Checking Polynomial Arithmetic—Casting Out 9's Reincarnated

Murray L. Lauber

Casting out 9's is a centuries-old method for checking computations. With the introduction of calculators and computers, it has lost most of its value. But, as we shall see, it is not a completely antiquated procedure. A generalization of it can be used to check polynomial arithmetic, that is, computations involving adding, subtracting, multiplying and dividing polynomials. In addition, it has some affinities with a type of code currently used in detecting and correcting errors in messages transmitted by computers.

A Brief Review of Casting Out 9's

To understand the basis of casting out 9's, let us take a short excursion into the world of modular arithmetic. In the language and notation of modular arithmetic, an integer, a, is congruent to another integer, b, modulo n, n a counting number, if $a=b+kn$, or $a-b=kn$, where k is an integer. That is, a and b differ by a multiple of n. This is written $a\equiv b(\text{mod } n)$. For example, using $n=9$, we know that $33\equiv 6(\text{mod } 9)$ because $33=6+(3*9)$. Another way of understanding this is to observe that 6 is the remainder when 33 is divided by 9. We will refer to the number less than 9 to which an integer is congruent modulo 9 as the mod 9 equivalent of the integer. For example, the mod 9 equivalent of 33 is 6. The process of finding the mod 9 equivalent of a number is appropriately referred to as casting out 9's because it subtracts a multiple of 9 from the number. For example, to find the mod 9 equivalent of 33, we subtract 3*9, or cast out three 9's, from 33.

Briefly, the method of checking computations with integers by casting out 9's is done as follows. Each number in the computation is changed to its mod 9 equivalent by casting out 9's to obtain an analogous problem modulo 9. In fact, computations can be checked as well by casting out 8's, 7's or any other counting number. For numbers represented in base 10, the particular beauty of casting out 9's is that it can be done simply by summing the digits of the numbers involved, recursively if necessary, to obtain single-digit numbers. Once the mod 9 equivalent of each of the numbers in the computation has been found, the computation is done using these single-digit numbers. The answer to this simple computation is then compared to the mod 9 equivalent of the answer to the original more complex computation, again using the method of summing digits. Some examples are given in Table 1.

A fuller exploration of casting out 9's is included in an article in *The Mathematics Teacher* (Lauber 1990). As noted in that article, casting out 9's has its analogues in other bases, for example, casting out 7's in base 8 arithmetic, casting out 4's in base 5 arithmetic, or, in general, casting out $(b-1)$'s in base b arithmetic. A variant of this general analogue, casting out $(x-1)$'s, is of particular use in checking polynomial arithmetic. We will focus specifically on integral polynomials, that is, polynomials with coefficients that are integers, but the analogue applies also to all real polynomials and even to those with complex coefficients.

What Is Casting Out $(x-1)$'s?

An integral polynomial in x may be thought of as a number base x. Consider, for example, the numbers 6347(base 10), 6347(base 8) and the polynomial $p(x) = 6x^3+3x^2+4x+7$. In expanded form, these may be written as follows.

6347(base 10) = $(6*10^3)+(3*10^2)+(4*10^1)+(7*10^0)$
6347(base 8) = $(6*8^3)+(3*8^2)+(4*8^1)+(7*8^0)$

In base 8, the number eight would be denoted by the digits 10. The digit 8 is used here to avoid confusion.

$p(x) = (6*x^3)+(3*x^2)+(4*x^1)+(7*x^0)$

Clearly, if $x = 10$, then $p(x)$ just becomes $(6*10^3)+(3*10^2)+(4*10^1)+(7*10^0)$ or 6347(base 10), and, if $x=8$, $p(x)$ becomes 6347(base 8). This illustrates the basic parallel between polynomials and numbers written in base 10 or some other base.

It should be clear, then, that casting out $(x-1)$'s from a polynomial in the variable x is the analogue to casting out 9's from a number in base 10. It should be apparent as well that the parallel in polynomial arithmetic to summing digits in base 10 arithmetic is summing the coefficients of the polynomials involved. To illustrate, consider the following examples.

