La Educación Matemática como parte de las Matemáticas Aplicadas

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

"*El mundo siempre necesita de herejes que desafíen las ortodoxias establecidas.*" B. Mandelbrot.

Resumen. El propósito de este trabajo es mostrar que el cambiar de enfoque de las matemáticas, de lo tradicional a concepciones modernas, permite explicar razonadamente la representación de los números y las operaciones básicas de la aritmética. Se busca además, llevar al aula de la educación elemental y media, parte de las matemáticas creadas por Gauss, Hensel, Kummer y Eisenstein, hoy ignoradas en los currícula de nuestro tiempo. Partiendo de las más simples entidades numéricas como son el uno y el cero se irá construyendo gradualmente un edificio donde se pueda dar cabida a la aritmética, al álgebra, al análisis, y demás matemáticas elementales.

Palabras Clave. Educación matemática, polinomios.

Abstract. The main purpose of this paper is to show how, by using a quite different approach to math in the regular curriculum, we can represent numbers in a reasonable way based on mathematics created by so great mathematicians as Gauss, Hensel, Kummer and Eisenstein among others, ignored today by the teachers of our own age at elementary and medium schools. Starting with the simplest numerical entities, as zero and one in the foundations, we shall be gradually constructing a building where we can make room for arithmetic, algebra, mathematical analysis and all elementary mathematics.

Key words and Phrases. Mathematics Education, Polynomials.

1 – Introducción.

La idea de convertir la educación matemática en cierta variedad de matemáticas aplicadas la sugirió Hyman Bass[1] hace algunos años. El título de esta exposición es tanto un interrogante como una inquietud que busca crear consciencia de la importancia que el estudio de las matemáticas tiene para la formación integral del ser humano; no sólo por su valor en las aplicaciones, sino más importante aun, por cuanto que su estudio y asimilación aporta a la estructuración racional del pensamiento del niño y del joven. Creemos que las matemáticas de nuestro tiempo, nos van a ayudar a sacar, la educación matemática del terrible estancamiento en el que ha permanecido al menos durante los últimos cien años.

En otros artículos[2] he llamado la atención sobre el monumental atraso en que la educación matemática ha permanecido en el último siglo, con relación a los sorprendentes desarrollos de las matemáticas en el mismo lapso. La dimensión de este atraso adquiere mayor relevancia cuando el ciudadano común se enfrenta a la tecnología que aplica en su vida

---

[1] Bass, H. *Mathematics, mathematicians and mathematics Education*. Bulletin of the American Mathematical Society. Vol. 42, No. 4. October 2005.

[2]Ver por ejemplo mis artículos: *El gran vacío entre la educación matemática y la frontera de las matemáticas.* Lecturas Matemáticas- Volumen 30 (2009), páginas 31-51, http://www.scm.org.co/revistas.php?modulo=Resultados&year=2009&revista=Lecturas
y *El estado de la educación matemática. De Felix Klein a Hyman Bass. Una apreciación personal* en: http://www.matematicasyfilosofiaenelaula.info/articulos.htm

diaria y se pregunta sobre el andamiaje matemático que soporta esta tecnología y no ve dónde, o por qué, las matemáticas están allí. El mismo docente de matemáticas, generalmente desconoce, las matemáticas que han hecho posible lograr el nivel tecnológico de la sociedad actual. Seguimos enseñando matemáticas antiguas a espaldas de todo el conocimiento que nos legaron Gauss, Fourier, Riemann, Klein, Hilbert, Frege, Russell, von Neumann, Gödel, Tarski y tantos otros.

Con este trabajo nos proponemos contribuir con las primeras puntadas hacia un nuevo enfoque de enseñanza de las matemáticas, que concilie las matemáticas de contenido moderno con la educación matemática de nuestro tiempo. Llevar matemáticas frescas desde el nicho mismo de su creación en el frente de la investigación, hasta el aula elemental de clase ha sido un verdadero reto. Pocos matemáticos lo han intentado. Entre éstos citemos a Félix Klein (1849-1925), quien a fines del siglo XIX divulgó entre los profesores de bachillerato la prueba de la trascendencia del número π. Con la prueba que Ferdinand Lindemann (1852-1939) dio de este hecho, se solucionó negativamente el clásico problema de la cuadratura del círculo.

Lo que pretendemos aquí es mostrar cómo, la introducción temprana de los polinomios en la escuela, va a permitir llegar con suficiente y sólida motivación, a muchos conceptos de matemáticas que hoy llamamos avanzados y que tienen relación con álgebra abstracta, análisis matemático, topología, teoría de probabilidades, etc.

Por su carácter expositivo, este artículo adolece de enunciados formales de teoremas y sus consabidas demostraciones. Más que un trabajo matemático en toda su extensión, es una exposición de motivos que justifica la necesidad de cambiar la misma estructura basal de la educación matemática, buscando nuevos enfoques, planteamientos e inquietudes que muestren cómo enseñar matemáticas en forma integral de modo que aparezcan como un cuerpo total de ideas y no como una teoría compartimentalizada, donde sus distintas áreas carecen de conexión visible entre una y otra.

2 – Aperitivo

Supongamos que el niño ya está familiarizado con los números enteros y que entiende algunas de sus propiedades intrínsecas respecto a dos operaciones definidas en ellos como son, la suma y la multiplicación. Empecemos con un conjunto X definido por:

$$X = \{0,\ 1,\ x,\ x+1,\ x^2, \ldots\}, \text{ donde } x \neq 0, \text{ y, } x \neq 1.$$

Asumamos definidas dos operaciones, + y $\bullet$ en X, según la tabla de la figura 1. Estas tablas de sumar y multiplicar, a diferencia de las que enseñamos en la escuela, son infinitas en el sentido de que presumimos que aquí aparece, explícitamente el resultado de todas las sumas y productos posibles definidos en X. Aunque este conjunto por definición es infinito, no por eso tiene que considerarse ajeno a la comprensión del niño ya familiarizado con los números naturales que usa para el conteo y que entiende que son infinitos.

La enseñanza tradicional de la aritmética parte de las tablas pitagóricas de sumar y multiplicar y se supone que a partir de allí se debe aprender a sumar y a multiplicar cualquier par de números.

