TIC´s. Teoría de Números y Formación Docente

Juan Carlos Canavelli [1]; María Mercedes Gaitán [1]; Elena T. F. de Carrera [1]

[1] Facultad Regional Paraná de la Universidad Tecnológica Nacional, Paraná, Entre Ríos, Argentina

Resumen

Vivimos en la era de la información y la comunicación. Admiramos y usamos cotidianamente las maravillas que la tecnología actual pone en nuestras manos: INTERNET, cámaras digitales, teléfonos celulares (muchas veces con cámaras digitales incorporadas), bibliotecas digitales, CD, DVD, MP3, MP4, iPod, etc. Pero… en la mayor parte de los casos se desconoce que en la base de toda esta asombrosa tecnología se encuentra la Teoría Elemental de Números. Este desconocimiento es particularmente pernicioso para el docente, pues lo priva tanto de un poderosísimo elemento motivador para sus clases, como de enseñar una rama fundamental de la Matemática con múltiples aspectos valiosos desde el punto de vista pedagógico. Paradójicamente, este tema no figura en el Currículo de la mayoría de nuestros Institutos de Profesorado, o bien, es apenas una pequeña parte de otras asignaturas. En este trabajo nos proponemos mostrar cómo conocimientos elementales de la Teoría de Números intervienen en las TIC's, así como enfatizar la gravitación de estos temas en la formación de los Profesores de Matemática del siglo XXI. Sin profesores competentes y entusiastas, jamás podremos insertarnos en esta "era del conocimiento".

Palabras clave: Tecnología, Teoría de Números, Formación Docente.

1. Introducción

Todos nos acostumbramos rápidamente a las maravillas que nos brinda la tecnología actual, y olvidamos las dificultades que teníamos no hace mucho tiempo y que hoy están superadas. Por ejemplo: los CD están reemplazando a los cassettes, permitiéndonos por un lado mayor capacidad de almacenamiento y por el otro una fidelidad antes desconocida. Análogamente los DVD están desplazando a los clásicos videos convencionales. En los supermercados ha cambiado totalmente la función del cajero, quien no suma ni recuerda mayores datos para decirnos el monto total de nuestra compra. Los pequeños celulares digitales han reemplazado a los antiguos equipos analógicos, incómodos y ruidosos. Ya estamos acostumbrados a las posibilidades que nos ofrecen las pequeñas cámaras digitales, que entre otras cosas nos permiten enviar una fotografía mediante el correo electrónico. Admiramos las claras fotos que nos llegan desde el espacio, y nos imaginamos a Galileo observando a través de su telescopio. Pero lo más asombroso es que todos estos logros tienen un fundamento común, y ese fundamento está en una antigua rama de la Matemática, la llamada Teoría Elemental de Números. Se siente una profunda emoción cuando se piensa que detrás de estos logros de la moderna tecnología está el pensamiento y la obra del griego Euclides (Siglo III antes de Cristo), del francés Fermat (1601-1665), del suizo Euler (1707-1783) y del alemán Gauss (1777-1855), y otros matemáticos…(Sí, matemáticos, como lo fueron más cerca nuestro, en el espacio y en el tiempo, los americanos Claude Shannon (1916-2001), padre de la revolución informática, y Richard Hamming (1915-1998), fundador y presidente de la Association for Computing Machinery (ACM). Alguien podrá pensar que estas afirmaciones son propias de un delirante, y que es inimaginable que realizaciones tan diversas como las que nos permiten escuchar música, calcular importes de una compra o ver detalles en un lejano planeta tengan algo en común. Veremos que lo anteriormente expresado es

totalmente correcto, y que, nos guste o *no*, la Matemática está en el fundamento de todas las modernas realizaciones tecnológicas.

