Parlem de zeros de polinomis, per exemple

Jaume Aguadé[1]

> Every sufficiently beautiful object is connected to all others.
>
> John Baez, *From the icosahedron to E_8*
>
> In the mathematics of the universe, beauty helps tell us whether things are false or true.
>
> Martin Amis, *The information*

Què podem dir sobre les solucions d'equacions com aquestes?

$$x^3 - 3x + 1 = 0,$$

$$x^5 - 1.34495506833944\,x^4 + 0.659756735077032\,x^3 - 0.143302837199138\,x^2 + 0.0129552063084713\,x - 0.000306554042370339 = 0,$$

$$x^{65537} - 1581982247548443768172410932259343634851424742665363968413873076343504940773148481149945232171222715993388474821666263727961914772770008788475091376828165719830208810861338878427161150818708276227629683922314980785381242081026191757207297505559192760474115515722435767111629129610036646607257503619757848611791607269920429231537400515524940052734470727434275765647212246860766443254344136503044238958515803718864349551971756876709062734099654136986735158605070269916789055271961829409895163099574029394486731603526826853483895807928682556852840038952601375144932228593905911530385972218226717421850004218528189285505 1 = 0.$$

Abans de contestar aquesta pregunta, fem algunes consideracions:[2]

[1]Catedràtic de Topologia jubilat a la Universitat Autònoma de Barcelona. Jaume.Aguade@uab.cat.

[2]Observem l'exponent de la tercera equació: 65537. Us diu res aquest nombre? $65537 = 2^{16} + 1$ és el cinquè primer de Fermat, el més gran que es coneix (els que es coneixen són 3, 5, 17, 257 i 65537 i es conjectura que no n'hi ha cap més). Els primers de Fermat representen el nombre de costats dels únics polígons regulars amb un nombre primer de costats que es poden dibuixar amb regle i compàs. Si entreu a qualsevol pàgina web amb protocol https hi trobareu aquest nombre 65537. Si algú de nosaltres sabés resoldre aquesta última equació als anells $\mathbb{Z}/(m)$, el caos mundial seria monumental.

- **Per què ens pot interessar trobar les solucions?** Per exemple, ens pot interessar per trobar els valors propis d'una matriu, un problema fonamental en moltes àrees de la ciència. Per exemple, en ecologia podem tenir diverses espècies convivint en un hàbitat, interactuant entre elles i l'evolució d'aquest sistema ens vindrà donada pels valors propis de la matriu d'interaccions, que són els zeros del seu polinomi característic.[3]

- **En quin àmbit treballem?** És clar que volem poder sumar, restar, multiplicar i dividir (excepte per zero, és clar!). Per tant, estarem treballant en un **cos**,[4] probablement en algun dels **cossos importants** a la ciència, la tecnologia o les matemàtiques.

  Quins són aquests cossos importants? N'hi ha uns quants i els estudiants hi han d'estar familiaritzats des de ben aviat. Hi ha dos tipus de cossos importants:

  – Els cossos que en podríem dir **reals**, no en el sentit tècnic de l'expressió sinó en el sentit de que són els cossos que tenen una existència més «concreta», més «sòlida», més «pràctica».

  – Un segon grup de cossos que també són molt importants i útils a la ciència i la tecnologia però són ben bé una **abstracció** matemàtica, en el sentit que no tenen una expressió «concreta» en el «món real».

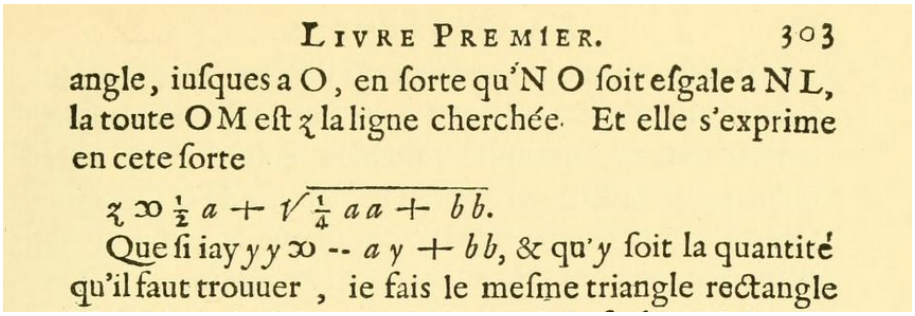
  Aquesta distinció ja existia quan jo era jove. Però des d'aquell moment fins ara ..... **els dos grups s'han intercanviat!!** I això, per inèrcia o pel que sigui, no ha arribat encara amb prou força a l'ensenyament.

