Beginning Abstract Algebra at Elementary School

Diego Pareja-Heredia. ***Universidad del Quindío***

Abstract

Decimal number representations can be seen as polynomials with coefficients in the set {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} with the property:

$$x^n = 10x^{n-1}$$

With this in mind, we define addition and multiplication on natural numbers the same way as we do with polynomials. However, there are two other types of multiplications, that we can introduce before the traditional one: a kind of inner product inside the number representation, and the multiplication by a scalar.

To find factors of a natural number, we could proceed with its associate polynomial. As a consecuence, we present an empirical procedure to verify primality without using division. With these polynomials we can also explain rationally the use of carriers inside the arithmetical algorithms.

Introduction. Mathematics education has been lagging far behind the develoment of mathematics, particulary along the past century[1]. The only way I can imagine to solve this slow down problem is through a radical change in the K-12 math curriculum. I propose in this paper to introduce algebra as early as at the 3rd grade followed with mathematics more advanced than the traditional one; hoping that students, at the end of their high school, can manage elements of real analysis; among other things: vector and abstract spaces. One way to do it, is beginning with polynomials along the study of nth-dimensional vector spaces.

According to Lynn Arthur Steen[2], a political scientist asks “Is Algebra Necessary?” to mean really that, algebra is not working in the curriculum and that, “something other than algebra is needed to enhance students’ understanding of where various numbers come from and what they actually convey”. He is addressing to K-12 curriculum, where algebra is one of the high school courses. So it may sound crazy to suggest, as I am doing here, to start teaching algebra at elementary school. However I think that the best way to show “students´ understanding of where various numbers come from and what they actually convey” is through the use of elementary algebra, beginning with the most simple functions: decimal polynomials.

[1] See: **Diego Pareja-Heredia. The Huge Gap between Math Education and the front of Mathematics** (Preliminary Version)
http://tsg.icme11.org/document/get/571

[2] Steen, L. A. *Can we make school mathematics work for all?* Notices of the AMS. December 2013. Can be read at: http://www.ams.org/notices/201311/rnoti-p1466.pdf

These notes are aimed to prospective teachers of elementary school mathematics. The topics described along these lines, are intended for kids at elementary school, nevertheless they need a previous makeup before entering the classroom.

Polynomials are algebraic expressions of the type

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 x^0 = \sum_{j=0}^{j=n} a_{n-j}x^{n-j} . \qquad (*)$$

Where { a_n, a_{n-1},..., a_0 } are coefficients taken from a specified set, and the indeterminate x can be defined on the set of real numbers. When the coefficients are taken in the set {0, 1, … , 9}, we´ll say that P is a decimal polynomial.

As we can see, (*) is made of sums and products (multiplications of integers) and $a_n x^n$ is a simplified form of writing $a_n \times x \times ... \times x,$ where x appears n times as a factor.

Addition and multiplication are closed operations in the set of natural numbers **N**. Perhaps, substraction and division are not; that is one of the reasons why, their algorithms are difficult to understand. Before any definition of substraction and division, it could be more convenient to introduce integers and rational numbers, where substraction and division are closed. Negative numbers can be assimilated at the kindergarten level in a ludic setting. Rational numbers can be introduced early at elementary school as a consecuence of the study of linear polynomials of the type:

$$f(x) = \frac{b}{a}x$$

Where a, b are integers and $a \neq 0$. From here, it is also possible to derive all the study of proportionality and the rule of three.

Elsewhere[3] I have made some historical remarks on the hindu-arabic representation of numbers as we write them now. In this paper we want to present a few examples of how the representation of natural numbers as polynomials, can help us to know some specific number characteristics, like: factors, primality, number qualities as in, Fibonacci, Fermat and Mersenne numbers, twin primes, etc.

The main purpose of these notes is to explain the reader, what kind of mathematics is behind the common arithmetic algorithms, and not to show alternative easy methods for calculations. Calculators, and in general, computers make this job soberly. Before we intent to explain any

[3] Pareja-Heredia, D. *¿Por qué 2 × 2 = 4, y no a 3 ó 5, por ejemplo?* en: http://www.matematicasyfilosofiaenelaula.info/articulos/porque2por2igual4.pdf

kind of mathematics, we should introduce our students in the basic techniques of logical thinking including relations as equality and basic notions of elementary geometry.

Natural Numbers as Polynomials.

The most amazing invention of indian mathematicians was that, natural numbers can be represented using just ten digits in a positional fashion, taking values for digits according the place they are located in the numeral. For instance, the numeral 7549 represents the sum:

7000 + 500 + 40 + 9 = $7\times1000+5\times100+4\times10+9=7\times10^3+5\times10^2+4\times10^1+9\times10^0$ =7549.

