Two Tricks with Arithmetic – courtesy of Yakov Perelman and Martin Gardner

William Chen

The first trick is due to Yakov Perelman. Ask someone to choose a 3-digit number *abc*, repeat the digits to obtain the 6-digit number *abcabc*, write it down on a piece of paper and pass it on to a second person. Ask the second person whether the number is divisible by 7, then do the division, write down the answer and pass it on to a third person. Ask the third person whether the number is divisible by 11, then do the division, write down the answer and pass it on to a fourth person. Ask the fourth person whether the number is divisible by 13, then do the division, write down the answer and pass it back to the first person who may be a little surprised to find the number *abc* being handed back to him.

The second trick is due to Martin Gardner. Ask someone to write down a number comprising quite a few digits, such as a telephone number (but not starting with 0). A second person will now scramble the order of the digits in any way to obtain a new number with the same number of digits. A third person now subtracts the smaller of the two numbers from the larger one, and then add up all the digits of the difference, and obtain a number that is divisible by 9.

The solution of the second problem leads us to the theory of congruences. We shall study a few problems in this area.

The solution of the first puzzle is very simple arithmetic. Suppose that *abc* has value x. Then *abcabc*, being the sum of *abc*000 and *abc*, has value $1001x$. This is the value of the number that the second person gets. The second person divides it by 7 and obtains the value $143x$. The third person divides this by 11 and obtains the value $13x$. Finally, the fourth person divides this by 13 and recovers the value x. So the whole trick is based on the simple fact that $1001 = 7 \times 11 \times 13$.

The solution of the second puzzle is based on the following well known result.

Theorem 1. *An integer is divisible by* 9 *if and only if the sum of its digits is divisible by* 9.

Example. Consider the numbers 2358 and 3457. Since $2 + 3 + 5 + 8 = 18$ is divisible by 9 and $3 + 4 + 5 + 7 = 19$ is not, it follows that 2358 is divisible by 9, but 3457 is not.

Sketch of Proof. Suppose that the digits of a number are given by *abcd*. Let V be its true value, S be the sum of the digits, and $D = V - S$ be their difference. Then

$$V = 1000a + 100b + 10c + d \qquad \text{and} \qquad S = a + b + c + d.$$

Then

$$D = (1000a + 100b + 10c + d) - (a + b + c + d) = 999a + 99b + 9c.$$

Clearly D is divisible by 9. Now if S is divisible by 9, then $V = S + D$, being the sum of two numbers which are both divisible by 9, must be divisible by 9. On the other hand, if V is divisible by 9, then $S = V - D$, being the difference of two numbers which are both divisible by 9, must be divisible by 9. ◯

We can now attempt to understand the second puzzle. Suppose that the first person comes up with a number with value x and sum of digits s. The second person scrambles the digits to obtain a new number with value y, but the sum of the digits remains s. By interchanging the roles of x and y if necessary, we may assume that $x \geq y$. By Theorem 1 above, the numbers

$$x - s \qquad \text{and} \qquad y - s$$

are both divisible by 9, and so their difference

$$(x - s) - (y - s) = x - y$$

is divisible by 9. But then the difference obtained by the third person is precisely $x - y$. By Theorem 1 above, the number obtained by adding the digits of $x - y$ is divisible by 9.

We also the the following results concerning divisibility.

Theorem 2. *An integer is divisible by* 3 *if and only if the sum of its digits is divisible by* 3*.*

Example. Consider the numbers 2358 and 3457. Since $2 + 3 + 5 + 8 = 18$ is divisible by 3 and $3 + 4 + 5 + 7 = 19$ is not, it follows that 2358 is divisible by 3, but 3457 is not.

For a criterion for divisibility by 11, we need to make the following convention. Suppose that a positive integer has decimal representation $abcdef\ldots$. Let us say that the digits $a, c, e, \ldots$ are called the odd-positioned digits, while the digits $b, d, f, \ldots$ are called the even-positioned digits.