+	0	1	x	x+1	…	•	0	1	x	x+1	…
0	0	1	x	x+1	…	0	0	0	0	0	…
1	1	x	x+1	x^2	…	1	0	1	x	x+1	…
x	X	x+1	x^2	x^2+1	…	X	0	x	x^2	x^2+x	…
x+1	x+1	x^2	x^2+1	x^2+x	…	x+1	0	x+1	x^2+x	x^3+1	…
…	…	…	…	…	…	…	…	…	…	…	…

***Fig.* 1.** Tablas de sumar, a la izquierda, y de multiplicar, a la derecha, definidas en el conjunto $X = \{0, 1, x, \ldots\}$. Las funciones + y • definidas en $X \times X$ son operaciones internas que asocian al par (x,y) los elementos $x+y$, y, $x \bullet y$, en X, respectivamente.

El proceso de lograr un nivel aceptable de suficiencia tardará años, con la decepcionante consecuencia de que fue tiempo perdido, primero porque el proceso de aprendizaje de las rutinas aritméticas no genera o refuerza aptitudes hacia las matemáticas y segundo porque en la vida adulta no va a tener la utilidad que se presumía, ya que los dispositivos electrónicos a nuestro alcance han llevado las rutinas aritméticas a la obsolescencia.

Las llamadas tablas pitagóricas no dan pistas de cómo llevar a cabo sumas o multiplicaciones arbitrarias. Los algoritmos que lo permiten deben aprenderse por aparte y deben practicarse una y otra vez hasta retenerlos de memoria. Estos procedimientos se realizan mecánicamente sin entender el porqué de los mismos. En esta irracionalidad del proceso de enseñanza-aprendizaje de la aritmética radica buena parte de la aversión que con el tiempo el estudiante va a tener hacia las matemáticas. En el proceso de buscar las razones en que se soportan los algoritmos para sumar y multiplicar, he escrito un par de artículos que muestran cómo, las operaciones aritméticas pueden explicarse racionalmente, y de paso, he propuesto algunas ideas para introducir y motivar el aprendizaje de conceptos como el de número y su representación.

Los segmentos más simples (partes sombreadas) que en el fondo generan las tablas de la figura 1, se reducen a dos matrices 3×3, que permiten construir inductivamente los elementos de X y además dan las bases lógicas para llenar en forma acertada el resto de las entradas de la tabla. De allí saldrán también ciertas nociones que se estudian en el álgebra elemental como reducción de términos semejantes, propiedades de las potencias, etc. Esta tabla está representada en la figura 2. La letra x representa un número, aunque podría representar una matriz, una función o algo más, no necesariamente un número.

+	0	1	•	0	1
0	0	1	0	0	0
1	1	x	1	0	1

***Fig.* 2.** Tablas de sumar y multiplicar básicas, a partir de las cuales se origina la tabla general de la figura 1.

Esta tabla nos permite, en primer lugar, dar un orden a los elementos de X y en segundo lugar, construir inductivamente sus elementos. Aceptemos que el orden natural es 0, 1, x, y que los elementos sucesivos se obtienen sumando 1 cada vez, a fin de hacer de X un conjunto inductivo. Por ejemplo, el siguiente elemento de x será x + 1 y el siguiente a él es

$(x + 1) + 1$. En este punto aparece la necesidad de introducir conceptos propios del algebra moderna como es la llamada, *propiedad asociativa* para la suma, la que justifica el paso "$(x + 1) + 1 = x + (1 + 1) = x + x$".

La tabla básica no nos dice como sumar $x + x$. Aquí de nuevo tenemos que recurrir al álgebra moderna que nos suple con dos nuevas propiedades que podemos aplicar para resolver el problema. La *existencia de un elemento unidad* para la multiplicación y la *propiedad distributiva* que sirve de puente entre las dos operaciones definidas en X. Con la ayuda de estas propiedades damos el siguiente paso:

$$\text{“}(x + 1) + 1 = x + (1 + 1) = x + x = (1) \bullet x + (1) \bullet x = (1 + 1) \bullet x = x \bullet x\text{”}. \qquad \mathbf{(1)}$$

A la expresión "$x \bullet x$" la denotaremos simplificadamente como x^2, que es el término que aparece en el sitio 4×4 de la tabla de la figura 1. De la expresión (**1**) se sigue la curiosa consecuencia[3]

$$\boxed{x + x = x \bullet x = x^2}$$

Esto nos dice que en la aritmética inducida por + y •, la expresión anterior tiene validez. Además, basados en ella, podemos obtener expresiones que en apariencia pueden lucir fuera de tono en el álgebra convencional del bachillerato.

Continuando con la generación de los elementos de X, el siguiente a x^2 será $x^2 + 1$, el siguiente a éste es: $(x^2 + 1) + 1 = x^2 + (1+1) = x^2 + x$. Continuando en esta tónica encontramos $(x^2 + x) + 1$, $x^2 + x + (1+1) = x^2 + (x + x) = x^2 + x^2 = (1)x^2 + (1)x^2 = (1+1) x^2 = x \bullet x^2 = x^3$. Como antes encontramos otra fórmula curiosa:

$$\boxed{x^2 + x^2 = (1)\, x^2 + (1)\, x^2 = xx^2 = x^3}$$

En general vamos a encontrar que para un entero positivo n,

$$\boxed{x^n + x^n = xx^n = x^{n+1}}$$

El último paso lo hacemos por definición, con el objeto de simplificar la escritura y para motivar más adelante la introducción de las propiedades correspondientes a la potenciación. De modo análogo podemos seguir generando todos los elementos de X.

Lo que estamos haciendo aquí se supone va dirigido a estudiantes de educación básica y no desde luego a profesionales de las matemáticas. Sin embargo, ciertos aspectos cruciales de la argumentación presumen conocimientos avanzados de matemáticas como teoría de anillos y módulos como se entienden en álgebra moderna.

El recurso de la tabla para sumar nos permitió enlistar los elementos de X. La tabla de multiplicar nos dará la posibilidad de descubrir algunas propiedades algebraicas del conjunto X. Miremos por ejemplo algunos productos, no sin antes advertir que el producto $x \bullet y$ se escribe convencionalmente como xy y que 0 y 1 juegan el papel de elementos

---

[3] Esta simple igualdad sirvió de motivación para escribir mi artículo, *¿Por qué 2×2=4 y no 5, por ejemplo?*, que aparece en: http://www.matematicasyfilosofiaenelaula.info/articulos/porque2por2igual4.pdf,

neutros para la suma y la multiplicación respectivamente y que la multiplicación es conmutativa. Se sigue de lo anterior que la estructura algebraica de (X, +, $\bullet$) es la de un anillo conmutativo con elemento unidad[4]. Repitamos algunas consecuencias de lo anterior.

