Example Proofs Involving the $(n \mod d)$-Function

The following statements are proved in this handout:

1. **To Prove**: $(67 \mod 9) = 4$

2. **To Prove**: $(-28 \mod 5) = 2$

3. **To Prove**: For every integer $b$,
   
   \[
   \text{if } (b \mod 16) = 10, \text{ then } (4b \mod 16) = 8.
   \]

4. **To Prove**: For all integers $c$ and $d$,
   
   \[
   \text{if } (c \mod 8) = 5 \text{ and } (d \mod 8) = 7,
   \]
   
   \[
   \text{then } (cd \mod 8) = 3.
   \]

---

1. **To Prove**: $(67 \mod 9) = 4$.

   **Proof**: By the Quotient-Remainder (Q-R) Theorem, there exist unique integers $q$ and $r$ such that $67 = 9q + r$ and $0 \leq r < 9$.

   Also, by the definition of $(n \mod d)$, $(67 \mod 9) = r$.

   Now, $67 = 9 \times 7 + 4$ and $0 \leq 4 < 9$.

   So, by the uniqueness of $q$ and $r$, $q = 7$ and $r = 4$.

   \[
   \therefore \text{ By substitution, } (67 \mod 9) = 4.
   \]

   **QED.**
(2) To Prove: \((-28 \mod 5) = 2\)

Proof: By the Q-R Theorem, there exist unique integers \(q\) and \(r\) such that
\[-28 = 5q + r\quad \text{and} \quad 0 \leq r < 5.\]
By definition of \((n \mod d)\), \((-28 \mod 5) = r\).
Now, \(-28 = 5 \times (-6) + 2\) and \(0 \leq 2 < 5\).
So, by the uniqueness of \(q\) and \(r\), \(q = -6\) and \(r = 2\).
\[\therefore\] By substitution, \((-28 \mod 5) = 2.\]
\[\therefore Q.E.D.\]

(3) To Prove: For every integer \(b\),
if \((b \mod 16) = 10\), then \((4b \mod 16) = 8\).

Proof: Let \(b\) be any integer such that \((b \mod 16) = 10\).

\[\text{[N.T.S:} (4b \mod 16) = 8]\]
By the Q-R Theorem, there exist unique integers \(q_1, r_1\) and \(q_2, r_2\) such that \(b = 16q_1 + r_1\) and \(0 \leq r_1 < 16\) and \(4b = 16q_2 + r_2\) and \(0 \leq r_2 < 16\).
By definition of \((n \mod d)\),
\((b \mod 16) = r_1\) and \((4b \mod 16) = r_2\).
Since \((b \mod 16) = 10\), \(r_1 = 10\) and \(b = 16q_1 + 10\),
by substitution,
Proof of (3) (continued): \[ 4b = 4(16q_1 + 10), \text{ by substitution} \]
\[ = 64q_1 + 40 \]
\[ = 16(4q_1) + 16 \times 2 + 8 \]
\[ = 16(4q_1 + 2) + 8, \text{ by Rules of Algebra}. \]

Let \( t = 4q_1 + 2 \). Then, \( t \) is an integer since sums and products of integers are integers.

\[ : 4b = 16t + 8, \text{ by substitution}. \]
\[ : 4b = 16t + 8 \text{ and } 0 \leq 8 < 16. \]

By the uniqueness of \( q_2 \) and \( r_2 \), \( q_2 = 5 \) and \( r_2 = 8 \).

As shown above, \( (4b \mod 16) = r_2 \).

\[ : (4b \mod 16) = 8, \text{ by substitution}. \]

For every integer \( b \), if \( (b \mod 16) = 10 \), then 
\[ (4b \mod 16) = 8, \text{ by Direct Proof}. \]

QED.

(14): To Prove: For all integers \( c \) and \( d \),

\[ \text{if } (c \mod 8) = 5 \text{ and } (d \mod 8) = 7 \]
\[ \text{then } (cd \mod 8) = 3. \]

Proof: Let \( c \) and \( d \) be any integers.

Suppose \( (c \mod 8) = 5 \) and \( (d \mod 8) = 7 \). [Suppose the \text{Irr. fact!}]

\[ [\text{N.T.S. : } (cd \mod 8) = 3] \]

(Continued on the next page)
By the Q-R Theorem there exist unique integers $q_1, r_1$ and $q_2, r_2$ and $q_3, r_3$ such that

$$c = 8q_1 + r_1 \text{ and } 0 \leq r_1 < 8 \text{ and }$$
$$d = 8q_2 + r_2 \text{ and } 0 \leq r_2 < 8 \text{ and }$$
$$cd = 8q_3 + r_3 \text{ and } 0 \leq r_3 < 8.$$

By definition of \((c \mod d)\), \((c \mod 8) = r_1,\)
\((d \mod 8) = r_2 \text{ and } (cd \mod 8) = r_3.$$

Since \((c \mod 8) = 5, r_1 = 5 \text{ and } c = 8q_1 + 5, \text{ by substitution.}\)
Since \((d \mod 8) = 7, r_2 = 7 \text{ and } d = 8q_2 + 7, \text{ by subst.}\)

\[\begin{align*}
\therefore cd &= (8q_1 + 5)(8q_2 + 7), \text{ by substitution} \\
&= 64q_1q_2 + 40q_2 + 56q_1 + 35 \\
&= 8(8q_1q_2 + 5q_2 + 7q_1) + 8\cdot 4 + 3 \\
&= 8(8q_1q_2 + 5q_2 + 7q_1 + 4) + 3 \\
&= 8t + 3, \text{ where } t = (8q_1q_2 + 5q_2 + 7q_1 + 4),
\end{align*}\]

and \(t\) is an integer since sums and products of integers are integers.

\[\therefore cd = 8t + 3 \text{ and } 0 \leq 3 < 8.\]

\[\therefore \text{ By the uniqueness of } 8q_3 \text{ and } 8r_3, r_3 = 3.\]

As shown above, \((cd \mod 8) = r_3 \text{. \therefore (cd \mod 8) = 3, by subst.}\)

\[\therefore \text{ For all integers } c \text{ and } d, \text{ if } (c \mod 8) = 5 \text{ and }\]
\((d \mod 8) = 7, \text{ then } (cd \mod 8) = 3, \text{ by Direct Proof.}\)

Q.E.D.