2. Teoría Elemental de Números

Comencemos observando que hablamos anteriormente de "*digital*". Esta palabra proviene del latín "*digitus*" que significa "*dedo*". Desde nuestra niñez asociábamos los dedos con los números naturales, y llamábamos Aritmética al estudio de dichos números. Pues bien, la Teoría Elemental de Números avanza un paso más, ya que trabaja exclusivamente con los números enteros. Debemos advertir que ya estamos vinculando las cámaras digitales, los celulares digitales, la futura -para nosotros-TV digital con la Matemática. Se podrá pensar que ante la existencia de otros números tales como racionales, irracionales y complejos es demasiado poco ambicioso circunscribirse a los enteros. Sin embargo estos números, "estudiados" en el Primer Año del Ciclo Medio presentan problemas aún sin resolver, temas como la conjetura de Goldbach, infinitud de números primos "mellizos", entre otros, así como algunos que recientemente, y tras siglos de esfuerzos, se lograron resolver, como la célebre conjetura de Fermat, demostrada a fines del Siglo XX. (Recordemos que Fermat vivió en el Siglo XVII…). Pues bien, la Teoría Elemental de Números comienza con conceptos familiares tales como divisibilidad, división entera o sea con cociente entero y resto igual, máximo común divisor, mínimo común múltiplo, números primos, teorema fundamental de la Aritmética… casi parece que nos acercamos a la Escuela Primaria. Sin embargo, y aquí comienzan las diferencias, el cálculo del máximo común divisor se efectúa mediante el algoritmo de Euclides que, al permitir expresarlo como combinación lineal de los números en juego, posibilita resolver ecuaciones diofánticas lineales. Sí diofánticas, nombre asignado por Diofanto de Alejandría, siglo III después de Cristo, que no son más que ecuaciones lineales, como por ejemplo: x + y + z = 25 en donde interesan sólo las soluciones enteras. Debemos destacar que las modernas computadoras efectúan el cálculo del máximo común divisor precisamente mediante el algoritmo de Euclides, y no mediante la factorización de los números y la formación del producto correspondiente. Luego de estos conceptos elementales, debemos considerar otro que también es elemental y clave para las aplicaciones actuales: la congruencia de números enteros.

2.1 Congruencia

Nos asombra que un concepto tan simple y potente sea en general ignorado en nuestras escuelas. Sencillamente diremos que dado un número natural n,conn>1,y dos números enteros a y b, éstos son congruentes módulo n si producen el mismo resto al dividirlos por n. Desde Gauss este concepto se representa simbólicamente así: a ≡b (mod n). Por ejemplo: 47 ≡22 (mod 5), pues al dividir (división entera, por supuesto) 47 por 5 el resto es 2, igual que al dividir 22 por 5. De otra forma: decimos que a ≡b (mod n) si n divide exactamente a la diferencia a – b. En el ejemplo anterior 5 divide exactamente a la diferencia:

47 – 22= 25.

Resulta muy fácil demostrar que la congruencia es una relación de equivalencia en Z, y en consecuencia produce una partición de este conjunto en clases de equivalencia. Representamos con Z/nZ, o bien con Z_n al conjunto de estas clases. Y aquí comienza la llamada aritmética modular o "aritmética del reloj", pues se definen operaciones entre estas clases tales como adición, sustracción y multiplicación, para señalar sólo algunas. Alguien podrá preguntarse qué tiene que ver el reloj (sea digital o analógico…) con todo esto. La respuesta es muy sencilla, pues desde siempre hemos estado usando aritmética modular, aunque sin advertirlo. Por ejemplo, si partimos de viaje a las 22 horas, y el viaje dura 10 horas, nadie duda que llegaremos a las 8 de la mañana (por supuesto, del día siguiente). De modo que podemos plantear: 22 (hora de partida) más 10 (duración del viaje) = 8 (hora de llegada). La expresión 22 + 10 = 8 puede espantar a más de uno, pero que es totalmente correcta en este contexto. ¿Así que 22 más 10 da 8? ... Lógico, pues estamos trabajando con horas (las que marca el reloj), y sus únicos valores son 0, 1, 2, …, 23, pues 24 ya coincide con la 0 hora del día siguiente. De otra forma, podemos pensar que estamos trabajando en Z_{24}. Claro que esto no es totalmente correcto, pues estamos identificando a una clase con uno de sus elementos, pero nos permite comprender por qué se habla de "aritmética del reloj". Por otra parte, es usual representar a cada clase de Z_n por el menor de sus elementos no negativo, con lo cual si n = 5 podemos decir que las clases se representan por el conjunto {0, 1, 2, 3, 4} (observemos que se trata de un conjunto finito).

