Manejo Compartido de un Secreto

Adriana Marcela Fonce Camacho

Universidad del Cauca

Facultad de Ciencias Naturales, Exactas y de la Educación

Departamento de Matemáticas

Programa de Matemáticas

Popayán

2011

Manejo Compartido de un Secreto

Adriana Marcela Fonce Camacho

Trabajo de Grado
En modalidad de Seminario de Grado, presentado como requisito parcial
para optar al título de Matemática

Director
Freddy William Bustos Rengifo

Universidad del Cauca
Facultad de Ciencias Naturales, Exactas y de la Educación
Departamento de Matemáticas
Programa de Matemáticas
Popayán
2011

Nota de aceptación

_____

_____

_____

_____

Director: Mat. Freddy William Bustos Rengifo

_____

Jurado: Mg. Martha Lucía Bobadilla Alfaro

_____

Jurado: Ph. D. Carlos Alberto Trujillo Solarte

Fecha de sustentación: Popayán, 10 de junio de 2011

En memoria de Dionicio López Farfan.
Siempre serás la lucesita
de mi camino.

Agradecimientos

Cada camino que recorremos trae consigo alegrías, tristezas, triunfos, derrotas, soluciones y problemas.

Cada camino que recorremos lo hacemos paso a paso superando dificultades y sonriendo con cada meta que cumplimos.

Cada camino que recorremos nos llena de experiencia y sabiduría.

En cada camino nos caemos, pero también nos volvemos a levantar.

Y en cada camino que tomamos encontramos personas que nos acompañan, ayudan, fortalecen, hieren, colaboran, animan, quieren, entre muchas otras más, y son ellas las que hacen que nuestro recorrido valga la pena.

Dios, amor, familia, amigos, maestros y compañeros hacen que cada camino sea maravilloso y lleno de felicidad.

Gracias a todos por estar a mi lado siempre acompañándome en cada paso que doy.

¡Dios los bendiga!

Adriana M. Fonce Camacho.

Índice general

Introducción

Imaginemos que tenemos una información (secreto) la cual podemos fraccionar en n partes; cada una de estas se entrega a una única persona de tal forma que si se quiere recuperar la información se pueda hacer sólo con un número mínimo de fracciones reunidas, es decir se reúne un número k (con $k < n$) de personas que poseen partes del secreto y con estas se puede acceder a la información inicial.

Un **Esquema para Compartir un Secreto** es un arreglo en el cual se fracciona una información y se entrega a un número determinado de personas con la posibilidad de recuperarla al reunir de nuevo las partes. Un **Esquema de Umbral para Compartir un Secreto** es aquel que permite recuperar la información inicial con un mínimo de partes (umbral). Este último depende de dos números, n que es la cantidad de partes en las que se fraccionó la información y k el umbral que se necesita para recuperar la información inicial.

Para ilustrar lo anterior: la bóveda de un banco se puede proteger de manera que entre un grupo de 5 personas, cualquier grupo de 3 o más puedan abrirla pero ningún grupo de menos de 3 tenga tal posibilidad. Para esto se puede adecuar a la bóveda con 10 cerraduras cada una de las cuales requiere de 3 llaves para abrirse, además a cada persona se le entregan 6 llaves para que pueda intervenir en los diferentes grupos de 3 en que podría

estar. En el caso general, si se quisiera autorizar a todos los grupos de k personas en un grupo de n, se deberían disponer $\binom{n}{k}$ cerraduras y a cada persona asignarle $\binom{n-1}{k-1}$ llaves. Esto resultaría poco práctico teniendo en cuenta que para $n = 10$ y $k = 3$ el número de cerraduras sería de 120 y a cada persona se le deberían asignar 36 llaves.

No conocemos un dato exacto de cómo o cuándo se planteó la necesidad de construir un esquema de umbral por primera vez, pero los primeros esquemas aplicables a números grandes fueron dados a conocer por *Adi Shamir (Massachusetts Institute of Tegnology)* [16] y *George Robert (Bob) Blakley Jr. (Texas A& M University)* [3] en 1979; el esquema de Shamir se basa en la interpolación de polinomios, mientras que el esquema de Blakley usa hiperplanos geométricos. También son conocidos otros esquemas como los presentados por *Asmuth* y *Bloom* [2] (1982) y *Maurice Mignotte* [11] (1983) los cuales se basan en el *Teorema Chino de los Residuos*.

Nuestro interés se centrará en un *Esquema de umbral* basado en el *Teorema chino de los residuos* usando como módulos los términos de una *Sucesión de Mignotte*.

Sorin Iftene profesor de la Universidad *Alexandru Ioan Cuza* en desarrollo de su tesis de doctorado [8] en Ciencias de la Computación presentada en el año 2007 ante la misma universidad, retoma los esquemas de umbral y en particular retoma el esquema propuesto por Mignotte, proponiendo un nuevo esquema que utiliza una Generalización del Teorema Chino de los Residuos, considerando como módulos los términos de una sucesión que surge de generalizar las sucesiones de Mignotte.

En este trabajo presentamos los elementos necesarios para comprender la propuesta de

Sorin Iftene y hacemos la correspondiente presentación de la misma.

Preliminares

El matemático, poeta y militar chino Sun Tsu vivió alrededor del siglo III a.C. Fue autor del libro *El arte de la guerra* y además planteó el siguiente problema:

Tengo un conjunto de objetos.
Cuando los cuento de tres en tres, me sobran dos;
cuando los cuento de cinco en cinco, me sobran tres;
cuando los cuento de siete en siete, me sobran dos.
¿Cuántos objetos poseo?

La solución al anterior acertijo la da el Teorema Chino de los Residuos.

Teorema 0.0.1 (**Teorema Chino de los Residuos**). *Sean $m_1, m_2, ..., m_n$ enteros positivos primos relativos por parejas, $a_1, a_2, ..., a_n$ enteros arbitrarios, entonces el sistema*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

tiene solución única módulo $m_1 \cdot m_2 \cdots m_n$.

Definición 0.0.1 (**Hiperplano geométrico**). *Un hiperplano geométrico es un subespacio de dimensión $n-1$ en un espacio de dimensión n. Si H es un hiperplano de V se dice que H tiene codimensión 1.*

Definición 0.0.2 (**Polinomio Interpolante de Lagrange o Interpolación de Lagrange**). *Dados $n+1$ puntos $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)$ en $\mathbb{R}^2$, con $x_0, x_1, \ldots, x_n$ distintos por parejas, existe un único polinomio*

$$p(x) = \sum_{k=0}^{n} y_k \cdot l_k(x)$$

de grado a lo más n llamado polinomio interpolante de Lagrange, el cual satisface $p(x_k) = y_k$ para todo $k = 0, 1, \ldots, n$. Cada $l_k(x)$ es un polinomio de grado n para todo $k = 0, 1, \ldots, n$ y es de la forma:

$$l_k(x) = \prod_{\substack{j=0 \\ j \neq k}}^{n} \frac{(x - x_j)}{(x_k - x_j)} \quad \text{para todo } k = 0, 1, \ldots, n.$$

Además los polinomios $l_k(x)$ son polinomios fundamentales de Lagrange que satisfacen

$$l_k(x - j) = \begin{cases} 1 & \text{si } k = j \\ 0 & \text{si } k \neq j \end{cases}$$

esto para todo $j, k = 0, 1, \ldots, n$

Teorema 0.0.2 (**Teorema de los Números Primos**). *Para todo $x \in \mathbb{R}^+$, $\pi(x)$ representa el número de primos menores o iguales a x, entonces $\pi(x) \approx \dfrac{x}{\ln x}$ o más precisamente*

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Capítulo 1

Esquemas de Umbral

En algunas ocasiones no queremos que una información se conozca en su totalidad por una única persona, entonces fraccionamos la información y entregamos sus partes de manera que la información repartida se pueda recuperar con la totalidad de las partes o con un número determinado de ellas. Esto se formaliza como sigue:

Definición 1.0.3 (**Esquema para compartir un secreto**). *Un esquema para compartir un secreto es un arreglo en el cual se fracciona una información en n partes que se entregan a n personas de manera que la información se puede recuperar.*

Cuando podemos recuperar la información en su totalidad con un número menor que el total de las partes estamos usando un esquema de umbral para compartir un secreto. Esto es:

Definición 1.0.4 (**Esquema de umbral**). *Un esquema de umbral es un esquema para compartir un secreto que permite recuperar la información inicial con un mínimo de partes, que depende de n y k, donde n es la cantidad de partes en las cuales se fracciona*

la información y k es el conjunto mínimo de partes que se debe reunir para recuperar la información (umbral).

No se conoce un dato exacto sobre como surgió este problema, sin embargo en 1979 se da una primera solución con los esquemas de umbral de *Adi Shamir* y *George Blakley.*
Existen diferentes esquemas de umbral de los cuales nombramos algunos a continuación.

1.1. Esquema de Shamir

Adi Shamir (1952), Criptógrafo israelí, Licenciado en Matemáticas de la Universidad de Tel Aviv (Israel) en 1973, maestro y doctor en Ciencias de la Computación. Actualmente es profesor del Instituto de Weizmann (Israel).

