

Axioma

La revista de los estudiantes y
profesores de matemática

HASTA PRONTO

Axioma N° 12

Axioma es una publicación bimestral dirigida a estudiantes y profesores de matemática.

Directora

Gisela Serrano de Piñeiro

Propietarios

Raquel Susana Kalizsky

Andrea Liliana Morales

Claudio Alejandro Salpeter

Gisela Beatriz Serrano

Colaboradores permanentes

Gustavo Piñeiro

Jorge Martínez

Colaboraron en este número

Carla Finiello

Yanina Martínez

Dirección postal

Sucursal 2 B

Casilla de Correo 72

(1402) Capital

Correo electrónico

pineiro@datamarkets.com.ar

La responsabilidad sobre las opiniones vertidas en notas firmadas es exclusiva de sus autores. Se autoriza la reproducción parcial o total de las notas con la condición de citar la fuente.

Registro de la Propiedad Intelectual N° 867689.

Suscripción por 5 números (incl. gastos de envío): \$ 11.-

Ejemplar suelto: \$ 3.-

Ejemplar atrasado: \$ 3.-

Editorial

Estimados lectores:

Diversas circunstancias han llevado al staff de Axioma a verse en la necesidad de hacer un alto en la publicación de la revista.

No sin tristeza hemos tomado tal decisión unánimemente; sin embargo, al lector no le resultará tan fácil librarse de nosotros. Tenemos la firme esperanza de retomar nuestra tarea, en forma más organizada o, mejor dicho, en forma organizada, el año entrante. Nos es imprescindible un período de replanteo, discusión y reestructuración.

Los suscriptores encontrarán información adicional referida a su suscripción en la sección Información.

Que esta editorial no sea un adiós sino, simplemente, un HASTA PRONTO.

Sumario

Apuntes sobre...	2	Grandes Matemáticos	22
Historia	6	Problemas	28
Entrevista	9	Comentarios de textos	30
Curiosidades Matemáticas	14	Información	32

Julio/ Agosto de 1998

Año 3 - N° 12

Apuntes sobre...

Matrices y Movimientos (Tercera parte).

Las rotaciones, simetrías, y traslaciones son estudiadas en el colegio secundario sin un claro motivo para ello. En esta sección comentaremos algunos hechos destacables acerca de estos movimientos y trataremos de ilustrar la importancia de su estudio.

Las razones que justifican la importancia del estudio de los “movimientos rígidos” (rotaciones, traslaciones y simetrías) sólo pueden comprenderse en el contexto del *programa de Erlangen*, enunciado por el matemático alemán Félix Klein en 1872.

De acuerdo con las ideas de Klein, una *geometría* en un conjunto A es un sistema de definiciones y teoremas que sea invariante bajo un grupo dado de transformaciones de A. Entendemos aquí por *grupo de transformaciones* a un conjunto **G**, no vacío, de funciones biyectivas (definidas de A en A) que verifique las siguientes condiciones:

- Para toda función $g \in G$ su inversa, g^{-1} , también pertenece a **G**.
- Si f y g son funciones de **G** entonces la composición de ambas fog también pertenece a **G**.

Cada grupo de transformaciones de A induce en este conjunto una *geometría*. Mostraremos, mediante algunos ejemplos concretos, cómo cada grupo **G** delimita las definiciones que la geometría puede contener y establece el alcance de sus teoremas.

Con el fin de construir algunos ejemplos de geometrías, tomemos el conjunto R de los números reales. Dentro de este conjunto, los objetos con los cuales trabajaremos serán los *intervalos semiabiertos*. Dados a y b números reales, $a < b$, definimos:

$$(a, b] = \{x \in R : a < x \leq b\}$$
$$[a, b) = \{x \in R : a \leq x < b\}$$

Consideraremos diversos grupos de transformaciones de R y veremos cómo, cada uno de ellos,

induce una geometría diferente. Describiremos ahora cuál será el grupo de transformaciones que utilizaremos en el primer ejemplo.

Para cada $k \in R$, sea F_k la función de R en R definida por: $F_k(x) = x + k$. Llamaremos, por su parte, **G₁** al conjunto formado por todas las funciones de la forma F_k (con $k \in R$). Es fácil probar que este conjunto **G₁** constituye un grupo de transformaciones de R .

Una vez que hemos determinado el grupo de transformaciones, estamos en condiciones de explicar una de las ideas más importantes en la concepción del programa de Erlangen: la noción de *congruencia*.

Sea **G** un grupo de transformaciones de A y sean B_1 y B_2 dos subconjuntos del conjunto A. Diremos que B_1 y B_2 son congruentes si y sólo si existe una función $f \in G$ tal que $f(B_1) = B_2$; donde $f(B_1) = \{f(x) : x \in B_1\}$, es decir, $f(B_1)$ es el conjunto resultante de aplicar la función f a cada uno de los puntos de B_1 .

A los efectos de la geometría inducida por **G**, dos subconjuntos que sean congruentes deben considerarse como completamente equivalentes. Es decir, dos subconjuntos congruentes deben tener exactamente **las mismas propiedades geométricas**. En este sentido, el grupo **G** condiciona las definiciones que puede contener la geometría, pues cualquier propiedad que definamos debe conservarse al aplicar cualquiera de las funciones de **G**.

Volvamos a considerar el grupo **G₁** de transformaciones de R . En este ejemplo concreto, dos intervalos semiabiertos I_1 e I_2 se dirán *congruentes* si y sólo si existe alguna función $F_k \in G_1$ tal que $F_k(I_1) = I_2$, donde $F_k(I_1) = \{F_k(x) : x \in I_1\}$.

Enunciamos la primera definición de la geometría inducida por el grupo \mathbf{G}_1 :

Definición 1: Llamaremos *longitud* de un intervalo semiabierto a la diferencia entre sus extremos. En símbolos:

$$\text{Long}((a,b]) = \text{Long}([a,b)) = b - a$$

Para que esta definición sea aceptable dentro de nuestra geometría, dos intervalos que sean congruentes deben tener exactamente la misma longitud (la longitud debe ser invariante bajo el grupo \mathbf{G}_1). Es decir, si I es un intervalo, entonces para toda $F_k \in \mathbf{G}_1$ debe verificarse que $\text{Long}(F_k(I)) = \text{Long}(I)$. Resulta sencillo demostrar que esta condición de invarianza efectivamente se cumple.

Imaginemos que estamos interesados en determinar condiciones necesarias y suficientes para que dos intervalos semiabiertos sean congruentes entre sí. Está claro que una condición necesaria es que ambos intervalos tengan la misma longitud. Sin embargo esta condición no es suficiente; en efecto, los intervalos $(0,1]$ y $[0,1)$ tienen la misma longitud, sin embargo no son congruentes entre sí. Este ejemplo nos sugiere la segunda definición de esta geometría:

Definición 2: Diremos que un intervalo está *orientado a derecha* si contiene a su extremo derecho. En caso contrario, diremos que está *orientado a izquierda*.

Desde luego, para que esta definición sea válida, la *orientación* de un intervalo debe ser, como la longitud, una propiedad invariante bajo \mathbf{G}_1 . Se prueba fácilmente que esta condición de invarianza efectivamente se cumple.

Basados en la longitud y la orientación podemos finalmente enunciar el primer teorema de la geometría:

Teorema 1: Dos intervalos semiabiertos son congruentes si y sólo si tienen la misma longitud y la misma orientación.

La demostración de este teorema es sencilla y queda como ejercicio para el lector.

Con el objeto de tener otras geometrías con las cuales comparar la que acabamos de esbozar brevemente, analicemos ahora un nuevo ejemplo de geometría en R . Los objetos geométricos que estudiaremos serán nuevamente los intervalos semiabiertos. Sin embargo ampliaremos el grupo de transformaciones. Para cada $k \in R$, llamemos como antes F_k a la función $F_k(x) = x + k$. Sea además G_k a la función definida por $G_k(x) = -x + k$. Tomemos como \mathbf{G}_2 al conjunto que contiene a todas las funciones de la forma F_k y también a las funciones G_k . Es fácil verificar que \mathbf{G}_2 es un grupo de transformaciones de R . Para evitar confusiones, llamaremos **geometría rígida** a aquella inducida por \mathbf{G}_1 y **geometría especular** a la geometría inducida por \mathbf{G}_2 .

El concepto de longitud, enunciado en la **Definición 1** para la geometría rígida, sigue siendo válido en la geometría especular. Es decir, la longitud es invariante bajo \mathbf{G}_2 . Sin embargo, el concepto de *orientación* (enunciado en la **Definición 2**) ya no es aceptable en esta nueva geometría.

En efecto, la introducción de las funciones del tipo G_k provoca que el intervalo $(a,b]$ sea congruente con el intervalo $[a,b)$. Por lo tanto no es aceptable introducir una propiedad que distinga uno del otro. Exactamente al contrario de lo que ocurría con la geometría rígida, para la geometría especular el intervalo $(a,b]$ es totalmente equivalente al intervalo $[a,b)$. De hecho, en la geometría especular es válido el siguiente teorema:

Teorema 2: Dos intervalos semiabiertos son congruentes si y sólo si tienen la misma longitud.

Puede apreciarse a través de estos dos ejemplos que cada grupo de transformaciones considerado determina qué propiedades es válido definir en la geometría correspondiente. Asimismo cada grupo establece qué teoremas son válidos; por ejemplo, el **Teorema 1** es válido en la geometría rígida, pero no en la geometría especular, mien-

tras que exactamente lo contrario ocurre con el **Teorema 2**.

Un tercer ejemplo de geometría de los intervalos semiabiertos de R podría estar inducida por el conjunto (que llamaremos \mathbf{G}_3) de todas las funciones H_k (con $k > 0$), donde H_k es la función definida por $H_k(x) = kx$. Este conjunto \mathbf{G}_3 es efectivamente un grupo de transformaciones de R y llamaremos **geometría elástica** a la geometría inducida por él. En esta nueva geometría el concepto de longitud desaparece (la longitud no es invariante bajo \mathbf{G}_3), sin embargo el concepto de orientación sí es aceptable. Dejamos como ejercicio para el lector el enunciado y demostración de un **Teorema 3** que establezca condiciones necesarias y suficientes para que dos intervalos semiabiertos sean congruentes en la geometría elástica.

Dijimos en el comienzo de esta nota que el programa de Erlangen justifica la importancia del estudio de los movimientos rígidos. Para comprender esta afirmación, consideremos cierto grupo de transformaciones de R^2 . Concretamente, sea \mathbf{G}_4 el conjunto que contiene a todas las funciones que pertenecen a algunas de las dos categorías siguientes:

- a) Traslaciones, rotaciones o simetrías axiales.
- b) Toda función que se obtenga como composición de funciones del tipo anterior.

El conjunto \mathbf{G}_4 resulta ser un grupo de transformaciones de R^2 . De hecho, \mathbf{G}_4 es el **menor** grupo de transformaciones que contiene a las traslaciones, rotaciones y simetrías (en la terminología de la teoría de grupos, \mathbf{G}_4 es el grupo **generado** por estas funciones).

De acuerdo con el programa de Erlangen, el grupo \mathbf{G}_4 induce en R^2 una cierta geometría, en ella dos subconjuntos de R^2 que sean congruentes con respecto a \mathbf{G}_4 deberán considerarse completamente equivalentes y tendrán exactamente las mismas propiedades geométricas.

Ahora bien, la geometría inducida en R^2 por el grupo \mathbf{G}_4 no es otra que la bien conocida geo-

metría euclíadiana del plano. Es famoso el siguiente teorema de la geometría elemental:

Teorema 4 (congruencia de triángulos):

- a) Si dos triángulos tienen dos lados y el ángulo comprendido entre ellos respectivamente congruentes, entonces son congruentes.
- b) Si dos triángulos tienen un lado y los ángulos adyacentes a él respectivamente congruentes, entonces son congruentes.
- c) Si dos triángulos tienen los tres lados respectivamente congruentes, entonces son congruentes.

El **Teorema 4** representa, para el estudio de las propiedades de los triángulos en la geometría euclíadiana de R^2 , el análogo del **Teorema 1** para el estudio de los intervalos semiabiertos en la geometría rígida (o el **Teorema 2** en la geometría especular).

En el **Teorema 4** la palabra "congruente" tiene el mismo significado que le hemos atribuido anteriormente. Dos subconjuntos B_1 y B_2 de R^2 (por ejemplo, dos triángulos, dos segmentos o dos ángulos) son congruentes si y sólo si existe alguna función $f \in \mathbf{G}_4$ tal que $f(B_1) = B_2$. En otros términos, B_1 y B_2 son congruentes si y sólo si existe una composición de traslaciones, rotaciones y simetrías que transforme B_1 en B_2 .

Del mismo modo, todas las definiciones conocidas de la geometría euclíadiana (longitud de un segmento, paralelismo o perpendicularidad de rectas, amplitud de un ángulo, etc.) son aceptables dentro de esta geometría debido a que son invariantes bajo rotaciones traslaciones y simetrías.

Por el contrario, está excluido de la geometría euclíadiana el estudio de cualquier propiedad que no se conserve por rotaciones traslaciones y simetrías. Por ejemplo, sin el contexto de un sistema de ejes cartesianos, los conceptos de *recta horizontal* o *recta vertical* no son admisibles en la geometría euclíadiana, pues la dirección de una recta cambia si se le aplica una rotación.

Si un par de rectas perpendiculares es privilegiado como sistema de ejes cartesianos, arbitrariamente llamados x e y , entonces estos conceptos adquieren sentido. Sin embargo, aún en ese caso, estas definiciones resultan ser subsidiarias del concepto de "paralelismo". Una *recta horizontal*

es meramente una recta paralela al eje x . Una *recta vertical* es una recta paralela al eje y . Si sólo intercambiamos los nombres de los ejes, toda recta *horizontal* pasa a ser *vertical*, y viceversa.

La importancia de los “movimientos rígidos” radica entonces en que se hallan en la raíz de la geometría euclíadiana elemental, pues marcan la diferencia entre las propiedades que esta geometría puede estudiar y aquellas que carecen de sentido en ella.

Veamos, para finalizar, un nuevo ejemplo de aplicación del programa de Erlangen. Llamemos \mathbf{G}_5 al conjunto de todas las funciones continuas y biyectivas de R^2 en R^2 tales que su inversa es también una función biyectiva. Este conjunto \mathbf{G}_5 es un grupo de transformaciones de R^2 y la geometría que define es la *topología plana*.

La topología plana estudia las propiedades de los subconjuntos de R^2 que sean invariantes por la aplicación de funciones biyectivas continuas.

Dos segmentos de recta cualesquiera son congruentes respecto de \mathbf{G}_5 . Por lo tanto el concepto euclíadiano de longitud no es aceptable dentro de la topología plana (del mismo modo que tampoco era aceptable en la que hemos denominado *geometría elástica*). Tampoco es aceptable diferenciar conceptos tales como *cuadrado*, *triángulo* o *círculo*, pues, todas estas figuras son congruentes respecto de \mathbf{G}_5 .

Un concepto que sí resulta aceptable dentro de la topología plana es el concepto de *curva*. En términos informales, una curva es la trayectoria (continua) descripta por un punto que se mueve en R^2 . Si al finalizar su movimiento, el punto vuelve a la posición inicial, entonces se dice que la curva es *cerrada*. La curva es *simple* si nunca se corta a sí misma. Una circunferencia y una elipse son ambas curvas simples cerradas, de hecho, curvas congruentes entre sí.

Una propiedad topológica de las curvas simples y cerradas (es decir, un teorema aceptable dentro de la topología plana) es el siguiente:

Teorema: Toda curva simple y cerrada divide al plano en dos regiones. Una de ellas acotada (la región *interior*) y la otra no acotada (la región *exterior*).

La topología plana es una de las ramas de estudio más interesantes dentro de la Matemática y recomendamos al lector interesado la búsqueda de información acerca del mismo.

Hemos visto entonces que el programa de Erlangen permite definir a la geometría elemental y a la topología plana como el estudio de las propiedades invariantes bajo ciertos grupos de transformaciones de R^2 . En el caso de la geometría euclíadiana, este grupo está generado por rotaciones, simetrías y traslaciones.

Aunque el espacio no nos permite desarrollar la idea con la extensión que merecería, no podemos terminar esta nota sin mencionar que también las geometrías no euclidianas pueden ser descriptas dentro del esquema del programa de Erlangen.

El excelente trabajo de Luis Santaló titulado *Geometrías No Euclidianas* (EUDEBA) muestra que, para la geometría no euclíadiana hiperbólica, puede tomarse como conjunto A el interior de una elipse. Definiendo adecuadamente el grupo \mathbf{G} de transformaciones de A, esta geometría no euclíadiana resulta ser, como en todos los ejemplos antes analizados, simplemente el estudio de las propiedades invariantes bajo el grupo \mathbf{G} .