Pensando como en el caso del reloj, podemos ahora escribir las tablas asociadas a la adición y multiplicación en Z_5 . Resulta:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Observemos que:

1. En un planeta donde el día dure sólo 5 horas, estas tablas resumen la "aritmética del reloj"
2. Advertimos inmediatamente que estamos trabajando con conceptos fundamentales de la llamada Álgebra Moderna (a veces también llamada Álgebra Abstracta… ¿Abstracta?...)En efecto si representamos con Z5 al conjunto {1, 2, 3,4}resulta:

   a) $(\mathbf{Z}_5, +)$ y$(\mathbf{Z}_5, \times)$ son grupos finitos.
   b) $(\mathbf{Z}_5, +, \times)$ es un anillo finito, que también resulta ser un ejemplo de campo (o cuerpo) finito.

La sencilla noción aritmética de congruencia nos llevó así naturalmente a las estructuras algebraicas, no definidas en la clásica forma axiomática, sino como una simple generalización de experiencias bien concretas. Sin embargo nuestro imaginario alumno podría decirnos: *"Entiendo todo lo que me están diciendo, pero….¿qué tiene que ver toda esta Matemática con la fotografía digital o con la telefonía celular digital?"* Aquí es donde aparece el genio de Shannon, que en 1948 (hace casi 60 años) escribió un trabajo que lo sitúa, a nuestro entender, como uno de los más grandes revolucionarios del Siglo XX, a saber: "A MATHEMATICAL THEORY OF COMMUNICATIONS", que se lo puede encontrar hoy como un archivo PDF en varios sitios de INTERNET. Antes de abandonar el tema matemático de congruencia, enunciaremos algunos teoremas y conceptos matemáticos, sí, teoremas, que no demostraremos, pero cuyo conocimiento nos resultará indispensable para comprender aspectos cruciales de la moderna tecnología:

Pequeño teorema de Fermat: "Si $a \in \mathbf{Z}$,y p es un número primo no divisor de a, entonces:

$$a^{p-1} \equiv 1 \pmod{p}$$

Ejemplos: $5^2 \equiv 1 \pmod 3$

$$4^4 \equiv 1 \pmod 5$$

Función φ de Euler (o indicador de Euler): Si n es un número natural, representamos con $\varphi(n)$ la cantidad de números naturales menores o iguales que n y coprimos con n. (recordemos que dos números enteros son coprimos si su máximo común divisor es 1)

Ejemplos:

$\varphi(3) = 2$ pues son coprimos con 3: 1 y 2

$\varphi(10) = 4$ pues son coprimos con 10: 1, 3, 7y 9 $\varphi(17) = 16$, $\varphi(18) = 6$, $\varphi(20) = 8$

Teorema de Euler-Fermat: Si $a \in \mathbf{Z}$,y n es un número natural coprimo con a, entonces:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Ejemplos: $10^2 \equiv 1 \pmod 3$

$$10^{16} \equiv 1 \pmod{17}$$

Observemos que esta última expresión significa que si al número 10^{16} lo dividimos por 17 el resto es 1. Muchas veces se utiliza el símbolo = en vez de ≡en tal caso.

Ejemplo: $14^{12} = 1 \pmod{17}$, mientras que escribiríamos $14^{12} \equiv 1 \pmod{17}$ También advertimos que estas dos últimas expresiones las podríamos haber obtenido directamente del teorema de Fermat, por lo que el de Euler-Fermat es una generalización de él. Veamos ahora un ejemplo donde el módulo no es un número primo.

Otro ejemplo: $27^4 \equiv 1 \pmod{10}$, afirmación que podemos interpretar diciendo que la última cifra de 27^4 es 1, como podemos comprobar inmediatamente con una calculadora.

Somos conscientes de que, según su preparación previa, algunos lectores estarán pensando algo similar a alguna de las siguientes alternativas:

1. Todo esto es demasiado elemental. ¿Para qué lo escriben?
2. ¿Qué tienen que ver todas estas afirmaciones con las TICs?
3. ¡BASTA DE MATEMÁTICA!

