ALGEBRA I - Práctica N°4 (Segunda parte) - Primer cuatrimestre de 2002

Números enteros

Ejercicio 27. Calcular la suma y el producto de los divisores positivos de

i) 10800 ii) 1125
iii) $2^{1000} \cdot 3^2$ iv) $6^{100} \cdot 12^{25}$

Ejercicio 28.

i) Sean p, q y r primos positivos distintos. Hallar la cantidad de divisores positivos de

$$a)\ p.q.r \qquad b)\ p\,.\,q^2.\,r^2 \qquad c)\ p^3.\,q^2.\,r$$

ii) Calcular la cantidad de divisores positivos de $(10!)^2$

Ejercicio 29. Calcular el mínimo número natural que tiene exactamente 15 divisores positivos.

Ejercicio 30. Determinar todos los $n \in \mathbb{N}$ tales que $(n : 48) = 6$, $14 \mid n$ y n tiene exactamente 12 divisores positivos.

Ejercicio 31. Determinar todos los $a, b \in \mathbb{Z}$ tales que $[a : b] = 2310$ y $(a : b) = 55$.

Ejercicio 32. Probar que no existen $m, n \in \mathbb{N}$ tales que $(m : n) = m - n$ y $[m : n] = m + 2n$.

Ejercicio 33. Sean $n, m \in \mathbb{N}$. Probar que n y m son cuadrados si y sólo si $(n : m)$ y $[n : m]$ son cuadrados.

Ejercicio 34. Sea $a \in \mathbb{Z}$. Probar que $(a^{100} \cdot (a+1)^{200} : (a+2)^{150}) = 1$ ó 2^{100} ó 2^{150}.

Ejercicio 35. Hallar **todas** las soluciones enteras x, y de las siguientes ecuaciones:

i) $3x + 8y = 7$
ii) $84x - 438y = 156$
iii) $84x + 438y = 154$
iv) $ax + (a^2 + 1)y = 2$ con $a \in \mathbb{Z}$ fijo.

Ejercicio 36. Hallar **todas** las soluciones **naturales** x, y de la ecuación

$$6000 = 39x + 54y$$

Ejercicio 37. Hallar **todos** los $x \in \mathbb{Z}$ tales que:

i) $5x \equiv 1 \ (8)$ ii) $13x \equiv 4 \ (6)$

iii) $22x + 5 \equiv 1 \ (14)$ iv) $x^2 \equiv 1 \ (7)$

v) $2x^2 \equiv 9 \ (5)$ vi) $x^2 - 5x \equiv 2 \ (11)$

Ejercicio 38.

i) Hallar un entero tal que dividido por 3, 5 y 7 dé restos 2, 3 y 2 respectivamente.

ii) Hallar un entero tal que dividido por 2, 3, 7 y 12 dé restos 1, 2, 6 y 5 respectivamente.

iii) Hallar 4 enteros consecutivos divisibles por 5, 7, 9 y 11 respectivamente.

Ejercicio 39. Encontrar todos los $x \in \mathbb{Z}$ que verifican simultáneamente:

$$\begin{cases} x \equiv 7 \ (17) \\ x \equiv 5 \ (331) \\ x \equiv 2 \ (72) \end{cases}$$

Ejercicio 40. Resolver módulo 180 el siguiente sistema de ecuaciones de congruencia:

$$\begin{cases} 7x \equiv 1 \ (20) \\ 5x \equiv 7 \ (18) \end{cases}$$

Ejercicio 41. Sea a un entero impar. Calcular los posibles restos de dividir a a^4 por 120.

Ejercicio 42. Probar que:

i) $105 \mid 11^{6n} - 1 \qquad \forall\, n \in \mathbb{N}$

ii) $168 \mid a^7 - a \qquad \forall\, a \in \mathbb{Z}$, a impar.

