Homework 19 Solutions

1. (a) **What does Fermat's Theorem say about powers** $\pmod{43}$**?**
   Since 43 is prime, Fermat's Theorem says that, for any a which is not a multiple of 43 (equivalently, $a \not\equiv 0 \pmod{43}$), we have that $a^{42} \equiv 1 \pmod{43}$.

   (b) **Compute** $3^{126} \pmod{43}$**.**
   Using Fermat's Theorem, we see that

$$3^{126} \equiv \left(3^{42}\right)^3 \equiv 1^3 \equiv \boxed{1} \pmod{43}.$$

   (c) **Compute** $2^{286} \pmod{43}$**.**
   Again using Fermat's Theorem, we see that

$$2^{286} \equiv \left(2^{42}\right)^6 \cdot 2^{34} \equiv 1^6 \cdot 2^{34} \equiv 2^{34} \pmod{43}.$$

   So now we just need to compute $2^{34} \pmod{43}$. Successive squaring gives

$$\begin{aligned} 2^2 &\equiv 4, \\ 2^4 &\equiv 16, \\ 2^8 &\equiv 256 \equiv 41 \equiv -2, \\ 2^{16} &\equiv 4, \\ 2^{32} &\equiv 16, \end{aligned}$$

   where all of the congruences are $\pmod{43}$. Finally, we have

$$2^{34} \equiv 2^{32} \cdot 2^2 \equiv 16 \cdot 4 \equiv 64 \equiv \boxed{21} \pmod{43}.$$

2. **Do the following computations.**

   (a) $5^{1007} \pmod{53}$.
   Since 53 is prime, Fermat's theorem tells us that $5^{52} \equiv 1 \pmod{53}$. Hence,

$$5^{1007} \equiv \left(5^{52}\right)^{19} \cdot 5^{19} \equiv 5^{19} \pmod{53}.$$

   Successive squaring gives

$$\begin{aligned} 5^2 &\equiv 25, \\ 5^4 &\equiv 625 \equiv 42 \equiv -11, \\ 5^8 &\equiv 121 \equiv 15, \\ 5^{16} &\equiv 225 \equiv 13, \end{aligned}$$

   where all of the congruences are $\pmod{53}$. Finally, we have

$$5^{19} \equiv 5^{16} \cdot 5^2 \cdot 5 \equiv 13 \cdot 25 \cdot 5 \equiv 65 \cdot 25 \equiv 12 \cdot 25 \equiv 300 \equiv \boxed{35} \pmod{53}.$$

   (b) $10^{998} \pmod{999}$.
   Since 999 is not prime, Fermat's Theorem does not apply. Nonetheless, we see directly that $10^3 \equiv 1000 \equiv 1 \pmod{999}$. Thus,

$$10^{998} \equiv \left(10^3\right)^{332} \cdot 10^2 \equiv \boxed{100} \pmod{999}.$$

(c) $7^{240} \pmod{53}$.

Fermat's theorem tells us that $7^{52} \equiv 1 \pmod{53}$. Thus,

$$7^{240} \equiv \left(7^{52}\right)^4 \cdot 7^{32} \equiv 7^{32} \pmod{53}.$$

Successive squaring gives

$$\begin{aligned} 7^2 &\equiv 49 \equiv -4, \\ 7^4 &\equiv 16, \\ 7^8 &\equiv 256 \equiv 44 \equiv -9, \\ 7^{16} &\equiv 81 \equiv 28 \equiv -25, \\ 7^{32} &\equiv 625 \equiv \boxed{42}, \end{aligned}$$

where all of the congruences are $\pmod{53}$.