Nuestra respuesta a la primera pregunta es que, efectivamente, son temas muy elementales, pero lamentablemente ignorados por muchos, en particular maestros e incluso profesores de Matemática (al menos esa es, hasta este momento, nuestra triste experiencia). Pasaremos a ver cómo se utilizan actualmente en uno de los campos de las TICs todos los conceptos anteriormente expuestos, con lo cual daremos respuesta a la segunda pregunta. Finalmente diremos que, efectivamente, podemos dejar por ahora la Matemática aquí, pero si se quiere avanzar en los fundamentos de las Tecnologías de la Información y de la Comunicación, ES NECESARIA MUCHA MÁS MATEMÁTICA. Por cierto no Matemática relacionada con el Cálculo Diferencial e Integral, sino con campos vinculados a la llamada MATEMÁTICA DISCRETA.

3. Criptografía

Se aplican los conceptos matemáticos anteriores, y muchos otros más abstractos, en campos tan concretos como la Codificación, la Compresión de Datos y la Criptografía. Daremos una brevísima explicación de cada un de las dos primeras, para deteneros algo más en la tercera, aunque reconocemos que sólo podemos dar un pantallazo de ésta. La Codificación permite corregir los errores que inexorablemente se cometen en la transmisión y en el almacenamiento de la información. Por ejemplo, cuando se graba música en un CD se ignora el hecho de que el material del mismo jamás es perfecto y homogéneo. Por otra parte el CD se ensucia con el uso, se raya, etc. Sin embargo la reproducción de dicha música es muy buena. ¿Milagro? ¡NO! Sucede sencillamente que la música está convertida en una cadena de ceros y unos o sea "digitalizada", con lo cual se pueden construir algoritmos que permiten detectar la presencia de errores en el almacenamiento y, lo que es más sorprendente, corregirlos. Sí, corregirlos a pesar de que inicialmente no se sabe cuáles son, ni dónde se producen... Realmente, parece milagroso, pero es sólo Matemática y Técnicas Digitales. Algo similar sucede con la telefonía celular, donde la información se ve alterada por la presencia de perturbaciones atmosféricas, obstáculos en el terreno, etc. Por cierto, es muy alta Matemática la que está involucrada en estos maravillosos logros. Precisamente muchas ideas fundamentales se deben al matemático Richard Hamming, pero a la fecha otros matemáticos perfeccionaron notablemente su trabajo. Por otra parte es sumamente conveniente comprimir datos, tanto sea cuando se transmiten o cuando se almacenan. Precisamente en la Compresión de Datos están basadas las técnicas que nos permiten ver un partido de fútbol que se está jugando en las antípodas o escuchar música por MP3. Pues bien, la base para dicha compresión fue una idea del norteamericano Doctor en Ingeniería David A. Huffman (1925-1999), siendo alumno de postgrado en el Instituto de Tecnología de Massachussets. Por otra parte muy pocos, si es que algunos, de nuestros adolescentes fascinados con MP3 sabe que esta tecnología fue inventada por Karlheinz Brandenburg (1954, --), un ingeniero y matemático alemán utilizando precisamente el código de Huffman. Sería muy extenso abarcar tantos aspectos de la Matemática aplicada a las Tecnologías de la Información y de la Comunicación, razón por la cual nos concentraremos en lo que tiene que ver con la confidencialidad y la identificación del emisor de un mensaje. Elegimos este tema, entre otros, por los siguientes motivos:

1. Se pueden comprender aspectos muy actuales con muy pocos elementos matemáticos, como los desarrollados.
2. Es particularmente valioso desde el punto de vista pedagógico, pues es conocida la predilección por las comunicaciones secretas por parte de los adolescentes y jóvenes…
3. Es imprescindible para desarrollar aspectos crecientes del comercio, como el llamado comercio electrónico.
4. Interesa a diversos especialistas, y tiene espacio en los medios de comunicación, la llamada "ley de firma digital" (ley 25.506, sancionada y promulgada en nuestro país en el año 2001, y reglamentada en el año 2002. Pues bien, "firma digital" es una parte de la Criptografía … y nuevamente aparece la palabrita "*digital"*.
5. En diversos países del mundo se lo está utilizando como elemento motivador para la enseñanza de la Matemática.

