Name: *Caleb McWhorter — Solutions*
MATH 308
Fall 2022
HW 12: Due 11/04

"Algebra is the intellectual instrument which has been created for rendering clear the quantitative aspects of the world."
–Alfred North Whitehead

Problem 1. (10pt) Showing all your work, complete the following:

(a) Find the last digit of 3^{300}.

(b) Find the last two digits of 13^{100}.

(c) Fermat's Little Theorem states that if p is prime, then $a^p \equiv a \mod p$. Verify this claim when $p = 5$ and $a = 3$.

(d) A generalization of Fermat's Little Theorem states that $a^{\varphi(n)} \equiv 1 \mod n$ if a is coprime to n, where $\varphi(n)$ is the Euler Phi function. Verify this claim when $n = 3$ and $a = 8$.

Solution.

(a) Given an n-digit number $a := a_{n-1}a_{n-2}\cdots a_3a_2a_1a_0$, we can write $a_{n-1}a_{n-2}\cdots a_2a_1 \cdot 10 + a_0$ so that $a \equiv a_{n-1}a_{n-2}\cdots a_2a_1 \cdot 10 + a_0 \equiv a_0 \mod 10$. For example, $175892 \equiv 175890 + 2 \equiv 17589 \cdot 10 + 2 \equiv 2 \mod 10$. Therefore, the last digit of an integer is its reduction modulo 10. Observe that...

$$
\begin{aligned}
3^0 &\equiv 1 \quad \text{mod } 10 & 3^{16} &\equiv 1^2 \equiv 1 \quad \text{mod } 10 \\
3^1 &\equiv 3 \quad \text{mod } 10 & 3^{32} &\equiv 1^2 \equiv 1 \quad \text{mod } 10 \\
3^2 &\equiv 9 \quad \text{mod } 10 & 3^{64} &\equiv 1^2 \equiv 1 \quad \text{mod } 10 \\
3^4 &\equiv 9^2 \equiv 81 \equiv 1 \quad \text{mod } 10 & 3^{128} &\equiv 1^2 \equiv 1 \quad \text{mod } 10 \\
3^8 &\equiv 1^2 \equiv 1 \quad \text{mod } 10 & 3^{256} &\equiv 1^2 \equiv 1 \quad \text{mod } 10
\end{aligned}
$$

But then we have...

$$3^{300} \equiv 3^{256+32+8+4} \equiv 3^{256} \cdot 3^{32} \cdot 3^8 \cdot 3^4 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \equiv 1 \quad \text{mod } 10$$

Therefore, the last digit of 3^{300} is 1.

(b) Given an n-digit number $a := a_{n-1}a_{n-2}\cdots a_3a_2a_1a_0$, we can write $a_{n-1}a_{n-2}\cdots a_2 \cdot 100 + a_1a_0$ so that $a \equiv a_{n-1}a_{n-2}\cdots a_2 \cdot 100 + a_1a_0 \equiv a_1a_0 \mod 100$. For example, $175892 \equiv 175800 + 92 \equiv 1758 \cdot 100 + 92 \equiv 92 \mod 100$. Therefore, the last two digits of an integer are its reduction modulo 100. Observe that...

$$
\begin{aligned}
13^0 &\equiv 1 \quad \text{mod } 100 & 13^8 &\equiv 61^2 \equiv 3721 \equiv 21 \quad \text{mod } 100 \\
13^1 &\equiv 13 \quad \text{mod } 100 & 13^{16} &\equiv 21^2 \equiv 441 \equiv 41 \quad \text{mod } 100 \\
13^2 &\equiv 13^2 \equiv 169 \equiv 69 \quad \text{mod } 100 & 13^{32} &\equiv 41^2 \equiv 1681 \equiv 81 \quad \text{mod } 100 \\
13^4 &\equiv 69^2 \equiv 4761 \equiv 61 \quad \text{mod } 100 & 13^{64} &\equiv 81^2 \equiv 6561 \equiv 61 \quad \text{mod } 100
\end{aligned}
$$

But then we have...

$$3^{100} \equiv 3^{64+32+4} \equiv 3^{64} \cdot 3^{32} \cdot 3^4 \equiv 61 \cdot 81 \cdot 61 \equiv 4941 \cdot 61 \equiv 41 \cdot 61 \equiv 2501 \equiv 1 \quad \text{mod } 100$$

Therefore, the last two digits of 13^{100} are 01.

