LOS NUMEROS PRIMOS Y LOS CODIGOS CIFRADOS

Oscar A. Cámpoli

Introducción

Este artículo tiene su origen en una charla para alumnos de la escuela secundaria donde se requería hablar de un tema de matemática aplicada de actualidad. La elección del tema está motivada por la lectura de un artículo de S. Landau aparecido en Notices of the American Mathematical Society (vol. 30, N° 1, 1983).

En el informe de la reunión sobre Las Aplicaciones en la Enseñanza y el Aprendizaje de la Matemática en la Escuela Secundaria, organizada por la Oficina de Ciencias de la Unesco para América Latina (Montevideo, 1974) se propone el tema de los códigos cifrados para ser desarrollado en la escuela secundaria. Sin embargo, creemos que el *método* de cifrado acerca del cual hablaremos en esta nota no es susceptible de dicho trato en la escuela secundaria debido al nivel de los conocimientos de matemática involucrados, que trataremos de justificar aquí.

Para finalizar esta introducción, quisiéramos agradecer al Ingeniero A.M. Niell y a sus ayudantes C. Jazán y C. Sagastizábal por la colaboración prestada para implementar algunos ejemplos numéricos en una PDP 11/23, los que sirvieron a su vez para poner en perspectiva las dificultades técnicas involucradas.

Generalidades

Para comenzar, recordemos que ha sido siempre muy valorada la capacidad de enviar un mensaje que no pueda ser comprendido por posibles interceptores y si por su destinatario. Al mismo tiempo, es muy importante para el destinatario tener la certeza sobre la procedencia del mensaje, pero éste es un problema sobre el que hablaremos más adelante.

La importancia de ésta capacidad, probablemente sea innecesaria su aclaración, va más allá de la obvia importancia en situaciones beligerantes. En las grandes transacciones comerciales es crucial a veces demorar su conocimiento público y tan es así que la mayoría de las grandes firmas internacionales subvencionan equipos de criptólogos, que así se llaman los especialistas en este tema de cifrado y descifrado de mensajes.

Dado el desarrollo que tienen en este momento las comunicaciones no es de extrañar entonces que la criptografía sea una rama muy importante y actual de la matemática.

Cualquier método de cifrado comienza por el establecimiento de una correspondencia biyectiva entre letras del alfabeto y números. Por ejemplo, si la correspondencia es la más obvia de todas:

A	B	C		Z
↕	↕	↕	...	↕
01	02	03		27

entonces la palabra "venda" se cifra en

2 4 0 5 1 5 0 4 0 1

(00 usualmente denota espacio entre palabras).

Sin embargo este cifrado es demasiado fácilmente *descifrable* y

por ello uno *opera* con los números de arriba antes de transmitirlos.

En lo que sigue voy a tratar de explicar en forma simplificada, aunque creo que con todos los ingredientes importantes, uno de estos métodos de cifrado. Fue publicado en 1978 (ver [5]) y es particularmente importante pues da una posible solución para dos de los problemas más graves del tema.

En efecto, este método funciona de manera tal que un posible interceptor, aunque conozca el *método* de cifrado y haya también interceptado el *código*, aún así está *prácticamente* imposibilitado de descifrarlo. De allí su nombre, que en inglés es Public Key System.

Este sistema se basa en la capacidad de las computadoras para comprobar si un número muy grande es o no primo versus la *incapacidad* de las mismas, con los conocimientos actuales, de *factorear* números compuestos muy grandes.

A modo de aclaración sobre estas frases, damos algunas cifras de un artículo muy interesante publicado en el Scientific American (ver [7]): en 7 minutos se puede responder si un número de 130 dígitos es o no primo mientras que usando el algoritmo más rápido conocido y la computadora más grande posible se tardaría 10^{16} años para factorear un producto de dos (¡no conocidos a priori!) primos de 65 dígitos cada uno.

El otro problema que este método aparentemente resuelve en forma simultánea es el ya mencionado de tener la certeza sobre la procedencia del mensaje, esto es, la legitimidad de una *firma*. Volveremos sobre esto último.