3.1 Criptografía clásica

En realidad la Criptografía se inició en la Antigüedad, pues desde siempre el hombre necesitó intercambiar mensajes en forma confidencial. Pero hasta el advenimiento de las modernas computadoras fue utilizada principalmente por los militares y los diplomáticos. Hoy la necesitamos todos. Alguien pensará *"pero…¿qué mensaje secreto necesito enviar yo?"* sin advertir que cuando consulta el saldo de su tarjeta de débito en un cajero automático o por Internet necesariamente está enviando y recibiendo información que puede ser interceptada y utilizada fraudulentamente en su perjuicio. Por lo tanto sin Criptografía no funcionaría ni la banca electrónica ni el comercio electrónico que no es más que efectuar compras utilizando INTERNET y la tarjeta de crédito. Pero sigamos con la Historia. Entre los diversos sistemas criptográficos inventados a lo largo de los tiempos queremos destacar el del emperador romano Julio César. Su idea era efectuar una sustitución de las letras del alfabeto utilizando una particular como **clave.** Para vincular conceptos, presentaremos el sistema con una visión actual, asignando un número entero a cada letra del alfabeto internacional y uno al espacio en blanco, según la siguiente tabla:

A ↔ 0

B ↔ 1

C ↔ 2

D ↔ 3

E ↔ 4

.

.

.

W ↔ 22

X ↔ 23

Y ↔ 24

Z ↔ 25

espacio en blanco ↔26

Supongamos que tomamos como clave la letra D, o lo que es lo mismo el número 3. O sea, la D será representada por la A. Ahora sencillamente ciframos los mensajes reemplazando cada letra del mensaje original por la que resulta de la siguiente tabla:

Texto cifrado Texto llano

D ↔ A

E ↔ B

F ↔ C

G ↔ D

H ↔ E

J ↔ F

I ↔ G

K↔ H

L ↔I

M ↔J

N ↔K

O ↔L

P ↔M

Q ↔N

R ↔O

S ↔P

T ↔Q

U ↔R

V ↔S

W ↔T

X ↔U

Y ↔V

Z ↔W

espacio en blanco ↔X

A ↔Y

B ↔Z

C ↔espacio en blanco

Ejemplo: El texto "LA PLATA" se transforma en:"IYXMIYQY". Se podría "matematizar" todo esto considerando que trabajamos con 27 objetos distintos (26 letras y un espacio), y que al finalizar comenzamos nuevamente. Estamos, en consecuencia, en $\mathbf{Z}_{27}$, y el texto cifrado se obtiene del texto llano restando, letra a letra, la clave numérica 3, trabajando módulo 27.

Ejemplo: LA PLATA →11 0 26 15 11 0 19 0 →+3→8 24 23128 24 16 24 →IYXMIYQY

A primera vista parece muy difícil que alguien que intercepte este último mensaje entienda que dice "LAPLATA". Sin embargo, este sistema ya era totalmente transparente para los "criptoanalistas", árabes del Siglo IX expertos en desencriptar mensajes. Fue perfeccionado por Vigenère en el Siglo XVI, quien construyó un sistema donde la clave tenía varias letras, por ejemplo FUTBOL, que

se repetía tantas veces cuanto sea necesario. Entonces se tomaba la primera letra del mensaje original y se la modificaba con la F como clave de Julio César. A la segunda con la U, a la tercera con la T, etc. De esta forma, una misma letra en el mensaje original tenía distintas representaciones en el mensaje cifrado.

Ejemplo:

Mensaje original: LA PLATA.

Clave: TOSE

Mensaje cifrado: DORTDOKE

Conviene aquí trabajar en **Z**27**,** en la forma que se indica:

LA PLATA →11 0261511 0 19 0 →TOSETOSE →1914 18 4 1914 18 4

Se obtiene 30 14 44 19 30 14 37 4 y por congruencia módulo 27 se tiene → 314 1719314 104 →DORTDOKE

La máxima realización de este sistema fue la máquina ***Enigma***, utilizada por las fuerzas armadas alemanas en la Segunda Guerra Mundial. Esta máquina automatizaba el proceso, de modo que se escribía el mensaje en alemán y se irradiaba por radio ya cifrado. Fue una proeza de los aliados el poder desencriptar estos mensajes. Este conocimiento fue determinante del desenlace de la guerra, y permitió salvar varias vidas.

