Math From Scratch Lesson 17: Modular Arithmetic

W. Blaine Dowler

January 2, 2012

Contents

1 Modular Arithmetic

Modular arithmetic is one of the concepts that is used frequently in computer science, and yet it is rarely a part of the public school curriculum. In lesson 14, we learned how to divide one number by another when a remainder is produced.

Modular arithmetic happens when one chooses a "base" to work under, and then examine only the remainder when dividing by that base.

In lesson 16, we looked at divisibility rules. In the case in which we looked at divisibility by 2, we looked only at the ones digit, discarding every higher placed digit. This is the same as working "mod 10," meaning we have chosen 10 as the base and replaced the number of interest with its remainder when divided by 10. For example, when testing to see if 125123 is divisible by 2, we can write

$$125123 = 12512 \cdot 10 + 3 \equiv 3 \, (mod \ 10)$$

Note the $\equiv$ symbol. Rather than equality, we show that the numbers are *equivalent*. To use this notation, we must first do two things:

1. Define equivalence relations formally.
2. Prove that the relation defined here, that x and y are congruent for some modulus n, truly is equivalence.

The first task is already complete; see page three of lesson one. An equivalence relation is a relation that is *symmetric* (meaning that, if $A \equiv B$ is true, then $B \equiv A$ is also true), *reflexive* (meaning that $A \equiv A$ is true for any possible A) and *transitive* (meaning that, if $A \equiv B$ and $B \equiv C$, then $A \equiv C$.) The fourth property defining equality, *antisymmetry*, does not apply; it is entirely possible for $A \equiv B$ to be true while $A \neq B$.

The second task is far more involved and complicated. Let us take each of the properties individually.

1.1 Transitivity

Let x and y be two integers, each of which is congruent to a when in modulus n. We have that $x = k \cdot n + a$ for some integer values of k and a with modulus n. Thus, $x \equiv a \, (mod \ n)$. If y is also congruent to a for modulus n, then we have $y = l \cdot n + a$. Thus, mod n, $x = k \cdot n + a \equiv l \cdot n + a = y \, (mod \ n)$.

1.2 Reflexivity

This is quite possibly the easiest property to prove, once transitivity has been established. If $x = k \cdot n + a$, then $x \equiv k \cdot n + a \, (mod \ n)$ and $k \cdot n + a \equiv x \, (mod \ n)$.

1.3 Symmetry

This is also simplified by the transitive relation. If $x \equiv y\,(mod\ n)$, then $x = k \cdot n + a$ and $y = l \cdot n + a$ for some values of a, k and l. Thus, we can appeal to transitivity to show that $x = k \cdot n + a \equiv l \cdot n + a = y\,(mod\ n)$ and $y = l \cdot n + a \equiv k \cdot n + a = x\,(mod\ n)$.

We have now shown that congruence modulo n is a proper equivalence relation for an arbitrary natural number n.

2 Congruence Classes

Let us examine various numbers under a specific modulus 3. We find that

$$\begin{aligned}
0 &\equiv 0\,(mod\ 3)\\
1 &\equiv 1\,(mod\ 3)\\
2 &\equiv 2\,(mod\ 3)\\
3 &\equiv 0\,(mod\ 3)\\
4 &\equiv 1\,(mod\ 3)\\
5 &\equiv 2\,(mod\ 3)\\
6 &\equiv 0\,(mod\ 3)\\
7 &\equiv 1\,(mod\ 3)\\
8 &\equiv 2\,(mod\ 3)\\
9 &\equiv 0\,(mod\ 3)\\
10 &\equiv 1\,(mod\ 3)\\
11 &\equiv 2\,(mod\ 3)\\
12 &\equiv 0\,(mod\ 3)\\
13 &\equiv 1\,(mod\ 3)\\
14 &\equiv 2\,(mod\ 3)\\
15 &\equiv 0\,(mod\ 3)\\
16 &\equiv 1\,(mod\ 3)\\
17 &\equiv 2\,(mod\ 3)\\
18 &\equiv 0\,(mod\ 3)\\
19 &\equiv 1\,(mod\ 3)\\
20 &\equiv 2\,(mod\ 3)
\end{aligned}$$

We see that a pattern has emerged, as the results cycle through the numbers 0, 1 and 2. In general, modulo n, the results will cycle $0, 1, 2, \ldots, n-1$. The most

interesting results occur when one does simple calculations with these numbers. Let us look at an addition table for numbers 0-10:

+	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	11
2	2	3	4	5	6	7	8	9	10	11	12
3	3	4	5	6	7	8	9	10	11	12	13
4	4	5	6	7	8	9	10	11	12	13	14
5	5	6	7	8	9	10	11	12	13	14	15
6	6	7	8	9	10	11	12	13	14	15	16
7	7	8	9	10	11	12	13	14	15	16	17
8	8	9	10	11	12	13	14	15	16	17	18
9	9	10	11	12	13	14	15	16	17	18	19
10	10	11	12	13	14	15	16	17	18	19	20

Now we replace every entry in the table its remainder when divided by 3.

