Math 221-001 201710
Assignment # 6 - Answers

1.

(a) Find the remainder when 8^{4325} is divided by 3;
Answer. We have $8 \equiv 2 \pmod 3$. Also, $2^2 \equiv 1 \pmod 3$. Then

$$8^{4325} \equiv 2^{4325} = 2 \times 2^{4324} = 2 \times (2^2)^{2162} \equiv 2 \pmod 3.$$

So the remainder is 2.
An even easier way is to notice that $8 \equiv (-1) \pmod 3$. So

$$8^{4325} \equiv (-1)^{4325} = -1 \equiv 2 \pmod 3.$$

(b) Find the last two digits of 8^{4325}.
Answer. Note that $8^{4325} = 2^{12975}$, since $8 = 2^3$. Since $2^{10} = 1024 \equiv 24 \pmod{100}$. With a little experimentation we find the following: $24^2 = 576$, and $576 \times 4 = 2304$. Thus

$$4 \equiv 2304 = 24^2 \times 4 \equiv (2^{10})^2 \times 2^{=}2^{22} \pmod{100}.$$

In other words $2^{22} \equiv 2^2 \pmod{100}$. Using long division, we find that $12975 = 589 \times 22 + 17$. Then, modulo 100,

$$\begin{aligned} 2^{12975} &= (2^{22})^{589} \times 2^{17} \equiv 2^{2\times 589} \times 2^{17} = 2^{1195} = 2^{22\times 54+7} = (2^{22})^{54} \times 2^7 \\ &\equiv 2^{2\times 54} \times 2^7 = 2^{115} = 2^{22\times 5} + 5 \equiv 2^{2\times 5} + 5 = 2^{15} = 2^{10}2^5 \\ &= 1024 \times 32 \equiv 24 \times 32 = 768 \equiv 68 \pmod{100}. \end{aligned}$$

Here is a slightly more efficient method: from the above expression $2^{22} \equiv 2^2 \pmod{100}$, we have the following:

$$2^{n+20} = 2^{n-2+22} = 2^{n-2}2^{22} \equiv 2^{n-2}2^2 = 2^{n-2+2} = 2^n \pmod{100}.$$

So the last two digits repeat on cycles of 20. Iterating the equality above,

$$2^{n+20k} \equiv 2^n \pmod{100}.$$

Then, as $12975 = 20 \times 648 + 15$, we have

$$2^{12975} = 2^{20\times 648+15} \equiv 2^{15} \pmod{100},$$

and we can jump directly into the last line of the first proof.
A third method: by the Lemma from class, the congruence $x \equiv 8^{4325} \pmod{100}$ is the same as the two simultaneous congruences

$$\begin{cases} x \equiv 8^{4325} \pmod 4 \\ x \equiv 8^{4325} \pmod{25} \end{cases}$$

since 4 and 25 are coprime. But $8 \equiv 0 \pmod 4$, so the first congruence reduces to $x \equiv 0 \pmod 4$. Since 8 is coprime with 25, Fermat's Little Theorem gives us $8^{24} \equiv 1 \pmod{25}$. From $4325 = 24 \times 180 + 5$, we obtain

$$8^{4325} = 8^{24\times 180+5} \equiv 8^5 \pmod{25} \equiv 68 \pmod{25}$$

(the last equality, either by calculating 8^5 directly, or by doing $8^2 = 64 \equiv 14 \pmod{25}$, $8^4 \equiv 14^2 = 196 \equiv 21 \pmod{25}$, $8^5 \equiv 21 \times 8 \equiv 68 \pmod{25}$). So 68 satisfies both congruences and is a solution of $x = 8^{4325} \pmod{100}$. As per the Lemma, the solution is unique module 100, so there is no ambiguity.

2. Is $6^{17} + 17^6$ divisible by 3? By 7?

   Answer. Modulo 3, $6 \equiv 0 \pmod 3$ and $17 \equiv 2 \pmod 3$. Thus

   $$6^{17} + 17^6 \equiv 0 + 2^6 \pmod 3.$$

   A power of two can never be a multiple of 3 (because of the uniqueness of the prime decomposition) and so $6^{17} + 17^6$ is not a multiple of 3.

   Modulo 7, $6 \equiv (-1) \pmod 7$ and $17 \equiv 3 \pmod 7$. Then

   $$6^{17} + 17^6 \equiv (-1)^{17} + 3^6 = -1 + 9^3 \equiv -1 + 2^3 = -1 + 8 = 7 \equiv 0 \pmod 7.$$

   So $6^{17} + 17^6$ is a multiple of 7.

3. Solve

   (a) $3x \equiv 1 \pmod{13}$;

   Answer. We need to isolate x. Since $(3, 13) = 1$, we know that 3 admits a multiplicative inverse. We could use the Euclidean Algorithm, or simply note that $3 \times 9 = 27 = 2 \times 13 + 1$. So $9 \times 3 \equiv 1 \pmod{13}$. Then, multiplying the congruence on both sides by 9, we get

   $$x \equiv 9 \pmod{13}.$$

   And that's the solution: $x = 9 + 13k$, $k \in \mathbb{Z}$.

   (b) $54x \equiv 17 \pmod{13}$;

   Answer. We can simplify the expression above, since $54 \equiv 2 \pmod{13}$ ($54 = 4 \times 13 + 2$). So, as $17 \equiv 4 \pmod{13}$, the equation becomes $2x \equiv 4 \pmod{13}$. This has the obvious solution $x = 2$, but are there others? Note that $7 \times 2 \equiv 1 \pmod{13}$. So multiplying by 7 we get

   $$x \equiv 7 \times 2x \equiv 7 \times 4 \equiv 2 \pmod{13}$$

   (since $4 \times 7 = 28 = 2 \times 13 + 2$). Thus $x \equiv 2 \pmod{13}$ is the solution, or $x = 2 + 13k$, $k \in \mathbb{Z}$.

(c) $57x + 7 \equiv 78 \pmod{53}$).

Answer. We have $57 \equiv 4 \pmod{53}$ and $78 \equiv 25 \pmod{53}$, so the congruence becomes

$$4x + 7 \equiv 25 \pmod{53}.$$

We can also subtract 7 from both sides to get

$$4x \equiv 18 \pmod{53}.$$

As 4 and 53 are coprime, we know that 4 admits a multiplicative inverse module 53. To find it, we use the Euclidean Algorithm:

$$\begin{array}{cccc} 1 & 0 & 53 & \\ 0 & 1 & 4 & 13 \\ 1 & -13 & 1 & \end{array}$$

We get (or we could have noticed directly) that $1 = 53 - 52 = 53 - 4 \times 13$). That is, $4 \times (-13) \equiv 1 \pmod{53}$. As $-13 + 53 = 40$, we have that $4 \times 40 \equiv 1 \pmod{13}$. So we can multiply the original congruence by 40 to get

$$x = 40 \times 4x \equiv 40 \times 18 \equiv 31 \pmod{53}.$$

So the solutions are of the form $x = 31 + 53k$, $k \in \mathbb{Z}$.

4. Prove that if m is an integer, then either $m^2 \equiv 0 \pmod{4}$ of $m^2 \equiv 1 \pmod{4}$ (Hint: prove it separately for m even and for m odd).

Answer. If m is even, then $m = 2k$ for some $k \in \mathbb{Z}$. Then $m^2 = 4k^2 \equiv 0 \pmod{4}$. If m is odd, then $m = 2k + 1$ for some $k \in \mathbb{Z}$. Then

$$m^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1 \equiv 0 \pmod{4}.$$