A_4 = A_1 \), \( A_{73} = A_1 \). Consider the remainders on division of \( k \) by 3.

9. Give the complete addition and multiplication tables for \( \mathbb{Z}(4) \).

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

\[
\begin{array}{cccc}
* & 0 & 1 & 2 & 3 \\
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 \\
2 & 0 & 2 & 0 & 2 \\
3 & 0 & 3 & 2 & 1 \\
\end{array}
\]

10. Solve the following equations for \(x\) in \(\mathbb{Z}(6)\).
   a) \(1 +_6 x = 0, \ x = 5;\)  
   b) \(2 +_6 x = 0, \ x = 4;\)  
   c) \(3 +_6 x = 0, \ x = 3;\)  
   d) \(4 +_6 x = 0, \ x = 2;\)  
   e) \(5 +_6 x = 0, \ x = 1.\)

11. Solve the following equations for \(x\) in \(\mathbb{Z}(5)\).
   a) \(1 \ast_5 x = 1, \ x = 1;\)  
   b) \(2 \ast_5 x = 1, \ x = 3;\)  
   c) \(3 \ast_5 x = 1, \ x = 2;\)  
   d) \(4 \ast_5 x = 1, \ x = 4.\)

12. For \(m, n\) in \(\mathbb{N}\) define \(m \sim n\) if \(m^2 - n^2\) is a multiple of 3.
   a) Show that \(\sim\) is an equivalence relation on \(\mathbb{N}\).
   (R) Because \(m^2 - m^2 = 0 = 3 \cdot 0\) for any \(m\) in \(\mathbb{N}\), then \(m \sim m\); that is, \(\sim\) is reflexive.
   (S) If \(m \sim n\) then \(m^2 - n^2 = 3 \cdot k\), so \(n^2 - m^2 = -(1)(m^2 - n^2) = -(3 \cdot k) = 3 \cdot (-k)\), so \(n \sim m\).
   (T) If \(m \sim n\) and \(n \sim p\) then \(m^2 - n^2 = 3 \cdot k\) and \(n^2 - p^2 = 3 \cdot l\), 
   so \(m^2 - p^2 = m^2 - n^2 + n^2 - p^2 = 3 \cdot k + 3 \cdot l = 3(k + l)\), so \(m \sim p\).
   b) \([0] = \{0, 3, 6, 9, ...\}\)  
   c) \([1] = \{1, 2, 4, 5, ...\}\)  
   d) Clearly there are no more equivalence classes.

13. The definition of \(m \equiv n \pmod{p}\) makes sense even if \(p = 1\).
   a) Clearly \(m \equiv n \pmod{1}\) for all \(m, n\) in \(\mathbb{Z}\), so there is only one equivalence class, 
      which we can represent by \([0]\).
   b) \(m \ \text{DIV} \ 1\) would be \(m\) and \(m \ \text{MOD} \ 1\) would be zero.
   c) \(\text{Sum} +_1\) and \(\text{Product} \ast_1\) are defined in this system, 
      but \(m +_1 n = (m + n) \ \text{MOD} \ 1 = 0\) and \(m \ast_1 n = (m \cdot n) \ \text{MOD} \ 1 = 0\)
      Thus Theorem 3 says \((m + n) \ \text{MOD} \ 1 = (m \ \text{MOD} \ 1) +_1 (n \ \text{MOD} \ 1)\) or \(0 = 0 +_1 0\)
      and it says \((m \cdot n) \ \text{MOD} \ 1 = (m \ \text{MOD} \ 1) \ast_1 (n \ \text{MOD} \ 1)\) or \(0 = 0 \ast_1 0\)