+	0	1	2	0	1	2	0	1	2	0	1
0	0	1	2	0	1	2	0	1	2	0	1
1	1	2	0	1	2	0	1	2	0	1	2
2	2	0	1	2	0	1	2	0	1	2	0
0	0	1	2	0	1	2	0	1	2	0	1
1	1	2	0	1	2	0	1	2	0	1	2
2	2	0	1	2	0	1	2	0	1	2	0
0	0	1	2	0	1	2	0	1	2	0	1
1	1	2	0	1	2	0	1	2	0	1	2
2	2	0	1	2	0	1	2	0	1	2	0
0	0	1	2	0	1	2	0	1	2	0	1
1	1	2	0	1	2	0	1	2	0	1	2

If we work out each addition explicitly for addition of 0, 1 and 2, we find identical results. In other words, it is worth exploring the idea that $x + y = z$ implies $x + y\,(mod\ n) = z\,(mod\ n)$. This turns out to be the case, as shown here:

Let $x = k \cdot n + a$ and $y = l \cdot n + b$. Then we have $x + y = k \cdot n + a + l \cdot n + b = (k + l) \cdot n + (a + b)$, which shows that, when working under a specific modulus n, addition of x and y is equivalent to adding the remainders of x and y modulo n. We can explore this concept further with multiplication and see if a similar result holds:

$$x \cdot y = (k \cdot n + a) \cdot (l \cdot n + b) = kln^2 + kn + ln + ab = (kln + k + l) \cdot n + ab$$

This holds true as well. Thus, when working under a modulus n, the addition and multiplication operations are preserved. The subtraction and division operations are worth a closer look, as the inverses are not intuitive.

3 Modular Subtraction

If you recall the definition of remainder when dividing two numbers, you will see that the remainder cannot be a negative number. How, then, do we define subtraction?

Let us look at the upper corner of our addition table for modulo 3 above:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We originally defined $-a$ as the number such that $a + (-a) = 0$. We can retain this definition and find that $-1 \equiv 2\,(mod\ 3)$ and $-2 \equiv 1\,(mod\ 3)$, as seen in the table above. Thus, in modular arithmetic, we no longer have negative numbers, as the inverses are *also* positive numbers; they are the numbers that "cycle" back to 0, or the modulus. Because addition is preserved, this works out identically in cases in which subtraction appears to make sense. For example,

$$2 - 1\,(mod\ 3) = 2 + (-1)\,(mod\ 3) = 2 + 2\,(mod\ 3) = 4\,(mod\ 3) = 1\,(mod\ 3)$$

which is exactly what we get from $2 - 1$ in regular arithmetic. In the general case, we can determine the negative to $x\,(mod\ n)$ by first determining the values of k and a in the equation $x = k \cdot n + a$ and then calculating $n - a = -x$. This will exist for every value of x.

4 Modular Division

Division is a little trickier. We first define the inverse of x under the division operation as that element x^{-1} such that $x \cdot x^{-1} = 1$. For modulo 3, we can read this off the multiplication table:

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

In this case, $1 = 1^{-1}$, as expected, and as it will be in every example by the very definition of 1. However, we find something somewhat surprising with the case of 2^{-1}. While we are used to the notion of fractions and the fact that $2^{-1} = \frac{1}{2}$ in normal operations, the nature of modular arithmetic has completely eliminated the need for fractions. In fact, $2^{-1} = 2$, which means 2 is its own inverse!

In other modular algebras, we find that some elements don't even have inverses. In traditional algebra, the lack of an inverse was unique to the element 0, but that is no longer the case. For example, let us examine the case modulo 6:

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

The elements 1 and 5 are their own inverses under multiplication, and elements 0, 2, 3 and 4 have no inverses at all! There are no elements that you can multiply 0, 2, 3 or 4 by to obtain 1 as the result. This is a topic we will return to after defining algebraic fields, after which these ideas may be explored more completely.

5 Modular Rings

It will now be shown that modular arithmetics satisfy all of the algebraic requirements of a ring. For abbreviated notion, we will take the set of numbers $\mathbb{Z}_n = \{0, 1, 2, \ldots n-1\}$ for notational simplicity, and omit the $(mod\ n)$ from every line, allowing it to be implied. The applicability of the eight ring axioms are proven if necessary as follows, provided $n \geq 2$:

5.1 Closure Under +

Let $x, y \in \mathbb{Z}_n$. Then $x + y = k \cdot n + a + l \cdot n + b = (k + l) \cdot n + (a + b) \equiv a + b$, and the algebra is closed under addition.

5.2 Associativity under +

This is inherited from the case for $\mathbb{Z}$.

5.3 Identity under +

All properties and the existence of 0 are inherited from $\mathbb{Z}$.

5.4 Inverses under +

These were calculated above, and a general method for calculating them has been defined. Therefore, we know they exist for all $x \in mathbbZ_n$.

5.5 Commutativity under +

This is inherited from the case for $\mathbb{Z}$.

5.6 Closure under ·

Let $x, y \in \mathbb{Z}_n$. Then $x \cdot y = (k \cdot n + a) \cdot (l \cdot n + b) = (kln + k + l) \cdot n + (a \cdot b) \equiv a \cdot b$, and the algebra is closed under multiplication.

5.7 Associativity under ·

This is inherited from the case for $\mathbb{Z}$.

5.8 Identity under ·

All properties and the existence of 1 are inherited from $\mathbb{Z}$.

6 Next

This leads us to congruence classes, totients and the Chinese Remainder Theorem in our next few lessons.