Math Circles Modular Arithmetic 1

Colin Curtis

July 26, 2020

Definition: 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 $a = b + km$.

A few computations: Find x (not necessarily one value)
$18 \equiv x \pmod{7}$ $\quad 52 \equiv x \pmod{12}$ $\quad x \equiv 4 \pmod{5}$ $\quad 9 \equiv 3 \pmod{x}$

Problem 0.0
Think about what it means to look at the integers (mod 2)? What does this tell us about the integer we take (mod 2)?

Problem 0.1
If we look at the integers (mod) m, then what are the outputs that we get for a using the definition above? Try looking at a few examples for say $m = 2, 3, 4$.

Problem 1.1:
Consider m to be a positive integer. Show for every integer a there exists a unique integer r such that $a \equiv r \pmod{m}$ and $0 \leq r < m$. This will be shown in a few steps that you'll complete. We call this the *Standard representation of an integer modulo m.*
a. Explain why $a = mq + r$ for integers q, r. How does this relate to the definition for modular arithmetic?
b. We know that r exists, and now to show that it is unique consider that we have two values for r, namely $a \equiv r \pmod{m}$ and $a \equiv r' \pmod{m}$. Manipulate these statements algebraically to show that $r = r'$ and we indeed have that the value is unique. This is a variation on *proof by contradiction* and it is the standard procedure to show uniqueness of some element. Take some time to think about the logic of this proof and what we assumed, and also explain why knowing that some object is unique is important. Namely we assumed that we had two values r and r', and mathematically showed that if two values exist for r, then they must be equal, hence there can only be one. Now you're done!

Problem 1.2
If $a \equiv b \pmod{m}$, show that $(a+m) \equiv b \pmod{m}$. This gives us a method for

simplifying (mod) m, whereby we just reduce multiples of m from a until we end up with a number b that is less than m.
a.Reduce these mod statements so that b satisfies the conditions from problem 1.1 (i.e. $b \leq m$). $31 \equiv 11 \pmod 6$ $\quad$ $7 \equiv 43 \pmod 3$

Problem 2.1
If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, show that $a \equiv c \pmod m$. Does this remind you of anything? If you're stuck then try to write out the definitions of mod m in terms of equalities.

Problem 2.2
If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $a + c \equiv b + d \pmod m$ and $ac \equiv bd \pmod m$. hint: for the second statement write out $ac - bd$ in terms of the definitions for a and c.

Problem 2.3
If $a \equiv b \pmod m$, then $a^k \equiv b^k \pmod m$ for all $k \geq 1$ Hint: use induction and 2.2.
Comment: this gives us a method for taking powers of numbers (mod) m, namely we just raise each term to the same power. If $b^k \geq m$ then we can reduce b^k using the method in problem 1.2
Find b**:** $x \equiv 2 \pmod 4 \implies x^2 \equiv b \pmod 4$
$x \equiv 3 \pmod 5 \implies x^2 \equiv b \pmod 5$

Problem 3
If $3 \nmid x$ (read as "3 does not divide x") and $3 \nmid y$, then $3|(x^2 - y^2)$. hint: write out what it means for 3 to not divide x in terms of mods and then use problem 2.3 to think about what the remainder of x^2 divided by 3 must be. Do the same for y^2.

Problem 4
Prove for all integers n, either $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod m$. Prove this by cases where n is either even or odd and formulate this mathematically.