La Matemática: Definiciones y Modelos

Lección inaugural del
curso académico 2005-2006
pronunciada por el

Excmo. Sr. D. Julio P. Lafuente López

Catedrático de la Universidad Pública de Navarra

Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

upna Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

La Matemática: Definiciones y Modelos

Lección inaugural del curso académico 2005-2006
pronunciada por el
Excmo. Sr. D. Julio P. Lafuente López
Catedrático de la Universidad Pública de Navarra

Matematika: Definizioak eta Ereduak
2005-2006 ikasturteko hasierako irakasgaia, Nafarroako
Unibertsitate Publikoko Katedraduna den
Julio P. Lafuente Lopez emanda

Julio P. Lafuente López
Catedrático de la Universidad Pública de Navarra

La Matemática: Definiciones y Modelos.

Julio P. Lafuente López

Excelentísimo Sr. Rector Magnífico;

Excelentísimo Sr. Presidente del Gobierno de Navarra;

Excelentísimo Sr. Presidente de las Cortes de Navarra;

Excelentísimas e Ilustrísimas Autoridades;

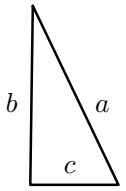
Miembros de la Comunidad Universitaria;

Señoras y Señores:

Si uno considera la duración promedio de la vida académica de un profesor y el número de profesores de una universidad, inmediatamente se da cuenta de que no es fácil ser el encargado de pronunciar la lección inaugural en esa universidad (o en cualquier otra) y que, méritos académicos aparte, suele venir propiciada por una ya (¡ay!) dilatada trayectoria vital (suponiendo una situación de normalidad universitaria, en la que se siguen los tradicionales criterios de ordenación académica y no coyunturas clientelistas, que de todo hay). Recuerdo las primeras aperturas de curso a las que asistí en mi universidad de origen, la de Zaragoza, recién ingresado en el mundo docente e investigador; sentía no poca admiración por aquellos venerables catedráticos que nos soltaban aquellas sesudas conferencias. Bien es verdad que, poco a poco, ya no me fueron pareciendo tan mayores; de hecho, progresivamente, fueron siendo gente joven, más o menos de mi edad. *Tempus fugit*. Sea como sea es un gran honor ser el encargado de dictar la lección inaugural del curso 2005-2006 en esta mi universidad, la Universidad Pública de Navarra.

Y siendo tan singular la ocasión, no me pareció del todo inoportuna la idea de aprovecharla para transmitir algunos aspectos de mi labor investigadora. Siempre he tropezado con dificultades para explicar mi trabajo de profesor universitario. He comprobado que, salvo en este ámbito, se identifica con la labor docente; se nota en que, por ejemplo, cuando ha finalizado la época de exámenes, cualquiera te dice, con no poca envidia, "Qué bien, ¿eh?, ya de vacaciones". Intentas explicar que, en realidad, no es así, que parte esencial de tu trabajo es la investigación y que, de hecho, esa parte se ve incrementada y favorecida muy notablemente cuando los alumnos están de vacaciones. Tras una primera reacción de perplejidad suele venir la pregunta: "Pero tú eres matemático, ¿no?, ¿qué es eso de investigar en

matemáticas?" (supongo que porque no te ven, con razón, con probetas o con microscopios; puedes paliar la reacción si previamente mencionas que hoy es necesario el uso de sofisticados programas informáticos y, en consecuencia, de laboratorios en los que los aparatos son ordenadores; aunque la fuerza de este argumento, sobre la faceta experimental de nuestro trabajo, debe de ser exigua: no parece hacer demasiada mella, a la hora de reconocerla, en nuestras autoridades académicas). Me ha dado un cierto resultado, en ocasiones, apelar al Teorema de Pitágoras, ya saben: En un triángulo rectángulo, el cuadrado de la hipotenusa es igual a la suma de los cuadrados de los catetos. (El ejemplo lo encuentro particularmente apañado porque, al llevar el nombre de Teorema, suena a algo inequívocamente matemático y, también, porque hasta para aquellos que, simultánea y sorprendentemente, presumen de cultos y de no saber absolutamente nada de matemáticas, les resulta incómodo manifestar que lo ignoran.) Pues bien, Pitágoras (su escuela)[1], descubrió la validez de ese enunciado tras una labor de investigación. Y sigue habiendo en matemáticas preguntas por contestar, fórmulas por descubrir, relaciones por establecer, y a eso nos dedicamos los que investigamos en matemáticas.



El Teorema de Pitágoras

$$a^2 = b^2 + c^2$$

Los problemas por resolver surgen, por un lado, de otras disciplinas. Tenemos la tendencia a no valorar aquello a lo que estamos acostumbrados, en este caso, a que las matemáticas resuelven muchos problemas en prácticamente cualquier campo del quehacer humano. Pero, si nos paramos a pensar, enseguida nos damos cuenta de que no tendría por qué ser así. Wigner publica un artículo[2] titulado, directamente, "La irrazonable eficacia de las matemáticas en las ciencias naturales", donde se resalta que "la enorme utilidad de las matemáticas en las ciencias naturales es algo que bordea lo misterioso" y que "no hay explicación razonable para ello". Pero es así. Y hoy por hoy no hay prácticamente disciplina que no base al menos algún aspecto de su progreso en alguna rama de las matemáticas.

