Everything You Need to Know About Modular Arithmetic...

Math 135, February 7, 2006

Definition Let $m > 0$ be a positive integer called the *modulus*. We say that two integers a and b are congruent modulo m if $b - a$ is divisible by m. In other words,

$$a \equiv b(\text{mod} m) \iff a - b = m \cdot k \text{ for some integer} k. \tag{1}$$

Note:

1. The notation ?? $\equiv$??(mod$m$) works somewhat in the same way as the familiar ?? =??.
2. a can be congruent to many numbers modulo m as the following example illustrates.

Ex. 1 The equation

$$x \equiv 16(\text{mod}10)$$

has solutions $x = \ldots, -24 - 14, -4, 6, 16, 26, 36, 46 \ldots$. This follows from equation (1) since any of these numbers minus 16 is divisible by 10. So we can write

$$x \equiv \cdots - 24 \equiv -14 \equiv -4 \equiv 6 \equiv 16 \equiv 26 \equiv 36 \equiv 46(\text{mod}10).$$

Since such equations have many solutions we introduce the notation $a(\text{MOD}m)$

Definition The symbol

$$a(\text{MOD}m) \tag{2}$$

denotes the smallest positive number x such that

$$x \equiv a(\text{mod}m).$$

In other words, $a(\text{MOD}m)$ is the remainder when a is divided by m as many times as possible. Hence in example 1 we have

$$6 = 16(\text{MOD}10) \text{ and } 6 = -24(\text{MOD}10) \text{ etc....}$$

Relation between "$x \equiv b$ mod m" and "$x = b$ MOD m"

$x \equiv b \bmod m$ is an EQUIVALENCE relation with many solutions for x while $x = b$ MOD m is an EQUALITY. So one can think of the relationship between the two as follows

$$x = b(\text{MOD } m) \text{ is the smallest positive solution to the equation } x \equiv b(\text{mod } m).$$

Since

$$0 < b(\text{MOD } m) < m$$

it is convention to take these numbers as the representatives for the class of numbers $x \equiv b(\text{mod } m)$.

Ex. 2 The standard representatives for all possible numbers modulo 10 are given by

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9$$

although, for example, $3 \equiv 13 \equiv 23 (\text{mod } 10)$, we would take the smallest positive such number which is 3.

Inverses in Modular arithmetic

We have the following rules for modular arithmetic:

$$\textbf{Sum rule: } \text{IF } a \equiv b(\text{mod } m) \text{ THEN } a + c \equiv b + c(\text{mod } m). \tag{3}$$
$$\textbf{Multiplication Rule: } \text{IF } a \equiv b(\text{mod } m) \text{ and if } c \equiv d(\text{mod } m) \text{ THEN } ac \equiv bd(\text{mod } m). \tag{4}$$

Definition An <u>inverse to a modulo m</u> is a integer b such that

$$ab \equiv 1(\text{mod } m). \tag{5}$$

By definition (1) this means that $ab - 1 = k \cdot m$ for some integer k. As before, there are may be many solutions to this equation but we choose as a representative the smallest positive solution and say that the inverse a^{-1} is given by

$$a^{-1} = b \text{ (MOD } m).$$

Ex 3. 3 has inverse 7 modulo 10 since $3 \cdot 7 = 21$ shows that

$$3 \cdot 7 \equiv 1(\text{mod } 10) \text{ since } 3 \cdot 7 - 1 = 21 - 1 = 2 \cdot 10.$$

5 does not have an inverse modulo 10. If $5 \cdot b \equiv 1(\text{mod } 10)$ then this means that $5 \cdot b - 1 = 10 \cdot k$ for some k. In other words

$$5 \cdot b = 10 \cdot k - 1 \text{ which is impossible.}$$

Conditions for an inverse of a to exist modulo m

Definition Two numbers are <u>relatively prime</u> if their prime factorizations have no factors in common.

Theorem Let $m \geq 2$ be an integer and a a number in the range $1 \leq a \leq m - 1$ (i.e. a standard rep. of a number modulo m). Then a has a multiplicative inverse modulo m if a and m are relatively prime.

