Universidad de Oviedo

Facultad de Ciencias

Teoría algebraica de números

Darío Sánchez Carpintero

Tutora: Consuelo Martínez López

9 de julio de 2023

Índice general

Introducción

La Teoría de Números, también conocida como Aritmética, tuvo como objetivo fundamental en su inicio el estudio de los números enteros. Esto hizo que resultara atractiva incluso para muchos aficionados sin estudios matemáticos especializados. Hoy en día es una rama de las matemáticas que aborda numerosos problemas, que tiene notables aplicaciones, especialmente en criptografía, utiliza variadas herramientas matemáticas -fundamentalmente algebraicas y analíticas – y tiene fuertes conexiones con otras ramas de las matemáticas, como la Combinatoria ó la Geometría Algebraica.

Siguiendo las ideas de Pierre Samuel en su libro "Teoría Algebraica de Números" se ha tratado de mostrar en este trabajo la evolución de la teoría y el importante papel desempeñado por los métodos algebraicos, dado que el punto de vista algebraico parece el más apropiado para contextualizar la mayoría de los problemas considerados. Por ejemplo, para encontrar soluciones a la ecuación de Fermat: $x^n + y^n = z^n$ lo mas adecuado es trabajar en el cuerpo ciclotómico con las n-raices de la unidad. Para otro tipo de ecuaciones, como la de Pell, los cuerpos de la forma $\mathbb{Q}(\sqrt{d})$ parecen los mas adecuados. Tanto cuerpos cuadráticos como raíces de la unidad parecen involucrados en el estudio de la ley de reciprocidad cuadrática.

El estudio de problemas importantes de la teoría de números obligó a salirse del marco tradicional de los enteros y su cuerpo de fracciones, los racionales, y considerar extensiones finitas de $\mathbb{Q}$ y los correspondientes anillos de enteros algebraicos. Las herramientas algebraicas han mostrado su potencia y utilidad en muchos problemas, pero quedan otros muchos por resolver

y, por supuesto, no puede esperarse que se resuelvan todos ellos sólo usando métodos algebraicos.

En este trabajo se comienza planteando, en el Capítulo 1 problemas tradicionales, la mayoría ligados a los números primos y a la búsqueda de soluciones (enteras) de ecuaciones diofánticas. Al pasar a trabajar en el anillo de enteros algebraicos de un cuerpo de números se plantea un nuevo problema: algunos de los anillos que aparecen no son dominios de factorización única y por tanto ya no se cumple el teorema fundamental de la aritmética.
Se llega así, de manera natural, a los anillos de Dedekind en los que se sustituye la factorización única de elementos como producto de irreducibles por una factorización de ideales como producto de ideales primos.

En el Capítulo 2 se explican los fundamentos algebraicos de la Teoría de Números, lo que ha permitido usar los conocimientos y competencias obtenidos en las asignaturas de Algebra I y II y ampliar el conocimiento de estructuras algebraicas.

Finalmente, en el Capítulo 3, se incluyen aplicaciones de la Teoría de Números en Criptografía, poniendo el énfasis en los resultados teóricos en los que se sustentan los métodos desarrollados para construir algunos sistemas de cifrados.

Capítulo 1

Problemas clásicos de Teoría de Números

La teoría de números depende en gran medida de las propiedades que poseen los números primos sobre $\mathbb{Z}$ por lo que no es de extrañar que su estudio resulte fundamental para la resolución de un abundante número de problemas, así como el interés en identificarlos de manera consistente. Es natural entonces comenzar observando algunas de estas propiedades.

1.1. Algunos resultados sobre primos

Comenzamos el apartado estudiando la infinitud de los primos. Esta es demostrada con el llamado Teorema de Euclides, con múltiples demostraciones. La más simples hace uso del Teorema Fundamental de la Aritmética, por reducción al absurdo:

Supongamos que existen n números primos distintos, $a_1, a_2, \ldots, a_n$. Consideramos ahora $N = a_1 \cdot a_2 \cdots a_n + 1$. Claramente, ninguno de los a_i divide a N, por lo que los únicos divisores de N serían 1 y N. En consecuencia,

N es un número primo distinto de los n dados, lo que lleva a contradicción. **CQD**

También se puede demostrar comprobando la divergencia de la serie dada por los inversos de los números primos. Dicha demostración se puede hacer obteniendo como cota

$$\sum_{p \leq N} 1/p \leq loglogN - 2$$

Se puede hacer uso también del siguiente resultado:

Postulado de Bertrand: $\forall n \geq 1,\ \exists\ p$ primo tal que $n < p \leq 2n$

Esto nos da a la vez, como resultado inmediato el teorema de Euclides, y una cota inferior para el número de primos en un intervalo cualquiera:
En el intervalo

$$(1, 2^N] = (1, 2] \cup (2, 4] \cup \cdots \cup (2^{N-1}, 2^N]$$

hay por lo menos N primos, cada uno en uno de los intervalos $(2^{n-1}, 2^n]$, $n \in \{1, 2, \ldots, N\}$.

Veamos ahora una demostración inductiva del Teorema Fundamental de la Aritmética:

Teorema Fundamental de la Aritmética: Todo número natural tiene una factorización como producto de primos, única salvo el orden de los factores.

Demostración: Para $n = 2$ el resultado es cierto de forma trivial. Supongamos que se verifica para todos los naturales n menores que algún $a > 1$. Definimos

$$D = \{d \mid d > 1, d|a\}$$

el conjunto de divisores de a distintos de 1. D es no vacío por estar a en él, así que tiene un elemento mínimo, p, que es primo. Si no fuera primo, habría un elemento estrictamente menor que p que divide a p y por tanto a a. Entonces

$$a = pb,\ p \text{ primo},\ b < a$$

Por hipótesis de inducción, como $b < a$, tenemos las descomposiciones

$$b = p_1 \cdots p_s, a = p \cdot p_1 \cdots p_s$$

y a no tiene otra descomposición en la que aparezca p.
Sea otra descomposición prima de a en la que no aparece p:

$$a = q_1 \cdots q_r$$

Tenemos que $q_1 \neq p$. Por definición de p, $p < q_1$, pues $q_1 \in D$. Dado $c = q_2 \cdots q_r$, se define

$$a_0 = a - pc = p(b - c) = (q_1 - p)c$$

Tenemos que $1 \leq a_0 < a$, y los divisores $(b - c), (q_1 - p)$ y c son menores que a. Por hipótesis de inducción, ellos y a_0 tienen una única factorización por primos, y p aparece en la de a_0, por lo que aparece en la de c o en la de $(q_1 - p)$.
No puede aparecer en la de $(q_1 - p)$, pues eso requeriría que $p|q_1$, y es imposible por ser primos distintos. Pero hemos supuesto que tampoco está en la descomposición de c. Suponer que hay dos descomposiciones de a distintas nos lleva a contradicción. **CQD**

1.1.1. Búsqueda de primos

Un objetivo de la teoría algebraica de números es conseguir condiciones necesarias y suficientes de primalidad, siendo de especial interés aquellas de las que se deducen algoritmos que generan primos con eficiencia y las que determinan la primalidad de un número. Un tal algoritmo es la criba de Eratóstenes, que, en particular, permite obtener todos los primos menores que cualquier valor dado, aunque pierde eficiencia como test de primalidad al considerar valores grandes.

Como apoyo para la búsqueda de primos se tiene el siguiente resultado:

Pequeño Teorema de Fermat: Para todo primo p y cualquier entero a,

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

Demostración: Sin perder generalidad, suponemos que a es positivo. Entonces, es posible usar el método de inducción. Para $a = 1$, es evidente. Asumimos que es cierto para $a = n$, entonces:

$$(n+1)^p = \sum_{i=0}^{p} \binom{p}{i} n^i = n^p + pn^{p-1} + \cdots + pn + 1$$

Para $0 < i < p$, $\binom{p}{i} = \dfrac{p!}{i!(p-i)!}$ tiene numerador divisible por p y denominador no divisible por p. Por el Teorema Fundamental de la Aritmética, $\binom{p}{i}$ es divisible por p para dichos i. Por tanto

$$(n+1)^p \equiv n^p + 1 \equiv n + 1 \pmod{p}$$

1.1.2. Primos de Mersenne

Definición: Se denota como **primo de Mersenne** a aquel de la forma $2^p - 1$ para algún primo p.
El concepto de primo de Mersenne se deriva de que, cuando se considera un número compuesto en lugar de uno primo, la expresión anterior siempre resulta ser compuesto. Se puede considerar la siguiente descomposición dado $n = ab$:

$$2^n - 1 = (2^a - 1)(2^{n-a} + 2^{n-2a} + \cdots + 2^a + 1)$$

Esto mismo incita la pregunta de si siempre que el exponente es primo, se obtiene un primo de Mersenne. Por desgracia, la respuesta es no: $2^{11} - 1$ es compuesto, y aún no se sabe si existen infinitos números de Mersenne.

Existe relación entre los primos de Mersenne y los llamados números perfectos, aquellos que son iguales a la suma de todos sus divisores propios (incluyendo 1):

Proposición: Dado $q = 2^p - 1$ un primo de Mersenne, $2^{p-1}q$ es un número perfecto.

Demostración: Los factores propios que dividen a $2^{p-1}q$ se pueden separar según sean o no divisibles por q:
La suma de los factores no divisibles es

$$1 + 2 + 2^2 + \cdots + 2^{p-1} = 2^p - 1 = q$$

La de los divisibles es

$$q(1 + 2 + \cdots + 2^{p-2}) = q(2^{p-1} - 1)$$

Por tanto, la suma de todos es

$$q + q(2^{p-1} - 1) = q(2^{p-1}) \qquad \textbf{C.Q.D}$$

Proposición: Todos los números perfectos pares son de la forma $(2^{p-1})(2^p - 1)$.

Demostración:

Para este resultado se hace uso de la función suma de factores σ, que verifica $\sigma(ab) = \sigma(a)\sigma(b)$ para cualesquiera a y b coprimos.
Considerando el número perfecto $2^n x$ tal que 2 no divide a x, se tiene que

$$2(2^n x) = 2^{n+1}x = \sigma(2^n x) = \sigma(2^n)\sigma(x) = (2^{n+1} - 1)\sigma(x)$$

Por ser x el único factor impar de la expresión, se tiene que $2^{n+1} - 1$ (también impar) divide a x. Consideramos entonces $y = \dfrac{x}{2^{n+1} - 1}$ y dividiento en la expresión anterior por $2^{n+1} - 1$, se obtiene la identidad

$$2^{n+1}y = \sigma(x) = x + y + \cdots = (2^{n+1} - 1)y + y + \cdots = 2^{n+1}y + \ldots$$

Para que esto se cumpla, no puede haber otros divisores. Entonces $y = 1$ y x es primo de la forma $2^{n+1} - 1$, por ser divisor propio de x. **CQD**

Este par de resultados forman el **Teorema de Euclides-Euler**.

Teorema: Denotando M_n al n-ésimo número de Mersenne, $2^n - 1$, se tiene que dado p primo y q divisor no trivial de M_p, $q \equiv 1 \pmod{p}$.

Este resultado es de gran ayuda para factorizar M_p. Veamos la demostración apoyándonos en la teoría de grupos:

Consideramos G el grupo de residuos distintos de cero módulo q. Como $2^p - 1 \equiv 0 \pmod{q}$, $2^p \equiv 1 \pmod{q}$ y se tiene que 2 genera un subgrupo cíclico de G de orden divisor de p. Como p es primo y 2 no es la identidad de G, el orden es p. Sabiendo que el orden del subgrupo debe dividir al de G (Teorema de Lagrange), p divide a $(q - 1)$.

Aunque no se haya podido demostrar que la secuencia de los M_n genere infinitos primos, sí se sabe que genera nuevos factores primos muy rápidamente. Se define un factor primitivo de M_n como un primo p que divide a M_n, pero no divide a ningún número de Mersenne menor. La generación de factores primos viene dada por los factores primitivos:

Teorema de Zsigmondy: Sea $M_n = 2^n - 1$. Entonces
para todo $n \neq 6,\ n > 1$, M_n tiene un factor primitivo

1.1.3. Números de Fermat

Se denota al **n-ésimo número de Fermat** como $F_n = 2^{2^n} + 1$. Esta expresión da como resultado un número primo cuando n toma valores entre 0 y 4. Euler probó que F_5 es divisible por 641 y se sospecha que solo hay un número finito de primos de Fermat.
Por otro lado, la factorización de los números de Fermat es bastante sencilla, como nos muestra el siguiente resultado:

Proposición: Dado p un primo tal que $p|F_n$, se tiene que $p = 2^{n+1}k + 1$ para algún $k \in \mathbf{N}$

Demostración: Sabemos que $2^{2^n} \equiv -1 \pmod{p}$ y p es impar. Por tanto,

$$2^{2^{n+1}} \equiv 1 \pmod{p}$$

Tomando $d = mcd(2^{n+1}, p-1)$ y obteniendo a y b según la Identidad de Bezout tales que $d = (2^{n+1})a + (p-1)b$, deducimos que

$$2^d = 2^{(2^{n+1})a+(p-1)b} = (2^{2^{n+1}})^a (2^{p-1})^b \equiv 1 \pmod{p}$$

aplicando el Pequeño Teorema de Fermat a $2^{p-1} \equiv 1 \pmod{p}$. Como $d|2^{n+1}, d = 2^c$ para algún c entre 0 y $n+1$, ergo

$$2^d = 2^{2^c} \equiv 1 \pmod{p}$$

Pero sabemos que $2^{2^n} \equiv -1 \pmod{p}$, y no es congruente con 1. Deducimos que $c = n+1$ y $d = 2^{n+1}$. Como d también divide a $p-1$, se concluye que $p = 2^{n+1}k + 1$ para algún k. **CQD**

1.1.4. Tests de primalidad.

Comprobar la primalidad de un número es tarea sencilla para valores pequeños: basta con estudiar la divisibilidad por primos pequeños. La complejidad de este método aumenta rápidamente con el tamaño, pues es análogo a un método de factorización, problema que aún no se ha resuelto en tiempo polinomial mediante herramientas clásicas.

Una alternativa es utilizar resultados de Teoría de Números que proporcionen condiciones necesarias o suficientes para determinar la primalidad. Un ejemplo es el Pequeño Teorema de Fermat, que nos da una condición necesaria.
El siguiente resultado, en cambio, provee una condición necesaria y suficiente:

Teorema de Wilson: Un entero $n > 1$ es primo si y solo si:

$$(n-1)! \equiv -1 \pmod{n}$$

Demostración

$\Rightarrow$ La demostración es trivial para $n = 2$. Sea $n = p$ con $p > 2$ primo. Si consideramos los enteros a tales que $1 < a < p - 1$, todos tienen inverso multiplicativo módulo p. Como su unicidad es obvia, si cada inverso es distinto del propio elemento, entonces se cancelarían todos los términos de $(p-1)!$ (excepto el propio $n - 1 \equiv -1$) módulo p.
Supongamos que no se cumple, es decir, $a^2 \equiv 1 \pmod{p}$. Entonces $p|(a+1)(a-1)$, y por primalidad se sigue que $a \equiv \pm 1 \pmod{p}$, esto es, a es 1 ó $p - 1$. **CQD**

$\Leftarrow$ Supongamos que $n = ab$, con $1 < a, b \leq n-1$. Consideramos 2 casos: $a = b$ y $a \neq b$

(Caso $a = b$) Si $a = b = 2$, se tiene que $3! = 6$ no es congruente con -1 módulo 4. Consideramos entonces $a > 2$. Claramente $a, 2a \leq n - 1$, y tanto a como $2a$ son factores de $(n-1)!$. Se sigue que $(n-1)! = 2a^2k = ab2k$ para algún k y

$$(n-1)! \equiv 0 \pmod{n}$$

(Caso $a \neq b$) Claramente a y b son factores distintos que se encuentran en $(n-1)!$. Se deduce que $(n-1)! = kab$ para algún k, y la congruencia módulo n es 0.

