How to Express Counting Numbers as a Product of Primes
Beginning Abstract Algebra at Elementary School
Diego Pareja-Heredia. ***Universidad del Quindío***

"The problem of distinguishing prime numbers from composite numbers, and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic". **C. F. Gauss.** *Disquisitiones Arithmeticae.*

Abstract

In this paper we explain the way how, we can obtain the prime decomposition of a natural number as a product of primes without using division at all.

Introduction. Expressing a natural number as a product of prime numbers, using only factoring and not division at all, is not usually taught at elementary schools. To my knowledge, classical mathematicians like Fermat, Gauss and Euler, among others, did not mention the process that I´ll explain here. Fermat mentions that he does not know other way to check primality, except dividing a number successively by the primes less or equal to its square root.

Throught centuries mathematicians have considered the process of reversing multiplication a very dificult task, and it really is. More precisely, if you have numbers a and b, you get easily the product $c = ab$. A quite different problem is to reverse the process to recover a and b, when you know c. This reverse proccess is called *factoring*.

In the same way as a real number can be defined as an equivalence class of Cauchy sequences of rational numbers, each natural number can be also defined as an equivalence class of some special polynomials. In my article Syntax and Semantics of Numerical Language[1] I used polynomials to express natural numbers, in such a way that, a number can be associated to a family of polynomials. When one of them is factored, we eventually get the prime representation of the number represented by the family. When none of them can be factored the number associated to the family will be prime.

Polynomials are algebraic entities very easy to handle. They are made of sums and multiplications. In this paper we work only with natural or counting numbers: 0, 1, 2, 3,…, and the letter x is just the symbol representing the number ten, namely, the base for our number system. Polynomials are algebraic expressions of the type

[11] See: **Pareja-Heredia, D.** *Sintax and Semantics of Numerical Lenguage at Elementary School* at: http://matematicasyfilosofiaenelaula.info/articulos.htm

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

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 digital polynomial. To each natural number we can associate a polynomial of the (*) type. However if we use the syntactic rule,

$$x^n = 10x^{n-1} , \qquad (**)$$

we can find more polynomials associated to a given number. More precisely, to every natural number is associated an equivalence class, which defines such a natural number n. If we find in a specific family a *factorable polynomial*, we will say that n is a composite or not prime number. Otherwise n will be a prime number.

The basis to understand all the theory behind factoring using this approach is the use of polynomial arithmetic related with addition and multiplication.

Example 1
If n = 713, the unique digital polynomial associated to it, is

$$P(x) = 7x^2 + x + 3$$

However, using the syntactic rule (**) above, we can also find the complete family

$\{7x^2 + x + 3$, $6x^2 + 11x + 3$, $5x^2 + 21x + 3$, $4x^2 + 31x + 3$, $3x^2 + 41x + 3$, $2x^2 + 51x + 3$, $x^2 + 61x + 3$, …, $6x^2 + 10x + 13$, …, $713\}$.

In all polynomial representations in this family, the number 713 remains as an invariant. When we add orderly the digit that precedes the last one in each summand, except the leader coefficient, we arrive to the unique digital polynomial associated to 713. For instance in the polynomial, $2x^2 + 51x + 3$, we add 2 + 5, to get $P(x) = 7x^2 + x + 3$, the digital polynomial associated to 713. Also in $6x^2 + 10x + 13$, we add 10 + 1 = 11 to get $6x^2 + 11x + 3$ and from here adding, 6 + 1 = 7, we get again, $P(x) = 7x^2 + x + 3$. Note that 713 is also a polynomial in the set. When we take x = 10, in each member of the family we arrive invariably to the numerical value 713.

The second polynomial above, can be factored as: $6x^2 + 11x + 3 = 6x^2 + 9x + 2x + 3 = 3x(2x + 3) + (2x + 3) = (2x + 3)(3x + 1) = 23 \cdot 31$. In this way we have naturally found the prime representation of 713.

As we can see, (*) is made of sums and products (multiplications of integers when the coefficients and the variable x take integer values) and $a_n x^n$ is a simplified form of writing

$a_n \cdot x \cdot \ldots \cdot x$, where x appears n times as a factor. With this in mind we can define natural numbers in a semantic manner as the common property for each the following families.

