Universidad de Valladolid

Facultad de Ciencias

Trabajo Fin de Grado

Grado en Matemáticas

Reparto de secretos con el Teorema Chino de los restos

Autor: Diego Munuera Merayo

Tutor: Prof. Antonio Campillo López

Indice

0

Presentación

0.1. El tema de esta memoria

La tendencia hacia la digitalización es seguramente el fenómeno más relevante del mundo actual, tanto desde un punto de vista social como económico y tecnológico. Esta tendencia se ha convertido en un fenómeno global imparable que ha transformado la sociedad y la economía. Ahora bien, con la digitalización también han aparecido un creciente número de situaciones nuevas, y con ellas nuevos riesgos y amenazas. Por ello se ha hecho imprescindible el desarrollar métodos que garanticen la seguridad de los ciudadanos y las empresas en sus relaciones a través de medios electrónicos.

Las técnicas y los mecanismos más importantes en la lucha por la seguridad de la información proceden de las matemáticas, y se articulan en nuevos campos de trabajo e investigación como son la Teoría de la Información, la Criptografía o la Teoría de Códigos correctores. Resulta llamativo que muchos de los desarrollos más novedosos en estos campos y en sus aplicaciones, tienen sus bases sobre de algunos de los resultados más clásicos y venerables de las matematicas, y más en concreto de la aritmética. Los conceptos de número primo y factorización, el algoritmo de Euclides o el teorema Chino de los restos, son ejemplos significativos de resultados clásicos de los que dependen los más modernos sistemas de proteccion de datos (comercio y votaciones electrónicas, firma digital) y están incorporados en una tarjeta electrónica o en el flujo de datos por internet.

En esta memoria nos centramos en una de las técnicas de proteción de datos con mayor relevancia práctica: los esquemas para repartir secretos. Un esquema para repartir secretos es un método por el que un secreto numérico es repartido entre un conjunto de participantes, de manera que ciertas coaliciones de participantes -previamente determinadas- puedan recuperarlo, mientras que para las coliciones no autorizadas resulte imposible hacerlo. El origen de estos esquemas está, como puede imaginarse, en la gestión de claves, pero sus aplicaciones actuales han desbordado con mucho esta aplicacion inicial y hoy en día los ERS son herramientas básicas en areas como las votaciones electrónicas, la computación multiparte y la criptografía corporativa (cada vez mas y más importante esta última).

El problema del reparto de secretos fue planteado por primera vez por A. Shamir en su artículo [28] de 1979. A raíz de la publicación de este trabajo fueron propuestos rápidamente cuatro métodos para llevarlo a cabo: uno por el propio Shamir, basado en la interpolación polinómica. Otro por G. Blakley [3], que utiliza la geometría proyectiva. Y los dos últimos, por M, Mignotte [23], y C.A. Asmuth y J. Bloom [1], basados ambos en el teorema Chino de los restos. Los cuatro métodos permiten fabricar esquemas del tipo llamado *umbral*, lo que significa que las coaliciones autorizadas para recuperar el secreto

son las que contienen en un número mínimo de participantes (el umbral).

0.2. Contenidos y estructura

El propósito de esta memoria es el estudio de los esquemas de reparto de secretos basados en teorema Chino de los restos, es decir, de los inicialmente propuestos por Mignote y Asmuth-Bloom, y asimismo de las modificaciones y ampliaciones que de ellos han ido derivandose con el tiempo. Hemos realizado un tratamiento unificado de esta teoría, recopilando las principales aportaciones realizadas en esta línea a través de artículos publicados por distintos autores.

Como ya hemos repetido, el origen de estos esquemas se encuentra en los trabajos de M. Mignotte [23] de 1982, y C. A. Asmuth y J. Bloom [1] de 1983. En estos trabajos se muestra como el teorema Chino de los restos puede ser utilizado para obtener esquemas que realizan estructuras umbrales a partir de secuencias de enteros coprimos (que serán los módulos en el sistema de ecuaciones en congruencias sobre el que se aplique el teorema Chino de los restos).

Posteriormente, en su tesis doctoral [14], S. Iftene propone una generalización del método de Mignotte, en la cuál que admite módulos no sean coprimos entre sí. De este modo se aumenta considerablemente la cantidad de estructuras de acceso que pueden realizarse. En particular, se sugiere un método de realización de las estructuras umbral ponderadas. Un estudio similar es realizado por K. Kaya en [19] para el método de Asmuth-Bloom. Hagamos notar que ambos autores provienen del mundo de las ciencias de la computación, y (aparentemente más interesados en desarrollar aplicaciones que en fundamentarlas) sus análisis matemáticos no son tan cuidadosos como sería deseable. Así, una parte de nuestro trabajo ha sido justificar de un modo riguroso la validez de sus sugerencias.

Aunque, en su formulación original, ambos tipos de están definidos sobre $\mathbb{Z}$, el teorema Chino de los restos puede establecerse también sobre $\mathbb{K}[X]$ siendo $\mathbb{K}$ un cuerpo. Una extensión del esquema de Mignotte a $\mathbb{F}_q[X]$ fue propuesta por T. Galibus y G. Matveev en [10]. En este trabajo se demuestra la importante propiedad de que toda estructura de acceso puede ser realizada por un esquema de Mignotte polinómico. El caso polinómico del esquema de Asmuth-Bloom fue tratado por Y. Ning, F. Miao, W. Huang, K. Meng, Y. Xiong y X. Wang en el artículo [24]. En particular, aquí se muestra que el esquema umbral de Shamir (sin duda el más conocido y utilizado) es en realidad un caso particular del de Asmuth-Bloom sobre $\mathbb{F}_q[X]$.

Para desarrollar estos contenidos hemos estructurado la memoria en 4 capítulos (más este preliminar).

El Capítulo 1 contiene una introducción general a la criptografía, con la que pretendemos encuadrar los esquemas para repartir secretos en el marco global de la criptografía de clave pública (y esta dentro de la criptografía en general), poniendo de manifiesto su papel e interés. También se hace un pequeño repaso de la teoría de los esquemas de reparto, poniendo de relieve en qué consisten y cuales son los pricipales puntos de interés a tener en cuenta en su estudio.

El Capítulo 2 está dedicado al teorema Chino de los restos, principal herramienta matemática usada a lo largo de la memoria. Exponemos distintas versiones del teorema, alguna de las cuales serán utilizadas en los desarrollos posteriores, y otras se incluyen para hacer más completo en tratamiento. También es tratado brevemente el algortimo de Euclides, fundamental para saber si dos enteros son coprimos, y para encontrar una solución explícita de un sistema de ecuaciones en congruencias.

El núcleo central de la memoria se encuentra en los capítulos 3 y 4, que son los dedicados al estudio de los esquemas de Mignotte y Asmuth-Bloom.

El Capítulo 3 trata el caso de los esquemas construidos sobre los enteros. Comenzamos en la Sección 3.1 describiendo el esquema de Mignotte original, basado en módulos coprimos, para, a continuación, describir la generalización de Iftene para módulos cualquiera. El caso de Asmuth-Bloom es tratado en la Sección 3.2. Una variación de este esquema, debida a K. Kaya, permite que los esquemas obtenidos estén cerca de ser perfectos. En esta sección también estudiamos esta variación. La Sección 3.3 está dedicada a las estructuras ponderadas. Siguiendo una sugerencia de Iftene demostramos con detalle como cualquier estructura umbral ponderada puede realizarse mediante un esquema de Mignotte. Finalmente, en la Sección 3.4 damos un paso más en esta línea, estudiando como los esquemas de Mignotte pueden ser aplicados a las estructuras de acceso generales (es decir, no necesariamente umbrales). El principal resultado en este sentido será establecido en el Capítulo 4. Por el momento mostramos un caso relevante: toda estructura ponderada es realizada por un esquema de Mignotte con módulos coprimos.

El Capítulo 4, y último, está dedicado a los esquemas de reparto sobre $\mathbb{F}_q[X]$ siendo $\mathbb{F}_q$ un cuerpo finito con q elementos. El papel de los número primos en $\mathbb{Z}$ lo juegan ahora los polinomios irreducibles. Así comenzamos estudiando la existencia y número de polinomios irreducibles sobre un cuerpo finito. La teoría de los esquemas polinómicos de Mignotte se desarrolla en la Sección 4.2. Esta sección contiene también el importante resultado, demostrado en [10], de que toda estructura de acceso puede ser realizada mediante un esquema polinómico de Mignotte. En la Sección 4.3 volvemos sobre un tema que quedó pendiente en el capítulo anterior, dedicado a los esquemas de reparto sobre los enteros. Como consecuencia de toda la teoría desarrollada, hemos podido establecer el Teorema 4.3.1 (que consideramos la aportación más interesante de esta memoria) y que parece ser desconocido en la literatura. El capítulo finaliza con la Sección 4.4. dedicada a los esquemas polinómicos de Asmuth-Bloom. Para no ser reiterativos, nos limitamos a tratar los esquemas umbral. Hemos incluido, eso sí, la demostración del llamativo hecho de que los esquemas de Shamir son un caso particular de los de Asmuth-Bloom polinómicos.

En cada caso, la teoría desarrollada se ilustra mediante ejemplos que hemos elaborado con el programa MAPLE.

0.3. Aportaciones personales

Las aportaciones principales que contiene este trabajo pueden clasificarse en dos tipos.

(a) Una exposición sistemática y rigurosa de los contenidos. Esta memoria trata de forma unificada y matemáticamente rigurosa una teoría que hasta el presente se encontraba dispersa en diversos artículos y documentos científicos (a veces con distinto lenguaje y distintas notaciones). Incluso, como se ha dicho, en ocasiones con un tratamiento matemático hecho estos documentos no muy cuidadoso.

(b) Algunas nuevas aportaciones a la teoría, que a su vez podemos clasificar en dos tipos: **(b1)** análisis y pequeñas aportaciones sobre resultados ya conocidos; y **(b2)** resultados novedosos. Respecto de los primeros, al tiempo que se desarrolla la teoría, hemos ido realizando pequeños análisis, aportaciones y sugerencias sobre los elementos que contiene. En este sentido, podemos citar los del Capítulo 3 en la subsección 3.1.3. respecto de las secuencias de Mignotte, o la subsección 3.3.2. en la que se estudian las estructuras umbral ponderadas de Mignotte.

En cuanto a los resultados teóricos novedosos que hemos obtenido, estos se centran en el problema de la realización de una estructura de acceso arbitraria mediante un esquema de Mignotte (sobre los enteros). En el Capítulo 3 hemos caracterizado las estructuras de acceso obtenidas mediante módulos coprimos, demostrando el siguiente resultado.

Proposición 3.4.3 *Sea $\mathscr{A}$ la estructura de acceso realizada mediante el esquema de Mignotte $\mathscr{R}$ con secuencia de módulos $\mathbf{m} : m_1, \ldots, m_n$ y espacio de secretos $\mathscr{S} = \{z \in \mathbb{Z} \mid \mathbf{m}^+ \leq s \leq \mathbf{m}^-\}$. Si los $m_1, \ldots, m_n$ son coprimos dos a dos, entonces $\mathscr{A}$ es una estructura umbral ponderada, con pesos reales.*

Hagamos notar que el problema de caracterizar las estructuras de acceso realizadas mediante módulos coprimos fue estudiado en [11], donde se obtiene un resultado más pobre que el nuestro. Siguiedo en la misma línea, en el Capítulo 4 dedicado a los esquemas polinómicos, observamos que la demostración de que toda estructura de acceso se realiza mediante un esquema polinómico de Mignotte [10], es también válida sobre $\mathbb{Z}$. Llegamos así a la más importante de nuestras aportaciones en esta memoria.

Teorema 4.3.1. *Toda estructura de acceso $\mathscr{A}$ puede ser realizada por un esquema de Mignotte $\mathscr{R}$ sobre $\mathbb{Z}$ basado en una secuencia de módulos enteros $\mathbf{m}$. Además, si los módulos que aparecen en $\mathbf{m}$ son coprimos entonces la estructura de acceso es umbral ponderada.*

1

Criptografía y el reparto de secretos

1.1. Sistemas criptográficos

La criptografía es la ciencia que estudia el intercambio seguro de información a través de canales inseguros. Esto se consigue poniendo de acuerdo a diversos usuarios sobre una método de cifrado que depende de una clave, la cuál puede cambiarse en cada transmisión. Cabe notar que para esto ha tenido que haber una comunicación (segura) previa.

Formalmente, la definición de criptosistema es la siguiente: [31].

Definición 1.1.1. Un *sistema criptográfico* (o *criptosistema*) es una terna $(\mathfrak{M}, \mathfrak{C}, \mathfrak{K})$, donde:

$\mathfrak{M}$ es el conjunto de mensajes originales;
$\mathfrak{C}$ es un conjunto de mensajes cifrados;
$\mathfrak{K}$ es un conjunto de *claves*;
junto con dos funciones de cifrado y descifrado:

$$c : \mathfrak{M} \times \mathfrak{K} \longrightarrow \mathfrak{C} \ , \ d : \mathfrak{C} \times \mathfrak{K} \longrightarrow \mathfrak{M}$$

tales que para todos $\mathbf{m} \in \mathfrak{M}$ y $\mathbf{c} \in \mathfrak{K}$, existe $\mathbf{d} \in \mathfrak{K}$ verificando $d(c(\mathbf{m}, \mathbf{c}), \mathbf{d}) = \mathbf{m}$.

Los mensajes originales $\mathbf{m} \in \mathfrak{M}$ suelen llamarse *mensajes en claro*. Elegida una *clave de encriptado* $\mathbf{c} \in \mathfrak{K}$, un mensaje en claro $\mathbf{m}$ se cifra mediante la función de cifrado c, dando lugar con esto al *mensaje cifrado* (o *encriptado*) $\mathbf{e} = c(\mathbf{m}, \mathbf{c})$. Un receptor legítimo conoce la clave de descifrado $\mathbf{d}$ correspondiente a la clave de cifrado $\mathbf{c}$ y recupera el mensaje original $\mathbf{m}$ a partir del mensaje cifrado $\mathbf{e}$ y la función de descifrado, como $\mathbf{m} = d(\mathbf{e}, \mathbf{d})$.

1.1.1. Un ejemplo: el código de César

Tomamos como mensajes en claro el conjunto de secuencias de letras del idioma utilizado. Las claves serán los enteros entre 0 y 26 (en el caso del idioma castellano y sin tener en cuenta espacios). El cifrado de un mensaje se hace letra a letra, desplazándola hacia adelante tantas posiciones como indica la clave. El descifrado consistirá en desplazar las letras ese mismo número de posiciones hacia atrás. Por ejemplo, el cifrado del mensaje en claro *IBM* con la clave 26 es *HAL*.[1] Si bien el sistema puede considerarse optimista,

[1] *2001. Una odisea en el espacio.*

ha sido utilizado a lo largo de la historia hasta fechas tan recientes como la guerra civil de los EE.UU.

Este método admite una interpretación simple en términos matemáticos: podemos identificar el conjunto de letras en castellano con $\mathbb{Z}/(27)$. Dada una clave de cifrado $\mathbf{c}$, la clave de descifrado es $\mathbf{d} = -\mathbf{c}(mod 27)$, y la operación de encriptado $c(\mathbf{m}, \mathbf{c}) = \mathbf{m} + \mathbf{c}(mod 27)$.

Una consecuencia inmediata de este ejemplo es que el espacio de claves debe ser suficientemente grande. Si no fuese así, un enemigo podría tratar de descifrar los mensajes simplemente probando todas las claves posibles. Esta estrategia se conoce como *ataque por fuerza bruta*.

El nombre del cifrado responde a que fue utilizado asiduamente por Julio César[2]. Se dice, además, que César utilizaba habitualmente la clave 3.

1.1.2. Un poco de historia

Como hemos querido ilustrar en el ejemplo anterior, ya desde la antigüedad existía la necesidad de comunicar mensajes de forma privada y secreta. La mayor parte del los sistemas criptográficos de la historia, más o menos ingeniosos, se han basado en la sustitución alfabética y han tenido como prototipo al de César. Esta tendencia ha pervivido hasta épocas más o menos recientes, como fue el caso de la máquina *Enigma*. Anectodtas a parte, estos métodos evidencian una tendencia a la búsqueda de sistemas criptográficos indescifrables. Tendencia que se ha visto superada por el inventivo humano en todas las ocasiones. En estas circunstancias surgen sistemas basados, no ya, en la imposibilidad sino que más bien en la dificulatad computacional de desencriptar el mensaje. La idea pasa a ser que la información no pueda obtenerse en un tiempo razonable, abandonando la idea de que no pueda obtenerse de ninguna forma.

En este contexto encontramos dos fechas fundamentales que marcan el camino hacia la criptografía actual. La primera es el año 1883 en que A. Kerchoffs publicó su trabajo [21]. Tras los fracasos sucesivos y sistemáticos de varios 'cifrados indescifrables' cada vez más sofisticados, se hizo evidente la necesidad de organizar la criptografía en torno a unas reglas rigurosas. Estas reglas son los llamados *principios de Kerchoffs*. En lenguaje actual, estos principios esencialmente corresponden a la definición de sistema criptográfico, añadidas las condiciones:

(1) El sistema debe ser prácticamente, si no matemáticamente, indescrifrable sin el conocimiento de la clave de descifrado.
(2) El sistema debe ser público y no debe suponer un problema que se conozca su modo de funcionamiento.
(3) Debe ser posible almacenar las claves de forma segura, y los usuarios deben poder modificar las claves a su gusto.
(4) La información cifrada debe ser fácilmente transmisible.
(5) El descifrado y el cifrado deben ser sencillos y realizables en unos pocos pasos.

A partir de estos trabajos, durante el siglo XX la teoría tuvo un gran avance. Formalizándose en torno a las matemáticas precedentes, y sustituyendo la idea de *cifrado*

[2]Citado por Suetonio y por el propio César en *De bello Gallico*

indescifrable por la de *sistema computacionalmente seguro*. En vez de buscarse un sistema imposible de romper se pasa a buscar un sistema imposible de romper en un tiempo razonable. Otra característica, a posteriori determinante de esta época, es la extensión del uso de técnicas criptográficas en sectores cada vez mayores de la sociedad. En efecto, hasta fechas relativamente recientes el uso de la criptografía era esencialmente gubernamental y militar. A partir de la segunda mitad del siglo XX se difunde su empleo en el mundo industrial y financiero. Convirtiéndose en un tema común en protección de datos personales, controles de acceso, tarjetas de crédito, comercio electrónico, firma digital, etc...

Los sistemas clásicos de intercambio de información, hoy llamados *simétricos* o *de clave privada*, estaban pensados para transmitir información entre pocos participantes, con lo que resultan inadecuados para las necesidades modernas. De esta forma se produjo la aparición de nuevos sistemas, llamados *asimétricos* o *de clave pública*. El nacimiento de estos puede fecharse en 1976, cuando W. Diffie y M. Hellman publicaron [7].

1.2. Sistemas de clave pública

Como acabamos de señalar, los sistemas criptográficos modernos se distinguen en sistemas de clave privada y de clave pública. Pasamos ahora a exponer esta distinción con mayor detalle:

1.2.1. Clave privada y clave pública

La diferencia esencial entre ambos tipos se basa en que, en los sistemas de clave privada, existe un número pequeño de usuarios, idealmente dos, y todos ellos tienen un papel simétrico. En efecto, las funciones de cifrado y descifrado c y d, son inversas entre sí, y, por lo general, el conocimiento de una de ellas permite fácilmente el cálculo de la otra.

Ahora bien, este esquema resulta inmanejable cuando el número de usuarios es grande, precisamente por los problemas de gestión de claves que acarrea: es necesario un par de claves por cada dos usuarios del sistema. Surge entonces la idea de clave pública, [27], en la que cada usuario i del sistema posee únicamente un par de claves $(\mathbf{c}_i, \mathbf{d}_i)$. La primera de ellas, $\mathbf{c}_i$, es de conocimiento público (dígase, conocida por todos usuarios del sistema), y será la empleada por cualquier otro usuario j que desee transmitir un mensaje $\mathbf{m}$ a i. Para ello j cifra el mensaje $\mathbf{m}$ como $\mathbf{e} = c(\mathbf{m}, \mathbf{c}_i)$. Por el contrario, la clave *privada* de i $\mathbf{d}_i$ es conocida únicamente por él mismo, quién la emplea para recuperar cualquiera de los mensajes cifrados que le llegan, $\mathbf{m} = d(\mathbf{e}, \mathbf{d}_i)$.

1.2.2. Condiciones de Diffie-Hellman

Para que un criptosistema de clave pública funcione de manera correcta y operativa, debe cumplir una serie de condiciones. Estas condiciones fueron enunciadas por Diffie y Hellman en [7].

(1) Para todo mensaje $\mathbf{m}$, debe verificarse que $d(c(\mathbf{m}, \mathbf{c}_i), \mathbf{d}_i) = \mathbf{m}$.
(2) Las operaciones de cifrado $c(\mathbf{m}, \mathbf{c}_i)$ y descifrado $d(\mathbf{e}, \mathbf{d}_i)$ deben ser fácilmente calcu-

lables para cualquier **m** **m**.
(3) Para casi todo mensaje **m**, hallar un equivalente a $\mathbf{d}_i$ o descifrar un mensaje encriptado **e** a partir de **e** y $\mathbf{c}_i$ debe ser computacionalmente intratable.
(4) Debe ser computacionalmente factible determinar cada par de claves $(\mathbf{c}_i, \mathbf{d}_i)$.

Nótese que, puesto que $\mathbf{c}_i$ y $\mathbf{d}_i$ son inversas , para cumplir las condiciones (3) y (4) es preciso que $\mathbf{c}_i$ se obtenga mediante algún procedimiento conocido, pero computacionalmente imposible de invertir sin el conocimiento de una cierta informacion complementaria, la cuál sólo posee i.
En este contexto introducimos la siguiente definición:

Definición 1.2.1. Una función $f : X \to Y$ es *de una vía* si para $x \in X$ es computacionalmente sencillo calcular $y = f(x)$ pero computacionalmente intratable calcular $f^{-1}(y)$.

Los procesos de una vía más utilizados en los sistemas criptográficos actuales surgen de la de teoría de números. Podemos nombrar, por ejemplo, la dificultad de encontrar la factorización prima de un entero (frente a la facilidad de multiplicar), utilizado en el sistema RSA por medio de la función ϕ de Euler para un entero producto de dos primos, o la dificultad de encontrar el logaritmo discreto en un grupo finito (frente a la facilidad de la exponenciación), utilizado en el sistema El Gamal.

1.2.3. Firma digital

Atendiendo a sus usos prácticos, la *firma digital*, es una de las aplicaciones más importantes de la criptografía de clave pública. Podríamos entender la firma digital como una análogo electrónico de la firma ordinaria (incluso tiene el mismo valor legal). No entraremos en detalle sobre ella, pero expondremos aquí algunas de sus bases.

El proceso por el que se realiza es el siguiente: un usuario i desea firmar un documento **m**. Para ello cifra **m** con su clave privada $\mathbf{e} = d(\mathbf{m}, \mathbf{d}_i)$. El documento firmado es el par $(\mathbf{m}, \mathbf{e})$, y la identidad de i queda probada porque conoce la clave $\mathbf{d}_i$, cosa que nadie más que él puede hacer. Un usuario j desea comprobar la validez de la firma. Para ello cifra **e** con la clave pública de i, obteniendo $\mathbf{m}' = c(\mathbf{e}, \mathbf{c}_i)$ y compara $\mathbf{m}'$ y **m**. Si el criptosistema elegido verifica que los procesos de cifrado y descifrado son inversos, entonces ambos mensajes coinciden, $\mathbf{m}' = \mathbf{m}$, y la firma es correcta.

