ESQUEMAS DE REPARTO DE SECRETOS SOBRE ENTEROS DE GAUSS

TRABAJO FIN DE MÁSTER

Curso: 2020/21

Autor: Diego Munuera Merayo
Tutor: Antonio Campillo López

Máster en Matemáticas
Facultad de Ciencias
Universidad de Valladolid

Índice

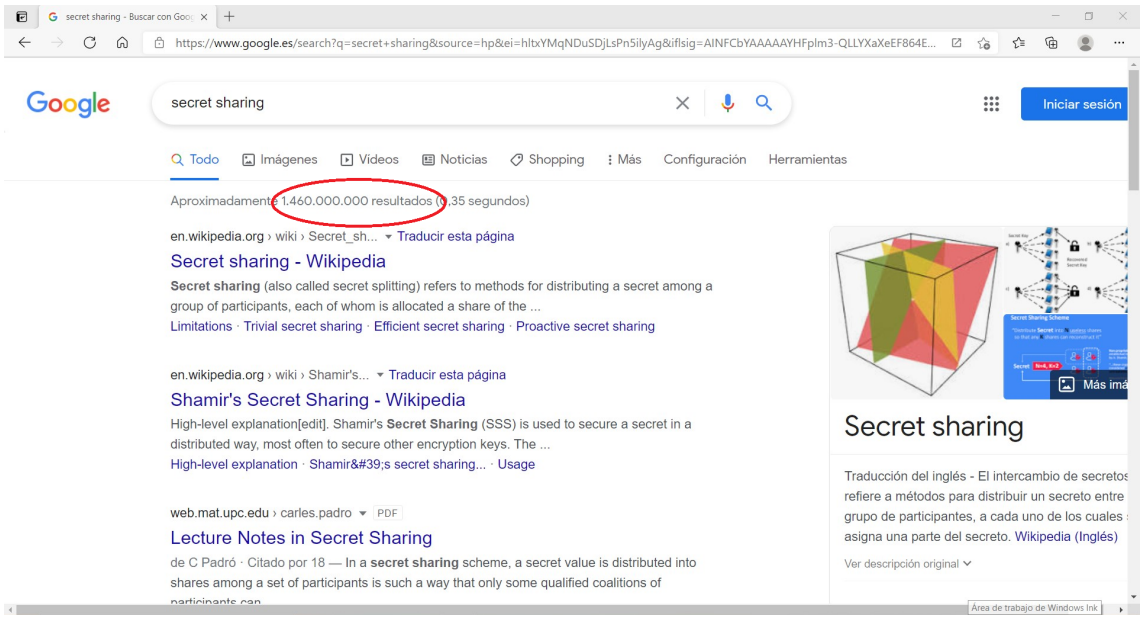
0

Presentación

0.1. El origen y el tema de este trabajo

El pasado curso académico 2019-2020 presenté en esta Universidad de Valladolid mi TFG titulado *Reparto de secretos con el Teorema Chino de los restos*, [21]. Como puede adivinarse, en él se trataban los esquemas de reparto de secretos cuyo funcionamiento se basa en el Teorema Chino. Esencialmente se trata de dos tipos de esquemas: el más importante debido originalmente a M. Mignotte [20], pero también el de C. A. Asmuth y J. Bloom [1].

Los esquemas de reparto de secretos constituyen hoy una importante rama dentro de la criptografía de clave pública, tanto por su interés teórico como por sus aplicaciones en seguridad y distribución de claves, votaciones electrónicas, computación multiparte, criptografía corporativa, [3, 4, 16, 31], etc. Una simple consulta a GOOGLE nos informa de que podemos encontrar actualmente unos 1500 millones de páginas dedicadas a este tema en el Internet.



Desde su formulacion original en el año 1983, los esquemas de Mignotte y de Asmuth-Bloom han recibido distintas extensiones y generalizaciones, [8, 9, 15, 19]. Inicialmente ambos estaban diseñados para producir sólamente esquemas del tipo llamado

umbral sobre los enteros (el modelo más simple de esquema de reparto). Posteriormente han sido adaptados para poder realizar esquemas más generales que los umbrales. Por otro lado, el teorema Chino de los restos puede establecerse sobre anillos más generales que $\mathbb{Z}$, los *dominios euclídeos*, por lo que una extensión análoga es factible para los esquemas de reparto basados en él, al menos teóricamente. En la práctica, la solución al problema Chino de los restos es también computacional para aquellos dominios euclídeos cuya función de Euclides tenga una expresión explícita. Y efectivamente, extensiones tales han sido llevadas a cabo en el anillo de polinomios sobre un cuerpo finito, $\mathbb{F}_q[X]$, [8, 23]. Otro dominio euclídeo bien conocido es el anillo de enteros de Gauss $\mathbb{Z}[i]$, que puede considerarse como el siguiente objetivo obvio para una extensión de este tipo.

Consultada la bibliografía, constatamos que esta extensión ha sido ya propuesta y desarrollada en el artículo [26], donde los autores extienden el esquema de Mignotte (de nuevo en su caso umbral más simple) a $\mathbb{Z}[i]$, y posteriormente utilizan esta herramienta para aplicarla en el reparto de imágenes (criptografía *visual*). Sin embargo esos autores cometen un error crucial al llevar a cabo esta extensión, puesto que no tienen en cuenta la no unicidad de la división euclídea sobre $\mathbb{Z}[i]$. Esto provoca que, por lo general, el secreto recuperado no coincida con el que se repartió, y en consecuencia que se obtengan falsos secretos.

El propósito de esta memoria es realizar esta extensión de manera correcta, obteniendo un esquema que funcione adecuadamente sobre $\mathbb{Z}[i]$; y también estudiar algunas de las propiedades más importantes del esquema obtenido. Desarrollaremos un esquema de Mignotte en su formulación general, trataremos sus características principales y probaremos que toda estructura de acceso es realizable mediante un esquema deeste tipo sobre $\mathbb{Z}[i]$. Para mostrar de manera práctica la viabilidad del esquema que presentamos, incluimos al final de la memoria una implementación en el programa MAPLE, que, a partir de una estructura de acceso arbitraria, computa el esquema que la realiza, y lleva a cabo los procesos de reparto de un secreto y su posterior recuperación mediante las participaciones calculadas.

0.2. Organizacion de la memoria

La memoria se estructura en 4 capítulos, más este preliminar y un Anexo al final.

El Capítulo 1 está dedicado a recopilar la información básica sobre los elementos que trataremos en los siguientes; a saber, los esquemas de reparto de secretos y el teorema Chino de los restos. Describimos los esquemas de Mignotte y de Asmuth-Bloom en distintas formulaciones, sobre el anillo de enteros $\mathbb{Z}$, y posteriormente sobre $\mathbb{F}_q[X]$ y $\mathbb{Z}[i]$. Terminamos mostrando mediante un ejemplo, como esta última extensión, en la forma desarrollada en [26], produce resultados erróneos, lo que constituye el punto de partida de nuestro trabajo: ¿por qué se producen estos errores? y ¿cómo se puede solucionar el problema?

Para ello, en el Capítulo 2 comenzamos a estudiar sistemáticamente los dominios euclídeos sobre los que se han llevado a cabo estas extensiones, es decir, prestando

especial atención al caso de $\mathbb{F}_q[X]$ y, sobre todo, al de $\mathbb{Z}[i]$. Probaremos que los únicos dominios euclídeos en los que la divisón euclídea es única son los cuerpos $\mathbb{K}$ y los anillos de polinomios $\mathbb{K}[X]$, lo que explica por qué la extensión del esquema de Mignotte a $\mathbb{F}_q[X]$ es correcta, mientras que una similar a $\mathbb{Z}[i]$ produce resultados erróneos; lo que de paso nos indica el camino para realizar correctamente esa extensión.

La extensión propiamente dicha del esquema de Mignotte a $\mathbb{Z}[i]$ se desarrolla en el Capítulo 3, con el que comienza el núcleo fundamental de la memoria. Tras analizar algunas propiedades de $\mathbb{Z}[i]$, definimos el esquema sobre este anillo y demostramos que esta definición funciona correctamente. A continuación estudiamos algunas de sus propiedades. En particular demostramos que toda estructura de acceso puede realizarse mediante un esquema de Mignotte sobre $\mathbb{Z}[i]$ y caracterizamos las obtenidas a partir de secuencias de módulos coprimos. Mostramos que las técnicas desarrolladas en capítulos anteriores son también suficientes en este caso, y realizamos una doble extensión del esquema: por un lado a uno general (no necesariamente umbral, como sucede siempre en la bibliografía y recogíamos en los capítulos anteriores), y por otro lado al conjunto numérico $\mathbb{Z}[i]$.

Durante el capitulo 4 nos ocuparemos del problema de los mentirosos: uno, -o varios- participantes pueden mentir sobre su participación, con el fín de obtener el secreto ilícitamente y engañar al resto. Mostraremos cómo para los esquemas generales de Mignotte sobre $\mathbb{Z}[i]$ esto no es tan simple de hacer. Para ello adoptaremos el punto de vista -inédito en la literatura- del participante deshonesto, buscando la mejor estrategia que puede seguir para maximizar, en lo posible, su impunidad.

La memoria termina con un Anexo en el que señalamos posibles extensiones de estos sistemas a otros conjuntos numéricos y, en definitiva, posibles líneas de investigación futuras. Además, como advertimos previamente, incluimos una implementación del esquema de Mignotte con el programa MAPLE. A partir de una estructura de acceso arbitraria, se computa el esquema que la realiza siguiendo el procedimiento diseñado en el Capítulo 3, y se llevan a cabo los procesos de reparto de un secreto y su posterior recuperación.

0.3. Nuevos resultados

Los resultados obtenidos en los Capítulos 3 y 4 son, por lo que sabemos, nuevos. En cuanto al Capítulo 3, esto incluye algunas propiedades de $\mathbb{Z}[i]$, la extensión del esquema de Mignotte a $\mathbb{Z}[i]$, la demostración de que toda estructura de acceso es realizable de esta forma y sobre este anillo, y la caracterización de las estructuras obtenidas en el caso de que los módulos tomados sean coprimos. Estos resultados han dado lugar a un artículo de investigación, que puede encontrarse en la base de datos arXiv [22] y que en este momento se encuentra sometido para su publicación en la revista *Journal of Algebra, Combinatorics, Discrete Structures and Applications*.

También son nuevos la aproximación al problema de los mentirosos del Capítulo 4 y las estrategias sugeridas para llevarlo a cabo.

1

Reparto de secretos mediante el teorema Chino de los restos

Este capítulo es esencialmente descriptivo y en buena parte sigue el esquema trazado en [21]. Nuestro propósito es enmarcar el problema del reparto de secretos mediante el teorema Chino, que será un tema recurrente a lo largo de la memoria. La exposición que presentamos dista mucho de ser exhaustiva. Un estudio detallado de estos temas puede encontrarse en [29, 32, 28] para la criptografía de clave pública en general, en [31, 32] para el reparto de secretos, y [5, 7, 25] para la base algebraica.

1.1. El reparto de secretos

En muchas situaciones prácticas, una información debe ser compartida (o una acción que dependa de ella debe ser llevada a cabo) por un grupo de personas de manera coordinada. El estudio de este problema ha dado lugar a los llamados *esquemas de reparto de secretos*, que forman hoy en día un activo campo de investigación. Como advertimos en la Presentación, además de sus utilidades obvias de gestión de claves y similares, estos esquemas juegan un papel relevante en temas como las votaciones electrónicas, la computación multiparte y la criptografía corporativa. En secciones posteriores de esta memoria nos centraremos en los esquemas de reparto de secretos obtenidos por aplicación del teorema Chino de los restos.

1.1.1. Esquemas para repartir secretos

El origen del estudio del reparto de secretos suele fecharse en 1979, año en que A. Shamir publicó su famoso artículo [30]. De manera formal, sean $\mathscr{P} = \{1, \ldots, n\}$ un conjunto de *participantes* y $\mathscr{S}$ un conjunto numérico finito y no vacío, al que llamaremos *conjunto de secretos*. Se desea repartir 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, uniendo las participaciones de sus miembros, recuperar s; y 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 se conoce como *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 $A' \in \mathscr{A}$.

Decimos 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 pueda descartarse ningún $s \in \mathscr{S}$ como posible secreto repartido. Algunos autores consideran una definición más restrictiva de esquema perfecto, exigiendo no solamente la condición anterior sino 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. Nos 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, esto es: dada una estructura de acceso $\mathscr{A}$ ¿existe algún esquema que la realice? (es decir, que la tenga efectivamente como estructura de acceso) y ¿cómo obtenerlo? 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 [17], mediante un método constructivo basado en la lógica booleana.

Estos resultados, sin embargo, no completan el estudio de la teoría, ya que otra cualidad importante de un esquema $\mathscr{R}$ es el tamaño de las participaciones s_i asignadas a cada participante. 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, la coalición $A \setminus \{i\}$ esté también autorizada. La participación s_i de un participante redundante i es irrelevante para el esquema.

Proposición 1.1.1. *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 $|\mathscr{S}| \sim |\mathscr{S}_i|$ para todo $1 \leq i \leq n$, es decir, si el tamaño de las participaciones es similar al 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 $\rho(\mathscr{R}) = 1$. Los esquemas de Ito, Saito y Nishizeki están lejos de ser ideales.

1.1.2. Esquemas umbral. El esquema de Shamir

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 $A \in \mathscr{A}$ son exáctamente los subconjuntos de $\mathscr{P}$ con al menos t participantes. En tal caso decimos que $\mathscr{A}$ es una estructura umbral de tipo (t,n). Estas son las estructuras más simples y para las que primeramente se obtuvieron esquemas de reparto.

El más conocido de todos los esquemas umbral (y de hecho, de todos los esquemas de reparto de secretos) se debe a Shamir [30]. 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 e igualmente probable. Es claro que el esquema es perfecto e ideal.

1.1.3. Esquemas umbral ponderados

En los esquemas umbral todos los participantes juegan un papel equivalente, lo que resulta poco compatible con muchas situaciones prácticas. Una variación obvia para tratar de resolver este problema es asignar pesos a los participantes. Así, tomaremos una n-upla $\mathbf{w} = (w_1,\ldots,w_n)$ de n enteros positivos y un umbral t. La *estructura de acceso umbral ponderada* asociada a $\mathbf{w}$ y t es la que tiene por coaliciones autorizadas a los subconjuntos de $\mathscr{P}$, los pesos de cuyos miembros sumen al menos t.

Una realización trivial de esta estructura puede obtenerse en la misma línea de la de Shamir, asignando a cada participante tantos datos como su peso. Observemos, no obstante, que esta realización obliga a repartir una cantidad de información muy superior a la del secreto compartido, y por tanto queda lejos de ser ideal.

1.2. El teorema Chino de los restos

Los esquemas de reparto que nos interesan están basados en el siguiente teorema.

1.2.1. El teorema para módulos coprimos

Teorema 1.2.1. (Chino de los restos para módulos coprimos) *Sean $m_1,\ldots,m_n \in \mathbb{Z}$ mayores o iguales que 2 y coprimos dos a dos, es decir* $\mathrm{mcd}(m_i,m_j)=1$ *para cada $i \neq j$. Dados enteros arbitrarios $a_1,\ldots,a_n \in \mathbb{Z}$, el sistema de ecuaciones en congruencias*

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

tiene 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

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

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

$$x = a_1 q_1 r_1 + \cdots + a_n q_n r_n \equiv a_i q_i r_i \equiv a_i \,(\mathrm{mod}\, m_i) \qquad i = 1, \ldots, n,$$

ya que r_i es inverso de q_i. Además esta solución es única módulo m. En efecto, si y fuera otra solucion, entonces $n_i | (x - y)$ 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.

1.2.2. El teorema Chino para módulos no coprimos

En el caso de que los módulos de las ecuaciones no sean coprimos, descomponemos cada una de las ecuaciones en tantas otras como factores primos posea el módulo que aparece en ella. El sistema transformado tiene solución si las nuevas ecuaciones obtenidas son compatibles entre sí.