El esquema de Adi Shamir se basa en la interpolación de polinomios y opera de acuerdo a lo siguiente: Para entregar las partes de la información

- Escogemos S en $\mathbb{R}$.
- Escogemos al azar a $a_1, a_2, \ldots, a_{k-1}$ y $a_0 = S$ $(k < n)$ luego construimos el polinomio:
$$q(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}.$$
- Entregamos las parejas (i, y_i) donde $y_i = q(i)$, para todo $i = 1, ..., n$.

La recuperación de la información funciona como sigue:
Si tenemos k de estas parejas $(i_1, y_{i_1}), ..., (i_k, y_{i_k})$, usamos interpolación de polinomios

para encontrar los coeficientes del polinomio de grado $k-1$, puesto que $a_0 = S$ entonces $q(0) = S$, así encontramos el secreto.
Si sólo tenemos $k-1$ parejas podríamos construir un polinomio de grado $k-2$ pero este no arroja información sobre S.

Usualmente se usa aritmética modular en lugar de aritmética real, para esto consideramos el conjunto de los enteros módulo un primo p, los cuales forman un cuerpo en el cual se puede utilizar la interpolación de polinomios. Escogemos S y un primo p mayor que S y n. Los coeficientes $a_1, a_2, ..., a_{k-1}$ de $q(x)$ se escogen de manera arbitraria en $[0, p)$ y los y_i se modulan módulo p.

Si sólo tenemos $k-1$ partes de S podemos construir un polinomio de grado $k-1$ para cada valor S' en $[0, p)$. La seguridad se garantiza con un intervalo $[0, p)$ grande.

Ejemplo

- **Aritmética real**

  Sea $S = 1234$ el secreto y queremos dividirla en 6 partes de forma que 3 personas puedan recuperar. Escogemos al azar los números $a_1 = 166, a_2 = 94$ y dado $a_0 = 1234$, construimos un polinomio de grado 3:

  $$p(x) = 1234 + 166x + 94x^2.$$

  Calculamos 6 puntos para obtener las parejas $(1, 1494), (2, 1942), (3, 2578), (4, 3402), (5, 4414), (6, 5614)$, que son las parejas a entregar.
  Supongamos que tenemos 3 de las anteriores parejas, digamos $(i_1, y_{i_1}) = (2, 1942)$, $(i_2, y_{i_2}) = (4, 3402), (i_3, y_{i_3}) = (5, 4414)$, usamos el método de interpolación de La-

grange para construir un polinomio. Entonces

$$l_0 = \frac{x-x_1}{x_0-x_1}\cdot\frac{x-x_2}{x_0-x_2} = \frac{x-4}{2-4}\cdot\frac{x-5}{2-5} = \frac{1}{6}x^2 - \frac{2}{3}x + \frac{10}{3}$$
$$l_1 = \frac{x-x_0}{x_1-x_0}\cdot\frac{x-x_2}{x_1-x_2} = \frac{x-2}{4-2}\cdot\frac{x-5}{4-5} = -\frac{1}{2}x^2 + \frac{7}{2}x - 5$$
$$l_2 = \frac{x-x_2}{x_2-x_0}\cdot\frac{x-x_1}{x_2-x_1} = \frac{x-2}{5-2}\cdot\frac{x-4}{5-4} = \frac{1}{3}x^2 - 2x + \frac{8}{3}.$$

Luego $p(x) = \sum_{i=0}^{2} y_i l_i(x)$, así

$$\begin{aligned} p(x) &= 1942(\frac{1}{6}x^2 - \frac{2}{3}x + \frac{10}{3}) + 3402(-\frac{1}{2}x^2 + \frac{7}{2}x - 5) + 4414(\frac{1}{3}x^2 - 2x + \frac{8}{3}) \\ &= 1234 + 166x + 94x^2, \end{aligned}$$

luego $p(0) = 1234$, es decir $S = 1234$.

Si tenemos sólo 2 parejas, se construye un polinomio lineal, pero este no arroja mayor información del secreto que hemos escondido.

- **Aritmética modular**

  Escogemos $S = 15$, $n = 5$, $k = 3$ y $p = 137$. Seleccionamos arbitrariamente a a_1, a_2 en $\mathbb{Z}_p$, esto es: $a_1 = 58$ y $a_2 = 121$, construimos el polinomio de grado 2

  $$p(x) = 15 + 58x + 121x^2,$$

  evaluamos los puntos $1, 2, 3, 4, 5$ y obtenemos las parejas:

  $$(1, 57), (2, 67), (3, 45), (4, 128), (5, 42)$$

  y estas son las que entregamos a los participantes.

  Supongamos ahora que se reúnen 3 participantes con las siguientes parejas:

  $$(3, 45), (4, 128), (5, 42),$$

usamos entonces el método de interpolación de Lagrange para construir un polinomio de grado 2, modulando los resultados:

$$l_0 = \frac{x-x_1}{x_0-x_1}\cdot\frac{x-x_2}{x_0-x_2} = \frac{x-4}{3-4}\cdot\frac{x-5}{3-5} = 69x^2+64x+10$$
$$l_1 = \frac{x-x_0}{x_1-x_0}\cdot\frac{x-x_2}{x_1-x_2} = \frac{x-3}{4-3}\cdot\frac{x-5}{4-5} = 139x^2+8x+122$$
$$l_2 = \frac{x-x_2}{x_2-x_0}\cdot\frac{x-x_1}{x_2-x_1} = \frac{x-3}{5-3}\cdot\frac{x-4}{5-4} = 69x^2+65x+6$$

así encontramos $p(x)$,

$$\begin{aligned} p(x) &= 45(69x^2+64x+10)+128(139x^2+8x+122)+42(69x^2+65x+6) \\ &= 121x^2+58x+15. \end{aligned}$$

Entonces evaluando $p(x)$ en 0 obtenemos $S = 15$ recuperando el secreto.

Si se tiene menos de k, por ejemplo $k-1$, podríamos escoger cualquier número $r \in \mathbb{Z}_{137}$ para construir el polinomio y suponer que $p(0) = r$ pero es claro que en cuanto el intervalo $[0, 137)$ existen muchas posibilidades.

1.2. Esquema de Blakley

George Robert (Bob) Blakley Jr, Criptógrafo americano, Licenciado en Física de la Universidad de Georgetown. Profesor de la Universidad de Illinois y la Universidad Estatal de New York, fue cofundador de la revista internacional de la Seguridad de la Información publicada por Spring-Verlag en 2000 y es miembro de su consejo asesor actualmente.

El esquema de Blakley se basa en hiperplanos geométricos de la siguiente manera:

- Dado n el numero de participantes, escogemos un primo p mayor que n.

- Nuestro secreto S es un valor que depende de un punto v en un espacio $\mathbb{Z}_p^{k+1}$.
- Establecemos n ecuaciones de hiperplanos geométricos de manera que cada uno de ellos pase por el punto v. Estas ecuaciones serán entregadas a los participantes.

El proceso de recuperación funciona como sigue:
Si tenemos k hiperplanos se intersectan obteniendo un subespacio de dimensión 1 que es la recta que une al punto v y al origen.
Si tenemos menos de k hiperplanos, supongamos $k-1$ su intersección arroja un subespacio de dimensión 2 que contiene al punto v pero en el cual no tenemos elementos para recuperarlo.

Ejemplo

1. Consideremos $n = 3$, $k = 2$, $p = 23$, y $v = (9, 1, 2)$ con $S = 9$, es decir S es la primera componente del punto escogido, para determinar las ecuaciones de los hiperplanos que debemos entregar construiremos una matriz así:

$$\begin{bmatrix} 9 & 1 & 2 \\ 1 & 4 & 6 \\ 8 & 5 & 1 \\ 11 & 10 & 1 \end{bmatrix}$$

   Dicha matriz debe cumplir con las siguientes condiciones:

   - Cada una de sus filas de contener un único 1 y las demás componentes son elementos de $\mathbb{Z}_p$ distintos.
   - Cada submatriz 2x2 debe ser invertible.

- Los determinantes de las submatrices de orden 2 deben ser distintos por parejas.

Con esta matriz obtenemos que las ecuaciones de los hiperplanos son:

$$59x + 9y + 35z = 0 \tag{1.1}$$

$$52x + 7y + 37z = 0 \tag{1.2}$$

$$42x + 13y + 18z = 0. \tag{1.3}$$

Para recuperar el secreto supongamos que tenemos dos de estas, sean 1.1 y 1.2, establecemos su intersección obteniendo el punto:

$$\begin{pmatrix} 35 \\ 31 \\ 1 \end{pmatrix}$$

este punto indica la recta sobre la cual se encuentra el punto v del cual sabemos que tiene un 1 en una de sus componentes. Tenemos entonces 3 candidatos a ser el punto v, estos dependen de las tres posibilidades de obtener un múltiplo del punto hallado con una componente 1, a saber:

$$\begin{pmatrix} 35 \\ 31 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 18 \\ 13 \end{pmatrix}, \quad \begin{pmatrix} 9 \\ 1 \\ 2 \end{pmatrix},$$

y el último de los anteriores es el punto que escogimos y el cual contiene el secreto.

