Temes diversos de

FONAMENTS DE LES MATEMÀTIQUES

Agustí Reventós

2014-15
2015-16
2016-17

Índex

Tema 1

Programa de l'assignatura

Aquesta[1] assignatura consta d'unes 40 hores de classe de teoria que intentarem distribuir aproximadament així.

Introducció

01. Introducció històrica. Situar en el temps els diversos resultats que apareixeran aquest curs: Euclides, Pascal, Fermat, Gauss, etc. [*Tema 2*].

02. Primeres proposicions dels *Elements*. Error visual en aplicar el criteri CCC. [*Tema 2*].

03. Pitàgores. Triangles semblants. Solució amb regle i compàs de l'equació de segon grau $x^2 - px + q = 0$. [*Tema 2*].
Càlcul de $\cos \frac{2\pi}{5}$. [10].

Teoria de Conjunts i Lògica Matemàtica

04. Teoria de conjunts. Unió i intersecció de conjunts. [1].

05. Teoria axiomàtica de conjunts. Paradoxa de Rusell. [*Tema 3*].

06. Axiomes de Peano. Inducció. [*Tema 3*].

07. Lògica matemàtica. [*Tema 4*].

08. Lògica matemàtica. [*Tema 4*].

09. Aplicacions entre conjunts. [1].

10. Aplicacions bijectives. [1].

[1] Una part d'aquests apunts els vaig escriure durant el curs 2014-15; les altres parts les vaig escriure el curs següent, a partir dels apunts del meu primer curs de Nuria Agulló, a qui agraeixo la gentilesa.

Permutacions

11. Permutacions. [*Tema 5*].

12. Descomposició en cicles disjunts. Ordre d'una permutació. [*Tema 5*].

13. Descomposició en producte de transposicions. Signe. [*Tema 5*].

14. El grup simètric S_4. [*Tema 7*].

Conjunt Quocient

15. Classes d'equivalència. [*Tema 8*].

16. Conjunt quocient. [*Tema 8*].

17. Construcció de $\mathbb{Z}$. Criteri de divisibilitat d'Euclides. [*Tema 8*].

18. Construcció de $\mathbb{Z}/(m)$. Grup, anell, i cos. [*Tema 8*].

19. Construcció de $\mathbb{Q}$. Notació decimal. [*Tema 8*].

Numerabilitat i Combinatòria

20. Numerabilitat. [1].

21. Combinatòria. [*Tema 9*].

22. Principi d'inclusió-exclusió. El problema dels desordres. [*Tema 9*].

Nombres Enters

23. m.c.d. i m.c.m. en llenguatge d'ideals. Identitat de Bézout. [*Tema 10*].

24. $\mathbb{Z}/(m)$, amb m primer, és un cos. Algorisme d'Euclides. [*Tema 10*].

25. Teorema fonamental de l'aritmètica. Infinits primers. [*Tema 10*].

Presentació en societat de la funció zeta de Riemann. [*Tema 2*].

26. Equacions diofàntiques. [*Tema 11*].

27. Petit teorema de Fermat. [*Tema 11*].

Nombre de xifres del període de $\frac{1}{p}$. [*Tema 11*].

28. La funció ϕ d'Euler. Congruència d'Euler. [*Tema 11*].

Sumes esteses als divisors d'un nombre. [*Tema 16*].

29. Teorema xinès del residu. Versió per a anells:

$$\mathbb{Z}/(M) \equiv \mathbb{Z}/(m_1) \times \cdots \times \mathbb{Z}/(m_k)$$

[*Tema 11*].

Polinomis

30. $\mathbb{C}$.

31. L'anell de polinomis $K[x]$. Fórmula del grau. $K[x]$ és domini d'integritat. $K[x]$ és anell Euclidià. [*Tema 13*].

32. Tots els ideals de $K[x]$ són principals. m.c.d. i m.c.m. de polinomis. Algorisme d'Euclides a $K[x]$. [*Tema 13*].

33. Polinomis irreductibles. Descomposició d'un polinomi com producte d'irreductibles. Zeros de polinomis. Ruffini. Irreductibles sobre $\mathbb{R}[x]$ i $\mathbb{C}[x]$. [*Tema 13*].

34. Arrels racionals de polinomis a coeficients enters. $K[x]/(p(x))$. [10].

35. Arrels múltiples. Un polinomi amb coeficients racionals, irreductible, no té arrels múltiples a $\mathbb{C}$. [1].

36. Irreductibles a $\mathbb{Z}/(p)$. [1], [10].

Temes Complementaris

37. Solució de la cúbica a *Ars Magna*. [*Tema 2*].

38. Sumes esteses als divisors d'un nombre. [*Tema 16*].

39. El sisè nombre de Fermat. [*Tema 15*].

40. Gauss i el polígon de 17 costats. [11].

41. Criteri d'Eisenstein. [*Tema 17*].

42. $\pi \notin \mathbb{Q}$. [*Tema 14*].

43. Polinomis simètrics. [*Tema 18*].

Tema 2

Introducció Històrica

Sense pretendre fer ara un capítol d'història de la matemàtica donarem només unes quantes referències històriques per centrar en el temps alguns dels resultats que apareixeran en aquesta assignatura al llarg del curs.

2.1 300 a.C. Euclides

A l'època d'Euclides, uns 300 anys abans de Crist, eren molts els resultats coneguts de geometria. A més, els grecs tenien prou clar què volia dir demostrar un resultat o teorema. Volia dir deduir-lo de resultats ja coneguts per raonaments lògics. Ara bé, aquests resultats ja coneguts, com s'havien demostrat? Doncs també a partir de resultats coneguts i raonaments lògics. Però i aquests resultats, com s'havien demostrat? Ja es veu la necessitat imperiosa que va tenir Euclides de buscar un inici a aquesta cadena de resultats uns lligats als altres, i anar molt en compte no fos cas que un resultat A es basés en un resultat B el qual es basés per la seva part en A arribant així a un cercle viciós o petició de principi, que hagués fet trontollar l'edifici de les matemàtiques.

Euclides, a la seva gran obra *Els Elements*, va voler ser molt rigorós i per això va donar un començament d'aquesta cadena de resultats, format aquest començament forçosament per resultats no demostrables, i va voler donar també una manera precisa d'anar passant d'un resultat a l'altre expressant de manera clara què entenia per *raonaments lògics*.

Concretament va donar 23 definicions, 5 nocions comunes, i els 5 postulats. Les definicions venien a ser com una descripció dels objectes que s'anaven a utilitzar, les nocions comunes eren les normes de la lògica i els postulats l'inici de la cadena.

Recordem-les.

Definicions

1. Un *punt* és allò que no té parts.
2. Una *línia* és una longitud sense amplada.
3. Les extremitats d'una línia són punts.
4. Una *línia recta* és una línia igualment distribuïda respecte els seus punts.
5. Una *superfície* és allò que té longitud i amplada únicament.
6. Les extremitats d'una superfície són línies.
7. Una *superfície plana* és una superfície igualment distribuïda respecte les seves línies rectes.
8. Un *angle pla* és la inclinació d'una respecte l'altra de dues línies en un pla que es tallen i no pertanyen a la mateixa línia recta.
9. I quan les línies que formen l'angle són línies rectes, l'angle es diu *rectilini*.
10. Quan una línia recta recolzada en una altra línia recta forma angles adjacents iguals, cadascun d'aquests angles es diu *recte*, i la línia recta recolzada en l'altra es diu *perpendicular* a aquesta.
11. Un angle *obtús* és un angle major que un angle recte.
12. Un angle *agut* és un angle menor que un angle recte.
13. Una *bora* és allò que és extremitat d'alguna cosa.
14. Una *figura* és allò contingut per una bora o bores.
15. Un *cercle* és una figura plana continguda per una línia tal que totes les línies rectes que surten cap a ella a partir d'un punt de la figura són iguals entre ells.
16. I el punt es diu el *centre* del cercle.
17. Un *diàmetre* del cercle és qualsevol línia recta dibuixada a través del centre i acabada en ambdues direccions per la circumferència del cercle, i una tal línia recta també biseca el cercle.
18. Un *semicercle* és la figura continguda pel diàmetre i la circumferència tallada per ell. I el centre del semicercle és el mateix que el centre del cercle.

19. *Figures rectilínies* són aquelles que estan contingudes per línies rectes, sent les figures *trilaterals* les contingudes per tres, *quadrilaterals* les contingudes per quatre, i *multilaterals* aquelles contingudes per més de quatre línies rectes.

20. D'entre les figures trilaterals, un *triangle equilàter* és aquell que té els tres costats iguals, un *triangle isòsceles* és aquell que té únicament dos costats iguals, i un *triangle escalè* és aquell que té els tres costats diferents.

21. A més, d'entre les figures trilaterals, un *triangle rectangle* és aquell que té un angle recte, un *triangle obtusangle* és aquell que té un angle obtús, i un *triangle acutangle* és aquell que té els tres angles aguts.

22. D'entre les figures quadrilaterals, un *quadrat* és la que és a la vegada equilateral i rectangle; un *rectangle* és la que és rectangle però no equilateral; un *rombe* és la que és equilateral però no rectangle; un *romboide* és la que té els costats i angles oposats iguals entre ells però no és ni equilateral ni rectangle. I els demés quadrilaterals es diran *trapezis*.

23. Línies *paral·leles* són aquelles que, estan en el mateix pla i prolongades indefinidament en els dos costats, no es tallen en cap direcció.

Nocions comunes

1. Coses iguals a una mateixa cosa són iguals entre elles.

2. Si iguals s'afegeixen a iguals els totals són iguals.

3. Si iguals es sostreuen d'iguals els restes són iguals.

4. Coses que coincideixen amb una altra són iguals a ella.

5. El total és major que la part.

Postulats

1. Podem dibuixar línies rectes des de qualsevol punt a qualsevol punt.

2. Podem prolongar una línia recta finita contínuament a una línia recta.

3. Podem descriure un cercle amb qualsevol centre i distància.

4. Tots els angles rectes són iguals.

5. Si una línia recta és tallada per dues línies rectes de manera que els angles interiors del mateix costat sumin menys de dos rectes, i si aquestes dues línies rectes es prolonguen indefinidament, llavors es tallen en el costat on estan aquests angles que sumen menys de dos rectes.

Els tres primers postulats diuen únicament que tenim un regle i un compàs. El quart postulat fa referència al problema del moviment i el cinquè és el famós postulat de les paral·leles i diu essencialment que *per un punt exterior a una recta hi passa una única paral.lela.* La dificultat ve de la unicitat no de l'existència.

Proposicions dels Elements

Reproduïm els enunciats de les primeres Proposicions dels Elements. Al llibre I n'hi ha 47.

Proposició 1. *Sobre una línia recta finita construir un triangle equilàter.*

Proposició 2. *Situar en un punt donat (com extrem) un segment igual a un de donat.*

Proposició 3. *Donats dos segments diferents, tallar del gran un segment igual al petit.*

Proposició 4 (CAC)**.** *Si dos triangles tenen dos costats respectius iguals, i tenen els angles compresos iguals, aleshores també tenen les bases iguals, els triangles són iguals, i els angles restants són iguals, concretament els oposats als costats iguals.*

Proposició 5 (Isòsceles)**.** *En triangles isòscels els angles en la base són iguals entre ells, i si els costats iguals s'allarguen, els angles sota la base són iguals.*

Proposició 6 (Isòsceles)**.** *Si en un triangle dos angles són iguals, aleshores els costats oposats als angles iguals també són iguals.*

Proposició 7. *Donats dos segments construïts des dels extrems d´un segment i convergents en un punt, no poden construir-se des dels extrems del mateix segment, i pel mateix costat, uns altres dos segments que es trobin en un altre punt i siguin iguals als dos segments, concretament iguals als que parteixen del mateix extrem.*

Proposició 8 (CCC)**.** *Si dos triangles tenen dos costats respectius iguals, i també tenen la base igual, aleshores també tenen iguals els angles compresos pels segments iguals.*

Proposició 9. *Bisecar un angle donat.*

Proposició 10. *Bisecar un segment donat*

Proposició 11. *Dibuixar una perpendicular a una recta donada des d'un punt d'aquesta recta.*

Proposició 12. *Dibuixar*[1] *una perpendicular a una recta donada per un punt exterior a ella.*

Proposició 13. *Si una recta s'aixeca sobre una altra, es generen o dos angles rectes o angles que sumen dos angles rectes.*

Proposició 14. *Si amb una recta i un punt a sobre d'ella, dos segments que no estan en el mateix costat produeixen angles adjacents que sumen dos angles rectes, aleshores els dos segments estan en línia recta l'un amb l'altre.*

Proposició 15. *Angles oposats pel vèrtex són iguals.*

Proposició 16. *Tot angle exterior d'un triangle és més gran que cadascun dels angles interiors no adjacents.*

Proposició 17. *En qualsevol triangle, la suma de dos angles és menor que dos angles rectes.*

Proposició 18. *En tot triangle, a major costat li correspon major angle.*

Proposició 19. *En tot triangle, a major angle li correspon major costat.*

Proposició 20. (Desigualtat triangular) *Cada costat d'un triangle és més petit que la suma dels altres dos i major que la diferència.*

El criteri angle-costat-angle apareix a la Proposició 26.

Proposició 26 (ACA)**.** *Si dos triangles tenen dos angles iguals dos a dos i un costat igual, concretament el que connecta els dos angles iguals, llavors tenen els altres angles i costats també iguals.*

Proposició 27. *27 Si una recta talla a dues rectes de manera que els angles alterns són iguals entre ells, aquestes dues rectes són paral·leles.*

A la Proposició 29 apareix per primer cop el cinquè postulat.

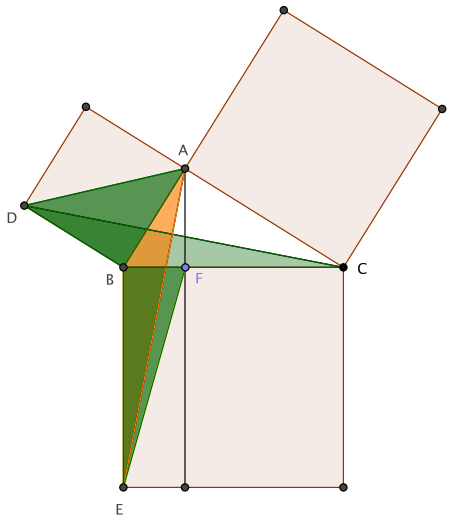
Proposició 29. *Si una recta talla dues línies paral·leles els angles alterns resultants són iguals entre ells.*

Proposició 32. *La suma dels angles d'un triangle és igual a dos angles rectes.*

Proposició 47. *Teorema de Pitàgores.*

La demostració d'Euclides es basa en aquest dibuix.

[1] Vegeu aquesta i altres construccions elementals, com ara la solució de l'equació de segon grau, a [11].



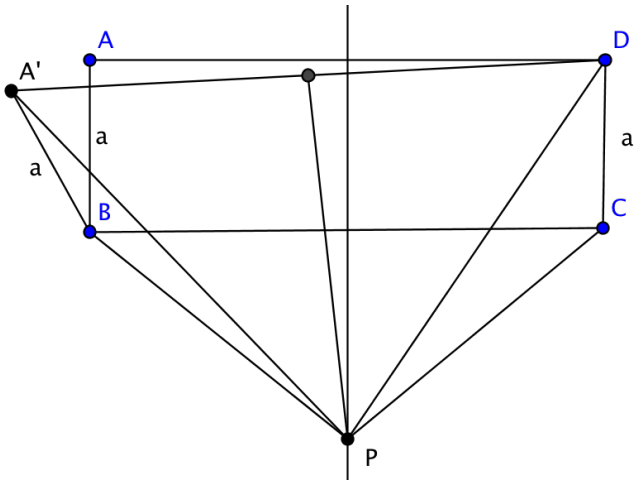
L'àrea del triangle $\triangle BDA$ és igual a l'àrea del triangle $\triangle BDC$ per tenir la mateixa base i la mateixa altura.

L'àrea del triangle $\triangle BDC$ és igual a l'àrea del triangle $\triangle BAE$ pel criteri CCC.

L'àrea del triangle $\triangle BAE$ és igual a l'àrea del triangle $\triangle BFE$ per tenir la mateixa base i la mateixa altura.

Això implica que l'àrea del quadrat sobre el catet AB és igual a l'àrea del rectangle de costats BE i BF. Fent el mateix argument sobre el costat AC tenim el resultat.

Atenció amb els dibuixos, mireu com el criteri CCC pot portar a pensar que un angle recte és obtús.

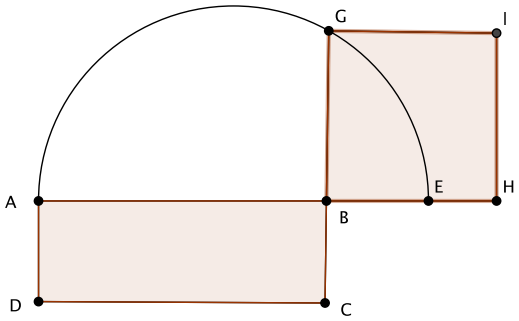


Començant amb el rectangle $ABCD$, girem el costat BA fins BA'. En particular tenim $AB = A'B = CD = a$. Les mediatrius de AD i $A'D$ es

tallen en P. Els triangles $\triangle PCD$ i $\triangle PBA'$ són iguals, pel criteri CCC i la propietat bàsica de la mediatriu. En particular $\angle DCP = \angle A'BP$, que porta a contradicció ja que $\angle PBC = \angle PCB$ ...

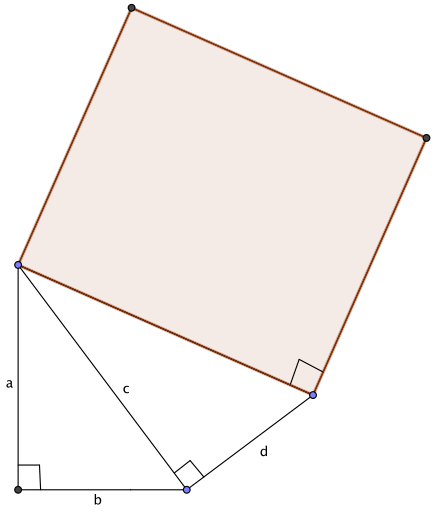
2.2 Quadratures

En el molt bon llibre [3] podeu trobar la quadratura del rectangle, de qualsevol polígon i de la lúnula d'Hipòcrates de Quios. Per quadrar el rectangle només hem de conèixer el teorema de l'altura.



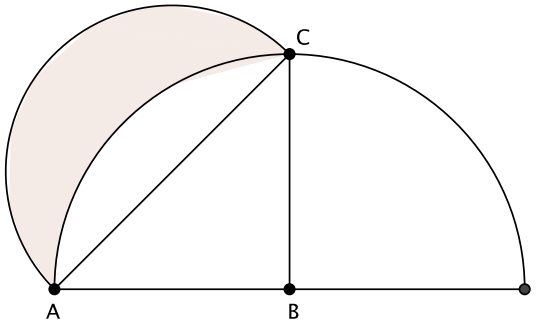
Sobre el costat AB es construeix el segment BE tal que $BE = BC$. A continuació es construeix el semicercle de diàmetre AE. La perpendicular a AB per B talla el semicercle en un punt G tal que BG és el costat d'un quadrat $BGIH$ que té la mateixa àrea que el rectangle donat.

Per quadrar un polígon només hem de pensar que es pot dividir en triangles, els quals es poden quadrar un per un, i després sumar quadrats segons la figura següent.



El quadrat gran té àrea $a^2 + b^2 + d^2$.

I la lúnula d'Hipòcrates és la de la figura següent.



Si diem L a l'àrea de la lúnula, $R = AB$ el radi del semicercle gran, i $\rho = \frac{AC}{2} = \frac{\sqrt{2R^2}}{2}$ el radi del semicercle petit tenim

$$L = \frac{\pi\rho^2}{2} - (\frac{\pi R^2}{4} - T) = T.$$

Com sabem quadrar triangles (només hem de construir el rectangle que té la mateixa base que el triangle i la meitat de l'altura) hem acabat.

Els altres llibres dels Elements

Resumim breument el contingut dels 13 llibres dels Elements[2].

1. Els fonaments de la geometria: Teoria dels triangles, paral·leles i àrea.
2. Àlgebra geomètrica.
3. Teoria de la circumferència.
4. Figures inscrites i circumscrites.
5. Teoria de les proporcions abstractes.
6. Figures geomètriques semblants i proporcionals.
7. Fonaments de la teoria dels nombres.
8. Continuació de proporcions a la teoria de nombres.
9. Teoria dels nombres.
10. Classificació dels incommensurables.
11. Geometria dels sòlids.
12. Mesurament de figures.

[2]Vegeu http://www.euclides.org/menu/elements_cat/indexeuclides.htm#Llibre%2011.

13. Sòlids regulars.

La Proposició 5 del llibre 6 diu

Proposició. Si dos triangles tenen els costats proporcionals, els triangles seran equiangles i tindran iguals els angles els quals subtendeixen els costats corresponents.

Observeu que la geometria elemental us ha permès calcular els sinus i cosinus d'alguns angles, concretament $\pi/4, \pi/6, \pi/3$, utilitzant propietats del triangle. Anàlogament, utilitzant geometria elemental, concretament la Proposició sobre triangles semblants que acabem de comentar, i les propietats del pentàgon, podem calcular, per exemple, $\cos(\pi/5)$ (vegeu el problema 7 de la meva llista de problemes resolts, [10]).

Però no oblideu que el calcul del cosinus d'un angle és molt difícl en general i es basa en la fórmula que veureu en els cursos d'Anàlisi

$$\cos x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!}, \quad \sin x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}.$$

En aquesta fórmula és fonamental que $\cos x$ vulgui dir el cosinus d'un angle que mesura x radians!

Construccions elementals amb regle i compàs

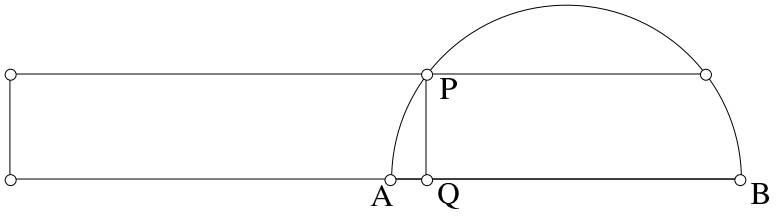
Em refereixo a construir bisectrius, mediatrius, perpendiculars, arrels quadrades, etc. Les podeu trobar a molts llocs, per exemple, a [11].

A partir de l'arrel quadrada podem construir les *arrels de l'equació de segon grau*

$$x^2 - qx + p = 0; \qquad p, q \in \mathbb{R}^+$$

suposat p, q construïts. En efecte, aquest problema equival a construir dos segments dels quals es coneix la seva suma, q, i el seu producte, p.

Per a això construïm primerament el segment $\sqrt{p}$.



Construïm després una circumferència de diàmetre $AB = q$ i una paral·lela a AB a distància $\sqrt{p}$. Sigui P un dels punts d'intersecció d'aquesta paral·lela amb la circumferència. La condició perquè es tallin és justament $q^2 - 4p \geq 0$, és a dir, discriminant positiu. Sigui Q el peu de la perpendicular des de P al diàmetre. Llavors els segments buscats són AQ i QB, ja que

clarament la seva suma és $AB = q$, i el seu producte és p, ja que $PQ = \sqrt{p}$ és la mitja proporcional de AQ i QB (teorema de l'altura).

Observem que hem agafat $p, q \in \mathbb{R}^+$ perquè ens interessem per les equacions de segon grau amb arrels positives.

Els tres problemes clàssics

Els tres problemes clàssics els podeu trobar ben explicats a molts llocs, per exemple a [11].

2.3 200 a.C. Arquimedes

Va viure a Siracusa on va morir l'any 212 a.C. a mans del consul romà Marcel. Se'l considera el precursor del calcul integral pel seu mètode d'exhaució. El seu nom està associat al cèlebre Principi fonamental de la hidrostàtica i és un dels creadors de l'Estàtica on la llei de la palanca també porta el seu nom. Les seves obres més conegudes son *El Mètode* i *Sobre l'esfera i el cilindre* on calcula l'àrea i el volum de l'esfera relacionant-lo amb l'àrea i el volum del cilindre circumscrit. Vegeu [6].

2.4 250 d.C. Diofant d'Alexandria

La seva obra més coneguda és *Aritmètica*. Va publicar 13 volums dels quals 6 s'han conservat. Justament sobre un exemplar d'aquest llibre és on Fermat va escriure que no tenia prou espai al marge per donar la demostració del seu famós teorema. Potser l'aportació més original de Diofant, en contra dels hàbits grecs tradicionals, és la d'introduir abreviatures simbòliques per representar els termes de les equacions, cosa que més endavant donaria pas a l'àlgebra. Aquest curs estudiarem les *equacions diofàntiques*, que apareixen ja a l'*Aritmètica*.

2.5 1247. Qin Jiushao

En un llibre de Qin Jiushao apareix el que avui anomenem *Teorema xinès del residu*. Però es troba rastre d'un problema anàleg al llibre de Sun Zi, el *Sunzi suanjing*, del segle III: Quants soldats té l'exèrcit de Han Xing si, formats en 3 columnes, queden dos soldats, formats en 5 columnes, queden tres soldats i, formats en 7 columnes, queden dos soldats?

També es fa referència a que els astrònoms xinesos el podrien haver utilitzat per resoldre problemes de calendari. L'inici del calendari xinès va ser fixat per la dinastia Wei en el *Shang yuan*. A partir d'aquest moment, una mena de Big Ban, es contava en períodes de 60 dies. I era l'inici també de

les fases de la lluna i el solsticis. Si en algun moment, el solstici d'hivern (el dia més curt de l'any) tenia lloc r dies després de l'inici del cicle de 60 dies i s dies després de lluna nova, quants dies N havien passat des del *Shang yaun*? Això planteja el sistema

$$\begin{aligned} N &= \overset{\bullet}{60} + r \\ N &= \overset{\bullet}{28} + s \end{aligned}$$

que és un cas particular del teorema xinès del residu.[3] Vegeu [9].

L'obra matemàtica xinesa més antiga és el *Jiuzhang Suanshu*, que vol dir quelcom com *Aritmètica*, i que data aproximadament del 300 a.C. Conté 246 problemes pràctics de la vida real. La traducció a l'anglès portava el nom de *Nou capítols de l'art matemàtic*.

2.6 1545. Cardano

Cap allà l'any 1500[4] **Scipione del Ferro**, professor a la Universitat de Bolonya, va saber resoldre l'equació cúbica sense terme quadràtic $x^3+mx = n$. Però no va fer públic el mètode ja que feien competicions amb altres matemàtics. A punt de morir va passar el mètode al seu alumne **De Fior** qui, al 1535, va reptar a **Tartaglia** (Niccolo Fontana[5]). Es van creuar una llista de 30 problemes cadascun, però els 30 problemes de De Fior eren equacions cúbiques sense terme quadràtic. En aquells moments Tartaglia només sabia resoldre les equacions cúbiques sense terme lineal $x^3+mx^2 = n$, però la nit del 13 de Febrer de 1535, amb el temps de la prova quasi exhaurit, va aconseguir resoldre l'equació cúbica sense terme quadràtic i per tant tots els problemes proposats per De Fior. Va guanyar, però va perdonar al seu rival la aposta que consistia en 30 bons banquets.

Cardano, un personatge molt controvertit, pressionava Tartaglia perquè li revelés el secret de la cúbica. Finalment, el 1539, Tartaglia li va revelar amb la condició de que Cardano jurés pel Sants Evangelis, com així va fer, que no revelaria mai aquest secret. No obstant el va revelar al seu alumne **Ferrari**. Ells dos, Cardano i Ferrari, varen aconseguir resoldre l'equació cúbica general, però com passaven per la cúbica sense terme quadràtic no podien publicar la solució.

---

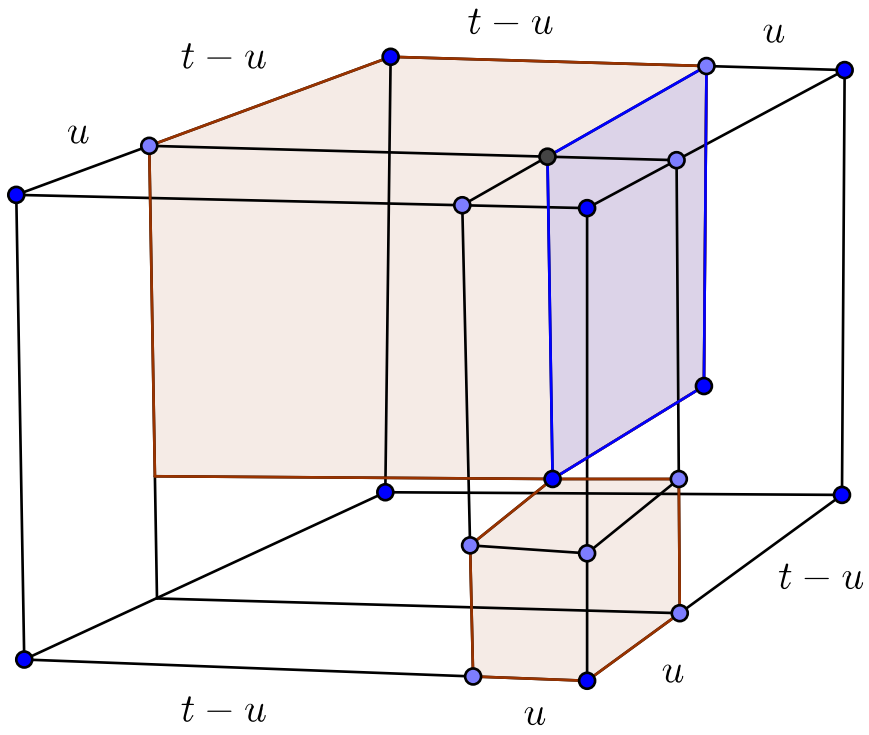
[3] La notació $\overset{\bullet}{a}$ vol dir múltiple de a.

[4] Mil anys de foscor! Una obra que va ajudar a sortir del pou fou *Margarita Philosophica*, del frare cartoixà Georg Reisch, publicada el 1503, i utilitzada com llibre de text a les universitats, contenia gramàtica, aritmètica, música, geometria, física i psicologia. Parla de Boethius i del seu llibre de l'anys 500 aproximadament *De Institutione Arithmetica*.

[5] Tartaglia vol dir tartamut o quec, sobrenom que se li aplicava ja que parlava malament degut a una ferida al coll feta per un soldat francès durant l'invasió del seu poble, Brescia.

Però un dia van descobrir que la resolució de la cúbica sense terme quadràtic no era de Tartaglia sinó de del Ferro, i es va considerar alliberat del seu juramment. Finalment, el 1545 publica *Ars Magna*, la seva gran obra, on apareix per primer cop impresa la solució de la cúbica.

Mirant el dibuix (seguim [3])



Cardano veu que

$$t^3 = u^3 + (t-u)^3 + 2tu(t-u) + u^2(t-u) + u(t-u)^2.$$

que simplificant és

$$(t-u)^3 + 3tu(t-u) = t^3 - u^3.$$

Això dóna la idea de que per resoldre la cúbica

$$x^3 + mx = n$$

hem de fer el canvi de variable $x = t-u$, $m = 3tu$ i $n = t^3 - u^3$. Ara l'objectiu és trobar t i u en funció de m i n i la solució serà $x = t-u$.

Manipulant les relacions anteriors obtenim

$$t^6 - nt^3 - \frac{m^3}{27} = 0,$$

equació fàcil ja que és de segon grau en t^3.

Obtenim

$$t = \sqrt[3]{\frac{n}{2} + \sqrt{\frac{n^2}{4} + \frac{m^3}{27}}}$$

i pràcticament hem acabat, ja que $u^3 = t^3 - n$ i per tant la solució de la cúbica és

$$x = t - u = \sqrt[3]{\frac{n}{2} + \sqrt{\frac{n^2}{4} + \frac{m^3}{27}}} - \sqrt[3]{-\frac{n}{2} + \sqrt{\frac{n^2}{4} + \frac{m^3}{27}}}.$$

2.7 1637. Descartes

René Descartes (1596-1650). Filosof racionalista francès. A la seva obra *Discours de la méthode* de 1637 hi inclou un apèndix titulat *La Géométrie* on introdueix el que avui es coneix com geometria analítica.

2.8 1640. Fermat

Pierre de Fermat (1601-1665). Advocat i matemàtic occità d'origen basc. El conegut com *Teorema de Nadal* de Fermat, perquè el va comunicar per carta a Marin Mersenne[6] el 25 de desembre de 1640, estableix que tot nombre primer de la forma $4m + 1$ es pot escriure de manera única com a suma de dos quadrats.[7]

No obstant és més conegut per haver afirmat que l'equació $x^n + y^n = z^n$ no té solució amb x, y, z enters. Aquest resultat es coneix com el *darrer teorema de Fermat*.

Aquest curs també estudiarem el conegut com petit teorema de Fermat, que apareix en una carta de 1640 a Frenicle de Bessy, que estableix que si a és un nombre enter i p és un nombre primer que no és un factor de a, llavors p ha de ser un factor primer de $a^{p-1} - 1$. No en va donar cap prova. Però, la motivació última per estudiar a quests tipus de números, era, com hem dit abans, l'estudi dels números perfectes.

En relació al polígon de 17 costats, que també estudiarem aquest curs, Fermat va afirmar, segons diu **Goldbach** en una carta a **Euler**, que els nombres de la forma $2^{2^n} + 1$ són primers. Euler va provar que per a $n = 5$

[6]Els nombres de Mersenne són els nombres de la forma $2^p - 1$ amb p primer. Se sap que aquest nombre és primer per a $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937$, que són els 24 primers primers tals que $2^{p-1}(2^p - 1)$ és perfecte (igual a la suma dels seus divisors). Euclides va provar que un nombre parell és perfecte si té aquesta forma amb p i $2^p - 1$ primers. Hi ha molts valors de p per als quals no se sap si el corresponent nombre de Mersenne és primer o no.

[7]Clarament tot nombre primer és de la forma $4k + 1$ o $4k - 1$, només cal mirar-lo a $\mathbb{Z}/(4)$. Es pot demostrar que hi ha infinits primers de cadascun d'aquests dos tipus.

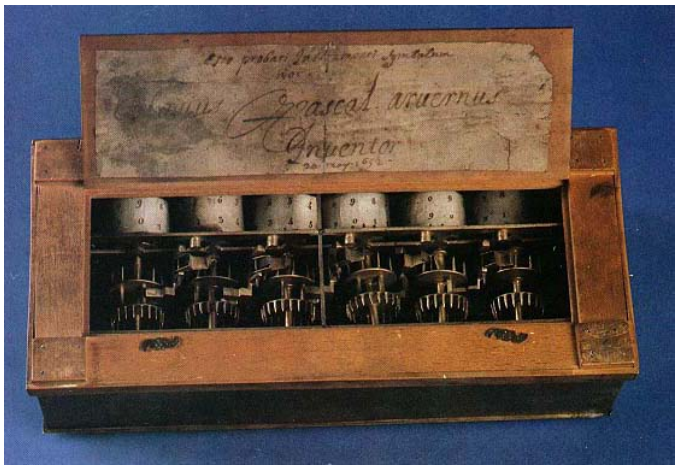
aquesta afirmació ja no és veritat. De fet, no s'ha trobat cap $n \geq 5$ per al qual aquest nombre sigui primer. Explicarem també durant el curs el mètode que va seguir Euler per veure que

$$2^{32} + 1 = 4294967297 = 641 \cdot 6700417.$$

i que, per tant, la conjectura de Fermat fallava ja per a $n = 5$.

2.9 1654. Pascal

Quan va aparèixer *La Géométrie* de Descartes **Blaise Pascal**(1623-1662) tenia 14 anys i dos anys més tard va impressionar Descartes amb els seus treballs. Va inventar l'avantpassat remot de les calculadores, *la pascalina*.



Va contribuir as inicis de la teoria de la probabilitat amb unes cartes molt famoses que es va creuar amb Fermat sobre problemes de daus que acabaven abans d'hora. El famós triangle de Pascal, format per nombres combinatoris, apareix al seu *Traité du Triangle Arithmetique* de 1654[8]. I el seu teorema sobre *l'hexàgon místic*, publicat a *Essai sur les coniques*, de 1640, forma part dels continguts clàssics de qualsevol llibre de geometria projectiva.

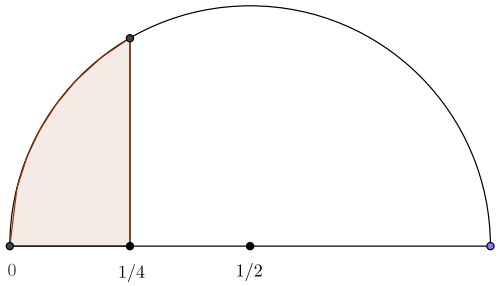
2.10 1666. Newton

Isaac Newton (1641-1727). Va néixer a Woolsthorpe-by-Colsterworth, Lincolnshire, Anglaterra. Aquest curs estudiarem la fórmula del binomi que ens diu com calcular $(a + b)^n$ quan n és un nombre enter. Newton la va generalitzar el 1665 al cas en que n és racional. Concretament va provar que

$$(1 + Q)^{m/n} = 1 + \frac{m}{n}Q + \frac{(\frac{m}{n})(\frac{m}{n} - 1)}{2}Q^2 + \frac{(\frac{m}{n})(\frac{m}{n} - 1)(\frac{m}{n} - 2)}{3 \cdot 2}Q^3 + \dots$$

[8]La notació $\binom{n}{k}$ fou introduïda per Andreas von Ettingshausen el 1826.

De seguida la va utilitzar de manera molt astuta per calcular π amb 7 xifres decimals exactes. Concretament calcula l'àrea de la figura adjunta de dues maneres diferents.



Primer, per geometria elemental, veu fàcilment que aquesta àrea val

$$\frac{\pi}{4} - \frac{\sqrt{3}}{32}.$$

Després, per càlcul integral, aproximant la funció a integrar per la fórmula del binomi aplicada a $(1-x)^{1/2}$. Concretament,

$$(1-x)^{1/2} = 1 - \frac{1}{2}x - \frac{1}{8}x^2 - \frac{1}{16}x^3 - \frac{5}{128}x^4 - \frac{7}{256}x^{5-\ldots}$$

Així

$$\int_0^{1/4} \sqrt{x}\sqrt{1-x}dx = 0,07677310678.$$

Igualant els dos valors obtinguts obté π.

El 1666 va descobrir el *mètode de les fluxions*, avui conegudes com *derivades*, i més endavant el *mètode invers de les fluxions*, és a dir, les *integrals* o *primitives*. Les fluxions apareixen a *Methodus fluxionum et serierum infiniturum* iniciat el 1664 però publicat el 1671 i les fluxions inverses a *De Analyisi* escrit el 1669 però publicat el 1711.

L'any 1687 Newton publica una de les obres més importants de tots els temps, titulada *Philosophiae Naturalis Principia Mathematica* i coneguda per tothom com els *Principia*. Allà dóna una descripció matemàtica de l'Univers. L'estudi de les còniques és extraordinari. És conegut que Newton va llegir els Elements d'Euclides i de segur que poc o molt el van influir. **Pierre-Simon Laplace** va dir: "Newton va ser el geni més gran que mai ha existit, i el més afortunat, ja que només es pot trobar el sistema en que es basa el Món més que una sola vegada".

2.11 1734. Euler

Leonard Euler (1707-1783). Nascut a Suissa va viure a Rússia i Prússia la major part de la seva vida. Un dels més grans i prolífics matemàtics. Dotat d'una memòria extraordinària, es diu que se sabia de memòria els 100 primers nombres primers i les seves potències fins grau 6, tenia una facilitat de càlcul prodigiosa.

Aquest curs intentarem explicar com va demostrar que la suma dels inversos dels quadrats de tots els nombre naturals és igual a $\pi^2/6$. És a dir,

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Ho va fer el 1734 a Sant Petersburg. Curiosament avui dia encara no es coneix quan val la suma dels inversos dels cubs de tots els nombre naturals.

La idea de la demostració és manipular la funció

$$g(x) = \frac{\sin x}{x} = 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \frac{x^8}{9!} - \dots$$

com si fos un polinomi, tot i que no ho és, i aplicar el resultat que veurem aquest curs de que tot polinomi descompon en producte de factors del tipus $x - r_i$ on r_i són es arrels.

Per exemple si un polinomi de grau 4 té arrels $1, 2, 3, 4$ el polinomi és

$$P(x) = a(x-1)(x-2)(x-3)(x-4),$$

que ens interessa escriure com[9]

$$P(x) = a(1-x)(2-x)(3-x)(4-x),$$

on a és una constant. Si, a més sabem que el terme independent del polinomi en qüestió és 1 (similarment a lo que li passarà a Euler) podem dividir cada factor per la corresponent arrel i escriure

$$P(x) = (1-x)(1-\frac{x}{2})(1-\frac{x}{3})(1-\frac{x}{4}).$$

Tornant al nostre cas, les arrels de $g(x)$ són $\pm k\pi$, amb $k \in \mathbb{N}$. Agrupant $k\pi$ amb $-k\pi$ de manera que $(x - k\pi)(x + k\pi) = (x - k^2\pi^2)$, i tenint en compte que el terme independent és 1 tenim

$$g(x) = \prod_{k\in\mathbb{N}} (1 - \frac{x^2}{k^2\pi^2})$$

Igualant el coeficient de x^2 a les dues expressions que tenim de $g(x)$, com suma infinita o com producte infinit hem acabat.

[9] Si tingéssim un nombre imparell d'arrels tindríem aquí un problema de signe.

Va demostrar diversos resultats de teoria de nombres enunciats sense prova per Fermat, com ara el petit teorema de Fermat o el teorema del dia de Nadal. Aquest curs veurem la funció Φ d'Euler que compta el nombre de coprimers amb n més petits que n. Per exemple, si p és primer, $\Phi(p) = p-1$. Com per a Fermat la motivació primera per a Euler era l'estudi dels nombres perfectes, tema que el va interessar durant tota la sega vida. Va veure, per exemple, que els nombres de Mersenne corresponents a valors $p = 11, 23, 83, 131, 179, 239, etc$ eren compostos. En una carta a Bernouilli de 1772 li diu que el nombre de Mersenne corresponenta $p = 31$ és primer i que per tant $2^{30}(2^{31}-1)$ era el vuité nombre perfecte.

També va escriure llibres de text que van revolucionar l'ensenyament de les matemàtiques, el més famós *Introductio in analysim infinitorum*, de 1748. La seva *Opera Omnia* (recull dels seus treballs fet després de la seva mort) consta de 73 volums!

2.12 1801. Gauss

Carl Frederich Gauss (1777-1854). Va néixer a Braunschweig, baixa Saxonia, i va morir a Göttingen, Alemanya. Sens dubte un dels més grans matemàtics de tots els temps. Amb 23 anys va publicar ja una obra que el feia immortal: *Disquisitiones Arithmeticae*.

Aquest curs veurem algunes coses que apareixen aquí, sobre tot el tema de congruències, i el que anomenarem $\mathbb{Z}-$mòduls, i si tenim temps explicarem la construcció del polígon de 17 costats, el primer resultat de Gauss, de quan tenia uns 18 anys, on va tancar un problema que portava sense solució uns 2000 anys! Aquest resultat generalitzat, en el sentit de saber quins polígons de n costats es poden dibuixar amb regle i compàs, apareix explícitament al *Disquisitiones*.

La notació que nosaltres utilitzarem

$$a \equiv b \pmod{n}$$

per dir que en dividir a entre n i b entre n obtenim el mateix residu, és de Gauss. Les controvèrsies entre el matemàtic francès **Adrian-Marie Legendre** (1752-1833) i Gauss arriben a fer que Legendre, ja molest per moltes altres coses digui: "Aquestes equacions entre residus de la divisió de diversos nombres per un mateix nombre primer, que es manipulen com les equacions ordinàries, no requereixen símbols nous d'igualtat ni de denominacions noves força incongruents, de les quals alguns geòmetres fan ús."

En una carta a Olbers de 1806 Gauss diu: "Sembla que és el meu destí estar en competència amb Legendre en quasi tots els meus treballs teòrics". Tres anys abans de la publicació del *Disquisitiones* de Gauss, Legendre va publicar *Essai sur la Théorie des nombres*, però probablement Gauss no el coneixia quan va escriure la seva obra, no oblidem que el whatsapp encara

no estava a ple rendiment. Però és cert que hi havia interseccions, com hem comentat. De fet Gauss, referint-se al llibre de Legendre diu: "Com aquest llibre va arribar a les meves mans un cop la major part de la meva obra estigués ja a la impremta, no he pogut mencionar en cap lloc l'analogia dels plantejaments".

Legendre, el 1798, va conjecturar que el nombre de nombres primers entre 1 i x estava donat per

$$\Pi(x) = \frac{x}{\ln x - 1.08366}.$$

Gauus el 1791 quan tenia 14 anys, va anotar a la seva taula de logaritmes que

$$\Pi(x) = \frac{x}{\ln x}.$$

Una comparació de les dues fórmules es veu una mica a la taula següent (vegeu [4]).

x	primers entre 1 i x	Legendre	Gauss
3	2		
10	4	8	
25	9	12	
100	25	28	
1000	168	172	178
10000	1229	1231	1246
100000	9592	9588	9630
1000000	78498	78543	78628

Aquest tipus de fórmules no es van provar fins el 1896 quan J. Hadamard i, independentment, Charles J. de la Vallèe Poussin van provar que

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

Però les idees estaven en els papers de Riemann, que va utilitzar el que avui anomenem funció zeta de Riemann per estudiar la distribució dels primers. Aquesta funció és

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

El primer que la va escriure, per a $s \in \mathbb{N}$, fou el genial Euler. El genial Riemann la va estendre a valors complexos de S, és a dir, va considerar l'anterior suma amb $s \in \mathbb{C}$.

