HW #12, Part II of #128 Solutions  

Spring 2017

Section 8.4 (From Epp’s Fourth Edition)

7.

(a) Verify that \(128 \equiv 2 \pmod{7}\)

Two methods of verification are shown here.

Method #1:

\[
\begin{align*}
128 - 2 &= 126 = 18 \times 7. \\
\therefore 7 \mid (128-2)
\end{align*}
\]

Method #2:

\[
\begin{align*}
126 &= 7 \times 18. \\
128 &= 2 + 7 \times 18
\end{align*}
\]

\[\therefore \text{By Theorem 8.4.1, } 128 \equiv 2 \pmod{7}.\]

Verify that \(61 \equiv 5 \pmod{7}\)

Method #1:

\[
\begin{align*}
61 - 5 &= 56 = 8 \times 7. \\
\therefore 7 \mid (61-5)
\end{align*}
\]

Method #2:

\[
\begin{align*}
61 &= 5 + 5 \times 7. \\
\therefore 61 = 5 + 7k \text{ with } k = 8.
\end{align*}
\]

\[\therefore \text{By Theorem 8.4.1, } 61 \equiv 5 \pmod{7}.\]

(b) Verify that \((128 + 61) \equiv (2 + 5) \pmod{7}\).

\[
128 + 61 = 189 \text{ and } 2 + 5 = 7.
\]

We need to show that \(189 \equiv 7 \pmod{7}\).

\[
189 - 7 = 182 \text{ and } 182 = 7 \times 26.
\]

\[\therefore 7 \mid (189-7) \quad \therefore 189 \equiv 7 \pmod{7}\]

This illustrates Theorem 8.4.3 (1).
2c) Verify that \((128 - 61) \equiv (2 - 5) \pmod{7}\)
\[
128 - 61 = 67 \quad \text{and} \quad 2 - 5 = -3
\]
Verify that \(67 \equiv -3 \pmod{7}\)
\[
67 - (-3) = 67 + 3 = 70 = 10 \times 7
\]
\[
\therefore 7 \mid (67 - (-3)) \quad \Rightarrow \quad 67 \equiv -3 \pmod{7}
\]
Also, \(67 = (-3) + 10 \times 7 \Rightarrow 67 \equiv -3 \pmod{7}\)

This illustrates Theorem 8.4.3 (2)

2d) Verify that \((128 \times 61) \equiv (2 \times 5) \pmod{7}\)
\[
128 \times 61 = 7808 \quad \text{and} \quad 2 \times 5 = 10
\]
Verify that \(7808 \equiv 10 \pmod{7}\)
\[
7808 - 10 = 7798 = 1114 \times 7
\]
\[
\therefore 7 \mid (7808 - 10) \quad \Rightarrow \quad 7808 \equiv 10 \pmod{7}
\]
Also, \(7808 = 10 + 1114 \times 7 \Rightarrow 7808 \equiv 10 \pmod{7}\)

This illustrates Theorem 8.4.3 (3)

The problem also illustrates the first part.
Sec 8.41  \#7c  Verify that $128^2 \equiv 2^2 \pmod{7}$
\[
128^2 = 16384 \quad \text{and} \quad 2^2 = 4
\]
Verify that $16384 \equiv 4 \pmod{7}$
\[
16384 - 4 = 16380 = 2340 \times 7
\]
\[
\therefore \ 7 \mid (16384 - 4) \implies 16384 \equiv 4 \pmod{7}
\]
Also $16384 = 4 + 2340 \times 7 \implies 16384 \equiv 4 \pmod{7}$

This illustrates Theorem 8.4.3 (4).

\#8

8a) Verify that $45 \equiv 3 \pmod{6}$
\[
45 - 3 = 42 = 7 \times 6
\]
\[
\therefore \ 6 \mid (45 - 3) \implies 45 \equiv 3 \pmod{6}
\]
Also $45 = 3 + 7 \times 6 \implies 45 \equiv 3 \pmod{6}$

Verify that $104 \equiv 2 \pmod{6}$
\[
104 - 2 = 102 = 17 \times 6
\]
\[
\therefore \ 6 \mid (104 - 2) \implies 104 \equiv 2 \pmod{6}
\]
Also $104 = 2 + 17 \times 6 \implies 104 \equiv 2 \pmod{6}$

8b Verify that $(45 + 104) \equiv (3+2) \pmod{6}$
\[
45 + 104 = 149 \quad \text{and} \quad 3 + 2 = 5
\]
Verify that $149 \equiv 5 \pmod{6}$
\[
149 - 5 = 144 = 24 \times 6
\]
\[
\therefore \ 6 \mid (149 - 5) \implies 149 \equiv 5 \pmod{6}
\]
Also $149 = 5 + 24 \times 6 \implies 149 \equiv 5 \pmod{6}$

This illustrates Theorem 8.4.3 (1)
See 8.4
8c Verify that \((45 - 104) \equiv (3 - 2) \pmod{6}\)
\[45 - 104 = -59 \quad \text{and} \quad 3 - 2 = 1\]

Verify that \(-59 \equiv 1 \pmod{6}\)
\[-59 - 1 = -60 = (-10) \times 6\]

\[\therefore 6 \mid (-59 - 1) \Rightarrow -59 \equiv 1 \pmod{6}\]
Also, \(-59 = +1 + (-10) \times 6 \Rightarrow -59 \equiv 1 \pmod{6}\)

This illustrates Theorem 8.4.3 (2)

8d Verify that \((45 \times 104) \equiv (3 \times 2) \pmod{6}\)
\[45 \times 104 = 4680 \quad \text{and} \quad 3 \times 2 = 6\]