Teorema 1.2.2. (Chino de los restos 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*

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

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

Demostración. Si existe solución, x, entonces para cada i, se verifica $x \equiv a_i \,(\mathrm{mod}\, m_i)$, luego $m_i | (x - a_i)$, y por tanto, para todo j, $\mathrm{mcd}(m_i, m_j) | (x - a_i)$. Análogamente se verifica que $\mathrm{mcd}(m_i, m_j) | (x - a_j)$, por lo que $\mathrm{mcd}(m_i, m_j) | ((x - a_j) - (x - a_i)) = a_i - a_j$. 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 $x \equiv a \,(\mathrm{mod}\, m)$ si y sólo si $x \equiv a \,(\mathrm{mod}\, p_k^{e_k})$ para todo primo de la factorización de m. Supongamos pues que $\mathrm{mcd}(m_i, m_j) | (a_i - a_j)$ para todos i, j. Sea p^e uno de los factores en la descomposición prima de $\mathrm{mcm}(m_1, \ldots, m_n)$. 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, $x \equiv a_i \,(\mathrm{mod}\, p^{e_i})$ 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 es de módulos coprimos, y por tanto el teorema Chino, 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 $x \equiv y \pmod{\text{mcm}(m_1, \ldots, m_n)}$. □

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

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, criptografía, etc., se han estudiado implementaciones eficientes del teorema, tanto en su versión original para módulos coprimos [10], como en su versión general, [6].

1.3. Esquemas de Mignotte

Pasamos ya a describir el esquema ed Mignotte, tanto en su version original [20], como algunas de sus generalizaciones.

1.3.1. El esquema de Mignotte 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 esquema. Dada una secuencia de este tipo, el esquema de Mignotte permite repartir un secreto del conjunto $\mathscr{S} = \{s \in \mathbb{Z} : m_{n-t+2} \cdots m_n < s < m_1 \cdots m_t\}$ como sigue: a cada participante i se le asigna su módulo m_i. Estos módulos pueden ser públicamente conocidos y reutilizados tantas veces como se desee. Dado el secreto $s \in \mathscr{S}$

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

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

Proposición 1.3.1. *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 está 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 $x \neq s$. □

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 puede 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 descartando los anteriormente mencionados, todavía existan 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 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 $(0 < s < m_1 \cdots m_t - m_{n-t+2} \cdots m_n)$. 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.

1.3.2. El esquema umbral de Mignotte para módulos no coprimos

El esquema umbral de Mignotte admite una extensión clara 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. 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 $\operatorname{mcm}(C) = \operatorname{mcm}(m_i \mid i \in C)$ y definimos

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

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

Tanto el funcionamiento del esquema como su análisis son completamente análogos a los del caso original. Dada una secuencia $\mathbf{m}$ que satisfaga la condición generalizada t de Mignotte y dado un secreto s del espacio de secretos $m^- < s < m^+$, 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

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

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 $\mathrm{mcm}(A)$. Como $s < m^+ \leq \mathrm{mcm}(A)$, deducimos que $s = x$. Para una coalición no autorizada B, como $\mathrm{mcm}(B) < t$, el sistema (S_B) proporciona una solución $x < \mathrm{mcm}(B) < s$, luego $x \neq s$.

1.3.3. Estructuras de acceso generales

Como mencionamos al comienzo del capítulo anterior, 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:

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

$$\mathscr{A} = \mathscr{A}(\mathbf{m}, m^+) = \{A \subseteq \mathscr{P} : \mathrm{mcm}(A) \geq m^+\}.$$

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

$$x \equiv s_i \pmod{m_i} \quad i \in C.$$

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

1.4. El esquema de Asmuth-Bloom

La segunda familia de esquemas de reparto basadas en el teorema Chino, es la de Asmuth-Bloom, [1]. Dado que estamos mayormente interesados en la de Mignotte, nos ocuparemos de esta familia de manera mucho más somera.

El esquema de Asmuth-Bloom se basa en los mismos principios que el Mignotte, pero 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 1.4.1. *El método descrito es correcto y proporciona un esquema umbral de tipo (t,n) 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 $m_{n-t+2} \cdots m_n < s + a m_0 < (a+1) m_0 \leq m_0 m_{n-t+2} \cdots m_n < m_1 \cdots m_t$.
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 $s + a m_0$ son soluciones, y ambas verifican $x, s + a m_0 < m_A$, la unicidad de la solución que garantiza el teorema Chino implica que $x = s + a m_0$, 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 $x < m_B \leq m_{n-t+2} \cdots m_n < s + a m_0$, deducimos que $x \neq s + a m_0$ 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 $s + a m_0 \pmod{m_B}$ es también solución del sistema (S_B), y ésta es única, se verifica que $s + a m_0 = x + \lambda m_B$ 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 posibles elecciones de λ. Como estas son 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. □

El esquema de Asmuth-Bloom es débilmente perfecto pero no fuertemente perfecto: 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. Obsérvese también que la condición de que m_0 sea primo no es necesaria. En efecto, esta condición se utiliza únicamente para asegurar que $\text{mcd}(m_0, m_A) = 1$ en la demostración, para lo que es suficiente que los $m_0, m_1, \ldots, m_n$ sean coprimos dos a dos.

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.

1.5. Dos extensiones de Mignotte y una de Asmuth-Bloom

Los esquemas de Mignotte y Asmuth-Bloom han sido extendidos por diversos autores, para poder ser definidos sobre conjuntos numéricos distintos de $\mathbb{Z}$. En esta sección describimos tres de estas extensiones, hechas a $\mathbb{F}_q[X]$ y $\mathbb{Z}[i]$. Como veremos, las correspondientes al primero de estos anillos son correctas, pero la extensión de Mignotte al segundo anillo no lo es.

1.5.1. Esquemas polinómicos de Mignotte

Sea $\mathbb{F}_q$ un cuerpo finito con q elementos, y sea $\mathbb{F}_q[X]$ el anillo de polinomios sobre $\mathbb{F}_q$. El teorema Chino de los restos se verifica en $\mathbb{F}_q[X]$ (como veremos en el capítulo próximo), lo que autoriza a extender los esquemas de reparto basados en él a este anillo. En el caso de Mignotte, esta extensión fue tratada y estudiada en [8, 9].

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 $\text{mcm}(C) = \text{mcm}\{m_i(X) \ : \ i \in C\}$. Si la secuencia $\mathbf{m}$ verifica que $\deg(\text{mcm}(A)) > \deg(\text{mcm}(B))$ para todos $A \in \mathscr{A}, B \notin \mathscr{A}$, definimos

$$m^+ = \text{mín}\{\deg(\text{mcm}(A)) \ : \ A \in \mathscr{A}\}, \qquad m^- = \text{máx}\{\deg(\text{mcm}(B)) \ : \ B \notin \mathscr{A}\}$$

y sea $\mathscr{S} = \{s(X) \in \mathbb{F}_q[X] \ : \ m^- < \deg(s(X)) < m^+\}$ 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 $\mathrm{mcm}(A)$. Como $\deg(s(X)) < \deg(\mathrm{mcm}(A))$, se verifica que $s(X) = x(X)$. Una coalición no autorizada B que desee recuperar el secreto, puede resolver el sistema

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

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

De manera complementaria a la anterior, dados un conjunto $\mathscr{P} = \{1,\ldots,n\}$ de n participantes y una secuencia $\mathbf{m}: m_1(X),\ldots,m_n(X)$ de n polinomios, tomemos dos enteros $m^- < m^+$ tales que el intervalo (m^-,m^+) no continene a $\deg(\mathrm{mcm}(C))$ para ningún $C \subseteq \{1,\ldots,n\}$. Consideremos entonces la estructura de aceso

$$\mathscr{A} = \mathscr{A}(m^-,m^+) = \{C \subseteq \{1,\ldots,n\} \ : \ \deg(\mathrm{mcm}(A)) \geq m^+\}$$

y el espacio de secretos $\mathscr{S} = \{s(X) \in \mathbb{F}_q[X] \ : \ m^- < \deg(s(X)) < m^+\}$. El mismo razonamiento de la Sección 1.3.3 anterior demuestra que el esquema polinómico de Mignotte basado en la secuencia $\mathbf{m}$, realiza la estructura de acceso $\mathscr{A}$ con el espacio de secretos $\mathscr{S}$.

1.5.2. Esquemas polinómicos de Asmuth-Bloom

Las extensión del esquema umbral de Asmuth-Bloom a $\mathbb{F}_q[X]$ fue llevada a cabo en [23] y sigue las mismas pautas que las del de Mignotte. 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

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

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

Proposición 1.5.1. *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 y no vamos a repetirlo 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.

Una propiedad interesante de este esquema, es que el esquema de Shamir (como hemos dicho, el más conocido de todos), puede verse como un caso particular del de Asmuth-Bloom polinómico. 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 $s_i = f(X) \pmod{X - \alpha_i} = f(\alpha_i)$.

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

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

La solución de este sistema es

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

es decir, justamente la expresión de Lagrange del polinomio interpolador de $f(X)$, luego $x(X) = f(X)$. El secreto es $x(X) \pmod X = x(0) = f(0)$.

1.5.3. Esquemas umbral de Mignotte sobre $\mathbb{Z}[i]$

Del mismo modo que $\mathbb{F}_q[X]$, el anillo de enteros de Gauss $\mathbb{Z}[i]$ admite un teorema Chino de los restos (cuyo estudio, de nuevo, relegamos al capítulo próximo). Esto permite extender a $\mathbb{Z}[i]$ los esquemas de reparto basados en este teorema.

El esquema de Mignotte, en su version umbral más simple, fue extendida al anillo $\mathbb{Z}[i]$ en el artículo [26], donde esta extensión se utiliza para desarrollar un método de reparto secreto de imágenes (pues el anillo $\mathbb{Z}[i]$ parece adaptarse particularmente bien a algunas características de ciertos formatos de imagen). Esta última parte pertenece al dominio de la ingeniería de 'software' y no vamos a indagar en ella, limitándonos a la parte relativa al reparto de secretos.

La descripción del método vuelve a ser análoga a las tratadas anteriormente (para el caso umbral). Sea N la norma en $\mathbb{Z}[i]$, es decir, $N(a+bi) = a^2 + b^2$. Para repartir un secreto entre los participantes $\mathscr{P} = \{1, \ldots, n\}$, de manera que t cualesquiera de ellos puedan recuperarlo, comenzamos tomando una secuencia $\mathbf{m} : m_1, \ldots, m_n$ de enteros gaussianos dos a dos coprimos, tales que $N(m_1) < \cdots < N(m_n)$ y $N(m_{n-t+2} \cdots m_n) < N(m_1 \cdots m_t)$. El conjunto de secretos es $\mathscr{S} = \{s \in \mathbb{Z}[i] : N(m_{n-t+2} \cdots m_n) \leq N(s) < N(m_1 \cdots m_t)\}$. El reparto de un secreto, y su posterior reconstrucción, siguen la pauta habitual: dado $s \in \mathscr{S}$, la participación de i es $s_i = s \pmod{m_i}$. Una coalición A con $|A| \geq t$, puede recuperar el secreto resolviendo el sistema

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

Veamos un ejemplo. Reproducimos literalmente (adaptando la notación) el Ejemplo 3.3 de [26].

Let us construct a $(2,3)$ *threshold secret sharing scheme based on a specific Euclidean domain, i.e. Gaussian integers* $\mathbb{Z}[i]$*. We choose three coprime Gaussian numbers,* $11+8i; -3-13i; 7+4i$ *and compute their norms 185; 178; 65 (*$N(a+bi) = a^2+b^2$*) respectively. Dealer chooses the norm of the secret inside the following interval* $185 < s < 11570$*. Suppose that dealer chooses the norm of the secret as 424 and a Gaussian integer* $18-10i$*. After choosing the secret, dealer computes the shares of participants as follows:*

$$\begin{array}{ll} 18-10i \equiv -1-7i \pmod{11+8i}) & \Rightarrow s_1 = -1-7i; \\ 18-10i \equiv 5-7i \pmod{-313i}) & \Rightarrow s_2 = 5-7i; \\ 18-10i \equiv 3 \pmod{7+4i}) & \Rightarrow s_3 = 3: \end{array}$$

Hence a $(2,3)$ *threshold secret sharing scheme is designed such that any 2 out of 3 participants can reconstruct the secret. We pick participants 1 and 3 and compute the secret in the following way:*

$$\mathbb{Z}[i]/(11+8i) \times \mathbb{Z}[i]/(7+4i) \to \mathbb{Z}[i]/(45+100i)$$

$$(-1-7i)(7+4i)[(7+4i)^{-1}(\text{mod } 11+8i)] + 3(11+8i)[(11+8i)^{-1}(\text{mod } 7+4i)]$$

After computing the inverse of Gaussian integers, we substitute the values and the secret is computed as follows

$$s = (-1-7i)(7+4i)(-12+2i) + 3(11+8i)(7-2i) \pmod{45+100i} \equiv 18-10i.$$

Sin embargo, aplicando el mismo procedimiento al secreto $s = 70-70i$ (nótese que $N(s) = 9800$, luego s es un secreto válido), las participaciones resultan ser $s_1 = 1+2i, s_2 = 4, s_3 = 3-i$. La coalición $\{2,3\}$ intenta recuperar este secreto. Realizando el mismo procedimiento que anteriormente, obtenemos la solución $s = -1+97i$, es decir, un secreto incorrecto.

Uno de nuestros objetivos en este TFM es entender por qué sucede esto. Y también estudiar como puede llevarse a cabo el proceso de manera correcta.

2

Dominios euclídeos. Polinomios y enteros de Gauss

En este capítulo estudiaremos los fundamentos teóricos que nos permiten comprender por qué las extensiones de los esquemas de Mignotte y Asmuth-Bloom a $\mathbb{F}_q[X]$, descritas en la Seccion **1.5** del capítulo anterior, son correctas, mientras que la extensión del primero a $\mathbb{Z}[i]$ no lo es. Asmismo nos permitirán realizar una extensión que sí sea correcta para este último caso. Durante esta sección utilizaremos como referencia fundamentalmente a [5, 7]. A lo largo de toda la memoria, y en particular para esta sección, supondremos todos los anillos conmutativos y con unidad.

2.1. División euclídea y dominios euclídeos

La noción de *dominio euclídeo*[1] 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 $a, b \in A$ con $b \neq 0$, se verifica $\varepsilon(ab) \geq \varepsilon(a)$.

(FE2) para todo par $a, b \in A$ con $b \neq 0$, existen $q, r \in A$ tales que $a = bq + r$ con $\varepsilon(r) < \varepsilon(b)$ o $r = 0$.

Decimos que A es un dominio euclídeo (DE) si admite una función euclídea ε. Todo cuerpo es trivialmente un DE. $\mathbb{Z}$ es también un dominio euclídeo con la función $\varepsilon(a) = |a|$. Otros ejemplos relevantes son $\mathbb{F}_q[X]$ y $\mathbb{Z}[i]$, como veremos más adelante.

Proposición 2.1.1. *Todo dominio euclídeo A es un dominio de ideales principales (DIP).*

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

Como consecuencia, en todo dominio euclídeo existen el máximo común divisor

[1] El adjetivo *euclídeo* ("relativo a Euclides") sigue sin estar reconocido por la RAE, que sólo acepta la lección tradicional *euclidiano*. Sin embargo, como la forma incorrecta *euclídeo* se ha impuesto en la literatura matemática en español de manera prácticamente absoluta, en esta memoria adoptamos esa pauta, dejando constancia mediante esta nota de la tal circunstancia.

(mcd) y el mínimo común múltiplo (mcm) de dos elementos (definidos salvo producto por unidades), y se verifica una identidad de Bézout.

