Homework #10A Solution

M325K
SPRING 2024

SECTION 8.4, # 17 from Epp's 4th Edition.

Problem: Determine (89^{307} mod 713).

SOLUTION:

$$307 = 256 + 32 + 16 + 2 + 1.$$

$$\therefore 89^{307} = (89^{256})(89^{32})(89^{16})(89^{2})(89^{1}).$$

$$\therefore 89^{307} \equiv (89^{256})(89^{32})(89^{16})(89^{2})(89) \pmod{713},$$

since congruence modulo 713 is a reflexive relation.

→ $89 \equiv 89 \pmod{713}$

→ $89^2 \equiv 78 \pmod{713}$ by Thm 8.4.1 since $89^2 = (713)(11) + 78$.

$89^4 = (89^2)^2 \equiv 78^2 \equiv 380 \pmod{713}$, by Theorem 8.4.3 and by Thm 8.4.1 since $78^2 = (713)(8) + 380$.

$\therefore 89^4 \equiv 380 \pmod{713}$

$89^8 = (89^4)^2 \equiv 380^2 \equiv 374 \pmod{713}$, by Thm 8.4.3 and by Thm 8.4.1 since $380^2 = (713)(202) + 374$.

$\therefore 89^8 \equiv 374 \pmod{713}$

$89^{16} = (89^8)^2 \equiv 374^2 \equiv 128 \pmod{713}$, by Thm 8.4.3 and by Thm 8.4.1 since $374^2 = (713)(196) + 128$.

→ $\therefore 89^{16} \equiv 128 \pmod{713}$.

Solution for Sec 8.4, #17 (continued)

$89^{32} = (89^{16})^2 \equiv 128^2 \equiv 698 \pmod{713}$, by Thm 8.4.3 and by Thm 8.4.1 since $128^2 = (713)(22) + 698$.

$\rightarrow$ $\therefore 89^{32} \equiv 698 \pmod{713}$.

$89^{64} = (89^{32})^2 \equiv 698^2 \equiv 225 \pmod{713}$, by Thm 8.4.3 and by Thm 8.4.1 since $698^2 = (713)(683) + 225$.

$\therefore 89^{64} \equiv 225 \pmod{713}$

$89^{128} = (89^{64})^2 \equiv 225^2 \equiv 2 \pmod{713}$, by Thm 8.4.3 and by Thm 8.4.1 since $225^2 = (713)(71) + 2$.

$\therefore 89^{128} \equiv 2 \pmod{713}$.

$\therefore 89^{256} = (89^{128})^2 \equiv 2^2 \equiv 4 \pmod{713}$ by Thm 8.4.3 and the fact that $2^2 = 4$.

$\rightarrow$ $\therefore 89^{256} \equiv 4 \pmod{713}$.

To Summarize:

$$\begin{aligned}
89^{256} &\equiv 4 \pmod{713} \\
89^{32} &\equiv 698 \pmod{713} \\
89^{16} &\equiv 128 \pmod{713} \\
89^{2} &\equiv 78 \pmod{713} \\
89 &\equiv 89 \pmod{713}
\end{aligned}$$

SOLUTION to Sec 8.4, #17 (continued)

RECALL that $89^{307} = (89^{256})(89^{32})(89^{16})(89^{2})(89)$

$\therefore (89^{256}) \equiv [(4)(698)(128)(78)(89)] \pmod{713}$ by Theorem 8.4.3.

$(89^{256})(89^{32}) \equiv (4)(698) \equiv 653 \pmod{713}$, by Thm 8.4.3 and by Thm 8.4.1 since $(4)(698) = (713)(3) + 653$.

$\therefore [(89^{256})(89^{32})] \equiv 653 \pmod{713}$.

$(89^{16})(89^{2})(89) \equiv (128)(78)(89) \equiv 178 \pmod{713}$ by Thm 8.4.3 and by Thm 8.4.1 since $(128)(78)(89) = (713)(1246) + 178$.

$\therefore [(89^{16})(89^{2})(89)] \equiv 178 \pmod{713}$.

$\therefore 89^{307} \equiv (653)(178) \equiv 15 \pmod{713}$, by Thm 8.4.3 and Thm 8.4.1 since $(653)(178) = (713)(163) + 15$.

$\therefore 89^{307} \equiv 15 \pmod{713}$ and $(15 \bmod 713) = 15$ since $15 = (713)(0) + 15$ and $0 \leq 15 < 713$.

$\therefore$ By Theorem 8.4.1, $(89^{307} \bmod 713) = (15 \bmod 713) = 15$

$\therefore (89^{307} \bmod 713) = 15$

[END of SOLUTION.]