In a positional numerical system, the numbers are represented as a systematic sequence of sums and products. This sequence is similar to a polynomial, where the variable x is replaced, in this case, by the number 10, the base of the numerical system. Then, the number 7549 can be seen as the polynomial:

$$P(x) = 7x^3+5x^2+4x+9$$

The numerical value of $P(x)$, at $x = 10$, will be 7549.

Vector Notation. Polynomials of one variable are characterized for their coefficients and for the indeterminate x with its exponents in descending order. In the above example these coefficients are (7 , 5 , 4 , 9) and the exponents are arranged like (x^3 , x^2 , x , x^0). The way of writing numbers and variables inside a parenthesis is common in vector analysis, where the order of the entries is important. Borrowing this notation we may now arrange our digits remembering that the order here, is sequencially decimal, where the highest power at left in our example, are thousands, then hundreds, tens, and units at right. That is exactlly the order in the vector (x^3 , x^2 , x , x^0**),** where, $x^0 = 1$**.**

In the decimal representation of 7549 we can introduce a new symbolism:

$P(x) = 7x^3 + 5x^2 + 4x + 9 = (7 , 5 , 4 , 9) \bullet (x^3, x^2, x , 1) = 7\times x^3 + 5\times x^2 + 4\times x + 9\times1$.

The operation "•" is the scalar product, dot product or inner product of the two vectors. This inner product will be studied in relation with Hilbert spaces, which are important to understand the roots of new technologies[4].

[4] These ideas were introduced in: http://www.matematicasyfilosofiaenelaula.info/conferencias/Del%20Bit%20a%20las%20Wavelets%20XVII%20CNM%20-%20CALI.pdf.

When a digit is relocated one place from right to left in the numeral, its value is multiplied by ten. This property can be stablished by the *fundamental formula*:

$$x^n = 10x^{n\text{-}1}$$

Which means literally that the n-th place (from right to left) in the numeral is ten times the value at the $(n-1)$ place from right to left. Perhaps, this formula reduces to a very simple fact: $x = 10$, the basis of the positional system. When we change this formula for

$$x^n = 2x^{n-1}$$

And the coefficients take their values in {0, 1} we will expressing numbers in binary form, just with digits **0** and **1**.[5]

After some practice in writing and reading numerals as polynomials, we introduce the definition of addition and multiplication. When we have a number represented by a polynomial, using the fundamental formula, we automatically get many more ways to exhibit the same number throught different polynomials, equivalent to the decimal one, which is unique. Let us take again the number 7549, represesented by the polynomial:

$$P(x) = 7x^3+5x^2+4x+9$$

By the fundamental property, $x^3 = 10x^2$, and since $7x^3 = 6x^3 + x^3 = 6x^3 + 10x^2$, we find that,

$$7x^3 + 5x^2 + 4x + 9 = 6x^3+x^3+5x^2+4x+9=6x^3+10x^2+5x^2+4x+9=6x^3+15x^2+4x+9.$$

Although the last polynomial is not decimal, its numerical value, when $x = 10$ is again 7549. We can make similar changes in each level, to find new representations of the number. This means that the polynomial representation is not unique for a specific number. However, the possibility to change the numeral let us find the factors of a natural number without any division proccess, as we shall see later.

Instead of introducting formal definitions for arithmetical operations, let us put some simple examples.

Example 1. *Adding numbers of same order.* To begin with, it is important to introduce students in managing the use of equalities, parenthesis, powers, signs for operations, and also to know some number properties like associative, commutative and distributive laws.

We say that two numbers *n, m;* have the same order when they are expressed in the form

$$n = ax^i,\ m = bx^i.$$ Here *i* is a positive integer.

Here a and b are digits. In elementary algebra we say they are similar monomials, i. e., the only differece could be the coefficient, a in the former and b in the latter. As polynomials,

[5] See: *Aritmetica en el Espectro de los Números Naturales* en: http://www.matematicasyfilosofiaenelaula.info/conferencias/aritmeticaespectronumerosnaturales.pdf

they are of the same degree. In decimal terms, we use the words: units, tens, hundreds, and so on, to classify these orders. To add them, we add the coefficients, in the following way:

$$n + m = ax^n + \ bx^n = (a+b)x^n.$$

If $a + b = 10 + k$, with $0 \leq k \leq 9$, we replace above and get $n + m = ax^n + \ bx^n = (a+b)x^n = (10+k)x^n = 10x^n + kx^n = x^{n+1} + kx^n$.

Example: Let m = 700 and n = 600.