iii) $2730 \mid a^{13} - a \qquad \forall\, a \in \mathbb{Z}$

iv) $\dfrac{a^7}{35} - \dfrac{a^5}{5} + \dfrac{7a^3}{5} - \dfrac{8a}{35} \in \mathbb{Z} \qquad \forall\, a \in \mathbb{Z}$

v) $336 \mid p^{12} - 1 \qquad \forall\, p$ primo, $p > 7$

Ejercicio 43. Calcular el resto de la división de:

i) 13^{2807} por 7

ii) 5.3^{1522} por 11

iii) 3^{999} por 15

iv) $4^{1605} + a^{20}$ por 15, con $(a : 15) = 1$

v) $\displaystyle\sum_{i=1}^{1759} i^{42}$ por 7

vi) $11^{11^{11}}$ por 40

Ejercicio 44. Encontrar todos los primos positivos p tales que $p \mid 2^p + 5$

Ejercicio 45. Hallar todos los $n \in \mathbb{N}$ tales que:

i) $3^n \equiv 5\ (11)$

ii) $15^n \equiv 2n\ (21)$

iii) $3^n - 2^n \equiv 5\ (7)$

Ejercicio 46. Hallar todos los $n \in \mathbb{N}$ tales que $n \mid 81^{102}$ y $n \equiv 1\ (11)$

Ejercicio 47. Hallar, para cada $a \in \mathbb{Z}$, $(a^{18} + 17 : 315)$

Ejercicio 48.

i) Determinar todos los $a \in \mathbb{Z}$ tales que $77 \mid 3^{205}.a + 5^{111}$

ii) Determinar todos los $a \in \mathbb{Z}$ tales que $(a^{64} + 15 : 34a) = 5$

iii) Determinar todos los $a \in \mathbb{Z}$ tales que $(3a^{98} - 5a^{50} + 4 : 140a) = 14$

Ejercicio 49. Sea $a \in \mathbb{Z}$ tal que $(3a^{13} + 10 : 280) = 35$. Hallar el resto de la división de a por 70.

Ejercicio 50. Escribir las tablas de suma y productos de restos de la división por 2, 3, 4 y 5.

Ejercicio 51.

Definición: Se dice que un elemento $a \in \mathbb{Z}_n$ es un *cuadrado* si existe $b \in \mathbb{Z}_n$ tal que $a = b^2$ en $\mathbb{Z}_n$

i) Calcular los cuadrados de $\mathbb{Z}_n$ para $n = 2$, 3, 4, 5, 6, 7, 8, 9, 11 y 13

ii) Probar que si a y b son cuadrados en $\mathbb{Z}_n$, ab es un cuadrado.

iii) Probar que si a es un elemento inversible de $\mathbb{Z}_n$ que es un cuadrado, a^{-1} es un cuadrado.

iv) Sea p primo positivo. Probar que, en $\mathbb{Z}_p$, $a^2 = b^2$ implica $a = b$ ó $a = -b$

v) Sea p primo positivo impar. Probar que en $\mathbb{Z}_p$ hay exactamente $\frac{(p-1)}{2}$ cuadrados no nulos.

vi) Sea p primo positivo impar. Probar que, en $\mathbb{Z}_{2p}$, $a^2 = b^2$ implica $a = b$ ó $a = -b$

vii) Probar que si n es un natural compuesto e impar, existen a y b en $\mathbb{Z}_n$ con $a^2 = b^2$ y $a \neq \pm b$

Ejercicio 52. Sea p primo positivo. Probar que:

i) Si $k < p$ es un natural, p divide a $\binom{p}{k}$. Dar algunos contraejemplos si p no es primo.

ii) Deducir del ítem anterior que, en $\mathbb{Z}_p$, vale $(a+b)^p = a^p + b^p$

Ejercicio 53. Escribir en base 2, 3 y 16 los siguientes números dados en base 10:

$$1 \qquad 7 \qquad 15 \qquad 128 \qquad 65535 \qquad 1024$$

Ejercicio 54. Determinar en cuántos ceros termina el desarrollo en base 2, 7 y 16 del número 20!

Ejercicio 55. Sea $s \in \mathbb{N}$ tal que $(1126)_s = (634)_{s+1}$. Probar que $s = 7$

Ejercicio 56. Cada entero m entre 0 y 255 puede escribirse en base 2 empleando a lo sumo 8 cifras binarias; por ejemplo $255 = (11111111)_2$; $135 = (10000111)_2$. A cada uno de estos números le asociamos otro, $\overline{m}$, que se obtiene invirtiendo cada una de sus cifras binarias; por ejemplo $\overline{255} = \overline{(11111111)}_2 = (00000000)_2$; $\overline{135} = \overline{(10000111)}_2 = (01111000)_2$. Probar que, para todo m entre 0 y 255, $-m \equiv \overline{m} + 1$ (256).

