UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

ALGUNS TESTOS DE PRIMERITAT

Autor: Francesc Xavier Bada Erta

Director: Dr. Xavier Guitart
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 13 de juny de 2022

Abstract

A primality test is an algorithm which determines whether a number is prime or composite. In this project we will study mainly two of these tests and their complexities. The first one is a probabilistic test, which means that it claims whether a number is prime or composite within a certain error margin; the second one is a deterministic test, which claims unequivocally the primality of a number.

Resum

Un test de primeritat és un algorisme que determina si un nombre és primer o compost. En aquest treball estudiarem principalment dos d'aquests testos i les seves complexitats. El primer és un test probabilístic, és a dir, afirma que un nombre és primer o compost amb un cert marge d'error; el segon és determinista, és a dir, afirma inequívocament la primeritat d'un nombre.

2020 Mathematics Subject Classification. 11-00 , 11A07, 11A41, 11A51, 11R18

Agraïments

Vull agrair a tothom qui m'ha fet costat d'una manera o altra al llarg d'aquest projecte.

En particular, vull agrair al Dr. Xavier Guitart, que ha estat disposat a reunir-se amb mi en tot moment, i ha respost tots els meus correus i dubtes -que no eren pas pocs- amb paciència i entusiasme; al meu amic David, que s'ha ofert en tot moment a donar-me un cop de mà; i a la resta dels meus companys, amb qui hem compartit rialles i ansietats sobre els nostres respectius treballs.

Índex

Introducció

La pregunta de si un nombre n és primer o no es coneix com el problema de la primeritat. Per resoldre aquest problema utilitzem com a eines els testos de primeritat, uns algorismes que donat un nombre n afirmen que n és primer o és compost. Existeixen dos tipus de testos de primeritat; els deterministes, que garanteixen amb tota certesa la primeritat d'un nombre; i els probabilístics, que no poden assegurar la veracitat del resultat però presenten una fita de l'error, que mitjançant certs processos, poden reduir tant com es desitgi.

Els problemes de factorització d'un nombre i la determinació de nombres primers són molt antics. Els registres històrics sobre l'estudi dels nombres primers es remunten a Euclides (segle III a.C.) tot i que hi ha evidències del coneixement d'aquests nombres per part de Pitàgores (segle VI a.C.). No obstant això, el primer mètode matemàtic per trobar aquests nombres el va dissenyar Eratòstenes (segle II a.C.) i es coneix per "garbell d'Eratòstenes". És un mètode senzill que serveix per trobar tots els nombres primers entre 1 i n: primer cal escriure tots els nombres entre 1 i n, aleshores marquem tots els nombres múltiples de 2, i després, recurrentment, marquem els múltiples del primer nombre no marcat. Al final del procés els nombres no marcats són els nombres primers que buscàvem. Ara bé, utilitzar el garbell d'Eratòstenes com a test de primeritat comporta certs inconvenients, com per exemple, una quantitat desorbitada d'operacions i espai. Per això, si volem determinar la primeritat d'un nombre, per molt que utilitzem un ordinador, no farem servir aquest algorisme. En canvi, sí que podem fer servir algun dels dos que estudiarem en aquest treball.

Abans d'introduir els testos de primeritat que estudiarem, analitzarem el càlcul de complexitats dels algorismes en general. És a dir, aprendrem a calcular l'eficiència d'un algorisme, per tal de poder comparar per un mateix problema i dos algorismes diferents, quin dels dos el resoldrà més de pressa.

El primer test que estudiarem és el test probabilístic de Miller-Rabin. De fet, podríem dir que aquest és un test per determinar si un nombre és compost, ja que si el test ens diu que n és compost, ho és amb tota certesa. Ara bé, si el test diu que n és primer, no podem garantir que el resultat sigui cert, donant una probabilitat d'error que és com a molt del 25%. Aquest és un test útil a nivell comercial, ja que si bé una probabilitat de l'error del 25% no sembla gaire satisfactòria, es pot repetir el test diverses vegades per tal que aquesta probabilitat es redueixi dràsticament. A més a més, el cost de l'algorisme és molt baix tant a nivell de càlcul com d'espai, però això ho veurem més endavant.

També farem un breu estudi sobre els cossos ciclotòmics, ja que quan estudiem el segon algorisme, l'AKS, ens trobarem amb l'anell $\mathbb{Z}[\zeta]/(n)$ on ζ denota una arrel primitiva de la unitat i n és un nombre del qual volem saber si és primer o compost. Si bé no és necessari fer aquest estudi per comprendre l'algorisme, pot ser interessant aprofundir en les estructures algebraiques que el sostenen.

Finalment estudiarem l'algorisme AKS. La particularitat d'aquest test és que va resoldre el problema de la primeritat en un temps polinomial respecte al nombre de dígits, un problema no resolt fins al 2002 quan M. Agrawal, N. Kayal i N. Saxena van presentar l'algorisme. Ara bé, a nivell comercial no té sentit utilitzar aquest test, perquè en comparació a d'altres, com el de Miller-Rabin, el temps de càlcul és desmesuradament més llarg.

Capítol 1

Anàlisi d'algorismes - Complexitat

Aquest capítol consisteix en una breu introducció al càlcul de complexitats d'algorismes per tal de poder analitzar correctament els algorismes que estudiarem més endavant. Les principals referències d'aquest capítol són: *Análisis de algoritmos - complejidad* [9] i *Técnicas de Diseño de Algoritmos* [7].

Donat un problema i un dispositiu on resoldre'l, és necessari donar un mètode precís adequat al dispositiu que el resolgui. A aquest mètode se'l denomina algorisme.

Un cop es disposa d'un algorisme que funciona correctament, és necessari definir criteris per mesurar el seu rendiment o comportament. Aquests criteris es centren principalment en la seva simplicitat i en l'ús eficient dels recursos.

L'ús eficient dels recursos es sol mesurar en funció de dos paràmetres: l'*espai*, és a dir, la memòria que utilitza, i el *temps*, el que tarda a executar-se. Ambdós representen els costos que suposa trobar la solució al problema plantejat mitjançant un algorisme. A més a més, aquests paràmetres ens permeten comparar algorismes entre si, permetent determinar quin és més adequat d'entre varis per resoldre un mateix problema. En aquest capítol ens centrarem a estudiar el temps.

El temps d'execució d'un algoritme dependrà de factors com: les dades d'entrada, la qualitat del codi, la capacitat de processament de la màquina utilitzada o la complexitat intrínseca de l'algorisme. A l'hora de mesurar el temps d'execució d'un algorisme hi ha dos estudis possibles: un proporciona una mesura teòrica, que consisteix en obtenir una funció que acoti (superiorment o inferiorment) el temps d'execució de l'algoritme; i l'altre ofereix una mesura real, que consisteix en mesurar el temps d'execució en un ordinador concret. Denotarem per $T(n)$ el temps d'execució teòric d'un algoritme per una entrada de mida n.

1.1 Operacions Elementals

A l'hora de mesurar el temps, sempre ho farem en funció del nombre d'operacions elementals (OE) que realitza l'algoritme, entenent per operacions elementals, les que l'ordinador realitza en un temps acotat per una constant. Així, considerem OE les operacions aritmètiques bàsiques, assignacions a variables del tipus predefinit pel compilador, les comparacions lògiques i els accessos a estructures indexades bàsiques, com vectors i matrius. Cada una d'aquestes comptabilitza com 1 OE.

Regles generals pel càlcul del nombre de OE:

- Considerarem que el temps d'una OE és, per definició, d'ordre 1.
- El temps d'execució d'una seqüència consecutiva d'instruccions es calcula sumant els temps d'execució de cada una de les instruccions.
- Si s'executa una sentència separada en casos $\{S_1, \ldots, S_n\}$ el temps d'execució és $T = T(C) + max(T(S_1), \ldots, T(S_n))$ on $T(C)$ és el temps de comparació entre casos. Els temps d'execució de les sentències "IF ... ELSE ..." es comptabilitzaran d'igual forma.
- El temps d'execució de bucles de n iteracions contenint una sentència S serà $T = T(C) + n(T(S) + T(C))$.
- El temps d'execució de crides a procediments recursius donarà lloc a equacions en recurrència.

1.2 Cotes de complexitat

Una vegada vistes les formes de calcular el temps d'execució T d'un algorisme, volem classificar aquestes funcions de forma que es puguin comparar. Per a això definim classes d'equivalència corresponents a funcions que "crèixen de la mateixa forma".

Donada una funció f, volem estudiar les funcions g que com a molt creixen tan de pressa com f. Al conjunt d'aquestes funcions se'l denomina cota superior de f i s'expressa $O(f)$. Coneixent la cota superior d'un algorisme podem assegurar que, en cap cas, el temps emprat serà superior al de la cota.

Definició 1.2.1. *Sigui $f : \mathbb{N} \to [0, \infty)$. Es defineix el conjunt de funcions d'ordre O de f com:*

$$O(f) = \{g : \mathbb{N} \to [0, \infty) | \exists c \in \mathbb{R}, c > 0, \exists n_0 \in \mathbb{N}, g(n) \leq cf(n) \ \forall n \geq n_0\}.$$

Direm que $t : \mathbb{N} \to [0, \infty)$ és d'ordre O de f si $t \in O(f)$.

Algunes de les propietats de O que s'obtenen directament de la definició són les següents:

1. Per a tota funció f es compleix que $f \in O(f)$.
2. $f \in O(g) \Rightarrow O(f) \subset O(g)$.
3. $O(f) = O(g) \Leftrightarrow f \in O(g)$ i $g \in O(f)$.
4. $f \in O(g)$ i $g \in O(h) \Rightarrow f \in O(h)$.
5. $f \in O(g)$ i $f \in O(h) \Rightarrow f \in O(\min(g, h))$.
6. Regla de la suma: $f_1 \in O(g)$ i $f_2 \in O(h) \Rightarrow f_1 + f_2 \in O(\max(g, h))$.
7. Regla del producte: $f_1 \in O(g)$ i $f_2 \in O(h) \Rightarrow f_1 \cdot f_2 \in O(g \cdot h)$.
8. Si existeix $\lim_{n\to\infty} \frac{f(n)}{g(n)} = k$ depenent dels valors de k s'obté:

(a) $k \neq 0$ i $k < \infty \Rightarrow O(f) = O(g)$.

(b) $k = 0 \Rightarrow f \in O(g)$ i $g \notin O(f)$, és a dir, $O(f) \subsetneq O(g)$.

9. $\lim_{n\to\infty} \frac{f(n)}{g(n)} = \infty \Rightarrow g \in O(f)$ i $f \notin O(g)$, és a dir, $O(g) \subsetneq O(f)$.

De les propietats anteriors es dedueix que la relació $\sim_O$, definida per $f \sim_O g$ si i només si $O(f) = O(g)$, és una relació d'equivalència. Sempre s'escull el representant més senzill per cada classe; d'aquesta manera definim els següents ordres de complexitat.

Conjunts o ordres de complexitat	
$O(1)$	Ordre constant
$O(\log n)$	Ordre logarítmic
$O(n)$	Ordre lineal
$O(n \log n)$	
$O(n^2)$	Ordre quadràtic
$O(n^a)$	Ordre polinomial (a $>$ 2)
$O(a^n)$	Ordre exponencial
$O(n!)$	Ordre factorial

També existeixen altres tipus de cotes, com per exemple les cotes inferiors Ω o les cotes d'ordre exacte Θ.

Definició 1.2.2. *Sigui $f : \mathbb{N} \to [0, \infty)$. Es defineix el conjunt de funcions d'ordre Ω de f com:*

$$\Omega(f) = \{g : \mathbb{N} \to [0, \infty) | \exists c \in \mathbb{R}, c > 0, \exists n_0 \in \mathbb{N}, g(n) \geq cf(n)\ \forall n \geq n_0\}.$$

Direm que una funció $t : \mathbb{N} \to [0, \infty)$ és d'ordre Ω de f si $t \in \Omega(f)$.

Definició 1.2.3. *Sigui $f : \mathbb{N} \to [0, \infty)$. Es defineix el conjunt de funcions d'ordre Θ de f com:*

$$\Theta(f) = O(f) \cap \Omega(f)$$

o, el que és igual:

$$\Theta(f) = \{g : \mathbb{N} \to [0, \infty) | \exists c, d \in \mathbb{R}, c, d > 0, \exists n_0 \in \mathbb{N}, cf(n) \leq g(n) \leq df(n)\ \forall n \geq n_0\}.$$

Direm que una funció $t : \mathbb{N} \to [0, \infty)$ és d'ordre Θ de f si $t \in \Theta(f)$.

1.3 Complexitat aritmètica bàsica

Al tractar amb nombres grans hem de deixar de considerar les operacions aritmètiques entres ells com a operacions elementals, ja que com veurem a continuació, la complexitat en funció de la mida dels paràmetres no és constant.

Si tenim k dígits en una base b, podem representar nombres fins a $b^k - 1$. Aleshores, si volem representar el nombre $N = b^k - 1$, aïllant k, veiem que necessitem $\log_b(N + 1)$ dígits.

Proposició 1.3.1. *La suma de dos nombres de n dígits en base $b \geq 2$ té com a màxim $n + 1$ dígits.*

L'algorisme habitual utilitzat per sumar dos nombres opera dígit a dígit, per tant, siguin x i y dos nombres de n bits. $(x+y)$ té com a molt $n+1$ bits i la complexitat de l'operació ha de ser $O(n)$.