Here a = 7, b = 6 and n + m can be written:

$n + m = 700 + 600 = 7 \times 100 + 6 \times 100 = 7 \times 10^2 + \ 6 \times 10^2 = (7+6)10^2 = 13 \times 10^2 = (10+3) \times 10^2 = 10 \times 10^2 + 3 \times 10^2 = 10^3 + 3 \times 10^2 = 1000 + 300 = 1300.$

We can get the addition of decimal polynomials throught their vector representation, as in the following example.

Example: The addition of the numbers 379 and 285 can be represented as the sum of the vectors (3 , 7 , 9) and (2 , 8 , 5). After reduction modulo ten, we get:

$$(3 , 7 , 9) + (2 , 8 , 5) = (3+2 , 7+8 , 9+5) = (5 , 15 , 14) = (5 , 15 + 1 , 4) = (5 , 16 , 4) = (5 + 1 , 6 , 4) = (6 , 6 , 4).$$

This proccess says that 379+285 = 664. The advantage of this procedure is that the carries are reduced easily at the last step. You can extent the vector if the former entry is greater or equal to 10.

Example 2. *Multiplication of a number by a polynomial*. If we assume that $P(x)$ is a polynomial and r a real number, then $rP(x)$ is the polynomial that results from multiplying each coefficient of P by the constant r. Suppose that r = 5 and $P(x) = 7x^3 + 5x^2 + 4x + 9$, then

$$r \times P(x) = 5 \times (7x^3 + 5x^2 + 4x + 9) = 35x^3 + 25x^2 + 20x + 45.$$

In the last equality, we have applied distributive law, introducting the factor inside the polynomial. When we go backwards, we say, we are taking the common factor 5 out of the polynomial. The last polynomial can be reduced module 10, i. e. transforming each coeficient as a new polynomial, $35 = 3x + 5$, $25 = 2x + 5$, $20 = 2x$, $45 = 4x + 5$. So we find

$35x^3 + 25x^2 + 20x + 45 = (3x + 5)\ x^3 + (2x + 5)\ x^2 + (2x)x + (4x + 5) = 3\,x^4 + 5\,x^3 + 2\,x^3 + 5\,x^2 + 2\,x^2 + 4x + 5 = 3\,x^4 + 7\,x^3 + 7\,x^2 + 4x + 5.$

Therefore, $rP(x)=5(7x^3+5x^2+4x+9)=3x^4+7x^3+7x^2+4x+5$, can be seen as the product of 5 times 7549 and the last polynomial is exactly 37745, the result of this multiplication.

We can also use vector symbolism to represent the above product as: $rP(x)$ = 5·(7,5,4,9) = (5×7, 5×5, 5×4, 5×9) = (35, 25, 20, 45). After reduction module 10 this vector can be associated to the vector (3,7,7,4,5). The operation "·" is called product by scalar and, "×", it is as before, to represent the usual natural number product. Note that the carries in the reduction module 10 can be added to the next entry from right to left in the vector to get the final result of the product $rP(x)$. In symbols:

5×7549 = 5·(7,5,4,9) = (3,7,7,4,5) = 37745.

As you can see the last "vector" has a different length than the first one. This is because we are not exactly in a vector space but just using the similarity around some properties.

So far, we have introduced three different products: 1) "×", the usual product for natural numbers; 2) the inner product "•" for vectors; and 3) "·" the multiplication by scalar, of a natural number by a vector.

In what order have we teach these three different products in elementary school?

It seems to me, the convinient order could be: "•","·", "×", leaving of course, the most dificult at the last.

Inner product "•", help us to give the right value to the digits at the numeral. For instance the number whose decimal representacion is 111, really means: $(1 , 1 , 1) \bullet (x^2 , x , 1) = x^2 + x + 1 = 10^2 + 10 +1 = 100 + 10 + 1$, in words: the first one has a value of one hundred, the second one means ten and third one has the value of one unity. The usual natural product "×", is essentially the same as the product of two polynomials (when x is taken as 10).

The appearience of x along these lines is not just to show an algebraic symbolism but also to suggest that in mathematics we can make abstractions representing through letters, not only numbers but concepts like order and value.

Example 3. *Multiplication of two polynomials.* The way to do it, is, multiplying each monomial from the first polynomial by each monomial of the second one. A simple case was made in example 2 above. To ilustrate, let us multiply 235 by 246. Translating to polynomials the multiplication could be seen as:

$(2x^2+3x+5)\times(2x^2+4x+6)=2x^2(2x^2+4x+6)+3x(2x^2+4x+6)+5(2x^2+4x+6)$ = $(2x^2)(2x^2)$ + $(2x^2)(4x)$ + $(2x^2)(6)$ + $3x(2x^2)$ + $3x(4x)$ + $3x(6)$ +$5(2x^2)$ +$5(4x)$ + $(5)(6)$ = $4x^4$ + $8x^3$ + $12x^2$ + $6x^3$ + $12x^2$ + $18x$ + $10x^2$ +$20x$ +30 = $4x^4$ +$14x^3$ +$34x^2$ + $38x$ + 30.