Aplicaciones: El sistema Fibonacci de numeración

Los sistemas s-ádicos (en base s), factorial o romano no son los únicos sistemas de numeración posibles. Algunas veces para resolver un problema es conveniente cambiar el sistema de numeración por otro más apropiado. Para ilustrar este hecho vamos a introducir el sistema Fibonacci. Representar un entero no negativo n en el sistema Fibonacci consiste en dar una sucesión n_1, n_2, ..., n_k de enteros no negativos que verifican:

i) $n = F_{n_1} + F_{n_2} + \cdots + F_{n_k}$

ii) $n_1 \geq n_2 + 2$, $n_2 \geq n_3 + 2$, ..., $n_k \geq 2$

La primera condición pide que expresemos a n como una suma de números de Fibonacci. La segunda exige que los números usados no sean consecutivos en la sucesión de Fibonacci y que el más pequeño tenga índice mayor o igual a 2.

Por ejemplo, $52 = 34 + 13 + 5$ es una representación válida de 52 ya que $34 = F_9$, $13 = F_7$ y $5 = F_5$. Podemos escribir entonces $52 = (10101000)_F$. En cambio, $14 = 8+5+1$ no es una representación válida porque si bien emplea únicamente números de Fibonacci, 8 y 5 son dos elementos consecutivos de la sucesión. La manera correcta de representar el 14 es $13 + 1$, es decir $14 = (100001)_F$.

Ejercicio 1. ¿Cuáles de las siguientes representaciones son válidas en el sistema Fibonacci?

$$4 = 2 + 1 + 1, \qquad 19 = 13 + 6, \qquad 33 = 21 + 8 + 3 + 1$$

Ejercicio 2. ¿A qué números corresponden las siguientes representaciones?

$$(10101010)_F, \qquad (1000001)_F, \qquad (10010010)_F$$

Ejercicio 3. Exhiba la representación en el sistema Fibonacci de

$$50, \qquad 10, \qquad 16, \qquad 100$$

Ahora que nos hemos familiarizado con este sistema de numeración, deberíamos preguntarnos si hay una manera sistemática de proceder para obtener representaciones (válidas) en el sistema Fibonacci. Además, sería bueno saber si dos representaciones de un mismo número tienen necesariamente que coincidir. La respuesta a ambas preguntas es afirmativa y lo invitamos a verificarlo por sus propios medios:

Ejercicio 4.

i) Escriba un algoritmo que produzca, para una entrada $n \in \mathbb{N}$, una representación en el sistema Fibonacci.

ii) Demuestre que dos representaciones de un mismo natural n en el sistema Fibonacci son necesariamente idénticas.

Ya que estamos en una sección de "aplicaciones," vamos a ver para qué puede servirnos un algoritmo que calcule representaciones en el sistema Fibonacci.

Recordemos el juego aquel en donde dos participantes extraen alternativamente fósforos sobre una mesa, en una cantidad limitada por el doble de fósforos que el otro jugador levantó en el turno previo. Quien se ve obligado a levantar el último fósforo pierde. Pues bien, la clave del juego consiste en representar, cada vez que nos toque jugar, la cantidad de fósforos que hay sobre la mesa en el sistema Fibonacci y retirar, a continuación, tantos fósforos como indique el número más pequeño de la representación. Si usted es curioso y de inteligencia vivaz, se estará preguntado si siempre va a poder aplicar este método sin quebrar las reglas del juego y, en ese caso, si procediendo de este modo va a tener la victoria asegurada. Haga el ejercicio que sigue y salga de dudas.

Ejercicio 5. Demuestre que si inicialmente la cantidad de fósforos no es un número de Fibonacci, entonces el jugador que comience siempre va a poder apalicar el procedimiento explicado arriba sin dejar de respetar las reglas del juego. Concluya que, procediendo de ese modo, el jugador gana. ¿Qué sucede si el número inicial era de Fibonacci?