Descripción del método

Para fijar ideas, digamos que el Banco Central de la República

Argentina (BCRA) desea enviar un mensaje secreto a la sucursal en Nueva York del Banco de la Nación Argentina (BN) y que el texto del mensaje es como antes "venda" que ya ha sido cifrado en forma obvia como

$$MO = 2405150401 \qquad (MO \text{ por mensaje original}).$$

El BCRA le dice al BN que elija dos números primos p y q muy grandes (por ejemplo, que ambos sean más grandes que 10^{50}) y que llame $n = p.q$ a su producto y $\varphi(n) = (p-1).(q-1)$. A continuación que elija un número a tal que el máximo común divisor de $\varphi(n)$ y a sea 1 (es decir, $\varphi(n)$ y a son números coprimos). Finalmente, el BCRA le pide al BN que le transmita por radio los números a y n (pero *no* los números p y q usados para obtener n).

El BCRA entonces transmite al BN el resto en la división por n del número $(2405150401)^a$.

Probablemente convenga aclarar de nuevo que dados los números a y $\varphi(n)$ es muy fácil comprobar en una computadora si son o no coprimos y entonces en caso de no serlos elegimos otro valor para a.

Damos a continuación un ejemplo numérico en donde los primos p y q usados no están dentro del rango recomendado debido a la poca capacidad de la computadora usada (PDP 11/23) pero que de todas maneras sirve como ilustración.

Si tomamos $p = 193707721$ y $q = 761838257287$ entonces $n = 147573952589677641 2927$ y $\varphi(n) = 14757395182764444 7920$ y podemos tomar $a = 2147483647$.

En este caso, el resto de la división de $(2405150401)^a$ por n es el número

$$MC = 95145814302036163581$$

que sería el número que BCPA transmite a BN.

¿Cómo hace BN para descifrar el mensaje?

Es muy simple implementar un programa de computadora para encontrar números x e y de modo tal que

$$a \cdot x + \varphi(n) \cdot y = 1 \quad .$$

En el ejemplo nuestro se puede verificar que si tomamos

$$x = 57915193210973670943$$

$$y = -842776986$$

entonces se cumple la ecuación anterior y además podemos también verificar que si tomamos el número MC (MC por mensaje codificado) y lo elevamos al número x de arriba y tomamos el resto en su división por n obtenemos el número

$$MD = 2405150401 \ .$$

Es un ejercicio muy simple verificar que el conocimiento del número $\varphi(n)$ es equivalente al conocimiento de la *factorización* de n y por lo dicho anteriormente, sólo BN dispone de esta información ya que nunca la emitió y nadie es capaz de deducirla.

El hecho de que sepamos a priori que si tomamos un número como el MD anterior y lo elevamos a la potencia a, tomamos el resto en su división por n; a dicho resto lo elevamos a la potencia x y tomamos nuevamente el resto en su división por n y así volvemos a obtener el número MD se basa en un teorema clásico de teoría elemental de números que se llama (pequeño) teorema de Fermat que a continuación describimos y probamos. Usamos para ello sólo propiedades elementales del máximo común divisor entre dos números y propiedades como la siguiente: si el resto de dividir a por m es igual al resto de dividir a' por m y el

resto de dividir b por m es igual al resto de dividir b' por m entonces el resto de dividir a+b por m es igual al resto de dividir a' + b' por m y el resto de dividir ab por m es igual al resto de dividir a'b' por m.

El teorema de Fermat.

Para comenzar necesitamos algunas definiciones y notaciones que nos ahorren un poco de escritura. Dados dos número enteros a y m denotamos (a,m) al máximo común divisor de ambos números y dados números enteros a, b y un número natural m, cuando ponemos

$$a \equiv_m b$$

queremos significar que el resto de la división de a por m es el mismo que el resto de la división de b por m y leemos "a es congruente con b módulo m".

Digamos además que si m es un número natural entonces $\varphi(m)$ es el número que da la cantidad de números naturales comprendidos entre 1 y m y que son *coprimos* con m (en los textos de teoría elemental de números podemos hallar la función φ bajo el nombre de "función φ de Euler").

Teorema (Pequeño teorema de Fermat)

Si a es un número entero, m un número natural y (a,m) = 1 entonces

$$a^{\varphi(m)} \equiv_m 1$$

Demostración.