Por otro lado, la propia Matemática, en su natural desarrollo, plantea problemas, y también a éstos se les dedican notables esfuerzos. Seguramente –ya que, por una vez, los medios de comunicación se hicieron eco de un

[1]Pitágoras de Samos, Samos, ca. 569 aC – Metapontum, ca. 500 aC. Sus discípulos se constituyeron gradualmente en una sociedad o hermandad que fue conocida como la Escuela Pitagórica; sus resultados se atribuyen usualmente a Pitágoras.

[2]E. P. Wigner, The unreasonable effectiveness of mathematics in the natural sciences, *Comm. Pure Appl. Math.* **13**, 1-14 (1960).

avance en Matemáticas– les sonará el llamado "Último Teorema de Fermat". El hijo Samuel de Pierre de Fermat[3] dio a conocer en 1670, entre otros escritos de su padre, que éste había anotado en el margen de una Aritmética de Diofanto[4] su enunciado con la acotación "He encontrado una demostración verdaderamente maravillosa que este margen es demasiado pequeño para contener". Verdaderamente maravillosa[5] debía ser, en efecto, ya que no fue encontrada una demostración hasta 1994 –tras un previo anuncio del año anterior que contenía un error– por Wiles[6]: trescientos veinticuatro años de esfuerzos[7] por parte de muchos de los mejores matemáticos de cada momento, coronados, por fin, con éxito[8]. De otros problemas actualmente planteados se teme que puedan quedar para siempre sin resolver.

Yendo ya a lo que había anunciado, mi labor en investigación, un resultado obtenido con otros colegas muy recientemente:

Teorema. *Sean p un primo impar y G un grupo p-resoluble en el que la clase de un p-subgrupo de Sylow[9] es, a lo más, 2. Sea R un p-subgrupo de G. Si $p = 3$, supongamos, además, que los 2-subgrupos de Sylow de G son abelianos. Entonces los sylowizadores de R en G son conjugados.*

Por ejemplo. Quizás resulte algo abstruso (sin contar con que el estilo pueda parecer pintoresco). Probemos con otro, en el que acaso el lenguaje sea un poco menos críptico, al fin y al cabo se refiere a algo de masivo uso cotidiano en cualquier transmisión de información: los Códigos Correctores de Errores.

---

[3] Pierre de Fermat, Beaumont-de-Lomagne, 17-8-1601 – Castres 12-1-1665. El denominado Último Teorema de Fermat dice: La ecuación $x^n + y^n = z^n$ no posee soluciones enteras x, y, z no nulas cuando $n > 2$. (Para $n = 2$ resulta un caso especial del Teorema de Pitágoras, que sí que tiene soluciones enteras no nulas, por ejemplo, $3^2 + 4^2 = 5^2$. Para los amantes de los enigmas: en una tablilla babilónica de allá por el 1500 aC aparece el caso $4961^2 + 6480^2 = 8161^2$, que no parece que se pueda obtener a base de tanteos.)

[4] Diofanto de Alejandría (Diophanti Alexandrini), 200/214 dC – 284/298 dC). Se considera a Diofanto el padre del Álgebra.

[5] Hoy se cree que la demostración que Fermat dijo encontrar no era tal, sino que contenía un error, que cabría calificar de genial, para el estado de la cuestión en la época, acerca de lo que se denomina hoy factorización única; de todas formas, una seguridad absoluta al respecto nunca podremos tener.

[6] Andrew Wiles, Modular elliptic curves and Fermat's Last Theorem, *Annals of Mathematics*, **141**, 443-551 (1995).

[7] Los esfuerzos dedicados al asunto durante todo ese tiempo no resultaron infructuosos. Propiciaron grandes avances en distintas especialidades matemáticas, particularmente la Teoría de Números y la Teoría de Anillos.

[8] Los matemáticos Chandrashekhar Khare y Jean-Pierre Wintenberger, e, independientemente, Luis Víctor Dieulefait, han anunciado, en abril de este mismo año, una resolución parcial de un importante problema abierto en teoría algebraica de números: la conjetura de Serre, proporcionando de este modo una nueva demostración del último teorema de Fermat, quizá más sencilla que la obtenida por Andrew Wiles.

[9] Peter Ludwig Mejdell Sylow, Oslo, 12-12-1832 – 7-9-1918. En 1872 publica un trabajo de 10 páginas en el que demuestra los hoy conocidos como los tres Teoremas de Sylow. Prácticamente todos los trabajos sobre grupos finitos los utilizan.

Teorema. *Sea C un $[n, k, d]$ código sobre el cuerpo $\mathbb{F}_q$, donde $d \geq 1$, con distribución de pesos $\sum_{i=0}^{n} A_i x^i$. Sea $t \in \mathbb{N}_0$ con $t \leq \frac{d-1}{2}$. Entonces la probabilidad de que una palabra se descodifique erróneamente, desde el punto de vista del emisor, es*

$$\sum_{i=1}^{n} A_i \sum_{j=0}^{t} \sum_{s=0}^{j} \left[\binom{i}{s} \left(\frac{p}{q-1} \right)^{i-s} \left(1 - \frac{p}{q-1} \right)^{s} \binom{n-i}{j-s} p^{j-s} (1-p)^{n-i-j+s} \right]$$

No se inquieten. Enseguida entendí que por cualquiera de estos caminos no debía seguir. Sería por mi parte un uso desconsiderado de mi posición actual, en la que Vds. están relativamente indefensos.