Ex 4 Continuing with example 3 we can write $10 = 5 \cdot 2$. Thus, 3 is relatively prime to 10 and has an inverse modulo 10 while 5 is not relatively prime to 10 and therefore has no inverse modulo 10.

Ex 5 We can compute which numbers will have inverses modulo 10 by computing which are relatively prime to $10 = 5 \cdot 2$. These numbers are $x = 1, 3, 7, 9$. It is easy to see that the following table gives inverses module 10:

Table 1: inverses modulo 10

x	1	3	7	9
x^{-1} MOD 10	1	7	3	9

Ex 6: We can solve the equation $3 \cdot x + 6 \equiv 8 (\text{mod } 10)$ by using the sum (3) and multiplication (4) rules along with the above table:

$$\begin{aligned} 3 \cdot x + 6 \equiv 8 (\text{mod } 10) &\implies \\ 3 \cdot x \equiv 8 - 6 \equiv 2 (\text{mod } 10) &\implies \\ (3^{-1}) \cdot 3 \cdot x \equiv (3^{-1}) \cdot 2 (\text{mod } 10) &\implies \\ x \equiv 7 \cdot 2 (\text{mod } 10) \equiv 14 (\text{mod } 10) \equiv 4 (\text{mod } 10) & \end{aligned}$$

Final example We calculate the table of inverses modulo 26. First note that

$$26 = 13 \cdot 2$$

so that the only numbers that will have inverses are those which are rel. prime to 26...i.e. they contain no factors of 2 or 13:

$$1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.$$

Now we write some multiples of 26

$$26, 52, 78, 104, 130, 156, 182, 208, 234...$$

A number a has an inverse modulo 26 if there is a b such that

$$a \cdot b \equiv 1 (\text{mod } 26) \text{or } a \cdot b = 26 \cdot k + 1.$$

thus we are looking for numbers whose products are 1 more than a multiple of 26. We create the following table

Table 2: inverses modulo 26

x	1	3	5	7	9	11	15	17	19	21	23	25
x^{-1} (MOD m)	1	9	21	15	3	19	7	23	11	5	17	25

since (using the list of multiples of 26 above)

$$\begin{aligned} 1 \cdot 1 = 1 &= 26 \cdot 0 + 1 \\ 3 \cdot 9 = 27 &= 26 + 1 \\ 5 \cdot 21 = 105 &= 104 + 1 \\ 7 \cdot 15 = 105 &= 104 + 1 \\ 11 \cdot 19 = 209 &= 208 + 1 \\ 17 \cdot 23 = 391 &= 15 \cdot 26 + 1 \\ 25 \cdot 25 = 625 &= 26 \cdot 24 + 1. \end{aligned}$$

So we can solve

$$y = 17 \cdot x + 12(\text{MOD } 26)$$

for x by first considering the congruence equation

$$y \equiv 17 \cdot x + 12 (\text{mod } 26)$$

and performing the following calculation (similar to ex 6) using the above table:

$$\begin{aligned} y \equiv 17 \cdot x + 12 (\text{mod } 26) &\implies \\ y - 12 \equiv 17 \cdot x (\text{mod } 26) &\implies \\ (17^{-1})(y - 12) \equiv (17^{-1}) \cdot 17 \cdot x (\text{mod } 26) &\implies \\ (23)(y - 12) \equiv (23) \cdot 17 \cdot x (\text{mod } 26) &\implies \\ 23 \cdot (y - 12) \equiv x (\text{mod } 26) & \end{aligned}$$

We now write $x = 23 \cdot (y - 12)(\text{MOD } 26)$.

The difference between

$$23 \cdot (y - 12) \equiv x (\text{mod } 26)$$

and

$$x = 23 \cdot (y - 12)(\text{MOD } 26)$$

is simply that in the first equation, a choice of y will yield many different solutions x while in the second equation a choice of y gives the value x such that x is the smallest positive solution...i.e. the smallest positive solution to the first equation.