1.3. Esquema de Asmuth-Bloom

Charles Asmuth y Jonathan Bloom, Ingenieros. El esquema de Asmuth-Bloom se basa en el Teorema Chino de los Residuos, haciendo uso de unas sucesiones especiales de enteros. Esto es, sean $r, m_1 < \cdots < m_n$ enteros positivos primos relativos por parejas tales que:

$$r \cdot m_{n-k+2} \cdots m_n < m_1 \cdots m_k.$$

Usando la anterior sucesión establecemos las parejas a entregar de la siguiente manera:

- La sucesión es pública para todos los participantes.
- Escogemos S en $\mathbb{Z}_r$.
- Tomamos γ arbitrario tal que $d = S + \gamma \cdot r \in \mathbb{Z}_{m_1 \cdots m_k}$ y además $d > r \cdot m_{n-k+2} \cdots m_n$.
- Las parejas (I_i, m_i) a entregar se forman de manera que $d \equiv I_i \pmod{m_i}$, para todo $i = 1, ..., n$.
- Entregamos a cada participante una pareja (I_i, m_i)

El esquema funciona de la siguiente manera:
Si tenemos k parejas podemos obtener a S, estableciendo el sistema de congruencias,

$$\begin{aligned} x &\equiv I_{i_1} \pmod{m_{i_1}}, \\ &\vdots \\ x &\equiv I_{i_k} \pmod{m_{i_k}}. \end{aligned}$$

Aplicamos el Teorema Chino de los Residuos y encontramos un $x_0 = d$ solución del sistema anterior, dado que x_0 es la solución única módulo $m_{i_1} \cdot m_{i_2} \cdots m_{i_k}$ y escogimos a $d < m_1 \cdots m_k < m_{i_1} \cdot m_{i_2} \cdots m_{i_k}$, ahora para encontrar a S hacemos $S \equiv x_0 \pmod{r}$, y

obtenemos el secreto S original.

Si tenemos menos de k pareja, supongamos $k-1$ entonces al establecer las congruencias:

$$\begin{aligned} x &\equiv I_{i_1} \pmod{m_{i_1}}, \\ &\vdots \\ x &\equiv I_{i_{k-1}} \pmod{m_{i_{k-1}}}, \end{aligned}$$

aplicamos nuevamente el teorema chino de los residuos y obtenemos un x_0' módulo $m_{i_1} \cdots m_{i_{k-1}}$ pero $m_{i_1} \cdots m_{i_{k-1}} < m_n \cdot m_{n-1} \cdots m_{n-k+2}$, así debemos buscar un número congruente con x_0' en el intervalo $(r \cdot m_{n-k+2} \cdots m_n, m_1 \cdots m_k)$ para luego encontrar su congruencia módulo r, lo cual resulta difícil si el intervalo lo hacemos muy grande.

Ejemplo

1. Sean $17, 19, 23, 29, 31, 37$, $r = 6$, donde $M = 17 \cdot 19 \cdot 23 = 7429$ y $N = 6 \cdot 31 \cdot 37 = 6882$, tenemos $M > N$ tomamos $S = 5$, y $\gamma = 1150$, tendremos pues que $d = 5 + 1150 \cdot 6 \in \mathbb{Z}_{17 \cdot 19 \cdot 23}$, establecemos con d de la siguiente manera:

$$\begin{aligned} d &\equiv 3 \pmod{17}, \\ d &\equiv 8 \pmod{19}, \\ d &\equiv 5 \pmod{23}, \\ d &\equiv 3 \pmod{29}, \\ d &\equiv 23 \pmod{31}, \\ d &\equiv 23 \pmod{37}, \end{aligned}$$

   luego las parejas a entregar serán $(3, 17), (8, 19), (5, 23), (3, 29), (23, 31), (23, 37)$.

   Para recuperar el secreto, supongamos que tenemos 3 de estas parejas, sean $(3, 17)$,

$(5, 23), (3, 29)$, establecemos el sistema de congruencias

$$x \equiv 3 \pmod{17},$$
$$x \equiv 5 \pmod{23},$$
$$x \equiv 3 \pmod{29}.$$

Aplicando el teorema chino de los residuos obtenemos $x_0 = 6905$ módulo 11339, entonces para encontrar S a x_0 lo modulamos con 6, es decir hacemos $6905 \equiv 5$ (mód 6), así encontramos el secreto.

supongamos que solo tenemos $(3, 17), (8, 19)$, establecemos el sistema:

$$x \equiv 3 \pmod{17},$$
$$x \equiv 8 \pmod{19},$$

aplicamos el teorema chino de los residuos y obtenemos $x_0' = 1338$ entonces buscaremos un los números congruente con 1338 en el intervalo $(6882, 7429)$.

Nota: El esquema de Mignotte será tratado con detalle en el siguiente capítulo.

Capítulo 2

Esquema de Mignotte

Maurice Mignotte matemático francés, profesor de la universidad Strasburg (Francia) en 1986 presentó un esquema de umbral basado en el teorema chino de los residuos y planteó las sucesiones de umbral o sucesiones de Mignotte las cuales usa para el desarrollo de este esquema.

Las sucesiones (k, n) de Mignotte nacen con el esquema de umbral que lleva el mismo nombre.

2.1. Sucesiones (k, n) de Mignotte

Definición 2.1.1 (**Sucesión** (k, n) **de Mignotte**). *Dados n, k enteros positivos con $2 \leq k \leq n$, una sucesión (k, n) de Mignotte es una sucesión creciente de enteros positivos primos relativos por parejas $m_1, ..., m_n$ tales que:*

$$M = m_1 \cdot m_2 \cdots m_k > m_n \cdot m_{n-1} \cdots m_{n-k+2} = N,$$

es decir, el producto de los k menores es mayor que el producto de los $k-1$ mayores.

Ejemplos

- Los números $5, 7, 9, 11, 13$ conforman una $(3, 5)$ sucesión de Mignotte, veamos $M = 5 \cdot 7 \cdot 9 = 315$ y $N = 11 \cdot 13 = 143$, así $M > N$

- Los números $127, 131, 137, 139, 149, 151, 157, 163, 167$ conforman una sucesión $(3, 9)$ de Mignotte, veamos $M = 127 \cdot 131 \cdot 137 = 2279269$ y $N = 163 \cdot 167 = 27221$ con $M > N$.

La construcción de sucesiones (k, n) de Mignotte no es un problema trivial, en [9] encontramos pautas para construir estas sucesiones dados cualesquiera n y k con $2 \leq k \leq n$. Enseguida presentaremos algunos resultados para la construcción de dichas sucesiones.

Lema 2.1.1. *La sucesión* $\left\{ \left(\frac{k^2}{k^2-1} \right)^{k^2} \right\}_{k=2}^{\infty}$, $k \geq 2$ *es una sucesión decreciente y además tiene como límite e.*

Demostración. Veamos que la sucesión es decreciente, para esto analizaremos el comportamiento de la siguiente función con x real.

$$f(x) = \left(\frac{x^2}{x^2-1} \right)^{x^2},$$

luego

$$f'(x) = 2x \left[\ln \frac{x^2}{x^2-1} - \frac{1}{x^2-1} \right] \left(\frac{x^2}{x^2-1} \right)^{x^2},$$

pero $\left(\frac{x^2}{x^2-1}\right)^{x^2} > 0$ y $\frac{1}{x^2-1} > \ln\frac{x^2}{x^2-1}$. Entonces la sucesión es decreciente.

Mostramos ahora que su limite es e, para esto hacemos un cambio de variable a variable real, definimos $f(x) = \left(\frac{x^2}{x^2-1}\right)^{x^2}$.

$$\lim_{x\to\infty}\left(\frac{x^2}{x^2-1}\right) = \lim_{x\to\infty} e^{x^2\ln\left(\frac{x^2}{x^2-1}\right)},$$

para esto

$$\begin{aligned}
\lim_{x\to\infty} x^2\ln\left(\frac{x^2}{x^2-1}\right) &= \lim_{x\to\infty}\frac{\ln\left(\frac{x^2}{x^2-1}\right)}{\frac{1}{x^2}} \\
&= \lim_{x\to\infty}\frac{\frac{1}{\frac{x^2}{x^2-1}}\cdot\frac{-2x}{(x^2-1)^2}}{\frac{-2x}{x^4}} \\
&= \lim_{x\to\infty}\frac{\frac{-2x}{x^2(x^2-1)}}{\frac{-2x}{x^4}} \\
&= \lim_{x\to\infty}\frac{x^4}{x^2(x^2-1)} \\
&= \lim_{x\to\infty}\frac{x^2}{x^2-1} = 1.
\end{aligned}$$

Así

$$\lim_{x\to\infty}\left(\frac{x^2}{x^2-1}\right)^{x^2} = e$$

$\star$

Del teorema de los números primos obtenemos los siguientes resultados que demostramos:

Proposición 2.1.1. *Sea p_n el n-ésimo primo y sea α un número real con $0 < \alpha < 1$. Denotamos con $\pi(n,\alpha)$ el número de primos en el intervalo $(p_n^\alpha, p_n]$. Entonces tenemos*

que para todos n, t suficientemente grandes se cumple

$$\pi(n+t,\alpha) \approx (n+t)\left(1-\frac{1}{\alpha p_{n+t}^{1-\alpha}}\right).$$