Otros juegos, otras representaciones

Muchos son los juegos que se pueden resolver a partir de una representación apropiada de los números involucrados. Aquí tiene el lector otros ejemplos para pensar.

Ejercicio 6. Un turista llega a un pueblo lejano y se dirige al único hotel que hay. Explica en la conserjería que quiere alojamiento por siete días pero que no tendrá dinero hasta ese entonces ya que espera a una persona que le debe una importante suma. El dueño del hotel le asegura que no duda de su palabra pero necesita algún recaudo para poder darle una habitación. El hombre no tiene más que una cadena de oro con siete eslabones y —casualmente— el precio de cada eslabón iguala aproximadamente al de cada día de hospedaje. Para no pagarle todo por adelantado, el viajante propone al hotelero darle cada día, en concepto de garantía, una cantidad de eslabones que sea igual a la cantidad de días adeudados. Cuando la persona que espera le traiga el dinero, recuperará la cadena. Pero si a la semana no llega, la perderá. Cerrado el trato, solamente queda un asunto por resolver: ¿cuál es la menor cantidad de eslabones que habrá que cortar para cumplir con lo pactado? Si usted estuviera en esa situación, ¿cómo procedería?

Ejercicio 7. Un malvado califa toma como rehenes a cuarenta personas y las encierra en las oscuras galerías de su palacio. Para darle más sabor a su secuestro, anuncia a los indefensos prisioneros que está dispuesto a liberar a algunos de ellos y les explica el método que ha de emplear para elegir a los que podrán irse. Se les entregará una piedra a cada uno. Al primero una de un kilo, al segundo otra de dos y así siguiendo hasta llegar al último, al que le será entregada una piedra de cuarenta kilos. Sobre una mesa colocará una balanza de dos platos y una barra de plomo de cuarenta kilos. El primero que pase tendrá que dividir en cuatro partes la barra de plomo. Contará para eso con una guillotina de gran precisión. Si elige los puntos de corte de modo de poder pesar la piedra que le ha sido entregada, quedará en libertad, si no, qudará encerrado por el resto de su vida. Para pesar la piedra con la balanza, podrá usar las partes que necesite de la barra de plomo previamente dividida. Después de éste irán pasando uno a uno todos los reenes. Aquellos que acierten a pesar sus piedras utilizando los trozos de plomo dejados por el primero, quedarán en libartad; los otros seguirán cautivos. Después de exponer sus condiciones a los prisioneros, el califa vio a uno de ellos solicitar con resolución ser quien dividiera la barra de plomo. Cuenta la leyenda que la inteligencia del héroe fue tan brillante que pudo salvar a todos sus camaradas. ¿Habrá sido cierta?

Ejercicio 8. Los dos contrincantes de nuestro juego de fósforos comprenden que al haber un algoritmo que permita jugar en forma óptima, el juego pierde todo interés. Por lo tanto convienen en dejarlo de lado y reemplazarlo por este otro. Los fósforos se dividirán en varios montoncitos iguales o diferentes en cantidad. Cada jugador quitará un número cualquiera de fósforos, pero al menos quitará uno. La única condición que respetarán será que, en cada turno, todos los fósforos extraídos deberán pertencer al mismo montón. El que retire el último fósforo perderá. ¿Habrá una estrategia óptima también en este caso?

Digresión histórica

Lo que sigue fue extraído del artículo de Théophile Got, *Un enigma matemático: el último teorema de Fermat*, que puede encontrarse en el libro "Las grandes corrientes del pensamiento matemático," pp. 94–103, EUDEBA (1976).

Gauss, llamado por sus pares el príncipe de los matemáticos, decía que la matemática es la reina de las ciencias, pero que la teoría de números es la reina de las matemáticas. Unas pocas páginas no pueden bastar para dar una idea de la dificultad, ni tampoco de la belleza, de los problemas que constituyen su objeto. Un esbozo semiteórico y semihistórico del más famoso de ellos, el último teorema de Fermat, podrá, no obstante, hacer presentir su interés.

Esta cuestión de análisis indeterminado sigue siendo, entre las numerosas proposiciones de Fermat, la única que, después de tres siglos, todavía no ha podido ser demostrada a pesar de los esfuerzos de una multitud de matemáticos, pequeños y grandes. Es por eso que se la llama el último teorema de Fermat [...]