  Els cossos importants que són *«abstraccions útils»* són els **reals** i els **complexos**. No cal dir que tothom hi ha d'estar familiaritzat, però també hem de ser conscients que això dels infinits decimals no és pas una cosa concreta ni una cosa que puguem comunicar a un ordinador. D'altra banda, els cossos importants més concrets, més pràctics, els que sí que podem utilitzar per comunicar-nos amb un ordinador, són els **cossos finits** —principalment els **cossos primers**— els **racionals** i els **cossos de nombres**.[5]

[3] Vegeu, però, la nota 14.

[4] Això descarta les equacions de la criptografia RSA com la tercera de més amunt.

[5] En les meves classes a alumnes de primer de matemàtiques no només he posat aquests cossos al mateix nivell que el cos real i el cos complex, sinó que els he donat, conscientment, una clara preeminència.



LIVRE PREMIER. 303

angle, iuſques a O, en ſorte qu'N O ſoit eſgale a N L, la toute O M eſt ∝ la ligne cherchée. Et elle s'exprime en cete ſorte

$$\propto \frac{1}{2}\, a + \sqrt{\frac{1}{4}\, aa + bb}.$$

Que ſi iay $yy \propto - ay + bb$, & qu'y ſoit la quantité qu'il faut trouuer, ie fais le meſme triangle rectangle

Figura 1: La fórmula de Descartes per resoldre $z^2 = az + b^2$.

I. L'EQUACIÓ DE SEGON GRAU

1 La famosa fórmula de l'equació de segon grau

Un bon lloc per on començar a parlar de trobar les solucions de les equacions polinòmiques és aquesta famosa fórmula de les equacions de grau 2 (FFE^2) que tots els estudiants coneixen:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Per cert, la sabeu demostrar? Com? Compleció de quadrats? Parlem-ne:

- Què és el que volem demostrar? Si el que volem demostrar és que la FFE^2 dóna zeros del polinomi $ax^2 + bx + c$, aleshores, la manera més **natural** de fer-ho és, simplement, **substituir x a l'equació per cadascun dels valors que dóna la fórmula**. O no?
- No es tracta de **descobrir** la FFE^2: fa molt de temps que la FFE^2 es coneix. Diuen que el primer que la va publicar tal com la coneixem avui va ser Descartes al llibre primer de *La Geometrie* (que formava un apèndix del famosíssim *Discours de la méthode*), però la seva versió geomètrica data, com a mínim, de l'any -2000.
- La diferència entre *trobar* una solució i *comprovar* una solució ens portaria a parlar de problemes P i problemes NP i de la famosa i irresolta pregunta «$P = NP$».
- També ens podria dur a parlar de la gairebé màgica troballa de *El Mètode* d'Arquimedes que va ser trobat el 1906 en un palimpsest del segle X que es va sobreescriure el segle XIII. Ara ens adonem que el mètode que seguia Arquimedes per trobar el

seus resultats —que posteriorment demostrava geomètricament— és tant o més interessant que les seves demostracions geomètriques rigoroses, perquè hi trobem els primers vestigis del *càlcul infinitesimal*.

- Amb l'equació de segon grau passa el mateix: el mètode de compleció del quadrat té interès per ell mateix perquè

  1. Ens diu que la *FFE*^{2} dóna *totes* les solucions.
  2. És un mètode que es pot utilitzar en altres àmbits com, per exemple, la classificació de les formes quadràtiques i de les quàdriques.

