Homework 24 Solutions

1. (a) **What are the last three digits of 7^{1217}?**

Asking for the last three digits is the same as asking for $7^{1217} \pmod{1000}$. We know that $1000 = 2^3 \cdot 5^3$, and thus

$$\phi(1000) = 2^3 \cdot 5^3 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400.$$

Since 7 and 1000 are relatively prime, Euler's theorem tells us that $7^{400} \equiv 1 \pmod{1000}$. Hence

$$7^{1217} \equiv \left(7^{400}\right)^3 \cdot 7^{17} \equiv 7^{17} \pmod{1000}.$$

Successive squaring gives

$$\begin{aligned} 7^2 &\equiv 49 \\ 7^4 &\equiv 2401 \equiv 401 \\ 7^8 &\equiv 160801 \equiv 801 \\ 7^{16} &\equiv 641601 \equiv 601 \end{aligned}$$

where all the congruences are taken (mod 1000). Thus

$$7^{17} \equiv 7^{16} \cdot 7 \equiv 601 \cdot 7 \equiv 4207 \equiv \boxed{207} \pmod{1000}.$$

(b) **What are the last two digits of $3^{\left(3^{333}\right)}$? Note: This is not the same number as $\left(3^3\right)^{333}$.**

This is the same as asking for $3^{\left(3^{333}\right)} \pmod{100}$. We know that $100 = 2^2 \cdot 5^2$ and thus

$$\phi(100) = 2^2 \cdot 5^2 \cdot \frac{1}{2} \cdot 45 = 40.$$

Since 3 and 100 are relatively prime, Euler's theorem implies that we can reduce the exponent of 3 in arithmetic (mod 40). More explicitly, let $x \equiv 3^{333} \pmod{40}$. Then Euler's theorem implies that $3^{\left(3^{333}\right)} \equiv 3^x \pmod{100}$.

At this point, it's clear that we should compute x. To do so, we will again use Euler's theorem. We see that $40 = 2^3 \cdot 5$ and thus $\phi(40) = 16$. Since 3 and 16 are relatively prime, we can write

$$3^{333} \equiv \left(3^{16}\right)^{20} \cdot 3^{13} \equiv 3^{13} \pmod{40}.$$

We have

$$\begin{aligned} 3^2 &\equiv 9 \pmod{40} \\ 3^4 &\equiv 81 \equiv 1 \pmod{40} \\ 3^{12} &\equiv \left(3^4\right)^3 \equiv 1 \pmod{40} \end{aligned}$$

and thus $3^{13} \equiv 3 \pmod{40}$. In other words, we've shown that $x \equiv 3 \pmod{40}$. Using this, we see that

$$3^{\left(3^{333}\right)} \equiv 3^3 \equiv \boxed{27} \pmod{100}.$$

2. (a) **Compute the 11th root of 2 (mod 105).**

We start by checking that 2 and 105 are relatively prime, which they obviously are. Next we compute $\phi(105)$. Since $105 = 3 \cdot 5 \cdot 7$, we have

$$\phi(105) = 3 \cdot 5 \cdot 7 \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 2 \cdot 4 \cdot 6 = 48.$$

Now we need to solve $11x + 48y = 1$. The Euclidean algorithm gives

$$\begin{aligned} 48 &= 4 \cdot 11 + 4 \\ 11 &= 2 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \end{aligned}$$

Going backwards we get

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (11 - 2 \cdot 4) = 3 \cdot 4 - 11 \\ &= 3(48 - 4 \cdot 11) - 11 = 3 \cdot 48 - 13 \cdot 11. \end{aligned}$$

So we can take $x = -13$, and thus $2^{1/11} \equiv 2^{-13} \equiv 2^{35} \pmod{105}$, where we've used Euler's theorem again to make the exponent positive.
The final step is to compute $2^{35} \pmod{105}$. Successive squaring gives:

$$\begin{aligned} 2^2 &\equiv 4 \\ 2^4 &\equiv 16 \\ 2^8 &\equiv 256 \equiv 46 \\ 2^{16} &\equiv 2116 \equiv 16 \\ 2^{32} &\equiv 46 \end{aligned}$$

where all of these congruences are taken (mod 105). Thus we have

$$2^{35} \equiv 2^{32} \cdot 2^2 \cdot 2 \equiv 46 \cdot 4 \cdot 2 = 368 \equiv \boxed{53} \pmod{105}.$$

(b) **Compute the 5th root of** 4 (mod 43)**.**
Since 43 is prime, we can apply Fermat's theorem. (Note that this agrees with what we get if we apply Euler's theorem, since $\phi(43) = 42$.) So we need to solve $5x + 42y = 1$. The Euclidean algorithm gives

$$\begin{aligned} 42 &= 8 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

Going backwards we get

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ 1 &= 5 - 2(42 - 8 \cdot 5) = -2 \cdot 42 + 17 \cdot 5. \end{aligned}$$

So we can take $x = 17$, and thus $4^{1/5} \equiv 4^{17} \pmod{43}$.
The final step is to compute $4^{17} \pmod{43}$. Successive squaring gives:

$$\begin{aligned} 4^2 &\equiv 16 \\ 4^4 &\equiv 256 \equiv 41 \equiv -2 \\ 4^8 &\equiv 4 \\ 4^{16} &\equiv 16 \end{aligned}$$

where all of these congruences are taken (mod 43). Thus we have

$$4^{17} \equiv 4^{16} \cdot 4 \equiv 16 \cdot 4 \equiv 64 \equiv \boxed{21} \pmod{43}.$$

3. **Determine** $x \pmod{703}$ **given that** $x \equiv 1 \pmod{19}$ **and** $x \equiv 4 \pmod{37}$**.**

Since $19 \cdot 37 = 703$, the Chinese remainder theorem guarantees that this problem has a unique solution. The first congruence implies that $x = 1 + 19y$ for some y. The second implies that $x = 4 + 37z$ for some z. Setting these equal gives $1 + 19y = 4 + 37z$, which simplifies to $19y + 37(-z) = 3$. The Euclidean algorithm gives

$$\begin{aligned} 37 &= 19 + 18 \\ 19 &= 18 + 1. \end{aligned}$$

Running it backwards gives

$$\begin{aligned} 1 &= 19 - 18 \\ 1 &= 19 - (37 - 19) = -37 + 2 \cdot 19. \end{aligned}$$

Multiplying this last line by 3 gives $-3 \cdot 37 + 6 \cdot 19 = 3$. Thus we can take $y = 6$, which gives $x = 1 + 19 \cdot 6 \equiv \boxed{115} \pmod{703}$.