El raonament d'Euler és el següent.

$$\frac{1}{1-\alpha x} = 1 + \alpha x + \alpha^2 x^2 + \dots$$

Si ho apliquem a una col·lecció de nombres α_i i multipliquem obtenim

$$\prod_i \frac{1}{1-\alpha_i x} = 1 + (\sum_i \alpha_i)x + (\sum_{i\leq j} \alpha_i\alpha_j)x^2 + \dots$$

Si ara pensem que les α_i són els inversos dels primers i posem $x = 1$ a l'anterior suma obtenim[10]

$$\prod_p \frac{1}{1-\frac{1}{p}} = \sum_{n=1}^{\infty} \frac{1}{n}$$

ja que a la successió

$$\frac{1}{p_1}, \frac{1}{p_2}, \dots, \frac{1}{p_1 p_1}, \frac{1}{p_1 p_2}, \dots, \frac{1}{p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}}, \dots$$

hi apareixen, en els denominadors, tots els naturals. Però com que aquesta serie és divergent, la igualtat anterior només ens diu que hi ha infinits primers, cosa que ja sabíem, de manera que per obtenir més informació apliquem la mateixa idea a les potències dels primers, és a dir, canviem α_i per les potències dels inversos dels primers, i tenim

$$\prod_p \frac{1}{1-\frac{1}{p^s}} = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s > 1$$

que és el naixement de la funció ζ de Riemann i la seva relació amb la distribució dels nombres primers.

Dos més dels problemes de paternitat entre Legendre i Gauss foren la *llei de reciprocitat quadràtica* i la *llei dels mínims quadrats*.

Al llarg de la seva vida va donar 5 demostracions diferents del teorema fonamental de l'àlgebra, teorema que aquest curs citarem sense demostració, ja que aquesta apareixerà en diverses assignatures de la carrera, i que diu que *un polinomi amb coeficients complexos i de grau n, té n arrels complexes*, contades amb la seva multiplicitat.

La seva aportació a la cartografia va ser tan important que encara avui els mapes de la terra, per exemple els de l'Institut Cartogràfic de Catalunya, es fan amb els seus mètodes.

Ja que hem parlat de Legendre diguem que, entre moltes altres coses, va tractar de posar al dia els Elements d'Euclides i va publicar fins a cinc edicions del seu llibre *Éléments de Géométrie* de 1794, que estava molt bé,

[10]Per exemple, per mirar el coeficient de x^3 ens imaginem els infinits productes $(1 + \alpha_i x + \alpha_i^2 x^2 + \dots)$ i veiem que un x^3 apareix en multiplicar tots els uns menys un per α_i^3, o en multiplicar tots els uns menys dos per $\alpha_i^2\alpha_j + \alpha_j^2\alpha_i$, $i < j$, o en multiplicar tots els uns menys tres per $\alpha_i\alpha_j\alpha_k$, $i < j < k$. Aquests tres cassos s'agrupen en $\sum_{i\leq j\leq k} \alpha_i\alpha_j\alpha_k$.

llevat que a les diverses edicions donava 'demostracions' diferents del cinquè postulat d'Euclides.

En una de les notes reprodueix la prova de Lambert de 1761 sobre la irracionalitat de π utilitzant el desenvolupament en fraccions contínues de la tangent d'un angle. Mirarem d'explicar-ho també aquest curs com aplicació de l'algorisme d'Euclides. I, a la mateixa nota, Legendre conjectura que π no és algebraic (zero d'un polinomi a coeficients enters), cosa que va demostrar el 1882 **Lindemann**.

2.13 1832. Galois

Évariste Galois (1811-1832) Va donar un mètode per saber quines equacions polinòmiques es podien resoldre per radicals, donant, en particular una nova demostració del teorema d'**Abel**[11] que diu que no hi ha una solució general per radicals per a l'equació de cinquè grau. L'any 1831 Poisson va recomanar a l'Acadèmia de Ciències Francesa que rebutgés el treball que Galois havia enviat per a la seva publicació. Treball extraordinari i fonamental en el món de les matemàtiques, on neix la teoria de grups. Galois va rebre la carta de refús a la presó. Dos dies després de ser alliberat va morir en duel. El 1846 **Liouville** va donar a conèixer el grandiós treball de Galois.

2.14 1874. Cantor

George Cantor (1845-1918) L'any 1874, en el treball *Ueber eine Eigeschaft des Inbegriffes aller reellen algebraischen Zahlen*, Cantor va demostrar que el conjunt dels nombres reals no és numerable. A classe donarem una demostració molt fàcil del propi Cantor de l'any 1891. De manera similar va provar que el conjunt de nombres algebraics és numerable cosa que demostrava l'existència de molts nombres transcendents, sense necessitat d'exhibir-ne ni tan sols un! Se'l considera l'iniciador de la teoria de conjunts que explicarem aquest curs. De fet, entre 1879 i 1884 va publicar una serie de 6 articles a *Mathematische Annalen* pensats per proporcionar una introducció a la *Teoria de conjunts*.

[11] No s'hauria d'explicar teoria de Galois sense tenir un bon coneixement del treball de Joseph Louis Lagrange *Rfelexions sur la résolution algébrique des équations* on apareix la famosa *resolvent de Lagrange* i on considera ja permutacions de les arrels, idea germinal del treball de Galois. El primer en afirmar que l'equació de cinquè grau no és resoluble per radicals va ser Paolo Ruffini el 1799, però la seva demostració no era correcta. Va ser Abel qui va tancar el tema en 1824.

2.15 1900. Hilbert

David Hilbert (1862-1943). El 1899 va publicar *Grundlagen der Geometrie* (Fonaments de la Geometria), un estudi sistemàtic dels seus axiomes bàsics que va representar una revolució, presentant la disciplina basada únicament en 21 axiomes i promovent l'enfocament axiomàtic de les matemàtiques. Aquesta obra es pot considerar de les més influents a les matemàtiques del segle XX.[12] Durant el segon Congrés Internacional de les Matemàtiques celebrat a París Hilbert va exposar una llista de 23 problemes oberts que van influir de manera extraordinària en el desenvolupament de les Matemàtiques del segle XX.

2.16 1995. Wiles

L'any 1995 Andrew Wiles resol la conjectura de Taniyama-Shimura, que implicava, junt amb altres resultats d'altres matemàtics, la demostració del *darrer Teorema de Fermat.*

2.17 2006. Perelman

Gregori Perelman tenia que anar a recollir la medalla Fields a l'ICM 2006, però no hi va anar malgrat ser la més alta distinció que pot rebre un matemàtic. Així mateix també va rebutjar el premi d'un milió de dòlars que, per haver resolt la Conjectura de Poincaré, li va atorgar el Clay Mathematics Institute el 2010.

[12] Paràgraf copiat de Wikipedia.

Tema 3

El conjunt $\mathbb{N}$ dels nombres naturals

3.1 Axiomàtica de conjunts

Aquest curs treballarem els conjunts de manera intuïtiva. Direm només que un *conjunt* és una col·lecció d'objectes, que anomenarem *elements* del conjunt. Però això no és pas una definició en el sentit matemàtic sinó tan sols una descripció, ja que dir que un conjunt d'objectes és una col·lecció d'objectes no és més que dir el mateix dues vegades en paraules diferents.

No obstant reprodueixo els primers axiomes de la teoria de conjunts, per tal de tenir una idea de per on van les coses.

Els termes *conjunt* i *element*, i el símbol $\in$ no es defineixen. Els axiomes ens diuen quines relacions hi ha entre aquests objectes.

Axioma 1. Existeix un conjunt.

Axioma 2. Dos conjunts són iguals si tenen els mateixos elements.

Axioma 3. Si A és un conjunt i $Q(x)$ una relació que conté la lletra x, existeix un conjunt B que consisteix exactament d'aquells elements $x \in A$ per als quals $Q(x)$ és cert.

A partir d'aquests teoremes es pode demostrar ja alguns resultats, com els dos teoremes que citem a continuació, però per anar més endavant s'han d'afegir encara més axiomes, vegeu per exemple [12].

Teorema 3.1. *Existeix un únic conjunt que no té elements.*

Teorema 3.2. *No existeix un conjunt que contingui tots els conjunts.*

És la paradoxa de **Rusell**[1]. Observem que hi ha conjunts que es pertanyen a ells mateixos com elements i altres que no. Per exemple el conjunt dels

[1]Bertand Rusell (1872-1970). La seva paradoxa és de 1901, quan mirava de descobrir algun error en la teoria dels infinits de Cantor. La seva obra més coneguda és *Principles of Mathematics* de 1903. A mi, de petit, em va impactar molt la seva obra *Why I am not a Christian*. Recordem que va ser premi Nobel de Literatura el 1950.

nombres parells no és un nombre parell (no es pertany a ell mateix com element). En canvi el conjunt de coses que no són taules no és una taula i es pertany doncs a ell mateix. O el conjunt d'idees abstractes és una idea abstracta i es pertany doncs a ell mateix.

Sigui $\mathcal{C}$ el conjunt de tots els conjunts.

Sigui

$$B = \{A \in \mathcal{C}; A \notin A\}$$

Llavors $B \in B$ si i només sí $B \notin B$.

L'axioma de la teoria de conjunts que es vulnera és l'axioma 3 de més amunt, que és el que ens assegura que aquesta B que acabem de definir és un conjunt (en la hipòtesis de que $\mathcal{C}$ ho sigui). Per tant $\mathcal{C}$ no pot ser un conjunt.

3.2 Axiomes de Peano

No donarem la construcció axiomàtica de $\mathbb{N}$ que es dóna habitualment un cop feta la teoria de conjunts ($\mathbb{N}$ *és el conjunt dels elements continguts en tot conjunt inductiu*).

No obstant acceptarem que $\mathbb{N}$ està definit pels axiomes de Peano. Això vol dir que $\mathbb{N}$ és un conjunt que té les 5 propietats següents[2].

1. $1 \in \mathbb{N}$.

2. Per a tot $n \in \mathbb{N}$ existeix un successor $S(n) \in \mathbb{N}$.

3. 1 no és següent de cap altre $n \in \mathbb{N}$, i.e. $\forall n \in \mathbb{N}, 1 \neq S(n)$.

4. Per a tot $m, n \in \mathbb{N}$, si $m \neq n$ llavors $S(m) \neq S(n)$.

5. Si $A \subseteq \mathbb{N}$ és tal que $1 \in \mathbb{N}$ i per a cada $x \in A$ es compleix que $S(x) \in A$, llavors $A = \mathbb{N}$.

El cinquè axioma es coneix com *principi d'Inducció.*

3.3 Inducció i primer element

Veurem que el principi d'inducció equival al principi del primer element.

Observem que la propietat 5 ens diu que $\mathbb{N}$ està format per l'1 i tots els seus successors, és a dir,

$$\mathbb{N} = \{1, S(1), SS(1), SSS(1), \dots\}$$

[2]Aquestes propietats caracteritzen $\mathbb{N}$ en el sentit de que qualsevol altre conjunt que les compleixi és "igual" a $\mathbb{N}$. Varen ser establerts l'any 1889 per Giuseppe Peano (1858-1932), matemàtic italià, a l'article *Arithmetices principia, nova methodo exposita.*

en particular, tot $n \in \mathbb{N}$, no sols té successor com diu l'axioma 2, sinó que és ell mateix (llevat de l'1) successor d'un altre nombre natural. I l'element 1 és *l'únic* que no és successor de ningú.

Escriurem $m < n$ quan $n = SSS \dots S(m)$. Si $S \subseteq \mathbb{N}$, direm que $s_0 \in S$ és el primer element de S si $s_0 < s$ per a tot $s \in S$, $s \neq s_0$.

Proposició 3.3. *Tot subconjunt no buit de* $\mathbb{N}$ *té primer element.*

Demostració. Sigui $A \subseteq \mathbb{N}$. Sigui $a_0 \in A$. Si $1 \in A$, hem acabat ja que llavors 1 és el primer element de A. Si $1 \notin A$, però $S(1) \in A$, hem acabat ja que llavors $S(1)$ és el primer element de A. Si $1, S(1) \notin A$, però $SS(1) \in A$, hem acabat ja que llavors $S(1)$ és el primer element de S. Aquest procés ens porta fins a a_0 en un nombre finit de passos, ja que $a_0 = SS \dots S(1)$. Si arribem fins a_0 és que a_0 és el primer element de A.

Proposició 3.4. *Si un conjunt compleix els quatre primers axiomes de Peano i té la propietat de que tot subconjunt no buit d'ell té primer element, llavors es compleix el cinquè axioma de Peano (principi d'inducció).*

Demostració. Sigui $A \subseteq \mathbb{N}$ subconjunt en les hipòtesis de l'axioma 5. Hem de veure $A = \mathbb{N}$. Sigui s_0 el primer element de A^c. Llavors $s_0 - 1$ (l'anterior de s_0)[3] pertany a A i per tant el seu successor també, contradicció ja que $s_0 \notin A$. Això vol dir $A^c = \emptyset$ (no pot existir s_0), i per tant $A = \mathbb{N}$.

Suma

La suma de nombres naturals es defineix per la fórmula

$$n + 1 = S(n); \qquad n + S(k) = S(n + k)$$

Per exemple, denotant per 2 al successor de 1, tenim

$$n + 2 = n + S(1) = S(n + 1) = SS(n).$$

Denotant per 3 al successor de 2, tenim

$$n + 3 = n + S(2) = S(n + 2) = SSS(n).$$

Etc.

[3]Suposem que un natural $1'$ no és successor de cap altre. Llavors $1' = 1$. En efecte, el conjunt $\{1, 1'\}$ té primer element, contradicció, ja que 1 seria successor de $1'$ o al revés. Com $s_0 \neq 1$, s_0 és successor d'algun element.

Tema 4

Lògica matemàtica

En Matemàtiques hi ha tres processos fonamentals: construir *objectes matemàtics*, formar *relacions* entre ells i *demostrar* que algunes d'aquestes relacions són verdaderes. Es diu llavors que són *teoremes*.

Els *objectes matemàtics* són el nombres, les funcions, les figures geomètriques, etc. Són abstraccions de coses reals. No existeixen a la Natura. Les *relacions* són afirmacions sobre les possibles propietats d'aquests objectes, i les relacions *verdaderes* són les que es poden deduir dels axiomes; els axiomes es poden pensar com un resum de les propietats més evidents dels objectes en qüestió. La successió de sil·logismes pels quals es passa dels axiomes a un teorema és una *demostració*.

Quan volem formalitzar tot això les coses es compliquen en gran manera.

Seguint Godement [5], com en tot el paràgraf anterior, acceptarem que una *relació*[1] és una successió de lletres i símbols matemàtics. De fet, cada *relació* la podem denotar per una única lletra de manera que el que es té de bon principi és només un conjunt de lletres.

4.1 Operacions lògiques elementals

Per tal de formar noves *relacions* a partir d'unes *relacions* prèviament donades definirem quatre operacions lògiques.

Disjunció. R *o* S .

Això vol dir que a partir de les *relacions* R i S formem una nova *relació* que es denota R *o* S i que es llegeix "R o S".

Negació. *no* R.

Això vol dir que a partir de la *relació* R formem una nova *relació* que es denota *no* R i que es llegeix "no R".

[1] Molts textos es limiten a considerar relacions que siguin certes o falses i a estudiar les seves taules de veritat. Això farem a les sessions de problemes. Vegeu per exemple [12].

Utilitzant aquestes dues normes en podem introduir encara dues més.

Conjunció. *R i S.*

Per definició "R i S" vol dir la *relació*: "no ((no R) o (no S))".

Això vol dir que a partir de les *relacions* R i S formem una nova *relació* que es denota "R i S" i que es llegeix R i S. Observem que les noves relacions "R o S" i "no R" no estan definides de cap manera, en canvi "R i S" està definit a partir de la disjunció i la negació.

Implicació. $R \Rightarrow S$.

Per definició "R⇒S" vol dir la *relació* "S o (no R)".

Això vol dir que a partir de les *relacions* R i S formem una nova *relació* que es denota "R⇒S" i que es llegeix *R implica S.*

També utilitzarem la notació "R ⇔ S", anomenada **doble implicació** o **equivalència lògica**, com una manera abreujada d'escriure "$(R \Rightarrow S\ )$ i $(S \Rightarrow R\ )$". Es llegeix dient *R és equivalent a S.*

Com exercici escriviu les possibles combinacions de les relacions R i S on R és la relació "el nombre enter n és múltiple de 6" i S és la relació "el nombre enter n és parell".

4.2 Relacions verdaderes

Per poder dir que una relació és verdadera necessitem un *sistema axiomàtic.* Això consisteix essencialment en donar una llista, com més curta millor, de relacions inicials que seran verdaderes per definició (són els *axiomes de la teoria*[2]) i en donar uns criteris, anomenats *axiomes lògics*[3] que permetin formar noves relacions a partir dels *axiomes de la teoria.* Aquestes noves relacions són, per definició, també verdaderes i s'acostumen a anomenar *Teoremes.*

Els axiomes lògics

Els *axiomes lògics*[4] són els següents:

A1. Si R és una relació, la relació

$$(R\ o\ R) \Rightarrow R$$

és verdadera.

[2]Serien els equivalents als 5 Postulats d'Euclides.

[3]Serien els equivalents als 5 criteris lògics d'Euclides, *el tot és més gran que la part*, etc.

[4]Posem els de Godement [5], però altres presentacions són possibles, en el sentit de que aquests axiomes no són pas únics.

A2. Si R i S són relacions, la relació

$$R \Rightarrow (R \; o \; S)$$

és verdadera.

A3. Si R i S són relacions, la relació

$$(R \; o \; S) \Rightarrow (S \; o \; R)$$

és verdadera.

A4. Si R, S i T són relacions, la relació

$$(R \Rightarrow S) \Rightarrow ((R \; o \; T) \Rightarrow (S \; o \; T))$$

és verdadera.

Definició 4.1. *Una relació es diu* verdadera *quan és un* axioma de la teoria *o una relació que s'ha obtingut a partir d'aquests axiomes de la teoria aplicant repetidament els 4 axiomes lògics anteriors i la norma següent:*

L1. Donades dues relacions R i S, si la relació "R⇒S" és verdadera, i si la relació R és verdadera, llavors la relació S és verdadera.

Per això la relació "R⇒S" s'interpreta dient que S és conseqüència lògica de R.

A la pràctica per demostrar que una certa relació S és verdadera, partirem d'una relació R que hem vist prèviament que és verdadera i anirem aplicant els axiomes lògics als axiomes de la teoria i a les relacions que ja sabem que són verdaderes, de manera que puguem dir en cada pas que la relació "$R \Rightarrow R_1$", "$R_1 \Rightarrow R_2$", etc. és verdadera. Per la Tautologia 4.1 que veurem més endavant, la relació "R⇒S" que obtenim al final del procés és verdadera.

Com es veu, els axiomes lògics fan referència a relacions arbitràries o genèriques, de manera que quan s'apliquen a relacions particulars donen com a resultat noves relacions particulars que són, per definició, verdaderes. Les relacions genèriques R, S, T que apareixen en els axiomes lògics anteriors no sabem si són verdaderes o no.

Acabem amb una definició conflictiva.

Definició 4.2. *Una relació R es diu* falsa *quan la relació "no R" és verdadera.*

Observem que no estem dient que una relació que no és verdadera sigui falsa!! El motiu és que donada una relació R es podria donar el cas de que no existís una demostració (la cadena de raonaments lògics) de R ni una demostració de "no R" . Aquestes relacions es diuen *indecidibles*. Per tant,

per veure que una relació és indecidible hauríem de demostrar que no es pot demostrar ni R ni "no R".

No s'han de confondre amb proposicions que encara no s'han demostrat, tipus conjectura de Goldbach, ja que no està demostrat que aquesta conjectura sigui una proposició indecidible, i potser es veurà en un futur que és verdadera o falsa.

Encara més, podrien haver-hi relacions verdaderes i falses a la vegada. Aquestes relacions es diuen *contradictòries*. La matemàtica accepta que en els seus sistemes axiomàtics no hi ha relacions contradictòries. No s'ha sabut demostrar, per procediments lògics, que no existeixen.

Resumint, una proposició pot ser *verdadera* (si es pot demostrar), *falsa* (si es pot demostrar "no R"), *indecidible* (no es pot demostrar ni R ni "no R"), *contradictòria* (verdadera i falsa).

Kurt Gödel va demostrar el 1930 que en la teoria dels nombres naturals existeixen relacions indecidibles. No es pot demostrar, doncs, en general **que tota relació és verdadera o falsa !!!!!!**

La idea es associar a cada símbol del sistema formal un nombre natural i per tant a cada relació un nombre (això es coneix com *la numeració de Gödel*).

Després es construeix una fórmula explícita oberta (és a dir, amb una variable lliure que pren valors en els nombres naturals) que quan s'avalua en el seu propi nombre de Gödel dóna lloc a una relació indecidible perquè afirma que ella mateixa no té demostració.[5]

Per tant, Gödel exhibeix una relació indecidible però no és explícitament una propietat sobre l'aritmètica en tant que sumes, productes, etc. de nombres naturals.

Un altra resultat important de Gödel és que no es pot demostrar que els axiomes de l'aritmètica no portin a contradicció, demostrant d'aquesta manera les limitacions del mètode axiomàtic.

També va demostrar que la negació de la hipòtesis del continu[6] no es pot deduir del sistema d'axiomes de la teoria de conjunts.[7]

Vegeu el capítol XIV del llibre *Gödel, Escher, Bach*, [7].

4.3 Tautologies

Els resultats que s'obtenen aplicant només els axiomes lògics es diuen tautologies. Utilitzarem molt els resultats següents.

[5] És verdadera la relació "aquesta relació no és verdadera" ?

[6] No hi ha un cardinal intermedi entre el cardinal dels naturals i el cardinal dels reals.

[7] De fet la hipòtesi del continu és independent dels axiomes habituals de la teoria de conjunts (Zermelo Fraenkel i l'axioma de l'elecció): d'aquests axiomes no es pot deduir ni la hipòtesi del continu ni la seva negació. És, dons, una relació indecidible en aquest sistema axiomàtic.

Tautologia 4.1. *Si R, S i T són relacions i si les relacions "R⇒S" i "S⇒T" són verdaderes, llavors la relació "R⇒T" és verdadera.*

Demostració. Per l'axioma A4, la relació

$$(S \Rightarrow T) \Rightarrow ((S\, o\, (no\, R)) \Rightarrow (T\, o\, (no\ R)))$$

és verdadera. Però això es pot escriure com

$$(S \Rightarrow T) \Rightarrow ((R \Rightarrow S) \Rightarrow (R \Rightarrow T)).$$

Com la relació"S⇒T" és verdadera, la relació "(R⇒ S)⇒ (R⇒T)" és verdadera, i com "R⇒S" és verdadera,"R⇒T" és verdadera, com volíem veure. □

Tautologia 4.2. *Si R és una relació, la relació "R o (no R)" és verdadera.*

Demostració. Volem veure que "R⇒R" és verdadera. Els axiomes A1 i A2 ens diuen que les relacions

$$R \Rightarrow (R\, o\, R), \quad (R\, o\, R) \Rightarrow R,$$

són verdaderes. Per la Tautologia 4.1, la relació "R⇒R" és verdadera i hem acabat. □

Molt important remarcar que del fet de que "R o (no R)" sigui verdadera no es dedueix que una de les dues relacions R o "no R" sigui verdadera. És el problema de la indecidibilitat.

Aquesta tautologia es coneix com *principi del tercer exclòs*, o en llatí, *tertii exclusi* o *tertium non datur*.

Tautologia 4.3. *Si R i S són relacions i una de les dues o les dues són verdaderes llavors la relació "R o S" és verdadera.*

Demostració. Suposem R verdadera. Per l'axioma A2, "R o S" és verdadera i hem acabat. Si S és verdadera, per l'axioma A2, "S o R" és verdadera, i per l'axioma A3 , "R o S" és verdadera. □

Que "R o S" sigui certa no permet deduir que almenys una de les dues relacions R o S és certa. És novament el problema de la indecidibilitat. No obstant *si la relació "R o S" és verdadera i R és falsa, llavors S és verdadera*, com veurem més endavant, Tautologia 4.9.

Tautologia 4.4. *Si R és una relació, la relació*

$$R \Leftrightarrow no(no\, R)$$

és verdadera.

Demostració. Per demostrar "⇒" hem de veure que la relació "(no(no R)) o (no R)" és verdadera. Però això és exactament el que diu la Tautologia 4.2 aplicada a [no R].

Per demostrar "⇐" hem de veure que la relació "R o (no(no(no R)))" és verdadera. Aplicant l'axioma A4 a la implicació verdadera

$$(no\,R) \Rightarrow no(no(no(R)))$$

tenim que la relació

$$((no\,R)\,o\,R) \Rightarrow (no(no(no)R)))\,o\,R)$$

és verdadera, i com el primer terme és una relació verdadera (Tautologia 4.2) resulta que el terme de la dreta és també una relació verdadera i per l'axioma A3 hem acabat. □

És a dir, R és verdadera si i només si "no (no (R))" és verdadera. Equivalentment, *R és verdadera si i només si (no R) és falsa*, ja que "no R" és falsa si i només si (per definició) "no (no (R))" és verdadera.

Tautologia 4.5. *Si R és una relació, la relació*

$$no(R\ o\ S) \Leftrightarrow (no\ R)\ i\ (no\ S)$$

és verdadera.

Demostració. Volem veure

$$no(R\ o\ S) \Leftrightarrow no[no[no\ R]\ o\ no[no\ S]]$$

La Tautologia 4.4 permet substituir[8] "no(no R)" per R i "no(no S)" per S, de manera que la relació anterior és equivalent a

$$no(R\ o\ S) \Leftrightarrow no(R\ o\ S)$$

i, per la Tautologia 4.2, hem acabat. □

Tautologia 4.6. *Si R és una relació, la relació "no (R i S)⇔ (no R) o (no S)" és verdadera.*

Demostració. Volem demostrar que la relació

$$no(no((no\ R)\ o\ (no\ S))) \Leftrightarrow (noR)\,o\,(noS)$$

és verdadera. Però això és conseqüència directa de la Tautologia 4.4. □

[8] Si A⇔ C, B⇔ D, llavors A o B ⇔ C o D. En efecte, per l'Axioma A4, A o B⇔ C o B, i C o B⇔ D o C.

Tautologia 4.7 (**Llei de les contrarecíproques**). *Si R i S són relacions, la relació*

$$(R \Rightarrow S) \Leftrightarrow ((noS) \Rightarrow (noR))$$

és verdadera.

Demostració. Volem veure que la relació

$$S\, o\, (noR) \Leftrightarrow ((noR)\, o\, no(no(S)))$$

és verdadera.

Pels axiomes A3 i A4 aquesta relació serà verdadera si la relació

$$S \Leftrightarrow (no(no(S)))$$

és verdadera, però aquesta relació és verdadera per la Tautología 4.4. □

Exemple. Prenem R la relació "x^2 és imparell" i S la relació "x és imparell". Per demostrar "R⇒ S" és més còmode demostrar "(no S)⇒ (no R)". És fàcil veure que la relació *no R* és *equivalent* a la relació "x^2 és parell"; i la relació *no S* és equivalent a la relació "x és parell". Així hem de demostrar que si x és parell, llavors x^2 és parell, la qual cosa és evident, ja que si $x = 2k$, llavors $x^2 = (2k)^2 = 4k^2$ que és parell.

Observi's que la relació

$$(R \Rightarrow S) \Rightarrow ((noR) \Rightarrow (noS))$$

no és verdadera. El típic exemple "tonto" és "si demà plou aniré al cine". Si no plou ves a saber que faré!!

Tautologia 4.8. *Si R i S són relacions, llavors la relació "R i S" és verdadera si i només si R és verdadera i S és verdadera.*

Demostració. Suposem primerament R verdadera i S verdadera. Per l'Axioma A2 la relació "S o (no R)" és verdadera. Equivalentment, la relació R⇒S és verdadera. Per la llei de les contrarecíproques, "no S⇒no R" és verdadera. Pels axiomes A4 i A1, la relació

$$(no\, S)\, o\, (no\, R) \Rightarrow (no\, R)\, o\, (no\, R) \Rightarrow noR$$

és verdadera. Novament per la llei de les contrarecíproques aplicada a la primera i tercera relació de l'anterior cadena d'implicacions tenim que la relació

$$no(no\, R)) \Rightarrow no((no\, S)\, o\, (no\, R))$$

és verdadera. Per les tautologies 4.4 i 4.1 tenim

$$R \Rightarrow no((no\, S)\, o\, (no\, R))$$

És a dir, "R⇒(R i S)" és verdadera, i com R és verdadera, "R i S" és verdadera, com volíem demostrar.

Per demostrar el recíproc provarem que

$$R\,i\,S \Rightarrow R, \quad R\,i\,S \Rightarrow S,$$

així si "R i S" és verdadera, R és verdadera i S és verdadera.

Però per la llei de les contrarecíproques "R i S⇒R" és verdadera si i només si "(no R)⇒no(no((no R) o (no S)))" i això, per la Tautologia 4.4, és equivalent a l'afirmació "(no R)⇒(no R) o (no S)" la qual és certa per l'axioma A2. Anàlogament es demostra que "R i S⇒ S" i hem acabat. □

Tautologia 4.9. *Si la relació "R o S" és verdadera i R és falsa, llavors S és verdadera.*

Demostració. Aplicant l'axioma A4 a la Tautologia 4.4 tenim que la relació

$$(R\ o\ S) \Leftrightarrow (no(no\ R)\ o\ S),$$

és verdadera. Però el terme de la dreta és, per definició d'implicació,

$$no(R) \Rightarrow S,$$

de manera que la relació

$$(R\ o\ S) \Leftrightarrow (no(R) \Rightarrow S),$$

és verdadera.

Per tant, si "R o S" és verdadera i "no R" és verdadera, S és verdadera. □

Nota. [El tercer exclòs] El *constructivisme* assegura que només existeixen els objectes matemàtics que es poden construir. Encara que de la no existència se'n derivi una contradicció, els constructivistes no ho accepten ja que aquest argument no ha construït l'objecte. Utilitzen la *lògica intuicionista*, que és la lògica clàssica però sense el principi del *tercer exclòs*. Aquest principi diu que per a tota proposició R la relació "R o no R" és verdadera. No confondre amb el principi de bivalència que diu que tota relació és verdadera o falsa.

Exemple 4.1. *Demostreu*[9] *que existeixen nombres irracionals a, b tals que a^b és racional.*

Solució. Sigui R la relació

$$(\sqrt{2})^{\sqrt{2}} \in \mathbb{Q}.$$

[9] Comentari de Wolfgang Pitsch sobre un exemple de Dov Jarden de demostració no constructiva.

Suposem R verdadera. Automàticament tenim dos nombres irracionals que un elevat a l'altre és racional.

Suposem R falsa. Vol dir "no R" verdadera. Això vol dir

$$(\sqrt{2})^{\sqrt{2}} \notin \mathbb{Q}.$$

Prenem

$$a = \sqrt{2})^{\sqrt{2}}, \quad b = \sqrt{2},$$

i tenim

$$a^b = 2 \in \mathbb{Q}.$$

Hem trobat dos nombres irracionals que un elevat a l'altre és racional.[10]

4.4 Reducció a l'absurd

Un mètode molt potent de demostració és el conegut com *reducció a l'absurd*. Consisteix en el següent: per demostrar que una certa relació R és verdadera suposem que és falsa (és a dir, que "no R" és verdadera). A continuació es raona aplicant els axiomes lògics fins arribar a trobar una certa relació contradictòria S, és a dir, que S sigui a la vegada verdadera i falsa[11]. Com que hem acceptat que en Matemàtiques això no passa diem que hem arribat a contradicció i que per tant, la hipòtesis que hem fet de que R fos falsa no es pot considerar.

Com hem dit, que R no sigui falsa no vol dir directament que sigui verdadera, però en aquest cas sí. En efecte, el fet de que hàgim sabut demostrar R a partir de"no R" vol dir que la relació "(no R)⇒ R" és verdadera[12].

Per l'axioma A4 la relació

$$((no\, R) \Rightarrow R) \Rightarrow (((no\, R)\, o\, R) \Rightarrow (R\, o\, R))$$

és verdadera. Per tant,

$$((no\, R)\, o\, R) \Rightarrow (R\, o\, R)$$

[10]Se sap, pel teorema de Gelfond-Schneider, que $\sqrt{2})^{\sqrt{2}} \notin \mathbb{Q}$.

[11]Es pot provar que si hi ha una relació contradictòria tota relació és contradictòria. En efecte, suposem R contradictòria i sigui S una relació. La relació "(no R)⇒(S o (no R))" és verdadera. Com "no R" és verdadera, "S o (no R)" és verdadera. És a dir, R⇒S és verdadera. Per tant, S és verdadera. Repetint el raonament amb "no S" obtenim que "no S" és verdadera, i per tant, S és contradictòria.

[12]Quan diem que hem demostrat una relació S a partir d'una relació R_0 volem dir que hem aplicat algun axioma o resultat verdader per obtenir una relació verdadera del tipus "$R_0 \Rightarrow R_1$", on R_1 és una nova relació. A continuació hem aplicat algun altre axioma o resultat verdader per obtenir una relació verdadera del tipus "$R_1 \Rightarrow R_2$", on R_2 és una nova relació, i així fins arribar a una relació verdadera del tipus "$R_k \Rightarrow S$". Això implica, per la Tautologia 4.1, que "$R_0 \Rightarrow S$" és verdadera, i per tant, si R_0 és verdadera, S també.

és verdadera. Per la Tautologia 4.2 $((no\, R)\, o\, R)$ és verdadera i per tant la relació "R o R" és verdadera, i ara per l'axioma A1 la relació R és verdadera.

Resumint, el mètode de demostració per *reducció a l'absurd* consisteix en suposar que la relació que es vol provar és falsa i arribar a contradicció.

Exemples.

L'exemple paradigmàtic d'aquesta situació és, per motius històrics, la demostració de que hi ha infinits nombres primers (proposició 20, llibre IX dels Elements).

Un exemple trivial seria el següent. Demostrar que no hi ha nombres enters m, n tals que $14m + 20n = 101$. Raonant per l'absurd podem suposar que sí que existeixen $m, n \in \mathbb{Z}$ tals que $14m + 20n = 101$. Però aquesta igualtat porta a contradicció ja que el primer terme és divisible per 2 i 101 no.

Hi ha solució amb $[(m \in \mathbb{Z})\ o\ (n \in \mathbb{Z})]$?

Substitucions en una relació

Sigui R una relació, A un objecte matemàtic i x una lletra. Al substituir totes les x que apareixen a R per A obtenim una nova relació, que es denota per $(A|x)R$, i es diu que s'ha obtingut *donant a x el valor A en R*. Si x no apareix a R simplement tornem a obtenir R.

Es diu que l'objecte matemàtic A *verifica la relació* R si la relació $(A|x)R$ és verdadera.

Es pot demostrar que

Teorema 4.3. *Sigui R una relació, A un objecte matemàtic i x una lletra. Si R és verdadera també és verdadera la relació obtinguda substituint x per A en R.*

4.5 Quantificadors

A part de la disjunció, negació, conjunció i implicació podem formar noves relacions a partir de les ja conegudes introduint dos símbols nous $\exists$ i $\forall$.

Quantificador existencial. Es denota per $\exists$ i, si x és una lletra i R una relació, s'escriu la nova relació com $(\exists x)R$ que es llegeix *existeix x tal que R.*

Quantificador universal. Es denota per $\forall$ i, si x és una lletra i R una relació, s'escriu la nova relació com $(\forall x)R$ que es llegeix *per a tot x es compleix R* i que es defineix per

$$no[(\exists x)(no\ R)].$$

Les normes de funcionament d'aquests quantificadors són delicades però nosaltres acceptarem que es comporten com indica a la pràctica les paraules 'existeix' i 'per a tot'. Remarquem-ne algunes.[13]

Q1. Si R és una relació i x una lletra llavors la relació

$$no((\exists x)R) \Leftrightarrow (\forall x)(no\ R)$$

és verdadera.

Q2. Si R i S són relacions i x una lletra llavors la relació

$$(\forall x)(R\ i\ S) \Leftrightarrow (\forall x)R\ i\ (\forall x)S$$

és verdadera.

Q3. Si R i S són relacions i x una lletra llavors la relació

$$(\exists x)(R\ o\ S) \Leftrightarrow (\exists x)R\ o\ (\exists x)S$$

és verdadera.

Observem que aplicant Q1 a "no R", i usant la Tautologia 4.4, obtenim

Q4. Si R és una relació i x una lletra llavors la relació

$$no((\forall x)R) \Leftrightarrow (\exists x)(no\ R)$$

és verdadera.

Aplicant aquestes normes es veu de seguida que

Q5. Si R és una relació i x i y una lletra llavors la relació

$$no[(\forall x)(\exists y)R] \Rightarrow (\exists x)(\forall y)(noR)$$

és verdadera.

[13] Són tautologies, en el sentit que es deriven de la definició de $\forall$ que hem donat a partir del símbol $\exists$ i de l'axioma de funcionament de $\exists$, que diu que si una relació R on apareix la lletra x és certa quan canviem x per un objecte matemàtic A, llavors la relació $(\exists x)R$ és verdadera. Més concretament

Axioma per $\exists$. Siguin R una relació, x una lletra i A un objecte matemàtic. Llavors la relació

$$(A|x)R \Rightarrow (\exists x)R$$

és verdadera.

Exemples

Exemples en llenguatge diari:

Q1. R la relació "la persona x és rossa". Acceptem que $(no\ R)$ vol dir "la persona x no és rossa". La negació de la frase "existeix una persona rosa' $(no((\exists x)R))$ és 'totes les persones són morenes' $(\forall x)(no\ R)$, entenguen per 'morenes' no rosses.

Q2. S la relació "la persona x és alta". És el mateix dir tota persona és "rossa i alta" $((\forall x)(R\ i\ S))$ que 'tota persona és rossa i tota persona és alta" $((\forall x)R\ i\ (\forall x)S)$.

Q3. És el mateix dir "existeix una persona que és rossa o alta" que "existeix una persona que és rossa o existeix una persona que és alta".

Q4. La negació de la frase "totes les persones són rosses" és que "existeix almenys una persona morena".

Nota

Quan escrivim $\exists x$ o $\forall x$ se suposa normalment que està clar pel context a on pertany aquest element x. Si no és així s'ha d'especificar.

Per exemple si diem $\forall x,\ x^3 \geq 0$, aquesta relació és verdadera si estem treballant amb nombres naturals, però falsa si estem treballant amb nombres enters. Per això escriurem, per exemple, $\forall x \in \mathbb{N},\ x^3 \geq 0$, o $\forall x \in \mathbb{Z},\ x^3 \geq 0$.

El mateix passa per afirmacions del tipus següent: $\exists x; x^2 - 1 < 0$ (que es llegeix, existeix x tal que el seu quadrat és menor que 1). Segons el conjunt en el que estiguem treballant serà certa o falsa (si el conjunt és el dels nombres naturals, és falsa; si el conjunt és el dels nombres reals, és certa).

Un altre exemple: denotem P el conjunt dels nombres parells i $\mathcal{P}$ el conjunt dels nombres primers: la conjectura de Goldbach es pot escriure com

$$\forall x \in P, \exists p_1 \in \mathcal{P}, \exists p_2 \in \mathcal{P};\ x = p_1 + p_2.$$

que es llegeix, tot nombre parell és suma de dos primers, o per a tot nombre parell x existeixen dos nombres primers p_1, p_2 tals que $x = p_1 + p_2$.

Exercicis

Exercici 4.4. *Negueu les relacions "per a tot $x \in$ R existeix $y \in \mathbb{R}$ tal que $y^3 = x$" i "els nombres x i y són imparells".*

Exercici 4.5. *Negueu*[14] *la relació "A tots els municipis hi ha alguna família tots els fills de la qual no han tingut xarampió ni la rubèola".*

Solució. Sigui $\mathcal{M}$ el conjunt de tots els municipis, $\mathcal{F}(x)$ el conjunt de totes les famílies del municipi x, $\mathcal{R}$ el conjunt de persones que han tingut la

[14] Exemple tret d'unes notes de Topologia de Jaume Aguadé.

rubèola i $\mathcal{X}$ el conjunt de persones que ha tingut el xarampió. Per a cada família $y \in \mathcal{F}(x)$ denotem $D(y)$ el conjunt format pels fills de la família y.

La relació que volem negar es pot escriure com

$$(\forall x \in \mathcal{M})(\exists y \in \mathcal{F}(x))S$$

on S és la relació "cadascun dels fills de la família y no ha tingut ni el xarampió ni la rubèola".

Per Q5 la negació demanada és

$$(\exists x \in \mathcal{M})(\forall y \in \mathcal{F}(x))(no\, S) \tag{4.1}$$

que es llegeix "existeix un municipi tal que totes les famílies d'aquest municipi compleixen (no S)"

Per negar S primer l'escrivim amb quantificadors.

$$(\forall z \in D(y))(z \in \mathcal{X}^c \cap \mathcal{R}^c)$$

Equivalentment

$$(\forall z \in D(y))(z \notin \mathcal{X} \cup \mathcal{R})$$

De manera que

$$(no\, S) \Leftrightarrow (\exists z \in D(y))(z \in \mathcal{X} \cup \mathcal{R})$$

Substituint aquest valor a (4.1) obtenim

$$(\exists x \in \mathcal{M})(\forall y \in \mathcal{F}(x))(\exists z \in D(y))(z \in \mathcal{X} \cup \mathcal{R})$$

Resumint, la negació de la frase "A tots els municipis hi ha alguna família tots els fills de la qual no han tingut xarampió ni la rubèola" és "existeix un municipi tal que totes les famílies d'aquest municipi tenen almenys un fill que ha tingut el xarampió o la rubèola"

Exercici 4.6. *Negueu que una funció $f : \mathbb{R} \longrightarrow \mathbb{R}$ sigui contínua a $x_0 \in \mathbb{R}$.*

Solució. Recordem que f és contínua en x_0 si i només si

$$\forall \epsilon > 0, \exists \delta > 0; |x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon$$

Això ho podem escriure com

$$(\forall \epsilon > 0)(\exists \delta > 0)R$$

on R és la relació

$$R : |x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon.$$

Així la negació de la condició de continuïtat és

$$no\Big[(\forall\epsilon>0)(\exists\delta>0)R\Big]$$

que sabem equival a

$$(\exists\epsilon>0)(\forall\delta>0)(noR).$$

Per negar R, recordem que "S⇒T" vol dir "T o (no S)" i per tant

$$no(S\Rightarrow T)\Leftrightarrow S\,i\,(noT).$$

Així la negació de R és

$$no\Big[|x-x_0|<\delta\Rightarrow|f(x)-f(x_0)|<\epsilon\Big]\Leftrightarrow|x-x_0|<\delta\ i\ |f(x)-f(x_0)|\geq\epsilon.$$

Resumint, f no és contínua en x_0 si

$$(\exists\epsilon>0)(\forall\delta>0)(|x-x_0|<\delta\ i\ |f(x)-f(x_0)|\geq\epsilon),$$

que es llegeix, *existeix* $\epsilon>0$ *tal que per a tot* $\delta>0$*, existeix* $x\in\mathbb{R}$ *tal que* $|x-x_0|<\delta\ i\ |f(x)-f(x_0)|\geq\epsilon$.

Exercici 4.7. *Negueu que un subconjunt* $K\subset\mathbb{R}^n$ *sigui compacte*[15].

Solució. K no és compacte si existeix un recobriment de K per oberts

$$K\subset\bigcup_\alpha U_\alpha$$

amb U_α oberts, el qual no admet cap subrecobriment finit, és a dir, K no està contingut en cap unió finita dels oberts U_α anteriors.

[15] K és compacte quan de tot recobriment de K per oberts se'n pot extreure un subrecobriment finit.

Tema 5

Permutacions

5.1 Definicions i notació

Definició 5.1. *Una permutació és una aplicació bijectiva de* $\mathbb{N}_n = \{1, 2, \ldots, n\}$ *en ell mateix.*

Per descriure una aplicació bijectiva $\sigma : \mathbb{N}_n \longrightarrow \mathbb{N}_n$ escriurem

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Per exemple, si $n = 3$, tenim les 6 permutacions següents:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Però també és molt útil la notació per *cicles*. Consisteix en posar de manifest només els elements que es mouen i no escriure els que es queden fixats. I els que es mouen posar-los un a continuació de l'altre, per exemple, la notació $(2, 3)$ vol dir que estem parlant d'una permutació que porta el 2 al 3, el 3 al 2, i deixa 1 fixat.

Així, les 6 permutacions anteriors s'escriuen com

$$\begin{aligned} \sigma_1 &= id \\ \sigma_2 &= (2, 3) \\ \sigma_3 &= (1, 2) \\ \sigma_4 &= (1, 2, 3) \\ \sigma_5 &= (1, 3, 2) \\ \sigma_6 &= (1, 3) \end{aligned}$$

Observem també que les permutacions σ_4 i σ_5 es poden escriure com

$$\begin{aligned} \sigma_4 &= (1,2,3) = (1,2) \circ (2,3) \\ \sigma_5 &= (1,3,2) = (1,3) \circ (3,2) \end{aligned}$$

(recordeu que en la composició d'aplicacions actua primer la de la dreta).

Si denotem per S_n el conjunt de les permutacions de n elements i per $|S_n|$ el seu cardinal tenim que

$$|S_n| = n!$$

En efecte, per construir una permutació σ mirem primer on va a parar el número 1. Tenim n possibilitats: que 1 vagi a 1, que 1 vagi a 2, etc, o que 1 vagi a n. Un cop elegida una d'aquestes n opcions hem de veure on va a parar el 2. Ara tenim només $n-1$ possibilitats, ja que com σ és injectiva, la imatge del 2 ha de ser diferent de la imatge de l'1. I així successivament.

Una altra manera de raonar el mateix és adonar-se de que l'argument que hem fet amb la imatge de l'1 ens diu que

$$|S_n| = |S_{n-1}|n$$

igualtat que, per recurrència, dóna el resultat.