  Tornem a la *FFE*^{2}:

  $$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

  És una fórmula que dóna seguretat als alumnes i, si volem fer una anàlisi crítica de tot el que hi ha en aquesta fórmula —que és molt— està bé començar «esquerdant» una mica aquesta seguretat. Per exemple, podem preguntar-nos

  ..... *i si el cos base és, per exemple,* $\mathbb{F}_{13}$*?*[6]

Si analitzem la *FFE*^{2} amb una mirada crítica implacable, això és el que hi veiem:

- Hi trobem una **divisió**. Atenció! hem d'assegurar-nos que el divisor no és zero. El divisor és $2a$ i, d'entrada ja veiem que si $a = 0$ (és a dir, si l'equació no és realment de segon grau) la fórmula deixa de ser vàlida. Això cal tenir-ho en compte, però no és cap problema, perquè les equacions de primer grau ja les sabem resoldre fàcilment. Però la cosa tampoc **no funciona** si $2 = 0$. És a dir, la *FFE*^{2} **no és vàlida** en els cossos de característica dos![7]

- A banda de la divisió per 2, la resta d'operacions que fem per verificar la *FFE*^{2} són perfectament vàlides qualsevol cos. És a dir:

  La FFE^2 *és vàlida a* ***tots*** *els cossos,*
  excepte els de característica dos.

  En particular, podem aplicar perfectament la *FFE*^{2} quan treballem sobre el cos $\mathbb{F}_{13}$. Tothom tranquil!

[6] M'agrada molt el cos de 13 elements perquè és el cos més petit que conté les arrels cúbiques i quartes de la unitat i, per exemple, em va ser molt útil en la modelització dels moviments del trencaclosques de l'article *Anàlisi d'un trencaclosques tipus Rubik: un pretext per parlar de modelització, grups, geometria, computació i programació*, Mat^2, vol. 2023, no. 2, pp. 26, 2023.

[7] Recordem que la característica dos és l'idioma matern dels ordinadors. Poca broma!

- La segona cosa que ens ha de fer reflexionar és la presència de l'estrany símbol $\sqrt{\ }$ que, encara que hi estiguem molt familiaritzats —potser, precisament, perquè hi estem molt familiaritzats— requereix que expliquem què significa exactament.

  $$\textit{Direm que } a = \sqrt{b} \textit{ si i només si } a^2 = b.$$

  Però això és incorrecte!

  $$\left.\begin{array}{rcl} (-1)^2 = 1 & \Rightarrow & -1 = \sqrt{1} \\ 1^2 = 1 & \Rightarrow & 1 = \sqrt{1} \end{array}\right\} \Rightarrow\ (1 = -1)\ \Rightarrow\ (2 = 0)$$

  I això no pot ser perquè, precisament, hem dit que estem deixant de banda el cas de característica 2. Ho hem de dir millor:

  $$\begin{array}{c} \sqrt{b} \textit{ és qualsevol element del cos} \\ \textit{que compleixi que el seu quadrat és igual a } b. \end{array}$$

  El problema és que, dit així, $\sqrt{b}$ ja no és un element ben definit del cos sinó que és, més aviat, un **conjunt** que pot ser buit, pot tenir un únic element o pot tenir-ne dos. Quan b té *dues* arrels quadrades diferents no hi ha, en general, cap criteri per triar-ne una o una altra:[8] no hi ha manera de distingir-les ... a no ser que estiguem en el cos real, que és un cos que té la curiosa propietat que tots els seus elements es classifiquen en tres grups: els positius, els negatius i el zero. Però això és una situació que només es dóna en el cos real i en el cos racional.

- En la majoria de cossos, hi ha equacions de segon grau que no tenen cap solució (en el mateix cos, s'entén). En aquests casos, com que la FFE^2 val sempre, el que succeeix és que l'arrel quadrada representa el conjunt buit. És a dir, la FFE^2 no només ens dóna les solucions sinó que també ens dóna l'*absència* de solucions.