En ninguno de los casos la congruencia vale -1 **CQD**

Aunque este método proporcione un método infalible para determinar la primalidad, en la práctica es imposible computar $n!$ en tiempo polinomial, lo que obliga a considerar otros métodos.
Por ejemplo, para comprobar la primalidad de un posible primo p, se puede utilizar la congruencia dada por el Pequeño Teorema de Fermat,

$$a^{p-1} \equiv 1 \pmod{p} \text{ siempre que } p \text{ sea primo}$$

para cualquier natural a. Parece funcionar entonces como test escoger al azar a con $1 < a < p$ y comprobar si la congruencia se verifica. Sin embargo, existen números compuestos tales que para toda base coprima con ellos se verifica la congruencia del Pequeño Teorema de Fermat. Estos son conocidos como números de Carmichael.
El hecho de que haya infinitos de ellos vuelve al test descrito anteriormente

poco válido como test de primalidad.

1.2. Ecuaciones diofánticas

1.2.1. La ecuación de Pitágoras

Las ecuaciones diofánticas son ecuaciones, generalmente polinomios de coeficientes enteros, para las que se busca obtener soluciones enteras. Un ejemplo es la ecuación dada por la longitud de los lados de un triángulo rectángulo, la ecuación de Pitágoras:

$$x^2 + y^2 = z^2$$

El objetivo es encontrar todas las soluciones enteras. Para ello, nos dedicaremos a buscar soluciones primitivas, es decir, soluciones tales que x, y, z no tengan factores primos comunes. Esto se deriva de que, dada una solución con factores comunes, siempre se puede deducir una solución primitiva dividiendo en la ecuación por el cuadrado de dichos factores. Entonces, partimos de una serie de suposiciones: sabemos que solo una de las incógnitas puede ser par (si dos de ellas son pares, entonces la tercera también, y se tiene que 2 es divisor común de las tres incógnitas), y esta no puede ser z. Esto es porque $x^2 + y^2 \equiv 0 \pmod 4$ no tiene solución para x e y impar. Suponemos que x es par.

Consideramos entonces $x = 2x'$ y de la expresión $x^2 = z^2 - y^2 =$
$= (z + y)(z - y)$ obtenemos

$$x'^2 = \frac{z+y}{2}\frac{z-y}{2}$$

Como consideramos z e y impares, ambos factores $(z \pm y)/2$ son enteros. Podemos deducir que son coprimos (si no lo son, la suma y la diferencia tienen un factor común, que también lo es de y y z) y por el Teorema Fundamental de la Aritmética concluimos que son cuadrados:

$$z + y = 2m^2, z - y = 2n^2, m > n, z \geq 0, y \geq 0$$

Así, obtenemos las soluciones primitivas de la ecuación de Pitágoras,

$$x = 2mn, z = m^2 + n^2, y = m^2 - n^2$$

con $m > n$, uno de ellos par y el otro impar.

1.2.2. Algunas formas cuadráticas

Es bien sabido que un anillo euclídeo es dominio de factorización única, es decir, se cumple el TFA. Esto es debido a cómo se puede realizar un proceso análogo al algoritmo euclídeo de la división con resto a partir de la norma del anillo.

Definición: Un anillo E se denomina **dominio euclídeo** si es dominio de integridad y existe una aplicación $N : E \setminus \{0\} \to \mathbb{N}$, llamada **norma**, que cumple:

1. $N(ab) = N(a)N(b)\ \forall a, b \in E$
2. $\forall a, b \in E,$ si $b \neq 0, \exists\ q, r \in E$ tales que $a = bq + r, r = 0$, o bien $N(r) < N(b)$

Vamos a considerar sobre el anillo $R = \mathbb{Z}[i]$ la norma dada por $N(x + iy) = x^2 + y^2$ como apoyo para buscar soluciones para la ecuación

$$n = x^2 + y^2$$

para algún n fijo. En particular, sabemos encontrar las soluciones para n primo.

Lema: Si p es 2 o congruente con 1 módulo 4, la congruencia

$$T^2 + 1 \equiv 0 \pmod{p}$$

tiene solución en los enteros

Demostración: Para p=2 es evidente. Sea $p = 4n + 1$ para algún $n > 0$. Por el teorema de Wilson

$$(p-1)! = (p-1)(p-2)\cdots 1 \equiv -1 \pmod{p}$$

Considerando

$$4n = p - 1 \equiv -1 \pmod{p}$$
$$4n - 1 = p - 2 \equiv -2 \pmod{p}$$
$$\vdots$$
$$2n + 1 = p - 2n \equiv -2n \pmod{p}$$

En consecuencia,
$(p-1)! = (4n)! = 1 \cdot 2 \cdots (2n-1)(2n)(2n+1)\cdots(4n) \equiv$
$1 \cdot 2 \cdots (2n-1)(2n)(-2n)\cdots(-1) \equiv ((2n)!)^2(-1)^{2n} \equiv -1 \pmod{p}$

Tomando $T = (2n)!$ obtenemos el resultado

Teorema: Un primo p puede escribirse como suma de dos cuadrados si y solo si $p = 2$ o $p \equiv 1 \pmod 4$

Demostración: De nuevo, el caso 2 es trivial. Como los cuadrados módulo 4 son 0 o 1, p congruente con 3 no puede ser suma de 2 cuadrados. Supongamos $p \equiv 1 \pmod 4$. Por el lema anterior, en el anillo $\mathbb{Z}[i]$ se puede escribir

$$kp = T^2 + 1 = (T + i)(T - i)$$

para algún par de enteros c y T.
Veamos que p no es reducible en R. Si suponemos lo contrario, p es primo en R por darse en este el TFA. Entonces p dividiría a $T \pm i$, pues divide a su producto, pero esto es imposible porque p no divide al coeficiente de i. Tenemos que $p = ab$ es producto de dos no unidades de R. Tomando la norma de p y ab,

$$p^2 = N(ab) = N(a)N(b)$$

Como ni a ni b son unidades, se tiene que $N(a) \neq 1, N(b) \neq 1$. De nuevo, por el TFA, $N(a) = N(b) = p$. Entonces, por definición de la norma dada sobre $\mathbb{Z}[i]$, existen x e y enteros tales que $a = x + iy$, $x^2 + y^2 = p$

En cuanto a las soluciones para n cualquiera, se tiene que n es suma de dos cuadrados si y solo si cada uno de sus factores primos congruentes con 3 módulo 4 aparece en la factorización de n con exponente par.

Otro resultado clásico es el Teorema de los Cuatro Cuadrados de Lagrange. Este enuncia que todo entero positivo se puede expresar como suma de cuatro cuadrados enteros.
La demostración se obtiene como consecuencia inmediata de las propiedades: el producto de dos sumas de cuatro cuadrados es una suma de cuatro cuadrados y todo primo se puede expresar como tal suma.

Proposición: El producto de dos sumas de cuatro cuadrados es una suma de cuatro cuadrados

Demostración: Basta desarrollar a ambos lados de la expresión de la identidad de los cuatro cuadrados de Euler
$(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2) =$
$= (aw+bx+cy+dz)^2 + (ax-bw-cz+dy)^2 + (ay+bz-cw-dz)^2 +$
$+ (az-by+cx-dw)^2$

Para el otro resultado necesitaremos hacer uso del siguiente lema:

Lema: Dado p un primo impar, existen dos enteros a y b tales que $a^2 + b^2 + 1 \equiv 0 \pmod{p}$

Demostración: Definimos los conjuntos
$$A = \left\{ a^2 |\ 0 \leq a \leq \frac{p-1}{2} \right\}$$
$$B = \left\{ -b^2 - 1 |\ 0 \leq b \leq \frac{p-1}{2} \right\}$$

Los elementos de A vistos como congruencia módulo p son distintos dos a dos. Basta observar que las únicas raíces posibles del polinomio $x^2 - a$ son a y $-a = p - a$. Como solo una de ellas puede ser menor que $\frac{p-1}{2}$, concluimos que los cuadrados son distintos.

Análogamente, los elementos de B módulo p también son distintos entre sí. Como en A y en B hay $\frac{p+1}{2}$ elementos módulo p, por solo existir p enteros módulo p entonces existen $a^2 \in A,\ -b^2-1 \in B$ tales que
$a^2+b^2+1 \equiv 0 \pmod{p}$ **CQD**

Proposición: Todo primo es suma de cuatro cuadrados.

Demostración: Para $p=2$, se tiene $p = 1^2+1^2+0^2+0^2$
Sea p un primo impar. Por el lema anterior, existen enteros m', a', b' tales que $m'p = a'^2+b'^2+1^2+0^2$. En particular, existen enteros m, a, b, c, d tales que $mp = a^2+b^2+c^2+d^2$

Si $m=1$, es el resultado deseado. Supongamos $m>1$, buscaremos $n<m$ tal que np sea suma de cuatro cuadrados, de forma que se acaba llegando al caso $n=1$.

Si m es par, entonces un número par de los a, b, c, d es par. Agrupamos los cuadrados en grupos de 2 de forma que los elementos de un grupo tengan la misma paridad, sin perder generalidad $(a^2+b^2)+(c^2+d^2)$. Tanto a^2+b^2 como c^2+d^2 son pares. Consideramos la siguiente identidad: si $2n = x^2+y^2$, entonces x e y tienen la misma paridad y $n = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2$ es suma de dos cuadrados.
Aplicando esta identidad a (a^2+b^2) y a (c^2+d^2) (ambas expresiones pares), entonces tanto $\dfrac{a^2+b^2}{2}$ como $\dfrac{c^2+d^2}{2}$ son sumas de dos cuadrados. Como conclusión inmediata, $\left(\frac{m}{2}\right)p$ es suma de cuatro cuadrados.

Si m es impar, consideramos $w \equiv a \pmod{m}$, $x \equiv b \pmod{m}$, $y \equiv c \pmod{m}$, $z \equiv d \pmod{m}$ tales que $-\frac{m}{2} < w, x, y, z < \frac{m}{2}$.
Se tiene que $w^2+x^2+y^2+z^2 < m^2$ y $w^2+x^2+y^2+z^2 \equiv 0 \pmod{m}$ por verificarlo también a, b, c, d. Se concluye que $w^2+x^2+y^2+z^2 = km$ para algún $0<k<m$. En la identidad de Euler
$(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2) =$
$= (aw+bx+cy+dz)^2 + (ax-bw-cz+dy)^2 + (ay+bz-cw-dz)^2 +$
$+ (az-by+cx-dw)^2$

la parte de la izquierda es kpm^2. Como módulo m $ax \equiv bw$ y $cz \equiv dy$, $ax - bw - cz + dy$ (y su cuadrado) es divisible por m^2. Se puede razonar de forma análoga para $ay + bz - cw - dz$ y $az - by + cx - dw$.
$aw + bx + cy + dz \equiv w^2 + x^2 + y^2 + z^2 \equiv 0 \pmod{m}$, por lo que su cuadrado es divisible por m^2.
Todo sumando de la expresión de la derecha, y en particular la expresión entera, es divisible por m^2. Concluimos que kp es suma de cuatro cuadrados: $\left(\frac{aw + bx + cy + dz}{m}\right)^2$, etc. **CQD**

Cuando se elige un entero $d > 1$ libre de cuadrados, se tiene que $\mathbb{Z}[\sqrt{d}]$ es un anillo con infinitas unidades y en el que se puede definir una norma N dada por $N(x + y\sqrt{d}) = x^2 - dy^2$. Esto nos da una pista para la solución de otra ecuación:

Teorema: Dado $d > 1$ entero libre de cuadrados, la ecuación

$$x^2 - dy^2 = 1$$

tiene infinitas soluciones con x e y enteros. En particular, cada solución se corresponde con una unidad en $R = \mathbb{Z}[\sqrt{d}]$, con norma 1, y toda unidad con norma 1 es de la forma $\pm u^n, n \in \mathbb{N}$ siendo u una unidad fija y de norma 1.

Este resultado se obtiene fácilmente como corolario del Teorema de las Unidades, que veremos en el capítulo siguiente.

En cambio, al considerar anillos $\mathbb{Z}[\sqrt{-d}]$ para resolver la ecuación $p = x^2 + dy^2$ hay problemas, en el sentido de que dicho anillo no siempre es euclídeo.

Podemos también encontrar soluciones para las ecuaciones Diofánticas del tipo

$$ax^2 + bxy + cy^2 = n$$

buscando valores enteros de x e y con a,b,c,n enteros fijos. Para ello, defimos el discriminante de la forma cuadrática $ax^2 + bxy + cy^2$ como

$$\Delta = b^2 - 4ac$$

Tenemos el siguiente teorema:

Teorema [Lagrange]: Sea Δ un entero no cuadrado. Podemos encontrar una forma cuadrática $ax^2 + bxy + cy^2$ de discriminante Δ y con una solución primitiva para

$$ax^2 + bxy + cy^2 = n \quad (A)$$

si y solo si la congruencia

$$z^2 + \rho z - \left(\frac{\Delta - \rho}{4}\right) \equiv 0 \pmod{n} \quad (B)$$

tiene una solución, siendo $\rho = \dfrac{1 - (-1)^b}{2}$

Demostración: Supongamos que (α, β) es una solución primitiva de (A). Podemos usar la identidad de Bezout y obtener enteros γ, δ tales que $\alpha\gamma + \beta\delta = 1$

Tomamos enteros X e Y tales que $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \alpha & -\delta \\ \beta & \gamma \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix}$

Notemos que $det \begin{bmatrix} \alpha & -\delta \\ \beta & \gamma \end{bmatrix} = 1$, por lo que es una matriz inversible sobre los enteros.

Sean

$$r = a\alpha\delta + c\beta\delta + \frac{b + \rho}{2}$$
$$s = a\delta^2 + b\delta\gamma + c\gamma^2$$

r es entero por compartir paridad ρ y b.
Sustituyendo x e y en (A) y operando, se obtiene

$$a(\alpha X - \delta Y)^2 + b(\alpha X - \delta Y)(\beta X + \gamma Y) + c(\beta X + \gamma Y)^2 =$$
$$= nX^2 + (2r + \rho)XY + sY^2 = n$$

La ecuación $nX^2 + (2r + \rho)XY + sY^2 = n$ (C) tiene la solución $X = 1,\ Y = 0$, que se corresponde con $\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha & -\delta \\ \beta & \gamma \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

El discriminante de (C) es $(2r+\rho)^2 - 4sn = \Delta$ (D), por lo cual tenemos una solución de (B) dada por $z = r$, $r^2 + \rho r - \left(\dfrac{\Delta - \rho}{4}\right) = sn$

Supongamos ahora que r es solución de (B). Podemos obtener s a partir de la ecuación (D) y tenemos como solución para (C) $X = 1,\ Y = 0$. Entonces tenemos una solución (primitiva) para la ecuación $nx^2+(2r+\rho)xy+s^2y^2 = n$, que tiene discriminante Δ **CQD**

Nótese que no estamos demostrando la existencia de solución (primitiva) de una forma cuadrática de discriminante Δ, sino la existencia de una forma cuadrática de discriminante Δ y con solución (primitiva).