Gustavo Piñeiro*

* Licenciado en Ciencias Matemáticas de la U.B.A.

Bibliografía:

* BELL, E. T. -*Historia de las Matemáticas* - FONDO DE CULTURA ECONÓMICA - México, 1992.

* HERNÁNDEZ, ROBERTO - *Conceptos básicos de matemática moderna* - EDITORIAL CÓDEX - Buenos Aires, 1966.

* SANTALÓ, LUIS - *Geometrías no euclidianas* - EUDEBA - Buenos Aires, 1976.

La esencia del número – segunda parte

En la entrega anterior se discutió acerca de la noción de número natural en la antigüedad, en el siguiente artículo vamos a tratar la definición de número natural a la que finalmente se llegó a fines del siglo XIX.

Los números naturales parecen representar lo más sencillo y conocido de la matemática. Sin embargo, aunque familiares, no se los entiende del todo. Muy pocas personas están preparadas para definir formalmente lo que se entiende por "número", "cero" o "uno".

Es importante hallar esta definición ya que la matemática puede considerarse integrada en su totalidad por proposiciones sobre los números naturales.

Varios matemáticos y lógicos han intentado encontrar esta definición, aunque la mayoría de estos intentos fracasaron en algún aspecto. Por ejemplo: Ha sido costumbre hacer una excepción con el numero uno y definir los demás por su intermedio. Así 2 era " $1+1$ " y 3 era " $2+1$ " y así sucesivamente. Este método solo era aplicable a los números finitos y establecía una gran diferencia entre 1 y los números restantes, y generalmente no se explicaba el significado de suma.

Uno de los matemáticos que se interesó por el tema fue Peano quién definió a los números naturales a partir de 3 ideas y 5 proposiciones primitivas. Las 3 ideas primitivas

son: cero, numero y sucesivo, mientras que las proposiciones son:

- 1- cero es un número.
- 2- el sucesivo de un número es un numero.
- 3- dos números nunca tienen un mismo sucesivo.
- 4- el cero es el sucesivo de ningún número.
- 5- toda propiedad que pertenezca a cero y al sucesivo de un número que tenga esa misma propiedad, pertenecerá a todos los números.

Consideremos brevemente como se deriva la teoría de los números naturales de estas 3 ideas y 5 proposiciones. Se comienza así: definimos a 1 como el sucesivo de 0, a 2 como el sucesivo de 1 y así siguiendo evidentemente podemos ir tan lejos como queramos, puesto que en virtud de la segunda proposición, todo numero que obtengamos tendrá un sucesivo y en virtud de la tercera, este no puede ser ninguno de los números ya definidos, porque si lo fuera 2 números diferentes tendrían un mismo sucesivo, y en virtud de la cuarta, ninguno de los números así obtenidos en esta sucesión puede ser 0. En

esta forma, los sucesivos que se obtienen constituyen una sucesión indefinida de números. En virtud de la proposición 5, todos los números están en la sucesión, que comienza con 0 y continúan con la de los sucesivos números, porque: a) 0 pertenece a esta sucesión y b) si un numero " n " pertenece a ella, lo mismo ocurre con su sucesivo " $n+1$ " de donde por inducción matemática todo numero pertenece a esta sucesión.

Sin embargo los procedimientos de Peano son menos absolutos de lo que parecen, porque las 3 ideas primitivas son susceptibles a recibir un número infinito de interpretaciones diferentes que satisfacen a las 5 proposiciones primitivas. Por ejemplo: supongamos que 0 signifique 100 y que por numero se entienda todo elemento de la sucesión de los números naturales a partir de 100. Entonces todas nuestras proposiciones primitivas quedarán satisfechas aún la cuarta, porque, si bien es cierto que 100 es sucesivo de 99, debe tenerse presente que 99 no es un número en el sentido que hemos dado ahora a la palabra numero. Es evidente que cualquier número puede

reemplazar a 100 para significar el 0.

Esta imposibilidad de definir cero, número y sucesivo por medio de los 5 axiomas, es decir explicarlos en términos de otros conceptos más simples, y la necesidad de entender su significado independientemente son un hecho importante, ya que un sistema en el que 1 significase 100, y 2 101, podría funcionar muy bien para la matemática pura, pero no serviría para la matemática cotidiana.

De acuerdo al libro "Introducción a la filosofía matemática" Russell expone estas razones por las cuales la teoría de Peano no es en realidad tan definitivo como parece, pero aún así representa para él, el perfeccionamiento matemático de la aritméticaización de la matemática.

En la primera parte del artículo nos acercamos a la noción de número: "... la evaluación de cualquier conjunto dado de elementos queda reducida a la selección de conjuntos de modelos que puedan ser puestos en correspondencia biunívoca con el conjunto dado..." Esta podría ser una de las respuestas a ¿qué es un número? Según Russell, Frege dio la correcta en su *Grundlagen der Arithmetik* en 1884. Este libro no despertó la suficiente atención quedando su definición de número totalmente ignorada, en consecuencia, el mismo Russell la resurgió en 1901 y hoy en día es la definición corriente.

A continuación trataremos de mostrar cuál fue el procedi-

miento y cuál el resultado de esta definición.

En los intento de dar una definición de número muchos filósofos se plantean una definición de pluralidad, pero número es lo que caracteriza a los números. Un trío de aves es un ejemplo del numero 3, y el numero tres es un ejemplo de numero. En consecuencia 3 es algo común a todos los tríos. Entonces un número es algo que caracteriza a determinados conjuntos, concretamente los que tengan ese número.

Un conjunto o clase puede definirse de dos maneras por extensión o comprensión. Una definición extensiva puede siempre reducirse a una comprensiva, en cambio una definición comprensiva no siempre puede reducirse a una extensiva.

A menudo podemos conocer bastante a una clase sin ser capaces de enumerar sus miembros. Nadie podría enumerar todos los habitantes de Buenos Aires, y sin embargo es mucho lo que se sabe de esta clase. Este hecho basta para mostrar que no es necesaria la definición por extensión para conocer una clase.

Cuando buscamos la definición de número estas observaciones son importantes; porque los mismos números forman un conjunto infinito y no pueden ser definidos por enumeración. Por lo tanto tal conjunto tiene que ser definido por comprensión, es decir por una propiedad común a todos los miembros.

El número es una manera de agrupar ciertos conjuntos que tienen un número dado de elementos. Podemos imaginar todas las parejas en un fajo, todos los tríos en otro y así sucesivamente obtenemos de este modo varios fajos de conjuntos donde cada fajo consiste en todos los conjuntos que tienen un número determinado de elementos.

Pero... ¿Cómo hemos de decidir si dos conjuntos pertenecen al mismo fajo? Es obvio que cuando tengan la misma cantidad de elementos, ¿Pero cuándo dos elementos tienen la misma cantidad de elementos?; si hay una relación "uno a uno" entre los elementos de una clase y los elementos de la otra, cuando esto sucede se dice que las clases son semejantes entre sí. Es fácil demostrar que esta relación de semejanza es una relación de equivalencia por lo tanto produce una partición del conjunto en subconjuntos disjuntos de manera tal que cada elemento se relacione con todos los elementos del conjunto y solamente con ellos. Cada subconjunto de la partición es una clase.

Es importante destacar que la noción de semejanza no exige un orden y ni tampoco las clases sean necesariamente infinitas. Podemos así emplear la noción de semejanza para decidir cuando han de pertenecer a un mismo fajo dos conjuntos.

Cada fajo es una clase, cuyos elementos son conjuntos, o sea clases, cada uno es pues una clase de clases. El fajo

compuesto por todas las parejas es una clase con un número infinito de elementos, cada uno de los cuales, es una clase de 2 elementos.

Sin embargo, cuando se intenta dar la autentica definición de número parece inevitable caer en una paradoja, ya que tendemos a pensar que la clase de las parejas es incuestionable en tanto que el número 2 es una entidad metafísica y nunca podemos tener la certeza de que exista. Por lo tanto, es más prudente limitarnos a la clase de las parejas, en lugar del número 2. En consecuencia se establece la siguiente definición:

El número de una clase es la clase de todas las clases semejante a ella

Así el número de una pareja será la clase de todas las parejas. A partir de aquí podemos proseguir a definir los núme-

ros en general como cualquiera de los fajos en que la semejanza agrupa a las clases. Un número será un conjunto de clases tales que dos cualquiera de ellas sean semejantes entre si y que ninguna clase no incluida en el conjunto se semejante a ninguna incluida en él. Ya definido el número de una clase podemos decir que:

Un número es todo aquello que sea el número de alguna clase.

Esta definición tiene la apariencia verbal de un círculo vicioso, pero de hecho no lo es. Hemos definido "el número de una clase dada" sin recurrir a la noción de número en general. Esta definición es aplicable a los conjuntos finitos queda por ver si también será aplicable a los conjuntos infinitos.

Como toda teoría, esta definición responde a un modelo

que tiene un determinado lugar en la historia y responde a determinadas necesidades, lo cual deja abierta la posibilidad de nuevas teorías que la reemplacen.

Carla Finiello *

Yanina Martínez *

Andrea Morales *

*Estudiante de 4º año del I.S.P. "Dr. J.V. González"

Bibliografía:

* DANTZIG, Tobias – *El número, lenguaje de la ciencia* – Hobbs - Sudamericana - Buenos Aires, 1971.

* NEWMAN, James – *El mundo de las matemáticas* – Ediciones Grijalbo - Barcelona, 1994.

* RUSSELL, Bertrand – *Introducción a la filosofía matemática* - Londres, 1956



Definición: Los agujeros negros son esos puntos donde Dios se ha equivocado y ha dividido por cero.

Visitando el mateuba MUSEUM

El profesor Leonard Echagüe es docente adjunto de *Matemática para la Arquitectura y el Diseño Industrial*, materia que se dicta en la Facultad de Arquitectura y Urbanismo de la U.B.A., cátedras de la Dra. Spinadel y del Arq. Matiello. Hace más de 15 años que se dedica al diseño matemático: *Hago modelos de topología, geometría diferencial, ese tipo de cosas, pero esto me pareció más interesante para el Departamento (de Matemática de la Facultad de Cs. Exactas y Naturales), porque es más social: no hace falta saber matemática para entenderlos, son muy sencillos, son conceptos que se ven directos.*



Leonard Echagüe
E-mail: visital@dm.uba.ar

Esta original idea de presentar un museo matemático surgió a propósito de su dictado de la materia. La realización, construcción, financiación y diseños particulares han estado enteramente a cargo de los alumnos del Curso Piloto de los años 1997/1998.

El resultado: un material interesantísimo y valioso por dos motivos. El primero: es accesible no sólo a los estudiantes y/o docentes de matemática, dado que no requiere un conocimiento profundo de la misma. El segundo: conjuga en una sola expresión las tres vertientes que componen este trabajo: la matemática

computacional (para la elaboración de los modelos), la matemática teórica (de donde surgen los modelos a realizar) y el trabajo de taller, con sus innumerables complicaciones (elección de materiales apropiados, precisión en lo constructivo, manejo de herramientas y maquinarias diversas, etc.)

Dialogamos con el prof. Leonard Echagüe.

¿Cómo surgió la realización de esta idea?

Parafraseando al alemán Hegel, para el cual la historia es el despliegue de La Idea, que se actualiza o efectiviza en los acontecimientos, más allá de las voluntades de sus personajes, este Museo responde en su efectivización también a una Idea (que por abuso de sentido filosófico denotamos con mayúscula y que, lógicamente, no es La Idea hegeliana).

Esta idea de los museos matemáticos, tan alemana también, de esa Alemania de fines del siglo XIX y principios del XX, con sus cátedras de matemática poseedoras de piezas de yeso y alambre ilustrando superficies y curvas algebraicas, esa Alemania que nos dio la Bauhaus, la Escuela de Frankfurt, el expresionismo plástico, el dodecafonismo musical, las filosofías de Schopenhauer, Nietzsche y Husserl, y el psicoanálisis, y que en matemática nos dio a Riemann, Klein y el genio hilbertiano como cúspide de su realización.

Se cultivaba por ese entonces también, un aspecto visual en la expresión de los conceptos matemáticos.

Hoy, a fines del siglo XX, por otras y no las mejores razones, se retorna a la imagen, la representación deja paso a la presentación que avanza implacable sobre su campo, las dinámicas sociales de los actos consumados avanzan sobre la de los diálogos acuerdistas previos.

Mas, sin embargo, podemos llenar de sentido este estado de vacío que se va imponiendo, justamente retomando ese otro uso de la imagen y de lo visual, uso para la expresión de ideas y contenidos, uso lúdico, uso comunicativo.

Este proyecto de museo es tributario de esa tradición, arriba evocada, de la visualización como expresión de las ideas y no como reemplazo de la abstracción, complementaria a la abstracción, posibilitadora y facilitadora de la abstracción.

¿Cuál es el modo de realización de esta idea?

En primer lugar, es interactivo. El concepto matemático se ilustra por la respuesta del modelo a la acción del que la ejecuta, esto hace a una consideración conceptual constructiva donde el que usa el modelo tiene intervención en cómo incorpora el concepto matemático a su bagaje cultural. En segundo término, hay un modo estándar de elección de los modelos Una forma rápida de definir estándar en este contexto sería decir "Los modelos que más o menos están en la sección matemática de la mayoría de los museos de ciencia..."

Precisando un tanto se quiere decir:

1. Que conste de la mínima cantidad de modelos necesarios para que se ilustren las propiedades matemáticas más elementales y conocidas.
2. Que la ilustración de propiedades y conceptos matemáticos sea directa, significando esto que el funcionamiento del modelo realiza el concepto, diferenciándose de los modelos sobre teorías matemáticas complejas (topología, álgebra superior) que requieren de su conocimiento para interpretar cómo el modelo ilustra las teorías.
3. Que su utilización sea sencilla y cómoda y que sean atractivos, llamativos o interesantes visualmente en su construcción.

¿Cuáles son las condiciones que posibilitan la realización de esta idea?

* *Un claro concepto de una matemática para el diseño industrial que logre:*

- *Un enfoque operacional de conceptos matemáticos aplicables mediante el uso de la computadora (software Maple V, AUTOCAD) y con su justa interpretación geométrica.*
- *Solidez en el manejo de las herramientas y de las reglas de las artes para pasar de la geometría al trabajo de los materiales adecuadamente en función de obtener el objeto-producto en la forma deseada.*

* *Respaldo institucional de:*

- *Unas cátedras dispuestas a afrontar las consecuencias de la innovación didáctico-tecnológica.*
- *Un departamento académico receptivo a la instalación de un nuevo ámbito en su seno.*
- *Una secretaría académica que sostiene por cargo propio a docentes innovadores.*

* *Alumnado consecuente:*

- *Varios grupos de alumnos dispuestos a financiar económicamente los materiales y a trabajar arduamente para conseguir lo requerido por el proyecto.*

Con relación a los alumnos, ¿cuántos componen un curso, cómo se logra organizarlos? Aproximadamente unas 60 personas y están divididas en dos grandes grupos: el de Diseño Industrial y el de Arquitectura; a su vez, conforman grupos de trabajo con tres a cinco alumnos por grupo. Los de Diseño Industrial fueron los encargados, esencialmente, de realizar las máquinas en tanto que los de Arquitectura tuvieron a su cargo dos tareas: la ambientación del Museo (iluminación, circuitos eléctricos, alfombra, tapiz, mesa y bancos de trabajo) y el rubro señalética.

