Example 12 Teacher's Solutions: Fast Modular Exponentiation

Worked Example

We already computed:

$$3^{544} \pmod{645} = 36$$

with full details shown in the worksheet.

—

Practice Problem Solutions

1. Easier: $2^{13} \pmod{19}$

   Binary expansion of $13 = (1101)_2$. Steps:

   $$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^4 \equiv 16,\ 2^8 \equiv 9 \pmod{19}.$$

   Multiply relevant powers: $2^8 \cdot 2^4 \cdot 2^1 \equiv 9 \cdot 16 \cdot 2 \equiv 288 \equiv 3 \pmod{19}$.

   Answer: $\boxed{3}$.

   —

2. Medium: $7^{45} \pmod{50}$

   Binary expansion of $45 = (101101)_2$. Steps:

   $$7^1 \equiv 7,\ 7^2 \equiv -1 \equiv 49 \pmod{50}.$$

   Notice $7^2 \equiv -1$. Then $7^{44} = (7^2)^{22} \equiv (-1)^{22} \equiv 1 \pmod{50}$. Multiply one more factor of 7: $7^{45} \equiv 7 \pmod{50}$.

   Answer: $\boxed{7}$.

   —

3. Harder: $11^{117} \pmod{221}$

   Note: $221 = 13 \cdot 17$. Apply the Chinese Remainder Theorem.

   Mod 13: $\varphi(13) = 12$. Reduce $117 \equiv 9 \pmod{12}$. So $11^{117} \equiv 11^9 \pmod{13}$. Compute: $11 \equiv -2 \pmod{13}$, so $(-2)^9 \equiv -512 \equiv 11 \pmod{13}$.

   Mod 17: $\varphi(17) = 16$. Reduce $117 \equiv 5 \pmod{16}$. So $11^{117} \equiv 11^5 \pmod{17}$. Compute: $11^2 = 121 \equiv 2 \pmod{17}$, $11^4 \equiv 2^2 = 4$, so $11^5 \equiv 11 \cdot 4 = 44 \equiv 10 \pmod{17}$.

   Solve CRT system:

   $$x \equiv 11 \pmod{13}, \quad x \equiv 10 \pmod{17}.$$

   Answer: $\boxed{142}$.