Demostración. Tenemos que $\pi(n+t,\alpha)$ es el número de primos en el intervalo $(p_{n+t}^{\alpha}, p_{n+t}]$ de aquí que:

$$\begin{aligned}
\pi(n+t,\alpha) &= \pi(p_{n+t}) - \pi(p_{n+t}^{\alpha}) \\
&\approx \frac{p_{n+t}}{\ln p_{n+t}} - \frac{p_{n+t}^{\alpha}}{\ln p_{n+t}^{\alpha}} \\
&= \frac{p_{n+t}}{\ln p_{n+1}} - \frac{p_{n+t}^{\alpha}}{\alpha \ln p_{n+t}} \\
&= \frac{p_{n+t}}{\ln p_{n+t}}\left(1-\frac{p_{n+t}^{\alpha-1}}{\alpha}\right) \\
&= \frac{p_{n+t}}{\ln p_{n+t}}\left(1-\frac{1}{\alpha p_{n+t}^{1-\alpha}}\right) \\
&\approx \pi(p_{n+t})\left(1-\frac{1}{\alpha p_{n+1}^{1-\alpha}}\right) \\
&= (n+t)\left(1-\frac{1}{\alpha p_{n+t}^{1-\alpha}}\right).
\end{aligned}$$

Con esto hemos confirmado la aproximación. ⋆

Proposición 2.1.2. *En particular, para cualesquiera k, n con $2 \leq k \leq n$ existen enteros t arbitrariamente grandes tales que*

$$\pi\left(t, \frac{k^2-1}{k^2}\right) > n.$$

Demostración. La sucesión decreciente $\left\{\left(\frac{k^2}{k^2-1}\right)^{k^2}\right\}_{k=2}^{\infty}$ toma su valor máximo en $k = 2$ y es $\frac{256}{81} < 5$. Como $5 > \left(\frac{k^2}{k^2-1}\right)^{k^2}$, entonces $\frac{k^2-1}{k^2}5^{\frac{1}{k^2}} > 1$, luego $\frac{k^2-1}{k^2}5^{\frac{1}{k^2}} - 1 > 0$.

Buscamos un entero h tal que

$$h > \frac{n}{\frac{k^2-1}{k^2}5^{\frac{1}{k^2}} - 1} = \frac{n}{\frac{k^2-1}{k^2}p_3^{\frac{1}{k^2}} - 1},$$

como $n \geq 2$ y $h \geq 1$ entonces $n + h \geq 3$, luego

$$h > \frac{n}{\frac{k^2-1}{k^2}p_3^{\frac{1}{k^2}} - 1} \geq \frac{n}{\frac{k^2-1}{k^2}p_{n+h}^{\frac{1}{k^2}} - 1}$$

$$h\left(\frac{k^2-1}{k^2}p_{n+h}^{\frac{1}{k^2}} - 1\right) > n$$

$$h\left(\frac{k^2-1}{k^2}p_{n+h}^{\frac{1}{k^2}}\right) > n + h$$

$$h > \frac{n+h}{\frac{k^2-1}{k^2}p_{n+h}^{\frac{1}{k^2}}}$$

$$n + h > \frac{n+h}{\frac{k^2-1}{k^2}p_{n+h}^{\frac{1}{k^2}}} + n$$

$$(n+h)\left(1 - \frac{1}{\frac{k^2-1}{k^2}p_{n+h}^{\frac{1}{k^2}}}\right) > n.$$

Haciendo $t = n + h$, tenemos la desigualdad requerida:

$$\pi\left(t, \frac{k^2-1}{k^2}\right) = \pi\left(n+h, \frac{k^2-1}{k^2}\right) \approx (n+h)\left(1 - \frac{1}{\frac{k^2-1}{k^2}p_{n+h}^{\frac{1}{k^2}}}\right) > n$$

$\star$

2.2. Construcción de Sucesiones (k, n) de Mignotte

Mostramos que para n y k dados con $2 \leq k \leq n$ se puede garantizar la existencia de al menos una sucesión (k, n) de Mignotte. Para esto utilizamos la proposición 2.1.2.
Tomamos un t arbitrariamente grande que garantiza que existen al menos n primos en el intervalo

$$\left(p_t^{\frac{k^2-1}{k^2}}, p_t\right]$$

Puesto que tenemos n o más primos en el intervalo, tomamos los n últimos reorganizándolos de la siguiente manera:

$$m_i = p_{t-n+1}, \quad i = 1, \ldots, n,$$

formamos ahora los productos

$$M = m_1 \cdot m_2 \cdots m_k \text{ y } N = m_n \cdot m_{n-1} \cdots m_{n-k+2}.$$

Ahora

$$m_1 \cdot m_2 \cdots m_k \geq p_t^{\frac{k^2-1}{k^2}},$$

puesto que para cada $j = 1 \ldots k$ tenemos $m_j > p_t^{\frac{k^2-1}{k^2}}$. Además

$p_t^{k-1} \geq m_n \cdot m_{n-1} \cdots m_{n-k+2}$ pues para cada $i = n-k+2, \ldots, n$ tenemos $m_i < p_t$.

También tenemos que

$$\frac{k^2-1}{k^2} - (k-1) = \frac{k^2-1-k^2+k}{k} = \frac{k-1}{k} > 0$$

de aquí que $p_t^{\frac{k^2-1}{k}} > p_t^{k-1}$ y entonces obtenemos

$$M = m_1 \cdot m_2 \cdots m_k \geq p_t^{\frac{k^2-1}{k}} > p_t^{k-1} \geq m_n \cdot m_{n-1} \cdots m_{n-k+2} = N.$$

Esto muestra que en efecto la sucesión constituida por los m_i es una sucesión (k, n) de Mignotte.

Ejemplo

Con ayuda de *Matlab* construimos una sucesión (k, n) de Mignotte.

- Con $n = 15$ y $k = 3$ el menor h que nos sirve es $h = 44$. Entonces $t = n + h = 59$ y Matlab nos da $p_t = 281$ y la siguiente lista de primos consecutivos:

$$197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 263, 269, 271, 277, 281.$$

  Veamos que es una sucesión de Mignotte,

$$M = (197 \cdot 199 \cdot 211) = 8271833 > 77837 = (277 \cdot 281) = N.$$

2.3. Esquema de Mignotte

Teorema 2.3.1 (**Construcción de un Esquema de Umbral**). *Para todos n y k con $2 \leq k \leq n$ existe un esquema (k, n) de umbral.*

Demostración. Consideremos $m_1, \ldots, m_n$ enteros positivos primos relativos por parejas, tales que estos determinen una sucesión de Mignotte. Sean

$$M = m_1 \cdot m_2 \cdots m_k \quad \text{y} \quad N = m_n \cdots m_{n-k+2}$$

sea S el secreto, un entero tal que $N \leq S \leq M$ y las parejas $(a_1, m_1), \ldots (a_n, m_n)$ definidas

por

$$\begin{aligned} S &\equiv a_1 \pmod{m_1}, \\ S &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ S &\equiv a_n \pmod{m_n}. \end{aligned}$$

Mostramos que el secreto S y las parejas $\{(a_1, m_1), (a_2, m_2), \ldots (a_n, m_n)\}$ definen un esquema (k, n) de umbral.
Conocidas k de estas parejas, supongamos $\{(a_{i_1}, m_{i_1}), \ldots (a_{i_k}, m_{i_k})\}$, consideramos el sistema de congruencias

$$\begin{aligned} x &\equiv a_{i_1} \pmod{m_{i_1}}, \\ x &\equiv a_{i_2} \pmod{m_{i_2}}, \\ &\vdots \\ x &\equiv a_{i_k} \pmod{m_{i_k}}. \end{aligned}$$

Aplicando el teorema chino de los residuos, este sistema tiene solución única módulo $m_{i_1} \cdot m_{i_2} \cdots m_{i_k}$, la que denotamos S'. Dado que $m_{i_1} \cdot m_{i_2} \cdots m_{i_k} \geq M > S > N$ y S también es solución de este sistema, tenemos que $S' = S$, entonces S' es el secreto buscado.

Supongamos ahora que conocemos menos de k parejas, es decir $\{(a_{i_1}, m_{i_1}) \ldots (a_{i_{k-1}}, m_{i_{k-1}})\}$,

consideremos

$$\begin{aligned} x &\equiv a_{i_1} \quad (\text{mód } m_{i_1}), \\ x &\equiv a_{i_2} \quad (\text{mód } m_{i_2}), \\ &\vdots \\ x &\equiv a_{i_{k-1}} \quad (\text{mód } m_{i_{k-1}}). \end{aligned}$$

Aplicando nuevamente el teorema chino de los residuos obtenemos una solución S' única módulo $m_{i_1} \cdot m_{i_2} \cdots m_{i_{k-1}}$. Como $S' \leq m_{i_1} \cdots m_{i_{k-1}} < N < S < M$ tendremos que buscar entre $\dfrac{M-N}{N}$ posibilidades para encontrar exactamente a $S \equiv S'$ (mód $m_{i_1} \cdot m_{i_2} \cdots m_{i_{k-1}}$). Aquí vemos que la seguridad del esquema depende de que el factor $\dfrac{M-N}{N}$ sea grande.$_\star$

Utilizando una sucesión (k, n) de Mignotte como la construida al principio tenemos que

$$\frac{M-N}{N} \geq \frac{p_t^{\frac{k^2-1}{k}} - p_t^{k-1}}{p_t^{k-1}} = p_t^{\frac{k-1}{k}} - 1.$$

Así para que el esquema tenga éxito a la hora de brindar seguridad debemos escoger t, en el momento de construir la sucesión (k, n) de Mignotte, de manera que $p_t^{\frac{k-1}{k}} - 1$ sea lo suficientemente grande para hacer difícil computacionalmente la búsqueda de secreto S. Por ejemplo si quisiéramos más de 1000 posibilidades de evaluación para S, el primo p_t debe ser tal que $p_t > 1001^{\frac{k}{k-1}}$.