1.2.3. La Ley de Reciprocidad Cuadrática

La ley de reciprocidad cuadrática es el resultado más importante sobre residuos cuadráticos. Esta ley estudia la existencia de soluciones de pares de ecuaciones del tipo

$$x^2 \equiv p \pmod{q},\ y^2 \equiv q \pmod{p}$$

En particular, existe solución para ambas si alguno de los dos es congruente con 1 módulo 4, y si ambos son congruentes con 3, solo una congruencia del par tiene solución. Como notación se introduce el símbolo de Legendre para un primo impar p y un entero a,

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p|a \\ 1 & \text{si } p \nmid a \text{ y } x^2 \equiv a \pmod{p} \text{ tiene solucion} \\ -1 & \text{en otro caso} \end{cases}$$

Estudiar las propiedades del símbolo de Legendre puede facilitar encontrar soluciones de ciertas ecuaciones Diofánticas.

Teorema [Criterio de Euler]: Sea p un primo impar.

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

Demostración: Es evidente si p es factor de a, así que suponemos que a y p son coprimos.
Por ser coprimos, $a^{p-1} \equiv 1 \pmod{p}$ y como las únicas raíces de 1 módulo p son ± 1, $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$

Sea g un elemento generador de $(\mathbb{Z}/p\mathbb{Z})^*$, $a \equiv g^j \pmod{p}$ para algún j. Supongamos que a es residuo cuadrático. Tenemos que j es par, $j = 2j'$ para algún j'. En consecuencia

$$a^{(p-1)/2} \equiv (g^j)^{(p-1)/2} = (g^{p-1})^j \equiv 1 \pmod{p}$$

En conclusión, $\left(\frac{a}{p}\right) = 1$ implica $a^{(p-1)/2} \equiv 1 \pmod{p}$

Veamos la implicación contraria. $a^{(p-1)/2} \equiv 1 \pmod{p}$ y $g^{j(p-1)/2} \equiv 1 \pmod{p}$. Como g tiene orden $p-1$, tenemos que $(p-1)|j(p-1)/2$ y $2(p-1)|j(p-1)$.

Deducimos entonces que j es par y a es residuo cuadrático módulo p, es decir, $\left(\frac{a}{p}\right) = 1$ **CQD**

Como corolario inmediato, obtenemos que el símbolo de Legendre es multiplicativo respecto al primer término,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Teorema [Ley de Reciprocidad Cuadrática]: Dados p, q primos impares, si $p \equiv q \equiv 3 \pmod{4}$,

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$$

Si al menos uno de los dos es congruente con 1 módulo 4, los símbolos son iguales.

Este teorema junto con las propiedades vistas y el siguiente resultado nos permitirá verificar de manera eficiente si un entero cualquiera es residuo cuadrático de un primo cualquiera.

Teorema: Si p es un primo impar, entonces

$$\left(\frac{2}{p}\right) = 1 \text{ si y solo si } p \equiv \pm 1 \pmod 8$$

Veamos una demostración poco pulida:
Por ser p impar, 8 divide a $p^2 - 1$. Siendo $\mathbb{F}$ el cuerpo con p^2 elementos, se tiene que $\mathbb{F}^*$ es un grupo cíclico de orden $p^2 - 1$, y existe un elemento de orden 8 en él, ξ. Denotando $G = \xi - \xi^3 - \xi^5 + \xi^7$, se puede comprobar, usando $\xi^4 = -1$, que $G^2 = 8$

Consideramos la función f dada por

$$f(j) = \begin{cases} 0 & \text{si j es par} \\ (-1)^{(j^2-1)/8} & \text{si j es impar} \end{cases}$$

que cumple la propiedad $f(p)f(pj) = f(j) \forall j \in \mathbb{Z}$. Buscamos 2 expresiones distintas para G^p:

1: $G^p = GG^{p-1} = G8^{(p-1)/2} = G\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)$

2: $G^p = (\sum_{j=0}^{7} f(j)\xi^j)^p = \sum_{j=0}^{7} f(j)\xi^{pj} = \sum_{j=0}^{7} f(p)f(pj)\xi^{pj} =$
$= f(p)\sum_{j=0}^{7} f(pj)\xi^{pj} = f(p)\sum_{j=0}^{7} f(j)\xi^j = f(p)G$

Concluimos que $f(p) = \left(\frac{2}{p}\right)$ por ser G distinto de 0, y $f(p)$ es 1 si y solo si p es congruente con ± 1 módulo 8 **CQD**.

La demostración de la Ley de Reciprocidad Cuadrática se puede hacer de forma similar a esta última y no se desarrollará, en parte por la pesadez de la notación.

Con estos resultados estamos en posición de calcular rápidamente símbo-

los de Legendre. Tomemos como ejemplo:

$$\left(\frac{1003}{401}\right) = \left(\frac{201}{401}\right) = \left(\frac{3}{401}\right)\left(\frac{67}{401}\right) = \left(\frac{401}{3}\right)\left(\frac{401}{67}\right)(-1)^2 =$$
$$= \left(\frac{2}{3}\right)\left(\frac{66}{67}\right) = (-1)\left(\frac{2}{67}\right)\left(\frac{3}{67}\right)\left(\frac{11}{67}\right) = \left(\frac{67}{3}\right)\left(\frac{67}{11}\right) = \left(\frac{1}{3}\right)\left(\frac{1}{11}\right) = 1$$

1.3. Alternativa al Teorema fundamental de la Aritmética

1.3.1. El TFA para ideales

Se sabe que en los anillos que poseen una norma se puede definir un algoritmo de división, y como consecuencia se prueba la existencia de un TFA. Tal norma es relativamente intuitiva cuando se consideran algunos anillos de enteros algebraicos sobre $\mathbb{Z}$ (es decir, anillos formados por las raíces de polinomios mónicos con coeficientes enteros), como ya se ha visto. Sin embargo, no todos esos anillos son euclídeos, y tampoco es posible obtener factorizaciones en primos de sus elementos.

De este obstáculo surge otra idea para replantear el concepto de factorización en un anillo de enteros: en lugar de obtener una descomposición en factores primos, se podría intentar descomponer sus ideales en un producto de ideales primos.

Desde aquí hasta el fin del capítulo se va a trabajar en un cuerpo $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ y en su anillo de enteros sobre $\mathbb{Z}$, para algún d libre de cuadrados. Denotamos este anillo $O_{\mathbb{K}}$ Consideramos entonces la norma y traza de $\alpha = x + y\sqrt{d}$

$$N(\alpha) = x^2 - dy^2$$
$$T(\alpha) = 2x$$

Caractericemos el anillo de enteros sobre $\mathbb{Q}(\sqrt{d})$. Si $d \equiv 2$ o $3 \pmod 4$ éste es $\mathbb{Z}[\sqrt{d}]$, y si $d \equiv 1 \pmod 4$, este es $\mathbb{Z}[(1+\sqrt{d})/2]$

Demostración: Por ser $\mathbb{Q}(\sqrt{d})$ extensión de grado 2, tenemos que en particular todos los elementos de su anillo de enteros son solución de una ecuación mónica de coeficientes enteros y de grado 2, $x^2 + bx + c = 0$.
Consideramos sus posibles soluciones $\dfrac{-b \pm \sqrt{b^2 - 4c}}{2}$. Podemos considerar que el término de la raíz es distinto de 0 para buscar elementos fuera de $\mathbb{Z}$. Consideramos 2 casos:

1. $d \not\equiv 1 \pmod 4$. En este caso no se puede cumplir la congruencia $b^2 \equiv 1 \pmod 4$. Estudiamos en su lugar $(b^2-4c)/4 = d$, resultado de introducir el denominador 2 en la raíz. Si consideramos $b = 2b'$ par, entonces se pueden encontrar soluciones para $((2b')^2 - 4c)/4 = d$, $b'^2 - c = d$. Obtenemos elementos del tipo $\dfrac{b}{2} \pm \dfrac{\sqrt{4d}}{2} = b' + \sqrt{d}$, b' entero.
2. $d \equiv 1 \pmod 4$, $d = 4n+1$. Buscamos soluciones enteras para $b^2 - 4c = = d = 4n + 1$ para incógnitas b y c, lo que es equivalente a resolver la congruencia $b^2 \equiv 1 \pmod 4$, que tiene solución siempre que b es impar. Obtenemos entonces elementos de la forma $\dfrac{b}{2} \pm \dfrac{\sqrt{d}}{2}$ con b impar. Si consideramos el caso par, se reducen a elementos del tipo anterior.

Los elementos generadores de los anillo de enteros en cada caso son los buscados.

Dado $\alpha = x + y\sqrt{d}$, definimos el conjugado de α, $\alpha^* = x - y\sqrt{d}$. Dado I un ideal, se define el ideal I^* como el conjunto de conjugados de los elementos de I. Se tiene que el conjugado de la suma y producto de ideales es la suma y producto de los ideales conjugados, respectivamente.

Consideramos $\delta \in O_{\mathbb{K}}$ verificando $O_{\mathbb{K}} = \mathbb{Z}[\delta]$.

Teorema: Sea I un ideal en $O_{\mathbb{K}}$. Entonces existen α, β en I tales que $I = (\alpha, \beta)$

Añadimos como notación, para $\alpha_1, \ldots, \alpha_k \in O_{\mathbb{K}}$,
$(\alpha_1, \ldots, \alpha_k) = (\alpha_1) + \cdots + (\alpha_k)$

Lema [Hurwitz]: Si α, β son elementos de $O_{\mathbb{K}}$ y $k \in \mathbb{Z}$ divide a $N(\alpha)$, $N(\beta)$ y $T(\alpha\beta^*)$ (siendo T la aplicación traza), entonces k divide a $\alpha\beta^*$ y $\alpha^*\beta$ en $O_{\mathbb{K}}$

Como corolario, sabemos que para todo I ideal en $O_{\mathbb{K}}$, II^* es un ideal principal de $\mathbb{Z}$, $k\mathbb{Z}$.

Podemos entonces definir la norma de un ideal en $O_{\mathbb{K}}$:
$N(I) = k$ para el entero positivo k tal que $II^* = k\mathbb{Z}$.

Corolario: Si $I \neq \{0\}$, J,K son ideales de $O_{\mathbb{K}}$ y IJ=IK, entonces J=K.

Podemos pasar a definir el concepto de divisibilidad de ideales. Dados dos ideales I,J en $O_{\mathbb{K}}$, decimos que I divide a J, I|J si existe un ideal $K \subseteq O_{\mathbb{K}}$ tal que J=IK. Además, se tiene como resultado que I|J si y solo si $J \subseteq I$.

Demostración:
Como el producto de ideales está contenido en su intersección, I|J implica J=IK y J está contenido en I.
Sean J, I ideales, $J \subseteq I$. Entonces $JI^* \subseteq II^* = (N(I))$. Para todo elemento $a \in JI^*$, N(I) divide a a. Podemos considerar

$$K = \frac{1}{N(I)} JI^*$$

ideal contenido en $O_{\mathbb{K}}$. Se tiene que

$$IK = \frac{1}{N(I)} I(JI^*) = \frac{N(I)}{N(I)} J = J$$

Por definición, I|J.

Ahora estamos en condiciones de probar el TFA para ideales:

Teorema Fundamental de la Aritmética para ideales: Todo ideal

propio no nulo de $O_{\mathbb{K}}$ se puede escribir como producto de ideales primos, siendo la factorización única salvo el orden.

Demostración: Si el ideal a considerar es maximal, entonces es primo. Sea I un ideal no maximal. Sabemos que está contenido en un ideal maximal y por tanto se puede escribir como producto de dos ideales. En particular, esos dos ideales tienen norma menor que la de I. Si se continúa descomponiendo los ideales no maximales, obtenemos ideales de norma cada vez estrictamente menor, por lo que la secuencia de factores de I termina tras un número finito de descomposiciones, y obtenemos una factorización en ideales maximales. Como los ideales maximales son también primos, concluimos la demostración notando que la unicidad se deriva de la propiedad cancelativa de ideales propios no nulos comunes a dos productos.

Capítulo 2

Fundamentos algebraicos de la teoría de números

El objetivo principal de este capítulo es intentar extender conceptos estudiados en el capítulo anterior sobre extensiones cuadráticas de $\mathbb{Q}$ a anillos más generales, en particular, a otros cuerpos de números (extensiones finitas de $\mathbb{Q}$). Entre estos conceptos nos enfocaremos en el TFA para ideales y veremos una demostración para el teorema de clases de ideales.

2.1. Preliminares

En este apartado se exponen algunos conceptos y resultados fundamentales sobre anillos e ideales, principalmente, que son necesarios para probar importantes resultados.

2.1.1. Ideales fraccionarios

Dado un dominio de integridad A y su cuerpo de fracciones K, se llama **ideal fraccionario de A** a cualquier I A-submódulo de K tal que $dI \subseteq A$ ($I \subseteq d^{-1}A$) para algún $d \in A$, es decir, tal que los elementos de I tienen un denominador común d.
Los ideales de A son en particular fraccionarios para $d = 1$, y se pueden denominar ideales enteros.

Se puede definir el producto de ideales fraccionarios de forma análoga al producto de ideales que ya conocemos, II' sería el conjunto de sumas finitas $\sum x_i y_i$ con $x_i \in I,\ y_i \in I'$. La intersección, suma y producto de dos ideales fraccionarios es a su vez un ideal fraccionario. Adicionalmente, si d y d' son sus denominadores comunes, el denominador común es d (o d'), dd' y dd' respectivamente.

2.1.2. Anillos de enteros

Dados un anillo R, A un subanillo de R y $x \in R$, se dice que x es entero sobre A si cumple cualquiera de las siguientes condiciones equivalentes:

- Existen $a_0, \ldots, a_{n-1} \in A$ tales que
$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$
es decir, x es raíz de un polinomio mónico con coeficientes en A
- El anillo $A[x]$ es un A-módulo de tipo finito
- Existe un subanillo de R que contiene a A y a x y que es A-módulo de tipo finito.

En las condiciones anteriores, el conjunto de los elementos de R enteros sobre A es un subanillo de R que contiene a A.
Se definen también

- **Clausura entera de A en R**: Dicho subanillo de los enteros de R sobre A.
- **Clausura entera de A**: La clausura entera de A en K, siendo A un dominio de integridad y K el cuerpo de fracciones de A.
- **R es entero sobre A** si todo elemento de R es entero sobre A.
- Un anillo es **íntegramente cerrado** si es un dominio de integridad y su clausura entera es él mismo.

Una propiedad básica es que la propiedad de un anillo de ser entero se conserva por transitividad, es decir, si C es un anillo, B subanillo de C y A subanillo de B tales que C es entero sobre B y B es entero sobre A, entonces C es entero sobre A.