En el cas de la multiplicació, en l'algorisme usual pel producte de dos nombres de n dígits: tenim n multiplicacions de complexitat n (1 bit per n bits) i després aproximadament $2n$ sumes de complexitat $2n$, que és un total de $(n^2+4n^2)=5n^2$ i, per tant, la complexitat de la multiplicació és de $O(n^2)$.

Cal destacar que existeixen algorismes més eficients per multiplicar dos nombres grans, com per exemple l'algorisme de Karatsuba, que aconsegueix reduir la complexitat del producte de dos nombres de n bits a $3n^{\log_2 3}$.

El quocient entre un dividend de n dígits i un divisor de m dígits amb l'algorisme habitual té una complexitat de $O(n^2)$. Ja que la generació de cada dígit del quocient requereix dos passos: la multiplicació del divisor per un dígit, amb complexitat $O(m)$; i la resta del resultat en el dividend, amb complexitat de $O(n)$. Com que hem de realitzar n/m passos la complexitat resultat és $O(m \cdot n \cdot n/m) = O(n^2)$.

També cal destacar que existeixen algorismes, com per exemple el de Newton-Raphson, que poden reduir la complexitat de la divisió a $O(M(n))$ on $M(n)$ és la complexitat l'algorisme multiplicatiu que escollim.

En la suma modular $(a+b)\%N$ apliquem que $(a+b)\%N = (a\%N + b\%N)\%N$. Ara com que $a, b \in [0, N-1] \Rightarrow (a+b) \in [0, 2(N-1)]$ que com a molt té 1 bit més. Com que els operands ja estan mòdul N, fem la suma bàsica i només cal tenir en compte que si $a+b > N-1$ cal restar-li N. Per tant, la complexitat és de l'operació és de $O(n)$ on n és el nombre de dígits de N.

En el cas de la multiplicació modular, fem primer la multiplicació bàsica i després en calculem el mòdul. Els dos processos tenen una complexitat de $O(n^2)$, per tant, la complexitat total també és de $O(n^2)$.

Finalment, analitzem la complexitat d'elevar un nombre m a la potència de n. La forma habitual de fer-ho consisteix en fer multiplicar n vegades el nombre m, però això pot ser molt costós. Fixem-nos doncs en el fet que podem expressar m^n de la següent manera

$$m^n = \sum_{i \leq \log_2(n)} m_i 2^i \quad \text{amb } m_i \in \{0,1\}.$$

Aleshores només necessitem $\log_2(n)$ operacions per calcular els $m_i 2^i$ i $\log_2(n)$ operacions més per multiplicar-los entre ells. En total només necessitem $2\log_2(n)$ operacions, és a dir $O(\log(n))$ operacions. A aquest mètode per elevar nombres se'l coneix com a exponenciació binària i el podem desenvolupar amb l'algorisme recursiu descrit a [6].

Algorisme 1.3.2. *Donada una base m i un exponent n calculem m^n amb la funció recursiva*

$$\text{Potència}(m,n) = \begin{cases} m, & \text{si } n = 1 \\ \text{Potència}(m^2, n/2), & \text{si } n \text{ és parell} \\ m \cdot \text{Potència}(m^2, (n-1)/2), & \text{si } n \text{ és senar} \end{cases}$$

1.4 Classificació de problemes

Per tal de resoldre un problema concret, hi poden haver diversos algorismes aplicables. Es diu que l'ordre de complexitat d'un problema és el del millor algorisme conegut per resoldre'l. D'aquesta manera es poden classificar els problemes en diferents classes.

Definició 1.4.1. *La* classe P *és el conjunt de problemes que es poden resoldre amb un algorisme conegut de complexitat polinòmica.*

Es diu que els problemes de classe P són tractables, és a dir, abordables a la pràctica. En canvi, aquells problemes pels quals la millor solució coneguda és de complexitat superior a la polinòmica, es diu que són problemes intractables.

Definició 1.4.2. *La* classe NP *és el conjunt de probleme que compleixen que les seves solucions es poden verificar en temps polinòmic. NP és l'acrònim en Anglès de* nondeterministic polinomial time.

La importància d'aquesta classe de problemes és que contenen molts problemes de cerca i optimització en els que es desitja saber si existeix una certa solució o si existeix una solució millor a les ja conegudes.

Clarament, si un problema està en P també està en NP.

Definició 1.4.3. *Un problema de decisió (diguem-li C) és de classe* NP-Complet *si compleix:*

1. *C està en NP.*
2. *Tot problema de NP és reduïble a C en temps polinomial.*

Una transformació polinòmica de L en C és un algorisme determinista que transforma en temps polinòmic instàncies $l \in L$ en instàncies $c \in C$ tals que la resposta a c és positiva si i només si la resposta a l ho és.

Com a conseqüència d'aquesta definició, en cas d'existir un algorisme en P per C, existiria una solució en P per tot problema de NP. D'aquí apareix la principal pregunta de la teoria de la computació, encara sense resposta: és P igual a NP?

Capítol 2

Miller-Rabin, un test de primeritat probabilístic

En aquest capítol analitzarem el test de Miller-Rabin, un test de primeritat probabilístic. Originalment, era un test determinista proposat per Gary L. Miller en l'article *Riemann's hypothesis and tests for primality* [10] el 1976. Però aquest, es basava en la hipòtesi generalitzada de Riemman, que a dia d'avui, no està demostrada. Va ser el 1980 quan Michael O. Rabin va proposar la seva versió probabilística, que no depèn de la hipòtesi generalitzada de Riemman, a l'article *Probabilistic algorithm for testing primality* [11].

Quan parlem d'un test de primeritat probabilístic, ens referim a un test que afirma amb una certa probabilitat si un nombre és primer o compost. L'algorisme presentat a continuació consisteix en repetir diverses vegades el test de Miller-Rabin amb inicialitzacions aleatòries. D'aquesta manera, donat un nombre n compost, l'algorisme determina ràpidament i amb alta probabilitat que n no és primer. D'altra banda, si n passa el test, és altament probable que n sigui un nombre primer.

La referència principal d'aquest capítol és l'article *Four primality testing algorithms* [12].

2.1 Conceptes previs

El test de Miller-Rabin es basa en el teorema següent.

Teorema 2.1.1. *Sigui $n > 9$ un enter senar compost. Podem escriure $n - 1 = 2^k m$ per algun $k \geq 1$ i algun enter senar m. Considerem el conjunt*

$$B = \{x \in (\mathbb{Z}/n\mathbb{Z})^* : x^m = 1 \text{ o } x^{m2^i} = -1 \text{ per algun } 0 \leq i < k\}.$$

Aleshores es compleix que

$$\frac{\#B}{\varphi(n)} \leq \frac{1}{4},$$

on φ és la funció φ d'Euler.

Demostració. Denotem per l al màxim exponent de 2 que compleix que 2^l divideix $p - 1$

per tot p divisor de n. Definim el conjunt

$$B' = \{x \in (\mathbb{Z}/n\mathbb{Z})^* : x^{m2^{l-1}} = \pm 1\}.$$

Volem veure que B està contingut en B'. Clarament si $x \in (\mathbb{Z}/n\mathbb{Z})^*$ i $x^m = 1$, aleshores $x^{m2^{l-1}} = 1$. I per tant x pertany a B'. Ara, si $x^{m2^i} = -1$ per algun $0 \leq i < k$, aleshores $x^{m2^i} \equiv -1 \pmod{p}$ per tot primer p divisor de n. En conseqüència, per tot p, la potència exacta de 2 dividint l'ordre de x mòdul p és 2^{i+1}. Com que $(\mathbb{Z}/p\mathbb{Z})^*$ és un grup cíclic, els ordres dels seus elements divideixen l'ordre del grup, i per tant, 2^{i+1} divideix $p-1$. Ara tenim que $l \geq 2^{i+1}$ i podem escriure $x^{m2^{l-1}} = (-1)^{2^{l-i-1}}$, que val -1 o 1 depenent de si $l = i+1$ o si $l > i+1$. Així doncs, x pertany a B', i per tant, $B \subset B'$.

Com que $\#B' \geq \#B$, si provem que $\frac{\#B'}{\varphi(n)} < \frac{1}{4}$ en particular haurem vist que $\frac{\#B}{\varphi(n)} < \frac{1}{4}$. Suposem doncs

$$\frac{\#B'}{\varphi(n)} \geq \frac{1}{4}. \tag{2.1.1}$$

Volem saber quants elements té B'. Pel teorema xinès del residu sabem que el nombre de x pertanyents a $(\mathbb{Z}/n\mathbb{Z})$ tals que $x^{m2^{l-1}} = 1$ és igual al producte del nombre de solucions de l'equació $X^{m2^{l-1}} \equiv 1 \mod p^{a_p}$ per tot p divisor de n, on p^{a_p} denota la potència exacta de p que divideix n. Com que $(\mathbb{Z}/p^{a_p}\mathbb{Z})^*$ és un grup cíclic d'ordre $(p-1)p^{a_p-1}$, l'ordre dels elements del grup han de dividir $(p-1)p^{a_p-1}$, i per tant, el nombre de solucions és $\mathrm{mcd}((p-1)p^{a_p}, m2^{l-1})$ i com que p no divideix m i 2^{l-1} divideix $p-1$ aquest nombre és igual a $\mathrm{mcd}((p-1), m)2^{l-1}$. Així que tenim

$$\#\{x \in (\mathbb{Z}/n\mathbb{Z})^* : x^{m2^{l-1}} = 1\} = \prod_{p|n} \mathrm{mcd}(p-1, m)2^{l-1}.$$

D'igual forma veiem que el nombre de solucions de l'equació $X^{m2^l} = 1$ mòdul p^{a_p} és igual a $\mathrm{mcd}(p-1, m)2^l$ i així podem deduïr el nombre de solucions de l'equació $X^{m2^{l-1}} = -1$ mòdul p^{a_p} amb la diferència

$$\mathrm{mcd}(p-1, m)2^l - \mathrm{mcd}(p-1, m)2^{l-1} = \mathrm{mcd}(p-1, m)2^{l-1}.$$

Obtenim doncs

$$\#B' = 2\prod_{p|n} \mathrm{mcd}(p-1, m)2^{l-1}.$$

I per tant, utilitzant la desigualtat (2.1.1) tenim

$$\frac{\#B'}{\varphi(n)} = 2\prod_{p|n} \frac{\mathrm{mcd}(p-1, m)2^{l-1}}{(p-1)p^{a_p} - 1} > \frac{1}{4}. \tag{2.1.2}$$

Com que $\mathrm{mcd}(p-1, m)2^{l-1}$ divideix $(p-1)/2$ podem deduir

$$\frac{1}{4} < 2\prod_{p|n} \frac{\mathrm{mcd}(p-1, m)2^{l-1}}{(p-1)p^{a_p} - 1} \leq 2\prod_{p|n} \frac{1}{2} = 2^{1-t}.$$

On $t \leq 2$ denota el nombre de primers diferents que divideixen n.

Suposem que $t = 2$. Si algun dels divisors primers de n té multiplicitat major a 1, la part esquerra de la desigualtat (2.1.2) és com a molt $2^{1-2}/3 = 1/6$ i això no és possible.

Per tant, ha de ser que $n = pq$ per dos primers diferents p i q. Ara la desigualtat (2.1.2) és

$$\frac{p-1}{\text{mcd}(p-1,m)2^l} \cdot \frac{q-1}{\text{mcd}(q-1,m)2^l} < 2.$$

Com que els factors de l'esquerra de la desigualtat són enters positius, els dos han de valdre 1. Per tant la potència exacta de 2 dividint tant $p-1$ com $q-1$ és 2^l i les parts senars de $p-1$ i $q-1$ divideixen m. Sigui r la part senar de $p-1$, és a dir, el enter senar que compleix $p = 1 + 2^l r$, i sigui r' la part senar de $q-1$. Considerant la relació $pq = 1 + 2^k m$ mòdul r, veiem que $2^k m \equiv 0$ i $p \equiv 1$ per tant, com que $q = 1 + 2^l r'$ obtenim $2^l r' \equiv 0 \pmod{r}$, és a dir, la part senar de $p-1$ divideix la part senar de $q-1$. Per simetria, veiem que r' divideix r i concloem que $p = q$. Com que això no és possible, cal $t = 1$, i aleshores $n = p^a$ per algun $a \geq 2$. De la desigualtat (2.1.2) veiem que $p^{a-1} < 4$ i aleshores cal que p sigui 3 i a sigui 2, contradient $n > 9$.

Tenim doncs que la desigualtat (2.1.1) no es compleix i això prova el teorema. □

Proposició 2.1.2. *Sigui n un nombre primer senar, les úniques arrels quadrades de 1 mòdul n són 1 i -1.*

Demostració. Sigui x tal que $x^2 \equiv 1 \pmod{n}$, aleshores $x^2 - 1 \equiv 0 \pmod{n}$. Com que $x^2 - 1 = (x+1)(x-1)$ i n és primer, es compleix que n divideix a $x+1$ o n divideix a $x-1$, és a dir, $x \equiv 1 \pmod{n}$ o $x \equiv -1 \pmod{n}$. □

2.2 Algorisme i complexitat

Quan un nombre qualsevol $x \in (\mathbb{Z}/n\mathbb{Z})^*$ està contingut al conjunt B del Teorema 2.1.1, diem que "n passa un test de Miller-Rabin" i que "n és un primer probable respecte la base x". Això és degut al fet que si n és primer senar, per tot $x \in (\mathbb{Z}/n\mathbb{Z})^*$, tenim que x pertany a B.