Reducing module ten, i.e, changing the numbers greater than ten, to polynomials, we find:

$4x^4 + 14x^3 + 34x^2 + 38x + 30 = 4x^4 + (x + 4)x^3 + (3x + 4)x^2 + (3x + 8)x + 3x = 4x^4 + x^4 + 4x^3 + 3x^3 + 4x^2 + 3x^2 + 8x + 3x = 5x^4 + 7x^3 + 7x^2 + 11x = 5x^4 + 7x^3 + 7x^2 + (10 + 1)x = 5x^4 + 7x^3 + 7x^2 + x^2 + x = 5x^4 + 7x^3 + 8x^2 + x$.

Last process can be simplified using inner product notation and adding the carries in the first vector, namely:

$4x^4 + 14x^3 + 34x^2 + 38x + 30 = (4, 14, 34, 38, 30) \bullet (x^4, x^3, x^2, x, 1) = (5, 7, 8, 1, 0) \bullet (x^4, x^3, x^2, x, 1) = 5x^4 + 7x^3 + 8x^2 + x$.

This polynomial represent the number 57810. This apparently long proccess is the logic explanation of the algorithm behind the multiplication: 235×246 = 57810.

One of the advantages of using polynomials, is the possibility to present algorithms straigh ahead tipographycally, in the sense that you begin the proccess with an input (the factors) and following a sequence of equalities, you finish with an output (the product of the two factors).

Now if we use a combination of vectorial and polynomial notation, the saving of space and time is considerable. Lets redo the above multiplication:

$235 \times 246 = 2x^2(2 , 4 , 6) + 3x(2 , 4 , 6) + 5(2 , 4 , 6) = (4x^2 , 8x^2 , 12x^2) + (6x , 12x , 18x) + (10 , 20 , 30) = (4x^2 + 6x + 10 , 8x^2 + 12x + 20 , 12x^2 + 18x + 30) = (470 , 940 , 1410) = (578, 1, 0) = (5 , 7 , 8 , 1 , 0) = 57810$.

And more yet, remembering that $x = 10$:

$235 \times 246 = (400 , 800 , 1200) + (60 , 120 , 180) + (10 , 20 , 30) = (400 + 60 + 10 , 800 + 120 + 20 , 1200 + 180 + 30) = (470 , 940 , 1410) = (470 , 940 + 141 , 0) = (470 , 1081 , 0) = (470 + 108 , 1 , 0) = (578 , 1 , 0) = 57810$.

Example 4. **Multiplication of two digits numbers**.

When we have numbers $(ax + b)$ and $(cx + d)$, represented in base 10, its product will be:

$(ax + b).(cx + d) = (ax).(cx + d) + (b).(cx + d) = (ax).(cx) + (ax).(d) + (b).(cx) + (b).(d) = (ac)x^2 + (ad + bc)x + bd = mx^2 + nx + l$.

The polynomial $(ac)x^2 + (ad + bc)x + bd$, has to be reduced module ten. Namely, we take coefficients, m, n, l, after reduction from right to left [from(bd) to (ac)], in such a way that l is obtained as $ac - 10k$, where k is is the maximum integer such that this difference is not negative; n also is found after reduction in the same way as before as the sum $(ad + bc)$ and the carry from ac; and finally m is found after reduction the sum ac and the carry from the previous step.

After reduction we get an expression with cuadratic form: $mx^2 + nx + l$.

The multiplication process then, take the pair, [($ax + b$), ($cx + d$)], into the cuadratic polynomial $mx^2 + nx + l$, where m could be greater or equal to 10. After reducting modulo ten we get a decimal polynomial of third degree.

Now, a question:

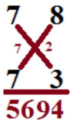
Is there some procedure that can reverse the above process?, namely, if we have the number $mx^2 + nx + l$, can we recapture its factors ($ax + b$) and ($cx + d$)?

The answer is yes; whenever, $mx^2 + nx + l$ be composite (or not prime number).