Definició 5.2. *Sigui $\tau \in S_n$. Direm que τ és una transposició dels elements $a, b \in \mathbb{N}_n$ si*

$$\begin{aligned} \tau(a) &= b \\ \tau(b) &= a \\ \tau(k) &= k,\ k \neq a, k \neq b \end{aligned}$$

Una propietat evident de les transposicions és que

$$\tau^2 = \tau \circ \tau = id.$$

En particular, coincideixen amb la seva inversa,

$$\tau^{-1} = \tau.$$

5.2 Ordre d'una permutació

Definició 5.3. *Sigui $\sigma \in S_n$. L'*ordre *de σ és el menor natural k tal que*

$$\sigma^k = id.$$

Per veure que tota permutació té un ordre, és a dir, que si la composem amb ella mateixa un nombre suficient de vegades acabarà reproduint la

identitat, només hem d'observar que S_n té un nombre finit d'elements ($n!$) i en canvi la successió

$$id, \sigma, \sigma^2, \sigma^2, \ldots$$

és infinita, de manera que hi haurà una potència que serà igual a una potència anterior, és a dir, existiran $p < q \in \mathbb{N}$ tals que $\sigma^q = \sigma^p$. Composant amb σ^{-p} tenim $\sigma^{q-p} = id$. L'ordre de la permutació σ és doncs el primer element del conjunt no buit

$$S = \{m \in \mathbb{N}; \sigma^m = id\}.$$

Proposició 5.4. *L'ordre d'un cicle de longitud r és r.*

Demostració. Considerem

$$\sigma = (a_1, \ldots, a_r).$$

Observem que

$$\begin{aligned} \sigma(a_1) &= a_2 \\ \sigma^2(a_1) &= \sigma(a_2) = a_3 \\ \sigma^3(a_1) &= \sigma^2(a_2) = \sigma(a_3) = a_4 \\ \vdots &\quad \vdots \end{aligned}$$

És a dir,

$$\sigma^j(a_1) = a_{j+1}, \quad j = 1, \ldots, r$$

En particular

$$\sigma^r(a_1) = a_{r+1} = a_1.$$

Hem vist així que a_1 és fix per σ^r, però el mateix argument que hem fet per a_1 el podem repetir per a qualsevol dels a_j i tenim, doncs, $\sigma^r = id$, com volíem. □

5.3 Teorema de descomposició

Definició 5.5. *Dues permutacions $\sigma, \tau \in S_n$ es diuen* disjuntes *si els elements moguts per una d'elles són fixos per l'altre.*

Introduint la notació

$$M(\sigma) = \{k \in N_n; \sigma(k) \neq k\}$$

podem dir que $\sigma, \tau \in S_n$ són *disjuntes* si

$$M(\sigma) \cap M(\tau) = \emptyset.$$

Proposició 5.6. *Permutacions disjuntes commuten.*

Demostració. Siguin $\sigma, \tau \in S_n$ amb $M(\sigma) \cap M(\tau) = \emptyset$. El punt clau de la demostració és la observació de que si $x \in M(\sigma)$, llavors $\sigma(x) \in M(\sigma)$. En efecte, si $\sigma(\sigma(x)) = \sigma(x)$, aplicant σ^{-1} als dos costats tindríem $\sigma(x) = x$ en contra de la hipòtesi que hem fet.

Dit això continuem la demostració del teorema estudiant tres casos.

1) $x \in M(\sigma)$. En aquest cas sabem que $\sigma(x) \in M(\sigma)$ i per tant, tant x com $\sigma(x)$ són fixos per τ. Així,

$$\sigma(\tau(x)) = \sigma(x); \quad \tau(\sigma(x)) = \sigma(x),$$

és a dir, en aquest cas σ i τ commuten.

2) $x \in M(\tau)$. En aquest cas sabem que $\tau(x) \in M(\tau)$ i per tant, tant x com $\tau(x)$ són fixos per σ. Així,

$$\sigma(\tau(x)) = \tau(x); \quad \tau(\sigma(x)) = \tau(x).$$

és a dir, en aquest cas σ i τ commuten.

3) $x \notin M(\sigma) \cup M(\tau)$. Vol dir que x és fix tant per σ com per τ i per tant

$$\sigma(\tau(x)) = \tau(\sigma(x)) = x$$

és a dir, en aquest cas σ i τ commuten. □

El recíproc d'aquest teorema no és cert. Per exemple $\sigma = (1,2) \circ (3,4)$ i $\tau = (1,2)$ commuten i $M(\sigma) \cap M(\tau) \neq \emptyset$.

Exemple 5.1. *Calculeu l'ordre de*

$$\sigma = (1,2,3) \circ (4,5)$$

Solució. Observem que σ no és un cicle sinó una composició de cicles disjunts, i que per tant commuten. Calculem potències.

$$\sigma^2 = (1,2,3) \circ (4,5) \circ (1,2,3) \circ (4,5) = (1,2,3)^2 \circ (4,5)^2 = (1,2,3)^2 = (1,3,2)$$

Anàlogament,

$$\begin{aligned} \sigma^3 &= (1,2,3)^3 \circ (4,5)^3 = (4,5) \\ \sigma^4 &= (1,2,3)^4 \circ (4,5)^4 = (1,2,3)^4 = (1,2,3) \\ \sigma^5 &= (1,2,3)^5 \circ (4,5)^5 = (1,2,3)^2 \circ (4,5) \\ \sigma^6 &= (1,2,3)^6 \circ (4,5)^6 = id \end{aligned}$$

Teorema 5.7 (Teorema de descomposició). *Tota permutació descompon en producte de cicles disjunts. Aquesta descomposició és única llevat de l'ordre.*

Sketch of the proof. Considerem una permutació $\sigma \in S_n$ i considerem la *òrbita* de 1. Això vol dir que considerem el conjunt

$$O(1) = \{1, \sigma(1), \sigma^2(1), \ldots, \sigma^s(1)\}$$

en el cas de que $\sigma^{s+1}(1) = 1$. Podem pensar $O(1)$ com un *cicle*.

A continuació prenem un element $c \in \mathbb{N}_n$ que no aparegui a la òrbita de 1. Considerem la seva òrbita $O(c)$, que és fàcil veure que és disjunta amb $O(1)$,

$$O(c) = \{c, \sigma(c), \sigma^2(c), \ldots, \sigma^t(c)\},$$

amb $\sigma^{t+1}(c) = c$, i la podem pensar també com un cicle.

Ara agafaríem un element que no estigués ni a $O(1)$ ni a $O(c)$ i així successivament. És clar que en acabar aquest procés tindrem σ descomposta en composició de cicles disjunts del tipus

$$\sigma = O(1) \circ O(c) \circ \ldots. \qquad \square$$

Teorema 5.8. *L'ordre d'una permutació σ és el mínim comú múltiple dels ordres dels cicles disjunts en els que descompon.*

Proof. Com en l'exemple 5.1. Si $\sigma = \tau_1 \circ \cdots \circ \tau_k$ és la descomposició en cicles disjunts de σ, degut a que commuten, tenim

$$\sigma^m = \tau_1^m \circ \cdots \circ \tau_k^m$$

i clarament per ser aquestes $\tau' s$ disjuntes, per tal de que aquesta expressió sigui la identitat cadascuna de les potencies de les τ_i, $i = 1, \ldots, k$, ha de ser igual a la identitat. Com volem el més petit m amb aquesta condició ha de ser m igual al mínim comú múltiple dels ordres de les τ_i. $\square$

Exemple 5.2. *Calculeu l'ordre de*

$$\sigma = (1, 2, 3) \circ (3, 4)$$

Solució. Si aquests cicles fossin disjunts l'ordre seria 6 però no és el cas. Per descompondre σ en producte de cicles disjunts, prenem un element, per exemple 1, i seguim la seva òrbita.

Calculem $\sigma(1)$. Quan apliquem $(3, 4)$ a 1 obtenim 1. A continuació apliquem $(1, 2, 3)$ a 1 i obtenim 2, és a dir, $\sigma(1) = 2$.

Anàlogament $\sigma(2) = 3$.

Per calcular $\sigma(3)$ apliquem $(3, 4)$ a 3 i obtenim 4. A continuació apliquem $(1, 2, 3)$ a 4 i obtenim 4, és a dir, $\sigma(3) = 4$.

Per calcular $\sigma(4)$ apliquem $(3, 4)$ a 4 i obtenim 3. A continuació apliquem $(1, 2, 3)$ a 3 i obtenim 1, és a dir, $\sigma(4) = 1$.

Per tant, la òrbita de 1 és

$$1, \sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 4.$$

És a dir, en notació de cicles,

$$\sigma = (1, 2, 3, 4)$$

i per tant σ té ordre 4.

5.4 Signe d'una pemutació

Observem primer el resultat següent.

Proposició 5.9. *Tota permutació descompon en producte de transposicions.*

Demostració. Només cal observar que tot cicle descompon en producte de transposicions i aplicar el teorema 5.7. I això és fàcil ja que

$$(a_1, a_2, \ldots, a_n) = (a_1, a_2) \circ (a_2, a_3) \circ \cdots \circ (a_{n-2}, a_{n-1}) \circ (a_{n-1}, a_n). \qquad \square$$

Teorema 5.10. *La paritat del nombre de transposicions en que descompon una permutació és un invariant.*

Demostració.[1] Suposem que una permutació σ descompon de dues maneres diferents com a producte de transposicions,

$$\sigma = \tau_1 \circ \cdots \circ \tau_k = \nu_1 \circ \cdots \circ \nu_s. \tag{5.1}$$

Volem demostrar que k és parell si i només si s és parell.

Composant per la dreta primer amb ν_s, després amb ν_{s-1}, i així successivament obtenim

$$\tau_1 \circ \cdots \circ \tau_k \circ \nu_s \circ \cdots \circ \nu_1 = id$$

ja que $\nu_i^2 = id$. És a dir, tindríem la identitat descomposta en producte de $k + s$ transposicions.

Tot està, doncs, en demostrar que si la identitat descompon en producte de r transposicions

$$id = t_1 \circ \cdots \circ t_r$$

llavors r és parell, ja que llavors tindrem $k + s$ parell i això implica que k i s són tots dos parells o tots dos imparells.

Sigui $m \in \{1, 2, \ldots, n\}$. Sigui t_j la primera transposició, contant per la dreta, on apareix m. És a dir, $\tau_j = (m, x)$. Mirem ara la transposició següent, es a dir, τ_{j-1}, ja que estem anant de dreta a esquerra.

[1] Aquesta demostració es deu a W. I. Miller, *Even and odd permutations,* Mathematics Associations of two-year Colleges, 1971. Reproduïda al llibre *Álgebra abstracta*, de J. B. Fraleigh.

Les possibilitats per a la parella $\tau_{j-1} \circ \tau_j$ són

$$\begin{aligned}&(m,x)\circ(m,x)\\&(m,y)\circ(m,x)\\&(x,y)\circ(m,x)\\&(y,z)\circ(m,x)\end{aligned}$$

Però és fàcil veure que

$$\begin{aligned}(m,x)\circ(m,x) &= id\\(m,y)\circ(m,x) &= (m,x)\circ(x,y)\\(x,y)\circ(m,x) &= (m,y)\circ(x,y)\\(y,z)\circ(m,x) &= (m,x)\circ(y,z)\end{aligned}$$

De manera que podem substituir $\tau_{j-1} \circ \tau_j$ per les respectives expressions que apareixen a la dreta de les igualtats anteriors.

D'aquesta manera la identitat continua descomposta en el mateix nombre r de transposicions (si estem en els cassos 2, 3 i 4 anteriors) o en $r-2$ (si estem en el primer cas dels quatre anteriors). Però el que és fonamental és que ara m apareix per primer cop, contant des de la dreta, a la transposició τ_{j-1}. Repetint el procés podríem fer que m aparegués per primer cop a τ_1, cosa impossible, ja que llavors m no quedaria fix per la identitat. Per tant, per a tot m, en realitzar el procés anterior sempre arribarà un moment en que estarem en el primer cas i dues transposicions contigües es transformaran en la identitat. És a dir, r anirà disminuint de dos en dos fins arribar a la identitat, per tant r és parell. □

Definició 5.11. *El signe d'una permutació σ és igual a*

$$sig(\sigma) = (-1)^k,$$

on k és el nombre de transposicions d'una descomposició de σ.

És a dir, el signe de σ és 1 o -1 segons σ descompongui en un nombre parell o imparell de transposicions. El teorema 5.10 ens diu que això és una bona definició.

En particular,

$$sig(\sigma \circ \tau) = sig(\sigma) \cdot sig(\tau)$$

i

$$sig(\sigma)^2 = 1$$

Càlcul pràctic del signe

Per saber el signe d'una permutació només hem d'anar reordenant la permutació i contant el nombre de salts que fem.

Per exemple, donada

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix}$$

posem

$$\begin{pmatrix} 4 & 2 & 1 & 5 & 3 \end{pmatrix}$$

Posem l'1 davant. Això ho fem amb un nombre parell de salts.

$$\begin{pmatrix} 4 & 1 & 2 & 5 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 4 & 2 & 5 & 3 \end{pmatrix}$$

A continuació posem el 2 en segon lloc. Això ho fem amb un salt.

$$\begin{pmatrix} 1 & 2 & 4 & 5 & 3 \end{pmatrix}$$

A continuació posem el 3 en tercer lloc. Això ho fem amb un nombre parell de salts.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

Com que hem necessitat un nombre imparell de salts, el signe de σ és -1.

La explicació es que cada vegada que fem un salt estem composant σ amb una transposició.

Així

$$(1,2) \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix}.$$

I

$$(1,4) \circ (1,2) \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}.$$

I

$$(2,4) \circ (1,4) \circ (1,2) \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}.$$

I

$$(3,5) \circ (2,4) \circ (1,4) \circ (1,2) \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}.$$

I

$$(3,4) \circ (3,5) \circ (2,4) \circ (1,4) \circ (1,2) \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Així

$$(3,4) \circ (3,5) \circ (2,4) \circ (1,4) \circ (1,2) \circ \sigma = id$$

d'on

$$\sigma = (1,2) \circ (1,4) \circ (2,4) \circ (3,5) \circ (3,4),$$

i $sig(\sigma) = (-1)^5 = -1$.

Tema 6

Parelles invertides i signe d'una permutació

Parelles invertides

Cada permutació $\sigma \in \mathcal{S}_n$ té assignat un nombre $P(\sigma)$ que és, per definició, el nombre de parelles *invertides per* σ. Una parella $i, j \in \{1, 2, \ldots, n\}$ es diu *invertida per* σ si $i < j$ i $\sigma(i) > \sigma(j)$.

Es pot contar fàcilment que si (a, b) és la transposició que porta a a b i b a a, llavors

$$P((a, b)) = 2(b - a) - 1.$$

En efecte,

$$(a, b) = \begin{pmatrix} 1 & \ldots & a & \ldots & b & \ldots & n \\ 1 & \ldots & b & \ldots & a & \ldots & n \end{pmatrix}$$

i per tant les parelles invertides només poden aparèixer quan contenen la a o la b, concretament són $(a, a+1), (a, a+2), \ldots, (a, b)$ i $(a+1, b), (a+2, b), \ldots, (b-1, b)$.

Com a conseqüència, el nombre de parelles invertides per una transposició és imparell.

En particular, $P((i, i+1)) = 1$, és a a dir, les transposicions d'elements consecutius tenen una única parella invertida, concretament la $(i, i+1)$. Notem també que $P(id) = 0$, ja que la identitat no inverteix cap parella.

Paritat de les parelles invertides

Considerem el polinomi

$$F(x_1, \ldots, x_n) = \prod_{i<j} (x_i - x_j).$$

Per exemple,

$$F(x,y) = x - y, \quad F(y,x) = y - x.$$

$$F(x,y,z) = (x-y)(x-z)(y-z), \quad F(y,x,z) = (y-x)(y-z)(x-z).$$

Per cada permutació σ considerem el quocient

$$\frac{F(x_{\sigma(1)},\ldots,x_{\sigma(n)})}{F(x_1,\ldots,x_n)} = \prod_{i<j} \frac{x_{\sigma(i)} - x_{\sigma(j)}}{x_i - x_j}$$

Tota parella que apareix en el numerador apareix també en el denominador (i recíprocament), en el mateix ordre o en ordre oposat segons sigui invertida o no per σ. Per tant

$$\prod_{i<j} \frac{x_{\sigma(i)} - x_{\sigma(j)}}{x_i - x_j} = (-1)^{P(\sigma)}.$$

És a dir, aquest quocient de polinomis de l'esquerra ens diu si hi ha un nombre parell o imparell de parelles invertides.

Comportament respecte el producte

Siguin σ, τ dues permutacions. Observem que

$$\begin{aligned}(-1)^{P(\sigma\tau)} &= \frac{F(x_{\sigma\tau(1)},\ldots,x_{\sigma\tau(n)})}{F(x_1,\ldots,x_n)} \\ &= \frac{F(x_{\sigma\tau(1)},\ldots,x_{\sigma\tau(n)})}{F(x_{\tau(1)},\ldots,x_{\tau(n)})} \cdot \frac{F(x_{\tau(1)},\ldots,x_{\tau(n)})}{F(x_1,\ldots,x_n)} = (-1)^{P(\sigma)}(-1)^{P(\tau)}.\end{aligned}$$

Aquest fet té com a conseqüència el resultat següent.

Teorema 6.1. *El signe d'una transposició coincideix amb la paritat del nombre de parelles invertides.*

Demostració. Suposem $\sigma = \tau_1 \circ \cdots \circ \tau_k$. Llavors

$$(-1)^{P(\sigma)} = \prod_{j=1}^{k} (-1)^{P(\tau_j)} = (-1)^k = sig(\sigma),$$

ja que, com hem vist abans, $P(\tau_j)$ és imparell. □

Com el nombre de parelles invertides és quelcom intrínsec a σ, que no depèn de com descomponem σ en producte de transposicions, aquest teorema és una nova demostració del teorema 5.10 que diu que la paritat del nombre de transposicions de qualsevol descomposició de σ és invariant.

Transposicions d'elements consecutius. Tercera demostració de la invariància de la paritat

Es basa en el fet de que tota transposició és producte de transposicions d'elements consecutius. Per exemple,

$$(2,5) = (2,3)(3,4)(4,5)(4,3)(2,3).$$

Lema 6.2. *Tota transposició descompon en producte d'un nombre imparell de transposicions d'elements consecutius.*

Demostració. Considerem la transposició (a,b) amb $a < b$. Tenim

$$(a,b) = (a,a+1)(a+1,a+2)\dots(b-1,b)(b-2,b-1)\dots(a,a+1).$$

Observem que tant davant com darrera de $(b-1,b) = (a+b-1-a,b)$ hi ha $b-a-1$ transposicions d'elements consecutius. Per tant, hem descompost (a,b) com producte d'un nombre imparell,

$$2(b-a-1)+1 = 2(b-a)-1,$$

de transposicions d'elements consecutius. □

Observem que el nombre de transposicions d'elements consecutius en que descompon (a,b) coincideix amb el nombre $P(a,b)$ de parelles invertides per la transposició (a,b).

Lema 6.3. *Per a tota permutació σ es compleix que*

$$P(\sigma \circ (i,i+1)) = P(\sigma) \pm 1.$$

Demostració. Si la parella $i, i+1$ és invertida per σ llavors no és invertida per $\sigma \circ (i,i+1)$, per tant $P(\sigma \circ (i,i+1)) = P(\sigma) - 1$. No hi ha més parelles a considerar ja que aquelles parelles que no contenen ni i ni $i+1$ són invertides per σ si i només si són invertides per $\sigma \circ (i,i+1)$. I les parelles del tipus (i,a) amb $a \neq i+1$, o $(i+1,b)$ amb $b \neq i$, no s'alteren en canviar i per $i+1$, ja que si $i < a$, també $i+1 < a$.

Finalment si la parella $i, i+1$ no és invertida per σ sí que és invertida per $\sigma \circ (i,i+1)$, és a dir, $P(\sigma \circ (i,i+1)) = P(\sigma) + 1$. □

Teorema 6.4. *La paritat del nombre de transposicions en que descompon una permutació és un invariant.*

Demostració. Sabem, per la demostració que hem donat del teorema 6.1, pàgina 62, que és suficient demostrar que si la identitat descompon com a producte de r transposicions,

$$id = t_1 \circ \dots \circ t_r$$

llavors r és parell.

Utilitzant ara la descomposició de les transposicions com a producte de transposicions d'elements consecutius donada pel lema 6.2 tindrem

$$id = t_1 \circ \cdots \circ t_r = T_1 \circ \cdots \circ T_m$$

on T_j són transposicions d'elements consecutius i m és la suma de r nombres imparells, és a dir, $m = \overset{\bullet}{2} + r$, i per tant, m és parell si i només si r és parell.

El problema queda doncs reduït a suposar que

$$id = T_1 \circ \cdots \circ T_m$$

amb T_j transposicions d'elements consecutius i demostrar que m és parell.

Aplicant el lema anterior tenim

$$P(T_1 \circ \cdots \circ T_m) = P(T_1 \circ \cdots \circ T_{m-1}) \pm 1 = P(T_1 \circ \cdots \circ T_{m-2}) \pm 1 \pm 1, \ldots$$

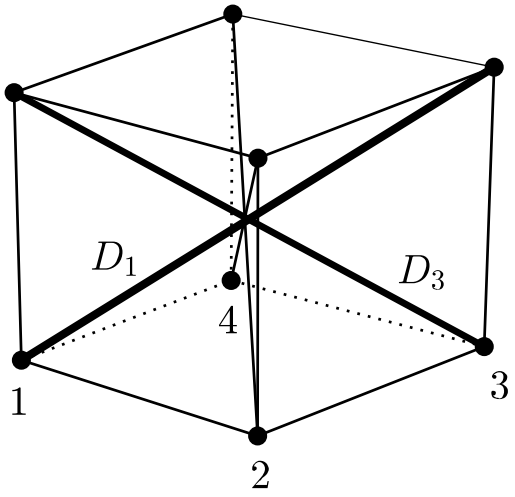
Això vol dir que aquest nombre és una suma de m cops ± 1, però el valor final ha de ser 0 ja que $P(id) = 0$, per tant, hi ha tants $+1$ com -1, i per tant m és parell, com volíem. □

Tema 7

S_4

S_3 es pot interpretar com el grup de les permutacions dels vèrtexs d'un triangle equilàter per moviments que deixen invariant el triangle. Concretament els sis elements corresponen a les tres simetries respecte de les tres altures (elements d'ordre 2), els dos girs de 120° respecte del baricentre clockwise i counterclockwise (elements d'ordre 3), més la identitat.

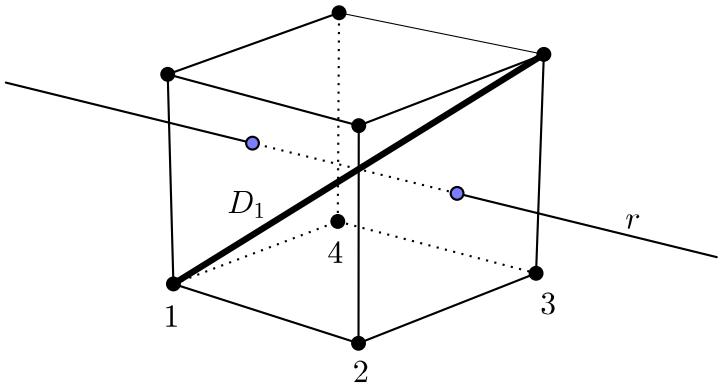
S_4 es pot interpretar com el grup de les permutacions de les diagonals del cub, per moviments que deixen invariant el cub.



Els 24 elements de S_4 són:

ordre 1	ordre 2	ordre 2	ordre 3	ordre 4
id	(1,2)	(1,2)(3,4)	(1,2,3)	(1,2,3,4)
	(1,3)	(1,3)(2,4)	(1,3,2)	(1,2,4,3)
	(1,4)	(1,4)(2,3)	(2,3,4)	(1,3,2,4)
	(2,3)		(2,4,3)	(1,3,4,2)
	(2,4)		(1,2,4)	(1,4,2,3)
	(3,4)		(1,3,4)	(1,4,3,2)
			(1,4,2)	
			(1,3,4)	

Els elements d'ordre 4 corresponen a rotacions de 90 graus al voltant de rectes perpendiculars a les cares en el seu punt mitjà, com la recta r de la figura. Hi ha tres d'aquestes rectes i dos possibilitats de gir que donen el sis elements d'ordre 4.



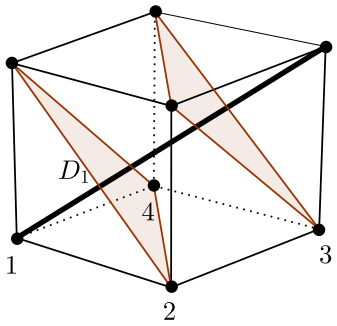
Observem, per exemple, que si girem 90° al voltant de r en el sentit de les agulles del rellotge la diagonal D_1 passa a la D_3, la D_3 passa a la D_2 i la D_4 a la D_1. Representa la permutació $(1, 3, 2, 4)$. Si girem en sentit contrari obtenim $(1, 4, 2, 3)$

Els elements d'ordre 2 sense punts fixos corresponen a aquestes mateixes rotacions però girant ara 180°.

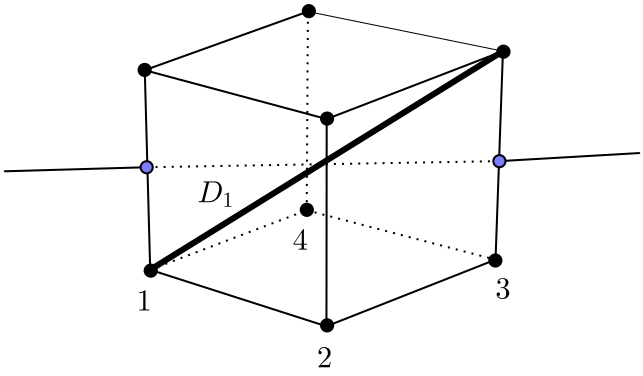
Observem, per exemple, que si girem 180° al voltant de r en el sentit de les agulles del rellotge la diagonal D_1 passa a la D_2 i la D_3 a la D_4. Representa doncs la permutació $(1, 2) \circ (2, 4)$.

Els elements d'ordre 3 corresponen a rotacions de 60 graus al voltant de les diagonals. Com hi ha 4 diagonals i dos sentits de gir obtenim els 8 elements d'ordre 3.

Per exemple, si girem 120 graus al voltant de D_1 la diagonal D_2 va a la D_4, la D_3 a la D_2, i la D_4 a la D_3. Es tracta, doncs, de l'element $(2, 4, 3)$.



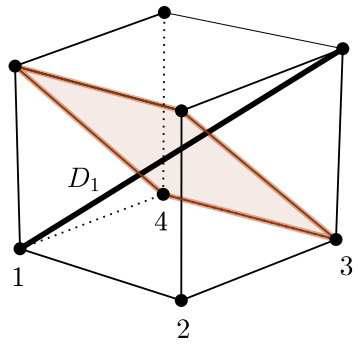
Els elements d'ordre 2 amb punts fixos es poden interpretar com girs de 180° al voltant dels eixos que passen pels punts mitjans d'arestes paral·leles oposades.



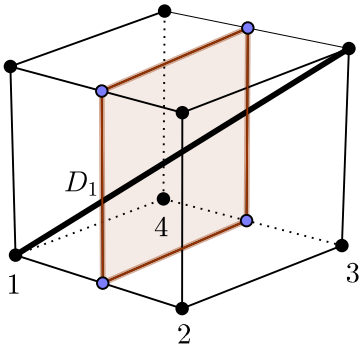
A la figura, les diagonals D_2 i D_4 són fixes, i D_1 va a D_3, i.e. es tracte de l'element $(1, 3)$.

Nota. Una altra manera d'interpretar els elements d'ordre 2, però que no dóna lloc a un morfisme de grups entre S_4 i $SO(3)$ (com vol el Carles Broto) és la següent.

Els elements d'ordre 2 amb punts fixos es poden interpretar com simetries respecte de plans determinats per arestes oposades. A la figura, les diagonals D_3 i D_4 són fixes, per estar contingudes al pla de simetria, i D_1 va a D_2, i.e. es tracte de l'element $(1, 2)$.



Els elements d'ordre 2 sense punts fixos es poden interpretar com simetries respecte de plans perpendiculars a les arestes en els seus punts mitjans. A la figura, les diagonals D_1 i D_2 es permuten, així com les D_3 i D_4, i.e. es tracte de l'element $(1, 2)$.



Tema 8

Relacions d'equivalència

8.1 Definicions. Conjunt quocient

Sigui X un conjunt. Una *correspondència* entre els elements de X és un subconjunt $\mathcal{R}$ de $X \times X$.

Si $(x, y) \in \mathcal{R}$ es diu que els elements $x, y \in X$ estan relacionats. En aquest cas escriurem $x \sim y$.

Definició 8.1. *Una correspondència entre els elements de X es diu que és una* relació d'equivalència *si es compleixen les tres condicions següents.*

1. *Reflexiva.* $x \sim x, \quad \forall x \in X.$
2. *Simètrica.* $x \sim y \Rightarrow y \sim x, \quad \forall x, y \in X.$
3. *Transitiva.* $(x \sim y, y \sim z) \Rightarrow x \sim z, \quad \forall x, y, z \in X.$

Observem que la propietat 1 ens diu que tots els elements (x, x) de la diagonal de $X \times X$ pertanyen a $\mathcal{R}$, el subconjunt de $X \times X$ que ens defineix la correspondència, i la propietat 2 ens diu que els subconjunt $\mathcal{R}$ és simètric respecte de la diagonal de $X \times X$.

Definició 8.2. *Sigui $\mathcal{R}$ una relació d'equivalència a X i sigui $x \in X$. La* classe *de x és el subconjunt de X donat per*

$$[x] = \{y \in X; y \sim x\}.$$

Veiem que classes diferents són disjuntes.

Proposició 8.3. *Siguin $x, y \in X$. Llavors $[x] = [y]$, o $[x] \cap [y] = \emptyset$.*

Demostració. Suposem primer $x \sim y$. Per veure $[x] \subseteq [y]$ prenem $z \in [x]$. Això vol dir $z \sim x$. Per la propietat transitiva, $z \sim y$, és a dir, $z \in [y]$.

El mateix argument mostra la inclusió contrària.

Suposem ara $x \not\sim y$. Per veure $[x] \cap [y] = \emptyset$ suposem que existís $z \in [x] \cap [y]$. Llavors $z \sim x$ i $z \sim y$. Per la propietat simètrica, $x \sim z$ i $z \sim y$, i per la propietat transitiva $x \sim y$, contradicció. Per tant, aquest z no pot existir i la intersecció és buida. □

Com que la igualtat

$$X = \bigcup_{x \in X} [x]$$

és clara, és a dir, X és igual a la unió de les seves classes, i aquestes són disjuntes, diem que les classes formen una *partició* de X.

Recíprocament, si tenim $X = \bigcup_{i \in I} X_i$, on I és un conjunt arbitrari d'índexs, amb $X_i \cap X_j = \emptyset$, $i \neq j$, llavors podem definir una relació sobre X, que serà d'equivalència, definint

$$x \sim y \Leftrightarrow \text{existeix } i \in I \text{ tal que } x, y \in X_i$$

Conjunt quocient

Sigui $\mathcal{R}$ una relació d'equivalència a X. El conjunt que té per elements les classes d'equivalència dels elements de X es denota per $X/\sim$, és a dir,

$$X/\sim = \{[x]; x \in X\},$$

i es diu que és el *conjunt quocient* de X determinat per la relació d'equivalència $\mathcal{R}$.

Exemple 8.1. A $\mathbb{R}^2$ definim la relació

$$P \sim Q \Leftrightarrow d(O, P) = d(O, Q), \quad \forall P, Q \in \mathbb{R}^2$$

on $O = (0, 0)$ i d és la funció distància.

És fàcil veure que és d'equivalència.

La classe d'un punt $P \in \mathbb{R}^2$ és

$$[P] = \{X \in \ R^2; X \sim P\} = \{X \in \ R^2; d(O, P) = d(O, X)\},$$

i és clar que aquest conjunt és la circumferència de centre O i radi $d(O, P)$.

$\mathbb{R}^2$ és la unió disjunta d'aquestes circumferències concèntriques (incloent la de radi 0).

Per tant, el conjunt quocient $\mathbb{R}^2/\sim$ és el conjunt que té per elements aquestes circumferències.

Cada circumferència, que té infinits punts de $\mathbb{R}^2$, passa a ser *un sol punt* de $R^2/\sim$.

Observem que tenim una aplicació bijectiva entre $X/\sim$ i l'interval $[0, \infty) \subset \mathbb{R}$. Concretament, a cada classe d'equivalència, que és un cercle de centre l'origen i radi $r \in \mathbb{R}$, li associem el punt $r \in [0, \infty)$.

Exemple 8.2 (Espai Projectiu). A $\mathbb{R}^2 \setminus \{(0,0)\}$ definim la relació

$$(x,y) \sim (x',y') \Leftrightarrow \exists \lambda \in \mathbb{R}, \lambda \neq 0, (x',y') = \lambda(x,y).$$

Veiem que és una relació d'equivalència.

Reflexiva. $(x,y) \sim (x,y)$ ja que prenent $\lambda = 1$ tenim $(x,y) = \lambda(x,y)$.

Simètrica. Si $(x,y) \sim (x',y')$, existeix $\lambda \in \mathbb{R}$, $\lambda \neq 0$, tal que $(x',y') = \lambda(x,y)$. Per tant, $(x,y) = \lambda^{-1}(x',y')$, i així $(x',y') \sim (x,y)$.

Transitiva. Si $(x',y') = \lambda(x,y)$ amb $\lambda \neq 0$, i $(x'',y'') = \mu(x',y')$ amb $\mu \neq 0$, llavors

$$(x'',y'') = \mu\lambda(x,y),$$

amb $\mu\lambda \neq 0$.

Mirem com són les classes. Si $(a,b) \in \mathbb{R}^2 \setminus \{(0,0)\}$, llavors

$$[(a,b)] = \{(x,y); (x,y) = \lambda(a,b), \lambda \in \mathbb{R}, \lambda \neq 0\}.$$

Geomètricament es tracta de la recta determinada pels punts $(0,0)$ i (a,b), excepte el $(0,0)$. O, equivalentment, dues semirectes per l'origen de direccions (a,b) i $-(a,b)$ respectivament.

Per tant, el conjunt quocient és el conjunt que té per elements aquestes rectes. Cada recta, que té infinits punts de $\mathbb{R}^2$, passa a ser *un sol punt* de $R^2 \setminus \{(0,0)\}/\sim$.

Per estudiar més detalladament aquest conjunt observem que totes les classes tenen exactament dos representants de mòdul 1, ja que

$$(a,b) \sim \pm\frac{1}{\sqrt{a^2+b^2}}(a,b).$$

És a dir, tenim dos punts antipodals de $S^1 = \{x \in \mathbb{R}^2; \|x\| = 1\}$ per cada classe d'equivalència.

Definim a S^1 una relació, que serà d'equivalència, posant

$$x \approx y \Leftrightarrow x = \pm y.$$

És a dir, relacionem cada punt amb ell mateix i l'antipodal. Denotem $P^1 = S^1/\approx$ el conjunt quocient de S^1 per aquesta relació d'equivalència.[1]

Tenim una aplicació bijectiva

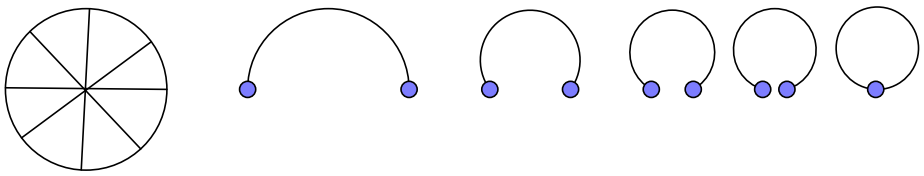
$$(\mathbb{R}^2 \setminus \{(0,0)\})/\sim \quad \longrightarrow \quad S^1/\approx$$

assignant a un dels dos representants de mòdul 1 de cada classe la seva classe a $S^1/\approx$. Aquesta aplicació, que no estaria ben definida si el conjunt imatge fos S^1, ja que dependria del representant, sí que està ben definida

[1] En general es denota P^n l'espai quocient de l'esfera S^n per la relació d'equivalència que identifica punts antipodals. Es diu que P^n és l'espai projectiu de dimensió n. Veureu a topologia que P^1 és *homeomorf* a S^1 però que això no és cert per a cap altre valor de n.

quan l'espai imatge és $S^1/\approx$, ja que les dues imatges que eren diferents a S^1 coincideixen en el quocient.

Podem pensar el conjunt quocient $S^1/\approx$ és a dir, S^1 amb els punts antipodals identificats, com un semicercle amb els dos punts extrems identificats. Aquesta identificació es pot fer 'realitat' pensant que el semicercle es va corbant fins fer arribar a coincidir aquest dos extrems en un sol punt, com indica la figura. Aquesta meravella no es pot fer en dimensions superiors, com hem dit al peu de pàgina.



El conjunt quocient $(\mathbb{R}^2 \setminus \{(0,0)\})/\sim$ és, doncs, el conjunt de rectes per l'origen de $\mathbb{R}^2$. Podem establir una bijecció entre aquest conjunt i $[0,\pi)$ associant a cada classe

8.2 L'anell $\mathbb{Z}$ dels nombres enters

Un altre exemple, molt important, de conjunt quocient apareix quan construïm el conjunt $\mathbb{Z}$ dels nombres enters a partir del conjunt $\mathbb{N}$ dels nombres naturals.

Per facilitar posteriorment la notació suposarem que $0 \in \mathbb{N}$. Equival a reescriure els axiomes de Peano canviant 1 per 0, i definint $n + 0 = n$. També posarem, a l'hora de definir producte, $n \cdot 0 = 0$. Així, doncs,

$$\mathbb{N} = \{0, 1, 2, \dots\}.$$

Considerem a $\mathbb{N} \times \mathbb{N}$ la relació següent:

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c.$$

Deixem com exercici veure que aquesta relació és una relació d'equivalència.

Conjunt quocient

Denotem el conjunt quocient per $\mathbb{Z}$, és a dir, posem

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim .$$

L'estructura d'anell de $\mathbb{Z}^2$

En aquest conjunt quocient hi podem definir dues operacions, la primera anomenada suma i la segona producte, de la manera següent.

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}$$

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)}$$

Deixem com exercici veure que aquestes definicions no depenen dels representants que s'elegeixin en cada classe.

Observem que l'element neutre de la suma és la classe

$$\overline{(0,0)}$$

i l'element neutre del producte és la classe

$$\overline{(1,0)}$$

L'oposat respecte de la suma de $\overline{(a,b)}$ és $\overline{(b,a)}$ ja que

$$\overline{(a,b)} + \overline{(b,a)} = \overline{(a+b, a+b)} = \overline{(0,0)}.$$

Així doncs, $\mathbb{Z}$ respecte de la suma és un *grup* (commutatiu). I, clarament, $\mathbb{Z}$ respecte la suma i el producte, és un *anell* (commutatiu). Vegeu les definicions de grup i anell a la pàgina 79.

Representant canònic. Observem que si $a \geq b$ llavors

$$\overline{(a,b)} = \overline{(a-b, 0)}.$$

(sabem restar nombres naturals només quan el primer és més gran que els segon). Anàlogament, si $a \leq b$ llavors

$$\overline{(a,b)} = \overline{(0, b-a)}.$$

Així, en tota classe, hi ha un representant amb un zero a la primera component o un representant amb un zero a la segona component. Es diu que és el representant canònic de la classe.

Notació. La classe $\overline{(a,0)}$ la denotarem per a. La classe $\overline{(0,a)}$ la denotarem per $-a$. Per això $\mathbb{Z}$ s'escriu com

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Amb aquesta notació observem que

$$(-a) \cdot (-b) = \overline{(0,a)} \cdot \overline{(0,b)} = \overline{(ab,0)} = ab$$

[2] Vegeu les definicions de grup, anell i cos a la secció 8.5, pàgina 79.

$\mathbb{N}$ *com subconjunt de* $\mathbb{Z}$.
L'aplicació

$$\varphi : \mathbb{N} \longrightarrow \mathbb{Z}$$

donada per

$$\varphi(n) = n = \overline{(n, 0)}$$

és un morfisme injectiu. És a dir, és injectiva, i conserva la suma i el producte,

$$\begin{aligned} \varphi(m+n) &= \varphi(m) + \varphi(n), \\ \varphi(m \cdot n) &= \varphi(m) \cdot \varphi(n). \end{aligned}$$

Deixem els detalls al lector.

8.3 Criteri de divisibilitat d'Euclides

Teorema 8.4. *Siguin* $D, d \in \mathbb{Z}$*, amb* $d \neq 0$*. Llavors existeixen dos únics enters* q, r *tals que*

$$D = dq + r, \quad 0 \leq r < |d|.$$

(Es diu que D *és el dividend,* d *el divisor,* q *el quocient i* r *el residu).*

Demostració. Existència. Primer cas, $D > 0, d > 0$. Definim el subconjunt S de $\mathbb{N}$ (ampliat amb el 0) següent:

$$S = \{x \in \mathbb{N}; x = D - dn, n \in \mathbb{Z}\}.$$

Primer observem que $S \neq \emptyset$, ja que $D \in S$ (només hem d'agafar $n = 0$). Sigui r el primer element de S. En particular,

$$r = D - dq, \quad q \in \mathbb{Z}.$$

Aquest r compleix que $r < d$. En efecte, si $r \geq d$ tindríem

$$0 \leq r - d = D - dq - d = D - d(q + 1)$$

i per tant $r - d \in S$, en contradicció amb que r sigui el primer element. Això demostra l'existència de q i r quan $D > 0, d > 0$.

Existència. Segon cas, $D < 0, d > 0$. Apliquem el cas anterior a $-D$. Tenim

$$-D = dq + r, \quad 0 \leq r < d.$$

Canviant el signe

$$D = d(-q) - r = d(-q) - d + d - r = d(-q - 1) + (d - r)$$

i com $0 \leq d - r < d$, ja hem escrit D com volíem. Això demostra l'existència de q i r quan $D < 0, d > 0$.

Existència. Tercer cas, $d < 0$. Apliquem el cas anterior corresponent a D i $-d$. Tenim

$$D = (-d)q + r, \quad 0 \leq r < |d|.$$

Però això es pot escriure com

$$D = d(-q) + r, \quad 0 \leq r < |d|.$$

i hem acabat.

Unicitat. Suposem

$$\begin{aligned} D &= dq_1 + r_1, \quad 0 \leq r_1 < |d|, \\ D &= dq_2 + r_2, \quad 0 \leq r_2 < |d|. \end{aligned}$$

Restant obtenim

$$0 = d(q_1 - q_2) + (r_1 - r_2).$$

Equivalentment

$$r_1 - r_2 = d(q_2 - q_1).$$

Però $r_1 - r_2$ és la diferència de dos elements de l'interval $[0, |d|)$ i per tant $r_1 - r_2 < |d|$. L'únic múltiple de d més petit que $|d|$ és 0, per tant ha de ser $q_1 = q_2$, i això implica $r_1 = r_2$. □

8.4 L'anell $\mathbb{Z}/(m)$

Un altre exemple, molt important, de conjunt quocient apareix quan estudiem els possibles residus que apareixen en dividir nombres enters entre un mateix nombre fixat m.

Sigui $m \in \mathbb{Z}$. Definim la relació

$$x \sim y \Leftrightarrow x - y = \overset{\bullet}{m}.$$

Veiem que és d'equivalència.

Reflexiva. $x \sim x$. Hem de veure que $x - x$ és múltiple de m, però això és clar, ja que $x - x = m \cdot 0$.

Simètrica. $x \sim y \Rightarrow y \sim x$. Hem de veure que si $x - y$ és múltiple de m, $x - y = mk$, llavors $y - x$ també és múltiple de m, però això és clar, ja que $y - x = m(-k)$.

Transitiva. $(x \sim y, y \sim z) \Rightarrow x \sim z, \quad \forall x, y, z \in \mathbb{Z}$. Hem de veure que si $x - y$ és múltiple de m, $x - y = mk$, i si $y - z$ és múltiple de m, $y - z = mr$, llavors $x - z$ també és múltiple de m, però això és clar, ja que

$$x - z = x - y + y - z = m(k + r).$$

Com $x \sim y$ si i només si $y = x + \overset{\bullet}{m}$, tenim que

$$[x] = \{x, x \pm m, x \pm 2m, x \pm 3m, \dots\}.$$

Pel criteri de divisibilitat d'Euclides, Teorema 8.4, sabem que per tot $D \in \mathbb{Z}$, existeixen $q, r \in Z$ únics tals que

$$D = mq + r, \quad 0 \leq r < m$$

Per tant, $D - r = \overset{\bullet}{m}$, és a dir, $D \sim r$, que és llegeix dient que *tot nombre enter és equivalent al residu de la seva divisió per* m. Com $0 \leq r < m$, en tota classe d'equivalència hi ha un representant més gran o igual a zero i estrictament més petit que m, és l'anomenat *representant canònic*.

També és clar que només poden haver-hi m classes d'equivalència diferents:

$$\begin{aligned}
[0] &= \{0, \pm m, \pm 2m, \pm 3m, \dots\} \\
[1] &= \{1, 1 \pm m, 1 \pm 2m, 1 \pm 3m, \dots\} \\
[2] &= \{2, 2 \pm m, 2 \pm 2m, 2 \pm 3m, \dots\} \\
\vdots &= \vdots \\
[m-1] &= \{m-1, m-1 \pm m, m-1 \pm 2m, m-1 \pm 3m, \dots\}
\end{aligned}$$

Per exemple, si $m = 2$ tenim dues classes

$$\begin{aligned}
[0] &= \{\dots, -2, 0, 2, 4, \dots\} \\
[1] &= \{\dots, -1, 1, 3, 5, \dots\}
\end{aligned}$$

Si $m = 3$ tenim tres classes

$$\begin{aligned}
[0] &= \{0, \pm 3, \pm 6, \pm 9, \dots\} = \{\dots, -6, -3, 0, 3, 6, \dots\} \\
[1] &= \{1, 1 \pm 3, 1 \pm 6, 1 \pm 9, \dots\} = \{\dots, -5, -2, 1, 4, 7, \dots\} \\
[2] &= \{2, 2 \pm 3, 2 \pm 6, 2 \pm 9, \dots\} = \{\dots, -4, -1, 2, 5, 8, \dots\}
\end{aligned}$$

Notació. Quan $x \sim y$ per la relació d'equivalència

$$x \sim y \Leftrightarrow y - x = \overset{\bullet}{m},$$

escrivim

$$x \equiv y \pmod{m}$$

i diem que x i y són *congruents mòdul* m.