El análisis indeterminado tiene como objetivo investigar si ciertas ecuaciones de varias incógnitas admiten soluciones enteras y hallar su expresión general. Diofanto de Alejandría, matemático del siglo IV, fue el primero en ocuparse de esto. He aquí el problema a propósito de cual Fermat enunció sus proposición. Hallar todos los triángulos rectángulos cuyos tres lados tienen medidas expresadas por números enteros, es decir, resolver en números enteros la ecuación indeterminada:

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

Puede suponerse que x, y y z son primos entre sí, pues de lo contrario bastaría dividirlos por el cuadrado de su máximo divisor común. No pueden ser impares los tres; uno de ellos, por tanto, es par y éste no puede ser x, pues el primer miembro sería divisible por 4 y el

segundo no. Supongamos, pues, que y es par y escribamos la ecuación:

$$x^2 - y^2 = z^2$$
$$o \qquad (x+y)(x-y) = z^2.$$

Los dos factores del primer miembro son impares y son primos entre sí, pues si no un factor común dividiría a su suma $2x$ y a su diferencia $2y$, y por consiguiente a x y a y, lo que es imposible ya que se ha supuesto que x e y son primos entre sí. Para que el producto de estos dos factores sea un cuadrado, es necesario entonces que sean cuadrados separadamente:

$$x + y = a^2, \qquad x - y = b^2$$

de donde se deduce

$$x = \frac{a^2 + b^2}{2} \qquad y = \frac{a^2 - b^2}{2} \qquad z = ab$$

siendo a y b números enteros impares cualesquiera. Esta es la solución general.

Era natural preguntarse si un cubo puede también ser la suma de dos cubos y, con mayor generalidad, si una potencia cualquiera puede ser la suma de dos potencias del mismo grado. A esta pregunta Fermat respondió con la negativa. Lo hizo en los siguientes términos, en 1637, en una anotación marginal de las Obras de Diofanto que acababan de ser reeditadas y enriquecidas con comentarios de Bachet de Méziriac:

> *Cubum in duos cubos aut quadrato-quadratum in duos quadrato-quadratos et nullam in infinitum, ultra quadratum, potestatem in generaliter duas ejusdem nominis fas est dividere.*
>
> *Cujus rei demostrationem, mirabilem sane, detexi; hane marginis exiguitas non caperet.*

Lo que significa:

"No es posible dividir un cubo en dos cubos, un bicuadrado en dos bicuadrados y, de manera general, una potencia cualquiera de exponente superior a dos en dos potencias de la misma especie.

"He descubierto una demostración bastante notable de esta proposición, pero no cabría en este margen."

Desdichadamente, la demostración que Fermat decía poseer en toda su generalidad no ha llegado hasta nosotros; solamente nos ha dejado el principio de la que empleó para los bicuadrados, el método del descenso infinito. Antes de hablar de los principales trabajos realizados para justificar o para refutar la aserción de Fermat, quizá no sea inútil consagrar algunas palabras a su biografía y a sus descubrimientos.

Fermat. Pierre Fermat nació en 1601 en Beaumont de Lomagne, pequeña ciudad de los confines del Languedoc y la Gascuña. Su padre, comerciante en cueros, después de haberle hecho dar una sólida instrucción en su hogar, lo envió a estudiar derecho a Tolosa. Aquí Fermat se convirtió en consejero del Parlamento. Murió en Castres en 1665.

"Mientras su carrera se deslizaba oscuramente, adquirió, mediante la comunicación en manuscritos de tratados compuestos en latín y por su correspondencia en francés con algunos sabios, todos los cuales se refrían exclusivamente a cuestiones matemáticas, el renombre de un geómetra extraordinario.

"Aparte de sus aptitudes matemáticas, Fermat poseía una gran erudición.

"Su carácter se manifiesta, a través de su correspondencia, afable, poco susceptible, sin orgullo, pero con esa pizca de vanidad que Descartes, su contrario en todos los aspectos y que mezclaba la acritud con la polémica, caracterizaba diciendo: 'El Sr. de Fermat es gascón; yo no lo soy.'