Obsérvese que la firma digital asegura no sólo la identidad del firmante, sino también la integridad del mensaje firmado.

1.2.4. Criptografía corporativa

Hasta este momento hemos supuesto que los participantes en la red criptográfica son personas (o entes) individuales. Sin embargo, en la práctica cobran cada vez más importancia los participantes *corporativos*: grupos, asociaciones o empresas formadas por varias personas. Esto da lugar a nuevos retos para la criptografía: ¿cómo gestionar una clave de acceso, descifrar una información sensible o firmar un documento de manera corporativa? La respuesta a estos problemas son los esquemas de reparto de secretos.

1.3. El reparto de secretos

El origen del estudio del reparto de secretos suele fecharse en 1979, año en que A. Shamir publicó su artículo [28]. En este trabajo se propone el siguiente problema combinatorio.

> Once cientíIficos trabajan en un proyecto. Desean mantener los documentos de su trabajo guardados en un armario que pueda abrirse sólo cuando al menos la mitad de ellos esté presente. Para ello han ideado hacer copias de la llave del armario, que se guardadan en cajas cerradas con candados, cada una de las cuales se abre con seis llaves concretas. ¿Cuál es el mínimo número de cajas necesario para ello?, ¿cuál es el mínimo número de llaves que cada científico debe llevar con él para que el sistema funcione?

La respuesta al problema es tan simple como descorazonadora: son precisas $\binom{11}{6} = 462$ cajas y cada científico debe llevar encima $\binom{10}{5} = 252$ llaves.

Esta situación puede generalizarse a casos más cotidianos, justificándose así que hoy en día los llamados *esquemas de reparto de secretos* sean un campo activo de investigación. Más allá de sus utilidades obvias (gestión de claves y similares), estos esquemas juegan un papel relevante en temas como votaciones electrónicas. En capítulos posteriores de este trabajo nos centraremos en los esquemas de reparto de secretos obtenidos por aplicación del teorema chino de los restos.

1.3.1. Esquemas para repartir secretos

Pasamos ahora a explicar más formalmente en qué consiste un esquema de reparto de secretos. Sean $\mathscr{P} = \{1, \ldots, n\}$ un conjunto de *participantes* y $\mathscr{S}$ un conjunto numérico finito y no vacío cualquiera, al que llamaremos *conjunto de secretos*. Se desea repatir un secreto $s \in \mathscr{S}$ entre los participantes. Para ello, cada participante recibirá un dato s_i sobre el secreto: su *participación*. Un gestor computa los $s_1, \ldots, s_n$ a partir de s y pone en conocimiento de cada i su participación s_i. Un *esquema de reparto de secretos* es un método $\mathscr{R}$ de calcular las participaciones s_i de manera que

• ciertas agrupaciones de participantes, previamente determinadas, puedan, al unir las participaciones de sus miembros, recuperar s; y que además esto pueda hacerse de manera computacionalmente eficiente;

• para cualquier otra coalición de participantes distinta de las anteriores, la información proporcionada por las participaciones de sus miembros no permita determinar el secreto.

El conjunto de agrupaciones autorizadas para recuperar el secreto es la *estructura de acceso* del esquema, que denotaremos por $\mathscr{A}$. Naturalmente, $\mathscr{A}$ es un conjunto monótono, es decir, si $A \subset A'$ y $A \in \mathscr{A}$, entonces también $A' \in \mathscr{A}$.

Diremos que un esquema de reparto es *débilmente perfecto* si para cada coalición $B \notin \mathscr{A}$, en base a la información conjunta de los participantes de B no puede descartar ningún $s \in \mathscr{S}$ como posible secreto repartido. Algunos autores consideran una definición

aún más restrictiva de esquema perfecto, exigiendo además que, en base a la información conjunta de los participantes de una coalición no autorizada B, todos los elementos $s \in \mathscr{S}$ sean igualmente probables como candidatos a ser el secreto repartido. Nosotros referiremos a esta condicion como *fuertemente perfecto*.

Uno de los problemas importantes en la teoría de esquemas para repartir secretos es el de la realizabilidad: dada una estructura de acceso $\mathscr{A}$ ¿existe algún esquema que la realice? (esto es, que la tenga efectivamente como estructura de acceso). Este es un problema relevante desde el punto de vista de las aplicaciones prácticas puesto que, en situaciones concretas, habitualmente se parte de una estructura de acceso preexistente y determinada por la situación a la que pretende aplicarse, y a continuación se busca un esquema que la realice. La respuesta a esta pregunta es afirmativa, como probaron Ito, Saito y Nishizeki [18], mediante un método constructivo basado en la lógica booleana, que fue poseriormente mejorado por Benaloh y Leichter [2], y por Harn *et alii* [13].

Estos resultados, sin embargo, no completan el estudio de la teoría, ya que en un sistema $\mathscr{R}$ también nos preocupa el tamaño de las participaciones s_i asignadas a los participantes. Denotemos por $\mathscr{S}_i$ el conjunto de todos los valores posibles que puede tomar s_i cuando s recorre $\mathscr{S}$. Decimos que i es *redundante* si no pertenece a ninguna coalición autorizada minimal, es decir, si para cualquier coalición autorizada A a la que i pertenezca, se tiene que $A \setminus \{i\}$ es también autorizada.

Proposición 1.3.1. *Si $\mathscr{R}$ es perfecto, entonces para todo participante no redundante i se verifica que $|\mathscr{S}_i| \geq |\mathscr{S}|$.*

Demostración. Sea A una coalición autorizada minimal que contiene a i, y sea $B = A \setminus \{i\}$ (que no esta autorizada). Para un cierto secreto $s^* \in \mathscr{S}$ sean $(s_j)_{j \in B}$ las correspondientes participaciones de los elementos de B. Por ser $\mathscr{R}$ perfecto, todo secreto es compatible con las $(s_j)_{j \in B}$, luego para cada $s \in \mathscr{S}$ existe $s_i(s) \in \mathscr{S}_i$ tal que las participaciones $((s_j)_{j \in B}, s_i(s))$ determinan s. Por tanto $|\mathscr{S}| \leq |\mathscr{S}_i|$. □

Decimos que un esquema de reparto $\mathscr{R}$ es *ideal* si el tamaño de las participaciones es similar tamaño del secreto repartido. De forma más precisa se define la *tasa de información* de i como $\rho_i = \log(|\mathscr{S}|)/\log(|\mathscr{S}_i|)$ (que es independiente de la base de logaritmos elegida), y la tasa de información de $\mathscr{R}$, que denotamos $\rho(\mathscr{R})$, como el mínimo de estos números sobre todos los participantes. Formalmente, el esquema de reparto $\mathscr{R}$ es ideal si $\rho(\mathscr{R}) = 1$.

1.3.2. Esquemas umbral

Una estructura de acceso $\mathscr{A}$ sobre n participantes es llamada *umbral* si existe un entero t (el umbral) de manera que las coaliciones autorizadas $A \in \mathscr{A}$ sean exáctamente los subconjuntos de $\mathscr{P}$ con al menos t participantes. En tal caso decimos que $\mathscr{A}$ es una estructura de tipo (t,n). Son estas las estructuras más simples y a las que primeramente nos dedicaremos en los próximos capítulos.

Los casos límite de las estructuras umbral $(1,n)$ y (n,n) admiten esquemas muy simples y no necesitan ningún estudio posterior. En efecto, en ambos casos podemos tomar $\mathscr{S} = \mathbb{Z}/m\mathbb{Z}$. Si $s \in \mathscr{S}$, un esquema umbral $(1,n)$ se obtiene con las participaciones

$s_i = s$. Un esquema umbral (n,n) se obtiene con participaciones que satisfagan $s_1 + \cdots + s_n = s \pmod m$ (por ejemplo, si $s_1, \ldots, s_{n-1}$ basta con tomar al azar en $\mathbb{Z}/m\mathbb{Z}$ y $s_n = s - (s_1 + \cdots + s_{n-1}) \pmod m$).

1.3.3. El esquema umbral de Shamir

Veamos ahora el ejemplo más conocido de esquemas umbral (y de hecho, de todos los esquemas de reparto de secretos). Este se debe a Shamir [28] y es como sigue: para construir un esquema umbral de tipo (t,n) sobre el cuerpo finito $\mathbb{F}_q$, comenzamos eligiendo elementos distintos y no nulos $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ y asignando cada α_i al participante i. Estos α_i pueden ser públicamente conocidos.

Un secreto será un elemento $s \in \mathbb{F}_q$. Para repartirlo, el gestor elige al azar un polinomio de grado exáctamente $t-1$, con la condición de que su término independiente sea s (es decir, $f(0) = s$). La participación de i es $f(\alpha_i)$.

Una coalición de t o más participantes conoce el valor del polinomio f en t puntos, luego puede recuperarlo (y consecuentemente recuperar s) mediante interpolación de Lagrange. Una coalición de menos de t participantes no obtienen niguna información sobre el secreto, ya que cualquier valor de $f(0)$ es igualmente posible. Es claro entonces que el esquema es perfecto e ideal.

2

Aritmética modular y multimodular. El teorema Chino de los restos

En este capítulo presentamos varias versiones del teorema Chino de los restos, herramienta fundamental en la que se basa este trabajo. Ofreceremos varias versiones del teorema y aprovecharemos tambien para introducir algunos conceptos y métodos artiméticos que usaremos en capítulos posteriores. Una referencia general para los conceptos y resultados algebraicos que se utilizan en este capítulo es el libro [6].

Podemos comenzar con una nota histórica, los indicios más antiguos que tenemos del teorema Chino datan del siglo III d.C. Concretamente de un libro del matemático Chino Tsun-Zu en el que se expone el siguiente problema:

> *Hay cosas cuyo número se desconoce. Si las contamos de tres en tres nos sobran 2; si las contamos de cinco en cinco nos sobran tres; y si las contamos de siete en siete nos sobran 2. ¿Cuántas cosas hay?*

Sun-Tzu ofrece una demostración de que el problema tiene solución, pero no un algoritmo efectivo para resolverlo. Para esto tendremos que esperar hasta el siglo VI, de la mano del matemático hindú Aryabhata. En la matemática occidental, las primeras referencias a este teorema pueden encontrarse en la obra de Fibonacci.

2.1. Anillos, ideales y anillos cociente

Expondremos ahora algunos conceptos fundamentales del álgebra. En la sección siguiente trataremos de nuevo estos conceptos detallándolos para el caso particular del anillo de enteros, por lo que inicialmente los establecemos de manera general. Al final del capítulo, tras el examen detallado de los enteros, volveremos brevemente a tratar anillos más generales. A lo largo de todo el trabajo, con la palabra *anillo* nos refereriremos a anillo conmutativo y unitario.

2.1.1. Anillos e ideales

Sea A un anillo conmutativo y unitario. Decimos que A es un *dominio de integridad* (o simplemente un *dominio*) si no posee divisores de cero, esto es, si para cada par de elementos $x, y \in A$, la condición $xy = 0$ implica que bien $x = 0$ o bien $y = 0$. Un *ideal* de A es un subconjunto no vacio $I \subseteq A$ tal que:

(I1) para todo par de elementos $x, y \in I$ se verifica que $x - y \in I$; y

(I2) para todo par de elementos $x \in I, a \in A$ se verifica que $xa \in I$.

Dado $x \in A$, el conjunto $(x) = xA = \{xa : a \in A\}$, es un ideal, el *ideal generado por* x.

Análogamente, dados $x_1,\ldots,x_n \in A$, el conjunto $(x_1,\ldots,x_n) = \{x_1a_1+\ldots+x_na_n \mid a_1,\ldots,a_n \in A\}$, es un ideal, el *ideal generado por* $x_1,\ldots,x_n$. Decimos que un ideal I es *principal* si puede ser generado por un único elemento. Si todos los ideales de un dominio A son principales, se dice que A es un *dominio de ideales principales (DIP)*. Los anillos que más nos interesarán en este trabajo son los enteros $\mathbb{Z}$ y los polinomios con coeficientes en un cuerpo, $\mathbb{K}[X]$, y ambos son DIP.

Una *unidad* de A es un elemento $x \in A$ que posee inverso multiplicativo, es decir, tal que existe $y \in A$ verificando $xy = 1$. Denotaremos el inverso de x por x^{-1}. El conjunto de todas las unidades de A forma un grupo multiplicativo, que denotamos por A^*. Es inmediato comprobar que una unidad x no puede ser un divisor de cero, ya que si $xy = 0$, entonces

$$0 = x^{-1}xy = 1y = y.$$

Es claro que el ideal generado por una unidad contiene a 1, luego es el anillo total A. Por tanto un ideal propio $I \neq A$ no contiene ninguna unidad.

2.1.2. Operaciones con ideales

Dados dos ideales I,J del anillo A, se definen su *suma* y su *producto* como

$$\begin{aligned} I+J &= \{x+y \mid x \in I, y \in J\} \\ IJ &= (\{xy \mid x \in I, y \in J\}). \end{aligned}$$

Es inmediato comprobar que $I+J$ es un ideal. IJ lo es por construcción. Además, claramente $IJ \subseteq I \cap J$ por definición de ideal.

2.1.3. Anillos cociente

Dados un anillo A y un ideal I de A, la relación en A

$$x \equiv y \qquad \text{si y sólo si} \qquad x-y \in I$$

es una realación de equivalencia. El cociente de A, módulo esta relación de equivalencia, se denota A/I. Sus elementos son las clases de equivalencia $x+I = \{x+a \mid a \in I\}$. Las operaciones de A se trasladan a A/I de la forma obvia: dados $x,y \in A$

$$(x+I)+(y+I) = (x+y)+I; \qquad (x+I)\cdot(y+I) = (xy)+I.$$

Es inmediato comprobar que estas operaciones están bien definidas. Con ellas A/I adquiere una estructura de anillo y la aplicación natural de paso al cociente

$$A \to A/I, \qquad a \mapsto a+I$$

es un homomorfismo suprayectivo de anillos. Nótese que la clase de 0 en A/I es el propio ideal I, y que si $I = A$ entonces $A/I = \{0+A\}$.

2.1.4. Producto de anillos

Dados anillos $A_1,\ldots,A_n$, su *producto* es el conjunto $A_1 \times \ldots \times A_n = \{(a_1,\ldots,a_n) \mid a_i \in A_i, i = 1,\ldots,n\}$. Con las operaciones inducidas por las de $A_1,\ldots,A_n$, coordenada a coordenada, $A_1 \times \ldots \times A_n$ posee también estructura de anillo.

En este trabajo, a menudo consideraremos ideales $I_1,\ldots,I_n$ de A, y el anillo $A/I_1 \times \ldots \times A/I_n$ con su estructura multimodular.

2.2. Euclides, Bézout y Euler

La versión tradicional del teorema Chino de los restos se establece sobre el anillo $\mathbb{Z}$ e involucra los anillos cociente $\mathbb{Z}/m\mathbb{Z}$. Comenzamos con unos resultados previos, extremadamente importantes en aritmética y con interesantes aplicaciones prácticas, algunas de las cuales aparecerán continuamente en capítulos posteriores.

2.2.1. La división euclídea en los enteros

Sea $\mathbb{Z}$ el anillo de los números enteros. La propiedad aritmética más importante de $\mathbb{Z}$ es la existencia de una *división euclídea* (o *euclidiana*, o *con resto*), como sigue:

Teorema 2.2.1. *Dados dos enteros n, m con $m \neq 0$, existen enteros q y r (cociente y resto) tales que $n = mq + r$ y $0 \leq r < |m|$. Además, con las condiciones anteriores, cociente y resto son únicos.*

Demostración. Probaremos primero la existencia de la división con resto y posteriormente su unicidad. Supongamos en primer lugar que n y m son no negativos. Consideremos el conjunto

$$R = \{n - mz \mid z \in \mathbb{Z}, n - mz \geq 0\}.$$

R es no vacío pues $n = n - m \cdot 0 \in R$. Sea r su mínimo y q el entero que lo proporciona, es decir $r = n - mq$. Entonces $n = mq + r$. Además, como $r - m < r$ no es mínimo de R, deducimos que $r - m < 0$, es decir $0 \leq r < m$. En general, si alguno de los enteros n o m es negativo, utilizando el razonamiento anterior, se verifica que $|n| = |m|q + r$, estando r en las codiciones enunciadas. Basta entonces considerar cada uno de los casos posibles según los signos de n y m. Probemos ahora la unicidad de la división. Si $n = mq_1 + r_1 = mq_2 + r_2$ con $0 \leq r_1 \leq r_2 < |m|$, entonces $m(q_1 - q_2) = r_2 - r_1$. Como $0 \leq r_2 - r_1 < |m|$, necesariamente $q_1 = q_2$, luego $r_1 = r_2$. □

Corolario 2.2.2. *Los ideales de $\mathbb{Z}$ son de la forma $m\mathbb{Z}$, para $m \in \mathbb{Z}$. En consecuencia $\mathbb{Z}$ es un dominio de ideales principales.*

Demostración. Los conjuntos $m\mathbb{Z}$ son claramente ideales. Recíprocamente veamos que todo ideal es de esta forma. Sea I un ideal de $\mathbb{Z}$. Como $\{0\} = (0)$, podemos suponer que $I \neq (0)$. Sea m el menor elemento positivo de I. Por definición de ideal, $m\mathbb{Z} \subseteq I$. Por otro lado, si $n \in I$, podemos escribir $n = mq + r$ con $0 \leq r < m$. De la igualdad anterior, $r = n - mq \in I$, luego $r = 0$ y $n \in m\mathbb{Z}$, con lo que $I = m\mathbb{Z}$. □

Al poseer una división con resto, se dice que $\mathbb{Z}$ es un *dominio euclídeo (DE)*. El (único) resto r de la divisón de n entre m que garantiza el teorema anterior, es el valor de *n módulo m*, denotado $r = n \pmod{m}$. Dos enteros, n, t son *congruentes módulo m*, denotado $n \equiv t \pmod{m}$ si $n \pmod{m} = t \pmod{m}$, es decir, si $n - t \in m\mathbb{Z}$, lo que equivale a decir que se da la igualdad de clases $n + m\mathbb{Z} = t + m\mathbb{Z}$ en el anillo $\mathbb{Z}/m\mathbb{Z}$. Con esto deducimos que los enteros $\{0, 1, \ldots, m-1\}$ forman un conjunto completo de representantes de todas las clases de equivalencia en $\mathbb{Z}/m\mathbb{Z}$.

2.2.2. Primos y factorización

Recordemos que un entero n es *primo* si no es una unidad (± 1) y carece de divisores propios. Todo entero puede escribirse de forma única (salvo producto por unidades) como producto de números primos (es decir, $\mathbb{Z}$ es un *dominio de factorización única (DFU)*). Este resultado se conoce como *Teorema fundamental de la aritmética* y gracias a él los números primos, y los conceptos derivados de máximo común divisor (mcd) y mínimo común múltiplo (mcm) constituyen los ladrillos fundamentales con los que se construye la aritmética. El teorema fue enunciado por primera vez por Euclides (Proposición 14 del Libro 9 de sus Elementos), aunque la primera demostración completa apareció en las *Disquisitiones Arithmeticae* de Carl Friedrich Gauss. Aunque todo DIP es un DFU, damos aquí una prueba directa del teorema, basada en el siguiente resultado.

Lema 2.2.3. (Euclides). *Si un número primo p divide al producto de dos enteros positivos, entonces p divide al menos a uno de ellos.*

Demostración. Si p es primo, el ideal $p\mathbb{Z}$ es maximal, ya que $\mathbb{Z}$ es un DIP y $p\mathbb{Z} \subseteq q\mathbb{Z}$ implica $q|p$. Supongamos que $p|ab$, luego $pr = ab$, y que p no divide a b. Entonces $b \notin p\mathbb{Z}$ con lo que $(p,b) = A$, y existen $t,z \in \mathbb{Z}$ tales que $tp + zb = 1$. Por tanto $a = tap + zab = tap + zrp = (ta + zr)p$, con lo que $p|a$. □

Teorema 2.2.4. (Fundamental de la aritmética). *Todo entero positivo $n > 1$ puede ser representado de una única manera como un producto de primos.*

Demostración. La unicidad es consecuencia del Lema de Euclides. En efecto, si n es un entero positivo que admite dos representaciones $n = p_1 \cdot p_2 \cdot \ldots p_r = q_1 \cdot q_2 \cdot \ldots q_t$, podemos proceder por inducción sobre r. Si $r = 1$ entonces n es primo y el resultado es trivial. Supuesto cierto para $r-1$ veamos que se cumple para r. Observamos que: $p_1|n = q_1 \cdot q_2 \cdot \ldots q_t$, luego por el lema de Euclides existe j tal que $p_i|q_j$, y al ser ambos primos resulta que: $p_i = q_j$. Basta ahora aplicar la hipótesis de inducción a $\frac{n}{p_i}$. Con lo que se concluye que ambas representaciones son iguales.
Veamos la existencia. Si el resultado no fuera cierto, sea n el menor entero positivo que no es producto de primos. En particular n no es primo, luego posee un divisor a y consecuentemente $n = ab$. Como a y b son menores que n, ambos pueden escribirse como producto de primos, y por tanto también lo hace n. □

La factorización única en $\mathbb{Z}$ (y en cualquier otro DFU) permite definir los conceptos de *números coprimos* (o *primos entre sí*), *máximo común divisor* (mcd) y *mínimo común múltiplo* (mcm). Exponemos el siguiente resultado fundamental.

Teorema 2.2.5. *(*Identidad de Bézout). Sean a,b dos enteros no nulos. Existen enteros t,z, tales que $ta + zb = \text{mcd}\,(a,b)$.

Demostración. Consideremos el ideal $I = (a,b) = \{xa + yb \,|\, x,y \in \mathbb{Z}\}$ y sea d su menor elemento positivo. Es suficiente probar que $d = \text{mcd}\,(a,b)$. Realizando la división euclídea, $a = dq + r$ con $0 \leq r < d$, luego $r = a - dq \in I$ y necesariamente $r = 0$, luego $d|a$. Análogamente $d|b$, luego d es divisor común de a y b. Cualquier otro divisor común δ divide también a cada uno de los elementos de I, luego $\delta|d$ y por tanto $d = \text{mcd}\,(a,b)$. □

Obsérvese que la demostración de la identidad de Bézout que acabamos de presentar, en particular muestra que dados $a, b \in \mathbb{Z}$, se verifica que $\mathrm{mcd}(a,b)$ es un generador del ideal (a,b). A veces se escribe $\mathrm{mcd}(a,b) = (a,b)$. Obsérvese también que la identidad de Bézout es válida sobre cualquier DIP.