Digamos que $r_1, r_2, \ldots, r_\nu$ $(\nu = \varphi(m))$ constituyen una fa-

milia de representantes módulo m de todos los números coprimos con m y que están comprendidos entre 1 y m. Con ésto queremos significar que dado cualquier número entero b tal que $(b,m) = 1$ podemos hallar un índice i entre 1 y ν de modo tal que

$$b \equiv_m r_i$$

y además si i, j son dos índices distintos entre 1 y ν entonces

$$r_i \not\equiv_m r_j$$

(esto es, r_i *no es* congruente con r_j módulo m).

Así las cosas, afirmamos que como consecuencia de la hipótesis de que $(a,m) = 1$ se cumple que

$$ar_1, ar_2, \ldots, ar_\nu$$

es otra familia de representantes módulo m de todos los números coprimos con m (aunque éstos no estén comprendidos ahora entre 1 y m).

En efecto, es obvio por las hipótesis que los números $ar_1, ar_2, \ldots, ar_\nu$ son todos coprimos con m. Además si tuviéramos algún par de índices $i \neq j$ tales que

$$ar_i \equiv_m ar_j$$

usando la hipótesis $(a,m) = 1$ podemos hallar enteros u y v tales que

$$1 = ua + vm$$

y luego

$$ar_i \equiv_m ar_j \text{ implica} \qquad uar_i \equiv_m uar_j \text{ implica}$$

$uar_i + vmr_i \equiv_m uar_j + vmr_j$ implica $(ua + vm)r_i \equiv_m (ua + vm)r_j$ implica $r_i \equiv_m r_j$ y ésto es un absurdo que provino de suponer $ar_i \equiv_m ar_j$. Esto prueba la afirmación hecha.

De esta afirmación sigue entonces que

$$(ar_1).(ar_2) \ldots (ar_\nu) \equiv_m r_1.r_2 \ldots r_\nu$$

ya que cada factor de la izquierda es congruente módulo m a uno y sólo uno de los factores de la derecha. Esta última ecuación se puede reescribir

$$(a^\nu - 1)\, r_1.r_2 \ldots r_\nu \equiv_m 0 \qquad \text{(recordar que } \nu = \varphi(m)\text{)}.$$

Ahora bien, como $r_1, r_2, \ldots, r_\nu$ son todos números coprimos con m, está claro que su producto $r_1.r_2.\ldots.r_\nu$ también es coprimo con m y de nuevo podemos entonces hallar números enteros s y t tales que

$$1 = s.r_1.r_2.\ldots.r_\nu + tm$$

y entonces

$$0 \equiv_m (a^\nu - 1)r_1.r_2.\ldots.r_\nu \qquad \text{implica}$$

$$0 \equiv_m (a^\nu - 1)(sr_1.r_2.\ldots.r_\nu + tm) \equiv_m a^\nu - 1$$

y de aquí sigue ahora que $a^{\varphi(m)} \equiv_m 1$ como queríamos probar.

Antes de volver a los códigos queremos mostrar una propiedad muy importante de la función φ de Euler que debemos también usar de alguna manera para justificar nuestro procedimiento.

Teorema.

Si m y n son dos números naturales *coprimos* entonces

$$\varphi(mn) = \varphi(m)\,\varphi(n).$$

Demostración.

Para demostrar este teorema, establecemos una correspondencia biyectiva entre el conjunto de números comprendidos entre 1 y mn y coprimos con mn y los *pares* de números formados por un número comprendido entre 1 y m y coprimo con m y otro comprendido entre 1 y n y coprimo con n.

Ahora bien, ésto es lo mismo que establecer una correspondencia biyectiva entre fracciones *propias* (es decir, comprendidas entre 0 y 1) irrèducibles de denominador mn y pares de fracciones propias irreducibles, una de denominador m y la otra de denominador n. Para hacerlo, procedemos como sigue.

Dipamos que $0 < \frac{h}{mn} < 1$, $(h, mn) = 1$. Es decir que $\frac{h}{mn}$ es una fracción propia irreducible de denominador mn.

Como $(m,n) = 1$ podemos hallar enteros u,v tales que

$$h = um + v'n$$

(notar que si $u'm + v'n = 1$ entonces $hu'm + hv'n = h$).