Theorem 3. *A positive integer with decimal representation* $abcdef\ldots$ *is divisible by* 11 *if and only if the difference between the sum of the odd-positioned digits and the sum of the even-positioned digits is divisible by* 11*; in other words, if and only if*

$$(a + c + e + \ldots) - (b + d + f + \ldots)$$

is divisible by 11*.*

Example. Consider the number 48035279358. We have

$$(4 + 0 + 5 + 7 + 3 + 8) - (8 + 3 + 2 + 9 + 5) = 27 - 27 = 0$$

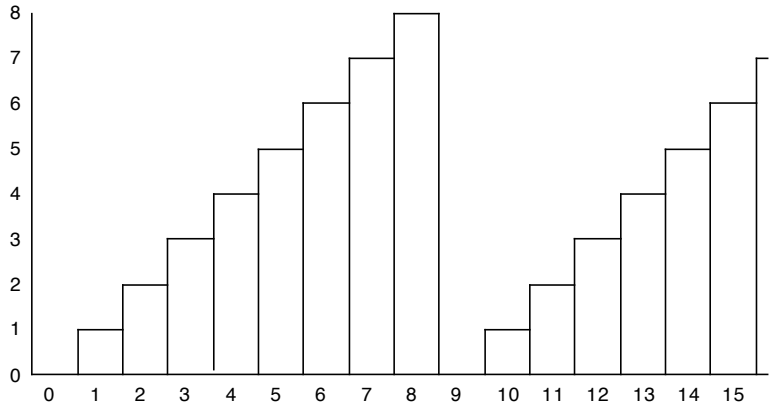
which is clearly divisible by 11, so 48035279358 is divisible by 11.

Let us return to the sketch of the proof of Theorem 1. There we have made use of the fact that the difference of the two numbers V and S is a multiple of 9. Using this fact, we carry the divisibility of S by 9 over to establish divisibility of V by 9, and *vice versa*. In other words, either both V and S are divisible by 9, or neither of them is divisible by 9. We recognize this fact by saying that V and S are congruent modulo 9.

We say that two integers x and y are congruent modulo 9 if the difference $x - y$ is divisible by 9. In this case, we write

$$x \equiv y \pmod 9.$$

For example, $3 \equiv 12 \pmod 9$, but $4 \not\equiv 8 \pmod 9$. Imagine an infinite 9-level "staircase" shown below, where we assign a step to each integer in an orderly fashion as shown. Then two integers are congruent modulo 9 if their steps are at the same level.



Of course, there is no need to restrict our discussion to modulo 9. Indeed, for every positive integer m, we say that two integers x and y are congruent modulo m if the difference $x - y$ is divisible by m. In this case, we write

$$x \equiv y \pmod{m}.$$

We can imagine an infinite m-level "staircase" where we assign a step to each integer in an orderly fashion in the same spirit as in the case when $m = 9$ above. Then two integers are congruent modulo m if their steps are at the same level.

We can even do arithmetic modulo m. Suppose that x and y are two integers. Then we can find the sum $x + y$ modulo m by finding a number s from $0, 1, 2, \ldots, m - 1$ such that

$$x + y \equiv s \pmod{m}.$$

We can also find the product xy modulo m by finding a number p from $0, 1, 2, \ldots, m - 1$ such that

$$xy \equiv p \pmod{m}.$$

Example. Consider the case when $m = 9$ again. Let $x = 4$ and $y = 7$. To find the sum $x + y$ modulo 9, we first realize that $x + y = 11$ in ordinary arithmetic. We now look at the numbers $0, 1, 2, \ldots, 8$ and see which one of these is congruent to 11 modulo 9. A little trial and error tells us that $2 \equiv 11 \pmod{9}$, so we conclude that $4 + 7 \equiv 2 \pmod{9}$. On the other hand, to find the product xy modulo 9, we first realize that $xy = 28$ in ordinary arithmetic. We now look at the numbers $0, 1, 2, \ldots, 8$ and see which one of these is congruent to 28 modulo 9. A little trial and error tells us that $1 \equiv 28 \pmod{9}$, so we conclude that $4 \times 7 \equiv 1 \pmod{9}$. We can check that we have the following addition and multiplication tables modulo 9.

$+$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

$\times$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

We can even establish a few simple results concerning arithmetic modulo m.

Theorem 4. *Suppose that* $x_1 \equiv x_2 \pmod{m}$ *and* $y_1 \equiv y_2 \pmod{m}$. *Then*
(i) $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$*; and*
(ii) $x_1 y_1 \equiv x_2 y_2 \pmod{m}$.