2.2.3. El algoritmo de Euclides y más sobre la identidad de Bézout

Este algoritmo se basa en la división euclídea: dados enteros $n, m \in \mathbb{Z}$ con $m \neq 0$, existen q y r, $0 \leq r < |m|$ tales que $n = mq + r$. Como hemos visto en la igualdad de Bézout, en esta situación, cualquier divisor común de n y m divide también a r, luego $\mathrm{mcd}(m,n)|r$. Si $r_1 = r \neq 0$ podemos dividir de nuevo, $m = rq_2 + r_2$ con $0 \leq r_2 < r$, y como antes los divisores comunes de n y m lo son también de r_2, luego $\mathrm{mcd}(m,n)|r_2$. Si iteramos este procedimiento:

$$\begin{aligned}
n &= mq_1 + r_1\,, & 0 \leq r_1 < m \\
m &= r_1 q_1 + r_2\,, & 0 \leq r_2 < r_1 \\
&\vdots & \vdots \\
r_{i-2} &= r_{i-1} q_{i-1} + r_i\,, & 0 \leq r_i < r_{i-1} \\
&\vdots & \vdots \\
r_{s-2} &= r_{s-1} q_{s-1} + r_s\,, & 0 \leq r_s < r_{s-1} \\
r_{s-1} &= r_s q_s\,, & r_{s+1} = 0
\end{aligned}$$

obtendremos un resto $r_{s+1} = 0$. Como en cada etapa $\mathrm{mcd}(r_{i-1}, r_{i-2})|r_i$, se verifica que $\mathrm{mcd}(n,m)|r_s$. Por otro lado, r_s divide a r_{s-1}, por la última igualdad, luego a r_{s-2} por la penúltima. Inductivamente r_s divide a n y m, luego $r_s = \mathrm{mcd}(n,m)$. Este el el *algoritmo de Euclides*.

Además, de la primera ecuación se obtiene que r_1 puede escribirse como $r_1 = x_1 n + y_1 m$, siendo x_1, y_1 enteros. Inductivamente, lo mismo sucede para todos los r_i. Si

$$r_{i-2} = x_{i-2} n + y_{i-2} m\,, \qquad r_{i-1} = x_{i-1} n + y_{i-1} m$$

entonces $r_i = r_{i-2} - r_{i-1} q_{i-1} = x_{i-2} n + y_{i-2} m - (x_{i-1} n + y_{i-1} m) q_{i-1} = x_i n + y_i m$. En particular, el último resto no nulo r_s, se pondrá $r_s = \mathrm{mcd}(n,m) = x_s n + y_s m$, que es la identidad de Bézout. La modificación del algoritmo de Euclides para llevar al cuenta de los restos y obtener los coeficientes x_s, y_s se llama *algoritmo de Euclides extendido*.

2.2.4. Las unidades de $\mathbb{Z}/m\mathbb{Z}$ y la función de Euler

El anillo cociente $\mathbb{Z}/m\mathbb{Z}$ es un cuerpo cuando $m\mathbb{Z}$ es un ideal maximal, y esto sucede si y sólo si m es un número primo, como vimos en el lema de Euclides. En otro caso no es siquiera un dominio de integridad. Si queremos caracterizar las unidades de $\mathbb{Z}/m\mathbb{Z}$ basta fijarnos en el siguiente resultado.

Proposición 2.2.6. *Sea $m \in \mathbb{Z}$ un entero positivo. Se verifica que*

$$(\mathbb{Z}/m\mathbb{Z})^* = \{t + m\mathbb{Z} \mid 1 \leq t < m, \mathrm{mcd}(t,m) = 1\}.$$

Demostración. Sea $t \in \mathbb{Z}$, $1 \leq t < m$, y sea $d = \text{mcd}(t,m)$. Según la identidad de Bézout, existen enteros x, y tales que $xt + ym = d$. Reduciendo esta igualdad módulo m obtenemos $xt \equiv d \pmod{m}$. Luego si $d = 1$ deducimos que $x \equiv t^{-1} \pmod{m}$. Si $d > 1$ existen enteros t', m' tales que $t = dt', m = dm'$. Por tanto $tm' \equiv 0 \pmod{m}$ y t no puede ser una unidad en $\mathbb{Z}/m\mathbb{Z}$, ya que en otro caso $t^{-1}tm' \equiv m' \equiv 0 \pmod{m}$, pero $0 < m' < m$. □

La demostración que hemos visto es constructiva y muestra como obtener efectivamente el inverso de un elemento a partir de la identidad de Bézout, y por tanto a partir del algoritmo de Euclides extendido.

Observemos que si m no es primo, de una relación del tipo $ua = ub$ en $\mathbb{Z}/m\mathbb{Z}$ no podemos deducir, en general, que $a = b$, ya que esta conclusión pasa por multiplicar ambos términos de la igualdad por u^{-1}, lo que require que u sea una unidad. Así por ejemplo $3 \cdot 1 = 3 \cdot 3 = 3 \cdot 5$ en $\mathbb{Z}/6\mathbb{Z}$. De manera análoga no es posible asegurar la existencia ni la unicidad de las soluciones de una ecuación $ax = b$ (de nuevo salvo que a sea una unidad). Por ejemplo en $\mathbb{Z}/6\mathbb{Z}$ la ecuación $3x = 3$ posee las soluciones $x = 1, 3, 5$, mientras que la ecuación $3x = 4$ no posee ninguna solución. Si m es primo, entonces todos sus elementos no nulos son unidades, y $\mathbb{Z}/m\mathbb{Z}$ es un cuerpo.

Como hemos dicho anteriormente, $(\mathbb{Z}/m\mathbb{Z})^*$ es un grupo multiplicativo. Su cardinal suele denotarse por $\phi(m)$, es decir

$$\phi(m) = |(\mathbb{Z}/m\mathbb{Z})^*| = |\{t \in \mathbb{Z} \,|\, 1 \leq t < m, \text{mcd}(t,m) = 1\}|.$$

La función ϕ así obtenida es la *función de Euler* o *indicador de Euler*, que juega un papel importante en la aritmética y la criptografía, y sobre la que volveremos en capítulos posteriores.

Proposición 2.2.7. *La función ϕ de Euler verifica las propiedades siguientes:*
(1) ϕ es multiplicativa: si $\text{mcd}(m,n) = 1$ *entonces* $\phi(mn) = \phi(m)\phi(n)$*;*
(2) si p es primo y $e \geq 1$, entonces $\phi(p^e) = (p-1)p^{e-1}$.

Demostración. (2) Si $t \leq p^e$, entonces $\text{mcd}(t, p^e) \neq 1$ si y sólo si t no es múltiplo de p, es decir, si es de la forma $p, 2p, \ldots, p^{e-1}p$. Por tanto $\phi(p^e) = p^e - p^{e-1} = (p-1)p^{e-1}$. □

La demostración de la propiedad (1) hace uso del teorema Chino de los restos y la veremos un poco más adelante. En todo caso, las propiedades anteriores hacen posible el cálculo de $\phi(m)$, a condición de conocer la descomposición de m en factores primos. Incluso proporcionan la fórmula explícita

$$\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

donde el producto se extiende a todos los divisores primos de m. En efecto, si $m = p_1^{e_1} \cdots p_r^{e_r}$, como producto de primos distintos, entonces

$$\phi(n) \quad = \quad \phi(p_1^{e_1}) \cdots \phi(p_r^{e_r})$$

$$
\begin{aligned}
&= p_1^{e_1}\left(1-\frac{1}{p_1}\right)\cdots p_r^{e_r}\left(1-\frac{1}{p_r}\right)\\
&= m\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right).
\end{aligned}
$$

Cuando m es producto de dos primos, $m = pq$, se verifica que $\phi(m) = (p-1)(q-1)$ (igualdad que es la base del sistema criptográfico RSA). Nótese que en esta situación, m es producto de dos primos, calcular $\phi(m)$ nos permite también factorizar m, ya que los factores p y q son las raíces del polinomio $x^2 - (m - \phi(m) + 1)x + m$.

2.3. El teorema Chino de los restos sobre $\mathbb{Z}$

Vamos ya con el teorema Chino. Comenzamos por las versiones clásicas, es decir sobre el anillo de enteros $\mathbb{Z}$.

2.3.1. El teorema para módulos coprimos

Teorema 2.3.1. (Chino de los restos. Versión en congruencias sobre $\mathbb{Z}$ para módulos coprimos) *Sean $m_1,\ldots,m_n \in \mathbb{Z}$ enteros mayores o iguales que 2 y dos a dos coprimos, esto es* $\mathrm{mcd}(m_i,m_j) = 1$ *para cada $i \neq j$. Dados enteros arbitrarios $a_1,\ldots,a_n \in \mathbb{Z}$, el sistema de ecuaciones en congruencias*

$$x \equiv a_i \,(\mathrm{mod}\, m_i) \qquad i = 1,\ldots,n,$$

admite solución. Además tal solución es única módulo $m_1\cdots m_n$.

Demostración. Sea $m = m_1\cdots m_n$ y para $i = 1,\ldots,n$, sea $q_i = m/m_i$. Como los m_i son coprimos dos a dos, deducimos que $\mathrm{mcd}(q_i,m_i) = 1$ para todo i, luego q_i es invertible en $\mathbb{Z}/m_i\mathbb{Z}$. Sea r_i su inverso (en $\mathbb{Z}/m_i\mathbb{Z}$) y consideremos

$$x = a_1q_1r_1 + \cdots + a_nq_nr_n.$$

Veamos que x es una solución de sistema de congruencias. Si $i \neq j$ se verifica que $m_i | q_j$, luego

$$x = a_1q_1r_1 + \cdots + a_nq_nr_n \equiv a_iq_ir_i \equiv a_i \,(\mathrm{mod}\, m_i) \qquad i = 1,\ldots,n,$$

ya que r_i es inverso de q_i. Además esta solución es única módulo m. En efecto, si y fuera otra solucion, entonces $m_i|(x-y)$ para todo i, con lo que, siendo los m_i coprimos, $m|(x-y)$, y por tanto $x \equiv y \,(\mathrm{mod}\, m)$. □

Obsérvese que la demostración del teorema anterior es constructiva y ofrece de forma explícita un método efectivo de resolver el sistema de congruencias.
Podemos también emplear el teorema de Euler: si $\mathrm{mcd}(a,n) = 1$, entonces $a^{\phi(m)} \equiv 1 \,(\mathrm{mod}\, m)$. En efecto, si $\mathrm{mcd}(a,m) = 1$ entonces $a \in \mathbb{Z}/m\mathbb{Z}$, que tiene cardinal $\phi(m)$. Entonces el teorema de Lagrange garantiza que $a^{\phi(m)} \equiv 1 \,(\mathrm{mod}\, m)$. Encontramos con esto que $x = a_1q_1^{\phi(m_1)} + \cdots + a_nq_n^{\phi(m_n)}$ es otra expresión de la solución del sistema de congruencias.

Ejemplo 2.3.2. El problema de Tsun-Zu, con el que comenzamos el capítulo, conduce al sistema de ecuaciones en congruencias

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7. \end{cases}$$

Dado que 3, 5 y 7 son coprimos, el sistema tiene solución única módulo $3 \cdot 5 \cdot 7 = 105$. Siguiendo el método descrito en la demostración del teorema consideremos $m = 105$, $q_1 = 35$, $q_2 = 21$, $q_3 = 15$. Utilizando el algoritmo de Euclides extendido, encontramos los inversos modulares de estos últimos, $r_1 = 2$, $r_2 = 1$, $r_3 = 1$. Solución del sistema es $2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$. Por tanto, la única solución módulo 105 es $233 \pmod{105} = 23$, y la solución general es $23 + 105\lambda$ siendo λ un entero no negativo.

Ejemplo 2.3.3. Posteriormente (**capítulo 3, ejemplo 3.1.2**) nos encontraremos el sistema

$$\begin{cases} x \equiv 429 \pmod{1013} \\ x \equiv 552 \pmod{1019} \\ x \equiv 397 \pmod{1021}. \end{cases}$$

De nuevo siguiendo el método descrito, sean $m = 1013 \cdot 1019 \cdot 1021 = 1053924187$, $q_1 = 1040399$, $q_2 = 1034273$, $q_3 = 1038361$. Utilizando el algoritmo de Euclides extendido, encontramos los inversos modulares de estos últimos, $r_1 = 401$, $r_2 = 934$, $r_3 = 766$. La solución del sistema es

$$429 \cdot 1040399 \cdot 401 + 552 \cdot 1034273 \cdot 934 + 397 \cdot 1038361 \cdot 766 = 777777777$$

módulo 1041537223.

Como consecuencia inmediata del teorema Chino encontramos lo siguiente:

Teorema 2.3.4. (Chino de los restos. Versión en isomorfismos sobre $\mathbb{Z}$) *Dados enteros $m_1, \ldots, m_n \in \mathbb{Z}$, mayores o iguales que 2 y dos a dos coprimos, se tiene el isomorfismo de anillos*

$$\mathbb{Z}/(m_1 \cdots m_n)\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$$

Antes de probar este teorema vamos a exponer algunos resultados de aritmética multimodular. Dados enteros $m_1, \ldots, m_n \in \mathbb{Z}$, mayores o iguales que 2 y no necesariamente coprimos, tenemos la aplicación

$$f : \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}, \qquad f(a) = (a + m_1\mathbb{Z}, \ldots a + m_1\mathbb{Z}).$$

Como las operaciones en cada $\mathbb{Z}/m_i\mathbb{Z}$ provienen de las de $\mathbb{Z}$, f es un homomorfismo de anillos.

Lema 2.3.5. $\ker(f)$ *es el ideal generado por $m = \operatorname{mcm}(m_1, \ldots, m_n)$. Por tanto f se extiende a un homomorfismo inyectivo $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$.*

Demostración. $a \in \mathbb{Z}$ esta en el núcleo de f si y sólo si es múltiplo de $m_1, \ldots, m_n$, es decir, si y sólo si es múltiplo de m. La seguna parte es consecuencia del primer teorema de isomorfía para anillos. □

Demostración del Teorema. Como los enteros $m_1, \ldots, m_n$ son coprimos dos a dos, se verifica $\text{mcm}(m_1, \ldots, m_n) = m_1 \cdots m_n$. Por tanto, según el lema anterior, se tiene un homorfismo inyectivo de anillos $f : \mathbb{Z}/m_1 \cdots m_n\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$, que será también sobreyectivo pues ambos son conjuntos finitos del mismo cardinal. Por lo tanto es un isomorfismo. □

Aunque los teoremas 2.3.1 y 2.3.1 son equivalentes, en cuanto a aplicaciones prácticas es claramente preferible la primera forma, puesto que muestra explícitamente como resolver el sistema de ecuaciones.

Nos disponemos ahora a demostrar la multiplicatividad de la función ϕ, que dejamos pendiente en la Proposición 2.2.7. Para ello emplearemos el siguiente lema:

Lema 2.3.6. *Dados enteros $m_1, \ldots, m_n \in \mathbb{Z}$, mayores o iguales que 2, se verifica que*

$$|(\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z})^*| = |(\mathbb{Z}/m_1\mathbb{Z})^*| \cdot \ldots \cdot |(\mathbb{Z}/m_n\mathbb{Z})^*|.$$

Demostración. Como las operaciones en $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$ se realizan coordenada a coordenada, un elemento $(a_1, \ldots, a_n) \in \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$ posee inverso si y sólo si cada a_i lo posee en $\mathbb{Z}/m_i\mathbb{Z}$. □

Corolario 2.3.7. *La función ϕ de Euler es multiplicativa, es decir si* $\text{mcd}(m,n) = 1$ *entonces $\phi(mn) = \phi(m)\phi(n)$.*

Demostración. Si $\text{mcd}(m,n) = 1$ entonces según el teorema Chino, $\mathbb{Z}/(mn)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, luego ambos anillos tienen la misma cantidad de unidades, $\phi(mn)$. Según el Lema 2.3.6 este último anillo contiene $\phi(m)\phi(n)$ unidades. Por tanto $\phi(mn) = \phi(m)\phi(n)$. □

La condición de que los módulos m_i sean coprimos dos a dos es esencial para que se verifique el teorema Chino que hemos visto. Así, por ejemplo, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ y $\mathbb{Z}/4\mathbb{Z}$ no son isomorfos (no lo son siquiera como grupos). Sin embargo sí existe una extensión del teorema, que muestra como las condiciones sobre los m_i pueden relajarse, manteniéndose la existencia de solución única bajo determinadas condiciones.

2.3.2. El teorema Chino para módulos no coprimos

Vamos a estudiar el teorema Chino en el caso de que los módulos de las ecuaciones no sean coprimos, recuérdese que esto era condición suficiente pero no necesaria. Para ello llevaremos el problema al caso anterior, descomponiendo cada una de las ecuaciones en tantas otras como factores primos posea el módulo que aparece en ella.

Lema 2.3.8. *Sea $m \in \mathbb{Z}$ y $m = t_1 \cdots t_r$ una escritura de m como producto de enteros coprimos dos a dos. Entonces para todo $a \in \mathbb{Z}$, la ecuación $x \equiv a \pmod{m}$ es equivalente al sistema de ecuaciones en congruencias*

$$(S) \qquad x \equiv a \pmod{t_i} \qquad i = 1, \ldots, r$$

en el sentido de que ambos tienen la misma solución módulo m.

Demostración. Si $x \equiv a \pmod{m}$ entonces $x = a + \lambda t_1 \cdots t_r$, luego $x \equiv a \pmod{t_i}$ para todo $i = 1, \ldots, r$. Recíprocamente, si x es solución de (S), entonces $t_i | x - a$ para todo i, y como estos enteros son coprimos, $m | x - a$, es decir $x \equiv a \pmod{m}$. La solución de (S) es única módulo $t_1 \cdots t_r = m$, y lo mismo le sucede a la solución de $x \equiv a \pmod{m}$. □

Una vez descompuestas todas las ecuaciones según los factores primos de sus módulos, el sistema tiene solución si las nuevas ecuaciones obtenidas son compatibles entre sí. En el caso de que obtengamos ecuaciones en congruencias módulo potencias de un mismo primo:

$$\begin{cases} x \equiv a \pmod{p^e} \\ x \equiv b \pmod{p^k} \end{cases}$$

con $e \geq k$, tiene solución si y sólo si $a \equiv b \pmod{p^k}$, y que $\text{mcd}(p^e, p^k)) = p^k$. En tal caso, la segunda ecuación es redundante y puede ser suprimida.

Teorema 2.3.9. (Chino de los restos. Versión en congruencias sobre $\mathbb{Z}$ para módulos no coprimos) *Sean $m_1, \ldots, m_n \in \mathbb{Z}$ enteros mayores o iguales que 2. Dados enteros arbitrarios $a_1, \ldots, a_n \in \mathbb{Z}$, el sistema de ecuaciones en congruencias*

$$x \equiv a_i \pmod{m_i} \qquad i = 1, \ldots, n,$$

tiene solución si y sólo si $a_i \equiv a_j \pmod{\text{mcd}(m_i, m_j)}$ para todos i, j. En tal caso, la solución es única módulo $\text{mcm}(m_1, \ldots, m_n)$.

Demostración. Si existe solución, x, entonces para cada i, se verifica $x \equiv a_i \pmod{m_i}$, luego $m_i | (x - a_i)$, y por tanto, para todo j, $\text{mcd}(m_i, m_j) | (x - a_i)$. Análogamente $\text{mcd}(m_i, m_j) | (x - a_j)$, por lo que $\text{mcd}(m_i, m_j) | ((x - a_j) - (x - a_i)) = a_i - a_j$. Para ver el recíproco, mostraremos que bajo las condiciones indicadas, el sistema puede reducirse a uno con módulos coprimos (que como ya sabemos, posee solución). Para ello observemos que dado $m \in \mathbb{Z}$ cuya factorización en primos es

$$m = p_1^{e_1} \cdots p_r^{e_r}$$

se verifica que $x \equiv a \pmod{m}$ si y sólo si $x \equiv a \pmod{p_k^{e_k}}$ para todo primo de la factorización de m. Supongamos pues que $\text{mcd}(m_i, m_j) | (a_i - a_j)$ para todos i, j. Sea p^e uno de los factores en la descomposición prima de $\text{mcm}(m_1, \ldots, m_n)$. Este p^e será factor de algunos de los m_j. Para cada $j = 1, \ldots, n$, sea e_j el máximo exponente tal que $p^{e_j} | m_j$. Pongamos que $e = e_i$, es decir, $e_j \leq e_i$ para todo j. En tal caso, $x \equiv a_i \pmod{p^{e_i}}$ implica que $x \equiv a_i \pmod{p^{e_j}}$ para todo j. Pero $p^{e_j} | \text{mcd}(m_i, m_j) | (a_i - a_j)$, luego $a_i \equiv a_j \pmod{p^{e_j}}$. Por tanto la condición $x \equiv a_i \pmod{p^{e_i}}$ implica que $x \equiv a_i \pmod{p^{e_j}}$, lo que a su vez implica que $x \equiv a_j \pmod{p^{e_j}}$. En consecuencia, nuestro sistema de ecuaciones en congruencias original tiene solución siempre que la tenga el sistema

$$x \equiv a_i \pmod{p^{e_i}} \qquad p | \text{mcm}(m_1, \ldots, m_n)$$

donde para cada $p | \text{mcm}(m_1, \ldots, m_n)$, hemos elegido el índice i tal que e_i es la máxima potencia de p que divide a $\text{mcm}(m_1, \ldots, m_n)$ de entre las que aparecen en alguno de los módulos m_j. Ahora bien, este sistema tiene módulos coprimos, y por tanto el teorema Chino de los restos, en su versión anterior, garantiza que posee solución. La demostración

de que esta es única es similar a la ya vista para el caso de módulos coprimos: si y fuera otra solución, entonces $x-y \equiv 0 \pmod{m_i}$ para todo i, luego $\text{mcm}(m_1,\ldots,m_n)|x-y$ por lo que $x \equiv y \pmod{\text{mcm}(m_1,\ldots,m_n)}$. □

Nótese que esta verión del teorema Chino es también constructiva, a condición de que seamos capaces de factorizar todos los módulos $m_1,\ldots,m_n$.

Ejemplo 2.3.10. En un capítulo posterior **capítulo 3, ejemplo 3.1.5** nos encontraremos el sistema

$$\begin{cases} x \equiv 225 \pmod{1002} \\ x \equiv 452 \pmod{1003} \\ x \equiv 681 \pmod{1004}. \end{cases}$$

Como

$$\begin{aligned} 1 &= \text{mcd}(1002,1003)|452-225=227, \\ 2 &= \text{mcd}(1002,1004)|681-225=456, \\ 1 &= \text{mcd}(1003,1004)|681-452229, \end{aligned}$$

el sistema tiene solución. La factorización de los módulos m_i es

$$1002 = 2\cdot 3\cdot 167,\ \ 1003 = 17\cdot 59,\ \ 1004 = 2^2\cdot 251.$$

Deducimos que $\text{mcm}(1002,1003,1004) = 2^2\cdot 3\cdot 17\cdot 59\cdot 167\cdot 251$, y que el sistema de ecuaciones original se reduce al sistema con módulos coprimos

$$\begin{cases} x \equiv 681 \pmod{4} \\ x \equiv 225 \pmod{3} \\ x \equiv 452 \pmod{17} \\ x \equiv 452 \pmod{59} \\ x \equiv 225 \pmod{167} \\ x \equiv 681 \pmod{251} \end{cases}$$

cuya única solución módulo $\text{mcd}(1002,1003,1004) = 504513012$ es $x = 777777$.