Proposición 2.1.2. *Sea A un DIP y sean $a,b \in A$ dos elementos no nulos. Existe $d \in A$ tal que $d = xa+yb$ con $x,y \in A$ y $d = \mathrm{mcd}(a,b)$.*

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

Además la división euclídea (con respecto a ε) permite un algoritmo de Euclides extendido completamente similar al del caso entero para calcular el máximo común divisor de dos elementos. También permite un teorema Chino de los restos. Como notación, dados $a,b,m \in A$, escribiremos $a \equiv b \pmod{m}$ cuando a y b pertenecen a la misma clase en el anillo cociente $A/(m)$.

Teorema 2.1.3. (Chino de los restos. Versión sobre dominios euclídeos) *Sea A un dominio euclídeo y sean $m_1,\ldots,m_n \in A$. Si $\mathrm{mcd}(m_i,m_j) = 1$ para todos $1 \leq i < j \leq n$, entonces $\mathrm{mcm}(m_1,\ldots,m_n) = m_1,\ldots,m_n = m$, y*

$$A/(m) \cong A/(m_1) \times \cdots \times A/(m_n)$$

Demostración. La aplicación natural $\phi : A \to A/(m_1) \times \cdots \times A/(m_n)$, que envía cada elemento en sus clases módulo $m_1,\ldots,m_n$, $\phi(a) = (a+(m_1),\ldots,a+(m_n))$, es un homomorfismo de anillos. $\phi(a) = 0$ si y sólo si a es divisible por cada uno de los m_i, y por tanto por su producto m. Así $\ker(\phi) = (m)$ y ϕ induce un homomorfismo inyectivo (al que seguimos llamando ϕ) $\phi : A/(m) \cong A/(m_1) \times \cdots \times A/(m_n)$. Para mostrar la sobreyectividad de esta aplicación, sean $a_1,\ldots,a_n \in A$. Mediante el algortimo de Euclides extendido, podemos calcular elementos $e_1,\ldots,e_n \in A$ tales que $e_i \equiv 1 \pmod{m_i}$ y $e_i \equiv 0 \pmod{m_j}$ para todo $j \neq i$. Esto es posible ya que $\mathrm{mcd}(m_i, m/m_i) = 1$, luego el algoritmo de Euclides produce x_i, y_i tales que $x_i m_i + y_i(m/m_i) = 1$, y basta tomar $e_i = y_i(m/m_i)$. Ahora

$$\phi(a_1e_1 + \ldots + a_ne_n) = (a_1,\ldots,a_n)$$

con lo que la aplicación es suprayectiva. □

Obsérvese que, al igual que en $\mathbb{Z}$, la demostración es constructiva y permite calcular la contraimagen de cualquier elemento. De hecho, esta demostración es una forma de ingerpolación de Lagrange para dominios euclídeos arbitrarios. Este teorema admite una extensión para módulos no coprimos, que es exáctamente similar al **Teorema 1.2.2**, tanto en su enunciado como en su demostración, que no repetiremos aquí.

Teorema 2.1.4. (Chino de los restos. Versión sobre dominios euclídeos para módulos no coprimos) *Sea A un dominio euclídeo y sean $a_1,\ldots,a_n,m_1,\ldots,m_n \in A$. El sistema de ecuaciones en congruencias*

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

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

Obsérvese finalmente, que esta versión es constructiva a condición de que seamos capaces de factorizar los módulos $m_1, \ldots, m_n$.

2.2. El dominio euclídeo $\mathbb{F}_q[X]$

Proposición 2.2.1. *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 sumo $n-m$ 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 (FE2), $\deg(r(X)) < \deg(g(X))$ o $r(X) = 0$. En efecto, 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 $r_1(X) - r_2(X) = 0$.

2.3. Unicidad de la división euclídea

Destaquemos que la unicidad de cociente y resto en la división euclídea, $a = bq + r$ con $\varepsilon(r) < \varepsilon(b)$ o $r = 0$, no se ha exigido en la definicion de función euclídea. Por ejemplo,

no es cierta ni siquiera sobre el anillo de enteros, ya que el resto puede tomarse positivo o negativo

$$5 = 2 \times 2 + 1, \qquad 5 = 2 \times 3 - 1$$

con $|-1| = |1| = 1$. Esta unicidad es esecial para poder definir unívocamente un representante de una clase en $A/(m)$, es decir, para definir una función *módulo*. Siempre que esto sea posible y todos los términos involucrados en el esquema de Mignotte pueden tomarse sin ambiegüedad, el esquema funcionará correctamente. Si $\mathbb{K}$ es un cuerpo, la división es única, con resto siempre 0. Asimismo en el anillo de polinomios $\mathbb{K}[X]$ esta unicidad se verifica siempre, como acabamos de ver. Sobre $\mathbb{Z}$ habitualmente la aseguramos imponiendo la condición extra de que el resto sea no negativo, aunque esta condición no procede de las (FE1,FE2). ¿En qué otros dominios euclídeos se verifica la unicidad? La respuesta puede encontrarse en [18].

Teorema 2.3.1. *Los únicos dominios euclídeos para los que se verifica la unicidad de la división eulídea son los cuerpos $\mathbb{K}$ y los anillos de polinomios sobre un cuerpo $\mathbb{K}[X]$.*

Para probar este teorema nos serán precisos unos resultados previos. Dado el anillo A, denotaremos por A^* el conjunto (grupo) de sus unidades. Dos elementos a y b son *asociados* si uno de ellos se obtiene del otro multiplicando por una unidad, $b = au$.

Sea A un dominio euclídeo con función euclídea ε. Para todo $a \in A$ no nulo, se verifica que $\varepsilon(a) \geq \varepsilon(1)$ por (FE1). Podemos suponer pues que $\varepsilon(1) = 0$, pues en otro caso basta sustituir ε por ε' definido $\varepsilon'(a) = \varepsilon(a) - \varepsilon(1)$, que continua siendo una función euclídea.

Lema 2.3.2. *Sea A un dominio euclídeo con función euclídea ε. Dados $a, b \in A$ no nulos, se verifican las siguientes propiedades:*
(a) si a y b son asociados, entonces $\varepsilon(a) = \varepsilon(b)$;
(b) si a es un divisor propio de b, entonces $\varepsilon(a) < \varepsilon(b)$;
(c) $A^* = \{a \in A : \varepsilon(a) = 0\}$.

Demostración. (a) $\varepsilon(a) \leq \varepsilon(ua) \leq \varepsilon(u^{-1}ua)$. (b) Dividiendo, $a = cb + r$. Si $r = 0$, entonces $a|b$ y $b|a$ por lo que ambos elementos serían asociados. Luego $r \neq 0$ y en consecuencia $\varepsilon(r) < \varepsilon(b)$. Por otro lado, como $a|b$, existe a' tal que $b = a'a$. Por tanto $r = a - cb = (1 - ca')a$, por lo que $\varepsilon(a) \leq \varepsilon(r)$, y deducimos que $\varepsilon(a) < \varepsilon(b)$. (c) es consecuencia de (a) y (b). □

Lema 2.3.3. *Sea A un dominio euclídeo con función euclídea ε. La división euclídea en A, con respecto a ε, es única si y sólo si para cada par de elementos no nulos $a, b \in A$, se verifica que $\varepsilon(a+b) \leq \max\{\varepsilon(a), \varepsilon(b)\}$.*

Demostración. Supongamos que esta condición sobre ε se verifica. Si

$$\begin{array}{ll} a = bq + r & \text{con } \varepsilon(r) < \varepsilon(b) \text{ o } r = 0; \\ a = bq' + r' & \text{con } \varepsilon(r') < \varepsilon(b) \text{ o } r' = 0 \end{array}$$

con $q \neq q'$ y $r \neq r'$, según las propiedades (FE1) y (FE2)

$$\varepsilon(b) \leq \varepsilon((q' - q)b) = \varepsilon(r' - r).$$

Si $r = 0$, entonces esta igualdad implica que $r' = 0$, luego $r = r', q = q'$. Si $r \neq 0, r' \neq 0$, nuestra condición sobre ε proporciona

$$\varepsilon(b) \leq \varepsilon((q'-q)b) = \varepsilon(r'-r) \leq \text{máx}\{\varepsilon(r'), \varepsilon(-r)\} < \varepsilon(b)$$

ya que $\varepsilon(r) = \varepsilon(-r)$. Pero esto es imposible, y por tanto la división es única. Recíprocamente, si la condición enunciada no se verifica, existen $a, b \in A$ tales que $\varepsilon(a+b) > \text{máx}\{\varepsilon(a), \varepsilon(b)\}$, luego tenemos las dos escrituras

$$a = 0(a+b) + a = 1(a+b) - b$$

verificando la condición (FE2). □

Lema 2.3.4. *Sea A un dominio euclídeo con función euclídea ε. Si la división euclídea en A, con respecto a ε, es única, entonces si denotamos por A^* al grupo de unidades, $K = A^* \cup \{0\}$ es un cuerpo.*

Demostración. Basta ver que la suma de dos unidades es de nuevo una unidad. Dadas $u_1, u_2 \in K$, se verifica que

$$\varepsilon(u_1 + u_2) \leq \text{máx}\{\varepsilon(u_1), \varepsilon(u_2)\} = 0$$

luego $u_1 + u_2 \in K$. □

*Demostración del **Teorema 2.3.1**.* Sea A un dominio euclídeo en el que la división euclídea es única. Si A es un cuerpo hemos acabado. Si no, sea $x \in A$ un elemento para el que $\varepsilon(x)$ es mínimo entre las no unidades de A. Según el Lema 2.3.2 (b), la sucesión $\varepsilon(x^k)$, $k = 0, 1, \ldots$ es estrictamente creciente. Por tanto, dado $a \in A$ no nulo, existe k tal que $\varepsilon(x^k) \leq \varepsilon(a) < \varepsilon(x^{k+1})$. Realizando la división, $a = q_k x^k + r_k$, con $r_k = 0$ o $\varepsilon(r_k) < \varepsilon(x^k)$. Veamos que $q_k \in A^*$. Si esto no fuera así, se tendría $q_k = lx + m$, con $m = 0$ o $\varepsilon(m) < \varepsilon(a)$, luego, en cualquier caso, con $m \in A^*$ y consecuentemente $l \neq 0$. Por el Lema 2.3.3

$$\varepsilon(a) \geq \varepsilon(a - x^k - r_k) = \varepsilon(lx^{k+1}) \geq \varepsilon(x^{k+1})$$

en contra de la elección de k. Por tanto $q_k \in A^*$. Si $r_k = 0$ hemos encontrado la escritura $a = q_k x^k$. Si $r_k \neq 0$ podemos aplicar iteradamente el mismo argumento, obteniendo por inducción una escritura

$$a = \sum_{j=0}^{k} q_j x^j, \qquad \text{con } q_j \in A^*$$

Esta escritura es única. En efecto, si $\sum_{j=n}^{t} s_j x^j = 0$ para ciertos $s_j \in A^*$, con $s_n \neq 0$, entonces

$$-s_n = x \left(\sum_{j=n+1}^{t} s_j x^{j-n-1} \right)$$

que implica $0 = \varepsilon(-s_n) \geq \varepsilon(x)$, lo que contradice la elección de x. Por tanto todos los s_j deben ser nulos. Hemos definido así un isomorfismo $A \cong K[x] \cong K[X]$. □

Entendemos ahora por qué las distintas versiones del esquema de Mignotte (y del de Asmuth-Bloom) funcionan correctamente sobre $\mathbb{Z}$ y $\mathbb{F}_q[X]$, ya que todos los elementos

que intervienen en ellas están definidos sin ambiguedad, mientras que no sucede así sobre $\mathbb{Z}[i]$, lo que conduce a errores. Nuestra próxima tarea es estudiar en detalle este anillo $\mathbb{Z}[i]$, para poder desarrollar sobre él una versión que sí funcione adecuadamente.

2.4. El dominio euclídeo $\mathbb{Z}[i]$

Se llama *anillo de enteros de Gauss* a $\mathbb{Z}[i] = \{a+bi \ : \ a,b \in \mathbb{Z}\} \subseteq \mathbb{C}$. Este anillo fue introducido por C.F. Gauss en [11], con el propósito de estudiar la ley de recíprocidad bicuadrática (que establece la relación entre las ecuaciones $x^4 \equiv p \pmod{q}$ y $x^4 \equiv q \pmod{p}$). En esta sección trataremos sus principales propiedades aritméticas, [5, 7]. Observemos en primer lugar que, como $\mathbb{C}$ es un cuerpo, $\mathbb{Z}[i]$ es un dominio de integridad.

2.4.1. División euclídea

Llamamos *norma* de un elemento $z = a+bi \in \mathbb{Z}[i]$ a $N(z) = z\bar{z} = a^2+b^2$, siendo $\bar{z}$ el conjugado complejo de z. Por tanto $N(z)$ es un entero no negativo y $N(z) \not\equiv 3 \pmod{4}$ (pues es suma de dos cuadrados). Como la conjugación es multiplicativa, también lo es la norma, $N(zv) = N(z)N(v)$, y N verifica la condición (FE1) de función euclídea.

Proposición 2.4.1. *Para todos $v,z \in \mathbb{Z}[i]$ con $z \neq 0$, se verifica $N(v) \leq N(vz)$.*

Otra consecuencia de la multiplicatividad de la norma es que las unidades deben tener norma 1. Existen cuatro elementos de norma 1, que son $\pm 1, \pm i$ y, como se comprueba trivialmente, los cuatro son unidades. La más importante propiedad aritmética de $\mathbb{Z}[i]$ es la existencia de una división con resto.

Teorema 2.4.2. *Dados $v,z \in \mathbb{Z}[i]$ con $z \neq 0$, existen $q,r \in \mathbb{Z}[i]$ tales que $v = zq+r$ y $N(r) < N(z)$.*

Como ya hemos tratado, a diferencia de lo que ocurre en $\mathbb{Z}$ o $\mathbb{F}_q[X]$, cociente q y resto r no son únicos. Por ejemplo

$$10i = (5+4i)(1+i)+(-1+i) = (5+4i)(1+2i)+(3-4i).$$

La unicidad es esencial para nosotros, ya que todas las herramientas aritméticas que utilizaremos (algoritmo de Euclides, módulo en un anillo cociente, teorema Chino) se basan en la división euclídea. Y naturalmente, en los esquemas de reparto de secretos, deseamos que el secreto recuperado sea exáctamente el mismo que se repartió. En la siguiente demostración del Teorema 2.4.2 veremos que tomando los q y r de una forma particular, se pueden asegurar su unicidad y la condición adicional $N(r) \leq N(z)/2$.

Demostración. Consideremos el número complejo $v/z = x+yi$. Sean a y b los (únicos) enteros más próximos a sus partes real e imaginaria, $-1/2 < x-a \leq 1/2$, $-1/2 < y-b \leq 1/2$, y sea $q = a+bi$. Entonces $N(v/z-q) \leq 1/2$ y se tiene la escritura y $v = zq+(z(v/z-q)) = zq+r$ con $r = z(v/z-q)$ y $N(r) = N(z(v/z-q)) = N(z)N(z/v-q) \leq N(z)/2$. $\square$

Como consecuencia de los dos resultados anteriores, $\mathbb{Z}[i]$ es un dominio euclídeo. Admite un algoritmo de Euclides y un teorema Chino de los restos operativos, similares a los de $\mathbb{Z}$. Debemos, no obstante, ser cuidadosos para mantener en todo momento la unicidad en los resultados obtenidos. Veremos más adelante que este algoritmo da un resto único bajo determinadas circunstancias.

2.4.2. Ideales de $\mathbb{Z}[i]$

Como es sabido (Proposición 2.1.1), todo DE es un DIP. Un ideal I de $\mathbb{Z}[i]$ está generado por un solo elemento z que tiene norma mínima de entre todos los de I. Claro está que si z es un generador de I, también lo son sus *asociados* (productos de z por una unidad) $-z, \pm zi$. Recíprocamente, estos son los únicos generadores de I: si v es otro generador, $I = (v)$, entonces $z = uv$ luego $N(z) = N(u)N(v)$ y como $N(z)$ es mínima, necesariamente $N(u) = 1$, es decir, u es una unidad y v y z son asociados. Se llama norma de I a la norma de cualquiera de sus generadores, denotada por $N(I)$.

