A propósito del último teorema de Fermat[1]

"... vibrando y forcejeando,...
acaba por ser todos los guarismos,
la vida entera".

César Vallejo, *Trilce*

Aroldo Kaplan

Verdaderas, concisas, irrelevantes, se ha dicho de las proposiciones de la matemática pura. ¿Podría haber mejor ejemplo que el así llamado Ultimo Teorema de Fermat? Enunciado alrededor de 1637 es, como veremos más abajo, en verdad *conciso*. Demostrarlo *verdadero,* sin embargo, es todo lo contrario. El último eslabón del argumento, completado por Andrew Wiles en lo que sin duda constituyó el acontecimiento matemático de los últimos años, ocupa cientos de páginas. Los eslabones previos ocupan varios cientos más y allí se entretejen ideas profundas y sutiles provenientes de las áreas más diversas de la matemática clásica y moderna. Aquí confiaremos en el rigor intelectual de Wiles y de los demás especialistas que hasta ahora han escrutado el argumento y que invitan a aceptarlo como válido.[2]

Lo de irrelevante —para el pensamiento y la cultura en general— será el tema principal de nuestra discusión.

FERMAT Y SU TEOREMA

Pierre de Fermat, abogado, matemático y poeta francés del siglo XVII, dejó escritos una serie de enunciados sobre Teoría de Números, aseverándolos como verdaderos pero cuidándose de no dejar indicios sobre sus razones, es decir, sin incluir las correspondientes demostraciones. Negándose por principio a publicar sus resultados en la manera y medios habituales, los mismos quedaron registrados en su prolífica correspondencia y en el margen de los

Aroldo Kaplan es
Profesor Titular del Departamento
de Matemáticas de la Universidad
de Massachusets en Hamherst.

libros que usaba como fuentes.

Luego de la publicación póstuma de sus escritos en 1670, la profundidad de los teoremas de Fermat fue rápidamente reconocida por los especialistas de la época, especialmente por Euler. El trabajo de producir, o re-producir, sus demostraciones, o de algunas veces hallarlos falsos, fue fuente de inspiración para varias generaciones de matemáticos, así como origen de fértiles teorías.

Hacia principios del siglo XIX los Teoremas de Fermat habían sido convincentemente probados en su totalidad, con la sola excepción que nos ocupa: de ahí lo de "Ultimo". Este estimuló a varias generaciones de matemáticos, impulsando el desarrollo de nuevas teorías que, además de aplicarse a la resolución de casos particulares del Teorema, pronto hallaron uso en otros ámbitos. Finalmente, la introducción de profundas ideas también de otros campos (Geometría, Teoría de Grupos, la "Filosofía" de Langlands), facilitó la síntesis de Wiles.

El Teorema en cuestión fue enunciado por Fermat a propósito de las así llamadas ternas pitagóricas: ternas de números enteros x, y, z, tales que al sumar los cuadrados de los dos primeros se obtiene el cuadrado del tercero. En otras palabras, tales que satisfacen la ecuación

$$x^2 + y^2 = z^2$$

Por ejemplo 3, 4, 5 forman tal terna, porque

$$3^2 + 4^2 = 9 + 16 = 25 = 5^2$$

Otra terna pitagórica es 5, 12, 13 así como 4961, 6480, 8161. Leyendo a Diofanto (siglo III) dar el método de producirlas todas,[3] Fermat anota en el margen, en latín, "... por el contrario, no es posible descomponer un cubo como suma de dos cubos, o un bicuadrado en suma de dos bicuadrados, o cualquier otra potencia como suma de otras dos de las mismas potencias".[4] Es decir, piensa a la ecuación de arriba como expresando que algunos cuadrados de números enteros —digamos 5^2— pueden descomponerse como suma de otros dos de tales cuadrados —3^2 y 4^2 en el ejemplo— y pasa

1. Versión de la conferencia "El Ultimo Teorema de Fermat y el fin de las matemáticas puras", dictada en ocasión del X aniversario de la Facultad de Matemática, Astronomía y Física, Universidad Nacional de Córdoba, julio 1993.

2. Andrew Wiles, profesor de la Universidad de Princeton, presentó una prueba del teorema. La misma estaba, a principios de 1994, aún en proceso de revisión y completación.