Sean A un anillo, E un A-módulo libre de rango finito, x un elemento de E y m_x el endomorfismo de E dado por la multiplicación por el elemento x, se puede representar dada una base (e_i) por una matriz (a_{ij}) en esta base. Se definen:

- Traza de x, $Tr(x) = Tr(m_x) = \sum_{i=1}^{n} a_{ii}$
  Alternativamente, es el coeficiente del término de orden 1 del polinomio característico de m_x
- Norma de x, $N(x) = det(m_x) = det(a_{ij})$
  Alternativamente, es el término independiente del polinomio característico de m_x

Al trabajar sobre un cuerpo de característica 0 $\mathbb{K}$ y una extensión algebraica finita suya, $\mathbb{L}$, se denotan también $Tr_{\mathbb{L}/\mathbb{K}}(x)$ y $N_{\mathbb{L}/\mathbb{K}}(x)$, respectivamente.
Cuando se toma x un elemento de $\mathbb{L}$ entero sobre A, entonces los coeficientes del polinomio característico (en particular $Tr_{\mathbb{L}/\mathbb{K}}(x)$ y $N_{\mathbb{L}/\mathbb{K}}(x)$) son enteros sobre A. Si además A es íntegramente cerrado, los coeficientes son elementos de A.

Sean B un anillo y A un subanillo de B tal que B es A-módulo libre de rango finito n. Para un sistema $(x_1, \ldots, x_n) \in B^n$, se define el **discriminante** de $(x_1, \ldots, x_n)$ al elemento de A dado por $D(x_1, \ldots, x_n) = det(Tr(x_i x_j))$

Proposición: Si $(y_1, \ldots, y_n)$ es otro sistema de elementos de B tal que $y_i = \sum_{i=1}^{n} a_{ij} x_j,\ a_{ij} \in A$, entonces $D(y_1, \ldots, y_n) = det(a_{ij})^2 D(x_1, \ldots, x_n)$

Como consecuencia directa, los discriminantes de las bases son asociados, y está bien definido el **discriminante** de B sobre A ($\mathfrak{D}_{B/A}$) como el ideal de A engendrado por el discriminante de cualquier base de B sobre A.

Otro resultado es que un sistema $(x_1, \ldots, x_n)$ es base de B sobre A si y solo si $D(x_1, \ldots, x_n)$ engendra $\mathfrak{D}_{B/A}$.
Se tiene también que dados K cuerpo finito o de carecterística 0 y L una extensión finita suya, el discriminante de cualquier base de L sobre K es distinto de 0.

Se denomina **cuerpo de números** a cualquier extensión finita y algebraica $\mathbb{K}$ de $\mathbb{Q}$. El grado de la extensión $[\mathbb{K} : \mathbb{Q}]$ se llama **grado de** $\mathbb{K}$.
Por abuso de notación, se llaman enteros de $\mathbb{K}$ a los elementos de $\mathbb{K}$ enteros sobre $\mathbb{Z}$, que forman un anillo A que es $\mathbb{Z}$-módulo libre del mismo rango que el grado de $\mathbb{K}$.
Por un resultado anterior, sabemos que los discriminantes de las bases de A como $\mathbb{Z}$-módulo difieren entre sí por el cuadrado de un elemento inversible en $\mathbb{Z}$, esto es, el cuadrado de ± 1. Se tiene entonces que para toda base del $\mathbb{Z}$-módulo A, su discriminante es único y se le llama **discriminante absoluto de** $\mathbb{K}$.

2.1.3. $\mathbb{Q}$-isomorfismos

Dado $\mathbb{K}$ un cuerpo de números de grado n, sabemos que existen n $\mathbb{Q}$-isomorfismos distintos de $\mathbb{K}$ en $\mathbb{C}$, es decir, n aplicaciones $\sigma_i : \mathbb{K} \to \mathbb{C}$ verificando que $\sigma_i(\mathbb{Q}) = \mathbb{Q}$. Además, si x es un elemento primitivo que genera la extensión $\mathbb{K}$, las aplicaciones quedan completamente determinadas por su ac-

ción sobre x, siendo esta $\sigma_i(x) = x_i$, y siendo $\{x_i\}_{i=1,\dots,n}$ el conjunto de raíces del polinomio irreducible de x, que sabemos también que son distintas:

En efecto, si consideramos $F(X)$ polinomio irreducible de grado n sobre $\mathbb{Q}$, sin perder generalidad mónico, $F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, si tiene una raíz múltiple x_i entonces el polinomio derivado $F'(X) = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1$ tiene como raíz a x_i. Por ser $F(X)$ polinomio mínimo para todas sus raíces, en particular lo es para x_i, y por tener $F'(X)$ menor grado que el polinomio mínimo de x_i, entonces $F'(X) = 0$. En particular, $nX^{n-1} = 0$ y $n \cdot 1 = 0$, lo que lleva a contradicción.

Si alguna de dichas raíces es compleja, sabemos que su conjugado es también una raíz. Se tiene entonces que hay un número par de raíces con parte imaginaria no nula, $2r_2$, y con el número de raíces reales r_1, se tiene que $n = r_1 + 2r_2$. Además, exactamente r_1 índices i verifican $\sigma_i(\mathbb{K}) \subset \mathbb{R}$

2.1.4. Retículos en $\mathbb{R}^n$

Veremos conceptos y resultados que serán útiles a la hora de presentar cotas para las normas de elementos e ideales, así como discriminantes.

Un subgrupo aditivo de $\mathbb{R}^n$ se dice discreto si para todo compacto K de $\mathbb{R}^n$, $K \cap \mathbb{R}^n$ es finito.
Además, $\mathbb{Z}^r, r \leq n$ es el único subgrupo discreto de $\mathbb{R}^n$ salvo isomorfismo, y está generado como $\mathbb{Z}$-módulo por r verctores linealmente independientes sobre $\mathbb{R}$

En particular, si el subgrupo discreto H es de rango n, se le llama **retículo** de $\mathbb{R}^n$.
Dada una base $e = (e_1, \dots, e_n)$ de H, y designando μ la medida de Lebesgue, llamamos **volumen del retículo H**,$v(H)$, a la medida del conjunto

$$P_e = \left\{ \sum_{i=1}^{n} \alpha_i e_i \mid 0 \leq \alpha_i < 1 \right\}$$

Se tiene que $\mu(P_e)$ es independiente de la base elegida. En efecto, sea $f = (f_1, \ldots, f_n)$ otra base de H. $f_i = \sum_{j=1}^{n} a_{ij} e_j,\ a_{ij} \in \mathbb{Z}$. Sabemos que el determinante de la matriz (a_{ij}) de cambio de base es una unidad en $\mathbb{Z}$ por lo que, considerando que $\mu(P_f) = |det(a_{ij})|\mu(P_e)$, y la igualdad es evidente al ver que las únicas unidades de $\mathbb{Z}$ son ± 1.

Sea $\mathbb{K}$ un cuerpo de números de grado n y sus $\mathbb{Q}$-isomorfismos asociados, σ_i, con r_1, r_2 los enteros dados anteriormente. Ordenamos los σ_i de forma que $\sigma_i(\mathbb{K}) \subset \mathbb{R}, 1 \leq i \leq r_1,\ \sigma_{j+r_2} = \bar{\sigma}_i, r_1 + 1 \leq j \leq r_1 + r_2$. Para $x \in \mathbb{K}$, definimos la aplicación $\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, y se llama **inmersión canónica de $\mathbb{K}$ en $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$**.

Tenemos los siguientes resultados:

Proposición: Dados M un $\mathbb{Z}$-submódulo de $\mathbb{K}$ y $(x_i)_{1 \leq i \leq n}$ una $\mathbb{Z}$-base de M, se tiene que $\sigma(M)$ es un retículo de $\mathbb{R}^n$ cuyo volumen es
$v(\sigma(M)) = 2^{-r_2}|det(\sigma_i(x_j))|$

Proposición: Sean d el discriminante absoluto de $\mathbb{K}$, A su anillo de enteros y $\mathfrak{a}$ un ideal de A (entero) no nulo. Entonces $\sigma(A)$ y $\sigma(\mathfrak{a})$ son retículos y sus volúmenes son:

$$v(A) = 2^{-r_2}|d|^{1/2}$$
$$v(\mathfrak{a}) = 2^{-r_2}|d|^{1/2}N(\mathfrak{a})$$

2.2. Anillos Noetherianos y de Dedekind.

Teorema: Dado A un anillo y M un A-módulo, los siguientes enunciados son equivalentes:

a) Toda familia no vacía de submódulos de M contiene un elemento maximal bajo la relación de inclusión.

b) Toda sucesión creciente $(M_n)_{n \geq 0}$ de submódulos de M es estacionaria

c) Todo submódulo de M es de tipo finito

Demostración:

$a \Rightarrow c)$ Sea E submódulo de M y Φ la familia de submódulos de tipo finito de E, que es no vacía por incluir al submódulo cero. Por a), Φ tiene un elemento maximal F. Para $x \in E$ consideramos el submódulo $F + Ax$, que es de tipo finito por ser generado por el sistema finito que genera a F más $\{x\}$. Por ser F maximal, $F + Ax \subseteq F$, y $x \in F$. Se deduce que E=F y E es de tipo finito.

$c \Rightarrow b)$ Sea $(M_n)_{n\geq 0}$ una sucesión creciente de submódulos de M. Entonces $E = \bigcup_{n\geq 0} M_n$ es un submódulo de M. Por c), E admite un sistema generador finito, $\{x_1, \ldots, x_q\}$. Para cada $i \in \{1, \ldots, q\}, \exists n(i)$ tal que $x_i \in M_{n(i)}$. Sea $n_0 = max\{n(1), \ldots, n(q)\}$. Claramente, $E \subseteq M_{n_0}$ y $E = M_{n_0}$. Se concluye que para $n \geq n_0$, $M_n = M_{n_0}$ y la sucesión es estacionaria a partir de n_0.

Para terminar el resultado, veamos la equivalencia de a) y b) con un resultado sobre los conjuntos ordenados:

Lema: Sea T un conjunto ordenado. Son equivalentes:

a) Toda familia no vacía de elementos de T contiene un elemento maximal.

b) Toda sucesión creciente $(t_n)_{n\geq 0}$ de elementos de T es estacionaria

Demostración:

$a \Rightarrow b)$ Si tomamos como elemento maximal de la sucesión a t_q, por ser esta creciente $t_n = t_q$ para n mayor que q, y es sucesión estacionaria.

$b \Rightarrow a)$ Consideramos S un subconjunto no vacío de T. Si suponemos que no existe elemento maximal en S, $\forall x \in S$, $\exists\ x' > x$. Por el axioma

de elección, existe $f : S \to S$ tal que $f(x) > x$. Por ser S no vacío, existe $t_0 \in S$. Definimos una sucesión $(t_n)_{n\geq 0}$ tomando $t_{n+1} = f(t_n)$, y resulta ser una sucesión creciente y no estacionaria, lo que contradice b). **CQD**

Un A-módulo M se llama **noetheriano** si verifica las condiciones equivalentes del teorema anterior. Respectivamente, a un anillo A se le llama noetheriano si lo es al considerarle como A-módulo.

Como corolario del teorema anterior, dado A un anillo de ideales principales, este es noetheriano (sus A-submódulos son sus ideales, que son de tipo finito por ser engendrados por un solo elemento).

Proposición: Dados A un anillo, E un A-módulo y E' submódulo de E, entonces E es noetheriano si y solo si E' y E/E' son noetherianos.

Demostración:

$\Rightarrow$ Los conjuntos ordenados de submódulos de E' y E/E' son isomorfos a los de submódulos de E contenidos en E' o que contienen a E', respectivamente. Por a) del teorema anterior, se deduce que E' y E/E' son noetherianos.

$\Leftarrow$ Sea $(F_n)_{n\geq 0}$ una sucesión creciente de submódulos de E. Por ser E' noetheriando, existe un entero n_0 tal que $F_n \cap E' = F_{n+1} \cap E'$ $\forall n \geq n_0$. De forma similar, por ser E/E' noetheriano, existe un entero n_1 tal que $(F_n + E')/E' = (F_{n+1} + E')/E'$ $\forall n \geq n_1$. Tomando n mayor que n_0 y n_1, veamos que $F_n = F_{n+1}$; basta ver que $F_{n+1} \subseteq F_n$. Sea $x \in F_{n+1}$. Como $(F_n + E')/E' = (F_{n+1} + E')/E'$, existen $y \in F_n$, $z, z' \in E'$ verificando $x + z = y + z'$, y $x - y = z' - z \in F_{n+1} \cap E' = F_n \cap E'$. Entonces $x - y \in F_n$ y x está en F_n por estarlo y. **CQD**

En conclusión, $F_{n+1} = F_n$ para n mayor que n_0 y n_1 y E es noetheriano.

Como corolario, el producto cartesiano de A-módulos noetherianos es noetheriano, y para un anillo noetheriano B, cualquier B-módulo de tipo finito es noetheriano.

Proposición: Dados A un anillo noetheriano íntegramente cerrado, K su cuerpo de fracciones de característica 0, L una extensión finita de K y A' la clausura entera de A en L, se tiene que A' es un A-módulo de tipo finito y un anillo noetheriano.
Este resultado se puede aplicar a los números enteros, siendo $\mathbb{Z}$ anillo íntegramente cerrado, y obtenemos que todo anillo de enteros sobre una extensión de $\mathbb{Q}$ es noetheriano.

Definición: Se define un **anillo de Dedekind** como un anillo noetheriano, íntegramente cerrado y tal que todo ideal primo no nulo suyo sea maximal.

Se puede obtener un resultado similar al anterior respecto a los anillos de Dedekind

Teorema: Sean A anillo de Dedekind, K su cuerpo de fracciones y de característica 0, L una extensión finita de K y A' la clausura entera de A en L. Se tiene que A' es anillo de Dedekind y A-módulo de tipo finito.

Demostración: Por construcción, A' es íntegramente cerrado, y es A-módulo de tipo finito y noetheriano por la proposición anterior. Veamos que todo ideal primo suyo no nulo $\mathfrak{p} \neq (0)$ es maximal. Sea $x \in \mathfrak{p},\ x \neq 0$. Tenemos una ecuación de dependencia entera de x sobre A de grado mínimo,

- $x^n + a_{n-1}x^{n-1} + \cdots + a_1x^1 + a_0 = 0 \qquad a_i \in A$

Por ser de grado mínimo, $a_0 \neq 0$ y $a_0 \in A'x \cap A \subseteq \mathfrak{p} \cap A$, y $\mathfrak{p} \cap A \neq 0$.
Como $\mathfrak{p} \cap A$ es un ideal primo de A, es también maximal por ser A de Dedekind, y $A/\mathfrak{p} \cap A$ es un cuerpo. A su vez $A/\mathfrak{p} \cap A$ se identifica con un subanillo de $A'/\mathfrak{p}$ y como A' es entero sobre A, $A'/\mathfrak{p}$ es entero sobre $A/\mathfrak{p} \cap A$. Concluimos que $A'/\mathfrak{p}$ es un cuerpo y $\mathfrak{p}$ es maximal en A'. **CQD**

De nuevo, trabajando sobre $\mathbb{Z}$, se obtiene que el anillo de los enteros de un cuerpo de numéros es de Dedekind, lo que se puede utilizar como sustituto para la propiedad de dominio de ideales principales, que no siempre se da.