Demostració. Sigui n un nombre primer senar. Escrivim $n = 2^k m + 1$ amb m senar i prenem $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Considerem la successió $x^m, x^{2m}, x^{2^2 m}, \ldots, x^{2^k m}$ i ens fixem en que cada terme és el quadrat de l'anterior. Pel petit teorema de Fermat $x^{2^k m} = x^{n-1} \equiv 1 \pmod{n}$ i per tant, $(x^{2^{k-1}m})^2 \equiv 1 \pmod{n}$. Per la Proposició 2.1.2 tenim que $x^{2^{k-1}m} \equiv \pm 1 \pmod{n}$. Si $x^{2^{k-1}m} \equiv -1 \pmod{n}$ ja tenim que $x \in B$, en cas contrari, $x^{2^{k-1}m} \equiv 1 \pmod{n}$ i $(x^{2^{k-2}m})^2 \equiv 1 \pmod{n}$. Per tant $x^{2^{k-2}m} \equiv \pm 1 \pmod{n}$ i podem iterar aquest procés. Aleshores concloem que algun dels termes $x^{2^i m}$ amb $0 \leq i < k$ és congruent amb -1 mòdul n i, per tant, $x \in B$, o tots els termes són congruents amb 1 mòdul n, en particular $x^m \equiv 1 \pmod{n}$ i, per tant, $x \in B$. □

Quan un nombre n no passa un test de Miller-Rabin per una certa base x, per la demostració anterior tenim que n és un nombre compost i diem que "x és testimoni que n és compost".

Pel Teorema 2.1.1 la probabilitat que un nombre compost n passi un test de Miller-Rabin és com a molt del 25%. Aleshores repetir el test de Miller-Rabin per certes bases aleatòries d'un nombre n és un algorisme probabilístic per determinar si un nombre n és primer o compost.

Anem a veure doncs la complexitat d'aquest algorisme. Comprovar si una base x de n és testimoni que n sigui compost consisteix en elevar x a una potència no superior a n, amb l'algorisme de l'exponenciació binària 1.3.2 això es pot fer amb $\log(n)$ multiplicacions mòdul n de cost $O(\log(n)^2)$. És a dir, un test de Miller-Rabin té una complexitat de $O((\log n)^3)$. Ara bé, si volem disminuir el marge d'error cal repetir el test diverses vegades, així doncs, per tenir un marge d'error menor a $(1/4)^k$ cal realitzar k testos i la complexitat resultant de l'algorisme és $O(k(\log(n))^3)$.

Capítol 3

Cossos ciclotòmics

Aquest capítol consisteix en un breu estudi dels cossos ciclotòmics, i més en general, dels nombres algebraics. La motivació d'aquest, és conèixer l'anell d'enters del cos generat per una arrel primitiva de la unitat, ja que aquest apareix en el capítol següent quan analitzem l'algorisme AKS, i així ens podem familiaritzar amb ell. Les referències principals en les quals es basa aquest estudi són els llibres: *A course in algebraic number theory* [2], *A first course in modular forms* [5] i *Algebraic number theory* [3].

Cal mencionar que la teoria presentada a continuació parteix d'un coneixement elemental previ en matèria d'estructures algebraiques i teoria de Galois. Tot i així, fem un petit recordatori dels cossos ciclotòmics.

Diem que un nombre complex ζ és una arrel n-èssima de la unitat si $\zeta^n = 1$. Una arrel n-èssima de la unitat ζ és primitiva si $\zeta^k \neq 1$ per tot $k \in \{1, 2, ..., n-1\}$. Si ζ_n és una arrel n-èssima primitiva de la unitat, el conjunt de les arrels n-èssimes primitives de la unitat és $\{\zeta_n^k : 1 \leq k \leq n \text{ i } \text{mcd}(k, n) = 1\}$. El nombre d'arrels primitives n-èssimes de la unitat és $\varphi(n)$ on φ indica la funció φ d'Euler.

S'anomena cos ciclotòmic n-èssim al cos de descomposició del polinomi $X^n - 1$ sobre $\mathbb{Q}$. Les arrels d'aquest polinomi en el seu cos de descomposició són les arrels de la unitat i, si ζ_n és una arrel primitiva de la unitat, les arrels de $X^n - 1$ són les potències de ζ_n. El cos ciclotòmic n-èssim és doncs $\mathbb{Q}(\zeta_n)$ i anomenem extensió ciclotòmica a l'extensió $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$. Sigui $\mathcal{P}$ el conjunt de les arrels n-èssimes primitives de la unitat, definim:

$$\Phi_n(X) := \prod_{\zeta \in \mathcal{P}} (X - \zeta).$$

Es compleix que $\Phi_n(X)$ pertany a $\mathbb{Q}[X]$ i és irreductible sobre $\mathbb{Q}$. Per tant, $\Phi_n(X)$ és el polinomi irreductible sobre $\mathbb{Q}$ de ζ_n, on ζ_n és una arrel n-èssima primitiva de la unitat, i el grau de l'extensió $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ és $\varphi(n)$.

A més a més, com que tota arrel n-èssima de la unitat és una arrel d-èssima primitiva de la unitat per algun d divisor de n, també es compleix que $X^n - 1$ és el producte de tots els polinomis ciclotòmics $\Phi_d(X)$ on d divideix n. Aquest és un resultat que utilitzarem més endavant.

Arribats a aquest punt, per seguir aprofundint en l'estudi dels cossos ciclotòmics és necessari introduir alguns conceptes relacionats amb els nombres algebraics.

3.1 Nombres algebraics

Definició 3.1.1. *Un nombre complex α és un nombre algebraic si és arrel d'un polinomi no nul amb coeficients racionals. És a dir, si existeix*

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0, on\ a_0, ..., a_n \in \mathbb{Q}$$

tal que $p(\alpha) = 0$.

És clar que tot nombre racional r és algebraic, ja que és arrel del polinomi $X - r$. Però no tots els nombres algebraics són racionals, per exemple, l'arrel quadrada d'un nombre racional r satisfà el polinomi $X^2 - r$.

El conjunt dels nombres algebraics, denotat $\overline{\mathbb{Q}}$, forma un cos. Això es mostra com a corol·lari del següent teorema.

Teorema 3.1.2. *Sigui $\alpha \in \mathbb{C}$. Les condicions següents són equivalents:*

(1) α és un nombre algebraic, i.e, $\alpha \in \overline{\mathbb{Q}}$.

(2) L'anell $\mathbb{Q}[\alpha]$ és un espai vectorial de dimensió finita sobre $\mathbb{Q}$.

(3) α pertany a un anell $R \subset \mathbb{C}$ que és un espai vectorial de dimensió finita sobre $\mathbb{Q}$.

Demostració. (1) $\Longrightarrow$ (2): Sigui $\alpha \in \overline{\mathbb{Q}}$, és arrel d'un polinomi $a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0, \quad a_0, ..., a_n \in \mathbb{Q}$. Aleshores $\alpha^n = -\sum_{i=0}^{n} b_i \alpha^i$ amb $b_i = a_i / a_n$ i, per tant, l'espai vectorial complex generat per $\{1, \alpha, ..., \alpha^{n-1}\}$ també conté α^n. De forma similar $\alpha^{n+1} = -\sum_{i=0}^{n} b_i \alpha^{i+1}$ i, per tant, α^{n+1} pertany a l'espai vectorial i inductivament també la resta de potències.

(2) $\Longrightarrow$ (3) trivial.

(3) $\Longrightarrow$ (1): Sigui $\{g_1, ..., g_n\}$ una base de l'anell R com a espai vectorial sobre $\mathbb{Q}$. Per cada producte $g_i \alpha$ existeix una combinació lineal racional dels generadors $\alpha g_i = \sum_{j=1}^{n} c_{ij} g_i$. Essent g el vector columna amb entrades g_i, i M la matriu $n \times n$ d'entrades $c_{ij} \in \mathbb{Q}$, es dedueix de l'expressió anterior que $\alpha g = Mg$. Aleshores α és valor propi de M i, per tant, satisfà el polinomi característic de M, un polinomi amb coeficients racionals.

□

Corolari 3.1.3. *Els nombres algebraics $\overline{\mathbb{Q}}$ formen un cos.*

Demostració. Siguin α i β nombres algebraics. Els anells $\mathbb{Q}[\alpha]$ i $\mathbb{Q}[\beta]$ tenen unes respectives bases $\{\alpha^i : 0 \leq i < n\}$ i $\{\beta^j : 0 \leq j < m\}$ com a espais vectorials sobre $\mathbb{Q}$. Sigui $R = \mathbb{Q}[\alpha, \beta]$, generat pel conjunt $\{\alpha^i \beta^j : 0 \leq i < n, 0 \leq j < m\}$ com a espai vectorial sobre $\mathbb{Q}$. Aleshores $\alpha\beta$ i $\alpha + \beta$ pertanyen a R i per la condició (3) del teorema són nombres algebraics. Si $\alpha \neq 0$, existeix un polinomi amb coeficients racionals tal que $p(\alpha) = 0$ i té un terme independent $c_0 \neq 0$. Sigui $\gamma = (p(\alpha) - c_0)/(-c_0\alpha) \in \mathbb{Q}[\alpha]$, es compleix $\gamma\alpha = 1$ i, per tant, $\gamma = \alpha^{-1}$ és un nombre algebraic per la condició (3) del teorema. □

Ara es poden considerar els nombres complexos α que satisfan polinomis amb coeficients en $\overline{\mathbb{Q}}$. Però de fet, $\overline{\mathbb{Q}}$ és algebraicament tancat, és a dir, que les arrels dels polinomis amb coeficients en $\overline{\mathbb{Q}}$ estan també en $\overline{\mathbb{Q}}$.

Corołari 3.1.4. *El cos $\overline{\mathbb{Q}}$ és algebraicament tancat.*

Demostració. Sigui $a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ un polinomi amb coeficients $a_i \in \overline{\mathbb{Q}}$ i α una de les seves arrels a $\mathbb{C}$. Com que cada $\mathbb{Q}[a_i]$ és un $\mathbb{Q}-$espai vectorial de dimensió finita, també ho és $R = \mathbb{Q}[a_0, ..., a_n]$. Sigui $R' = R[\alpha]$. Si $\{v_i : 1 \leq i < m\}$ és una base de R, aleshores $\{v_i\alpha^j : 1 \leq i < m, 0 \leq j < n\}$ és un conjunt generador de R'. (No és necessariament una base, ja que α podria satisfer un polinomi de menor grau). Per la condició (3) del teorema $\alpha \in \overline{\mathbb{Q}}$. □

3.2 Cossos de nombres

Definició 3.2.1. *Un cos de nombres és un cos $K \subset \overline{\mathbb{Q}}$ que compleix que el grau de l'extensió $[K : \mathbb{Q}]$ és finit.*

Per cada $\alpha \in \overline{\mathbb{Q}}$ existeix el seu polinomi mínim o irreductible $p(X) \in \mathbb{Q}[X]$, que és el polinomi mònic de grau menenor tal que $p(\alpha) = 0$ i se'l denota per $\text{Irr}(\alpha, \mathbb{Q})$. El grau de α es defineix com el grau de $\text{Irr}(\alpha, \mathbb{Q})$.

Teorema 3.2.2. *Sigui K un cos de nombres de grau n. Aleshores existeix $\alpha \in K$ tal que grau(α) = n. I en particular tenim que*

$$K = \mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} \quad | \quad a_0, ..., a_{n-1} \in \mathbb{Q}\}$$

Demostració. Com que totes les extensions finites sobre $\mathbb{Q}$ són separables, per ser $\mathbb{Q}$ un cos de característica 0, el teorema de l'element primitiu ens diu que són simples. □

Teorema 3.2.3. *Sigui $K = \mathbb{Q}(\alpha_1)$ un cos de nombres de grau n. Existeixen n $\mathbb{Q}$-homomorfismes de cossos no trivials diferents*

$$\sigma_i : K \to \mathbb{C} \quad (i = 1, 2, ..., n).$$

Els elements $\sigma_i(\alpha_1) = \alpha_i$ són els diferents $\mathbb{Q}-$conjugats de α_1, és a dir, les diferents arrels de $Irr(\alpha_1, \mathbb{Q})$.