Casting Out 9's

(a) By finding the remainder when dividing by 9:

$6347 = (705*9)+2$

(b) By summing digits recursively:

$6347 \rightarrow 6+3+4+7 = 20 \rightarrow 2+0 = 2$

Casting Out $(x-1)$'s

(a) By finding the remainder when dividing by $x-1$:

Synthetic division of $6x^3+3x^2+4x+7$ by $x-1$ yields a remainder of 20:

-1 |	6	3	4	7
	-0	-6	-9	-13
	6	9	13	20

(b) By summing the coefficients:

$6+3+4+7 = 20$

Table 2 gives three examples of checking computations with integral polynomials by casting out $(x-1)$'s, employing the method of summing the coefficients. The problem of addition of polynomials in (a) probably does not require further explanation. In (b), the product $(3x^3+2x^2-3x+6)(2x^2+7x-3)$ is checked. The sum of the coefficients of $3x^3 + 2x^2 - 3x + 6$ is $3+2-3+6 = 8$. The sum of the coefficients of $2x^2+7x-3$ is $2+7-3 = 6$. The product of these sums, $8*6$, is 48. The reader may check that the product of the two polynomials is $6x^5+25x^4-x^3-15x^2+51x-18$. The sum of the coefficients of this product is $6+25-1-15+51-18=48$. Thus the mod$(x-1)$ equivalent of the product of the two polynomials involved is equal to the product of the mod$(x-1)$ equivalents of the two polynomials. (It may be instructive to relate that, in my first attempt at finding this product, I quickly discovered, through casting out $(x-1)$'s, that the answer was incorrect.)

Checking division of polynomials is illustrated in (c) in Table 2. The reader may verify that when $3x^5-2x^4+x^3-4x^2+6x+9$ is divided by x^2-3x+7, the quotient is $3x^3+7x^2+15x-8$ and the remainder is $-75x+65$. This may be restated in terms of the division algorithm as follows.

$3x^5-2x^4+x^3-4x^2+6x+9=$
$(3x^3+7x^2+15x-8)(x^2-3x+7)+(-75x+65)$.

The corresponding statement mod$(x-1)$, $13 = [(-39)*5] + 208$, is true. To ease computation, this statement could be further converted to its mod 9 equivalent using casting out 9's, but some care is needed in finding this mod 9 equivalent of -39 because it is negative. Its mod 9 equivalent may be found as follows: $-39 \rightarrow -(3+9) = -12 \rightarrow -(1+2) = -3$. But $-3 \equiv 6 \pmod 9$ because $-3=6+(-1)(9)$. The reader is invited to complete the construction of the mod 9 equivalent of the statement $13=[(-39)*5]+208$.

Why Casting Out $(x-1)$'s Works

There are several possible levels of mathematical justification for summing coefficients to check polynomial arithmetic. We will examine two of them. The first is direct, bypassing the ideas of modular arithmetic and casting out $(x-1)$'s. Consider, for example, the product of a third degree polynomial $p(x) = a_0+a_1x+a_2x^2+a_3x^3$ and a second degree polynomial $q(x) = b_0+b_1x+b_2x^2$. Then

$$p(x)q(x)=(a_0+a_1x+a_2x^2+a_3x^3)(b_0+b_1x+b_2x^2)$$

Using the commutative, associative and distributive properties, we obtain

$$\begin{aligned} p(x)q(x) &= (a_0+a_1x+a_2x^2+a_3x^3)b_0 \\ &\quad + (a_0+a_1x+a_2x^2+a_3x^3)b_1x \\ &\quad + (a_0+a_1x+a_2x^2+a_3x^3)b_2x^2 \\ &= (a_0b_0+a_1b_0x+a_2b_0x^2+a_3b_0x^3) \\ &\quad + (a_0b_1x+a_1b_1x^2+a_2b_1x^3+a_3b_1x^4) \\ &\quad + (a_0b_2x^2+a_1b_2x^3+a_2b_2x^4+a_3b_2x^5) \\ &= a_0b_0+(a_1b_0+a_0b_1)x+(a_2b_0+a_1b_1+a_0b_2)x^2 \\ &\quad + (a_3b_0+a_2b_1+a_1b_2)x^3 \\ &\quad + (a_3b_1+a_2b_2)x^4+a_3b_2x^5 \end{aligned}$$

The sum of the coefficients of $p(x)q(x)$ is

$$a_0b_0 + \{a_1b_0+a_0b_1\} + \{a_2b_0+a_1b_1+a_0b_2\} + \{a_3b_0+a_2b_1+a_1b_2\} + \{a_3b_1+a_2b_2\} + a_3b_2.$$

This sum is equal to $\{a_0+a_1+a_2+a_3\}\{b_0+b_1+b_2\}$, which is just the product of the sum of the coefficients of $p(x)$ and the sum of the coefficients of $q(x)$.

