Finite Number Systems

Friday, October 27, 2017
Jim Riley

Abstract: *We're accustomed to infinite number systems, such as the integers and the real numbers, but there are finite number systems with many of the same properties.*

We'll define a commutative ring, which is a number system with the same properties as the integers. Of course, the integers are a commutative ring.

We'll define a field, which is a commutative ring where every non-0 element has a multiplicative inverse; examples of fields include the rational, real, and complex numbers.

We'll explore $\boldsymbol{Z}_{12}$*, a finite commutative ring with 12 elements that uses modular ("clock") arithmetic*

We'll explore $\boldsymbol{Z}_{7}$, *a finite field with 7 elements.*

$\boldsymbol{Z}_{12}$ *and* $\boldsymbol{Z}_{7}$ *aren't unique. In fact, for every whole number n* 2*, there's a finite commutative ring* $\boldsymbol{Z}_{n}$*. Also, for every prime number p, the commutative ring* $\boldsymbol{Z}_{p}$ *is a finite field.*

Finally, we'll look at some applications of modular arithmetic of the type used in $\boldsymbol{Z}_{12}$ *and* $\boldsymbol{Z}_{7}$.

all familiar with the integers, sometimes known as ***Z*** (after the German word *zahlen*, meaning The integers consist of the whole numbers 0, 1, 2, 3, 4, ... together with the negative numbers -1 2, 3, 4, ... And we all know how to add, subtract, multiply, and divide in the integers although part of the reason why the

Here are the key properties that define how things work in the integers:

1. The integers are ***closed*** under addition and multiplication; that is, the result of adding or multiplying two integers is

To get a feel for how these
3 + 2*x* = 9 in this set:

1. The equation says 2*x* can be any number that you can add to 3 to get 9.
2. According to the addition table, that means 2*x* = 6.
3. Therefore *x* can be any number such that multiplying it by 2 gives 6.
4. The multiplication table says 2x3 = 6 and 2x9 = 6, so the solutions are *x* = 3 and *x* = 9.

Note that 3 would also be a solution to the same equation in our everyday numbers, but 9

Exercise: Use the tables above to find all the solutions you can for the equation 8*x* + 4 = 0 in $\boldsymbol{Z}_{12}$.

From the addition table above, we can see that 0 is the additive identity in $\boldsymbol{Z}_{12}$, just like in regular arithmetic, and each of our 12 numbers has an additive inverse:

1 + 11 = 0

s additive inverse

6 + 6 = 0, so 6 is its own additive inverse

Following the notation , we could say 1 = 11, 11 = 1, 2 = 10, 10 = 2, etc. in $\boldsymbol{Z}_{12}$.

From the multiplication table for arithmetic mod 12, we can also see that 1 is the multiplicative identity, again just like in regular arithmetic.

$\boldsymbol{Z}_{12}$ has most of the properties of a commutative ring. It would be tedious to check that the addition and multiplication are associative, and that the distributive property holds, but I promise you that $\boldsymbol{Z}_{12}$ really does satisfy those requirements as well, which means $\boldsymbol{Z}_{12}$ is in fact a commutative ring!

, though, $\boldsymbol{Z}_{12}$ is a *finit* [illegible]

+

So sure enough, $\boldsymbol{Z}_7$ is a field, even though it has only 7 elements! In fact, if p is any prime number, $\boldsymbol{Z}_p$ is a field; because of by $\boldsymbol{F}_p$ instead of $\boldsymbol{Z}_p$. There are other types of finite fields as well, but the number of elements in a finite field is always a power of some prime number.

Exercise: Use the multiplication table above to calculate 5^7 in $\boldsymbol{F}_7$. Do the same with 5^7. Do you see a pattern? If you re feeling ambitious, verify that the pattern holds for every element of $\boldsymbol{F}_7$. (In fact, in any finite field with p elements, where p is a prime, $a^n = a$ for every element a of the field.)

Historical note: Finite fields are also known as ***Galois fields***, in honor of the French mathematician Evariste Galois (1811 1832) who discovered them. Galois (prounounced Gal WAH) made profound contributions to algebra whole branch of algebra called Galois theory based on his work before his tragic death in a duel at the age of 20. He filled a notebook with his ideas the night before the duel, just in case.