Y es que cualquier tema matemático precisa de una previa comprensión de los conceptos empleados, es decir, de la aprehensión de una serie de definiciones, que puede ser ardua de conseguir. Revisando lo anterior, un *primo* no es aquí el hijo de una tía o de un tío carnal, sino un número natural que sólo es divisible por sí mismo y por la unidad; con lo que también hay que saber qué significa *divisible*. Un *grupo* en este contexto no lo es mediático, ni de presión, ni siquiera político o cosas así; es un tipo particular de estructura algebraica con una operación binaria interna que satisface unas determinadas propiedades. Así que también hay que saber qué es una estructura algebraica, qué es una operación binaria interna y, luego, los conceptos que aparecen al aclarar estos términos. Etc., etc.

Y éste es otro de los inconvenientes a los que nos enfrentamos cotidianamente los matemáticos, sobre todo los que nos dedicamos preferentemente a la investigación en matemática abstracta (el Teorema de Pitágoras y el Último Teorema de Fermat entran en esta consideración). De hecho, en la gradación que hay en las Ciencias actuales: Matemáticas, Físicas, Químicas, Geológicas y Biológicas, cuanto más al comienzo nos encontremos, mayor es la dificultad en transmitir al no especialista una idea que le deje con la sensación de haber entendido algo (Wilson[10] aún propone un hiato entre las Matemáticas, cuyo objeto no tiene por qué ser la explicación de un fenómeno natural, y el resto, Ciencias Naturales).

Es, fundamentalmente, una cuestión de entender las definiciones implicadas. Se trata de establecer con toda claridad, sin ningún tipo de ambigüedad, de qué se está hablando y qué se dice de ello. Esto es algo muy alejado del uso corriente del lenguaje y, sobre todo, del de algunas tertulias y controversias políticas, en que se habla, eso sí, con gran pasión, no se sabe muy bien qué de qué (cuántas discusiones se evitarían fijando previamente los conceptos a debate). De ahí también el particular aspecto que toman los enunciados matemáticos, con una previa descripción precisa de la situación (*hipótesis*), seguida de la afirmación que, al respecto, se hace (*tesis*). Luego vendrá la

[10] Edward O. Wilson, mirmecólogo, padre de la Sociobiología y precursor de la Psicología Evolutiva. En *Consilience: La unidad del conocimiento*. Galaxia Gutenberg, 1999.

inexcusable *demostración*. Eso hace que cualquier texto matemático, con sus Axiomas, Definiciones, Lemas, Teoremas, Proposiciones, Corolarios, Demostraciones, Ejemplos y Observaciones, no sea, literariamente hablando, demasiado confortable, aun haciendo abstracción de la formulación empleada.

En las definiciones está la esencia de cualquier problema bien establecido. Hace mucho que les digo a mis alumnos que, cuando se pongan a estudiar cualquier tema matemático, dediquen el 90 % del tiempo a las definiciones y el resto a lo demás, en lugar de hacer lo contrario o, peor, no dedicar apenas tiempo a las definiciones. Definiciones que actualmente se pueden dar en cinco minutos han surgido tras una decantación de cientos de años de quehacer matemático, así que no debería extrañar que lleven mucho dentro y que requieran de atención y energía para comprenderlas. Muy probablemente, la razón de que a muchos estudiantes les resulten especialmente difíciles las matemáticas haya que buscarla en conceptos insuficiente o erróneamente asimilados en su momento, que enturbian la comprensión de los nuevos.

Inevitablemente, cualquier definición está referida a conceptos anteriores. Como antes, cuando *grupo* nos llevaba a *estructura algebraica* y *operación binaria interna* y de ahí tendríamos que seguir. Pero eso no se puede hacer indefinidamente. ¿Se han puesto alguna vez a pensar en qué contiene un diccionario? Porque, de hecho, las palabras se definen. Y, como lo hacen, claro, por medio de otras palabras y sólo hay un número finito de entradas, necesariamente contienen círculos viciosos en los que una palabra acaba siendo definida por ella misma. Se cuenta que el récord lo alcanzó un diccionario en el que una entrada era:

CONEJO. m. v. liebre.

Y otra:

LIEBRE. f. v. conejo.

La única solución para evitar esto sería la de establecer un cierto número de palabras que no se definen y, a partir de ellas, introducir todas las demás. ¿Difícil? Pues es lo que la Matemática actual hace.

Porque, de una forma u otra, salvo en determinadas presentaciones que son, a la postre, reducibles a lo que a continuación se expone, sólo hay tres conceptos que no se definen: el de *pertenencia*, el de *elemento* y el de *conjunto*. Lo que aparece resumido en la escueta fórmula

$$x \in A$$

que se lee "x pertenece al conjunto A" o "x es elemento del conjunto A". Así que lo que se pide es que estemos todos de acuerdo en que tenemos clara esa idea, pero que no se va a definir. Y esto no cuesta demasiado, si se acepta que no debe haber ambigüedades. Si hablamos, por ejemplo, del conjunto de los asistentes a este acto de apertura de curso, todos tendremos claro de qué se habla y si una persona concreta pertenece o no al conjunto.

De ahí, con las reglas de la lógica y con las definiciones adecuadas, sale todo lo demás. El conjunto *vacío*

$$\emptyset$$

es el que no posee elementos y se identifica con el número cero,

$$0$$

El conjunto cuyo único elemento es el conjunto vacío (no debe repugnar el considerar que un conjunto sea elemento de otro conjunto: piénsese, por ejemplo, en la liga de fútbol, en la que participan equipos que, a su vez, están formados por sus jugadores), o sea

$$\{\emptyset\}$$

se identifica con el número uno,

$$1$$

Y así salen todos los llamados *números naturales*. Y de ahí los *enteros*, los *racionales*, etc. (Inquieta un poco que todo se base en el vacío.)