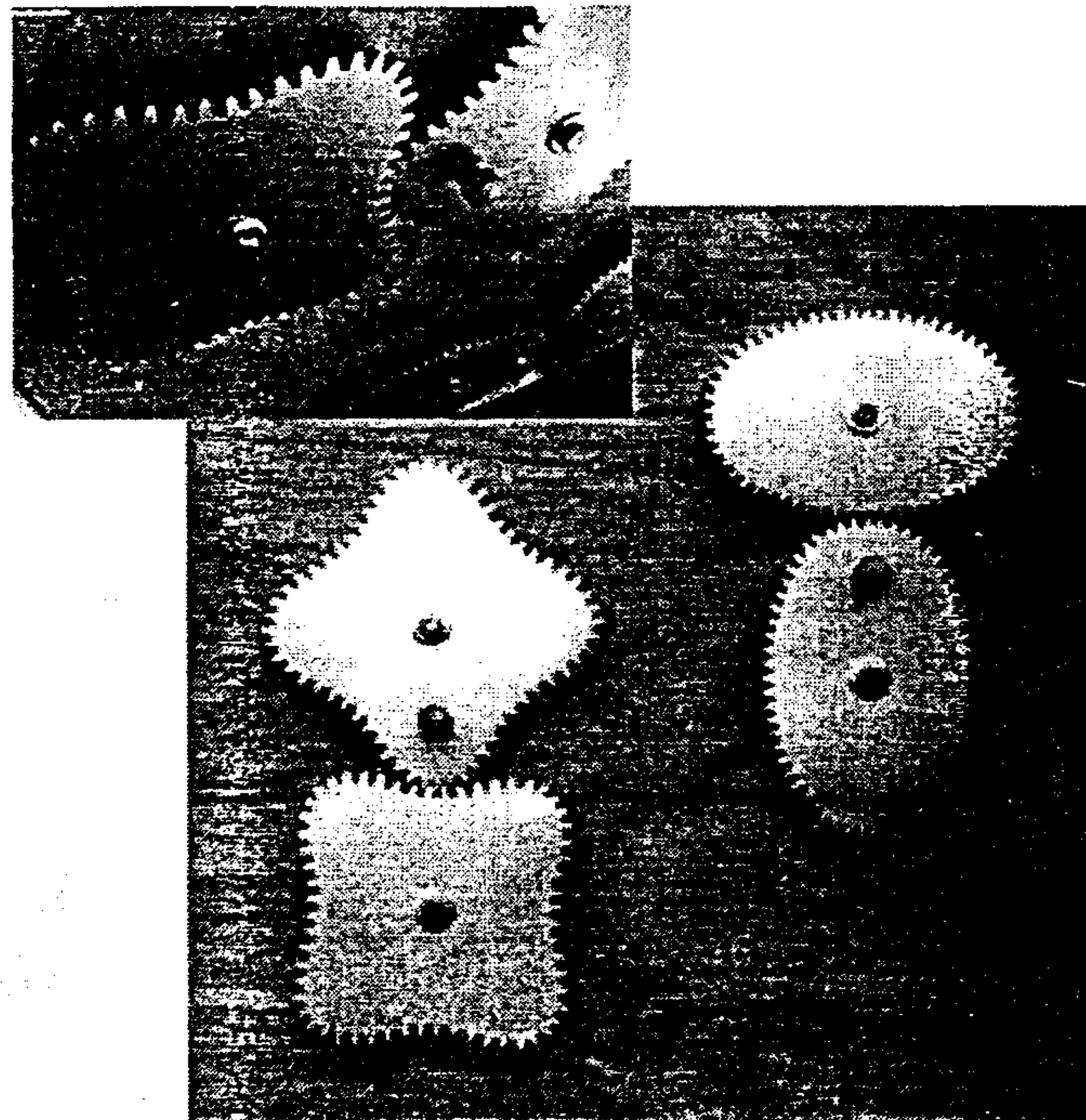
Recorrida por el Museo

Con todas estas aclaraciones, iniciamos la recorrida por el Museo, a medida que Leonard va explicando el funcionamiento de cada una de las máquinas y objetos expuestos.

Máquina de Plateau de superficies mínimas: se llena una cuba con agua jabonosa y al sumergir marcos metálicos de formas diversas produce superficies de film jabonoso. Se pueden observar un catenoide, una superficie de Schwarz, un helicoide y un camino mínimo.

Máquina de poleas (una circular y otra elíptica), las levas rotantes de forma circular excéntrica y elíptica focal con tomas de movimiento radiales y tangenciales y las bielas encadenadas, en las que un punto de la barra central describe una curva.

Máquina de engranajes: este es el modelo más difícil del lugar porque los engranajes están hechos a mano en resina poliéster.



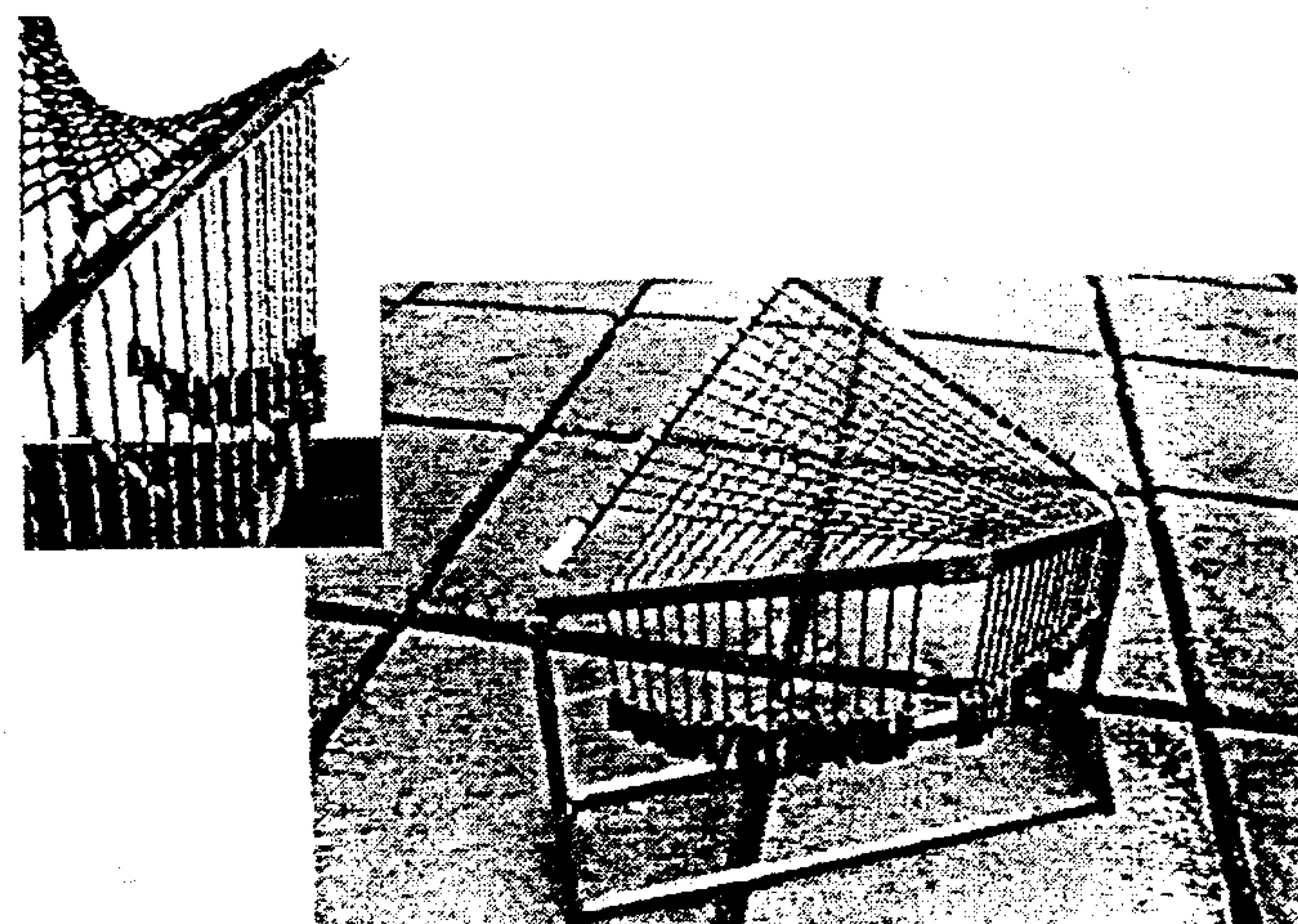
Máquina de engranajes

Se trata de dos juegos de engranajes dentados de formas elíptica y oval tetralobulada. La

construcción del óvalo lobulado se hace de acuerdo con Artobolevski, autor de un libro de mecanismos muy grande. Se observa que a una rotación uniforme de un engranaje, su pareja responde de modo variable. Estas curvas cerradas son unos de los pocos ejemplos de rotación dentada entre curvas iguales.

Máquina de hiperboloide: muestra cómo se genera una superficie reglada a partir de dos segmentos de rectas alabeadas que giran entre sí. El móvil genera un hiperboloide circular y pasa por una ramura de forma hiperbólica que corresponde al corte del hiperboloide con un plano vertical.

Máquinas de cuádricas: son dos mecanismos que generan respectivamente, un paraboloide hiperbólico (la silla de montar) y un hiperboloide. Están construidos con marcos móviles de madera y sogas. Han sido copiados de otros museos así como hay diseños que son totalmente míos.



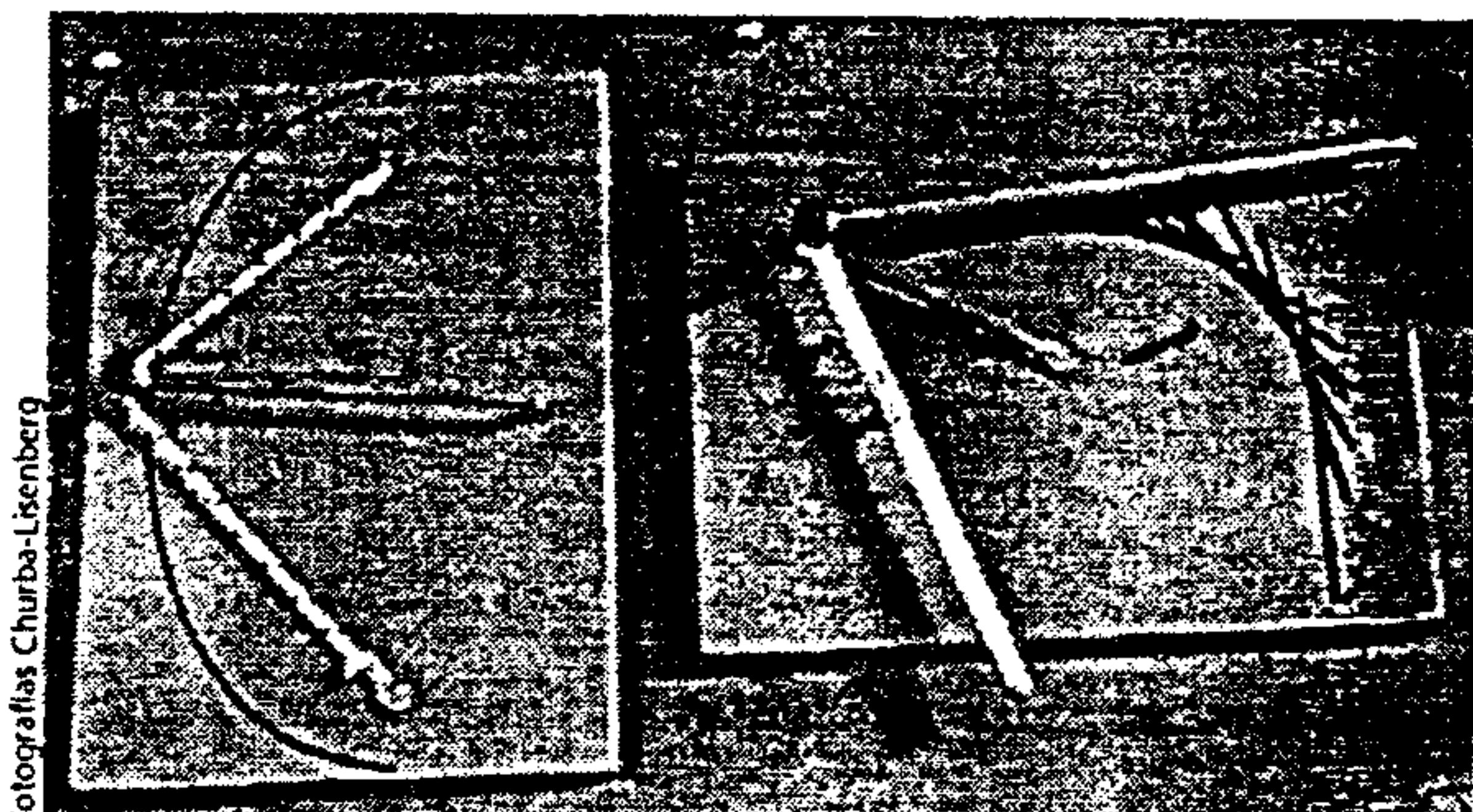
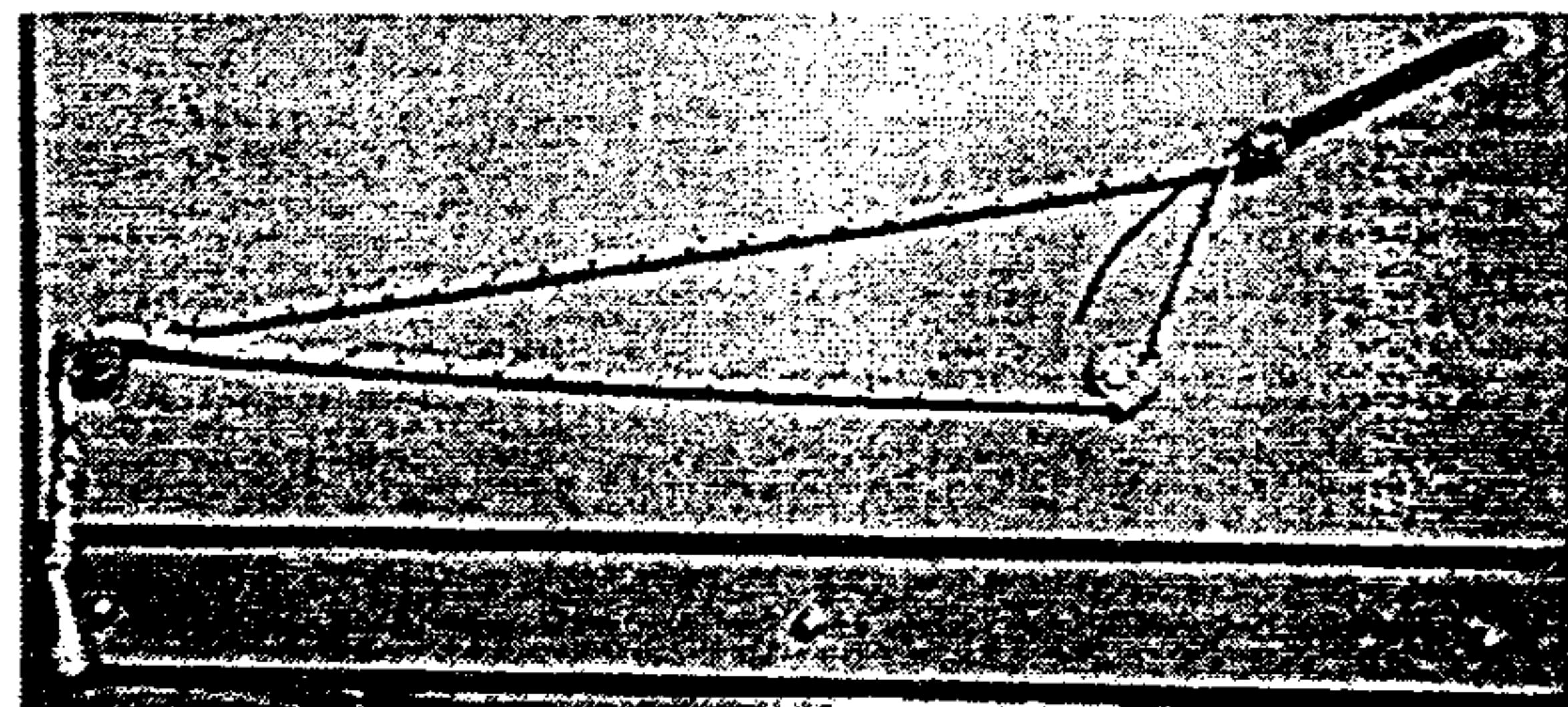
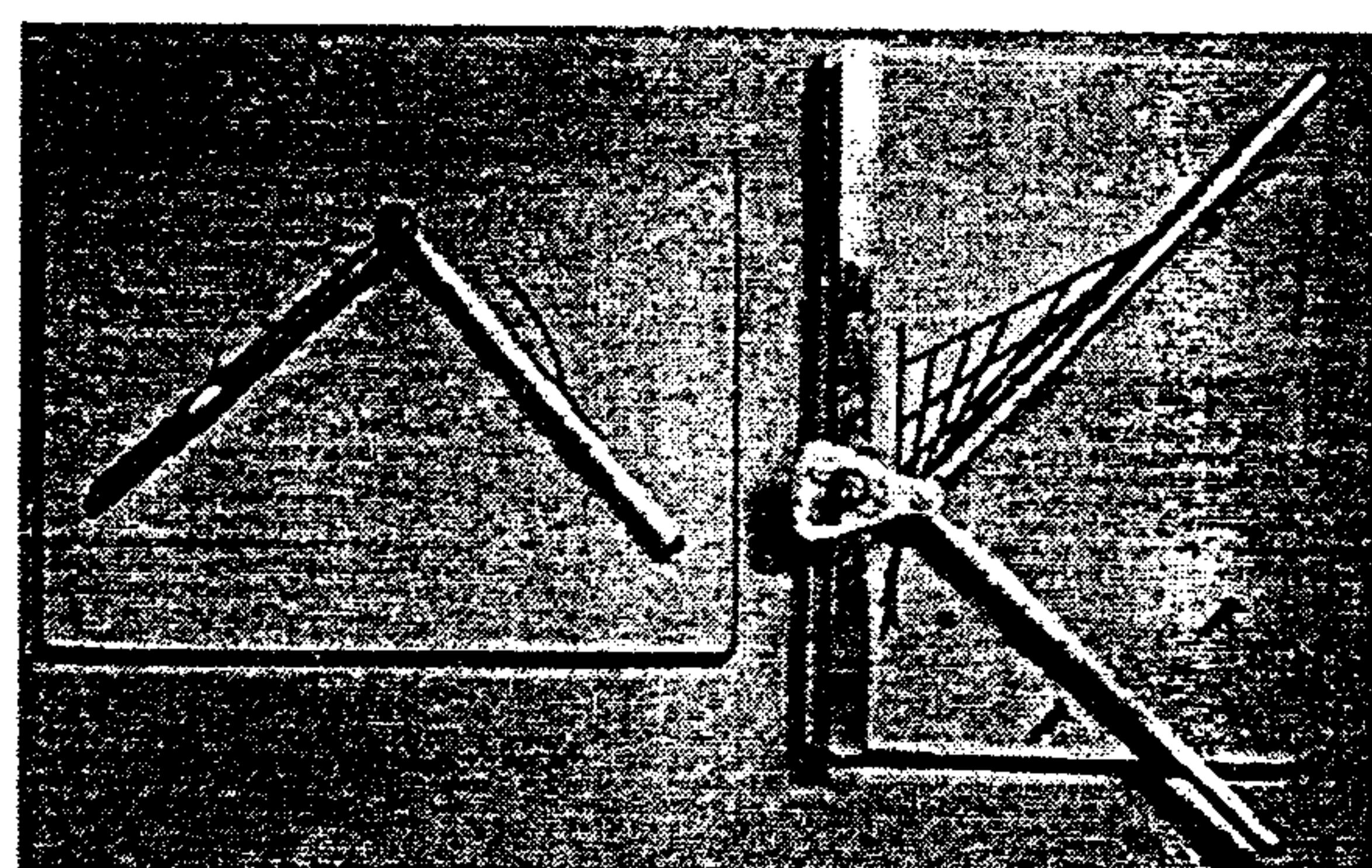
Máquinas de cuádricas