Proposició 8.5. *$a \equiv b \pmod{m}$ si i només si en dividir a entre m i b entre m obtenim el mateix residu.*

Demostració. Suposem primer que $a - b = \overset{\bullet}{m}$, i fem les divisions indicades. Tenim

$$\begin{aligned}
a &= mq_1 + r_1, \quad 0 \leq r_1 < m, \\
b &= mq_2 + r_2, \quad 0 \leq r_2 < m.
\end{aligned}$$

Restant,

$$a - b = m(q_1 - q_2) + (r_1 - r_2).$$

Com $a - b$ és múltiple de m, d'aquesta igualtat deduïm que

$$r_1 - r_2 = \overset{\bullet}{m}.$$

Però pel mateix argument que hem fet en demostrar la unicitat del teorema 8.4, aquest múltiple de m ha de ser 0, i per tant $r_1 = r_2$, com volíem.

Recíprocament, si

$$\begin{aligned} a &= mq_1 + r, \quad 0 \leq r < m, \\ b &= mq_2 + r, \quad 0 \leq r < m, \end{aligned}$$

restant obtenim $a - b = \overset{\bullet}{m}$ com volíem. □

Conjunt quocient

El conjunt quocient, que no es denota $\mathbb{Z}/\sim$ sinó $\mathbb{Z}/(m)$, consisteix en

$$\begin{aligned} \mathbb{Z}/(2) &= \{[0],[1]\} \\ \mathbb{Z}/(3) &= \{[0],[1],[2]\} \\ \mathbb{Z}/(4) &= \{[0],[1],[2],[3]\} \\ &\vdots \\ \mathbb{Z}/(m) &= \{[0],[1],[2],\ldots,[m-1]\} \end{aligned}$$

etc.

Observem que $\mathbb{Z}/(m)$ té m elements.

Notació. Hem denotat $[x]$ a la classe de $x \in \mathbb{Z}$, la qual és un subconjunt de $\mathbb{Z}$. En canvi, quan posem

$$[x] \in \mathbb{Z}/(m)$$

la classe de x, $[x]$, passa a ser un *element* del conjunt $\mathbb{Z}/(m)$. Per evitar aquesta possible confussió, quan consideri les classes com elements del conjunt quocient, escriurem $\overline{x} \in \mathbb{Z}/(m)$ en lloc de $[x] \in \mathbb{Z}/(m)$. És a dir,

$$\begin{aligned} \mathbb{Z}/(2) &= \{\overline{0},\overline{1}\} \\ \mathbb{Z}/(3) &= \{\overline{0},\overline{1},\overline{2}\} \\ \mathbb{Z}/(4) &= \{\overline{0},\overline{1},\overline{2},\overline{3}\} \end{aligned}$$

etc.

L'estructura d'anell de $\mathbb{Z}/(m)$

El que fa interessant el conjunt quocient $\mathbb{Z}/(m)$ és que s'hi pot definir, de manera natural, una suma i un producte i respecte d'aquestes operacions $\mathbb{Z}/(m)$ serà un anell.

Sigui π la projecció canònica

$$\begin{array}{rccc} \pi: & \mathbb{Z} & \longrightarrow & \mathbb{Z}/(m) \\ & x & \mapsto & \overline{x} \end{array}$$

Definició de suma

Siguin $\overline{x}, \overline{y} \in \mathbb{Z}/(m)$. Definim

$$\overline{x} + \overline{y} = \overline{x + y}.$$

Aquesta definició és correcta, en el sentit de que no depèn del representat elegit. En efecte, si $\overline{x} = \overline{z}$ i $\overline{y} = \overline{t}$ llavors $z = x + \overset{\bullet}{m}$ i $t = y + \overset{\bullet}{m}$. Per tant, $z + t = x + y + \overset{\bullet}{m}$ i

$$\overline{z + t} = \overline{x + y}.$$

Observem que la definició de suma es pot escriure com

$$\pi(x) + \pi(y) = \pi(x + y),$$

de manera que π és morfisme respecte de la suma.

Definició de producte

Siguin $\overline{x}, \overline{y} \in \mathbb{Z}/(m)$. Definim

$$\overline{x} \cdot \overline{y} = \overline{xy}.$$

Aquesta definició és correcta, en el sentit de que no depèn del representat elegit. En efecte, si $\overline{x} = \overline{z}$ i $\overline{y} = \overline{t}$ llavors $z = x + \overset{\bullet}{m}$ i $t = y + \overset{\bullet}{m}$. Per tant, $zt = xy + \overset{\bullet}{m}$ i

$$\overline{zt} = \overline{xy}.$$

Observem que la definició de producte es pot escriure com

$$\pi(x) \cdot \pi(y) = \pi(xy),$$

de manera que π és morfisme respecte del producte, i per tant, morfisme d'anells.

Exemple 8.3. *Taules de sumar i multiplicar de* $\mathbb{Z}/4$ *i* $\mathbb{Z}/5$.

$\mathbb{Z}/(4),+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}/(4),\bullet$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}/(5),+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\mathbb{Z}/(5),\bullet$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Veurem més endavant la gran diferència que hi ha en l'estructura de $\mathbb{Z}/(m)$ segons m sigui primer o no. Per exemple, mirant la taula de multiplicar de $\mathbb{Z}/(5)$, ometent el producte per 0, veiem que multiplicar és permutar. Si multipliquem elements diferents de zero obtenim elements diferents de zero. En canvi, això no és cert a $\mathbb{Z}/(4)$. Veurem que si m és primer $\mathbb{Z}/(m)$ és un cos.

Criteris de divisibilitat

Una de les aplicacions immediates de $\mathbb{Z}/(m)$ és la seva gran utilitat per donar criteris de divisibilitat. A [10] en podeu trobar diversos. Donem ara, només com exemple, el criteri de divisibilitat per 3.

Proposició 8.6. *Un nombre escrit en base decimal és divisible per* 3 *si i només si la suma dels seus dígits és divisible per* 3*.*

Demostració. En efecte, només cal veure que

$$n = a_k \dots a_1 a_0 = \sum_{i=0}^{k} a_i 10^i,$$

pensat a $\mathbb{Z}/3$ és

$$\overline{n} = \overline{a_k} + \cdots + \overline{a_0} = \overline{a_k + \cdots + a_0},$$

ja que la classe de 10, i les seves potències, a $\mathbb{Z}/(3)$, és $\overline{1}$.

Com que un nombre és divisible per 3 si i només si la seva classe mòdul 3 és zero, hem acabat. □

8.5 Grup, anell, domini d'integritat i cos

Un **grup** és un conjunt G en el que hi definida una operació "+"

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ a\,,\, b & \mapsto & a+b \end{array}$$

que compleix les propietats

$$\begin{aligned} a+(b+c) &= (a+b)+c && \text{Asociativa} \\ a+0 &= 0+a=a && \text{Existeix element neutre} \\ a+(-a) &= (-a)+a=0 && \text{Existeix element oposat} \end{aligned}$$

Si, a més, $a+b=b+a$ per a tota parella $a,b\in G$, es diu que el grup és *commutatiu* o *abelià*.

Si en lloc d'utilitzar el signe "+" per denotar aquesta operació s'utilitza el signe "$\cdot$", es diu que utilitzem notació multiplicativa, i l'element neutre es denota per 1 i l'oposat de a per a^{-1}. També s'utilitza molt la lletra e per denotar l'element neutre del grup.

Un **anell** és un conjunt A en el que hi ha definides dues operacions "+" i "$\cdot$" tals que $(A,+)$ és un grup abelià, i

$$\begin{aligned} a\cdot(b\cdot c) &= (a\cdot b)\cdot c && \text{Asociativa} \\ a\cdot 1 &= 1\cdot a=a && \text{Existeix element neutre} \\ a\cdot(b+c) &= a\cdot b+a\cdot c && \text{Distributiva per la dreta} \\ (b+c)\cdot a &= b\cdot a+c\cdot a && \text{Distributiva per l'esquerra} \end{aligned}$$

Si, a més, $a\cdot b=b\cdot a$, per a tota parella $a,b\in A$, diem que A és un anell commutatiu.

Diem que un element a d'un anell A, $a\neq 0$, és un **divisor de zero** si existeix $b\in A$, $b\neq 0$, tal que $a\cdot b=0$. En aquets cas, evidentment, també b és un divisor de zero. Per exemple, $\overline{2}$ és un divisor de zero a $\mathbb{Z}/(4)$ ja que $\overline{2}\cdot\overline{2}=\overline{0}$.

Un **domini d'integritat** és un anell commutatiu sense divisors de zero. Per exemple $\mathbb{Z}$, o $\mathbb{Z}/(5)$.

Un **cos** és un anell tal que tot element (excepte el neutre de la suma) té invers respecte del producte. Per exemple, $\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}/(5)$.

Teorema 8.7 (Weddenburn)**.** *Tot domini d'integritat finit és un cos.*

Demostració. Sigui $a\neq 0$. Volem veure que té invers. Considerem la successió $a,a^2,a^3,\ldots$. Com té infinits elements i el domini un nombre finit existeixen $m<n$ tals que $a^m=a^n$. Llavors

$$0=a^m-a^n=a^m(1-a^{n-m}).$$

Per ser domini d'integritat ha de ser $a^m=0$ o $1=a^{n-m}$. Però $a^m=0$ no es pot donar ja que llavors a seria divisor de zero. Per tant, ha de ser $1=a^{n-m}$, i això ens diu que a té invers ja que

$$1=a(a^{n-m-1}). \qquad \square$$

8.6 El cos $\mathbb{Q}$ del nombres racionals

El conjunt $\mathbb{Q}$ dels nombres racionals es pot introduir com el conjunt quocient

$$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^* / \sim$$

on

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

(Comproveu que aquesta relació és d'equivalència).

En aquest conjunt quocient s'hi pot introduir una suma i un producte per

$$\begin{aligned} \overline{(a,b)} + \overline{(c,d)} &= \overline{(ad+bc, bd)} \\ \overline{(a,b)} \cdot \overline{(c,d)} &= \overline{(ac, bd)}. \end{aligned}$$

Deixem com exercici veure que aquestes definicions són correctes, en el sentit de que no depenen del representant escollit.

La classe $\overline{(0,1)}$ és l'element neutre de la suma i la classe $\overline{(1,1)}$ és l'element neutre del producte. Tot element, diferent del $\overline{(0,1)}$, té invers, ja que

$$\overline{(a,b)} \cdot \overline{(b,a)} = \overline{(1,1)}.$$

A partir d'aquí es comprova fàcilment que $(\mathbb{Q}, +, \cdot)$ és un cos.

Observem que l'aplicació $\varphi : \mathbb{Z} \longrightarrow \mathbb{Q}$ donada per

$$\varphi(a) = \overline{(a,1)}$$

és un morfisme d'anells injectiu. Això permet pensar $\mathbb{Z} \subset \mathbb{Q}$.

També podem definir una relació d'ordre a $\mathbb{Q}$, que respecte l'ordre de $\mathbb{Z}$, definint

$$\overline{(a,b)} \leq \overline{(c,d)} \Leftrightarrow ad \leq bc.$$

Notació. La classe $\overline{(a,b)}$ es denota per $\dfrac{a}{b}$. A més, si $0 \leq a \leq 9$ posarem

$$\begin{aligned} \overline{(a,10)} &= \frac{a}{10} = 0,a \\ \overline{(a,100)} &= \frac{a}{100} = 0,0a \\ \overline{(a,1000)} &= \frac{a}{1000} = 0,00a \end{aligned}$$

etc. La notació decimal amb comes

$$0, abc\cdots = \frac{a}{10} + \frac{b}{100} + \frac{c}{1000} + \ldots$$

va ser introduïda per l'astrònom Giovanni Antonio Magini sobre el 1600.

Però que té que veure la notació $\dfrac{D}{d}$ amb la divisió euclidiana de D entre d?

Si casualment $D, d \in \mathbb{Z}$ són divisibles, es a dir, $D = dq$, llavors $\dfrac{D}{d} = \dfrac{q}{1}$, de manera que la línia horitzontal entre D i d es pot interpretar efectivament com la divisió entera entre D i d, ja que la classe $\dfrac{q}{1}$ s'identifica amb el nombre enter q.

Si D i d no són divisibles posem

$$\begin{aligned} D &= dq_1 + r_1, & 0 \leq r_1 < d. \\ 10r_1 &= dq_2 + r_2, & 0 \leq r_2 < d. \\ 10r_2 &= dq_3 + r_3, & 0 \leq r_3 < d. \\ 10r_3 &= dq_4 + r_4, & 0 \leq r_4 < d. \\ \vdots &= \vdots \end{aligned}$$

A més, es veu fàcilment que $q_j < 10$, per tot $j > 1$. Com que tots els r_j són menors que d, un cop hàgim fet aquesta successió de divisions d vegades, i probablement abans, trobarem un r_j igual a un r_k ja considerat. A partir d'allà les divisions seran iguals a les anteriors, és a dir, es repetiran cíclicament.

Anem substituint i tenim

$$\begin{aligned} \frac{D}{d} &= q_1 + \frac{r_1}{d} = q_1 + \frac{10r_1}{10d} = q_1 + \frac{q_2}{10} + \frac{r_2}{10d} = q_1 + \frac{q_2}{10} + \frac{10r_2}{100d} \\ &= q_1 + \frac{q_2}{10} + \frac{q_3}{100} + \frac{r_3}{100d} = q_1 + \frac{q_2}{10} + \frac{q_3}{100} + \frac{10r_3}{1000d} \\ &= q_1 + \frac{q_2}{10} + \frac{q_3}{100} + \frac{q_4}{1000} + \frac{r_4}{1000d} \\ &= \dots \end{aligned}$$

Quan es comencin a repetir les r_j es repetiran també les q_j i per tant, en notació decimal, tenim

$$\frac{D}{d} = q_1,\, q_2 q_3 \dots q_\alpha \dots q_\beta q_\alpha \dots q_\beta \dots$$

Això és el que passa, per exemple, quan dividim 1 entre 7:

$$\begin{array}{llllllll} 1 & & & & & & & |7 \\ \cline{8-8} 1 & 0 & & & & & & 0,142857 \\ & 3 & 0 & & & & & \\ & & 2 & 0 & & & & \\ & & & 6 & 0 & & & \\ & & & & 4 & 0 & & \\ & & & & & 5 & 0 & \\ & & & & & & 1 & \end{array}$$

Quan obtenim residu 1 com a l'inici, els quocients ja s'aniran repetint i tenim per tant

$$\frac{1}{7} = 0, \overbrace{142857}\overbrace{142857}\dots$$

Tema 9

Combinatòria

9.1 Variacions amb repetició

Definició 9.1. *Una* variació amb repetició *és una llista* **ordenada** *de longitud r formada per n elements d'un cert conjunt Y, que es poden o no anar repetint.*

Sigui $Y = \{y_1, \ldots, y_n\}$. Una variació amb repetició de longitud r d'aquests n elements és, doncs, una r-pla $(z_1, \ldots, z_r)$ amb $z_i \in Y$.

Per exemple, si $Y = \{y_1, y_2, y_3\}$, les variacions de longitud 2 d'aquests 3 elements són: $(y_1, y_1), (y_1, y_2), (y_1, y_3), (y_2, y_1), (y_2, y_2), (y_2, y_3), (y_3, y_1), (y_3, y_2), (y_3, y_3)$.

I les variacions de longitud 4 d'aquests 3 elements són: $(y_1, y_1, y_1, y_1), (y_1, y_1, y_1, y_2), (y_1, y_1, y_1, y_3), (y_1, y_1, y_2, y_1)$, etc.

Anem a comptar quantes variacions amb repetició de longitud r, formades per n elements hi ha.

Podem pensar que tenim r posicions

$$\square \quad \square \quad \square \quad \square \quad \cdots \quad \square$$

i a cada posició hi podem posar n elements diferents. Al primer quadrat pot haver-hi qualsevol element de Y, al segon també, etc.

Per tant

$$VR_n^r = n^r.$$

Observem que aquestes llistes fetes amb elements de Y es poden interpretar com aplicacions de $\mathbb{N}_r$ a Y.

En efecte, donada una llista només hem de definir $\varphi : \mathbb{N}_r \longrightarrow Y$ per

$$\begin{aligned} \varphi(1) &= \text{L'element de } Y \text{ situat en el primer lloc,} \\ \varphi(2) &= \text{L'element de } Y \text{ situat en el segon lloc,} \\ \vdots &= \vdots \\ \varphi(r) &= \text{L'element de } Y \text{ situat en el lloc R.} \end{aligned}$$

Anàlogament, donada una aplicació $\varphi : \mathbb{N}_r \longrightarrow Y$ es confecciona fàcilment la llista corresponent.

Com que Y és bijectiu amb $\mathbb{N}_n$ podem concloure que les variacions de longitud r formades amb n elements, amb repetició, es corresponen amb les aplicacions de $\mathbb{N}_r$ a $\mathbb{N}_n$.

Exemple 1. Quantes quinieles possibles hi ha? Podem pensar que tenim una llista de 14 quadrats, i a cada quadrat hi ha un element del conjunt $Y = \{1, X, 2\}$. Per tant, $VR_3^{14} = 3^{14}$.

Exemple 2. Si X té n elements, quants elements té $\mathcal{P}(X)$? Com que hi ha una bijecció entre $\mathcal{P}(X)$ i les aplicacions de X al conjunt $\{0, 1\}$, i d'aquestes n'hi ha $VR_2^n = 2^n$, $\mathcal{P}(X)$ té 2^n elements.

9.2 Variacions

Definició 9.2. *Una* variació *és una llista* **ordenada** *de longitud r formada per n elements d'un cert conjunt Y, que no es poden repetir.*

Com les variacions amb repetició de la secció anterior, però ara els elements de Y no es poden repetir. En particular ha de ser $r \leq n$.

En aquest cas tenim r posicions

$$\square \quad \square \quad \square \quad \square \quad \cdots \quad \square$$

i al primer quadrat hi ha un element de Y (n possibilitats), al segon quadrat un element de Y diferent a l'element que ocupa el primer lloc ($n-1$ possibilitats), al tercer quadrat un element de Y diferent als elements que ocupen el primer i segon lloc ($n-2$ possibilitats), etc.

Per tant,

$$V_n^r = n(n-1)\ldots(n-(r-1)).$$

Recordant que $\binom{n}{r} = \dfrac{n!}{(n-r)!\,r!}$ tenim que

$$V_n^r = \binom{n}{r} r!$$

Exemple 1. Quants cicles d'ordre r hi ha a S_n? Els cicles s'escriuen agafant r elements del conjunt $Y = \{1, 2, \ldots, n\}$. Són llistes ordenades de

r elements que no es poden repetir. Per tant són variacions de longitud r formades per n elements, i en principi sembla que n'hi hagin, doncs,

$$V_n^r.$$

Però ara ens adonem que els cicles són cíclics!, i que per tant, llistes iguals per permutacions cícliques representen el mateix cicle (per exemple, $(y_1, y_2, y_3) = (y_2, y_3, y_1) = (y_3, y_1, y_2)$). Així la resposta correcta és

$$\text{Nombre de cicles} = V_n^r/r.$$

Observem que les variacions de longitud r formades amb elements de $Y = \{y_1, \ldots, y_n\}$ es poden interpretar com aplicacions injectives de $\mathbb{N}_r$ a Y. És la mateixa idea de la secció anterior.

En el cas particular en que $n = r$, és a dir, llistes ordenades de longitud n formades amb n elements diferents, les variacions reben el nom de **Permutacions**. Es poden interpretar, doncs, com les aplicacions bijectives[1] de $\mathbb{N}_n$ a $\mathbb{N}_n$.

9.3 Combinacions

Definició 9.3. *Una* combinació *és una llista de r objectes formada per n elements d'un conjunt Y, que no es poden repetir,* **sense importar l'ordre**.

La única diferència entre *variacions* i *combinacions* és que dues variacions que difereixen només en l'ordre, es consideren com a combinacions iguals.

Per tant

$$C_n^r = V_n^r/r! = \binom{n}{r}.$$

L'exemple paradigmàtic és el nombre de subconjunts de r elements que té un conjunt Y de n elements. Hem de fer una llista amb r elements de Y i no importa l'ordre. Per tant Y té $\binom{n}{r}$ subconjunts de r elements.

En particular, si tenim present que els subconjunts de Y es poden agrupar en els subconjunts amb cap element, els subconjunts amb un element, els subconjunts de 2 elements, etc. tenim

$$2^n = \sum_{k=0}^{n} \binom{n}{k}.$$

Si tenim present que els subconjunts de r elements de Y estan dividits entre els que contenen un element donat $a \in Y$ i els que no el contenen, tenim

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

[1] Tota aplicació injectiva de $\mathbb{N}_n$ a $\mathbb{N}_n$ és bijectiva.

Exemple 1. Calculeu el coeficient de $a^{n-k}b^k$ en el desenvolupament de $(a+b)^n$. Imaginem el producte

$$(a+b)\cdot(a+b)\ldots(a+b)$$

i pensem que per obtenir a^k hem de triar k $a's$ del producte anterior. Podem pensar que y_1 és el primer factor $(a+b)$, y_2 el segon factor $(a+b)$, etc. Elegir k $a's$ és elegir k d'aquestes y_i. Els y_i elegits no es poden repetir, i no importa l'ordre. Per tant, el coeficient és $\binom{n}{k}$. És a dir,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k$$

9.4 Combinacions amb repetició

Definició 9.4. *Una combinació amb repetició és una llista de longitud r formada per n elements d'un cert conjunt Y, que n'hi pot haver de repetits,* **sense importar l'ordre** *(si dues llistes coincideixen llevat de l'ordre són iguals).*

Suposem, per exemple, $n=3$ i $r=2$. Això vol dir que tenim un conjunt de 3 elements $Y=\{y_1,y_2,y_3\}$ i volem formar parelles del tipus (y_j,y_k), considerant-les iguals si només difereixen en l'ordre, i acceptant parelles del tipus (y_i,y_i).

En aquest cas hi ha 6 parelles possibles

$$(y_1,y_1),(y_1,y_2),(y_1,y_3),(y_2,y_2),(y_2,y_3),(y_3,y_3),$$

però com les podem contar en general?

Doncs prenent $n+r-1=4$ espais

$$\square\,\square\,\square\,\square$$

i marcant $n-1=2$ d'aquests espais. Això ho podem fer de

$$CR_n^r = \binom{n+r-1}{n-1} = \binom{4}{2}$$

maneres diferents.

Un cop fet això, els quadrats en blanc abans del primer quadrat negre s'omplen amb y_1. Els quadrats en blanc entre el primer quadrat negre i el segon s'omplen amb y_2. Els quadrats en blanc a la dreta del darrer quadrat negre s'omplen amb y_3.

$$\blacksquare\,\blacksquare\,\square\,\square \quad \longrightarrow (y_3,y_3)$$

$$\blacksquare\,\square\,\blacksquare\,\square \quad \longrightarrow (y_2,y_3)$$

$$\blacksquare\,\square\,\square\,\blacksquare \quad \longrightarrow (y_2, y_2)$$

$$\square\,\blacksquare\,\blacksquare\,\square \quad \longrightarrow (y_1, y_3)$$

$$\square\,\blacksquare\,\square\,\blacksquare \quad \longrightarrow (y_1, y_2)$$

$$\square\,\square\,\blacksquare\,\blacksquare \quad \longrightarrow (y_1, y_1)$$

En aquest exemple $r < n$, però això no té importància. Per exemple, hi ha 15 combinacions amb repetició de longitud 4 formades per 3 elements. En efecte,

$$CR_3^4 = \binom{3+4-1}{3-1} = \binom{6}{2} = 15.$$

I les podem explicitar com abans fent llistes de 6 quadrats i agafant-ne 2.

$$\blacksquare\,\blacksquare\,\square\,\square\,\square\,\square \quad \longrightarrow (y_3, y_3, y_3, y_3)$$

$$\blacksquare\,\square\,\blacksquare\,\square\,\square\,\square \quad \longrightarrow (y_2, y_3, y_3, y_3)$$

$$\blacksquare\,\square\,\square\,\blacksquare\,\square\,\square \quad \longrightarrow (y_2, y_2, y_3, y_3)$$

$$\blacksquare\,\square\,\square\,\square\,\blacksquare\,\square \quad \longrightarrow (y_2, y_2, y_2, y_3)$$

$$\blacksquare\,\square\,\square\,\square\,\square\,\blacksquare \quad \longrightarrow (y_2, y_2, y_2, y_2)$$

$$\square\,\blacksquare\,\blacksquare\,\square\,\square\,\square \quad \longrightarrow (y_1, y_3, y_3, y_3)$$

$$\square\,\blacksquare\,\square\,\blacksquare\,\square\,\square \quad \longrightarrow (y_1, y_2, y_3, y_3)$$

$$\square\,\blacksquare\,\square\,\square\,\blacksquare\,\square \quad \longrightarrow (y_1, y_2, y_2, y_3)$$

$$\square\,\blacksquare\,\square\,\square\,\square\,\blacksquare \quad \longrightarrow (y_1, y_2, y_2, y_2)$$

$$\square\,\square\,\blacksquare\,\blacksquare\,\square\,\square \quad \longrightarrow (y_1, y_1, y_3, y_3)$$

$$\square\,\square\,\blacksquare\,\square\,\blacksquare\,\square \quad \longrightarrow (y_1, y_1, y_2, y_3)$$

$$\square\,\square\,\blacksquare\,\square\,\square\,\blacksquare \quad \longrightarrow (y_1, y_1, y_2, y_2)$$

$$\square\,\square\,\square\,\blacksquare\,\blacksquare\,\square \quad \longrightarrow (y_1, y_1, y_1, y_3)$$

$$\square\,\square\,\square\,\blacksquare\,\square\,\blacksquare \quad \longrightarrow (y_1, y_1, y_1, y_2)$$

$$\square\,\square\,\square\,\square\,\blacksquare\,\blacksquare \quad \longrightarrow (y_1, y_1, y_1, y_1)$$

Exemple. El problema del cambrer, [1] pag 119.

9.5 Permutacions amb repetició

Definició 9.5. *Una permutació amb repetició és una llista* **ordenada** *de longitud r formada per n elements d'un cert conjunt Y, i en aquesta llista haver elements de repetits.*

La idea és pensar per un moment que els elements que es poden repetir són diferents entre ells, calcular llavors com permutacions ordinàries, i dividir finalment per les permutacions que deixen invariants aquests elements repetits. Per exemple, si volem saber quantes paraules (tinguin sentit o no) es poden formar amb quatre $A's$, tres $B's$ i dues $C's$, pensem que les lletres que tenim són $A_1, A_2, A_3, A_4, B_1, B_2, B_3, C_1, C_2$ i sabem que hi ha 9! permutacions d'aquestes 9 lletres. Ara bé, dues d'aquestes permutacions que difereixen només en l'ordre de les A_i, quan substuïm novament les A_i per A seran iguals. Per tant, ja no tenim 9! ordenacions diferents sinó només 9!/4!. Anàlogament amb les $B's$ i les $C's$, de manera que

$$PR_n^{k_1,\dots,k_n} = \frac{r!}{k_1!\dots k_n!} = \binom{r}{k_1,\dots,k_n}, \qquad \sum_i k_i = r.$$

Exemple 1. Problema del cinema, [1], pag 123.

Exemple 2. Els coeficients multinomials de l'expressió

$$(x_1 + \cdots + x_n)^m = \sum_{k_1+\cdots+k_n=m} C_{k_1\dots k_n} x_1^{k_1} \dots x_n^{k_n}$$

estan donats per

$$C_{k_1\dots k_n} = PR_n^{k_1,\dots,k_n} = \binom{m}{k_1,\dots,k_n}$$

En efecte, per formar el producte

$$x_1^{k_1} \dots x_n^{k_n}$$

hem format paraules de longitud r a les quals apareix k_1 vegades la variable x_1, k_2 vegades la variable x_2, …, k_n vegades la variable x_n.

Per exemple, si volem calcular

$$(x_1 + x_2 + x_3)^4 = (x_1 + x_2 + x_3)(x_1 + x_2 + x_3)(x_1 + x_2 + x_3)(x_1 + x_2 + x_3)$$

i ens preguntem pel coeficient de $x_1^2 x_2 x_3$, hem d'observar que aquesta expressió apareix quan en efectuar el producte elegim x_1 en el primer i segon factor, x_2 en el tercer i x_3 en el quart, o bé quan elegim x_1 en el primer factor, x_2 en el segon, x_3 en el tercer i x_1 en el quart, etc. és a dir, hem de

considerar totes les expressions del tipus

$$x_1x_1x_2x_3$$
$$x_1x_2x_3x_1$$
$$x_2x_3x_1x_1$$
$$\vdots$$

que no són més que permutacions amb repetició del tipus $PR_3^{2,1,1}$.

Nota. Quants sumands té el sumatori $\sum_{k_1+\cdots+k_n=m}$?

És a dir, quants nombres multinomials hi ha (fixades m i n)? Equival a trobar totes les solucions de l'equació $y_1 + \cdots + y_n = m$, amb $y_i \geq 0$.

Posem m quadrats blancs amb i entre ells $n-1$ quadrats negres, i convenim que y_1 és el nombre de quadrats blancs que hi ha abans del primer quadrat negre, etc.

$$\square\,\square\,\square\,\blacksquare\,\square\,\ldots$$

Equival a pensar que tenim $m + n - 1$ quadrats i que en pintem $n - 1$ de negre. Per tant tenim

$$\binom{m+n-1}{n-1}$$

sumands.

Nom	*Fórmula*	*Definició*	*Exemple*
Variacions amb repetició	$VR_n^r = n^r$	Llista **ordenada** de longitud r formada per n elements que es poden o no anar repetint.	Quinieles. Aplicacions de $\mathbb{N}_r$ a $\mathbb{N}_n$.
Variacions	$V_n^r = n(n-1)\dots(n-(r-1))$	Llista **ordenada** de longitud r formada per n elements que no es poden repetir.	Aplicacions injectives de $\mathbb{N}_r$ a $\mathbb{N}_n$.
Permutacions	$P_n = n!$	Cas particular de variacions amb $n = r$	Aplicacions bijectives de $\mathbb{N}_n$ a $\mathbb{N}_n$
Combinacions	$C_n^r = \binom{n}{r}$	Llista de r objectes elegits d'entre n objectes donats, que no es poden repetir, **sense importar l'ordre**.	Nombre de subconjunts de r elements d'un conjunt de n elements.
Combinacions amb repetició	$CR_n^r = \binom{n+r-1}{n-1}$	Llista de r objectes elegits d'entre n objectes donats, però que n'hi pot haver de repetits, **sense importar l'ordre**.	El problema del cambrer.
Permutacions amb repetició	$PR_n^{k_1,\dots,k_n} = \binom{r}{k_1,\dots,k_n} = \frac{r!}{k_1!\dots k_n!}$ $(\sum_i k_i = r)$	Llista **ordenada** de r objectes elegits d'entre n objectes donats, però que n'hi pot haver de repetits.	Coeficients multinomials.

9.6 El principi d'inclusió-exclusió

Quan un conjunt X és finit denotem $|X|$ el nombre d'elements de X, i diem que $|X|$ és el *cardinal* de X.

Proposició 9.6. *Siguin A i B conjunts finits disjunts, és a dir, $A \cap B = \emptyset$. Llavors $|A \cup B| = |A| + |B|$.*

Demostració. Per definició, un conjunt X és finit si existeix una bijecció entre X i $\mathbb{N}_n = \{1, \ldots, n\}$ per a algun $n \in \mathbb{N}$. Tenim doncs $f : A \longrightarrow \mathbb{N}_n$ i $g : B \longrightarrow \mathbb{N}_m$ bijectives, amb $n, m \in \mathbb{N}$. Definim $h : A \cup B \longrightarrow \mathbb{N}_{n+m}$ per

$$h(x) = \begin{cases} f(x) & \text{si } x \in A, \\ \\ g(x) + n & \text{si } x \in B. \end{cases}$$

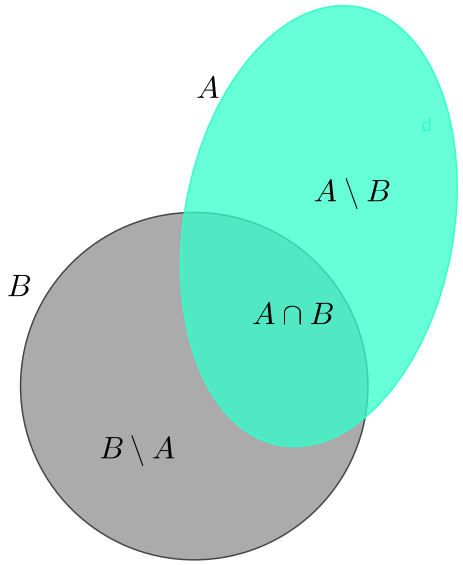
És clar que està ben definida i és bijectiva. □

Proposició 9.7. *Siguin A i B conjunts finits. Llavors*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Demostració. Escrivim $A \cup B$ com unió disjunta de tres subconjunts.

$$A \cup B = (A \setminus B) \cup (A \cap B) \cup (B \setminus A).$$



Utilitzant dos cop la proposició 9.6 veiem que

$$|A \cup B| = |(A \setminus B)| + |(A \cap B)| + |(B \setminus A)|. \tag{9.1}$$

Per altra banda, i també per la proposició 9.6, tenim

$$|A| = |A \setminus B| + |A \cap B|, \quad |B| = |B \setminus A| + |A \cap B|.$$

Substituint a (9.1) tenim

$$|A \cup B| = (|A| - |A \cap B|) + |(A \cap B)| + (|B| - |A \cap B|) = |A| + |B| - |A \cap B|.$$

Proposició 9.8. *Siguin A, B i C conjunts finits. Llavors*

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Demostració. Aplicant la Proposició 9.7 tenim

$$\begin{aligned} |A \cup B \cup C| &= |A \cup B| + |C| - |(A \cup B) \cap C| \\ &= |A| + |B| - |A \cap B| + |C| - |(A \cap C) \cup (B \cap C)| \\ &= |A| + |B| - |A \cap B| + |C| - |(A \cap C)| - |(B \cap C)| \\ &+ |(A \cap C) \cap (B \cap C)| \\ &= |A| + |B| + |C| - |A \cap B| - |(A \cap C)| - |(B \cap C)| \\ &+ |A \cap B \cap C|. \qquad \square \end{aligned}$$

Proposició 9.9. *Siguin $A_1, \ldots, A_n$ conjunts finits. Llavors*

$$\begin{aligned} |A_1 \cup \cdots \cup A_n| &= \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| + \\ &+ \cdots + (-1)^{n+1} |A_1 \cap \cdots \cap A_n| \end{aligned}$$

Demostració. Exercici d'inducció (vegeu [1], pàgina 116.). $\square$

Exemple 9.1. *Un carter ha d'ensobrar n cartes, amb els noms dels destinataris ja escrits a cada carta, en n sobres, que porten també aquests noms dels destinataris escrits. Té pressa i ho fa a l'atzar. Quina és la probabilitat de que no encerti cap destinatari.*

Demostració. Sigui A_i el conjunt format per totes les maneres d'ensobrar tals que la carta del destinatari i va a parar al sobre de destinatari i. Podem pensar que $A_i \subset S_n$, on S_n és el grup de permutacions de n elements, i A_i són les $\sigma \in S_n$ tals que $\sigma(i) = i$.

Les maneres d'ensobrar que no encerten cap destinatari són les $\sigma \in S_n$ tals que $\sigma(1) \neq 1, \ldots, \sigma(n) \neq n$, equivalentment

$$\sigma \in (A_1 \cup \cdots \cup A_n)^c.$$

El problema ens demana doncs quantes permutacions hi ha a S_n que no tenen cap punt fix.

Per contar-les només hem de calcular

$$|(A_1 \cup \cdots \cup A_n)^c|.$$

Abans però notem que, de manera molt evident,

$$|A_i| = (n-1)!, \quad |A_i \cap A_j| = (n-2)!, \quad |A_i \cap A_j \cap A_k| = (n-3)!, etc.$$

Llavors

$$\begin{aligned}
|(A_1 \cup \cdots \cup A_n)^c| &= |S_n| - |(A_1 \cup \cdots \cup A_n)| \\
&= n! - \sum_{i=1}^{n} |A_i| + \sum_{1 \le i < j \le n} |A_i \cap A_j| \\
&- \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| + \\
&+ \cdots + (-1)^n |A_1 \cap \cdots \cap A_n| \\
&= n! - n(n-1)! + \binom{n}{2}(n-2)! \\
&- \binom{n}{3}(n-3)! + \cdots + (-1)^n \\
&= n!(\frac{1}{2} - \frac{1}{3} + \cdots + \frac{(-1)^n}{n!})
\end{aligned}$$

La probabilitat de que el carter no endevini cap destinatari és, doncs,

$$P = \frac{casos\, favorables}{casos\, possibles} = \frac{|(A_1 \cup \cdots \cup A_n)^c|}{|S_n|} = \frac{1}{2} - \frac{1}{3} + \cdots + \frac{(-1)^n}{n!} \simeq e^{-1} \simeq 0,3678.$$

Tema 10

m.c.d. i m.c.m.

10.1 Ideals

Sigui[1] $b \in \mathbb{Z}$. Denotem (b) el conjunt dels múltiples de b, és a dir,

$$(b) = \{n \in \mathbb{Z}; n = \lambda b, \lambda \in \mathbb{Z}\}.$$

Dues propietats evidents del conjunt (b) són

$$\begin{aligned} a \in (b), c \in (b) &\Rightarrow a + c \in (b) \\ a \in (b), c \in \mathbb{Z} &\Rightarrow ac \in (b) \end{aligned}$$

Definició 10.1. *Un* ideal[2] *de* $\mathbb{Z}$ *és un subconjunt* $I \subseteq \mathbb{Z}$ *tal que*

$$\begin{aligned} a \in I, c \in I &\Rightarrow a + c \in I \\ a \in I, c \in \mathbb{Z} &\Rightarrow ac \in I \end{aligned}$$

Clarament (b) és un ideal, però de fet tots els ideals de $\mathbb{Z}$ són així.

Proposició 10.2. *Sigui* I *un ideal de* $\mathbb{Z}$. *Existeix*[3] $b \in \mathbb{Z}$ *tal que* $I = (b)$.

Demostració. Si $I = \{0\}$ prenem $b = 0$. Suposem, doncs, $I \neq \{0\}$. Com si $a \in I$ llavors també $a(-1) = -a \in I$ podem assegurar que a I sempre hi ha elements positius. Sigui b el nombre enter positiu més petit de I.

Llavors $I = (b)$. En efecte, que $(b) \subseteq I$ és clar, per la segona condició de la definició d'ideal.

[1] Aquesta secció segueix essencialment [2].

[2] Podem canviar $\mathbb{Z}$ per un anell qualsevol i tenim la definició de *ideal* d'un anell.

[3] Els ideals d'un anell arbitrari generats per un element es diuen *principals*. Aquesta proposició diu doncs que tots els ideals de $\mathbb{Z}$ són principals. També es diu que $\mathbb{Z}$ és un anell principal.

Per veure $I \subseteq (b)$ prenem $a \in I$ i dividim

$$a = bq + r, \quad 0 \leq r < b.$$

Llavors, $r = a - bq$, i per les dues propietats de la definició d'ideal tenim que $r \in I$, però com b és l'element més petit positiu de I ha de ser $r = 0$, és a dir, $a = bq$, i per tant $a \in (b)$ com volíem veure. □

Notació. Si a és un múltiple de c, és a dir $a = \lambda c$, per algun $\lambda \in \mathbb{Z}$, escrivim

$$a = \overset{\bullet}{c}$$

o equivalentment

$$c|a,$$

que és llegeix c *divideix* a o c és un *divisor* de a. No s'ha de confondre *divideix* amb *divisible*. Quan c *divideix* a diem també que a és *divisible* per c o que a és *múltiple* de c. Així, per exemple, podem dir que 4 és un divisor de 8, o que 4 divideix a 8, i també que 8 és divisible per 4 o que 8 és múltiple de 4.

Proposició 10.3. *Siguin $a, c \in \mathbb{Z}$. Llavors*

$$(a) \subseteq (c) \Leftrightarrow c|a$$

Demostració. ($\Rightarrow$). Com $a \in (c)$, a és múltiple de c.

($\Leftarrow$). Suposem $a = \mu c$. Prenem $x \in (a)$. Llavors $x = \lambda a = \lambda\mu c$, i per tant, $x \in (c)$. □

En particular $(a) = (b)$ si i només si $a = \pm b$.

10.2 Intersecció d'ideals. m.c.m.

Proposició 10.4. *La intersecció d'ideals és un ideal.*

Demostració. Veiem que $(a_1) \cap (a_2)$ és tancat per la suma. Sigui $a, b \in (a_1) \cap (a_2)$. Llavors $a = \overset{\bullet}{a_1}$, $a = \overset{\bullet}{a_2}$, $b = \overset{\bullet}{a_1}$ i $b = \overset{\bullet}{a_2}$. Així

$$a + b = \overset{\bullet}{a_1} + \overset{\bullet}{a_1} = \overset{\bullet}{a_1}$$

$$a + b = \overset{\bullet}{a_2} + \overset{\bullet}{a_2} = \overset{\bullet}{a_2}$$

i per tant

$$a + b \in (a_1) \cap (a_2).$$

Veiem ara que $(a_1) \cap (a_2)$ és tancat pel producte per elements de $\mathbb{Z}$. Sigui $a \in (a_1) \cap (a_2)$ i $\lambda \in \mathbb{Z}$. Com $a = \overset{\bullet}{a_1}$ i $a = \overset{\bullet}{a_2}$ és clar que $\lambda a = \overset{\bullet}{a_1} = \overset{\bullet}{a_2}$, i per tant, $\lambda a \in (a_1) \cap (a_2)$. □

Com tots els ideals de $\mathbb{Z}$ són *principals*, té sentit la definició següent.

Definició 10.5 (m.c.m.). *Siguin $a_1, a_2 \in \mathbb{Z}$. Es defineix el* mínim comú múltiple *de a_1 i a_2, m.c.m.(a_1, a_2), com qualsevol dels enters $\pm m$ tal que*

$$(a_1) \cap (a_2) = (m).$$

El nom de *mínim comú múltiple* és ben lògic, ja que com que $m \in (a_1) \cap (a_2)$, m és múltiple de a_1 i múltiple de a_2. A més, si un cert nombre n és múltiple de a_1 i de a_2, llavors $n \in (a_1) \cap (a_2) = (m)$ i per tant, n és múltiple de m. Per tant $|m|$ és el més més petit dels múltiples positius comuns de $|a_1|$ i $|a_2|$.

Anàlogament definim $m.c.m.(a_1, \ldots, a_k)$ com qualsevol dels enters $\pm m$ tals que

$$(a_1) \cap \cdots \cap (a_k) = (m).$$

10.3 Ideal generat per dos ideals. m.c.d.

És molt clar que la unió d'ideals no és un ideal. Per exemple, els números 2 i 3 pertanyen a $(2) \cup (3)$ i en canvi $2 + 3$ no és múltiple de 2 ni de 3, és a dir, $5 \notin (2) \cup (3)$.

Però el que sí té sentit és considerar l'ideal més petit que conté els ideals (a) i (b).

Aquest ideal el denotarem (a, b) i està donat per

$$(a, b) = \{ra + sb; r, s \in \mathbb{Z}\}$$

És fàcil veure que, efectivament, (a, b) és ideal. Observem que tant a com b pertanyen a (a, b).

També és clar que qualsevol ideal que contingui (a) i (b) ha de contenir totes les expressions del tipus $ra + sb$, de manera que (a, b) està contingut en qualsevol ideal que contingut (a) i (b).

Definició 10.6 (m.c.d.). *Siguin $a, b \in \mathbb{Z}$. Es defineix el màxim comú divisor de a i b, m.c.d.(a, b), com qualsevol dels enters $\pm d$ tal que*

$$(a, b) = (d).$$

Observem que $m.c.d.(a, 0) = a, \forall a \in \mathbb{Z}$.

Anàlogament es defineix $m.c.d.(a_1, \ldots, a_k)$ com qualsevol dels enters $\pm d$ tals que

$$(a_1, \ldots, a_k) = (d)$$

on $(a_1, \ldots, a_k)$ és l'ideal generat per $a_1, \ldots, a_k$. Vegeu una observació sobre el cas $k = 3$ a [10].

Proposició 10.7 (Identitat de Bézout). [4] *Sigui $d = m.c.d.(a, b)$. Existeixen enters p, q tals que*

$$d = pa + qb$$

Demostració. Conseqüència directa de que $d \in (a, b)$. □

El nom de màxim comú divisor és ben lògic ja que $a \in (d)$ vol dir que $d|a$, i $b \in (d)$ vol dir que $d|b$, per tant d és un divisor comú de a i de b.

A més, si $d'|a$ i $d'|b$, llavors, per la identitat de Bézout, $d'|d$, és a dir, $|d|$ és el més gran dels divisors comuns positius de $|a|$ i $|b|$.

Una propietat molt útil és la següent.