Ejemplos

- Los números $5, 7, 9, 11, 13$ conforman una sucesión $(3, 5)$ Mignotte, $M = 315$ y $N =$

143. Con $N < S < M$ de manera que:

$$\begin{aligned} S &\equiv 0 \pmod 5, \\ S &\equiv 4 \pmod 7, \\ S &\equiv 1 \pmod 9, \\ S &\equiv 4 \pmod{11}, \\ S &\equiv 1 \pmod{13}, \end{aligned}$$

entregamos las parejas $(0,5)$, $(4,7)$, $(1,9)$, $(4,11)$, $(1,13)$. Si tenemos $(0,5)$, $(1,9)$ y $(1,13)$ resolvemos el sistema

$$\begin{aligned} x &\equiv 0 \pmod 5, \\ x &\equiv 1 \pmod 9, \\ x &\equiv 1 \pmod{13}, \end{aligned}$$

aplicando el teorema chino de los residuos y obtenemos que la respuesta es $S' = 235 = S$. Si tenemos sólo dos parejas, supongamos $(4,7)$ y $(4,11)$, con el sistema

$$\begin{aligned} x &\equiv 4 \pmod 7, \\ x &\equiv 4 \pmod{11}, \end{aligned}$$

y nuevamente aplicando el teorema chino de los residuos tenemos $S' = 4$ módulo 77, luego $S \equiv 4 \pmod{77}$. Ahora, entre N y M tenemos

$$235 \equiv 312 \equiv 4 \pmod{77}.$$

- Los números $19, 23, 29, 31, 37, 41, 43, 47$ conforman una sucesión $(4,8)$ de Mignotte con $M = 392863$ y $N = 8286$, tomando $S = 87320$ establecemos las respectivas

congruencias para fraccionar y repartir nuestro secreto.

Si se dispone sólo de tres congruencias,

$$\begin{aligned} x &\equiv 12 \pmod{23}, \\ x &\equiv 1 \pmod{29}, \\ x &\equiv 0 \pmod{37}. \end{aligned}$$

Usando el teorema chino de los residuos obtenemos $S' = 3630$, quien es congruente con S módulo 24679, pero $N < S < M$. Debemos buscar entre más de $\dfrac{M-N}{N}$ posibilidades en este caso 15.

- Usando la sucesión $(3, 15)$ de Mignotte encontrada

$$197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 263, 269, 271, 277, 281,$$

y $S = 8193996$ y obtenemos las parejas

$$(175, 197), (171, 199), (22, 211), (84, 223), (204, 227), (147, 229), (85, 233), (120, 239),$$
$$(237, 241), (101, 251), (65, 257), (231, 263), (256, 269), (40, 271), (59, 277), (36, 281).$$

Supongamos que tenemos 3 de las anteriores parejas $(175, 197), (84, 223), (36, 281)$. Establecemos el sistema de congruencias:

$$\begin{aligned} x &\equiv 175 \pmod{197}, \\ x &\equiv 84 \pmod{223}, \\ x &\equiv 36 \pmod{281}, \end{aligned}$$

aplicando el teorema chino de los residuos obtenemos que la solución es $x' = 8193996$ (mód 12344611) y $x' = S$.

Si sólo tenemos 2 supongamos $(204, 227), (237, 241)$, establecemos el sistema:

$$x \equiv 204 \pmod{227},$$
$$x \equiv 237 \pmod{241},$$

así aplicando el teorema chino de los residuos obtenemos una solución $x' = 42653$ (mód 54707), luego para encontrar a S debemos buscarlo en $(77837, 8271833)$ y en este caso tenemos aproximadamente 105 posibilidades.

- Si deseamos una sucesión $(3, 15)$ de Mignotte en donde hayan más de 200 posibilidades buscamos un primo $p_t > 200^{3/2}$ con $t \geq 59$. Con $t = 410$ obtenemos $p_t = 2833$ y la sucesión

$$2713, 2719, 2729, 2731, 2741, 2749, 2753, 2767, 2777,$$
$$2789, 2797, 2801, 2803, 2819, 2833$$

con $M = 2713 \cdot 2719 \cdot 2729 = 20130869663 > 7986227 = 2819 \cdot 2833 = N$ y $\dfrac{M - N}{N} > 2519$.

2.4. Comentarios

Una mejora que proponemos para el esquema de Mignotte es que la sucesión no sea pública. En el esquema normal los participantes conocen el intervalo (N, M), así estos pueden conocer donde se encuentra el secreto S y además el número de posibilidades para encontrarlo cuando se conocen menos parejas que el umbral k. Teniendo los participantes $k - 1$

parejas o menos podrían establecer una cota mínima y empezar a buscar el secreto pero no tienen una constante superior con la cual acotar las posibilidades para encontrar a S, volviendo las posibilidades infinitas.

Invito a estudiar esta mejora en el esquema de Mignotte.

Ejercicio propuesto

- Trate de establecer un intervalo (N, M) donde se encuentre el secreto S con las siguientes parejas $(28, 211), (121, 227)$ sabiendo que $k = 3$.

Capítulo 3

Esquema de Mignotte Generalizado

Sorin Iftene, Matemático, Rumano propone un nuevo esquema basándose en una generalización del teorema chino de los residuos y generalizando las sucesiones (k, n) de Mignotte. En esta sección presentamos en detalle la construcción de dicho esquema y las sucesiones (k, n) de Mignotte generalizadas cumpliendo así el objetivo principal de este trabajo.

3.1. Una generalización del Teorema Chino de los Residuos

En el teorema chino de los residuos, el que los módulos sean primos relativos por parejas es condición suficiente para que exista solución al sistema de congruencias. A continuación presentamos una generalización en la cual los módulos del sistema no son primos relativos por parejas.

En primer lugar mostramos un resultado en el cual se establece una ley de distribución entre el máximo común divisor y el mínimo común múltiplo cuando se involucran tres números.

Lema 3.1.1. *Si a, b, c son enteros positivos, entonces $(a, [b, c]) = [(a, b), (a, c)]$.*

Demostración. veamos que los dos términos de la igualdad propuesta se dividen mutuamente.

- Por definición de máximo común divisor tenemos

$$(a, b) \mid a \quad \text{y} \quad (a, b) \mid b.$$

Combinando con la noción de mínimo común múltiplo,

$$b \mid [b, c] \quad \text{de donde} \quad (a, b) \mid [b, c].$$

Tenemos entonces

$$(a, b) \mid a \quad \text{y} \quad (a, b) \mid [b, c],$$

de donde

$$(a, b) \mid (a, [b, c]).$$

Análogamente se concluye

$$(a, c) \mid (a, [b, c])$$

y como $(a, [b, c])$ es múltiplo de (a, c) y de (a, b), entonces

$$[(a, b), (a, c)] \mid (a, [b, c]).$$

- Ahora involucramos enteros x, y, z, w tales que $(a, b) = ax + by$ y $(a, c) = az + cw$. También usamos el hecho de que para enteros positivos k, m, n tenemos las igualdades $[k, m](k, m) = km$ y $((k, m), n) = (k, m, n) = ((k, m), (k, n))$. En su momento introduciremos además los enteros

$$r = \frac{c}{(a, b, c)} \quad s = \frac{ax + by}{((a, b), (a, c))} \quad t = \frac{[a, (b, c)]}{a}.$$

Reescribimos entonces

$$\begin{aligned}
[(a, b), (a, c)] &= \frac{(a, b)(a, c)}{((a, b), (a, c))} \\
&= \frac{(ax + by)(az + cw)}{((a, b), (a, c))} \\
&= axw\frac{c}{(a, b, c)} + az\frac{(ax + by)}{((a, b), (a, c))} + \frac{bcyw}{(a, (b, c))} \\
&= a(xwr + zs) + \frac{bcyw[a, (b, c)]}{a(b, c)} \\
&= a(xwr + zs) + \frac{bc}{(b, c)}yw\frac{[a, (b, c)]}{a} \\
&= a(xwr + zs) + [b, c](ywt)
\end{aligned}$$

Esto muestra que $[(a, b), (a, c)]$ es combinación de a y $[b, c]$ de donde

$$(a, [b, c]) \mid [(a, b), (a, c)].$$

En conclusión hemos garantizado la igualdad propuesta. ⋆

La proposición siguiente garantiza que lo demostrado para el mínimo común múltiplo de dos números se puede extender al caso en que tenemos el mínimo común múltiplo de cualquier cantidad finita de números.

Proposición 3.1.1. *Sean $a, b_1, \ldots, b_n$ enteros positivos tales que $[b_1, \ldots, b_n] = m$, entonces $(a, m) = [(a, b_1), (a, b_2), \ldots, (a, b_n)]$.*

Demostración. Utilizando principio de inducción matemática: Para $n = 2$, tenemos el Lema 3.1.1. Supongamos el resultado válido para cualquier entero menor que n y sean $b_1, b_2, \ldots, b_n$ enteros arbitrarios, entonces

$$\begin{aligned}(a, [b_1, \ldots, b_{n-1}, b_n]) &= [(a, [b_1, \ldots, b_{n-1}]), (a, b_n)] \\ &= [[(a, b_1), \ldots (a, b_{n-1})], (a, b_n)] \\ &= [(a, b_1), \ldots (a, b_{n-1}), (a, b_n)]\end{aligned}$$

$\star$

Nota: Se usó la asociatividad del mínimo común múltiplo, esto es que para $r \geq 2$, los enteros positivos s_i satisfacen $[[s_1, \ldots, s_r], s_{r+1}] = [s_1, \ldots, s_r, s_{r+1}]$.