Example 5. Consider in the previous example ($ax + b$) = 78 and ($cx + d$) = 73. In this case a = 7, b = 8; c = 7, and d = 3. The multiplication takes the form:

$(7x + 8)\times(7x + 3) = (7\times7)\,x^2 + (7\times3 + 8\times7)x + (8\times3) = 49\,x^2 + (21 + 56)\,x + 24 = 49x^2 + 77x + 24 = (4\,x + 9)\,x^2 + (7x + 7)x + (2x + 4) = 4x^3 + 9x^2 + 7x^2 + 7x + 2x + 4 = 4x^3 + 16x^2 + 9x + 4 = 4x^3 + (10 + 6)x^2 + 9x + 4 = 4x^3 + (x + 6)x^2 + 9x + 4 = 4x^3 + x^3 + 6x^2 + 9x + 4 = 5x^3 + 6x^2 + 9x + 4 =$ 5694.

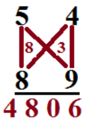
We remark two interesting facts in the preceding procedure. 1) multiplication is made sequencially step by step, where we are explaining the origin of each result. 2) with some practice many steps can be omitted in order to reduce the procedure to a short schema derived from the colored parts above:



Here, first, we find the last 4 (under the bar), from the product 8×3 = 24 leaving a carry of 2 (at right in the middle); second, adding the cross products to the carry, we get 7×3 + 7×8 + 2 = 79, writing 9 under the bar and leaving a carry of 7(at left in the middle); finally, we add this carry to the product 7×7 to find 56, and write it under the bar.

Example 6. Take now ($ax + b$) = 54, and ($cx + d$) = 89. Here a = 5, b = 4 and c = 8 and d = 9. The product is found, reducing some steps:

$(5x + 4)\times(8x + 9) = 40x^2 + 45x + 32x + 36 = 40x^2 + 77x + 36 = 4x^3 + 7x^2 + 7x + 3x + 6 = 4x^3 + 7x^2 + 10x + 6 = 4x^3 + 7x^2 + x^2 + 6 = 4x^3 + 8x^2 + 0x + 6 = 4806$. Following simplification as in example 5, with carries inside the cross section, we get:



Schemas as in the above examples show how to find, rapidly, products of two digit numbers. However it is not our interest to compete with calculators, instead we try to explain rationally, where the algorithm for multiplication comes from. Similar schemas can be found for more than two digits numbers, although no so simple as that shown above.

The Inverse Proccess. Multiplication is a function from $\mathbb{N}\times\mathbb{N}$ in $\mathbb{N}$, such that, the pair (u,v) from $\mathbb{N}\times\mathbb{N}$ is asociated uniquely to the number $u.v$ in $\mathbb{N}$,where $u.v$ is another way to write the product of u and v. Numbers u and v are called the factors and $u.v$ will be the product. For instance, take the pair (5, 6), multiplication takes this pair to the number 30, a number again in $\mathbb{N}$. We´ll say that multiplication is a closed operation in $\mathbb{N}$. In Example 4, we ask for a procedure to find factors $(ax + b)$ and $(cx + d)$ if we know their product $mx^2 + nx + l$. As a matter of fact, given a number associated to a decimal polynomial of that form, and not a prime, we can find its factors. The problem can be seen as factoring a quadratic polynomial, a topic in a high school algebra course. In a general setting, factoring integer numbers is a difficult task; to get a fast algorithm for factoring integers is practically impossible. This is why the RSA[6] algorithm, used in coding theory, is considered safe.

We learn at elementary school an empirical method of finding the prime factors of an integer n. The proccess is based in succesive divisions by primes $\leq \sqrt{n}$. Here we introduce a method to find the factors of n without using any division but factoring a polynomial associated to n. Before showing examples how todo it, its good idea to learn some general rules to simplify the process of checking primality of an integer. This rules derive from theorems in elementary number theory, comprenhensible to young people, which are presented below.

Theorem 1. Any integer multiple of two, has its last digit either 0 or an even cipher (2, 4, 6, 8). Conversely, any integer ended in 0, 2, 4, 6, 8, has at least a 2 as a factor.

Proof. A number, say, m has 2, as a factor, when $m = 2\times P(x) = 2\times(a_n\, x^n + a_{n-1}x^{n-1} + \ldots + a_0) = 2\times a_n\, x^n + 2\times a_{n-1}x^{n-1} + \ldots + 2\times a_0$. Since a_0 is a digit in $\{0, 1, 2, \ldots, 9\}$, then $2\times a_0$, takes values in $\{0, 2, 4, 6, 8, 0\}$. This proves the first part.