Proposició 10.8. *Siguin $a, b \in \mathbb{Z}$. Llavors*

$$m.c.d.(a, b) = m.c.d.(a + \lambda b, b), \quad \forall \lambda \in \mathbb{Z}.$$

Demostració. Veurem la igualtat d'ideals

$$(a, b) = (a + \lambda b, b).$$

La inclusió "$\supseteq$" és òbvia. Veiem la inclusió "$\subseteq$". Prenem $\mu a + \nu b$ un element arbitrari de (a, b). Tenim

$$\mu a + \nu b = \mu a + \nu b + \mu\lambda b - \mu\lambda b = \mu(a + \lambda b) + \rho b$$

amb $\rho = \nu - \mu\lambda$. Per tant, $\mu a + \nu b \in (a + \lambda b, b)$ com volíem veure. Com que aquests ideals són iguals, és clar que

$$m.c.d.(a, b) = m.c.d.(a + \lambda b, b), \quad \forall \lambda \in \mathbb{Z}. \quad \square$$

D'aquí es desprèn que *el màxim comú divisor del dividend i el divisor és igual al màxim comú divisor del divisor i el residu.* En efecte, si

$$D = dq + r, \quad 0 \leq r < d$$

tenim

$$m.c.d.(D, d) = m.c.d.(D - dq, d) = m.c.d.(r, d).$$

Definició 10.9. *Sigui $a, b \in \mathbb{Z}$. Si $m.c.d.(a, b) = 1$, es diu que a i b són* coprimers *o* primers entre ells*.*

El resultat següent, que fa referència a nombre coprimers, és molt important per les moltes aplicacions posteriors que en farem. Es coneix com Teorema d'Euclides, tot i que la versió dels *Elements* és el Corol·lari 10.11.

Teorema 10.10 (Euclides). *Si $a|bc$, i $m.c.d.(a, b) = 1$, llavors $a|c$.*

[4] Autor de *Cours complet de mathématiques à l'usage de la marine et de l'artillerie*, qui devient plus tard le livre de référence des candidats au concours d'entrée à l'École polytechnique.

Demostració. Per la identitat de Bézout existeixen $p, q \in \mathbb{Z}$ tals que

$$pa + qb = 1.$$

Multiplicant per c,

$$pac + qbc = c.$$

Llavors a divideix a cadascun dels dos sumands de l'esquerra d'aquesta igualtat, i per tant, $a|c$ com volíem. □

La proposició 30 del llibre VII dels Elements[5] és el corol·lari següent.

Corol·lari 10.11 (Euclides). *Si $p|bc$ i p és primer, llavors $p|b$ o $p|c$.*

Demostració. És clar que, per ser p primer, $m.c.d.(p, b) = 1$ o $m.c.d.(p, b) = p$. En el primer cas, pel teorema anterior, $p|c$. En el segon cas, $p|b$. □

Una manera útil de manipular el m.c.d. és la propietat següent.

Proposició 10.12. *Sigui $d = m.c.d.(a, b)$ i posem $a = a'd$ i $b = b'd$. Llavors*

$$m.c.d.(a', b') = 1.$$

Demostració. Per la identitat de Bézout, existeixen $p, q \in \mathbb{Z}$, tals que

$$pa + qb = d.$$

Però també sabem que a i b són múltiples de d, de manera que podem escriure $a = a'd$ i $b = b'd$ amb $a', b' \in \mathbb{Z}$. Substituint a la identitat de Bézout tenim

$$pa'd + qb'd = d$$

i per tant

$$pa' + qb' = 1,$$

que implica directament $m.c.d.(a', b') = 1$. □

Una relació important entre màxim comú divisor i mínim comú múltiple és la següent.

Proposició 10.13.

$$m.c.d.(a, b) \cdot m.c.m.(a, b) = ab.$$

Demostració. Denotem $d = m.c.d.(a, b)$, $m = m.c.m.(a, b)$. Per la proposició 10.12, sabem que existeixen $a', b' \in \mathbb{Z}$ tals que

$$a = a'd,\ b = b'd,\ m.c.d.(a', b') = 1.$$

Veurem ara que

$$m = a'b'd = a'b = ab'.$$

[5] Aquesta proposició diu: *Si dos nombres, al multiplicar-se entre si, fan algun nombre i algun nombre primer mesura el seu producte, també mesurarà a un dels nombres inicials.*

En efecte, és clar que $a'b'd$ és múltiple de a i múltiple de b. Veiem que és el mínim. Sigui m' múltiple comú de a i b. Posem

$$m' = \lambda a = \mu b.$$

Això implica $\lambda a'd = \mu b'd$, és a dir, $\lambda a' = \mu b'$. Pel teorema d'Euclides, 10.10, $a'|\mu$, és a dir, existeix δ tal que $\mu = a'\delta$. Així,

$$m' = \mu b = a'\delta b = \delta a'b'd,$$

que ens diu que qualsevol múltiple de a i b és múltiple de $a'b'd$.

Per tant

$$m = a'b'd.$$

Ara l'enunciat de la proposició és clar ja que

$$m.c.d.(a,b) \cdot m.c.m.(a,b) = dm = da'b'd = ab. \quad \square$$

Observem que aquest resultat no es generalitza trivialment al producte de màxim comú divisor i mínim comú múltiple de més de dos nombres. Quan val

$$m.c.m.(2,6,8) \cdot m.c.d.(2,6,8)?$$

10.4 Teorema fonamental de l'aritmètica

Recordem que $p \in \mathbb{Z}$ és diu *primer* si els únics divisors que té són ± 1, $\pm p$. Per conveni, es considera que $0, \pm 1$ no són primers.

Lema 10.14. *Tot nombre enter n, $n \neq 0, \pm 1$, admet un divisor primer.*

Demostració. Podem suposar $n > 1$ ja que en cas contrari raonaríem sobre $-n$. Sigui

$$S = \{x \in \mathbb{N}; x > 1, x|n\}$$

el conjunt dels divisors de n més grans que 1. $S \neq \emptyset$ ja que $n \in S$. Sigui p el primer element de S. Aquest p, que és un divisor de n, és primer. En efecte, si p no fos primer tindria un divisor q, $p = qr$, amb $1 < q < p$. Llavors tindríem

$$n = \lambda p = \lambda qr,$$

i q seria un divisor de n més gran que 1, és a dir, tindríem $q \in S$, però com $q < p$ això és una contradicció, i per tant, p és primer. $\square$

Teorema 10.15 (**Fonamental de l'aritmètica).** *Tot nombre enter descompon de manera única, llevat d'ordre i signe, com producte de primers.*

Demostració. Prenem $n \in \mathbb{Z}$ i suposem $n > 1$. En cas contrari argumentem sobre $-n$. Si n és primer hem acabat. En cas contrari apliquem el lema anterior.

Tindrem $n = p_1 m_1$, amb p_1 primer i $1 < m_1 < n$. Si m_1 és primer, hem acabat. En cas contrari apliquem el lema a m_1 i tenim $m_1 = p_2 m_2$, amb $1 < m_2 < m_1$. Així,

$$n = p_1 p_2 m_2, \quad p_1, p_2 \text{ primers.}$$

Repetim el procés amb m_2, etc. Com que el nombre que estem considerant és cada cop més petit i més gran que 1, en un nombre finit de passos tindrem

$$n = p_1 p_2 \dots p_r,$$

que, agrupant els primers que resultin iguals, i recordant que raonem sobre n o $-n$, s'escriu com

$$n = \pm p_1^{\alpha_1} \dots p_k^{\alpha_k}.$$

Veiem ara la unicitat d'aquesta descomposició. Suposem

$$p_1 \dots p_k = q_1 \dots q_s$$

amb p_i, q_j primers eventualment repetits. Com p_1 divideix al terme de l'esquerra també divideix al de la dreta. Tindrem

$$p_1 | q_1 (q_2 \dots q_s).$$

Pel Corol·lari 10.11, $p_1 | q_1$ o bé $p_1 | q_2 \dots q_s$. Equivalentment, $p_1 = \pm q_1$ o bé $p_1 | q_2 \dots q_s$. En aquest segon cas, novament pel Corol·lari 10.11, $p_1 = \pm q_2$ o bé $q_2 | q_3 \dots q_s$. Repetint el procediment arribarem després de $s - 1$ passos a que $p_1 = \pm q_{s-1}$ o $p_1 = \pm q_s$

Per tant, podem afirmar que hi ha un q_j, $1 \leq j \leq s$ tal que $p_1 = q_j$. Ara simplifiquem p_1 amb el corresponent q_j i repetim el procés. Si $k < s$, després de k simplificacions com l'anterior arribaríem (reordenant les q_j) a

$$1 = q_{k+1} \dots q_s$$

cosa impossible, i per tant $k = s$. □

Acabem amb la Proposició 20 del llibre IX dels Elements[6].

Teorema 10.16. *Hi ha infinits nombres primers.*

Demostració. Suposem que hi ha un nombre finit k de primers, $p_1, \dots, p_k$, Considerem el nombre enter

$$n = p_1 \dots p_k + 1.$$

Sabem, pel Lema 10.14, que n admet un divisor primer. Ha de ser un dels p_i anteriors. Però llavors

$$1 = n - p_1 \dots p_k$$

seria divisible per aquest p_i (els dos termes de la dreta són múltiples de p_i) i això és una contradicció. □

[6] Hia ha més nombres primers que qualsevol quantitat proposada de nombres primers.

10.5 Càlcul pràctic del m.c.d. i m.c.m.

Lema 10.17. *Sigui $n \in \mathbb{Z}$ i p un nombre primer tal que $p^r | n$. Llavors la descomposició en factors primers de n és de la forma*

$$n = p^\alpha Q,$$

amb $\alpha \geq r$ i Q és el producte de potències de primers diferents de p.

Demostració. Si p aparegués en la descomposició de n amb exponent $s < r$, tindríem

$$n = p^s Q$$

on Q=*producte de potències de primers diferents de* p. Però com $n = p^r \lambda$, per algun $\lambda \in \mathbb{Z}$, tenim

$$p^s Q = p^r \lambda,$$

és a dir,

$$Q = p^{r-s} \lambda$$

i p dividiria Q la qual cosa és una contradicció (com es veu fàcilment aplicant repetidament el Coro1l·lari 10.11 com hem fet a la demostració del teorema 10.15). □

Càlcul del m.c.m.

Considerem la descomposició en factors primers de $a, b \in \mathbb{Z}$,

$$\begin{aligned} a &= p_1^{\alpha_1} \dots p_k^{\alpha_k} q_1^{\beta_1} \dots q_r^{\beta_r} \\ b &= p_1^{\gamma_1} \dots p_k^{\gamma_k} \overline{q}_1^{\delta_1} \dots \overline{q}_s^{\delta_s} \end{aligned}$$

amb els q_j diferents dels p_i i dels $\overline{q}_l$, i aquests diferents dels p_i.

Com $p_1^{\alpha_1}$ divideix a, també divideix a qualsevol múltiple de a, en particular divideix $m = m.c.m.(a, b)$. Per tant, pel Lema 10.17, p_1 apareix a la descomposició en factors primers de m amb un exponent igual a superior a α_1.

Aquest argument val igual per a tots els factors primers i les seves potències que apareixen a la descomposició de a i b.

Per tant,

$$m = p_1^{\lambda_1} \dots p_k^{\lambda_k} q_1^{\beta_1} \dots q_r^{\beta_r} \overline{q}_1^{\delta_1} \dots \overline{q}_s^{\delta_s}$$

amb

$$\lambda_i = \text{màxim } (\alpha_i, \gamma_i), \quad i = 1, \dots, k,$$

ja que, pel comentari anterior, totes aquestes potències de primers han d'aparèixer a la descomposició en factors primers de m, i és clar que en aquesta descomposició no hi pot aparèixer cap altre nombre primer ni cap dels que hi

apareix hi pot aparèixer elevat a una potència més gran que la considerada, ja que si fos així tindríem un nombre, que seria múltiple de a i b, però que seria més gran que m i per tant no seria el mínim múltiple comú.

Resumint: *el mínim comú múltiple de dos nombres està format pel producte dels factors primers d'aquests nombres, comuns i no comuns, sempre amb el major exponent.*

Exemple 10.1. *Calculeu el* $m.c.m.(124, 1280)$.

Solució. Com $124 = 2^2 \cdot 31$ i $1280 = 2^7 \cdot 5$ tenim que $m.c.m.(124, 1280) = 2^7 \cdot 5 \cdot 31 = 39680$.

Càlcul del m.c.d.

Sigui $d = m.c.d.(a, b)$ i suposem

$$d = p_1^{\mu_1} \dots p_k^{\mu_k}$$

Llavors $p_1^{\mu_1}$ divideix a i b, i per tant, pel Lema 10.17, p_1 apareix a la descomposició en factors primers de a i b elevat, en cada cas, a un exponent més gran o igual a μ_1.

Per tant, procedint al revés, per calcular d només hem de trobar els factors primers comuns que apareixen a la descomposició de a i de b. Si p és un d'aquests factors primers que apareix elevat a α en la descomposició de a i elevat a β en la descomposició de b, llavors ha d'aparèixer elevat a μ amb $\mu \leq \alpha$ i $\mu \leq \beta$ en la descomposició de d.

Com d no és un divisor qualsevol de a i b sinó el més gran dels divisors comuns ha de ser $\mu = \min(\alpha, \beta)$.

Resumint: *el màxim comú divisor de dos nombres està format pel producte dels factors primers comuns d'aquests nombres, sempre amb el menor exponent.*

Exemple 10.2. *Calculeu el* $m.c.d.(124, 1280)$.

Solució. Com $124 = 2^2 \cdot 31$ i $1280 = 2^7 \cdot 5$ tenim que $m.c.d.(124, 1280) = 2^2 = 4$.

m.c.d. i m.c.m. de més de dos nombres

Aquests criteris, tant el del m.c.d. com el del m.c.m., es generalitzen sense dificultat al cas de més de dos nombres.

El mínim comú múltiple de dos o més nombres està format pel producte dels factors primers d'aquests nombres, comuns i no comuns, sempre amb el major exponent.

El màxim comú divisor de dos o més nombres està format pel producte dels factors primers comuns d'aquests nombres, sempre amb el menor exponent.

Observem finalment que d'aquesta observació es dedueix que si tenim k nombres coprimers, és a dir,

$$m.c.d.(a_1, \ldots, a_k) = 1,$$

llavors

$$m.c.m.(a_1, \ldots, a_k) = a_1 \cdot \cdots \cdot a_k.$$

Exemple 10.3. *Calculeu* $m.c.d.(a, b, c)$ *i* $m.c.m.(a, b, c)$ *amb* $a = 2^2 \cdot 5^3 \cdot 7$, $b = 2^3 \cdot 17$, $c = 2^5 \cdot 3^6 \cdot 7^2$

Solució. $m.c.m.(a, b, c) = 2^5 \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 17$. $m.c.d.(a, b, c) = 2^2$.

10.6 Algorisme d'Euclides

Una manera de procedir per trobar el m.c.d. de dos nombres D i d i els seus coeficients de Bézout és disposar els càlculs com s'indica a la taula següent, que no és més que manera pràctica d'aplicar l'algorisme d'Euclides.

	q_1	q_2	q_3	q_4	
D	**d**	r_1	r_2	r_3	
1	0	α_1	α_2	α_3	
0	1	β_1	β_2	β_3	

Ara explicarem com s'omple aquesta taula, però ho farem de tal manera que sempre es complirà que

$$r_i = \alpha_i D + \beta_i d$$

és a dir, *la segona fila és igual a la tercera multiplicada per* D*, més la quarta multiplicada per* d.

La taula estarà completada quan obtinguem un zero a la segona fila, és a dir, $r_{k+1} = 0$. Llavors

$$m.c.d.(D, d) = r_k, \quad r_k = \alpha_k D + \beta_k d.$$

És a dir, r_k és el màxim comú divisor de D i d, i α_k, β_k són els seus coeficients de Bézout.

Per omplir la taula

D	**d**				
1	0				
0	1				

primer es comença dividint D entre d:

$$D = dq_1 + r_1,$$

i escrivim

$$r_1 = D - dq_1 = \alpha_1 D + \beta_1 d.$$

amb $\alpha_1 = 1$, $\beta_1 = -q_1$.

El quocient q_1 es col·loca a sobre de d, el residu r_1 es col·loca a la segona fila, a la dreta de d, i sota seu α_1 i β_1.

	$\mathbf{q_1}$				
D	**d**	$\mathbf{r_1}$			
1	0	α_1			
0	1	β_1			

Aix, en aquesta primera fase del procés, es compleix ja que *la segona fila és igual a la tercera multiplicada per D, més la quarta multiplicada per d.*

Observem que, per la proposició 10.8, $m.c.d.(D, d) = m.c.d.(d, r_1)$.

A continuació dividim d entre r_1

$$d = r_1 q_2 + r_2$$

i escrivim

$$r_2 = d - r_1 q_2.$$

Substituint r_1 pel seu valor obtenim

$$r_2 = d - (\alpha_1 D + \beta_1 d) q_2 = \alpha_2 D + \beta_2 d$$

amb

$$\begin{aligned} \alpha_2 &= -\alpha_1 \\ \beta_2 &= 1 - \beta_1 q_2 \end{aligned}$$

Incorporant, com abans, aquests valors a la taula tenim

	q_1	$\mathbf{q_2}$			
D	**d**	$\mathbf{r_1}$	$\mathbf{r_2}$		
1	0	1	α_2		
0	1	β_1	β_2		

Observem que, per la proposició 10.8,

$$m.c.d.(D, d) = m.c.d.(d, r_1) = m.c.d.(r_1, r_2).$$

A continuació dividim r_1 entre r_2

$$r_1 = r_2 q_3 + r_3$$

i escrivim

$$r_3 = r_1 - r_2 q_3.$$

Substituint r_1 i r_2 pels seus valors obtenim

$$\begin{aligned} r_3 &= (\alpha_1 D + \beta_1 d) - (\alpha_2 D + \beta_2 d) q_3 \\ &= (\alpha_1 - \alpha_2 q_3) D + (\beta_1 - \beta_2 q_3) d \\ &= \alpha_3 D + \beta_3 d \end{aligned}$$

amb

$$\begin{aligned} \alpha_3 &= \alpha_1 - \alpha_2 q_3 \\ \beta_3 &= \beta_1 - \beta_2 q_3 \end{aligned} \tag{10.1}$$

Incorporant, com abans, aquests valors a la taula tenim

	q_1	q_2	q_3		
D	d	r_1	r_2	r_3	
1	0	α_1	α_2	α_3	
0	1	β_1	β_2	β_3	

Observem que, per la proposició 10.8,

$$m.c.d.(D, d) = m.c.d.(d, r_1) = m.c.d.(r_1, r_2) = m.c.d.(r_2, r_3).$$

Si continuéssim el procés aniríem obtenint noves α's i β's relacionades amb les anteriors sempre de la mateixa manera que indiquen les relacions (10.1)

En general, doncs, per completar la taula només haurem d'anar trobant α's i β's relacionades recurrentment entre si, per les fórmules:

$$\begin{aligned} \alpha_i &= \alpha_{i-2} - q_i \alpha_{i-1} \\ \beta_i &= \beta_{i-2} - q_i \beta_{i-1} \end{aligned}$$

fins arribar a tenir un zero a la segona fila, $r_{k+1} = 0$, ja que llavors, el terme anterior r_k és el màxim comú divisor de D i d. En efecte, per la proposició 10.8,

$$m.c.d.(D, d) = m.c.d.(d, r_1) = m.c.d.(r_1, r_2) = \cdots = m.c.d.(r_k, r_{k+1}) = r_k.$$

Exemple 10.4. *Calculeu el màxim comú divisor i els coeficients de Bézout de $D = 127$ i $d = 52$.*

Dividim 127 entre 52. Quocient 2, resta 23.

	2				
127	52	**23**			
1	0	1			
0	1	-2			

A continuació dividim 52 entre 23. Quocient 2, resta 6.

	2	**2**			
127	52	23	**6**		
1	0	1			
0	1	-2			

I calculem α_2 i β_2 per la fórmula de recurrència $\alpha_2 = \alpha_0 - q_2\alpha_1$, $\beta_2 = \beta_0 - q_2\beta_1$.

	2	2			
127	52	23	6		
1	0	1	$\mathbf{-2}$		
0	1	-2	$\mathbf{-5}$		

A continuació dividim 23 entre 6. Quocient 3, resta 5.

	2	2	**3**		
127	52	23	6	**5**	
1	0	1	-2		
0	1	-2	5		

I calculem α_3 i β_3 per la fórmula de recurrència $\alpha_3 = \alpha_1 - q_3\alpha_2$, $\beta_3 = \beta_1 - q_3\beta_2$.

	2	2	3		
127	52	23	6	5	
1	0	1	-2	**7**	
0	1	-2	5	**-17**	

A continuació dividim 6 entre 5. Quocient 1, resta 1.

	2	2	3	**1**	
127	52	23	6	5	**1**
1	0	1	-2	7	
0	1	-2	5	-17	

I calculem α_4 i β_4 per la fórmula de recurrència $\alpha_4 = \alpha_2 - q_4\alpha_3$, $\beta_4 = \beta_2 - q_4\beta_3$.

	2	2	3	1	
127	52	23	6	5	1
1	0	1	-2	7	**-9**
0	1	-2	5	-17	**22**

Conclusió: el $mcd(127, 52) = 1$, i $22 \cdot 52 + (-9) \cdot 127 = 1$.

10.7 Equacions diofàntiques

Una equació diofàntica és una equació lineal[7] del tipus

$$ax + by = c,$$

amb $a, b, c \in \mathbb{Z}$, i de la que cerquem els valors de x, y que la satisfan, amb $x, y \in \mathbb{Z}$.

Proposició 10.18. *L'equació diofàntica $ax + by = c$ té solució si i només si $d|c$, on $d = m.c.d.(a, b)$.*

Demostració. Suposem que existeixen $x_0, y_0 \in \mathbb{Z}$ tals que $ax_0 + by_0 = c$. Com d divideix a i b, divideix al primer terme d'aquesta equació, i per tant divideix al segon, és a dir, $d|c$.

Suposem ara que $d|c$ i escrivim, per Bézout,

$$a\alpha + b\beta = d, \quad \alpha, \beta \in \mathbb{Z}.$$

Com $c = \mu d$, $\mu \in \mathbb{Z}$, multiplicant l'anterior equació per μ tenim

$$a\alpha\mu + b\beta\mu = \mu d = c, \quad \alpha, \beta \in \mathbb{Z},$$

per tant

$$\begin{aligned} x &= \alpha\mu \\ y &= \beta\mu \end{aligned}$$

són solució de l'equació diofàntica donada. □

Observem que aquesta demostració ens dóna un mètode general per calcular una solució particular de l'equació diofàntica: només hem de calcular els coeficients de Bézout de a i b i multiplicar-los per c/d.

Teorema 10.19. *Sigui $ax+by = c$ una equació diofàntica i sigui $x_0, y_0 \in \mathbb{Z}$ una solució. Sigui $d = m.c.d.(a, b)$ i posem $a = a'd$, $b = b'd$. Llavors tota solució x_1, y_1 de $ax + by = c$ és de la forma*

$$\begin{aligned} x_1 &= x_0 + \lambda b' \\ y_1 &= y_0 - \lambda a'. \end{aligned}$$

per algun $\lambda \in \mathbb{Z}$, i tota expressió d'aquest tipus és solució.

[7] Wikipedia: Existeix un algorisme general per a trobar les solucions d'una equació diofàntica de primer ordre, però no per a ordres superiors. Aquest problema general ha estat sense obtenir una resposta definitiva durant molts segles i David Hilbert l'inclogué com un dels seus famosos 23 problemes. El 1970, Yuri Matiyasevich demostrà finalment que és impossible obtenir una solució general per a una equació diofàntica d'ordre qualsevol.

Demostració. Primer comprovem que, per tota λ, els nombres enters $x_0 + \lambda b', y_0 - \lambda a'$ són solució. En efecte,

$$a(x_0 + \lambda b') + b(y_0 - \lambda a') = ax_0 + by_0 = c$$

ja que $ab' = a'db' = a'b$.

Ara suposem que $x_1, y_1 \in \mathbb{Z}$ és una solució. Llavors

$$a(x_0 - x_1) + b(y_0 - y_1) = 0.$$

Per tant,

$$a'd(x_1 - x_0) = b'd(y_0 - y_1) \tag{10.2}$$

Simplificant la d veiem que $a'|b'(y_0 - y_1)$ i com, per la Proposició 10.12, $m.c.d.(a', b') = 1$, aplicant el Teorema d'Euclides, Teorema 10.10, tenim que

$$a'|(y_0 - y_1).$$

Pel mateix argument, $b'|(x_1 - x_0)$. Podem escriure doncs $y_0 - y_1 = \lambda a'$ i $x_1 - x_0 = \mu b'$ amb $\lambda, \mu \in \mathbb{Z}$. Substituint a (10.2) tenim

$$a'\mu b' = b\lambda a'$$

és a dir, $\lambda = \mu$. Per tant,

$$\begin{array}{rcl} x_1 & = & x_0 + \lambda b' \\ y_1 & = & y_0 - \lambda a', \end{array}$$

com volíem veure. □

Exemple 10.5. *Resoleu l'equació diofàntica*

$$45x + 21y = 3.$$

Solució. Mirem primer si el màxim comú divisor dels coeficients divideix el terme independent. Com $m.c.d.(45, 21) = 3$, l'equació té solució.

Primer hem de trobar una solució particular. Per a això hem de trobar els coeficients de Bézout de 45 i 21, i multiplicarlos per $c/d = 3/3 = 1$.

Ara bé, els coeficients de Bézout de 45 i 21 són els mateixos que els de 15 i 7 (l'equació donada és equivalent a $15x + 7y = 1$).

Aquests coeficients de Bézout els podem trobar aplicant l'algorisme d'Euclides, o a ull. En aquest cas, com que $15 = 7 \cdot 2 + 1$, tenim directament que $15 \cdot (1) + 7 \cdot (-2) = 1$.

Així, una solució particular de $15x + 7y = 1$ és $x = 1$, $y = -2$.

La solució general s'obté sumant a la solució particular la solució general de la homogènia $15x + 7y = 0$.

$$\begin{array}{rcll} x & = & 1 + 7\lambda, & \\ y & = & -2 - 15\lambda, & \text{per a tot } \lambda \in \mathbb{Z}. \end{array}$$

Podeu trobar més exemples a [10].

Tema 11

Congruències

11.1 Elements invertibles de $\mathbb{Z}/(m)$

Proposició 11.1. *Sigui $a \in \mathbb{Z}$ i denotem $\bar{a}$ la classe de a a $\mathbb{Z}/(m)$. Llavors*

$$\bar{a} \text{ és invertible} \Leftrightarrow m.c.d.(a, m) = 1$$

Demostració. Primer de tot observem que, per la Proposició 10.8, l'enunciat anterior és independent de quin representant de la classe de a elegim.

Suposem primerament que $\bar{a}$ és invertible. Existeix una classe $\bar{b} \in \mathbb{Z}/(m)$ tal que $\bar{a}\bar{b} = \bar{1}$. Equivalentment, $ab - 1 = \lambda m$, per algun λ. De la igualtat

$$1 = ab - \lambda m$$

es veu clarament que qualsevol divisor comú de a i m és divisor de 1, i per tant, $m.c.d.(a, m) = 1$.

Recíprocament, si $m.c.d.(a, m) = 1$, existeixen, per la identitat de Bézout, enters p, q tals que

$$pa + qm = 1.$$

Prenent classes,[1]

$$\bar{p}\bar{a} + \bar{q}\bar{m} = \bar{p}\bar{a} = \bar{1}.$$

Per tant, $\bar{a}$ és invertible i el seu invers és $\bar{p}$. □

Corol·lari 11.2. *Si p és primer, $\mathbb{Z}/(p)$ és un cos.*

Demostració. Conseqüència directa del teorema anterior. □

[1] Aquí utilitzem que la projecció canònica $\pi : \mathbb{Z}/(m) \longrightarrow \mathbb{Z}/(m)$ és morfisme d'anells.

11.2 Petit teorema de Fermat

El conegut com petit teorema de Fermat diu que *si a és un nombre enter i p és un nombre primer que no és un factor de a, llavors p ha de ser un factor primer de $a^{p-1}-1$.*

Equivalentment,

Teorema 11.3. *Siguin $a, p \in \mathbb{Z}$, amb p primer i m.c.d.$(a,p)=1$. Llavors*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demostració. La demostració es basa en observar que *multiplicar* per $\bar{a}$ a $\mathbb{Z}/(p)$ equival a *permutar* els elements de $\mathbb{Z}/(p)$. Això és conseqüència de que l'aplicació

$$\begin{array}{ccc} \mathbb{Z}/(p) & \longrightarrow & \mathbb{Z}/(p) \\ \bar{x} & \mapsto & \bar{a}\bar{x} \end{array}$$

és injectiva.

En efecte, com $m.c.d.(a.p)=1$, tenim que $\bar{a} \neq \bar{0}$ a $\mathbb{Z}/(p)$. Per tant, per ser $\mathbb{Z}/(p)$ un cos, $\bar{a}$ és invertible. Llavors, si $\bar{a}\bar{x} = \bar{a}\bar{y}$, multiplicant per l'invers de $\bar{a}$ als dos costats, obtenim $\bar{x} = \bar{y}$. Per tant, l'aplicació *multiplicar* per $\bar{a}$ és injectiva (de fet, és bijectiva).

Així, doncs, com que $\bar{a}\bar{0} = \bar{0}$, tenim la igualtat de conjunts

$$\{\bar{1}, \bar{2}, \ldots, \overline{p-1}\} = \{\bar{a}\bar{1}, \bar{a}\bar{2}, \ldots, \bar{a}\overline{p-1}\}.$$

Si multipliquem tots els elements del conjunt de l'esquerra i tots els elements del conjunt de la dreta (que són iguals) obtindrem el mateix resultat. Igualant i simplificant obtenim

$$\bar{1} = \bar{a}^{p-1},$$

que equival a

$$a^{p-1} \equiv 1 \pmod{p}. \quad \square$$

11.3 Nombre de xifres del període de $1/p$

Seguim Klein, [8], per donar una aplicació interessant del petit teorema de Fermat.

Recordem que el petit teorema de Fermat diu que si a i p són coprimers llavors

$$a^{p-1} \equiv 1 \quad (p).$$

En particular, si $a = 10$ i p és un primer, $p \neq 2$, $p \neq 5$, tenim

$$10^{p-1} \equiv 1 \quad (p).$$

Teorema 11.4. *El nombre de xifres del període a l'expressió decimal de* $1/p$*, amb* p *primer diferent de* 2 *i* 5*, és el menor nombre* $\delta > 0$ *tal que*

$$10^{\delta} \equiv 1 \quad (p).$$

Demostració. Pel teorema de Fermat aquest δ existeix ja que sabem que $10^{p-1} \equiv 1\,(p)$. Si $p-1$ és el nombre més petit amb aquesta propietat, tenim $\delta = p-1$, en cas contrari, pel principi del primer element, existirà $1 < \delta < p-1$ que serà el més petit tal que $10^{\delta} \equiv 1\,(p)$.

La congruència del teorema es pot escriure com

$$\frac{10^{\delta}-1}{p} \in \mathbb{Z}$$

o bé

$$\frac{10^{\delta}}{p} = \frac{1}{p} + n, \quad n \in \mathbb{Z},$$

la qual es pot interpretar dient que *les xifres decimals de* $\dfrac{10^{\delta}}{p}$ *i* $\dfrac{1}{p}$ *són iguals.*

Però com

$$\frac{10^{\delta}}{p} = 10^{\delta} \cdot \frac{1}{p}$$

el número $\dfrac{10^{\delta}}{p}$ s'obté de $\frac{1}{p}$ corrent la coma δ llocs cap a la dreta, i com tenen les mateixes xifres decimals això implica que l'expressió decimal té període δ (o múltiple de δ, però per ser δ el més petit amb la propietat considerada és exactament el període). □

Exemple. Si $p = 3$, com que $10 \equiv 1\ (3)$, tenim $\delta = 1$, i efectivament el període és 1, ja que $1/3 = 0,333....$

Si $p = 11$, com que $10 \not\equiv 1\ (11)$, però $10^2 \equiv 1\ (11)$ tenim $\delta = 2$, i efectivament el període és 2, ja que $1/11 = 0,090909....$

Si $p = 7$, com que $10 \not\equiv 1\ (7)$, $10^2 \not\equiv 1\ (7)$, $10^3 \not\equiv 1\ (7)$, $10^4 \not\equiv 1\ (7)$, $10^5 \not\equiv 1\ (7)$, però $10^6 \equiv 1\ (11)$ tenim $\delta = 6$, i efectivament el període és 6, ja que $1/7 = 0,142857142857....$

Corol·lari 11.5. *El nombre de xifres del període a l'expressió decimal de* $1/p$*, amb* p *primer diferent de* 2 *i* 5*, és un divisor de* $p-1$*.*

Demostració. Sabem que

$$10^{p-1} \equiv 1\ (p)$$

Sigui δ el nombre de xifres del període. Pel teorema anterior sabem que δ és el menor enter positiu tal que

$$10^{\delta} \equiv 1\ (p).$$

Dividim $p-1$ entre δ i tenim $p-1 = q\delta + r$, amb $0 \leq r < \delta$. Llavors

$$10^{p-1} = 10^{q\delta+r} = (10^{\delta})^q 10^r \equiv 10^r \equiv 1\ (p)$$

Si $r \neq 0$, δ no seria el més petit amb aquesta propietat. Per tant, ha de ser $r = 0$ i $p-1$ és múltiple de δ.

11.4 La funció ϕ d'Euler

Aquesta funció compta el nombre de coprimers, més petits que ell, que té cada nombre enter.

Concretament

$$\phi(n) = |\{x \in \mathbb{N}; 1 \leq x \leq n, m.c.d.(x,m) = 1\}|.$$

Per la proposició 11.1, pàgina 111, sabem que

$$\phi(n) = |\mathbb{Z}^*/(n)|$$

on $\mathbb{Z}^*/(n)$ és el subgrup multiplicatiu[2] de $\mathbb{Z}/(n)$ format pels elements invertibles. Per exemple,

$$\begin{array}{rcll} \phi(2) & = & 1, & \{1\} \\ \phi(3) & = & 2, & \{1,2\} \\ \phi(4) & = & 2, & \{1,3\} \\ \phi(5) & = & 4, & \{1,2,3,4\} \\ \phi(6) & = & 2, & \{1,5\} \\ \phi(7) & = & 6, & \{1,2,3,4,5,6\} \end{array}$$

La fórmula general és la següent.

Teorema 11.6. *Sigui*

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

la descomposició en factors primers de $n \in \mathbb{Z}$. Llavors

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k}).$$

Demostració. Sigui

$$A_i = \{x \in \mathbb{N}; 1 \leq x \leq n, x \text{ és múltiple de } p_i\}.$$

És a dir,

$$A_i = \{p_i, 2p_i, 3p_i, \dots, \frac{n}{p_i} p_i\}$$

[2] $\mathbb{Z}^*/(m)$ no és un subanell de $\mathbb{Z}/(m)$ ja que no és tancat per la suma.

i per tant

$$|A_i| = \frac{n}{p_i}.$$

Observem ara que

$$\phi(n) = |(A_1 \cup \cdots \cup A_k)^c|$$

ja que

$$x \in (A_1 \cup \cdots \cup A_k)^c = A_1^c \cap \cdots \cap A_k^c$$

si x no és múltiple de p_1, ni de p_2, etc. Per tant, x i n no tenen factors primers en comú, és a dir, $m.c.d.(x, m) = 1$, i aquests són justament els elements que compta la funció ϕ d'Euler.

Pel principi d'inclusió-exclusió tenim

$$\begin{aligned}
\phi(n) &= |(A_1 \cup \cdots \cup A_k)^c| \\
&= n - |A_1 \cup \cdots \cup A_k| \\
&= n - \sum_{i=1}^{k} |A_i| + \sum_{1 \le i < j \le k} |A_i \cap A_j| - \sum_{1 \le i < j < r \le k} |A_i \cap A_j \cap A_r| \\
&+ \cdots + (-1)^k |A_1 \cap \cdots \cap A_k|.
\end{aligned}$$

Ara bé,

$$A_i \cap A_j = \{p_i p_j, 2p_i p_j, 3p_i p_j, \ldots \frac{n}{p_i p_j} p_i p_j\}$$

de manera que

$$|A_i \cap A_j| = \frac{n}{p_i p_j}.$$

Anàlogament,

$$|A_i \cap A_j \cap A_r| = \frac{n}{p_i p_j p_r},$$

etc.

Substituint aquests valors a l'expressió de $\phi(n)$ obtenim

$$\begin{aligned}
\phi(n) &= n - \sum_{i=1}^{k} \frac{n}{p_i} + \sum_{1 \le i < j \le k} \frac{n}{p_i p_j} - \sum_{1 \le i < j < r \le k} \frac{n}{p_i p_j p_r} + \cdots + (-1)^k \frac{n}{p_1 \ldots p_k} \\
&= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_k}).
\end{aligned}$$

11.5 Congruència d'Euler

Denotem[3] per $\mathbb{Z}^*/(m)$ el subgrup multiplicatiu dels elements invertibles de $\mathbb{Z}/(m)$. Recordem que $\mathbb{Z}^*/(m)$ té $\Phi(m)$ elements.

[3]La demostració que ara donarem de la congruència d'Euler implica la congruència (o petit teorema) de Fermat, teorema 11.3, que hem demostrat a la pàgina 112. I la demostració que farem ara és essencialment la mateixa que allà, però en aquell moment encara no havíem introduït la funció ϕ d'Euler.

Teorema 11.7. *Sigui a coprimer amb m i denotem $\bar{a} \in \mathbb{Z}^*/(m)$. L'aplicació $f_a : \mathbb{Z}^*/(m) \longrightarrow \mathbb{Z}^*/(m)$ donada per*

$$f_a(\overline{x}) = \overline{a}\,\overline{x}$$

és bijectiva.

Demostració. f_a està ben definida, en el sentit de que $\overline{a}\,\overline{x} \in \mathbb{Z}^*/(m)$. És fàcil veure, com a la demostració de 11.3, que f_a és injectiva, i per tant, bijectiva. És a dir, és una permutació dels elements de $\mathbb{Z}^*/(m)$. □

Teorema 11.8 (Congruències d'Euler i Fermat)**.** *Siguin a i m enters coprimers. Llavors*

$$a^{\Phi(m)} \equiv 1 \pmod{m}$$

Demostració. Si denotem per $\overline{x}_1, \ldots, \overline{x}_{\Phi(n)}$ tots els elements de $\mathbb{Z}^*/(m)$ es compleix que

$$\overline{x}_1 \cdot \overline{x}_2 \cdot \cdots \cdot \overline{x}_{\Phi(m)} = \overline{a}\,\overline{x}_1 \cdot \overline{a}\,\overline{x}_2 \cdot \cdots \cdot \overline{a}\,\overline{x}_{\Phi(m)},$$

ja que a dreta i esquerra d'aquesta igualtat hi ha els mateixos elements permutats. Simplificant els x_i obtenim el resultat. □

Exemple 11.1. *Resoleu la congruència*

$$5x \equiv 3 \mod 24.$$

Solució[4]. Com que $\Phi(24) = 8$, i 5 i 24 són coprimers, sabem que

$$5^8 \equiv 1 \pmod{24}$$

i, per tant,

$$3 \cdot 5^8 \equiv 3 \pmod{24}.$$

Equivalentment,

$$5 \cdot 3 \cdot 5^7 \equiv 3 \pmod{24}.$$

Per tant,

$$x \equiv 3 \cdot 5^7 \pmod{24}.$$

Com $5^2 \equiv 1 \pmod{24}$, tenim que

$$x \equiv 3 \cdot 5 \pmod{24}.$$

Exemple 11.2. *Quines són les dues últimes xifres de* 1003^{1003}.

[4]Es pot fer d'altres maneres, però ara volem aplicar Fermat.

Solució. Com 3 i 100 són coprimers sabem que

$$3^{\Phi(100)} \equiv 1 \mod 100$$

Com $\Phi(100) = 40$ i $1003 \equiv 3 \mod 100$, tenim que

$$1003^{40} \equiv 3^{40} \equiv 1 \mod 100.$$

Com,

$$1003^{1003} = 1003^{25 \cdot 40} \cdot 1003^3 = (1003^{40})^{25} \cdot 1003^3$$

tenim que

$$1003^{1003} \equiv 1003^3 \equiv 3^3 \mod 100.$$

Per tant 1003^{1003} acaba en 27.

11.6 Teorema xinès del residu

Ja hem comentat a la pàgina 20 que l'origen remot de l'avui conegut com *Teorema xinès del residu* és el problema següent: Quants soldats té l'exèrcit de Han Xing si, formats en 3 columnes, queden dos soldats, formats en 5 columnes, queden tres soldats i, formats en 7 columnes, queden dos soldats?

Si diem n al nombre de soldats d'aquest exèrcit, les hipòtesis anteriors es poden escriure com

$$\begin{aligned} n &= 3x + 2 \\ n &= 5y + 3 \\ n &= 7z + 2 \end{aligned} \tag{11.1}$$

Si mirem les dues primeres equacions obtenim una equació diofàntica

$$3x - 5y = 1$$

que té solució

$$\begin{aligned} x &= 7 + 5\lambda \\ y &= 4 + 3\lambda, \quad \lambda \in \mathbb{Z}. \end{aligned}$$

Substituint el valor de x a la primera equació i igualant amb la tercera obtenim

$$15\lambda + 23 = 7z + 2.$$

Resolent l'equació diofàntica

$$7z - 15\lambda = 21$$

obtenim

$$\begin{aligned} z &= -42 + 15\mu \\ \lambda &= -21 + 7\mu \quad \mu \in \mathbb{Z}. \end{aligned}$$

i per tant $n = 7(-42+15\mu)+2 = 105\mu - 292$. Possibles soldats de l'exèrcit: 23, 128, 232, etc.

Observem finalment que les equacions (11.1) es poden escriure com

$$n \equiv 2 \pmod 3 \tag{11.2}$$
$$n \equiv 3 \pmod 5 \tag{11.3}$$
$$n \equiv 2 \pmod 7 \tag{11.4}$$

En aquesta secció veurem una manera més general de resoldre aquest tipus de problemes.

Ens plantegem resoldre el sistema

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned} \tag{11.5}$$

en el cas particular en que $m_1, \ldots, m_k$ són coprimers dos a dos, és a dir, $m.c.d.(m_i, m_j) = 1$, $i, j = 1, \ldots, k$.

Denotem

$$\begin{aligned} M &= m_1 \cdot \cdots \cdot m_k \\ M_i &= \frac{M}{m_i}, \qquad i = 1, \ldots, k \end{aligned}$$

i resolem les k equacions, independents les unes de les altres (no és pròpiament un sistema), amb incògnites $y_1, \ldots, y_k$,

$$\begin{aligned} M_1 y_1 &\equiv a_1 \pmod{m_1} \\ &\vdots \\ M_k y_k &\equiv a_k \pmod{m_k} \end{aligned}$$

Cadascuna d'aquestes congruències es pot resoldre com una equació en el $\mathbb{Z}/(m_i)$ corresponent o resolent la corresponent equació diofàntica.

Suposem doncs aquestes equacions resoltes i les $y_1, \ldots, y_k$ conegudes. Aquestes y_j estan definides mòdul múltiples de m_j, en el sentit de que si y_j és solució llavors $y_j + \overset{\bullet}{m}_j$ també és solució. Elegim, per a cada $j = 1, \ldots, k$, un dels valors d'aquestes y_j.

Llavors la solució general del sistema donat és

$$x = \sum_{i=1}^{k} M_i y_i + \lambda M, \quad \forall \lambda \in \mathbb{Z}. \tag{11.6}$$

Que aquesta x és solució és evident ja que si prenem la seva classe mòdul m_j, $j = 1, \ldots, k$, tenim

$$\overline{x} = \sum_{i=1}^{k} \overline{M}_i \overline{y}_i + \lambda \overline{M} = \overline{M}_j \overline{y}_j$$

ja que tant M com les M_i amb $i \neq j$ són múltiples de m_j.

I és clar que la darrera igualtat de classes equival a

$$x \equiv M_j y_j \pmod{m_j}$$

i com

$$M_j y_j \equiv a_j \pmod{m_j}$$

tenim que

$$x \equiv a_j \pmod{m_j}$$

com volíem demostrar.

Ara bé, tota solució es pot escriure com a la igualtat (11.6)? Veurem que sí. En efecte, sigui x la solució de (11.5) donada per (11.6) i sigui x' una altra solució d'aquest sistema. Llavors

$$x - x' \equiv 0 \pmod{m_i}, \qquad i = 1, \ldots, k.$$

Equivalentment,

$$x - x' = \mu_i m_i, \quad \mu_i \in \mathbb{Z}, \quad i = 1, \ldots, k.$$

Així, $x - x'$ és múltiple de tots els m_i i per tant, per la pròpia definició de mínim comú múltiple, pàgina 97, $x - x'$ és múltiple de $m.c.m.(m_1, \ldots, m_k)$. Però com els m_i són coprimers dos a dos,

$$m.c.m.(m_1, \ldots, m_k) = m_1 \cdot \cdots \cdot m_k = M.$$

Això és conseqüència de que si posem $m = m.c.m.(m_1, \ldots, m_k)$, per definició,

$$(m_1) \cap (m_2) \cap \cdots \cap (m_k) = (m).$$

Però, per ser $m.c.d.(m_1, m_2) = 1$, tenim $m.c.m.(m_1, m_2) = m_1 m_2$, i per tant, $(m_1) \cap (m_2) = (m_1 m_2)$. Així,

$$(m_1 m_2) \cap (m_3) \cap \cdots \cap (m_k) = (m).$$

Per ser $m.c.d.(m_1 m_2, m_3) = 1$, tenim $m.c.m.(m_1 m_2, m_3) = m_1 m_2 m_3$, i per tant, $(m_1 m_2) \cap (m_3) = (m_1 m_2 m_3)$. Així,

$$(m_1 m_2 m_3) \cap (m_4) \cap \cdots \cap (m_k) = (m).$$

Repetint el procés arribem a $m = M$ com volíem.

Per tant,

$$x - x' = \mu M, \mu \in \mathbb{Z},$$

i per tant x' és pot escriure com indica la igualtat (11.6).