Demostració. Siguin $\alpha_2, \ldots, \alpha_n$ els $\mathbb{Q}$-conjugats de α_1, cada α_i $(i = 1, \ldots, n)$ té per polinomi mínim a $p(X) = Irr(\alpha_1, \mathbb{Q})$. Per tant, hi ha un únic isomorfisme de cossos $\sigma_i : \mathbb{Q}(\alpha_1) \to \mathbb{Q}(\alpha_i)$ definit per $\sigma_i(\alpha_1) = \alpha_i$. De fet, si $\alpha \in \mathbb{Q}(\alpha_1)$, $\alpha = q(\alpha_1)$ per un $q(X) \in \mathbb{Q}[X]$ de grau més petit que n i s'ha de complir que $\sigma_i(\alpha) = q(\alpha_i)$. Recíprocament, si σ és un $\mathbb{Q}$-homomorfisme, σ deixa invariant a $\mathbb{Q}$ i, per tant, $0 = \sigma(p(\alpha_1)) = p(\sigma(\alpha_1))$, de manera que $\sigma(\alpha_1)$ és una de les arrels de $p(X)$ i σ és un dels σ_i. □

Exemple 3.2.4. Sigui $K = \mathbb{Q}(\sqrt[3]{2})$. Aleshores $p(X) = X^3 - 2$. Les arrels del polinomi són:

$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \omega\sqrt[3]{2}, \quad \alpha_3 = \omega^2\sqrt[3]{2}, \quad ,\omega = e^{2\pi i/3}.$$

i els homomorfismes són:

$$\sigma_1 : \alpha \mapsto \sqrt[3]{2}, \quad \sigma_2 : \alpha \mapsto \omega\sqrt[3]{2}, \quad \sigma_3 : \alpha \mapsto \omega^2\sqrt[3]{2}$$

Definició 3.2.5. *Sigui E/F una extensió de cossos finita i separable de grau n. Pel teorema de l'element primitiu existeix un element α de E tal que $E = F(\alpha_1)$. Siguin $\alpha_1, \ldots, \alpha_n$ les n arrels del $Irr(\alpha_1, F)$ i siguin $\{\sigma_1, \ldots, \sigma_n\}$ els n diferents morfismes de E en una clausura algebraica de E que fixen F i compleixen $\sigma_i(\alpha_1) = \alpha_i$. Aleshores definim la norma de α_1 en l'extensió E/F com*

$$N_{E/F}(\alpha_1) := \prod_{i=0}^{n} \sigma_i(\alpha_1).$$

Sigui K un cos de nombres de grau n. Com que $\mathbb{Q}$ és un cos de característica 0, K és una extensió finita i separable sobre $\mathbb{Q}$. Per tant, la norma de l'extensió $K/\mathbb{Q}$ sempre està ben definida.

Proposició 3.2.6. *Siguin F, K, E cossos de nombres tals que $F \subseteq K \subseteq E$ i l'extensió E/F és finita i separable. Aleshores es compleix*

$$N_{E/F} = N_{K/F} \circ N_{E/K}.$$

És a dir, les normes són transitives.

Demostració. Sigui $\overline{E}$ una clausura algebraica de E. Siguin $\{\sigma_1, \ldots, \sigma_n\}$ els diferents morfismes de K en $\overline{E}$ que fixen F i siguin $\{\tau_1, \ldots, \tau_m\}$ els diferents morfismes de E en $\overline{E}$ que fixen K. Ara l'extensió $\overline{E}/F$ és finita i separable, ja que també ho és l'extensió E/F, i és normal per ser $\overline{E}$ la clausura algebraica de E. Aleshores l'extensió $\overline{E}/F$ és de Galois i, a més a més, els morfismes σ_i i τ_i són automorfismes de $\overline{E}$. Té sentit doncs considerar la composició

$$N_{K/F}(N_{E/K}(x)) = \prod_{i=1}^{n} \sigma_i(\prod_{j=1}^{m} \tau_j(x)) = \prod_{i=1}^{n} \prod_{j=1}^{m} \sigma_i(\tau_j(x)).$$

Cada $\sigma_i\tau_j = \sigma_i \circ \tau_j$ és un F-homomorfisme de E en $\overline{E}$ i el nombre de morfismes ve donat per $mn = [E : K][K : F] = [E : F]$. Veiem ara que tots els morfismes $\sigma_i\tau_j$ són diferents en E. Si $\sigma_i\tau_j = \sigma_t\tau_l$ en E, aleshores $\sigma_i = \sigma_t$ en K, ja que τ_j i τ_l són la identitat quan els restringim a K. Això implica que $i = t$ i, per tant, $\tau_j = \tau_l$ en E, i això només es compleix si $j = l$. Així doncs, $\sigma_i\tau_j$ són mn morfismes diferents de E en $\overline{E}$ que fixen F i, per tant, $N_{K/F}(N_{E/F}(x)) = N_{E/F}(X)$. □

Proposició 3.2.7. *Sigui K un cos de nombres de grau n i sigui $\alpha \in K$ de grau d. Aleshores $N(\alpha) = (-1)^n a_0^{n/d}$, on a_0 és el terme constant del polinomi mínim de α.*

Demostració. Com que $[K : \mathbb{Q}] = n$ i $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ per multiplicitat dels graus d'extensions de cossos tenim que $[K : \mathbb{Q}(\alpha)] = n/d$. Tenim que α pertany a $\mathbb{Q}(\alpha)$ i, per tant, $N_{K/\mathbb{Q}(\alpha)}(\alpha) = \alpha^{n/d}$. També tenim que $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \prod_{i=0}^{d} \alpha_i$ on α_i són les arrels de $\mathrm{Irr}(\alpha, \mathbb{Q})$ i, per tant, $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = (-1)^d a_0$ on a_0 denota el terme constant de $\mathrm{Irr}(\alpha, \mathbb{Q})$. Finalment, per transitivitat de les normes

$$N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}(\alpha)}(N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)) = N_{K/\mathbb{Q}(\alpha)}((-1)^d a_0) = ((-1)^d a_0)^{n/d} = (-1)^n a_0^{n/d}.$$

□

3.3 Enters algebraics

L'anell d'enters $\mathbb{Z}$ en el cos dels nombres racionals $\mathbb{Q}$ té una analogia natural en el cos dels nombres algebraics $\overline{\mathbb{Q}}$. Sigui $\alpha \in \overline{\mathbb{Q}}$, el denominador de α, den(α), es defineix com el mínim comú múltiple dels denominadors dels coeficients del seu polinomi mínim.

Definició 3.3.1. *Un nombre complex α és un enter algebraic si és un nombre algebraic amb $den(\alpha) = 1$. El conjunt d'enters algebraics es denota $\overline{\mathbb{Z}}$.*

Els enters algebraics dins del cos dels racionals $\mathbb{Q}$ són els enters usuals $\mathbb{Z}$ i els anomenem enters racionals.

Lema 3.3.2. *Sigui $\alpha \in \overline{\mathbb{Q}}$ i $den(\alpha) = d$. Aleshores $d\alpha \in \overline{\mathbb{Z}}$.*

Demostració. Sigui $p(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a0$ el polinomi mínim de α. Multiplicant $p(X)$ per d^n s'obté:

$$(dX)^n + a_{n-1}d \cdot (dX)^{n-1} + ... + a_1d^{n-1} \cdot (dX) + a_0d^n.$$

Aleshores el polinomi $X^n + a_{n-1}dX^{n-1} + ... + a_1d^{n-1}dX + a_0d^n$ és el polinomi mínim de $d\alpha$ i té els coeficients enters, per tant, $d\alpha \in \overline{\mathbb{Z}}$.

□

Teorema 3.3.3. *Sigui $\alpha \in \mathbb{C}$. Les condicions següents són equivalents:*

(1) α és un enter algebraic, i.e, $\alpha \in \overline{\mathbb{Z}}$.

(2) L'anell $\mathbb{Z}[\alpha]$ és finitament generat com a grup abelià.

(3) α pertany a un anell $R \subset \mathbb{C}$ que és un finitament generat com a grup abelià.

Demostració. (1) $\implies$ (2): Sigui $\alpha \in \overline{\mathbb{Z}}$, α satisfà un polinomi $X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0, \quad a_1, ..., a_n \in \mathbb{Z}$. Aleshores $a^n = -\sum_{i=0}^{n-1} a_i\alpha^i$ de forma que α^n pertany al grup Abelià generat per $\{1, \alpha, \ldots, \alpha^{n-1}\}$. D'igual manera $\alpha^{n+1} = -\sum_{i=0}^{n-1} a_iX^{i+1}$, per tant, α^{n+1} també pertany al grup, i inductivament es demostra que ho fan la resta de potències de α.

(2) $\implies$ (3) trivial.

(3) $\implies$ (1): Sigui $\{g_1, ..., g_n\}$ una base de l'anell R com a grup Abelià. Per cada producte $g_i\alpha$ existeix una combinació lineal dels generadors $\alpha g_i = \sum_{j=1}^{n} c_{ij}g_i$. Essent g el vector columna amb entrades g_i, i M la matriu $n \times n$ d'entrades $c_{ij} \in \mathbb{Z}$, es dedueix de l'expressió anterior $\alpha g = Mg$. Aleshores α és valor propi de M i, per tant, satisfà el polinomi característic de M, un polinomi amb coeficients enters. □

Corołari 3.3.4. *Els enters algebraics $\overline{\mathbb{Z}}$ formen un anell.*

Demostració. Siguin α i β enters algebraics. Els anells $\mathbb{Z}[\alpha]$ i $\mathbb{Z}[\beta]$ tenen les respectives bases $\{\alpha^i : 0 \leq i < n\}$ i $\{\beta^j : 0 \leq j < m\}$ com a grups Abelians finitament generats. Sigui $R = \mathbb{Z}[\alpha, \beta]$, generat pel conjunt $\{\alpha^i\beta^j : 0 \leq i < n, 0 \leq j < m\}$ com a grup Abelià. Aleshores $\alpha\beta$ i $\alpha + \beta$ pertanyen a R i per la condició (3) del teorema són enters algebraics.

□

Corołari 3.3.5. *Els enters algebraics formen un anell íntegrament tancat, és a dir, que tot polinomi mònic amb coeficients a $\overline{\mathbb{Z}}$ té totes les arrels a $\overline{\mathbb{Z}}$.*

Demostració. Sigui $a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ un polinomi amb coeficients $a_i \in \overline{\mathbb{Z}}$ i α una de les seves arrels. Com que cada $\mathbb{Z}[a_i]$ és finitament generat com a grup Abelià, també ho és $R = \mathbb{Z}[a_0, ..., a_n]$. Sigui $R' = R[\alpha]$. Si $\{v_i : 1 \leq i < m\}$ és una base de R, aleshores $\{v_i\alpha^j : 1 \leq i < m, 0 \leq j < n\}$ és un conjunt generador de R'. Per la condició (3) del teorema $\alpha \in \overline{\mathbb{Z}}$. □

3.4 Anells d'enters

Definició 3.4.1. *Sigui K un cos de nombres. L'anell d'enters de K denotat per $\mathcal{O}_K$ és l'anell d'enters algebraics en K. És a dir, $\mathcal{O}_K = \overline{\mathbb{Z}} \cap K$.*

Teorema 3.4.2. *Sigui K un cos de nombres de grau d. L'anell d'enters $\mathcal{O}_K$ és un grup abelià lliure de rang d i existeix una base $\{\alpha_1, ..., \alpha_d\} \subset \mathcal{O}_K$ tal que*

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_d = \{m_1\alpha_1 + \cdots + m_d\alpha_d \quad | \quad m_1, \ldots, m_d \in \mathbb{Z}\}.$$

([3] 1.2.3).

Exemple 3.4.3. Sigui $d \in \mathbb{Z}$ amb $d \neq 1$ lliure de quadrats, $K = \mathbb{Q}(\sqrt{d})$ i $\alpha = a + b\sqrt{d}$ amb $a, b \in \mathbb{Q}$ enter algebraic. Com que α satisfà l'equació $X^2 - 2aX + a^2 - b^2d = 0$ tenim que $2a, a^2 - b^2d \in \mathbb{Z}$. En particular, $a \in \mathbb{Z}$ o $a = m + \frac{1}{2}$ per algun $m \in \mathbb{Z}$.

Si $a \in \mathbb{Z}$, com que $a^2 - b^2d \in \mathbb{Z} \Rightarrow b^2d \in \mathbb{Z}$. Si $b = p/q$ amb $p, q \in \mathbb{Z}, q \neq 1$ i $\mathrm{mcd}(p, q) = 1 \Rightarrow \frac{d}{q^2} \in \mathbb{Z}$, però això no és possible, ja que d és lliure de quadrats, per tant, $b \in \mathbb{Z}$.

Si $a = m + \frac{1}{2}$, $\frac{1}{2} + b\sqrt{d}$ també és enter algebric. Aleshores $\frac{1}{4} - b^2d \in \mathbb{Z}$. Això és possible si i només si $b = n + \frac{1}{2}$ per algun $n \in \mathbb{Z}$. Aleshores $\frac{1}{2} + b\sqrt{d} = \frac{1}{2} + n\sqrt{d} + \frac{\sqrt{d}}{2}$ i com que $n\sqrt{d}$ satisfà l'equació $X^2 - n^2d$ és un enter algebraic, per tant, $\frac{1+\sqrt{d}}{2}$ també és enter algebraic. Però si $b = n + \frac{1}{2} \Leftrightarrow \frac{1}{4} - \frac{d}{4} - n^2d - nd \in \mathbb{Z} \Leftrightarrow \frac{1}{4} - \frac{d}{4} \in \mathbb{Z} \Leftrightarrow d \equiv 1 \pmod 4$.

En conclusió, si $d \in \mathbb{Z}$ amb $d \neq 1$ lliure de quadrats i $K = \mathbb{Q}(\sqrt{d})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ si $d \not\equiv 1 \pmod 4$ i $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si $d \equiv 1 \pmod 4$.

Definició 3.4.4. *Sigui K un cos de nombres de grau n i sigui $x = \{x_1, \ldots, x_n\}$ un conjunt de n elements de K. Definim el discriminant de x en K com:*

$$D(x) := \det((\sigma_i(x_j))_{i,j=1,2,...,n})^2$$

on σ_i $(i = 1, \ldots, n)$ són els diferents $\mathbb{Q}$-automorfismes de K.