(c) We have...

$$3^5 \equiv 3^2 \cdot 3^2 \cdot 3 \equiv 9 \cdot 9 \cdot 3 \equiv 4 \cdot 4 \cdot 3 \equiv 16 \cdot 3 \equiv 1 \cdot 3 \equiv 3 \mod 5$$

But then $3^5 \equiv 3 \mod 5$.

(d) We have $\gcd(a, n) = \gcd(8, 3) = 1$ so that 8 and 3 are coprime. Now $\phi(3) = 3 - 1 = 2$. But then we have...

$$8^{\phi(3)} \equiv 8^2 \equiv 2^2 \equiv 4 \equiv 1$$

But then $8^{\phi(3)} \equiv 1 \mod 3$.

Problem 2. (10pt) Showing all your work, compute the following:

(a) Compute 147 modulo 3.

(b) Compute 147 modulo 3 by writing $147 = 1 \cdot 100 + 4 \cdot 10 + 7 \cdot 1$.

(c) Compute $a_2a_1a_0$ modulo 3 by writing $a_2a_1a_0 = a_2 \cdot 100 + a_1 \cdot 10 + a_0 \cdot 1$. When is $a_2a_1a_0$ divisible by 3? Explain.

(d) Using the previous parts, give a necessary and sufficient condition for an integer to be divisible by 3.

Solution.

(a) Because we have $147 = 3(49) + 0$, we have $147 \equiv 0 \mod 3$. Notice that $147 \equiv 0 \mod 3$ implies that 147 is divisible by 3.

(b) Using the fact that $10 \equiv 1 \mod 3$, we have...

$$\begin{aligned} 147 &\equiv 1 \cdot 100 + 4 \cdot 10 + 7 \cdot 1 \\ &\equiv 1 \cdot 10^2 + 4 \cdot 10^1 + 7 \cdot 10^0 \\ &\equiv 1 \cdot 1^2 + 4 \cdot 1^1 + 7 \cdot 1^0 \\ &\equiv 1 + 4 + 7 \\ &\equiv 12 \\ &\equiv 0 \mod 3 \end{aligned}$$

(c) Using the fact that $10 \equiv 1 \mod 3$, we have...

$$\begin{aligned} a_2a_1a_0 &\equiv a_2 \cdot 100 + a_1 \cdot 10 + a_0 \cdot 1 \\ &\equiv a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 \\ &\equiv a_2 \cdot 1^2 + a_1 \cdot 1^1 + a_0 \cdot 1^0 \\ &\equiv a_2 + a_1 + a_0 \end{aligned}$$

Because $a_2a_1a_0$ is divisible by 3 if and only if $a_2a_1a_0 \equiv 0 \mod 3$. By the work above, $a_2a_1a_0$ is divisible by 3 if and only if $a_2+a_1+a_0 \equiv 0 \mod 3$, i.e. if and only if $a_2+a_1+a_0$ is divisible by 3. Therefore, a three digit number is divisible by 3 if and only if the sum of its digits is divisible by 3.

(d) We would predict using (c) that an integer is divisible by 3 if and only if the sum of its digits is divisible by 3. We can confirm this. If we have an n digit number, say $a = \sum_{i=0}^{n-1} a_i \cdot 10^i$, then a is divisible by 3 if and only if $a \equiv 0 \mod 3$. But this is...

$$0 \equiv a \equiv \sum_{i=0}^{n-1} a_i \cdot 10^i \equiv \sum_{i=0}^{n-1} a_i \cdot 1^i \equiv \sum_{i=0}^{n-1} a_i = a_{n-1} + a_{n-2} + \cdots + a_1 + a_0$$

Problem 3. (10pt) Use the Chinese Remainder Theorem to solve the following system of linear congruences

$$\begin{aligned} 2x &\equiv 1 \mod 3 \\ x - 3 &\equiv 0 \mod 4 \\ 3x + 2 &\equiv 4 \mod 5 \end{aligned}$$

Solution. First, we put this system of congruences into the form stated in the Chinese Remainder Theorem, i.e. a collection of congruences of the form $x \equiv a_i \mod n_i$. Observe...

$$\begin{aligned} 2x &\equiv 1 \mod 3 \\ 2^{-1} \cdot 2x &\equiv 2^{-1} \cdot 1 \mod 3 \\ x &\equiv 2 \cdot 1 \mod 3 \\ x &\equiv 2 \mod 3 \end{aligned}$$

$$\begin{aligned} x - 3 &\equiv 0 \mod 4 \\ x &\equiv 3 \mod 4 \end{aligned}$$

$$\begin{aligned} 3x + 2 &\equiv 4 \mod 5 \\ 3x &\equiv 2 \mod 5 \\ 3^{-1} \cdot 3x &\equiv 3^{-1} \cdot 2 \mod 5 \\ x &\equiv 2 \cdot 2 \mod 5 \\ x &\equiv 4 \mod 5 \end{aligned}$$

