HW #10B, PART III Solutions $\qquad$ M 325K SPRING 2024

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:	Method #2
$128 - 2 = 126 = 18 \times 7.$	$126 = 7 \times 18$
$\therefore 7 \mid (128-2)$	$\therefore 128 = 2 + 7 \times 18$

$\therefore$ By Theorem 8.4.1, $128 \equiv 2 \pmod 7$.

Verify that $61 \equiv 5 \pmod 7$

Method #1	Method #2
$61 - 5 = 56 = 8 \times 7$	$61 = 5 + 56 = 5 + 7 \times 8$
$\therefore 7 \mid (61-5)$	$\therefore 61 = 5 + 7k$ with $k = 8$.

$\therefore$ By Theorem 8.4.1,

$61 \equiv 5 \pmod 7$.

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

$128 + 61 = 189$ and $2 + 5 = 7$.

We need to show that $189 \equiv 7 \pmod 7$.

$189 - 7 = 182$ and $182 = 7 \times 26$.

$\therefore 7 \mid (189 - 7)$ $\qquad$ $\therefore 189 \equiv 7 \pmod 7$

This illustrates Theorem 8.4.3 (1).

Sec 8.4 #7 (continued)

7c) Verify that $(128-61) \equiv (2-5) \pmod 7$

$128-61=67$ and $2-5=-3$

Verify that $67 \equiv -3 \pmod 7$

$67-(-3) = 67+3 = 70 = 10\times 7$

$\therefore 7 \mid (67-(-3)) \Rightarrow 67 \equiv (-3) \pmod 7$

Also, $67 = (-3) + 10\times 7 \Rightarrow 67 \equiv (-3) \pmod 7$

This illustrates theorem 8.4.3 (2)

7d Verify that $(128\times 61) \equiv (2\times 5) \pmod 7$

$128\times 61 = 7808$ and $2\times 5 = 10$

Verify that $7808 \equiv 10 \pmod 7$

$7808-10 = 7798 = 1114\times 7$

$\therefore 7 \mid (7808-10) \Rightarrow 7808 \equiv 10 \pmod 7$

also $7808 = 10 + 1114\times 7 \Rightarrow 7808 \equiv 10 \pmod 7$

This illustrates Theorem 8.4.3 (3)

~~128 mod 7 = 2 since 128 = 18×7+2 and 0≤2<7.~~
~~61 mod 7 = 5 since 61 = 8×7+5 and 0≤5<7.~~
~~So, this problem also illustrates Corollary 8.4.4, the first part.~~

#7 (continued)

Sec 8.4: #7e Verify that $128^2 \equiv 2^2 \pmod 7$

#7e $128^2 = 16{,}384$ and $2^2 = 4$

Verify that $16{,}384 \equiv 4 \pmod 7$

$16{,}384 - 4 = 16380 = 2340 \times 7$

$\therefore 7 \mid (16384 - 4) \Rightarrow 16{,}384 \equiv 4 \pmod 7$

Also $16{,}384 = 4 + 2340 \times 7 \Rightarrow 16{,}384 \equiv 4 \pmod 7$

This illustrates Theorem 8.4.3 (4).

#8

8a) Verify that $45 \equiv 3 \pmod 6$

$45 - 3 = 42 = 7 \times 6$

$\therefore 6 \mid (45 - 3) \Rightarrow 45 \equiv 3 \pmod 6$

Also $45 = 3 + 7 \times 6 \Rightarrow 45 \equiv 3 \pmod 6$

Verify that $104 \equiv 2 \pmod 6$

$104 - 2 = 102 = 17 \times 6$

$\therefore 6 \mid (104 - 2) \Rightarrow 104 \equiv 2 \pmod 6$

Also $104 = 2 + 17 \times 6 \Rightarrow 104 \equiv 2 \pmod 6$

8b Verify that $(45 + 104) \equiv (3 + 2) \pmod 6$

$45 + 104 = 149$ and $3 + 2 = 5$

Verify that $149 \equiv 5 \pmod 6$.

$149 - 5 = 144 = 24 \times 6$

$\therefore 6 \mid (149 - 5) \Rightarrow 149 \equiv 5 \pmod 6$

Also $149 = 5 + 24 \times 6 \Rightarrow 149 \equiv 5 \pmod 6$

This illustrates Theorem 8.4.3 (1).

Sec 8.4

8c Verify that $(45-104) \equiv (3-2) \pmod 6$

$45-104=-59$ and $3-2=1$

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 $(45 \times 104) \equiv (3 \times 2) \pmod 6$

$45 \times 104 = 4680$ and $3 \times 2 = 6$

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 $45^2 \equiv 3^2 \pmod 6$

$45^2 = 2025$ and $3^2=9$.