Now suppose the number m has in its last cipher an even number, say a_0 will be one of the numbers: 0, 2, 4, 6, 8. If $a_0 = 0$, then m can be written as: $m = a_n\, x^n + a_{n-1}x^{n-1} + \ldots + a_1x + 0 = x^n + a_{n-1}x^{n-1} + \ldots + x = x(a_nx^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1) = 10(a_nx^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1) = 2\times5(a_nx^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1) = 2\times(5(a_nx^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1))$. This means that m has 2 as a factor. When a_0 is 2, 4, 6 or 8, the proof is similar, remembering that $x = 10 = 2\times5$.

Theorem 2. A number $m = \sum_{j=0}^{j=n} a_{n-j}x^{n-j}$ has 3 as a factor if

[6] The RSA algorithm is the most commonly used for providing privacy and ensuring authenticity of digital data.

$$\sum_{j=0}^{j=n} a_{n-j} = 3k \text{, where } k \text{ is positive integer.}$$

Usually this theorem is mentioned in terms of divisibility as: *m* is divisible by 3 if the sum of its digits is a multiple of 3.

Proof. Since

$\sum_{j=0}^{j=n} a_{n-j} = 3k$, we have $a_0 + a_1 + \ldots + a_n = 3k$, and consequently, $a_0 = 3k - (a_1 + \ldots + a_n)$.

Then

$$m = \sum_{j=0}^{j=n} a_{n-j}x^{n-j} = \sum_{j=1}^{j=n} a_{n-j}x^{n-j} + a_0 = \sum_{j=1}^{j=n} a_{n-j}x^{n-j} + (3k - (a_1 + \ldots + a_n)) =$$

$$\sum_{j=1}^{j=n} a_{n-j}x^{n-j} + 3k - a_1 - \ldots - a_n) = a_nx^n - a_n + \ldots + a_1x - a_1 + 3k =$$

$$(10^n - 1)a_n + \ldots + (10 - 1)a_1 + 3k = 9 \,..^{n\text{- times}}.\, 9a_n + \ldots + 9a_1 + 3k =$$

$$3(3..^{n\text{-times}}.3a_n + \ldots + 3a_1 + k) = 3l.$$

Where *l* is the number inside the parenthesis. This shows that 3 is a factor of *m*.

Similarly we can show that an integer number has a factor like 5 if this number ends in either 0 or 5. To check if 7 is a factor of *m* we try to arrange the polynomial representation of *m*, looking for 7´s in this representation. See the following example.

Example 7. Look for the prime factors of *m* = 1547.

$m = 1547 = 1x^3 + 5x^2 + 4x + 7 = 15x^2 + 4x + 7 = 14x^2 + x^2 + 4x + 7 = 14x^2 + 10x + 4x + 7 = 14x^2 + 14x + 7 = 7(2x^2 + 2x + 1) = 7(x^2 + 12x + 1) = 7(x^2 + 10x + 2x + 1) = 7(x^2 + 10x + 21) = 7[(x^2 + 3x) + (7x + 21)] = 7[x(x + 3) + 7(x + 3)] = = 7(x+3)(x + 7) = 7\times13\times17$.

Observe the above proccess. We start with 1547 as an input, after a finite number of steps we arrive to an output, the numbers 7, 13, 17, the prime factors of 1547. This proccess is an example of a proof with an algorithm inside it. We could also make a computer program for this proof. This suggest that we can teach our elementary school students the first steps in coding early in the elementary school.

Example 8. When numbers are small, factoring could be easy. However we can factor numbers considerably large like those shown at the final of this paper. The number 144 is a Fibonacci number, the square of twelve and also its factoring takes a pair of lines.

$144 = x^2 + 4x + 4 = (x^2 + 2x) + (2x + 4) = x(x + 2) + 2(x + 2) = (x + 2)(x + 2) = (x + 2)^2 = 12^2 = (4\times3)^2 = (4)^2(3)^2 = (2^2)^2 3^2 = 2^4 3^2$.

So the prime factors of 144 are 2 and 3. By the way, 144 and 8 are the only integer powers which are also Fibonacci numbers. Fibonacci numbers are those integers in the sequence 1, 1, 2, 3, 5 ,8, 13, 21, 34, 55, …, where the integer in the $n + 1 - th$ place is the sum of its two predecessors, $n - th$ and $(n - 1) - th$.

Example 9. Find the prime factors of **1849**.

1849 $= x^3 + 8x^2 + 4x + 9 = 10x^2 + 8x^2 + 4x + 9 = 18x^2 + 4x + 9 = 16x^2 + 24x + 9 = (4\times4)x^2 + 24x + (3\times3) = (4x)^2 + 12x + 12x + (3)^2 = 4x(4x + 3) + 3(4x + 3) = (4x + 3)(4x + 3) = 43\times43 = 43^2$.