Exemple 11.3. *Resoleu el problema de l'exèrcit de Han Xing utilitzant el teorema xinès del residu.*

Solució. Hem de resoldre el sistema (11.2). Com els mòduls $3, 5, 7$ són coprimers podem utilitzar el teorema xinès del residu. Prenem

$$\begin{aligned} M &= 3 \cdot 5 \cdot 7 = 105 \\ M_1 &= \frac{M}{3} = 35, \\ M_2 &= \frac{M}{5} = 21, \\ M_3 &= \frac{M}{7} = 15, \end{aligned}$$

i resolem les 3 equacions,

$$\begin{aligned} 35y_1 &\equiv 2 \pmod 3 \\ 21y_2 &\equiv 3 \pmod 5 \\ 15y_3 &\equiv 2 \pmod 7 \end{aligned}$$

i obtenim

$$\begin{aligned} y_1 &= 1 \\ y_2 &= 3 \\ y_3 &= 2 \end{aligned}$$

(o bé, $y_1 = 2 + \overset{\bullet}{3}$, $y_2 = 1 + \overset{\bullet}{5}$, $y_3 = 2 + \overset{\bullet}{7}$). La solució general (11.6), és doncs,

$$x = M_1y_1 + M_2y_2 + M_3y_3 + \lambda M = 35 \cdot 1 + 21 \cdot 3 + 15 \cdot 2 + 105\lambda = 128 + 105\lambda.$$

11.7 Teorema xinès del residu a $\mathbb{Z}/(M)$

Teorema 11.9. *Siguin $m_1, \ldots, m_k$ enters coprimers dos a dos. Sigui $M = m.c.m.(m_1, \ldots, m_k) = m_1 \cdot \cdots \cdot m_k$. Llavors*

$$\mathbb{Z}/(M) \cong \mathbb{Z}/(m_1) \times \cdots \times \mathbb{Z}/(m_k).$$

Demostració. Aclarim primer que la notació $\cong$ vol dir que els dos anells que hi han a esquerra i dreta d'aquest símbol són isomorfs: hi ha una aplicació entre ells, bijectiva, que conserva suma i producte.

Definim aquesta aplicació així:

$$\begin{array}{ccc} \mathbb{Z}/(M) & \longrightarrow & \mathbb{Z}/(m_1) \times \cdots \times \mathbb{Z}/(m_k) \\ [x] & \mapsto & ([x], \ldots, [x]) \end{array}$$

Totes les $[x]$ que apareixen en aquesta darrera fila són diferents: la primera indica la classe de x a $\mathbb{Z}/(M)$ i les altres indiquen la classe de x en el corresponent $\mathbb{Z}/(m_i)$.

La primera cosa que hem de veure és que aquesta aplicació està ben definida. Això vol dir que si $[x] = [y] \in \mathbb{Z}/(M)$ llavors $[x] = [y] \in \mathbb{Z}/(m_i)$. Però això és evident, ja que $[x] = [y] \in \mathbb{Z}/(M)$ implica $y - x = \overset{\bullet}{M}$ i clarament qualsevol múltiple de M és múltiple de m_1, és a dir, $y - x = \overset{\bullet}{m_i}$, i per tant $[x] = [y] \in \mathbb{Z}/(m_i)$, $i = 1, \ldots, k$.

Veiem ara que és injectiva. Suposem

$$[x] = [y] \in \mathbb{Z}/(m_i), \quad i = 1, \ldots, k.$$

Això vol dir que

$$y - x = \overset{\bullet}{m_i}, \quad i = 1, \ldots, k.$$

Però quan un nombre enter és múltiple de diversos nombres enters és múltiple del seu mínim comú múltiple, però com els m_i són coprimers dos a dos, el seu mínim comú múltiple és el seu producte. Per tant $y - x = \overset{\bullet}{M}$, és a dir,

$$[x] = [y] \in \mathbb{Z}/(M).$$

Veiem ara que és exhaustiva. Prenem

$$([y_1], \ldots, [y_k]) \in \mathbb{Z}/(m_1) \times \cdots \times \mathbb{Z}/(m_k)$$

Hem de trobar $[x] \in \mathbb{Z}/(M)$ tal que $[x] = [y_i] \in \mathbb{Z}/(m_i)$, $i = 1, \ldots, k$.

És a dir, hem de resoldre el sistema de congruències de k equacions i una incògnita

$$x \equiv y_i, \, (\mathrm{mod}\, m_i) \quad i = 1, \ldots, k.$$

El teorema xinès del residu ens diu que aquest sistema té solució, i que dues solucions diferents difereixen en múltiples de M, és a dir, donen la mateixa classe a $\mathbb{Z}/(M)$.

La classe a $\mathbb{Z}/(M)$ d'aquesta solució és la antiimatge buscada i per tant l'aplicació és exhaustiva.

Deixem al lector comprovar que aquesta aplicació conserva suma i producte. □

Exemple 11.4. *Resoleu l'equació $x^2 = x$ a $\mathbb{Z}/(15)$.*

Solució. Com

$$x^2 - x = x(x - 1) = 0$$

si estiguéssim en un cos les dues úniques solucions serien $x = 0$ i $x = 1$, però com $\mathbb{Z}/(15)$ no és un cos les coses es compliquen una mica. Considerem l'aplicació

$$\begin{array}{ccccc} \Phi : \mathbb{Z}/(15) & \longrightarrow & \mathbb{Z}/(3) \times \mathbb{Z}/(5) \\ [x] & \mapsto & ([x], [x]) \end{array}$$

Sigui $[a] \in \mathbb{Z}/(15)$ solució de l'equació $x^2 = x$ a $\mathbb{Z}/(15)$. Aplicant Φ a la igualtat $[a]^2 = [a]$, i recordant que Φ és morfisme, obtenim $\Phi([a]^2) = \Phi[a] \cdot \Phi[a] = \Phi[a]$ és a dir, a $\mathbb{Z}/(3) \times \mathbb{Z}/(5)$,

$$([a], [a]) \cdot ([a], [a]) = ([a], [a])$$

Com que el producte a $\mathbb{Z}/(3) \times \mathbb{Z}/(5)$ és component a component l'anterior igualtat és equivalent a les dues igualtats

$$[a]^2 = [a] \text{ a } \mathbb{Z}/(3)$$
$$[a]^2 = [a] \text{ a } \mathbb{Z}/(5)$$

Com $\mathbb{Z}/(3)$ i $\mathbb{Z}/(5)$ són cossos, les solucions són $[a] = [0]$ 0 $[a] = [1]$ a $\mathbb{Z}/(3)$ i $[a] = [0]$ 0 $[a] = [1]$ a $\mathbb{Z}/(5)$.

Per tant podem determinar a estudiant les quatre possibilitats següents.

Primer cas. $[a] = [0] \in \mathbb{Z}/3$ i $[a] = [0] \in \mathbb{Z}/(5)$.

Busquem $a \in \mathbb{Z}$ tal que la seva classe a $\mathbb{Z}/(3)$ sigui $[0]$ i la seva classe a $\mathbb{Z}/(5)$ sigui també $[0]$. Sabem, pel Teorema xinès del residu, que aquest a existeix i que el podem trobar resolent el sistema

$$\begin{aligned} a &\equiv 0, \mod(3), \\ a &\equiv 0, \mod(5). \end{aligned}$$

Obtenim que a és múltiple de 15, i així $[a] = [0] \in \mathbb{Z}/(15)$ és solució de $x^2 = x$ a $\mathbb{Z}/(15)$.

Segon cas. $[x] = [0] \in \mathbb{Z}/3$ i $[x] = [1] \in \mathbb{Z}/(5)$. Busquem $a \in \mathbb{Z}$ tal que la seva classe a $\mathbb{Z}/(3)$ sigui $[0]$ i la seva classe a $\mathbb{Z}/(5)$ sigui $[1]$. Hem de resoldre el sistema

$$\begin{aligned} a &\equiv 0, \mod(3), \\ a &\equiv 1, \mod(5). \end{aligned}$$

Obtenim que $a = 6$ més qualsevol múltiple de 15, i així $[a] = [6] \in \mathbb{Z}/(15)$ és solució de $x^2 = x$ a $\mathbb{Z}/(15)$.

Tercer cas. $[x] = [1] \in \mathbb{Z}/3$ i $[x] = [0] \in \mathbb{Z}/(5)$. Busquem $a \in \mathbb{Z}$ tal que la seva classe a $\mathbb{Z}/(3)$ sigui $[1]$ i la seva classe a $\mathbb{Z}/(5)$ sigui $[0]$. Hem de resoldre el sistema

$$\begin{aligned} a &\equiv 1, \mod(3) \\ a &\equiv 0, \mod(5) \end{aligned}$$

Obtenim que $a = 10$ més qualsevol múltiple de 15, i així $[a] = [10] \in \mathbb{Z}/(15)$ és solució de $x^2 = x$ a $\mathbb{Z}/(15)$.

Quart cas. $[x] = [1] \in \mathbb{Z}/3$ i $[x] = [1] \in \mathbb{Z}/(5)$. Busquem $a \in \mathbb{Z}$ tal que la seva classe a $\mathbb{Z}/(3)$ sigui $[1]$ i la seva classe a $\mathbb{Z}/(5)$ sigui $[1]$. Hem de resoldre el sistema

$$\begin{aligned} a &\equiv 1, \mod(3) \\ a &\equiv 1, \mod(5) \end{aligned}$$

Obtenim que $a = 1$ més qualsevol múltiple de 15, i així $[a] = [1] \in \mathbb{Z}/(15)$ és solució de $x^2 = x$ a $\mathbb{Z}/(15)$.

Resumint l'equació de segon grau $x^2 = x$ te quatre solucions a $\mathbb{Z}/(15)$: $[0], [1], [6], [10]$.

Tema 12

Nombres complexos

Operacions aritmètiques, mòdul i conjugació [1,2]

El pas dels números racionals als números reals es justifica perquè hi ha magnituds físiques o geomètriques que no es poden mesurar amb números racionals; per exemple, la diagonal d'un quadrat prenent la longitud del costat com a unitat de mesura. En canvi, la necessitat d'ampliar el camp dels números reals i passar als números complexos prové de l'aritmètica o de l'àlgebra: per exemple una equació tan senzilla com $x^2 + 1 = 0$ no té solució en el camp real.

El mateix exemple que acabem de posar ens fa veure que el que ens falta és, com a mínim, un número que elevat al quadrat doni -1. Per aquest motiu introduïm un número, anomenat la *unitat imaginària* i representat per i, que compleixi $i^2 = -1$.

Un *número complex* és, per definició, un número de la forma

$$z = x + iy,$$

on x, y són números reals i i la unitat imaginària. El número x s'anomena la *part real* de z i s'escriu $x = \mathrm{Re}(z)$ i y n'és la *part imaginària*, $y = \mathrm{Im}(z)$. El conjunt de tots els números complexos el representarem per $\mathbb{C}$. Els números reals s'identifiquen amb els números complexos que tenen part imaginària nul·la. Els números complexos que tenen nul·la la part real s'anomenen *imaginaris purs*.

Així, doncs, donar un número complex és equivalent a donar un parell ordenat de números reals

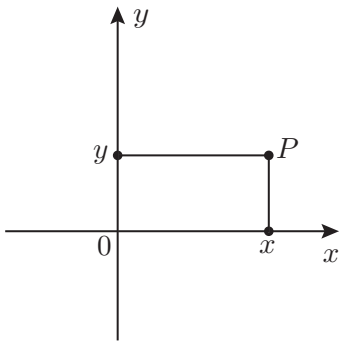
$$z = x + iy \longleftrightarrow (x, y)$$

i, per tant, hi ha una correspondència bijectiva entre elements de $\mathbb{C}$ i punts de $\mathbb{R}^2$.

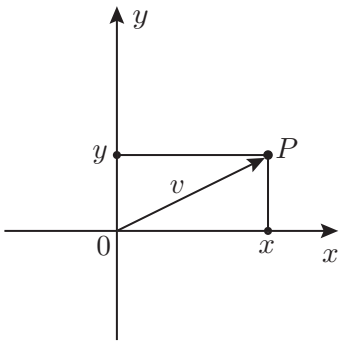
[1] Durant el curs 2015-2016 el tema "Nombres Complexos" va ser explicat pel Professor Julià Cufí, qui posteriorment va tenir la gentilesa de passar-me aquestes notes escrites.

[2] Capítol basat en uns apunts del professor Joaquim Bruna.

$z = x + iy \in \mathbb{C} \longleftrightarrow P = (x, y) \in \mathbb{R}^2$



El punt P és la representació geomètrica de z i té com a coordenades les parts real i imaginària de z.



D'altra banda cada punt P de $\mathbb{R}^2$ determina un vector lliure del pla: és el vector v que té per representant el vector fix $\overrightarrow{0P}$, és a dir, v té per components les coordenades de P.

Així, doncs, hi ha tres categories d'elements, de naturalesa diferent però que es corresponen biunívocament que són: números complexos, punts de $\mathbb{R}^2$ i vectors lliures de $\mathbb{R}^2$.

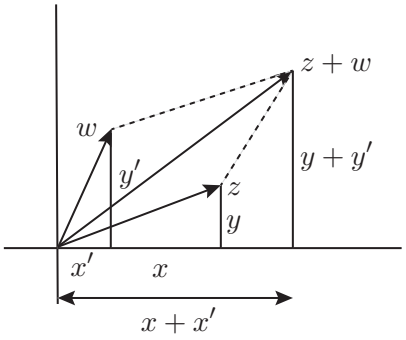
Definim ara una primera operació entre números complexos que és la suma:

Si $z = x + iy$, $w = x' + iy'$ posem $z + w = (x + x') + i(y + y')$.

Si pensem en els vectors associats a z i w (que continuarem anomenant z i w) tenim de seguida una interpretació geomètrica de la suma: la suma dels números z, w es correspon amb la suma dels vectors z, w:
Respecte de la suma els números complexos formen un grup: l'element neutre és el $0 = 0 + i0$ i l'oposat de $z = x + iy$ és $-z = -x - iy$ $(= -x + i(-y))$ i, és evident, que la suma és associativa i commutativa.

Ara definim el producte o *multiplicació* de dos números complexos per:

Si $z = x + iy$, $w = x' + iy'$ posem $z \cdot w = (xx' - yy') + i(xy' + x'y)$.



Aquesta definició és la mateixa que s'obté si fem el producte de z per w aplicant la propietat distributiva i tenim en compte que hem exigit $i^2 = -1$. És molt fàcil de comprovar que la multiplicació és commutativa, associativa i distributiva respecte de la suma:

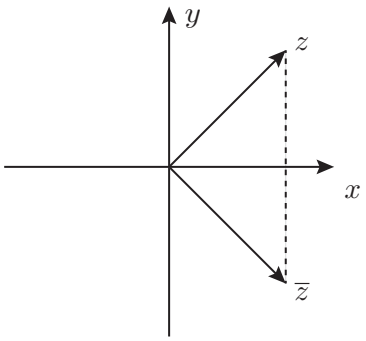
$$z \cdot w = w \cdot z, \quad z \cdot (w \cdot \tau) = (z \cdot w) \cdot \tau, \quad z(w + \tau) = z \cdot w + z \cdot \tau.$$

També hi ha un element neutre que és el número $1 = 1 + 0i$.

Ens agradaria ara poder interpretar geomètricament aquest producte; és a dir saber, donats $z, w \in \mathbb{C}$, quina o quines operacions geomètriques hem de fer amb els vectors corresponents a z i w per tal d'obtenir el vector corresponent a $z \cdot w$. Però aquesta pregunta no la podrem respondre fins més endavant i, d'alguna manera, tot el que farem a partir d'ara va encaminat a aquesta qüestió.

Per començar associarem a cada número complex dos números, un de complex i l'altre real no negatiu.

Si $z \in \mathbb{C}$, $z = x + iy$ definim el *conjugat* de z com el número $\overline{z} = z - iy$.



És clar que $\overline{z}$ és el simètric de z respecte de l'eix real. És immediat de

comprovar les igualtats següents:

$$\overline{z+w} = \overline{z} + \overline{w}; \qquad \overline{z \cdot w} = \overline{z} \cdot \overline{w},$$

$$\mathrm{Re}(z) = \frac{z+\overline{z}}{2}; \quad \mathrm{Im}(z) = \frac{z-\overline{z}}{2i}.$$

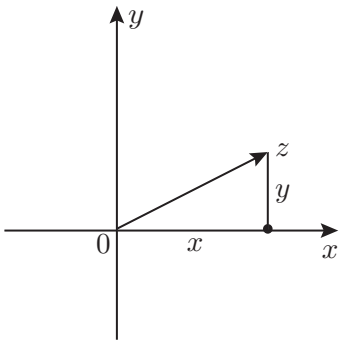
D'altra banda associem a $z \in \mathbb{C}$ el número real no negatiu, anomenat mòdul de z, definit per

$$|z| = \sqrt{x^2+y^2} \quad \text{si} \quad z = x+iy,$$

on s'entén que es pren l'arrel quadrada no negativa. És clar que $|z| = 0$ si i només si $z = 0$ i es compleix la relació:

$$z \cdot \overline{z} = |z|^2 = x^2 + y^2.$$

La interpretació geomètrica de $|z|$ és molt clara: el teorema de Pitàgores ens diu que $|z|$ és la



distància a l'origen del punt de $\mathbb{R}^2$ que representa z o bé la longitud del vector que correspon a z. És molt important d'establir les relacions que hi ha entre el mòdul i les operacions a $\mathbb{C}$. Són les següents:

$$1) \quad |z+w| \leq |z| + |w|, \qquad\qquad 2) \quad |z \cdot w| = |z| \cdot |w|.$$

La primera, anomenada també *desigualtat triangular* té una interpretació geomètrica: en un triangle, un costat és més petit o igual que la suma dels altres dos:

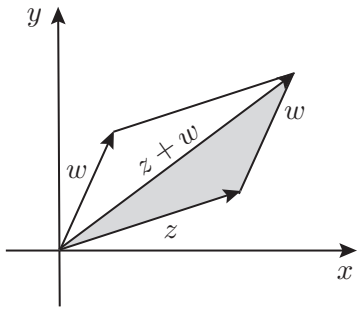
Demostrem-la:

Posem $z = x+iy$, $w = x'+iy'$ i, en lloc de 1) provem que

$$|z+w|^2 \leq (|z| + |w|)^2$$

que li és equivalent. Tenim

$$|z+w|^2 = |(x+x') + i(y+y')|^2 = x^2 + x'^2 + 2xx' + y^2 + y'^2 + 2yy',$$
$$(|z| + |w|)^2 = |z|^2 + |w|^2 + 2|z||w| = x^2 + y^2 + x'^2 + y'^2 + 2|z||w|$$



i, per tant, cal veure que

$$xx' + yy' \leq |z||w| \quad \text{o bé} \quad (xx' + yy')^2 \leq |z|^2|w|^2$$

que vol dir:

$$x^2x'^2 + y^2y'^2 + 2xx'yy' \leq x^2x'^2 + x^2y'^2 + y^2x'^2 + y^2y'^2$$

o sigui

$$2xx'yy' \leq x^2y'^2 + y^2x'^2$$

que és conseqüència de la desigualtat elemental:

$$2ab \leq a^2 + b^2 \text{ per a } a, b \in \mathbb{R},$$

certa ja que és equivalent a $(a-b)^2 \geq 0$.

Finalment provem la desigualtat 2); elevant al quadrat com abans tenim:

$$\begin{aligned} |z \cdot w|^2 = (xx' - yy')^2 + (xy' + x'y)^2 = x^2 \cdot x'^2 + y^2y'^2 - 2xx'yy' + \\ + x^2y'^2 + x'^2y^2 + 2xx'yy' = (x^2 + y^2)(x'^2 + y'^2) = |z|^2|w|^2. \end{aligned}$$

Ara podem veure que $\mathbb{C}$ amb la suma i el producte és un cos. Pel que hem dit només falta veure que si $z \in \mathbb{C}$ i $z \neq 0$ llavors z té un *invers* respecte del producte, és a dir, existeix $z' = z^{-1}$ tal que $z \cdot z' = 1$.

Definim $z^{-1} = \frac{\overline{z}}{|z|^2}$. Llavors

$$z \cdot z^{-1} = z \cdot \frac{\overline{z}}{|z|^2} = \frac{|z|^2}{|z|^2} = 1$$

com volíem.

Si $z = x + iy$ tenim, per a l'invers de z, $z^{-1} = \frac{1}{z}$:

$$\frac{1}{z} = \frac{1}{x+iy} = \frac{\overline{z}}{|z|^2} = \frac{x - iy}{x^2 + y^2} = \frac{x}{x^2 + y^2} - i\frac{y}{x^2 + y^2}.$$

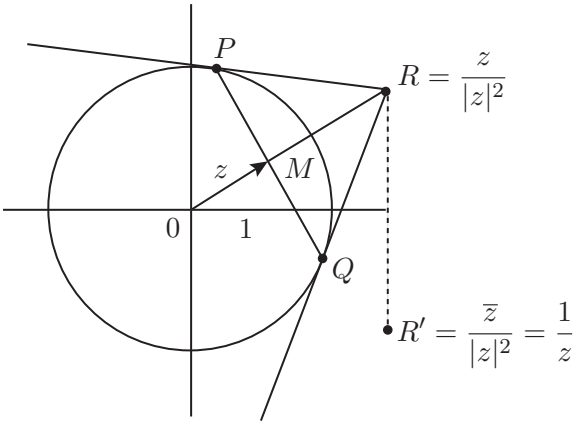
Si definim el quocient de dos complexos z i w, $w \neq 0$, per

$$\frac{z}{w} = z \cdot \frac{1}{w},$$

es comprova de seguida que

$$\left|\frac{1}{z}\right| = \frac{1}{|z|}; \quad \left|\frac{z}{w}\right| = \frac{|z|}{|w|}.$$

Per acabar aquest apartat veurem que l'invers de z, $\frac{1}{z}$, es pot interpretar (i construir) geomètricament



Suposem que el número complex z compleix $z \neq 0$ i $|z| < 1$ (si $|z| > 1$ podem aplicar prèviament una dilatació i si $|z| = 1$ és $\frac{1}{z} = \overline{z}$). Considerem la semirecta que surt de l'origen i passa per M, el punt que representa z, i també la perpendicular a aquesta semirecta per M la qual tallarà al cercle unitat en els punts P i Q. Tracem les tangents a la circumferència unitat per P i Q, les quals es tallen en un punt R, i finalment fem el simètric de R respecte de l'eix real, obtenint R'. Si acceptem que les distàncies de 0 a M i de 0 a R són inverses l'una de l'altra tindrem: $\overline{0M} = |z|$, $\overline{0R} = \frac{1}{|z|}$ i, per tant, al punt R li correspon el número complex $\frac{z}{|z|} \cdot \frac{1}{|z|} = \frac{z}{|z|^2}$ i R' serà $\frac{\overline{z}}{|z|^2} = \frac{1}{z}$.

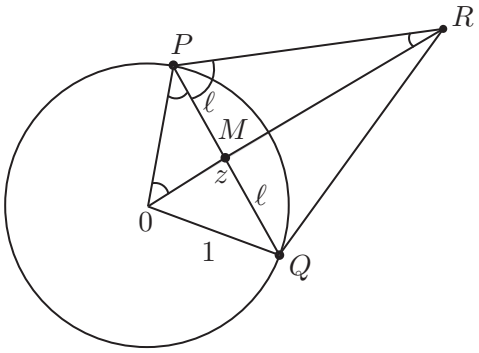
Per tal de justificar que el producte de distàncies $\overline{0M}$ i $\overline{0R}$ són inverses, observem el dibuix següent:
Els dos triangles amb els angles marcats iguals són semblants i, per tant,

$$\frac{\overline{0M}}{\ell} = \frac{\ell}{\overline{MR}}$$

que dóna

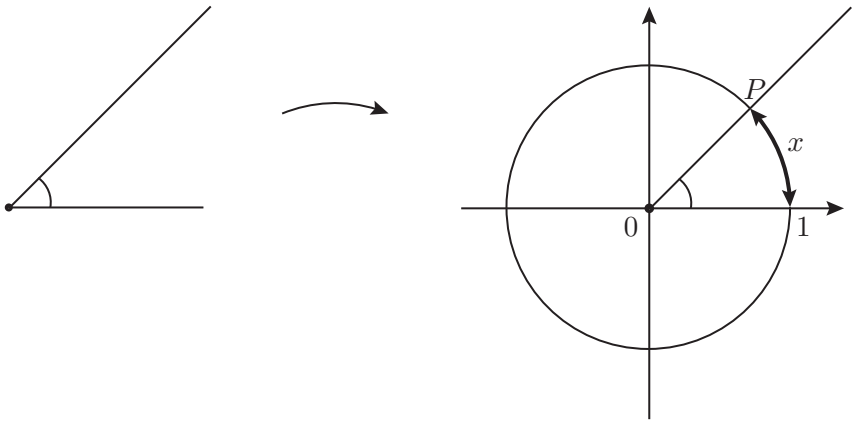
$$\ell^2 = \overline{0M} \cdot \overline{MR} = \overline{0M}(\overline{0R} - \overline{0M});$$

és a dir $\overline{0M} \cdot \overline{0R} = \ell^2 + \overline{0M}^2 = 1$, tal com volíem veure.



Un repàs breu de trigonometria

Comencem parlant del problema de la mesura d'angles. Aquest problema és equivalent al de la mesura d'arcs sobre una circumferència donada. En efecte, fixem una circumferència centrada a l'origen, el radi de la qual prendrem com a unitat de mesura. Donat un angle (determinat per dues semirectes amb origen comú) el podem transportar de manera que el seu vèrtex vagi a l'origen de coordenades i un dels costats vagi a la part positiva de l'eix $0X$; llavors l'altre costat tallarà la circumferència unitat en un punt P que determinarà amb el punt $(1, 0)$ un arc. La longitud d'aquest arc és, per definició, la mida de l'angle inicial.



Així doncs, hem de mesurar arcs sobre la circumferència; amb aquesta finalitat prendrem com a arc unitat l'arc que té longitud 1, és a dir, que la seva longitud és igual al radi de la circumferència. Aquest arc unitat s'anomena *radian*.

D'altra banda recordem que, per definició, el número π és la longitud d'una semicircumferència de radi 1. Així doncs, tota la circumferència és un arc de longitud 2π radians, mitja circumferència fa π radians i un quart de circumferència, $\frac{\pi}{2}$ radians. Una altra mesura d'angles és el grau; tenint

en compte que π radians, mitja circumferència corresponen a $180°$, és molt fàcil fer la conversió d'una unitat de mesura a una altra.

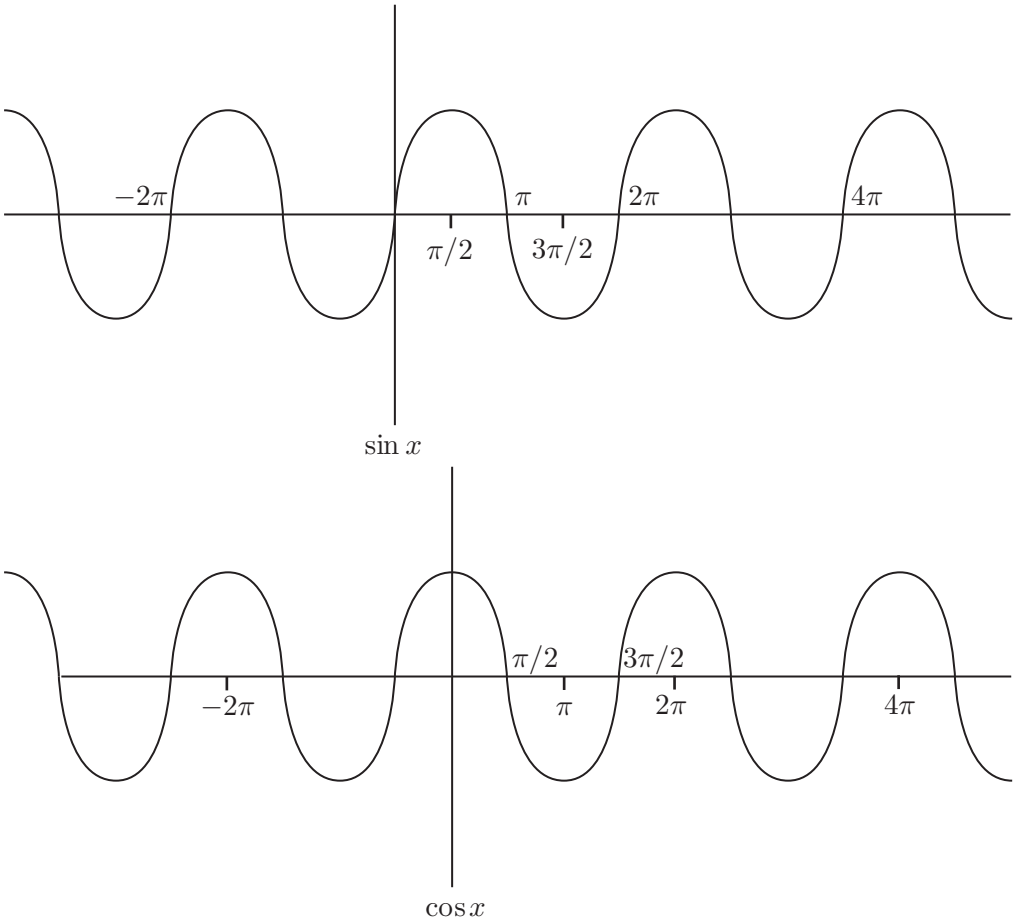
Si l'arc de mida x comença en el punt 1 i acaba en el punt P, les coordenades de P són, per definició, el *sinus* i el *cosinus* de x

$$P = (\cos x, \sin x).$$

En general si $x \geq 0$ és un número real podem considerar l'arc de longitud x comptada en sentit directe a partir del punt 1; aquest arc acabarà en un punt (potser després de fer unes quantes voltes a la circumferència) les coordenades del qual seran $\cos x$, l'abscisa i $\sin x$, l'ordenada. Si $x < 0$ podem fer el mateix però comptant l'arc de longitud $|x|$ en sentit invers (el de les agulles del rellotge).

Per definició, les funcions $\sin x$, $\cos x$ tenen el període 2π, és a dir:

$$\sin(x + 2\pi) = \sin x, \quad \cos(x + 2\pi) = \cos x, \quad x \in \mathbb{R}.$$

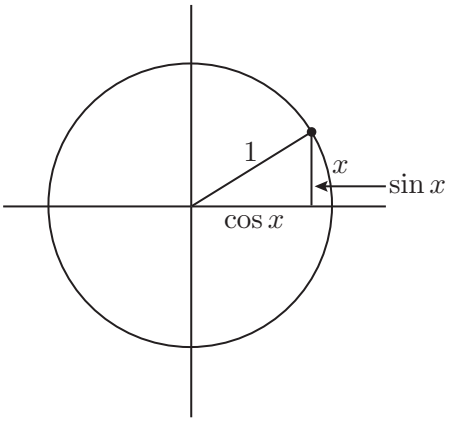


També es complirà:

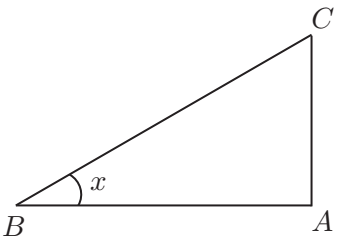
$$\begin{aligned} \sin(-x) &= -\sin x, & \cos(-x) &= \cos x, \\ \sin(x+\pi/2) &= \cos x, & \cos(x+\pi/2) &= -\sin x, \end{aligned}$$

i de l'aplicació del teorema de Pitàgores resulta:

$$\sin^2 x + \cos^2 x = 1.$$



Si tenim un triangle rectangle ABC qualsevol, la definició de $\sin x$, $\cos x$ i el teorema de Thales donen

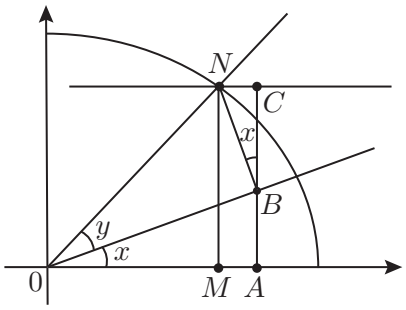


$$\sin x = \frac{\overline{AC}}{\overline{BC}}; \quad \cos x = \frac{\overline{BA}}{\overline{BC}}.$$

Les relacions més importants entre les raons trigonomètriques sinus i cosinus són les que fan referència a la suma d'angles:

$$\begin{aligned} \sin(x+y) &= \sin x \cdot \cos y + \cos x \cdot \sin y, \\ \cos(x+y) &= \cos x \cdot \cos y - \sin x \cdot \sin y. \end{aligned}$$

La segona és conseqüència de la primera, la qual es pot provar amb l'esquema següent:



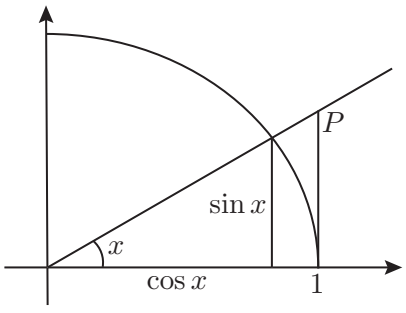
$$\begin{aligned}
&\overline{AC} = \overline{MN} = \sin(x+y),\\
&\overline{AB} = \overline{0B} \cdot \sin x = \cos y \cdot \sin x,\\
&\overline{BC} = \overline{BN} \cdot \cos x = \sin y \cdot \cos x,\\
&\overline{AC} = \overline{AB} + \overline{BC}.
\end{aligned}$$

A partir d'aquestes fórmules i fent servir que $\sin \pi/2 = 1$, $\sin \pi = 0, \ldots$ es poden obtenir:

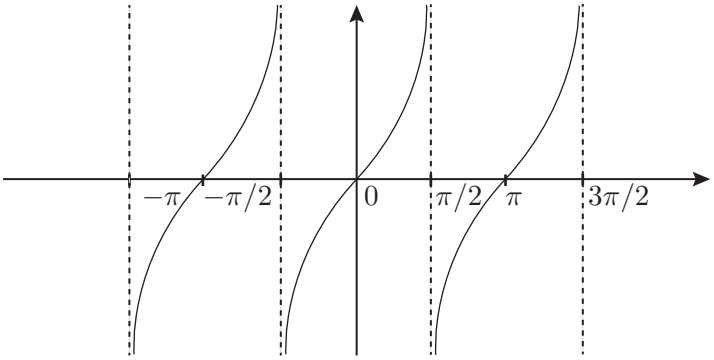
$$\sin \frac{\pi}{4} = \cos \frac{\pi}{4} = \frac{\sqrt{2}}{2}; \quad \sin \frac{\pi}{3} = \cos \frac{\pi}{6} = \frac{\sqrt{3}}{2}; \quad \cos \frac{\pi}{3} = \sin \frac{\pi}{6} = \frac{1}{2}.$$

Una altra raó trigonomètrica important és la tangent que es defineix per

$$\tan x = \frac{\sin x}{\cos x} \quad \text{si} \quad \cos x \neq 0.$$



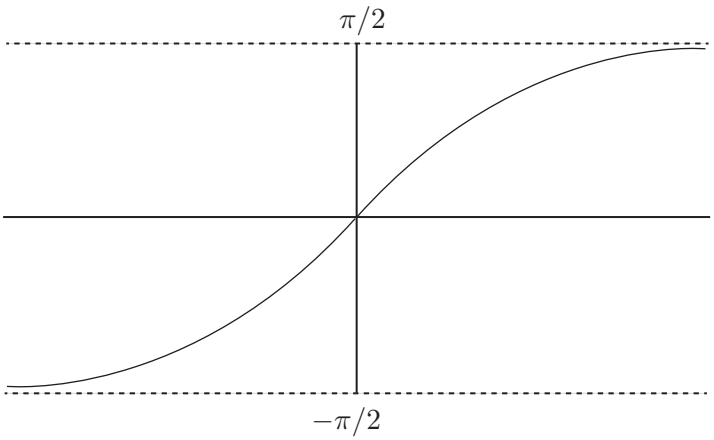
És clar que $\tan x$ és la longitud del segment que va des del punt 1 al punt P. També es veu de seguida, a partir del comportament de $\sin x$, $\cos x$ que la funció $\tan x$ només està definida si $x \neq \frac{\pi}{2} + k\pi$, $k \in Z$ i que la seva gràfica té la forma



Donat $y \in \mathbb{R}$ hi ha molts angles x tals que $\tan x = y$ però només n'hi ha un entre $-\pi/2$ i $\pi/2$. Aquest angle s'anomena $\arctan y$; és a dir

$$x = \arctan y \Longrightarrow y = \tan x, \quad x \in (-\pi/2, \pi/2).$$

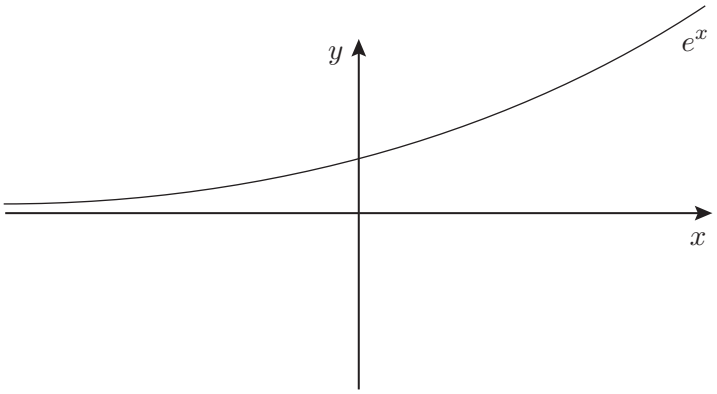
La funció arctan té una gràfica aproximada



i realitza una aplicació bijectiva i bicontínua entre la recta i l'interval $(-\pi/2, \pi/2)$.

L'exponencial complexa

Ja coneixem la funció exponencial de variable real e^x que té una gràfica de la forma



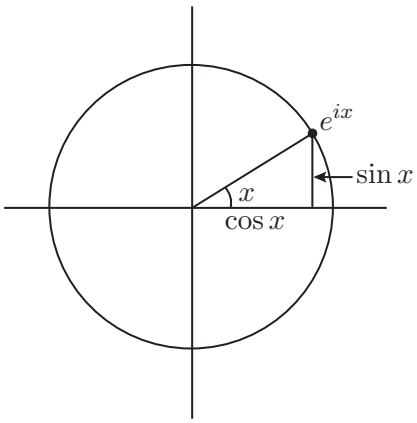
i que satisfà la relació fonamental

$$e^{x+y} = e^x \cdot e^y, \quad x, y \in \mathbb{R}.$$

Ara volem estendre-la al cas que l'exponent sigui complex de manera que es conservi aquesta relació fonamental. Si l'exponent és imaginari pur posem, per definició,

$$e^{ix} = \cos x + i \sin x, \quad x \in \mathbb{R}.$$

Així doncs, e^{ix} és un punt de la circumferència unitat de coordenades $\cos x$, $\sin x$ i és, per tant, el punt on acaba l'arc de longitud x que comença en el punt 1.



Per tant, $|e^{ix}| = 1$; així mateix tenim

$$\begin{aligned} e^{i(x+y)} &= \cos(x+y) + i \sin(x+y) = \cos x \cdot \cos y - \sin x \cdot \sin y + \\ &\quad + i(\sin x \cdot \cos y + \cos x \cdot \sin y) = \\ &= (\cos x + i \sin x) \cdot (\cos y + i \sin y) = e^{ix} \cdot e^{iy}, \end{aligned}$$

tal com volíem.

Com que $|e^{ix}| = 1$ tenim també:

$$\frac{1}{e^{ix}} = e^{\overline{ix}} = \cos x - i \sin x = e^{-ix}$$

i

$$\mathrm{Re}(e^{ix}) = \cos x = \frac{e^{ix} + e^{-ix}}{2}, \quad \mathrm{Im}(e^{ix}) = \sin x = \frac{e^{ix} - e^{-ix}}{2i}.$$

Si fem servir ara que $e^{imx} = (e^{ix})^m$, $m \in N$ tenim

$$\cos(mx) + i \sin(mx) = (\cos x + i \sin x)^m$$

i prenent per exemple $m = 3$ obtenim

$$\cos(3x) = \mathrm{Re}(\cos x + i \sin x)^3 = \cos^3 x - 3 \cos x \cdot \sin^2 x,$$
$$\sin(3x) = \mathrm{Im}(\cos x + i \sin x)^3 = 3 \cos^2 x \cdot \sin x - \sin^3 x.$$

Si $z \in \mathbb{C}$ i $z = x + iy$ posem per definició:

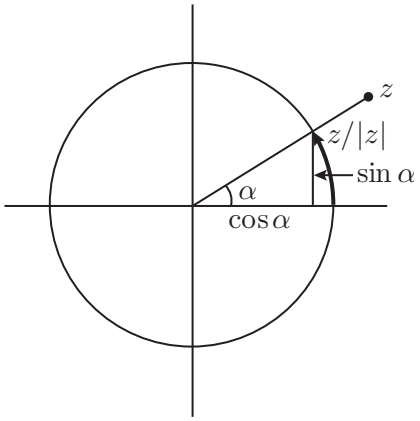
$$e^z = e^x \cdot e^{iy} = e^x(\cos y + i \sin y).$$

És clar que es compleix $e^{i(x+2\pi)} = e^{ix}$, $e^{z+2\pi i} = e^z$ i

$$|e^z| = e^x = e^{\mathrm{Re}(z)}.$$

Forma polar d'un número complex

Si z és un número complex, $z \neq 0$, considerem $\frac{z}{|z|}$; aquest número complex té mòdul 1 i, per tant, està representat per un punt del cercle unitat el qual determina a partir de la part positiva de l'eix $0X$ un arc. Sigui α, amb $0 \leq \alpha < 2\pi$, la mida d'aquest arc.



Llavors tenim

$$\frac{z}{|z|} = e^{i\alpha} = \cos\alpha + i\sin\alpha$$

o bé $z = |z|e^{i\alpha} = |z|(\cos\alpha + i\sin\alpha)$.

Si treiem la condició $0 \leq \alpha < 2\pi$ podem trobar altres arcs que també compleixen la igualtat anterior. De fet tenim

$$\frac{z}{|z|} = e^{i(\alpha+2k\pi)}, \quad k \in \mathbb{Z},$$

i, per tant,

$$z = |z|e^{i(\alpha+2k\pi)} = |z|(\cos(\alpha + 2k\pi)) + i\sin(\alpha + 2k\pi).$$

Qualsevol arc γ tal que $\frac{z}{|z|} = e^{i\gamma}$ sanomena un *argument* de z i l'arc α tal que $\frac{z}{|z|} = e^{i\alpha}$ i, a més, $0 \leq \alpha < 2\pi$ s'anomena l'argument principal de z. Així doncs un número $z \in \mathbb{C}$, $z \neq 0$, té infinits arguments i si α és l'argument principal de z:

$$\arg z = \{\alpha + 2k\pi;\, k \in Z\}$$

és el conjunt dels arguments de z. L'argument principal es representa per $\operatorname{Arg} z$.

Per exemple

$$\operatorname{Arg}(1+i) = \frac{\pi}{4}, \quad \arg(1+i) = \left\{\frac{\pi}{4} + 2k\pi : k \in Z\right\}.$$

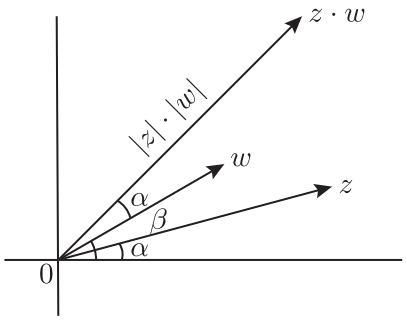
Si $x \in \mathbb{R}$, $x > 0$, $\operatorname{Arg}(x) = 0$, si $\alpha < 0$, $\operatorname{Arg}(x) = \pi$.

$$\operatorname{Arg}(-2i) = \frac{3\pi}{2}, \quad \arg(-2i) = \left\{\frac{3\pi}{2} + 2k\pi : k \in Z\right\}.$$

L'expressió de z en funció de $|z|$ i $\arg(z)$, $z = |z|e^{i\alpha}$, s'anomena la forma *polar* de z i permet, finalment, donar una interpretació geomètrica del producte de dos números complexos: posem $z = |z|e^{i\alpha}$, $w = |w|e^{i\beta}$, on $\alpha \in \arg(z)$, $\beta \in \arg(w)$. Llavors:

$$z \cdot w = |z| \cdot |w| \cdot e^{i\alpha} \cdot e^{i\beta} = |z| \cdot |w| \cdot e^{i(\alpha+\beta)}$$

és a dir, $\alpha + \beta \in \arg(z \cdot w)$ i, com sabem, $|z| \cdot |w| = |z \cdot w|$. Per tant, $z \cdot w$ té com a mòdul el producte dels mòduls de z i w i com a argument una suma d'arguments de z i w.



És a dir, per a multiplicar z, w cal girar respecte de l'origen el vector de w un angle igual a l'argument de z i després, en la direcció resultant, agafar un vector de longitud $|z|\cdot|w|$, que vol dir aplicar al vector w girat una homotècia respecte de l'origen de raó $|z|$.