Es posible fijar un único generador (de entre los cuatro asociados) para cada ideal I. El método más simple es tomar de entre esos generadores asociados, aquel que esté en el primer cuadrante. A veces se usa también el método siguiente.

Sea $I = (z)$ con $z = a + bi$. Veamos primero el caso en que $N(I)$ es impar. En ese caso, uno de los enteros a o b (pero no ambos) es impar. Por tanto, uno y sólo uno de los asociados de z, $a+bi, -a-bi, b-ia, -b+ia$ tiene parte real impar y positiva. Es ese el que elegimos como generador normalizado. Veamos ahora el caso en que $N(I)$ es par. Como a y b son ambos pares o ambos impares, z es divisible entre $1+i$. Si $N(z) = 2$ elegimos el generador $1+i$. Si $N(z) > 2$, dividimos reiteradamente z entre $1+i$ hasta obtener un cociente z' tal que $N(z') = 2$ o $N(z')$ sea impar. Entones elegimos el asociado de z' según los criterios anteriores y deshacemos el proceso.

2.4.3. Primos en $\mathbb{Z}[i]$

Puesto que $\mathbb{Z}[i]$ es u DIP, los conceptos de *primo* e *irreducible* son equivalentes en $\mathbb{Z}[i]$. En esta sección vamos a caracterizar los primos de $\mathbb{Z}[i]$. Naturalmente, si z es primo también lo son sus asociados $-z, \pm zi$, y su conjugado $\bar{z}$ (por la multiplicabilidad de la conjugación).

Los primeros candidatos a ser primos en $\mathbb{Z}[i]$ son los primos en $\mathbb{Z}$. No todo primo de $\mathbb{Z}$ se mantiene primo en $\mathbb{Z}[i]$. Por ejemplo, $2 = (1+i)(1-i) = -i(1+i)^2$.

Proposición 2.4.3. *Un primo p de $\mathbb{Z}$ es reducible en $\mathbb{Z}[i]$ si y sólo si $p = 2$ o $p \equiv 1 \pmod 4$.*

Para probar este resultado, utilizaremos el teorema de los dos cuadrados[2] que afirma que un primo (de $\mathbb{Z}$) $p > 2$ es suma de dos cuadrados si y sólo si $p \equiv 1 \pmod 4$. Demostraremos este teorema en un apéndice, al final del capítulo.

Demostración. Como hemos visto, 2 es reducible en $\mathbb{Z}[i]$. Sea pues $p > 2$. Si p es reducible en $\mathbb{Z}[i]$, entonces $p = (a+bi)(c+di)$, no siendo ninguno de esos factores una

[2]El problema fue inicialmente propuesto por Diofanto, y la solución enunciada por Fermat (naturalmente, sin demostración) y probada por Euler. Incluimos una prueba en un apéndice al final del capítulo.

unidad. Entonces $p^2 = N(p) = (a^2+b^2)(c^2+d^2)$. Como esta es una igualdad en $\mathbb{Z}$, donde p es primo, deducimos $p = a^2+b^2 = c^2+d^2$, luego $p \equiv 1 \pmod 4$. Recíprocamente, si $p \equiv 1 \pmod 4$ entonces p es suma de dos cuadrados, con lo que $p = a^2+b^2 = (a+bi)(a-bi)$. □

Proposición 2.4.4. *Sea $z = a+bi \in \mathbb{Z}[i]$.*
(1) Si $N(z) = p$, siendo p un primo de $\mathbb{Z}$, entonces z es primo en $\mathbb{Z}[i]$.
(2) Si z es primo en $\mathbb{Z}[i]$, entonces bien $N(z) = p$, o bien $N(z) = p^2$ para algún primo p de $\mathbb{Z}$ asociado de z.

Demostración. (1) Si $z = uv$ entonces $p = N(z) = N(u)N(v)$, con lo que $N(u) = 1$ o $N(v) = 1$ y alguno de ellos es una unidad en $\mathbb{Z}[i]$. (2) Como $N(z) = z\bar{z}$, se verifica que $z|N(z)$. Sea $N(z) = p_1 \cdots p_t$ la descomposición en primos de $N(z)$ sobre $\mathbb{Z}$. Por ser z primo, $z|p_i$ para alguno de los p_i anteriores. Llamemos p a este primo y escribamos $z = pv$ para algún $v \in \mathbb{Z}[i]$. Entonces $N(z)|N(p) = p^2$ en $\mathbb{Z}$, luego $N(z) = p$ ó $N(z) = p^2$. En ese último caso, como $z = pv$, deducimos que $p^2 = N(z) = N(p)N(v) = p^2N(v)$, luego $N(v) = 1$ y v es una unidad. □

A partir de estos resultados podemos caracterizar los primos de $\mathbb{Z}[i]$.

Teorema 2.4.5. *Un elemento $z \in \mathbb{Z}[i]$ es primo en $\mathbb{Z}[i]$ si y sólo si*
(i) su norma $N(z)$ es prima en $\mathbb{Z}$; o
(ii) es asociado de un primo p de $\mathbb{Z}$ con $p \equiv 3 \pmod 4$ (y por tanto $N(z) = p^2$).

De este modo, la factorización de $N(z)$ en $\mathbb{Z}$ puede ser utilizada para encontrar la factorización de z en $\mathbb{Z}[i]$. Recordemos que, como vimos en el Teorema 2.1.4, cuando se desea resolver un sistema en conguencias cuyos módulos no son coprimos, es esencial conocer la factorización prima de estos módulos. Podemos utilizar en la expresión de cada factor primo, la escritura descrita en la Sección 2.4.2 para hacerla única.

Ejemplo 2.4.6. Calculemos la factorización de $z = 43+1247i$. Como $N(z) = 1556858 = 2 \cdot 43^2 \cdot 421$, y $43 \equiv 3 \pmod 4$ es primo en $\mathbb{Z}[i]$, resulta $z = (1+i) \cdot 43 \cdot v$, siendo v un primo de norma 421. Ahora bien, $421 = 15^2+14^2$ de manera única. Operando obtenemos $v = 15+14i$.

2.4.4. Factorización y máximo común divisor

Como en cualquier DFU, todo elemento $z \in \mathbb{Z}[i]$ admite una factorización como producto de primos, que es única salvo orden y producto por unidades, es decir, salvo elección de los asociados de cada primo. Obsérvese que para todo primo z de $\mathbb{Z}[i]$, o bien $N(z) = 2$ o bien $N(z)$ es impar. En el primer caso elegimos el asociado $1+i$ de z; en el segundo, el asociado de la forma $a+bi$ con a impar y positivo.

Se define el máximo común divisor de dos enteros de Gauss u, v, de la forma habitualen un DE, como el mayor elemento z que divide simultáneamente a ambos. Dado que en $\mathbb{Z}[i]$ no existe un orden compatible con sus operaciones, 'mayor' significa que para todo $w \in \mathbb{Z}[i]$ tal que $w|u, w|v$, también $w|z$. Es decir, $z = \text{mcd}(u,v)$ es el divisor común de mayor norma. Equivalentemente, en términos de ideales, $(z) = (u,v)$. Por consiguiente,

el máximo común divisor está definido salvo producto por unidades, y podemos hacerlo único, de nuevo como en la Sección 2.4.2.

Conocida la factorización de u y v es inmediato encontrar $\mathrm{mcd}(u,v)$. Por supuesto es más simple calcularlo utilizando el algoritmo de Euclides, que funciona de manera absolutamente similar a la de $\mathbb{Z}$. También es similar al caso de $\mathbb{Z}$ el algoritmo de Euclides extendido, que proporciona explícitamente los coeficientes de la identidad de Bézout.

2.4.5. El anillo cociente $\mathbb{Z}[i]/(z)$

La mayor dificultad operativa en el manejo de los anillos cociente (y en el proceso de tomar módulos) radica en el hecho de que no se tiene unicidad en la división euclídea, $v = zq + r$, ni siquiera imponiendo al condición $N(r) \leq N(z)/2$. Como este hecho es relevante para la implementación de los esquemas de reparto de secretos, lo ilustramos mediante un ejemplo.

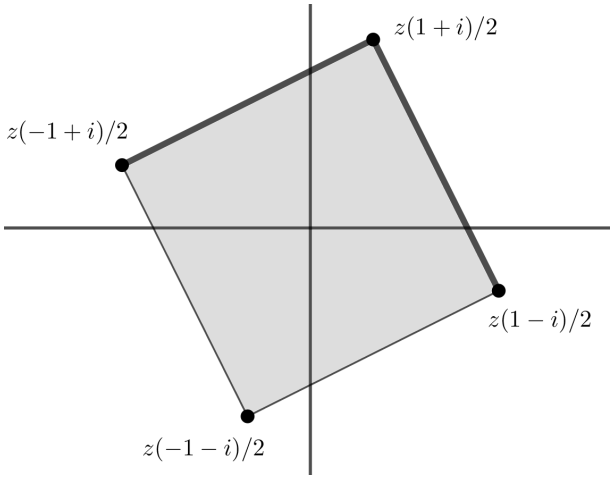
Ejemplo 2.4.7. Consideremos el anillo cociente $\mathbb{Z}[i]/(1+i)$. Elementos $u \in \mathbb{Z}[i]$ con norma $N(u) \leq N(1+i)/2 = 1$ son $\{0, \pm 1, \pm i\}$, y todos ellos pueden aparecer como restos mod $1+i$. Sin embargo no representan clases distintas en el cociente, pues $-i \equiv 1 \pmod{1+i}$. De hecho $\mathbb{Z}[i]/(1+i) = \{0+(1+i), 1+(1+i)\}$.

Así pues, para encontrar un representante normalizado de $v \pmod z$ seguiremos el procedimiento de división establecido en la demostración del Teorema 2.4.2 que, al realizar la división euclídea $v = zq + r$, siempre proporciona un resto r en el conjunto

$$\mathscr{F}(z) = \{z(\alpha + \beta i) \in \mathbb{C} \,:\, -\frac{1}{2} < \alpha \leq \frac{1}{2}, -\frac{1}{2} < \beta \leq \frac{1}{2}\}.$$

Diremos que $\mathscr{F}(z)$ el el *recinto fundamental* de z y, para los propósitos de esta memoria, que el representante r de $v + (z)$ en $\mathscr{F}$, obtenido como se describe en la demostración del Teorema 2.4.2, es el *valor principal* de $v \pmod z$; lo escribiremos $r = v \pmod{\mathbf{mod}\ z}$. Obsérvese que, geométricamente, $\mathscr{F}(z)$ es el cuadrado semiabierto de $\mathbb{C}$ con centro en 0 y vértices

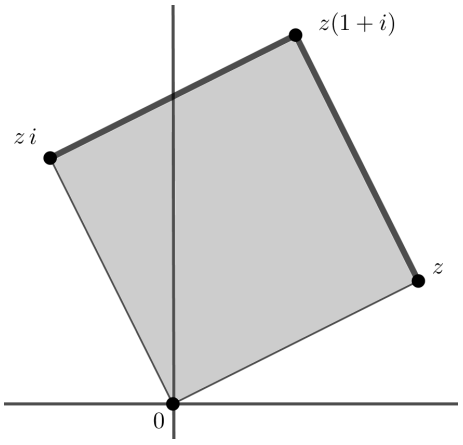
$$z(\tfrac{1}{2} + \tfrac{1}{2}i),\ z(\tfrac{1}{2} - \tfrac{1}{2}i),\ z(-\tfrac{1}{2} - \tfrac{1}{2}i),\ z(-\tfrac{1}{2} + \tfrac{1}{2}i).$$



Como el cuadrado se ha tomado semiabierto y su lado mide $|z| = \sqrt{N(z)}$, el resto en este conjunto es único.

Proposición 2.4.8. *Sea $z \in \mathbb{Z}[i]$, $z \neq 0$. El anillo cociente $\mathbb{Z}[i]/(z)$ tiene cardinal $N(z)$.*

Para demostrar esta proposición, en lugar del recinto fundamental que acabamos de definir, vamos a elegir otro (trasladado del fundamental) que nos permitirá simplificar las cuentas. Así, en la demostración del Teorema 2.4.2, sustituimos la condición $-1/2 < x-a \leq 1/2$, $-1/2 < y-b \leq 1/2$ por la condición $0 < x-a \leq 1$, $0 < y-b \leq 1$. Como entonces, para toda clase $v+(z)$ fijamos un representante único en el conjunto $F = \{z(\alpha+\beta i) \mid \alpha, \beta \in (0,1]\} \subset \mathbb{C}$. Recíprocamente, todo entero de Gauss $u \in F$ es representante de alguna clase (de la clase $u+(z)$ por ejemplo). Por tanto, el cardinal del cociente $\mathbb{Z}[i]/(z)$ coincide con el número de enteros de Gauss en F. Geométricamente F es un cuadrado semiabierto, de vértices $0, z, z+iz, iz$ (como en la figura, que corresponde a $z = 2+i$).



Para calcular $|\mathbb{Z}[i]/(z)|$ vamos a utilizar un resultado geométrico conocido como teorema de Pick.

Lema 2.4.9 (Teorema de Pick)**.** *Un polígono P de $\mathbb{R}^2$ con vértices en puntos de $\mathbb{Z}^2$, tiene área $a+b/2-1$, siendo a el número de puntos de $\mathbb{Z}^2$ en el interior de P y b el número de puntos de $\mathbb{Z}^2$ en la frontera de P.*

Para no llevar la exposición demasiado lejos de nuestros intereses, que se centran en el reparto de secretos, no vamos a probar aquí el teorema de Pick. Una demostración puede encontrarse en [2].

Demostración de la Proposición 2.4.8. El área de F es $N(z)$, puesto que cada lado del cuadrado mide $|z|$. Cada entero de Gauss en el interior de F corresponde a una clase en $\mathbb{Z}[i]/(z)$. Los enteros de Gauss en la frontera de F aparecen por pares (en lados opuestos de F), que corresponden a la misma clase (por eso hemos tomado el cuadrado semiabierto). Finalmente, los cuatro vértices de F corresponden a la misma clase. En total, el número de clases es $a+(b-4)/2+1 = area(F) = N(z)$, según el teorema de Pick.[3] □

[3]Por otro lado, el resultado es intuitivamente claro: cada entero de Gauss ocupa un cuadrado de una unidad de lado; por tanto F contiene tantos enteros de Gauss como su área.

2.4.6. El problema del círculo de Gauss

Estrechamente relacionado con la última pregunta que nos hemos formulado está el *problema del círculo de Gauss:* ¿cuántos enteros de Gauss hay en un círculo de $\mathbb{C}$ con radio $r \geq 0$ centrado en 0? o equivalentemente si $r \in \mathbb{Z}$, ¿cuántos $z \in \mathbb{Z}[i]$ con $N(z) \leq N(r)$ existen? Denotaremos este número por $\mathfrak{N}(r)$.

Son conocidas fórmulas explícitas para $\mathfrak{N}(r)$, por ejemplo, [13],

$$\mathfrak{N}(r) = 1 + 4 \sum_{j=0}^{\infty} \left(\left\lfloor \frac{r^2}{4j+1} \right\rfloor - \left\lfloor \frac{r^2}{4j+3} \right\rfloor \right).$$

Sin embargo estas fórmulas son, como se ve, difíciles de calcular. Afortunadamente existen muy buenas aproximaciones sencillas, que son más que suficientes para nuestros propósitos. Por ejemplo, el mismo argumento que antes utilizábamos: un recinto regular de $\mathbb{C}$ contiene aproximadamente tantos enteros de Gauss como su área, proporciona la aproximación

$$\mathfrak{N}(r) \sim \pi r^2$$

que resulta muy satisfactoria. La tabla siguiente muestra los valores de $\mathfrak{N}(r)$ y $\lfloor \pi r^2 \rfloor$ para $0 \leq r \leq 10$.

r	0	1	2	3	4	5	6	7	8	9	10
$\mathfrak{N}(r)$	1	5	13	29	49	81	113	149	197	253	317
$\lfloor \pi r^2 \rfloor$	0	3	12	28	50	78	113	153	201	254	314

2.5. Apéndice. El teorema de los dos cuadrados

La pregunta de qué primos pueden ser escritos como suma de dos cuadrados fue ya planteada por Diofanto. En 1640 Fermat anunció el teorema de los dos cuadrados en una carta a Mersenne, sin demostración. La primera prueba de este teorema se debe a Leonhard Euler. Actualmente son conocidas muchas demostraciones de este resultado. La que incluimos aquí procede de [33].