La parte de las Matemáticas que desarrolla el concepto de conjunto se denomina, cómo no, Teoría de Conjuntos, y es el sostén de todo ulterior desarrollo matemático. Así como la Matemática es el fundamento de todas las demás Ciencias, la Teoría de Conjuntos es el fundamento de la Matemática. La introdujo Cantor[11] a partir de 1874 e, inmediatamente, tuvo una entusiasta acogida por todos los matemáticos, ya que, además de proveer de un lenguaje de uso universal, permitió obtener con rigor resultados relativos a la idea de infinito que, hasta entonces, habían resultado muy oscuros. Pero inmediatamente se le abrieron una serie de importantes, digamos, agujeros. Examinemos el más conocido, quizás por ser el más fácil de introducir. Consideremos el conjunto X cuyos elementos son los conjuntos que no se pertenecen a sí mismos. Pues bien, no cuesta nada darse cuenta de que da lo mismo decir que X es elemento de X que decir que X no es elemento de X . Con escritura matemática se expresa así:

$$X \in X \iff X \notin X$$

(que se lee: X pertenece a X si y sólo si X no pertenece a X). Esto, desde luego, no puede ser, algo anda mal. Es lo que se llama una paradoja, en este caso, la conocida como paradoja de Russell[12].

Estamos en el IV Centenario del Quijote. Quizás entiendan mejor esta paradoja, y otras del mismo jaez, si recordamos el episodio en que Sancho,

[11] George Cantor, San Petersburgo, 1845 – Halle 1918.

[12] Por Bertrand Arthur William Russell, Ravenscroft, 1872 – Penrhyndeudraeth, 1970. Matemático y filósofo. Introdujo la paradoja en 1901. El propio Cantor había descubierto otra paradoja, que hoy lleva su nombre, en 1879.

por fin Gobernador de una Ínsula, debe resolver un conflicto[13]. Así se lo presentan:

—Señor, un caudaloso río dividía dos términos de un mismo señorío, y esté vuestra merced atento, porque el caso es de importancia y algo dificultoso... Digo, pues, que sobre este río estaba una puente, y al cabo della una horca y una como casa de audiencia, en la cual de ordinario había cuatro jueces que juzgaban la ley que puso el dueño del río, de la puente y del señorío, que era en esta forma: «Si alguno pasare por esta puente de una parte a otra, ha de jurar primero adónde y a qué va; y si jurare verdad, déjenle pasar, y si dijere mentira, muera por ello ahorcado en la horca que allí se muestra, sin remisión alguna». Sabida esta ley y la rigurosa condición della, pasaban muchos, y luego en lo que juraban se echaba de ver que decían verdad y los jueces los dejaban pasar libremente. Sucedió, pues, que tomando juramento a un hombre juró y dijo que para el juramento que hacía, que iba a morir en aquella horca que allí estaba, y no a otra cosa.

Tras hacérselo repetir, Sancho entendió perfectamente el problema:

—A mi parecer, este negocio en dos paletas le declararé yo, y es así: el tal hombre jura que va a morir en la horca, y si muere en ella, juró verdad y por la ley puesta merece ser libre y que pase la puente; y si no le ahorcan, juró mentira y por la misma ley merece que le ahorquen.

Hubo una primera propuesta salomónica de Sancho, consistente en que a la parte del individuo que había dicho la verdad se la dejase pasar libremente y a la que había mentido se la ahorcase, que enseguida abandonó cuando se le hicieron patentes los indeseados inconvenientes de la misma –lo que hoy llamaríamos *efectos colaterales*. Finalmente optó por seguir un consejo general que le había dado D. Quijote: que, en caso de duda en la administración de justicia, debía optar por la misericordia, y mandó que se dejase pasar sin daño al hombre.

¿Cómo se resuelve esto en Matemáticas? La solución más extendida es la del denominado sistema de Zermelo-Fraenkel-Skolem o ZFS[14] que, por dar sólo la idea, establece que hay *clases*[15] que pueden ser definidas por las reglas ordinarias de la teoría de conjuntos que, sin embargo, no son conjuntos, por lo que no se les puede dar el tratamiento de tales. Es el caso de la paradoja de Russell: X es una clase, pero no un conjunto, así que no puede entrar a formar parte de la definición de X , con lo que se destruye la paradoja. En este terreno de fundamentos de las Matemáticas hay mucha sutileza y hay que andarse siempre con pies de plomo.

[13]Segunda parte del ingenioso caballero don Quijote de la Mancha. Capítulo LI. Publicada en el año 1615: la esencia de la paradoja de Russell con casi tres siglos de antelación.

[14]Después de los trabajos de Ernst Zermelo, Berlín, 27-7-1871 – Friburgo, 21-5-1953, a partir de 1908 y de Abraham Fraenkel, Munich, 17-2-1891 – Jerusalén, 15-10-1965 y Thoralf Skolem, Sandsvaer, 23-5-1887 – Oslo, 23-3-1963, a partir de 1922.

[15]El concepto de clase sustituye al de conjunto como concepto primitivo. *Conjunto* se define como una clase que es elemento de otra.