$0 = \{P(x)$, when all coefficients in (*) are zero$\}$.

$1 = \{P(x)$, when all coefficients in (*) are zero, except $a_0 = 1\}$. We define 2, …, 9 in the same way.

$10 = \{x, 10\}$, $11 = \{x + 1, 11\}$, … , $99 = \{9x + 9, 8x + 19, \ldots, 99\}$

$100 = \{x^2, 10x, 9x + 10, \ldots, 100\}$, $101 = \{x^2 + 1, 10x + 1, 9x + 11\ldots, 101\}$, … ,

$147 = \{x^2 + 4x + 7, x^2 + 3x + 17, \ldots, 147\}$, … ,

$999 = \{9x^2 + 9x + 9, 8x^2 + 19x + 9, 8x^2 + 18x + 19, \ldots, 999\}$

$1000 = \{x^3, 9x^2 + 10x, \ldots, 1000\}$, etc.

To create the elements in each equivalence class, we have made use of the syntactic property (**).

For instance 2845would be associated to the family

$\{2x^3 + 8x^2 + 4x + 5,\ x^3 + 18x^2 + 4x + 5,\ 28x^2 + 4x + 5,\ x^3 + 10x^2 + 8x^2 + 4x + 5,\ x^3 + 18x^2 + 4x + 5, \ldots, 2845\}$.

If we want to know the prime factors of this number, we look for a member of the family that let us find its factors. We use in this case the symbol "≡" to emphasize that we are in a class of equivalence.

$2845 \equiv 2x^3 + 8x^2 + 4x + 5 \equiv 20x^2 + 8x^2 + 4x + 5 \equiv 28x^2 + 4x + 5 \equiv 25x^2 + 30x + 4x + 5 \equiv 25x^2 + 30x + 4x + 5 \equiv 25x^2 + 30x + 45 = 5(5x^2 + 6x + 9) = 5 \cdot 569$. Since the latter numbers are both primes we have found the prime representation of 2845. We can also show that 569 is prime checking that in its polynomial family there is not a factorable polynomial. In fact:

$569 = \{5x^2 + 6x + 9, 4x^2 + 16x + 9, 3x^2 + 26x + 9, 2x^2 + 36x + 9, 3x^2 + 22x + 49, 2x^2 + 32x + 49, \ldots\}$.

None of those polynomials are factorable and so 569 is a prime.

Addition and multiplication are closed operations in the set of natural numbers, namely, the sum and the product of two natural numbers are again natural numbers. 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 at the beginning of the elementary school the sets o integers and rational numbers, where substraction and division are closed operations. 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.

The Fundamental theorem of Arithmetic. Since the time of Euclid or probably since babylonian times, we know that any natural number is either prime, or it can be represented by a product of primes in an unique way up to the order of the prime factors. Prime numbers are building blocks from which, each integer can be build up by multiplication. Primes play a role similar to LEGO parts in building a house or another LEGO construction.

The procedure that we will explain here, takes a natural number and after a finite number of steps we find its prime factors. The interesting fact is, that this method goes through a chain of logical steps represented by equivalent polynomials, until one gets at the end, the prime representation of the starting number. From here on we use the symbol '=' instead of the appropiate one '≡' inside the equivalence classes of polynomials.

Example 2
Find the prime factors of 5183.

Solution. To begin with, we write the digital polynomial associated to 5183, namely,

$$P(x) = 5x^3 + x^2 + 8x + 3$$

This polynomial is at the same class as the following polynomials

$$50x^2 + x^2 + 8x + 3 = 51x^2 + 8x + 3 = 50x^2 + 18x + 3 = 49x^2 + 28x + 3,$$

The last polynomial can be factored as the product of two linear polynomials using simple transformations as you can see through the following equalities

$$5183 = 5x^3 + x^2 + 8x + 3 = 51x^2 + 8x + 3 = 50x^2 + 18x + 3 = 49x^2 + 28x + 3 = 49x^2 + 21x + 7x + 3 = 7x(7x + 1) + 3(7x + 1) = (7x + 1)(7x + 3) = 71 \cdot 73.$$

Both 71 and 73 are primes, so the prime representation of 5183 is 71·73. To find the prime representation of 5183, using the traditional method of succesive divisions, we have to check with 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67 and finally with 71,.