Con los siguientes teoremas se intenta obtener una descomposición en producto de ideales primos de los ideales fraccionarios de los anillos de Dedekind.

Lema: Si un ideal primo contiene un producto de ideales, entonces contiene a uno de ellos.

Lema: En un anillo noetheriano, todo ideal contiene un producto de ideales primos. Si además es anillo íntegro, todo ideal no nulo suyo contiene un producto de ideales primos no nulos.

Teorema: Sea A un anillo de Dedekind no cuerpo. Todo ideal maximal de A es inversible en el monoide de los ideales fraccionarios de A (sobre su cuerpo de fracciones K)

Demostración: Sea $\mathfrak{m}$ ideal maximal de A, $\mathfrak{m} \neq (0)$ por no ser A un cuerpo. Definimos el ideal

$$\mathfrak{m}' = \{x \in K \mid x\mathfrak{m} \subseteq A\}$$

que es claramente un ideal fraccionario al admitir como denominador a cualquier elemento de A no nulo. Veamos que $\mathfrak{m}\mathfrak{m}' = A$.

Se ve de forma inmediata que $\mathfrak{m}\mathfrak{m}' \subseteq A$, por definición de $\mathfrak{m}'$.

Se tiene que $A \subseteq \mathfrak{m}'$ y $\mathfrak{m} = \mathfrak{m}A \subseteq \mathfrak{m}\mathfrak{m}'$. Por ser $\mathfrak{m}$ maximal y $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{m}' \subseteq A$, o bien $\mathfrak{m} = \mathfrak{m}\mathfrak{m}'$ o bien $\mathfrak{m}\mathfrak{m}' = A$.

Supongamos que $\mathfrak{m} = \mathfrak{m}\mathfrak{m}'$. Sea $x \in \mathfrak{m}'$. Por hipótesis, $x\mathfrak{m} \subseteq \mathfrak{m}$, y toda potencia x^n verifica $x^n\mathfrak{m} \subseteq \mathfrak{m}$ y se puede tomar como denominador común cualquier elemento no nulo de $\mathfrak{m}$, por lo que $A[x]$ es un ideal fraccionario de A. Por ser A noetheriano, $A[x]$ es de tipo finito, x es entero sobre A y, por ser A íntegramente cerrado, $x \in A$. Se concluye que $\mathfrak{m}' = A$.

Ahora, sea $a \in \mathfrak{m},\ a \neq 0$. Aa contiene un producto de ideales primos no nulos, $\mathfrak{p}_1 \dots \mathfrak{p}_n$, n mínimo (sin perder generalidad). Entonces $\mathfrak{m} \supseteq Aa \supseteq \mathfrak{p}_1 \dots \mathfrak{p}_n$. Por ser $\mathfrak{m}$ primo, contiene a alguno de los $\mathfrak{p}_i$ y por ser este maximal, $\mathfrak{m} = \mathfrak{p}_i$. Suponemos $i = 1$. Si denotamos $\mathfrak{b} = \mathfrak{p}_2 \dots \mathfrak{p}_n$, entonces $\mathfrak{m}\mathfrak{b} \subseteq Aa$ y

$\mathfrak{b} \nsubseteq Aa$ por ser n mínimo. Entonces $\exists b \in \mathfrak{b}$ tal que $b \notin Aa$.
Como $\mathfrak{m}\mathfrak{b} \subseteq Aa$, $\mathfrak{m}b \subseteq Aa$ y $\mathfrak{m}ba^{-1} \subseteq A$. Por definición, $ba^{-1} \in \mathfrak{m}'$. Sin embargo, como $b \notin Aa$, entonces $ba^{-1} \notin A$, por lo que $\mathfrak{m}' \neq A$, lo que es absurdo.

Como el absurdo proviene de suponer $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$, concluimos que $\mathfrak{m}\mathfrak{m}' = A$ **CQD**

Teorema: Sean A anillo de Dedekind y P el conjunto de ideales primos no nulos de A:

a) Todo ideal fraccionario no nulo $\mathfrak{b}$ de A se escribe de modo único como producto (finito) de potencias enteras (en $\mathbb{Z}$) de ideales de A:

$$\mathfrak{b} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{b})}$$

con $n_{\mathfrak{p}}(\mathfrak{b}) \in \mathbb{Z}$ casi todos nulos

b) El monoide de los ideales fraccionarios no nulos de A es un grupo

Demostración: Demostramos primero la existencia de una descomposición. Por ser $\mathfrak{b}$ fraccionario, existe un elemento d en A tal que $d\mathfrak{b} \subseteq A$, esto es, $d\mathfrak{b}$ es ideal de A. Entonces $\mathfrak{b} = (d\mathfrak{b}).(Ad)^{-1}$ y nos reducimos al caso de un ideal entero. Sea Φ la familia de ideales no nulos de A que no se pueden expresar como producto de ideales primos. Supongamos que es no vacía: por ser A noetheriano existe un elemento maximal $\mathfrak{a} \neq A$ por ser A producto (vacío) de ideales primos de A. Existe un ideal maximal $\mathfrak{p}$ que contiene a $\mathfrak{a}$, se puede tomar un elemento maximal de la familia de ideales no triviales que contienen a $\mathfrak{a}$ (existe por ser A noetheriano).
Por el teorema anterior, se puede tomar $\mathfrak{p}'$ el ideal fraccionario inverso de $\mathfrak{p}$. Se verifica $\mathfrak{a}\mathfrak{p}' \subseteq \mathfrak{p}\mathfrak{p}' = A$. Por darse $\mathfrak{p}' \supsetneq A$, se tiene que $\mathfrak{a}\mathfrak{p}' \supsetneq \mathfrak{a}$. En caso contrario, si $x \in \mathfrak{p}'$, para todo n entero $x^n\mathfrak{a} \subseteq \mathfrak{a}$ y x es entero sobre A, ergo (A íntegramente cerrado) $x \in A$, lo que es imposible porque $\mathfrak{p}' \neq A$(si no, $\mathfrak{p}' = A$, $\mathfrak{p}'\mathfrak{p} = \mathfrak{p} \neq A$).
Por el carácter maximal de $\mathfrak{a}$ en Φ, $\mathfrak{a}\mathfrak{p}' \notin \Phi$, y $\mathfrak{a}\mathfrak{p}'$ es producto de ideales primos $\mathfrak{p}_1 \dots \mathfrak{p}_n$. Multiplicando por $\mathfrak{p}$, se concluye que $\mathfrak{a}$ es producto de ideales primos.

Veamos ahora la unicidad. Supongamos $\prod_{\mathfrak{p}\in P}\mathfrak{p}^{n_\mathfrak{p}(\mathfrak{b})} = \prod_{\mathfrak{p}\in P}\mathfrak{p}^{m_\mathfrak{p}(\mathfrak{b})}$, esto es, $\prod_{\mathfrak{p}\in P}\mathfrak{p}^{n_\mathfrak{p}(\mathfrak{b})-m_\mathfrak{p}(\mathfrak{b})} = A$. Se separan los $n(\mathfrak{p})$ y los $m(\mathfrak{p})$ no nulos negativos y positivos para obtener

$$\mathfrak{p}_1^{\alpha_1}\dots\mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1}\dots\mathfrak{q}_l^{\beta_l}$$

De exponentes positivos y $\mathfrak{p}_i \neq \mathfrak{q}_j$, $\mathfrak{p}_i, \mathfrak{q}_j \in P$. Entonces $\mathfrak{p}_1$ contiene al producto de los $\mathfrak{q}_j$ y, por ser primo, contiene a uno de ellos, sin perder generalidad $\mathfrak{q}_1$. Por ser $\mathfrak{p}_1$ y $\mathfrak{q}_1$ maximales, se deduce $\mathfrak{p}_1 = \mathfrak{q}_1$, lo que lleva a contradicción.

b) es consecuencia directa de a) y de la existencia de ideal inverso para un ideal primo. **CQD**

Hemos visto que la familia I(A) de ideales fraccionarios es grupo. Si consideramos la familia de ideales fraccionarios principales F(A), de la forma Ax, $x \in K*$, podemos definir el grupo cociente C(A)=I(A)/F(A), que se denomina el grupo de las clases de ideales de A.

Una vez vista la descomposición de ideales en anillos de Dedekind, estamos en posición de estudiar el concepto de norma de un ideal entero sobre un cuerpo de numéros $\mathbb{K}$, de grado n y A su anillo de enteros.

Proposición: Dado $x \in A, x \neq 0$, se tiene que $|N(x)| = card(A/Ax)$

Dado un ideal $\mathfrak{a}$ de A entero y no nulo, se define la **norma de** $\mathfrak{a}$, $N(\mathfrak{a}) = card(A(\mathfrak{a}))$
Se tiene que el número $N(\mathfrak{a})$ es finito: si se toma $a \in \mathfrak{a}$, $Aa \subseteq \mathfrak{a}$. Es evidente que $card(A/\mathfrak{a}) \leq card(A/Aa)$. Además, como $a \in A$, se tiene que $N(a) \in \mathbb{Z}$ por ser A el anillo de enteros de $\mathbb{K}$ (sobre $\mathbb{Z}$). Por tanto, $card(A/Aa)$ es finito y $card(A/\mathfrak{a})$ también.

Como última parte de la sección, veamos que dados dos ideales enteros no nulos de A, $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

Demostración: Es suficiente demostrarlo en el caso en que $\mathfrak{b}$ es un ideal maximal $\mathfrak{m}$.

$card(A/\mathfrak{am}) = card(A/\mathfrak{a})card(\mathfrak{a}/\mathfrak{am})$. Veamos que $card(\mathfrak{a}/\mathfrak{am}) = card(A/\mathfrak{m})$. Como $\mathfrak{a}/\mathfrak{am}$ es un A-módulo anulado por $\mathfrak{m}$, es un espacio vectorial sobre $A/\mathfrak{m}$ cuyos subespacios son sus A-submódulos de la forma $\mathfrak{q}/\mathfrak{am}$, donde $\mathfrak{q}$ es un ideal tal que $\mathfrak{am} \subseteq \mathfrak{q} \subseteq \mathfrak{a}$. Por la descomposición en ideales maximales de $\mathfrak{am}$ y $\mathfrak{a}$, no existen ideales comprendidos estrictamente entre ambos. Se deduce que no existen subespacios vectoriales propios de $\mathfrak{a}/\mathfrak{am}$ sobre $A/\mathfrak{m}$, por lo que la dimensión de $\mathfrak{a}/\mathfrak{am}$ como espacio vectorial sobre $A/\mathfrak{m}$ es 1. Por tanto, $card(\mathfrak{a}/\mathfrak{am}) = card(A/\mathfrak{m})$. **CQD**

2.3. Finitud del grupo de clases de ideales

Proposición: Sean K un cuerpo de números de grado n, r_1, r_2 los enteros que determinan las raíces del polinomio mínimo de un elemento primitivo de K, d su discriminante absoluto y $\mathfrak{a}$ un ideal entero no nulo de K. Entonces, tal ideal contiene un elemento no nulo x tal que

$$|N_{\mathbb{K}/\mathbb{Q}}(x)| = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|d|^{1/2}N(\mathfrak{a})$$

Corolario: Con la misma notación, toda clase de ideales de K contiene un ideal $\mathfrak{b}$ entero tal que

$$N(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|d|^{1/2}$$

Corolario: Sean K cuerpo de números de grado n y d su discriminante absoluto. Para $n \geq 2$ se tiene que $|d| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$. Además, $\frac{n}{log|d|}$ está acotado por una constante independiente de $\mathbb{K}$.

Como consecuencia inmediata, se tiene que todo cuerpo de números $\mathbb{K} \neq \mathbb{Q}$ tiene como discriminante absoluto d de $\mathbb{K}$, $|d| \neq 1$

Teorema [Dirichlet]: Para todo cuerpo de números $\mathbb{K}$, el grupo de clases de ideales de $\mathbb{K}$ es finito.

Demostración: Como consecuencia directa del primer corolario, hay una cantidad finita de enteros que se pueden corresponder con la norma de un ideal $\mathfrak{b}$ entero. Será suficiente ver que el conjunto de ideales enteros con norma igual alguno de esos enteros es también finito. Sea $\mathfrak{b}$ tal que $card(A/\mathfrak{b}) = q$ (con A el anillo de enteros de $\mathbb{K}$), se sigue que $q \in \mathfrak{b}$; A/$\mathfrak{b}$ es un grupo de orden q, y $q \in A$. Se deduce fácilmente que en tal grupo cociente q se identifica con 0, por lo que $q \in \mathfrak{b}$.
Obtenemos entonces que $\mathfrak{b}$ contiene a Aq, y por finitud de A/Aq (la norma de todo ideal de A es finita), tenemos un número finito de ideales que contienen a Aq. **CQD**

Teorema [Hermite]: En $\mathbb{C}$ hay un número finito de cuerpos de númeross de discriminante d dado.

2.4. Unidades

Por unidades, nos referimos a los elementos del anillo de enteros de K inversibles, que forman un grupo multiplicativo denotado A*.

Proposición: Sea $\mathbb{K}$ un cuerpo de números y $x \in \mathbb{K}$. Para que x sea una unidad en $\mathbb{K}$, es necesario y suficiente que x sea un entero de K, de norma ± 1.

Demostración: Se tiene que si x es un elemento entero inversible, x^{-1} también lo es y $N(x), N(x^{-1}) \in \mathbb{Z}$, y como $1 = N(1) = N(xx^{-1})$, se tiene que $N(x) = \pm 1$.
Recíprocamente, si x es un entero de K con $N(x) = \pm 1$, se verifica que x tiene un polinomio característico de la forma $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x \pm 1 = 0,\ a_i \in \mathbb{Z}$, se puede deducir $\pm(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)x = 1$ y $\pm(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)$ es el inverso de x y es un entero de $\mathbb{K}$, por lo que x es una unidad.

Teorema de las unidades: Sean $\mathbb{K}$ un cuerpo de números de grado n, r_1 y r_2 los enteros dados por los isomorfismos de $\mathbb{K}$ y $r = r_1 + r_2 - 1$. El grupo

de las unidades de $\mathbb{K}$ A* es isomorfo a $\mathbb{Z}^r \times G$, siendo G un grupo cíclico formado por las raíces de la unidad contenidas en $\mathbb{K}$.

Como caso particular, caracterizaremos completamente las unidades sobre cuerpos cuadráticos trabajando separadamente sobre cuerpos reales e imaginarios.

Proposición: Si $\mathbb{K}$ es un cuerpo cuadrático imaginario, el grupo multiplicativo de las unidades de $\mathbb{K}$ está formado por:

1. El conjunto de las raíces cuartas de la unidad, {1,-1,i,-i}, si $\mathbb{K} = \mathbb{Q}[i]$
2. El conjunto de las raíces sextas de la unidad, $\left(\frac{1+\sqrt{-3}}{2}\right)^j$, $j = 0, 1, \ldots, 5$, si $\mathbb{K} = \mathbb{Q}[\sqrt{-3}]$
3. ± 1 en otro caso

Demostración: Por el teorema de las unidades, sabemos que las únicas unidades de $\mathbb{K}$ forman un grupo finito cíclico. Consideramos $\mathbb{K} = \mathbb{Q}[\sqrt{-m}]$ con $m > 0$ sin factores cuadrados.