Sea p un entero primo. Si $p = 2$ entonces $p = 1 + 1$ es suma de dos cuadrados. Si p es impar, entonces $p \equiv 1$ o $3 \pmod 4$. Como los únicos cuadrados en $\mathbb{Z}/4\mathbb{Z}$ son 0 y 1, si p es suma de dos cuadrados, necesariamente $p \equiv 1 \pmod 4$.

Teorema 2.5.1. *Todo primo $p \equiv 1 \pmod 4$ es suma de dos cuadrados.*

La demostración de este teorema requiere de unos resultados previos. Sea S un conjunto finito y sea $f : S \to S$. Decimos que f es una *involución* si $f^2 = id$, es decir, si $f(f(x)) = x$ para todo $x \in S$. Un elemento $x \in S$ es un *punto fijo* de f si $f(x) = x$.

Lema 2.5.2. *Si $f : S \to S$ es una involución, entonces el cardinal del conjunto de puntos fijos de f tiene la misma paridad que el cardinal de S.*

Demostración. Si todos los puntos de S son fijos el resultado es obvio. En otro caso, para cada punto no fijo $a \in S$ se verifica que $a \neq f(a)$ y $f(f(a)) = a$, luego estos puntos pueden agruparse por pares $(a, f(a))$. Por tanto el cardinal del conjunto de puntos fijos de f tiene la misma paridad que el cardinal de S. □

Sea p un primo, $p \equiv 1 \pmod 4$. Escribamos $p = 4z_0 + 1$. Consideremos el conjunto

$$S = \{(x,y,z) \in \mathbb{N}_0^3 \ : \ p = x^2 + 4yz\}.$$

Obsérvese que S es finito, y que ningún elemento $(x,y,z) \in S$ puede contener una coordenada nula ni verificar $x = y - z$ ó $x = 2y$, por ser p primo. Por tanto podemos escribir $S = S_1 \cup S_2 \cup S_3$, siendo

$$\begin{aligned} S_1 &= \{(x,y,z) \in S \ : \ x < y - z\}, \\ S_2 &= \{(x,y,z) \in S \ : \ y - z < x < 2y\}, \\ S_3 &= \{(x,y,z) \in S \ : \ 2y < x\}. \end{aligned}$$

Proposición 2.5.3. *El conjunto S que hemos definido tiene cardinal impar.*

Demostración. Consideremos la aplicación $f : S \to S$,

$$f(x,y,z) = \begin{cases} (x+2z, z, y-x-z) & \text{si } (x,y,z) \in S_1; \\ (2y-x, y, x-y+z) & \text{si } (x,y,z) \in S_2; \\ (x-2y, x-y+z, y) & \text{si } (x,y,z) \in S_3. \end{cases}$$

Una comprobación rutinaria muestra que f está bien definida y que es una involución. Además se verifica que $f(x,y,z) \in S_3$ si $(x,y,z) \in S_1$ y que $f(x,y,z) \in S_1$ si $(x,y,z) \in S_3$. Calculemos los puntos fijos de f. Por lo anterior, estos deben estar necesariamente en S_2. Ahora bien, si $(x,y,z) \in S_2$ es uno de ellos, entonces $x = y$ con $p = x^2 + 4yz = x^2 + 4xz = x(x+4z)$. De aquí deducimos que $x = y = 1$ y que $z = z_0$. Como $(1,1,z_0)$ sí es un punto fijo de f, deducimos que es el único punto fijo. Según el Lema 2.5.2, la paridad del cardinal de S coincide con la del conjunto de puntos fijos, luego es impar. □

Demostración del Teorema 2.5.1. Consideremos la aplicación $g : S \to S$, $g(x,y,z) = (x,z,y)$. Como el cardinal de S es impar, de nuevo según el Lema 2.5.2, g posee algún punto fijo (x,y,z). Luego $y = z$, y como $(x,y,z) \in S$, se verifica que $p = x^2 + 4yz = x^2 + 4y^2$, con lo que p es suma de dos cuadrados. □

3

Un esquema de Mignotte sobre $\mathbb{Z}[i]$

Este capítulo contiene el núcleo fundamental de la memoria. Es aquí donde estableceremos la (una) extensión del esquema de reparto de Mignotte, en su versión más general, a $\mathbb{Z}[i]$. Para ello será preciso asegurar en todo momento que los elementos que intervienen en esta extensión estén definidos correctamente y de manera unívoca, garantizando así que el secreto recuperado coincida exáctamente con el original que se repartió originalmente. Una vez hecho esto, estudiaremos también algunas propiedades del esquema obtenido.

3.1. La extensión propuesta

Comenzamos desarrollando algunos resutados sobre la aritmética del dominio euclídeo $\mathbb{Z}[i]$, que utiliaremos más adelante.

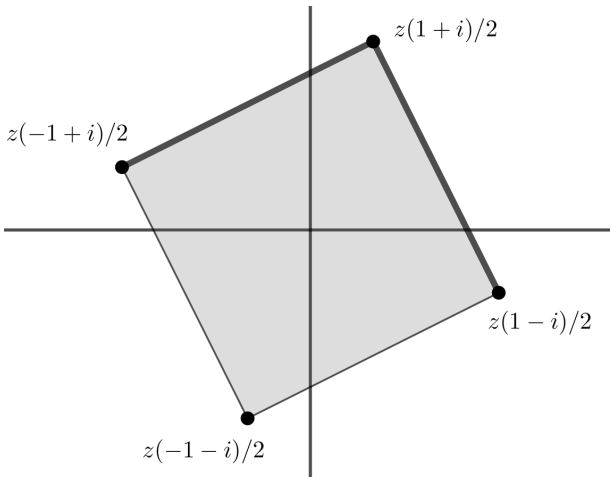
3.1.1. Recintos fundamentales y módulos principales

En el capítulo anterior hemos definido el recinto fundamental $\mathscr{F}(z)$ de un entero de Gauss $z \in \mathbb{Z}[i]$,

$$\mathscr{F}(z) = \{z(\alpha+\beta i) \in \mathbb{C} \,:\, -\frac{1}{2} < \alpha, \beta \leq \frac{1}{2}\}$$

que, geométricamente, es el cuadrado semiabierto de $\mathbb{C}$, centrado en 0, de lado $|z| = \sqrt{N(z)}$ y con vértices

$$z(\tfrac{1}{2}+\tfrac{1}{2}i),\ z(\tfrac{1}{2}-\tfrac{1}{2}i),\ z(-\tfrac{1}{2}-\tfrac{1}{2}i),\ z(-\tfrac{1}{2}+\tfrac{1}{2}i).$$



También hemos visto como para todo $v \in \mathbb{Z}[i]$, la división euclídea $v = qz + r$ deja un único resto r en $\mathscr{F}(z)$. Además el cálculo de este resto es operativo, siguiendo el procedimiento descrito en la demostración del **Teorema 2.4.2**, y se verifica que $N(r) \leq N(z)/2$. Para los efectos de esta memoria, diremos que tal r es el *módulo principal* de v por z, y escribiremos

$$r = v \ (\textbf{mod}\ z).$$

Además de $\mathscr{F}(z)$ consideraremos el *recinto fundamental estricto* de z, que es el conjunto $\mathscr{F}^o(z)$ de los puntos que están en $\mathscr{F}(z)$ pero no en su frontera

$$\mathscr{F}^o(z) = \{z(\alpha+\beta i) \in \mathbb{C} \ : \ \alpha,\beta \in \mathbb{R}, -\tfrac{1}{2} < \alpha,\beta < \tfrac{1}{2})\}$$

y la *clausura* de $\mathscr{F}(z)$

$$\overline{\mathscr{F}}(z) = \{z(\alpha+\beta i) \in \mathbb{C} \ : \ \alpha,\beta \in \mathbb{R}, -\tfrac{1}{2} \leq \alpha,\beta \leq \tfrac{1}{2})\}.$$

Claramente $\mathscr{F}^o(z) \subset \mathscr{F}(z) \subset \overline{\mathscr{F}}(z)$. La siguientes proposiciones establecen algunas propiedades que serán importantes para nuestra extensión del esquema de Mignotte.

Proposición 3.1.1. *Sean $v, z \in \mathbb{Z}[i]$, $z \neq 0$.*
(a) Si $N(v) < N(z)/2$, entonces $\mathscr{F}(v) \subset \mathscr{F}(z)$.
(b) $\{u \in \mathbb{Z}[i] : N(u) < N(z/2)\} \subset \mathscr{F}^o(z) \cap \mathbb{Z}[i] \subset \{u \in \mathbb{Z}[i] : N(u) \leq N(z)/2\}$.

Demostración. (a) Como tanto $\mathscr{F}(v)$ como $\mathscr{F}(z)$ son cuadrados centrados en 0, es suficiente comprobar que la mayor norma de un elemento de $\mathscr{F}(v)$ es menor que la menor norma de un elemento de la frontera de $\mathscr{F}(z)$. Estas normas se alcanzan en $v(\frac{1}{2}+\frac{1}{2}i)$ y $z(\frac{1}{2})$ respectivamente, luego la inclusión es consecuencia de las desigualdades

$$N\left(v(\tfrac{1}{2}+\tfrac{1}{2}i)\right) = \tfrac{1}{2}N(v) < \tfrac{1}{4}N(z) = N\left(z(\tfrac{1}{2})\right).$$

(b) La inclusión de la izquierda se debe a que el elemento con menor norma en la frontera de $\mathscr{F}(z)$ tiene norma $N(z)/4$. La contención de la derecha se debe a la propiedad $N(r) \leq N(z)/2$ de la división euclídea en $\mathbb{Z}[i]$. □

Las unidades de $\mathbb{Z}[i]$ coinciden con sus elementos de norma 1, es decir, $\pm 1, \pm i$. Los *asociados* de un entero gaussiano z son los productos uz, siendo u una unidad. Así los asociados de z son $\pm z, \pm iz$. Naturalmente dos asociados z y uz generan el mismo ideal en $\mathbb{Z}[i]$. Por tanto, dados $z_1, \ldots, z_n \in \mathbb{Z}[i]$, las expresiones $\text{mcd}(z_1, \ldots, z_n)$ y $\text{mcm}(z_1, \ldots, z_n)$ están definidas salvo asociados. Notemos que en general $\mathscr{F}(z) \neq \mathscr{F}(uz)$ luego, para $v \in \mathbb{Z}[i]$, puede darse $v \ (\textbf{mod}\ z) \neq v \ (\textbf{mod}\ uz)$. Por ejemplo, $z/2 \in \mathscr{F}(z)$ pero $z/2 \notin \mathscr{F}(-z)$ y, si $z/2 \in \mathbb{Z}[i]$, entonces $z/2 \ (\textbf{mod}\ z) = z/2, z/2 \ (\textbf{mod}\ -z) = -z/2$.

Proposición 3.1.2. *Sean u, v, z, tres enteros gaussianos tales que u es una unidad. Se verifican las siguientes propiedades.*
(a) $\mathscr{F}^o(z) = \mathscr{F}^o(uz)$ y $\overline{\mathscr{F}}(z) = \overline{\mathscr{F}}(uz)$.
(b) Si $v \ (\textbf{mod}\ z) \in \mathscr{F}^o(z)$, entonces $v \ (\textbf{mod}\ uz) = v \ (\textbf{mod}\ z)$.

Demostración. La demostración de (a) se sigue directamente de las definiciones de $\mathscr{F}^o(z)$ y $\overline{\mathscr{F}}(z)$. (b) Si $v = qz + r$ entonces también $v = (q/u)uz + r$, luego el resultado es consecuencia de (a). □

Como consecuencia de este resultado, si se verifica que $v \pmod{\text{mcm}(z_1,\ldots,z_n)} \in \mathscr{F}^o(\text{mcm}(z_1,\ldots,z_n))$ para alguna elección concreta de $\text{mcm}(z_1,\ldots,z_n)$ y alguna elección concreta de $v \pmod{\text{mcm}(z_1,\ldots,z_n)}$, entonces el entero gaussiano dado por la expresión v (**mod** $\text{mcm}(z_1,\ldots,z_n)$) está determinado unívocamente, y además se verifica que v (**mod** $\text{mcm}(z_1,\ldots,z_n)) \in \mathscr{F}^o(\text{mcm}(z_1,\ldots,z_n))$.

Proposición 3.1.3. *Sean v_1, v_2, z enteros gaussianos tales que $v_1, v_2 \in \overline{\mathscr{F}}(z)$. Si $v_1 \equiv v_2 \pmod{z}$ y $v_1 \in \mathscr{F}^o(z)$, entonces $v_1 = v_2$.*

Demostración. Si $v_1 \equiv v_2 \pmod{z}$ con $v_1 \in \mathscr{F}^o(z), v_2 \in \overline{\mathscr{F}}(z)$, entonces existe una unidad u tal que $v_1, v_2 \in \mathscr{F}(uz)$. El resultado es consecuencia de la unicidad del resto en un recinto fundamental. □

3.1.2. El esquema de Mignote en $\mathbb{Z}[i]$

Una vez que todas las herramientas algebraicas que precisamos han sido desarrolladas, vamos a especificar el esquema.

Sea $\mathscr{P} = \{1,\ldots,n\}$ un conjunto de n participantes entre los que deseamos repartir un secreto. Sea $\mathbf{m} : m_1, m_2, \ldots, m_n$, una secuencia de n enteros de Gauss no nulos y no necesariamente coprimos. Asignamos m_i al participante i. Como en capítulos anteriores, dada una coalición $C \subseteq \mathscr{P}$ de participantes, escribiremos $\text{mcm}(C) = \text{mcm}\{m_i \ : \ i \in C\}$. Diremos que $N(\text{mcm}(C))$ es la norma de C.

Sean m^-, m^+ dos enteros tales que $4m^- < m^+$ y el intervalo (m^-, m^+) no contiene la norma de ninguna coalición de participantes, es decir, tal que para toda coalición C, o bien $N(\text{mcm}(C)) \leq m^-$ o bien $N(\text{mcm}(C)) \geq m^+$. Asociada a estos datos, podemos considerar la estructura de acceso que tiene como coaliciones autorizadas

$$\mathscr{A} = \{A \subseteq \mathscr{P} \ : \ N(\text{mcm}(A)) \geq m^+\}.$$

Obviamente la familia $\mathscr{A}$ es monótona, luego define una estructura de acceso válida. Vamos a construir un esquema de reparto $\mathscr{R}$ de tipo Mignotte, que permite realizar esta estructura y tiene como conjunto de secretos a

$$\mathscr{S} = \{s \in \mathbb{Z}[i] \ : \ m^- \leq N(s) < \frac{m^+}{4}\}.$$

El procedimiento es como sigue. Dado un secreto $s \in \mathscr{S}$, el gestor calcula las participaciones s_i como $s_i = s$ (**mod** m_i). En este proceso no es realmente necesario tomar módulos normalizados, pero sí conveniente, ya que puede reducir el tamaño de las participaciones. Cuando una coalición autorizada A desea recuperar el secreto, resuelve el sistema de ecuaciones en congruencias

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

cuya solución es única módulo $\text{mcm}(A)$. El secreto es x (**mod** $\text{mcm}(A)$).

Nótese que para cualquier coalición C, el sistema correspondiente, (S_C), posee solución, puesto que $s \pmod{\text{mcm}(C)}$ lo es. Así sólo necesitamos del teorema Chino un método para encontrarla y garantizar su unicidad.