Establecido lo anterior procedemos a presentar la generalización del Teorema Chino de los Residuos.

Teorema 3.1.1 (Generalización del Teorema Chino de los Residuos). *Sean $m_1, m_2, \ldots, m_n$ son enteros positivos y $a_1, a_2, \ldots, a_n$ enteros arbitrarios, el sistema*

$$\begin{aligned}x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_n \pmod{m_n},\end{aligned}$$

tiene solución si y sólo si para todos $i \neq j$, se cumple que $(m_i, m_j) \mid a_i - a_j$. Además, si hay solución esta es única módulo $[m_1, m_2, \ldots m_n]$

Demostración.

- Si existe una solución, llamémosla c. Para $i \neq j$ tenemos $m_j \mid c - a_j$ y $m_i \mid a_i - c$ y consecuentemente $(m_i, m_j) \mid a_i - a_j$.

  Veamos la unicidad de la solución. Si c y d son soluciones, $m_i \mid c - d$ para todo i y por definición de mínimo común múltiplo, $[m_1, \ldots, m_n] \mid c - d$. Esto es, $c \equiv d \pmod{[m_1, ..., m_n]}$.

- Para el recíproco utilicemos principio de inducción matemática. Inicialmente consideramos $n = 2$:

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$

  donde $(m_1, m_2) \mid a_1 - a_2$. La congruencia $m_2 \cdot x \equiv a_1 - a_2 \pmod{m_1}$ tiene (m_1, m_2) soluciones, sea c una de estas, entonces

$$m_2 \cdot c + a_2 \equiv a_1 \pmod{m_1},$$
$$m_2 \cdot c + a_2 \equiv a_2 \pmod{m_2}.$$

  Así, $m_2 \cdot c + a_2$ es solución del sistema (con la unicidad garantizada anteriormente). Ahora supongamos que el resultado es válido siempre que se tengan n congruencias y consideramos $m_1, \ldots, m_n, m_{n+1}$, enteros positivos, $a_1, \ldots, a_n, a_{n+1}$, enteros arbitrarios tales que:

$$(m_i, m_j) \mid a_i - a_j \quad \text{para} \quad i \neq j.$$

Al considerar el sistema

$$\begin{aligned} x &\equiv a_1 \quad (\text{mód } m_1), \\ x &\equiv a_2 \quad (\text{mód } m_2), \\ &\vdots \\ x &\equiv a_{n+1} \quad (\text{mód } m_{n+1}), \end{aligned}$$

tenemos por hipótesis inductiva que el sistema correspondiente a las primeras n congruencias tiene solución única módulo $[m_1, \ldots, m_n] = m$. Llamemos c a tal solución y planteemos el sistema:

$$x \equiv c \quad (\text{mód } m) \tag{3.1}$$

$$x \equiv a_{n+1} \quad (\text{mód } m_{n+1}). \tag{3.2}$$

Para cada $i = 1, \ldots, n$ tenemos, $m_i \mid c - a_i$ y $(m_i, m_{n+1}) \mid a_i - a_{n+1}$, luego $(m_i, m_{n+1}) \mid c - a_{n+1}$, de donde

$$[(m_1, m_{n+1}), (m_2, m_{n+1}), \ldots, (m_n, m_{n+1})] \mid c - a_{n+1}.$$

Reescribiendo el divisor según la proposición demostrada, obtenemos

$$(m, m_{n+1}) \mid c - a_{n+1}$$

y por el caso $n = 2$, el sistema que establece 3.1 y 3.2 tiene solución única módulo $[m, m_{n+1}] = [m_1, \ldots, m_{n+1}]$.

Finalmente, si d es la solución del anterior sistema tenemos:

$$\begin{aligned} d &\equiv c \equiv a_i \quad (\text{mód } m), \\ d &\equiv a_{n+1} \quad (\text{mód } m_{n+1}). \end{aligned}$$

Como $d \equiv c \pmod{m}$ y c es solución del sistema correspondiente a las primeras n congruencias, entonces $d \equiv a_i \pmod{m_i}$ para cada $i = 1, \ldots, n$. Así d es solución del sistema con las $n+1$ congruencias. El principio de inducción nos garantiza entonces la validez del Teorema. $\star$

Ejemplos

- Consideremos el sistema de congruencias:

$$\begin{aligned} x &\equiv 12 \pmod{15}, \\ x &\equiv 2 \pmod{10}, \\ x &\equiv 6 \pmod{12}, \\ x &\equiv 9 \pmod{21}, \end{aligned}$$

para que este sistema tenga solución debe cumplirse que cada máximo común divisor entre cada par debe dividir la resta, respectivamente esto es:

$$\begin{aligned} (15, 10) = 5 \quad &; \quad 5 \mid 12 - 2, \\ (10, 12) = 2 \quad &; \quad 2 \mid 2 - 6, \\ (12, 21) = 3 \quad &; \quad 3 \mid 6 - 9, \\ (15, 12) = 3 \quad &; \quad 3 \mid 12 - 6, \\ (15, 21) = 3 \quad &; \quad 3 \mid 12 - 9, \\ (10, 21) = 1 \quad &; \quad 1 \mid 2 - 9. \end{aligned}$$

Luego por las hipótesis del teorema tenemos que el sistema de congruencia tiene

solución, para esto resolvemos el sistema

$$\begin{array}{ll} x \equiv 12 & (\text{mód } 15) \\ x \equiv 2 & (\text{mód } 10) \end{array} \quad ; \quad 5 \mid 12-2,$$

encontramos la solución a la siguiente congruencia $10x \equiv 10 \pmod{15}$, así tenemos las siguientes soluciones: $x = 1, 4, 7, 10, 13$. Si tomamos $x = 1$, entonces la solución esta dada por:

$$\begin{aligned} 10 \cdot 1 + 2 &\equiv 12 \pmod{15}, \\ 10 \cdot 1 + 2 &\equiv 2 \pmod{10}, \end{aligned}$$

luego la solución será $12 \pmod{30}$.
Ahora si $x = 4$, entonces

$$\begin{aligned} 10 \cdot 4 + 2 &\equiv 12 \pmod{15}, \\ 10 \cdot 4 + 2 &\equiv 2 \pmod{10}. \end{aligned}$$

La solución en este caso será $42 \pmod{30}$ pero $42 \equiv 12 \pmod{30}$, análogamente se prueba para $x = 7, 10, 13$.

Planteamos ahora el sistema

$$\begin{array}{ll} x \equiv 12 & (\text{mód } 30) \\ x \equiv 6 & (\text{mód } 12) \end{array} \quad ; \quad 6 \mid 12-6,$$

resolvemos la congruencia $12x \equiv 6 \pmod{30}$, en este caso tomamos $x = 3$ y la solución está dada por $42 \pmod{60}$.

Ahora resolvemos el sistema

$$\begin{array}{ll} x \equiv 42 & (\text{mód } 60) \\ x \equiv 9 & (\text{mód } 21) \end{array} \quad ; \quad 3 \mid 42 - 9,$$

así al resolver la congruencia $21x \equiv 33 \pmod{60}$, que tiene como solución $x = 13$ obtenemos la solución al sistema de congruencias que es $282 \pmod{420}$. Comprobemos:

$$\begin{aligned} 282 &\equiv 12 \pmod{15}, \quad ; \quad 15 \mid 282 - 12 = 270, \\ 282 &\equiv 2 \pmod{10}, \quad ; \quad 10 \mid 282 - 2 = 280, \\ 282 &\equiv 6 \pmod{12}, \quad ; \quad 12 \mid 282 - 6 = 276, \\ 282 &\equiv 9 \pmod{21}, \quad ; \quad 21 \mid 282 - 9 = 272. \end{aligned}$$

- Consideremos el sistema de congruencias:

$$\begin{aligned} x &\equiv 9 \pmod{15}, \\ x &\equiv 6 \pmod{21}, \\ x &\equiv 15 \pmod{26}, \\ x &\equiv 12 \pmod{33}, \\ x &\equiv 11 \pmod{34}, \end{aligned}$$

veamos que se cumplen las condiciones del teorema, esto es

$$\begin{aligned}
(15, 21) = 3 \quad &; \quad 3 \mid 9 - 6, \\
(15, 26) = 1 \quad &; \quad 1 \mid 9 - 15, \\
(15, 33) = 3 \quad &; \quad 3 \mid 9 - 12, \\
(15, 34) = 1 \quad &; \quad 1 \mid 9 - 11, \\
(21, 26) = 1 \quad &; \quad 1 \mid 6 - 15, \\
(21, 33) = 3 \quad &; \quad 3 \mid 6 - 12, \\
(21, 34) = 1 \quad &; \quad 1 \mid 6 - 11, \\
(26, 33) = 1 \quad &; \quad 1 \mid 15 - 12, \\
(26, 34) = 2 \quad &; \quad 2 \mid 15 - 11, \\
(33, 34) = 1 \quad &; \quad 1 \mid 12 - 11.
\end{aligned}$$

Así podemos aplicar el teorema y encontramos que la solución al sistema es 13509 (mód 510510).