Si $m \equiv 1$ o $2 \pmod 4$, entonces $-m \equiv 2$ o $3 \pmod 4$ y el anillo de enteros sería $\mathbb{Z} + \mathbb{Z}\sqrt{-m}$. Si $x = a + b\sqrt{-m}$, $N(x) = a^2 + mb^2 \geq 0$. Si x es unidad, entonces $N(x) = 1$. Para $m \geq 2$, esto solo es posible si $b = 0,\ a = \pm 1$. Si $m = 1$ ($\mathbb{K} = \mathbb{Q}[i]$), entonces se tienen además las unidades $a = 0,\ b = \pm 1$.

En el caso $m \equiv 3 \pmod 4$, el anillo de los enteros de $\mathbb{K}$ es $\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-m}}{2}$. Para $x = a + b\dfrac{1+\sqrt{-m}}{2}$, se tiene que $N(x) = \left(a + \dfrac{b}{2}\right)^2 + \dfrac{mb^2}{4}$ ($N(x) \in \mathbb{Z}$) y vale 1 cuando x es unidad. Si $m \geq 7$, entonces solo es posible si $b = 0,\ a = \pm 1$. Para $m = 3$, también existen las soluciones $x = \dfrac{\pm 1 \pm \sqrt{-m}}{2}$

Proposición: Si $\mathbb{K}$ es un cuerpo cuadrático real, las unidades positivas de $\mathbb{K}$ forman un grupo multiplicativo isomorfo a $\mathbb{Z}$. Entonces, este grupo admite

un único generador mayor que 1 denominado **unidad fundamental de** $\mathbb{K}$

Demostración:

Consideramos $\mathbb{K} = \mathbb{Q}[\sqrt{d}]$ con $d \geq 2$ sin factores cuadrados y $x = a + b\sqrt{d}$ una unidad de $\mathbb{K}$. Sabemos que N(x) es una unidad en $\mathbb{Z}$, entonces $N(x) = (a + b\sqrt{d})(a - b\sqrt{d}) = \pm 1$. De esta igualdad se puede deducir que $x, -x, x^{-1}, -x^{-1}$ son $\pm a \pm b\sqrt{d}$. Si $x \neq \pm 1$, solo uno de ellos es mayor que 1, y las unidades mayores que 1 de $\mathbb{K}$ son las unidades de la forma $a + b\sqrt{d}$ con $a, b > 0$. La existencia de un único generador es evidente por la isomorfía a $\mathbb{Z}$.

2.5. Descomposición de ideales primos en una extensión

En general, los ideales primos sobre el anillo de enteros de un cuerpo de números no son primos sobre el anillo de enteros de una extensión suya. Si tenemos en cuenta que los anillos de enteros de cuerpos de números son anillos de Dedekind, podemos obtener descomposiciones en producto de ideales primos. Antes de estudiar estas descomposiciones, nos fijaremos en ciertos subanillos del cuerpo que ayudarán a reducir los casos posibles a anillos principales, viendo que se conserva la propiedad de anillo de Dedekind.

2.5.1. Anillos de fracciones

Sean A dominio de integridad, K su cuerpo de fracciones y S un conjunto multiplicativo, es decir, un subconjunto de A cerrado para la multiplicación y que contiene a 1 y no a 0. Se define el **anillo de fracciones de A respecto a S**, $S^{-1}A$ al conjunto cociente de A×S respecto a la relación de equivalencia dada por $(a, s)R(a', s')$ si $as' = a's$

Representando $\frac{a}{s}$ la clase de equivalencia de (a, s) podemos identificar $S^{-1}A$ con

$$\left\{\frac{a}{s} \in K \mid a \in A, s \in S\right\}$$

y es un subanillo de K que contiene a A

Proposición: Sean A dominio de integridad, S subconjunto multiplicativo de A, y $A' = S^{-1}A$.

1. Todo ideal $\mathfrak{b}'$ de A' verifica $(\mathfrak{b}' \cap A)A' = \mathfrak{b}'$, y la aplicación $\varphi(\mathfrak{b}') = \mathfrak{b}' \cap A$ es una aplicación inyectiva del conjunto los ideales de A' en el de los de A.

2. $\varphi(\mathfrak{p}') = \mathfrak{p}' \cap A$ es una biyección del conjunto ordenado (inclusión) de los ideales primos de A' sobre el de los ideales primos $\mathfrak{p}$ de A tales que $\mathfrak{p} \cap S = \emptyset$. Su aplicación inversa viene dada por $\theta(\mathfrak{p}) = \mathfrak{p}A'$

Demostración: Empezamos por 1).
Si $\mathfrak{b}'$ es un ideal de A', $\mathfrak{b}' \cap A \subseteq \mathfrak{b}'$ y $(\mathfrak{b}' \cap A)A' \subseteq \mathfrak{b}'$ por ser $\mathfrak{b}'$ ideal de A'.

Veamos la inclusión opuesta. Sea $x \in \mathfrak{b}',\ x = \frac{a}{s}$. Entonces $sx \in \mathfrak{b}',\ a \in \mathfrak{b}'$ y $a \in \mathfrak{b}' \cap A$. Por tanto, $x = \frac{1}{s} \cdot a \in A'(\mathfrak{b}' \cap A)$. Deducimos $\mathfrak{b}' \subseteq A'(\mathfrak{b}' \cap A)$. La inyectividad de φ se deduce de la existencia de la aplicación $\theta(\mathfrak{b}) = A'\mathfrak{b}$, que cumple $\theta \circ \varphi = id_{A'}$.

Veamos ahora 2).
Si $\mathfrak{p}'$ es ideal primo de A', entonces $\mathfrak{p} = A \cap \mathfrak{p}'$ es un ideal primo de A (es evidente que $A/\mathfrak{p}' \cap A$ es anillo íntegro por serlo $A'/\mathfrak{p}'$). Además, $\mathfrak{p} \cap S = \emptyset$. Supongamos que $s \in \mathfrak{p} \cap S$, entonces $s \in \mathfrak{p}'$ y $1 = \frac{1}{s} \cdot s \in A'\mathfrak{p}' = \mathfrak{p}'$ y $\mathfrak{p}' = A'$, lo cual no es posible por ser $\mathfrak{p}'$ ideal primo.

Recíprocamente, si $\mathfrak{p}$ es ideal primo de A con $\mathfrak{p} \cap S = \emptyset$, veamos $\mathfrak{p}' = \mathfrak{p}A'$ es ideal primo de A' y $\mathfrak{p}' \cap A = \mathfrak{p}$.

Veamos que $\mathfrak{p}A' = \left\{ \frac{p}{s} \mid p \in \mathfrak{p}, s \in S \right\}$.
Sea $x \in \mathfrak{p}A'$. $x = \sum p_i \frac{a_i}{s_i},\ p_i \in \mathfrak{p},\ a_i \in A,\ s \in S$, suma finita. Se reduce a $x = \sum \frac{b_i}{s} p_i,\ b_i \in \mathfrak{p}$, s el denominador común de los s_i. Como $\mathfrak{p}$ es ideal de A, $x = \frac{p}{s},\ p = \sum b_i p_i \in \mathfrak{p}$. Como $S \cap \mathfrak{p} = \emptyset$, entonces $1 \notin \mathfrak{p}$ y $1 \neq \frac{p}{s}$.

Sigue ver que $\mathfrak{p}'$ es primo: sean $\frac{a}{s},\ \frac{b}{t} \in A'$ tales que $\frac{ab}{st} \in \mathfrak{p}A'$. Se tiene que $\frac{ab}{st} = \frac{p}{u},\ p \in \mathfrak{p}, u \in S$ y se deduce $abu = pst \in \mathfrak{p}$. Como $\mathfrak{p} \cap S = \emptyset$, $u \notin \mathfrak{p}$ y por ser $\mathfrak{p}$ ideal primo, o bien a o bien b son elementos de $\mathfrak{p}$, de donde $\frac{a}{s}$ o bien $\frac{b}{t}$ son elementos de $\mathfrak{p}A' = \mathfrak{p}'$

Por último, falta ver que $\mathfrak{p} = (\mathfrak{p}A') \cap A$. El contenido a la derecha es trivial.
Para el otro contenido, sea $x \in (\mathfrak{p}A') \cap A,\ x = \frac{p}{s}$. Entonces $sx \in \mathfrak{p}$ y $x \in \mathfrak{p}$ por no ser s elemento de $\mathfrak{p}$.

Quedaría demostrar que las aplicaciones φ y θ son biyecciones (sobre los conjuntos de primos definidos) inversas la una de la otra, lo que se ve de inmediato al realizar las composiciones de las dos formas. **CQD**

Corolario: Dado un anillo noetheriano íntegro, todo anillo de fracciones suyo es noetheriano.

Proposición: Dados R dominio de integridad, A subanillo de R, S subconjunto multiplicativo de A, B la clausura entera de A en R. Entonces la clausura entera de $S^{-1}A$ en $S^{-1}R$ es $S^{-1}B$.

Demostración: Tomamos un elemento de $S^{-1}B$ de la forma $\frac{b}{s}, b \in B, s \in S$. Tomamos la ecuación de dependencia entera de b sobre A y

la modificamos dividiendo por s^n para obtener

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$
$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_0}{s^n} = 0$$

y $\dfrac{b}{s}$ es entero sobre $S^{-1}A$. De forma similar, si $\frac{x}{s}$ es un elemento de $S^{-1}R$ entero sobre $S^{-1}A$, su ecuación de dependencia entera es

$$\left(\frac{x}{s}\right)^n + \frac{c_{n-1}}{t_{n-1}}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{c_0}{t_0} = 0$$

para alguna colección finita de $c_i \in A,\ t_i \in S$. Si se multiplica la expresión anterior por $(t_0 \cdot t_1 \ldots t_{n-1})^n$, se obtiene una ecuación de dependencia entera de $\dfrac{x \cdot t_0 \ldots t_{n-1}}{s}$ con coeficientes en A, por lo que este es entero sobre A y pertenece a B. Para finalizar, $\dfrac{x}{s} = \dfrac{1}{t_0 \cdot t_1 \ldots t_{n-1}} \dfrac{x \cdot t_0 \cdot t_1 \ldots t_{n-1}}{s}$ es un elemento de $S^{-1}B$ y se concluye que $S^{-1}B$ es la clausura entera de $S^{-1}A$ en $S^{-1}R$. **CQD**

Corolario: Dado un anillo íntegramente cerrado, todo anillo de fracciones suyo es íntegramente cerrado.

Corolario: Dado un anillo de Dedekind, todo anillo de fracciones suyo es un anillo de Dedekind.

Proposición: Sean A anillo de Dedekind, $\mathfrak{p}$ ideal primo no nulo suyo y $S = A - \mathfrak{p}$. Entonces $S^{-1}A$ es un anillo principal y existe un elemento primo p de $S^{-1}A$ tal que todos los ideales no nulos de $S^{-1}A$ son los engendrados por las potencias de p, $(p^n)_{n\geq 0}$.

Demostración: El único ideal primo no nulo de A disjunto con S es $\mathfrak{p}$. Entonces el único ideal primo de $S^{-1}A$ es $\mathfrak{p}S^{-1}A = \mathfrak{B}$. Como $S^{-1}A$ es de Dedekind, todo ideal suyo es producto de ideales primos de la forma $\mathfrak{B}^n,\ n \geq 0$. Sea $p \in \mathfrak{B} - \mathfrak{B}^2$. El ideal (p) está contenido en $\mathfrak{B}$ y no está contenido en $\mathfrak{B}^2$. Por descomposición en producto de primos, $(p) = \mathfrak{B}$ y $p^n = \mathfrak{B}^n, n \geq 0$. En conclusión, $S^{-1}A$ es dominio de ideales principales y sus

ideales son de la forma buscada. Además p es primo por ser generador de un ideal primo. **CQD**

Proposición: Dados A y S en las condiciones de anillo de fracciones y un ideal $\mathfrak{m}$ maximal de A con $S \cap \mathfrak{m} = \emptyset$, entonces $S^{-1}A/\mathfrak{m}S^{-1}A \simeq A/\mathfrak{m}$

2.5.2. Descomposición de ideales primos

De aquí en adelante, se consideran A un anillo de Dedekind, K su cuerpo de fracciones, L una extensión de grado n de K y B la clausura entera de A en L, también de Dedekind.
Dado $\mathfrak{p}$ un ideal primo de A, se considera el ideal $B\mathfrak{p}$ de B, que posee una descomposición en ideales primos

$$B\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{B}_i^{e_i}$$

siendo $\mathfrak{B}_i$ ideales primos de B y e_i enteros positivos. Estos $\mathfrak{B}_i$ quedan determinados por el ideal $\mathfrak{p}$.

Proposición: Los $\mathfrak{B}_i$ son los ideales primos $\mathfrak{D}$ tales que $\mathfrak{D} \cap A = \mathfrak{p}$

Demostración: Veamos que para un ideal primo $\mathfrak{D}$, $\mathfrak{D} \cap A = \mathfrak{p}$ si y solo si $\mathfrak{D} \supseteq \mathfrak{p}B$

$\Rightarrow$ Se tiene que $\mathfrak{p} \subseteq \mathfrak{D},\ \mathfrak{p}B \subseteq \mathfrak{D}B = \mathfrak{D}$

$\Leftarrow$ Por ser $\mathfrak{D}$ ideal primo de B, $\mathfrak{D} \cap A$ es ideal primo de A y además contiene a $\mathfrak{p}$, pues $\mathfrak{p}B \supseteq \mathfrak{p}$. Por ser $\mathfrak{p}$ maximal, llegamos al resultado deseado.

Por la descomposición de ideales en anillos de Dedekind, basta fijarse en que el exponente de un ideal primo de la descomposición de $\mathfrak{p}B$ es mayor que 0 solo si $\mathfrak{p}B$ está contenido en dicho ideal primo. **CQD**

$A/\mathfrak{p}$ se puede identificar con un subanillo de $B/\mathfrak{B}_i$. Como sabemos que

B es un A-módulo de tipo finito y ambos $A/\mathfrak{p}$ y $B/\mathfrak{B}_i$ son cuerpos, se puede considerar $B/\mathfrak{B}_i$ como un espacio vectorial de dimensión finita sobre $A/\mathfrak{p}$, denotando por f_i a esta dimensión.
Cabe destacar que $B\mathfrak{p} \cap A = \mathfrak{p}$ y $B/B\mathfrak{p}$ es también un espacio vectorial de dimensión finita sobre $A/\mathfrak{p}$.

Definición: Se llama **grado residual de $\mathfrak{B}_i$ sobre A** a f_i e **índice de ramificación de $\mathfrak{B}_i$ sobre A** a e_i.
Decimos que un ideal primo **se ramifica** en B si alguno de los índices de ramificación cumple $e_i \geq 2$.

Lema: Sea A anillo íntegramente cerrado, K su cuerpo de fracciones (de característica 0), L una extensión de grado n de K y A' la clausura entera de A en L. Entonces A' es un A-submódulo de un A-módulo libre de rango n. Además, si A es anillo principal, entonces A' es A-módulo libre de rango n.