Proposición 3.1.4. *El método descrito es correcto y proporciona un esquema de reparto para la estructura $\mathscr{A}$.*

Demostración. Una coalición autorizada A puede resolver el sistema y, a partir de su solución x, calcular $x \ (\mathbf{mod}\ \mathrm{mcm}(A)) \in \mathscr{F}(\mathrm{mcm}(A))$. Como se verifica que $N(s) < m^+/4 \leq N(\mathrm{mcm}\ (A))/4$, según las Proposiciones 3.1.1 y 3.1.2, se verifica que $s \in \mathscr{F}^o(\mathrm{mcm}(A))$ para cualquier elección de $\mathrm{mcm}(A)$. Así, según la Proposición 3.1.3, se verifica que $x \ (\mathbf{mod}\ \mathrm{mcm}(A)) = s$, luego el secreto recuperado es correcto. Una coalición no autorizada B puede encontrar una solución x de (S_B) módulo $\mathrm{mcm}(B)$. Como $N(s) \geq m^- \geq N(\mathrm{mcm}(B)) > N(x)$, deducimos que $s \neq x$. B puede también calcular $x \ (\mathbf{mod}\ \mathrm{mcm}(B)) \in \mathscr{F}(\mathrm{mcm}(B))$. Pero como $N(s) > m^-/2 > N(\mathrm{mcm}(B))/2$, de nuevo según la Proposición 3.1.1, se verifica que $s \notin \mathscr{F}(\mathrm{mcm}(B))$, por lo que $x \ (\mathbf{mod}\ \mathrm{mcm}(B)) \neq s$. □

3.1.3. Un ejemplo

Para fabricar un esquema de reparto umbral sobre seis participantes, con umbral 4. consideramos la secuencia $\mathbf{m} : 100+89i, 100-89i, 98+93i, 98-93i, 101+90i, 101-90i$. En este caso, todos los módulos son primos. Puede comprobarse que el intervalo $(6113415248054, 107002269048912168)$ no contiene la norma de ninguna coalición (con respeto a $\mathbf{m}$). En efecto, toda coalición de 4 o más participantes tiene norma mayor, y toda coalición de 3 o menos, tiene norma menor. El espacio de secretos será

$$\mathscr{S} = \{s \in \mathbb{Z}[i] \ : \ 6113415248054 \leq N(s) \leq 26750567262228042\}.$$

Tomemos el secreto $s = 12345678 + 4567890i$, que tiene norma 173281384331784. Las participaciones son

$$\begin{array}{lll} s_1 = -69+15i, & s_2 = -11-54i, & s_3 = 31+35i, \\ s_4 = -13-26i, & s_5 = 21+64i, & s_6 = -62-33i. \end{array}$$

La coalición autorizada $A = \{1,2,3,4\}$ desea recuperar el secreto. Para ello resuelve el sistema

$$\begin{cases} x \equiv -69+15i \pmod{100+89i} \\ x \equiv -11-54i \pmod{100-89i} \\ x \equiv \ \ 31+35i \pmod{98+93i} \\ x \equiv -13-26i \pmod{98-93i} \end{cases}$$

lo que le proporciona la solución $x = 12345678+4567890i = s$, igual al secreto repartido. Si la coalición no autorizada $B = \{2,3,4\}$ desea recuperar el secreto, puede resolver el sistema

$$\begin{cases} x \equiv -11-54i \pmod{100-89i} \\ x \equiv \ \ 31+35i \pmod{98+93i} \\ x \equiv -13-26i \pmod{98-93i} \end{cases}$$

que le proporciona la solución $x = -1252807+314941i \neq s$, y que no le permite recuperar el secreto.

3.1.4. Sobre el ejemplo de [26]

Como hemos señalado ya muchas veces, la extensión del esquema de Mignotte a $\mathbb{Z}[i]$ dada en [26] no funciona correctamente. En la Sección **1.5.3** mostramos un ejemplo de esta extensión (tomado de [26]), en el que dos secretos eran repartidos. En un caso la recuperación era correcta y en el otro claramente no lo era. Veamos ahora la razón de aquellos hechos.

Recordemos que se construía un esquema umbral $(2,3)$ mediante la secuencia $\mathbf{m} : 11+8i, -3-13i, 7+4i$. Dejando aparte la inconsecuencia de tomar módulos en $\mathbb{Z}[i]$ sin ninguna precaución previa, los autores afirman que el espacio de secretos asociado a esta secuencia es

$$\mathscr{S} = \{s \in \mathbb{Z}[i] \ : \ 185 \leq N(s) < 11570\}.$$

Sin embargo, según nuestros cálculos, el espacio de secretos debe ser

$$\mathscr{S} = \{s \in \mathbb{Z}[i] \ : \ 185 \leq N(s) < 2892\}.$$

El primero de los secretos repartidos en la Sección **1.5.3** era $s = 18-10i$, cuya norma es 424 y es, por tanto, un secreto válido. La recuperación era correcta. El segundo de los secretos repartidos era $s = 70-70i$, cuya norma es 9800 y por tanto no es un secreto válido (en nuestro análisis). La recuperación no puede por tanto ser correcta.

3.2. Algunas propiedades

Terminamos el capítulo estudiando algunas propiedades del esquema que hemos construido.

3.2.1. Tasa de información

Calcular la tasa de información del esquema nos lleva al *problema del círculo de Gauss*, que describimos en la Sección **2.4.6**, y que, recordemos, pregunta cuántos enteros de Gauss hay en un círculo de $\mathbb{C}$ con radio $r \geq 0$ centrado en 0, ó equivalentemente si $r \in \mathbb{Z}$, cuántos $z \in \mathbb{Z}[i]$ con $N(z) \leq N(r) = r^2$ existen. Denotamos este número por $\mathfrak{N}(r)$ y, como vimos en esa Sección **2.4.6**, lo aproximamos por:

$$\mathfrak{N}(r) \sim \pi r^2.$$

El número de posibles secretos que pueden repartirse es aproximadamente

$$|\mathscr{S}| = \mathfrak{N}(\frac{\sqrt{m^+ - 1}}{2}) - \mathfrak{N}(\sqrt{m^- - 1}) \sim \pi \left(\frac{m^+}{4} - m^- \right).$$

Incluimos por completitud una expresión exacta para esta cantidad, aunque a menudo resulte más conveniente utilizar la aproximación.

$$|\mathscr{S}| = \mathfrak{N}(\frac{\sqrt{m^+ - 1}}{2}) - \mathfrak{N}(\sqrt{m^- - 1})$$

$$= 4\sum_{j=0}^{\infty}(\lfloor\frac{m^+-1}{16j+16}\rfloor - \lfloor\frac{m^+-1}{16j+12}\rfloor) - \{4\sum_{j=0}^{\infty}(\lfloor\frac{m^--1}{4j+1}\rfloor - \lfloor\frac{m^--1}{4j+3}\rfloor)\}$$

Por otro lado, el conjunto $\mathscr{S}_i$ de posibles participaciones para el participante i es el conjunto de clases de congruencia en el anillo cociente $\mathbb{Z}[i]/(m_i)$, que como vimos en la **Proposición 2.4.8**, es $N(m_i)$. La tasa de información del participante i es

$$\rho_i \sim \left(\frac{m^+}{4} - m^-\right)/N(m_i).$$

3.2.2. El esquema no es perfecto

El esquema no es perfecto (como sucede con el de Mignotte original). Una coalición no autorizada B puede resolver (S_B) y calcular $x = s \pmod{\text{mcm}(B)}$. Por tanto puede deducir que el secreto es de la forma $x + \lambda\ \text{mcm}(B)$ para algún $\lambda \in \mathbb{Z}[i]$. Consecuentemente puede descartar todos los secretos de $\mathscr{S}$ que no satisfagan esa condición. Como $N(\text{mcm}(B)) < m^-$, de este modo B puede reducir la cantidad de secretos a aproximadamente

$$\frac{\pi(m^+ - 4m^-)/4}{N(\text{mcm}(B))} > \frac{\pi(m^+ - 4m^-)}{4m^-}.$$

Por tanto este número debe ser suficientemente grande para garantizar la seguridad del sistema. De nuevo por completitud incluimos la expresión exacta, valiendo las mismas consideraciones que hacíamos previamente.

$$\left\{4\sum_{j=0}^{\infty}(\lfloor\frac{m^+-1}{16j+16}\rfloor - \lfloor\frac{m^+-1}{16j+12}\rfloor) - \{4\sum_{j=0}^{\infty}(\lfloor\frac{m^-}{4j+1}\rfloor - \lfloor\frac{m^-}{4j+3}\rfloor)\}\right\}/N(lcm(B))$$

Ejemplo 3.2.1. Sea $\mathbf{m}$ la secuencia de enteros gaussianos coprimos $\mathbf{m} : 15+14i, 10-18i, 13+16i$. Tomemos $m^- = 425, m^+ = 178504$. Esta elección conduce a una estructura umbral $(2,3)$. El conjunto de secretos es $\mathscr{S} = \{s \in \mathbb{Z}[i] : 425 \leq N(s) \leq 44625\}$ y su cardinal es

$$|\mathscr{S}| = \mathfrak{N}(\sqrt{44625}) - \mathfrak{N}(\sqrt{424}) \sim 138858,$$

mientras que el conjunto de posibles participaciones tiene cardinal a lo sumo $N(13+16i) = 425$. Por supuesto, el esquema no es perfecto. Como hemos descrito, una coalición no autorizada B puede reducir el conjunto de secretos a uno de tamaño aproximadamente

$$\frac{\pi\left((m^+/4) - (m^-)\right)}{m^-} \approx 327.$$

3.2.3. Toda estructura puede realizarse mediante un esquema de Mignotte en $\mathbb{Z}[i]$

Una cuestión interesante es caracterizar las estructuras de acceso que pueden realizarse mediante un esquema de Mignotte en $\mathbb{Z}[i]$. El siguiente teorema esta inspirado en resultados de [8].

Teorema 3.2.2. *Para cualquier estructura de acceso $\mathscr{A}$ sobre n participantes y cualquier entero S, existe una secuencia $\mathbf{m} : m_1, \ldots, m_n$, de enteros gaussianos tales que el esquema de Mignotte sobre $\mathbb{Z}[i]$ procedente de $\mathbf{m}$ realiza la estructura $\mathscr{A}$ con un conjunto de secretos $\mathscr{S}$ de cardinal $|\mathscr{S}| \geq S$.*

Demostración. Sea $\mathscr{A}$ una estructura de acceso sobre el conjunto $\mathscr{P}$ de n participantes y sean $B_1,\ldots,B_t$ las coaliciones maximales no autorizadas para $\mathscr{A}$. Tomemos t enteros gaussianos coprimos $\mu^{(1)},\ldots,\mu^{(t)}$, con $N(\mu^{(j)})>8$ para todo $j=1,\ldots,t$, y sea $\mu=\mu^{(1)}\cdots\mu^{(t)}$. Para $i=1,\ldots,n$ y $j=1,\ldots,t$, definamos

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

y $m_i=\mu_i^{(1)}\cdots\mu_i^{(t)}$. El esquema de Mignotte asociado a la secuencia $\mathbf{m}:m_1,\ldots,m_n$ realizala estructura $\mathscr{A}$. Para verlo, sean

$$m^+=N(\mu)\ \text{ y }\ \ell=m^+/\text{mín}\{N(\mu^{(1)}),\ldots,N(\mu^{(t)})\}.$$

Notemos que $4\ell<m^+$. 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 $i\in A\setminus B_j$. Así $\mu_i^{(j)}=\mu^{(j)}$ luego $\mu^{(j)}|\text{mcm}(A)$. Este argumento es cierto para todo $j=1,\ldots,t$, por lo que concluimos que $\text{mcm}(A)=\mu$, y por tanto $N(\text{mcm}(A))=m^+$. Recíprocamente, sea B una coalición no autorizada. Existe j tal que $B\subseteq B_j$. Deducimos que $\mu_i^{(j)}=1$ para todo $i\in B$, y por tanto $N(\text{mcm}(B))\leq m^+/N(\mu^{(j)})\leq\ell$. Hemos probado así que $\mathscr{A}=\{A\subseteq\mathscr{P}\mid N(\text{mcm}(A))\geq m^+\}$, luego la secuencia $\mathbf{m}:m_1,\ldots,m_n$ realiza la estructura $\mathscr{A}$ con conjunto de secretos $\mathscr{S}=\{s\in\mathbb{Z}[i]\ :\ m^-\leq N(s)<\frac{m^+}{4}\}$, siendo $m^-=\text{máx}\{N(\text{mcm}(B_1)),\ldots,N(\text{mcm}(B_t))\}\leq\ell$. Como $\frac{m^+}{4}-m^-\geq\ell$, eligiendo los enteros gaussianos $\mu^{(1)},\ldots,\mu^{(t)}$ con norma suficientemente grande, es claro que podemos conseguir $|\mathscr{S}|\geq S$. □

3.2.4. Estructuras umbral ponderadas

El caso más simple de la construcción de Mignotte se da cuando los enteros gaussianos que aparecen en la secuencia $\mathbf{m}$ son coprimos dos a dos. Recordemos que una estructura de acceso $\mathscr{A}$ es *umbral ponderada* cuando existen una n-upla $\mathbf{w}=(w_1,\ldots,w_n)$ de pesos positivos y un umbral t de manera que $\mathscr{A}=\{A\subseteq\mathscr{P}:\sum_{i\in A}w_i\geq t\}$.

Proposición 3.2.3. *Si los enteros gaussianos de la secuencia $\mathbf{m}:m_1,m_2,\cdots,m_n$ son coprimos dos a dos, entonces para cada m^+ la estructura de acceso $\mathscr{A}(\mathbf{m},m^+)$ es umbral ponderada.*

Demostración. Una coalición C está autorizada si y sólo si $N(\text{mcm}(C))=\prod_{i\in C}N(m_i)\geq m^+$, es decir, si y sólo si $\sum_{i\in C}\log(N(m_i))\geq\log(m^+)$, luego $\mathscr{A}(\mathbf{m},m^+)$ es una estructura umbral ponderada con pesos $\log(N(m_i))$, $j=1\ldots,n$, y umbral $\log(m^+)$.
Observemos que podemos tomar pesos reales. En efecto, una estructura umbral ponderada de tipo (w,t,n) no varía al multiplicar w y t por un mismo coeficiente real positivo d, esto es: $\mathscr{A}$ es una estructura (w,t,n) si y sólo si es (wd,td,n). Sea entonces $\mathscr{A}$ una estructura (w,t,n), según lo anterior podemos suponer que $t=1$. Consideramos:

$$\varepsilon=min\{1-w(B):B\subset\mathscr{P},w(B)<1\}>0$$

Para cada $1 \leq i \leq n$, sea w_i' racional y tal que $w_i \leq w_i' \leq w_i + (\varepsilon/n)$. Si B es una coalición no autorizada, se verifica $w`(B) < w(B) + \varepsilon \leq 1$. Por otra parte, si $A$ está autorizada $w'(A) \geq w(A) \geq 1$. Por lo tanto $\mathscr{A}$ es del tipo $(w`, 1, n)$. Para pasar de $w_i' \in \mathbb{Q}$ a enteros basta considerar el máximo común múltiplo de todos sus denominadores d, y resulta que $\mathscr{A}$ es de tipo (dw', d, n). Por lo tanto $\mathscr{A}$ es umbral ponderada y con pesos enteros. □

Ejemplo 3.2.4. Sea **m** la secuencia de enteros gaussianos coprimos $\mathbf{m} : 6+5i, 1-9i, 13+16i$. Tomemos $m^- = 5002, m^+ = 25925$. Estos datos proporcionan la estructura de acceso cuyas coaliciones autorizadas minimales son $\{1,3\}$ y $\{2,3\}$ (las mismas del Ejemplo **??**), que es umbral ponderada con pesos $1,1,2$ y umbral $t = 3$.

4

El problema de los mentirosos

Una de las debilidades potenciales de los esquemas para repartir secretos es el *problema de los mentirosos*: cuando una coalición autorizada de participantes se dispone a recuperar el secreto repartido, alguno (o algunos) de sus miembros pueden mentir sobre su participación, de manera que la coalición recupere un secreto falso y sólamente esos participantes deshonestos se hagan con el auténtico. Una buena descripción general de esta situación se encuentra en [24].