3.2 Criptografía moderna

El advenimiento de las computadoras también revolucionó el mundo de la Criptografía, volviendo obsoletos todos los sistemas utilizados hasta entonces. Simplemente con potencia de cálculo y fuerza bruta se pueden romper todos los sistemas de cifrado que hemos visto. Hace apenas un poco más de tres décadas, dos neoyorkinos, ambos tecnólogos y matemáticos, tuvieron una idea genial que les permitió utilizar una red abierta para poder compartir un secreto. Se trata de Martin E. Hellman, profesor en la Universidad de Stanford y Whitfield Diffie, actual Jefe de Seguridad en Sun Microsystems. Y esta idea genial es una simple aplicación de conceptos de la Teoría Elemental de Números. Se puede ver y escuchar, en un video reciente sobre los festejos por los 30 años del inicio de esta nueva era, a estos auténticos revolucionarios del siglo

XX. Explicaremos muy brevemente la idea de Diffie-Hellman. El trabajo completo se lo puede bajar de INTERNET, como un común archivo PDF, en diversos sitios, por ejemplo en: citeseer.ist.psu.edu/diffie76new.html. Supongamos que dos amigos, Alicia y Benito, se comunican mediante una red abierta y quieren utilizarla para compartir un secreto (que podrían utilizar, por ejemplo, como clave secreta). Para ello eligen un número *g*, utilizado como base, y un número *n*, que será el módulo. Estos números se los comunican sin importar que alguien los intercepte. Luego Alicia elige un número α, que sólo ella conoce, y envía a Benito el número $A = g^{\alpha} \pmod n$. A su vez Benito elige el número β, que mantiene en secreto, y envía a Alicia el número $B = g^{\beta} \pmod n$. No les interesa que alguien conozca n, g, A y B. Con números bien elegidos, no hay por ahora método conocido que permita calcular los exponentes secretos αy β. Es trivial que $B^{\alpha} \pmod n = A^{\beta} \pmod n$ El primer miembro sólo puede ser calculado por Alicia, mientras que el segundo sólo por Benito. Como ambos miembros son iguales, los podemos llamar C y éste es el número que comparten Alicia y Benito, y sólo ellos.

Ejemplo:
Sean: g = 17 y n = 97
Supongamos que α= 12 y β= 35
Entonces: $A = 17^{12} \pmod{97} = 64$, y
$B = 17^{35} \pmod{97} = 60$
Finalmente: $60^{12} \pmod{97} = 50$ y
$64^{35} \pmod{97} = 50$.

Observemos que el número 50 nunca fue transmitido. Sin embargo su conocimiento es compartido por Alicia y Benito, que pueden estar a miles de kilómetros de distancia. Resulta sorprendente y maravilloso que elementales propiedades matemáticas permitan este logro.

Claro que a este número le pueden asociar una palabra, pero a priori no se sabe cuál será, ni siguiera si tiene sentido. El objetivo más interesante es, sin embargo, lograr intercambiar mensajes con significado utilizando una red abierta. Esta proeza fue lograda un año más tarde por tres investigadores que se hallaban trabajando en el Instituto de Tecnología de Massachussets, el famoso MIT, también utilizando conceptos y métodos de la Teoría Elemental de Números. Se trata de Ronald **R**ivest, Adi **S**hamir y Leonard **A**dleman, y el sistema que inventaron lleva el nombre RSA. Hoy RSA es el nombre de una gran empresa de seguridad informática, surgida del conocimiento de elementales conceptos aritméticos y una enorme imaginación. Trataremos de explicar en forma muy elemental este sistema, desarrollando luego un

ejemplo también muy sencillo, trabajando con números pequeños.

Supongamos entonces que Alicia quiere recibir un mensaje de Benito. Para ello elige dos números primos "grandes", *p* y *q*, y calcula su producto n=pq. Luego elige otro número *e*, coprimos con $\varphi(n) = (p - 1)(q - 1)$, y calcula el número *d* talque $ed = 1 \pmod{\varphi(n)}$. Debemos acotar que para este último cálculo se utiliza el Algoritmo de Euclides. Con este procedimiento, Alicia posee **dos claves**, una que hace **pública**, formada por los números n y e, y otra que mantiene **secreta**,y esta formada por los números p, q y d. Alguien podrá pensar que esto es ingenuo, pues si n = pq, basta factorizar n para tener dos elementos de la clave secreta, con cuyo conocimiento es fácil calcular el tercero. Sucede que con los conocimientos matemáticos y la tecnología actual es PRÁCTICAMENTE IMPOSIBLE factorizar un número como n. Supongamos que Benito quiere enviarle un mensaje a Alicia, y que dicho mensaje, expresado en números, sea *m*. Entonces calcula el número $c = m^e \pmod{n}$, y envíael número c sin preocuparse que alguien lo intercepte.Alicia entonces calcula el número$c^d \pmod{n}$, ¡**y recupera m!**En efecto, trabajando siempre módulo n, resulta: $c^d = m^{ed} = m^{1 + k\varphi(n)} = m$, resultando la última igualdad deuna aplicación del teorema de Euler-Fermat.

