WHY CASTING OUT NINES?

Ana Paula Garrão, PhD
Universidade dos Açores,/Departamento de Matemática, Portugal
Margarida Raposo Dias, PhD
Universidade dos Açores,/CMATI, Departamento de Matemática, Portugal

Abstract:
In this paper our purpose is to answer questions like: Why casting out nines works? Why it fails? Why casting out nines and not, for example, "casting out elevens"?
The casting out nines method was used to "check" the results of operations on positive integers. Although not currently taught in elementary school it hides mathematical concepts that will help to understand important current applications such as internet security.
We present the mathematical concepts behind the casting out nines method: some tests for computing remainders and the congruence relation modulo *n* and its properties.

Keywords: Divisibility; Congruence relation modulo *n*; Remainder in integer division.

Introduction

Casting out nines method was a well known process since elementary school, used to "check" the results of operations on positive integers. Currently it is not used, but it hides many mathematical concepts such as divisibility, decimal decomposition of an integer number and congruences, used in important current applications such as internet security.

In this paper our purpose is to answer questions like: Why casting out nines works? Why it fails? Why casting out nines and not, for example, "casting out elevens"?

In section 2 we present the mathematical concepts behind the casting out nines method: the congruence relation modulo *n* and its properties and some tests of divisibility.

The casting out nines method is a particular case of *casting out* ***n*** *method*, $n \in \mathbb{N}$, described in section 3. In section 4 we try to answer why, traditionally, the preferred is n=9 (casting out nines).

2. Remainder in integer division

Tests for the correctness of operations on integers, as casting out nines, are based in finding the remainder in integer division. In this section we present the mathematical ideas behind those processes.

Proposition 2.1*Let a and n be integer numbers, with* $n \neq 0$. *Then exists two integers q (quotient) and r (remainder), uniquely determined, such that*

$$a = nq + r, \ \ with \ \ 0 \leq r < |n|.$$

Notice that in integer division of one number *a* by *n*, one can get the remainder removing from *a* the largest multiple of the *n* lower than *a*.

An integer number *a* is said to be *divisible* by an integer number $n \neq 0$ (or that *n dividesa*), and we denote this by $n|a$, if the remainder, *r*, of the division of *a* by *n* is zero.

The following properties are the mathematical justification of the technique used in casting out *n*.

Proposition 2.2 *Let* $n \neq 0$ *be an integer number and* $\rho: \mathbb{Z} \to \{0,1,\dots,n-1\}$ *the map where* $\rho(x)$ *is the remainder of the division of x by n. Then:*

(i) $\rho(x) = \rho(y)$ if and only if $n|(x-y)$;

(ii) $\rho(x \pm y) = \rho\big(\rho(x) \pm \rho(y)\big)$;

(iii) $\rho(xy) = \rho\big(\rho(x)\rho(y)\big)$.

Proof: Let $x, y \in \mathbb{Z}$. By the division algorithm, we have

$x = nq_1 + \rho(x)$ and $y = nq_2 + \rho(y)$, with $q_1, q_2 \in \mathbb{Z}$.

(i) Then $x - y = n(q_1 - q_2) + \rho(x) - \rho(y)$ (1) .

If $\rho(x) = \rho(y)$ from (1) we have $n|(x-y)$.

If $n|(x-y)$, in (1) $\rho(x) - \rho(y) = 0$, thus $\rho(x) = \rho(y)$.

(ii) Then $x \pm y = n(q_1 \pm q_2) + \rho(x) \pm \rho(y)$ (2) .

If $\rho(x) \pm \rho(y) \geq n$ or $\rho(x) \pm \rho(y) < 0$ then exists $q_3 \in \mathbb{Z}$ such that

$\rho(x) \pm \rho(y) = nq_3 + \rho(\rho(x) \pm \rho(y))$. So we have from (2)

$x \pm y = n(q_1 \pm q_2 + q_3) + \rho(\rho(x) \pm \rho(y))$. Thus $\rho(x \pm y) = \rho\big(\rho(x) \pm \rho(y)\big)$.

(iii) Then $xy = nq' + \rho(x)\rho(y)$ with $q' = nq_1q_2 + q_1\rho(y) + q_2\rho(x)$. (3)

If $\rho(x)\rho(y) \geq n$ then exists $q_3 \in \mathbb{Z}$ such that

$\rho(x)\rho(y) = nq_3 + \rho(\rho(x)\rho(y))$. So we have from (3)

$xy = n(q' + q_3) + \rho(\rho(x)\rho(y))$. Thus $\rho(xy) = \rho\big(\rho(x)\rho(y)\big)$.