This demonstration that the sum of the coefficients of the product of $p(x)$ and $q(x)$ is equal to the product of the sums of their coefficients can be generalized to polynomials of any degree by induction. A similar argument can be constructed pertaining to the sum or difference of two polynomials. Thus the method of summing coefficients can be used to check polynomial arithmetic involving combinations of multiplication, addition and subtraction. Because by the division algorithm, division can be stated in terms of multiplication and addition, division of polynomials can also be checked by this method.

Another level of justification employs the notions of modular arithmetic. Its focus is initially on casting out $(x-1)$'s rather than summing coefficients. It is based on the following theorem:

Theorem: Let p(x) *and* q(x) *be polynomials with integral coefficients and* n *be a natural number. If* a, r *and* s *are integers such that* p(a) ≡ r(mod n) *and* q(a) ≡ s(mod n), *then*

(a) [p(a)+q(a)] ≡ (r+s)(mod n);
(b) p(a)q(a) ≡ *rs*(mod n).

A proof of (b) uses the definition of congruence modulo n given earlier along with the associative and distributive properties as follows:

$$p(a) \equiv r(\text{mod } n) \text{ and } q(a) \equiv s(\text{mod } n)$$

$$\Rightarrow \begin{cases} p(a)=r+kn \text{ for some integer } k, \text{ and} \\ q(a)=s+jn \text{ for some integer } j \end{cases}$$

$$\Rightarrow p(a)q(a)=(r+kn)(s+jn)$$

$$\Rightarrow p(a)q(a)=rs+rjn+kns+kjn^2$$

$$\Rightarrow p(a)q(a)=rs+(rj+ks+kjn)n$$

$$\Rightarrow p(a)q(a) \equiv rs(\text{mod } n)$$

The proof of part (a) is left to the reader.

This theorem may be restated in terms of remainders after dividing by n. Part (b), for example, says basically that the remainder when the product of $p(a)$ and $q(a)$ is divided by n is the same as the product of the remainders when $p(a)$ and $q(a)$ are each divided by n. That is, if we cast out n's before taking the product, we will get the same result as if we cast out n's after taking the product.

Putting $a=x$ and $n=x-1$ in the above theorem, and assuming x is an integer, justifies casting out $(x-1)$'s as a way of checking computations involving integral polynomials. What remains to be demonstrated is that casting out $(x-1)$'s from a polynomial, that is, finding the remainder when we divide it by $x-1$, is the same as summing its coefficients. This is quite easy to do. The remainder theorem guarantees that if a polynomial $p(x)$ is divided by $(x-1)$, then the remainder is $p(1)$. The only other observation needed is that $p(1)$ is just equal to the sum of the coefficients of $p(x)$. This follows because any power of 1 is just equal to 1. For example, if $p(x) = 3x^5-2x^4+x^3-4x^2+6x-9$, then $p(1) = 3-2+1-4+6-9$.

Each of these methods of justification has its own appeal. The latter is more general in one sense because it applies neatly to polynomials of any degree. But it has deficiencies as well. For example, it cannot be used to justify casting out $(x-1)$'s as a means of checking computations with nonintegral polynomials because, strictly speaking, the theory of modular arithmetic applies only to integral quantities. The first justification, though not so tidy, has the advantage of being generalizable to all real polynomials, and even to complex polynomials.

Polynomial Codes—An Outgrowth of Modular Arithmetic

Although it is too big a topic to cover in this article, it is of interest that the concept of quotient rings, a generalization of modular arithmetic, and employing some of the same basic notions as the procedure of casting out $(x-1)$'s, forms the basis for powerful error correcting/detecting codes for computer messages. There are some parallels, as well as some differences, between polynomial codes and casting out $(x-1)$'s. Polynomial codes do not have the capability of checking computations, but they are capable of detecting and correcting errors in the bits of "words" transmitted in computer messages. Polynomial codes are more powerful than casting out $(x-1)$'s in that they are capable of correcting as well as detecting errors. They are also of more practical significance because they serve a larger role in our technological society. For brief descriptions of the nature, along with some examples, of polynomial codes and other error detecting/correcting codes, refer to Laufer (1984, 1–61, 476–85), Lax (1991, 209–64), Biggs (1989, 375–98) and Gersting (1987, 339–67).