Primes like 71 and 73 are called twin primes and they have the form p, $p + 2$, where both of them are primes. We can find many pairs of twin primes but nobody knows if this set is finite or infinity.

Example 3

Find the prime factors of 2623.

Solution. Let us start with 2623 and through equalities we'll arrive to its prime representation.

$2623 = 26x^2 + 2x + 3 = 25x^2 + 12x + 3 = 24x^2 + 22x + 3 = 24x^2 + 18x + 4x + 3 = 6x(4x + 3) + (4x + 3) = (4x + 3)(6x + 1) = 43 \cdot 61$.

Since 43 and 61 are both primes, this is the prime representation for 2623.

Example 4
Find the prime factors of 2310.

Solution. The <u>first step</u> in our procedure is to find inside number 2310 all prime digital factors, such as 2, 3, 5 and 7. Systematically we put these prime factors out the digital polynomial

$$P(x) = 2x^3 + 3x^2 + x .$$

Since $x = 10 = 2 \cdot 5$, we find

$2310 = 2x^3 + 3x^2 + x = x(2x^2 + 3x + 1) = 2 \cdot 5(2x^2 + 3x + 1) = 2 \cdot 5(23x + 1) = 2 \cdot 5(21x + 2x + 1) = 2 \cdot 5(21x + 21) = 2 \cdot 5 \cdot 21(x + 1) = 2 \cdot 5 \cdot 3 \cdot 7(x + 1) = 2 \cdot 3 \cdot 5 \cdot 7(x + 1) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$.

It follows that the prime representation of 2310 is $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. Number 2310 is a very special number: it is between two consecutive prime numbers, 2309 and 2311 and it is also the product of the first five prime numbers. I call this type of numbers: *trust numbers of first class.* It is an open question whether this type of numbers are or not finite.

Example 5
Not all cases are so simple as those seen before. Finding prime factors for 2831 takes more time.

$2831 = 2x^3 + 8x^2 + 3x + 1 = 28x^2 + 3x + 1 = 27x^2 + 13x + 1 = 26x^2 + 23x + 1 = 25x^2 + 33x + 1 = 24x^2 + 41x + 7 \cdot 3 = 22x^2 + 61x + 7 \cdot 3 = 21x^2 + 71x + 7 \cdot 3 = 20x^2 + 81x + 7 \cdot 3 = 19x^2 + 91x + 7 \cdot 3 = 18x^2 + 101x + 7 \cdot 3 = 17x^2 + 111x + 7 \cdot 3 = 16x^2 + 121x + 7 \cdot 3 = 15x^2 + 125x + 9 \cdot 9 = 14x^2 + 135x + 9 \cdot 9 = 14x^2 + 126x + 9x + 9 \cdot 9 = 14x(x + 9) + 9(x + 9) = (x + 9)(14x + 9) = 19 \cdot 149$.

Since both, 19 and 149 are prime numbers we conclude that $19 \cdot 149$ is the prime reprentation of 2831. This example shows how far we have to go with the process: from 28 to 14 in the coefficient of x^2.

Example 6
Find the greatest common submultiple of 1131 and 2509.

Submultiples of a natural number n are factors k and l greater than 1 that satisfy the condition $k \cdot l = n$.

The greatest common submultiple of a pair of numbers m and n is the greatest of all common factors of m and n.

Solution

To begin with, let us find the prime representation of 1131 and 2509.

$1131 = x^3 + x^2 + 3x + 1 = 11x^2 + 3x + 1 = 3(3x^2 + 7x + 7) = 3(2x^2 + 17x + 7) = 3(2x^2 + 15x + 27) = 3(2x^2 + 6x + 9x + 3\cdot 9) = 3[2x(x + 3) + 9(x + 3)] = 3(x + 3)(2x + 9) = 3\cdot 13\cdot 29$

$2509 = 2x^3 + 5x^2 + 9 = 25x^2 + 9 = 24x^2 + 10x + 9 = 23x^2 + 20x + 9 = 22x^2 + 30x + 9 = 21x^2 + 40x + 9 = 20x^2 + 50x + 9 = 19x^2 + 60x + 9 = 19x^2 + 57x + 3x + 9 = 19x(x + 3) + 3(x + 3) = (x + 3)(19x + 3) = (x + 3)(x^2 + 9x + 3) = 13\cdot 193$. (13 and 193 are prime numbers).