Un estudio detallado de esta versión del teorema puede encontrarse por ejemplo en [25]. Dada su importancia en numerosos algoritmos asociados a procesos de codificación, computación, etc., se han estudiado implementaciones eficientes de este algoritmo, tanto en su versión original para módulos coprimos [12], como en su versión general, [9].

Ejemplo 2.3.11. El teorema Chino de los restos, especialmente en su versión para módulos coprimos, se utiliza en muchos sistemas de computación, cuando es necesario realizar operaciones con enteros muy grandes. Elegidos módulos $m_1,\ldots,m_n$ coprimos entre sí, el isomorfismo

$$\mathbb{Z}/m_1\cdots m_n\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z}\times\cdots\times\mathbb{Z}/m_n\mathbb{Z}$$

permite trasladar operaciones con enteros en el rango $[0, m_1\cdots m_n)$ a operaciones modulares en los $\mathbb{Z}/m_i\mathbb{Z}$, y recíprocamente. Al ser el isomorfismo entre anillos, funciona bien para sumas y productos, pero no para divisiones. Para ver un ejemplo, tomemos los

módulos que usamos en el **ejemplo 2.3.3**: $m_1 = 1013, m_2 = 1019, m_3 = 1021$. Deseamos calcular a^2 siendo $a = 12345$. Como

$$a \,(\text{mod } 1013) = 189, \quad a \,(\text{mod } 1019) = 117, \quad a \,(\text{mod } 1021) = 93,$$

el problema de calcular a^2 en $\mathbb{Z}$ se traslada al de calcular los cuadrados de estos números en los correspondientes anillos modulares. Operando

$$\begin{aligned} a^2 \,(\text{mod } 1013) &= 189^2 \,(\text{mod } 1013) = 266, \\ a^2 \,(\text{mod } 1019) &= 117^2 \,(\text{mod } 1019) = 442, \\ a^2 \,(\text{mod } 1021) &= 93^2 \,(\text{mod } 1021) = 481. \end{aligned}$$

Finalmente trasladamos los resultados obtenidos a $\mathbb{Z}$. En este ejemplo sólo estamos realizando un cuadrado. En aplicaciones reales, podemos estar interesados en cálculos que impliquen miles de operaciones. El resultado final se trasladará a $\mathbb{Z}$ una vez realizadas todas ellas. Para obtener el resultado entero del cálculo, planteamos el sistema

$$\begin{cases} x \equiv 226 \pmod{1013} \\ x \equiv 442 \pmod{1019} \\ x \equiv 481 \pmod{1021}. \end{cases}$$

cuya solución es $x = 152399025$. Como $a^2 < m_1 m_2 m_3 = 1053924187$, concluimos que $a^2 = 152399025$.

En palabras de las ciencias de la computación, este tipo de técnicas son conocidas como SRN (Sistemas de Residuos Numéricos).

2.4. Una versión en términos de anillos e ideales

Podemos establecer una versión aún más general del teorema chino del resto, en términos del álgebra comnmutativa, mediante anillos e ideales. Sea A un anillo conmutativo y con unidad. Un ideal propio I de A es *primo* si para cada par de elementos $x, y \in A$, la condición $xy \in I$ implica que bien $x \in I$ o bien $y \in I$. Equivalentemente I es primo si A/I es un dominio de integridad. Dos ideales I, J de A son *coprimos* (o *comaximales*) si $I + J = A$, es decir, si existen $x \in I, y \in J$ tales que $x + y = 1$.

Lema 2.4.1. *Si A es conmutativo. Si los ideales I, J son coprimos, entonces $IJ = I \cap J$.*

Demostración. Hemos visto ya que $IJ \subseteq I \cap J$ para todo par de ideales. Recíprocamente, si I, J son coprimos, existen $x \in I, y \in J$ tales que $x + y = 1$. Si $a \in I \cap J$, entonces $a = ax + ay \in IJ$, luego $I \cap J \subset IJ$ y se tiene la igualdad. □

Teorema 2.4.2. (Chino de los restos. Versión para anillos) *Sea A un anillo conmutativo y unitario. Si los ideales I, J son coprimos, entonces se tiene el isomorfismo de anillos*

$$A/IJ \cong A/I \times A/J.$$

Demostración. La aplicación natural

$$f : A \to A/I \times A/J, \quad f(a) = (a+I, a+J)$$

está bien definida y es un homomorfismo de anillos. Si $a+I = a+J = 0$, entonces $a \in I \cap J = IJ$, luego $\ker(f) = IJ$. Veamos que es sobreyectiva. Como I, J son coprimos, todo $a \in A$ se escribe $a = x+y$ con $x \in I, y \in J$. Por tanto, todo elemento de A/I es de la forma $a+I = y+I$ con $y \in J$. Análogamente, todo elemento de A/J será $x+J$ con $x \in I$. En consecuencia, todo elemento $(y,x) \in A/I \times A/J$ es imagen por f de $x+y \in A$. □

Podemos extender este resultado a:

Corolario 2.4.3. *Sea A un anillo conmutativo y unitario. Dados ideales $I_1, \dots I_n$ de A tales que cada uno de ellos es coprimo con el resto, entonces se tiene el isomorfismo:*

$$A/(I_1, \dots I_n) \cong A/I_1 \times \cdots \times A/I_n$$

No es posible establecer para anillos generales una versión de este resultado similar a la obtenida en el Teorema 2.3.1, ya que no contamos con 'restos' análogos a los que produce la división euclídea, ni factorización única, ni por tanto puede definirse el máximo común divisor de dos elementos.

No obstante, existe un tipo de anillos para los que todo esto sí es posible, de manera completamente similar a lo estudiado en $\mathbb{Z}$.

2.5. El teorema Chino sobre dominios euclídeos

2.5.1. Dominios euclídeos

La noción de *dominio euclídeo* proviene del propósito de sistematizar las posibilidades que ofrece la división euclídea. En concreto, dado un dominio de integridad A, llamaremos *función euclídea* a toda función $\varepsilon : A \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ que satisfaga las condiciones siguientes:

(FE1) para todo par $x, y \in A$ con $y \neq 0$, se verifica $\varepsilon(xy) \geq \varepsilon(x)$.
(FE2) para todo par $x, y \in A$ con $y \neq 0$, existen $q, r \in A$ tales que $x = yq + r$ con $\varepsilon(r) < \varepsilon(y)$ o $r = 0$.

Decimos que A es un dominio euclídeo si admite una función euclídea ε. Por ejemplo, $\mathbb{Z}$ es un dominio euclídeo con la función $\varepsilon(x) = |x|$. Otro ejemplo relevante para este trabajo es el siguiente.

Proposición 2.5.1. *Si $\mathbb{K}$ es un cuerpo, el anillo de polinomios $\mathbb{K}[X]$ es un dominio euclídeo con la función euclídea $\varepsilon(f(X)) = \deg(f(X))$.*

Demostración. Sean $f(X), g(X) \in \mathbb{K}[X]$ dos polinomios con $g(X) \neq 0$. La funcion deg verifica la condición (FE1) ya que $\deg(f(X)g(X)) = \deg(f(X)) + \deg(g(X)) \geq \deg(f(X))$. Comprobemos la condición (FE2) mostrando la existencia de la división euclídea de $f(X)$ entre $g(X)$. Si $\deg(f(X)) < \deg(g(X))$ basta tomar $q(X) = 0, r(X) = f(X)$ para concluir.

Supongamos pues $\deg(f(X)) \geq \deg(g(X))$. Restando a $f(X)$ un múltiplo adecuado de $g(X)$ podemos cancelar su término de mayor grado. Si

$$\begin{aligned} f(X) &= a_n X^n + \cdots + a_1 X + a_0 \\ g(X) &= b_m X^m + \cdots + b_1 X + b_0. \end{aligned}$$

con $a_n b_m \neq 0$ y $n \geq m$, consideramos los polinomios

$$q_1(X) = \frac{a_n}{b_m} X^{n-m}, \qquad f_1(X) = f(X) - g(X)q_1(X)$$

que verifican $\deg(f_1(X)) < \deg(f(X))$ ó $f_1(X) = 0$. Si $\deg(f_1(X)) < \deg(g(X))$, como $f(X) = g(X)q_1(X) + f_1(X)$, tomamos $r(X) = f_1(X), q(X) = q_1(X)$ y hemos acabado. En otro caso repetimos el proceso con $f_1(X)$ y $g(X)$ obteniendo polinomios $f_2(X), q_2(X)$ tales que $f_1(X) = g(X)q_2(X) + f_2(X)$ y $\deg(f_2(X)) < \deg(f_1(X))$ ó $f_1(X) = 0$. Por tanto $f(X) = g(X)q_1(X) + f_1(X) = g(X)q_1(X) + g(X)q_2(X) + f_2(X)$. Iterando el proceso, al cabo de a lo mas $n-m$ pasos obtendremos un polinomio $f_s(X) = f_{s-1}(X) - g(X)q_s(X)$ que verifica $\deg(f_s(X)) < \deg(g(X))$ o $f_s(X) = 0$. Para ese polinomio $f(X) = g(X)(q_1(X) + \cdots + q_s(X)) + f_s(X)$, luego basta tomar $q(X) = q_1(X) + \cdots + q_s(X), r(X) = f_s(X)$ para obtener una división euclídea $f(X) = g(X)q(X) + r(X)$ con las condiciones requeridas. □

Remarquemos que la división euclídea, $f(X) = g(X)q(X) + r(X)$, además de existir es única, con la condición $\deg(r(X)) < \deg(g(X))$ o $r(X) = 0$. La demostración es análoga a la del caso entero: si $f(X) = g(X)q_1(X) + r_1(X) = g(X)q_2(X) + r_2(X)$ entonces $r_2(X) - r_1(X) = g(X)(q_1(X) - q_2(X))$ con $r_1(X) - r_2(X) = 0$ o $\deg(r_1(X) - r_2(X)) < \deg(g(X))$, por lo que $q_1(X) - q_2(X) = 0$ y $r_1(X) - r_2(X) = 0$.

Recordemos que una no unidad $x \neq 0$ de un dominio de integridad A es *irreducible* si no puede ser expresada como producto de dos no unidades, esto es, si para cada escritura $x = ab$ o bien a o bien b es una unidad de A. Cuando A es un DIP y $x \in A$ es irreducible entonces el ideal (x) es maximal, ya que $(x) \subseteq (y)$ implica $x = ay$, luego si $(y) \neq A$ entonces y no es una unidad, con lo que a sí lo es, y se tiene $(y) = (x)$. En consecuencia, si x es irreducible, entonces el anillo cociente $A/(x)$ es un cuerpo.

Proposición 2.5.2. *Todo dominio euclídeo A es un DIP.*

Demostración. Sea I un ideal de A. Sea x un elemento de I con $\varepsilon(x)$ mínimo. Veamos que $I \subseteq (x)$. Sea $y \in I$. Realizando la división euclídea, $y = xq + r$, luego $r = y - xq \in I$. Como $\varepsilon(x)$ es mínimo en I, no puede suceder que $\varepsilon(r) < \varepsilon(x)$ y por tanto $r = 0$, de donde $y \in (x)$. □

Como consecuencia, en todo dominio euclídeo existen el mcd y el mcm de dos elementos, y se verifica una identidad de Bézout.

Proposición 2.5.3. *Sea A un DIP y sean $x, y \in A$ dos elementos no nulos. Existe $d \in A$ tal que $d = ax + by$ con $a, b \in A$ y $d = \mathrm{mcd}(x, y)$.*

Demostración. Siendo A un DIP, dados x, y, existe $d \in A$ tal que $(x, y) = (d)$, luego $d = ax + by$ para ciertos $a, b \in A$. Como $(x) \subseteq (d)$ e $(y) \subseteq (d)$ deducimos que $d|x$ y $d|y$. Si d' es otro elemento tal que $d'|x$, $d'|y$, entonces $d'|ax + by = d$. Por tanto $d = \mathrm{mcd}(x, y)$. □

Además la división euclídea (con respecto a ε) permite un algoritmo de Euclides extendido (que no es preciso repetir aquí al ser esta completamente similar al del caso entero) para calcular ambos.

2.5.2. El teorema Chino para dominios euclídeos

Despues de todo nuestro estudio, el enunciado formal del teorema en este caso tan general, es el mismo con el que empezamos.

Teorema 2.5.4. (Chino de los restos. Versión en congruencias sobre dominios euclídeos) *Sea A un dominio euclídeo y sean* $a_1,\dots,a_n,m_1,\dots,m_n \in A$. *El sistema de ecuaciones en congruencias*

$$x \equiv a_i \,(\mathrm{mod}\ m_i) \qquad i = 1,\dots,n,$$

tiene solución si y sólo si $a_i \equiv a_j \,(\mathrm{mod}\ \mathrm{mcd}(m_i,m_j))$ *para todo par de índices* i, j. *En tal caso, la solución es única módulo* $\mathrm{mcm}(m_1,\dots,m_n)$.

Demostración. Es completamente similar a las de los teoremas **2.3.1.** y **2.3.9.**. Si los módulos son coprimos entre sí, entonces como en el **teorema 2.3.1.** el elemento

$$x = a_1 q_1 r_1 + \cdots + a_n q_n r_n$$

es solución. Nótese que los inversos modulares r_i en A/m_i pueden calcularse mediante el algoritmo de Euclides. Si los módulos m_i no son coprimos entre sí, entonces procedemos como en la demostración de **teorema 2.3.9.**. Podemos descomponer los módulos como productos de potencias de irreducibles, transformando así el sistema de ecuaciones en otro equivalente que sí sea de módulos coprimos. Por tanto, cuando dicha descomposición como producto de potencias irreducibles se pueda calcular, también se podrá calcular la solución x mediante el algoritmo de Euclides.

□

Nótese además que esta demostración es también válida cuando A es un D.I.P. Sin embargo, en este caso no disponemos de un algoritmo de Euclides que nos permita obtener de forma directa una expresión para la solución del sistema.

Encontramos por último que, también en este caso, el teorma garantiza la existencia de un homomorfismo inyectivo

$$A/(m_1 m_2 \cdots m_n) \to A/m_1 \times \cdots \times A/m_n$$

cuya imagen está formada por las n-uplas $(a_1,\dots,a_n)$ tales que $a_i \equiv a_j \,(\mathrm{mod}\ \mathrm{mcd}(m_i,m_j))$ para todo par de índices i, j.

En el capítulo 4, utilizaremos frecuentemente este teorema aplicado al anillo $\mathbb{K}[X]$, siendo $\mathbb{K}$ un cuerpo finito. Según lo expuesto anteriormente $\mathbb{K}[X]$ es un domino euclídeo, luego el teorema tiene completa validez.

3

Esquemas de reparto de secretos sobre $\mathbb{Z}$

Durante este y el siguiente capítulo nos dedicaremos a estudiar los esquemas de reparto de secretos basados en el teorema Chino de los restos. Como dijimos anteriormente, dado un conjunto de participantes $\mathscr{P} = \{1, \ldots, n\}$, una estructura de acceso $\mathscr{A}$ es llamada *umbral* si existe un entero t tal que $\mathscr{A} = \{A \subseteq \{1, \ldots, n\} \,|\, |A| \geq t\}$. Esto es, si son necesarios y suficientes t participantes para recuperar el secreto. Las estructuras y los esquemas umbral resultan ser los más simples, por lo que es natural que nuestro estudio comience por ellos.

Ya se ha citado que el interés por el reparto de secretos comienza con el artículo [28] de A. Shamir. A raíz de la publicación de este trabajo fueron propuestos muy rápidamente cuatro tipos de esquemas de reparto, todos ellos para el caso de las estructuras umbral. El primero por parte del propio Shamir (que de hecho ya aparece en el artículo mencionado) basado en la interpolación polinómica sobre un cuerpo finito $\mathbb{F}_q$.

Otro método fue propuesto por Blakley [3], utilizando la geometría proyectiva sobre $\mathbb{F}_q$. Y unos tercer y cuarto métodos por Mignotte [23], y Asmuth y Bloom [1], basados ambos en el teorema Chino de los restos sobre $\mathbb{Z}$. Estos dos últimos son los que describimos y estudiamos a continuación. Nos ocuparemos primero del de Mignotte. El de Asmuth-Bloom será tratado en la sección siguiente.

3.1. Esquemas umbral de Mignotte

La formulación original de M. Mignotte se basa en las propiedades aritméticas del anillo $\mathbb{Z}$ para fabricar esquemas umbral. Esta formulación original ha sido después generalizada por diversos autores para adaptarla a tareas específicas de diversos protocolos criptográficos. Entre estas modificaciones y generalizaciones (algunas de las cuales iremos viendo en esta memoria) podemos destacar los trabajos de S. Iftene [15], [14], [16]. Ocurre que algunos de los autores de estos trabajos proceden del mundo de las ciencias de la computación, con lo que, al gusto matemático, sus argumentos y demostraciones son demasiado laxos con respecto a la rigurosidad. Por tanto, una de las tareas que nos hemos propuesto durante esta memoria es desarrollarlos con el rigor que merecen.

3.1.1. El esquema de Mignotte original

Pasamos ahora a exponer el esquema en su versión original: Sean $1 < t < n$ el umbral y el cardinal del conjunto de participantes del esquema que deseamos fabricar. Diremos que una secuencia estrictamente creciente de n números enteros positivos, $\mathbf{m}$: $m_1 < \cdots < m_n$, satisface la condición t de Mignotte si los m_i son coprimos dos a dos y se verifica que $m_{n-t+2} \cdots m_n < m_1 \cdots m_t$. Estos enteros m_i son llamados los *módulos* del

sistema. Dada una secuencia de este tipo, el esquema de Mignotte permite repartir un secreto del conjunto $\mathscr{S} = \{s \in \mathbb{Z} \,|\, m_{n-t+2} \cdots m_n < s < m_1 \cdots m_t\}$ de la siguiente manera:

a cada participante i se le asigna su módulo m_i. Estos módulos pueden ser de conocimiento público, y reutilizarse tantas veces como se desee. Dado el secreto $s \in \mathscr{S}$

• la participación del participante i es $s_i = s \pmod{m_i}$, $i = 1, \ldots, n$;
• cualquier coalición $A \subseteq \mathscr{P}$ de t o más participantes, puede recuperar s resolviendo el sistema en congruencias

$$(S_A): \quad x \equiv s_i \pmod{m_i} \qquad i \in A.$$

Proposición 3.1.1. *El método descrito es correcto y proporciona un esquema umbral de tipo* (t,n).

Demostración. Para cada conjunto $C \subseteq \mathscr{P}$ ponemos $m_C = \prod_{i \in C} m_i$. La condiciones $m_1 < \cdots < m_n$ y $m_{n-t+2} \cdots m_n < m_1 \cdots m_t$ implican que para cualquier par de coaliciones A, B con $|A| \geq t$ (autorizada) y $|B| < t$ (no autorizada), se verifica que $m_B \leq m_{n-t+2} \cdots m_n < s < m_1 \cdots m_t \leq m_A$. Como A esta autorizado, de acuerdo con el teorema Chino de los restos, el sistema de ecuaciones (S_A) posee una única solución x módulo m_A. Como s es solución y $s < m_A$, necesariamente $x = s$. Como $|B| < t$, el sistema (S_B) proporciona una solución $x < m_B \leq m_{n-t+2} \cdots m_n < s$, luego $x \neq s$. □

Ocurre, eso sí, que el esquema de Mignotte no es perfecto. Una coalición no autorizada B puede resolver (S_B), cuya solución x le proporciona el valor $x = s \pmod{m_B}$ (puesto que para el auténtico secreto s, el número $s \pmod{m_B}$ es también solucion del sistema (S_B)). Por tanto s será de la forma $s = x + \lambda m_B$, para algún λ entero con la condición $m_{n-t+2} \cdots m_n < x + \lambda m_B < m_1 \cdots m_t$. Así, la coalición B puede descartar todos los elementos de $\mathscr{S}$ que no cumplen esta condición, y sólo debe considerar como posibles secretos los $\lfloor (m_1 \cdots m_t - m_{n-t+2} \cdots m_n - 1)/m_B \rfloor$ que sí la cumplen, lo que podría permitir un ataque por fuerza bruta. Como $m_B \leq m_{n-t+2} \cdots m_n$, para hacer que este ataque sea computacionalmente inviable, los enteros m_i deben elegirse de manera que, aún al descartar los anteriormente mencionados, existan todavía muchos secretos posibles. Es decir, de manera que $(m_1 \cdots m_t - m_{n-t+2} \cdots m_n)/m_{n-t+2} \cdots m_n$ sea lo suficientemente grande.

El esquema de Mignotte tiene, sin embargo, la ventaja del pequeño tamaño de las participaciones s_i $(0 \leq s_i < m_i)$ en relación al tamaño del secreto repartido $(m_{n-t+2} \cdots m_n < s < m_1 \cdots m_t)$. Si, como es razonable, todos los m_i se toman del mismo orden de magnitud, $m_i \sim m$, el número de secretos posibles (expurgados los descartables por una coalición no autorizada, como acabamos de describir) es del orden de $(m^t - m^{t-1})/m^{t-1} \sim m$. Luego el esquema es aproximadamente ideal y puede ser usado en situaciones en las que el tamaño sea un criterio relevante.

3.1.2. Un ejemplo

Volvamos al problema combinatorio de Shamir que enunciamos en el capítulo 1. Para no distraernos con demasiados datos, pongamos que seis científicos desean poder abrir el armario cuando al menos la mitad de ellos, tres, esté presente. Esto es, deseamos fabricar un esquema umbral de tipo $(3,6)$. Digamos que los científicos consideran

suficientemente seguro un espacio de secretos de tamaño 1000. Tomemos

$$m_1 = 1009,\ m_2 = 1013,\ m_3 = 1019,\ m_4 = 1021,\ m_5 = 1031,\ m_6 = 1033$$

(que son primos consecutivos) lo que conduce al espacio de secretos

$$\mathscr{S} = \{s \in \mathbb{Z} \,|\, 1065023 < s < 1041537223\}$$

de cardinal mucho mayor que 1000. Digamos también que secreto a repartir (la clave de la cerradura del armario) es $s = 777777777$. Las participaciones son

$$s_1 = 217,\ s_2 = 429,\ s_3 = 552,\ s_4 = 397,\ s_5 = 656,\ s_6 = 54.$$

Si la coalición autorizada $A = \{2,3,4\}$ quiere recuperar el secreto, resuelve el sistema

$$\begin{cases} x \equiv 429 \pmod{1013} \\ x \equiv 552 \pmod{1019} \\ x \equiv 397 \pmod{1021} \end{cases}$$

cuya única solución módulo 1041537223 es $x = 777777777 = s$. Si ahora la coalición no autorizada $B = \{2,4\}$ quiere recuperar el secreto, puede resolver el sistema

$$\begin{cases} x \equiv 429 \pmod{1013} \\ x \equiv 397 \pmod{1021} \end{cases}$$

cuya única solución módulo 1034273 es $x = 4481$. Por tanto esta coalición no recupera el secreto. Sin embargo sí puede deducir que $s = 4481 + 1034273\,\lambda$, para algún λ. Como hemos explicado anteriormente, esta condición le permite reducir el espacio $\mathscr{S}$ a $\lfloor (1040472200-1)/1034273 \rfloor = 1005$ valores de s posibles, lo que esta de acuerdo con el nivel de seguridad que pedimos.