El sistema ZFS consta de diez *axiomas* (hechos que se aceptan sin demostración), como es inexcusable al establecer cualquier modelo. Las matemáticas son, frecuentemente, tachadas de pesadas e ininteligibles, y estamos asistiendo a una continua disminución de sus contenidos en los planes de estudios de todos los niveles de enseñanza (el último informe PISA[16] ha hecho saltar las alarmas; ojalá sea verdad que se va a potenciar la enseñanza del lenguaje y de las matemáticas). Pese a ello, se apela a lo matemático para hacer ver que un argumento es irrebatible: considérese por ejemplo el uso vulgar de matemático como sinónimo de apodíctico o de inevitable en situaciones tales, y de nuevo apelo a la liga de fútbol, como cuando al llegar a tal jornada se dice del equipo que sea que ya es, matemáticamente, campeón de liga. Sin embargo, lo que está claro en Matemáticas es que todo depende del modelo en el que se esté trabajando: de los axiomas y las definiciones que lo caracterizan. No exagero. Por ejemplo, la expresión

$$1 + 1 = 0$$

es falsa (lo admito, una barbaridad), si estamos hablando, pongamos por caso, de números naturales; pero es cierta en otras estructuras –modelos. De hecho, se utiliza continuamente en muchos procesos de, entre otros, transmisión de información. (En realidad eso no es tan misterioso, y no está muy lejos de la afirmación de que la suma de dos números impares es par.) Pero voy a referirme a otro ejemplo que viene del campo de la Geometría.

Para un estudiante que aprende las primeras nociones geométricas, la Geometría es el modelo que se denomina Geometría Euclídea y está acostumbrado a identificarla con el entorno real en el que vive. Es necesario que acceda a estudios más avanzados para entender la Geometría como una disciplina abstraída de la realidad, en la que se establecen unos axiomas (que se le aproximan intuitivamente) a partir de los cuales se obtienen propiedades geométricas, que son aplicables a lo real si el sistema axiomático, el modelo, es adecuado. Cuando ha conseguido esto se ha producido un cambio cualitativo esencial en la mentalidad de nuestro estudiante.

Algo así fue respecto del pensamiento científico el intento de axiomatización de la Geometría contenido en los Elementos de Euclides[17]. Es un primer paso, ya que no hay conceptos primitivos (es decir, no definidos), y a todo se le quiere dar un significado real, aunque idealizado. Esto hace que las primeras definiciones nos parezcan hoy ingenuas, v. gr.

[16] Programme for International Student Assessment. Es una evaluación normalizada que se realiza a escolares de quince años, desarrollada conjuntamente por los países participantes. La primera evaluación se efectuó en 2000 en 43 países, la segunda en 2003 en 41 y se espera que para la tercera, a realizarse en 2006, participen al menos 58 países. España lo hace desde la primera edición.

[17] Se sabe poco de la vida de Euclides, lo que nos ha llegado a través de los comentarios del historiador griego Proclo (Proclo de Bizancio, Bizancio, 410 – Atenas, 485). Vivió en Alejandría en torno al año 300 aC. Sí que se conoce bien su obra, siendo la más importante un tratado de geometría titulado Los Elementos.

Punto:	Es lo que no tiene partes.
Línea:	Es una longitud sin anchura.
Recta:	Es aquella línea que yace igualmente respecto de todos sus puntos.

Etc. Después de las primeras definiciones siguen un total de cinco postulados, a saber:

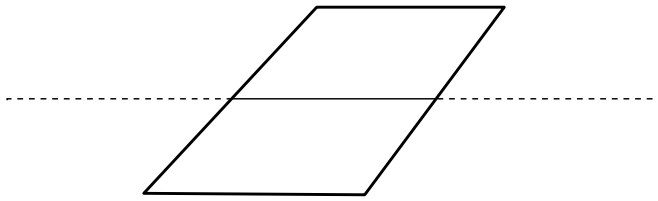
Postulado primero. Si P y Q son dos puntos distintos cualesquiera, existe una única recta que pasa por P y Q.

Postulado segundo. Toda recta limitada puede prolongarse indefinidamente en cualquier dirección.

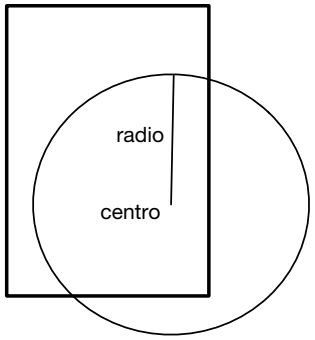
Postulado tercero. Con cualquier centro y cualquier radio se puede trazar una circunferencia.

Postulado cuarto. Todos los ángulos rectos son iguales.

Es de notar la sencillez de estos cuatro postulados, en los que se revela un especial cuidado con las cuestiones de constructibilidad y la necesidad de abstraer la realidad. Es claro que sobre una hoja las rectas aparecen cercenadas

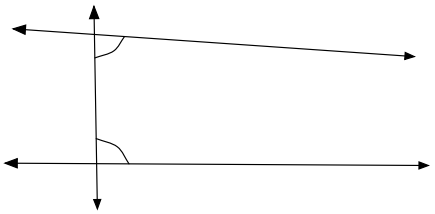


y que el radio de una circunferencia que se pueda dibujar queda limitado por el tamaño de la hoja.



Sorprende también la búsqueda exhaustiva de rigor que revela el cuarto postulado: no se quería dar nada por supuesto sin establecerlo explícitamente. Después hay un último postulado que choca por lo prolijo de su enunciado y su mayor alejamiento de la intuición.