3. Es fácil ver que para *cualquier* par de números enteros p, q, la terna de números $x=4pq$, $y=P^2 - q^2$, $z=p^2+q^2$, es pitagórica. El Teorema en Diofanto afirmaba que *toda* terna pitagórica debe ser un múltiplo de una de éstas. Alguna forma de este principio debía ser conocida por los babilonios hace tres mil quinientos años, ya que fueron capaces de producir ejemplos como 4961, 6480, 8161.

4. Y continúa Fermat: "He descubierto una hermosa demostración de esta proposición, aunque este margen resulte demasiado estrecho para detallarla".

a afirmar que las correspondientes descomposiciones para exponentes más grandes, como $x^3 + y^3 = z^3$, $x^4 + y^4 = z^4$, $x^5 + y^5 = z^5$, etcétera, son imposibles, siempre. En breve, que ninguna ecuación de la forma

$$x^n + y^n = z^n$$

puede tener soluciones enteras cuando el exponente n es mayor que dos —salvo, por supuesto, las soluciones : "triviales", donde uno de los tres enteros es cero.

El problema está evidentemente fuera del alcance de la computación bruta, ya que es *a-priori* imposible verificar caso por caso la afirmación de que para todos los números x, y, z, n, distintos de cero y con $n>2$, el número z^n será distinto del número $x^n + y^n$. Es necesario, en cambio, argumentar "en abstracto", mostrando, por ejemplo, que la hipótesis de que una solución existe lleva necesariamente a una contradicción. Para algunos exponentes es posible llevar esto a cabo con métodos relativamente elementales,[5] seguramente conocidos por Fermat —aunque su convicción en la validez general del enunciado probablemente se basaba en un error. Hasta hace poco, mediante el uso de una formidable artillería teórica, se había conseguido demostrar el Ultimo Teorema en muchos casos particulares, incluyendo a todo exponente n menor que cuatro millones, y a todas las ternas de números x, y, z, menores que 10^{10^6}, es decir ¡un uno seguido de un millón de ceros!

Pero, por abismales que sean estos guarismos, insiste el imperativo matemático, ¿qué son comparados con las infinitas posibilidades restantes? Al fin y el cabo, si bien 10^{10^6} es probablemente mucho mayor que el número total de partículas elementales en el universo, también es inmensamente menor que la cantidad de posibles *conjuntos* formables con las mismas. Un resultado tal como "el Ultimo Teorema de Fermat es cierto para todo exponente menor que 10^{10^6}" suena insatisfactorio para el oído matemático, como una sinfonía inconclusa cuyos últimos acordes quizás esconden la clave. La detección de algún exponente gigantesco para el cual un tal Teorema falle o la demostración completamente general del mismo, tiene frecuentemente más consecuencias para el resto de la Teoría que la seguridad de saberlo cierto para los primeros treinta y tres trillones trescientos treinta y tres exponentes.

5. Por ejemplo, si n es múltiplo de 4, la existencia de una solución no trivial de la ecuación $x^n + y^n = z^n$ implica la existencia de otra para $x^4 + y^4 = z^4$. Los cuadrados x^2, y^2, z^2, serán entonces una terna pitagórica. Reduciendo al caso en que x, y, z, son positivos y coprimos, y utilizando la descripción de tales ternas en la nota anterior, se construye otra solución similar pero cuyo "z" es menor que el anterior. Esto es imposible, ya que tal proceso (de "descenso" como lo llamaba Fermat) no puede continuar indefinidamente.

NUMEROS: METAFISICA

El Ultimo Teorema de Fermat pertenece a lo que habitualmente se denomina Teoría de Números, que trata específicamente de las propiedades de los números naturales: 1, 2, 3, ..., y de las ecuaciones satisfechas por los mismos.

Estos son los que primero aparecen, tanto histórica como cognitivamente, y que, en diversos sentidos, generan eventualmente a todos los demás (enteros, racionales, reales, complejos, modulares, p-ádicos...).