- Finalment, fixem-nos en el símbol $\pm$ que apareix a la FFE^2. Segons el que acabem de dir, aquest $\pm$ l'hem de considerar com formant part de l'arrel quadrada i, de fet, ens el podríem estalviar. Com que estem en característica diferent de 2, si a és una arrel quadrada de b, aleshores $-a$ també és arrel quadrada de b. Pensem, doncs, que el símbol $\pm$ de la fórmula està posat aquí només per recordar-nos que l'arrel quadrada pot ser que no sigui única.

Parlem una mica més de l'arrel quadrada o, més exactament, de les arrels quadrades. Aquí, copiant Marcellus de Hamlet, podríem dir que *"Hi ha quelcom que és podrit, a l'arrel quadrada"*:

[8] És difícil, en aquest moment, adonar-se la la importància cabdal del fet que les dues solucions siguin *indistingibles*: aquí comença, precisament, la **teoria de Galois**.

$\sqrt{a}$ *és qualsevol nombre que compleixi* $x^2 - a = 0$.

La solució de l'equació $x^2 - a = 0$ *és* $\pm\sqrt{a}$.

Això és una *petitio principii* de manual! o, si ho preferiu, una tautologia ridícula!

> El Professor: Quines són les solucions de $x^3 - 3x + 1 = 0$?
> L'Alumne: Són $\mathcal{R}(1, 0, -3, 1)$.
> El Professor: Què vol dir $\mathcal{R}$?
> L'Alumne: $x = \mathcal{R}(a, b, c, d)$ vol dir $ax^3 + bx^2 + cx + d = 0$.
> El Professor *(fent un apart):* La mare del Tano!

Com resolem aquesta delicada situació? La resposta és simple i important:

> **La fórmula de l'equació de segon grau no resol l'equació de segon grau, només redueix el problema de trobar les solucions de qualsevol equació de segon grau al problema —presumiblement més senzill— de resoldre unes equacions de segon grau concretes: les de la forma** $x^2 + c = 0$**.**

2 I la fórmula en característica dos?

Saber que podem resoldre l'equació de segon grau —o, per ser més exactes, reduir qualsevol equació de segon grau a una *arrel quadrada*— en tots els cossos menys els de característica dos ens hauria de despertar la curiositat per saber quina és la formula que funciona en característica dos. Vegem-la.

És senzill de veure que **no tindrem una fórmula com la** FFE^2**, de cap manera**. Suposem que la tinguéssim, que

$$x = f(a, b, c)$$

fos una fórmula que ens donés les solucions de l'equació $ax^2 + bx + c = 0$ i de manera que f, per complicada que sigui, només utilitzi sumes, multiplicacions, divisions i arrels quadrades. Apliquen ara aquesta fórmula a l'equació $x^2 + x + 1 = 0$ sobre el cos de quatre elements $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$. Les solucions de l'equació són, precisament, α i $1 + \alpha$. Observem:

- Si la fórmula fos correcta, tindríem $f(1, 1, 1) \in \{\alpha, 1 + \alpha\}$.
- Sobre el cos $\mathbb{F}_2$, tot element té arrel quadrada.
- f només té sumes, multiplicacions, divisions i arrels quadrades, partint de $(1, 1, 1)$.
- En conclusió, $\alpha \in \mathbb{F}_2$, que és una contradicció.

El que ens diu això és que en característica dos, és **impossible** reduir totes les equacions de grau dos a arrels quadrades i, per tant, l'única cosa que podem esperar és trobar una fórmula que ens redueixi l'equació de segon grau a les arrels quadrades i *alguna altra equació de segon grau* presumiblement més senzilla. Això és possible i la solució és aquesta:

$$\begin{array}{c} ax^2+bx+c=0 \\ a\neq 0 \end{array} \quad \Longleftrightarrow \quad \begin{cases} x=\sqrt{\dfrac{c}{a}}, & b=0 \\ x=\dfrac{b}{a}\left[\epsilon+\mathfrak{R}\left(\dfrac{ac}{b^2}\right)\right], & b\neq 0,\ \epsilon=0,1 \end{cases}$$