□

Example 2.3

Let *x*=15 and *y*=23.

1. If *n*=6 then $\rho(x) = 3$, $\rho(y) = 5$.

We have $\rho(x+y) = \rho(38) = 2$ and $\rho\big(\rho(x) + \rho(y)\big) = \rho(8) = 2$.

$\rho(x-y) = \rho(-8) = 4$ and $\rho\big(\rho(x) - \rho(y)\big) = \rho(-2) = 4$.

$\rho(xy) = \rho(345) = 3$ and $\rho\big(\rho(x)\rho(y)\big) = \rho(15) = 3$.

2. If *n*=9 then $\rho(x) = 6$, $\rho(y) = 5$.

We have $\rho(x+y) = \rho(38) = 2$ and $\rho\big(\rho(x) + \rho(y)\big) = \rho(11) = 2$.

$\rho(x-y) = \rho(-8) = 1$ and $\rho\big(\rho(x) - \rho(y)\big) = \rho(1) = 1$.

$\rho(xy) = \rho(345) = 3$ and $\rho\big(\rho(x)\rho(y)\big) = \rho(30) = 3$.

The operation of finding the remainder of the division between integer numbers can be referred as the modulo operation. In this case the remainder of the division of *a* by a fixed positive integer number *n*, is denoted by $a(mod\ n)$.

Furthermore if $a(mod\ n) = b(mod\ n)$ we say that *a* is *congruenttobmodulon,* and it is denoted by $a \equiv b\ (mod\ n)$.

For example, we have $24 \equiv 51\ (mod\ 9)$ since, with *n*=9 , $\rho(24) = \rho(51) = 6$.

Thus Proposition 2.2 can be expressed in terms of the congruence relation modulo *n*.

In fact the congruence relation modulo *n* identifies two integers if and only if their difference is a multiple of *n* , thus it may be regarded as an "equality" up to multiples of *n* . The items (ii) and (iii) can be expressed as:the modulo of a sum is the modulo of the sum of the modulos, as well as, the modulo of a product is the modulo of the product of modulos.

The congruence relation modulo *n* is an equivalence relation compatible with the operations of addition and multiplication. This congruence relation and its properties allow us to find the remainder in integer division without having to explicitly carry out the division.

Proposition 2.4*Let* $z = a_n a_{n-1} \dots a_1 a_0$*, be an integer number written in base 10. The remainder of the division of z:*

(i) by 9 (or by 3, respectively) is the remainder of the division of the sum of its digits by 9 (or by 3, respectively);

(ii) by 2 (or by 5, respectively) is the remainder of the division of its rightmost digit by 2 (or by 5, respectively);

(iii) by 4 (or by 25, respectively) is the remainder of the division of the number formed by its last two digits by 4 (or by 25, respectively);

(iv) by 11 is the remainder of the division of the sum of its digits taken with alternating signs, $a_0 - a_1 + a_2 - \cdots + (-1)^n a_n$ *, by 11.*

Proof:

(i) Let $z = a_n a_{n-1} \ldots a_1 a_0$, be an integer number written in base 10.

Then $z = a_n.10^n + a_{n-1}.10^{n-1} + \cdots + a_1.10 + a_0$. Since $10^i \equiv 1\ (mod\ 9)$, for all $i \in \mathbb{N}_0$, we have $z \equiv a_n + a_{n-1} + \cdots + a_1 + a_0\ (mod\ 9)$. That is the remainder of the division of *z* by 9 is the remainder of the division of the sum of its digits by 9.

Analogously, since $10^i \equiv 1\ (mod\ 3)$, $i \in \mathbb{N}_0$, the remainder of the division of *z* by 3 is the remainder of the division of the sum of its digits by 3.

(ii) Let $z = a_n a_{n-1} \ldots a_1 a_0$, be an integer number written in base 10.

Then $z = a_n.10^n + a_{n-1}.10^{n-1} + \cdots + a_1.10 + a_0$. Since $10^i \equiv 0\ (mod\ 2)$, for all $i \in \mathbb{N}$, we have $z \equiv a_0\ (mod\ 2)$. That is the remainder of the division of *z* by 2 is the remainder of the division of its rightmost digit by 2.

Analogously, since $10^i \equiv 0\ (mod\ 5)$, $i \in \mathbb{N}$, the remainder of the division of *z* by 5 is the remainder of the division of its rightmost digit by 5 .