Proposició 3.4.5. *Sigui $z = \{z_1, \ldots, z_n\}$ una base de l'anell d'enters $\mathcal{O}_K$, el discriminant $D(z)$ pren el mateix valor per tota base de $\mathcal{O}_K$. Se l'anomena discriminant del cos K i el denotem per D_K. ([2] 2.3.7).*

Teorema 3.4.6. *Sigui $K = \mathbb{Q}(\alpha)$, $p(X)$ el polinomi mínim de α i, D el discriminant de la base $\{1, \alpha, \cdots, \alpha^{n-1}\}$ de K. Si les arrels del polinomi mínim són $\{\alpha_1, \cdots, \alpha_n\}$ amb $\alpha = \alpha_1$, aleshores el discriminant D és igual a $\prod_{i<j}(\alpha_i - \alpha_j)^2$.*

Demostració. Siguin σ_i els $\mathbb{Q}$-homomorfismes que envien α a α_i, $i = 1, \cdots, n$. Aleshores $\sigma_i(\alpha^j) = \alpha_i^j$, $0 \leq j \leq n-1$. El discriminant D és el quadrat del determinant de la matriu

$$M = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{bmatrix}$$

Veiem que M és un determinant de Vandermonde, el resultat del qual és $\prod_{i<j}(\alpha_i - \alpha_j)$, i per tant, el discriminant D és igual a $\prod_{i<j}(\alpha_i - \alpha_j)^2$. □

Corołari 3.4.7. *Sota les condicions del teorema, $D = (-1)^{\binom{n}{2}} N(p'(\alpha))$ on $p'(X)$ és la derivada del polinomi $p(X)$.*

Demostració. Sigui $c = (-1)^{\binom{n}{2}}$. Ja hem vist en el teorema que $D = \prod_{i<j}(\alpha_i - \alpha_j)^2$ i com que $(\alpha_i - \alpha_j)(\alpha_j - \alpha_i) < 0$ per tot $i \neq j$ i hi ha $(n-1)n/2 = \binom{n}{2}$ parelles (i, j) tals que $i < j$, tenim

$$D = \prod_{i<j}(-1)(\alpha_i - \alpha_j)(\alpha_j - \alpha_i) = c\prod_{i\neq j}(\alpha_i - \alpha_j) = c\prod_i \prod_{j\neq i}(\alpha_i - \alpha_j).$$

Com que $p(X) = (X - \alpha_1)\cdots(X - \alpha_n)$ la seva derivada val

$$p'(X) = \sum_{k=1}^{n} \prod_{j\neq k}(X - \alpha_j)$$

i en evaluar $p(X)$ en α_i tots els sumands s'anul·len llevat de $\prod_{j\neq i}(\alpha_i - \alpha_j)$, per tant,

$$D = c\prod_{i=1}^{n} p'(\alpha_i).$$

Aplicant que $p'(\alpha_i) = p'(\sigma_i(\alpha)) = \sigma_i(p'(\alpha))$ i que $N(p'(\alpha)) = \prod_{i=1}^{n} \sigma_i(p'(\alpha))$ obtenim que $D = cN(p'(\alpha))$. □

3.5 Ideals en anells d'enters

Sigui K un cos de nombres i $\mathcal{O}_K$ el seu anell d'enters. Un *ideal* I en $\mathcal{O}_K$ és un subconjunt no buit de $\mathcal{O}_K$ amb les següents propietats:

1. $a, b \in I \Rightarrow a + b \in I$.
2. $a \in I, r \in \mathcal{O}_K \Rightarrow ra \in I$.

L'ideal que només conté el 0 es denota (0). De la propietat (1.) es dedueix que tot ideal és un subgrup additiu en $\mathcal{O}_K$.

Definició 3.5.1. *Un ideal principal I és aquell que es pot generar (com a ideal) per un sol element, és a dir, que existeix $\alpha \in I$ tal que $I = \{r\alpha \mid r \in \mathcal{O}_K\}$.*

Definició 3.5.2. *Un ideal $\wp$ es diu primer, si no és igual a $\mathcal{O}_K$ i per tot $a, b \in \mathcal{O}_K$ amb $ab \in \wp$ es compleix que $a \in \wp$ o $b \in \wp$.*

Proposició 3.5.3. *Tot ideal primer $\wp \in \mathcal{O}_K$ diferent de (0) és maximal. ([3] 1.3.4).*

Proposició 3.5.4. *Si $\mathcal{O}_K$ és un grup abelià lliure de rang n. Tot ideal I de $\mathcal{O}_K$ diferent de (0) és també un grup abelià lliure de rang n.*

Demostració. Com que $\mathcal{O}_K$ és un grup abelià lliure i I és un subgrup de $\mathcal{O}_K$, tenim que I també és un grup abelià lliure, només cal veure doncs que té rang n. Sigui $\{x_1, \ldots, x_n\}$ una base de $\mathcal{O}_K$ i sigui t un element no nul de I, aleshores els elements $tx_1, \ldots, tx_n$ pertanyen a I i són linealment independents, per tant, són una base de I. □

Definició 3.5.5. *Sigui K un cos de nombres i $\mathcal{O}_K$ el seu anell d'enters. Sigui I un ideal de $\mathcal{O}_K$ diferent de (0), definim la norma de I com el cardinal de l'anell quocient $\mathcal{O}_K/I$, és a dir, $N(I) = |\mathcal{O}_K/I|$.*

Sota les condicions de la definició anterior, sigui ara $x = \{x_1, \ldots, x_n\}$ una base de $\mathcal{O}_K$ i $z = \{z_1, \ldots, z_n\}$ una base de I. Si D_K és el valor del discriminant de K, és a dir, el discriminant $D(x)$, podem relacionar el discriminant de z amb la norma de I de la següent manera

$$D(z) = N(I)^2 D_K = |\mathcal{O}_K/I|^2 D_K.$$

De forma similar, si $v = \{v_1, \ldots, v_n\}$ és una base d'un grup abelià lliure J de rang n de K, el discriminant de v compleix

$$D(v) = |\mathcal{O}_K/J|^2 D_K. \tag{3.5.1}$$

([2] 4.2.5 i 7.1.8).

Proposició 3.5.6. *Siguin I, J ideals tals que $IJ \subset \wp$ on $\wp$ és un ideal primer. Aleshores $I \subset \wp$ o $J \subset \wp$.*

Demostració. Es suposa que ni I ni J estan continguts en $\wp$. Clarament $\wp \subset I + \wp$. Com que $\wp$ és primer, és maximal i, per tant, $I + \wp = \mathcal{O}_K$. D'igual forma $J + \wp = \mathcal{O}_K$. Aleshores $(I + \wp)(J + \wp) = \mathcal{O}_K$, d'altra banda, $(I + \wp)(J + \wp) = IJ + I\wp + J\wp + \wp^2 \subset \wp$ i apareix una contradicció. Per tant, cal que $I \subset \wp$ o $J \subset \wp$. □

Existeixen diversos cossos de nombres els quals els seus anells d'enters són dominis d'ideals principals i, per tant, dominis de factorització única. Però això no sempre es compleix, per exemple, en $\mathbb{Z}[\sqrt{-5}]$ tenim que $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$. Aquests quatre factors són irreductibles en $\mathbb{Z}[\sqrt{-5}]$ de manera que en aquest anell no hi ha factorització única.

Tot i així, el següent teorema dona, en certa manera, un substitut respecte a la factorització única en un anell d'enters.

Teorema 3.5.7 (Teorema fonamental de l'aritmètica). *Sigui K un cos de nombres i $\mathcal{O}_K$ el seu anell d'enters. Tot ideal diferent de (0) en $\mathcal{O}_K$ factoritza de manera única com a producte d'ideals primers ([3] 1.3.6).*

Definició 3.5.8. *Sigui P un ideal primer de $\mathbb{Z}$ diferent de (0) i sigui K un cos de nombres. Definim l'elevació de P a $\mathcal{O}_K$ com l'ideal $P\mathcal{O}_K$.*

Pot ser que $P\mathcal{O}_K$ no sigui un ideal primer de $\mathcal{O}_K$, però pel teorema fonamental de l'aritmètica tenim que

$$P\mathcal{O}_K = \prod_{i=0}^{g} P_i^{e_i}.$$

On P_i són ideals primers de $\mathcal{O}_K$ i e_i són enters positius.

D'altra banda, podem prendre un ideal primer Q diferent de (0) en $\mathcal{O}_K$ i formar un ideal primer P en $\mathbb{Z}$ fent la intersecció $P = Q \cap \mathbb{Z}$. Aleshores diem que Q cau en P, o que, P és una contracció de Q.

Proposició 3.5.9. *Sigui K un cos de nombres i sigui P un ideal primer de A. Considerem l'elevació de P en $\mathcal{O}_K$. Els ideals $P_1, \ldots, P_g$ que apareixen en la factorització en ideals primers de $P\mathcal{O}_K$ són precisament els ideals de $\mathcal{O}_K$ que cauen en P. ([2] 4.1.2).*

Definició 3.5.10. *Sigui K un cos de nombres i P un ideal primer de $\mathbb{Z}$. Considerem l'elevació $P\mathcal{O}_K$ de P com $\prod_{i=0}^{g} P_i^{e_i}$. Anomenem a cada enter positiu e_i índex de ramificació de P_i sobre P. També diem que P ramifica en $P\mathcal{O}_K$ si $e_i > 1$ per almenys un i.*

Proposició 3.5.11. *Si k és un cos de nombres i P un ideal primer de $\mathbb{Z}$, es compleix que $\mathbb{Z}/P$ és un subcos de $\mathcal{O}_K/P_i$ i $\mathcal{O}_K/P_i$ és una extensió finita de $\mathbb{Z}/P$.*

Demostració. L'aplicació de $\mathbb{Z}/P$ a $\mathcal{O}_K/P_i$ definida per $a+P \mapsto a+P_i$ és un homomorfisme ben definit injectiu, ja que $P = P_i \cap \mathbb{Z}$. L'anell d'enters $\mathcal{O}_K$ és un $\mathbb{Z}$-mòdul finitament generat (un grup abelià lliure finitament generat) i, per tant, $\mathcal{O}_K/P_i$ és un $\mathbb{Z}/P$-mòdul que, a més a més, és un espai vectorial de dimensió finita sobre $\mathbb{Z}/P$. □

Al grau f_i de l'extensió $\mathcal{O}_K/P_i$ sobre $\mathbb{Z}/P$ l'anomenem grau relatiu de P_i sobre P. I relacionant els graus relatius amb els índexs de ramificacions obtenim el següent resultat.

Teorema 3.5.12. *Sigui K un cos de nombres de grau n i sigui P un ideal primer de $\mathbb{Z}$ tal que la seva elevació $P\mathcal{O}_K$ és igual a $\prod_{i=0}^{g} P_i^{e_i}$. Aleshores es compleix*

$$\sum_{i=0}^{g} f_i e_i = [\mathcal{O}_K/P\mathcal{O}_K : \mathbb{Z}/P] = n.$$

([2] 4.1.6).

Recordem que n, és a dir, el grau del cos de nombres K, coincideix amb el rang de $\mathcal{O}_K$ com a grup abelià.

3.6 Anell d'enters de cossos ciclotòmics

L'objectiu d'aquesta secció és veure que si ζ_n és una arrel n-èssima primitiva de la unitat, l'anell d'enters de $\mathbb{Q}(\zeta_n)$ és $\mathbb{Z}[\zeta_n]$. Aquest és un resultat general, però com que en el capítol següent només tractarem el cas particular en què $n = p^r$, on p és un nombre primer i r és un nombre natural, només demostrarem l'enunciat sota aquestes condicions. Al llarg de la secció suposarem que $n = p^r$ llevat que s'especifiqui el contrari.

Proposició 3.6.1. $\Phi_{p^r}(1) = p$.

Demostració. Com ja hem vist anteriorment, $\Phi_n(X)$ és el producte de tots els polinomis ciclotòmics $\Phi_d(X)$ on d és un divisor de n. Aleshores deduïm que

$$X^{p^r} - 1 = \Phi_{p^r}(X) \cdot (X^{p^{r-1}} - 1)$$

i, per tant,

$$\Phi_{p^r}(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = \frac{t^p - 1}{t - 1} = 1 + t + \cdots + t^{p-1}.$$

on $t = X^{p^{r-1}}$. Finalment, substituint $X = 1$ obtenim $\Phi_{p^r}(X) = p$. □

Proposició 3.6.2. *Si ζ és una arrel n-èssima primitiva de la unitat, la norma de $(1-\zeta)$ és $\pm p$, i més en general, la norma de $(1-\zeta^{p^s})$ és $\pm p^{p^s}$ per tot $0 \leq s < r$.*

Demostració. El polinomi mínim de $(1-\zeta)$ és $\Phi_{p^r}(1-X)$, que té per terme constant $a_0 = \Phi_{p^r}(1-0) = p$. Aplicant que $N(1-\zeta) = (-1)^{p^r} a_0^{p^r/p^r} = (-1)^{p^r} a_0$ ja hem demostrat el cas particular. Ara, per tot $0 < s < r$, ζ^{p^s} és una arrel p^{r-s}-èssima de la unitat, així que aplicant el mètode previ obenim que $N_1(1-\zeta^{p^s}) = \pm p$, on N_1 és la norma en l'extensió de $\mathbb{Q}(\zeta^{p^s})$ sobre $\mathbb{Q}$.

