20200204

Modular Division

Recall that one of our goals in defining arithmetic on $\mathbb{Z}_n$ was ***closure*** – when we apply the arithmetic operator to two elements of $\mathbb{Z}_n$, the result should also be in $\mathbb{Z}_n$.

For addition, multiplication and subtraction, that was easy. For division, not so much. But we will see what we can do.

When we write x = a/b, we understand that it is equivalent to x = a * $\frac{1}{b}$. This lets us replace the division operator by a multiplication operator – notice that this is the same trick that we pulled when we defined modular subtraction by turning it into modular addition. The problem is that now we are stuck with that annoying $\frac{1}{b}$ ... a term that we call **the reciprocal (or inverse – which is the term I prefer)** of b, which we often write as b^{-1}

Given x $\in \mathbb{Z}_n$, what value y $\in \mathbb{Z}_n$ should be chosen as x^{-1} ? Recall that in "normal" arithmetic, $x * x^{-1} = 1$ for all x except for 0.

So it seems reasonable that in modular arithmetic, we should let x^{-1} be the element y $\in \mathbb{Z}_n$ that satisfies x $\otimes$ y = 1

Unfortunately, it turns out that in many of the sets $\mathbb{Z}_n$ there are elements other than 0 that have no inverse. (Note that 0 never has a reciprocal) For example, consider $\otimes$ for $\mathbb{Z}_6$

$\otimes_6$	**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 only elements of $\mathbb{Z}_6$ that have reciprocals are 1 and 5. This is not an accident ... these are the only elements of $\mathbb{Z}_6$ that are relatively prime with 6.

<Recall: two integers are relatively prime if their greatest common divisor is 1. So 2 and 6 are not relatively prime because gcd(2,6) = 2. Note that two numbers can be relatively prime even if neither of them is a prime number. For example, 8 and 9 are relatively prime. >

Claim: In $\mathbb{Z}_n$, element a has an inverse if and only if a and n are relatively prime (i.e. $gcd(a,n) = 1$)

Proof: Suppose a has an inverse, ie there is an element $b \in \mathbb{Z}_n$ such that $a \otimes b = 1$

$\Rightarrow (a * b)\%n = 1$

$\Rightarrow a * b = k * n + 1$ for some integer k

$\Rightarrow a * b + n * (-k) = 1$

$\Rightarrow gcd(a,n) = 1$ (see footnote)[1]

$\Rightarrow a$ and n are relatively prime

Suppose a and n are relatively prime, ie $gcd(a,n) = 1$

$\Rightarrow$ there exist integers x and y such that $a * x + n * y = 1$ (see the same footnote)

$\Rightarrow$ we can write $x = k * n + r$ where $r \in \mathbb{Z}_n$ ($r = x\%n$)

$\Rightarrow a * (k * n + r) + n * y = 1$

$\Rightarrow a * r + n * (k * a + y) = 1$

Now apply $\%\ n$ to both sides ...

$\Rightarrow (a * r + n * (k * a + y))\%n = 1\%n$

The term $n * (k * a + y)$ disappears because it is a multiple of n, and $1\%n = 1$, so we are left with

$(a * r)\%n = 1$

i.e.

$a \otimes r = 1$

i.e.

a has an inverse

[1] There is a theorem that tells us that if p and q are integers, then there exist integers x and y such that $p * x + q * y = 1$ if and only if $gcd(p,q) = 1$. This result is usually presented during the proof of Euclid's Algorithm for finding the $gcd()$ of two integers.

This innocent seeming result is actually hugely important. It lets us put the whole $\oslash$ problem away. But first, a couple of results that follow immediately from this one:

Claim: In $\mathbb{Z}_n$, if x has an inverse then the inverse is unique.

Proof: Easy. Assume $x \otimes a = 1$ and $x \otimes b = 1$. Show a = b (exercise)

Definition: If x has an inverse, we say that x is ***invertible***. We use x^{-1} to represent the inverse of x.

Claim: Every element of $\mathbb{Z}_n$ except 0 has an inverse if and only if n is prime

Proof: If n is prime, then $gcd(x,n) = 1 \;\; \forall x \in \{1 \ldots n-1\}$
$\Rightarrow x^{-1}$ exists $\;\; \forall x \in \{1 \ldots n-1\}$

If x^{-1} exists $\;\; \forall x \in \{1 \ldots n-1\}$
$\Rightarrow gcd(x,n) = 1 \;\; \forall x \in \{1 \ldots n\text{-}1\}$
$\Rightarrow$ n is prime

To illustrate that last claim about primes, let's look at the $\otimes$ table for $\mathbb{Z}_7$

$\otimes$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6
2	0	2	4	6	**1**	3	5
3	0	3	6	2	5	**1**	4
4	0	4	**1**	5	2	6	3
5	0	5	3	**1**	6	4	2
6	0	6	5	4	3	2	**1**

I've highlighted the 1's in the table to show that each non-zero element does have an unique inverse. From this table we can see that in $\mathbb{Z}_7$, $2^{-1} = 4$, $5^{-1} = 3$, etc

Claim: if a^{-1} = b, then b^{-1} = a

Proof: exercise

Now, finally, we can define $\oslash$:

In $\mathbb{Z}_n$, let y be an invertible element, and let x be any element. Then $x \oslash y = x \otimes y^{-1}$

If we think of y^{-1} as $\frac{1}{y}$, it is clear that this is exactly parallel to the observation we made about "normal" division: x / y = x * $\frac{1}{y}$

Example: in $\mathbb{Z}_6$, what is 5 $\oslash$ 2? Answer: It is undefined, since 2 is not invertible in $\mathbb{Z}_6$

Example: in $\mathbb{Z}_7$, what is 5 $\oslash$ 2? Answer: 2^{-1} = 4, so 5 $\oslash$ 2 = 5 $\otimes$ 4 = 6

Now this may seem a bit weird ... we are saying that 5 divided by 2 is equal to 6. What kind of sense does that make? How can dividing a number by 2 give a result that is bigger than the original number?