The number 43 is a prime and the only prime factor of 1849 is 43. As highlighted (in red) above we see the square of $4x$, the square of 3 and two times $(4x)(3)$. Then 1849 is a perfect square, and also its associated trinomial: $16x^2 + 24x + 9$ is. No all integers factor so easyly as 1849. The following examples take more time.

Example 10. Check if **1157** is prime or composite.

1157 $= x^3 + x^2 + 5x + 7 = 10x^2 + x^2 + 5x + 7 = 11x^2 + 5x + 7 = 10x^2 + 15x + 7 = 9x^2 + 25x + 7 = 9x^2 + 23x + 27 = 8x^2 + 33x + 3\times9 = 8x^2 + 24x + 9x + 3\times9 = 8x(x + 3) + 9(x + 3) = (x + 3)(8x + 9) = 13\times89$.

As you can see we don't need so far, any division to find that **1157** is a composite (not prime) integer.

Example 11. Let us try now with **5183.**

5183 $= 5x^3 + x^2 + 8x + 3 = 51x^2 + 8x + 3 = 50x^2 + 18x + 3 = 49x^2 + 28x + 3 = (7\times7)\, x^2 + 28x + 3 = (7\times7)\, x^2 + (7\times3)\, x + 7x + 3 = 7x(7x + 3) + (7x + 3) = (7x + 1)(7x + 3) = 71\times73$.

We have here simplified a little bit the steps and reductions. The key step above, is to get the decomposition of $28x$ as the sum of $21x + 7x$ in order to have the factoring of first and third terms in the quadratic trinomial.

Checking primality of **5183** using the normal procedure takes at least 17 trials to conclude that **5183** is composite. The pair 71 and 73 is an example of twin primes: sucesive primes of the form (p , p + 2), with p a prime. Other examples are: (3, 5); (11,13); (17, 19); (29,31); (41,43); …,etc.

Example 12. Numbers obtained from the formula $\mathbf{M}_p = 2^p - 1$, when $p = 2, 3, \ldots$, are called Mersenne numbers. The first Mersenne prime numbers, with p prime are 3, 7, 31 and 127. However $\mathbf{M}_{11} = 2^{11} - 1 = 2047$ is composite as you can see it in its decimal decomposition.

2047 $= 2x^3 + 4x + 7 = 20x^2 + 4x + 7 = 18x^2 + 24x + 7 = 16x^2 + 44x + 7 = 16x^2 + 42x + 27 = (2\times 8)x^2 + 42x + (3\times 9) = 16x^2 + (2\times 9 + 8\times 3)x + 27 = 16x^2 + 24x + 18x + 27 = 8x(2x + 3) + 9(2x + 3) = (2x + 3)(8x + 9) = 23\times 89$. So 2047 is composite with prime factors, 23 and 89.

Mersenne numbers are important nowadays because they are associated to the largest known primes such as $\mathbf{M}_{57,885,161} = 2^{57.885.161} - 1$, considered as of May 2014 the largest prime in history.

Example 13. The number **98363** is a very published number as you can find it in the web. It is composite with three factors. The procedure to factorize it, consists in trying to find theirs factors through the trial and error method, looking for prime factors; first with the small primes 2, 3, 5, 7, 11, 13 and 17; then make the try with 19. The case for 2, 3, 5 is simple using the theorems above. When we express this number as a polynomial we can verify that 7 is not a factor. After 11, the method is the same as with 19, which we do it in the following lines[7].

We take the first two monomials and look for the factor 19 = x + 9 inside them. We repeat the process for the following two monomials plus the first residue, till we finish all the monomials as it is shown below. Here, the highlight has its explanation at the end of the paragraph.

98363 $= 9x^4 + 8x^3 + 3x^2 + 6x + 3 = 5x^3(x + 9) + 3x^3 + 3x^2 + 6x + 3 = 5x^3(x + 9) + x^2(x + 9) + 14x^2 + 6x + 3 = 5x^3(x + 9) + x^2(x + 9) + 7x(x +9) + 13x + 3 = 5x^3(x + 9) + x^2(x + 9) + 7x(x +9) + 7(x + 9) = (x + 9)(5x^3 + x^2 + 7x + 7) = 19\times$**5177**.

$9x^4 + 8x^3 = 5x^4 + 48x^3 = 5x^4 + 45x^3 + 3x^3 = 5x^3(x + 9) + 3x^3$, which we reeplace above

$3x^3 + 3x^2 = x^3 +23x^2 = x^3 +9x^2 + 14x^2 = x^2(x + 9) + 14x^2$. We again replace above.