Com que $(1-\zeta^{p^s})$ pertany a $\mathbb{Q}(\zeta^{p^s})$ tots els $\mathbb{Q}(\zeta^{p^s})$-automorfismes deixen fix a $(1-\zeta^{p^s})$ i, per tant, la norma de $(1-\zeta^{p^s})$ en l'extensió $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}(\zeta^{p^s})$ és $N_0(1-\zeta^{p^s}) = (1-\zeta^{p^s})^b$ on

$$b = [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta^{p^s})] = \varphi(p^r)/\varphi(p^{r-s}) = p^s.$$

I, per tant, aplicant la transitivitat de les normes a la cadena $\mathbb{Q}(\zeta), \mathbb{Q}(\zeta^{p^s}), \mathbb{Q}$, podem calcular

$$N(1-\zeta^{p^s}) = N_1(N_0(1-\zeta^{p^s})) = N_1((1-\zeta^{p^s})^b) = \pm p^b = \pm p^{p^s}.$$

□

Teorema 3.6.3. *Si ζ és una arrel p^r-èssima primitiva de la unitat, aleshores l'anell d'enters de $\mathbb{Q}(\zeta)$ és $\mathbb{Z}[\zeta]$.*

Demostració. Com que ζ és arrel del polinomi $X^{p^r} - 1$, tenim que ζ pertany a $\mathcal{O}_{\mathbb{Q}(\zeta)}$ i en conseqüència $\mathbb{Z}(\zeta) \subseteq \mathcal{O}_{\mathbb{Q}(\zeta)}$. Per tant, per demostrar la igualtat només hem de veure que $\mathcal{O}_{\mathbb{Q}(\zeta)} \subseteq \mathbb{Z}(\zeta)$.

Prenem $z = \{1, \zeta, \ldots, \zeta^{\varphi(p^r)-1}\}$ com a base del grup abelià lliure $\mathbb{Z}[\zeta]$ i calculem el discriminant de la base z en $\mathbb{Q}(\zeta)$ utilitzant la fórmula $D(z) = \pm N(\Phi'_{p^r}(\zeta))$ 3.4.7. Per calcular la derivada de Φ_{p^r} derivem la igualtat

$$(X^{p^{r-1}} - 1) \cdot \Phi_{p^r}(X) = X^{p^r} - 1$$

i obtenim

$$(X^{p^{r-1}} - 1)\Phi'_{p^r}(X) + p^{r-1} X^{p^{r-1}-1} \Phi_{p^r}(X) = p^r X^{p^r-1}.$$

Substituint $X = \zeta$ anul·lem el sumand que conté $\Phi_{p^r}(\zeta)$ i podem aïllar $\Phi'_{p^r}(\zeta)$

$$\Phi'_{p^r}(\zeta) = \frac{p^r \zeta p^r - 1}{\zeta^{p^{r-1}} - 1}.$$

Aplicant la Proposició 3.6.2 calculem la norma del denominador

$$N(\zeta^{p^{r-1}} - 1) = N(-1) \cdot N(1 - \zeta^{p^{r-1}}) = \pm 1 \cdot (\pm p^{r-1}) = \pm p^{r-1}.$$

Com que ζ és una arrel de la unitat, $N(\zeta) = \pm 1$, i com que p^r pertany a $\mathbb{Q}$, $N(p^r) = p^{r\varphi(p^r)} = p^{rp^{r-1}(p-1)}$. Finalment,

$$N(\Phi'_{p^r}(\zeta)) = \frac{p^{rp^{r-1}(p-1)}(\pm 1)^{p^r-1}}{\pm p^{r-1}} = \pm p^{r(p-1)p^{r-1}-p^{r-1}} = \pm p^{p^{r-1}(pr-r-1)}.$$

Ara hem vist que el discriminant de z en $\mathbb{Q}(\zeta)$ és potència de p i com que z és una base del grup abelià lliure $\mathbb{Z}[\zeta]$ es compleix la igualtat (3.5.1)

$$D(z) = |\mathcal{O}_{\mathbb{Q}(\zeta)}/\mathbb{Z}[\zeta]|^2 D_{\mathbb{Q}(\zeta)},$$

on $D_{\mathbb{Q}(\zeta)}$ és el discriminant del cos $\mathbb{Q}(\zeta)$ i, per tant, $|\mathcal{O}_{\mathbb{Q}(\zeta)}/\mathbb{Z}[\zeta]|$ és potència de p. És a dir, si $m \in \mathbb{N}$ és prou gran, $p^m(\mathcal{O}_{\mathbb{Q}(\zeta)}/\mathbb{Z}[\zeta]) = 0$ o, equivalentment, $p^m\mathcal{O}_{\mathbb{Q}(\zeta)} \subseteq \mathbb{Z}[\zeta]$. Finalment, veurem que $\mathbb{Z}[\zeta] + p^m\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathcal{O}_{\mathbb{Q}(\zeta)}$ que juntament amb el resultat anterior implica que $\mathcal{O}_{\mathbb{Q}(\zeta)} \subseteq \mathbb{Z}[\zeta]$ i, per tant, $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$.

Considerem l'ideal (p). Utilitzant la Proposició 3.6.1 tenim que

$$p = \Phi_{p^r}(1) = \prod_{\zeta'}(1-\zeta') = \prod_{\zeta'}\frac{1-\zeta'}{1-\zeta}(1-\zeta) = v(1-\zeta)^{\varphi(p^r)},$$

on v és una unitat de $\mathbb{Z}[\zeta]$, ja que si ζ_0 i ζ_1 són dos arrels p^r-èssimes primitives de la unitat, $\zeta_1 = \zeta_0^s$ per algun s no múltiple de p. Aleshores, $(1-\zeta_0^s)/(1-\zeta_0) = 1+\zeta_0+\cdots+\zeta_0^{s-1} \in \mathbb{Z}[\zeta_0]$, de forma equivalent, $(1-\zeta_0)/(1-\zeta_1) \in \mathbb{Z}[\zeta_1] = \mathbb{Z}[\zeta_0]$ i

$$\frac{1-\zeta_1}{1-\zeta_0} \cdot \frac{1-\zeta_0}{1-\zeta_1} = 1.$$

Per tant, l'ideal (p) coincideix amb l'ideal $(1-\zeta)^{\varphi(p^r)}$. Per comoditat denotem $\beta = 1-\zeta$. Veiem que (β) és un ideal primer, ja que en cas contrari $(p) = (\beta)^{\varphi(p^r)}$ tindria més de $\varphi(p^r)$ factors primers i això no és possible segons el Teorema 3.5.12. El teorema també afirma que el grau de l'extensió $\mathcal{O}_{\mathbb{Q}(\zeta)}/(\beta)$ sobre $\mathbb{Z}/(p)$ és 1, i en conseqüència la injecció

$$\frac{\mathbb{Z}}{(p)} \hookrightarrow \frac{\mathcal{O}_{\mathbb{Q}(\zeta)}}{(\beta)}$$

és en realitat un isomorfisme. Per tant, si $q \in \mathcal{O}_{\mathbb{Q}(\zeta)}$, existeix un $t \in \mathbb{Z}$ tal que $q + (\beta) = t + (p)$. Com que $(p) = (\beta)^{\varphi(p^r)}$ veiem que $q = (\beta) + t$ i en conseqüència

$$\mathcal{O}_{\mathbb{Q}(\zeta)} \subseteq \beta\mathcal{O}_{\mathbb{Q}(\zeta)} + \mathbb{Z} \subseteq \beta\mathcal{O}_{\mathbb{Q}(\zeta)} + \mathbb{Z}[\zeta]$$

i, ja que $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta)}$ obtenim la igualtat $\mathcal{O}_{\mathbb{Q}(\zeta)} = \beta\mathcal{O}_{\mathbb{Q}(\zeta)} + \mathbb{Z}[\zeta]$. Multiplicant per β als dos costats tenim $\beta\mathcal{O}_{\mathbb{Q}(\zeta)} = \beta^2\mathcal{O}_{\mathbb{Q}(\zeta)} + \beta\mathbb{Z}[\zeta]$. Fixem-nos ara que si $q \in \mathcal{O}_{\mathbb{Q}(\zeta)}$, tenim $q = q_1 + q_2$ amb $q_1 \in \mathbb{Z}[\zeta]$ i $q_2 \in \beta\mathcal{O}_{\mathbb{Q}(\zeta)}$. També tenim que $q_2 = q_3 + q_4$ amb $q_3 \in \mathbb{Z}[\zeta]$ i $q_4 \in \beta^2\mathcal{O}_{\mathbb{Q}(\zeta)}$. Aleshores $q = (q_1 + q_3) + q_4$ i, per tant, $\mathcal{O}_{\mathbb{Q}(\zeta)} = \beta^2\beta\mathcal{O}_{\mathbb{Q}(\zeta)} + \mathbb{Z}[\zeta]$. Podem iterar aquest procés fins que $\mathcal{O}_{\mathbb{Q}(\zeta)} = \beta^{\varphi(p^r)}\mathcal{O}_{\mathbb{Q}(\zeta)} + \mathbb{Z}[\zeta]$ i utilitzant que $\beta^{\varphi(p^r)} = p$ podem seguir iterant fins a obtenir el resultat desitjat $\mathcal{O}_{\mathbb{Q}(\zeta)} = p^m\mathcal{O}_{\mathbb{Q}(\zeta)} + \mathbb{Z}[\zeta]$. □

Capítol 4

AKS, un test de primeritat determinista d'ordre polinomial

El *problema de la primeritat* consisteix en esbrinar si un nombre natural és primer o compost. Hi ha mètodes molt antics per resoldre aquest problema, per exemple, el *garbell d'Eratòstenes (200 a.C)*, però aquests mètodes són ineficients quan es desitja analitzar nombres grans. Per decidir la primeritat d'un nombre n, el garbell d'Eratòstenes requereix un temps d'execució proporcional a n. D'altra banda, la quantitat de dígits que es necessiten per escriure aquest nombre és proporcional a $\log(n)$.

En termes de complexitat computacional es diu que un algorisme hauria de requerir un temps polinòmic respecte la quantitat de dígits. En aquest cas, es desitja un algorisme que decideixi en un temps proporcional a $\log^k n$, si n és un nombre primer o compost. Utilitzant la notació *O gran*, aquesta proporció s'abreuja com $O(\log^k n)$.

L'estiu de 2002 tres informàtics indis M. Agrawal, N. Kayal i N. Saxena van presentar l'algorisme denominat a partir dels seus cognoms (AKS), resolent per primer cop el problema de la primeritat en ordre polinomial. Anteriorment, es sabia que el problema de la primeritat estava en NP i gràcies a l'algorisme AKS ara se sap que el problema està en P. D'aquí el nom de l'article "*Primes is in P*" [1].

Les referències principals d'aquest capítol són l'article *Four primality testing algorithms* [12] i *Prime numbers, a computational perspective* [4].

4.1 Conceptes previs

Sigui r un nombre primer, $\Phi_r(X) = X^{r-1} + \cdots + X + 1$ el polinomi ciclotòmic de grau $r-1$ i ζ_r un zero de $\Phi_r(X)$. Denotem per $\mathbb{Z}[\zeta_r]$ l'anell de nombres generat per ζ_r sobre $\mathbb{Z}$. Per qualsevol $n \in \mathbb{Z}$, $\mathbb{Z}[\zeta_r]/(n)$ és l'anell quocient $\mathbb{Z}[\zeta_r]$ mòdul el seu ideal principal (n). Si $n \neq 0$, aquest és un anell finit. Aquest resultat apareix de considerar una base $\{1, \zeta_r, \ldots, \zeta_r^{r-2}\}$ de $\mathbb{Z}[\zeta_r]$ i, per tant, $\mathbb{Z}[\zeta_r]/(n) = \{\alpha_0 + \alpha_1\zeta_r + \cdots + \alpha_{r-2}\zeta_r^{r-2} \quad | \quad \alpha_0, \alpha_1, \ldots, \alpha_{r-2} \in \mathbb{Z}/n\mathbb{Z}\}$.

Teorema 4.1.1. *Sigui n un enter positiu senar i r un nombre primer. Suposem que*

1. *n no és divisible per cap primer $\leq r$.*
2. *l'ordre de n (mod r) és com a mínim $(\log n / \log 2)^2$.*

3. per cada $0 \leq j < r$ es compleix $(\zeta_r + j)^n = \zeta_r^n + j$ en $\mathbb{Z}[\zeta_r]/(n)$.

Aleshores n és una potència d'un nombre primer.