Máquina de integrar: este mecanismo está formado por un carro de movimiento horizontal y dos subcarros (uno derivador y otro integrador) de movimiento vertical. El derivador toma la ordenada de la función haciendo que la guía del integrador quede inclinada de manera tal que la tangente de su ángulo sea proporcional a aquella ordenada. Esto hace que el derivador indique la pendiente de la curva trazada por el integrador o, lo

mismo, que éste integre la curva del derivador. Fue diseñado por Abdank Abakanowitz. Una detallada explicación del mismo se encuentra en el libro *Análisis Matemático*, de Rey Pastor, Pi Calleja y Trejo.

Máquinas lógicas: están constituidas por tres circuitos lógicos eléctricos. Al cumplirse la veracidad de las fórmulas que representan, se encienden las respectivas lámparas

Máquinas de cónicas: son cinco mecanismos que permiten dibujar curvas por trazado puntual (trazador angular recto de semicircunferencia, trazador de elipse, trazador de hipérbola) o tangencial (trazador de parábolas, trazador de elipses). Están sacadas de un libro de geometría de Descartes.



Máquinas de cónicas

Máquina de evolventes y evolutas: están representadas tres curvas: la catenaria, la

tractriz y la cicloide. Esta última es evolvente y evoluta de sí misma, la catenaria es evoluta de la tractriz y la tractriz es evolvente de la catenaria.

Máquina de cicloides y trocoïdes: están constituidas por ruedas dentadas que giran, en un caso, sobre una recta dentada y en el otro, sobre otra rueda dentada fija.

Máquina de Moëbius: Está inspirada en una del Museo de California que vi dibujada. Está hecha en bronce que es lo más barato. El carrito que recorre la banda en su zona central, muestra cómo la flecha cambia de dirección, debido a que la cinta no tiene un campo normal, y de sentido, al dar una vuelta completa.

Billar elíptico: permite demostrar la propiedad de reflexión de los focos de una elipse; si una bola pasa por un foco y choca contra la banda lateral, rebotará pasando, necesariamente, por el otro foco.

Alfombra circular: representa un teselado hiperbólico. Mide 3,50 m de diámetro.



Alfombra representando un teselado de plano hiperbólico

Apilables cónicos: es un cono integrado por cuatro piezas, cada una de las cuales representa la intersección con un plano, formando una

elipse, una hipérbola y una parábola. Lo interesante de esto son los cálculos matemáticos para dar las plantillas. Este cono está apoyado sobre una Mesa cuya base es un hiperboloide.

Máquina de Galton: es una máquina de probabilidades, compuesta por unas 800 bolillas de acero que tienen que atravesar un entramado de clavos. Al acomodarse en cada tronera, resulta una gaussiana, que es mucho más puntada que la curva normal de probabilidades que conocemos de los libros. Los clavos están colocados bastante cerca unos de otros para evitar efectos de inercia y lograr que la probabilidad de ir a izquierda o derecha sea efectivamente.

Es interesante observar algunos detalles constructivos, como por ejemplo, el montaje de la máquina sobre un eje giratorio fijado a la pared, teniendo en cuenta que el peso es cercano a los 30 Kg.

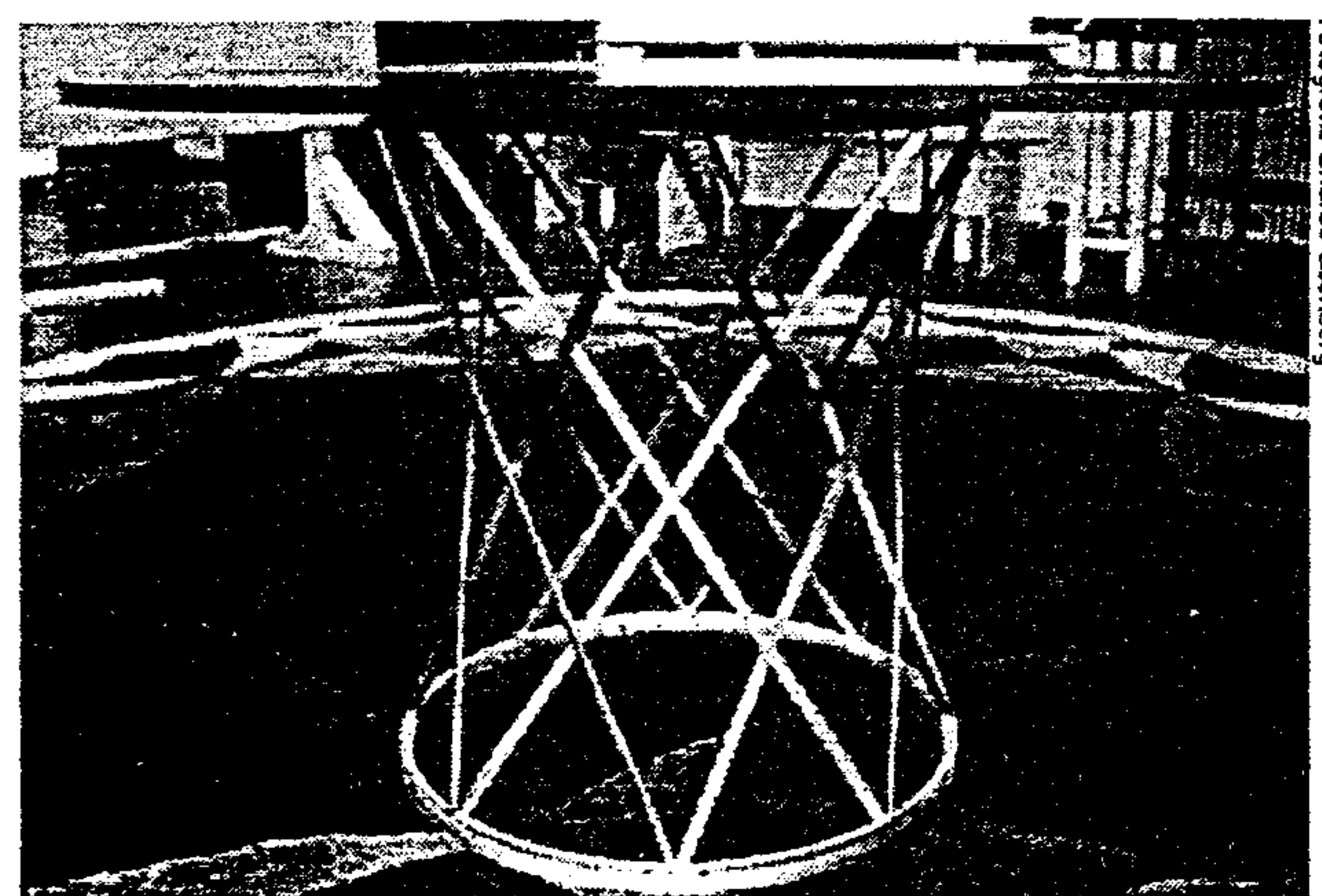
Máquina de transformación de un catenoide en un helicoide: permite observar una transformación localmente isométrica. La superficie de tela que recubre al catenoide de revolución también "viste" al helicoide circular recto.

Máquina de caída de carril por recta y cicloide: consta de dos tubos, uno recto y otro curvado según la forma de cicloide, a los que están adosados sendos carros de rodamiento. Permite observar que soltando ambos carros al mismo tiempo, llega primero al piso el que recorre la cicloide ya que minimiza el tiempo.

Máquinas de cadenas colgantes: describen claramente la diferencia entre la catenaria (densidad de masa proporcional a la longitud de arco) y la parábola (densidad de masa proporcional a la coordenada horizontal). Se logran colgando pesos de una cadena que cumplan las propiedades enunciadas.

En todo lo expuesto hay lazos conceptuales, ya que la parábola aparece aquí, en el cono, en el parabolóide y en las trazadoras de cónicas;

la catenaria, en las cadenas, en las burbujas de la máquina de Plateau y en el catenoide; el helicoide aparece como superficie mínima y en la isometría con el catenoide.



Mesa matemática

Es interesante ver cómo se pueden materializar las curvas, ya que al nivel del profesorado estamos acostumbrados a estudiarlas a través de alguna fórmula o a dibujarlas.

Una herramienta fuerte que hay para las curvas son las bases de Groebner que son para resolver ecuaciones polinomiales. Hay varias ecuaciones dando vueltas; los trazados de las bielas, por ejemplo, salen con bases de Groebner, porque son ecuaciones pitagóricas, la computadora las resuelve sola, saca el trazado de las curvas.

¿Qué se requiere para cargar el programa Maple?

Nada. Con una 386 con 3 mega, funciona. Seguimos conversando animadamente por un largo rato. Salí con la impresión de haber conocido una cantidad enorme de elementos que, a disposición de nuestros alumnos y de nosotros mismos, nos muestra un nuevo panorama que completa y complementa nuestra actividad cotidiana en las aulas.

Raquel Kalizsky*

* Prof. de Matemática egresada del I.S.P. "Dr. J. V. González"

Curiosidades matemáticas.

Teoría de Números y Criptografía.

El presente artículo es una versión corregida y aumentada de la charla que el autor dictó el viernes 21 de agosto de 1998 en el I.S.P. Dr. Joaquín V. González. Durante la misma se introdujeron conceptos relativos a la Teoría de Números, y se mostraron algunas de sus aplicaciones actuales.

La clave pública

Nuestro objetivo en esta nota es mostrar algunas de las ideas centrales de la Teoría de Números. Exhibiremos resultados fundamentales de esta rama de la Matemática y mostraremos asimismo aplicaciones modernas de ellos. Veremos cómo la Teoría de Números resulta útil para la elaboración de métodos de codificación de mensajes, en particular estudiaremos el problema de la construcción de una **clave pública**.

El hecho de codificar un mensaje puede asimilarse completamente al proceso de aplicar una cierta función, que llamaremos COD, a una cadena de símbolos (el mensaje). La aplicación de esta función COD da como resultado una nueva cadena de símbolos (el mensaje codificado).

Existe asimismo otra función, que llamaremos DEC, la cual corresponde al proceso de decodificación del mensaje. Dado el mensaje codificado, esta función nos devuelve el mensaje original. La función DEC es, por supuesto, la inversa de COD.

Un método sencillo de codificación consiste en reemplazar cada letra del mensaje por un número. Por ejemplo, podemos establecer que A se reemplace por 01, B por 02, etc. Pueden asimismo agregarse números que representen los espacios entre palabras o los signos de puntuación. La función COD se definiría entonces como aquella que sustituye cada letra (o signo de puntuación) por el número establecido, mientras que la función DEC sería la que efectúa la sustitución opuesta.

En el ejemplo que acabamos de esbozar, así como en muchos otros ejemplos, quien conozca la definición de la función COD conocerá también inmediatamente la definición de DEC. Es decir,

quien sepa codificar un mensaje, inevitablemente sabrá también decodificarlo.

El problema de la clave pública consiste en elaborar un código tal que el sistema de codificación pueda hacerse público, al mismo tiempo el método de decodificación permanece en secreto. Es decir, el problema consiste en hallar una función COD tal que, aún sabiendo su definición, no seamos capaces de deducir la definición de DEC.

Si poseyéramos una clave pública podríamos recibir mensajes codificados sin temor de que estos sean interceptados por terceros. El sistema COD de codificación podría ser perfectamente público, sin embargo los mensajes que nos enviasen estarían a salvo, pues sólo nosotros conoceríamos el método DEC para decodificarlos.

Otra aplicación posible para una clave pública deriva de su utilidad para la validación de firmas. Imaginemos, por ejemplo, que el Sr. Juan Xavier Equis va a enviar un cierto mensaje (de vital importancia) al Sr. José Zeta.

Por motivos que no viene al caso detallar, existe la posibilidad de que el Sr. Zeta sospeche que el mensaje que recibe es falso y crea que no es en verdad Juan X. Equis quien se lo ha enviado. ¿Cómo puede entonces Juan X convencer a José Z. de que es él, y no un impostor, quien le envía el mensaje?

Imaginemos además que la comunicación se envía por un medio electrónico, por lo que la prueba de la autenticidad no puede establecerse a partir de un análisis caligráfico de la firma ni ningún otro procedimiento similar. La prueba debe obtenerse exclusivamente a partir del **contenido** del mensaje.

El dilema podría resolverse si Juan X. fuera el afortunado poseedor de una clave pública. Su-

pongamos, entonces, que fuera posible hallar dos funciones COD y DEC (una la inversa de la otra) tales que, mientras que COD es conocida públicamente, por el contrario DEC sólo es conocida por Juan X. (y nadie más en el mundo). Para simplificar el ejemplo, digamos que tanto COD como DEC transforman cadenas de letras en cadenas de letras.

Si Juan X. desea probar que es él en verdad quien envía el mensaje sólo debe apelar al siguiente procedimiento. Escribe su nombre: "Juan Xavier Equis" y le aplica la función DEC (sólo conocida por él). Obtendrá así una cadena ilegible de letras, digamos: "aaBNbbGyyyuiT". Juan firma entonces el mensaje con esta cadena ilegible de letras.

José Zeta recibe el mensaje y le aplica a la cadena ilegible que lleva como firma la públicamente conocida función COD. Como ésta es la inversa de DEC, José obtendrá como resultado la cadena original "Juan Xavier Equis".

De este modo José Z. sabrá sin lugar a dudas que la firma del mensaje que recibió se obtuvo mediante la aplicación de la función DEC. Como la única persona que conoce la definición de DEC es Juan Equis, entonces José estará seguro de que es aquél, y nadie más, quien ha enviado el mensaje.⁽¹⁾

El problema del que vamos a ocuparnos entonces es el de la construcción efectiva de una clave pública. Esta construcción requiere la utilización de varios elementos provenientes de la Teoría de Números.

La función de Euler

Para comenzar a adentrarnos en el tema, recordemos algunas definiciones básicas. Decimos que un entero $p > 1$ es **primo** si sus únicos divisores positivos son el propio número p y el número 1. Los primeros primos positivos son: 2, 3, 5, 7, 11, 13. Por razones técnicas, el número 1 no se considera primo.

