Problem 1

Factor $21,000,000$ and use the factorization to find $\phi(21,000,000)$.

$$\begin{aligned}21000000 &= 21 \cdot 10^6\\ &= 3 \cdot 7 \cdot (2 \cdot 5)^6\\ &= 3 \cdot 7 \cdot 2^6 \cdot 5^6\\ &= 2^6 \cdot 3^1 \cdot 5^6 \cdot 7^1\end{aligned}$$

Thus, we have

$$\begin{aligned}\phi(21000000) &= 21000000(1 - \frac{1}{2})\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)\\ &= 21000000 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7}\\ &= 21000000 \cdot \frac{1}{\cancel{2}} \cdot \frac{\cancel{2}}{\cancel{3}} \cdot \frac{4}{5} \cdot \frac{\cancel{6}\,2}{7}\\ &= 21000000 \cdot \frac{8}{35}\\ &= 4800000\end{aligned}$$

Problem 2

Calculate 17^{17} and 35^{35} modulo 48.

$(17, 48) = 1$ and $(35, 48) = 1$, so it seems that we can use Euler's theorem! $48 = 2^4 \cdot 3$.

$$\begin{aligned}\phi(48) &= 48\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\\ &= 48 \cdot \frac{1}{2} \cdot \frac{2}{3}\\ &= 48 \cdot \frac{1}{\cancel{2}} \cdot \frac{\cancel{2}}{3}\\ &= 16\end{aligned}$$

Thus, $17^{16} \equiv 35^{16} \equiv 1 \pmod{48}$.

$$\begin{aligned}17^{17} &\equiv 17^{16+1} \pmod{48}\\ &\equiv 17^{16} \cdot 17^1 \pmod{48}\\ &\equiv 1 \cdot 17 \pmod{48}\\ &\equiv \mathbf{17} \pmod{\mathbf{48}}\end{aligned}$$

$$\begin{aligned}35^{35} &\equiv 35^{16 \cdot 2+3} \pmod{48}\\ &\equiv (35^{16})^2 \cdot 35^3 \pmod{48}\\ &\equiv 1^2 \cdot 42875 \pmod{48}\\ &\equiv 42875 \pmod{48}\\ &\equiv \mathbf{11} \pmod{\mathbf{48}}\end{aligned}$$

Problem 3

Calculate $650^{650} \pmod{240}$.

$650 = 240*2+170$, so $650^{650} \equiv (240\cdot 2+170)^{650} \equiv 170^{650} \pmod{240}$. $240 = 16\cdot 15$. $(16,15) = 1$, so we can use the Chinese Remainder Theorem. First, we need to find $170^{650} \pmod{16}$.

$$\begin{aligned}170^{650} &\equiv (16\cdot 10+10)^{650} \pmod{16}\\ &\equiv 10^{650} \pmod{16}\end{aligned}$$

$16 = 2^4$, so if we multiply by 5^4, we get 10^4. Thus, $16|10^4$, so $10^4 \equiv 0 \pmod{16}$.

$$\begin{aligned}10^{650} &\equiv 10^{4\cdot 162+2} \pmod{16}\\ &\equiv (10^4)^{162}\cdot 10^2 \pmod{16}\\ &\equiv 0^{162}\cdot 10^2 \pmod{16}\\ &\equiv 0 \pmod{16}\end{aligned}$$

So, $170^{650} \equiv 0 \pmod{16}$. Now, let's calculate $170^{650} \pmod{15}$.

$$\begin{aligned}170^{650} &\equiv (15\cdot 11+5)^{650} \pmod{15}\\ &\equiv 5^{650} \pmod{15}\end{aligned}$$

Now, let's make a list of $5^n \pmod{15}$.

$$\begin{aligned}5^1 &\equiv 5 \pmod{15}\\ 5^2 &\equiv 25 \equiv 10 \pmod{15}\\ 5^3 &\equiv 50 \equiv 5 \pmod{15}\\ 5^4 &\equiv 25 \equiv 10 \pmod{15}\\ 5^5 &\equiv 50 \equiv 5 \pmod{15}\\ &\vdots\end{aligned}$$

As we can see, this is a cycle between 5 and 10. 5 to an even power $\equiv 10 \pmod{15}$ and 5 to an odd power $\equiv 5 \pmod{15}$. Since 650 is even, $5^{650} \pmod{15} \equiv 10 \pmod{15}$. So, we have two congruences:

$$\begin{aligned}170^{650} &\equiv 0 \pmod{16}\\ 170^{650} &\equiv 10 \pmod{15}\end{aligned}$$

Now, let's use the Chinese Remainder Theorem with $x = 170^{650}$.

$$\begin{aligned}x &\equiv 0 \pmod{16} &&(1)\\ x &= 16k_1 \text{ for } k_1 \in \mathbb{Z}\\ 16k_1 &\equiv 10 \pmod{15} &&(2)\\ k_1 &\equiv 10 \pmod{15}\\ k_1 &= 10+15k_2 \text{ for } k_2 \in \mathbb{Z}\\ x &= 16(10+15k_2)\\ x &= 160+240k_2\\ x &\equiv 160 \pmod{240} &&(3)\end{aligned}$$

Thus, $650^{650} \equiv 160 \pmod{240}$.

Problem 4

The number 137 is prime. What are the possibilities for a^{68} to be congruent to, modulo 137.