Postulado quinto. Si una recta, al cortar a otras dos, forma de un mismo lado ángulos internos menores que dos rectos, esas dos rectas pueden prolongarse hasta que se corten del mismo lado en que están los ángulos menores que dos rectos.



No es de extrañar que desde un primer momento se tratase de demostrar este quinto postulado a partir de los cuatro anteriores. Es decir, demostrar que el quinto no era en realidad un axioma, sino un teorema. El mismo Euclides parece reacio a utilizarlo, ya que no es hasta la Proposición 29 de los Elementos cuando aparece empleado por primera vez. Los intentos de efectuar esa demostración llenan dos milenios de historia, no siendo hasta el siglo XIX, con los trabajos de Bolyai y Lobachevsky[18], cuando la cuestión se resuelve negando la posibilidad de dicha demostración y naciendo una nueva Geometría, la denominada Hiperbólica, en la que siendo válidos los cuatro primeros axiomas, no lo es el quinto.

Entretanto, muchos matemáticos creyeron haber hecho esa demostración, pero se basaron en enunciados que hoy se sabe que son equivalentes a la verificación del quinto postulado (dicho de otra manera, que se pueden sustituir por él)[19]. Uno de ellos, el debido a Playfair, se emplea hoy comúnmente, incluso con el nombre de Quinto Postulado de Euclides:

[18] János Bolyai, Kolozsvár, 15-12-1802 – Marosvásárhely, 27-1860 y Nikolai Ivanovich Lobachevsky, Nizhny Novgorod, 1-12-1792 – Kazan, 24-2-1856, realizaron la hazaña más o menos a la vez e independientemente, apareciendo los correspondientes trabajos publicados en 1831 y 1829, respectivamente. De hecho, la Geometría que sólo emplea los primeros cuatro postulados se denomina hoy Absoluta o Neutra, la que también emplea el quinto, Euclídea y la que emplea su contrario, Hiperbólica. Hasta la Proposición 29, exclusive, Euclides hace, pues, Geometría Absoluta, siendo esa Proposición de Geometría Euclídea.

[19] La mención de los nombres que creyeron haber demostrado el quinto postulado es instructiva; seguiremos los más importantes mencionando la proposición que, bien inconscientemente, bien a sabiendas pero dándola como evidente, utilizaron para conseguir la demostración.

- Posidonio de Apamea, Apamea, ca. 135 aC – ca. 50 aC. Filósofo estoico, cuya escuela surgió en Rodas. *Dos rectas paralelas son equidistantes.*

- Claudio Ptolomeo, Astrónomo y Geógrafo, propuso el sistema geocéntrico que perduró por mas de 1400 años. Nació en algún lugar de Egipto ca. 85 dC.; murió en Alejandría el 165 dC. *Cuando un par de rectas paralelas es cortado por una transversal, la suma de los ángulos internos a un lado de la misma es igual a la suma de los ángulos internos del otro lado.*

- Proclus Diadochus, Constantinopla, 412 – Atenas, 485, filósofo neoplatónico. *La distancia entre dos rectas paralelas está acotada.*

- Christopher Clavius, Bamberg, 25-3-1538 – Roma, 2-2-1612. Matemático. *Si tres puntos*

Postulado de las paralelas. Por un punto exterior a una recta se puede trazar una y sólo una paralela a dicha recta.

Los enunciados a que nos hemos referido fueron afinándose más y más según avanzaba el tiempo, de forma que no es extraño que se pudieran tomar como verdades evidentes. También ha de aparecer aquí Gauss, el *Princeps Mathematicorum*[20], aunque necesario es advertir que en ningún momento pensó haber demostrado el quinto postulado; antes bien hay que incluirlo en el tándem Bolyai-Lobachevsky como descubridor de la geometría no euclídea, incluso adelantándose en algunos años. Sin embargo, el miedo a la reacción de la mentalidad vigente, sustentado por el respeto que sentía por las ideas de Kant[21] –el cual había llegado a afirmar que la Geometría Euclídea es consustancial al ser humano– hizo que ocultase sus trabajos sobre el tema. Gauss vio que la siguiente proposición (quizás la más chocante entre todas las que hemos presentado) es equivalente al quinto postulado:

Gauss: Existen triángulos de área tan grande como se quiera.

Desde luego, puede repugnar negar que eso sea cierto, estaría muy alejado de la intuición. Pero, repetimos, en la Geometría Hiperbólica las cosas no son así. En particular, en ésta, por un punto exterior a una recta se pueden trazar infinitas rectas que no cortan a la dada. De hecho hay otra Geometría, la Elíptica, en la que toda recta que pasa por un punto exterior a una recta dada la corta[22].

Por no perdernos, recordemos que todo esto son modelos, abstracciones. No debemos fiarnos de la intuición y, menos, de los dibujos, en los que todo

---

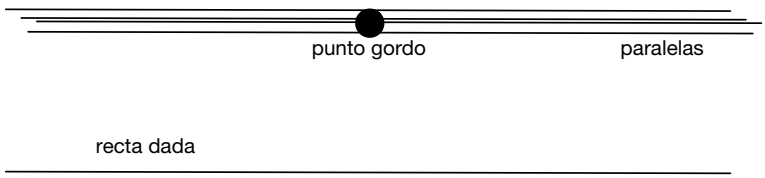
están del mismo lado de una recta y equidistan de ella, los tres puntos están alineados.
- John Wallis, Ashford, Kent, 23-11-1616 – Oxford, 28-10-1703. Matemático y criptógrafo. *Dado un triángulo cualquiera existe siempre uno semejante de magnitud arbitraria.*
- Giovanni Girolamo Saccheri, San Remo, 5-9-1667 – Milán, 25-10-1733. Filósofo, teólogo y matemático. *La suma de los ángulos interiores de un triángulo es igual a dos rectos.*
- John Playfair, Benvie, 10-3-1748 – Burntisland, 20-7-1819. Matemático. *Por un punto exterior a una recta se puede trazar una y sólo una paralela a dicha recta.*
- Adrien Marie Legendre, París, 18-9-1752 – 10-1-1833. Matemático. *Por un punto cualquiera tomado en el interior de un ángulo se puede siempre trazar una recta que encuentre los dos lados del ángulo.*

