Modular Arithmetic

Modular arithmetic is quite a useful tool in number theory. In particular, it can be used to obtain information about the solutions (or lack thereof) of a specific equation. This page gives a fairly detailed introduction. Another good introduction, in the form of an interactive tutorial, can be found in Part 2 of Math Alive: Cryptography.

Contents

- I. An Introductory Example
- II. Definition and Further Examples
- III. Properties of Congruence
- IV. Exercises

I. An Introductory Example

Everyone knows that set of integers can be broken up into the following two classes:

- the even numbers (..., –6, –4, –2, 0, 2, 4, 6,...); and
- the odd numbers (..., –5, –3, –1, 1, 3, 5,...).

There are certain generalizations we can make about the arithmetic of numbers based on which of these two classes they come from. For example, we know that the sum of two even numbers is even. The sum of an even number and an odd number is odd. The sum of two odd numbers is even. The product of two even numbers is even, etc.

Modular arithmetic lets us state these results quite precisely, and it also provides a convenient language for similar but slightly more complex statements. In the above example, our *modulus* is the number 2. The modulus can be thought of as the number of classes that we have broken the integers up into. It is also the difference between any two "consecutive" numbers in a given class.

Now we represent each of our two classes by a single symbol. We let the symbol "0" mean "the class of all even numbers" and the symbol "1" mean "the class of all odd numbers". There is no great reason why we have chosen the symbols 0 and 1; we could have chosen 2 and 1, or –32 and 177, but 0 and 1 are the conventional choices.

The statement "the sum of two even numbers is even" can be expressed by the following:

$$0 + 0 \equiv 0 \bmod 2.$$

Here, the "≡" symbol is not equality but *congruence*, and the "mod 2" just signifies that our modulus is 2. The above statement is read "Zero plus zero is congruent to zero, modulo two." The statement "the sum of an even number and an odd number is odd" is represented by

$$0 + 1 \equiv 1 \bmod 2.$$

Those examples are natural enough. But how do we write "the sum of two odd numbers is even"? It is the (at first strange looking) expression

$$1 + 1 \equiv 0 \bmod 2.$$

Here the symbols "≡" and "mod 2" are suddenly very important! We have analogous statements for multiplication:

$$\begin{gathered} 0 \times 0 \equiv 0 \bmod 2, \\ 0 \times 1 \equiv 0 \bmod 2, \\ 1 \times 1 \equiv 1 \bmod 2. \end{gathered}$$

In a sense, we have created a number system with addition and multiplication but in which the only numbers that exist are 0 and 1. You may ask what use this has. Well, our number system is the system of *integers modulo 2*, and because of the previous six properties, **any arithmetic done in the integers translates to arithmetic done in the integers modulo 2**. This means that if we take any equality involving addition and multiplication of integers, say

$$12 \times 43 + 65 \times 78 = 5586,$$

then reducing each integer *modulo 2* (i.e. replacing each integer by its class "representative" 0 or 1), then we will obtain a valid congruence. The above example reduces to

$$0 \times 1 + 1 \times 0 \equiv 0 \bmod 2,$$

or $0 + 0 \equiv 0 \bmod 2$.

More useful applications of reduction modulo 2 are found in solving equations. Suppose we want to know which integers might solve the equation

$$3a - 3 = 12.$$

Of course, we could solve for a, but if we didn't need to know what a is exactly and only cared about, say, whether it was even or odd, we could do the following. Reducing modulo 2 gives the congruence

$$1a + 1 \equiv 0 \bmod 2,$$

or

$$a \equiv -1 \equiv 1 \bmod 2,$$

so any integer a satisfying the equation $3a - 3 = 12$ must be odd.

Since any integer solution of an equation reduces to a solution modulo 2, it follows that **if there is no solution modulo 2, then there is no solution in integers**. For example, assume that a is an integer solution to

$$2a - 3 = 12,$$

which reduces to

$$0 \cdot a + 1 \equiv 0 \bmod 2,$$

or $1 \equiv 0 \bmod 2$. This is a contradiction because 0 and 1 are different numbers modulo 2 (no even number is an odd number, and vice versa). Therefore the above congruence has no solution, so a couldn't have been an integer. This proves that the equation $2a - 3 = 12$ has no integer solution.