3.1.3. Sobre las secuencias de Mignotte

Uno de los primeros problemas que surgen con este esquema puede ser el de encontrar secuencias **m** adecuadas satisfaciendo la condición t de Mignotte. Esto lleva a considerar dos tipos de preguntas:

(a) ¿Cómo de difícil es encontrar una secuencia de n enteros mutuamente coprimos?
(b) ¿De qué tamaño deben ser los m_i para que el espacio de secretos sea tan grande como se quiera?

Sobre la primera pregunta, según puede leerse en [32], la probabilidad de que dos enteros tomados al azar sean coprimos es $6/\pi^2$, bastante grande. Evitando tomar enteros con factores primos pequeños, como 2,3,5, no parece nada complicado encontrar secuencias de números mutuamente coprimos.

Sobre la segunda cuestión, hemos notado ya que el espacio de secretos (excluidos los descartables por una coalición no autorizada) es del mismo orden los los módulos m_i tomados. En el ejemplo anterior hemos usado una secuencia formada por módulos primos consecutivos, para obtener un esquema $[3,6]$ para el que pedíamos un espacio de secretos con al menos $\Delta = 1000$ elementos. Para tener una idea del orden de los módulos

necesarios, en relación con Δ, hemos realizado una búsqueda por computadora de las menores secuencias $\mathbf{m}$ admisibles formadas por coprimos consecutivos (siempre para un esquema $[3,6]$). Como esperabamos, los elementos de estas secuencias son del mismo orden que Δ. En concreto obtenemos:

$$\begin{aligned}
\Delta = 10, &\quad \mathbf{m} = 21,22,23,25,29,31\\
\Delta = 100, &\quad \mathbf{m} = 112,113,115,117,121,127\\
\Delta = 1000, &\quad \mathbf{m} = 1011,1012,1013,1015,1019,1021\\
\Delta = 10000, &\quad \mathbf{m} = 10011,10012,10013,10015,10019,10021\\
\Delta = 100000, &\quad \mathbf{m} = 100015,100016,100017,100019,100021,100027.
\end{aligned}$$

Para este experimento hemos elegido un esquema $[3,6]$, con umbral igual a la mitad de los participantes, no sólo porque esos eran los datos de nuestro ejemplo, sino que también de cara al siguiente resultado.

Proposición 3.1.2. *Sea* $\mathbf{m} : m_1 < \cdots < m_n$ *una secuencia de n números enteros positivos cualesquiera. Si* $m_{n-t^*+2}\cdots m_n < m_1 \cdots m_{t^*}$ *para algún* $t^* \geq \lceil n/2 \rceil$*, entonces se verifica que* $m_{n-t+2}\cdots m_n < m_1 \cdots m_t$ *para todo t,* $1 < t < n$*.*

Demostración. Supongamos primero que $t^* = \lceil n/2 \rceil$ Si n es par, entonces $t^* = n/2$ y $n - t^* + 2 = t^* + 2$ y los m_i verifican $m_{t^*+2}\cdots m_n < m_1 \cdots m_{t^*}$. Si $t > t^*$, por la condición $m_1 < m_2 < \cdots < m_n$, se tiene $m_{n-t+2}\cdots m_{t^*+1} < m_{t^*+1}\cdots m_t$ (en ambos casos hay $t - t^*$ factores que corresponden a m_i consecutivos). Multiplicando las dos desigualdades obtenemos $m_{n-t+2}\cdots m_n < m_1 \cdots m_t$. Si $t < t^*$, dividiendo los dos términos de la desigualdad $m_{t^*+2}\cdots m_n < m_1 \cdots m_{t^*}$ entre $m_{t^*+2}\cdots m_{n-t+1}$ obtenemos

$$m_{n-t+2}\cdots m_n < m_1 \cdots m_t \frac{m_{t+1}}{m_{t^*+2}} \cdots \frac{m_{t^*}}{m_{n-t+1}} < m_1 \cdots m_t.$$

Si n es impar entonces $n - t^* + 2 = t^* + 1$ y un razonamiento análogo al anterior prueba el resultado. Finalmente, si $t^* > \lceil n/2 \rceil$, entonces los productos $m_{n-t^*+2}\cdots m_n$ y $m_1 \cdots m_t^*$ poseen $2t - n - 1$ factores m_i comunes. Tras simplificar estos factores en los dos términos, nos encontramos en el caso $t = \lceil n/2 \rceil$ anteriormente visto. □

En consecuencia, si una secuencia $\mathbf{m} : m_1 < \cdots < m_n$ satisface la condición de Mignotte para algún $t^* \geq \lceil n/2 \rceil$, entonces la satisface para todo t, y puede ser utilizada para la fabricación de cualquier esquema umbral sobre n participantes.

3.1.4. El esquema umbral de Mignotte para módulos no coprimos

Podemos extender el esquema de Mignotte utilizando la versión general en congruencias del teorema Chino de los restos sobre $\mathbb{Z}$, que no requiere que los módulos sean coprimos dos a dos **teorema 2.3.9**. Esta extensión fue primeramente sugerida en [15].

Sean n,t, dos enteros, $1 < t < n$. Dada una secuencia creciente $\mathbf{m} : m_1 < \cdots < m_n$ de enteros positivos, para $C \subseteq \{1,\ldots,n\}$ escribimos $\text{mcm}(C) = \text{mcm}(m_i |\ i \in C)$ y

definimos

$$\begin{aligned} \mathbf{m}_{t-1}^{+} &= \text{máx}\{\text{mcm}(B) \mid B \subseteq \{1,\ldots,n\}, |B| = t-1\}, \\ \mathbf{m}_{t}^{-} &= \text{mín}\{\text{mcm}(A) \mid A \subseteq \{1,\ldots,n\}, |A| = t\}. \end{aligned}$$

Diremos que la secuencia $\mathbf{m}$ satisface la condición generalizada t de Mignotte si $\mathbf{m}_{t-1}^{+} < \mathbf{m}_{t}^{-}$. Claramente esta condición generalizada es equivalente a la condición usual de Mignotte cuando los m_i son coprimos. Pero como esta condición de coprimos ahora ya no se exige, podemos usar una mayor variedad de secuencias $\mathbf{m}$ en el esquema generalizado que en el original.

Tanto el funcionamiento del esquema como su análisis resultan análogos al caso original. Dada una secuencia $\mathbf{m}$ que satisfaga la condiciñon generalizada t de Mignotte, y dado un secreto s del espacio de secretos $\mathbf{m}_{t-1}^{+} < s < \mathbf{m}_{t}^{-}$, el gestor calcula las participaciones de cada i , $s_i = s \pmod{m_i}$, $i = 1,\ldots,n$. Una coalición autorizada $A \subseteq \mathscr{P}$, con al menos t participantes, recupera s resolviendo el sistema en congruencias

$$(S_A): \quad x \equiv s_i \pmod{m_i} \qquad i \in A.$$

No necesitamos preocuparnos por si este sistema posee solución (que es la parte complicada del teorema Chino en su version general): naturalmente que en este caso la tiene puesto que s lo verifica. La parte que nos interesa del teorema es que asegura la unicidad de la solución x de (S_A) módulo $\text{mcm}(A)$. Como $s < \mathbf{m}_{t}^{-} \leq \text{mcm}(A)$, deducimos que $s = x$. Para una coalición no autorizada B, como $\text{mcm}(B) < t$, el sistema (S_B) proporciona una solución $x < \text{mcm}(B) < s$, luego $x \neq s$.
La mayor dificultad de este método generalizado parece hayarse en encontrar nuevas secuencias admisibles $\mathbf{m}$ que no lo fueran ya para el esquema original (o múltiplos de éstas, $dm_1,\ldots,dm_n$). Al realizar experimentos numéricos con ayuda de computadora observamos, sin embargo, que estas secuencias son extraordinariamente abundantes (si bien no hemos encontrado ningua caracterización 'operativa' para ellas). En particular, estos experimentos nos sugieren aventurarnos a sugerir la siguiente **conjetura**:

Para cada par (t,n), $1 < t < n$, existe un entero $M(t,n)$ tal que para todo $m_1 > M(t,n)$, la secuencia $m_1, m_1+1,\ldots,m_1+n-1$, de n enteros consecutivos, satisface la condición generalizada t de Mignotte. Incluso, también mediante experimentos por computadora, hemos calculado candidatos para algunos de estos $M(t,n)$ para valores pequeños, obteniendo:

$$M(3,6) = 20, M(4,6) = 100, M(3,7) = 19, M(4,7) = 114, M(3,8) = 20, M(4,8) = 798.$$

3.1.5. Un ejemplo del esquema umbral de Mignotte para módulos no coprimos

Pongamos de nuevo que queremos fabricar un esquema umbral de tipo $(6,3)$. Tomemos la secuencia $\mathbf{m}$ definida por

$$m_1 = 1001,\ m_2 = 1002,\ m_3 = 1003,\ m_4 = 1004,\ m_5 = 1005,\ m_6 = 1006$$

para los que $\mathbf{m}_2^{+} = 1011030$, $\mathbf{m}_3^{-} = 168506340$ y se satisface por tanto la condición generalizada de Mignotte con $t = 3$. Esta elección conduce al espacio de secretos

$$\mathscr{S} = \{s \in \mathbb{Z} \mid 1011030 < s < 168506340\}.$$

Se reparte el secreto $s = 777777$. Las participaciones son $s_1 = 20$, $s_2 = 225$, $s_3 = 452$, $s_4 = 681$, $s_5 = 912$, $s_6 = 139$. Si la coalición autorizada $A = \{2,3,4\}$ quiere recuperar el secreto, resuelve el sistema

$$\begin{cases} x \equiv 225 \pmod{1002} \\ x \equiv 452 \pmod{1003} \\ x \equiv 681 \pmod{1004} \end{cases}$$

cuya única solución módulo $\text{mcd}(1002,1003,1004) = 504513012$ es $x = 777777$. Si la coalición no autorizada $B = \{2,4\}$ quiere recuperar el secreto, puede resolver el sistema

$$\begin{cases} x \equiv 237 \pmod{1002} \\ x \equiv 683 \pmod{1004} \end{cases}$$

cuya única solución módulo $\text{mcm}(1002,1004) = 503004$ es $x = 274773 \neq s$. Por tanto esta coalición no recupera el secreto pero deduce que $s = 274773 + 503004\lambda$, para algún λ. Esta condición le permite reducir el espacio $\mathscr{S}$ a $\lfloor (167495310-1)/503004 \rfloor = 333$ valores de s posibles. Concluimos que para lograr el mismo nivel de seguridad que pedimos en el sistema de Mignotte original, es preciso incrementar el tamaño de los modulos m_i (lo que era de esperar, ya que ahora estos no son primos entre sí).

3.2. Esquemas umbral de Asmuth-Bloom

La segunda familia de esquemas de reparto de secretos basada en el teorema Chino de los restos, fue desarrollada por C. Asmuth y J. Bloom, de forma independiente y prácticamente simultánea a la de Mignotte.

3.2.1. El esquema de Asmuth-Bloom original

Exponemos ahora el esquema de Asmuth-Bloom. Este se basa en los mismos principios que el Mignotte, pero permite aumentar su seguridad haciendo menos directa la relación entre el secreto repartido y las participaciones deducidas a partir de este, manteniendo el reducido tamaño de estas. Otra ventaja de este método es que nos permite fijar de antemano el tamaño del espacio de secretos.

Sean $1 < t < n$ el umbral y el cardinal del conjunto de participantes del esquema que deseamos fabricar. Tomemos una secuencia de enteros $\mathbf{m} : m_0 < m_1 < \cdots < m_n$, coprimos dos a dos, m_0 primo, y verificando $m_0 m_{n-t+2} \cdots m_n < m_1 \cdots m_t$. El esquema de Asmuth-Bloom permite repartir un secreto del conjunto $\mathscr{S} = \{s \in \mathbb{Z} \,|\, 0 \leq s < m_0\}$ entre los n participantes como sigue: dado el secreto $s \in \mathscr{S}$

• el gestor elige al azar un entero positivo a con $m_{n-t+2} \cdots m_n / m_0 < a < m_{n-t+2} \cdots m_n$. La participación de i es $s_i = s + a m_0 \pmod{m_i}$, $i = 1, \ldots, n$;
• una coalición $A \subset \mathscr{P}$ de t o más participantes puede recuperar s resolviendo el sistema en congruencias

$$(S_A): \quad x \equiv s_i \pmod{m_i} \qquad i \in A,$$

y reduciendo la única (módulo m_A) solución obtenida, $s = x \pmod{m_0}$.

Proposición 3.2.1. *El método descrito es correcto y proporciona un esquema umbral de tipo (n,t) débilmente perfecto.*

Demostración. Nótese en primer lugar que $m_{n-t+2}\cdots m_n/m_0 < a < m_{n-t+2}\cdots m_n$ y $0 \leq s < m_0$ implican que $m_{n-t+2}\cdots m_n < s+am_0 < (a+1)m_0 \leq m_0 m_{n-t+2}\cdots m_n < m_1\cdots m_t$.

Veamos primero que el esquema es correcto, es decir que las coaliciones autorizadas, y sólo ellas, recuperan el secreto. Sea $A \subseteq \mathscr{P}$ una coalición autorizada, $|A| \geq t$. Resolviendo el sistema (S_A) los participantes de esa coalición encuentran una solución x módulo $m_A \geq m_1\cdots m_t$. Como ambas x y $s+am_0$ son soluciones, y ambas verifican $x, s+am_0 < m_A$, la unicidad de la solución que garantiza el teorema Chino implica que $x = s+am_0$, con lo que $s = x \pmod{m_0}$ y A recupera el secreto.

Veamos ahora que una coalición no autorizada no recupera el secreto. Sea B no autorizada, $|B| \leq t-1$, luego $m_B \leq m_{n-t+2}\cdots m_n$ ya que $m_1 < m_2 < \cdots < m_n$. Resolviendo el sistema (S_B) los participantes de esa coalición encuentran una solución x única módulo m_B. Como $x < m_B \leq m_{n-t+2}\cdots m_n < s+am_0$, deducimos que $x \neq s+am_0$ y la coalición B no recupera el secreto.

Veamos finalmente que el esquema es débilmente perfecto, es decir, que la coalición no autorizada B no puede descartar ningún elemento de $\mathscr{S}$ como posible secreto repartido. Resolviendo el sistema (S_B) los participantes de esa coalición encuentran una solución x módulo m_B. Como $s+am_0 \pmod{m_B}$ es también solución del sistema (S_B), y ésta es única, se verifica que $s+am_0 = x+\lambda m_B$ para algún entero $\lambda \geq 0$ tal que $x+\lambda m_B \leq m_1\cdots m_t$. Como $m_B \leq m_{n-t+2}\cdots m_n$ ya que B no está autorizado, por las condiciones impuestas a los m_i se verifica que $m_0 m_B \leq m_0 m_{n-t+2}\cdots m_n < m_1\cdots m_t$. En consecuencia, como $x < m_B$, para todo $0 \leq \lambda < m_0$ el número $x+\lambda m_B$ satisface $0 \leq x+\lambda m_B \leq m_B+(m_0-1)m_B = m_0 m_B < m_1\cdots m_t$, luego $x+\lambda m_B$ es un posible secreto. Además, como $\mathrm{mcd}(m_0, m_B) = 1$ (ya que los m_i son coprimos), todos estos posibles secretos son distintos: en efecto, si $x+\lambda m_B \equiv x+\mu m_B \pmod{m_0}$, entonces $m_0|(\lambda-\mu)m_B$, de donde $m_0|(\lambda-\mu)$ y como $0 \leq \lambda-\mu < m_0$, necesariamente $\lambda-\mu = 0$. Por tanto, para B existen tantos posibles secretos . Como estas son al menos m_0, hay tantos secretos posibles para la coalición B como elementos existen en el espacio de secretos, m_0. Es decir, todos los secretos del espacio son compatibles con lo que sabe B. El esquema es pues débilmente perfecto. □

Nota 3.2.2. (1) El esquema de Asmuth-Bloom es débilmente perfecto pero no fuertemente perfecto. En [26] se demuestra que, según la elección de los m_i, algunas coaliciones no autorizadas pueden deducir variaciones significativas entre las probabilidades de los $s \in \mathscr{S}$ de ser los auténticos secretos repartidos. Veremos un ejemplo de esta situación un poco más adelante, en la **subsección 3.2.3**. En el mismo trabajo [26] se introducen los conceptos de *asintóticamente perfecto* y *asintóticamente ideal*, y se demuestra que cuando los módulos son primos consecutivos, los esquemas obtenidos son asintóticamente perfectos e ideales.
(2) Obsérvese también que la condición de que m_0 sea primo no es necesaria. En efecto, esta condición se utiliza únicamente para asegurar que $\mathrm{mcd}(m_0, m_A) = 1$ en la demostración, para lo que es suficiente que los $m_0, m_1, \ldots, m_n$ sean coprimos dos a dos. La hemos matenido en la descripción del método para ser fieles a su formulación original, pero la omitiremos a partir de ahora.

El tamaño del espacio de secretos es $|\mathscr{S}| = m_0$ y el de las participaciones es

$|\mathscr{S}_i| = m_i$. Por tanto, la tasa de información del esquema es $\rho = \log(m_0)/\log(m_n)$. Si todos los m_i pudieran tomarse del mismo orden, el esquema sería ideal.

3.2.2. El esquema de Asmuth-Bloom modificado

En su tesis doctoral [20], [19], K. Kaya propone un pequeño cambio en las condiciones impuestas sobre los m_i del esquema de Asmuth-Bloom, que hace que este sea casi fuertemente perfecto. En concreto, supondremos ahora que los $m_0 < m_1 < \cdots < m_n$ son coprimos dos a dos (sin necesidad de que m_0 sea primo) y que se verifica $m_0^2 m_{n-t+2} \cdots m_n < m_1 \cdots m_t$. El resto del esquema permanece como en su formulación original, expuesta en la sección anterior.

Proposición 3.2.3. *Si $m_0^2 m_{n-t+2} \cdots m_n < m_1 \cdots m_t$, el método de Asmuth-Bloom proporciona un esquema umbral de tipo (n,t) que es aproximadamente fuertemente perfecto.*

Demostración. Si $m_0^2 m_{n-t+2} \cdots m_n < m_1 \cdots m_t$ etonces $m_0 m_{n-t+2} \cdots m_n < m_1 \cdots m_t$ y todos los razonamientos de la demostracion de la Proposición 3.2.1 siguen siendo válidos. Veamos pues que el esquema está próximo a ser fuertemente perfecto. Sea B una coalición no autorizada, $|B| < t$. Como ya vimos, resolviendo el sistema (S_B) los participantes de esa coalición encuentran una solución x única módulo m_B. Como $s + am_0 \pmod{m_B}$ es también solución del sistema, y ésta es única, se verifica que $s + am_0 = x + \lambda m_B$ para algún entero $\lambda \geq 0$ tal que $x + \lambda m_B \leq m_1 \cdots m_t$. Calculemos para cuantos λ se cumple esta desigualdad. Si $\lambda < (m_1 \cdots m_t)/m_B$, entonces $1 + \lambda \leq (m_1 \cdots m_t)/m_B$, y como $x < m_B$ se tiene $x + \lambda m_B < (1+\lambda) m_B \leq m_1 \cdots m_t$. Recíprocamente, si $\lambda \geq (m_1 \cdots m_t)/m_B$, entonces $x + \lambda m_B \geq m_1 \cdots m_t + x$. Por tanto, en promedio la coalición B debe considerar $m_1 \cdots m_t / m_B$ valores posibles de λ. Nótese que las condiciones $m_0^2 m_{n-t+2} \cdots m_n < m_1 \cdots m_t$ y $m_B \leq m_{n-t+2} \cdots m_n$, conjuntamente implican que $m_0^2 m_B < m_1 \cdots m_t$, luego que $(m_1 \cdots m_t)/m_B > m_0^2$. Es decir, existen muchos valores de λ que proporcionan posibles secretos.

Siendo $m_0, m_1, \ldots, m_n$ coprimos, se mantiene la propiedad $\text{mcd}(m_0, m_B) = 1$, y como en la demostración de la Proposición 3.2.1, los $x + \lambda m_B \pmod{m_0}$ toman todos los valores de $\mathbb{Z}/m_0\mathbb{Z}$. Dados dos de esos valores, $0 \leq \lambda, \mu < (m_1 \cdots m_t)/m_B$, se verifica que $x + \lambda m_B \equiv x + \mu m_B \pmod{m_0}$ si y sólo si $m_0 | \lambda - \mu$. Por tanto, en promedio cada valor de $\mathbb{Z}/m_0\mathbb{Z}$ se alcanza de la forma $x + \lambda m_B \pmod{m_0}$ para $(m_1 \cdots m_t)/(m_0 m_B)$ valores de λ, y el esquema es (aproximadamente) fuertemente perfecto. □

Naturalmente, la ganancia en el carácter perfecto se hace a costa de perder en su tasa de información. Si, de nuevo, suponemos que todos los m_i son del mismo orden, $m_i \sim m$, la condición $m_0^2 m_{n-t+2} \cdots m_n < m_1 \cdots m_t$ implica $m_0^2 m^{t-1} < m^t$ luego $m_0 = |\mathscr{S}| < \sqrt{m}$ y la tasa del esquema es $\rho = \log(m_0)/\log(m) < \log(\sqrt{m})/\log(m) = 1/2$.

3.2.3. Un ejemplo

Como en el ejemplo tratado en la sección 3.1.2, volvamos al problema combinatorio (PC): seis científicos desean fabricar un esquema umbral de tipo $(6,3)$ con un espacio de secretos de tamaño 1000. Tomemos así $m_0 = 1013$ (que es primo). Digamos también que secreto a repartir (la clave de la cerradura del armario) es $s = 777$.

Seguimos primero el esquema de **Asmuth-Bloom original**. Para ello el gestor del esquema elige los módulos m_i. Pongamos que ha elegido

$$m_0 = 1013,\ m_1 = 1021,\ m_2 = 1031,\ m_3 = 1033,\ m_4 = 1034,\ m_5 = 1035, m_6 = 1037,$$

(como se ve, todos del mismo orden que m_0). A continuación el gestor elige (al azar) el entero $a = 201920$ y calcula la participación de cada i, que es $s_i = s + am_0 \pmod{m_i} = 204545737 \pmod{m_i}$, $i = 1, \ldots, n$,

$$s_1 = 639,\ s_2 = 492,\ s_3 = 374,\ s_4 = 891,\ s_5 = 757,\ s_6 = 598.$$

Reunida la coalición autorizada $A = \{2,3,4\}$, resuelven el sistema de ecuaciones en congruencias

$$\begin{cases} x \equiv 492 \pmod{1031} \\ x \equiv 374 \pmod{1033} \\ x \equiv 891 \pmod{1034} \end{cases}$$

cuya única solución módulo 1101233782 es $x = 204545737$. La coalición recupera el secreto como $s = \mod(1013) = 777$.

Una coalición no autorizada $B = \{2,3\}$ no puede recuperar el secreto $s = 777$, pero sí puede deducir distintas probabilidades de serlo entre los elementos de $\mathbb{Z}/1013\mathbb{Z}$. En concreto, calculando puede obtenerse que algunos elementos de $\mathbb{Z}/1013\mathbb{Z}$ son el doble de probables que otros como candidatos a ser el auténtico secreto s, y el esquema está lejos de ser fuertemente perfecto.