Este tema ha recibido una considerable atención en la literatura. En general, los métodos sugeridos para solucionar el problema se basan en incluir información redundante en base a la cual pueda detectarse la mentira, e incluso al mentiroso. Esta información redundante se presenta a veces aumentando el número de participaciones que recibe cada participante, e.g. [12], y a veces aumentando el número de participantes que intervienen en cada coalición autorizada, [14]. Para el caso particular de los esquemas de tipo Mignotte, sorprendentemente no hemos encontrado más que un sólo trabajo en el que se aborda este estudio, [27], y únicamente para los esquemas umbral obtenidos a partir de secuencias de módulos primos en el caso entero (es decir, el caso original de Mignotte y el más simple posible).

En este capítulo trataremos el problema de los mentirosos para los esquemas de Mignotte generales sobre el anillo de enteros de Gauss $\mathbb{Z}[i]$, tal y como los hemos desarrollado en el capítulo anterior. Al contrario de lo que sucede en otros esquemas de reparto (por ejemplo, en los umbrales de Shamir, donde cualquier mentira es admisible) mentir (bien) en los esquemas generales de Mignotte no resulta tan sencillo y, sin las precauciones adecuadas, puede ser detectado incluso sin medidas adicionales. Por este motivo, y porque no hemos encontrado nada similar en la literatura, como ejercicio puramente académico, hemos decidido orientar el capítulo desde el punto de vista del mentiroso. Así pues, *el problema de los mentirosos* no significa el problema *causado* por los mentirosos, sino el problema *que tienen* los metirosos para llevar a cabo sus engaños.

Para simplificar el estudio, nos limitaremos a tratar el caso de un único participante deshonesto.

Nótese, además, que este método para mentir supone que los módulos asociados a cada participante son conocidos por todos ellos. Esta información suele considerarse pública en la literatura, pero de hecho no hay ninguna ventaja ni ninguna necesidad en que lo sea. Por supuesto, cuando una coalición se dispone a recuperar un secreto, la información sobre sus módulos pasa a ser pública, pero no tiene por qué serlo antes de este momento.

4.1. Cómo mentir

Mantendremos toda la notación introducida en capítulos anteriores. En particular sea $\mathscr{P} = \{1,\ldots,n\}$ un conjunto de n participantes entre los que deseamos repartir un secreto. Sea $\mathbf{m} : m_1, m_2, \ldots, m_n$, una secuencia de n enteros de Gauss no nulos y no necesariamente coprimos. Asignamos m_i al participante i. Dada una coalición $C \subseteq \mathscr{P}$ escribiremos $\mathrm{mcm}(C) = \mathrm{mcm}\{m_i : i \in C\}$ y diremos que $N(\mathrm{mcm}(C))$ es la norma de C. Sean m^-, m^+ dos enteros tales que $4m^- < m^+$ y el intervalo (m^-, m^+) no contiene la norma de ninguna coalición de participantes. Consideramos la estructura de acceso que tiene como coaliciones autorizadas a

$$\mathscr{A} = \{A \subseteq \mathscr{P} : N(\mathrm{mcm}(A)) \geq m^+\}$$

y el esquema de reparto de Mignotte basado en $\mathbf{m}$ que la realiza, con conjunto de secretos

$$\mathscr{S} = \{s \in \mathbb{Z}[i] : m^- \leq N(s) < \frac{m^+}{4}\}.$$

4.1.1. Participantes esenciales

Supongamos que, una vez repartido un secreto $s \in \mathscr{S}$, una coalición autorizada $A = \{1,\ldots,k\}$ (salvo reordenación) decide recuperarlo. Cada miembro de la coalición aporta su participación $s_i \equiv s \pmod{m_i}$. Sin embargo, uno de los participantes, pongamos 1, decide mentir. Para ello aporta una participación falsa $s_1' \neq s_1$. La coalición resuelve el sistema

$$(S_A') : \begin{cases} x \equiv s_1' \pmod{m_1} \\ x \equiv s_i \pmod{m_i}, \ i = 2,\ldots,k \end{cases}$$

y obtiene el (falso) secreto s'. La existencia y consistencia de la solución s' serán tratadas en secciones próximas. Por el momento nos interesa otro aspecto de este proceso. Si la coalición $A^* = \{2,\ldots,k\} = A \setminus \{1\}$ está también autorizada, puede recuperar el secreto resolviendo el sistema

$$(S_{A^*}) : \ x \equiv s_i \pmod{m_i}, \ i = 2,\ldots,k$$

obteniendo ahora el verdadero secreto $s \neq s'$, y detectando el fraude. De hecho esta idea es la base de los sistemas introducidos en [14] para detectar mentirosos.

Diremos que el participante 1 es *esencial* para la coalición autorizada A si $A^* = A \setminus \{1\}$ no está autorizada. Según el razonamiento que hemos expuesto, un participante sólo puede mentir a las coaliciones para las que sea esencial. En adelante, supondremos siempre cierta esta condición.

4.1.2. Obtención ilícita del secreto

De nuevo, supongamos que repartido el secreto $s \in \mathscr{S}$, una coalición autorizada $A = \{1,\ldots,k\}$ decide recuperarlo. Cada miembro de la coalición aporta su participación $s_i \equiv s \pmod{m_i}$. El participante esencial 1 decide mentir, para lo que aporta una participación falsa $s_1' \neq s_1$. Si esta mentira no es detectada, la coalición resuelve el sistema

$$(S_A') : \begin{cases} x \equiv s_1' \pmod{m_1} \\ x \equiv s_i \pmod{m_i}, \ i = 2,\ldots,k. \end{cases}$$

Si el sistema tiene solución s' y $s' \in \mathscr{S}$, la coalición la da por válida. Nótese que $s' \neq s$ es un secreto falso, ya que $s_1 \not\equiv s' \pmod{m_1}$. El participante deshonesto 1 puede, no obstante, recuperar el secreto auténtico s, resolviendo

$$\begin{cases} x \equiv s_1 \pmod{m_1} \\ x \equiv s' \pmod{m_i}, \ i = 2, \ldots, k. \end{cases}$$

que sí tiene solución y es la correcta, ya que $s_i \equiv s' \pmod{m_i}$ para todo $i = 2, \ldots, k$. Por tanto, siendo 1 esencial, si el engaño tiene éxito, permite al participante deshonesto recuperar el secreto en solitario. Para que el engaño tenga éxito deben concurrir las dos condiciones siguientes:

(a) el sistema (S'_A) debe ser compatible,
(b) su solución s' debe pertenecer al espacio de secretos.

4.1.3. Compatibilidad del sistema

En las versiones originales del sistema, los $m_1, \ldots, m_n$ son mutuamente coprimos, con lo que el sistema (S'_A) tiene siempre solución, independientemente del valor elegido para s'_1 (recordemos que en este caso, el esquema de reparto resulta umbral ponderado). Esto facilita la mentira (lo cual da un *plus* de interés a los sistemas en los que estos números no son coprimos).

Supongamos pues que $\text{mcd}\{m_1, \ldots, m_n\} \neq 1$. Según la versión general del teorema Chino de los restos, **Teorema 2.14** , el sistema (S'_A) tiene solución si y sólo si

$$\begin{cases} s'_1 \equiv s_i \pmod{\text{mcd}(m_1, m_i)}, \ 2 \leq i \leq k \\ s_i \equiv s_j \pmod{\text{mcd}(m_i, m_j)}, \ 2 \leq i < j \leq k. \end{cases}$$

Naturalmente 1 desconoce los valores $s_2, \ldots, s_k$. Sin embargo, sí sabe que las condiciones pedidas en la segunda fila de la ecuación se satisfacen automáticamente (suponiendo que sea el único mentiroso de la coalición). En cuanto a las de la primera fila, para su participación legítima s_i, se verifica que $s_1 \equiv s_i \pmod{\text{mcd}(m_1, m_i)}$, $2 \leq i \leq k$, puesto que el sistema no adulterado tiene solución. Por tanto, su única opción es tomar $s'_1 \neq s_1$ que sea solución del sistema

$$s'_1 \equiv s_1 \pmod{\text{mcd}(m_1, m_i)}, \ 2 \leq i \leq k.$$

Como s_1 es la única solución módulo $\text{mcm}\{\text{mcd}(m_1, m_2), \ldots, \text{mcd}(m_1, m_k)\}$, esto es equivalente a $s'_1 \equiv s_1 \pmod{\text{mcm}\{\text{mcd}(m_1, m_2), \ldots, \text{mcd}(m_1, m_k)\}}$. Podemos simplificar esta expresión utilizando el siguiente resultado.

Lema 4.1.1. $\text{mcm}\{\text{mcd}(m_1, m_2), \ldots, \text{mcd}(m_1, m_k)\} = \text{mcd}(m_1, \text{mcm}\{m_2, \ldots, m_k\})$.

Demostración. Si p^r divide a $\text{mcm}\{\text{mcd}(m_1, m_2), \ldots, \text{mcd}(m_1, m_k)\}$, siendo p un primo de Gauss y r máximo con esta condición, entonces divide asimismo a algún $\text{mcd}(m_1, m_i)$, $2 \leq i \leq k$. Por tanto p^r divide a m_1 y a m_i, luego a $\text{mcm}\{m_2, \ldots, m_k\}$, y a $\text{mcd}(m_1, \text{mcm}\{m_2, \ldots, m_k\})$. Recíprocamente, si p^r divide a $\text{mcd}(m_1, \text{mcm}\{m_2, \ldots, m_k\})$, entonces divide a ambos, m_1 y $\text{mcm}\{m_2, \ldots, m_k\}$, luego a alguno de los m_i, $2 \leq i \leq k$. Por tanto p^r divide a $\text{mcd}(m_1, m_i)$ y consecuentemente a $\text{mcm}\{\text{mcd}(m_1, m_2), \ldots, \text{mcd}(m_1, m_k)\}$. □

En definitiva, se verifica el siguiente resultado.

Proposición 4.1.2. *El sistema (S'_A) con la participación falsa s'_1 del participante 1, tiene solución si y sólo si $s'_1 \equiv s_1 \pmod{\mathrm{mcd}(m_1, \mathrm{mcm}(A^*))}$, siendo $A^* = \{2,\ldots,k\} = A \setminus \{1\}$.*

4.1.4. Pertenencia al espacio de secretos

Continuando en la misma situación anterior, el participante 1 de la coalición $A = \{1,\ldots,k\}$ decide mentir sobre su participación, proporcionando s'_1 en lugar del verdadero s_1, lo que llevará al falso secreto s' en lugar del verdadero s. El segundo problema del mentiroso es que puede suceder $s' \notin \mathscr{S}$, con lo que la mentira quedaría en evidencia (y además 1 no recuperaría el secreto). Como el mentiroso no conoce los $s_2,\ldots,s_k$, este riesgo parece imposible de evitar. Veremos no obstante como puede intentar minimizarlo.

Como $s \in \mathscr{S}$, la mejor opción para que $s' \in \mathscr{S}$ parece ser hacer que s y s' sean lo más 'cercanos' posible, es decir, hacer que $N(s-s')$ sea lo más pequeña posible. Notemos que, como los $s_2,\ldots,s_k$ son verdaderos, ambos s y s' son soluciones del sistema

$$x \equiv s_i \pmod{m_i},\ \ i = 2,\ldots,k$$

se verifica que $s' \equiv s \pmod{\mathrm{mcm}(A^*)}$, siendo como antes $A^* = \{2,\ldots,k\} = A \setminus \{1\}$. Realizando la división euclídea normalizada del **Teorema 2.4.2**, de s entre $\mathrm{mcm}(A^*)$, obtenemos

$$s = a\,\mathrm{mcm}(A^*) + r$$

con $N(r) < N(\mathrm{mcm}(A^*))/2$. Asimismo será $s' = a'\,\mathrm{mcm}(A^*) + r$, y por tanto $N(s-s') = N(a-a')N(\mathrm{mcm}(A^*))$. Luego esta norma es siempre múltiplo de $N(\mathrm{mcm}(A^*))$, y es lo más pequeña posible, cuando $N(a-a')$ es lo más pequeña posible. Veamos cómo hacerla así.

Observemos que si s es solución del sistema

$$(S_A):\ \ x \equiv s_i \pmod{m_i},\ \ i = 1,\ldots,k$$

entonces $s' = s + \lambda\,\mathrm{mcm}(A^*)$, $\lambda \in \mathbb{Z}[i]$, lo es del sistema

$$(S'_A):\ \begin{cases} x \equiv s_1 + \lambda\,\mathrm{mcm}(A^*) \pmod{m_1} \\ x \equiv s_i \pmod{m_i},\ \ i = 2,\ldots,k \end{cases}$$

ya que $s + \lambda\,\mathrm{mcm}(A^*) \pmod{m_i} = s \pmod{m_i} \equiv s_i \pmod{m_i}$ para $i = 2,\ldots,k$, y $s \equiv s_1 \pmod{m_1}$. De este modo, tomando $s'_1 = s_1 + \lambda\,\mathrm{mcm}(A^*)$ (**mod** m_1) aseguramos que $N(s-s') = N(\lambda)N(\mathrm{mcm}(A^*))$. En particular, si λ es una unidad, entonces $N(s-s') = N(\mathrm{mcm}(A^*))$ es lo menor posible.

En definitiva, la mejor opción para el mentiroso es elegir la falsa participación s'_1 de la forma $s'_1 = s_1 + \lambda\,\mathrm{mcm}(A^*)$ (**mod** m_1), siendo $\lambda \neq 0$ de norma lo más pequeña posible (idealmente λ debería ser una unidad). No se garantiza así la pertenencia de s' al espacio de secretos, cosa que parece imposible a priori pues desconoce s, pero se maximiza la probabilidad de que esto suceda. En todo caso, el éxito de esta estrategia depende del tamaño de $N(\mathrm{mcm}(A^*))$, que no depende de 1. Observemos no obstante, que $N(\mathrm{mcm}(A^*)) < m^-$ ya que 1 es esencial y A^* no esta autorizada.

4.1.5. Compatibilidad entre las dos condiciones

En las últimas secciones hemos encontrado dos condiciones para que el engaño del participante esencial 1 de la coalición $A = \{1, \ldots, k\}$ prospere. A saber

(M1) $s_1' \equiv s_1 \pmod{\text{mcd}(m_1, \text{mcm}(A^*))}$;
(M2) $s_1' = s_1 + \lambda \text{mcm}(A^*)$ (**mod** m_1), con $\lambda \in \mathbb{Z}[i]$ de norma lo menor posible y no nulo, siendo $A^* = \{2, \ldots, k\}$. Veamos que ambas condiciones son compatibles entre sí.

Según (M2), será $s_1' = s_1 + \lambda \text{mcm}(A^*) + \mu m_1$, con $\lambda, \mu \in \mathbb{Z}[i]$. Escribamos $d = \text{mcd}(m_1, \text{mcm}(A^*))$. Si $d = 1$, la condición (M1) es trivial. Si $d \neq 1$, entonces $d | m_1$ y $d | \text{mcm}(A^*)$, luego $d | (\lambda \text{mcm}(A^*) + \mu m_1)$ cualesquiera que sean λ y μ. Por tanto se verifica $s_1' \equiv s_1 \pmod{d}$, es decir (M1). En definitiva, al mentiroso le basta tomar s_1' verificando la condición (M2), con lo que la (M1) se verificará automáticamente.