Conclusion

Casting out $(x-1)$'s has a lot of potential as a subtopic of polynomials in the high school mathematics curriculum. It could be a very useful tool in the mathematical repertoires of high school and college students because of its usefulness in checking polynomial arithmetic. It has the potential to illustrate a variety of methods of mathematical justification. It has value, as well, for illustrating how the centuries-old method of checking computations, casting out 9's, though now mostly obsolete because of calculators and computers, can be generalized into the still-useful tool of casting out $(x-1)$'s. In addition, it has significant affinities with the still-more-general notion of quotient rings that form the basis of polynomial codes. Perhaps through a brief study of casting out $(x-1)$'s, students' curiosity could be inspired to research the polynomial codes concept and thus begin to explore some notions usually reserved for college or university courses in abstract algebra. The progressive levels of generalization, from casting out 9's to casting out $(x-1)$'s to polynomial codes, could be used to illustrate how mathematics has developed historically, from particular to general, and to demonstrate the increasing power that accompanies the movement to higher levels of generalization.

References

Biggs, N. L. *Discrete Mathematics. Rev. ed. New York: Oxford University Press, 1989.*

Gersting, J. L. *Mathematical Structures for Computer Science.* 2d ed. New York: Freeman, 1987.

Lauber, M. L. "Casting Out Nines—An Explanation and Extensions." *The Mathematics Teacher* (November 1990).

Laufer, H. B. *Discrete Mathematics and Applied Modern Algebra.* Boston: BWS, 1984.

Lax, R. F. *Modern Algebra and Discrete Structures.* New York: Harper Collins, 1991.

Table 1 Examples of Casting Out 9's

	Problem	Summing Digits Recursively			Analogous Problem Modulo 9
a)	164	1+6+4 = 11	1+1 = 2		2
	x 27	2+7 = 9	0		x 0
	4428	4+4+2+8 = 18	1+8 = 9	0	0
b)	4389	4+3+8+9 = 24	2+4 = 6		6
	+ 2186	2+1+8+6 = 17	1+7 = 8		+ 8
	6575	6+5+7+5 = 23	2+3 = 5	5 = 1+4	14
c)	23.98	2+3+9+8 = 22	2+2 = 4		4
	x 4.31	4+3+1 = 8			x 8
	103.3538	1+0+3+3+5+3+8 = 23	2+3 = 5	5 = 3+2	32

Table 2 Examples of Casting Out $(x-1)$'s

	Problem	Sum of Coefficients	Analogous Problem Modulo $(x-1)$
a)	$4x^4 - 2x^3 + 10x^2 - 6x + 3$	$4 - 2 + 10 - 6 + 3 = 9$	9
	$+\ 7x^3 - 8x^2 - 2x + 6$	$7 - 8 - 2 + 6 = 3$	+ 3
	$4x^4 + 5x^3 + 2x^2 - 8x + 9$	$4 + 5 + 2 - 8 + 9 = 12$	12
b)	$3x^3 + 2x^2 - 3x + 6$	$3 + 2 - 3 + 6 = 8$	8
	x $2x^2 + 7x - 3$	$2 + 7 - 3 = 6$	x 6
	$6x^5 + 25x^4 - x^3 - 15x^2 + 51x - 18$	$6 + 25 - 1 - 15 + 51 - 18 = 48$	48
c)	Dividend: $3x^5 - 2x^4 + x^3 - 4x^2 + 6x + 9$	$3 - 2 + 1 - 4 + 6 + 9 = 13$	13
	Divisor: $\div\ x^2 - 3x + 7$	$1 - 3 + 7 = 5$	÷ 5
	Quotient: $3x^3 + 7x^2 + x - 50$	$3 + 7 + 1 - 50 = -39$	− 39
	Remainder: $-151x + 359$	$-151 + 359 = 208$	208

OR

$$3x^5 - 2x^4 + x^3 - 4x^2 + 6x + 9 = (3x^3 + 7x^2 + x - 50)(x^2 - 3x + 7) + (-151x + 359)$$

is analogous to

$$13 = (-39)(5) + 208$$

[which is true]