Mostremos ahora el esquema de **Asmuth-Bloom modificado**. Manteniendo el mismo cardinal del conjunto de secretos posibles, $m_0 = 1013$, el tamaño de los módulos m_i (es decir, el número de dígitos que los forman) se incrementa en aproximadamente el doble, ya que imponemos $m_0^2 m_{n-t+2} \cdots m_n < m_1 \cdots m_t$. Tras una búsqueda por computadora, los más pequeños que hemos encontrado verificando esta condición son

$$\begin{aligned} m_1 = 1026197, &\quad m_2 = 1026199, \quad m_3 = 1026217, \\ m_4 = 1026218, &\quad m_5 = 1026219, \quad m_6 = 1026221. \end{aligned}$$

Manteniendo los mismos valores del secreto $s = 777$ y el coeficiente $a = 201920$ que en el caso anterior, las participaciones son ahora

$$\begin{aligned} s_1 = 332534, &\quad s_2 = 332136, \quad s_3 = 328554, \\ s_4 = 328355, &\quad s_5 = 328156, \quad s_6 = 328554, \end{aligned}$$

de nuevo de tamaño el doble del secreto (y muy similares entre sí puesto que también lo son los módulos m_i). No nos detenemos a mostrar como se recupera el secreto, puesto que es absolutamente análogo al caso anterior. Simplemente notamos que la misma coalición no autorizada que antes, $B = \{2,3\}$, no puede recuperar el secreto, pero sí puede seguir deduciendo distintas probabilidades en los elementos de $\mathbb{Z}/1013\mathbb{Z}$ de serlo. Pero ahora la relación entre probabilidades más altas y más bajas es

$$R = \frac{1014}{1013} \approx 1{,}001$$

muy próxima a 1, mejora que hemos obtenido al precio de duplicar el tamaño de todos los datos.

3.3. Estructuras umbral ponderadas

En las estructuras de acceso umbral, todos los participantes juegan un papel equivalente. Sin embargo, en algunas aplicaciones de los esquemas de reparto, puede desearse que algunos participantes tengan un papel más relevante que otros (por ejemplo si el secreto se reparte entre diferentes cargos de una compañía). Para responder a esta necesidad surgen las estructuras ponderadas.

3.3.1. Pesos y estructuras ponderadas

Dado un conjunto de participantes $\mathscr{P} = \{1, \ldots, n\}$, un *vector de pesos* sobre $\mathscr{P}$ es una n-upla $\mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{Z}^n$ de enteros positivos. Dados un tal vector $\mathbf{w}$ y un umbral $t \in \mathbb{Z}$, se llama *estructura umbral ponderada* de tipo $(\mathbf{w}, t, n)$ a la estructura de acceso

$$\mathscr{A} = \{A \subseteq \mathscr{P} \,|\, \mathbf{w}(A) \geq t\}$$

siendo $\mathbf{w}(C) = \sum_{i \in C} w_i$. El problema de construir esquemas que realicen estas estructuras fue tambien abordado por Shamir quien sugiere la solución obvia: dar a cada participante tantas participaciones como indica su peso. Esta solución contradice el principio de que cada participante recibe una única participación. Los esquemas umbral basados en el teorema chino pueden ser usados también en este problema y solventar este incoveniente, realizando una estructura umbral ponderada y asignando una sola participación a cada participante.

Para no ser reiterativos en los argumentos, en esta sección y en la siguiente, nos limitaremos a considerar esquemas de tipo Mignotte.

3.3.2. Estructuras umbral ponderadas de Mignotte

Proposición 3.3.1. *Toda estructura umbral ponderada puede ser realizada mediante un esquema de Mignotte con módulos m_i coprimos dos a dos.*

El método para encontrar el esquema de Mignotte que realiza una estructura umbral ponderada, que es bastante evidente, se sugiere de forma confusa en [17] y [16] Sección 2.4. Vamos a describirlo a continuación, completando las demostraciones matemáticas que se omiten en esos trabajos. Para ello utilizaremos el **lema 2.3.8.**

Demostración de la Proposición. Queremos construir un esquema de reparto $\mathscr{R}$ que realice la estructura de acceso $\mathscr{A}$ ponderada de tipo $(\mathbf{w}, t, n)$ sobre $\mathscr{P}$. Sea $N = \mathbf{w}(\mathscr{P})$ la suma de todos los pesos. Vamos a utilizar una estructura umbral auxiliar $\mathscr{A}'$ de tipo (t, N), sobre un conjunto $\mathscr{P}'$ con N participantes. Cada participante i de $\mathscr{P}$ está asociado a w_i participantes $i_1, \ldots, i_{w_i}$ en $\mathscr{P}'$, y correspondientemente cada agrupación $C \subseteq \mathscr{P}$ está asociada a una agrupación $C' = \cup_{i \in C} \{i_1, \ldots, i_{w_i}\}$ de $\mathscr{P}'$.

Por los resultados de las secciones anteriores, la estructura $\mathscr{A}'$ sobre $\mathscr{P}'$ puede realizarse mediante un esquema umbral $\mathscr{R}'$ proveniente de una secuencia de N módulos coprimos $\mathbf{m}' : m'_{1,1}, \ldots, m'_{1,w_1}; \ldots; m'_{n,1}, \ldots, m'_{n,w_n}$. Una coalición $A' \subseteq \mathscr{P}'$ está autorizada por $\mathscr{R}'$ si y sólo si $|A'| \geq t$.

Detallemos como es el esquema de reparto $\mathscr{R}$ que realiza la estructura de acceso ponderada $\mathscr{A}$ sobre $\mathscr{P}$. Para $i = 1, \ldots, n$, sea $m_i = m'_{i,1}, \ldots, m'_{i,w_i}$, factorización que conoce

el participante i. El conjunto de secretos a repartir es el mismo que el del esquema auxiliar $\mathscr{R}'$. Dado un secreto s válido, las participaciones de s según $\mathscr{R}$ son los n números $s_i = s \pmod{m_i}$. Una coalición C quiere recuperar el secreto. Para ello resuelve el sistema

$$(S_C) \qquad x \equiv s_i \pmod{m_i} \qquad i \in C$$

que según el Lema anterior será equivalente al sistema:

$$(S'_C) \qquad x \equiv s_i \pmod{m'_{i,j}} \qquad i \in C,\ j = 1, \ldots, w_i$$

y este corresponde al esquema umbral $\mathscr{R}'$. Como los sistemas son equivalentes, C recupera el secreto con (S_C) si y sólo si C' lo recupera con (S'_C). Pero, siendo $\mathscr{R}'$ umbral (t,N), esto sucede si $|C'| \geq t$. Como $|C'| = \mathbf{w}(C)$, el esquema $\mathscr{R}$ realiza la estructura ponderada $\mathscr{A}$, como queríamos demostrar. □

3.3.3. Un ejemplo

Vamos a realizar una estructura umbral ponderada de tipo $((2,2,1,1),3,4)$, es decir, una estructura sobre 4 participantes con pesos 2,2,1,1, de manera que recupere el secreto cualquier coalición con peso al menos 3. Para ello usamos una estructura umbral auxiliar sobre $2+2+1+1=6$ participantes, de umbral 3. Como sabemos, esta estructura auxiliar la podemos realizar mediante 6 módulos coprimos, de manera que el producto de 3 cualesquiera de ellos sea siempre mayor que el producto de 2 cualesquiera de ellos. Por ejemplo, siguiendo las notaciones anteriores, tomemos

$$m'_{11} = 101,\ m'_{12} = 103,\ m'_{21} = 107,\ m'_{22} = 109,\ m'_3 = 113,\ m'_4 = 114.$$

El producto de dos cualesquiera de estos números es 12882 a lo más, mientras que el producto de tres cualesquiera de ellos es a lo menos 1113121. Los secretos a repartir son los enteros s tales que $12882 < s < 1113121$. Los módulos de los cuatro participantes en la estructura ponderada son

$$m_1 = m'_{11}m'_{12} = 10403,\ m_2 = m'_{21}m'_{22} = 11663,\ m_3 = m'_3 = 113,\ m_4 = m'_4 = 114.$$

El reparto y la recuperación del secreto se llevan a cabo como siempre. Dado el secreto $s = 77777$, las participaciones son $s_i = s \pmod{m_i}$, es decir

$$s_1 = 4956,\ s_2 = 7799,\ s_3 = 33,\ s_4 = 29.$$

La coalición autorizada $\{1,3\}$ quiere resuperar el secreto. Para ello resuelve el sistema

$$\begin{cases} x \equiv 4956 \pmod{10403} \\ x \equiv 33 \pmod{113} \end{cases}$$

cuya solución es $77777 = s$. Nótese que este sistema de ecuaciones es equivalente al sistema auxiliar

$$\begin{cases} x \equiv 4956 \pmod{101} \\ x \equiv 4956 \pmod{103} \\ x \equiv 33 \pmod{113} \end{cases}$$

que corresponde a una coalición de tres participantes en el esquema umbral auxiliar $(3,6)$, lo que garantiza que la recuperación del secreto es correcta. Si la coalición no autorizada $\{3,4\}$ quiere resuperar el secreto, puede resolver

$$\begin{cases} x \equiv 33 \pmod{113} \\ x \equiv 29 \pmod{114} \end{cases}$$

cuya solución es $485 \neq s$.

3.4. El esquema de Mignotte para estructuras de acceso generales

En las estructuras de acceso umbral todos los participantes juegan un papel similar. Sin embargo, las corporaciones 'humanas' a las que estos sistemas se aplican suelen ser más complejas, con participantes organizados en una estructura de conveniencia. Esto obliga a considerar en muchos casos estructuras de acceso no umbral. Cuando la estructura de acceso esta determinada simplemente ponderando la importancia de cada participante mediante un peso, podemos aplicar los resultados de la sección anterior. Sin embargo esto no agota las posibilidades, es decir, existen estructuras de acceso que no son umbral ponderadas. El siguiente ejemplo procede de [2].

Ejemplo 3.4.1. Consideremos la estructura de acceso $\mathscr{A}$ sobre cuatro participantes que tiene como agrupaciones autorizadas minimales a $\{1,2\}$ y $\{3,4\}$. Si $\mathscr{A}$ fuera una estructura umbral ponderada respecto de los pesos w_1, w_2, w_3, w_4 y el umbral t, se verificaría $w_1 + w_2 \geq t, w_3 + w_4 \geq t$, luego $w_1 + w_2 + w_3 + w_4 \geq 2t$. Por tanto, o bien $w_1 + w_3 \geq t$ o bien $w_2 + w_4 \geq t$. Pero ni $\{1,3\}$ ni $\{2,4\}$ están en $\mathscr{A}$.

3.4.1. Estructuras de acceso generales

Como mencionamos al comienzo del capítulo, en general una estructura de acceso sobre un conjunto $\mathscr{P}$ con n participantes es cualquier familia $\mathscr{A} \subseteq 2^{\mathscr{P}}$ que sea monótona, es decir, verificando que si $A \subset A'$ y $A \in \mathscr{A}$, entonces también $A' \in \mathscr{A}$. Claramente, una estructura de este tipo queda unívocamente determinada por sus elementos minimales. Denotamos por $\mathscr{A}_0$ el conjunto de estas agrupaciones autorizadas minimales, y nos referimos a $\mathscr{A}_0$ como *base* de $\mathscr{A}$.

El conjunto de agrupaciones no autorizadas se denota habitualmente por $\overline{\mathscr{A}}$, es decir $\overline{\mathscr{A}} = 2^{\mathscr{P}} \setminus \mathscr{A}$. Similarmente a lo que ocurre con $\mathscr{A}$, $\overline{\mathscr{A}}$ queda completamente determinado por el conjunto de las agrupaciones no autorizadas maximales.

La extensión del esquema de Mignotte para módulos no necesariamente coprimos sugiere directamente otra extensión del método para estructuras cualesquiera. Un proceso análogo podría hacerse también para el esquema de Asmuth-Bloom. Como hicimos en la sección 3.3.2, para no ser reiterativos en las argumentaciones, nos centraremos en los esquemas de tipo Mignotte.

3.4.2. De secuencias a estructuras

Sean $\mathscr{P}$ un conjunto de n participantes y $\mathbf{m} : m_1, \ldots, m_n$, una secuencia de n enteros positivos distintos. Ordenemos el conjunto $\{\text{mcm}(C) \,|\, C \subseteq \mathscr{P}\}$ de manera creciente

y tomemos dos enteros $\mathbf{m}^+, \mathbf{m}^-$ tales que el intervalo $(\mathbf{m}^+, \mathbf{m}^-)$ no contenga ningún elemento del conjunto anterior, es decir, tal que para toda coalición C, o bien $\text{mcm}(C) \leq \mathbf{m}^+$ o bien $\text{mcm}(C) \geq \mathbf{m}^-$. En estas condiciones podemos asociar a $\mathbf{m}$ y $\mathbf{m}^+$ la estructura de acceso sobre $\mathscr{P}$

$$\mathscr{A} = \mathscr{A}(\mathbf{m}, \mathbf{m}^+) = \{A \subseteq \mathscr{P} \,|\, \text{mcm}(A) \geq \mathbf{m}^-\}.$$

Efectivamente, $\mathscr{A}$ es monótona y no vacía si $\text{mcm}(\mathscr{P}) \geq \mathbf{m}^-$. La descripción del esquema de reparto para esta estructura, y su análisis, son similares a los vistos para el método de Mignotte habitual: el conjunto de secretos es $\mathscr{S} = \{s \in \mathbb{Z} \,|\, \mathbf{m}^+ < s < \mathbf{m}^-\}$. Un secreto s de este espacio conduce a las participaciones $s_i = s \,(\text{mod}\, m_i)$, $i = 1, \ldots, n$. Una coalición C de participantes puede intentar recuperar el secreto encontrando la solución x del sistema de ecuaciones

$$x \equiv s_i \,(\text{mod}\, m_i) \quad i \in C.$$

Si $C \in \mathscr{A}$ entonces $s < \mathbf{m}^- \leq \text{mcm}(C)$ y $x = s$. Si $C \notin \mathscr{A}$ entonces $\text{mcm}(C) \leq \mathbf{m}^+ < s$ y $x \neq s$.

Ejemplo 3.4.2. En el Ejemplo 3.4.1 mostramos que la estructura de acceso con base $\mathscr{A}_0 = \{\{1,2\},\{3,4\}\}$ no puede ser ponderada. Sin embargo sí es obtenida por el método que acabamos de describir, con la secuencia de módulos $\mathbf{m} : 5, 12, 8, 9$, y la elección $\mathbf{m}^+ = 45, \mathbf{m}^- = 60$. Para comprobalo examinemos todas las coaliciones de dos participantes

$$\begin{aligned}
\text{mcm}(m_1, m_2) = \text{mcm}(5,12) = 60 &\quad \text{luego la coalición } \{1,2\} \text{ está autorizada;} \\
\text{mcm}(m_1, m_3) = \text{mcm}(5,8) = 40 &\quad \text{luego la coalición } \{1,3\} \text{ no está autorizada;} \\
\text{mcm}(m_1, m_4) = \text{mcm}(5,9) = 45 &\quad \text{luego la coalición } \{1,4\} \text{ no está autorizada;} \\
\text{mcm}(m_2, m_3) = \text{mcm}(12,8) = 24 &\quad \text{luego la coalición } \{2,3\} \text{ no está autorizada;} \\
\text{mcm}(m_2, m_4) = \text{mcm}(12,9) = 36 &\quad \text{luego la coalición } \{2,4\} \text{ no está autorizada;} \\
\text{mcm}(m_3, m_4) = \text{mcm}(8,9) = 72 &\quad \text{luego la coalición } \{2,5\} \text{ está autorizada;}
\end{aligned}$$

Mediante un cálculo similar se prueba que ninguna coalición de un solo participante está autorizada, mientras que todas las coaliciones de tres o cuatro participantes están autorizadas. Y por lo tanto, que la estructura de acceso obtenida es exáctamente la deseada.

3.4.3. Estructuras de Mignotte con módulos coprimos

En el **ejemplo 3.4.1** mostramos que la estructura de acceso con base $\mathscr{A}_0 = \{\{1,2\}, \{3,4\}\}$, que no es ponderada, sí puede ser realizada por un esquema de Mignotte con módulos $\mathbf{m} : 5, 12, 8, 9$. Sin embargo, no puede ser realizada por ningún esquema de Mignotte módulos coprimos dos a dos. Estamos ya en disposición de explicar a qué se debe esto.

Proposición 3.4.3. *Sea $\mathscr{A}$ la estructura de acceso realizada mediante el esquema de Mignotte $\mathscr{R}$ con secuencia de módulos $\mathbf{m} : m_1, \ldots, m_n$ y espacio de secretos $\mathscr{S} = \{z \in \mathbb{Z} \mid \mathbf{m}^+ \leq s \leq \mathbf{m}^-\}$. Si los $m_1, \ldots, m_n$ son coprimos dos a dos, entonces $\mathscr{A}$ es una estructura umbral ponderada, con pesos reales.*

Demostración. Una coalición C esta autorizada si y sólo si $\text{mcm}(C) \geq \mathbf{m}^-$. Como los módulos son coprimos dos a dos, esto sucede cuando $\prod_{i \in C} m_i \geq \mathbf{m}^-$, es decir, cuando

$$\sum_{i \in C} \log(m_i) \geq \log(\mathbf{m}^-).$$

Por tanto $\mathscr{A}$ es una estructura ponderada real, con pesos $\log(m_1),\ldots,\log(m_n)$, y umbral $\log(\mathbf{m}^-)$.

A nosotros, no obstante, nos interesa que los pesos y el umbral resulten números enteros. Nos fijamos entonces en que una estructura ponderada de tipo $(\mathbf{w},t,n)$ no cambia al multiplicar $\mathbf{w}$ y t por un coeficiente real positivo d, es decir, $\mathscr{A}$ es $(\mathbf{w},t,n)$ si y sólo si es $(d\mathbf{w},dt,n)$. Sean pues $\mathbf{w}$ y t reales y sea $\mathscr{A}$ de tipo $(\mathbf{w},t,n)$. Según el comentario anterior, podemos suponer $t=1$. Sea $\varepsilon>0$ el número real definido por la igualdad

$$\varepsilon = \text{mín}\{1-\mathbf{w}(B) \mid B\subseteq\mathscr{P},\mathbf{w}(B)<1\}.$$

Para $1\leq i\leq n$, sea w_i' un número racional tal que $w_i\leq w_i'<w_i+(\varepsilon/n)$. Si B es una coalición no autorizada de $\mathscr{A}$, como $|B|\leq n$, se verifica que $\mathbf{w}'(B)<\mathbf{w}(B)+\varepsilon\leq 1$. Recíprocamente, si A está autorizada, entonces $\mathbf{w}'(A)\geq\mathbf{w}(A)\geq 1$. Por tanto $\mathscr{A}$ es también de tipo $(\mathbf{w}',1,n)$. Para transformar ahora los $w_i'\in\mathbb{Q}$ en enteros basta considerar el máximo común múltiplo de todos sus denominadores, d, y $\mathscr{A}$ es de tipo $(d\mathbf{w}',d,n)$

Llegamos de esta forma a que $\mathscr{A}$ es una estructura umbral ponderada con pesos y umbral enteros.

□

4

Esquemas de reparto de secretos sobre $\mathbb{F}_q[X]$

Si $\mathbb{K}$ es un cuerpo, el anillo de polinomios $\mathbb{K}[X]$ comparte algunas importantes propiedades aritméticas con $\mathbb{Z}$, de las cuales la más relevante es la existencia de una división con resto: dados $f(X), g(X) \in \mathbb{K}[X]$ con $\deg(f) \geq \deg(g)$, existen polinomios $q(X), r(X)$, con $r(X) = 0$ o $\deg(r) < \deg(g)$ tales que $f(X) = g(X)q(X) + r(X)$. En otras palabras, $\mathbb{F}_q[X]$ es un dominio euclídeo para la función euclídea 'grado'. Por tanto, también tenemos en $\mathbb{K}[X]$ un algoritmo de Euclides y un teorema Chino de los restos, computable algorítmicamente, análogos a los de $\mathbb{Z}$.

Estas propiedades permiten extender los métodos de reparto de secretos vistos para $\mathbb{Z}$, al anillo $\mathbb{K}[X]$. Además este anillo tiene una propiedad que resultará especialmente favorable para estas extensiones: en contraste con lo que sucede en $\mathbb{Z}$, en $\mathbb{K}[X]$, para cada entero $r > 0$ existen muchos polinomios irreducibles y muchos polinomios coprimos de grado r.

4.1. Polinomios sobre cuerpos finitos

Sea $\mathbb{F}_q$ un cuerpo finito con q elementos. En esta sección daremos fórmulas para los números de polinomios irreducibles y polinomios coprimos de cada grado r en $\mathbb{F}_q[X]$. Las unidades de $\mathbb{F}_q[X]$ son los elementos de $\mathbb{F}_q^*$, por lo que todos los polinomios que consideramos se entenderán mónicos. Los resultados de esta sección proceden de [10]. Un estudio completo de la teoría de polinomios sobre cuerpos finitos puede encontrarse en [22] .

4.1.1. Polinomios irreducibles

Sea $\mathbb{K}$ un cuerpo arbitrario. Un polinomio no constante $f(X) \in \mathbb{K}[X]$ es *irreducible* si no puede descomponerse como producto de dos polinomios no constantes de $\mathbb{K}[X]$. En tal caso el ideal $(f(X)) \subset \mathbb{K}[X]$ es maximal, ya que al ser $\mathbb{K}[X]$ un DIP, la condición $(f(X)) \subseteq (g(X))$ equivale a $f(X) = g(X)q(X)$ para algún polinomio $q(X)$. Por tanto $f(X)$ es irreducible si y sólo si $\mathbb{K}[X]/(f(X))$ es un cuerpo.

Proposición 4.1.1. *Sea a un elemento algebraico sobre $\mathbb{K}$. Existe un único polinomio mónico e irreducible $f(X) \in \mathbb{K}[X]$ tal que $f(a) = 0$. Para todo polinomio $g(X) \in \mathbb{K}[X]$ con $g(a) = 0$, se verifica que $g(X)$ es múltiplo de $f(X)$.*

Demostración. Sea $f(X)$ un polinomio mónico en $\mathbb{K}[X]$ del menor grado posible entre los que tienen a a como raíz. Tal polinomio existe pues a es algebraico sobre $\mathbb{K}$. Claramente $f(X)$ es irreducible, pues si $f(X) = f_1(X)f_2(X)$ entonces a sería raíz de $f_1(X)$ o de $f_2(X)$, que tienen menor grado que $f(X)$. Si $g(X) \in \mathbb{K}[X]$ verifica que $g(a) = 0$, entonces

realizando la división euclídea, $g(X) = f(X)t(X) + h(X)$ con $h(X) = 0$ o $\deg(h(X)) < \deg(f(X))$. Por tanto $0 = g(a) = f(a)t(a) + h(a)$, es decir $h(a) = 0$ y, por la elección de $f(X)$, necesariamente $h(X) = 0$, luego $g(X)$ es múltiplo de $f(X)$. En particular, si $t(X) \in \mathbb{K}$ entonces $g(X)$ no es mónico; si $t(X) \notin \mathbb{K}$ entonces $g(X)$ es reducible. Por tanto $f(X)$ es único con las codiciones anteriores. □

El polinomio $f(X)$ cuya existencia asegura la proposición anterior es el *irreducible* de a sobre $\mathbb{K}$. Obviamente si $a \in \mathbb{K}$, entonces $f(X) = X - a$. A continuación exponemos un resultado que usaremos posteriormente.