- Consideremos el siguiente sistema de congruencias:

$$\begin{aligned} x &\equiv 3 \pmod 8, \\ x &\equiv 5 \pmod{10}, \\ x &\equiv 10 \pmod{13}, \\ x &\equiv 11 \pmod{24}, \\ x &\equiv 23 \pmod{29}, \\ x &\equiv 27 \pmod{43}, \\ x &\equiv 17 \pmod{53}, \\ x &\equiv 45 \pmod{85}, \\ x &\equiv 49 \pmod{91}. \end{aligned}$$

Tiene solución $x = 1313330795 \pmod{12269133240}$, esta solución la indica *mupad*.

3.2. Sucesiones (k, n) de Mignotte Generalizadas

Sorin Iftene en 2006 presenta una nueva propuesta para un esquema de umbral generalizando el esquema de Mignotte al apoyarse en una sucesión con términos no primos relativos por parejas. Esta propuesta surge mientras desarrollaba su tesis de doctorado en Ciencias de la Computación.

Presentaremos a continuación los resultados obtenidos por Sorin Iftene.

Definición 3.2.1 (Sucesión (k, n) de Mignotte Generalizada). *Sea n un entero positivo, $n \geq 2$ y $2 \leq k \leq n$. Una sucesión (k, n) de Mignotte generalizada es una*

sucesión $m_1, m_2, \ldots, m_n$ de enteros positivos tales que

$$\beta = \max_{1\leq i_1<\ldots<i_{k-1}\leq n}([m_{i_1}, ..., m_{i_{k-1}}]) < \min_{1\leq i_1<\ldots<i_k\leq n}([m_{i_1}, ..., m_{i_k}]) = \alpha.$$

Nota: Claramente la anterior definición es una generalización de las sucesiones (k, n) de Mignotte, dado que en éstas el mínimo de los mínimos comunes múltiplos de conjuntos de k elementos y el máximo de los mínimos comunes múltiplos de conjuntos de $k-1$ elementos, coinciden respectivamente con el producto de los k menores y el producto de los $k-1$ mayores. Esto porque los m_i, $1 \leq i \leq n$ son primos relativos por parejas.

Iftene sugiere en [5] una manera de construir una sucesión (k, n) de Mignotte generalizada.

Lema 3.2.1. *Sean $m_1, m_2, \ldots, m_n$ enteros que conforman una sucesión (k, n) de Mignotte con $M = m_1 \cdot \cdots \cdot m_k$, $N = m_n \cdot \cdots \cdot m_{n-k+2}$ y δ tal que $(\delta, m_i) = 1$ para todo $1 \leq i \leq n$. Entonces los números $\delta \cdot m_1, \delta \cdot m_2, \ldots, \delta \cdot m_n$ conforman una sucesión (k, n) de Mignotte generalizada.*

Demostración. Consideremos la sucesión $\delta \cdot m_1, \delta \cdot m_2, \ldots, \delta \cdot m_n$ y veamos que es una sucesión (k, n) de Mignotte generalizada. En general para encontrar el mínimo común múltiplo de t elementos de la anterior sucesión $\delta \cdot m_{i_1}, \ldots, \delta \cdot m_{i_t}$ hacemos

$$[\delta \cdot m_{i_1}, \ldots, \delta \cdot m_{i_t}] = \delta[m_{i_1}, \ldots, m_{i_t}] = \delta \cdot m_{i_1} \cdots m_{i_t}$$

de aquí,

$$\beta = \max_{1\leq i_1<\ldots<i_{k-1}\leq n}([\delta \cdot m_{i_1}, ..., \delta \cdot m_{i_{k-1}}]) = \delta \cdot m_1 \cdots m_k = \delta \cdot N,$$
$$\alpha = \min_{1\leq i_1<\ldots<i_k\leq n}([\delta \cdot m_{i_1}, ..., \delta \cdot m_{i_k}]) = \delta \cdot m_n \cdots m_{k+2} = \delta \cdot M$$

como $M > N$, entonces $\alpha > \beta$.

Esto muestra que la anterior es una sucesión (k, n) de Mignotte generalizada. $\star$

Ejemplos

1. La Sucesión $5, 7, 9, 11, 13$ es una sucesión $(3, 5)$ de Mignotte, si tomamos $\delta = 2$ quien es primo relativo con cada uno de los términos de la sucesión, obtenemos $10, 14, 18, 22, 26$ la cual es una sucesión $(3, 5)$ de Mignotte generalizada con

$$\alpha = 630 \quad \text{y} \quad \beta = 286.$$

2. Los números $15, 21, 33, 26, 34$ conforman una sucesión $(3, 5)$ de Mignotte generalizada, con:

3-Conjuntos	**MCM**	**2-Conjuntos**	**MCM**
[15,21,26]	1170	[15,21]	105
[15,21,33]	1155	[15,26]	309
[15,21,34]	3570	[15,33]	165
[15,26,33]	4290	[15,34]	510
[15,26,34]	6630	[21,26]	546
[15,33,34]	5610	[21,33]	231
[21,26,33]	6006	[21,34]	714
[21,26,34]	9282	[26,33]	858
[21,33,34]	7854	[26,34]	442
[26,33,34]	14586	[33,34]	1122

$$\alpha = 1155 \quad \text{y} \quad \beta = 1122.$$

3.3. Esquema de Mignotte Generalizado

Sea $m_1, m_2, \ldots, m_n$ una sucesión (k, n) de Mignotte generalizada con

$$\beta = \max_{1 \leq i_1 < \ldots < i_{k-1} \leq n} ([m_{i_1}, ..., m_{i_{k-1}}]),$$

$$\alpha = \min_{1 \leq i_1 < \ldots < i_k \leq n} ([m_{i_1}, ..., m_{i_k}]).$$

- La sucesión es pública para todos los participantes.
- Escogemos a S un número arbitrario, tal que $\beta < S < \alpha$.
- Las parejas $(I_1, m_1), (I_2, m_2), \ldots, (I_n, m_n)$ se escogen de manera que $S \equiv I_i \pmod{m_i}$.

La recuperación de la información funciona como sigue:
Supongamos que conocemos k de las anteriores parejas, $(I_{i_1}, m_{i_1}), \ldots, (I_{i_k}, m_{i_k})$ donde $1 \leq i_1 < \cdots < i_k \leq n$, así establecemos el sistema de congruencias

$$\begin{aligned} x &\equiv I_{i_1} \pmod{m_{i_1}} \\ x &\equiv I_{i_2} \pmod{m_{i_2}} \\ &\vdots \\ x &\equiv I_{i_k} \pmod{m_{i_k}}. \end{aligned}$$

Aplicando la generalización del teorema chino de los residuos presentada anteriormente obtenemos la solución única $S' \pmod{[m_{i_1}, \ldots, m_{i_k}]}$. Afirmamos que $S' = S$ puesto que $S < \alpha$ y

$$\alpha < [m_{i_1}, ..., m_{i_k}].$$

Si tenemos menos de k parejas supongamos $(I_{i_1}, m_{i-1}), \ldots, (I_{i_{k-1}}, m_{i_{k-1}})$ donde $1 \leq i_1 < \cdots < i_{k-1} \leq n$, establecemos nuevamente el sistema de congruencias

$$\begin{aligned} x &\equiv I_{i_1} \quad (\text{mód } m_{i_1}), \\ &\vdots \\ x &\equiv I_{i_{k_1}} \quad (\text{mód } m_{i_{k-1}}). \end{aligned}$$

Aplicando nuevamente la generalización del teorema chino de los residuos obtenemos una solución única S' (mód $[m_{i_1}, \ldots, m_{i_{k-1}}]$), además $S' \equiv S$ (mód $[m_{i_1}, \ldots, m_{i_{k-1}}]$) pero $S' \neq S$ puesto que $S > \beta$ y

$$\beta > [m_{i_1}, ..., m_{i_{k-1}}],$$

así para encontrar a S debemos buscar entre $\dfrac{\alpha - \beta}{\beta}$ posibilidades lo que indica que debemos construir sucesiones (k, n) de Mignotte generalizadas con un intervalo (β, α) grande.

Ejemplo

1. Los números $454, 458, 466, 478, 591, 597, 633, 669$ conforman una sucesión $(3, 8)$ de Mignotte generalizada con $\alpha = 24224078$ y $\beta = 319782$, escogiendo $S = 10101011$, obtenemos las parejas $(419, 454), (279, 458), (461, 466), (393, 478), (230, 591), (368, 597), (230, 633), (449, 669)$.

   Supongamos que conocemos 3 de dichas parejas $(419, 454), (393, 478), (230, 633)$, entonces conformamos el sistema de congruencias correspondiente:

$$\begin{aligned} x &\equiv 419 \quad (\text{mód } 454), \\ x &\equiv 393 \quad (\text{mód } 478), \\ x &\equiv 230 \quad (\text{mód } 633), \end{aligned}$$

aplicamos la generalización del teorema chino de los residuos obteniendo $x = 10101011$ (mód 68684298) y dado que la generalización nos arroja una solución única, entonces $x = S$.

Si sólo conocemos dos de las anteriores parejas, supongamos $(279, 458), (368, 597)$ nuevamente establecemos el sistema de congruencias:

$$x \equiv 279 \pmod{458},$$
$$x \equiv 368 \pmod{597},$$

así aplicando la generalización del teorema chino de los residuos obtenemos $x = 257675$ quien es congruente con S módulo 273426, en este caso para encontrar a S tenemos 74 posibilidades.

