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 $p = 3$ and $a = 8$.

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.

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

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

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.