$14x^2 + 6x = 7x^2 + 76x = 7x(x +9) + 13x$. Replace above and proceed finally with:

$13x + 3 = 7x + 63 = 7(x + 9)$. All terms will have the common factor (x + 9).

We have now to find the factors, if any, of **5177.**

[7] This same factoring was made using binary system in: http://www.matematicasyfilosofiaenelaula.info/conferencias/aritmeticaespectronumerosnaturales.pdf

5177 = $5x^3 + x^2 + 7x + 7 = 51x^2 + 7x + 7 = 50x^2 + 17x + 7 = 49x^2 + 27x + 7 = 48x^2 + 37x + 7 = (3\times16)x^2 + 37x + 7 = (3\times16)x^2 + 16x + 21x + 7 = 16x(3x + 1) + 7(3x + 1) = (3x + 1)(16x + 7) = 31\times167$. Since 167 is prime,the number 98363 factors as:

98363 = 19×**5177 =** 19×31×167.

The above example suggests how to find the factor $(x + 9)$ of a given integer m, and also how to get a proccess which makes division posible, as in the case when we find above that: $9x^4 + 8x^3 = 5x^4 + 48x^3 = 5x^4 + 45x^3 + 3x^3 = 5x^3(x + 9) + 3x^3$, which means that, if we divide $9x^4 + 8$ by $(x + 9)$ we get a quotient of $5x^3$ and a residue of $3x^3$. When we arrive, after a finite number of repetitions of this procedure, to a residue of zero, we say that the number m is divisible by $(x + 9)$, namely by 19.

A couple of examples to practice this procedure are the following, where we want to factorize the odd number below the 10000th prime number and a number in between the two twin primes, 104549 and 104551.

Example 14. By checking with first primes 3, 7, 11, …, try to factorize 104727, the odd number previous to the 10000th prime. Note that the sum of its digits is a multiple of 3, so we can express it in the form $3k$.

104727 = $x^5 + 4x^3 + 7x^2 + 2x + 7 = 10x^4 + 4x^3 + 7x^2 + 2x + 7 = 9x^4 + 12x^3 + 27x^2 + 27 = 3(3x^4 + 4x^3 + 9x^2 + 9)$. Now we check with 7 the number 34909.

$3x^4 + 4x^3 + 9x^2 + 9 = 28x^3 + 6x^3 + 9x^2 + 9 = 28x^3 + 69x^2 + 9 = 28x^3 + 63x^2 + 60x + 9 = 28x^3 + 63x^2 + 56x + 49 = 7(4x^3 + 9x^2 + 8x + 7) = 7\times4987$. Therefore, knowing that 4987 is prime, we conclude that:

104727 = $3(3x^4 + 4x^3 + 9x^2 + 9) = 3\times7\times4987$.

Example 15. Using the same procedure as before, factorize 104550.

104550 = $x^5 + 4x^3 + 5x^2 + 5x = 10x^4 + 4x^3 + 5x^2 + 5x = 10x^4 + 4x^3 + 5x^2 + 5x = 9x^4 + 12x^3 + 24x^2 + 15x = 3x(3x^3 + 4x^2 + 8x + 5) = 30\times3485 = 2\times3\times5\times3485$.

3485 = $3x^3 + 4x^2 + 8x + 5 = 34x^2 + 8x + 5 = 30x^2 + 45x + 35 = 5(6x^2 + 9x + 7) = 5\times697$.

697 = $6x^2 + 9x + 7 = 5x^2 + 19x + 7 = 4x^2 + 29x + 7 = 4x^2 + 28x + x + 7 = 4x(x + 7) + (x + 7) = (x +7)(4x + 1) = 17\times41$. Replacing above, we get,

104550 = $2\times3\times5\times3485 = 2\times3\times5\times5\times697 = 2\times3\times5\times5\times17\times41 = 2\times3\times5^2\times17\times41$.

Numbers like 104550, which are in between twin primes, are factors of 2 and 3 (in the particular case of 104550, also of 5), because they are even and 104499, 104550, 104551 are three consecutive integers the first and the third are not factors of 3, then, the middle one has to be a multiple of 3. If we were able to show that there are infinite numbers of this type we may show that there are infinite twin primes, a long lasting conjecture.

In general it is not an easy job to find the prime factors of an integer number. However throught these examples we have shown how to get them by trial and error, using polynomial factoring.

A good practice to get acquainted with this technique, is to go through a table of primes and factoring numbers which are not in the table. For instance, 2869 is a composite number not in the table, in between the 416th y the 417th primes. In the same way, as in example 12, we try with 3, 7, …, 17 and we discover that 19 is a factor. Another prime factor will be 151.

First amended version: Armenia, Colombia, July 2014.