Math Circles Modular Arithmetic 2

Colin Curtis*

August 2, 2020

Recall: Let m be an integer, and let a, b be integers as well. Then we write $a \equiv b \pmod{m}$ (read "a is congruent to b mod m" if $m|(a-b)$ (read "m divides a minus b"), namely $a-b$ is a multiple of m. This is equivalent to the fact that there exists an integer k such that $a = b + km$.

Fermat's Little Theorem: Let p be any prime number, and let a be any integer. Then $a^{p-1} \equiv 1 \pmod{p}$. We can multiply through by a and get an equivalent form of $a^p \equiv a \pmod{p}$.

Example 1: let $a = 2$ and $p = 7$. Then $a^{p-1} = 2^6 = 64$. Notice that $64 = 7(9) + 1$, so using the definition for modulo we see that indeed $2^{7-1} \equiv 1 \pmod{7}$.

Example 2: Find $2^{35} \pmod{7}$
Solution: We notice that we're working mod 7, so by Fermat's Little Theorem we have $2^6 \equiv 1 \pmod{7}$. We recall that we can take positive exponents of both sides of a modulo expression, so raise both sides to the 5 power since we don't want to exceed the 35 power. Thus $(2^6)^5 \equiv 1^5 \pmod{7}$. Then multiply both sides by 2^5 to get the desired 35 power. Hence $2^{35} \equiv 2^5 \equiv 32 \equiv 4 \pmod{7}$, so $2^{35} \equiv 4 \pmod{7}$.

Problem 1: Find $128^{129} \pmod{17}$
hint: First find 128 (mod 17), then use Fermat's little theorem and raise each side to a suitable power.

Problem 2: Find the remainder when $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$ is divided by 7.
hint: use Fermat's Little Theorem on the numbers $2, 3, 4, 5, 6$ looking mod 7, then raise each part to a suitable power as in the previous problem and add all the results together.

Problem 3: Define the sequence $a_n = 4^{a_{n-1}}$ where $a_1 = 1$. Show by induction that $a_n \equiv 4 \pmod{7}$ for all $n \geq 1$.

*Problems taken from http://math.cmu.edu/ cargue/arml/archive/15-16/number-theory-09-27-15-solutions.pdf

Problem 4: Find all integers x such that $x^{86} \equiv 6 \pmod{29}$.
hint: use Fermat's Little Theorem on x and 29 and raise each side to a suitable power and add multiples of 29 onto the right hand side of the congruence until you get a perfect square that you can factor.

Problem 5: Show that $x^p \equiv x \pmod{p}$ by using induction on x, where x is any integer and p is a prime number. Use the fact that $(x+1)^p \equiv x^p + 1 \pmod{p}$ in the inductive step.