¿Qué son los números naturales? Entidades a la vez obvias y elusivas, objeto de uso e interés en la ciencia y en la mística, la finanza y la filosofía... ¿Qué constituye su Teoría? ¿Es posible explicar su trascendencia "apriorísticamente", recurriendo a las posibles aplicaciones sólo como confirmación ulterior de su necesidad? En efecto, argumentaremos aquí que la Teoría de Números debería considerarse como la verdadera *Ciencia de la Distinción Fundamental.*

La distinción en cuestión es la encarnada en las oposiciones sujeto-predicado, sustantivo-adjetivo, objeto-propiedad, elemento-conjunto. La atribución de significado a las afirmaciones del tipo "tal cosa tiene tal propiedad", o "tal objeto pertenece a tal conjunto", es tan característica del lenguaje y el entendimiento humanos, que esta afirmación puede pecar de trivial. Insistimos que hablar de predicados o propiedades es esencialmente equivalente a hablar de conjuntos o clases. Enunciar una propiedad dada es lógicamente equivalente a describir su rango, es decir, el conjunto de objetos que la poseen. Asimismo, todo conjunto corresponde a una propiedad —la de pertenecer a ese conjunto. Para mantenernos en lo primitivo y evitar problemas lógicos, consideraremos en principio sólo conjuntos finitos, correspondientes a propiedades de rango finito, es decir, predicables, a lo más de una cantidad finita de objetos (aunque ésta pueda ser arbitrariamente grande, dependiendo de la propiedad de que se trate). Las ciencias —exactas o no, exceptuando quizás a la matemática— no verían aquí una limitación demasiado grande.

Como primer paso hacia la consitución de la ciencia de esta distinción fundamental, cabe preguntarse: ¿qué propiedades tienen, en cuanto tales, los conjuntos finitos? Es decir, ¿qué propiedades *absolutas* tienen, lo más independientes posibles de la naturaleza de los objetos que las satisfacen?

La búsqueda de propiedades absolutas —invariantes— del mundo es característica de las ciencias, pero cada una restringe su atención a ciertos objetos, a ciertos predicados, y formula leyes invariantes por ciertas transformaciones particulares entre objetos o conjuntos. La Antropología, la Lingüística, la Física, en tanto ciencias, se interesan por leyes generales —no proposiciones aisladas sobre los tabúes de una única familia polinesia, o sobre el núcleo de un determinado átomo de hidrógeno. Al mismo tiempo, el valor de este imperativo de generalidad depende de la misma particularidad de los enunciados científicos: una buena ley lingüística sobre, digamos, la sintaxis de verbos, será invariante si se sustituye un verbo por otro cualquiera o si se traduce a otro lenguaje, pero no si un verbo se sustituye por un sustantivo o por un protón.

Aquí, en cambio, nos estamos preguntando por los "absolutos en serio". No restringimos la naturaleza de los objetos o de las propiedades a considerar, ¡y requerimos la invariancia por *toda* transformación de unos objetos en otros! ¿Queda algo?

Lo que queda —lo único— luego de tamaña limpieza conceptual, es la *cardinalidad* de un conjunto, en el siguiente sentido. En vez de cosificar a ésta como "el número" de elementos del conjunto, lo que nos devolvería a la pregunta inicial, consideramos a la cardinalidad como una *propiedad* de conjuntos, a saber aquella que hace que un conjunto dado se pueda poner en correspondencia biunívoca con algunos conjuntos pero no con otros.

Notemos que para determinar si dos conjuntos finitos A y B pueden ponerse en correspondencia biunívoca, no hace falta saber contar: basta asignarle a cada elemento de A un elemento bien especificado de B, de manera que todo elemento de B resulte asignado a un único elemento de A. Si esto es posible, decimos que A y B "son equivalentes" o que tienen "la misma cardinalidad", o "el mismo número de elementos". Recién después, si queremos, diremos qué significa por ejemplo, "tener cinco elementos": significa, digamos, que tienen la misma cardinalidad que el siguiente conjunto de símbolos:

@ # % * &

Así, el problema de la "naturaleza" de los números se esfuma de manera parecida a la del calor, al reconocer a éste como una propiedad de —en vez de una substancia en— los cuerpos. Pensaremos entonces a los números como las únicas propiedades absolutas de los conjuntos finitos —absolutas en el sentido de ser invariantes por toda sustitución de elementos por otros o, equivalentemente, independientes de la naturaleza específica de los elementos que los constituyen.

