Modular arithmetic

In class, we have seen rules for addition, subtraction, and multiplication modulo a positive integer m. Next, we will study division modulo m.

We have seen that the $\equiv$ relation is similar to equality in many respects, especially when we do simple arithmetic. What happens if we wish to divide? If $ac = bc \pmod m$, for some integers a, b, c, does it mean that we can divide both sides by c? Taking $a = 5, b = 7, c = 7, m = 14$, we see that $5 \times 7 \equiv 7 \times 7 \pmod{14}$, but $5 \not\equiv 7 \pmod{14}$. Considering a few more examples, we see that division is sometimes possible. For example,

$$\begin{aligned} 15 \times 9 &\equiv 57 \times 9 \pmod{14}, \qquad \text{and} \\ 15 &\equiv 57 \pmod{14}. \end{aligned}$$

Similarly,

$$\begin{aligned} 3 \times 55 &\equiv 31 \times 55 \pmod{14}, \qquad \text{and} \\ 3 &\equiv 31 \pmod{14}. \end{aligned}$$

Evidently, the rules for modular division are different from those for the integers. The property that distinguishes the last two examples from the first is that the numbers by which we are dividing (9 and 55) and the modulus 14 are co-prime, i.e., have GCD equal to 1. Indeed, we have that

Proposition 1 *For any integers a, b, c, m such that $m > 1$ and $\gcd(c, m) = 1$, if $ac \equiv bc \pmod m$, then $a \equiv b \pmod m$.*

Proof : If $m|[(a - b)c]$, and $\gcd(c, m) = 1$, by a property we proved in class we have $m|(a - b)$. ■

Division of a real number x by another real $y \neq 0$ is the same as multiplying x by $1/y$ (also written as y^{-1}), and that y^{-1} is also called the *multiplicative inverse* of y. Do we have a similar notion of a multiplicative inverse modulo m? The defining property of multiplicative inverse y^{-1} is that when we multiply y with its inverse, we get 1. Going back to the examples above, where we were able to divide by 9 and 55, we see that

$$\begin{aligned} 9 \times 11 &\equiv 1 \pmod{14}, \qquad \text{and} \\ 55 \times 13 &\equiv 1 \pmod{14}. \end{aligned}$$

So 11 and 13 are the multiplicative inverses of 9 and 55, respectively, modulo 14. How do we find these multiplicative inverses? Given an integer a such that $\gcd(a, m) = 1$, how do we find its inverse a^{-1}, i.e., an integer b such that $ab \equiv 1 \pmod m$? The Bézout Lemma again comes to our rescue, and gives us a method to find the inverse b.

Theorem 2 *For any integer a such that $\gcd(a, m) = 1$, there is an inverse a^{-1}, i.e., an integer b such that $ab \equiv 1 \pmod m$.*

Proof : By the Bézout Lemma, there are integers x, y such that $ax + my = \gcd(a, m) = 1$. In other words $ax - 1 = -my$ or equivalently, $ax \equiv 1 \pmod m$. So we may take x to be the inverse we seek. ■

When $\gcd(a, m) \neq 1$, a multiplicative inverse modulo m cannot exist. Suppose, for sake of contradiction, that it does. Say it is b, and we have $ab \equiv 1 \pmod m$, i.e., $ax - 1 = my$ for some integer y. Let $d = \gcd(a, m)$. Since $d|a$ and $d|m$, we have that $d|(ax - my)$, i.e., $d|1$. This is impossible, as $d = \gcd(a, m) > 1$. In particular, the integer 7 does not have a multiplicative inverse modulo 14.

The proof of Theorem 2 above also provides a way for finding the multiplicative inverse of a given number when it exists. Using the Extended Euclidean algorithm, we find integers x, y such that $ax + my = 1$ whenever $\gcd(a, m) = 1$. The number x would then be a multiplicative inverse for a, modulo m.

Example 1 *Find a multiplicative inverse of* 55 *modulo* 14.

Solution : We use the Extended Euclidean algorithm.

Step	a	b	division: $a = bq + r$	r	u	v	$x = v$	$y = u - vq$
1	55	14	$55 = 3 \times 14 + 13$	13	1	-1	-1	4
2	14	13	$14 = 1 \times 13 + 1$	1	0	1	1	-1
3	13	1	$13 = 13 \times 1 + 0$	0	1	0	0	1
4	1	0					1	0

So we see that $55(-1) + 14(4) = 1$, i.e., $55(-1) \equiv 1 \pmod{14}$, so -1 is a multiplicative inverse of 55 modulo 14. This is consistent with the one we presented above, as $-1 \equiv 13 \pmod{14}$. ■