"No era por el camino de la Imprenta por donde su nombre se había difundido en el mundo de los sabios; por sí mismo no había hecho imprimir más que una disertación geométrica y eso manteniéndose en el anomimato. Este opúsculo apareció en 1660.

"Ha dejado casi todos sus teoremas sin demostraciones. Era propio del espíritu del tiempo proponerse problemas unos a otros. A menudo se ocultaba el método propio a fin de reservarse triunfos nuevos, tanto por sí mismo como para la propia nación; pues había, sobre todo, una gran rivalidad entre los geómetras fanceses y los geómetras ingleses. De ahí que se hayan perdido la mayoría de las demostraciones de Fermat. (Legendre: prefacio a su Teoría de Números).

Los trabajos de Fermat son todos de primer orden.

Su Introducción a los lugares planos, exactamente contemporánea de la geometría de Descartes, no solamente restaura por conjeturas la obra perdida de Apolonio sobre los lugares planos, sino que también constituye un tratado conciso de geometría analítica, más completo en ciertos aspectos que el de Descartes.

Según d'Alembert, Lagrange, Laplace, Fournier, Emile Picard, etcétera, el origen del cálculo infinitesimal hay que hacerlo remontar a las dos Memorias sobre la teoría de los Máximos y sobre las Tangentes y las Cuadraturas de Fermat; la memoria de Leibniz sobre el cálculo diferencial —Nova methodus pro maximis et minimis— es posterior en cinco años a la publicación, póstuma, de las memorias de Fermat y su autor reconoce en una de sus cartas a Wallis todo lo que debe a Fermat.

El principio del tiempo mínimo de recorrido que permitió a Fermat demostrar las leyes de la refracción y hallar la expresión exacta del índice de refracción como relación de las velocidades de la luz en los medios es ya una genial anticipación de los métodos del cálculo

de variaciones, creado por Euler y Lagrange más de un siglo después, y de los principios de acción mínima de Maupertuis y Hamilton, que tienen tanta importancia en mecánica analítica.

Fermat comparte con Pascal el mérito de la creación del Cálculo de Probabilidades; sus ideas sobre los principios fundamentales de este cálculo eran incluso más justas que las del último.

Pero fue sobre todo en la Teoría de Números, iniciada por Diofanto en la antigüedad, donde Fermat no tuvo rival. Pascal, que lo llamaba el primer hombre del mundo, escribía: Buscad en otras partes quién os siga en vuestras invenciones numéricas; en cuanto a mí os confieso que estoy muy lejos de ello; no soy capaz más que de admirarlas.

Basta citar el teorema, que lleva su nombre, según el cual para todo número natural a la diferencia $a^p - a$ es divisible por p si p es primo, así como los resultados sobre la ecuación $x^2 - Dy^2 = 1$, que también lleva su nombre. Nunca se halló que Fermat se equivocara; los matemáticos han logrado demostrar todas las proposiciones que él había dejado sin demostración, con excepción de la que nos ocupa, pero no han logrado refutarla.

[...]

Ejercicio 9. Demueste que la ecuación de Fermat $x^n = y^n + z^n$ no tiene soluciones enteras con y e z menores que n. (Indicación: suponga $y \leq z < x$ y use que $y < z + 1 \leq x$.)

Aplicación: Fermat y la Criptografía

La sl encriptación es un recurso comunmente usado para proteger la trasmisión de información a través de canales no del todo confiables. El mecanismo básico de cualquier método de encriptación funciona del siguiente modo:

1. La información es *encriptada* (codificada) transformando su forma inicial (leíble) llamada *texto limpio* a una forma interna llamada *texto cifrado*. Este texto cifrado carece de significado aparente.
2. El texto cifrado se puede almacenar en un archivo o transmitir a través de algún canal de comunicaciones.
3. El receptor del texto cifrado debe *desencriptar* (decodificar) el texto para llevarlo nuevamente a su forma original, limpia.

Si una persona no autorizada gana acceso a la información encriptada, le resultará inútil a menos que sepa desencriptarla. Justamente, el objetivo deseado es desarrollar esquemas de encriptación que sean imposibles (o al menos muy difíciles) de quebrar.