The only common submultiple of 1131 and 2509 is 13 and so, it is also, the maximun.

The Basic Rules of finding the Prime Factors of a Natural Number

As mentioned above, the process of reversing multiplication is, in general, a quite dificult task. However for small numbers, as those familiar to the classroom, the process is made in elementary terms and the only prerequisite is to know polynomial addition and multiplication. Below, I present, succintly some rules to facilitate the process of finding the prime factors of a natural number n. Of course, these rules can be completed and improved for a better comprehension.

Rule 1. Express the number n as a cuadratic polynomial of the type $ax^2 + bx + c$. The process is supposed to end, before or when we arrive to a polynomial of the type $[a/2]x^2 + mx + s$, where $[a/2]$ means the greatest integer either less or equal to $a/2$.

Rule 2. Check and put out digital prime factors like 2, 3, 5 and 7. For example, numbers 135, 5712 and 1428 can be expressed:

$135 = x^2 + 3x + 5 = 10x + 3x + 5 = 10x + 35 = 5(2x + 7) = 5\cdot 27 = 5\cdot 3^3$

$5712 = 5x^3 + 7x^2 + x + 2 = 57x^2 + x + 2 = 56x^2 + x^2 + x + 2 = 56x^2 + 10x + 12 = 2(28x^2 + 5x + 6) = 2^2(14x^2 + 2x + 8) = 2^3(7x^2 + x + 4) = 2^4(3x^2 + 5x + 7) = 2^4(3x^2 + 3x + 2x + 7) = 2^4(3x^2 + 3x + 27) = 2^4\cdot 3(x^2 + x + 9) = 2^4\cdot 3(11x + 9) = 2^4\cdot 3(7x + 4x + 9) = 2^4\cdot 3(7x + 49) = 2^4\cdot 3\cdot 7(x + 7) = 2^4\cdot 3\cdot 7\cdot 17$.

$1428 = 14x^2 + 2x + 8 = 2(7x^2 + x + 4) = 2^2(3x^2 + 5x + 7) = 2^2\cdot 3(x^2 + x + 9) = 2^2\cdot 3\cdot 7\cdot 17$.

In the last example we used some shortcuts and used the fact that $x^2 + x + 9 = 11x + 9 = 7x + 4x + 9 = 7x + 7\cdot 7 = 7(x + 7) = 7\cdot 17$.

The above process could be done finding directly from the given numbers, the factors 2, 3, 5 and 7.

Rule 3. If the number n to be factored as $n = k\cdot l$, ends with the digit:

i) **1**, we imagine that *k* and *l*, either, both end in 1, or one of them ends with 3 and the other with 7, or both of them ends with 9. This is because the last digit of the products 1·1, 3·7, 9.9 is exactly 1. This means that when we make the traits, we must check at all of these possibilities.

ii) **3,** we may suppose that *k* and *l*, either, one of them has 1 and the other 3, as the last digit, or one of them has 7 and the other one 9 as the last digit. In both cases the product ends with 3.

iii) **7,** we imagine that *k* and *l*, either, one of them has 1 and the other 7, as the last digit, or one of them has 3 and the other one 9 as the last digit. In both cases the product ends with 7.

iv) **9,** as before, *k* and *l*, either, one of them has 1 and the other 9, as the last digit, or both of them have 7 as the last digit. In both cases the product ends with 9.

Rule 4. When the last digit of *n* is even, namely, **0, 2, 4, 6, 8**, we can factor 2, all times we need it, and follow the process with rules 1 and 2. We can make the same thing when the last digit is **5**.

Rule 5. Never try to evoy rule 2 in the the first try. If you don’t put out all prime digits 2, 3, 5 and 7 at the beginning, you will not find the right factors at all.

Conclusion

The rules above are just guides to perform our task of finding prime factors of a given number. Practicing with specific numbers can help us to master the process. An advice is to construct the Erathostenes Cribe from 1 to 1000 or beyond. And better yet, it is take the process as a pastime. It is really nice to discover that, each number has its own characteristics in the process of factoring.

First corrected draft:

Armenia, Colombia, December 2015