Pólya's Paragon

Fun With Numbers (Part 3)

Shawn Godin

Last time I left you with the task of looking for patterns in the following table:

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49
50	51	52	53	54	55	56
57	58	59	60	61	62	63
64	65	66	67	68	69	70
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Notice the interesting pattern that shows up, each column just forms an arithmetic progression with common difference 7. Thus, if two numbers are in the same column, they must differ by a multiple of 7. They must also have the same remainder when you divide them by 7. Mathematicians say that each column in the table forms an *equivalence class*. The numbers in any one column are *equivalent* in that they yield the same remainder when you divide them by 7.

Calculate each of the following and try to see how they are related.

$$3+5\,,\qquad 10+19\,,\qquad 31+12\,,\qquad 45+20\,.$$

I hope you have come up with some ideas. In each case, we were adding a number from column 3 to a number from column 5. We ended up with a number in column 1. We can easily justify this by noticing that each pair of numbers can be written as $7a+3$ and $7b+5$ for some integers a and b. Their sum is

$$(7a+3)+(7b+5) \;=\; 7(a+b+1)+1\,.$$

Similar things happen when you look at subtraction and multiplication. (You should check this out yourself.)

Mathematicians, being extremely lazy beasts, are always looking for a short way of writing things. To show that the numbers 33 and 5 are in the same equivalence class, they write

$$33 \;\equiv\; 5 \pmod 7\,.$$

We read this as "33 is congruent to 5 modulo 7". What this means is that if we divide 33 and 5 by 7, we get the same remainder, or (equivalently) 33 and 5 differ by a multiple of 7.

We have been investigating some of the basic properties of congruences. We can write them down as follows.

Theorem (Properties of congruences). If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$\begin{aligned} a + c &\equiv b + d \pmod{m} \\ a - c &\equiv b - d \pmod{m} \\ a \times c &\equiv b \times d \pmod{m} \\ a^k &\equiv b^k \pmod{m} \end{aligned}$$

This theorem is the basis for *modular arithmetic*. We do the regular operations of arithmetic (except division, which is a little trickier), but instead of using all the numbers, we reduce our operations to m equivalence classes. For example,

$$45 + 20 \equiv 3 + 5 \equiv 8 \equiv 1 \pmod{7}$$

All very pretty, but how is it of any use? One use, before the advent of the pocket calculator, was to check long calculations for errors using *digital sums*. Let's see how this works.

The digital sum of a number is obtained by adding all the digits of the number. If the result is larger than 9, the process is repeated until the result is between 1 and 9 inclusive. For example, to calculate the digital sum of 43 658 912, we would first calculate $4+3+6+5+8+9+1+2 = 38$; then, since the result is larger than 9, we would calculate $3 + 8 = 11$; and finally, $1 + 1 = 2$, which is the digital sum. You may be surprised to find out that if you calculate the remainder when 43 658 912 is divided by 9, the result is also 2.

To check a calculation, you can find the digital sums of the numbers involved. For example, if a friend of yours has calculated

$$23\,495 \times 103\,621 = 2\,433\,505\,395\,,$$

you would look at the digital sums of the two numbers being multiplied, as well as the digital sum of the answer. You would get 5, 4, and 3, respectively. But, $5 \times 4 = 20$, which has a digital sum of 2. Since that does not match the digital sum of the answer, the answer must be wrong.

This method does not always work. If the digital sums match, there may still be an error (try to come up with an example). On the other hand, if the digital sums do not match, you are certain that the answer is wrong.

For homework, try to determine why the method of the digital sums works. (*Hint:* it is related to doing arithmetic modulo 9). Next time we will look at how we can use modular arithmetic to develop divisibility rules.