Homework 20 Solutions

Problems

1. **(a) What does Fermat's Theorem say about powers** $\pmod{53}$**?**

   (b) Compute $3^{109} \pmod{53}$**.**

   (c) Compute $2^{270} \pmod{53}$**.**

   If $a \not\equiv 0 \pmod{53}$ then $a^{52} \equiv 1 \pmod{53}$.

   $3^{52} \equiv 1 \pmod{53}$ so $3^{109} \equiv 3^5 \equiv 243 \equiv \boxed{31} \pmod{53}$

   $2^{52} \equiv 1 \pmod{53}$ so $2^{270} \equiv 2^{10} \equiv \boxed{17} \pmod{53}$

2. **(a) What is the last digit of** 3^{991}**?**

   (b) Compute $3^{991} \pmod{11}$**.**

   (c) Compute $26^{991} \pmod{13}$**.**

   We compute $\pmod{10}$. Note that $3^4 \equiv 81 \equiv 1 \pmod{10}$.

   So $3^{991} \equiv 3^3 \equiv 7 \pmod{10}$. Hence the last digit is $\boxed{7}$.

   By Fermat we know that $3^{10} \equiv 1 \pmod{11}$. So $3^{991} \equiv 3^1 \equiv \boxed{3} \pmod{11}$.

   $26 \equiv 0 \pmod{13}$, so $26^{991} \equiv \boxed{0} \pmod{13}$.

3. (a) **Create a power table for arithmetic** $\pmod{13}$**. This will be a table whose rows correspond to numbers in arithmetic** $\pmod{13}$ **(that is, the numbers** $\{0, 1, 2, \ldots, 12\}$**), and whose entries are their various powers. Compute the powers from the 1st up to the 13th power for each number. (Remember, for example, that** $10 \equiv -3 \pmod{13}$ **and you can use this to avoid doing the computations for 10 once you've done them for 3.)**

   (b) **Compute** $2^{742} \pmod{13}$.

   The zeroth and first row are easy:

   $0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0$

   $1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1$

   and row 12 is just

   $12, 1, 12, 1, 12, 1, 12, 1, 12, 1, 12, 1, 12$

   We can just compute powers of 2 by repeatedly doubling until we get 12, and then negate the first half:

   $2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1, 2$

   The third row just has every 4th power of 2, since $2^4 \equiv 3$, but this is just $3, 9, 1$ repeating:

   $3, 9, 1, 3, 9, 1, 3, 9, 1, 3, 9, 1, 3$

   Likewise powers of 4 are the even powers of 2:

   $4, 3, 12, 9, 10, 1, 4, 3, 12, 9, 10, 1, 4$

   and similarly powers of 8 are the threeven powers of 2:

   $8, 12, 5, 1, 8, 12, 5, 1, 8, 12, 5, 1, 8$

   We get most of the remaining rows from reading backwards, as we know their inverses from the 11th column of the above:

   $5, 12, 8, 1, 5, 12, 8, 1, 5, 12, 8, 1, 5$

   $7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1, 7$

$9, 3, 1, 9, 3, 1, 9, 3, 1, 9, 3, 1, 9$

$10, 9, 12, 3, 4, 1, 10, 9, 12, 3, 4, 1, 10$

Row 6 is row 7 with the odd terms switched in sign:

$6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1, 6$

and row 11 is row 6 reversed:

$11, 4, 5, 3, 7, 12, 2, 9, 8, 10, 6, 1, 11$

$2^{742} \equiv 2^{61\times 12+10} \equiv 2^{10} \equiv \boxed{10} \pmod{13}$