NUMEROS: FISICA

Si los conjuntos finitos de elementos arbitrarios, o los predicados de rango finito, constituyen nuestro tema, la verdadera Ciencia de los mismos debería identificarse con el estudio de las relaciones, u operaciones, también invariantes, que se pueden establecer entre los mismos. Que esta identificación no siempre se aplique en otras ciencias se debe a que los ámbitos y requerimientos de invariancia nunca son formulables tan simple y exhaustivamente como en nuestro caso.

Curiosamente, la Teoría de Conjuntos usual, o de Predicados, *no* satisface nuestros requerimientos. De las tres operaciones básicas: complemento, unión, intersección —o, para predicados, negación, disyunción, conjunción—, la primera no se aplica en nuestro contexto (el complemento de un conjunto finito no necesariamente es un conjunto finito) mientras que las otras dos no satisfacen el requerimiento de invariancia. En efecto, el que la unión o intersección de un par de conjuntos A y B sea o no equivalente a la unión o intersección de otro par, A' y B', depende de la naturaleza de los objetos que los constituyen, en la medida en que éste determina cuántos elementos comunes tiene cada par. El principio de invariancia absoluta requeriría que cada vez que A sea equivalente a A', y B a B', $A \cup B$ resulte equivalente a $A' \cup B'$, y $A \cap B$ a $A' \cap B'$, lo cual es evidentemente falso. En términos más pedestres: el número de elementos en la unión o intersección de dos conujuntos depende de los elementos que ambos tengan en común, no sólo del número de elementos en cada uno.

Un ejemplo de operación entre conjuntos finitos que es en cambio absolutamente invariante, es el *producto cartesiano* A x B, definido como el conjunto de pares ordenados (a,b) formados por un primer elemento de A y uno segundo de B. Otro ejemplo es lo que podemos pensar como *unión disjunta* A + B de dos conuntos, describible fijando dos objetos distinguidos o_1, o_2, distintos entre sí (arquetipos de "diferencia") y definiendo

$$A \oplus B = (A \otimes \{o_1\}) \cup (B \otimes \{o_2\})$$

Estas operaciones carecen de las propiedades formales habituales; por ejemplo, no son conmutativas, como lo son la unión e intersección. Sin embargo, poseen la invariancia deseada: si A es equivalente a A', y B es equivalente a B', entonces A + B resulta equivalente a A' + B', y A x B a A' x B'. En términos pedestres, la cardinalidad del producto cartesiano es siempre el producto aritmético (multiplicación) de las cardinalidades de los factores, mientras que la cardinalidad de la unión disjunta es siempre la suma aritmética de las cardinalidades de cada término.[6]

No es extraño que las operaciones aritméticas usuales broten espontáneamente del requerimiento de invariancia. Si el número de elementos de un conjunto es su único invariante absoluto, la Ciencia de los conjuntos, como estudio de las relaciones invariantes que se pueden establecer entre los mismos, debería reducirse precisamente al estudio de las propiedades de esos invariantes, es decir, de los números naturales.

En efecto, es posible describir exactamente las relaciones entre conjun-

6. (i) Un par ordenado es no sólo un conjunto de dos elementos. El orden de los mismos también se toma en cuenta: cuál es el primero y cuál es el segundo. Por ejemplo con el par de números 3, 8 podemos considerar dos —distintos— pares ordenados (3, 8) y (8, 3).
(ii) La *unión disjunta,* como lo sugiere el nombre, es una construcción de un nuevo conjunto a partir de dos datos A, B que "ignora" la intersección $A \cap B$. El recurso técnico, —elegir dos objetos distintos o_1, o_2— permite usar un conjunto, el de todos los pares ordenados (a, o_1) con a en A que es esencialmente una "copia" de A y, análogamente, todos los pares (b, o_2). Como nunca puede ocurrir que $(a_1, o_1) = (b, o_2)$ —porque $o_1 \neq o_2$— no hay elementos en la intersección de las copias de A y B. Piensen por ejemplo que si a tiene 5 elementos y B tiene 7 elementos y si hay 4 elementos en la intersección, entonces $A \cup B$ tiene 8 elementos. Pero $A \oplus B$ tiene 12 = 5 + 7