Teorema: $\sum_{i=1}^{q} e_i f_i = [B/B\mathfrak{p} : A/\mathfrak{p}] = n$

Demostración: Para la primera igualdad, consideramos la cadena de ideales

$$B \supset \mathfrak{B}_1 \supset \mathfrak{B}_1^{\,2} \supset \cdots \supset \mathfrak{B}_1^{\,e_1} \ldots \mathfrak{B}_q^{\,e_q} \supset B\mathfrak{p}$$

No hay ideales comprendidos entre dos términos consecutivos $\mathfrak{B}$ y $\mathfrak{B}\mathfrak{B}_i$, ergo $\mathfrak{B}/\mathfrak{B}\mathfrak{B}_i$ es un espacio vectorial de dimensión 1 sobre $B/\mathfrak{B}$. Es además un espacio vectorial de dimensión f_i sobre $A/\mathfrak{p}$. Como para cada i hay e_i cocientes de términos de la forma $\mathfrak{B}/\mathfrak{B}\mathfrak{B}_i$, se deduce que la dimensión $[B/B\mathfrak{p} : A/\mathfrak{p}]$ es igual a la suma de dichos cocientes, esto es, $\sum_{i=1}^{q} e_i f_i$.

Para la segunda igualdad, vamos a tratar de reducirnos a un anillo A' principal y B' A'-módulo libre de rango n. Para ello, consideramos $S = A - \mathfrak{p}$ subconjunto multiplicativo de A, y los anillos de fracciones $A' = S^{-1}A$, $B' = S^{-1}B$. A' es un anillo principal cuyo único ideal maximal es $\mathfrak{p}A'$ y B' es la clausura entera de A' en L. Tenemos entonces que $[B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = n$. En efecto, existe una base de B' sobre A' de n elementos y basta considerar como base de $B'/\mathfrak{p}B'$ sobre $A'/\mathfrak{p}A'$ a la reducción de la anterior módulo $\mathfrak{p}B'$

Vamos a estudiar la factorización del ideal $\mathfrak{p}B'$. De $\mathfrak{p}B = \prod_{i=1}^{q} \mathfrak{B}_i^{e_i}$, de-

ducimos que $\mathfrak{p}B' = \prod_{i=1}^{q}(B'\mathfrak{B}_i)^{e_i}$.
Los $B'\mathfrak{B}_i$ son ideales primos no nulos de B', pues $\mathfrak{B}_i \cap S = \emptyset$ por ser $\mathfrak{B}_i \cap A = \mathfrak{p}$.

De la primera parte del resultado, obtuvimos que

$$\sum_{i=1}^{q} e_i[B'/B'\mathfrak{B}_i : A'/A'\mathfrak{p}] = [B'/B'\mathfrak{p} : A'/A'\mathfrak{p}]$$

No obstante, $A'/A'\mathfrak{p} \simeq A/\mathfrak{p}$ y $B'/B'\mathfrak{B}_i \simeq B/\mathfrak{B}_i$, y se sigue que

$$[B'/B'\mathfrak{B}_i : A'/A'\mathfrak{p}] = f_i$$

En conclusión, $n = [B'/B'\mathfrak{p} : A'/A'\mathfrak{p}] = \sum_{i=1}^{q} e_i f_i$. **CQD**

Proposición: $B/B\mathfrak{p}$ es isomorfo a $\prod_{i=1}^{q} B/\mathfrak{B}_i^{e_i}$

Definición: Dados K y L cuerpos de números con $K \subseteq L$ y A y B sus respectivos anillos de enteros, se llama **ideal discriminante** de B sobre A (o de K sobre L), $\mathfrak{D}_{B/A}$ ($\mathfrak{D}_{L/K}$) al ideal de A engendrado por el discriminante de una base de L sobre K contenida en B.

Teorema: Un ideal primo $\mathfrak{p}$ de A se ramifica en B si y solo si contiene al ideal $\mathfrak{D}_{B/A}$. Además, hay un número finito de ideales primos de A que se ramifican en B.

La finitud de ideales primos que se ramifican es consecuencia directa de la primera parte del teorema y de la descomposición del ideal discriminante en producto finito de ideales primos.

Como consecuencia, al trabajar en un cuerpo de números K, se pueden descomponer en él aquellos números primos p de $\mathbb{Z}$ tales que el ideal (p) contenga al ideal discriminante $\mathfrak{D}_{K/\mathbb{Q}}$, es decir, aquellos que dividan al discriminante (como elemento de $\mathbb{Z}$).

Capítulo 3

Aplicaciones a criptografía

En la actualidad, como consecuencia de la creciente relevancia de la seguridad informática y la criptografía, se ha desarrollado un gran interés en el estudio de métodos de cifrado de mensajes cuya clave de descifrado sea difícil de obtener. Estas claves se relacionan con las llamadas funciones de una vía, funciones inversibles, siendo la función inversa tal que la cantidad de tiempo necesario para calcularla se considere suficientemente grande para ser segura. Sin embargo, sigue siendo necesario obtener la función inversa para descifrar, y será útil depender de información adicional para calcularla. Cuando existe tal información, se denominará función de una vía con trampa. La principal función de una vía con trampa que veremos es la exponenciación modular, cuya función inversa es una raíz discreta.

Empezamos definiendo un **criptosistema** como una familia de transformaciones que se aplican a un posible mensaje que se quiere transmitir, el llamado texto en claro. La transformación particular que se elija iría asociada a una única clave de cifrado y de descifrado, que se pueden considerar una la "función inversa" de la otra. Los criptosistemas de clave pública tienen la característica de que solo uno de los usuarios posee la clave de descifrado o clave privada, que incluye la trampa, siendo solo este el que pueda descifrar el texto en claro, mientras que la clave de cifrado (o clave pública) se hace pública, incluyéndose posibles adversarios ajenos a la transmisión del mensa-

je. La seguridad se basa en parte de la dificultad de que el adversario pueda llegar a obtener la clave privada.

Los criptosistemas más comunes hacen un gran uso de los resultados de teoría de números, especialmente sobre congruencias modulares y números primos.

En este capítulo veremos algunos criptosistemas de clave pública, los resultados de primalidad y factorización que hacen que sean correctos y los problemas en los que se basa la seguridad de los sistemas.

3.1. Criptografía de clave pública

El objetivo fundamental de la criptografía es la transmisión de mensajes entre dos individuos, que se denotarán A y B en adelante, tal que un posible adversario a la escucha de la transmisión no sea capaz de deducir los contenidos del mensaje a partir de la información interceptada. Para este fin se utilizan los criptosistemas, familias de claves que permiten cifrar y descifrar la información a transmitir.
En función de si la clave de cifrado (la forma de cifrar el mensaje) se mantiene oculta o no, se consideran dos tipos distintos de criptosistemas: de clave privada o simétrica y de clave pública o asimétrica, respectivamente.

Como los criptosistemas de clave pública son significativamente más lentos que los de clave privada, se suele restringir su uso a situaciones específicas, por ejemplo llegar a una decisión secreta entre A y B para elegir una clave de un criptosistema de clave pública.

Sabemos que cualquier posible adversario conoce la clave de cifrado, y la clave de descifrado se puede considerar como una función inversa de esta; aparece el concepto de función de una vía, una función cuya inversa sea difícil de computar. Se considerará que es difícil si no se tiene un algoritmo que lo logre en un tiempo polinomial en el tamaño de la clave.

Utilizaremos funciones de una vía que posean una trampa, es decir, cuya inversa se pueda computar fácilmente al conocer alguna información previa, sin la cual se comportaría como una función de una vía. Nos centraremos en ejemplos de algunos esquemas cuya seguridad está basada en distintos problemas computacionalmente difíciles de resolver, en particular los problemas de factorización, logaritmo discreto y el problema de la mochila. La trampa en este caso sería, trivialmente, el haber construido el problema a partir de una información conocida.

3.1.1. RSA

La función de una vía con trampa utilizada en el RSA está justificada por la dificultad computacional del problema de la factorización. El método utilizado es como sigue: primero se eligen dos números primos grandes, p y q, y se toma $N = pq$. Como conocemos la factorización de N, es sencillo calcular $\varphi(N) = (p-1)(q-1) = pq - p - q + 1$. Después, se elige al azar (o de forma pseudoaleatoria) un número e tal que $1 \leq e \leq \varphi(N)$ y e coprimo con $\varphi(N)$. Por último, se calcula $d = e^{-1} \pmod{\varphi(N)}$. Los números N y e forman la clave pública, mientras que p, q y d constituyen la clave privada. e y d se llaman exponente de cifrado y exponente de descifrado, respectivamente. La razón por la que p y q se mantienen privados es que mientras no se conozca la factorización de N es costoso calcular $\varphi(N)$, y por tanto obtener d.

Supongamos que un usuario, A, quiere mandar un mensaje al poseedor de la clave privada, B, y que el texto en claro, P, es un elemento de $\mathbb{Z}/N\mathbb{Z}$. Suponemos también que N es suficientemente grande para que no se pierda información al hacer la congruencia, $N > P$. El proceso de transmisión del mensaje es como sigue:

1. A realiza la operación $C = P^e \pmod{N}$ se obtiene el texto cifrado, C, y este es enviado a B
2. B descifra el texto en claro haciendo uso del exponente de descifrado, $P' = C^d \pmod{N} = P^{ed} \pmod{N}$

El resultado que nos garantiza que $P' = P$ es una generalización del Pequeño Teorema de Fermat

Proposición: Dados $a, m \in \mathbb{N}$ tales que $mcd(a, m) = 1$, entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$

Demostración: Supongamos que m es potencia de algún primo p, $m = p^\alpha$. Utilizaremos inducción sobre α.
Si $\alpha = 1$, el resultado se cumple por el Pequeño Teorema de Fermat. Supongamos que se cumple para $\alpha - 1$ y $\alpha \geq 2$. $\varphi(p^{\alpha-1}) = p^{\alpha-1} - p^{\alpha-2}$, y por hipótesis de inducción, $a^{p^{\alpha-1}-p^{\alpha-2}} = 1 + bp^{\alpha-1}$ para algún b. Si elevamos ambos lados de la expresión a la potencia p, obtenemos $\varphi(a^{p^\alpha}) = a^{p^\alpha - p^{\alpha-1}} = (1 + bp^{\alpha-1})^p$. Todos los términos de la expresión obtenida del binomio de Newton $(1 + bp^{\alpha-1})^p$, excepto el 1, son divisibles por p^α, pues el último es $p^{p(\alpha-1)} \geq p^\alpha$ y los coeficientes del binomio del resto son divisibles por p e incluyen al menos la primera potencia de p^α. Por tanto, $a^{p^\alpha - p^{\alpha-1}} - 1 \equiv 0 \pmod{()p^\alpha}$, y concluimos este caso.

El el caso en el que m se descompone como producto de primos distintos, hacemos uso de la multiplicatividad de φ. Sea p^α una de estas potencias.
Consideramos $m = p^\alpha q$ y
$a^{\varphi(m)} = a^{(p^\alpha - p^{\alpha-1})\varphi(q)} = (a^{p^\alpha - p^{\alpha-1}})^{\varphi(q)} \equiv (1)^{\varphi(q)} \pmod{p^\alpha} \equiv 1 \pmod{p^\alpha}$

Si utilizamos la propiedad "Dados x, y, n, n' tales que $x \equiv y \pmod{n}$, $x \equiv y \pmod{n'}$ y $mcd(n, n') = 1$, entonces $x \equiv y \pmod{nn'}$" aplicada a $a = b = 1$, n y n' potencias distintas de primos de la factorización de m, se obtiene que $a^{\varphi(m)} \equiv 1 \pmod{m}$. **CQD**

Utilizando este resultado, concluimos que

$$P' = P^{ed} = P^{1+b\varphi(N)} = P(P^{\varphi(N)})^b \equiv P \pmod{N}$$

y el descifrado se realiza correctamente por tomarse P' como resto módulo N y ser $P < N$.

Es importante disponer de métodos para generar de forma aleatoria los primos p y q de manera que estos no se puedan replicar fácilmente, lo cual

desincentiva recurrir a tipos de primos especiales, como por ejemplo los de Mersenne. Sería válido como método para generar un primo aleatorio generar un entero aleatorio m y luego tomar el menor primo p tal que $m \geq p$. Un procedimiento similar podría utilizarse para obtener el exponente de cifrado e, comprobando la coprimalidad con $\varphi(N)$ en lugar de la primalidad.

Como apunte, a la hora de escoger p y q es importante hacerlo de manera que N no sea factorizado rápidamente por los algoritmos de factorización más comunes, entre ellos:

- El algoritmo por fuerza bruta: se comprueba la divisibilidad de N por todos los primos en orden creciente menores que $\sqrt{N}$.
- El método de Fermat: desde $a = \lceil \sqrt{N} \rceil$ hasta N se comprueba si la diferencia $a^2 - N^2$ es un cuadrado perfecto b^2, en cuyo caso $N = (a + b)(a - b))$

Teniendo en cuenta estos algoritmos, se obtienen como condiciones adicionales que p y q no sean demasiado pequeños (fuerza bruta) y que no estén demasiado cerca entre ellos y por ende a la raíz cuadrada de N (Feramt). Otra condición importante es que el mcd de $p - 1$ y $q - 1$ sea relativamente pequeño y que cada uno tenga un factor primo grande.

Es buena idea además que el exponente de cifrado no sea demasiado pequeño para evitar que al cifrar el texto el claro P, P^e sea menor que N y se pueda realizar el descifrado a partir de una raíz real.

3.1.2. El problema del logaritmo discreto

El logaritmo discreto en un grupo finito es una operación en $\mathbb{Z}/n\mathbb{Z}$ análoga al caso real; dado y que sabemos que es de la forma $b^x \pmod{n}$, entonces x es el logaritmo discreto de y en base b, $x = log_b y$. La exponenciación modular se puede realizar rápidamente mediante el método de cuadrados sucesivos, pero

no se ha descubierto un método sencillo para la operación inversa. Algunos algoritmos para la resolución de logaritmos discretos son

- Cálculo por fuerza bruta.
- Algoritmo paso enano-paso gigante, que es más rápido que el anterior a costa de requerir una gran capacidad de almacenamiento.
- Criba de cuerpos de números, se utiliza sobre cuerpos finitos $\mathbb{Z}/p\mathbb{Z}$ y es asintóticamente (para p) el mejor método conocido.

En este contexto planteamos el **protocolo de intercambio de claves de Diffie-Hellmann**, un método para que dos individuos A y B compartan una clave obtenida al azar y conocida únicamente por ellos mismos. El procedimiento es el siguiente:

1. Se eligen un primo p (grande) y g una raíz primitiva módulo p, es decir, g genera el grupo multiplicativo $\mathbb{Z}_p^*$.
2. A elige $a \in \{1, \ldots, p-1\}$ y envía a B $g^a \pmod p$
3. B elige $b \in \{1, \ldots, p-1\}$ y envía a A $g^b \pmod p$
4. A y B realizan $(g^b)^a \pmod p$ y $(g^a)^b \pmod p$ respectivamente. Ambos conocen g^{ab}, que es la clave que compartirán.

Al trabajar con el protocolo Diffie-Hellmann, aplicamos implícitamente la **hipótesis Diffie-Hellmann**: conocidos g una raíz primitiva módulo p, $g^a \pmod p$ y $g^b \pmod p$, no es computacionalmente factible obtener $g^{ab} \pmod p$. Esta hipótesis es al menos tan fuerte como la dificultad del problema del logaritmo discreto, pues si este fuera fácil de resolver también sería sencillo obtener ab a partir de a y b.