Pero, si $h = um + v'n$ está claro que cualquiera sea el entero t se tiene

$$h = (u - tn)m + (v' - tm)n$$

y por lo tanto sigue que podemos elegir enteros u, v' tales que

$$h = um + v'n \qquad \text{con} \qquad 0 < u < n$$

(que $u \neq 0$, $u \neq n$ sigue de la hipótesis $(h, mn) = 1$).

Tenemos así

$$\frac{h}{mn} = \frac{um + v'n}{mn} = \frac{u}{n} + \frac{v'}{m} \quad , \qquad 0 < \frac{u}{n} < 1$$

y entonces $\frac{u}{n}$ es una fracción propia que es además irreducible ya que un factor común entre u y n es obviamente un factor común entre h y mn.

La misma razón sirve para decir que $\frac{v'}{m}$ es necesariamente una fracción irreducible aunque podría no ser propia.

Además como $0 < \frac{h}{mn} = \frac{u}{n} + \frac{v'}{m} < 1$ sigue que

$$-\frac{u}{n} < \frac{v'}{m} < 1 - \frac{u}{n}$$

y entonces si no se cumple que $\frac{v'}{m} > 0$ tomamos $\frac{v}{m} = \frac{v'}{m} + 1$ y tenemos entonces que $\frac{v}{m} = \frac{v' + m}{m}$ es una fracción propia irreducible de denominador m.

La correspondencia se establece entonces por

$$\frac{h}{mn} \rightarrow \left(\frac{u}{n}, \frac{v}{m}\right)$$

y es un ejercicio verificar su biyectividad dando la correspondencia inversa, que se construye de manera parecida.

Aplicaciones del teorema de Fermat.

Volviendo al método anterior de cifrado digamos que como teníamos $n = p.q$ con p y q primos distintos, podemos aplicar el último teorema y de ello sigue entonces que $\varphi(n) = \varphi(p).\varphi(q)$.

Ahora bien, si p es un número primo está claro que cualquier número entero comprendido entre 1 y p-1 es coprimo con p y por lo tanto

$$\varphi(n) = (p-1)(q-1)$$

como habíamos escrito antes.

Además el número MO (mensaje original) anterior (puede así comprobarse) es coprimo con n y por lo tanto todas sus potencias lo son y luego si x e y son número enteros tales que

$$ax + \varphi(n)y = 1$$

sigue que

$$((MO)^a)^x \equiv {}_n(MO)^{ax} \equiv {}_n(MO)^{1-\varphi(n)y} \equiv {}_nMO(MO^{-y})^{\varphi(n)} \equiv {}_nMO$$

como habíamos afirmado antes.

Probablemente convenga ahora aclarar que no es necesario verificar que el mensaje original MO sea coprimo con n ya que si MO es menor que p y menor que q es, por lo antes notado, coprimo con p y con q y luego con p.q = n. En casos, como en el nuestro, en que MO no es menor que el menor entre p y q siempre podemos partir MO en bloques de modo tal que cada uno de los bloques sea menor que el menor entre p y q. Recordemos que en cualquier caso concreto los números p y q son muy grandes y por lo tanto las frases que podemos lograr con ésta restricción son suficientemente largas.

Antes de dejar el tema de las aplicaciones del teorema de Fermat quisiera mencionar el hecho de que éste teorema es también muy importante en otra de las etapas de la aplicación práctica de éste método de cifrado, esto es, en la *determinación* de números primos nuevos.

Muy suscintamente, éste tipo de aplicación del teorema de Fermat

es recíproca de la anterior. En efecto, si p es un número primo ya hemos destacado que $\varphi(p) = p-1$. Luego si a es un número natural entre 1 y p-1 se debe cumplir (por Fermat) que

$$a^{p-1} \equiv_p 1$$

luego, si hallamos un a en las condiciones anteriores tal que

$$a^{p-1} \not\equiv_p 1$$

sabemos con certeza que p *no es* primo. Después de probar varios (y cuanto mejor elegidos, mejor) valores de a podemos llegar a convencernos de que p es primo ya que la *probabilidad* de que así sea es más grande a medida que más y mejores valores de a probamos.

Este tema da para mucho y es motivo de estudio en la actualidad (ver [2] por ejemplo).