1) $xx = x^2 = x + x$. Según lo vimos arriba.

2) $x(x+1) = xx + x1 = x\,x + 1x = x^2 + x$.

3 $(x + 1)\,(x + 1) = (x + 1)^2 = x(x+1) + 1(x+1) = x^2 + x1 + 1x + 1 = x^2 + (x + x) + 1 = x^2 + x^2 + 1 = (1+1)\,x^2 + 1 = x\,x^2 + 1 = x^3 + 1$. Así:

$$\boxed{(x + 1)^2 = x^3 + 1}.$$

4) $(x + 1)^3 = (x+1)\,(x + 1)^2 = (x + 1)\,(x^3 + 1) = (x^4 + x) + (x^3 + 1) = x^4 + x^3 + x + 1$.

5) $(x + 1)^4 = (x + 1)\,(x + 1)^3 = x(x^4 + x^3 + x + 1) + x^4 + x^3 + x + 1 = x^5 + x^4 + x^2 + x + x^4 + x^3 + x + 1 = x^5 + (x^4 + .x^4) + x^3 + x^2 + (x + x) + 1 = x^5 + x^5 + x^3 + x^2 + x^2 + 1 = x^6 + x^4 + 1$.

6) $x^3 \bullet x^3 = (1+1)\,x^3 = xx^3 = x^4$.

7) En general para un natural n dado, i) $x^n + x^n = (1+1)\,x^n = x\,x^n = x^{n+1}$, ii) $x^n - 1 = x^{n-1} + x^{n-2} + \ldots + x + 1$.

8) Para m y n naturales i) $x^m\, x^n = x^{m+n}$, ii) $(x^m)^n = x^{mn}$

9) Para n natural, la propiedad 7 también se puede escribir como .

$$\boxed{x^n = x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1 + 1}.$$

10) Cuando n es impar, $x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + \ldots - x + 1)$.

La propiedad $x^n = x^{n-1} + x^{n-2} + \ldots + x + 1 + 1$, que llamaré el *Efecto Dominó*, muestra que la potencia x^n se puede expresar como suma de potencias sucesivas de x, empezando en $x^0 = 1$ y continuando hasta x^{n-1} y sumando 1. El nombre de efecto dominó se debe a que al sumar 1 a la derecha del signo igual las potencias van sucesivamente aumentando de uno en uno hasta llegar a x^n.

Las fórmulas anteriores que involucran números naturales se pueden probar por inducción o pueden constatarse para cada caso particular de n. Hay varias cosas que llaman la atención en las fórmulas de arriba: a) la expresión $(x + 1)^2 = x^3 + 1$. b) el teorema del binomio en su forma clásica no luce igual a las expresiones binomiales en X. 3) La ley de los exponentes coincide en el producto de potencias pero difiere en la suma de potencias iguales. Se observa también que las expresiones o "polinomios" que resultan en estas operaciones, todas tienen coeficientes, 0, ó, 1. ¿Será válido esto siempre que se opere con los elementos de X? La respuesta es si. Todo elemento de X tiene la forma

[4] Para un estudio detallado de estos temas se puede consultar los textos de algebra moderna, por citar uno de los más clásicos: van der Waerden, B. L. *Algebra.* Vol. I. Springer-Verlag. Berlin. 1991.

$$p\,(x) = \sum_{i=0}^{i=n} a_{n-i}x^{n-i}\text{ , donde } a_i \in \{0,1\}\text{ , } a_n \neq 0\,. \qquad \textbf{(2)}$$

.

3 – Cuerpos Numéricos y cuerpos p-ádicos

Cuerpos Numéricos. A expresiones como (**2**) estamos acostumbrados a verlas como polinomios con indeterminada *x*, y pensadas como funciones de variable real o compleja. Sin embargo podemos pensar de ellas como entidades abstractas, donde se pueda definir las mismas operaciones que se definen en los enteros y aún más allá, entenderlas como expansiones infinitas del tipo:

$$p(x) = \sum_{i=0}^{i=\infty} b_i x^i \text{ , con } b_i \text{ en un cuerpo } \boldsymbol{F}.$$

Esto permite definir formalmente la adición y el producto de este tipo de polinomios.

En efecto si, $a(x) = \sum_{i=0}^{i=n} a_{n-i}x^{n-i}$, y, $b(x) = \sum_{j=0}^{j=l} b_{l-j}x^{l-j}$, definimos:

$a(x) + b(x) = \sum_{i=0}^{i=n} a_{n-i}x^{n-i} + \sum_{j=0}^{j=l} b_{l-j}x^{l-j} = \sum_{k=0}^{k=m}(a_{m-k}+b_{m-k})x^{m-k}$, con los ajustes apropiados a que haya lugar cuando los grados de los polinomios no coinciden.

$a(x)b(x) = \left(\sum_{i=0}^{i=n} a_{n-i}x^{n-i}\right)\left(\sum_{j=0}^{j=l} b_{l-j}x^{l-j}\right) = \sum_{i+j=0}^{n+l}\left(\sum_{k=0}^{i+j} a_k b_{(i+j)-k}\right)x^{(i+j)-k}$, donde a_i , y, $b_j \in \boldsymbol{F}$.

En forma similar se puede definir la sustracción. Si el anillo de donde se toman los coeficientes es además un cuerpo también se puede definir el algoritmo de la división. Las cuatro operaciones básicas, +, –, **•**, ÷ definidas en los polinomios van a depender de los coeficientes.

Queremos que el conjunto de estos polinomios sea cerrado con respecto a las operaciones +, –, •, con el objeto que el conjunto sea al menos un anillo. Este conjunto de polinomios con coeficientes en el cuerpo ***F*** se denota como ***F***[*x*] y se conoce como el anillo de polinomios con indeterminada *x*. Cuando el cuerpo ***F*** $\subseteq$ ***C***, (***C*** el conjunto de los números complejos), el anillo de polinomios resultante se conoce como *cuerpo de números* y tiene una representación concreta denotada por ***F***(α), donde α es una raíz compleja. Más exactamente si *p* (*x*) es un polinomio primo, ***F***[*x*] / *p* (*x*) ***F***[*x*] es isomorfo a ***F***(α), donde α es una raíz de *p* (*x*).