[20]Carl Friedrich Gauss, Brunswick, 30-4-1777 – Göttingen, 23-2-1855. Matemático, astrónomo, físico, geodesta e inventor. El apelativo de *Princeps Mathematicorum* con que se le conoce se debe al hecho de que, para la mayoría, ha sido el más grande matemático de todos los tiempos.

[21]Emmanuel Kant, Königsberg, 22-4-1724 – 12-2-1804. Además de filósofo, fue también matemático y un estimable físico.

[22]Fue el matemático David Hilbert, Königsberg, 23-1-1862 – Göttingen, 14-2-1943, el primero en desarrollar un sistema axiomático riguroso respetando el espíritu de los Elementos. En éste, la negación de la validez del Quinto Postulado de Euclides conduce obligatoriamente a la Geometría Hiperbólica. En la Geometría Elíptica, la infinitud a la que hace mención el Segundo Postulado de Euclides no se da, permaneciendo válidos los otros tres Postulados.

punto y toda línea tienen un grosor. La gramática parda estudiantil conoce eso desde siempre, como lo muestra el denominado Teorema del Punto Gordo: Por un punto exterior a una recta se pueden trazar tantas rectas paralelas a la dada como se quiera, con tal que el punto sea lo suficientemente gordo.



Lo anterior debería bastar para comprender que una pregunta del estilo de cuál de las tres Geometrías es la real, no tiene sentido alguno. Pero mantiene su vigencia la de cuál es la que mejor se adecua al mundo real. Es cierto que es la Euclídea la que se emplea ordinariamente, por ejemplo, para trazar una carretera, tender un puente o construir una casa. Pero es que se demuestra que para distancias pequeñas las tres se comportan igual (luego tendremos un atisbo de qué significa "pequeñas"). Pero en algunos trabajos de Física parece preferirse una cierta modificación de la Elíptica. Y hay quien sostiene que nuestra manera binocular de ver el mundo casa mejor con la Hiperbólica. El propio Einstein[23] apuntó la posibilidad de que según el estado espacio-temporal existente pueda ser más adecuado utilizar un tipo u otro de Geometría.

Supongamos que llegamos a tener instrumentos de medida suficientemente precisos. ¿Habrá alguna manera de ver cuál de las tres geometrías es la más adecuada? El enunciado idóneo para hacerlo parece ser el de Saccheri.

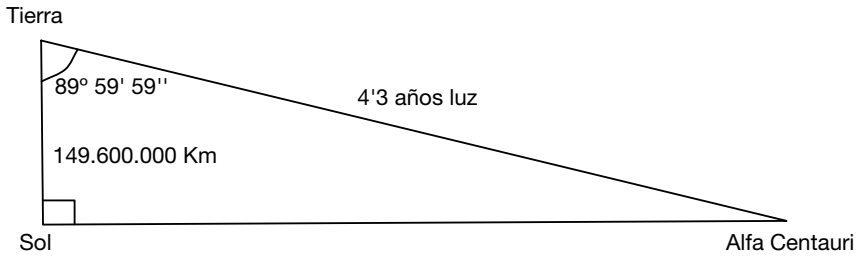
Saccheri: La suma de los ángulos interiores de un triángulo es igual a dos rectos.

Llamemos defecto de un triángulo a la diferencia que hay entre dos rectos y la suma de sus tres ángulos. El que dicho defecto sea negativo, nulo o positivo caracteriza, respectivamente, a las Geometrías Elíptica, Euclídea e Hiperbólica. Pues bien: cogemos un triángulo, medimos sus ángulos, sumamos, comparamos con 180^o y ya estamos listos. Pero es que en distancias pequeñas el defecto, de ser no nulo, sería muy próximo a 0, tanto, que ni los instrumentos más precisos podrían detectarlo. Muy bien, pues consideremos distancias grandes.

Consideremos el triángulo formado por la Tierra, el Sol y la estrella Alfa Centauri (una de las más próximas, a "sólo" 4'3 años luz; es de advertir que

[23] Albert Einstein, Ulm, 4-3-1879 – Princenton, 18-4-1955. Con Isaac Newton, Woolsthorpe, 4-1-1643 – Londres, 31-3-1727, los mayores genios de la Física.

la figura en modo alguno está a escala: si quisiésemos hacer eso, quedaría reducida a un segmento de recta).



Los astrónomos han comprobado que en el momento en que el ángulo correspondiente al Sol es recto, el correspondiente a la Tierra es de $89^o\ 59'\ 59''$. Los errores de medición superan con mucho el posible defecto del triángulo. Estamos hablando, para lo que nos ocupa, de distancias pequeñas. Se demuestra, por otro lado, que si el defecto de un triángulo es no nulo, el defecto de otro triángulo interior es menor en valor absoluto, así que el restringirse a distancias más pequeñas no hace sino agravar el problema de la medida.