Lema 4.1.2. *Sean r,s,t,q cuatro enteros no negativos. Se verifican las siguientes propiedades en $\mathbb{K}[X]$.*
(a) $X^t - 1 = (X-1)(X^{t-1} + \cdots + X + 1)$;
(b) $X^s - 1$ divide a $X^{ts} - 1$;
(c) $X^s - 1$ divide a $X^r - 1$ si y sólo si s divide a r.
(d) $q^s - 1$ divide a $q^r - 1$ si y sólo si s divide a r.
(e) $X^{q^s} - X$ divide a $X^{q^r} - X$ si y sólo si s divide a r.

Demostración. (a) es una simple comprobación. (b) Según el apartado (a) podemos escribir

$$X^{ts} - 1 = (X^s)^t - 1 = (X^s - 1)((X^s)^{t-1} + \cdots + X^s + 1).$$

(c) Realizando la división euclídea, sea $r = st + h$ con $0 \leq h < s$. Entonces

$$X^r - 1 = X^h(X^{ts} - 1) + X^h - 1.$$

Como hemos visto, $X^s - 1$ divide a $X^{ts} - 1$. Por tanto $X^s - 1$ divide a $X^r - 1$ si y sólo si $X^s - 1$ divide a $X^h - 1$. Ahora bien, como $0 \leq h < s$, esto sucede si sólo si $h = 0$, luego si s divide a r. La prueba de (d) es similar a la anterior. (e) Dada la descomposición $X^{q^s} - X = X(X^{q^s-1} - 1)$, deducimos que $X^{q^s} - X$ divide a $X^{q^r} - X$ si si sólo si $X^{q^s-1} - 1$ divide a $X^{q^r-1} - 1$. Según (c) esto sucede si y sólo si $q^s - 1$ divide a $q^r - 1$, y según (d) si y sólo si s divide a r. □

4.1.2. Número de polinomios irreducibles sobre un cuerpo finito

Como $\mathbb{F}_q$ es un cuerpo, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ y según el teorema de Lagrange $a^{q-1} = 1$ para todo $a \in \mathbb{F}_q^*$, o $a^q = a$ para todo $a \in \mathbb{F}_q$. Por tanto $\mathbb{F}_q$ puede verse como el cuerpo de descomposición del polinomio $X^q - X \in \mathbb{F}_p[X]$, siendo p la característica de $\mathbb{F}_q$.

Lema 4.1.3. *Sea $f(X) \in \mathbb{F}_q[X]$ un polinomio irreducible de grado s. Entonces $f(X)$ divide a $X^{q^s} - X$ y por tanto tiene todas sus raices en $\mathbb{F}_{q^s}$.*

Demostración. El anillo cociente $\mathbb{F}_q[X]/(f(X))$ es un cuerpo que contiene la raíz $x = X + (f(X))$ de $f(X)$. Por tanto $f(X)$ es el polinomio irreducible de x sobre $\mathbb{F}_q$. Como $\mathbb{F}_q[X]/(f(X))$ contiene q^s elementos, x también es raíz de $X^{q^s} - X$ luego, según la **Proposición 4.1.1**, se deduce que $f(X) | X^{q^s} - X$. Ahora bien, $X^{q^s} - X$ tiene todas sus raices en $\mathbb{F}_{q^s}$, luego también las tiene $f(X)$. □

Corolario 4.1.4. *Sea $f(X) \in \mathbb{F}_q[X]$ un polinomio irreducible de grado s. Entonces $\mathbb{F}_{q^s} = \mathbb{F}_q[\alpha]$ siendo α una raíz de $f(X)$.*

Demostración. Según el lema anterior $\alpha \in \mathbb{F}_{q^s}$, luego $\mathbb{F}_q[\alpha] \subseteq \mathbb{F}_{q^s}$. Los elementos $1, \alpha, \ldots, \alpha^{s-1}$ del espacio vectorial $\mathbb{F}_q[\alpha]$ sobre $\mathbb{F}_q$, son linealmente independientes, pues una combinación lineal nula de los mismos llevaría a un polinomio con α como raíz de grado menor que s. Así la dimensión de $\mathbb{F}_q[\alpha]$ es al menos s y su cardinal al menos $q^s = |\mathbb{F}_{q^s}|$. Por tanto se da la igualdad $\mathbb{F}_{q^s} = \mathbb{F}_q[\alpha]$. □

Proposición 4.1.5. *Sean s, r dos enteros, $s \leq r$. Sea $f(X) \in \mathbb{F}_q[X]$ un polinomio irreducible de grado s. Entonces $f(X)$ divide a $X^{q^r} - X$ si y sólo si s divide a r.*

Demostración. Si s divide a r entonces $f(X)|(X^{q^s} - X)|(X^{q^r} - X)$ según los lemas anterior y 4.1.2 (e). Recíprocamente, si $f(X)|X^{q^r} - X$ entonces toda raíz α de $f(X)$ lo es también de $X^{q^r} - X$ luego según el corolario anterior $\mathbb{F}_{q^s} = \mathbb{F}_q[\alpha] \subseteq \mathbb{F}_{q^r}$. Por tanto $\mathbb{F}_{q^s}^*$ es un subgrupo de $\mathbb{F}_{q^r}^*$, por lo que $q^s - 1$ divide a $q^r - 1$, y de acuerdo con el apartado (d) del **Lema 4.1.2** concluimos que $s|r$. □

Corolario 4.1.6. *$X^{q^r} - X$ es el producto de todos los polinomios irreducibles sobre $\mathbb{F}_q$ con grado divisor de r.* □

Denotemos por $N_q(r)$ el número de polinomios irreducibles de grado r sobre $\mathbb{F}_q$. Sumando los grados de todos estos polinomios, el corolario anterior implica que

$$q^r = \sum_{s|r} s N_q(s). \tag{1}$$

Es posible despejar el valor de $N_q(r)$ en esta ecuación, dando una fórmula explícita para este valor (suponiendo que conozcamos la factorización de un entero como producto de primos). Para ello usaremos la siguiente herramienta.

Definición 4.1.7. Se llama *función de Moebius* a la función $\mu : \mathbb{Z}_{>0} \to \{-1, 0, 1\}$ definida del modo siguiente: si $n = p_1^{e_1} \cdots p_s^{e_s}$ es la descomposición de n en factores primos, entonces

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1; \\ 0 & \text{si } e_i \geq 2 \text{ para algún } i; \\ (-1)^s & \text{si } e_i = 1 \text{ para todo } i. \end{cases}$$

Lema 4.1.8. *Sea $n \in \mathbb{Z}_{>0}$. Se verifica que*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1; \\ 0 & \text{si } n > 1. \end{cases}$$

Demostración. Si $n = 1$ el resultado es evidente. Sea $n > 1$ y sean $p_1, \ldots, p_s$, los divisores primos (distintos) de n. Entonces

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{s} \mu(p_i) + \sum_{1 \leq i < j \leq s} \mu(p_i p_j) + \cdots + \mu(p_1 p_2 \ldots p_s) \\ &= 1 + \binom{s}{1}(-1) + \binom{s}{2}(-1)^2 + \cdots + \binom{s}{s}(-1)^s \\ &= (1-1)^s = 0 \end{aligned}$$

según la fórmula del binomio de Newton. □

La siguiente fórmula nos permite despejar $N_q(r)$ en la ecuación (1).

Teorema 4.1.9. (Fórmula de inversión de Moebius) *Sea $\varphi : \mathbb{Z}_{>0} \to \mathbb{Z}$ una función cualquiera, y sea $\Phi : \mathbb{Z}_{>0} \to \mathbb{Z}$ definida como*

$$\Phi(n) = \sum_{d|n} \varphi(d).$$

Entonces se verifica que

$$\varphi(n) = \sum_{d|n} \mu(d)\Phi(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d})\Phi(d).$$

Demostración. Es consecuencia de las igualdades:

$$\sum_{d|n} \mu(d)\Phi(\frac{n}{d}) = \sum_{d|n} \mu(d) \sum_{e|(n/d)} \varphi(e) = \sum_{e|n} \sum_{d|(n/e)} \mu(d)\varphi(e) = \sum_{e|n} \varphi(e) \sum_{d|(n/e)} \mu(d) = \varphi(n).$$

donde la última igualdad se deduce del **Lema 4.1.8**. □

Un primer ejemplo de aplicación de la fórmula de inversión se obtiene para la función ϕ de Euler (que definimos en la **Subsección 2.2.4**). En este caso $\Phi(n) = n$ es la función identidad, y la fórmula de inversión que expresa ϕ en función de Φ es la misma que la fórmula obtenida en la **Proposición 2.2.7**.

Corolario 4.1.10. *El número de polinomios irreducibles de grado r sobre $\mathbb{F}_q$ es*

$$N_q(r) = \frac{1}{r} \sum_{s|r} \mu(s) q^{r/s} = \frac{1}{r} \sum_{s|r} \mu(\frac{r}{s}) q^s.$$

Demostración. Basta aplicar la fórmula de inversión a la función $\varphi(r) = rN_q(r)$. □

Ejemplo 4.1.11. Evaluando la fórmula del corolario, encontrarmos los valores de $N_q(r)$ para algunos grados r pequeños.

r	$N_q(r)$	r	$N_q(r)$	r	$N_q(r)$
1	q	4	$(q^4 - q^2)/4$	7	$(q^7 - q)/7$
2	$(q^2 - q)/2$	5	$(q^5 - q)/5$	8	$(q^8 - q^4)/8$
3	$(q^3 - q)/3$	6	$(q^6 - q^3 - q^2 + q)/6$	9	$(q^9 - q^3)/9$

Cuadro 4.1. Valores de $N_q(r)$

4.1.3. Existen polinomios irreducibles de cualquier grado

Como consecuencia de este corolario, para todo entero positivo r existen polinomios irreducibles de grado r sobre $\mathbb{F}_q$, puesto que la suma anterior es siempre positiva.

Proposición 4.1.12. *El número $N_q(r)$ de polinomios irreducibles de grado r sobre $\mathbb{F}_q$ verifica*

$$\frac{1}{r}\left(q^r - \frac{q^{\lfloor r/2\rfloor+1}-q}{q-1}\right) \leq N_q(r) \leq \frac{1}{r}\left(q^r + \frac{q^{\lfloor r/2\rfloor+1}-q}{q-1}\right).$$

Demostración. Según el Corolario 4.1.10

$$N_q(r) = \frac{1}{r}\sum_{s|r}\mu(\frac{r}{s})q^s = \frac{1}{r}\left(q^r + \sum_{s|r,s\neq r}\mu(\frac{r}{s})q^s\right).$$

Las desigualdades enunciadas son consecuencia de la acotación

$$\left|\sum_{s|r,s\neq r}\mu(\frac{r}{s})q^s\right| \leq \sum_{s=1}^{\lfloor r/2\rfloor} q^s = \frac{q^{\lfloor r/2\rfloor+1}-q}{q-1}$$

ya que el mayor divisor propio s de r satisface $s \leq \lfloor r/2\rfloor$. □

Ejemplo 4.1.13. Para hacernos una idea concreta de la cantidad de polinomios irreducibles que existen sobre $\mathbb{F}_q$, hemos calculado los valores de $N_q(r)$ sobre el cuerpo $\mathbb{F}_2$. Primero para algunos valores pequeños, $1 \leq r \leq 9$.

r	$N_2(r)$	r	$N_2(r)$	r	$N_2(r)$
1	2	4	3	7	18
2	1	5	6	8	30
3	2	6	9	9	56

Cuadro 4.2. Algunos valores de $N_2(r)$

Para valores mayores de r, $N_q(r)$ crece muy rápidamente. Veamos el intervalo $10 \leq r \leq 48$. Mostraremos también algunos valores para el caso de $\mathbb{F}_3$.

Si observamos las tablas anteriores, notamos que los $N_q(r)$ son crecientes con r a partir de $r = 2$. Esto sucede para todo q.

Corolario 4.1.14. *Para todo cuerpo $\mathbb{F}_q$ con $q > 3$, la sucesión $(N_q(r))$ es estrictamente creciente con $r = 1, 2, \ldots$. Para $q = 2$ y $q = 3$ la sucesión es estrictamente creciente a partir de $r = 2$.*

Demostración. Basta aplicar las acotaciones obtenidas en la **Proposición 4.1.12**. □

r	$N_2(r)$	r	$N_2(r)$	r	$N_2(r)$
10	99	23	364722	36	1908866960
11	186	24	698870	37	3714566310
12	335	25	1342176	38	7233615333
13	630	26	2580795	39	14096302710
14	1161	27	4971008	40	27487764474
15	2182	28	9586395	41	53634713550
16	4080	29	18512790	42	104715342801
17	7710	30	35790267	43	204560302842
18	14532	31	69273666	44	399822314775
19	27594	32	134215680	45	781874934568
20	52377	33	260300986	46	1529755125849
21	99858	34	505286415	47	2994414645858
22	190557	35	981706806	48	5864061663920

Cuadro 4.3. Más valores de $N_2(r)$

r	$N_3(r)$	r	$N_3(r)$	r	$N_3(r)$
1	3	4	18	7	312
2	3	5	48	8	810
3	8	6	116	9	2184

Cuadro 4.4. Algunos valores de $N_3(r)$

4.1.4. Número de polinomios coprimos

Denotaremos por $C_q(r)$ (respectivamente, por $C_q^*(r)$), el máximo cardinal posible para un conjunto $\mathscr{C}_r(q)$ de polinomios (mónicos) en $\mathbb{F}_q[X]$, de grado r (respectivamente, de grado $\leq r$) y coprimos dos a dos.

Proposición 4.1.15. *Para todo entero positivo r, se verifica que*

$$C_q(r) = N_q(r) + \sum_{i=1}^{\lfloor r/2 \rfloor} N_q(i), \quad C_q^*(r) = \sum_{i=1}^{r} N_q(i)$$

Demostración. Probemos la primera igualdad. Sea $\mathscr{C}_r(q)$ un conjunto de polinomios (mónicos) en $\mathbb{F}_q[X]$, de grado r y coprimos dos a dos. Cada $f(X) \in \mathscr{C}_r(q)$, o bien es irreducible o bien posee algún factor irreducible de grado $\leq \lfloor n/2 \rfloor$, que no puede volver a aparecer como factor en ningún otro $g(X) \in \mathscr{C}_r(q)$. Esto implica la desigualdad $\leq$ en la fórmula enunciada. Recíprocamente, para cada polinomio $h(X)$ irreducible de grado $l \leq \lfloor r/2 \rfloor$ elijamos un polinomio irreducible $h'(X)$ de grado $r-l$, de manera que a distintos $h(X)$ les correspondan distintos $h'(X)$. Esto es posible porque la sucesión $(N_q(r))$ es creciente. Entonces el conjunto $\{h(x)h'(X) \mid h(X) \text{ es irreducible de grado } \leq \lfloor r/2 \rfloor\} \cup \{f(X) \mid f(X) \text{ es irreducible de grado } r\}$ esta formado por polinomios coprimos dos a dos, de donde deducimos la desigualdad $\geq$ en la primera fórmula enunciada, salvo para $C_2(3)$. Para este valor, un argumento similar, tomando ahora $l \geq \lfloor r/2 \rfloor$, prueba que la fórmula

también es correcta. La segunda fórmula es evidente, ya que cada polinomio posee algún factor irreducible. □

4.2. El esquema de Mignotte en $\mathbb{F}_q[X]$

Los esquemas de reparto de secretos siguen en $\mathbb{F}_q[X]$ el mismo patrón estudiado en $\mathbb{Z}$, simplemente sustituyendo la función euclídea $|z|$ de $\mathbb{Z}$ por la función euclídea $\deg(f(X))$ sobre $\mathbb{F}_q[X]$. Para no repetir argumentaciones, en lo que sigue trataremos los esquemas de tipo Mignotte, en su versión más general, estudiada en el capítulo anterior. Recordemos que las unidades de $\mathbb{F}_q[X]$ son los elementos no nulos de $\mathbb{F}_q$. Así, todos los polinómios que consideremos se entenderán mónicos.

4.2.1. Esquemas polinómicos de Mignotte

Sean $\mathscr{P} = \{1, \ldots, n\}$ un conjunto de n participantes y $\mathscr{A}$ una estructura de acceso sobre $\mathscr{P}$. Dada una secuencia $\mathbf{m} : m_1(X), \ldots, m_n(X)$ de n polinomios y una coalición $C \subseteq \mathscr{P}$, escribiremos $\operatorname{mcm}(C) = \operatorname{mcm}\{m_i(X) \mid i \in C\}$. Si la secuencia $\mathbf{m}$ verifica que $\deg(\operatorname{mcm}(A)) > \deg(\operatorname{mcm}(B))$ para todos $A \in \mathscr{A}, B \notin \mathscr{A}$, definimos

$$\mathbf{m}^- = \min\{\deg(\operatorname{mcm}(A)) \mid A \in \mathscr{A}\}, \qquad \mathbf{m}^+ = \max\{\deg(\operatorname{mcm}(B)) \mid B \notin \mathscr{A}\}$$

y sea $\mathscr{S}\{s(X) \in \mathbb{F}_q[X] \mid \mathbf{m}^+ < \deg(s(X)) < \mathbf{m}^-\}$ el espacio de secretos a repartir. El esquema polinómico de Mignotte funciona de la forma esperada: dado un secreto $s(X) \in \mathscr{S}$, cada participante i recibe la participación $s_i(X) = s(X) \pmod{m_i(X)}$. Una coalición autorizada A que desea recuperar el secreto resuelve el sistema:

$$(S_A): \quad x(X) \equiv s_i(X) \pmod{m_i(X)} \quad i \in A$$

cuya solución es única módulo $\operatorname{mcm}(A)$. Como $\deg(s(X)) < \deg(\operatorname{mcm}(A))$, se verifica que $s(X) = x(X)$. Una coalición no autorizada B que desee recuperar el secreto puede resolver el sistema:

$$(S_B): \quad x(X) \equiv s_i(X) \pmod{m_i(X)} \quad i \in B$$

Pero como $\deg(\operatorname{mcm}(A)) < \deg(s(X))$, se verifica que $s(X) \neq x(X)$ y B no recupera el secreto.

4.2.2. Estructuras umbral

Si los polinomios de una secuencia $\mathbf{m} : m_1(X), \ldots, m_n(X)$ son coprimos dos a dos, entonces los cálculos (incluyendo los requeridos por el teorema chino del resto) se simplifican, ya que $\operatorname{mcm}(C) = \prod_{i \in C} m_i(X)$, luego $\deg(\operatorname{mcm}(C)) = \sum_{i \in C} \deg(m_i(X))$. Este hecho nos conduce al resultado:

Proposición 4.2.1. *Toda esquema polinómico de Mignotte $\mathscr{R}$ con módulos $\mathbf{m} : m_1(X), \ldots, m_n(X)$ coprimos, es un esquema umbral ponderado. En particular, si todos los módulos son del mismo grado, entonces el esquema es umbral.*

Demostración. Sea $\mathscr{S} = (\mathbf{m}^+, \mathbf{m}^-) \cap \mathbb{Z}$ el espacio de secretos. Una coalición C está autorizada si y sólo si $\deg(\text{mcm}(C)) = \sum_{i \in C} \deg(m_i(X)) \geq \mathbf{m}^-$, luego $\mathscr{R}$ es un esquema umbral ponderado con pesos $w_i = \deg(m_i(X))$ y umbral $t = \mathbf{m}^-$. En el caso particular en que todos los $m_i(X)$ son del mismo grado, r, entonces $\deg(\text{mcm}(C)) = r|C|$ y la condición $\deg(\text{mcm}(C)) > \mathbf{m}^-$ simplemente significa $|C| \geq \lceil \mathbf{m}^-/r \rceil$. Es decir, la estructura de acceso es umbral. □

El mismo razonamiento, en sentido inverso, muestra que toda estructura umbral puede realizarse mediante un esquema polinómico de Mignotte basado en polinomios irreducibles del mismo grado, siempre que existan suficientes polinomios irreducibles de ese grado. Tras esto podemos obtener un resultado análogo al obtenido en la **Proposición 3.3.1** del **Capítulo 3** sobre los enteros. Su demostración es también similar, por lo que la omitimos.

Corolario 4.2.2. *Sea n un entero positivo.*
(a) Toda estructura umbral ponderada $(t, \mathbf{w}, n)$ *puede realizarse mediante un esquema polinómico de Mignotte en* $\mathbb{F}_q[X]$.
(b) Si $n \leq N_r(q)$ *entonces toda estructura umbral* (t,n) *puede realizarse mediante un esquema polinómico de Mignotte en* $\mathbb{F}_q[X]$ *basado en polinomios irreducibles de grado r.*
(c) Si $n \leq C_r(q)$ *entonces toda estructura umbral* (t,n) *puede realizarse mediante un esquema polinómico de Mignotte en* $\mathbb{F}_q[X]$ *basado en polinomios de grado r coprimos dos a dos.*

4.2.3. Un ejemplo

Volvamos con los seis científicos de los capítulos anteriores. Pongamos que han decidido que, dada la aportación de cada uno a la beca que financia su investigación, su importancia relativa (su peso en el esquema de reparto) es 3,2,1,1,1,1. Podrá recuperar el secreto cualquier coalición de peso al menos 5. Fabriquemos un esquema de Mignotte ponderado para estos pesos sobre el anillo $\mathbb{F}_3[X]$ (siendo el cuerpo base tan pequeño, el espacio de secretos será igualmente pequeño a menos de tomar polinomios de grados altos). Para ello, buscaremos seis polinomios coprimos de los grados adecuados. Como no existen tantos polinomios coprimos de grado 1 como participantes con peso 1, podemos tomar cualquier múltiplo de los pesos, con tal de que multipliquemos también el umbral. Sea $\mathbf{w} = (6,4,2,2,2,2)$ y el umbral $t = 10$, obtenido al multiplicar por 2 en el esquema original. Tomemos

$$\begin{aligned} m_1 &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\ m_2 &= X^4 + X^3 + X^2 + X + 3 \\ m_3 &= X^2 + 2 \\ m_4 &= X^2 + 3 \\ m_5 &= X^2 + X + 1 \\ m_6 &= X^2 + X + 2 \end{aligned}$$

(todos ellos irreducibles). Los posibles secretos son los polinomios de grado 9. Por ejemplo, $s(X) = X^9 + 3X^8 + X^7 + 3X^6 + X^5 + 3X^4 + X^3 + 3X^2 + X$. Las participaciones de este

secreto son

$$\begin{aligned} s_1 &= 3X^5+3X^3+X^2+X+3 \\ s_2 &= 3X^3+2X+2 \\ s_3 &= X \\ s_4 &= X \\ s_5 &= 3X+3 \\ s_6 &= 4X+4 \end{aligned}$$

La coalición $\{1,2\}$ desea recuperar el secreto. Resuelve el sistema

$$\begin{cases} x(X) \equiv & 3X^5+3X^3+X^2+X+3 \pmod{X^6+X^5+X^4+X^3+X^2+X+1} \\ x(X) \equiv & 3X^3+2X+2 \pmod{X^4+X^3+X^2+X+3} \end{cases}$$

cuya solución es $X^9+3X^8+X^7+3X^6+X^5+3X^4+X^3+3X^2+X = s(X)$, única módulo $X^{10}+X^9+3X^8+4X^7+2X^6+2X^5+2X^4+X^3+4X+3$. La coalición de científicos 'rasos' $\{3,4,5,6\}$ puede intentar recuperar el secreto, resolviendo

$$\begin{cases} x(X) \equiv & X \pmod{X^2+2} \\ x(X) \equiv & X \pmod{X^2+3} \\ x(X) \equiv & 3X+3 \pmod{X^2+X+1} \\ x(X) \equiv & 4X+4 \pmod{X^2+X+2} \end{cases}$$

cuya única solución, módulo $X^8+2X^7+9X^6+13X^5+28X^4+27X^3+34X^2+18X+12$, es $X^6+3X^4+X^2+X+3 \neq s(X)$. Es decir, esta coalición no recupera el secreto.