tos finitos que satisfacen el requerimiento de invariancia. Son todas de la forma general "el conjunto construido de tal manera, a partir de tales conjuntos, mediante las operaciones de producto cartesiano y unión disjunta, es equivalente a aquél construido de tal otra manera a partir de tales otros conjuntos". En términos de nuestros invariantes, estas relaciones serán las describibles mediante ecuaciones entre variables numéricas naturales, ligadas por la suma y el producto. Por ejemplo, el que la ecuación $x^2 + y^2 = z^2$ tenga infinitas soluciones naturales, y el que $x^3 + y^3 = z^3$ no tenga ninguna, son típicos ejemplos de tales proposiciones.[7]

La verdadera "Teoría de Conjuntos", entonces, debería ser ni más ni menos, la venerable Teoría de Números, específicamente el estudio de las Ecuaciones Diofánticas: ecuaciones de la forma P=Q, donde P y Q son polinomios a coeficientes naturales —o enteros— en variables naturales. Describir las propiedades de las soluciones de sistemas de ecuaciones diofánticas,[8] aparece ahora como un imperativo epistemológico primario. Desde este punto de vista, el Ultimo Teorema de Fermat resulta importante como parte de tal empresa, no tanto por la forma particular de la ecuación involucrada.

TEORIA Y REALIDAD

El que los números naturales surjan "vibrando y forcejeando" en tantos dominios humanos, no constituye ahora ninguna sorpresa, ya que son las únicas propiedades invariantes de la noción más básica.

De acuerdo a lo que hemos visto, el que las operaciones aritméticas de suma y producto, y sus propiedades más elementales también surjan así, tampoco sorprende.

El misterio ahora parece ser por qué la Teoría de Números "superior", no "surge" más de lo que parece hacerlo, siendo "la única ciencia de lo más fundamental". Una posible respuesta es que el desarrollo de proyectos intelectuales hasta sus últimas consecuencias no es necesariamente productivo: frecuentemente es una exageración. Los mismos practicantes de este arte tienden a compartir variantes más o menos arrogantes de esta actitud, explicando que trabajan en Teoría de Números "así cuando les pregunten por la utilidad práctica de lo que hacen, pueden contestar sin miedo a equivocarse: ninguna"; o, más rimbombantemente, "sólo por el honor del espíritu humano". En efecto, dentro de las matemáticas, la Teoría de

7. Para visualizar "conjuntísticamente" lo que afirman estas dos ecuaciones, notemos que, por ejemplo, x^2 es el número de objetos en un cuadrado de objetos con x objetos por lado. Las soluciones a la primera ecuación corresponden ahora a cuadrados de objetos que son unión disjunta de otros dos cuadrados, mientras que la no solubilidad de la segunda significa que un cubo de objetos no puede ser unión disjunta de otros dos.

8. Esto se haría en una verdadera geometría analítica "natural" (la usual es "real").

Números ha sido siempre un paradigma de lo irremediablemente inaplicable. Siendo lo más puro de las matemáticas puras, explicar cuál puede ser su impacto-en-el-mundo implica necesariamente hacerlo para todas éstas.

Este acoplamiento en realidad contribuye a dar una respuesta parcial a nuestra preocupación. En primer lugar la interacción entre la Teoría de Números "superior" y el resto de las matemáticas puras no es puesta en duda, desde que se le incorporaron las técnicas del análisis infinitesimal en el siglo XVIII, e impulsó el desarrollo de buena parte del Algebra Moderna. Y ahora menos que nunca, ya que los trabajos de Wiles citados arriba aparecen como corolarios de teorías y métodos mucho más emparentados con la Física-Matemática que con los abstractos enunciados de la Teoría de Números. Las matemáticas constituyen hoy un cuerpo orgánico en el cual es difícil o contraproducente separar conceptual y pedagógicamente unos temas de otros: el Algebra del Análisis, la Geometría de la Teoría de Números, lo puro de lo aplicado. Para existir y ser efectiva, necesita del desarrollo armónico y desprejuiciado de sus partes. Su notable rol modelador es cada vez más evidente: geometría y teoría de grupos en física, análisis en tomografía, sistemas dinámicos en fisiología y meteorología, teoría de nudos en biología y física, lógica matemática en informática, *ondelettes* en la reproducción musical y en comunicaciones, ... La Teoría de Números, en tanto parte de ese cuerpo orgánico, hereda al menos algo de la responsabilidad por este contemporáneo reencuentro entre lo imaginario y lo real. Junto con su rol pedagógico, esto era todo lo que se podía decir en favor de la relevancia de esta Teoría. Pero por suficientes que sean estos argumentos para calmar las preocupaciones éticas de algunos practicantes o para fundamentar proyectos de investigación, admitamos que se quedan algo cortos. Esperaríamos que una única teoría de lo más fundamental se hiciese sentir un poco mejor que eso, que sus ecos fuesen más obvios y más allá de lo meramente tecnológico.