Less trivially, consider the system of equations

$$6a - 5b = 4,$$
$$2a + 3b = 3.$$

Modulo 2, these equations reduce to

$$0 + 1b \equiv 0 \bmod 2,$$
$$0 + 1b \equiv 1 \bmod 2.$$

This says that b is both even and odd, which is a contradiction. Therefore we know that the original system of equations has no integer solutions, and to prove this we didn't even need to know anything about a.

As shown by the preceding examples, one of the powers of modular arithmetic is the ability to show, often very simply, that certain equations and systems of equations have no integer solutions. Without modular arithmetic, we would have to find all of the solutions and then see if any turned out to be integers.

II. Definition and Further Examples

Of course, there is nothing special about the number 2. Any integer (except 0) will work for the modulus m. We now give the mathematical definition of congruence.

Definition. Let $m \neq 0$ be an integer. We say that two integers a and b are *congruent modulo m* if there is an integer k such that $a - b = km$, and in this case we write

$$a \equiv b \bmod m.$$

Notice that the condition "$a - b = km$ for some integer k" is equivalent to the condition "m divides $a - b$".

In the previous section we used the modulus $m = 2$. Although we wrote congruences using only 0 and 1, really any integers are valid. Modulo 2, all of the even numbers are congruent to each other since the difference of any two even numbers is divisible by 2:

$$\ldots \equiv -6 \equiv -4 \equiv -2 \equiv 0 \equiv 2 \equiv 4 \equiv 6 \equiv \ldots \quad \bmod 2.$$

Also, every odd number is congruent to every other odd number modulo 2 since the difference of any two odd numbers is even:

$$\ldots \equiv -5 \equiv -3 \equiv -1 \equiv 1 \equiv 3 \equiv 5 \equiv \ldots \quad \bmod 2.$$

Therefore, anywhere we wrote "0" we could have written any other even number, and similarly "1" could have been replaced by any odd number. For example, instead of writing $0 \times 1 + 1 \times 0 \equiv 0 \bmod 2$, an equally valid statement would have been

$$10 \times (-13) + 27 \times 6 \equiv -122 \bmod 2.$$

Let's now look at other values for the modulus m. For example, let $m = 3$. All multiples of 3 are congruent to each other modulo 3 since the difference of any two is divisible by 3. Similarly, all numbers of the form $3n + 1$ are congruent to each other, and all numbers of the form $3n + 2$ are congruent to each other.

$$\ldots \equiv -9 \equiv -6 \equiv -3 \equiv 0 \equiv 3 \equiv 6 \equiv 9 \equiv \ldots \mod 3.$$
$$\ldots \equiv -8 \equiv -5 \equiv -2 \equiv 1 \equiv 4 \equiv 7 \equiv \ldots \mod 3.$$
$$\ldots \equiv -7 \equiv -4 \equiv -1 \equiv 2 \equiv 5 \equiv 8 \equiv \ldots \mod 3.$$

How about when $m = 1$? The difference of *any* two integers is divisible by 1, so all integers are congruent to each other modulo 1:

$$\ldots \equiv -3 \equiv -2 \equiv -1 \equiv 0 \equiv 1 \equiv 2 \equiv 3 \equiv \ldots \mod 1.$$

For this reason, $m = 1$ is not very interesting, and reducing an equation modulo 1 doesn't give any information about its solutions.

The modulus $m = 12$ comes up quite frequently in everyday life, and its application illustrates a good way to think about modular arithmetic — the "clock arithmetic" analogy. If it's 7:00, what time will it be in 25 hours? Since $25 \equiv 1 \mod 12$, we simply add 1 to 7:

$$7 + 25 \equiv 7 + 1 \equiv 8 \mod 12.$$

So the clock will read 8:00. Of course, we don't need the formality of modular arithmetic in order to compute this, but when we do this kind of computation in our heads, this is really what we are doing.