Demostració. La condició (2) implica que $n \not\equiv 1 \pmod{r}$. Aleshores existex un divisor primer p de n no congruent amb $1 \pmod{r}$. Aquest fet es dedueix de que si n factoritza en producte de primers com $p_1^{k_1} \cdots p_t^{k_t}$ i per tot p_i amb $1 \leq i \leq t$, $p_i \equiv 1 \pmod{r}$ aleshores $n \equiv 1 \pmod{r}$. Denotarem per A la $\mathbb{F}_p$-àlgebra $\mathbb{Z}[\zeta_r]/(p)$, que és un quocient de l'anell $\mathbb{Z}[\zeta_r]/(n)$. Per tot $k \in \mathbb{Z}$ coprimer amb r denotem σ_k l'automorfisme d'anells de A definit per $\sigma_k(\zeta_r) = \zeta_r^k$. Essent Δ el grup d'automorfismes de A en A, l'aplicació $(\mathbb{Z}/r\mathbb{Z})^* \mapsto \Delta$ donada per $k \mapsto \sigma_k$ és un isomorfisme ben definit. Anomenem Γ al subgrup de Δ generat per l'automorfisme de Frobenius σ_p i per σ_n. Considerem també el subgrup de A^*:

$$G = \{a \in A^* : \sigma_n(a) = a^n\}.$$

Al ser A un anell diferent de $\{0\}$, té ideals maximals. Sigui $\mathfrak{m}$ un ideal maximal de A, definim $k = A/\mathfrak{m}$. Com que k és un cos finit, és una extensió finita de $\mathbb{F}_p$ generada per una arrel r-èssima primitiva de la unitat. Sigui $H \subset k^*$ la imatge de G per l'aplicació $\pi : A \to k$. El grup H és cíclic per ser subgrup de $(\mathbb{F}_{p^f})^*$. Es compleix el següent diagrama commutatiu:

$$\begin{array}{ccc} G & \subset & A^* \\ \downarrow \pi & & \downarrow \pi \\ H & \subset & k^* \end{array}$$

Com que Δ és commutatiu, per tot $g \in G$ i per tot $\sigma \in \Delta, \sigma_n(\sigma(g)) = \sigma(\sigma_n(g)) = \sigma(g^n) = \sigma(g)^n \Rightarrow \sigma(g) \in G$ i, per tant, Δ actua en G. Com que σ_n i σ_p actuen en G elevant-lo a les potències de n i p respectivament, cada $\sigma_m \in \Gamma$ actua elevant $g \in G$ a una certa potència e_m. Aquesta e_m està ben determinada mòdul l'exponent $\exp(G)$ de G (mínim $z \in \mathbb{N} \mid \forall g \in G, g^z = 1$). Aleshores l'aplicació:

$$\begin{array}{ccc} \Gamma & \longrightarrow & (\mathbb{Z}/exp(G)\mathbb{Z})^* \\ \sigma_m & \longrightarrow & e_m \end{array}$$

és un homomorfisme de grups ben definit. Com que H és cíclic, si el seu ordre és s, tenim que per tot $h \in H, h^s = 1$ i, per tant, s divideix l'exponent de G i l'aplicació $\sigma_m \mapsto e_m$ indueix un homomorfisme:

$$\Gamma \longrightarrow (\mathbb{Z}/s\mathbb{Z})^*$$

Si $m \equiv p^i n^j \pmod{r}$, l'aplicació envia $\sigma_m \in \Gamma$ a $e_m \equiv p^i n^j \pmod{s}$.

Sigui $q = n/p$ i considerem els productes $\sigma_p^i \sigma_q^j \in \Gamma$ per $0 \leq i, j \leq [\sqrt{\#\Gamma}]$. Com que $(1 + [\sqrt{\#\Gamma}]) > \#\Gamma$, existeixen com a mínim dos parells ordenats $(i, j) \neq (i', j')$ pels quals $\sigma_p^i \sigma_q^j$ i $\sigma_p^{i'} \sigma_q^{j'}$ són el mateix element de Γ. Aleshores les seves imatges en el grup $(\mathbb{Z}/s\mathbb{Z})^*$ també coincideixen, és a dir, $p^i q^j \equiv p^{i'} q^{j'} \pmod{s}$. Cal veure que $p^i q^j < n^{max(i,j)}$, $p^i q^j = p^i \frac{n^j}{p^j} = p^{i-j} n^j$ i separant en casos:

1. si $i \leq j$, $\quad p^{i-j} n^j \leq n^j = n^{max(i,j)}$.
2. si $j < i$, $\quad p^{i-j} n^j < n^{i-j} n^j = n^i = n^{max(i,j)}$

Proposició. *Es compleix que:*

$$s > n^{[\sqrt{\#\Gamma}]}.$$

Aleshores $n^{max(i,j)} \leq n^{[\sqrt{\#\Gamma}]} < s$. Equivalentment, es pot veure que $p^{i'}q^{j'} < s$ i, per tant, $p^i q^j = p^{i'}q^{j'}$ en $\mathbb{Z}$. Com que $(i,j) \neq (i',j')$ això només és possible si n és una potència de p. Veiem-ho per contrarecíproc.

Si n no és de la forma p^f per algun $f \geq 1$, q factoritza en producte de primers com $q = p^{f_0}q_1^{f_1}\dots q_t^{f_t}$ amb $q_u \neq 1$ per tot $1 \leq u \leq t$ i $q_u \neq q_v$ si $u \neq v$. Aleshores com que $\mathbb{Z}$ és un domini de factorització única, si $(i,j) \neq (i',j')$

$$p^i q^j = p^{(i+f_0^j)}q_1^{f_1^j}\dots q_t^{f_t^j} \neq p^{(i'+f_0^{j'})}q_1^{f_1^{j'}}\dots q_t^{f_t^{j'}} = p^{i'}q^{j'}$$

□

Demostració $s > n^{[\sqrt{\#\Gamma}]}$.

Una primera cota necessària és

$$s \geq \#G^{1/[\Delta:\Gamma]}. \tag{4.1.1}$$

Sigui C un conjunt de representants de les classes laterals del grup quocient Δ/Γ, considerem l'homomorfisme

$$\begin{array}{ccc} G & \longrightarrow & \prod_{i\in C} k^* \\ a & \longrightarrow & (\sigma_i(a)\ (mod\ \mathfrak{m}))_{i\in C} \end{array}$$

Veiem que si $a \in G$ compleix que $\sigma_i(a) = 1$ per alguna i, aleshores $\sigma_{in}(a) = \sigma_i(a^n) = \sigma_i(a)^n = 1$ i d'igual forma $\sigma_{ip}(a) = 1$, és a dir, $\sigma(a) = 1$ per tots els elements σ de la classe lateral de Γ que continguin σ_i. Aleshores, si $a \in G$ té la propietat que $\sigma_i(a) = 1$ per tot $i \in C$, també es compleix que $\sigma_i(a) = 1$ per tot $i \in (\mathbb{Z}/r\mathbb{Z})^*$. Equivalentment, $\sigma_i(a-1) = 0$ per tot $i \in (\mathbb{Z}/r\mathbb{Z})^*$. Escrivint $a-1$ com a $f(\zeta_r)$ per algun polinomi $f(X) \in \mathbb{F}_p[X]$, això implica que $\sigma_i(f(\zeta_r)) = f(\zeta_r^i) = 0$ per tot $i \in (\mathbb{Z}/r\mathbb{Z})^*$. Com que $\Phi_r(X)$ és el polinomi de grau menor anul·lat per ζ_r, $\Phi_r(X)$ divideix $f(X)$ en $\mathbb{F}_p[X]$, és a dir, $a-1 = \Phi_r(\zeta_r)\cdot q(\zeta_r) = 0$ aleshores $a = 1$, i per tant, l'homomorfisme definit prèviament és injectiu.

Com que per cada $i \in C$, la imatge de G en l'aplicació

$$\begin{array}{ccc} G & \longrightarrow & k^* \\ a & \longrightarrow & \sigma_i(a)\ (mod\ \mathfrak{m}) \end{array}$$

és igual a H, la injectivitat de l'homomorfisme implica que $\#G \leq s^{\#C} = s^{[\Delta:\Gamma]}$ i, per tant, $s \geq \#G^{1/[\Delta:\Gamma]}$.

Una segona estimació és que

$$\#G \geq 2^{r-1}. \tag{4.1.2}$$

Primer volem veure que els factors de $\Phi_r(X) = (X^r-1)/(X-1)$ tenen com a mínim grau 2 en l'anell $\mathbb{F}_p[X]$. Suposem que existeix $\alpha \in (\mathbb{Z}/p\mathbb{Z})$ tal que $\Phi_r(\alpha) = 0$, aleshores $\alpha^r = 1$ i com que r és primer, no existeix cap $1 \leq r' < r$ tal que $\alpha^{r'} = 1$. Per tant, α té ordre r a $(\mathbb{Z}/p\mathbb{Z})^* \Rightarrow r|p-1$, que no és possible perquè $p \not\equiv 1 \pmod r$.

Ara veiem que els elements $\zeta_r + j$ per tot $0 \leq j < r-1$ no estan continguts en cap ideal maximal $\mathfrak{m}$ de l'anell A. Si $\zeta_r + j \in \mathfrak{m} \Rightarrow \overline{\zeta_r + j} = \overline{0}$ en $A/\mathfrak{m} \Rightarrow \overline{\zeta_r} = \overline{-j}$ en $A/\mathfrak{m} \cong \mathbb{F}_{p^f}$.

Aleshores $\Phi_r(\overline{-j}) = \Phi_r(\overline{\zeta_r}) = \overline{0}$, però $\Phi_r(\overline{-j}) \in \mathbb{F}_p \cong (\mathbb{Z}/p\mathbb{Z})$ i ja hem vist que $\Phi_r(X)$ no té arrels a $(\mathbb{Z}/p\mathbb{Z})$. Com que tots els elements $\zeta_r + j$ no estan continguts en ideals maximals de A, són unitats de A, i per la condició (3.) del teorema, per cada subconjunt $J \subset \{0, 1, \ldots, r-2\}$ l'element

$$\prod_{j \in J} (\zeta_r + j)$$

pertany a G.

Tots aquests elements són diferents. De fet, com que el polinomi ciclotòmic $\Phi_r(X)$ té grau $r-1$, els dos únics elements que podrien coincidir són els dels casos corresponents a $J = \{0, 1, \ldots, r-2\}$ i $J = \emptyset$. Perquè això passi cal que $\prod_{j=0}^{r-2}(X+j) = 1$ en $\mathbb{F}_p[X]$, és a dir, cal que $\Phi_r(X)$ divideixi $\prod_{j=0}^{r-2}(X+j) - 1$. Com que els dos polinomis són mònics del mateix grau, cal que siguin iguals. Veient que el terme constant de $\prod_{j=0}^{r-2}(X+j) - 1$ és -1 i el terme constant de $\Phi_r(X)$ és 1, aquests polinomis només poden ser iguals si $p = 2$, però això és impossible, doncs p divideix n i n és senar.

Com que hi ha 2^{r-1} subconjunts de $J \subset \{0, 1, \ldots, r-2\}$, queda clar que $\#G \geq 2^{r-1}$.

L'última cota necessària és

$$2^{\#\Gamma} > n^{\sqrt{\#\Gamma}}. \tag{4.1.3}$$

o equivalentment $\#\Gamma > (\log n / \log 2)^2$. Que s'obté del fet que $\sigma_n \in \Gamma$ té ordre més gran que $(\log n / \log 2)^2$, ja que l'ordre de σ_n és igual a l'ordre de n, que per la condició (2.) del teorema és superior a $(\log\ n / \log 2)^2$.

Combinant les desigualtats (4.1.1), (4.1.2) i (4.1.3) anteriors es conclou:

$$s \geq \#G^{1/[\Delta:\Gamma]} \geq 2^{(r-1)/[\Delta:\Gamma]} = 2^{(r-1)/(\#\Delta/\#\Gamma)} = 2^{\#\Gamma} > n^{\sqrt{\#\Gamma}} \geq n^{[\sqrt{\#\Gamma}]}.$$

□

4.2 Algorisme AKS

Algorisme 4.2.1. *Sigui $n > 1$ un nombre enter positiu.*

1. *Primer comprovar que n no és una potència d'un enter.*
2. *Provant successivament $r = 2, 3, \ldots,$ determinar el nombre primer r més petit que no divideixi n ni cap dels nombres $n^i - 1$ per $1 \leq i \leq (\log n / \log 2)^2$.*
3. *Per tot $0 \leq j \leq r-1$ comprovar que $(\zeta_r + j)^n = \zeta_r^n + j$ a l'anell $\mathbb{Z}[\zeta_r]/(n)$.*

Si n no passa el test és un nombre compost. Si el passa és un nombre primer.

Cal comprovar que l'algorisme és correcte:

Si n és primer, a $\mathbb{Z}[\zeta_r]/(n)$, $(\zeta_r + j)^n = \zeta_r^n + j^n$ i pel teorema petit de Fermat (p *primer*, $a \in \mathbb{N} \Rightarrow a^p = a \pmod p$), $\zeta_r^n + j^n = \zeta_r^n + j$, per tant, n passa el test.

Si n passa el test, comprovem les condicions del Teorema 4.1.1. Per definició de r, el nombre n no té divisors $\leq r$ i es compleix la primera condició del teorema. Com que r no divideix cap dels nombres $n^i - 1$ per $1 \leq i \leq (\log n / \log 2)^2$, l'ordre de n mòdul r excedeix $(\log n / \log 2)^2$ i es compleix la segona condició del teorema. Finalment, el tercer pas de

l'algorisme és equivalent a la tercera condició del teorema. Per tant, deduïm del teorema que n és la potència d'un primer, però com que n ha passat el primer pas de l'algorisme, n ha de ser primer.

4.3 Complexitat de l'algorisme

Ara anem a realitzar l'estudi de la complexitat de l'algorisme per verificar que, efectivament, el problema de la primeritat està en P. És a dir, que l'algorisme resol el problema en temps polinomial respecte al nombre de dígits. Com que en base decimal podem expressar n amb $\log(n)$ dígits, volem que l'algorisme determini si n és primer o compost amb complexitat $O(\log^k(n))$ amb $k \in \mathbb{N}$.

Abans de res introduïm unes definicions i proposicions que necessitarem per acotar la r de l'algorisme.