4.1.6. Un ejemplo

Utilizando los datos del ejemplo de la **Sección 3.1.3** para fabricar un esquema de reparto sobre seis participantes de tipo $(6,4)$, consideramos la secuencia $\mathbf{m} : 100 + 89i, 100 - 89i, 98 + 93i, 98 - 93i, 101 + 90i, 101 - 90i$. Puede comprobarse que el intervalo $(6113415248054, 107002269048912168)$ no contiene la norma de ninguna coalición (con respeto a $\mathbf{m}$). El espacio de secretos será

$$\mathscr{S} = \{s \in Z[i] \ : \ 6113415248054 \leq N(s) \leq 26750567262228042\}.$$

Tomemos el secreto $s = 12345678 + 4567890i$, que tiene norma 173281384331784. Las participaciones son

$$\begin{array}{lll} s_1 = -69 + 15i, & s_2 = -11 - 54i, & s_3 = 31 + 35i, \\ s_4 = -13 - 26i, & s_5 = 21 + 64i, & s_6 = -62 - 33i. \end{array}$$

La coalición autorizada $A = \{1,2,3,4\}$ desea recuperar el secreto. Si todos los participantes son honestos, el sistema de ecuaciones en congruencias que debe resolver la coalición es

$$\left\{ \begin{array}{ll} x \equiv -69 + 15i & (\text{mod } 100 + 89i) \\ x \equiv -11 - 54i & (\text{mod } 100 - 89i) \\ x \equiv \ \ 31 + 35i & (\text{mod } 98 + 93i) \\ x \equiv -13 - 26i & (\text{mod } 98 - 93i) \end{array} \right.$$

cuya solución $x = 12345678 + 4567890i = s$, es igual al secreto repartido.

Supongamos que el participante 1 decide mentir para obtener sólo él el secreto y engañar al resto. Para ello calcula $\text{mcm}(A^*) = 1825300 - 1624517i$ y elige su participación falsa

$$\begin{array}{rcl} s_1' & = & s_1 + \text{mcm}(A^*) \ (\textbf{mod } m_1) \\ & = & (-69 + 15i) + (1825300 - 1624517i) \ (\textbf{mod } m_1) \\ & = & 50 - 15i. \end{array}$$

Con este dato, cuando la coalición decida recuperar el secreto resolverá el sistema viciado

$$\begin{cases} x \equiv 50-15i & (\mathrm{mod}\ 100+89i) \\ x \equiv -11-54i & (\mathrm{mod}\ 100-89i) \\ x \equiv 31+35i & (\mathrm{mod}\ 98+93i) \\ x \equiv -13-26i & (\mathrm{mod}\ 98-93i) \end{cases}$$

cuya solución $s' = -78444744 + 136409309i$, no es el secreto repartido. En este caso,

$$N(-78444744 + 136409309i) = 24761077443083017$$

luego $s' \in \mathscr{S}$: la estrategia del participante deshonesto ha tenido éxito y su mentira no ha sido detectada. Ahora, como sabe que

$$\begin{cases} s_2 \equiv s' & (\mathrm{mod}\ 100-89i) \\ s_3 \equiv s' & (\mathrm{mod}\ 98+93i) \\ s_4 \equiv s' & (\mathrm{mod}\ 98-93i) \end{cases}$$

el mentiroso puede fácilmente deducir los valores s_2, s_3, s_4 y recuperar s.

Si, por el contrario, 1 hubiera elegido su participación falsa 'al azar', sin tomar mayores precauciones, por ejemplo $s'_1 = 24 + 44i$, el sistema a resolver por la coalición sería

$$\begin{cases} x \equiv 24+44i & (\mathrm{mod}\ 100+89i) \\ x \equiv -11-54i & (\mathrm{mod}\ 100-89i) \\ x \equiv 31+35i & (\mathrm{mod}\ 98+93i) \\ x \equiv -13-26i & (\mathrm{mod}\ 98-93i) \end{cases}$$

que tiene solución $s' = -1252807 + 314941i$, de norma

$$N(-1252807 + 314941i) = 1668713212730 < 6113415248054$$

luego $s' \notin \mathscr{S}$. La mentira sería inmediatamente detectada (aunque no el mentiroso).

5

Anexo.
Implementaciones y trabajos futuros

Proponemos también, de cara a trabajos futuros, unas líneas por las que parece natural seguir investigando. En primer lugar el esquema de Asmuth-Bloom debería poder extenderse a los enteros de Gauss sin demasiada complicación, siguiendo técnicas similares a las que hemos desarrollado aquí.
Por otra parte, parece razonable preguntarse a qué otros dominios de números pueden extenderse estos (u otros) esquemas. Por ejemplo a cuerpos de números cuyos anillos de enteros sean euclídeos y cuya función de Euclides sea la expresión dada por la norma. Entre ellos podemos destacar los enteros de Einsestein, esto es: $\mathbb{Z}[x] = \{a+bx : a,b \in \mathbb{Z}, x = (1/2)+(i/2)\sqrt{3}\}$. Al realizar la extensión nos encontraríamos con los mismos problemas que en los enteros gaussianos, es decir, tendríamos que preguntarnos en qué condiciones la división da lugar a un resto único. No queriendo profundizar mucho en este tema diremos que, en principio, deberíamos ser capaces de encontrar una cierta región en la cual el resto fuese único. Teniendo esto en cuenta y fijándonos en que su grupo de unidades tiene 6 elementos, debería ser posible encontrar un análogo al recinto fundamental. Los siguientes casos a considerar deberían ser los tres cuerpos de números cuadráticos imaginarios $Q(\sqrt{-m})$ para $m = 2,7,11$, cuyo problema de la unicidad del resto pudiera ser más asequible al tener el grupo de unidades sólo dos elementos, -1 y 1. Estos tres cuerpos, junto a los de los racionales de Gauss y a los de Einsestein son los únicos cinco cuerpos cuadráticos imaginarios cuyo anillo de enteros es un dominio euclídeo y su función de Euclides está dada por la norma. Esos cinco son también, por tanto, los únicos cuerpos cuadráticos con esas dos propiedades cuyo grupo de unidades (de su anillo de enteros) es finito. En una segunda etapa, podrían considerarse los cuerpos de números cuadráticos reales, es decir los del tipo $Q(\sqrt{m})$ con $m > 1$, cuyo anillo de enteros tenga las dos propiedades anteriores. En este caso hay exactamente 16 valores de m para los cuales se cumplen dichas propiedades, y también se conocen otros 12 cuerpos ciclotómicos que satisfacen dichas propiedades. En estos veintiocho casos, el grupo de las unidades es infinito, por lo que el problema de la unicidad del resto tiene esta dificultad adicional.

Para terminar esta memoria incluimos un programa en Maple que muestra de manera práctica la viabilidad del esquema de Mignotte que presentamos en el Capítulo 3, y mediante el cuál hemos desarrollado los ejemplos de las secciones anteriores. A partir de una estructura de acceso arbitraria, el programa computa el esquema que la realiza, y lleva a cabo los procesos de reparto de un secreto y su posterior recuperación mediante las participaciones calculadas. A continuación incluimos el código fuente del programa. Para hacer más claro su funcionamiento, incluimos una ejecución del programa, para un conjunto de 5 participantes y la estructura de acceso que tiene por coaliciones autorizadas minimales a $\{1,3\},\{2,5\},\{3,4\},\{4,5\}$ y $\{1,2,5\}$.

Un esquema de reparto de secretos para cualquier estructura de acceso
según el método de Mignotte en Z[i]

Vamos a construir un esquema de Mignotte en Z[i] para realizar una estructura de acceso arbitraria, siguiendo
A continuación repartiremos un secreto y luego lo recuperaremos.

Comenzamos cargando el paquete GaussInt de Maple, que contiene órdenes de cálculo con enteros de Gauss.
```
> restart; with(GaussInt);
```

1. Introducción de datos sobre la estructura de acceso y el espacio de secretos

Introducimos los datos sobre la estructura de acceso:
número de participantes
```
> n := 5;
                                    5
```
coaliciones autorizadas minimales
```
> AutorizadasMinimales := {{1, 3}, {2, 5}, {3, 4}, {4, 5}, {1, 2, 3}, {1, 2, 5}, {3, 4, 5}, {1, 2, 4, 5}};
{{1, 3}, {2, 5}, {3, 4}, {4, 5}, {1, 2, 3}, {1, 2, 5}, {3, 4, 5}, {1, 2, 4, 5}}
```
tamaño mínimo exigido al conjunto de secretos
```
> tamaño := 1000000;
                                 1000000
```

2. Cálculo de las estructuras no autorizadas

La realización del esquema de Mignotte que hemos detallado en la memoria, se basa en las estructuras no auto
Para calcularlas utilizaremos el siguente programa auxiliar que determina si una coalición de participantes e
```
> autorizado := proc (C::set)::integer; local aut, it, i; aut := 0; for i to nops(AutorizadasMinimales) while
```
por ejemplo
```
> autorizado({1, 3, 5}); autorizado({1, 4});
                                    1
                                    0
```
Utilizando ese programa, calculamos las estructuras no autorizadas
```
> NoAutorizadas := {{}}; for j to n do temp := {}; for i to nops(NoAutorizadas) do if autorizado(‘union‘(NoAu
{{}, {1}, {2}, {3}, {4}, {5}, {1, 2}, {1, 4}, {1, 5}, {2, 3}, {2, 4}, {3, 5},

  {1, 2, 4}}
```
y nos quedamos on las maximales
```
> contenidas := [1]; for i from 2 to nops(NoAutorizadas) do contenido := 0; for j from i+1 to nops(NoAutoriza
                    {{1, 5}, {2, 3}, {3, 5}, {1, 2, 4}}
```

3. Cálculo de la secuencia de módulos

Una vez conocidas las coaliciones no autorizadas maximales podemos calcular la secuencia de módulos del esque
Siguiendo el procedimiento descrito en la memoria, partimos de un conjunto de enteros gaussianos mu (tantos c
Comenzamos fijando los coeficientes mu
```
> nautm := nops(NoAutorizadasMaximales); lPrimos := GIsieve(ceil(root[nautm](4*tamaño)))[2]; for i from ceil(
           [9 + 44 I, 10 + 43 I, 12 + 43 I, 23 + 38 I, 29 + 34 I]
```
y, a partir de ellos, la secuencia de modulos m
```
> M := Array(1 .. n, 1 .. nautm, fill = 1); for i to n do for j to nautm do if member(i, NoAutorizadasMaximal
[-1729 + 946 I, -1784 + 915 I, -1465 + 1354 I, -57185 - 67562 I, -1404 + 1369 I

  ]
```
y también el espacio de secretos: los secretos posibles son los que tienen norma comprendida entre
```
                      #msup(mi("m"),mo("&uminus0;"))
```
  y
```
                       1
                       - LinearAlgebra:-Transpose(m)
                       4
> mmenos := GInorm(mul(j, j = mus[2 .. nautm])); mmas := GInorm(mul(j, j = mus[1 .. nautm]));
                                 7663836361
                               15457957940137
```
cuyo cardinal es
```
> evalf(Pi*((1/4)*mmas-mmenos));
```

```
                                   13
                          1.211657513 10

4.  Reparto de un secreto

Dado un secreto del espacio de secretos
> Secreto := 12345+678910*I;
                          12345 + 678910 I
comprobamos si está en el espacio de secretos
> if GInorm(Secreto) < mmenos then print(‘Norma demasiado pequeña‘) elif GInorm(Secreto) > (1/4)*mmas then pr
                          Secreto correcto
Calculemos  las participaciones. Maple no incorpora una función modulo sobre los enteros de Gauss (recordemos
Por lo tanto, primero programamos el módulo que allí definimos
> ModPrincipal := proc (v, z) description "calcula v modulo z"; z*(v/z-round(Re(v/z))-I*round(Im(v/z))) end p
Vamos ya con las participaciones
> Participaciones := [seq([ModPrincipal(Secreto, Modulos[i]), Modulos[i]], i = 1 .. n)];
   [[455 + 205 I, -1729 + 946 I], [1 + 239 I, -1784 + 915 I],

     [-481 + 796 I, -1465 + 1354 I], [7045 - 12387 I, -57185 - 67562 I],

     [105 + 649 I, -1404 + 1369 I]]
Cada participación y módulo se hace llegar al participante correspondiente de manera secreta.

5.  Recuperación del secreto

Una coalición de participantes desea recuperar el secreto. Por ejemplo
> Coalicion := {1, 2, 3};
                              {1, 2, 3}
Veamos primero si está autorizada
> autorizado(Coalicion);
                                   1
La información que posee la coalición es la participación y el módulo de cada uno de sus miembros
> DatosCoalicion := {seq(Participaciones[Coalicion[i]], i = 1 .. nops(Coalicion))};
        {[-481 + 796 I, -1465 + 1354 I], [1 + 239 I, -1784 + 915 I],

          [455 + 205 I, -1729 + 946 I]}
Sobre estos datos aplicaremos el teorema Chino de los restos. Lamentablemente, Maple sólo incorpora la versio
> DatosCoprimos := {}; for i to nops(Coalicion) do factores := GIfacset(DatosCoalicion[i][2]); factores := {s
     {[10 I, 9 + 44 I], [-16 + 12 I, 12 + 43 I], [-2 - 6 I, 10 + 43 I],

       [11 - 21 I, 23 + 38 I]}
y ahora pordemos aplicar el teorema Chino a estos resultados
> SecretoRecuperado := GIchrem([seq(DatosCoprimos[i][1], i = 1 .. nops(DatosCoprimos))], [seq(DatosCoprimos[i
                          12345 + 678910 I
 Recordemos que el autentico secreto era
> Secreto;
                          12345 + 678910 I
>
```

Referencias

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

[2] S. Clemens, P. O'Daffer, T. Cooney, Geometría con aplicaciones y solución de problemas. Addison-Wesley, 1989.

[3] 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.

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

[5] 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.

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

[7] J. Fraleigh, A First Course In Abstract Algebra, Addison-Wesley, 1976.

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

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

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

[11] C. F. Gauss, Theoria residuorum biquadraticorum. Commentatio secunda, Commentarii Societatis Regiae Scientiarum Gottingensis 7 (1832) 1–34.

[12] H. Ghodosi, J. Pierprzyk, Cheating Prevention in Secret Sharing. En E. P. Dawson, A. Clark, C. Boyd (editores), Information Security and Privacy-ACISP 2000. Lecture Notes in Computer Science-1841. Springer, 2000, 328-341

[13] G. H. Hardy, On the Expression of a Number as the Sum of Two Squares, The Quarterly Journal of Mathematics 46 (1915), 263-283.

[14] L. Harn, C. Lin, Detection and identification of cheaters in (t,n) secret sharing scheme, Designs, Codes and Cryptography 52 (2009), 15-24.

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

[16] S. Iftene, Secret sharing schemes with applications in security protocols, Scientific Annals of Cuza University 16 (2006), 63–96.

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

[18] M. A. Jodeit, Uniqueness in the division algorithm, The American Mathematical Monthly 74 (1967), 835–836.

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

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

[21] D. Munuera-Merayo, Reparto de secretos con el Teorema Chino de los restos. Trabajo fin de grado. Universidad de Valladolid, 2020. Disponible en https://uvadoc.uva.es/bitstream/handle/10324/43950/TFG-G4589.pdf?sequence=1&isAllowed=y

[22] D. Munuera-Merayo, On Mignotte Secret Sharing Schemes Over Gaussian Integers, arXiv: 2104.06361. Disponible en https://arxiv.org/abs/2104.06361

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

[24] W. Ogata, K. Kurosawa, D. Stinson, Optimum secret sharing scheme against cheating, SIAM Journal on Discrete Mathematics 20 (2006), 79-95.

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

[26] I. Ozbek, F. Temiz, I. Siap, A generalization of the Mignotte's scheme over Euclidean domains and applications to secret image sharing, Journal of Algebra, Combinatorics, Discrete Structures and Applications 6 (2019), 147–161.

[27] D. Pasailă, V. Alexa, S. Iftene, Cheating detection and cheater identification in CRT-based secret sharing schemes. En Cryptology ePrint archive, International Association for Cryptologic Research. Disponible en https://eprint.iacr.org/2009/426.pdf

[28] Francisco José Plaza Martín, Manual de Criptografía. Fundamentos matemáticos de la Criptografía para un estudiante de Grado. Ediciones Universidad Salamanca. 2021.

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

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

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

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

[33] D. Zagier, A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, The American Mathematical Monthly 97 (1990), 144.