

A parents' guide to modular arithmetic

Modular arithmetic is a very useful modification of our usual notions of arithmetic. Don't get the idea that this is some kind of new educational approach to the teaching of arithmetic! Modular arithmetic has been used by mathematicians for a very long time and is one of the foundational concepts in modern mathematics. Even so, the basic idea is very easy. In fact, what makes modular arithmetic so useful, is that it is often *much* easier than usual arithmetic.

There is a separate modular arithmetic for each positive whole number. I'll illustrate with arithmetic "modulo 7". What this means is: the only thing we care about a given whole number is the remainder you get after dividing by 7. So, arithmetic modulo 7 is just about the addition, subtraction, multiplication and division of the *remainders* of whole numbers after dividing by 7.

First of all, the remainders can only be 0,1, 2, 3, 4, 5, or 6. You only have to do arithmetic with these seven numbers! Here's the addition table for numbers modulo 7:

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

For example $2 + 3 = 5$, because if you divide 5 by 7, it goes 0 times, with a remainder of 5. $3 + 6 = 2$, because if you divide 9 by 7, it goes 1 time, with remainder 2. Note that you can subtract any two numbers modulo 7 without having any negative numbers around. One way to think about this is, adding any multiple of seven doesn't change the remainder, so you can always juggle things to get a positive answer. For instance:

$$3 - 5 = (3 + 7) - 5 = 10 - 5 = 5 \pmod{7}$$

(we put in the " mod 7" so no one looking at this will think we really believe that $3-5=5$ in whole-number arithmetic). Here is the subtraction table (where we are taking $v-h$, v being a number in the left-hand column, and h being a number in the top row):

-	0	1	2	3	4	5	6
0	0	6	5	4	3	2	1
1	1	0	6	5	4	3	2
2	2	1	0	6	5	4	3
3	3	2	1	0	6	5	4
4	4	3	2	1	0	6	5
5	5	4	3	2	1	0	6
6	6	5	4	3	2	1	0

So, for example, $-5 = 0 - 5 = 2 \pmod{7}$. Multiplication is the same idea: $3 \times 4 = 12 = 5 \pmod{7}$, because 12 divided by 7 is 1 with a remainder 5. Here is the multiplication table (I omit the $\times 0$ part)

\times	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Look at the last line: this is the same (omitting the 0) as the first line in the subtraction table. This is no accident: $6 = -1 \pmod{7}$ (since $6 + 1 = 7 = 0 \pmod{7}$), so multiplying by 6 is the same as multiplying by -1, that is, taking the negative of a given number. If you look along the diagonal, you see all the perfect squares modulo seven: 1, 2, 4. Notice that exactly *half* of the 6 possible non-zero numbers mod 7 occur, and that each one occurs twice. This is the case for numbers modulo any odd prime number p : exactly $(p - 1)/2$ of the $p - 1$ non-zero numbers mod p are perfect squares, and each perfect square is the square of two different numbers mod p .

Exercise: Find all the cube roots of 1 modulo 7. That is, find all the numbers $x \pmod{7}$ with $x^3 = 1 \pmod{7}$.

Something else very interesting appears in the multiplication table: you can solve every division problem (except of course, dividing by 0) without using fractions! For example $3 \div 5 = 2 \pmod{7}$, because $2 \times 5 = 3 \pmod{7}$. To see that you can solve *every* division problem, just note that, in each row of the multiplication table, all six non-zero numbers modulo 7 occur, and each occurs just once. So, to divide for example 4 by 3, you want to solve $3 \times x = 4$, so look along the multiples

of 3 in the table until you come to 4: $3 \times 6 = 4 \pmod{7}$, so $4 \div 3 = 6 \pmod{7}$.

This last fact, that every division problem modulo seven can be solved, is true not just for numbers modulo seven, but it is also not true for all modular number systems. In fact, this division property for the system of numbers modulo some whole number n is true exactly when n is a *prime number*.

For example, you can see quite clearly that you have a problem with division modulo 6 if you write down the multiplication table for integers modulo 6:

\times	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Only the 1s row and the 5s row give you all the numbers 1,2,3,4,5, so you can only safely divide by 1 and 5. The 2s, 3s and 4s rows are pretty strange: If you try to solve $4 \div 2 = x$, this should mean $2 \times x = 4$, for which there are *two* answers: $x = 2$ (the expected one) and $x = 4$. Somewhat stranger is the equation $2 \times 4 = 4$, since clearly $2 \neq 1$. Probably the strangest thing is the equation $2 \times 3 = 0 \pmod{6}$ (as well as other similar equations of non-zero numbers multiplying to 0).

Here is why the division problem modulo n can be solved for numbers modulo a prime number, but not modulo a non-prime (**feel free to skip the explanation if you don't feel up to it, you won't need this for our Math League problems**): There are exactly $n - 1$ non-zero remainders when dividing by n , so, there are $n - 1$ non-zero numbers modulo n . Every division problem can be solved modulo n exactly when each row in the multiplication table for numbers modulo n has $n - 1$ *different* numbers. Now imagine the row you get by multiplying by the number m , for some number m between 1 and $n - 1$. There are of course $n - 1$ entries, namely the numbers $m \times a \pmod{n}$, as a goes from 1 to $n - 1$. You fail to get all $n - 1$ non-zero numbers modulo n exactly when one (or both) of two things happen:

- (1) $m \times a = m \times b \pmod{n}$ for some pair of numbers $a \neq b \pmod{n}$
- (2) $m \times c = 0 \pmod{n}$ for some number $c \neq 0 \pmod{n}$.

In fact, if (1) happens, then so does (2): if $m \times a = m \times b$, then $m \times a - m \times b = 0$ and since $m \times a - m \times b = m \times (a - b)$, we have (2) with $c = a - b$ (which is not $0 \pmod{n}$ if $a \neq b \pmod{n}$).

But, what does it mean to have two number m, c , both not 0 modulo n , but with $mc = 0 \pmod n$? It means that neither m nor c are divisible by n , but $m \times c$ is divisible by n . This cannot happen if n is a prime number: if n is prime and $m \times c$ has n as a prime factor, then either m has n as a prime factor or c does. If n is *not* a prime number, then $n = m \times c$, with neither m nor c equal to 1, so n divides $m \times c$, but n does not divide m and n does not divide c (why not?). **End of explanation, it's safe to continue reading!**

For this reason, the arithmetic of numbers modulo a prime number p plays a very important role in modern mathematics. In fact, the main method of encoding messages for sending sensitive data over the internet (the RSA procedure) uses the arithmetic of numbers modulo very large prime numbers as its basis.

In any case, you should now be well prepared to help your child with his Math League exercises in modular arithmetic!