Existe una variedad de métodos que alcanzan este objetivo. Los más comunes proveen un algoritmo general de encriptación E, un algoritmo general de desencriptación D y una o más claves secretas. Además, se deben verificar las siguientes propiedades:

1. $D \circ E(m) = m$ para cualquier mensaje m.
2. E y D deben ser eficientes
3. La seguridad del sistema debe depender de la privacidad de las claves pero no de la privacidad de los algoritmos.

Un punto débil de estos esquemas es el de la distribución de las claves: antes de que la comunicación se lleve a cabo, las claves secretas tienen que poder enviarse con seguridad. Una solución a este problema es usar un esquema de encriptación llamado de *clave pública*. Cada usuario tiene dos claves una privada y otra pública y dos usuarios pueden comunicarse conociendo solamente la clave pública el uno del otro.

En lo que sigue vamos a ver un algoritmo basado en estos conceptos. La clave pública es un par (e, n); la clave privada es un par (d, n). Los números e, d y n son naturales, y n es el mismo en las dos claves. Cada mensaje se puede representar mediante un entero m entre 0 y $n-1$. Esta transformación de un mensaje en un número entero impone una limitación en la longitud del mensaje original; sin embargo, un mensaje largo podría romperse en varios mensajes más cortos, cada uno de ellos en correspondencia con un entero menor que n. Las funciones E y D se definen como sigue:

$$E(m) = m^e \bmod n = C$$
$$D(C) = C^d \bmod n.$$

La cuestión fundamental es la elección de las claves de encriptación y desencriptación. El natural n se lo toma como el producto de dos números primos grandes (de al menos 100 cifras decimales). Estos primos, que llamaremos p y q, se eligen al azar en una forma que no vamos a discutir ahora. Es así que

$$n = p \times q.$$

El valor de d se lo elige, también al azar, como un número coprimo con el producto $(p-1) \times (q-1)$. Esto es, d satiface:

$$(d : (p-1)) = 1 \text{ y } (d : (q-1)) = 1.$$

Finalmente el entero e se calcula a partir de p, q y d como el inverso multiplicativo de d en $\mathbb{Z}_{(p-1)(q-1)}$. Es decir:

$$e \times d \bmod (p-1) \times (q-1) = 1.$$

Es importante tener en cuenta que aunque n es públicamente conocido, los naturales p y q no lo son. Esto se debe a que la dificultad inherente de la factorización hace imposible que existan algoritmos eficientes para calcular p y q partiendo de n. Por este motivo resulta prácticamente imposible calcular el valor de d aún conociendo el de e.

Ilustremos este esquema con un ejemplo. Tomemos $p = 5$ y $q = 7$. Entonces $n = 35$ y $(p-1)(q-1) = 24$. Ya que 11 es coprimo con 24, podemos elegir $d = 11$ y como $11 \times 11 = 1$ módulo 24, también podemos tomar $e = 11$. Supongamos ahora que $m = 3$. Entonces:

$$C = E(3) = 3^{11} \bmod 35 = 12$$

y

$$D(C) = 12^{11} \bmod 35 = 3 = m.$$

Así, si codificamos m usando e, podemos decodificarlo usando d.

Ejercicio. Demuestre que las funciones E y D del método recién descripto son inversas una de otra; es decir, $E \circ D(m) = m$ y $D \circ E(m) = m$ cualquiera sea el entero m, $0 \leq m \leq n-1$. (Sugerencia: use el Teorema de Fermat).

Es interesante observar que no existe una demostración que asegure que para quebrar este mecanismo de encriptación sea necesario factorizar el entero n. De hecho es un problema abierto (aún no resuelto) dar o bien una demostración o bien un método alternativo. En la actualidad, a pesar de esto, hay una fuerte tendencia a creer que en efecto la factorización es imprescindible y el algoritmo se utiliza en aplicaciones reales donde la seguridad es verdaderamente importante.

Referencias.

"Operating System Concepts"; *Silberschatz, Peterson, Galvin.* Adison Wesley. pp 427–430.

"The Z80180 and Big-number Arithmetic"; *Burton S. Kaliski, Jr.*; "Dr. Dobb's Journal" Nro. 204, Sep-93. pp 50–58.

"Privacidad + Encriptación = PGP"; *Daniel Sentinelli*; "Virus Report" Nro. 16. pp 8-10.