Definición: Definimos el sistema de clave pública ElGamal, basado en el intercambio de claves Diffie-Hellmann, a partir de sus componentes y el proceso de transmisión del mensaje:

- Se eligen un primo p y g una raíz primitiva módulo p.
- **Clave pública:** $(p, g, g^b \pmod p)$, para algún b tal que $0 \leq b \leq p-2$
- **Clave privada:** (b)
- **Cifrado:** Sea M el mensaje que se quiere transmitir. Fijando $0 \leq a \leq p-2$, el cifrado es la dupla $(C_1, C_2) = (g^a \pmod p, M(g^b)^a \pmod p)$
- **Descifrado:** $M = C_2(C_1^b)^{-1} \pmod p = Mg^{ab}((g^a)^b)^{-1} \pmod p = = M \pmod p$

Tomando inspiración del procedimiento utilizado en Diffie-Hellman, es posible diseñar sistemas criptográficos en los que no se requiere un intercambio de claves previo. La idea es que A enviaría un mensaje cifrado por una clave que sólo A conoce y sería cifrado de nuevo por B mediante un sistema de cifrado independiente del anterior y sólo conocido por B. Para finalizar, A devuelve a B el mensaje previo después de aplicar el descifrado de la clave de A, tras lo que B puede descifrar el mensaje inicial utilizando su clave. Este método es conocido como **protocolo de tres envíos**. Un ejemplo de criptosistemas de este tipo es el siguiente:

Definición: Se define el **criptosistema de Massey-Omura** al siguiente proceso:

1. Se elige un cuerpo finito $\mathbb{F}_q$, de conocimiento público.
2. A y B eligen respectiva e independientemente e_A, e_B, $0 \leq e_A, e_B \leq q-1$, $mcd(e_A, q-1) = mcd(e_B, q-1) = 1$
3. A y B obtienen respectivamente $d_A = e_A^{-1} \pmod{q-1}$, $d_B = e_B^{-1} \pmod{q-1}$
4. M es el mensaje que se quiere enviar. A envía a B $M^{e_A} \pmod p$
5. B devuelve a A $M^{e_A e_B} \pmod p$
6. A vuelve a mandar a B $(M^{e_A e_B})^{d_A} \pmod p = M^{e_B} \pmod p$

7. Por último, B descifra el mensaje, $M \pmod p = M^{e_B d_B} \pmod p$

El protocolo de Diffie-Hellmann así como los criptosistemas que utilizan el sistema de tres envíos son particularmente vulnerables a un tipo de ataques conocido como ataque del hombre en el medio, en el que un adversario suplanta simultáneamente a A y a B en sus envíos de mensajes con B y A respectivamente. Por este motivo es de gran importancia acompañarlos de firmas digitales para confirmar la legitimidad de los usuarios.

3.1.3. El problema de la mochila

El planteamiento del problema en su forma más básica es considerar la forma de rellenar completamente una mochila de volumen V con un total de k objetos cada uno de volumen v_i.

Definición: La definición formal del problema de la mochila es la siguiente:
Dados un conjunto de k enteros $\{v_i\}$ y un entero V, encontrar una k-tupla de ceros y unos, esto es, un entero de k bits $n = (\epsilon_{k-1}\epsilon_{k-2}\dots\epsilon_0)$ donde los ϵ_i determinan la expresión binaria de n, verificando

$$\sum_{i=0}^{k-1} \epsilon_i v_i = V$$

si tal k-tupla existe.

Este problema puede tener una, varias o ninguna solución en función de los enteros $\{v_i\}$ y V elegidos. Nos enfocaremos en un caso particular, la mochila supercreciente, en la que la sucesión de los $\{v_i\}$ es una sucesión supercreciente, es decir, $v_i \geq \sum_{j=0}^{i-1} v_j$, $\forall 1 \leq i \leq k$.

A diferencia del problema general, el supercreciente se puede resolver fácilmente, sin más que comprobar en orden decreciente de índices i si v_i es menor que el volumen restante en la mochila. Si esto se cumple se toma $\epsilon_i = 1$

y en caso contrario $\epsilon_i = 0$, y se considera que el volumen disponible se reduce correspondientemente.
Esta diferencia de dificultad nos da una idea para un criptosistema de clave pública: el criptosistema knapsack (mochila en inglés) o sistema Merkle-Hellman.

Definición: Suponemos que se quiere transmitir un mensaje M en su expresión binaria de k bits. El **criptosistema knapsack** se construye de la siguiente manera:

1. Se eligen una k-tupla supercreciente $\{v_{k-1} \dots v_0\}$, $m \geq \sum_{i=0}^{k-1} v_i$ y a un entero coprimo con m y menor que m.
2. Se calculan $b = a^{-1} \pmod m$ y la k-tupla $\{w_i\}$ dada por $w_i = av_i \pmod m$
3. La clave pública es la k-tupla $\{w_{k-1} \dots w_0\}$
4. La clave privada es la tupla $(b, m, \{v_i\}_{i=0}^{k-1})$
5. El cifrado C de un mensaje en claro $M = (\epsilon_{k-1} \dots \epsilon_0)$ se realiza calculando $C = \sum_{i=0}^{k-1} \epsilon_i w_i \pmod m$
6. El descifrado de C se obtiene calculando $V = bC \pmod m = \sum_{i=0}^{k-1} \epsilon_i v_i \pmod m = \sum_{i=0}^{k-1} \epsilon_i v_i$ y resolviendo el problema de la mochila supercreciente para volumen de la mochila V y volumen de los objetos v_i. La resolución del problema devuelve evidentemente $(\epsilon_{k-1} \dots \epsilon_0) = M$.

Un adversario que esté a la escucha solo llega a conocer los $\{w_i\}$ y tendría que plantearse el problema de la mochila $C = \sum_{i=0}^{k-1} \epsilon_i w_i$, que no es supercreciente por realizarse un producto modular; a primera vista este sistema es seguro. No obstante, el problema resultante es obtenido por una transformación simple de un problema supercreciente, por lo cual se pudo desarrollar un algoritmo para resolverlo en tiempo polinomial (en k)
A pesar de que aún no se haya obtenido algoritmos en tiempo polinomial para algunos ajustes del sistema anterior, se sigue cuestionando la viabilidad de los criptosistemas de clave pública basados en el problema de la mochila, desde el punto de vista de la seguridad.

3.2. Tests de primalidad en criptografía

En la sección anterior hemos indicado un método sencillo para obtener primos de forma (pseudo)aleatoria, que es tomar un número al azar y tomar el primer número mayor que él que se compruebe que sea primo; claramente, si queremos que el sistema correspondiente sea viable, necesitamos que esta comprobación sea rápida.

Históricamente, los métodos que garantizaban la primalidad no eran computacionalmente eficientes, había necesidad de un punto intermedio entre certeza y tiempo: los tests probabilísticos, que dan condiciones suficientes para que un número sea compuesto. Los números compuestos que estos tests no cataloguen como tales se denominan pseudoprimos.

No fue hasta el año 2002 cuando se consiguió diseñar un algoritmo en tiempo polinomial para determinar la primalidad: el algoritmo AKS.

3.2.1. Pseudoprimos

Definición: Si n es un número compuesto y a es un número coprimo con n, se dice que n es **pseudoprimo de base** a si $a^{n-1} \equiv 1 \pmod{n}$, es decir, pasa el test de primalidad dado por el Pequeño Teorema de Fermat.

Ya definimos un número de Carmichael como aquel que es pseudoprimo de cualquier base coprima con él. Enunciaremos algunas propiedades de estos números.

Proposición: Sea n un entero impar. Entonces:

- Si n posee factores cuadrados entonces no es un número de Carmichael
- Si n no posee factores cuadrados, es de Carmichael si y solo si $p-1|n-1$ $\forall$ p divisor primo de n

- Si n es número de Carmichael entonces es producto de al menos 3 números primos.

3.2.2. Pseudoprimos de Euler

Definición: Dados n y a enteros con $n = p_1 \dots p_m$ la descomposición en factores primos de n. Se define el símbolo de Jacobi $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_m}\right)$ el producto de los símbolos de Legendre de a y los primos de la descomposición de n.

Por las propiedades del símbolo de Legendre, sabemos que si n es primo impar, entonces $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$.

Definición: Se denomina pseudoprimo de Euler de base b a cualquier entero impar compuesto tal que $mcd(n, b) = 1$ y verifique la congruencia anterior.

Se puede ver elevando al cuadrado ambos lados de la congruencia que un pseudoprimo de Euler de base b es también pseudoprimo de base b.

Se podría esperar que hubiera un análogo a los números de Carmichael para los pseudoprimos de Euler. Sin embargo, los siguientes resultados indican que este no es el caso:

Fijado un entero impar n, denotamos la congruencia $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$ por (*) (consideramos $mcd(a, n) = 1$.

1. Si a verifica (*) y a' no, entonces aa' tampoco verifica la congruencia. En consecuencia, si (*) es falso para algún a, entonces hay al menos tantos a para los que la congruencia es falsa como para los que se cumple.

2. Existe al menos un a para el que no se cumple (*).

Tenemos que para un entero impar n cualquiera, este es un pseudoprimo de Euler para menos de la mitad de las posibles bases.
Tiene sentido utilizar (*) como test de primalidad para k bases menores que n tomadas al azar. Este es el **test de primalidad de Solovay-Strassen**.

3.2.3. Pseudoprimos fuertes

El siguiente criterio está basado en que para un número primo p las únicas raíces de la unidad módulo p son ± 1.
Dada una base cualquiera a coprimo con n se tendría que $a^{n-1} \equiv 1 \pmod{n}$ y se procedería a tomar las posibles raíces de esa potencia, las potencias $(n-1)/2,\ (n-1)/4, \ldots, (n-1)/2^s$, siendo $n-1 = 2^s t$ con t impar. El test en sí se realiza partiendo de a^t y elevando sucesivamente al cuadrado, $a^{2t}, a^{2^2 t}, \ldots, a^{2^s t}$. El test termina cuando se obtiene en uno de los cuadrados -1, y el número n se declara compuesto si se llega a la potencia $a^{2^{s-1} t}$ y esta no es -1. Este es el llamado **test de Miller-Rabin**.

Definición: Sean n entero impar compuesto y a coprimo con n. Se denota $n-1 = 2^s t$ con t impar. Si se cumple alguna de las condiciones

- $a^t \equiv 1 \pmod{n}$
- $\exists r$ tal que $0 \leq r < s$ y $a^{2^r t} \equiv -1 \pmod{n}$

entonces n es llamado **pseudoprimo fuerte de base** a.

Proposición: Sea n pseudoprimo fuerte de base a. Entonces n es pseudoprimo de Euler de base b. Además, si $n \equiv 3 \pmod{4}$, el recíproco es cierto.

Los números enteros impares (n), de forma similar a los pseudoprimos de Euler, son pseudoprimos fuertes para, a lo sumo, un cuarto de las bases a tales que $0 < a < n$

3.2.4. Algoritmo AKS

Este algoritmo hace uso de un resultado similar al Pequeño Teorema de Fermat, en anillos de polinomios sobre cuerpos finitos:

Proposición: Sean a y p enteros coprimos. Entonces p es primo si y solo si $(x-a)^p \equiv (x^p - a) \pmod{p}$

Demostración: Si p es primo, para $0 < i < p$, el coeficiente de x^i es $\binom{p}{i}$, que es 0 módulo p. La potencia de a es 1 por el Pequeño Teorema de Fermat.

Ahora supongamos que p es compuesto. Sea q un primo divisor de p y k la mayor potencia de q tal que $q^k | p$. Tenemos que q^k no divide a $\binom{p}{q}$ y además q^k es coprimo con a^{p-q}. Deducimos que el coeficiente de x^q es distinto de 0 módulo p. En conclusión, $(x-a)^p \not\equiv (x^p - a) \pmod{p}$. **CQD**

Esta comprobación por sí sola es computacionalmente pesada. Entonces se considera como forma de facilitar los cálculos la reducción de la congruencia módulo $x^r - 1$ para algún r, además del módulo n: $(x-a)^n \equiv (x^n - a) \pmod{(n, x^r - 1)}$. Se le pida al r elegido que sea primo y que la factorización de $(r-1)$ incluya un factor primo mayor que $\sqrt{r}$.

El algoritmo aplicado a n es el siguiente:

1. Si $n = a^b$ para algún par de enteros a, b, n es COMPUESTO
2. Se busca el menor primo $2 \leq r < n$ verificando:

   $mcd(r, n) = 1$ (si no, es COMPUESTO);

   Sea q el mayor factor primo de $r-1$, comprobar que verifica $q \geq 4\sqrt{r} log(n)$ y $n^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}$
3. Para $1 \leq a \leq 2\sqrt{r+1} log(n)$, si $(x-a)^n \not\equiv (x^n - a) \pmod{n, x^{r+1} - 1}$, n es COMPUESTO
4. Si se llega al final del bucle, n es primo.

La comprobación de la primalidad de los r en el primer bucle está justificada por el siguiente lema que acota los números con las condiciones que exigimos:

Lema: Existen constantes positivas c_1 y c_2 tales que existe un r en el intervalo $[c_1 log(n)^6,\ c_2 log(n)^6]$ tal que $r-1$ tiene un factor primo $q \geq 4\sqrt{r}log(n)$ y q divide al orden de n módulo r.

Una cota logarítmica en función de n reduce drásticamente el tiempo de ejecución del bucle.

Conclusiones

El objetivo de este trabajo ha sido mostrar algunos importantes problemas clásicos de la Teoría de Números y cómo los esfuerzos por resolverlos han llevado, no sólo a utilizar herramientas algebraicas, sino a construir nuevas estructuras y a su correspondiente estudio.

También se ha querido hacer una ligera introducción a la Criptografía para mostrar cómo estos conceptos están en la base de muchos diseños criptográficos actuales, después de que, en un giro inesperado del desarrollo matemático, una de las disciplinas mas teórica y "pura" pasara a ser una de las ramas matemáticas con mayores aplicaciones en un campo tan actual y esencial como la seguridad de la información.

Bibliografía

[1] Manindra Agrawal, Neeraj Kayal y Nitin Saxena, *PRIMES in P* (Indian Institute of Technology Kanpur, 2002)

[2] N. Bourbaki, *Algèbre* (Hermann, 1965)

[3] N. Bourbaki, *Algèbre conmutative* (Hermann, 1948)

[4] T. ElGamal, *A public key criptosystem and a signature scheme based on discrete logarithms* (IEEE Transactions on Information Theory IT-31, 1985)

[5] Graham Everest y Thomas Ward, *An Introduction to Number Theory* (Springer, 2005)

[6] Larry C. Grove, *Algebra* (Dover Publications, Inc., 2004)

[7] M. E. Hellman, *The mathematics of public key cryptography* (Scientific American, 1979)

[8] Thomas W. Hungerford, *Algebra* (Springer, 2003)

[9] Neal Koblitz, *A Course in Number Theory and Cryptography* (Springer, 1991)

[10] E. Kranakis, *Primality and Cryptography* (John Wiley & Sons, 1986)

[11] P. Samuel, *Théorie algébrique des nombres* (Hermann, 1967)

[12] P. Samuel, O. Zariski, *Commutative Algebra* Vol. **I**
(Van Nostrand, 1958)