Sketch of Proof. The assumptions tell us that both $x_1 - x_2$ and $y_1 - y_2$ are divisible by m. To prove (i), we need to show that $(x_1 + y_1) - (x_2 + y_2)$ is divisible by m. To prove (ii), we need to show that $x_1 y_1 - x_2 y_2$ is divisible by m. Now

$$(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2)$$

is the sum of two numbers which are both divisible by m, and so is also divisible by m. On the other hand, we have

$$x_1 y_1 - x_2 y_2 = x_1 y_1 - x_2 y_1 + x_2 y_1 - x_2 y_2 = (x_1 y_1 - x_2 y_1) + (x_2 y_1 - x_2 y_2) = (x_1 - x_2) y_1 + x_2 (y_1 - y_2).$$

Note that $(x_1 - x_2) y_1$ is divisible by m, since $x_1 - x_2$ is. Also $x_2 (y_1 - y_2)$ is divisible by m, since $y_1 - y_2$ is. Hence the sum $(x_1 - x_2) y_1 + x_2 (y_1 - y_2)$ is also divisible by m. ◯

Example. Consider the case when $m = 9$ again. We have $2488 \equiv 4 \pmod{9}$ and $6476 \equiv 5 \pmod{9}$. It follows that

$$2488 + 6476 \equiv 4 + 5 \equiv 0 \pmod{9} \qquad \text{and} \qquad 2488 \times 6476 \equiv 4 \times 5 \equiv 2 \pmod{9}.$$

There is no need to find the sum $2488 + 6476$ or the product 2488×6476. Of course, sometimes we are simply given the problem of finding the sum and product of 2488 and 6476 modulo 9 without the knowledge that $2488 \equiv 4 \pmod{9}$ and $6476 \equiv 5 \pmod{9}$. However, if we divide 2488 and 6476 by 9, then we can see quite easily that we have remainders 4 and 5 respectively, so that $2488 \equiv 4 \pmod{9}$ and $6476 \equiv 5 \pmod{9}$. We can then proceed to find the sum and product of 2488 and 6476 modulo 9 as shown above.

We can also solve simple linear congruence equations. We illustrate the simple technique by some simple examples, and make some comments along the way.

Example. Consider the congruence equation $5 + x \equiv 3 \pmod{9}$. If there is any solution, then there must a solution from among $x = 0, 1, 2, \ldots, 8$. We have the following table:

x	0	1	2	3	4	5	6	7	8
$5 + x$	5	6	7	8	0	1	2	3	4

From this, we conclude that the solution required is $x = 7$. Alternatively, we can subtract 5 from both sides of the given congruence equation to obtain $x \equiv -2 \pmod{9}$, and then note that $-2 \equiv 7 \pmod{9}$.

Example. Consider the congruence equation $5x \equiv 3 \pmod{9}$. If there is any solution, then there must a solution from among $x = 0, 1, 2, \ldots, 8$. We have the following table:

x	0	1	2	3	4	5	6	7	8
$5x$	0	5	1	6	2	7	3	8	4

From this, we conclude that the solution required is $x = 6$. Note that we cannot work as if we were dealing with an equation like $5x = 3$ and divide both sides by 5, for then we end up with a fraction and a mess!

Example. Consider the congruence equation $6x \equiv 2 \pmod{8}$. If there is any solution, then there must a solution from among $x = 0, 1, 2, \ldots, 7$. We have the following table:

x	0	1	2	3	4	5	6	7
$6x$	0	6	4	2	0	6	4	2

From this, we conclude that the solutions required are $x = 3$ and $x = 7$. Note that the solution is not unique even when we impose the restriction that x comes from the range $0, 1, 2, \ldots, 7$.

Example. Consider the congruence equation $2x \equiv 1 \pmod 8$. If there is any solution, then there must a solution from among $x = 0, 1, 2, \ldots, 7$. We have the following table:

x	0	1	2	3	4	5	6	7
$2x$	0	2	4	6	0	2	4	6

From this, we conclude that the congruence equation has no solution.

Our last two examples send us the very important message that great care must be exercised when we study linear congruence equations. When we look at a linear equation of the form

$$ax = b,$$

where a is non-zero, then we have precisely one solution, namely

$$x = \frac{b}{a}.$$

However, suppose that we look at a linear congruence equation of the form

$$ax \equiv b \pmod m.$$

First of all, we must not divide both sides by a under any circumstances. Secondly, we must be aware that there may be more than one solution x from the range $0, 1, 2, \ldots, m-1$, or there may be no solution at all. The correct way to handle this congruence equation is then to work out ax for every $x = 0, 1, 2, \ldots, m$, and then determine what the solutions of the congruence are, if any.

We mention the following result which is beyond the scope of our present lectures. The linear congruence

$$ax \equiv b \pmod m$$

is soluble precisely when b is divisible by the greatest common divisor (a, m) of a and m. In this case, the number of solutions x in the range $0, 1, 2, \ldots, m-1$ is equal to the greatest common divisor (a, m).