Cuerpos p-ádicos

Sabemos desde el tiempo de Georg Cantor que los conjuntos **N**, **Z**, **Q,** de los números, naturales, enteros, racionales y el conjunto de todas las soluciones de ecuaciones polinómicas con coeficientes racionales (los números algebraicos) tienen el mismo cardinal. Esto significa que hay, en cierto sentido, una equivalencia entre estos cuatro conjuntos. La pregunta que uno se hace es, ¿se pueden representar todos ellos, usando el mismo patrón, sin recurrir por ejemplo al signo menos (sustracción para **Z**) o al cociente (división, para **Q**) o los radicales (para los números algebraicos)? La respuesta es sí. La idea está en formalizar conceptos como suma de polinomios de infinitos términos como lo hicimos arriba. Miremos un par de ejemplos[5] de cómo puede hacerse para cocientes y para números negativos.

Ejemplo 1. Representar la fracción 24/17 como una serie formal, es decir, como un polinomio de infinitos términos.

Tomemos como base a 3 para expandir los números 24 y 17, así: $24 = 0\times 3^0 + 2\times 3^1 + 2\times 3^2 = 0\times p^0 + 2\times p^1 + 2\times p^2 = 2p + 2p^2$, y, $17 = 2\times 3^0 + 2\times 3^1 + 1\times 3^2 = 2\times p^0 + 2\times p^1 + 1\times p^2 = 2 + 2p + p^2$. Por lo tanto,

$$\frac{24}{17} = \frac{2p+2p^2}{2+2p+p^2} = p + p^3 + 2p^5 + p^7 + p^8 + 2p^9 + \ldots$$

La anterior igualdad debe entenderse en el sentido formal, no como una igualdad usual en la que se puede reemplazar p para obtener una identidad. Para verificar que la igualdad se da, basta multiplicar el denominador por la serie y hacer las reducciones apropiadas recordando la condición de que p vale 3.

$$(2+2p+p^2)(p + p^3 + 2p^5 + p^7 + p^8 + 2p^9 + \ldots) = (2p+2p^2) +$$
$$(p^3 + 2p^3) + 2p^4 + p^5 + 4p^5 + 4p^6 + 2p^7 + 2p^7 + 2p^8 + 2p^8 + p^9 + 2p^9 + 4p^9 + \ldots).$$

Salvo los dos primeros términos, los restantes se van agrupando para determinar potencias cada vez mayores hasta "desaparecer en el infinito".

Ese desaparecer en el infinito significa que, con una métrica diferente a la usual, las potencias mayores disminuyen su valor absoluto hasta reducirse a cero. La métrica a que hacemos referencia se conoce hoy como *ultramétrica* y el valor absoluto que la genera se llama *valor absoluto p-ádico.*

Ejemplo 2. Representar, – 1, como una serie de potencias de un número primo.

En efecto

$-1 = (p-1) + (p-1)\,p + (p-1)\,p^2 + (p-1)\,p^3 + \ldots$, para todo $p \neq \mathbf{1}$. Así, al menos formalmente, un número negativo se puede expresar como suma de potencias de un número primo.

Los cocientes de enteros y los números negativos se pueden expresar como series formales de potencias de números primos lo que podría sugerir que todo número racional se puede expresar como una serie formal del tipo

$x = \sum_{i=0}^{i=\infty} b_{n_o+i}\, p^{n_o+i} = b_{n_o} p^{n_o} + b_{n_o+1} p^{n_o+1} + \ldots$, donde n_0 puede ser un entero negativo.

[5] Tomados de: Gouvea, F. Q. *p-adic Numbers. An Introduction.* Springer-Verlag. New York. 2003.

Estas series se conocen en análisis de variable compleja como series de Laurent y como Kurt Hensel (1861-1941) probó, todo número real es susceptible de expresarse en esta forma. Los números así expresados se denominan números p-ádicos[6].

4) – Los números como eje de la educación matemática

El concepto de número es la idea matemática intuitiva por excelencia. Empieza a aparecer en la mente del infante desde los primeros meses de vida. Es para algunos autores[7] una idea connatural a la especie humana, que se hereda y trasmite genéticamente. Este concepto es puramente abstracto y tenemos acceso a él a través del lenguaje hablado o escrito o trasmitido de un individuo a otro con el recurso de símbolos. La simbología del lenguaje escrito nos ha permitido tener conocimiento del desarrollo de la cultura a lo largo de la historia y en particular conocer y apropiarnos de los avances matemáticos de generaciones pasadas.

Los siglos diecinueve y veinte fueron particularmente ricos en producción matemática. Esa gran producción, sin embargo, no ha llegado al aula de clase de la educación básica, generando así, un gran desfase entre lo que se enseña a ese nivel, y lo que está al frente del desarrollo de las matemáticas. Buscando acortar esta brecha he propuesto algunas alternativas que combinan la enseñanza de las matemáticas elementales con el aderezo de conceptos que, aunque avanzados, podrían estar al alcance de las mentes jóvenes. Particularmente la representación de los números nos permite introducir conceptos algebraicos por la vía de entidades fáciles de captar como son los polinomios de una sola variable.

Aunque la definición formal de polinomio no es nada intuitiva[8], su representación induce a creer que sólo se trata de productos y de sumas de variables, lo que es fácil de captar e interpretar, más aun si se reemplazan los coeficientes y las variables por números. Lo que pretendemos aquí explicar es la manera como teniendo la idea intuitiva de número, puede uno, buscando su representación formal, llegar a los polinomios y de allí, en forma racional, a los algoritmos para las cuatro operaciones básicas que se enseñan en la escuela.

Es importante enfatizar que los números, sin ser todas las matemáticas, se constituyen para la educación básica, en el eje central, por cuanto que ellos aparecen en la formulación, interpretación y solución de muchos problemas, no sólo en matemáticas, también en física, química y aun, en la vida real misma.