CODIGOS

Consideremos un texto cualquiera en un lenguaje cualquiera (natural, genético-molecular, musical o digitalmente telecomunicado) como una sucesión de objetos básicos (letras), tomadas de un conjunto finito (alfabeto), estructuradas en trozos (palabras), tomados de un conjunto finito (léxico).

Textos en lenguajes sofisticados, como los de los tres primeros ejemplos, poseerán órdenes adicionales de organización: gramaticales, sintácticos, literarios. Todas estas estructuras, responsables de la efectividad de un lenguaje para codificar o transmitir mensajes y de su capacidad de significación, son frecuentemente formulables en término de sustituciones, amalgamientos e invariancia que parecen estar sólo unos escalones más allá de los aplicables a los conjuntos finitos. Entonces, es quizás en estos ámbitos donde deberían escucharse aquellos ecos.

La Teoría Matemática de Códigos trata de los sistemas formales de codificación usados en ingeniería para la transmisión y el procesamiento de información. El tema fundamental, un código, no es más que lo que arriba llamamos léxico. ¿Qué podrá decir una lingüística así de empobrecida, que voluntariamente ignora todo "contexto"? En la práctica importan ciertos parámetros específicos del léxico: su riqueza, que determina su densidad informativa potencial; la facilidad con que se detectan errores en un texto; su eficiencia para ser (o no) decodificado. Estos parámetros son frecuentemente antagónicos; por ejemplo, mientras más rico sea el léxico, mayor será la probabilidad de que un error cambie una palabra por otra igualmente permitida y, por lo tanto, sea indetectable. El problema fundamental de la Teoría de Códigos es encontrar los que optimizan adecuadamente a tales parámetros.

Los mejores códigos construidos hasta ahora están basados en la aritmética modular. En estos casos el alfabeto consiste de un número primo de símbolos (o una potencia de un primo). La elección de código, o léxico de palabras admisibles, explota la estructura aritmética inherente en un tal alfabeto, de la siguiente manera. Identificando a un alfabeto de q letras con la lista de números

$$Fq = 0, 1, 2, \ldots, q\text{-}1$$

bajo las operaciones de "suma y producto módulo q", en las cuales se reemplaza el resultado de las operaciones usuales por el resto de su división por q, el alfabeto Fq constituye un *cuerpo*. Esta estructura algebraica, formalmente similar a la de los números reales, aunque finita, permite pensar a Fq como una "recta", y a las posibles palabras de una longitud n dada, como puntos del espacio multidimensional Fq^n, producto cartesiano n copias de Fq consigo mismo.[9] Así un código deviene un subconjunto arbitrario de un tal espacio.

Esta matematización no es en vano: si se elige el código en forma geométricamente natural —por ejemplo, como una recta o un objeto geométrico más general de Fq^n— los parámetros relevantes en comunicación resultan expresables en término de invariantes geométrico-aritméticos del objeto correspondiente. La teoría de estos invariantes ya existe: denominada "geometría algebraica sobre cuerpos finitos", ha sido un área activa de investigación por más de un siglo, sin aparente motivación externa. En los casos más elementales, el código consiste de todas las palabras de la forma

$$(f(P1), f(p2), \ldots, f(Pk))$$

9. Esto es análogo a la conocida identificación de la recta con los números reales y a la construcción de sistemas de coordenadas en el plano o el espacio. Ver, por ejemplo, H. Alagia, "Números y Utopías", *Estudios*, Número 1, Córdoba, 1993, págs. 73-74.