Anàlogament resuta, per al quocient,

$$\frac{z}{w} = \frac{|z|e^{i\alpha}}{|w|e^{i\beta}} = \frac{|z|}{|w|} \cdot e^{i(\alpha-\beta)}.$$

Dit d'una altra manera, al multiplicar, els mòduls es multipliquen i els arguments se sumen i al dividir els mòduls es divideixen i els arguments es resten. Observem però que la igualtat

$$\operatorname{Arg}(z \cdot w) = \operatorname{Arg}(z) + \operatorname{Arg}(w)$$

no és certa en general; només es pot dir que

$$\operatorname{Arg}(z) + \operatorname{Arg}(w) \in \arg(z \cdot w).$$

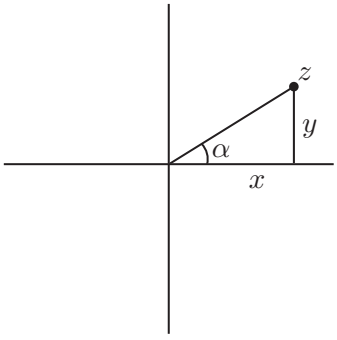
Si tenim z en forma polar és molt fàcil passar a la seva forma cartesiana o binòmica; en efecte

$$z = x + iy = |z| \cdot e^{i\alpha} = |z| \cdot (\cos\alpha + i \sin\alpha),$$

per tant,

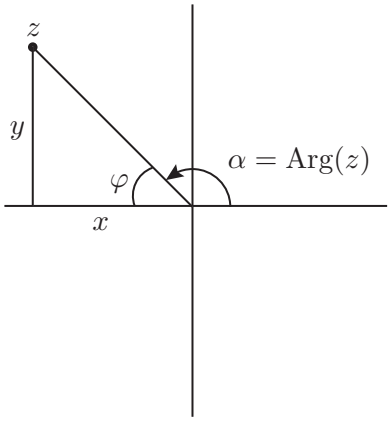
$$x = |z| \cos\alpha, \quad y = |z| \sin\alpha, \quad \text{si } \alpha \in \arg(z).$$

Per tal de fer el pas recíproc observem que si $z = x + iy$, llavors $|z| = \sqrt{x^2 + y^2}$, i $\arg(z)$ quant val? Si per exemple busquem $\operatorname{Arg}(z)$ i z és del primer quadrant ($x > 0$, $y \geq 0$) tenim:



$$\operatorname{Arg}(z) = \arctan\frac{y}{x}$$

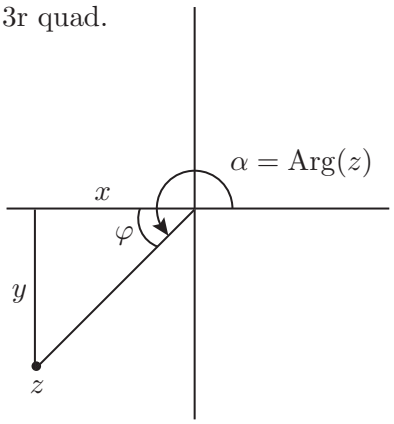
En els altres quadrants s'ha d'adaptar el triangle anterior a cada cas. Per exemple, en el segon quadrant:



$$\varphi = \arctan \frac{y}{|x|} \quad \text{i} \quad \alpha = \pi - \varphi.$$

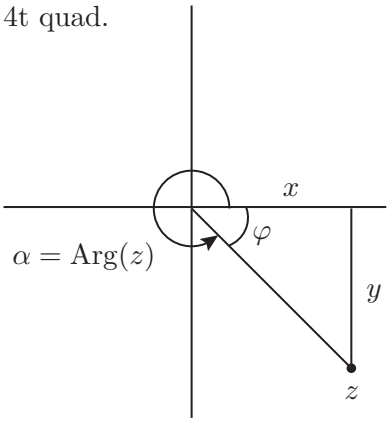
I en els altres quadrants:

3r quad.



$$\varphi = \arctan \frac{|y|}{|x|}, \quad \alpha = \pi + \varphi$$

4t quad.



$$\varphi = \arctan \frac{|y|}{x}, \quad \alpha = 2\pi - \varphi.$$

Per exemple si $z = 1 - \sqrt{3}i$, tenim:

$$|z| = 2, \quad \text{Arg}(z) = 2\pi - \frac{\pi}{3} = \frac{5\pi}{3}.$$

Imaginem-nos ara que volem calcular z^{5000}! a partir de la forma binòmica de z:

$$(1 - \sqrt{3}i)^{5000}.$$

Si ho féssim amb el binomi de Newton ens sortiria una expressió de 5001 termes amb uns números combinatoris no gens fàcils de calcular. En canvi si ho fem en forma polar tenim

$$(1 - \sqrt{3}i)^{5000} = (2e^{i5\pi/3})^{5000} = 2^{5000} e^{i5\pi \cdot 5000/3}$$

i ara només cal buscar l'argument principal d'aquest número; com que

$$\frac{25000}{3} = 8333 + \frac{1}{3}$$

resulta

$$e^{i\frac{25000}{3}\pi} = e^{i8333\pi} \cdot e^{i\pi/3}$$

i $e^{i8333\pi} = e^{i8332\pi} \cdot e^{i\pi} = -1$.

Per tant,

$$(1 - \sqrt{3}i)^{5000} = -2^{5000} e^{i\pi/3} = -2^{5000} \left(\frac{1}{2} + i\frac{\sqrt{3}}{2} \right).$$

Arrels de números complexos

Recordem primer què passa en el camp dels números reals. Sigui $a \in \mathbb{R}$ i $n \in N$, i busquem $x \in \mathbb{R}$ amb $x = \sqrt[n]{a}$, és a dir, $x^n = a$. Se sap que si $a > 0$, hi ha un únic número $x > 0$ tal que $x^n = a$, sigui qui sigui $n \in N$. Ara, d'acord amb la regla dels signes veiem que si $a < 0$ i $n = \dot{2}$ no hi pot haver cap número x amb $x^n = a$. En canvi si $a < 0$ però $n \neq \dot{2}$ el que acabem de dir ens assegura que també hi ha un únic x real, $x < 0$, tal que $x^n = a$. Finalment, la mateixa regla dels signes diu que si $a > 0$, $n = \dot{2}$ i $x^n = a$, també és $(-x)^n = a$. Resumint:

1) Si $n = \dot{2}$ i $a > 0$ hi ha dos valors reals de x tals que $x^n = a$. Si $n = \dot{2}$ i $a < 0$ no hi ha cap $x \in \mathbb{R}$ amb $x^n = a$.

2) Si $n \neq \dot{2}$ i $a \in \mathbb{R}$ hi ha un únic número real $x \in \mathbb{R}$ amb $x^n = a$.

En el camp complex la situació és diferent i de fet la introducció de la unitat imaginària i amb $i^2 = -1$ és un intent de fer possible l'extracció d'arrels quadrades de números negatius. Veurem que això és possible i, més generalment, tenim

- En el cos $\mathbb{C}$ tot número $a \neq 0$ té n arrels n-èsimes diferents per a cada $n \in N$. És a dir, existeixen $z_0, z_1, z_2, \ldots, z_{n-1} \in \mathbb{C}$ i dfferents entre si, amb $z_j^n = a$, $j = 0, 1, \ldots, n-1$.

Per tal de provar-ho escrivim el número $a \in \mathbb{C}$, $a \neq 0$ en forma polar

$$a = |a|e^{i\alpha} \quad \text{on} \quad \alpha = \text{Arg}(a),$$

per exemple, i sigui $z \in \mathbb{C}$ un número desconegut al qual imposem la condició $z^n = a$.

Si posem $z = |z|e^{i\varphi}$ amb $\varphi \in \arg(z)$ i escrivim $z^n = a$, per tal de trobar $|z|$ i φ, tenim

$$z^n = |z|^n e^{in\varphi} = |a|e^{i\alpha},$$

d'on es dedueix $|z|^n = |a|$, és a dir, $|z| = \sqrt[n]{|a|}$, l'única arrel n-èsima positiva de $|a|$. Pel que fa als arguments, la igualtat anterior exigeix

$$n\varphi = \alpha + 2k\pi \quad \text{amb} \quad k \in Z,$$

o bé

$$\varphi = \frac{\alpha}{n} + \frac{2\pi}{n}k, \quad k \in Z.$$

Així hem trobat $|z|$ de manera única i, en principi, infinits valors de $\varphi \in \arg(z)$. Però de fet només obtenim n valors diferents de z perquè donant a k els valors $0, 1, 2, \ldots$ obtenim

$$k = 0 : \varphi = \frac{\alpha}{n}, \quad k = 1 : \varphi = \frac{\alpha}{n} + \frac{2\pi}{n}, \quad k = 2 : \varphi = \frac{\alpha}{n} + \frac{2\pi}{n} \cdot 2, \ldots$$
$$\ldots, k = n-1 : \varphi = \frac{\alpha}{n} + \frac{2\pi}{n}(n-1), \quad k = n : \varphi = \frac{\alpha}{n} + 2\pi,$$

però $e^{i\frac{\alpha}{n}} = e^{i(\frac{\alpha}{n}+2\pi)}$. Més formalment: si per a cada $k \in Z$ fem la divisió euclidiana per n tindrem

$$k = nq + r \quad \text{amb} \quad r = 0, 1, \ldots, n-1$$

i $e^{i\frac{2\pi}{n}k} = e^{i\frac{2\pi}{n}(nq+r)} = e^{i2nq} \cdot e^{i\frac{2\pi}{n}r} = e^{i\frac{2\pi}{n}r}$. Així doncs la solució al problema $z^n = a$ són els n números

$$z_j = |a|^{1/n} e^{i(\frac{\alpha}{n} + \frac{2\pi}{n}j)}, \quad j = 0, 1, \ldots, n-1$$

els quals són tots diferents perquè no pot ser que

$$\frac{2\pi}{n}j = \frac{2\pi}{n}j' + 2\pi k, \quad 0 \le j, j' \le n-1$$

perquè aquesta igualtat donaria lloc a

$$j - j' = n \cdot k = \dot{n},$$

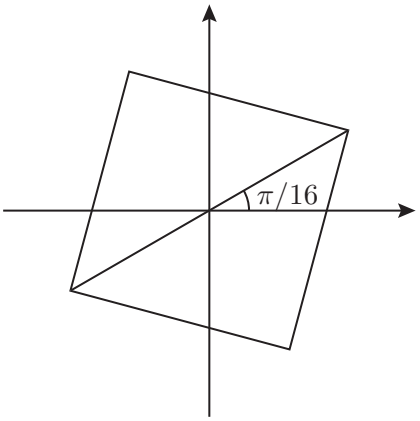
que és impossible perquè $|j - j'| \le n - 1$.

Per exemple calculem $z = \sqrt[4]{a}$, quan $a = 1 + i$. Tenim

$$1 + i = \sqrt{2}e^{i\pi/4}$$

i obtenim $|z| = |a|^{1/4} = 2^{1/8}$ i $\varphi \in \arg(z) = \frac{\pi}{16} + \frac{\pi}{2}k$, $k = 0, 1, 2, 3$ que donen

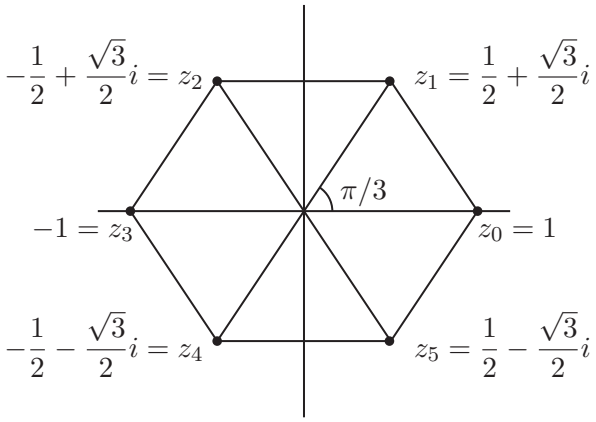
$$z_0 = 2^{1/8}e^{i\frac{\pi}{16}}, \quad z_1 = 2^{1/8}e^{i\frac{9}{16}\pi}, \quad z_2 = 2^{1/8}e^{i\frac{17}{16}\pi}, \quad z_3 = 2^{1/8}e^{i\frac{25}{16}\pi},$$



En general els punts que representen $\sqrt[n]{a}$ seran els vèrtexs d'un polígon regular de n costats perquè passem d'un vèrtex al següent fent un gir de $\frac{2\pi}{n}$ radians.

En el cas particular $a = 1$, les arrels n-èsimes s'anomenen arrels n-èsimes de la unitat i són els vèrtexs d'un polígon regular de n costats de radi 1 que té un vèrtex en el punt 1. Per exemple per a $n = 6$ tenim

$$z_j = e^{i\frac{\pi}{3}j}, \quad j = 0, 1, \ldots, 5.$$



Observem que si anomenem τ a l'arrel n-èsima de 1, $\tau = e^{i\frac{2\pi}{n}}$, llavors el conjunt de les n arrels n-èsimes de la unitat és un grup que té a τ com a generador perquè

$$z_0 = 1 = \tau^0, \quad z_1 = \tau, \quad z_2 = \tau^2, \ldots, z_{n-1} = \tau^{n-1}.$$

L'arrel τ s'anomena arrel n-èsima primitiva de la unitat. Qualsevol arrel n-èssima $\tau \neq 1$ compleix la relació:

$$1 + \tau + \tau^2 + \cdots + \tau^{n-1} = 0.$$

Per comprovar-ho només cal escriure:

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

i observar que $\tau^n - 1 = 0$ i $\tau - 1 \neq 0$.

Potències d'exponent racional

Si $z \in \mathbb{C}$ i n és natural la potència z^n té un sentit unívoc; és $z^n = z \cdot \overset{n)}{z \ldots} z$. El mateix passa si n és enter, posant per definició

$$z^{-n} = \frac{1}{z^n} \quad \text{si} \quad n \geq 0 \text{ i } z \neq 0.$$

Si ara considerem $q \in Q$ i volem definir z^q, com ho podem fer?

Posem $q = \frac{m}{n}$ i suposem $m, n > 0$. Llavors podem definir per a $z \in \mathbb{C}$, $z \neq 0$:

$$z^q = z^{\frac{m}{n}} = (z^{1/n})^m$$

que serà un conjunt de números complexos. En efecte, si $z = |z|e^{i\alpha}$, tindrem

$$z^{\frac{m}{n}} = (z^{1/n})^m = (|z|^{1/n} \cdot e^{i(\frac{\alpha}{n} + \frac{2\pi}{n}k)})^m = |z|^{\frac{m}{n}} \cdot e^{i(\alpha\frac{m}{n} + \frac{2\pi}{n}m \cdot k)}, \quad k = 0, 1, \ldots, n-1 \tag{12.1}$$

i aquesta definició no depèn de l'expressió de q com a quocient d'enters. Si ara imposem que l'expressió de q és irreduïble, és a dir, $\text{mcd}(m, n) = 1$ llavors els números anteriors són tots diferents. En efecte, en cas contrari tindríem

$$\frac{2\pi}{n}mk = \frac{2\pi}{n}mk' + 2\pi r$$

o sigui

$$m(k - k') = n \cdot r = \dot{n}$$

i com que n és primer amb m hauria de dividir $k - k'$, cosa que és impossible perquè $|k - k'| \leq n - 1$.

Així doncs a (12.1) hi ha tants números diferents com el denominador de l'expressió irreduïble de q.

També podríem considerar de posar $z^q = z^{\frac{m}{n}} = (z^m)^{1/n}$ que és un conjunt de n números i, per tant, en general no coincidirà amb el conjunt de números (12.1). Ara serà

$$(z^m)^{1/n} = (|z|^m e^{im\alpha})^{1/n} = |z|^{\frac{m}{n}} e^{i(\frac{m}{n}\alpha + \frac{2\pi}{n}k)}, \quad k = 0, 1, \ldots, n-1. \tag{12.2}$$

Observem que cada número de (12.1) apareix a (12.2); en efecte per a $k = 0, \ldots, n-1$, podem trobar $k' \in \{0, 1, \ldots, n-1\}$ i $r \in Z$ de manera que

$$\frac{2\pi}{n}m \cdot k = \frac{2\pi}{n} \cdot k' + 2\pi r$$

o bé $m \cdot k = k' + r \cdot n$: si $m \cdot k \leq n-1$, prenem $r = 0$; si $m \cdot k = n, n+1, \ldots, 2n-1$, prenem $r = 1$ i així successivament.

Per tant si $\mathrm{mcd}(m,n) = 1$, els conjunts (12.1) i (12.2) coincideixen i tenen n elements. En cas contrari només és correcte prendre (12.1) com a definició de $z^{m/n}$.

Per exemple si $z = 1$, $q = \frac{1}{2} = \frac{2}{4}$, tenim

$$\sqrt{1} = \{-1, 1\}; \quad (1^{1/4})^2 = \{1, -1, i, -i\}^2 = \{-1, 1\}$$

però $(1^2)^{1/4} = \sqrt[4]{1} = \{1, -1, i, -1\}$. S'ha d'anar en compte doncs amb les igualtats entre potències fraccionàries de complexos. Per exemple, una igualtat aparentment tan trivial com

$$(z^n)^{1/n} = z$$

no és certa, ja que el terme de l'esquerra representa un conjunt de n números complexos, un dels quals és z.

Apèndix

El cos dels números complexos no es pot ordenar.

Hem vist que $\mathbb{C}$, amb la suma i el producte té estructura de cos, i $\mathbb{R}$ és un subcos de $\mathbb{C}$. Hem vist també que algunes operacions que no són possibles a $\mathbb{R}$ ho són a $\mathbb{C}$, com per exemple l'extracció d'arrels quadrades de números reals negatius. Però, en canvi al passar de $\mathbb{R}$ a $\mathbb{C}$, hi ha alguna propietat que es perd com, per exemple, l'ordre. És impossible definir a $\mathbb{C}$ una relació d'ordre total compatible amb la suma i el producte, és a dir, que compleixi:

1) $z \leq w$, $z' \leq w' \Rightarrow z + z' \leq w + w'$.

2) $z > 0$, $w > 0 \Rightarrow z \cdot w > 0$.

En efecte imaginem una ordenació total que complís aquestes propietats. Tindríem $i > 0$ o bé $i < 0$.

Si $i > 0$, llavors $i^2 = -1 > 0$ i sumant 1 als dos membres de la desigualtat queda $0 > 1$; però per una altra banda $-1 > 0$ donaria $1 > 0$ i arribem a una contradicció. El mateix passa si partim del supòsit $i < 0$.

Tema 13

Polinomis

13.1 L'anell de Polinomis $K[x]$

Sigui K un cos. Un polinomi és una expressió del tipus

$$P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \qquad a_i \in K.$$

Es diu que a_i és el *coeficient* i-èssim del polinomi. Un tal polinomi es diu que té *grau* n, ja que la potència més gran de x que apareix a l'expressió de $P(x)$ és x^n. Això vol dir que estem suposant, en l'anterior escriptura, que $a_n \neq 0$. Si fos zero ja no l'hagéssim escrit. En canvi els coeficients anteriors, $a_i, 0 \leq i < n$, poden ser o no iguals a zero.

Així, $P(x) = a_0 + a_1x + a_2x^2$, amb $a_2 \neq 0$, té grau 2; $P(x) = a_0 + a_1x$, amb $a_1 \neq 0$, té grau 1; $P(x) = a_0$, amb $a_0 \neq 0$, té grau 0. Això deixa fora de joc el polinomi $P(x) = 0$!!!

Per motius únicament de comoditat, que es veuran més endavant, definim que el polinomi $P(x) = 0$ té grau $-\infty$.

Dos polinomis són *iguals* quan el coeficient i-èssim de l'un coincideix amb el coeficient i-èssim de l'altre, per a tota i.

La suma de polinomis es defineix 'component a component', és a dir, si

$$P(x) = \sum_{i=0}^{n} a_ix^i, \quad Q(x) = \sum_{j=0}^{m} b_jx^j, m \geq n$$

llavors

$$P(x) + Q(x) = \sum_{k=0}^{m} (a_k + b_k)x^k$$

on estem suposant que $a_k = 0$ quan $k > n$.

La condició $m \geq n$ no és cap restricció ja que en sumar dos polinomis un té grau més gran o igual a l'altre, i les operacions que manipulem són commutatives.

El producte de polinomis es defineix de manera que sigui distributiu respecte de la suma formal que apareix en l'escriptura del polinomi.

Així, amb la mateixa notació anterior,

$$P(x)Q(x) = \sum_{k=0}^{n+m} (\sum_{i+j=k} a_i b_j) x^k.$$

Per exemple, si $n = m = 2$, tenim

$$\begin{aligned} P(x)Q(x) &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 \\ &+ (a_1b_2 + a_2b_1)x^3 + a_2b_2x^4. \end{aligned}$$

És fàcil veure que $K[x]$ amb la suma i el producte que acabem de definir té estructura d'anell commutatiu. L'element neutre de la suma és el polinomi $P(x) = 0$, i l'element neutre del producte és el polinomi $P(x) = 1$.

Teorema 13.1 (Fórmula del grau)**.** *El grau del producte és la suma dels graus.*

Demostració. Suposem que els polinomis donats són diferents de zero. El coeficient de major grau del producte és el producte dels coeficients de major grau corresponents, $a_n b_m$. I, com que estem sobre un cos, el producte d'elements diferents de zero és diferent de zero. □

Escriurem

$$\operatorname{grau}(P(x)Q(x)) = \operatorname{grau} P(x) + \operatorname{grau} Q(x). \tag{13.1}$$

Aquesta fórmula és la que justifica haver definit $\operatorname{grau} 0 = -\infty$ ja que si la volem estendre al cas en que $Q(x) = 0$ (només l'hem demostrat quan tots dos polinomis són diferents de zero) tindríem

$$\operatorname{grau}(P(x) \cdot 0) = \operatorname{grau} P(x) + \operatorname{grau} 0,$$

és a dir,

$$\operatorname{grau} 0 = \operatorname{grau} P(x) + \operatorname{grau} 0.$$

La única manera que aquesta igualtat sigui certa per a tot $P(x)$ és definir $\operatorname{grau} 0 = -\infty$ amb el conveni de sumació natural $-\infty + k = -\infty$, $\forall k \in \mathbb{N}$. Així, doncs, la fórmula (13.1) és certa en tot cas, és a dir, tant si els polinomis són zero com si no.

Corol·lari 13.2. *$K[x]$ és domini d'integritat.*

Demostració. Si $P(x)Q(x) = 0$, tenim $\operatorname{grau} P(x) + \operatorname{grau} Q(x) = -\infty$, i per tant, o bé $\operatorname{grau} P(x) = -\infty$ o $\operatorname{grau} Q(x) = -\infty$. És a dir, un dels dos és el polinomi zero. □

Corol·lari 13.3. *Els únics elements invertibles de $K[x]$ són els polinomis de grau zero, és a dir, els elements de K.*

Demostració. Si $P(x)Q(x) = 1$, tenim $\operatorname{grau} P(x) + \operatorname{grau} Q(x) = 0$, i per tant, $\operatorname{grau} P(x) = \operatorname{grau} Q(x) = 0$. □

Corol·lari 13.4. *A $K[x]$ podem simplificar polinomis no nuls.*

Demostració. Suposem $P(x)Q(x) = P(x)R(x)$ amb $P(x) \neq 0$. Llavors $P(x)(Q(x)-R(x)) = 0$. I per ser domini d'integritat ha de ser $Q(x) = R(x)$. □

Observem que no cal que $P(x)$ sigui invertible per a poder-lo simplificar.

13.2 $K[x]$ és un anell Euclidià

Teorema 13.5. *Donats dos polinomis $D(x), d(x)$, amb $d(x) \neq 0$, existeixen polinomis $q(x)$ i $r(x)$ tals que*

$$D(x) = d(x)q(x) + r(x), \qquad \operatorname{grau} r(x) < \operatorname{grau} d(x).$$

A més, $q(x), r(x)$ són únics en aquestes condicions.

Demostració. Si $\operatorname{grau} D(x) < \operatorname{grau} d(x)$ posem

$$D(x) = d(x) \cdot 0 + D(x)$$

i hem acabat. Així, doncs, el que ens cal demostrar és que *donat un polinomi $D(x)$ de grau m, i un polinomi $d(x) \neq 0$ de grau més petit o igual a m, existeixen polinomis $q(x)$ i $r(x)$ tals que*

$$D(x) = d(x)q(x) + r(x), \qquad \operatorname{grau} r(x) < \operatorname{grau} d(x).$$

I això ho fem pe inducció sobre m. Si $m = 0$, tant $D(x)$ com $d(x)$ són constants (elements de K). Denotem-los D, d amb $d \neq 0$. Llavors podem posar

$$D = d \cdot \frac{D}{d} + 0$$

i com $\operatorname{grau} 0 = -\infty < 0$ hem acabat.

Suposem el resultat cert fins a $m - 1$.

Sigui $D(x) = a_0 + \cdots + a_m x^m$ i $d(x) = b_0 + \cdots + b_n x^n$ amb $m \geq n$. Considerem el polinomi

$$A(x) = D(x) - \frac{a_m}{b_n} d(x) x^{m-n}.$$

Com $\operatorname{grau} A(x) < m$, tenim, per hipòtesis d'inducció,

$$A(x) = d(x)q(x) + r(x), \qquad \operatorname{grau} r(x) < \operatorname{grau} d(x).$$

Substituint aquest valor de $A(x)$ a la fórmula anterior tenim

$$D(x) = A(x) + \frac{a_m}{b_n} d(x) x^{m-n} = d(x)q(x) + r(x) + \frac{a_m}{b_n} d(x) x^{m-n} = d(x)q_1(x) + r(x)$$

amb $q_1(x) = q(x) + \frac{a_m}{b_n} x^{m-n}$. Això acaba la demostració. □

13.3 $K[x]$ és un anell d'ideals principals

Teorema 13.6. *$K[x]$ és un anell d'ideals principals.*

Demostració. Sigui I un ideal de $K[x]$. Suposem que I no es redueix al 0. Com I conté elements diferents de zero, prenem $d(x)$ un element de I de grau mínim entre els elements de I diferents de zero. És a dir, que a I no hi ha cap polinomi diferent de zero de grau estrictament més petit que el grau de $d(x)$.

Sigui $D(x) \in I$. Dividim i obtenim $D(x) = d(x)q(x)+r(x)$, amb $\operatorname{grau} r(x) < \operatorname{grau} d(x)$. Per les propietats d'ideal (tancat per la suma d'elements de I i pel producte per elements de $K[x]$) veiem que

$$r(x) = D(x) - d(x)q(x) \in I.$$

Però com $\operatorname{grau} r(x) < \operatorname{grau} d(x)$ ha de ser $r(x) = 0$, i per tant $D(x) = d(x)q(x)$. Per tant, tot element $D(x) \in I$ és múltiple de $d(x)$, i.e. $I = (d(x))$ com volíem demostrar. □

Observem que

$$(d(x)) = (q(x)) \Leftrightarrow q(x) = \lambda d(x), \lambda \in K.$$

Es diu que el generador de l'ideal I està determinat *llevat d'escalars.*

m.c.d. i m.c.m.

Com a $\mathbb{Z}$.

La única diferència és que sobre $\mathbb{Z}$ el m.c.d. i el m.c.m. queden determinats llevat del signe i aquí queden determinats llevat d'escalars. Per això a vegades es parla *d'un* màxim comú divisor en lloc *del* màxim comú divisor (o mínim comú múltiple).

Concretament, donats $P(x), Q(x) \in K[x]$ definim el màxim comú divisor per

$$m.c.d.(P(x), Q(x)) = d(x) \Leftrightarrow (P(x), Q(x)) = (d(x))$$

Recordeu que la notació $(P(x), Q(x))$ vol dir *ideal generat* per $P(x)$ i $Q(x)$, és a dir totes les combinacions del tipus

$$a(x)P(x) + b(x)Q(x), \quad a(x), b(x) \in K[x].$$

I el mínim comú múltiple

$$m.c.m.(P(x), Q(x)) = m(x) \Leftrightarrow (P(x)) \cap (Q(x)) = (m(x)).$$

És fàcil veure (com a $\mathbb{Z}$) que $m(x)$ té grau mínim entre els múltiples comuns a $P(x)$ i $Q(x)$. I que $d(x)$ és el que té grau més gran entre els

divisors comuns de $P(x)$ i $Q(x)$. Això es dedueix de Bézout, que ara diu que existeixen polinomis $\alpha(x), \beta(x)$ tals que

$$\alpha(x)P(x) + \beta(x)Q(x) = d(x).$$

També es veu, amb el mateix argument que a $\mathbb{Z}$, que si $a(x)|b(x)c(x)$ i $m.c.d.(a(x), b(x)) = 1$, llavors $a(x)|c(x)$. Això permet demostrar, com a $\mathbb{Z}$, que (llevat d'escalars)

$$m.c.d.(P(x), Q(x)) \cdot m.c.m.(P(x), Q(x)) = P(x) \cdot Q(x).$$

Per trobar el màxim comú divisor utilitzarem l'algorisme d'Euclides exactament com a $\mathbb{Z}$, ja que aquest algorisme es basa en el fet de que si $D = dq+r$ llavors $m.c.d.(D, d) = m.c.d.(d, r)$ igualtat certa siguin D, d, q, r nombres enters o polinomis.

Exemple 13.1. *Racionalitzar*

$$\frac{1}{(\sqrt[3]{7})^2 + 2\sqrt[3]{7}}.$$

Solució. Posem $a = \sqrt[3]{7}$, de manera que l'objectiu és posar en forma de polinomi en a l'expressió

$$\frac{1}{a^2 + 2a}.$$

Observem que $\sqrt[3]{7}$ és arrel del polinomi $x^3 - 7$.

Per a això trobem el $m.c.d.(x^2+2x, x^3-7)$ i els seus coeficients de Bézout.

	$x-2$	$\frac{1}{4}x + \frac{15}{16}$	
x^3-7	x^2+2x	$4x-7$	$\frac{105}{16}$
1	0	1	$-\frac{1}{4}x - \frac{15}{16}$
0	1	$-x+2$	$\frac{1}{4}x^2 + \frac{7}{16}x - \frac{7}{8}$

Per tant,

$$(x^3-7)\cdot(-\frac{1}{4}x - \frac{15}{16}) + (x^2+2x)\cdot(\frac{1}{4}x^2 + \frac{7}{16}x - \frac{7}{8}) = \frac{105}{16}$$

Posant ara $x = a = \sqrt[3]{7}$ tenim

$$(a^2+2a)\cdot(\frac{1}{4}a^2 + \frac{7}{16}a - \frac{7}{8}) = \frac{105}{16},$$

que simplificant dóna

$$(a^2+2a)\cdot(4a^2+7a-14)=105,$$

i per tant,

$$\frac{1}{a^2+2a}=\frac{4a^2+7a-14}{105}.$$

Resumint,

$$\frac{1}{(\sqrt[3]{7})^2+2\sqrt[3]{7}}=\frac{1}{105}(4(\sqrt[3]{7})^2+7\sqrt[3]{7}-14).$$

13.4 Polinomis irreductibles sobre K

Definició 13.7. *Un polinomi $P(x)\in K[x]$, de grau més gran o igual a 1, s'anomena* irreductible sobre K*, o* irreductible a $K[x]$*, si no es pot escriure com a producte de dos polinomis de $K[x]$ de grau més petit que el grau de $P(x)$.*

Equivalentment, els seus únics divisors de $P(x)$ són de la forma λ, o $\lambda P(x)$, amb $\lambda\in K$.

Observeu que tots el polinomis de grau 1 són irreductibles.

En general és difícil saber si un polinomi és irreductible o no.

Teorema 13.8. *Tot polinomi $P(x)\in K[x]$ és producte de polinomis irreductibles, i aquesta descomposició és única llevat de l'ordre i d'escalars.*

Demostració. Com a $\mathbb{Z}$. □

Per exemple, a $\mathbb{Q}[x]$,

$$x^2-1=(x+1)(x-1)=(8x+8)(\frac{x}{8}-\frac{1}{8}).$$

De vegades es pot veure que un polinomi és reductible estudiant els seus zeros.

Definició 13.9. *Diem que un element $a\in K$ és un* zero *del polinomi $P(x)$ si $P(a)=0$.*

També es diu que a és una arrel de $P(x)$.

Teorema 13.10 (Ruffini)**.** *Un polinomi $P(x)$ és divisible per $(x-a)$ si i només si $P(a)=0$.*

Demostració. Només hem de dividir $P(x)$ entre $x - a$ i observar que el residu és de grau zero. □

En particular, doncs, si un polinomi de grau més gran o igual a 2, té un zero a K, és reductible sobre K.[1]

Però pot ser que $P(x)$ no tingui cap zero i sigui també reductible, per exemple, a $\mathbb{Q}[x]$, el polinomi de grau 4, $(x^2 + 1)(x^2 + 2)$.

Observem, com un corol·lari al teorema de Ruffini, que tot polinomi de grau n de $K[x]$ té com a molt n zeros a K (contats amb multiplicitat).

Diem que a és un zero de $P(x)$ amb *multiplicitat* k si $P(x) = (x-a)^k Q(x)$ i $Q(a) \neq 0$.

També es dedueix que si dos polinomis de grau $\leq n$ coincideixen sobre $n + 1$ elements del cos, llavors són iguals. En efecte, la diferència d'aquests polinomis seria un polinomi de grau $\leq n$ amb $n + 1$ zeros.

Si el cos és petit, podem tenir polinomis diferents que coincidixen sobre tots els elements del cos. Per exemple, $x - 2$ i $x^3 - 2$ a $\mathbb{Z}/(3)[x]$.

13.5 Irreductibles sobre $\mathbb{C}$

Teorema 13.11 (Teorema Fonamental de l'Àlgebra)**.** *Tot polinomi de* $\mathbb{C}[x]$ *té almenys un zero a* $\mathbb{C}$*.*

Com a corol·lari veiem que tot polinomi de grau n de $\mathbb{C}[x]$ té exactament n zeros a $\mathbb{C}$ (contats amb multiplicitat). I també,

Corol·lari 13.12. *Els polinomis irreductibles de* $\mathbb{C}[x]$ *són els de grau* 1*.*

13.6 Irreductibles sobre $\mathbb{R}$

Si $P(x) \in \mathbb{R}[x]$ és molt fàcil veure que si admet una arrel complexa admet la conjugada. Pensem $P(x) \in \mathbb{C}[x]$ i el descomponem en factors irreductibles. A continuació aparellem les arrels complexes (amb part imaginària diferent de zero) amb les seves conjugades. Obtenim

$$(x - (a + bi))(x - (a - bi)) = (x - a)^2 + b^2$$

i aquest polinomi de la dreta té coeficients reals.

Corol·lari 13.13. *Els polinomis irreductibles de* $\mathbb{R}[x]$ *són els de grau* 1 *o* 2*.*

Exercici 13.14. *Descomponeu, sobre* $\mathbb{R}$ *i sobre* $\mathbb{C}$*, el polinomi* $P(x) = x^3+1$*. Estudieu les funcions simètriques elementals de les arrels.*

Exercici 13.15. *Descomponeu, sobre* $\mathbb{R}$ *i sobre* $\mathbb{C}$*, el polinomi* $P(x) = x^4+1$*. Estudieu les funcions simètriques elementals de les arrels.*

[1] Agraeixo a Arnau Mas la correcció d'una primera versió d'aquesta secció dels apunts.

13.7 Màxim comú divisor en cossos diferents

Siguin $a(x), b(x) \in K[x]$ i sigui L un cos que conté el cos K. Penseu, si voleu, $K = \mathbb{Q}$ i $L = \mathbb{C}$.

Llavors *el màxim comú divisor de a i b, pensats com polinomis a $K[x]$, és el mateix* (potser multiplicat per elements de L) *que el màxim comú divisor de a i b, pensats com polinomis a $L[x]$.*

En efecte,[2] posem $m.c.d._K(a,b) = d_K$ i $m.c.d._L(a,b) = d_L$. Això vol dir

$$(a,b)_K = (d_K), \qquad (a,b)_L = (d_L)$$

on $(a,b)_K$ és l'ideal generat per a i b a $K[x]$ i $(a,b)_L$ és l'ideal generat per a i b a $L[x]$.

Clarament

$$(a,b)_K \subset (a,b)_L$$

de manera que $d_K \in (d_L)$ i per tant $grau\, d_K \geq grau\, d_L$. Ara bé,

$$d_L = pa + qb, \quad p, q \in L[x]$$

però com $a = a'd_K, b = b'd_K$ amb $a', b' \in K[x]$ tenim

$$d_L = (pa' + qb')d_K$$

i per tant $grau\, d_K \leq grau\, d_L$. Tenen doncs el mateix grau. Per tant, $d_L = \mu d_K$ amb $\mu \in L$.

13.8 Arrels múltiples

Teorema 13.16. *Sigui $p \in K[x]$. Llavors p té un factor irreductible múltiple si i només si $grau\, m.c.d.(p, p') \geq 1$.*

Demostració. Suposem primerament $p = q^r b$, amb $q \in K[x]$ irreductible, $b \in K[x]$, i $r \geq 2$.[3] Derivant,

$$p' = rq^{r-1}q'b + q^r b'.$$

Per tant, q^{r-1} és divisor comú de p i p', i té grau més gran o igual a 1.

Recíprocament, sigui $a \in K[x]$ un factor irreductible del màxim comú divisor de p i p', de grau més gran o igual a 1.

Llavors a la descomposició en factors primers de p tenim $p = a^r b$ amb $b \in K[x]$, i $m.c.d.(a,b) = 1$, per a un cert r que volem veure que $r \geq 2$. Com abans,

$$p' = ra^{r-1}a'b + a^r b'.$$

[2] Es dedueix directament del fet de que l'algorisme d'Euclides no surt de $K[x]$, però he volgut escriure-ho d'una altra manera.

[3] Si $q \nmid b$ (no divideix) es diu que q té multiplicitat r.

Així, a divideix $a^{r-1}a'b$, i com és coprimer amb b ha de dividir $a^{r-1}a'$. Si $r = 1$, tindríem que a dividiria a' cosa impossible ja que el grau de a' és menor que el grau de a. Això implica, per ser $grau\, a \geq 1$, $r \geq 2$ com volíem. □

Corol·lari 13.17. *Siugi $p \in \mathbb{Q}[x]$ irreductible. Llavors p no té arrels múltiples a $\mathbb{C}[x]$.*

Demostració. Pel teorema anterior $m.c.d.(p, p')$ és un polinomi de grau zero, és a dir, un element de $\mathbb{Q}$. I, per la secció anterior, aquest element de $\mathbb{Q}$ és també el $m.c.d.(p, p')$ considerats com polinomis a[4] $\mathbb{C}[x]$.

Sigui

$$p = (x - \alpha_1)^{r_1} \dots (x - \alpha_k)^{r_k}, \quad \alpha_i \in \mathbb{C}.$$

Si per algún i tinguéssim $r_i \geq 2$ llavors el polinomi $(x - \alpha_i)$ apareixeria com factor comú en tots els sumands que apareixen al derivar p, i seria doncs un divisor comú de p i p', cosa que no pot ser. Per tant, per tot i, $r_i = 1$. □

[4]El mateix argument val sobre $\mathbb{R}[x]$, la única diferència és que a $\mathbb{C}[x]$ el irreductibles són de grau 1.

Tema 14

$\pi \notin \mathbb{Q}$

Comencem amb un criteri d'irracionalitat que es deriva del desenvolupament en fracció contínua d'un nombre donat.

Teorema 14.1. *Suposem que la successió il·limitada*

$$x = \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \dots}}}$$

amb $a_i, b_i \in \mathbb{Z}$, $m.c.d.(a_i, b_i) = 1$, $|a_i| < |b_i|$ *a partir d'un valor de* i, *és convergent. Llavors* $x \notin \mathbb{Q}$.

Demostració. És fàcil veure que ens podem limitar al cas en que $|a_i| < |b_i|$ per a tot i. Com

$$-1 < \frac{a_{i+1}}{b_{i+1}} < 1, \tag{14.1}$$

sumant b_i tenim

$$b_i - 1 < b_i + \frac{a_{i+1}}{b_{i+1}} < b_i + 1.$$

Com que a_i i b_i estan separats almenys una unitat l'anterior desigualtat implica

$$|a_i| < |b_i + \frac{a_{i+1}}{b_{i+1}}|. \tag{14.2}$$

De (14.1) i (14.2) deduïm que la fracció

$$\frac{a_i}{b_i + \frac{a_{i+1}}{b_{i+1}}}$$

té el mateix signe que $\frac{a_i}{b_i}$ i és, en valor absolut, més petita que 1.

Anàlogament,

$$\cfrac{a_{i-1}}{b_{i-1}+\cfrac{a_i}{b_i+\cfrac{a_{i+1}}{b_{i+1}}}}$$

té el mateix signe que $\frac{a_{i-1}}{b_{i-1}}$ i és, en valor absolut, més petita que 1.

Per recurrència, x té el mateix signe que $\frac{a_1}{b_1}$ i $|x|<1$.

Suposem x racional, és a dir

$$x=\frac{a_1}{b_1+p_1}=\frac{p}{q},$$

on

$$p_1=\cfrac{a_2}{b_2+\cfrac{a_3}{b_3+\dots}}$$

Llavors

$$p_1=\frac{qa_1-pb_1}{p}=\frac{r}{p},$$

amb $r=qa_1-pb_1$.

Com p_1 té la mateixa estructura que x (com fracció contínua) sabem que $|p_1|<1$, i.e. $|r|<|p|$.

Resumint, si $x=p/q$ podem construir un racional $p_1=r/p$ amb numerador r estrictament més petit que p en valor absolut.

Posant

$$\frac{r}{p}=\frac{a_2}{b_2+p_2}$$

amb

$$p_2=\cfrac{a_3}{b_3+\cfrac{a_4}{b_4+\dots}}$$

tindríem

$$p_2=\frac{pa_2-rb_2}{r}=\frac{r_2}{r},$$

amb $r_2=pa_2-rb_2$.

Com p_2 té la mateixa estructura que x (com fracció contínua) sabem que $|p_2|<1$, i.e. $|r_2|<|r|$.

Procedint recursivament així tenim un mètode per anar construint racionals amb numerador amb mòdul cada cop estrictament més petit. El procés és infinit, però en canvi només tenim un nombre finit de passos perquè aquest valor absolut arribi a zero. Contradicció. Per tant $x\notin\mathbb{Q}$.

Teorema 14.2. $\pi\notin\mathbb{Q}$.

Demostració. Donem la prova de Lambert de 1761[1]. Fem el desenvolupament de la tangent com a fracció contínua.

$$\tan x = x + \frac{x^3}{3} + \frac{2}{15}x^5 + \cdots = \cfrac{x}{\cfrac{1}{1 + \cfrac{x^2}{3} + \cfrac{2}{15}x^4 + \ldots}}$$

En fer la divisió de 1 entre $1+\dfrac{x^2}{3}+\dfrac{2}{15}x^4+\ldots$ obtenim quocient 1 i residu $-\frac{x^2}{3} - \frac{2}{15}x^4 + \ldots$. Per tant, recordant que $D/d = q + r/d$,

$$\tan x = \cfrac{x}{1 - \cfrac{\cfrac{x^2}{3} + \cfrac{2}{15}x^4 + \ldots}{1 + \cfrac{x^2}{3} + \cfrac{2}{15}x^4 + \ldots}} = \cfrac{x}{1 - \cfrac{x^2}{\cfrac{1 + \cfrac{x^2}{3} + \cfrac{2}{15}x^4 + \ldots}{\cfrac{1}{3} + \cfrac{2}{15}x^2 + \ldots}}}$$

En fer la divisió de $1 + \dfrac{x^2}{3} + \dfrac{2}{15}x^4 + \ldots$ entre $\dfrac{1}{3} + \dfrac{2}{15}x^2 + \ldots$ obtenim quocient 3 i residu $-\frac{1}{15}x^2+\frac{2}{15}x^4+\ldots$ Per tant, recordant que $D/d = q+r/d$, i traient com abans x^2 factor comú tenim

$$\tan x = \cfrac{x}{1 - \cfrac{x^2}{3 - \cfrac{x^2}{\cfrac{\cfrac{1}{3} + \cfrac{2}{15}x^2 + \ldots}{\cfrac{1}{15} - \cfrac{2}{15}x^2 + \ldots}}}}$$

Repetint el procés obtenim finalment el desenvolupament en fracció contínua de $\tan x$.

$$\tan x = \cfrac{x}{1 - \cfrac{x^2}{3 - \cfrac{x^2}{5 - \cfrac{x^2}{7 - \cfrac{x^2}{9 - \ldots}}}}}$$

Si $x = p/q$ aquest desenvolupament està en les hipòtesis del teorema (14.1) ja que els termes de la successió $\frac{p^2}{3q}, \frac{p^2}{5q}, \frac{p^2}{7q}, \ldots$ són menors que 1 a partir d'un lloc, i representa doncs un nombre irracional.

Com $\tan \frac{\pi}{4} = 1$, que és racional, $\frac{\pi}{4}$ no pot ser racional i hem acabat.

[1] *Mémoires sur quelques propriétés remarquables des quantités transcendantes, circulaires et logarithmiques.* Mémoires de l'Académie royale des sciences de Berlin, année 1761/1768, 265-322.

Tema 15

El sisè nombre de Fermat

El gran Fermat la va ben cagar quan va dir que els nombres de la forma

$$2^{2^n}+1$$

són primers. L'afirmació és certa per a $n=1,2,3,4$, però és falsa a partir d'aquí. No es coneix una demostració general d'aquest fet.

Euler va fer la serie de teoremes següents que porten de manera natural al teorema 15.5 on es veu que si el sisè nombre de Fermat $2^{2^5}+1$ admet un divisor, aquest ha de ser de la forma $64k+1$. Va provar amb $k=10$ i ho va clavar, ja que efectivament, el sisè nombre de Fermat és divisible per 641.

Teorema 15.1. *Sigui a un nombre parell i sigui p un nombre primer divisor de $a+1$. Llavors $p \equiv 1_{(2)}$.*

Demostració. Un divisor del nombre imparell $a+1$ ha de ser imparell. De fet, l'únic primer parell és 2.

Teorema 15.2. *Sigui a un nombre parell i sigui p un nombre primer divisor de a^2+1. Llavors $p \equiv 1_{(4)}$.*

Demostració. Només cal veure que $p \not\equiv 3_{(4)}$ ja que tot nombre primer compleix que $p \equiv 1_{(4)}$ o $p \equiv 3_{(4)}$. Suposem $p=4k+3$ per a algun $k \in \mathbb{N}$. Com que $a^{p-1} \equiv 1_{(p)}$, tenim

$$a^{4k+2} \equiv 1_{(p)}.$$

Però Euler s'adona de que

$$a^{4k+2}+1 = (a^2+1)\cdot(a^{4k}-a^{4k-2}+a^{4k-4}+\cdots+a^4-a^2+1).$$

Prenem classes a $\mathbb{Z}/(p)$, tot tenint en compte que com a^2+1 és múltiple de p, la seva classe a $\mathbb{Z}/(p)$ és zero. Tenim

$$a^{4k+2} \equiv -1_{(p)}.$$

En particular tindríem $1 \equiv -1_{(p)}$, que com que $p \neq 2$, no es pot donar.