La forma en que recibimos la representación de los números de la cultura árabe fue como secuencia de símbolos $b_n b_{n-1} \ldots b_1 b_0$, que interpretada en su valor nominal corresponde a:

$$b_n\, b_{n-1} \ldots b_1\, b_0 = \sum_{i=0}^{i=n} b_{n-i} 10^{n-i} = b_n\, 10^n + b_{n-1}\, 10^{n-1} + \ldots + b_1\, 10^1 + b_0\, 10^0,\ b_i \in \{0, \ldots, 9\}.$$

---

[6] Un estudio detallado de este tema puede verse en: Gouvea, F. Q. *Opus cit. Pág.* 43 y siguientes.

[7] Devlin, K. *The Math Gene. How Mathematical Thinking Evolved and Why Numbers are like Gossip.* Basic Books. 2000.

[8] Ver por ejemplo la definición en: Adkins, W. A. et al. *Algebra. An Approach via Module Theory.* Springer-Verlag. New York. 1992. Pags. 54-56

La pregunta que uno se hace es: ¿por qué escribimos los números naturales en esa forma y no en otra? Desde que el sistema decimal hizo su aparición en occidente en la edad media por conducto de la cultura árabe parece que esta forma de representar los números llegó para quedarse y convertirse en el sistema de representación universal. Sin embargo hay formas simples de representar los números y de introducir los algoritmos de la aritmética de manera más sencilla que aquella que acompaña la aritmética heredada del sistema hindú arábigo. Entre las razones que se dan para que el sistema decimal haya permanecido y permeado toda la cultura humana están primero el balance entre el número de símbolos para representar los números, no son demasiados ni muy pocos y segundo la asociación del número diez con los dedos de las manos que es una medida universal para el ser humano.

El hecho de usar sistema binario no nos impide seguir usando el sistema decimal en nuestra simbología, particularmente en los exponentes de la representación de los números y en la confrontación de las ventajas y desventajas de los dos sistemas posicionales.

El sistema descrito en la sección **2** no es otra cosa que aritmética binaria, soslayada dentro de polinomios con coeficientes en $\{0,1\}$ y que al reemplazar a x por 2, el conjunto X descrito allí, coincide con $\boldsymbol{Z}^+ \cup \{0\} = \{0, 1, 2, 3, \ldots\}$**.**

La aritmética binaria es sencilla en razón a que las tablas de sumar y multiplicar son casi obvias y fáciles de recordar. Si nos olvidamos del dos podemos hacer todas las operaciones que queramos usando los sencillos algoritmos de la suma, resta, multiplicación y división de polinomios y si se quiere luego para llevar el resultado a representación decimal, se cambia la x por 2 y se usa aritmética decimal. La conversión de números en base decimal a binaria es simple; se reduce a partir en mitades, repetitivamente, y anotar los residuos hasta lograr un cociente de 1. Esto es equivalente a tomar la mayor potencia de dos implícita en el número y así descendiendo hasta la potencia de menor grado incluida. Las cifras binarias aparecen con 1´s y 0´s, según aparezcan o no las respectivas potencias de 2. Por ejemplo 25 $= (1)2^4 + (1)\,2^3 + (0)\,2^2 + (0)\,2^1 + (1)\,2^0$ y así su representación binaria será 11001. Aquí aparece 0 en el lugar de las potencias ausentes, 2^2, y, 2^1.

En otros artículos[9] he mostrado ejemplos relacionados con las cuatro operaciones aritméticas básicas. Aquí vamos a describir el comportamiento de los números enteros vistos en sistema binario con respecto a su primalidad, es decir a su condición de ser primos o compuestos.

La representación p-ádica introduce la posibilidad de ver los números en un contexto más rico desde el punto de vista teórico, y también desde el punto de vista práctico. Usando este enfoque se puede introducir conceptos de: geometría a través de la métrica de los valores absolutos; de análisis como en las series de potencias; de topología, como la noción de continuidad y fundamentalmente de álgebra abstracta a través de estructuras que sustentan el andamiaje de los cuerpos numéricos.

El álgebra que reposa en la estructura de los números que se estudian en la escuela elemental y media aparece naturalmente cuando se enseña los números con un enfoque contemporáneo, donde la prioridad es el estudio de sus propiedades y no tanto de sus aplicaciones. Esas propiedades aparecen tempranamente como es el caso de la caracterización de los enteros como primos y compuestos. Una de las aplicaciones de la

---

[9] Ver por ejemplo *Del Bit a las Wavelets,* y *El Poder del Dos*, que aparecen en: www.matematicasyfilosofiaenelaula.info

teoría de números a la vida moderna es la criptografía en la que descansa la seguridad de los códigos secretos que nos protegen contra la invasión a la privacidad de nuestras tarjetas de crédito y de cuentas de Internet, las que aspiramos no estén al alcance de intrusos.

Una propuesta diferente en cuanto al estudio de los números y sus propiedades, reposa en el enfoque *p-ádico*, sugerido por Ernst Kummer y estudiado por su alumno Kurt Hensel a fines del siglo XIX. Este enfoque, como vimos arriba, introduce los polinomios tempranamente, permitiendo a los niños acceder a las matemáticas avanzadas desde la primaria, para lograr en el bachillerato, siguiendo el mismo enfoque, una comprensión de temas modernos como, geometrías no euclidianas, análisis matemático, álgebra moderna y topología.

Una noción importante y útil en cuanto a aplicaciones es la factorización de números naturales, que por elemental que parezca, llega a niveles de sofisticación tan altos, al punto de estar en la base del cifrado de la información que circula en las redes de información a través de la Web. El parentesco entre la factorización de los números y de los polinomios está ligado al estudio del algebra moderna mediante resultados importantes como son el lema de Gauss, y teoremas de Eisentein y de Hensel. Digamos primero que con cada número natural hay por lo menos un polinomio asociado a él, específicamente, el polinomio que según la base, lo representa. Si $p(x)$ es el polinomio que representa al número n, los factores primos de n tendrán su representación en los factores primos de p.

Por ejemplo si $n = 25$, y la base es 2, $p(x) = x^4 + x^3 + 1$ es el polinomio que representa a 25. Puesto que $25 = 5 \times 5$, los factores primos de p van a coincidir con la representación polinómica para 5, que en base 2, es $x^2 + 1$. En efecto $x^2 + 1$ es primo en $P[x]$, el anillo de polinomios con coeficientes en {0, 1} y $(x^2 + 1)(x^2 + 1) = x^4 + x^2 + x^2 + 1 = x^4 + x^3 + 1 =$ 25 (puesto que $x^2 + x^2 = x^3$, según vimos en la sección 2). Por lo tanto factorizar en los números naturales tiene su contraparte en la factorización de polinomios que los representan.