4.2.4. Toda estructura es realizable por un esquema polinónico de Mignotte

A la vista de los resultados de la Sección 4.2.2 resulta natural preguntarnos qué otras estructuras de acceso $\mathscr{A}$ son realizables mediante un esquema polinónico de Mignotte, esto es, ¿para qué estructuras $\mathscr{A}$ sobre $\mathscr{P}$ existe una secuencia de polinomios $\mathbf{m} : m_1(X), \ldots, m_n(X)$ tal que $\deg(\text{mcm}(A)) > \deg(\text{mcm}(B))$ para todos $A \in \mathscr{A}, B \notin \mathscr{A}$? Encontramos que esto sucede para todas, como probaron Galibus y Matveev en [10].

Teorema 4.2.3. *Toda estructura de acceso es realizable mediante un esquema polinónico de Mignotte.*

Demostración. Sea $\mathscr{A}$ una estructura de acceso sobre un conjunto $\mathscr{P}$ con n participantes. Sean $B_1, \ldots, B_u$ las coaliciones no autorizadas maximales de $\mathscr{A}$. Vamos a construir iteradamente u secuencias de módulos $\mathbf{m}^{(1)}, \ldots, \mathbf{m}^{(u)}$, con $\mathbf{m}^{(j)} : {m_1}^{(j)}(X), \ldots, {m_n}^{(j)}(X)$, de manera que $\mathbf{m}^{(u)}$ realice la estructura $\mathscr{A}$. Para simplificar la notación, dada una coalición $C \subseteq \mathscr{P}$, escribiremos $\text{mcm}^{(j)}(C) = \text{mcm}\{{m_i}^{(j)}(X) \mid i \in C\}$.
Consideremos la primera coalición maximal no autorizada, B_1, y sea $f_1(X)$ un polinomio irreducible cualquiera. Para $1 \leq i \leq n$ definimos

$${m_i}^{(1)}(X) = \begin{cases} 1 & \text{si } i \in B_1 \\ f_1(x) & \text{si } i \notin B_1. \end{cases}$$

Para toda coalición autorizada A, existe un participante $i \in A \setminus B_1$, luego $\deg(\mathrm{mcm}^{(1)}(A)) > \deg(\mathrm{mcm}^{(1)}(B_1))$. Supongamos construida de esta forma $\mathbf{m}^{(j-1)}$ tal que se verifique que $\deg(\mathrm{mcm}^{(j-1)}(A)) > \deg(\mathrm{mcm}^{(j-1)}(B_h))$ para todo $h \leq j-1$ y toda coalición autorizada A. Sea $f_j(X)$ un polinomio de grado $\deg(f_j(X)) > \deg(\mathrm{mcm}^{(j-1)}(B_j))$ que sea coprimo con todos los $f_h(X)$, $1 \leq h < j$. Entonces $f_j(X)$ también es coprimo con todos los ${m_i}^{(j-1)}(X)$, $i = 1, \ldots, n$. Definamos

$$ {m_i}^{(j)}(X) = \begin{cases} {m_i}^{(j-1)}(X) & \text{si } i \in B_j \\ {m_i}^{(j-1)}(X) f_j(X) & \text{si } i \notin B_j. \end{cases} $$

Sea A una coalición autorizada. Como, de nuevo, existe un participante en $A \setminus B_j$, se verifica $\deg(\mathrm{mcm}^{(j)}(A)) = \deg(f_j(X)) + \deg(\mathrm{mcm}^{(j-1)}(A))$. Luego para $h \leq j-1$

$$ \deg(\mathrm{mcm}^{(j)}(A)) > \deg(f_j(X)) + \deg(\mathrm{mcm}^{(j-1)}(B_h)) \geq \deg(\mathrm{mcm}^{(j)}(B_h)), $$

y para $h = j$, $\deg(\mathrm{mcm}^{(j)}(A)) \geq \deg(f_j(X)) > \deg(\mathrm{mcm}^{(j-1)}(B_j)) = \deg(\mathrm{mcm}^{(j)}(B_j))$. Tras u iteraciones obtenemos la secuencia $\mathbf{m}_u$ que satisface la condición $\deg(\mathrm{mcm}^{(u)}(A)) > \deg(\mathrm{mcm}^{(u)}(B_h))$ para todo $1 \leq h \leq u$ y toda coalición autorizada A. Por tanto $\mathbf{m}_u$ realiza la estructura $\mathscr{A}$. □

Obsérvese que esta demostración es constructiva y muestra efectivamente como obtener una secuencia de módulos $\mathbf{m}$ que realiza $\mathscr{A}$. Hagamos notar que, en la demostración original de este teorema dada en [10], se exige que los $f_j(X)$ sean irreducibles, condición que, como hemos visto, es prescindible.

4.2.5. Un ejemplo

Los seis científicos han vuelto a cambiar de opinión sobre la mejor manera de acceder al secreto, llegando ahora al acuerdo de que pueda hacerlo cualquier coalición que contenga al menos un participante de entre $\{1,2\} \subset \mathscr{P}$ y al menos dos de entre $\{3,4,5,6\} \subset \mathscr{P}$.

Las coaliciones maximales no autorizadas para esta estructura de acceso $\mathscr{A}$ son $B_1 = \{3,4,5,6\}$, $B_2 = \{1,2,3\}$, $B_3 = \{1,2,4\}$, $B_4 = \{1,2,5\}$ y $B_5 = \{1,2,6\}$. Obsérvese que $\mathscr{A}$ no es umbral ponderada. Si lo fuera, con umbral t y pesos w_1 para los participantes $1,2$, y w_2 para los $3,4,5,6$, como $\{1,2\}$ no está auorizada, $2w_1 < t$; como $\{1,3,4\}$ sí lo está, entonces $w_1 + 2w_2 \geq t$. De la primera condición, $w_1 < t/2$ con lo que, de la segunda, $w_2 > t/4$. Pero $\{3,4,5,6\}$ no está autorizada.

Basta proceder según la demostración del teorema, obtenemos las siguentes secuencias de módulos en el anillo $\mathbb{F}_3[X]$:

• para B_1 tomamos $f_1(X) = X$ con lo que

$$ m_1^{(1)}(X) = m_2^{(1)}(X) = X,\ m_3^{(1)}(X) = m_4^{(1)}(X) = m_5^{(1)}(X) = m_6^{(1)}(X) = 1; $$

• para B_2 tomamos $f_2(X) = X^2 + 2$ con lo que

$$ m_1^{(2)}(X) = m_2^{(2)}(X) = X,\ m_3^{(2)}(X) = 1,\ m_4^{(2)}(X) = m_5^{(2)}(X) = m_6^{(2)}(X) = X^2 + 2; $$

• para B_3 tomamos $f_3(X) = X^3 + X + 1$ con lo que

$$\begin{aligned} m_1^{(3)}(X) &= m_2^{(3)}(X) = X, \\ m_3^{(3)}(X) &= X^3 + X + 1, \\ m_4^{(3)}(X) &= X^2 + 2, \\ m_5^{(3)}(X) &= m_6^{(3)}(X) = (X^2+2)(X^3+X+1) = X^5 + 3X^3 + X^2 + 2X + 2; \end{aligned}$$

• para B_4 tomamos $f_4(X) = X^7 + X + 1$ con lo que

$$\begin{aligned} m_1^{(4)}(X) &= m_2^{(4)}(X) = X, \\ m_3^{(4)}(X) &= X^7 + X + 1, \\ m_4^{(4)}(X) &= X^9 + 2X^7 + X^3 + X^2 + 2X + 2, \\ m_5^{(4)}(X) &= X^5 + 3X^3 + X^2 + 2X + 2, \\ m_6^{(4)}(X) &= X^{12} + 3X^{10} + X^9 + 2X^8 + 2X^7 + X^6 + X^5 + 3X^4 + 4X^3 + 3X^2 + 4X + 2; \end{aligned}$$

• para B_5 tomamos $f_5(X) = X^{13} + X^{10} + X^9 + X^6 + X^2 + X + 1$ con lo que

$$\begin{aligned} m_1^{(5)}(X) &= m_2^{(4)}(X) = X, \\ m_3^{(5)}(X) &= X^{20} + X^{17} + X^{16} + X^{14} + 2X^{13} + X^{11} + 2X^{10} + 2X^9 + X^8 + 2X^7 + X^6 \\ &\quad + X^3 + 2X^2 + 2X + 1, \\ m_4^{(5)}(X) &= X^{22} + 2X^{20} + X^{19} + X^{18} + 2X^{17} + 3X^{16} + 2X^{15} + 2X^{14} + 5X^{13} + 2X^{12} \\ &\quad + 4X^{11} + 5X^{10} + 6X^9 + 3X^8 + 4X^7 + 2X^6 + X^5 + 2X^4 + 4X^3 + 5X^2 + 4X + 2, \\ m_5^{(5)}(X) &= X^{18} + 3X^{16} + 2X^{15} + 3X^{14} + 5X^{13} + 4X^{12} + 4X^{11} + 4X^{10} + X^8 + 3X^7 \\ &\quad + 3X^6 + 4X^5 + 4X^4 + 6X^3 + 5X^2 + 4X + 2, \\ m_6^{(5)}(X) &= X^{12} + 3X^{10} + X^9 + 2X^8 + 2X^7 + X^6 + X^5 + 3X^4 + 4X^3 + 3X^2 + 4X + 2, \end{aligned}$$

que son finalmente los polinomios que pemiten realizar la estructura $\mathscr{A}$.

4.3. Esquemas de Mignotte sobre $\mathbb{Z}$

En el **Teorema 4.2.3** hemos mostrado que toda estructura de acceso es realizable mediante un esquema de Mignotte polinómico. Ahora bien, el enunciado de este teorema y su demostración pueden exportarse, con los cambios obvios, al caso entero $\mathbb{Z}$, lo que no hemos encontrado en la literatura. Juntando esto con los resultados que aparecen en el capítulo anterior, podemos enunciar el siguiente resultado:

Teorema 4.3.1. *Toda estructura de acceso $\mathscr{A}$ puede ser realizada por un esquema de Mignotte $\mathscr{R}$ sobre $\mathbb{Z}$ basada en una secuencia de enteros* $\mathbf{m}$. *Además, si los módulos que aparecen en* $\mathbf{m}$ *son coprimos entonces la estructura de acceso obtenida es umbral ponderada.*

Demostración. La segunda parte del enunciado fue probada en el capítulo anterior, en concreto en la **Proposición 3.4.3.**. Así, es suficiente probar la primera, esto es, que toda estructura de acceso puede ser realizada por un esquema de Mignotte $\mathscr{R}$ sobre $\mathbb{Z}$.

Sea pues $\mathscr{A}$ una estructura de acceso sobre el conjunto $\mathscr{P}$ de n participantes y sean $B_1,\ldots,B_u$ las coaliciones maximales no autorizadas para $\mathscr{A}$. Tomemos u enteros coprimos $\mu^{(1)},\ldots,\mu^{(u)}$. Para $i=1,\ldots,n$ y $j=1,\ldots,u$, sea

$$\mu_i^{(j)} = \begin{cases} 1 & \text{si } i \in B_j \\ \mu^{(j)} & \text{si } i \notin B_j \end{cases}$$

y sea $m_i = \mu_i^{(1)} \cdots \mu_i^{(u)}$. El esquema de Mignotte asociado a la secuencia $\mathbf{m} : m_1,\ldots,m_n$ realiza la estructura $\mathscr{A}$. Para ver que así es, definamos

$$\mathbf{m}^- = \mu^{(1)} \cdots \mu^{(u)}\,, \qquad \mathbf{m}^+ = m^+ / \text{mín}\{\mu^{(1)},\ldots,\mu^{(u)}\}.$$

Sea $A \in \mathscr{A}$ una coalición autorizada. Para cada coalición no autorizada maximal B_j existe un participante i (dependiente de j) tal que $i \in A \setminus B_j$. Por tanto $\mu_i^{(j)} = \mu^{(j)}$ luego $\text{mcm}(A) = \mu^{(1)} \cdots \mu^{(u)}$, con lo que $\text{mcm}(A) = \mathbf{m}^-$. Recíprocamente, si B es una coalición no autorizada, existe j tal que $B \subseteq B_j$. Por tanto $\mu_i^{(j)} = 1$ para todo $i \in B$, luego $\text{mcm}(B)) \leq \mathbf{m}^- / \mu^{(j)} \leq \mathbf{m}^+$. Hemos probado así que $\mathscr{A} = \{A \subseteq \mathscr{P} \mid \text{mcm}(A) \geq \mathbf{m}^-\}$, es decir que la secuencia $\mathbf{m} : m_1,\ldots,m_n$ realiza la estructura $\mathscr{A}$ con espacio de secretos $\mathscr{S} = \{s \in \mathbb{Z} \,:\, \mathbf{m}^+ < s < \mathbf{m}^-\}$. □

4.4. Esquemas umbral de Asmuth-Bloom en $\mathbb{F}_q[X]$

Tratemos ahora los esquemas polinómicos de Asmuth-Bloom. Nos limitaremos a las estructuras de acceso umbrales. El contenido de esta sección se basa principalmente en [24].

4.4.1. Esquemas umbral polinómicos de Asmuth-Bloom

El esquema umbral de Asmuth-Bloom pueden trasladarse a $\mathbb{F}_q[X]$ con las adaptaciones obvias. Deseamos construir un esquema umbral (t,n) sobre el conjunto $\mathscr{P} = \{1,\ldots,n\}$ de n participantes.

Sean d un entero positivo y $m_0(X) = X^d$. Tomemos una secuencia de polinomios $\mathbf{m} : m_0(X) = X^d, m_1(X),\ldots,m_n(X)$, coprimos dos a dos, con $d \leq \deg(m_1(X)) \leq \cdots \leq \deg(m_n(X))$, y verificando $\deg(X^d m_{n-t+2}(X) \cdots m_n(X)) \leq \deg(m_1(X) \cdots m_t(X))$. El esquema de Asmuth-Bloom permite repartir un secreto del conjunto

$$\mathscr{S} = \{f(X) \in \mathbb{F}_q[X] \,|\, 0 \leq \deg(f(X)) < d\} \cong \mathbb{F}_q[X]/(X^d)$$

entre los n participantes como sigue: dado el secreto $s(X) \in \mathscr{S}$

• el gestor elige al azar un polinomio $a(X)$ tal que

$$\deg(m_{n-t+2}(X) \cdots m_n(X)) - d < \deg(a(X)) < \deg(m_{n-t+2}(X) \cdots m_n(X));$$

la participación de i es $s_i(X) = s(X) + a(X)X^d \pmod{m_i(X)}$, $i = 1, \ldots, n$;
• una coalición $A \subset \mathscr{P}$ de t o más participantes puede recuperar $s(X)$ resolviendo el sistema en congruencias

$$(S_A): \quad x(X) \equiv s_i(X) \pmod{m_i(X)} \qquad i \in A,$$

y reduciendo la única (módulo $m_A(X)$) solución obtenida, $s(X) = x(X) \pmod{X^d}$.

Proposición 4.4.1. *El método descrito es correcto y proporciona un esquema umbral de tipo (n,t) con tasa de información $\rho = \deg(m_0(X))/\deg(m_n(X))$.*

El análisis de la corrección del método es idéntico al del caso entero por lo que lo omitiremos aquí. Obsérvese que ahora todos los polinomios $m_0(X), \ldots, m_n(X)$ pueden tomarse del mismo grado d (en cuyo caso el esquema es ideal) siempre que sean coprimos dos a dos. Esto es posible, cuando existen suficientes polinomios coprimos de grado d, es decir, según los resultados de la Sección 4.1.4, cuando $n \leq C_q(d)$.

4.4.2. Relación con el esquema de Shamir

En esta subsección veremos que el esquema de Shamir es un caso particular del de Asmuth-Bloom polinómico.

Para construir un esquema (t,n) por el método polinómico de Asmuth-Bloom, tomemos $d = 1$, $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ distintos y no nulos, y sean $m_0(X) = X$, $m_i(X) = X - \alpha_i$, $i = 1, \ldots, n$. Esta elección conduce al espacio de secretos $\mathscr{S} = \mathbb{F}_q$.

Dado un secreto $s \in \mathbb{F}_q$, se elije al azar un polinomio $a(X)$ de grado $t-2$ y se calcula $f(X) = s + a(X)X$. Por tanto $f(X)$ es un polinomio al azar, de grado $t-1$ y con $f(0) = s$. Las participaciones a repartir son $s_i(X) = f(X) \pmod{X - \alpha_i} = f(\alpha_i)$.

Como vemos, las participaciones del secreto son las mismas que en el esquema de Shamir. Veamos que también la recuperación del secreto es igual. Dada una coalición A con t miembros, A recupera el secreto resolviendo el sistema

$$(S_A): \quad x(X) \equiv s_i(X) \pmod{X - \alpha_i} \qquad i \in A.$$

La solución de este sistema puede obtenerse como describimos en el **Teorema 2.3.1** del **Capítulo 2**. En este caso, operando sobre la fórmula que da la solución, obtenemos

$$x(X) = \sum_{i \in A} s_i \prod_{j \in A, j \neq i} \frac{X - \alpha_j}{\alpha_i - \alpha_j}$$

que resulta ser la expresión de Lagrange del polinomio interpolador de $f(X)$, luego $x(X) = f(X)$. El secreto resulta ser entonces: $x(X) \pmod{X} = x(0) = f(0)$.

Referencias

[1] C. A. Asmuth, J. Bloom, A modular approach to key safeguarding, IEEE Transactions on Information Theory 29 (1983), 208–210.

[2] J. Benaloh, J. Leichter, Generalized secret sharing and monotone functions. En S. Goldwasser (editor), Advances in Cryptology-CRYPTO '88, LNCS-403, Springer-Verlag, 1990, 27–35.

[3] G. R. Blakley, Safeguarding cryptographic keys. En National Computer Conference-1979, American Federation of Information Processing Societies Proceedings-48, 1979, 313–317.

[4] R. Cramer, I.B. Damgård, Secure Multiparty Computation and Secret Sharing. Cambridge University Press, 2015.

[5] R. Cramer, M. K. Franklin, B. Schoenmakers, M. Yung, Multi-authority secret-ballot elections with linear work. En U. Maurer (editor), Advances in Cryptology - EuroCrypt '96. LNCS-1070, Springer-Verlag, 1996, 72–83.

[6] F. Delgado de la Mata, C. Fuertes Fraile, S. Xambó, Introducción al álgebra. Vol. 2: Anillos, factorización y teoría de cuerpos. Universidad de Valladolid, 1999.

[7] W. Diffie, M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22 (1976), 644–654.

[8] C. Ding, D. Pei, and A. Salomaa, Chinese Remainder Theorem: Applications in Computing, Coding and Cryptography. World Scientific, 1996.

[9] A. S. Fraenkel, New proof of the generalized Chinese remainder theorem, Proceedings of American Mathematical Society 14 (1963), 790–791.

[10] T. Galibus, G. Matveev, Generalized Mignotte Sequences in Polynomial Rings, Electronic Notes in Theoretical Computer Science 186 (2007), 43–48.

[11] T. Galibus, G. Matveed, N. Shenets, Some structural and security properties of the modular secret sharing. Proceeding of SYNASC'08. IEEE Comp. Soc.Press, 2009, 197–200.

[12] H. Garner, The residue number system, IRE Transactions on Electronic Computers 8 (1969), 140–147.

[13] L. Harn, H Chingfang, M. Zhang, T. He, M. Zhang, Realizing secret sharing with general access structure, Information Sciences 367-368 (2016), 209–220.

[14] S. Iftene, Secret sharing schemes with applications in security protocols Sci. Ann. Cuza Univ. 16 (2006), 63–96.

[15] S. Iftene, General secret sharing based on the chinese remainder Theorem with applications in e-voting, Electronic Notes in Theoretical Computer Science 186 (2007), 67–84.

[16] S. Iftene, Secret sharing schemes with applications in security protocols. Tesis Doctoral, Universidad Al I Cuza, Iasi (Rumanía), 2007.

[17] S. Iftene, I. Boureanu, Weighted threshold secret sharing based on the chinese remainder theorem, Scientific Annals of Cuza University 15 (2005) 161–172.

[18] M. Ito, A. Saito, T. Nishizeki, Secret sharing scheme realizing general access structure. En Proceedings of IEEE Globecom'87, 1987, 99–102.

[19] K. Kaya, Threshold cryptography with Chinese remainder theorem. Tesis Doctoral, Universidad de Bilkent (Turquía), 2009.

[20] K. Kaya, A. Selcuk, Threshold cryptography based on Asmuth-Bloom secret sharing, Information sciences 177 (2007), 4148–4160.

[21] A. Kerckhoffs, La cryptographic militaire, Journal des sciences militaires (1883), 5–38.

[22] R. Lidl, H. Niederreiter, Finite fields and their applications, Cambridge University Press, 1985.

[23] M. Mignotte, How to share a secret. En Proceedings of the Workshop on Cryptography Burg Feuerstein, 1982. LNCS-149, Springer-Verlag, 1983, 371–375.

[24] Y. Ning, F. Miao, W. Huang, K. Meng, Y. Xiong, X. Wang, Constructing Ideal Secret Sharing Schemes based on Chinese Remainder Theorem. International Conference on the Theory and Applications of Cryptology and Information Security – ASIACRYPT 2018. LNCS-11274. Springer, 2018, 310–331.

[25] O. Ore, The general Chinese remainder theorem, American Mathematical Monthly 59 (1952), 365–370,

[26] M. Quisquater, B. Preneel, J. Vandewalle, On the security of the threshold schemes based on the Chinese Remainder Theorem. En Proceedings of the 5th International Workshop on Practice and Theory in Public Key Cryptosystems, LNCS-2274, Springer-Verlag, 2002, 199–210.

[27] A. Salomaa, Public-key Cryptography, Springer-Verlag, 1996.

[28] A. Shamir, How to share a secret? Communications of ACM 22 (1979), 612–613.

[29] Singh, S. The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography. Doubleday, 1999.

[30] D. Stinson, An explication of secret sharing schemes, Designs, Codes and Cryptography 2 (1992), 357–390.

[31] D. Stinson, Cryptography: Theory and Practice. Discrete Mathematics and Its Applications, CRC Press 2005.

[32] L. Toth, The probability that k positive integers are pairwise relatively prime, Fibonacci Quarterly 40 (2002), 13–18.