(iii) Let $z = a_n a_{n-1} \ldots a_1 a_0$, be an integer number written in base 10.

Then $z = a_n.10^n + a_{n-1}.10^{n-1} + \cdots + a_2.10^2 + a_1.10 + a_0$. Since $10^i \equiv 0\ (mod\ 4)$, for all $i \in \mathbb{N}$, with $i \geq 2$, we have $z \equiv a_1.10 + a_0\ (mod\ 4)$. That is the remainder of the division of *z* by 4 is the remainder of the division of the number formed by its last two digits by 4.

Analogously, since $10^i \equiv 0\ (mod\ 25)$, for all $i \in \mathbb{N}$, with $i \geq 2$, the remainder of the division of *z* by 25 is the remainder of the division of the number formed by its last two digits by 25.

(iv) Let $z = a_n a_{n-1} \ldots a_1 a_0$, be an integer number written in base 10.

Then $z = a_n.10^n + a_{n-1}.10^{n-1} + \cdots + a_1.10 + a_0$. Since $10 \equiv -1\ (mod\ 11)$, we have $10^{2i} \equiv 1\ (mod\ 11)$ and $10^{2i+1} \equiv -1\ (mod\ 11)$, for all $i \in \mathbb{N}$. Therefore

$$z \equiv a_0 - a_1 + a_2 - \cdots + (-1)^n a_n (mod\ 11).$$

That is the remainder of the division of *z* by 11 is the remainder of the division ofthe sum of its digits taken with alternating signs.

The *digital sum* of a positive integer number $z = a_n a_{n-1} \ldots a_1 a_0$, written in base 10 is the sum of its digits, $a_n + a_{n-1} + \cdots + a_1 + a_0$. The *digital root* (or repeated digital sum) of a positive integer number *z*, denoted by dr(*z*), is obtained by an iterative process of summing digits, using, on each iteration, the result from the previous iteration. The process continues until a single-digit number is reached. For example, dr(1598)=5, because 1+5+9+8=23 and 2+3=5.

Extract the digital root of *z* is, essentially, get the remainder of the division of *z* by nine, with an exception when the number *z* is a multiple of nine, because the digital root of *z* is nine, but the remainder of the division for *z* by nine is zero.

When getting the remainder of the division of a positive integerby nine we might remove ("cast out") any nines that appear as digits in the original number and also can remove together any digits that sum to 9, since $9 \equiv 0 (\mathrm{mod}\ 9)$ and the congruence relation modulo *n* is compatible with addition. This procedure can save time in the case of very large numbers.

Example 2.5

As we mentioned above, the digital root of 1598 is 5. It can be obtained removing the digit 9 and the digits 8 and 1.

In fact $1598 \equiv 1 + 5 + 9 + 8\ (mod\ 9)$ by Proposition 2.4 (i). Since $9 \equiv 0 (\mathrm{mod}\ 9)$and the congruence relation is compatible with addition we obtain $1598 \equiv 5\ (mod\ 9)$.

Casting out *n* method

We now give the steps of *casting out* ***n*** *method*, with $n \in \mathbb{N}$, used to "check" the results of operations addition and multiplication, that relies on Proposition 2.2.

Let n be a positive integer number and $\rho: \mathbb{N} \to \{0,1, \dots, n-1\}$ the map where $\rho(x)$ is the remainder of the division of *x* by *n*.

Addition: Suppose we add two positive integers x, y, and find the result *S*. We want to "check" its correctness.

We act as follows:

1. Calculate $x + y = S$.
2. Determine $\rho(x)$ and $\rho(y)$.
3. Calculate $\rho\big(\rho(x) + \rho(y)\big)$.
4. Calculate $\rho(S)$.

The following scheme is a practical way to present the steps described above.

$\rho(x)$	$\rho\big(\rho(x) + \rho(y)\big)$
$\rho(y)$	$\rho(S)$

Multiplication: Suppose we multiply two positive integers x, y, and find the result *P*. We want to "check" its correctness.

We act as follows:

1. Calculate $x\ y = P$
2. Determine $\rho(x)$ and $\rho(y)$.
3. Calculate $\rho\big(\rho(x)\rho(y)\big)$.
4. Calculate $\rho(P)$.

The following scheme is a practical way to present the steps described above.

$\rho(x)$	$\rho\big(\rho(x)\rho(y)\big)$
$\rho(y)$	$\rho(P)$

In both cases, if we get different numbers in steps 3 and 4, by Proposition 2.2, we are sure to have made a mistake.