5) – Los números en conexión con el Álgebra Abstracta

Factorización de Polinomios en *X*. Denotemos como $B[x]$ el anillo de polinomios con coeficientes en $\{0,1\}$.Vimos como todos los elementos del conjunto X, definido al principio, se reducían a polinomios con coeficientes en $\{0,1\}$. En esta sección definimos factores primos de un polinomio. Tenemos que aclarar lo que significamos por elementos primos en un anillo. Consideremos sólo elementos no nulos en $B[x]$.

Definición. Un polinomio $p \neq 0$, se dice primo o irreducible si sólo admite una factorización trivial del tipo $p = ab$, donde a o b es una unidad. Por ejemplo $x^2 + 1$ es primo, visto como polinomio con coeficientes en {0, 1}, mientras que $x^3 + 1$, no lo es, porque se deja dividir por $x + 1$ o si se quiere, se puede expresar como el producto $(x + 1)$ $(x + 1)$.

Criterio de Primalidad. Un polinomio binario $p(x)$ es primo si y solo si $p(2)$ es primo. Aquí $p(2)$ corresponde al valor numérico de p cuando se reemplaza a x por 2. Observe que al tomar $x = 2$ en la definición de X al comienzo, no encontramos otra cosa que los enteros no negativos. Por lo tanto con cada polinomio binario está asociado un número natural y recíprocamente cada número natural está asociado a un polinomio binario. Por ejemplo el número 17 está asociado al polinomio $p(x) = x^4 + 1$, porque $p(2) = 2^4 + 1 = 17$. Se comprueba que por ser 17 primo, $x^4 + 1$ es también un polinomio irreducible. En efecto, $x^4 + 1$ no se deja dividir por los primos menores que él que son: x, $x+1$, $x^2 + 1$, $x^2 + x + 1$, $x^3 + x + 1$, $x^3 + x^2 + 1$.

Cuando se factoriza un número natural n en factores primos existe una correspondencia entre los factores primos de n y los factores primos de $p(x)$ en $B[x]$, es decir, si $p(x) \in B[x]$, es el polinomio asociado a n, entonces hay en $B[x]$ polinomios primos que corresponden a los factores primos de n. Miremos unos ejemplos.

EJEMPLO 1
Si queremos saber si 5183 es primo[10], lo usual es dividir sucesivamente por los primos menores o iguales que la raíz cuadrada del número. El número será primo si ninguno de los primos menores que $\sqrt{5183}$ lo divide exactamente. Este proceso es dispendioso porque hay que hacer veinte verificaciones. La alternativa es hallar su representación polinómica binaria y tratar de hallar un factor primo. Si existe este factor primo, el número en cuestión será compuesto.
El polinomio binario asociado a 5183 es $p(x) = x^{12} + x^{10} + x^5 + x^4 + x^3 + x^2 + x + 1 = x^{12} + x^{10} + x^6 - 1 = x^6(x^6 + x^4 + 1) - 1 = x^6(x^3 + 1)^2 - 1 = [x^3(x^3 + 1)]^2 - 1 = ([x^3(x^3 + 1)] - 1)([x^3(x^3 + 1)] + 1)$. Se sigue que $f(x) = [x^3(x^3 + 1)] - 1$, y, $g(x) = [x^3(x^3 + 1)] + 1$, son factores de $p(x)$. Por lo tanto $f(2) = 71$, y, $g(2) = 73$, son factores de 5163, lo que muestra que el número es compuesto. Este par de números primos que difieren en dos es un ejemplo de un par de primos gemelos, pares de los cuales no conocemos mucho, y ni siquiera sabemos si el conjunto de ellos es o no, infinito, aunque sabemos que hay una fuerte evidencia de que lo sea.

No todo número se deja trabajar tan fácilmente como el anterior pero con alguna práctica en la factorización de los primeros polinomios binarios se adquiere habilidad para factorizar polinomios de mayor grado. El siguiente ejemplo muestra como la factorización de un número ayuda a la factorización de su polinomio asociado. Aquí al igual que en el caso anterior los polinomios factores primos que surgen están asociados a una pareja de números primos gemelos. La consecuencia que encontramos es que números del tipo $g_n^2 - 1$, donde g_n es el número que está entre los dos primos gemelos, son fáciles de factorizar, por cuanto que $g_n^2 - 1 = (g_n - 1)(g_n + 1)$.

EJEMPLO 2. Factorizar el polinomio $x^{13} + x^{11} + x^7 + x^5 + x + 1$ asociado al número 10403.

Puesto que $10403 = 102^2 - 1 = (102 - 1)(102 + 1)$ y $102 = x^6 + x^5 + x^2 + x$, se tiene:

[10] Este número aparece en el libro de Neal Koblitz, *Random Curves. Journeys of a Mathematician*. Springer-Verlag. Berlin, Heidelberg. 2008 (Pag. 336). El número está relacionado con un juego de dados en el que se asigna probabilidades cuando aparece un número primo en el lanzamiento de dos dados.

10403 = $x^{13} + x^{11} + x^{7} + x^{5} + x + 1$ = (102 – 1)(102 + 1) = ($x^{6} + x^{5} + x^{2} + x - 1$)($x^{6} + x^{5} + x^{2} + x + 1$) = ($x^{6} + x^{5} + x^{2} + 1$)($x^{6} + x^{5} + x^{2} + x + 1$).

En efecto,
$(x^{6} + x^{5} + x^{2} + 1)(x^{6} + x^{5} + x^{2} + x + 1) = (x^{6} + x^{5} + x^{2})^{2} + x(x^{6} + x^{5} + x^{2}) + (x^{6} + x^{5} + x^{2}) + (x^{6} + x^{5} + x^{2} + x + 1) = x^{12} + x^{12} + x^{9} + x^{10} + x^{8} + x^{4} + x^{7} + x^{6} + x^{3} + x^{6} + x^{5} + x^{2} + x^{6} + x^{5} + x^{2} + x + 1 = x^{13} + x^{11} + x^{7} + x^{5} + x + 1$.