En el esquema de Mignotte vimos cómo podíamos generar sucesiones de Mignotte y hallar un intervalo donde la búsqueda del secreto sea lo suficientemente difícil. Con el lema 3.2.1 podemos obtener sucesiones generalizadas que dependen de las sucesiones de Mignotte lo cual implica generar muchos números primos. Iftene deja abiertos dos problemas: construir sucesiones de Mignotte generalizadas con miras a que las operaciones modulares a realizar al momento de la implementación sean rápidas y construir sucesiones de Mignotte generalizadas con un factor $\frac{\alpha - \beta}{\beta}$ grande sin involucrar muchos primos.

3.4. Implementación

Dado un esquema de Mignotte generalizado basado en una sucesión (k, n) de Mignotte generalizada y conocidos los correspondientes α, β, el proceso para recuperar la informa-

ción conociendo k parejas involucra los siguientes cálculos.

- Dados $(I_{i_1}, m_{i_k}), \ldots, (I_{i_k}, m_{i_k})$, usamos el algoritmo de Euclides para hallar $(m_{i_1}, m_{i_2}) = d_2$ obteniendo $d_2 = m_{i_1}s_1 + m_{i_2}r_1$, hallamos $M_2 = [m_{i_1}, m_{i_2}] = \dfrac{m_{i_1} \cdot m_{i_2}}{d_2}$.Entonces $c_2 = s_1\dfrac{I_{i_1} - I_{i_2}}{d_2}$ es solución de la congruencia

$$m_{i_2}x \equiv I_{i_1} - I_{i_2} \pmod{m_{i_1}}.$$

  y $b_2 = m_{i_2} \cdot c_2 + I_{i_2}$ módulo M_2 es la solución a las primeras dos congruencias.

- Calculamos $d_3 = (m_{i_3}, M_2) = (m_{i_3}, [m_{i_1}, m_{i_2}])$ obteniendo $d_3 = m_{i_3}s_2 + M_2r_2$, y $M_3 = [m_{i_1}, m_{i_2}, m_{i_3}] = [[m_{i_1}, m_{i_2}], m_{i_3}] = [M_2, m_{i_3}] = \dfrac{M_2 \cdot m_{i_3}}{d_3}$. Entonces $c_3 = s_2\dfrac{b_2 - I_{i_3}}{d_3}$ es solución de la congruencia

$$m_{i_3}x \equiv b_2 - I_{i_3} \pmod{M_2},$$

  y $b_3 = m_{i_3} \cdot c_3 + I_{i_3}$ solución de las primeras tres congruencias módulo M_3.

- En general en el paso t-ésimo hacemos $d_{t+1} = (m_{i_{t+1}}, M_t)$ con $d_{t+1} = m_{i_{t+1}}s_t + M_tr_t$ y

$$\begin{aligned} M_{t+1} &= [m_{i_1}, \ldots, m_{i_{t+1}}] = [[m_{i_1}, \ldots, m_{i_t}], m_{i_{t+1}}] \\ &= [M_t, m_{i_{t+1}}] = \frac{m_{i_{t+1}} \cdot M_t}{d_{t+1}}. \end{aligned}$$

  Entonces $c_{t+1} = s_t\dfrac{b_t - I_{i_{t+1}}}{d_{t+1}}$ es solución de la congruencia

$$m_{i_{t+1}}x \equiv b_t - I_{i_{t+1}} \pmod{M_t},$$

y $b_{t+1} = m_{i_{t+1}} \cdot c_{t+1} + I_{i_{t+1}}$ es la solución de las primeras $t+1$ congruencias módulo M_{t+1}.

En $k-1$ pasos encontramos la solución del sistema de k congruencias, módulo
$M_k = [M_{k-1}, m_{i_k}] = [m_{i_1}, \ldots, m_{i_k}]$.
Veamos como funciona la implementación del esquema con un ejemplo.

Ejemplo.

- Los números $17, 18, 19, 20, 21$ conforman una sucesión $(3, 5)$ de Mignotte generalizada, con $\alpha = 1260$ y $\beta = 420$. Sea $S = 737$ el secreto que ocultaremos, obtenemos las parejas

$$(6, 17), (17, 18), (15, 19), (17, 20), (2, 21).$$

Supongamos que conocemos 3 parejas $(17, 18), (17, 20), (2, 21)$, establecemos el sistema de congruencias:

$$\begin{aligned} x &\equiv 6 \pmod{17}, \\ x &\equiv 17 \pmod{20}, \\ x &\equiv 2 \pmod{21}. \end{aligned}$$

Siguiendo el proceso descrito en la implementación:
Encontramos $(18, 20) = 2 = 20 - 18$ y $[18, 20] = 180$, entonces $s_1 = 1$
y $c_2 = \dfrac{17 - 17}{2} 1 = 0$ y la solución a las dos primeras congruencias es $b_2 = 20(0) + 17 = 17 \pmod{340}$ quien es solución de las primeras dos congruencias.

Ahora encontramos $(180, 21) = 3 = 180(2) + 21(-17)$ y $[18, 20, 21] = 1260$, así $s_2 = -17$ y $c_3 = \frac{47-2}{3}(-17) = -255 \equiv 1005 \pmod{1260}$ y entonces $b_3 = 21(1005) + 2 = 21107 \equiv 947 \pmod{1260}$ quien es solución del sistema de 3 congruencias.

Comentarios Finales

- El Teorema Chino de los Residuos es una herramienta antigua y relativamente sencilla en la cual se tiene acceso en el curso de teoría de números. Sin embargo, fue esta herramienta la principal motivación de este trabajo por su conexión con un problema de criptografía. Esto es un indicador de que problemas muy interesantes y de actualidad pueden estar apoyados en conceptos relativamente elementales.

- Al presentar los esquemas de umbral para compartir un secreto, se espera motivar el estudio de los mismos en la Universidad, invitando a profundizar en la descripción de alguno de ellos en particular el esquema de Blakley.

- Una mejora a la seguridad en los esquemas de Mignotte y su generalización se puede obtener si las correspondientes sucesiones no son públicas, pues no existe forma de acotar el intervalo de búsqueda.

- La construcción de sucesiones (k, n) de Mignotte generalizadas es por si mismo un problema que puede motivar a futuros trabajos de grado de la Universidad o iniciar algún proyecto de investigación.

Bibliografía

[1] Acedo, A, A. Molina, M, A. Silvia, R. Marciano, M. y Portilla, E, A. *Análisis de los Secretos Compartidos para la Autenticación de nodos en las Wireless Sensor Networks mediante el algoritmo de Shamir*. Ciencia e Ingeniería Neogranadina, Vol. 18, Núm. 2, Diciembre. Universidad Militar de Nueva Granada. 2008.

[2] Asmuth, C, A. Bloom, J. *A modular approach to key safeguarding*. IEEE Transactions on Information Theory 2. 1982

[3] Blakley, G, R. *Safeguarding cryptographic keys*. Texas A&M University. Texas. 1979.

[4] Donovan, D. *Some Interesting Constructions for Secret Sharing Scheme*. The University of Queensland. 1994.

[5] Iftene, S. *A generalization of Mignotte's secret sharing scheme*. "Al. I. Cuza"& University. Rumania. 2004.

[6] Iftene, S. *Compartmented Secret Sharing Based on the Chinese Remainder Theorem*. "Al. I. Cuza"& University. Rumania. 2005.

[7] Iftene, S. Ciobâcă, S. Grindei, M. *Compartmented Threshold RSA based on the Chinese Remainder Theorem*. "Al. I. Cuza"& University. Rumania. 2008.

[8] Iftene, S. *Secret Sharing Scheme whit Aplications in Security Protocols*. "Al. I. Cuza"& University. Rumania. 2007. (Tesis de doctorado.)

[9] Iftene, S. Florin, Ch. *The General Chinese Remainder Theorem*. "Al. I. Cuza"& University. Rumania. 2007.

[10] Kranakis, E. *Primality and Cryptography*. Wiley-Teubner Series in Computer Science. pp 7-10. 1987.

[11] Mignotte, M. *How to share a secret*. Université Louis Pasteur. Strasbourg. 1983.

[12] Moreno, B, L. Garay, C, E. *Las Matemáticas en la Seguridad de la Información*. I Congreso Nacional de Investgación Estudiantil del IPN. Instituto Politécnico Nacional. Ciudad de Mexico. 2005.

[13] Morillo, P. *Las Matemáticas en la Criptologia*. Encuentros Multidisciplinares Vol. 8, Nro. 23, Mayo-Agosto. 2006

[14] Bozkurt, N, I. Kayo, K. Selçuk, A, A. Güloğlu, A, M. *Threshold Cryptography Based on Blakley Secret Sharing*. Bilkent University. Ankara. Turquia. 2008.

[15] Ore, O. *The General Chinese Remainder Theorem*. The American Mathematical Monthly, Vol. 59, Nor. 6. 1952.

[16] Shamir, A. *How to share a secret*. Institute of Thecnology. Masachussetts. 1979.

[17] Villar, J. Pradó, C. Sáez, G. *Compartición de Secretos en Criptografía*. Revisa IEEE Buran, Nro. 10 Diciembre 1997.