Dados dos enteros a y b , indicaremos por $(a:b)$ a su máximo común divisor. Diremos asimismo que a y b son **coprimos** si $(a:b) = 1$; esta afir-

mación equivale a decir que no existe ningún primo p que sea a la vez divisor de a y de b .

Una vez que hemos repasado estos conceptos básicos podemos encarar la definición de la herramienta más importante de las que utilizaremos en esta nota. Nos referimos a la llamada **función Φ de Euler** (Φ es la letra griega "fi" mayúscula). Dado un número natural n , llamaremos $R(n)$ al conjunto:

$$R(n) = \{k \in \mathbb{N} : 1 \leq k \leq n \wedge (n:k) = 1\}$$

Donde \mathbb{N} es el conjunto de los números naturales. Por ejemplo:

$R(1) = \{1\}$	$R(2) = \{1\}$
$R(3) = \{1, 2\}$	$R(4) = \{1, 3\}$
$R(5) = \{1, 2, 3, 4\}$	$R(6) = \{1, 5\}$

Definimos la función $\Phi: \mathbb{N} \rightarrow \mathbb{N}$ del siguiente modo: $\Phi(n)$ es igual a la cantidad de elementos (o *cardinal*) del conjunto $R(n)$. A partir de los ejemplos precedentes podemos ver que:

$\Phi(1) = 1$	$\Phi(2) = 1$	$\Phi(3) = 2$
$\Phi(4) = 2$	$\Phi(5) = 4$	$\Phi(6) = 2$

A fin de que pueda Ud. familiarizarse con esta definición así como con algunas de las características básicas de la función Φ , le sugerimos que, antes de continuar la lectura, resuelva el siguiente ejercicio:

Ejercicio 1: a) Calcular el valor de $\Phi(7)$, $\Phi(8)$, $\Phi(9)$ y $\Phi(10)$.

b) Sea $p \in \mathbb{N}$ un número primo y $a \in \mathbb{N}$ un entero positivo cualquiera. Demostrar que si p no es divisor de a entonces $(a:p) = 1$.

c) Demostrar que si $p \in \mathbb{N}$ es un número primo entonces $\Phi(p) = p-1$.

Demostremos por nuestra parte que si p es un número primo positivo y $n \in \mathbb{N}$ entonces se verifica que $\Phi(p^n) = p^{n-1}(p-1)$.

En efecto, veamos cómo podemos construir el conjunto $R(p^n)$, formado por todos los números

entre 1 y p^n que sean coprimos con p^n . Para ello debemos observar que k es coprimo con p^n si y sólo k no es múltiplo de p . Ahora bien, entre 1 y p^n los números que sí son múltiplos de p son los siguientes:

$$1p; 2p; 3p; 4p; \dots; p^{n-2}p = p^{n-1}; p^{n-1}p = p^n \quad (1)$$

Por lo tanto, al construir $R(p^n)$ los números que aparecen en la lista (1) deben ser retirados del conjunto de todos los números entre 1 y p^n . Como la lista (1) contiene p^{n-1} números, entonces $R(p^n)$ tendrá un cardinal igual a $p^n - p^{n-1}$. En consecuencia, $\Phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$, que es lo que queríamos demostrar.

Una propiedad importante

Uno de los teoremas esenciales relacionados con la función Φ afirma que si n y m son dos números naturales tales que $(n:m) = 1$, entonces $\Phi(nm) = \Phi(n)\Phi(m)$. Por ejemplo $\Phi(6) = \Phi(2 \cdot 3) = \Phi(2)\Phi(3) = 1 \cdot 2 = 2$. El **ejercicio 2**, tal como aparece más abajo, muestra paso a paso una forma de realizar la demostración de este teorema.

Ejercicio 2: Sean $n \in \mathbb{N}$ y $m \in \mathbb{N}$ dos enteros tales que $(n:m) = 1$. El objetivo de este ejercicio es demostrar que $\Phi(nm) = \Phi(n)\Phi(m)$.

- a) Probar que existen $A \in \mathbb{Z}$ y $B \in \mathbb{Z}$ tales que $mA \equiv 1(n)$ y $nB \equiv 1(m)$.
 - b) Sean $a \in \mathbb{N}$ y $b \in \mathbb{N}$ dos números cualesquiera tales que $1 \leq a \leq n$, $1 \leq b \leq m$. Definimos el número X como $X = amA + bnB$ (donde A y B son los números del punto anterior). Probar que X verifica simultáneamente que $X \equiv a \pmod{n}$ y $X \equiv b \pmod{m}$.
 - c) Sea $Y \in \mathbb{Z}$ un entero que verifica simultáneamente que $Y \equiv a \pmod{n}$ e $Y \equiv b \pmod{m}$. Demostrar que existe $k \in \mathbb{Z}$ tal que $Y = X + knm$.
 - d) Deducir que, dados $a \in \mathbb{N}$ y $b \in \mathbb{N}$ dos números cualesquiera tales que $1 \leq a \leq n$, $1 \leq b \leq m$, existe un único $X \in \mathbb{N}$, $1 \leq X \leq nm$, que verifica simultáneamente que $X \equiv a \pmod{n}$ y $X \equiv b \pmod{m}$.
- (Nota:** Este enunciado es un caso particular del llamado Teorema Chino del Resto).

e) Sea $X \in \mathbb{N}$ el número mencionado en el punto anterior. Probar que si $(a:n) = 1$ y $(b:m) = 1$ entonces $(X:nm) = 1$.

f) Para cada $k \in \mathbb{N}$ sea $R(k) = \{x \in \mathbb{N} : 1 \leq x \leq k \wedge (x:k) = 1\}$.

Definimos la función $F: R(n) \times R(m) \rightarrow R(nm)$ del siguiente modo: $F(a,b) = X$ donde X es el número mencionado en el punto d). Deducir de los puntos anteriores que F está bien definida y es biyectiva.

g) Deducir de f) que $\Phi(nm) = \Phi(n)\Phi(m)$ si $(n:m) = 1$.

h) Mostrar con un contraejemplo que la afirmación es falsa si $(n:m) \neq 1$.

Gracias al principio de inducción, es fácil verificar que este teorema puede generalizarse del siguiente modo. Si n_1, \dots, n_r son números naturales coprimos dos a dos entonces:

$$\Phi(n_1 \cdot n_2 \cdots n_r) = \Phi(n_1)\Phi(n_2) \cdots \Phi(n_r) \quad (2)$$

Esta propiedad, junto con el resultado que nos dice que $\Phi(p^n) = p^{n-1}(p-1)$, nos permiten deducir, en cierto modo, una fórmula para calcular la función Φ . En efecto, sea n un número natural mayor que 1. Consideremos su descomposición en factores primos:

$$n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

Donde p_1, \dots, p_r son todos números primos diferentes. Si llamamos $n_k = p_k^{m_k}$ ($1 \leq k \leq r$), entonces los números n_1, \dots, n_r son coprimos dos a dos y podemos aplicarles la fórmula indicada en (2). Tenemos así que:

$$\Phi(n) = \Phi(p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r})$$

$$\Phi(n) = \Phi(n_1 \cdot n_2 \cdots n_r)$$

$$\Phi(n) = \Phi(n_1)\Phi(n_2) \cdots \Phi(n_r)$$

$$\Phi(n) = \Phi(p_1^{m_1})\Phi(p_2^{m_2}) \cdots \Phi(p_r^{m_r})$$

$$\boxed{\Phi(n) = p_1^{m_1-1}(p_1 - 1)p_2^{m_2-1}(p_2 - 1) \cdots p_r^{m_r-1}(p_r - 1)}$$

Es esencial destacar que, para calcular $\Phi(n)$ mediante esta fórmula, es necesario conocer

previamente la descomposición de n en factores primos.

Veamos por ejemplo cómo podemos calcular $\Phi(108)$. Tenemos que $108 = 4 \cdot 27 = 2^2 \cdot 3^3$; luego:

$$\begin{aligned}\Phi(108) &= \Phi(2^2 \cdot 3^3) \\ \Phi(108) &= \Phi(2^2)\Phi(3^3) \\ \Phi(108) &= 2^{2-1}(2-1) \cdot 3^{3-1}(3-1) \\ \Phi(108) &= 36\end{aligned}$$

Para que pueda Ud. afianzar su conocimiento de las propiedades hasta ahora estudiadas de la función Φ , le sugerimos que resuelva los siguientes ejercicios. La solución de todos ellos se obtiene a partir de esas mismas propiedades.

Le hacemos notar que resulta particularmente interesante el **Ejercicio 6**. Éste provee una demostración, basada en la función Φ , de la existencia de infinitos números primos.

Ejercicio 3: Sea $n \in \mathbb{N}$. Probar las siguientes afirmaciones:

- a) Si n es impar entonces $\Phi(2n) = \Phi(n)$.
- b) Si n es par entonces $\Phi(2n) = 2\Phi(n)$.
- c) Si n es múltiplo de 3 entonces $\Phi(3n) = 3\Phi(n)$.
- d) Si n no es múltiplo de 3 entonces $\Phi(3n) = 2\Phi(n)$.
- e) $\Phi(n) = n/2$ si y sólo si $n = 2^k$, $k \geq 1$.

Ejercicio 4: Sean $n \in \mathbb{N}$, $m \in \mathbb{N}$. Probar las siguientes afirmaciones:

- a) Si $n|m$ entonces $\Phi(n)|\Phi(m)$.
- b) $(n:m)\Phi(n)\Phi(m) = \Phi(nm)\Phi((n:m))$.
- c) $\Phi(n)\Phi(m) = \Phi((n:m))\Phi([n:m])$. Donde $[n:m]$ es el m.c.m. entre n y m .

Ejercicio 5:

- a) Hallar todas las soluciones de $\Phi(n) = 8$, $\Phi(n) = 6$, $\Phi(n) = 10$, $\Phi(n) = 16$, $\Phi(n) = 18$, $\Phi(n) = 108$.
- b) Probar que para todo k la ecuación $\Phi(n) = k$ tiene a lo sumo un número finito de soluciones.
- c) **Problema abierto** (conjetura de Carmichael): Para todo k , si la ecuación $\Phi(n) = k$ tiene solución, entonces tiene al menos dos soluciones. Por ejemplo $\Phi(27) = 18 = \Phi(19)$.

Ejercicio 6: El objetivo de este ejercicio es utilizar la función Φ para dar una demostración de la existencia de infinitos primos.

- a) Supóngase que hubiera sólo finitos primos. Sean p_1, \dots, p_r todos los números primos y sea N el producto de todos ellos. Probar que si $m > 1$ entonces $(N:m) \neq 1$.
- b) Deducir de a) que $\Phi(N) = 1$. Por otra parte $\Phi(N) = (p_1-1)\dots(p_r-1)$. Mostrar que se ha llegado a una contradicción y deducir que hay infinitos números primos.

Las funciones multiplicativas

La función Φ es un caso particular de una importante familia de funciones: las **funciones multiplicativas**. Una función $f : \mathbb{N} \rightarrow \mathbb{N} \cup \{0\}$ se dice *multiplicativa* si y sólo si $f(nm) = f(n)f(m)$ toda vez que n y m sean coprimos.

Muchas de las funciones más interesantes de la Teoría de Números resultan ser en verdad funciones multiplicativas. Por ejemplo, caen dentro de este tipo las funciones $\sigma : \mathbb{N} \rightarrow \mathbb{N}$ y $\tau : \mathbb{N} \rightarrow \mathbb{N}$ definidas del siguiente modo:

$\sigma(n) =$ suma de todos los divisores positivos de n (incluyendo el propio n)

$\tau(n) =$ cantidad total de divisores positivos de n (incluyendo el propio n)

Ejercicio 7:

- a) Demostrar que σ y τ son funciones multiplicativas.
- b) Tal como se hizo con la función Φ , hallar fórmulas que permitan calcular $\sigma(n)$ y $\tau(n)$ a partir de la descomposición en primos de n .

Es evidente que σ y τ representan cantidades cuyo estudio es de sumo interés en la Teoría de Números. Por citar un ejemplo, mencionemos a los *números perfectos*.

Se dice que un número natural $n > 1$ es *perfecto* si y sólo si es igual a la suma de sus divisores positivos **propios** (es decir, distintos de n).

Los primeros dos números perfectos son 6 y 28. En efecto, los divisores propios positivos de 6 son 1, 2 y 3; mientras que $1 + 2 + 3 = 6$. Los di-

visores propios positivos de 28 son 1, 2, 4, 7 y 14; mientras que $1 + 2 + 4 + 7 + 14 = 28$.

Notemos que si n es perfecto entonces la suma de todos sus divisores positivos (con n inclusive) debe ser igual a $2n$. Tenemos así que la función σ nos permite caracterizar a los números perfectos. En efecto, un número n es perfecto si y sólo si $\sigma(n) = 2n$.

Aunque el estudio de los números perfectos se remonta al propio Euclides, aún hoy en día se desconoce si existe una cantidad finita o infinita de ellos. Por otra parte, todos los números perfectos conocidos son pares, sin embargo es un problema abierto el saber si existe algún número perfecto impar.

Otro ejemplo de función multiplicativa, que tiene un notable interés teórico, es la llamada función μ de Möbius. Esta función se define del modo siguiente:

$$\mu(1) = 1.$$

$\mu(n) = 0$ si n es divisible por algún cuadrado mayor que 1. Por ejemplo, $\mu(12) = 0$ pues 12 es divisible por 4.

$\mu(n) = (-1)^r$ si n es el producto de r primos diferentes. Por ejemplo, $30 = 2 \cdot 3 \cdot 5$, por lo que $r = 3$ y entonces $\mu(30) = (-1)^3 = -1$.

Ejercicio 8: Demostrar que μ es una función multiplicativa.

El espacio disponible no nos permite desarrollar a conciencia la explicación de porqué la función μ es tan importante. Digamos, sin embargo, que el lector interesado podrá encontrar en el libro de Hans Riesel mencionado en la bibliografía, aplicaciones de las funciones μ y Φ al problema de hallar, en la forma más rápida que sea posible, la factorización en primos de un número n de gran cantidad de cifras. (2)

Breve repaso de congruencias

A pesar de que el estudio de las funciones multiplicativas es atrapante, la verdad es que ahora

debemos volver al tema principal de esta nota, que es, específicamente, el estudio de la función Φ de Euler.

Antes de pasar a la última de las propiedades de esta función que mencionaremos, recordemos brevemente la definición de *congruencia*.

Decimos que dos enteros a y b son *congruentes módulo n* si $b-a$ es múltiplo de n . Equivalentemente, a y b son congruentes módulo n si y sólo si tienen el mismo resto en la división entera por n . En símbolos, esta situación se describe del siguiente modo: $a \equiv b \pmod{n}$.

Distintas aplicaciones y teoremas relativos a este concepto pueden encontrarse en la sección *Apuntes sobre...* de Axioma N° 1, 2 y 3. Enunciemos simplemente aquí las propiedades básicas de la congruencia. Si Ud. no se encuentra suficientemente familiarizado con ella, le sugerimos que, como ejercicio, demuestre la validez de las mismas.

- a) La congruencia módulo n es una relación de equivalencia en el conjunto \mathbb{Z} de los números enteros.
- b) Si $a \equiv b \pmod{n}$ entonces $a - c \equiv b - c \pmod{n}$.
- c) Si $a \equiv b \pmod{n}$ entonces $ac \equiv bc \pmod{n}$.
- d) Si $a \equiv b \pmod{n}$ entonces $a^k \equiv b^k \pmod{n}$.

Para nuestros fines actuales será importante recordar además la siguiente propiedad.

Dados dos enteros a y n , llamaremos $r_n(a)$ al resto que se obtiene al dividir a por n . Por ejemplo $r_3(7) = 1$, $r_5(2) = 2$ y $r_5(25) = 0$. Este número $r_n(a)$ verifica que $0 \leq r_n(a) < n$ y además $a \equiv r_n(a) \pmod{n}$. Por ejemplo, para $r_3(7) = 1$ tenemos que $0 \leq 1 < 7$ y además $7 \equiv 1 \pmod{3}$.

La propiedad que nos interesa destacar dice que, recíprocamente, si r es un número entero tal que $0 \leq r < n$ y además $a \equiv r \pmod{n}$ entonces necesariamente $r = r_n(a)$.

El teorema de Euler-Fermat

El teorema de Euler-Fermat vincula a la función Φ con el concepto de congruencia. Específicamente:

mente este teorema afirma que si a y n son dos números coprimos entonces $a^{\Phi(n)} \equiv 1(n)$.