Si encontráramos un método para hallar los números $g^{2}{}_{n} - 1$, estaríamos ad portas de hallar un proceso que conduzca a la obtención de un número arbitrio de parejas de primos gemelos y si se muestra que hay infinitos de estos números llegaríamos a la anhelada prueba de que el conjunto de primos gemelos es infinito.

La siguiente tabla muestra los primeros pares de primos gemelos y su representación binaria junto al número, que en su factorización, los genera. Se observa en la tabla que g_n es múltiplo de 6, mientras que $g^{2}{}_{n} - 1$ a partir de n = 3 termina en 3 o en 9. Interesante sería conocer si esto es siempre cierto.

Tabla de los primeros primos gemelos g_n – 1, g_n + 1 y su representación binaria

n	g_n	$g_n^{2} - 1$	$B(g_n^{2} - 1)$	$g_n - 1$	$B(g_n - 1)$	$g_n + 1$	$B(g_n + 1)$
1	4	15	$x^3 + x^2 + x + 1$	3	$x + 1$	5	$x^2 + 1$
2	6	35	$x^5 + x + 1$	5	$x^2 + 1$	7	$x^2 + x + 1$
3	12	143	$x^7 + x^3 + x^2 + x + 1$	11	$x^3 + x + 1$	13	$x^3 + x^2 + 1$
4	18	323	$x^8 + x^6 + x + 1$	17	$x^4 + 1$	19	$x^4 + x + 1$
5	30	899	$x^9 + x^8 + x^7 + x + 1$	29	$x^4 + x^3 + x^2 + 1$	31	$x^4 + x^3 + x^2 + x + 1$
6	42	1783	$x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + x^2 + x + 1$	41	$x^5 + x^3 + 1$	43	$x^4 + x^3 + x + 1$
7	60	3599	$x^{11} + x^{10} + x^9 + x^3 + x^2 + x + 1$	59	$x^5 + x^4 + x^3 + x + 1$	61	$x^5 + x^4 + x^3 + x^2 + 1$
8	72	5183	$x^{12} + x^{11} + x^5 + x^4 + x^3 + x^2 + x + 1$	71	$x^6 + x^2 + x + 1$	73	$x^5 + x^3 + 1$
9	102	10403	$x^{13} + x^{11} + x^7 + x^5 + x + 1$	101	$x^6 + x^5 + x^2 + 1$	103	$x^6 + x^5 + x^2 + x + 1$
10	108	11663	$x^{13} + x^{11} + x^{10} + x^8 + x^7 + x^3 + x^2 + x + 1$	107	$x^6 + x^5 + x^3 + x + 1$	109	$x^6 + x^5 + x^3 + x^2 + 1$
11	138	19043	$x^{14} + x^{11} + x^9 + x^6 + x^5 + x + 1$	137	$x^7 + x^3 + 1$	139	$x^7 + x^3 + x + 1$

EJEMPLO 3. Factorizar el número N= 627, usando representación binaria.

Puesto que 627 = 512 + 64 + 32 + 16 + 2 + 1, la representación binaria de N es: $x^9 + x^6 + x^5 + x^4 + x + 1$ y el problema de factorizar N se convierte en el problema de hallar los factores primos de su polinomio binario asociado.

El primer paso es chequear si el polinomio tiene a x +1 (el primer polinomio binario primo y asociado con el número 3) como factor.

$x^9+x^6+x^5+x^4+x+1 \;=\; x^6(x^3+1)+x^4(x+1)+(x+1)=x^6(x+1)^2+x^4(x+1)+(x+1) \;=$ $(x+1)[\,x^6(x+1)+x^4+1\,]=(x+1)(\;x^7+x^6+x^4+1)$.

Pero $x^6=x^5+x^4+x^3+x^2+x+x$ y así:
$x^7+x^6+x^4+1=x^7+x^5+x^4+x^3+x^2+x+x+x^4+1=$
$x^3(x^4+1)+x(x^4+1)+(x^4+1)+x^4+x^2+x \;=\; (x^4+1)(x^3+x+1)+x(x^3+x+1) \;=$
$(x^3+x+1)(x^4+x+1)$. Por lo tanto.
$627=\; x^9+x^6+x^5+x^4+x+1=(x+1)(\,x^7+x^6+x^4+1)\;=(x+1)\;(x^3+x+1)(x^4+x+1)\;=$
$3\times 11\times 19$.

EJEMPLO 4. Factorizar el número 1729 en factores primos usando su representación binaria[11].
$1729=x^{10}+x^9+x^7+x^6+1$. Este polinomio se puede factorizar en factores primos usando los procedimientos elementales usados en el álgebra de bachillerato pero que se pueden asimilar desde la educación primaria. Por ensayo y error usando el procedimiento de factores comunes, encontramos,

$x^{10}+x^9+x^7+x^6+1\;=\;x^6(x^4+x+1)+x^9+1$.
Por otro lado
$x^9+1\;=\;(x^3+1)(x^6-x^3+1)\;=\;(x^3+1)(x^5+x^4+x^3+1)=(x+1)^2(x^5+x^4+x^3+1)$.

También,
$x^5+x^4+x^3+1=(x+1)x^4+(x+1)^2=\;(x+1)(x^4+x+1)$. Sustituyendo arriba,
$x^9+1\;=\;(x+1)^3(x^4+x+1)$. Volviendo a la primera igualdad encontraremos finalmente la factorización definitiva

$1729=x^{10}+x^9+x^7+x^6+1\;=\;x^6(x^4+x+1)+x^9+1\;=\;x^6(x^4+x+1)+(x+1)^3(x^4+x+1)=$ $(x^4+x+1)(x^6+x^4+x^3+x+1)\;=\;(x^4+x+1)(x^3+x^2+1)(x^2+x+1)\;=\;7\times 13\times 19$, por cuanto que

$x^6+x^4+x^3+x+1 \;=\; x^5+x^4+x^3+x^2+x^2+x^4+x^3+x+1 \;=$
$x^2(x^3+x^2+1)+x(x^3+x^2+1)+(x^3+x^2+1)\;=\;(x^3+x^2+1)(x^2+x+1)$.

EJEMPLO 5. Factorizar $2^{11}-1$.
Este es un ejemplo de los llamados números de Mersenne, $M_n\;=\;2^n-1$ .y el primero para el cual siendo *n* primo M_n es compuesto. La cacería de números primos de Mersenne se ha extendido a nivel global dando como resultado el hallazgo de los mayores primos conocidos.