Because 3, 4, and 5 are coprime, the Chinese Remainder Theorem states that there is a unique solution modulo $M = \prod_i n_i = 3 \cdot 4 \cdot 5 = 60$. The Chinese Remainder Theorem also states that an integer solution to this system is $x = \sum a_i N_i M_i$. We have...

$$\begin{aligned} a_1 &= 2 \\ a_2 &= 3 \\ a_3 &= 4 \end{aligned}$$

Also, we have...

$$\begin{aligned} M_1 &= M/n_1 = 60/3 = 20, \text{i.e. } M_1 = 4 \cdot 5 = 20 \\ M_2 &= M/n_2 = 60/4 = 15, \text{i.e. } M_2 = 3 \cdot 5 = 15 \\ M_3 &= M/n_3 = 60/5 = 12, \text{i.e. } M_3 = 3 \cdot 4 = 12 \end{aligned}$$

Finally, $N_i := M_i^{-1} \mod n_i$. Now observe...

$$\begin{aligned} N_1 &:= M_1^{-1} \equiv 20^{-1} \equiv 2^{-1} \equiv 2 \mod 3 \\ N_2 &:= M_2^{-1} \equiv 15^{-1} \equiv (-1)^{-1} \equiv -1 \equiv 3 \mod 4 \\ N_3 &:= M_3^{-1} \equiv 12^{-1} \equiv 2^{-1} \equiv 3 \mod 5 \end{aligned}$$

We can check these: $20 \cdot 2 \equiv 2 \cdot 2 \equiv 4 \equiv 1 \mod 3$, $15 \cdot 3 \equiv 3 \cdot 3 \equiv 9 \equiv 1 \mod 4$, and $12 \cdot 3 \equiv 2 \cdot 3 \equiv 6 \equiv 1 \mod 5$. But then the solution to this system of congruences is...

$$\begin{aligned} \sum_{i=1}^{3} a_i N_i M_i &\equiv a_1 N_1 M_1 + a_2 N_2 M_2 + a_3 N_3 M_3 \\ &\equiv 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 4 \cdot 12 \cdot 3 \\ &\equiv 80 + 135 + 144 \\ &\equiv 20 + 15 + 24 \\ &\equiv 59 \mod 60 \end{aligned}$$

We can check this solution:

$$\begin{aligned} 2 \cdot 59 \equiv 2 \cdot 2 \equiv 4 &\equiv 1 \mod 3 \\ 59 - 3 \equiv 56 &\equiv 0 \mod 4 \\ 3 \cdot 59 + 2 \equiv 3 \cdot 4 + 2 \equiv 12 + 2 \equiv 2 + 2 &\equiv 4 \mod 5 \end{aligned}$$

Problem 4. (10pt) Show that there are no integer solutions to $x^3 + 7y^2 = 5$.

Solution. If there is a solution pair, x, y, to the equation $x^3 + 7y^2 = 5$, then reducing both sides modulo 7, there must be a mod 7 solution pair, $\overline{x}$, $\overline{y}$. But reducing modulo 7, we have...

$$5 \equiv \overline{x}^3 + 7\overline{y}^2 \equiv \overline{x}^3 + 0 \cdot \overline{y}^2 \equiv \overline{x}^3$$

But then 5 is a cube modulo 7. However, observe...

$$\begin{aligned}
0^3 &\equiv 0 \mod 7 \\
1^3 &\equiv 1 \mod 7 \\
2^3 &\equiv 8 \equiv 1 \mod 7 \\
3^3 &\equiv 3^2 \cdot 3 \equiv 9 \cdot 3 \equiv 2 \cdot 3 \equiv 6 \mod 7 \\
4^3 &\equiv 4^2 \cdot 4 \equiv 16 \cdot 4 \equiv 2 \cdot 4 \equiv 8 \equiv 1 \mod 7 \\
5^3 &\equiv 5^2 \cdot 5 \equiv 25 \cdot 5 \equiv 4 \cdot 5 \equiv 20 \equiv 6 \mod 7 \\
6^3 &\equiv 6^2 \cdot 6 \equiv 36 \cdot 6 \equiv 1 \cdot 6 \equiv 6 \mod 7
\end{aligned}$$

But no cube modulo 7 is 5, i.e. 5 is not a cube modulo 7. Therefore, there is no solution modulo 7 so that there cannot be an integer solution pair x, y to the original equation.