Por ejemplo, tomemos $n = 108$ y $a = 17$. Ya vimos que $\Phi(108) = 36$. Por lo tanto, dado que 17 y 108 son coprimos, tenemos que $17^{36} \equiv 1(108)$; es decir $17^{36} - 1$ es múltiplo de 108.

El **ejercicio 9** muestra, paso a paso, cómo obtener una demostración del teorema de Euler-Fermat.

Ejercicio 9:

Sean $n \in \mathbb{N}$, $a \in \mathbb{Z}$ tales que $(a:n) = 1$. Sean $m = \Phi(n)$ y $R(n) = \{x \in \mathbb{N} : 1 \leq x \leq n \wedge (x:n) = 1\}$, digamos que $R(n) = \{r_1, r_2, \dots, r_m\}$. Nótese que para todo i , $1 \leq i \leq m$, se verifica que $(r_i:n) = 1$.

- Probar que para todo i , $1 \leq i \leq m$, se verifica que $(ar_i:n) = 1$. Deducir que dado i , $1 \leq i \leq m$, existe un número j , $1 \leq j \leq m$ tal que $ar_i \equiv r_j(n)$.
- Probar que si $k \neq j$ entonces r_k no es congruente a r_j módulo n . Deducir que para todo i , $1 \leq i \leq m$, existe un único número j , $1 \leq j \leq m$ tal que $ar_i \equiv r_j(n)$.
- Deducir de b) que existe una función biyectiva $g: \{1, \dots, m\} \rightarrow \{1, \dots, m\}$ tal que para todo i , $1 \leq i \leq m$, $ar_i \equiv r_{g(i)}(n)$.
- Probar que: $ar_1 ar_2 \dots ar_m \equiv r_1 r_2 \dots r_m (n)$. Deducir que $a^{\Phi(n)} r_1 r_2 \dots r_m \equiv r_1 r_2 \dots r_m (n)$.
- Probar que si $s|bc$ y $(s:b) = 1$ entonces $s|c$.
- Probar que $(r_1 r_2 \dots r_m : n) = 1$ y deducir que $a^{\Phi(n)} \equiv 1(n)$.

Si en particular n es un número primo, $n = p$, se tiene $\Phi(p) = p-1$. En consecuencia, para este caso en concreto, el teorema afirma que si $(a:p) = 1$ entonces $a^{p-1} \equiv 1(p)$.

Esta última afirmación se conoce como el Pequeño Teorema de Fermat (para distinguirlo del famoso Último Teorema). El Teorema de Euler-Fermat es, justamente, la generalización que obtuvo Leonhard Euler para el Pequeño Teorema.

Ejercicio 10: Determinar las últimas dos cifras del número 7^{999} .

Construcción de la clave pública

Iniciaremos ahora la última etapa de este artículo. Explicaremos a continuación cómo los conceptos que hemos venido estudiando permiten resolver el problema que dejamos planteado en el comienzo de la nota: la construcción de una clave pública.

Recordemos que el problema nos pide hallar dos funciones (COD y su inversa DEC) tales que la definición de una de ellas sea públicamente conocida mientras que la definición de la otra permanece en secreto.

Tanto la función COD que construiremos, como la función DEC, se aplicarán a un número natural y darán por resultado otro número natural. No obstante, en el ejemplo que desarrollamos en el comienzo de la nota, COD y DEC se aplicaban ambas a cadenas de letras. No existe, sin embargo, ninguna contradicción. Para conciliar ambas situaciones sólo necesitamos un procedimiento estándar, públicamente conocido, que transforme cadenas de letras en cadenas de números (y viceversa). Por ejemplo, como ya fue mencionado, podemos establecer que A se cambie por 01, B por 02, C por 03 y así sucesivamente. De esta forma cualquier cadena de letras podrá transformarse en un número natural y, reciprocamente, cualquier mensaje así transformado en un número podrá reconstruirse fácilmente.

Conocido este procedimiento para transformar letras en números (y viceversa), podemos asumir sin inconvenientes que la clave pública quedará efectivamente construida si obtenemos dos funciones COD y DEC que transformen números en números.

La construcción de la clave comienza con dos primos positivos p y q . Ambos números deben ser muy grandes, digamos de 200 o 300 cifras cada uno.

Sea $n = pq$ (n será un número de alrededor de 500 cifras). El número n será públicamente conocido, mientras que **p** y **q** permanecerán ambos en secreto.

Tal vez aquí Ud. desee protestar: *¿Cómo que p y q son secretos? Todo lo que necesito hacer es factorizar el número n y así obtendré p y q.*

Ahora bien, existen algoritmos bien conocidos que permiten determinar más o menos rápidamente si un número grande es primo (³). Sin embargo, cuando el número resulta ser compuesto, estos algoritmos no nos dan su factorización en primos.

De hecho, cualquier algoritmo conocido tardaría **miles de años** en hallar la factorización en primos de un número compuesto tan grande como el número n que hemos definido más arriba. Por lo tanto, aunque **teóricamente** sería posible conocer p y q a partir de n; en la práctica estos números primos permanecerán en completo secreto, pues aun la más rápida supercomputadora conocida tardaría siglos en hallarlos.

Recordemos además que para calcular el valor de $\Phi(n)$ resulta necesario conocer previamente la factorización en primos de n. Dado que esta factorización permanecerá en secreto, entonces **también será secreto el valor de $\Phi(n)$** . Notemos que $\Phi(n) = (p-1)(q-1)$.

El último ingrediente que necesitamos para la construcción de la clave pública es un par de números enteros e y d tales que $ed \equiv 1 \pmod{\Phi(n)}$. El número e será público, mientras que d permanecerá en secreto.

Si $\Phi(n)$ fuera conocida, entonces sería fácil hallar d a partir del número e (mediante el algoritmo de Euclides). Sin embargo, dado que $\Phi(n)$ es secreto, no existe manera de calcular d. Su secreto, como el de p y q, se encuentra completamente a salvo.

Estamos en condiciones de describir la construcción de la clave pública. Las herramientas fundamentales son los números n y e (públicamente conocidos) y el número d (que permanece en secreto).

En primer lugar, mediante algún procedimiento estándar, el mensaje que queremos codificar se transforma en un número natural. Llamemos a a este número. Debemos suponer además que se verifica que $0 < a < n$. En el caso de que así no fuera, el número obtenido al transformar el men-

saje en cifras se corta en varios bloques, cada uno de los cuales sea un número menor que n.

La función COD (pública) consiste en elevar el número a a la potencia e y luego tomar resto módulo n. En símbolos:

$$\text{COD}(a) = r_n(a^e)$$

Llamemos b = COD(a). La función DEC consiste en elevar el número b a la potencia d (el número secreto) y luego tomar resto módulo n. es decir:

$$\text{DEC}(b) = r_n(b^d)$$

Tanto DEC como COD tienen como dominio y codominio el conjunto de los números enteros entre 0 y n-1. Demostremos que, efectivamente, DEC es la función inversa de COD.

Sea b = COD(a) debemos probar que $\text{DEC}(b) = a$. Observemos en primer lugar que, como $ed \equiv 1 \pmod{\Phi(n)}$, entonces $ed = 1 + k\Phi(n)$ para algún entero k. Por otra parte $b = \text{COD}(a) = r_n(a^e)$. Por lo tanto $b \equiv a^e \pmod{n}$. Tenemos entonces que:

$$b^d \equiv (a^e)^d \pmod{n} \quad (3)$$

Ahora bien:

$$(a^e)^d = a^{ed} = a^{k\Phi(n)+1} = [a^{\Phi(n)}]^k a \quad (4)$$

Por otra parte, podemos asumir que $(a:n) = 1$. En efecto, dado que $0 < a < n$; si a y n no fueran coprimos la única posibilidad sería que $a = p$ o bien $a = q$. Pero estos números son desconocidos. Por otra parte la probabilidad de que, por casualidad a llegara a ser efectivamente igual a p o a q es tan baja (del orden de 10^{-500}) que, a todos los efectos, puede considerarse que es completamente nula. Por lo tanto, podemos estar seguros de que a y n serán coprimos.

En consecuencia, el Teorema de Euler-Fermat nos dice que:

$$a^{\Phi(n)} \equiv 1 \pmod{n} \quad (5)$$

De (3), (4) y (5) deducimos que:

$$b^d \equiv (a^e)^d \equiv [a^{\Phi(n)}]^k a \equiv 1^k a \equiv a \pmod{n}$$

Es decir, $b^d \equiv a \pmod{n}$. Como $0 < a < n$, la propiedad de la congruencia que hemos destacado cuando hicimos el repaso de este concepto nos dice que:

$$a = r_n(b^d)$$

Es decir, según la definición de DEC, vale que:

$$a = \text{DEC}(b)$$

Esta última igualdad es justamente lo que queríamos demostrar y prueba que DEC es efectivamente la función inversa de COD. Dado que COD es pública y DEC es completamente secreta, podemos decir que hemos logrado hallar un procedimiento para la construcción de una clave pública.

Para finalizar, veamos un ejemplo numérico donde se apliquen estas ideas. Por cuestiones de comodidad nuestro ejemplo será desarrollado utilizando números pequeños. Sin embargo, debe tenerse presente que, para que la clave pública efectivamente funcione, los números involucrados deberían ser muchísimo más grandes.

Tomemos para nuestro ejemplo $p = 3$ y $q = 23$. Por lo tanto el número público n será 69, pues $n = pq = 3 \cdot 23 = 69$. Además $\Phi(69) = 44$.

Definimos $e = 5$ (este número también será público) y $d = 9$. Dado que $ed = 45$ entonces es claro que $ed \equiv 1 \pmod{\Phi(n)}$.

Codifiquemos un mensaje breve. Digamos que una vez que ha sido transformado en un número nuestro mensaje dice: "8". Para codificarlo emplearemos el procedimiento público. Por lo tanto calculamos 8^5 y hallamos su resto módulo 69. Cálculos mediante sabemos que $8^5 = 32768$ y su resto módulo 69 es 62. El mensaje codificado dice "62".

Para decodificar este número 62 necesitamos conocer el número secreto 9. La decodificación consiste en calcular el resto módulo 69 de 62^9 . Para facilitar los cálculos, notemos que, dado que $62 \equiv -7 \pmod{69}$ entonces $62^9 \equiv (-7)^9 \pmod{69}$.

Pero $(-7)^9 = -40353607 = 69 \cdot (-584834) - 61$. En consecuencia $62^9 \equiv (-7)^9 \equiv -61 \equiv 8 \pmod{69}$, es decir

62^9 tiene resto 8 al dividir por 69, y es "8" precisamente el número que obtenemos al decodificar el mensaje.

El proceso de decodificación fue posible porque conocíamos la cifra secreta 9. En una situación real, en la que estarían involucrados números realmente grandes, sin este conocimiento no habría sido posible decodificar el mensaje.

Gustavo Piñeiro*

* Licenciado en Ciencias Matemáticas de la U.B.A.

Notas:

⁽¹⁾ Un procedimiento alternativo, pero equivalente, es que Juan X. escriba: *Aquí te envío codificada la frase "Hace frío en julio"* (o cualquier otra) y a continuación la cadena ilegible que se obtiene de aplicar DEC a *"Hace frío en julio"* (o la frase correspondiente). José Z. aplica COD a esta cadena ilegible y si obtiene como resultado *"Hace frío en julio"* entonces sabrá que sin dudas Juan X. es el autor del mensaje.

⁽²⁾ Como se menciona después en esta misma nota, en realidad no es posible hallar **muy rápidamente** la factorización en primos de un número n muy grande.

⁽³⁾ En general, se trata de algoritmos *probabilísticos*. Estos algoritmos nos permiten estimar la probabilidad de que un cierto número p sea primo. Sin embargo, un número del que se sepa que existe una probabilidad del 98 % o 99 % de que sea primo, a todos los efectos prácticos, puede ser considerado efectivamente como primo.

Bibliografía:

* GENTILE, ENZO - *Aritmética Elemental en la Formación Matemática* - O.M.A. - Buenos Aires, 1997. (Nota: Los ejercicios 3, 4, 5, 6 y 10 han sido tomados de este libro.)

* GENTILE, ENZO - *Notas de Álgebra I* - EUDEBA. - Buenos Aires, 1986.

* RIESEL, HANS - *Prime Numbers and Computer Methods for Factorization* - BIRKHAUSSER - Boston, 1985.

* VINOGRÁDOV, I. - *Fundamentos de la teoría de los números* - MIR - Moscú, 1977.

Grandes Matemáticos

Blaise Pascal (1623 - 1662)

El estado de Francia durante la vida de Blaise Pascal.

Durante el transcurso del siglo XVII, y a lo largo del reinado de los tres primeros Borbones: Enrique IV, Luis XIII y Luis XIV, se consolidó, definitivamente, el poder de la realeza en Francia. Prueba de esto son la supresión de los Estados Generales -la asamblea representativa de la nación francesa-; la anulación de las libertades provinciales, el dominio ejercido sobre la nobleza reduciéndola a una “nobleza cortesana” es decir, dependiente de la realeza, y el aniquilamiento de los derechos de los protestantes que llegaron a no poder profesar su culto en el reino de Francia.

Junto a esta consolidación del absolutismo, Francia crecía en poder y prestigio internacional, convirtiéndose en la potencia dominante en Europa en el siglo XVII (resultado de sus guerras victoriosas contra las dos ramas de los Habsburgo, la española y la austriaca). En todos estos sucesos tuvieron una decisiva intervención dos personajes: el cardenal Richelieu, ministro y consejero de Luis XIII, y Mazarino, el sucesor de éste, que se desempeñó como ministro y consejero de Luis XIV en la primera parte de su largo reinado.

Su niñez

Hijo de Antoinette Bégon y de Etienne Pascal, un culto magistrado, nació el 19 de junio de 1623 en Clermont-Ferrand, Francia, Blaise Pascal. Su hermana mayor, Gilberte había nacido 3 años antes y en 1625 nació Jacqueline, su hermana menor.

Un año después del nacimiento de su tercer hija, muere Antoinette y la familia Pascal fija nueva residencia en París. Habiendo quedado a cargo de sus tres pequeños hijos, Etienne se encarga personalmente de su educación. Blaise demuestra prontamente estar en posesión de una inteligencia precoz. Su padre lo introduce hacia 1635 en los círculos literarios y científicos de París. Padre e hijo frecuentan sobre todo la “academia” del padre Mersenne. En esta época Blaise compone un tratado de los sonidos y redescubre por sí mismo, sin libros ni ayuda alguna, los primeros teoremas de geometría.