---

[11] Este número tiene una historia curiosa, principalmente porque el matemático inglés Godfrey Harold Hardy, según una conocida anécdota, le atribuye a Srinivasa Ramanujan la afirmación de que 1729 es un número muy interesante por cuanto que es el primer entero positivo que se puede expresar como la suma de dos cubos en dos formas diferentes. Ver mi artículo *Srinivasa Ramanujan* en: http://www.matematicasyfilosofiaenelaula.info/historiam.htm.

$2^{11}-1 = 2047 = x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1 = x^{10}+x^8+x^7+x^6 + x^8+x^7+x^6+x^5+x^4+x^4+x^5+x^4+x^3+x^2+x+1 = x^6(x^4+x^2+x+1)+ x^4(x^4+x^2+x+1)$ $x^7+x^4+x^5+x^4+x^3+x^2+x+1 = x^6(x^4+x^2+x+1)+x^4(x^4+x^2+x+1)+ x^3(x^4+x^2+x+1)+(x^4+x^2+x+1) = (x^4+x^2+x+1)(x^6+x^4+x^3+1) = 23\times 89.$

La diferencia entre la factorización aritmética usual y la que presentamos en los ejemplos anteriores está en que aquí no efectuamos división alguna, todo el proceso es algebraico, las manipulaciones que se llevan a cabo están sustentadas en la aritmética binaria y en general las propiedades de los polinomios se cumplen, excepto algunas, entre ellas el hecho de que el polinomio,

$$\sum_{i=0}^{i=n} x^{n-i} = x^n + x^{n-1} + \ldots + x^2 + x + 1$$

No es factorizable en K[x], donde K es un cuerpo arbitrario, pero si lo es en ciertos casos, en la aritmética binaria como lo vimos con

$2^{11}-1 = x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1 = (x^4+x^2+x+1)(x^6+x^4+x^3+1).$

EJEMPLO 6. Factorizar $2^{32}+1$. Este es el primer número de Fermat que no es primo. Los llamados primos de Fermat tienen la forma

$$\mathrm{F}(n) = 2^{2^n}+1$$

Y son primos para n = 0, 1, 2, 3, 4. Leonhard Euler mostró que F(5) = 4294967297 = 641×6700417.

Para simplificar la escritura de los números que entran en juego en la demostración, supongamos que: $a = 2^7$, b = 5; y así $a-b^3 = 3$, $2^4 = 1+3b$. Entonces

$2^{32}+1 = (2\times 2^7)^4+1 = 2^4a^4+1 = (1+3b)a^4+1 = [1 + (a-b^3)b]a^4 + 1 = a^4 + a^5b+1-a^4b^4 = a^4(1+ab)+(1-a^2b^2)(1+a^2b^2) = a^4(1+ab)+(1-ab)(1+ab)(1+a^2b^2) = (ab+1)[a^4+(1-ab)(1+a^2b^2)]$.

Esto prueba que $ab + 1 = 2^7\times 5+1 = 641$ divide a $2^{32}+1$. Esto traducido a lenguaje binario es:

$x^{32}+1 = [x^7(x^2+1) + 1][x^{28}+(1\text{-}x^7(x^2+1))(1 + x^{14}(x^2+1)^2)] = (x^9+x^7+1)[x^{28}+(1-x^9-x^7)(x^{18}+x^{17}+x^{14}+1)]$.

Un ejercicio de rutina muestra que el último producto da $x^{32}+1$.

Las operaciones básicas de la aritmética se pueden llevar a cabo sin mayor dificultad, incluyendo los consabidos algoritmos para la multiplicación y la división, cuyo aprendizaje ofrece tanta dificultad a los niños. La ventaja sobre el método convencional es que en el sistema binario las opciones de selección son mínimas cuando tratamos el caso de la división, como lo veremos en el siguiente ejemplo.

EJEMPLO 7. Dividir 2047 entre 89, usando sistema binario.

Se trata de hallar el cociente de $x^{11} - 1$ y $x^6 + x^4 + x^3 + 1$. Parodiando el método que nos enseñaron en el álgebra del bachillerato y recordando las propiedades de los polinomios binarios, encontramos,

$$
\begin{array}{l|l}
x^{11} \qquad\qquad\qquad\qquad - 1 & x^6 + x^4 + x^3 + 1. \\ \cline{2-2}
\underline{- x^{10} - x^8 - x^7 - x^4} & x^4 + x^2 + x + 1 \\
\quad x^9 + x^6 + x^5 + x^4 - 1 & \\
\quad \underline{- x^8 - x^6 - x^5 - x^2} & \\
\qquad x^8 + x^3 + x^2 - 1 & \\
\qquad \underline{- x^7 - x^5 - x^4 - x} & \\
\qquad\quad x^6 + x^4 + x^3 + 1 & \\
\qquad\quad \underline{- x^6 - x^4 - x^3 - 1} & \\
\qquad\qquad\quad 0 &
\end{array}
$$

Lo que nos da que $x^{11} - 1 = (x^6 + x^4 + x^3 + 1)(x^4 + x^2 + x + 1)$.

Los ejemplos anteriores nos llevan a proponer la idea de trabajar en los primeros años de la escuela primaria el concepto de número ligado al concepto de polinomio y el estudio de los números primos en consonancia con la primalidad de los polinomios asociados a los números. La factorización de números está muy ligada a la criptografía, la ciencia relacionada con la encriptación de la información. Por lo tanto dar importancia a la teoría elemental de números es acercarnos a las matemáticas de nuestro tiempo y a reducir la brecha entre las matemáticas avanzadas y la enseñanza elemental de las mismas.

El propósito de este trabajo ha sido mostrar que algunos temas que hoy se estudian en la escuela secundaria es posible llevarlos a la educación primaria enfatizando más en las razones que soportan las matemáticas, que en las aplicaciones rutinarias de las mismas, hoy dejadas a las máquinas. Queda mucho por decir y argumentar en torno a la necesidad de dar un vuelco a la educación matemática a fin de ponerla a tono con las nuevas tendencias culturales y científicas de la humanidad y de acercarla a las fronteras del desarrollo matemático de nuestro tiempo.

Armenia, Colombia, Diciembre de 2010