There are two cases for a: it is coprime to 137, or it is not. If a is not coprime to 137, then they share a factor $\neq 1$. However, the only other factor of 137 is 137, so $137|a$. Thus, in this case, $a^{68} \equiv 0 \pmod{137}$. If a is coprime to 137, then we can use Fermat's little theorem: $a^{136} \equiv 1 \pmod{137}$. Let $a^{68} \equiv x \pmod{137}$. We notice that $a^{136} = a^{68\cdot 2} \equiv a^{68} \cdot a^{68}$. Since modulus is multiplicative, $a^{68} \cdot a^{68} \equiv a^{136} \pmod{137}$. Thus, $x^2 \equiv 1 \pmod{137}$. This means that either $x \equiv 1 \pmod{137}$ or $x \equiv -1 \pmod{137}$ when a is coprime to 137. So, the possibilities for a^{68} to be congruent to modulo 137 are 0, 1, and -1.

Problem 5

Verify that 25 is a base-7 pseudoprime.

We need to verify that $7^{25} \equiv 7 \pmod{25}$. Since $(7, 25) = 1$, we can use Euler's theorem. First, we need to find $\phi(25)$.

$$\begin{aligned} 25 &= 5^2 \\ \phi(25) &= 25\left(1 - \frac{1}{5}\right) \\ &= 25 \cdot \frac{4}{5} \\ &= 20 \end{aligned}$$

Thus, $7^{20} \equiv 1 \pmod{25}$. Let's make a list of the repeated squaring method.

$$\begin{aligned} &7^1 \equiv 7 \pmod{25} \\ &7^2 \equiv 7^2 \equiv 49 \equiv 24 \pmod{25} \\ &7^4 \equiv 24^2 \cdot 576 \equiv 1 \equiv 576 \equiv 1 \pmod{25} \end{aligned}$$

Now, lets calculate $7^{25} \pmod{25}$.

$$\begin{aligned} 7^{25} &\equiv 7^{20+4+1} \pmod{25} \\ &\equiv 7^{20} \cdot 7^4 \cdot 7^1 \pmod{25} \\ &\equiv 1 \cdot 1 \cdot 7 \pmod{25} \\ &\equiv 7 \pmod{25} \end{aligned}$$

Thus, $7^{25} \equiv 7 \pmod{25}$, so we have shown that 25 is a base-7 pseudoprime.

Problem 6

Verify that $2047 = 23 \cdot 89$ is a base-2 pseudoprime.

We need to verify that $2^{2047} \equiv 2 \pmod{2047}$. Since $(2, 2047) = 1$, we can use Euler's theorem. First, we need to find $\phi(2047)$. We are given that $2047 = 23 \cdot 89$.

$$\begin{aligned} \phi(2047) &= 2047\left(1 - \frac{1}{23}\right)\left(1 - \frac{1}{89}\right) \\ &= 2047 \cdot \frac{22}{23} \cdot \frac{88}{89} \\ &= 22 \cdot 88 \\ &= 1936 \end{aligned}$$

So, $2^{1936} \equiv 1 \pmod{2047}$. Now, let's make a list with the repeated squaring method.

$$\begin{aligned}
2^1 &\equiv 2 \pmod{2047}\\
2^2 &\equiv 4 \pmod{2047}\\
2^4 &\equiv 16 \pmod{2047}\\
2^8 &\equiv 256 \pmod{2047}\\
2^{16} &\equiv 256^2 \equiv 65536 \equiv 32 \pmod{2047}\\
2^{32} &\equiv 32^2 \equiv 1024 \pmod{2047}\\
2^{64} &\equiv 1024^2 \equiv 1048576 \equiv 512 \pmod{2047}
\end{aligned}$$

Now, let's calculate $2^{2047} \pmod{2047}$.

$$\begin{aligned}
2^{2047} &\equiv 2^{1936+64+32+8+4+2+1} \pmod{2047}\\
&\equiv 2^{1936} \cdot 2^{64} \cdot 2^{32} \cdot 2^8 \cdot 2^4 \cdot 2^2 \cdot 2^1 \pmod{2047}\\
&\equiv 1 \cdot 512 \cdot 1024 \cdot 256 \cdot 16 \cdot 4 \cdot 2 \pmod{2047}\\
&\equiv 2 \cdot 256 \cdot 1024 \cdot 256 \cdot 16 \cdot 4 \cdot 2 \pmod{2047}\\
&\equiv 1024 \cdot (256 \cdot 256) \cdot (16 \cdot 4 \cdot 2 \cdot 2) \pmod{2047}\\
&\equiv 4 \cdot 256 \cdot 256^2 \cdot 16^2 \pmod{2407}\\
&\equiv 4 \cdot 256 \cdot 32 \cdot 256 \pmod{2047}\\
&\equiv 4 \cdot 256^2 \cdot 32 \pmod{2047}\\
&\equiv 4 \cdot 32 \cdot 32 \pmod{2047}\\
&\equiv 4 \cdot 32^2 \pmod{2047}\\
&\equiv 4 \cdot 1024 \pmod{2047}\\
&\equiv 4096 \pmod{2047}\\
&\equiv 2047 \cdot 2 + 2 pmod 2047\\
&\equiv 2 \pmod{2047}
\end{aligned}$$

Thus, $2^{2047} \equiv 2 \pmod{2047}$, so we have shown that 247 is a base-2 pseudoprime.