With $m = 12$, there are only 12 numbers ("hours") we ever need to think about. We count them 1, 2, 3, ..., 10, 11, 12, 1, 2, ... , starting over after 12. The numbers 1, 2, ..., 12 represent the twelve equivalence classes modulo 12: Every integer is congruent to exactly one of the numbers 1, 2, ..., 12, just as the hour on the clock always reads exactly one of 1, 2, ..., 12. These classes are given by

$$12n + 1,\ 12n + 2,\ 12n + 3,\ \ldots,\ 12n + 11,\ 12n$$

as n ranges over the integers.

Of course, the minutes and seconds on a clock are also modular. In these cases the modulus is $m = 60$. If we think of the days of the week as labeled by the numbers 0, 1, 2, 3, 4, 5, 6, then the modulus is $m = 7$. The point is that we measure many things, both in mathematics and in real life, in periodicity, and this can usually be thought of as an application of modular arithmetic.

III. Properties of Congruence

It is fairly easy to show that for any integers a, b, c, and $m \neq 0$, the following properties hold:

reflexivity: $a \equiv a \mod m$.
symmetry: If $a \equiv b \mod m$, then $b \equiv a \mod m$.
transitivity: If $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$.

Therefore congruence modulo m is an equivalence relation, and this relation partitions the integers into m equivalence classes:

$$mn + 0,\ mn + 1,\ mn + 2,\ \ldots,\ mn + (m - 1).$$

(Since $0 \equiv m \mod m$, we can either choose 0 or m as a representative for the first class. It is conventional to choose 0.) To be a little more formal than we were above, we can write the equivalence class of an integer a as $[a]$. The brackets signify that this is an equivalence *class* and not simply a number. In this way we can write

$$\begin{gathered}
\ldots = [-3m] = [-2m] = [-m] = [0] = [m] = [2m] = [3m] = \ldots, \\
\ldots = [-3m + 1] = [-2m + 1] = [-m + 1] = [1] = [m + 1] = [2m + 1] = [3m + 1] = \ldots, \\
\ldots = [-3m + 2] = [-2m + 2] = [-m + 2] = [2] = [m + 2] = [2m + 2] = [3m + 2] = \ldots, \\
\ldots = [-3m + 3] = [-2m + 3] = [-m + 3] = [3] = [m + 3] = [2m + 3] = [3m + 3] = \ldots, \\
\vdots \\
\ldots = [-2m - 1] = [-m - 1] = [-1] = [m - 1] = [2m - 1] = [3m - 1] = [4m - 1] = \ldots .
\end{gathered}$$

(Notice that each congruence symbol "≡" has been replaced by equality "=".) With this notation, we have the following property for any integers a and b, which justifies "reduction under addition":

$$[a + b] = [a] + [b].$$

Similarly, for any integers a and b we have

$$[a \cdot b] = [a] \cdot [b],$$

justifying "reduction under multiplication". (In the fancy language of abstract algebra, these two properties can be summarized by saying that reduction modulo m is a homomorphism of rings. In this case the two rings are the ring of integers and the ring of integers modulo m.)

IV. Exercises

1. Show that the system of equations

$$\begin{aligned} 11x - 5y &= 7, \\ 9x + 10y &= -3. \end{aligned}$$

has no integer solutions.

2. Show that the system of equations

$$\begin{aligned} 24x - 5y &= 10, \\ 11x - 9y &= 13. \end{aligned}$$

has no integer solutions.

3. Show that if x, y, z are integers such that $x^2 + y^2 = z^2$, then at least one of them is divisible by 2, at least one is divisible by 3, and at least one is divisible by 5.

4. Show that if x, y, z are integers such that $x^3 + y^3 = z^3$, then at least one of them is divisible by 7.

Projects • Expositions
Pascal's Simplices • Pythagorean Triples • Regular Polygons
Regular Polyhedra • Regular Polytopes • Sums of Consecutive Powers
Mathematical Induction • Modular Arithmetic • Polynomial Equations
Investigations • Calculators • Popular Books
Eric S. Rowland