Definició 4.3.1. *Per tot primer $p \leq x$ definim la funció*

$$\theta(x) = \sum_{p \leq x} \log p = \log(\prod_{p \leq x} p),$$

i la funció

$$\psi(x) = \sum_{p^i \leq x} \log p = \log(\prod_{p^i \leq x} p).$$

[8]

Proposició 4.3.2. *Existeix una constant $a > 0$ tal que $\psi(x) > ax$.*

Demostració. El conjunt $\{1, 2, \cdots, n\}$ només inclou $[n/p]$ múltiples de p, $[n/p^2]$ múltiples de p^2, i així successivament. Per això

$$n! = \prod_p p^{j(n,p)}, \tag{4.3.1}$$

on

$$j(n,p) = \sum_{m \geq 1} [\frac{n}{p^m}].$$

Definim

$$N = \frac{2n!}{n!} = \prod_{p \leq 2n} p^{k_p},$$

i de la igualtat (4.3.1) deduim que

$$k_p = \sum_{m=1}^{\infty} ([\frac{2n}{p^m}] - 2[\frac{n}{p^m}]).$$

Cada un dels termes del sumatori és 1 o 0 en funció de si $[\frac{2n}{p^m}]$ és senar o parell respectivament. A més a més tots els termes valen 0 quan $p^m > 2n$ o equivalentment $m > [\frac{\log 2}{\log p}]$. Per tant

$$k_p \leq [\frac{\log 2}{\log p}].$$

Ara veiem que

$$\log N = \sum_{p \leq 2n} k_p \log p \leq \sum_{p \leq 2n} [\frac{\log 2}{\log p}] \log p = \sum_{p^m \leq 2n} \log p,$$

I també veiem que

$$N = \frac{2n!}{n!} = \frac{n+1}{1} \cdot \frac{n+2}{2} \cdot \ldots \cdot 2nn \geq 2^n,$$

i, per tant, $\sum_{p^m \leq 2n} \log p \geq n \log 2$. Per $x \geq 2$ podem pendre $n = [x/2] \geq 1$ i tenim

$$\sum_{p^m \leq x} \log p = \sum_{p^m \leq 2n} \log p \geq 2 \log 2 \geq \frac{1}{4} x \log 2.$$

□

Proposició 4.3.3. *Existeix una constant $a > 0$ tal que $\theta(x) > ax$.*

Demostració. Com que les desigualtats $p^2 \leq x$, $p^3 \leq x$,... són equivalents a $p \leq x^{1/2}$, $p \leq x^{1/3}$,... tenim que

$$\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \cdots = \theta(x) + \sum_{m \geq 2} \theta(x^{1/m}).$$

Veiem que els sumands del sumatori valen 0 quan $x^{1/m} < 2$, és a dir, quan $m > [\log x / \log 2]$. De la definició de θ veiem que $\theta(x) < x \log x$ per tot $x \geq 2$. I, per tant,

$$\sum_{m \geq 2} \theta(x^{1/m}) < \sum_{m \geq 2} x^{1/m} \log x \leq \frac{\log x}{\log 2} x^{1/2} \log x.$$

És a dir,

$$\psi(x) = \theta(x) + O(x^{1/2} (\log x)^2).$$

Per la Proposició 4.3.2 tenim que

$$\theta(x) > Ax - B(x^{1/2}(\log x)^2) \text{ per unes constants } A > 0, B > 0.$$

Definim $f(x) = (Ax - B(x^{1/2}(\log x)^2))/x$. Prenem un a tal que $0 < a < A$ i com que $\lim_{x \to \infty} f(x) = A$ existeix $x_0 > 0$ tal que $f(x) > a$ si $x > x_0$. És a dir, $Ax - B(x^{1/2}(\log x)^2) > ax$ si $x > x_0$. Ara considerem la funció $\theta(x)/x$ a l'interval $[2, x_0]$, com que és tancat i acotat i la funció és sempre positiva a l'interval, existeix un mínim $b > 0$ de la funció a l'interval. Per tant, $\theta(x) > bx$ per tot $x \in [2, x_0]$, i en conseqüència, $\theta(x) > \min(a, b)x$ per tot $x \in [2, \infty)$. □

Ara calculem les complexitats de cada un dels passos de l'algorisme. El primer pas consisteix a veure que n no és potència d'un primer. Així doncs, comprovem que $\sqrt[m]{n}$ no pertany a $\mathbb{Z}$ per tot m entre 2 i $\log n / \log 2$. Ja que $\log n / \log 2 > \sqrt{n}$. Utilitzant el mètode de Newton podem calcular $\sqrt[m]{n}$ amb la iteració

$$x \mapsto x - \frac{x^m - n}{m x^{m-1}}.$$

Com que el mètode de Newton té un ordre de convergència quadràtic en tenim prou amb realitzar $\log n$ iteracions [13]. En cada iteració cal fer m multiplicacions i una divisió. Per tant, la complexitat de veure si $\sqrt[m]{n} \in \mathbb{Z}$ és

$$O(\log n \cdot (m+1)(\log n)^2) = O(m(\log n)^3).$$

Com que $m < \log n / \log 2$ tenim que $O(m(\log n)^3) < O(\log^4 n)$. Finalment, cal utilitzar el mètode de Newton per $m = 2, \ldots, \log n / \log 2$ i això ens dona una complexitat total del primer pas de $O(\log^5 n)$.

En el segon pas, hem de trobar el menor primer r que no divideixi n ni cap dels nombres $n^i - 1$ per $1 \leq i \leq (\log n / \log 2)^2$. Equivalentment, podem comprovar que n^i no és congruent amb 1 (mod r). Per tant, hem de fer r vegades $[\log n / \log 2]^2$ multiplicacions mòdul r. Aleshores la complexitat d'aquest pas és

$$O(r \cdot [\log n / \log 2]^2 \cdot \log^2 r) = O(r \log^2 n \log^2 r) = O(r(\log r \log n)^2).$$

En el tercer pas de l'algorisme hem d'elevar a la potència de n diversos elements, r vegades. Per elevar un nombre a la potència de n utilitzem l'algorisme de l'exponenciació binària 1.3.2. I, per tant, hem de realitzar r vegades $O(\log(n))$ multiplicacions en l'anell $\mathbb{Z}[\zeta_r]/(n)$. Aquest anell és isomorf a $\mathbb{Z}[X]/(\Phi_r(X), n)$ els elements dels quals, tenen r coeficients de $\log(n)$ dígits. Com que la complexitat que utilitzem pel producte de nombres de t dígits és $O(t^2)$ tenim que la complexitat total del pas és

$$O(r \cdot \log(n) \cdot (r \log(n))^2) = O((r \log(n))^3). \tag{4.3.2}$$

Com que l'ordre de n mòdul r és més gran que $(\log n / \log 2)^2$ tenim que $r > (\log n / \log 2)^2$ i en conseqüència el tercer pas de l'algorisme és el que té una complexitat més alta.

Com que la complexitat de l'algorisme depèn de la mida de r, cal fer-ne una estimació. Tal com hem definit r, sabem que el producte $n \prod_i (n^i - 1)$ on $i \leq (\log n / \log 2)^2$ és divisible per tots els primers $l < r$. Per tant, podem pendre les següents desigualtats

$$\prod_{l<r} l < n \prod_i (n^i - 1) \leq n \prod_i n^i.$$

I aplicant el logaritme als dos costats obtenim

$$\sum_{l<r} \log l \leq \log n + \sum_{i=1}^{(\frac{\log n}{\log 2})^2} i \log n = \log n + \log n \sum_{i=1}^{(\frac{\log n}{\log 2})^2} i = O(\log^5 n). \tag{4.3.3}$$

Utilitzant la Proposició 4.3.3 veiem que $\sum_{l<r} \log l > ar$ per una constant $a > 0$ i, per tant, tenim de l'equació (4.3.3) que $r = O(\log^5 n)$.

Finalment, obtenim de (4.3.2) que la complexitat total de l'algorisme AKS és

$$O((\log^5 n \cdot \log n)^3) = O((\log^6 n)^3) = O(\log^{18} n).$$

Cal destacar que l'objectiu d'aquesta secció era veure com efectivament el problema de la primeritat estava en P, és a dir, comprovar que l'algorisme requereix una complexitat polinòmica respecte al nombre de dígits. És per això que alguns dels passos descrits poden realitzar-se amb una complexitat inferior a la mostrada. Per exemple, tal com hem comentat a la Secció 1.3, hi ha mètodes per realitzar la multiplicació de nombres de t dígits amb una complexitat inferior a $O(t^2)$.

Conclusions

En les conclusions d'aquest treball farem un breu resum de la memòria, destacant els aspectes més importants de cada capítol.

Com no podia ser d'altra manera, aquest treball ha començat amb l'estudi de complexitats algorísmiques, ja que un dels aspectes més rellevants a tenir en compte dels testos de primeritat és la seva complexitat. Hem introduït les operacions elementals i hem explicat com comptabilitzar-les amb cotes de complexitat. També hem proposat cotes de complexitat de les operacions més recurrents en els algorismes, que ens han permès calcular les complexitats d'aquests més endavant.

En el capítol del test de Miller-Rabin, hem enunciat i demostrat el teorema en el qual es basa; comprovant com, efectivament, la probabilitat d'error del test és inferior al 25%. També hem vist que la complexitat d'aquest test és de $O(\log(n)^3)$ permetent utilitzar-lo a nivell pràctic.

Abans d'introduir el segon test del treball, hem parlat dels cossos ciclotòmics. Aquest capítol partia d'assumir els conceptes que s'expliquen a l'assignatura d'equacions algebraiques, al grau de matemàtiques, i ens ha servit per familiaritzar-nos amb estructures algebraiques que hem vist en el test AKS. Hem introduït el concepte de cos de nombres; definint les seves normes, els seus anells d'enters i els discriminants. També hem parlat dels ideals en anells d'enters i hem enunciat el teorema fonamental de l'aritmètica. Finalment, hem parlat dels cossos ciclotòmics, i utilitzant les nocions anteriors, hem demostrat que si p és primer, l'anell d'enters del cos generat per una arrel p^r-èssima primitiva de la unitat ζ sobre $\mathbb{Q}$ és $\mathbb{Z}[\zeta]$.

En l'últim capítol, el del test AKS, hem presentat el teorema en el qual està basat i hem vist la seva demostració, Hem presentat l'algorisme i la prova que funciona correctament. I finalment, hem calculat la seva complexitat, comprovant com el problema de la primeritat està en P, és a dir, es pot resoldre en temps polinòmic respecte el nombre de dígits.

Bibliografia

[1] Manindra Agrawal, Neeraj Kayal i Nitin Saxena. ?PRIMES is in P? A: *Ann. of Math. (2)* 160.2 (2004), pàg. 781 - 793. ISSN: 0003-486X. DOI: 10.4007/annals.2004.160.781. URL: https://doi-org.sire.ub.edu/10.4007/annals.2004.160.781.

[2] Robert B. Ash. *A course in algebraic number theory*. Dover Publications, Inc., Mineola, NY, 2010, pàg. viii+112.

[3] Frits Beukers. *Algebraic number theory*. Febr. de 2011. URL: https://www.math.leidenuniv.nl/~evertse/dio2011-algnumbers.pdf.

[4] Richard Crandall i Carl Pomerance. *Prime numbers a computational perspective*. Springer Science+Business Media, Inc., 2000, pàg. 604. ISBN: 978-0387-25282-7.

[5] Fred Diamond i Jerry Shurman. *A first course in modular forms*. Vol. 228. Graduate Texts in Mathematics. Springer-Verlag, New York, 2005, pàg. xvi+436. ISBN: 0-387-23229-X.

[6] *Exponenciació binària*. URL: https://ca.wikipedia.org/wiki/Exponenciaci%C3%B3_bin%C3%A0ria.

[7] Rosa Guerequeta i Antonio Vallecillo. *Técnicas de Diseño de Algoritmos*. Servicio de Publicaciones de la Universidad de Málaga., 1998, pàg. 326. ISBN: 84-7496-666-3. URL: http://190.57.147.202:90/jspui/bitstream/123456789/451/1/tecnicas_de_diseno_de_algoritmos.pdf.

[8] G. H. Hardy i E. M. Wright. *An introduction to the theory of numbers*. Fourth. Oxford University Press, Ely House, London W. 1, 1960, pàg. xvi+426. ISBN: 0-19-853310-7.

[9] Jose A. Manas. *Análisis de algoritmos - complejidad*. Febr. de 2017. URL: https://www.dit.upm.es/~pepe/doc/adsw/tema1/Complejidad.pdf.

[10] Gary L. Miller. ?Riemann's hypothesis and tests for primality? A: *J. Comput. System Sci.* 13.3 (1976), pàg. 300 - 317. ISSN: 0022-0000. DOI: 10.1016/S0022-0000(76)80043-8. URL: https://doi-org.sire.ub.edu/10.1016/S0022-0000(76)80043-8.

[11] Michael O. Rabin. ?Probabilistic algorithm for testing primality? A: *J. Number Theory* 12.1 (1980), pàg. 128 - 138. ISSN: 0022-314X. DOI: 10.1016/0022-314X(80)90084-0. URL: https://doi-org.sire.ub.edu/10.1016/0022-314X(80)90084-0.

[12] René Schoof. ?Four primality testing algorithms? A: *Algorithmic number theory: lattices, number fields, curves and cryptography*. Vol. 44. Math. Sci. Res. Inst. Publ. Cambridge Univ. Press, Cambridge, 2008, pàg. 101 - 126.

[13] Eric W. Weisstein. *Newton's Method*. URL: https://mathworld.wolfram.com/NewtonsMethod.html.