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, $2025 = 9 + 336 \times 6 \Rightarrow 2025 \equiv 9 \pmod 6$

This illustrates Theorem 8.4.3 (4).

Sec 8.4

#9b. Assume that a, b, c, d, n are integers,
with $n > 1$, 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 $a \equiv c \pmod{n}$,
$a = c + kn$ for some $k \in \mathbb{Z}$ by Theorem 8.4.1 (3)

Since $b \equiv d \pmod{n}$
$b = d + ln$ for some $l \in \mathbb{Z}$ by Theorem 8.4.1 (3).

$$\begin{aligned} \therefore (a-b) &= (a) - (b) \\ &= (c+kn) - (d+ln) \\ &= c + kn - d - ln \\ &= (c-d) + (k-l)n \\ &= (c-d) + tn \text{ where } t = k-l, \end{aligned}$$

which is an integer.

$\therefore (a-b) \equiv (c-d)$ by Theorem 8.4.1 (3).

QED.

SECTION 8.4, Problem #14 Solution

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

Solution:

$14^2 = 196 = (55)(3) + 31$ and $0 \le 31 < 55$.

$\therefore$ $(14^2 \bmod 55) = 31$ by definition of the "$(k \bmod 55)$" function.

$14^4 = (14^2)^2 \equiv 31^2 \equiv 26 \pmod{55}$

by Theorem 8.4.3 and by Theorem 8.4.1 since $31^2 = (55)(17) + 26$

$\therefore 14^4 \equiv 26 \pmod{55}$

$\therefore$ By Theorem 8.4.1, $(14^4 \bmod 55) = (26 \bmod 55) = 26$.

$\therefore$ $(14^4 \bmod 55) = 26$

$14^8 \equiv (14^4)^2 \equiv 26^2 \equiv 16 \pmod{55}$ by Theorem 8.4.3 and by Theorem 8.4.1 since $26^2 = (55)(12) + 16$.

$\therefore 14^8 \equiv 16 \pmod{55}$, and so, by Theorem 8.4.1,
$(14^8 \bmod 55) = (16 \bmod 55) = 16$.

$\therefore$ $(14^8 \bmod 55) = 16$.

$14^{16} = (14^8)^2 \equiv 16^2 \equiv 36 \pmod{55}$ by Theorem 8.4.3 and by Theorem 8.4.1 since $16^2 = (55)(4) + 36$

$\therefore 14^{16} \equiv 36 \pmod{55}$.

$\therefore$ By Theorem 8.4.1, $(14^{16} \bmod 55) = (36 \bmod 55) = 36$.

$\therefore$ $(14^{16} \bmod 55) = 36$.

SECTION 8.4, #15 Determine $(14^{27} \bmod 55)$

In Problem #14, the following values were found.

$(14^2 \bmod 55) = 31$
$(14^4 \bmod 55) = 26$
$(14^8 \bmod 55) = 16$
$(14^{16} \bmod 55) = 36$

Since $31 = 55 \times 0 + 31$ and $0 \leq 31 < 55$, $(31 \bmod 55) = 31$

Similarly, $(26 \bmod 55) = 26$, $(16 \bmod 55) = 16$, and $(36 \bmod 55) = 36$.

Then $(14^2 \bmod 55) = (31 \bmod 55)$ by substitution, so $14^2 \equiv 31 \pmod{55}$ by Thm 8.4.1

Similarly, $14^4 \equiv 26 \pmod{55}$, $14^8 \equiv 16 \pmod{55}$, and $14^{16} \equiv 36 \pmod{55}$.

Since $27 = 16 + 8 + 2 + 1$ as a sum of powers of 2,

$14^{27} = 14^{16} \times 14^8 \times 14^2 \times 14^1$

So, $14^{27} \equiv (36)(16)(31)(14) \pmod{55}$, by Thm 8.4.3.

Since $(36)(16)(31)(14) = 249{,}984$,

$14^{27} \equiv 249{,}984 \pmod{55}$

Since $249{,}984 = (55)(4{,}545) + 9$,

$249{,}984 \equiv 9 \pmod{55}$ by Theorem 8.4.1.

$\therefore 14^{27} \equiv 9 \pmod{55}$ by Transitivity of "$\equiv \pmod{55}$"

Sec. 8.4, #15 Solution (Continued)

Recall $14^{27} \equiv 9 \pmod{55}$. $\therefore (14^{27} \bmod 55) = (9 \bmod 55)$ by Thm 8.4.1.

Since $9 = 55 \times 0 + 9$ and $0 \le 9 < 55$,
$(9 \bmod 55) = 9$.

$\therefore (14^{27} \bmod 55) = 9$ by Substitution.