Firma de mensajes.

Como mencionáramos antes, es muy importante a veces tener la certeza sobre la procedencia del mensaje. Pensemos por un momento en que alguien interceptó la comunicación cuando el BN enviaba n y a a BCRA y a posteriori del mensaje del BCPA el interceptor manda una contra orden. ¿Cómo puede eliminarse este problema?

Una solución posible para ésto está en un doble uso del método anterior que pasamos a explicar.

Hemos ya dicho que BN pensó en p, en q y en a y envió a BCPA los valores de $n = p.q$ y a. Además de ésto, imaginemos que el BCRA por su parte pensó también en dos números primos p' y q' y un número a' tal que fuese coprimo con $\varphi(p'.q') = (p'-1)(q'-1)$ y

le envía al BN los valores $n' = p'.q'$ y a'.

El BCPA (y sólo él) puede encontrar ahora números enteros x', y' tales que

$$a'x' + \varphi(n').y' = 1$$

y en lugar de enviar como antes el resto en la división por n de MC^a envía a BN el resto en la *división por* n' del resto en la división por n de MC^a elevado a la potencia x' ; es decir, llamemos como antes MC al resto en la división por n de MC^a, entonces el BCRA envía a BN el resto en la división por n' de $MC^{x'}$. Llamemos MF (mensaje firmado) a éste número.

¿Cómo decodifica BN?

Está claro que puede hacer lo siguiente

$$(MC^{x'})^{a'} \equiv_{n'} MC$$

y luego como antes

$$MC^x \equiv_n MC .$$

Como lo único que puede conocer un posible interceptor son los valores a, n, a', n', nunca podría calcular x' y por lo tanto el BN está seguro que sólo el BCPA puede haber enviado tal mensaje (y cualquier otro).

Para terminar damos un par de otras referencias.

Como texto de teoría general de códigos podemos mencionar el libro de A. Sinkov ([6]). Mencionaremos también la publicación de Blakley y Borosh ([4]) como una ampliación en cuanto al método descripto, sus problemas y algunas soluciones. Por un texto en castellano de teoría elemental de números puede verse ([8]).

Referencias y bibliografía

1) S. Landon. Primes, Codes and the National Security Agency. Notices of the American Mathematical Society vol. 30, N° 1, 1983.

2) R. Rumely. Recent Advances in Primality Testing. Notices of the American Mathematical Society vol. 30, N° 5, 1983.

3) Las Aplicaciones en la Enseñanza y el Aprendizaje de la Matemática en la Escuela Secundaria.
Informe de la Peunión organizada por la Oficina de Ciencias de la Unesco para América Latina (Montevideo, 1974).

4) G.P. Blakley y I. Borosh - Rivest-Shamir-Adleman Public Key Cryptosystems do not always conceal messages, Comp. and Maths. with Appls. vol. 5, (1979), p.p. 169-178.

5) R.L. Rivest, A. Shamir y L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Comm. of the ACM - Beb. 1978, vol. 21, N° 2, p.p. 120-126.

6) A. Sinkov. Elementary Cryptanalysis. New Mathematical Library N° 22. Mathematical Association of America.

7) M. Gardner. Mathematical Games. Scientific American. August 1977. p.p. 120-124.

8) I. Niven y H. Zuckerman. Introducción a la Teoría de los Números. Limusa-Wiley S.A. México, 1969.

Publicaciones recientes

1) Factoring on a Computer by H.C. Williams the Math Intell. Vol. 6, # 3, 1984, p. 29.

2) Proof Checking the RSA Public Key Encryption Algorithm by R.S. Boyer and J.S. Moore The Amer. Math. Monthby vol. 91, # 3, march 1984 p.181.

3) Factorization and Primality Tests by J.D. Dixon. Then Amer. Math. Monthly vol. 91, # 6 June-July 1984, p. 333.

4) Lecture Notes on Primality Testing and Factoring A Short Course at Kent State University by Carl Pomerance. Math. Assoc. of Amer. Notes # 4.

Facultad de Matemática, Astronomía y Física (IMAF)
Universidad Nacional de Córdoba
Valparaíso y R. Martínez - Ciudad Universitaria
5000 Córdoba.