Section 4 - The Quotient Remainder Theorem

- The Quotient-Remainder Theorem;
- Modular Arithmetic (\textit{div} and \textit{mod} functions);
- Proofs Requiring Division into Cases;
- Representations of the Integers.
- The Parity Theorem
Quotient-Remainder Theorem

- **Theorem:** Given any integer \( n \) and a positive integer \( d \), there exist unique integers \( q \) and \( r \) such that: \( n = d \cdot q + r \), and \( 0 \leq r < d \).

- **Example:** If \( n = 27 \) and \( d = 5 \), then consider:
  
  \[
  \begin{align*}
  27 &= 0 \cdot 5 + 27 \\
  27 &= 1 \cdot 5 + 22 \\
  27 &= 2 \cdot 5 + 17 \\
  27 &= 3 \cdot 5 + 12 \\
  27 &= 4 \cdot 5 + 7 \\
  27 &= 5 \cdot 5 + 2 \quad \text{here, } r = 2 \text{ and } q = 5. \\
  27 &= 6 \cdot 5 + (-3)
  \end{align*}
  \]
**div and mod Functions**

- **Definition:** Given a nonnegative integer \( n \) and a positive integer \( d \),
  
  \[ n \div d = \text{the integer quotient obtained when } n \text{ is divided by } d; \]
  
  \[ n \mod d = \text{the integer remainder obtained when } n \text{ is divided by } d. \]

- Symbolically, if \( n \) and \( d \) are positive integers:
  
  \[ n \div d = q \text{ and } n \mod d = r, \text{ where } n, d, q, \text{ and } r \]
  
  are as described in the Quotient-Remainder Theorem.
**div and mod Examples**

- Consider the previous example of \( n = 27 \) and \( d = 5 \). Since \( 27 = 5 \cdot 5 + 2 \) yields \( q = 5 \) and \( r = 2 \), we have that:
  
  \[
  27 \text{ div } 5 = 5; \\
  27 \text{ mod } 5 = 2.
  \]

- More:
  
  \[
  100 \text{ div } 10 = 10 \quad 100 \text{ mod } 10 = 0 \\
  100 \text{ div } 8 = 12 \quad 100 \text{ mod } 8 = 4 \\
  10 \text{ div } 100 = 0 \quad 10 \text{ mod } 100 = 10 \\
  365 \text{ div } 7 = 52 \quad 365 \text{ mod } 7 = 1
  \]
Representations of the Integers

• Recall, we have claimed previously that every integer is either even or odd.

• Consider:
  Even: ... −10 −8 −6 −4 −2 0 2 4 6 8 10 ...  
  Odd: ... −9 −7 −5 −3 −1 1 3 5 7 9 11 ...

• We note that all the evens are \( n = 2q = 2q + 0 \) and all the odds are \( n = 2q + 1 \).

• Moreover, each successive integer alternates parity (its mod 2 value).
More Representations of Integers

- If we continue representing integers via the Quotient-Remainder Theorem, we observe:

<table>
<thead>
<tr>
<th>Modulus</th>
<th>Forms</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$2n$ $2n + 1$</td>
</tr>
<tr>
<td>3</td>
<td>$3n$ $3n + 1$  $3n + 2$</td>
</tr>
<tr>
<td>4</td>
<td>$4n$ $4n + 1$  $4n + 2$ $4n + 3$</td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>$k$</td>
<td>$kn$ $kn + 1$ $kn + 2$ ... $kn + (k-1)$</td>
</tr>
</tbody>
</table>
Division into Cases

• Sometimes when proving a theorem, the logical flow will fork into different directions, each of which need investigation.

• This is analogous to needing IF THEN ELSE instead of just IF THEN in programming flow.

• An example is the Parity Theorem.

• **Theorem**: Any two consecutive integers have opposite parity.
Division into Cases (cont’d.)
Proof: Let $m$ be an integer, so its successor is $(m+1)$. Show $m$ and $(m+1)$ have opposite parity.

Case 1 ($m$ even): If $m$ is even, there is an integer $k$ such that $m = 2k$, hence $(m+1) = 2k + 1$, thus $(m+1)$ is odd. So, $m$ even implies $(m+1)$ is odd.

Case 2 ($m$ odd): If $m$ is odd, there is integer $k$ such that $m = 2k + 1$. Hence:

$(m+1) = (2k + 1) + 1 = 2k + 2 = 2(k +1)$, and so $(m+1)$ is even. So, $m$ odd implies $(m+1)$ is even.

Therefore, consecutive integers have opposite parity. QED
The Square of an Odd Integer

**Theorem:** If \( n \) is an odd integer, \((n^2 \mod 8) = 1\).

**Proof:** Let \( n \) be an odd integer, so it has the representation modulo 4 of \( n = 4q+1 \) or \( 4q+3 \).

**Case 1:** Let \( n = 4q+1 \). Thus \( n^2 = (4q+1)^2 \)
\[
= 16q^2 + 8q + 1 = 8(2q^2 + q) + 1.
\]

**Case 2:** Let \( n = 4q+3 \). Thus \( n^2 = (4q+3)^2 \)
\[
= 16q^2 + 24q + 9 = 16q^2 + 24q + 8 + 1
= 8(2q^2 + 3q + 1) + 1.
\]

Therefore, in either case, \((n^2 \mod 8) = 1\). QED