En un relato hecho por la hermana de Blaise, ésta cuenta que su padre era un hombre con gran vocación matemática, de hecho, el “caracol de Pascal” es una curva llamada así en honor al padre y no a Blaise. Así nos cuenta: “Mi padre, era hombre muy ins-

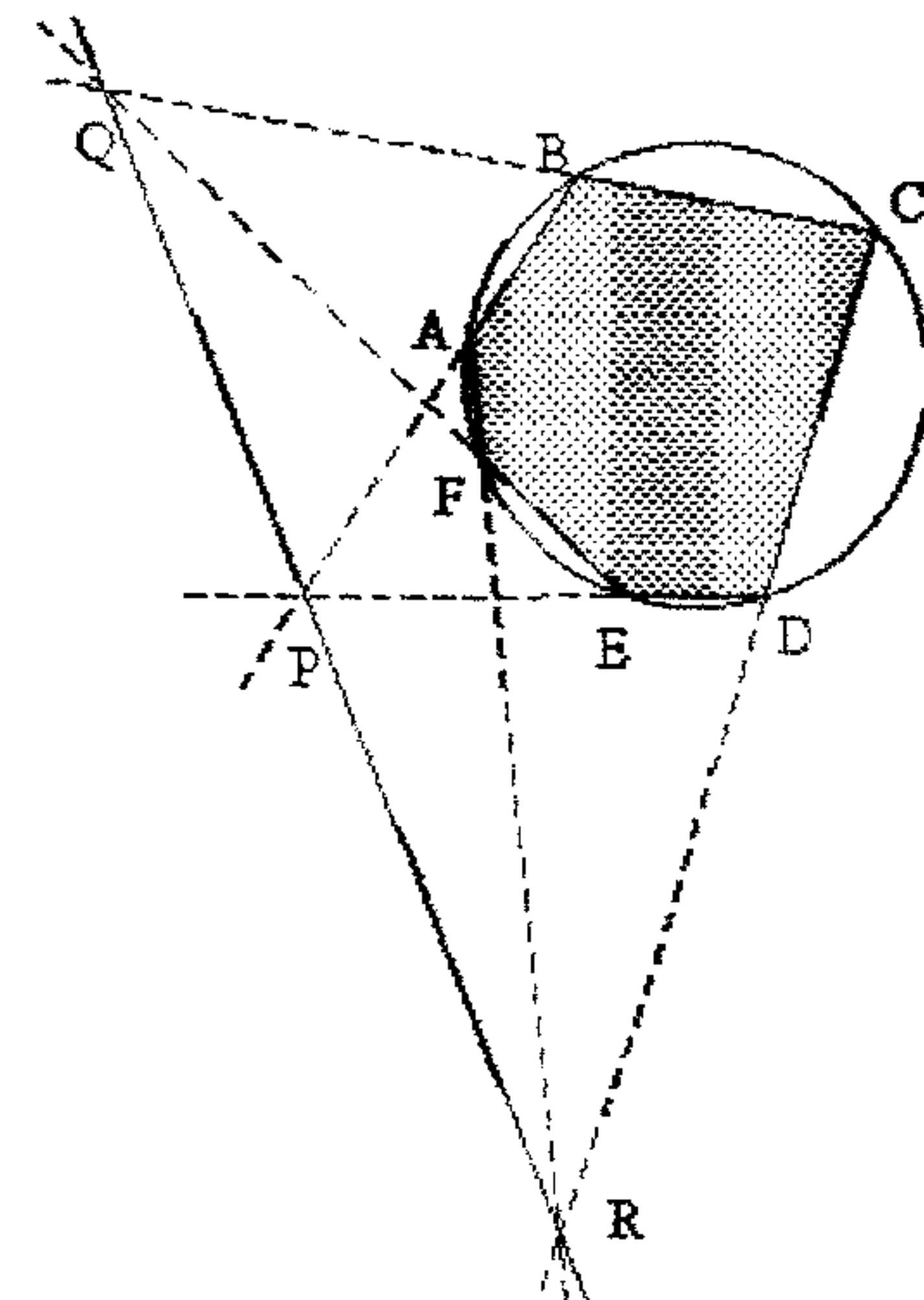
truido en la Matemática y se trataba con todos los cultivadores de esta ciencia que venía a menudo a nuestra casa; pero como deseaba que mi hermano se dedicase a las lenguas y sabía que la matemática es una disciplina que absorbe por completo al espíritu, no quiso que conociera nada de ella ante el temor de que abandonase el estudio del latín. En vista de ello, mi hermano le preguntó un día qué era la Matemática, y mi padre le contestó que tenía por objeto dibujar figuras exactas y encontrar las relaciones entre sus elementos, al mismo tiempo le prohibió que volviera a hablar más de esto; pero a su espíritu, que no podía permanecer estrecho a tan pequeños límites, le bastó saber que la matemática trataba de construir figuras infaliblemente exactas para que soñara con ella en sus horas de recreo; y cuando estaba sólo en su habitación, donde tenía la costumbre de jugar, tomaba un carbón y dibujaba en el suelo, procurando hacer un círculo perfectamente redondo, un triángulo cuyos lados y ángulos fueran iguales y otras cosas semejantes, buscando enseguida las proporciones de aquellas figuras. Pero como mi padre había puesto especial cuidado en ocultarle todo lo que a matemática se refería, mi hermano

ignoraba incluso el nombre de las figuras y tuvo que ponérselos él: al círculo le llamaba "redondel" y a la recta "barra", etc. Luego de establecer estas definiciones enunció axiomas y por último hizo demostraciones perfectas, y como en estas cosas se pasa de unas a otras llevó sus investigaciones tan adelante que logró llegar hasta la trigésimosegunda proposición del primer libro de Euclides (*la suma de los ángulos interiores de un triángulo vale dos rectos*). Un día entró mi padre en su cuarto encontrándole tan abstraído que no advirtió su presencia. No sé quién se sorprendió más, si el hijo al ver a su padre, a causa de la expresa prohibición que le había hecho, o el padre al ver al hijo en medio de aquellas cosas; pero la sorpresa del padre fue mayor aún cuando, al preguntarle qué hacia, le dijo lo que buscaba, que no era otra cosa que la trigésimosegunda proposición de Euclides. Mi padre le preguntó lo que le había hecho pensar en tal cosa y mi hermano le respondió dándole cuenta de sus demostraciones anteriores y, retrocediendo y hablando siempre de barras y redondeles, llegó a sus definiciones y axiomas. Entonces mi padre le dio los Elementos de Euclides para que los leyera en sus horas de recreo. Mi hermano los leyó y los entendió el sólo, sin necesidad de ninguna explicación y llegó a tanto que a los dieciséis años escribió un tratado de "Cónicas", que supone tan

gran esfuerzo que se decía que desde Arquímedes no se había visto nada igual."

Su obra

A los 16 años contribuye al resurgimiento de la geometría mediante un artículo. Pero, según su propia confesión, las propiedades de las cónicas que componían su *Essay pour les coniques* escrito en 1640, le habían sido inspiradas por Girard Desargues, geómetra a quien conoció en las reuniones científicas que se celebraban en la celda del padre Mersenne y que más tarde dieron lugar a la creación de la Academia de Ciencias de Francia (1666). El origen de la inspiración que llevó a Pascal a escribir su pequeño "Ensayo" queda reconocida por él mismo con toda franqueza, ya que, después de citar un teorema de Desargues escribe: "*Quisiera decir que debo lo poco que he descubierto yo mismo sobre el tema a sus escritos*". Este artículo consistía en una sola página impresa, pero sin duda una de las páginas más fecundas de la historia. En ella aparece la proposición que el autor describe como el "hexagrama místico" y que desde entonces se conoce con el nombre de "Teorema de Pascal": dibujemos un hexágono ABCDEF (no necesariamente regular) inscripto en una circunferencia, prolonguemos un par de lados opuestos AB y DE, por ejemplo, hasta que se encuentren en un punto P, prolonguemos otro par de lados opuestos BC y EF, hasta que se encuentren en un punto Q, finalmente prolonguemos el tercer par de lados opuestos CD y FA hasta que se encuentren en R. Entonces, afirma Pascal, P, Q y R estarán situados en una línea recta.



El joven Pascal desarrolla este ensayo sobre las cónicas en el marco de lo que posteriormente se denominaría geometría proyectiva (el inicio del estudio de esta rama de la matemática se le atribuye a Pascal y Desargues, y fue retomada por Poncelet en el siglo XIX).

La obra de Pascal fue desconocida en su época. La geometría analítica creada por Descartes y por Fermat, y el cálculo creado por Newton y Leibniz, demostraron ser tan útiles a las ciencias físicas, que los matemáticos se concentraron en estos temas, de modo que el estudio de la geometría proyectiva permaneció inactivo durante casi doscientos años.

A los 18 años, y a fin de facilitar la labor de su padre, encargado de la recaudación de impuestos en Rouen, Pascal ideó y construyó una "máquina aritmética", considerada como la primera máquina de calcular, de la cual vendió unas cincuenta y que más tarde Leibniz mejoró. Últimamente se ha mencionado a un precursor alemán, Schickard que en 1624 habría construido una máquina de calcular algo más perfecta que la de Pascal.

Para esta época comienza a sufrir los primeros achaques de su enfermedad.

En 1645 publica una carta en la que se dirige al canciller con el fin de solicitarle la concesión de la patente de su máquina aritmética, ya denominada por entonces "pascaline". Al año siguiente Etienne sufre un accidente, los médicos que lo atienden ponen en contacto a la familia Pascal con las ideas jansenistas (doctrina profesada por Jansenio, prelado y teólogo holandés -1585-1638-, que tendía a limitar la libertad humana, partiendo de que la gracia se concede a ciertos seres desde su nacimiento y se niega a otros). Blaise tiene entonces su primera crisis religiosa; aunque no abandonará todavía el trabajo científico, sus preocupaciones se centrarán poco a poco en el estudio del hombre, en detrimento de las "ciencias abstractas".

Junto con su padre y el matemático Pierre Petit, Pascal confirma el experimento de Torricelli sobre el vacío. Del mismo, extraerá un importante principio de hidrostática, el llamado "Principio de Pascal", que funda la teoría de la presión hidráulica, el enunciado del mismo es: *Un líquido transmite en todas direcciones la presión que se ejerce sobre él.* En 1647 Pascal vive en París con su hermana Jacqueline. Enferma y es visitado en dos ocasiones por Descartes. Publica "Nuevos experimentos sobre el vacío" y escribe el "Prefacio para un tratado sobre el vacío". Polemiza con el jesuita R.P. Noël acerca de la posible existencia del vacío.

En 1648, siguiendo las instrucciones de Pascal su cuñado Périer verifica en el Puy-de-Dôme las hipótesis de Torricelli, y él mismo hace lo propio en la torre de Saint-Jacques de París. Publica la *Relación del gran experimento sobre el equilibrio de los líquidos.*

Las experiencias de Torricelli llegaron a oídos de Blaise Pascal, que en la misma época vivía en la ciudad de Ruan. Entusiasmado con las ideas del físico italiano, repitió las experiencias y se convenció de que aquel tenía razón. Además, aprovechando que en su villa se construían tubos de vidrio, hizo construir uno de alrededor de once metros de largo, y realizó la experiencia de Torricelli, pero con agua,

comprobando que alcanzaba una altura de 10,33 metros.

Debido a una disputa con físicos que sostenían todavía la vieja doctrina del horror al vacío, Pascal hizo esta experiencia hasta con vino, aplastando los argumentos de los adversarios.

Si la teoría de Torricelli es correcta, pensó Pascal, ¿qué debe ocurrir cuando se hace la experiencia de Torricelli a distintas alturas, subiendo una montaña, por ejemplo? La presión atmosférica debe ir disminuyendo, y por lo tanto la columna de mercurio, que al nivel del suelo tiene una altura de 76 cm, debe ir disminuyendo también.

Pascal decidió realizar el experimento, pero por su salud no pudo hacerlo personalmente. Envío a unos amigos, quienes ascendieron el Puy de Dome, en la Auvernia, en 1649. Con gran emoción, los expedicionarios comprobaron que a medida que ascendían por la montaña, el nivel del mercurio bajaba. El descenso alcanzó unos 8 cm al llegar a la cima.

Unos meses antes, había redactado en latín -en la actualidad perdido- la *Generación de las secciones cónicas*, que pudo ser utilizado por Leibniz. En esta época tanto él como su hermana Jacqueline mantienen un estrecho contacto con el convento de Port-Royal en el cual Jacqueline ingresará, a pesar de la disconformidad de su hermano, al año siguiente de la muerte de su padre, acaecida en 1651. Luego

de este hecho Pascal lleva una vida mundana. Habiendo obtenido la patente de su máquina aritmética, se la dedica, en una carta, a la reina Cristina de Suecia. En el siguiente año escribe dos nuevos tratados sobre fluidos: *Sobre el equilibrio de los líquidos y Sobre el peso de la masa del aire* que verán la luz póstumamente en 1663.

Una rama de la matemática que tiene a Pascal como co-fundador junto a Fermat, es el cálculo de probabilidades. Cuando la política de Luis XIV hizo que los nobles cesaran en sus guerras e ingresasen a la ociosa vida cortesana, los juegos de azar se pusieron de moda entre ellos. Así, los dados, cartas y ruletas, reemplazaron a las armas para distracción de los caballeros. Para evitar el hastío, las reglas de juego sufrián modificaciones, y la nobleza se interesó, por ejemplo, en determinar si había más probabilidades de sacar un 6 con un dado en cuatro tiradas que sacar un "doble 6" con dos dados en veinticuatro jugadas. Este problema fue propuesto por Antonio Gombaud, Caballero de Le Méré, a su amigo Pascal en 1654, quien a su vez, le escribe una carta a Fermat proponiéndoselo. En la misma dice: "No tengo tiempo de enviarle la demostración de una dificultad que asombraba grandemente al señor de Méré, pues él es un fino espíritu, pero no es geómetra (lo cual, como usted sabe, es un gran defecto) y ni tan solo com-

prende que una linea matemática sea divisible hasta el infinito y cree entender que ella está compuesta de puntos en número finito y jamás le he podido sacar de aquí. Si usted lograra hacerlo, lo haría perfecto.

"El me decía, pues, que había encontrado falsedad en los números por la siguiente razón:

"Si uno acepta de sacar 6 con un dado, hay ventaja en aceptar por cuatro jugadas como 671 es a 625.

"Si uno acepta de hacer "sonnés" (sacar dos 6 de una vez) con dos dados, hay desventaja en aceptar por 24 jugadas. Sin embargo 24 es a 36 (que es el número de posibilidades con los dos dados) como 4 es a 6 (que es el número de posibilidades con un solo dado).

"He aquí lo que constitúa su gran escándalo, que le hacía decir en voz alta que las proporciones no eran constantes y que la aritmética se contradecía; pero usted verá fácilmente la razón por los principios en que usted está trabajando."

Fermat muestra que tal paradoja no existe:

- La probabilidad de no sacar 6 en una jugada es de 5/6, luego la de no sacar 6 en 4 jugadas es $(5/6)^4 = 625/1296$, por lo tanto la de sacar al menos un 6 es $1 - (5/6)^4 = 671/1296$. Es decir, que la razón entre sacar y no sacar 6 es $671/625 > 1$ como afirmaba el Caballero de Le Méré.

- La probabilidad de no sacar doble seis con los dos dados es $35/36$ y de no sacar doble 6 en 24 jugadas es $(35/36)^4$. La probabilidad de sacar al menos un doble 6 será $1 - (35/36)^4$, y la razón entre sacar y no sacar doble 6 es menor que uno.

Por lo tanto, si bien es cierto que hay desventajas a apostar en sacar el doble 6, no es menos cierto que el cálculo correcto desdice que la aritmética se contradiga... cuando se la usa correctamente. La diferencia entre ambas probabilidades es muy pequeña: 0,516 para la primera y 0,491 para la segunda.

Pero el problema que inspiró a Pascal y Fermat en sus trabajos fue el famoso "problema de los puntos", propuesto también por el Caballero de Le Meré. En este problema gana el primero de dos jugadores que consiga n puntos; suponiendo que se abandona el juego cuando uno haya hecho a puntos y el otro b puntos, ¿en qué proporción habrá que dividir entre ellos el dinero apostado? Esto se reduce a calcular las probabilidades que tiene cada uno de ganar en el momento de abandonar el juego. Se supone que los jugadores tienen las mismas oportunidades para ganar un punto.

Pascal escribió a Fermat sobre este problema, y la correspondencia intercambiada constituyó el verdadero punto de partida de la moderna Teoría de

Probabilidades. Ambos resolvieron correctamente el problema pero con razonamientos distintos. En una parte de su trabajo, Pascal se equivocó y Fermat corrigió su error.

Las soluciones que dieron eran para valores particulares de puntos faltantes.

Ni Fermat ni Pascal expusieron sus resultados por escrito, pero en 1657, el matemático y físico holandés Christian Huygens publicó un breve tratado titulado: "De vaticiniiis in ludo aleae" (Sobre los razonamientos relativos a los juegos de dados), inspirado en la correspondencia de estos dos matemáticos franceses.

En la actualidad se cree que Girolamo Cardano (1501-1576) fue el verdadero pionero de la Teoría de las Probabilidades. En un pequeño manual del jugador, Cardano, jugador empedernido, discute la equiprobabilidad, la media, tablas de frecuencias. Sin embargo no puede decirse que su obra influyera en el desarrollo de la probabilidad.

Pascal redacta un folleto llamado *Tratado aritmético* (a veces inapropiadamente llamado "triángulo de Pascal", que será publicado póstumamente en 1665) donde aparecen los números combinatorios con su expresión general y algunas de sus propiedades (el triángulo en sí databa de hacia más de 600 años, pero Pascal descubrió algunas propiedades inéditas). Por ejem-

plo: En todo triángulo aritmético si dos celdas son contiguas en la misma base, entonces el número que figura en la superior es al número que figura en la inferior como el número de celdas desde la superior al extremo más alto de dicha base es al número de las que van de la inferior hasta el extremo mas bajo, ambas inclusive.

Por ejemplo:

$$\begin{array}{c} 1 \\ 1 \ 1 \\ 1 \ 2 \ 1 \\ 1 \ 3 \ 3 \ 1 \\ 1 \ 4 \ \underline{6} \ \underline{4} \ 1 \end{array}$$

4 es a 6, como 2 es a 3.

En este mismo año, 1654, finaliza el "período mundano" de su vida. Pascal visita con frecuencia a su hermana Jacqueline en Port-Royal y la noche del 23 de noviembre se produce su conversión, que plasma en su célebre *Memorial*. Pascal se retira durante algunas semanas en Port-Royal, escribiendo *La conversión del pecador*. Interviene en la polémica entre jansenistas y jesuitas, suscitada al producirse la condena del jansenista Antoine Arnauld por la Sorbona en 1656, escribiendo las dieciocho cartas de las *Provinciales*, donde critica la moral de la Compañía de Jesús, así como sus presupuestos filosóficos y teológicos, que son puestas en el Índice de libros prohibidos de la Iglesia. En esta misma época trabaja en su *Apología del*

cristianismo (que no terminará y será editada en forma inconclusa en 1670 con el título *Pensamientos*) y sus *Escritos sobre la gracia*, que aparecerán en 1779.