Well, remember that in "normal" math, saying "x / y = z" is the same as saying "y * z = x"

We just have to accept that in modular math, the "division operator" has nothing to do with cutting a number up into equal sized parts, and everything to do with being the inverse of the multiplication operation.

In $\mathbb{Z}_7$, we see that 2 $\otimes$ 6 = 5, so it ***is*** reasonable to say 5 $\oslash$ 2 = 6

Example: in $\mathbb{Z}_6$, what is 2 $\oslash$ 5? Answer: 5^{-1} = 5, so 2 $\oslash$ 5 = 2 $\otimes$ 5 = 4

Again, we can confirm that this makes sense because 5 $\otimes$ 4 = 2

Now what about $5 \oslash 2$ in $\mathbb{Z}_6$? Well $gcd(2, 6) \neq 1$, so 2^{-1} does not exist in $\mathbb{Z}_6$ ... so we cannot compute $5 \otimes 2^{-1}$ in $\mathbb{Z}_6$

An interesting question: when $x \neq 0$, can we always say $x \oslash x = 1$ is a valid equation for $\mathbb{Z}_n$ even if x^{-1} does not exist in $\mathbb{Z}_n$? It would correspond nicely with “normal” arithmetic, in which $x/x = 1$ is true $\forall x \neq 0$. The truth is I have never seen this done. I think one of the problems with it would be that in modular arithmetic the $x \oslash y$ operation is explicitly defined as $x \otimes y^{-1}$ ... so “ $x \oslash x$“ simply means “ $x \otimes x^{-1}$ “ ... and if x^{-1} doesn’t exist then we can’t compute $x \otimes x^{-1}$

For completeness, here is the $\oslash$ table for $\mathbb{Z}_7$

$\oslash$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	-	0	0	0	0	0	0
1	-	1	4	5	2	3	6
2	-	2	1	3	4	6	5
3	-	3	5	1	6	2	4
4	-	4	2	6	1	5	3
5	-	5	6	4	3	1	2
6	-	6	3	2	5	4	1

In this table “-” means “undefined”. Notice that each column (except for the 0 column) is a complete permutation of $\mathbb{Z}_7$. This demonstrates that $a \oslash c = b \oslash c \Rightarrow a = b$ .... which is actually very easy to prove. This would be a good exercise.

Here is the $\oslash$ table for $\mathbb{Z}_6$

$\oslash$	**0**	**1**	**2**	**3**	**4**	**5**
0	-	0	-	-	-	0
1	-	1	-	-	-	5
2	-	2	-	-	-	4
3	-	3	-	-	-	3
4	-	4	-	-	-	2
5	-	5	-	-	-	1

We see that most elements of this table are undefined, which is what we expect given that 1 and 5 are the only elements of $\mathbb{Z}_6$ that are invertible.

This brings us to a really interesting sub-topic of modular arithmetic that I talked about for about 30 seconds in class ... but I'll include it here anyway!

When we look at $\otimes$ and $\oslash$ for $\mathbb{Z}_n$, we have seen that the numbers that are not relatively prime with n behave “badly”. These numbers do not have inverses; their multiplication table rows show duplicates, and their division table columns have undefined entries.

What if we just ignore those numbers? In other words, what if we reduce all our multiplication and division tables by crossing out the rows and columns for the numbers that are not relatively prime with n?

This won't make much difference when n is prime: we just lose the row and column for 0. But consider n = 6. The only numbers in $\mathbb{Z}_6$ that are relatively prime with 6 are 1 and 5, so our tables become

$\otimes$	**1**	**5**
1	1	5
5	5	1

$\oslash$	**1**	**5**
1	1	5
5	5	1

That's weird – on this reduced set, $\otimes$ and $\oslash$ are exactly the same

Let's look at a larger example: n = 10. The numbers in $\mathbb{Z}_{10}$ that are relatively prime with 10 are $\{1, 3, 7, 9\}$ so we throw away the rows and columns for $\{0, 2, 4, 5, 6, 8\}$

The reduced tables look like this:

$\otimes$	**1**	**3**	**7**	**9**
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$\oslash$	**1**	**3**	**7**	**9**
1	1	7	3	9
3	3	1	9	7
7	7	9	1	3
9	9	3	7	1

We can see that within these tables, everything is "well-behaved" - every number has an inverse, and – importantly – the operations are **closed**: we never get any undefined values or rogue values that are outside the set we are working on.

Because of these desirable properties, the arithmetic of these reduced sets has been heavily studied – I encourage you to explore **group theory** to learn more.

Ok, that's all lots of fun. We've shown that we can do arithmetic in a meaningful (though sometimes a bit surprising) way on finite sets. But is it useful? It turns out that the ideas we have explored here are vital to modern cryptography, which means they are vital to e-commerce. In a very real sense, companies like Amazon could not exist without modular arithmetic.