Acaso no dispongamos nunca de instrumentos lo suficientemente precisos para dilucidar esta cuestión. En cualquier caso, las teorías físicas modernas, a partir de la Teoría de la Relatividad General de Einstein, manejan un modelo de Universo en el que el espacio-tiempo no puede aislarse de su contenido (materia, energía, energía oscura, etc.).

Espero haberles convencido de la importancia de las definiciones, por un lado, y de que cualquier verdad matemática lo es sólo, al menos en principio, dentro del modelo en el que está enunciada, por otro. ¿Tiene esto alguna consecuencia práctica? A mí, al menos, me hace recelar de todo lo que se presente como verdad absoluta.

Quiero acabar esta lección con un par de reflexiones en torno a si las Matemáticas son o no necesarias y si es o no necesaria su enseñanza.

La cuestión importante es, desde luego, la última. Porque acerca de la necesidad de las Matemáticas nadie va a argumentar en contra: no compromete admitirla y, además, a la vista de que se emplean prácticamente para todo, sería muy embarazoso hacerlo. A lo mejor, acerca de que hay que enseñar –luego, aprender– matemáticas, tampoco haya mucha oposición: se enseñan cuatro fórmulas para luego aplicarlas, y ya está. Pero eso no es tan sencillo: como he dicho, ya las definiciones se aprenden con esfuerzo, requieren tiempo y dedicación, y sólo la comprensión suficiente de un desarrollo matemático va a permitir a quien luego lo quiera utilizar en otra rama científica, técnica o de cualquier otro tipo, adaptarlo a sus necesidades con auténtico provecho. Se requiere, al respecto, formación, no meramente información. No basta con saber, hay que entender.

Las aplicaciones de las Matemáticas surgen de cualquiera de sus especialidades, por abstractas que sean, a pesar de quienes, sin ningún fundamento,

se refieren a ellas como a matemáticas hechas sólo para matemáticos o como a meros "divertimentos"matemáticos. La búsqueda del conocimiento es algo tan característicamente humano, que no debería ser necesaria su justificación. En una ocasión, uno de los estudiantes de Euclides le preguntó que qué ganaba con lo que había aprendido de la geometría. El maestro ordenó inmediatamente que se le entregase un óbolo, para que "ganara" algo, dando a entender que aquel muchacho no había comprendido nada. Pero, en estos tiempos que, en muchos aspectos, se me antojan de un pragmatismo desaforado y miope, quizás no esté de más resaltar el hecho obvio de que cualquier desarrollo práctico se basa en conocimientos fundamentales anteriores.

Por ejemplo, ya antes hemos mencionado a Einstein, en este año en que se celebra el centenario de la aparición de algunos de sus trabajos más significativos[24]. Pues bien, la Teoría de la Relatividad General fue posible gracias a los resultados sobre geometría del espacio, una investigación en matemática abstracta, que había desarrollado Riemann[25] muchos años atrás.

Mi campo de investigación pertenece al Álgebra, una de las ramas más abstractas de las Matemáticas. Y con ésta, en relación con la Criptografía, ocurre lo mismo que con las Matemáticas en relación con las Ciencias Naturales. La Teoría de Números, parte del Álgebra, resulta tener una *irrazonable eficacia* en la Criptografía[26]. Ha servido para encontrar los métodos criptográficos que son hoy universalmente usados. En particular, los de clave pública como el RSA[27], están basados en el concepto antes mencionado de número primo (en éste se emplea un teorema de Fermat sobre este tipo de números, conocido como Teorema Pequeño de Fermat[28] –del que sí nos dejó su demostración). Mirando hacia adelante, aunque todavía parece algo lejana su operatividad, ya se vislumbran los ordenadores cuánticos, que harán inservibles (porque los violarán inexorablemente) todos los actuales sistemas criptográficos. Pues ya se están desarrollando, y esta vez dentro de la Teoría de Grupos, que es el campo concreto del Álgebra en el que se enmarca mi labor investigadora, sistemas criptográficos que operarán con seguridad en computación cuántica.

[24]El año 1905 suele referirse como el *Annus mirabilis* de Einstein. Con sólo 26 años y en apenas seis meses, Einstein publica en la revista alemana Annalen der Physic cuatro artículos sobre el efecto fotoeléctrico, el movimiento browniano, la Teoría de la Relatividad Especial y la relación entre masa y energía. Algo así había ocurrido antes una sóla vez, en otro año milagroso, el de 1666, en el que Newton sentó las bases del Cálculo Diferencial (parte importante de las Matemáticas), la Mecánica, la Teoría de la gravedad y la del color.

[25]Georg Friedrich Bernhard Riemann, Breselenz, 17-9-1826 – Selasca, 20-7-1866. Matemático.

[26]Neal Koblitz, *Algebraic Aspects of Cryptography*, Algorithms and Computation in Mathematics Vol. 3, Springer-Verlag, New York, 1998.

[27]Desarrollado en 1978 por Ron Rivest, Adi Shamir, y Leonard Adleman.

[28]Si p es un primo y n es un número natural no divisible por p, entonces $n^{p-1} \equiv 1 \mod p$.

Una buena formación matemática en todos los niveles de estudio es la única forma de asegurar que se dispondrá de profesionales, en cualquier especialidad, capaces de innovar y de enfrentarse con éxito a los cambios que, cada vez en mayor número, nos reserva el futuro.

He dicho.