7. The Division Algorithm

**Theorem.** [Division Algorithm] Suppose $a > 0$ and $b$ are integers. Then there is a unique pair of integers $q$ and $r$ such that

$$b = aq + r \quad \text{where} \quad 0 \leq r < a.$$  

The number $q$ is called the **quotient** and $r$ is called the **remainder**.

**Example:** $b = 23$ and $a = 7$. Here $23 = 3 \times 7 + 2$, so $q = 3$ and $r = 2$. In grade school you would have said “7 goes into 23 three times with a remainder of two.” When you learned about fractions (in the fourth grades), you wrote $\frac{23}{7} = 3 \frac{2}{7}$. Observe also that the restriction that the remainder $r$ lies in the range $0 \leq r \leq a - 1$ is essential for uniqueness. For example, it is true that $23 = 2 \times 7 + 9$, but we cannot use $r = 9$ as a remainder because it is larger than the divisor 7; given $b = 23, a = 7$, the *only* values of $q$ and $r$ satisfying $23 = 7q + r$, $0 \leq r \leq 6$ are 3 and 2, respectively.

We can verify the division algorithm by induction on the variable $b$. It simplifies the discussion to assume that the divisor $a$ is greater than 1.

**Question #23.** What are the values of $q$ and $r$ if $a = 1$?

**First Step:** $b = 1$. Here

$$1 = 0 \times a + 1$$

When $b = 1$, the quotient is $q = 0$ and the remainder is $r = 1$.

**Next step:** Assume the division algorithm holds for the positive integer $b$, that is, assume

$$b = q \times a + r$$

Can we figure out the values of $q$ and $r$ for $b + 1$? That’s easy.

$$b + 1 = q \times a + (r + 1)$$

Use the old value of $q$ and just increase $r$ by 1.

Wait a minute. What if $r = a - 1$? When we add 1 to $r$, the new value will not lie between 0 and $a - 1$.

For example, if $a = 5$ and $b = 22$, then from $22 = 4 \times 5 + 2$ we get the next statement $23 = 4 \times 5 + 3$. But if we start with $24 = 4 \times 5 + 4$, the next statement becomes $25 = 4 \times 5 + 5$, which is true, but the remainder 5 does not lie in the required range.
How can we handle this case?

**Exercise #24.** Complete the induction argument that demonstrates the “existence” part of the Division Algorithm. That is, prove that the required integers \( q \) and \( r \) exist such that \( b = qa + r, \ 0 \leq r < a \).

**Exercise #25.** Prove the “uniqueness” part of the Division Algorithm. That is, prove that the integers \( q \) and \( r \) are unique, which means that if \( (q_1, r_1) \) satisfies \( b = q_1a + r_1, \ 0 \leq r_1 < a \) and \( (q_2, r_2) \) also satisfies \( b = q_2a + r_2, \ 0 \leq r_2 < a \), then \( q_1 = q_2 \) and \( r_1 = r_2 \).

The next theorem shows a connection between the division algorithm and congruences.

**Theorem #26.** Let \( a, b, \) and \( n > 0 \) be integers. Then \( a \equiv b \pmod{n} \) if and only if \( a \) and \( b \) have the same remainder when divided by \( n \).

**Exercise #27.** Use congruences to find the following remainders:

1. when \( 2009 \times 1864 + 195 \) is divided by 7
2. when \( 2 \times 3 \times 4 \times 5 \times \cdots \times 19 \times 20 \) is divided by 11
3. when \( 2^{100} \) is divided by 7
4. make up your own problem and solve it

### 8. Mod \( n \) Tables

Here are the addition and multiplication tables for 5-clock arithmetic:

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( \times )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Let’s examine the times table. The zero row and zero column consists of all 0’s. What did we expect? Zero times anything is zero. If we ignore the 0 row and column, the rest of the times table has some interesting properties. Notice, for example, the numbers 1, 2, 3, and 4 are scrambled when we multiply by 2, 3, or 4. That is, each of the rows list the numbers 1, 2, 3, 4 in some order. In the second row we get 2, 4, 1, 3; in the third row we get
3, 1, 4, 2; in the last row the numbers are backwards 4, 3, 2, 1. This scrambling phenomenon is the key idea in constructing the secret codes discussed in a future section.

**Problem** #28. Construct the $+$ and $\times$ tables for the 7-clock.

**Problem** #29. Construct the $+$ and $\times$ tables for the 6-clock.

**Problem** #30. Give the 7th row of the multiplication table for a 31-clock.