Verify that \(4680 \equiv 6 \pmod{6}\)
\[4680 - 6 = 4674 = 779 \times 6\]

\[\therefore 6 \mid (4680 - 6) \Rightarrow 4680 \equiv 6 \pmod{6}\]
Also, \(4680 = 6 + 779 \times 6 \Rightarrow 4680 \equiv 6 \pmod{6}\)

This illustrates Theorem 8.4.3 (3)

8e Verify that \(45^2 \equiv 3^2 \pmod{6}\)
\[45^2 = 2025 \quad \text{and} \quad 3^2 = 9\]

This illustrates Theorem 8.4.3 (4)

Verify that \(2025 \equiv 9 \pmod{6}\)
\[2025 - 9 = 2016 = 336 \times 6\]

\[\therefore 6 \mid (2025 - 9) \Rightarrow 2025 \equiv 9 \pmod{6}\]
Also, \(2025 = 9 + 336 \times 6 \Rightarrow 2025 \equiv 9 \pmod{6}\)
See 8.4

9b. Assume that \( a, \ b, c, d, n \) are integers, with \( n \geq 1 \), and also assume that \( a \equiv c \pmod{n} \) and \( b \equiv d \pmod{n} \).

To Prove:

\[ (a-b) \equiv (c-d) \pmod{n} \]

Proof: Since \( a \equiv c \pmod{n} \),

\[ a = c + kn \text{ for some } k \in \mathbb{Z} \text{ by Theorem 8.4.1 (3)} \]

Since \( b \equiv d \pmod{n} \),

\[ b = d + ln \text{ for some } l \in \mathbb{Z} \text{ by Theorem 8.4.1 (3)} \]

\[ (a-b) = (a) - (b) \]
\[ = (c+kn) - (d+ln) \]
\[ = c+kn - d - ln \]
\[ = (c-d) + (k-l)n \]
\[ = (c-d) + tn \text{ where } t = k-l, \text{ which is an integer.} \]

\[ (a-b) \equiv (c-d) \pmod{n} \text{ by Theorem 8.4.1 (3), } \]

Q.E.D.
SECTION 8.4 (EPP'S FOURTH EDITION), #14 Solution

Determine \((14^m \mod 55)\) for \(m = 2, 4, 8, 16\).

Solution: \((14^2 \mod 55) = 31\), by a simple calculation (justified since \(0 \leq 14 < 55\)).

\[
14^2 \equiv 31 \pmod{55}, \text{ by Theorem (N18)}^4,
\]

since \((14^2 \mod 55) = 31\).

\[
14^4 = (14^2)^2 \equiv 31^2 \pmod{55}.
\]

\[
(14^4 \mod 55) = (31^2 \mod 55) = 26, \text{ by Theorem 8.4.1 and a simple calculation}.
\]

\[
14^4 \equiv 26 \pmod{55}, \text{ by Theorem (N18)}^4, \text{ since } (14^4 \mod 55) = 26.
\]

\[
14^8 = (14^4)^2 \equiv 26^2 \pmod{55}, \text{ by Theorem 8.4.3}.
\]

\[
(14^8 \mod 55) = (26^2 \mod 55) = 16, \text{ by Theorem 8.4.1 and a simple calculation}.
\]

\[
14^8 \equiv 16 \pmod{55}, \text{ by Theorem (N18)}^4, \text{ since } (14^8 \mod 55) = 16.
\]

\[
14^{16} = (14^8)^2 \equiv 16^2 \pmod{55}, \text{ by Theorem 8.4.3}.
\]

\[
(14^{16} \mod 55) = (16^2 \mod 55) = 36, \text{ by Theorem 8.4.1 and a simple calculation}.
\]
Sec 8.4. #15: Determine \((14^{27} \mod 55)\).

In Problem 14, the following values were found:
\[
\begin{align*}
(14^2 \mod 55) &= 31 \\
(14^4 \mod 55) &= 26 \\
(14^8 \mod 55) &= 16 \\
(14^{16} \mod 55) &= 36 \\
\end{align*}
\]

By Theorem (N18) 4
\[
\begin{align*}
14^2 &\equiv 31 \pmod{55} \\
14^4 &\equiv 26 \pmod{55} \\
14^8 &\equiv 16 \pmod{55} \\
14^{16} &\equiv 36 \pmod{55} \\
\end{align*}
\]

Since \(27 = 16 + 8 + 2 + 1\) as a sum of powers of 2,
\[
14^{27} = 14^{16} \times 14^8 \times 14^2 \times 14^1 \\
\equiv (36) \times (16) \times (31) \times (14) \pmod{55}, \text{ by Thm 8.4.3.}
\]
Now, \(36 \times 16 \times 31 \times 14 = 249,984\). 

By substitution,
\[
\begin{align*}
\text{Also, } 249,984 &= 55(4,545) + 9 \quad \text{and} \quad 0 \leq 9 < 55, \\
\therefore (249,984 \mod 55) &= 9 \quad \text{by definition of the "mod" function}, \\
\therefore 249,984 &\equiv 9 \pmod{55}, \text{ by Theorem (N18) 4.} \\
\text{Recall, } 14^{27} &\equiv 249,984 \pmod{55} \\
\therefore 14^{27} &\equiv 9 \pmod{55} \quad \text{by Transitive of "\(\equiv\) mod 55"}
\end{align*}
\]

\[
(14^{27} \mod 55) = (9 \mod 55) = 9, \text{ by Theorem 8.4.1.}
\]