Teorema 15.3. *Sigui a un nombre parell i sigui p un nombre primer divisor de a^4+1. Llavors $p \equiv 1_{(8)}$.*

Demostració. Com p és imparell $p \not\equiv 0_{(8)}$, $p \not\equiv 2_{(8)}$, $p \not\equiv 4_{(8)}$, $p \not\equiv 6_{(8)}$. Hem de descartar els cassos $p \equiv 3_{(8)}$, $p \equiv 5_{(8)}$ i $p \equiv 7_{(8)}$.

Casos $p \equiv 3_{(8)}$ i $p \equiv 7_{(8)}$. Apliquem el teorema 15.2 al nombre primer p i al nombre parell a^2. Si p divideix $(a^2)^2+1 = a^4+1$ (justament la hipòtesi que tenim) llavors $p \equiv 1_{(4)}$. Però això implica immediatament que $p \not\equiv 3_{(8)}$ i $p \not\equiv 7_{(8)}$.

Cas $p \equiv 5_{(8)}$. Suposem $p = 8k+5$. Pel petit Teorema de Fermat

$$a^{8k+4} - 1 = \overset{\bullet}{p}. \tag{15.1}$$

Per altra banda

$$a^{8k+4} + 1 = (a^4+1) \cdot (a^{8k} - a^{8k-4} + a^{8k-8} + \cdots + a^8 - a^4 + 1),$$

i, en particular

$$a^{8k+4} + 1 = \overset{\bullet}{p}. \tag{15.2}$$

Restant (15.1) i (15.2) obtenim que 2 és múltiple de p, cosa que no pot ser.

Teorema 15.4. *Sigui a un nombre parell i sigui p un nombre primer divisor de a^8+1. Llavors $p \equiv 1_{(16)}$.*

Demostració. Com p és imparell, només hem d'estudiar els casos $p \equiv 1_{(16)}$, $p \equiv 3_{(16)}$, $p \equiv 5_{(16)}$, $p \equiv 7_{(16)}$, $p \equiv 9_{(16)}$, $p \equiv 11_{(16)}$, $p \equiv 13_{(16)}$, $p \equiv 15_{(16)}$.

Pels teoremes anteriors, i per ser

$$a^8 + 1 = (a^2)^4 + 1 = (a^4)^2 + 1,$$

veiem que $p \equiv 1_{(4)}$ i $p \equiv 1_{(8)}$. La primera igualtat elimina els cassos $p \equiv 3_{(16)}$, $p \equiv 7_{(16)}$, $p \equiv 11_{(16)}$, $p \equiv 15_{(16)}$; i la segona elimina els cassos $p \equiv 5_{(16)}$ i $p \equiv 13_{(16)}$.

Només resta eliminar el cas $p \equiv 9_{(16)}$ per tenir demostrat el teorema. Suposem $p = 16k+9$. Pel petit Teorema de Fermat

$$a^{16k+8} - 1 = \overset{\bullet}{p}. \tag{15.3}$$

Per altra banda

$$a^{16k+8} + 1 = (a^8+1) \cdot (a^{16k} - a^{16k-8} + a^{16k-16} + \cdots + a^{16} - a^8 + 1),$$

i, en particular

$$a^{16k+8} + 1 = \overset{\bullet}{p}. \tag{15.4}$$

Restant (15.3) i (15.4) obtenim que 2 és múltiple de p, cosa que no pot ser.

Teorema 15.5. *Sigui a un nombre parell i sigui p un nombre primer divisor de $a^{16}+1$. Llavors $p \equiv 1_{(32)}$.*

Demostració. As before.

Teorema 15.6. *Sigui a un nombre parell i sigui p un nombre primer divisor de $a^{32}+1$. Llavors $p \equiv 1_{(64)}$.*

Demostració. As before.

Tema 16

Sumes esteses als divisors d'un nombre

16.1 Funcions multiplicatives

Seguirem Vinogradov, [13].

Definició 16.1. *Direm que una funció $\theta : \mathbb{N} \longrightarrow \mathbb{N}$ és una funció multiplicativa si*

$$\theta(a \cdot b) = \theta(a) \cdot \theta(b), \quad \textit{quan m.c.d.(a,b)=1.}$$

En particular $\theta(1) = 1$.

Teorema 16.2. *Sigui θ una funció multiplicativa. Sigui*

$$a = p_1^{\alpha_1} \cdot p_r^{\alpha_r}$$

la descomposició en factors primers de $a \in \mathbb{N}$. Llavors

$$\sum_{d|a} \theta(d) = \prod_{i=1}^{r} [1 + \theta(p_i) + \theta(p_i^2) + \cdots + \theta(p_i^{\alpha_i})].$$

Demostració. Fem només un exemple perquè a partir d'ell es veu clarament el raonament que faríem en el cas general.

Prenem $a = 180 = 2^2 \cdot 3^2 \cdot 5$. Els 18 divisors de a són

$$1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180.$$

De manera que el sumatori és

$$\sum_{d|a} \theta(d) = \theta(1) + \theta(2) + \cdots + \theta(60) + \theta(90) + \theta(180)$$

I el producte

$$\begin{aligned}\prod_{i=1}^{r}[\dots] &= [1+\theta(2)+\theta(2^2)]\cdot[1+\theta(3)+\theta(3^2)]\cdot[1+\theta(5)]\\ &= [\theta(1)+\theta(2)+\theta(2^2)]\cdot[\theta(1)+\theta(3)+\theta(3^2)]\cdot[\theta(1)+\theta(5)]\\ &= [\theta(2^0)+\theta(2^1)+\theta(2^2)]\cdot[\theta(3^0)+\theta(3^1)+\theta(3^2)]\cdot[\theta(5^0)+\theta(5^1)]\end{aligned}$$

En efectuar els productes indicats obtindrem una suma de 18 sumands del tipus

$$\theta(2^i)\theta(3^j)\theta(5^k), \qquad 0\le i,j\le 2; \quad 0\le k\le 1.$$

Per ser θ multiplicativa tenim

$$\theta(2^i)\theta(3^j)\theta(5^k)=\theta(2^i3^j5^k), \qquad 0\le i,j\le 2; \quad 0\le k\le 1.$$

Però els nombres de la forma $2^i3^j5^k$, amb $0\le i,j\le 2;\ 0\le k\le 1$, són justament tots els divisors de a. Per tant

$$\prod_{i=1}^{r}[\dots]=\sum_{d|a}\theta(d),$$

com volíem demostrar.

Teorema 16.3. *la funció ϕ d'Euler és multiplicativa.*

Demostració. Conseqüència directa del resultat que diu que

$$\phi(a)=a(1-\frac{1}{p_1})\cdot\dots\cdot(1-\frac{1}{p_r})$$

on p_i són els primers divisors de a.

Teorema 16.4. *La suma de la funció ϕ d'Euler aplicada als divisors d'un nombre reprodueix el propi nombre. És a dir,*

$$\sum_{d|a}\phi(d)=a.$$

Demostració. Sigui $a=p_1^{\alpha_1}\dots p_r^{\alpha_r}$ la descomposició en factors primers de a. Per ser ϕ multiplicativa tenim

$$\begin{aligned}\sum_{d|a}\phi(d) &= \prod_{i=1}^{r}[1+\phi(p_i)+\phi(p_i^2)+\dots+\phi(p_i^{\alpha_i})]\\ &= \prod_{i=1}^{r}[1+(p_i-1)+(p_i^2-p_i)+\dots+(p_i^{\alpha_i}-p_i^{\alpha_i-1})]\\ &= \prod_{i=1}^{r}p_i^{\alpha_i}=a. \qquad \square\end{aligned}$$

Demostració alternativa[1]. Considerem el conjunt

$$A = \{(x,d); 1 \leq x \leq d, m.c.d.(x,d) = 1, d|a\}$$

Observem que si fixem d, hi ha $\phi(d)$ parelles de la forma $(x,d) \in A$. Per tant

$$|A| = \sum_{d|n} \phi(d).$$

Ara contarem els elements de A d'una altre manera. Concretament establirem una bijecció entre A i $\{1,2,\ldots,a\}$ i això ja demostrarà la igualtat que volem.

Aquesta bijecció és la següent.

$$\begin{array}{rccc} F: & A & \longrightarrow & \{1,2,\ldots,a\} \\ & (x,d) & \mapsto & \dfrac{x}{d}\, a \end{array}$$

F és injectiva. Si $F(x,d) = F(x',d')$, llavors

$$\frac{x}{d}\, a = \frac{x'}{d'}\, a$$

i per tant

$$xd' = x'd.$$

Com x és coprimer amb d, $x|x'$ (teorema d'Euclides). Anàlogament $x'|x$ i per tant $x = x'$. Però això implica $d = d'$ i F és injectiva.

F és exhaustiva. Sigui $m \in \{1,2,\ldots,a\}$. Hem de veure que té antiimatge. Sigui $\delta = m.c.d.(m,a)$ i posem $m = m'\delta$, $a = a'\delta$ amb $m.c.d.(m',a') = 1$. Llavors $(m',a') \in A$ i

$$F(m',a') = \frac{m'}{a'}\, a = m'\delta = m. \qquad \square$$

16.2 La funció de Moebius

La funció de Moebius és una funció $\mu : \mathbb{N} \longrightarrow \{-1,0,1\}$ donada per

$$\mu(p_1^{\alpha_1} \ldots p_k^{\alpha_k}) = \begin{cases} 0 & \text{si alguna } \alpha_i > 1, \\ (-1^k) & \text{en cas contrari.} \end{cases}$$

Se sobreentén que els p_i són primers i $\alpha_i \geq 1$.

Aquesta funció és multiplicativa.

[1] Vegeu [1], p. 140.

Teorema 16.5. *Sigui θ una funció multiplicativa i sigui*

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

la descomposició en factors primers de n. Llavors

$$\sum_{d|n} \mu(d)\theta(d) = \prod_{i=1}^{k}(1 - \theta(p_i)).$$

Demostració. Apliquem el teorema 16.2 a la funció θ_1 donada per

$$\theta_1(a) = \theta(a)\mu(a), \forall a \in \mathbb{N}.$$

Tenim

$$\sum_{d|a} \theta_1(d) = \prod_{i=1}^{k}[1 + \theta(p_i)\mu(p_i) + \theta(p_i^2)\mu(p_i^2) + \dots + \theta(p_i^{\alpha_i})\mu(p_i^{\alpha_i})].$$

Però $\mu(p_i^s) = 0$, si $s > 1$, i $\mu(p_i) = -1$, de manera que substituint tenim

$$\sum_{d|a} \theta(d)\mu(d) = \prod_{i=1}^{k}[1 - \theta(p_i)]. \quad \square$$

Corol·lari 16.6. *Sigui Φ la funció Φ d'Euler. Llavors*

$$\sum_{d|n} \mu(d)\frac{n}{d} = \phi(n)$$

Demostració. Apliquem el teorema anterior amb $\theta(a) = \frac{1}{a}$, que és multiplicativa. $\square$

Aquesta fórmula és una mena d'invers de la fórmula del teorema 16.4 i es coneix com *fórmula d'inversió*. De fet, és trivial ja que es pot escriure com

$$\sum_{d|n} \mu(d)\frac{1}{d} = \prod_{p_i \, factor \, primer \, de \, n} (1 - \frac{1}{p_i})$$

i si fem aquest producte del segon terme (recordeu els càlculs de la pàgina 29) veiem que surten tots els divisors de n formats per productes dels seus factors primers diferents (no apareixen p_i^2 ni potències superiors) i amb alternància de signe. Això és el primer terme i una motivació per a la definició de μ.

Corol·lari 16.7. *La suma de la funció de Moebius estesa als divisors d'un nombre és* 0 *o* 1. *Concretament*

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

Demostració. Apliquem el teorema anterior amb $\theta(a) = 1$, que és multiplicativa. □

Proposició 16.8. *Siguin* $a, n \in \mathbb{N}$.

$$\sum_{k=1}^{n} e^{2\pi i \frac{ak}{n}} = \begin{cases} n, & \textit{si } a \textit{ és múltiple de } n, \\ 0, & \textit{en cas contrari.} \end{cases}$$

Demostració. És la suma dels termes d'una progressió geomètrica de raó $r = e^{2\pi i \frac{a}{n}}$. Per tant, si $r \neq 1$,

$$\sum_{k=1}^{n} e^{2\pi i \frac{ak}{n}} = \frac{e^{2\pi i a} r - e^{2\pi i \frac{a}{n}}}{r - 1} = 0.$$

Clarament si a és múltiple de n, $r = 1$, i la suma és n. □

Proposició 16.9. *La funció de Moebius d'un nombre* n *és la suma de les arrels* n*-èssimes primitives de la unitat. És a dir,*

$$\mu(n) = \sum_{m.c.d.(k,n)=1} e^{2\pi i \frac{k}{n}}, \qquad 1 \leq k < n.$$

Demostració. Denotem

$$\mathcal{A}(n) = \sum_{m.c.d.(k,n)=1} e^{2\pi i \frac{k}{n}}, \qquad 1 \leq k < n.$$

Demostrarem que $\mathcal{A}$ és multiplicativa, que val -1 quan n és primer i 0 si n és el quadrat d'un primer.

Així, si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ tindrem

$$\mathcal{A}(n) = \mathcal{A}(p_1^{\alpha_1}) \dots \mathcal{A}(p_k^{\alpha_k}) = \mu(n)$$

1) És multiplicativa. Siguin a i b coprimers.Volem veure que

$$\mathcal{A}(ab) = \mathcal{A}(a)\mathcal{A}(b),$$

és a dir,

$$\sum_{m.c.d.(\lambda,ab)=1} e^{2\pi i \frac{\lambda}{ab}} = \left(\sum_{m.c.d.(k,a)=1} e^{2\pi i \frac{k}{a}} \right) \left(\sum_{m.c.d.(j,b)=1} e^{2\pi i \frac{j}{b}} \right)$$

amb $1 \leq \lambda < ab$, $1 \leq k < a$ i $1 \leq j < b$. Però el segon terme és igual a

$$\sum_{\substack{m.c.d.(k,a)=1 \\ m.c.d.(j,b)=1}} e^{2\pi i \frac{kb+aj}{ab}},$$

i, per la Proposició 16.10, sabem que quan la classe[2] de k recorre tots els elements invertibles de $\mathbb{Z}/(a)$ (això és essencialment el que vol dir la condició $m.c.d.(k,a)=1$) i la classe de j recorre tots els elements invertibles de $\mathbb{Z}/(b)$ (això és essencialment el que vol dir la condició $m.c.d.(k,a)=1$), les classes de les expressions $kb+aj$ recorren tots els elements invertibles de $\mathbb{Z}/(ab)$. Cadascuna d'elles té un representant canònic entre 1 i ab. Per tant, aquesta darrera suma està estesa a tots els λ, $1\leq\lambda<ab$, tals que $m.c.d.(\lambda,ab)=1$, i coincideix doncs amb $\mathcal{A}(ab)$.

2) Suposem $n=p$, primer. En aquest cas la suma que apareix a la definició de $\mathcal{A}$ està estesa a $1,2,\ldots,p-1$. Sabem, per la proposició 16.8 amb $a=1$, que si aquesta suma està estesa de $1,2,\ldots,p$ és zero. Per tant,

$$\mathcal{A}(p)=\sum_{k=1}^{p-1}e^{2\pi i\frac{k}{n}}=-e^{2\pi i}=-1$$

3) Suposem $n=p^2$, p primer. En aquest cas la suma que apareix a la definició de $\mathcal{A}$ està estesa

$$\begin{gathered}1,2,\ldots,p-1,\\ p+1,p+2,\ldots,2p-1,\\ 2p+1,2p+2,\ldots,3p-1,\\ \vdots\\ (p-1)p+1,(p-1)p+2,\ldots,p^2-1.\end{gathered}$$

Sabem, per la proposició 16.8 amb $a=1$, que si aquesta suma està estesa de $1,2,\ldots,p^2$ és zero. Per tant,

$$\mathcal{A}(p^2)=\sum_{k\in\text{taula anterior}}e^{2\pi i\frac{k}{p^2}}=-\sum_{k=p,2p,\ldots,p^2}e^{2\pi i\frac{k}{p^2}}=-\sum_{j=1}^{p}e^{2\pi i\frac{j}{p}}=0.$$

La proposició següent és una petita variació del teorema xinès del residu.

Proposició 16.10. *Siguin $a,b\in\mathbb{N}$ coprimers. Els nombres $q\in\mathbb{N}$ coprimers amb el producte ab, amb $1\leq q<ab$, són exactament els residus de dividir per ab els nombres*

$$ay+bx,$$

amb x coprimer amb a, i y coprimer amb b.

[2] L'expressió

$$e^{2\pi i\frac{kb+aj}{ab}}$$

no varia si canviem k per qualsevol representant de la seva classe $[k]\in\mathbb{Z}/(a)$ ni si canviem j per qualsevol representant de la seva classe $[j]\in\mathbb{Z}/(b)$, ni si directament canviem $kb+aj$ per qualsevol representant de la seva classe $[kb+aj]\in\mathbb{Z}/(ab)$.

Demostració. Denotem $\mathbb{Z}^*/(m)$ el subgrup de $\mathbb{Z}/(m)$ format pels elements invertibles (classes de coprimers amb m). Considerem l'aplicació

$$F : \mathbb{Z}^*/(a) \times \mathbb{Z}^*/(b) \longrightarrow \mathbb{Z}^*/(ab)$$

donada per

$$F([x],[y]) = [ay + bx].$$

Per provar que aquesta aplicació està ben definida hem de provar que no depèn del representant i que la imatge està realment a $\mathbb{Z}^*/(ab)$.

1) No depèn del representant, ja que si $[x] = [x']$ i $[y] = [y']$, tenim $y' = y + \overset{\bullet}{b}$ i $x' = x + \overset{\bullet}{a}$, i per tant,

$$ay' + bx' = ay + bx + a\overset{\bullet}{b} + b\overset{\bullet}{a} = ax + by + \overset{\bullet}{\overline{ab}},$$

i per tant, $[ay + bx] = [ay' + bx']$.

2) Hem de veure que $[ay + bx] \in \mathbb{Z}/(ab)$ és invertible,. i.e. $[ay + bx] \in \mathbb{Z}^*/(ab)$.

Ara bé, això es equivalent a provar que

$$m.c.d.(ay + bx, ab) = 1.$$

Per a això observem que si hi hagués un primer p que dividís aquests dos nombres, tindríem en particular que $p|ab$, i per tant $p|a$ o $p|b$. L'argument és el mateix en els dos cassos de manera que suposem $p|a$. Llavors, com $p|(ay + bx)$ ha de ser $p|bx$. Però p no pot dividir b ja que $m.c.d.(a, b) = 1$, i tampoc pot dividir x ja que $m.c.d.(x, a) = 1$. Contradicció. Per tant, no hi ha cap primer p que divideixi a la vegada $ay + bx$ i ab, i.e. $m.c.d.(ay + bx, ab) = 1$.

Així, doncs, F està ben definida. A més és injectiva. En efecte, si $F([x],[y]) = F([x'],[y'])$, tindríem

$$ay + bx = ay' + bx' + \overset{\bullet}{\overline{ab}},$$

i per tant,

$$b(x - x') = a(y' - y) + \overset{\bullet}{\overline{ab}} = \overset{\bullet}{a}.$$

Però a i b són coprimers, de manera que $a|(x' - x)$ i $b|(y' - y)$. Per tant, $[x] = [x']$ a $\mathbb{Z}/(a)$ i $[y] = [y']$ a $\mathbb{Z}/(b)$.

Com els conjunts implicats són finits, F és bijectiva.

Ara la demostració de la proposició és fàcil. En efecte, donat $q \in \mathbb{N}$, amb $1 \leq q < ab$, i coprimer amb ab, considerem $[q] \in \mathbb{Z}^*/(ab)$. Llavors, existeixen classes úniques $[x] \in \mathbb{Z}^*/(a)$ i $[y] \in \mathbb{Z}^*/(b)$ tals que

$$F([x],[y]) = [ay + bx] = [q].$$

Per tant, $ay + bx = q + \overset{\bullet}{ab} = ab\lambda + q$, i com $1 \leq q < ab$, q és el reste de dividir $ay + bx$ entre ab, com volíem demostrar. □

Nota. Notem que aquest resultat demostra també que la funció Φ d'Euler és multiplicativa, ja que expressions del tipus $ax + by$, amb a, b fixats i $m.c.d.(x, b) = m.c.d.(y, a) = 1$, $1 \leq x < b, 1 \leq y < a$, n'hi ha $\Phi(a)\Phi(b)$.

Nota. Notem també que la diferència fonamental amb el teorema xinès és que F no és morfisme d'anells. Això pot ser un inconvenient en altres situacions, però aquí te l'avantatge de permetre generar els invertibles dec $\mathbb{Z}/(ab)$ d'una manera trivial a partir dels invertibles de $\mathbb{Z}/(a)$ i $\mathbb{Z}/(b)$.

Exemple 16.1. *Calculeu, usant el resultat anterior, els invertibles de* $\mathbb{Z}/(72)$.

Demostració. Descomponem $72 = 8 \cdot 9$ i trobem els invertibles de $\mathbb{Z}/(8)$ i $\mathbb{Z}/(9)$. Tenim

$$\mathbb{Z}^*/(8) = \{1, 3, 5, 7\},$$

$$\mathbb{Z}^*/(9) = \{1, 2, 4, 5, 7, 8\},$$

Estic identificant les classes amb els seus representants canònics. Les combinacions $ax + by = 8x + 9y$, amb $x \in \mathbb{Z}^*/(9)$ i $y \in \mathbb{Z}^*/(8)$ són les entrades de la taula següent.

	1	2	4	5	7	8
1	17	25	41	49	65	1
3	35	43	59	67	11	19
5	53	61	5	13	29	37
7	71	7	23	31	47	55

Exemple 16.2. *Calculeu, usant el teorema xinès del residu, els invertibles de* $\mathbb{Z}/(72)$.

Demostració. L'isomorfisme del teorema xinès

$$\begin{array}{ccc} \mathbb{Z}/(72) & \longrightarrow & \mathbb{Z}/(8) \times \mathbb{Z}/(9) \\ [x] & \mapsto & [x], [x] \end{array}$$

porta invertibles a invertibles. Els invertibles de la dreta són $(1,1), (1,2)$, $(1,4), (1,5), (1,7), (1,8), (3,1)$, *etc.* Mirem qui és, per exemple, la antimatge de $(5,5)$. Busquem $z \equiv 5 \bmod(8)$, i $z \equiv 5 \bmod(9)$. Resolem pel mètode dels residus xinesos, és a dir resolem les dues equacions

$$9z \equiv 5 \bmod(8)$$
$$8w \equiv 5 \bmod(9)$$

Obtenim $z = 5$, $w = 4$, de manera que la solució és $9 \cdot 5 + 8 \cdot 4 = 77 = 5$.

Observem que $F([5], [5]) = [13]$ en canvi en el teorema xinès $[5] \mapsto ([5], [5])$.

Exercici 16.11. *Observeu que hi ha una relació curiosa entre la funció μ de Moebius i la funció ζ de Riemann. Concretament*

$$\frac{1}{\zeta} = \prod_p (1 - \frac{1}{p^s}) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

Demostració. Es veu de seguida. □

Nota. Una altra aplicació interessant de la funció μ de Moebius és la següent.

Sigui N_n^p el nombre de polinomis mònics irreductibles de grau n a $\mathbb{Z}/(p)[x]$. Llavors

$$N_n^p = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) p^d.$$

Vegeu [1], p. 359.

Exercici 16.12 (Enunciat mal parit)**.** *Demostreu que*

$$\cos(40^\circ) + \cos(80^\circ) + \cos(160^\circ) = 0.$$

Solució. Com que $40^\circ = \frac{2\pi}{9}$ radians, ja es veu de seguida (je, je) que el que s'ha de considerar és la suma de les arrels primitives novenes de la unitat.

És a dir, hem de considerar

$$\sum_{k=1,2,4,5,7,8} e^{2\pi i \frac{k}{9}}.$$

Els qui coneixen la funció μ de Moebius saben que aquesta suma és igual a $\mu(9) = \mu(3^2) = 0$.

Nosaltres seguim el problema com si fóssim μ-Moebius ignorants.

Ens adonem que $e^{2\pi i \frac{1}{9}}$ és conjugat de $e^{2\pi i \frac{8}{9}}$, que $e^{2\pi i \frac{2}{9}}$ és conjugat de $e^{2\pi i \frac{7}{9}}$, i que $e^{2\pi i \frac{4}{9}}$ és conjugat de $e^{2\pi i \frac{5}{9}}$.

Per tant, la part real de la suma anterior és igual a

$$2(\cos 2\pi \frac{1}{9} + \cos 2\pi \frac{2}{9} + \cos 2\pi \frac{4}{9}).$$

Podem veure que aquesta suma és zero sense usar la funció μ de Moebius. Només ens hem d'adonar que podem substituir-la per

$$2(\cos 2\pi \frac{1}{9} + \cos 2\pi \frac{7}{9} + \cos 2\pi \frac{13}{9}).$$

En efecte, $e^{2\pi i \frac{7}{9}} = e^{2\pi i \frac{9-2}{9}} = e^{-2\pi i \frac{2}{9}}$ i $e^{2\pi i \frac{13}{9}} = e^{2\pi i \frac{9+4}{9}} = e^{2\pi i \frac{4}{9}}$.

Ara, aquesta suma de cosinus és la part real de

$$e^{2\pi i \frac{1}{9}} + e^{2\pi i \frac{7}{9}} + e^{2\pi i \frac{13}{9}}$$

i això és la suma d'una progressió geomètrica de raó $e^{2\pi i \frac{6}{9}}$, i aplicant la fórmula de la suma dels termes d'una progressió geomètrica veiem directament que aquesta suma (i per tant la seva part real) és zero.

Passant els radians a graus hem acabat.

Tema 17

Criteri d'Eisenstein

Utilitzarem que, pel fet de ser K un cos, l'anell de polinomis $K[x]$ és un domini d'integritat. Això es veu de seguida mirant el coeficient de major grau del producte de dos polinomis. Aquest coeficient és justament igual al producte dels coeficients de major grau d'aquests polinomis, que són, per definició, diferents de zero. Si el producte fos zero, per ser K cos, un dels dos hauria de ser zero, contradicció.[1]

Definició 17.1. *Direm que* $P(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ *és* primitiu *si* $m.c.d.(a_0, a_1, \ldots, a_n) = 1$.

Tot i que la teoria de polinomis la fem sobre un cos arbitrari i $\mathbb{Z}$ no és un cos, no hi ha problema en considerar *polinomis amb coeficients enters*, ja que $\mathbb{Z} \subseteq \mathbb{Q}$ i per tant $Z[x] \subseteq \mathbb{Q}[x]$, és a dir, tot polinomi amb coeficients enters és un polinomi amb coeficients racionals.

Lema 17.2 (Lema de Gauss)**.** *El producte de primitius és primitiu.*

Demostració. Siguin $P(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ i $Q(x) = b_0 + b_1x + \cdots + b_mx^m \in \mathbb{Z}[x]$ primitius. Suposem que $P(x)Q(x)$ no és primitiu. Això vol dir que hi ha un nombre primer $p \in \mathbb{Z}$ que divideix a tots els coeficients de $P(x)Q(x)$.

Prenem classes a $\mathbb{Z}/(p)[x]$. Això vol dir considerar els polinomis que tenen per coeficients les classes a $\mathbb{Z}/(p)$ dels coeficients dels polinomis donats a $\mathbb{Z}[x]$.

Així la classe de $P(x)$ és

$$\bar{P}(x) = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n \in \mathbb{Z}/(p)[x],$$

on $\bar{a}_i$ vol dir la classe del nombre enter a_i a $\mathbb{Z}/(p)$.

[1] Òbviament, si canviem K per un domini d'integritat aquest argument continua sent vàlid.

Llavors és clar que a

$$\overline{P(x)} \cdot \overline{Q(x)} = \overline{P(x)Q(x)}$$

i com $\overline{P(x)Q(x)} = 0$, ja que estem suposant que tots els seus coeficients són múltiples de p, i $\mathbb{Z}/(p)[x]$ és domini d'integritat, ha de ser $\overline{P(x)} = \overline{0}$ o $\overline{Q(x)} = \overline{0}$. En el primer cas, tots els coeficients de $P(x)$ han de ser múltiples de p, en contradicció amb que $P(x)$ és primitiu i en el segon cas, tots els coeficients de $Q(x)$ han de ser múltiples de p, en contradicció amb que $Q(x)$ és primitiu. □

Exemple. Multipliquem un parell de primitius. Agafem un parell de polinomis que tinguin un coeficient igual a 1, i així ens assegurem que m.c.d. dels coeficients és igual a 1.

Si els dos termes independents, o els dos termes de major grau, són iguals a 1, llavors també el terme independent del producte, o el terme de major, són iguals a 1, i el producte és primitiu. Posem un exemple on hi hagin uns però que no passi això, per exemple $P(x) = 1+2x+8x^2$ i $Q(x) = 8+x+2x^2$. Multiplicant obtenim

$$P(x)Q(x) = 8 + 17x + 20x^2 + 12x^3 + 16x^4$$

que és primitiu, ja que 17 no és parell com tots els altres coeficients. Justament aquest 17 prové de sumes i productes que involucren els coeficients iguals a 1 de $P(x)$ i $Q(x)$.

Observem que a la definició 13.7 no hem definit *polinomi irreductible*, sinó *polinomi irreductible sobre K*. Això posa un problema quan parlem de polinomis a coeficients enters, que ja hem comentat que els podem considerar com polinomis sobre $\mathbb{Q}$ (o sobre $\mathbb{C}$). Què vol dir que un polinomi a coeficients enters sigui *irreductible*?

Donarem la definició següent amb l'únic objectiu d'alleugerir la notació posteriorment.

Definició 17.3. *Un polinomi $P(x) \in \mathbb{Z}[x]$ de grau més gran o igual a 1, s'anomena* irreductible sobre $\mathbb{Z}$*, si no es pot escriure com a producte de dos polinomis de $\mathbb{Z}[x]$ de grau estrictament més petit que el grau de $P(x)$.*

Corol·lari 17.4 (Corol·lari al Lema de Gauss)**.** *Sigui $P(x) \in \mathbb{Z}[x]$ de grau més gran o igual a 1. Llavors $P(x)$ és irreductible a $\mathbb{Z}[x]$ si i només si és irreductible a $\mathbb{Q}[x]$.*

Demostració. Que si $P(x)$ és irreductible sobre $\mathbb{Q}[x]$ és irreductible sobre $\mathbb{Z}[x]$ és clar, ja que si fos producte de dos polinomis amb coeficients a $\mathbb{Z}$, com $\mathbb{Z} \subset \mathbb{Q}$, també seria producte de polinomis de $\mathbb{Q}[x]$.

Suposem doncs que $P(x)$ és irreductible sobre $\mathbb{Z}[x]$. Suposem, per reducció a l'absurd, que $P(x)$ és reductible sobre $\mathbb{Q}[x]$, és a dir,

$$P(x) = G(x)H(x), \qquad G(x), H(x) \in \mathbb{Q}[x]$$

amb $G(x)$ i $H(x)$ de grau estrictament més petit que el grau de $P(x)$. En particular, cap dels dos pot tenir grau zero.

Posem

$$\begin{aligned} P(x) &= \lambda P_1(x) \\ G(x) &= \mu G_1(x) \\ H(x) &= \nu H_1(x) \end{aligned}$$

amb $P_1(x), G_1(x), H_1(x)$ primitius, amb coeficients enters, i $\lambda \in \mathbb{Z}$, $\mu, \nu \in Q$, tots tres positius.

Observem que λ és el màxim comú divisor dels coeficients de $P(x)$. L'existència de μ i ν és també clara, ja que només hem de multiplicar $G(x)$ pel mínim comú múltiple m dels denominadors dels seus coeficients per tenir un polinomi $mG(x)$ amb coeficients enters. Clarament $mG(x) = \delta G_1(x)$ amb $G_1(x)$ primitiu i δ igual al màxim comú divisor dels coeficients de $mG(x)$. Així $G(x) = (\delta/m)G_1(x) = \mu G_1(x)$, amb $\mu \in \mathbb{Q}$, com volíem. Mateix argument per a $H(x)$.

Així, $P(x) = G(x)H(x)$ equival a $\lambda P_1(x) = \mu\nu G_1(x)H_1(x)$. Pel Lema de Gauss $G_1(x)H_1(x)$ és primitiu. Posem $\mu\nu = p/q$, de manera que $\lambda q P_1(x) = pG_1(x)H_1(x)$.

Prenent ara el màxim comú divisor dels coeficients als dos costats obtenim[2] $\lambda q = p$, per tant, $\lambda = \mu\nu$ i $P_1 = G_1(x)H_1(x)$.

Així,

$$P(x) = \lambda P_1(x) = \lambda G_1(x)H_1(x) = [\lambda G_1(x)]H_1(x)$$

i com $\lambda G_1(x) \in \mathbb{Z}[x]$ i $H_1(x) \in \mathbb{Z}[x]$, tindríem una descomposició de $P(x)$ com a producte de dos polinomis de amb coeficients enters de grau estrictament més petit que el grau de $P(x)$, i per tant $P(x)$ no seria irreductible a $Z[x]$, contradicció.

Corol·lari 17.5. *Sigui $P(x) \in \mathbb{Z}[x]$ primitiu, de grau més gran o igual a 1. Llavors $P(x)$ descompon com a producte de polinomis irreductibles primitius.*

Demostració. Pensem $P(x) \in \mathbb{Q}[x]$ i apliquem el teorema de factorització:

$$P(x) = q_1(x) \cdot q_2(x) \dots q_k(x)$$

amb $q_i(x) \in \mathbb{Q}[x]$, $i = 1, 2, \dots, k$. Ara repetim l'argument del corol·lari anterior. Existeixen $\lambda_i \in \mathbb{Q}$ tals que $q_i(x) = \lambda_i \bar{q}_i(x)$ amb $\bar{q}_i(x) \in \mathbb{Z}[x]$ primitius.

Deduïm, com en el corol·lari anterior, utilitzant que el producte de tots els $\bar{q}_i(x)$ és un polinomi primitiu, que $1 = \lambda_1 \cdot \lambda_2 \dots \lambda_k$ i per tant

$$P(x) = \bar{q}_1(x) \cdot \bar{q}_2(x) \dots \bar{q}_k(x)$$

com volíem. □

[2]Recordem $m.c.d.(ca, cb) = c \cdot m.c.d.(a, b)$.

Teorema 17.6 (Criteri d'Eisenstein)**.** *Sigui*

$$P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x], \qquad a_n \neq 0.$$

Sigui p un nombre primer tal que

1. $p|a_0, p|a_1, \ldots, p|a_{n-1}$.
2. $p \nmid a_n$.
3. $p^2 \nmid a_0$.

Llavors $P(x)$ és irreductible sobre $\mathbb{Q}$.

Demostració. Pel Corol·lari 17.4 només cal provar que és irreductible sobre $\mathbb{Z}$. Suposem

$$P(x) = (b_0 + b_1x + \cdots + b_ux^u)(c_0 + c_1x + \cdots + c_vx^v)$$

amb $b_i, c_j \in \mathbb{Z}$, $u + v = n$, $u, v \geq 1$.

Com que $a_0 = b_0c_0$ i $p|a_0$ ha de ser que p divideixi a b_0 o a c_0. Suposem, sense perdre generalitat, $p|b_0$. Si també fos cert que $p|c_0$, llavors $p^2|b_0c_0$, cosa que, per hipòtesis no és certa. Per tant tenim que $p|b_0$ i $p \nmid c_0$.

Com que $a_n = b_uc_v$ i $p \nmid a_n$, p no pot ser divisor ni de b_u ni de c_v, i.e. $p \nmid b_u$ i $p \nmid c_v$.

Observem, doncs, que $p|b_0$ i $p \nmid b_u$. Això ens permet parlar del més petit k tal que $p \nmid b_k$.

Com que

$$a_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0,$$

veiem que $p|b_kc_0$, ja que divideix a_k i a tots els sumands anteriors a b_kc_0. Però com $p \nmid b_k$, ha de ser $p|c_0$, contradicció. □

Exemple 1. Anem a veure que $P(x) = 1 + x + x^2 + x^3 + x^4$ és irreductible sobre $\mathbb{Q}$.[3]

Si intentem aplicar el criteri d'Eisenstein necessitem un primer p tal que $p|1$ i $p^2 \nmid 1$. Com que no hi ha cap primer amb aquestes condicions no el podem aplicar.

Però podem fer el truc habitual de posar $x = y + 1$. Llavors obtenim un polinomi

$$Q(y) = 1 + (y + 1) + (y + 1)^2 + (y + 1)^3 + (y + 1)^4.$$

Fent operacions obtenim

$$Q(y) = 5 + 10y + 10y^2 + 5y^3 + y^4.$$

[3]Tot polinomi ciclotòmic de grau $p - 1$, amb p primer, és irreductible sobre $\mathbb{Q}$.

Ara podem aplicar el criteri d'Eisenstein amb $p = 5$. En efecte, 5 divideix a tots els coeficients, excepte al de grau superior, i 5^2 no divideix al terme independent. Per tant $Q(y)$ és irreductible sobre $\mathbb{Q}$.

Això implica que el polinomi inicial $P(x)$ és irreductible sobre $\mathbb{Q}$, ja que si $P(x) = P_1(x)P_2(x)$, amb aquests $P_i(x)$ de grau ≥ 1, llavors tindríem $Q(y) = Q_1(y)Q_2(y)$, amb $Q_i(y) = P_i(y+1)$, i $Q(x)$ seria reductible.

Exemple 2. Anem a veure que $36 + 66x + 3x^3$ és irreductible sobre $\mathbb{Q}$. Els primers que podríem utilitzar per aplicar Eisenstein, han de ser divisors de 36 i 66 però do de 3. Això només ho compleix $p = 2$. Però llavors $p^2 = 4$ sí que divideix el terme independent, i no podem aplicar el criteri d'Eisenstein.

Fem-ho directament. Suposem que descompon. Tindríem

$$36 + 66x + 3x^3 = (a + bx)(c + dx + ex^2).$$

Igualant coeficients obtenim

$$\begin{aligned} 36 &= ac \\ 66 &= bc + ad \\ 0 &= ae + bd \\ 3 &= be \end{aligned}$$

Com $a, b, c, d, e \in \mathbb{Z}$ ha de ser $b = 3$ i $e = 1$, o bé $e = 3$ i $b = 1$. Si $b = 3$ i $e = 1$, el sistema anterior es redueix a

$$\begin{aligned} 36 &= ac \\ 66 &= 3c + ad \\ 0 &= a + 3d \end{aligned}$$

d'on deduïm $c = 22 + d^2$ i $12 = -dc$, i això no pot ser ja que $c \geq 22$ i $c|12$.

Si $b = 1$ i $e = 3$, el sistema anterior es redueix a

$$\begin{aligned} 36 &= ac \\ 66 &= c + ad \\ 0 &= 3a + d \end{aligned}$$

d'on deduïm $c = 66 + 3a^2$ i $36 = ac$, i això no pot ser ja que $c \geq 66$ i $c|36$.

Per tant el polinomi donat és irreductible sobre $\mathbb{Q}$.

Si no coneguéssim el Corol·lari 17.4 podríem intentar resoldre el sistema anterior pensant que $a, , b, c, d, e \in \mathbb{Q}$, però sabem que no cal provar-ho.

Nota. En les hipòtesis del criteri d'Eisenstein, i abans d'aplicar-lo, és útil saber si el polinomi donat té arrels racionals. És fàcil veure que si el nombre racional $\frac{r}{s}$ és arrel de $a_0 + a_1x + \cdots + a_nx^n$, llavors $s|a_n$ i $r|a_1$. Vegeu la llista de problemes del curs.

Tema 18

Polinomis simètrics

Teorema 18.1. *Tot polinomi simètric és un polinomi en els polinomis simètrics elementals.*

Demostració. Ens limitarem a explicar el mètode de Waring. Donat el polinomi simètric $P(x_1, \ldots, x_n)$ ens fixem en el terme $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ amb $i_1 \geq i_2 \geq \cdots \geq i_n$. Per exemple, si $n = 3$, i tenim un sumand del polinomi de la forma x^2y^3z, per ser simètric el polinomi, vol dir que també tenim els termes x^2z^3y, z^2y^3x, z^2x^3y, y^2x^3z i y^2z^3x. En aquest cas elegiríem el terme x^3y^2z ja que $3 \geq 2 \geq 1$.

Considerem el polinomi

$$f = a\, s_1^{i_1 - i_2} \cdot s_2^{i_2 - i_3} \cdot \cdots \cdot s_{n-1}^{i_{n-1} - i_n} \cdot s_n^{i_n}$$

on s_j són les funcions simètriques elementals

$$\begin{aligned} s_1 &= x_1 + \cdots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\ \ldots &= \ldots \\ s_n &= x_1x_2 \ldots x_n \end{aligned}$$

i a és el coeficient del terme $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ en el polinomi P.

A continuació escrivim

$$P_1 = P - f$$

de manera que el terme inicial desapareix (s'ha de raonar), i podem repetir el procés sobre P_1 que té grau lexicogràfic més petit.

Exemple 1. $P(x) = x_1^2 + x_2^2 + x_3^2$. En aquest cas $i_1 = 2$, $i_2 = i_3 = 0$.

Per tant

$$f = s_1^2.$$

Considerem

$$P_1 = P - f = -2x_1x_2 - 2x_1x_3 - 2x_2x_3 = -2s_2.$$

Com P_1 ja és simètric elemental aturem el procés i tenim

$$P = P_1 + f = -2s_2 + s_1^2$$

Exemple 2. $P(x) = x_1^3 + x_2^3 + x_3^3$. En aquest cas el terme més gran en ordre lexicogràfic és x_1^3. Per tant, $i_1 = 3$, $i_2 = i_3 = 0$. Així

$$f = s_1^3.$$

Considerem

$$P_1 = P - f = -3x_1^2x_2 - 3x_1^2x_3 - 3x_2^2x_1 - 3x_2^2x_3 - 3x_3^2x_1 - 3x_3^2x_2 - 6x_1x_2x_3.$$

Ara apliquem el mètode a P_1.

En aquest cas el terme més gran en ordre lexicogràfic és $-3x_1^2x_2$. Per tant, $i_1 = 2$, $i_2 = 1$ i $i_3 = 0$. Així

$$g = -3s_1s_2.$$

Considerem

$$P_2 = P_1 - g = 3s_3.$$

Com P_2 ja és simètric elemental aturem el procés i tenim

$$P = P_1 + f = P_2 + g + s_1^3 = 3s_3 - 3s_1s_2 + s_1^3.$$

Exemple 3. $P(x) = x_1^4x_2x_3 + x_2^4x_3x_1 + x_3^4x_1x_2$. En aquest cas el terme més gran en ordre lexicogràfic és $x_1^4x_2x_3$. Per tant, $i_1 = 4$, $i_2 = i_3 = 1$. Així

$$f = s_1^3s_3.$$

Considerem

$$P_1 = P - f = -3x_1^3x_2^2x_3 - 3x_1^2x_2^3x_3 - 3x_1x_2^2x_3^3 - 3x_1x_2^3x_3^2 - 3x_1^2x_2x_3^3 - 3x_1^3x_2x_3^2 - 6x_1^2x_2^2x_3^2.$$

Ara apliquem el mètode a P_1.

En aquest cas el terme més gran en ordre lexicogràfic és $-3x_1^3x_2^2x_3$. Per tant, $i_1 = 3$, $i_2 = 2$ i $i_3 = 1$. Així

$$g = -3s_1s_2s_3 = -3x_1^3x_2^2x_3 - 3x_1^3x_2x_3^2 - 3x_1^2x_2^3x_3 - 3x_1x_2^3x_3^2 - 3x_1^2x_2x_3^3 - 3x_1x_2^2x_3^3 - 9x_1^2x_2^2x_3^2.$$

Considerem

$$P_2 = P_1 - g = 3s_3^2.$$

Per tant,

$$P = P_1 + f = P_2 + g + f = 3s_3^2 + s_1^3s_3 - 3s_1s_2s_3.$$

Bibliografia

[1] R. Antoine, R. Camps i J. Moncasi. *Introducció a l'àlgebra abstracta*. Manuals UAB, 46, 2007.

[2] M. Castellet i I. Llerena. *Àlgebra Lineal i Geometria*, volum 1. Manuals UAB, 1990.

[3] W. Dunham. *Viaje a través de los genios*. Pirámide, 1993. Traducció de la versió anglesa de 1990, editada per John Wiley and Sons.

[4] A. García-Azcárate. *Legendre. La honestidad de un científico*. Nivola, 2002.

[5] R. Godement. *Algebra*. Tecnos, 1967.

[6] P. M. Gonzàlez-Urbaneja. Arquimedes, un savi entre la història i la llegenda. *Butlletí de la Societat Catalana de Matemàtiques*, 23(1):5–56, 2008.

[7] Douglas Hofstadter. *Gödel, Escher, Bach*. Basic Books, 1979.

[8] F. Klein. *Matemàtica Elemental desde un punto de vista superior*. Nivola, 2006. Traducció de l'original *Elementarmathematik vom höheren Standpunkt aus*, Berlin, 1924-1928, 3 vols.

[9] J. Pla. *Liu Hui,* Nueve capítulos *de la matemàtica china*. Nivola, 2009.

[10] A. Reventós. *Problemes de Fonaments de les Matemàtiques*. `http://mat.uab.cat/~agusti/problemesresolts.pdf`, 2011-14.

[11] A. Reventós. Gauss i el polígon de 17 costats. *Nou Biaix*, 35:6–38, 2014.

[12] C. Schumacher. *Chapter zero*. Addison Wesley, 2001.

[13] I. Vinogradov. *Fundamentos de la teoria de los números*. Mir, Moscú, 1970.