If we get the same number in steps 3 and 4, the result found passed the test, but we are not certain the operation was carried out correctly, we only deduce that the correct result and the one we found are congruent modulo *n*. This is the reason why casting out *n* sometimes fails since it doesn't detect all errors.

Example 3.1: Suppose we add two positive integers, say $x = 149\ , y = 232$, and find the result 149+232=381. We want to "check" its correctness. We can use any value for *n*.

Using $n = 9$, we have the following scheme:

5	3
7	3

Using $n = 4$, we have the following scheme:

1	1
0	1

In both cases, we are not certain the operation was carried out correctly. We only deduce that the correct result and the one we found are congruent modulo *n*.

If in this example we find the **wrong** result 371, we have

Using $n = 9$

5	3
7	1

We are sure to have made a mistake.

Note that, using, for example *n*=6, we also are sure to have made a mistake:

5	3
4	5

But, using, for example *n*=2, we would not notice the mistake:

1	1
0	1

In the first two cases the error is detected because 371(wrong result) and 381(right result) are not congruent modulo 9 neither modulo 6.

In the last case the error is not detected because 371 and 381 are congruent modulo 2.

Example 3.2: Suppose we multiply two positive integers, say $x = 15$, $y = 23$, and find the result $15 \times 23 = 345$. We want to "check" its correctness. We can use any value for *n*.

Using $n = 9$, we have the following scheme:

6	3
5	3

Using $n = 4$, we have the following scheme:

3	1
3	1

In both cases, we are not certain the operation was carried out correctly.

If in this example we find the **wrong** result 75, using $n = 9$

6	3
5	3

we would not notice the mistake, because 345 and 75 are congruent modulo 9.

However using $n = 4$

3	1
3	3

we are sure to have made a mistake. In this case we detect the mistake since 345 and 75 are not congruent modulo 4.

Casting out nines versus casting out *n*

As we saw this procedure to "check" if the operation was carried out correctly can be used with any *n*>0. Let us now answer why, traditionally, the preferred is *n*=9 (casting out nines).

The method to compute the remainder of the division of a positive integer number by three is similar to that of nine (Proposition 2.4 (i)), why don't we use casting out threes? Because a random answer to an arithmetic operation has probability $1/9$ of passing the test of casting out nines while the corresponding probability is $1/3$ for casting out threes.

Casting out nines method doesn't detect all errors. One of them is when, accidentally, we write two adjacent digits in the wrong order. If we use casting out elevens, this kind of error is detected. In fact to compute the remainder of the division of a positive integer number by 11 we alternately add and subtract digits, starting from the right (Proposition 2.4 (iv)). For

instance, to calculate the remainder of the division of 1537 by 11, we do 7-3+5-1 which is 8. If we change the adjacent digits 5 and 3 we get 1357 and we do 7-5+3-1 which is 4. When we obtain a negative number we add 11. For example, to calculate the remainder of the division of 6213 by 11, we do 3-1+2-6 which is $-2 \equiv -2+11 \equiv 9 \pmod{11}$, so the remainder is 9.

However compute the remainder of the division of one number by nine is more accessible and fast, reason why was preferred casting out nines.

On using *casting out n method*, the only difference is in the "shortcut" to compute the remainder in the integer division by *n*.

Once the test to compute the remainder in integer division by nine is the most accessible, and some way amusing, the casting out nines method is the preferred.

Conclusion

The question "Why casting out nines?" can be completed this way: Why casting out nines works? Why casting out nines fails? Why casting out nines and not, for example, casting out elevens? Those questions were answered throughout the text.

But the original question can be seen in another sense: Why discuss casting out nines nowadays?

Indeed currently the casting out nines method is not used. One reason is the generalized use of electronic calculators and another is because it is not really a method to check the results of operations on integers.

In our opinion the richness of the mathematical ideas behind this method justifies its approach nowadays. In fact mathematical concepts such as divisibility and arithmetic modular are used in important current applications such as internet security.

References:

Baldoni, M. W., Ciliberto, C., Piacentini Cattaneo, G.M. Elementary Number Theory, Cryptography and Codes. Springer, 2009

Fernandes, Rui L., Ricou, Manuel. Introdução à Álgebra. IST Press. Portugal, 2004

Benson, Donald C. The Moment of Proof: Mathematical Epiphanies; web site http://books.google.pt/books?id=8_vbuzxrpfIC&pg

QED Infinity Web site http://www.qedinfinity.com/textbook/fundamentals-of-mathematics/2-techniques-of-numerical-calculations/