Ejemplo:

p= 647; q=853; n= 551891

$\varphi(551\,891) = 550\,392$; e = 79; d = 6967
En efecto: $6967 \times 79 = 1 \pmod{550\,392}$
Si m = 3769, resulta $c = 3769^{79} \pmod{551891} = 528197$
Finalmente $528197^{6967} \pmod{551\,891} = 769$, y Alicia recupera el mensaje (que, por supuesto, nunca pasó por la red).

Nuevamente, resulta sorprendente, y hasta diríamos incomprensible, que sean conceptos y métodos matemáticos tan antiguos los que permitan resolver un problema tan actual.

Se presenta ahora el problema de que un intruso, aprovechando que conoce la clave pública de Alicia, le envíe el mensaje m = 3769 haciéndose pasar por Benito. Alicia debe estar segura de que el mensaje se lo envió Benito y no este intruso. Alicia debe poder identificar al emisor del mensaje, aunque esté situado a miles de kilómetros, puedan estar actuando hackers, etc. Esto se logra con la llamada *firma digital*. No expondremos la sencilla idea que permite esta identificación, diremos sólo que exige que Benito, simétricamente, elija otros números primos secretos, etc…

Para finalizar este tema, debemos indicar:

1. Los usuarios de Criptografía, Alicia y Benito, no necesitan saber toda la Matemática subyacente. Hay software que hace el trabajo, y resulta una situación similar a la que se daba con la máquina Enigma en la Segunda Guerra Mundial. Análogamente, cualquier usuario de la banca electrónica no necesita conocer la tecnología que sustenta sus operaciones.
2. Existen hoy otros poderosos sistemas Criptográficos, tanto de clave pública como secreta (ElGamal, AES, los que utilizan curvas elípticas, etc.), pero TODOS utilizan avanzados conceptos y métodos matemáticos. Hoy la Criptografía pasó a ser un tema de la INFORMÁTICA, en conjunción con la MATEMÁTICA APLICADA.
3. El conocimiento de estas disciplinas es el único medio de valorar estos logros y tal vez contribuir a otros nuevos. De otra forma estaremos comprando (o en el más económico de los casos "pirateando"), "vidrios de colores". De nosotros depende, en gran medida, que no se repita en el Siglo XXI en esta querida y sufrida Latinoamérica lo que ya sucedió en los siglos XV y XVI.

4. La Formación Docente

Llegamos así al núcleo de la cuestión, pues en la era del conocimiento en la que estamos viviendo, el agente más importante en el desarrollo económico y social de un pueblo es el docente, quien tiene por tarea transmitir a las nuevas generaciones algunos de los conocimientos elaborados por la humanidad a lo largo de la historia e incentivarlas a que efectúen sus propios aportes. Entendemos perfectamente que al observar nuestra realidad pueda parecer que estamos delirando, pero esto no nos exime de plantear los que estimamos son los pasos correctos para que nuestro país vuelva al camino que lo lleve a ser el que soñaron nuestros próceres. Con dolor advertimos que las naciones que hoy más están avanzando lo hacen sobre ideas que ya tenía, entre nosotros y en el Siglo XIX, Domingo Faustino Sarmiento. Se comprende entonces la responsabilidad económica y social de los Institutos de Formación Docente, que son

o debieran ser-las fuentes generadoras de la riqueza de las naciones en este siglo. En particular, nos referiremos a la formación de los Profesores de Matemática. Por un lado advertimos el entusiasmo que despierta la tecnología en los jóvenes estudiantes. Es natural que así sea pues se han desarrollado en un mundo impregnado de realizaciones tecnológicas impensadas hace unas décadas. El docente con conocimiento del fundamento matemático de las más impactantes tecnologías tiene así para sus clases una excelente base para motivar a sus alumnos. Y sabemos que es fundamental que el alumno **quiera** aprender para que efectivamente aprenda. Alguien dijo, con mucha razón, que "*quien quiere hacer algo encuentra los medios, quien no quiere hacerlo, encuentra la excusa*". Nuestra experiencia nos muestra que muchos alumnos, al comprender la importancia de la Teoría Elemental de Números en la tecnología moderna, quieren aprender Matemática. Sin embargo, advertimos que este tema es ignorado, o tratado muy superficialmente, en muchos Institutos de Formación Docente. Esta situación priva a los futuros docentes de dos elementos fundamentales para su tarea:

1. El conocimiento de una rama de la Matemática de gran valor educativo.
2. Un poderoso elemento motivador para realizar el esfuerzo y trabajo que implica el aprender Matemática.

Sería injusto olvidar la obra realizada entre nosotros por el Dr. Enzo R. Gentile, quie siempre remarcó la importancia de la Teoría Elemental de Números en la formación matemática en todos los niveles. A través de sus cursos y publicaciones contribuyó significativamente a mantener viva entre nosotros esta rama de la Matemática. Debemos mencionar también la magnífica obra que realizó y realiza en nuestro país la Olimpíada Matemática Argentina, que tanto ha contribuido a que nos mantengamos en niveles satisfactorios en el orden internacional. Hay un doble mérito en la tarea de la Olimpíada Matemática Argentina: por un lado utiliza la tecnología en el estudio y la difusión de la Matemática tal como utilización de página web y software y por el otro, difunde la Teoría Elemental de Números a través de libros como "aritmética" que en nuestra opinión, por sus méritos, debiera ser un texto utilizado en todos los Institutos de Formación Docente en Matemática de nuestro país.

Conclusión

La Matemática está en la base de las más modernas realizaciones tecnológicas, en particular lo está la Teoría de Números que fundamenta muchas de las TICs. Tanto la Codificación, como la Compresión de Datos y la Criptografía resultan de la aplicación de conceptos y métodos de esta teoría matemática. Es entonces de gran importancia que los Profesores de Matemática conozcan los rudimentos de la Teoría de Números y de su aplicación actual. De tal manera poseerán, además de un conocimiento fundamental de su disciplina, un poderosísimo elemento motivador para sus clases.

Referencias

[1] Becker, M. E., Pietrocola, N. y Sanchez, C.: *aritmética.* RED OLÍMPICA. Olimpíada Matemática Argentina. 2001.

[2] Gentile, E. R.: *ARITMÉTICA ELEMENTAL.* OEA, 1985.

[3] Singh, S.: *LOS CÓDIGOS SECRETOS.* Editorial DEBATE. 2000

Sitios en INTERNET:

[1] www.certicom.com (Criptografías con curvas elípticias – en inglés).

[2] www.oma.org.ar (Olimpíada Matemática Argentina).

[3] www.rsa.com (Compañía RSA – en inglés).

Dirección de Contacto de los Autores:

Juan Carlos Canavelli
Avda Almafuerte 1033
Paraná, Entre Ríos Argentina
e-mail: jcanavelli@frp.utn.edu.ar

María Mercedes Gaitán
Avda Almafuerte 1033
Paraná, Entre Ríos Argentina e-mail:
mgaitan@frp.utn.edu.ar

Elena T F de Carrera
Avda Almafuerte 1033
Paraná, Entre Ríos Argentina
e-mail: ecarrera@frp.utn.edu.ar

Juan Carlos Canavelli: Investigador Categoría III. Prof Consulto UTN. Director del Dpto. Materias Básicas en la FR Paraná, UTN. Prof. Titular Ordinario de Análisis de Señales y Sistemas UTN, Prof. Titular Ordinario Fac de Ing. UNER.

María Mercedes Gaitán: Prof. Matemática, Física y Cosmografía . Ing . en Construcciones, UTN. Maestría en Educación (falta Tesis), UNER. Prof. Asociada Ordinaria FRP, UTN. Prof. Asociada Fac. Cia. y Tecnología, UADER.

Elena T F de Carrera: Investigador Categoría I SPU. M.Sc. UBA, Lic en Matemática Aplicada, UNL. Prof. Titular Ordinaria UNL. Directora del Dpto. Matemática, FBCB, UNL. Prof. Titular Ordinaria FR Paraná, UTN.