donde f es un polinomio arbitrario con coeficientes en Fq, de grado fijo, y P1, P2,..., Pk, son elementos fijos de Fq. Estos, o variantes de éstos, están detrás de mucha de la tecnología corriente —la de discos compactos, por ejemplo. Ya aquí la Teoría de Números superior resulta esencial, al menos en sus aspectos más clásicos.[10]

Pero son los códigos, basados en los aspectos más sutiles de la Teoría, los que recientemente han causado especial sensación, por lo inesperado de su eficiencia. Denominados "algebro-geométricos", optimizan los parámetros de relevancia comunicacional mucho más allá de lo que se consideraba eran sus barreras naturales.[11] En los mismos, las palabras todavía poseen la forma general señalada arriba, pero los polinomios (funciones sobre la "recta" Fq) son reemplazados por funciones meromorfas sobre variedades análogas a las superficies de Riemann, pero modeladas sobre la clausura algebraica del cuerpo Fq (en vez de la del cuerpo real). Los p_i pasan a ser ciertas colecciones de puntos ("divisores racionales") en esas variedades.

Aquí sí que estamos en el ámbito de la verdadera Teoría de Números, de sus partes más sofisticadas. Los problemas matemáticos de los que se trata están, tanto en sus aspectos generales como en los detalles más específicos, muy cerca de los involucrados en los trabajos de Wiles. También lo están de aquellos que brotan ahora en Física, en los modelos "sigma-no lineales" de gravitación cuántica. Gran parte de estos problemas comunes tienen que ver con la abundancia de puntos, divisores, o subvariedades racionales en variedades algebraicas convenientes (curvas elípticas o algebraicas, variedades de Calabi-Yau) sobre distintos cuerpos.

Esto en cuanto a los ecos.

Para las otras insatisfacciones mencionadas habría que mirar a estructuras más finas, contextuales. Señalemos que aun en las cuestiones de los parámetros elementales de la teoría de códigos, el papel del contexto puede ser crucial tanto para decodificar la información (o para ocultarla) como para la capacidad correctiva. Al aumentar el grado de complejidad, el papel del contexto, de la sintaxis es todavía más obvio.

Desde el punto de vista bio-evolutivo, D. Bickerton[12] nos señala estas diferencias de complejidad y apunta a sus consecuencias: "Un vocabulario rico y sutilmente estructurado podría haber resultado suficiente para representar a nuestro entorno y a todo lo que pensáramos que el mismo pudiese contener. Pero si íbamos a poder intercambiar entre nosotros esas repre-

10. En la práctica las palabras del código o léxico se transmiten a través de un canal a un receptor. Pero el canal es "ruidoso": si una palabra p es enviada, normalmente se recibe otra palabra q diferente de p (digamos: "la señal recibida es una deformación de la señal emitida"). El problema ingenieril que se plantea es cómo corregir estos errores para mejorar el mensaje. Para algunos detalles matemáticos ver *Bulletin Am. Math. Soc.*, vol. 27, Número 2, pág. 306 (1992).

11. Por ejemplo la cota de Gilbert-Varshamov, que provee una estimación del tamaño de un código.

12. "Language and Species", U. of Chicago Press, 1990 (Traducción del autor).

sentaciones... con el correspondiente y vasto incremento de capacidad cognitiva que conlleva el poder manipular y transmitir nuestros pensamientos, ... todo esto sin tener que reflexionar un instante sobre 'cómo' hacerlo, entonces la triple estructura derivada de la Predicabilidad, la Gramatización y la Sintaxis (la más importante de las cuales es la Sintaxis) era esencial. No importa cuán rico fuese el vocabulario, esos pensamientos no podrían haberse constituido sin la presencia de un sistema específico para organizarlos".

Nada nos impide especular sobre la matemática que se revelará en el estudio de las estructuras profundas del lenguaje y sobre cuán importante será para resolver el misterio del origen de este último. Sería un buen destino para esa teoría de la distinción fundamental llegar a ser ya más que "todos los guarismos, la vida entera".