Sólo volvería a los estudios matemáticos durante un breve período 1658-1659, cuando desafía a los matemáticos europeos a que resuelvan el problema de la cicloide o "ruleta", que él había resuelto previamente. Una noche de 1658, mientras un dolor de muela le impedía dormir decidió, como distracción contra el dolor, dedicarse al estudio de la "cicloide". Esta curva está engendrada por un punto de una circunferencia que gira sin resbalar a lo largo de una recta.

Milagrosamente, el dolor cesó, lo que Pascal interpretó como un signo de que el estudio de la matemática no desagrada a Dios.

En el "Tratado sobre los senos de un cuadrante de círculo" en 1658, Pascal se aproximó extraordinariamente a lo que pudo haber sido el descubrimiento del cálculo; tan cerca estuvo de ello que Leibniz escribiría más tarde que fue leyendo esta obra de Pascal cuando se le mostró súbitamente la luz.

Publica *Historia de la ruleta*. Expone en Port-Royal el plan de su *Apología* y redacta, al parecer, *Del espíritu geométrico* y *Del arte de persuadir*.

Un par de años más tarde, se instala en Auvergne, debido al agravamiento de su enfermedad y escribe *Oración por el buen uso de las enfermedades* y *Discurso sobre la condición de los grandes*.

Los jansenistas son obligados a firmar la condenación de Jansenio, Jacqueline Pascal muy afectada por esta controversia muere en octubre de 1661, Pascal enfrenta al director de Port-Royal, que es partidario de firmar la condena, pero su postura no es aceptada por la mayoría de los jansenistas y Pascal deja de participar de la controversia.

En 1662 recibe autorización para gestionar, en una empre-

sa de transportes que ha fundado, la primera línea de ómnibus de París. A finales de junio de este mismo año su enfermedad se agrava y el 19 de agosto, Pascal muere en París a causa de un tumor maligno en su estómago que se propagó a su cerebro.

Claudio Salpeter*

Gisela Serrano de Piñeiro*

* Prof. de Matemática, egresado del I.S.P. "Dr. J. V. González"

Bibliografía:

* MAIZTEGUI y SÁBATO - *Introducción a la Física* - Ed. Kapelusz.

* PASCAL, BLAISE - *Pensamientos* - Madrid, Sarpe, 1984.

* REY PASTOR, J. y BABINI, J. - *Historia de la Matemática* - Barcelona, Gedisa, 1985.

* SANTALO, LUIS - *La probabilidad y sus aplicaciones* - Buenos Aires, Editorial Ibero-América, 1955.

* SECCO ELLAURI, O. y BARIDON, P. - *Historia Universal (época moderna)* - Buenos Aires, Editorial Kapelusz, 1972.



Teorema: *Todos los números naturales son interesantes.*

Demostración: (*Por reducción al absurdo*).

Supongamos que hay números naturales no interesantes. Entonces debe existir uno que sea el menor de todos.

Ahora, por ser el menor de los números no interesantes, sin duda, resulta interesante.

Esta contradicción proviene de haber supuesto la existencia de números naturales no interesantes.

Luego, el teorema queda demostrado.

Problemas y Juegos de Ingenio

Problemas Propuestos

1. Colaboración del Prof. Jorge Martínez: Un número natural de tres cifras (ninguna nula) tiene exactamente seis divisores y sus únicos divisores primos son 2 y 13. Hallar este número.

2. Colaboración del Prof. Jorge Martínez: Sea la tabla

1
2, 3, 4
3, 4, 5, 6, 7
4, 5, 6, 7, 8, 9, 10

Demostrar que la suma de los términos de cada fila horizontal es un cuadrado.

Soluciones a los Problemas de Axioma N° 11:

1. De "Snark" - lista de e-mail - John Abreu: *Recordé el siguiente truco:*

a.- Escribe dos fracciones cuyo producto sea 2; por ejemplo:

$$\frac{11}{13} \text{ y } \frac{26}{11}$$

b.- Sumale 2 a ambas fracciones:

$$\frac{37}{13} \text{ y } \frac{48}{11}$$

c.- Divide ambas fracciones:

$$\frac{407}{624} \text{ o } \frac{624}{407}$$

d.- Eleva el numerador al cuadrado y sumale el denominador al cuadrado:

$$407^2 + 624^2 = 165649 + 389376 = 555025$$

e.- Saca la raíz cuadrada del resultado:

$$\sqrt{555025} = 745.$$

f.- CONCLUSIÓN:

$$407^2 + 624^2 = 745^2 \dots$$

UNA TERRA PITAGÓRICA!!!!

PROBLEMA: ¿Funciona siempre este método? Si funciona, demostrarlo; en caso contrario dar un contraejemplo.

* Respuesta dada por Verónica Hauresz (Prof. de Matemática, egresada del I.S.P. "Dr. Joaquín V. González"):

¡Sí!, vale siempre.

Veamos la demostración:

a) Sean $\frac{a}{b}, \frac{c}{d}$ tal que $\frac{a}{b} \cdot \frac{c}{d} = 2 \Rightarrow d = \frac{ac}{b^2}$, por

lo tanto las fracciones elegidas son: $\frac{a}{b}, \frac{2b}{a}$

$$\text{b)} \frac{a}{b} + 2 = \frac{a+2b}{b}, \quad \frac{2b}{a} - 2 = \frac{2(b-a)}{a}$$

$$\text{c)} \frac{a+2b}{b} \cdot \frac{2(b-a)}{a} = \frac{a(a+2b)}{2b(b-a)}$$

$$\begin{aligned} \text{d)} & a^2(a+2b)^2 + 4b^2(b-a)^2 = \\ & = a^2(a^2 + 4ab + 4b^2) + 4b^2(b^2 - 2ab + a^2) \\ & = a^4 + 4a^3b + 4a^2b^2 + 4b^4 - 8ab^3 - 4a^2b^2 \\ & = a^4 + 4a^3b + 8a^2b^2 + 8ab^3 + 4b^4 \\ & = (a^2 + 2ab + 2b^2)^2 \end{aligned}$$

pues

$$\begin{aligned} & (a^2 + 2ab + 2b^2)(a^2 - 2ab - 2b^2) = \\ & = a^4 + 2a^3b + 2a^2b^2 + 2a^3b - 4a^2b^2 + 4ab^3 + \\ & 2a^2b^2 + 4ab^3 + 4b^4 \\ & = a^4 + 4a^3b + 8a^2b^2 + 8ab^3 + 4b^4 \end{aligned}$$

f) Conclusión:

$$[a(a+2b)]^2 + [2b(a-b)]^2 = [a^2 + 2ab + 2b^2]^2$$

2. De "Notas de Álgebra I" - Enzo R. Gentile - EUDEBA: Una banda de 13 piratas obtuvo un cierto número de monedas de oro. Los mismos trataron de distribuirlas entre si equitativamente, pero les sobraban 8 monedas. Imprevistamente dos de ellos contrajeron sarampión y murieron. Al volver a intentar el reparto sobraban ahora 3 monedas. Posteriormente 3 de ellos se ahogaron comiendo caramelos... con papel. Pero al intentar distribuir las monedas quedaban cinco. Se trata de saber cuántas monedas había en juego y también si Morgan estaba entre los piratas.

* Respuesta dada por Verónica Hauresz (Prof. de Matemática, egresada del I.S.P. "Dr. Joaquín V. González"):

Llamemos n al número de monedas, n debe verificar:

$$n = 13 \cdot k + 8$$

$$n = 11 \cdot h + 3$$

$$n = 8 \cdot t + 5$$

Si tomamos $n = 333$ lo verifica pues,

$$333 - 8 = 13 \cdot 25$$

$$333 - 3 = 11 \cdot 30$$

$$333 - 5 = 8 \cdot 41$$

pero además lo verifica

$$n = 333 + 8 \cdot 11 \cdot 13 \cdot k$$

Por lo tanto no podremos determinar el número de monedas en juego, aunque sí sabemos que el mínimo es 333.

Nota del autor Dr. Enzo Gentile: Obviamente Morgan no estaba en el grupo de piratas, pues era reconocidamente supersticioso y no habría integrado un grupo de 13 piratas.

3. De "Matemáticas para los estudiantes de humanidades" - Morris Kline - Ed. Fondo de Cultura Económica: Para ilustrar las virtudes del cálculo, Fermat enseñó que se podía utilizar para demostrar que de todos los rectángulos con el mismo perímetro el cuadrado es el de área máxima. Haz esta misma demostración.

* Respuesta dada por Verónica Hauresz (Prof. de Matemática, egresada del I.S.P. "Dr. Joaquín V. González"):

Dado el rectángulo de base a y altura b :

$$\text{Perímetro} = 2 \cdot a + 2 \cdot b$$

$$\text{Área} = a \cdot b$$

como el perímetro es constante entonces

$$b = \frac{P - 2a}{2}, \text{ con lo cual el área dependerá únicamente del valor de } a: A(a) = \frac{a}{2}(P - 2a).$$

Esta

función área es una parábola cóncava hacia abajo y su máximo lo alcanza en su vértice: $\left(\frac{P}{4}, \frac{P^2}{16}\right)$.

Con lo cual $a = \frac{P}{4}$, al igual que b .

4. De "Introducción a las Matemáticas finitas" - Walter Feibes - Ed. Limusa: Si todas las calles siguen un arreglo rectangular, ¿en cuántas maneras puede uno caminar 6 cuadras hacia el oeste y 8 cuadras hacia el norte?

Podemos pensar en cada recorrido posible como una secuencia de elecciones por norte o por oeste en cada caso. Así por ejemplo tendremos que:

NNNOONONNOOONN

es un recorrido posible, donde N representa norte y O oeste.

Visto de esta manera únicamente debemos contar cuantas secuencias distintas podemos realizar:

$$\binom{14}{8} = \binom{14}{6} = \frac{14!}{8! \cdot 6!} = 3003$$

5. Colaboración del Prof. Alfredo Coccolla: Demuestre que $\sqrt[20]{2} + \sqrt[30]{3} > 2$.

* Respuesta dada por Elisa Palombella y Verónica Hauresz (Prof. de Matemática, egresadas del I.S.P. "Dr. Joaquín V. González"):

Para todo número real $a > 1$, y $n \in \mathbb{N}$, $\sqrt[n]{a} > \sqrt[n]{1} = 1$.

Como $2 > 1$ entonces $\sqrt[20]{2} > 1$.

Como $3 > 1$ entonces $\sqrt[30]{3} > 1$.

Luego, sumando miembro a miembro, $\sqrt[20]{2} + \sqrt[30]{3} > 1 + 1 = 2$

¡Hasta el próximo número!

Comentarios de textos

Hoy comentaremos un texto de estudio y una "novela":

1) "Grafos y sus aplicaciones". - Oysten Ore - Colección La Tortuga - Euler editores, Madrid, 1995. 155 páginas.

La teoría de grafos es hoy una herramienta polifuncional en la Matemática y la gran cantidad de aplicaciones de grafos en campos tan diversos como Álgebra, Topología, Combinatoria, Investigación operativa, Geometría, y Probabilidad, ha determinado que los profesores de Matemática se interesen en este tema.

Por otra parte, son muchas las ciencias y disciplinas que requieren el auxilio de los grafos, para expresar sus conceptos, por ejemplo: Sociología, Psicología, Química, Arquitectura, por nombrar algunas.

Este libro de Ore, es una excelente oportunidad para ponerse en contacto con los grafos, o bien si ya los conocemos, profundizar nuestras ideas sobre el tema. Según Ore, el objetivo del texto es: "...dar una idea del tipo de análisis que puede llevarse a cabo haciendo uso de los grafos..." Afortunadamente, no se requiere un gran aparato matemático para comprender las ideas centrales del asunto.

La disposición del libro consta de 13 capítulos seriados, el primero de los cuales lleva el alentador título "*¿Qué es un grafo?*" donde se comienza desde la definición. En los demás capítulos se van introduciendo (con gran cantidad de ejemplos y aplicaciones) los conceptos fundamentales: conexión, ciclos eulerianos y hamiltonianos, árboles, grafo orientado, órdenes parciales y grafos planos.

Los problemas hiperclásicos de la teoría de grafos están admirablemente tratados, a saber: los puentes de Konigsberg, el problema del viajante, la ruta más corta, los sólidos platónicos y el conocido problema de los cuatro colores. Al final de cada capítulo hay una selección de problemas cuyas soluciones se dan en el capítulo 10. Una seleccionada bibliografía sobre el tema y un glosario acompañan el final del libro.

Es un libro ideal para autodidactas, por su claridad y consistencia.

Pasemos ahora al notable:

2) "El diablo de los números". - Hans Magnus Enzensberger - Ed. Siruela - Madrid, 1998. 259 páginas.

Hans M. Enzensberger es uno de los ensayistas de actualidad más prestigiosos en Europa. Es hombre de profunda cultura clásica y él mismo se declara "no matemático". Sin embargo, inquieto y lúcido, deja entrever en esta deliciosa novela su afición a la Matemática, homenajeando a esta ciencia que tanto lo fascina.

El autor dedica el libro a "todos aquellos que temen a las Matemáticas". El protagonista de esta novela es un niño (Robert) al cual no le gusta la Matemática simplemente porque... no la entiende.

En una de sus frecuentes pesadillas, el niño sueña con una especie de gnomo que se autodesigna como el "diablo de los números", pero que en realidad es un matemático muy completo (caso de existir).

Durante 12 noches, el niño soñará con este diablo, quien, gradualmente lo irá introduciendo en un fascinante mundo donde a partir de sumas y productos escolares se va construyendo un Cosmos que culmina en las series y la topología y aún más en algunos problemas abiertos de la Matemática.

Los diálogos de esta novela son sorprendentes y en ellos se habla desde los números primos hasta los límites y el infinito. Ante un problema el diablo sentenciará: *"Intuir algo tampoco está mal. Probar si es cierto lo que intuyes, aún mejor."*

El fin, algo previsible, es que el niño ya no temerá más a su sufrido docente (El señor Bockel) y a sus cálculos necesarios pero simples y rutinarios, al fin, porque ha comenzado a entender. ¿Una metáfora? Quizás, ¿una crítica a la

enseñanza tradicional? No lo creo. Me quedo con el agradecimiento de Enzensberger a su primer profesor de Matemática, quien le demostró una y mil veces que en la Matemática predomina el placer y no el espanto.

"... Una tarde, al intervalo, la Chancha le decía a Lalín: cruzámela, viejo, que entro y hago gol. Empieza el segundo jastán, Lalín se la cruza, en efecto, y el negro la agarra, entra y hace gol, tal como

se lo había dicho. Volvió Seoane con lo brazo abierto, corriendo hacia Lalín, gritándole: viste, Lalín, viste, y Lalín contestó: sí pero yo no me diviero..."

Ernesto Sábato
Sobre héroes y tumbas

Hasta la próxima

Prof. Jorge A. Martínez*

* Prof. de Matemática, egresado del I.S.P. N° 2 "Mariano Acosta".



Un programa de radio

Un programa de radio, muestra lo que el esfuerzo y las ganas son capaces de generar en beneficio de la comunidad.

Una mínima presentación

Desde el aula es el nombre de un programa de radio. *Educación y sociedad* es la bajada. En ese espacio entran y salen todos los temas: la educación en tiempos democráticos, los libros de texto, los actos escolares, educación y trabajo, computación en la escuela, educación sexual, los juegos, la ley Federal (un listado incompleto de los programas que venimos proponiendo). Desde la vida cotidiana en las escuelas hasta la discusión político-gremial. Desde la revisión de las disciplinas que enseñamos hasta la discusión salarial. Porque no creemos en las *zonas* ni en las *novedades educativas*.

Desde el aula es eso. Un lugar al que podés acercarte (para proponer temas, para contar alguna experiencia con tu curso, para discutir o denunciar). Un lugar desde donde podemos salir no sólo a debatir los problemas que nos tiran sino también a proponer los temas que nos importan.

Para comunicarte con nosotros, podés venir a *La Tribu* (Lambaré 873), en el horario del programa; llamar al teléfono de la radio (865-7554); o por e-mail: mangone@cvtci.com.ar / atenea@cvtci.com.ar.

Te esperamos.

Desde el aula, educación y sociedad, se emite los días martes de 17 a 18 horas, por FM *La Tribu*, 88.7.

Nuestros mejores deseos de éxito.