Aquesta curiosa fórmula requereix alguns comentaris:

- A l'arrel quadrada no hi hem posat el $\pm$ perquè no té sentit en característica dos. D'altra banda, la bonica fórmula $(x+a)^2=x^2+a^2$ —vàlida en característica 2— ens diu que l'arrel quadrada, si existeix, és única.
- Hi apareix la funció $\mathfrak{R}(u)$ que, per definició, indica una solució de l'equació $x^2+x=u$.
- És evident que si α és una solució de $x^2+x=u$, aleshores $1+\alpha$ és l'altra solució. Això explica el $\epsilon=0,1$ de la fórmula.

La demostració d'aquesta fórmula en característica dos és igual de senzilla que la de la fórmula clàssica: N'hi ha prou amb fer el canvi de variable $y=ax/b$. En resum:

> **En característica dos, sabem resoldre totes les equacions de segon grau si sabem resoldre les de la forma $x^2+c=0$ i les de la forma $x^2+x+c=0$.**

3 Com calculem les arrels quadrades?

Hem vist que la *FFE*^{2} ens redueix el problema de les equacions de segon grau al càlcul d'arrels quadrades i, en el cas de característica dos, a calcular la funció $\mathfrak{R}(u)$ que sovint s'anomena la *2-arrel*. Per poder dir que tenim el problema de l'equació de segon grau completament resolt ens falta discutir si és possible calcular arrels quadrades i com ho podríem fer. Aquí la situació depèn clarament de quin sigui el cos on treballem i ens donarem per satisfets si sabem trobar arrels quadrades a $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, els cossos finits i els cossos de nombres. Parlem per separat de cadascun d'aquests casos.

3.1 Els racionals i els reals

Calcular l'arrel quadrada d'un nombre racional (o decidir que no en té) és essencialment trivial. Calcular l'arrel quadrada d'un nombre real positiu voldrà dir, és clar, tenir un

algorisme prou eficient que ens doni una aproximació decimal de l'arrel quadrada amb tants decimals com vulguem. Alguns d'aquests algorismes es coneixen des dels temps més remots (n'hi ha un que formava part del currículum escolar quan jo estudiava). Sense entrar en més detalls, podem considerar aquests casos com a plenament resolts.

3.2 Els complexos

El càlcul de les arrels quadrades d'un nombre complex es redueix fàcilment al càlcul d'arrels quadrades reals, utilitzant aquesta fórmula senzilla de demostrar

$$|z| = 1 \quad \Rightarrow \quad \sqrt{z} = \begin{cases} \pm \dfrac{1+z}{|1+z|}, & z \neq -1 \\ \pm i, & z = -1. \end{cases}$$

3.3 Els cossos finits

Quan parlem de resoldre equacions sobre un cos finit, hem de començar fent aquesta observació important:

> *Des d'un punt de vista teòric, resoldre qualsevol equació $f(x) = 0$ sobre un cos finit k és una trivialitat: n'hi ha prou amb anar substituint x per cadascun dels elements de k i veure en quins casos l'equació es compleix. Si el nombre d'elements de k és petit, això es pot fer trivialment. Però els cossos finits que tenen interès pràctic —per exemple, en criptografia— tenen molts elements. De l'ordre de més de 10^{600}. Per tant, quan parlem de resolució d'equacions de segon grau en cossos finits estem parlant de* trobar algorismes eficients per trobar les solucions*, algorismes que siguin prou ràpids per ser aplicats als cossos que ens interessen.*

Comencem pels **cossos finits de característica dos**, és a dir, els cossos $\mathbb{F}_{2^m}$ per algun $m > 0$. Curiosament, la resposta en aquest cas és trivial: en aquest cos **tots** els elements tenen arrel quadrada —i en tenen només una. Els elements diferents de zero de $\mathbb{F}_{2^m}$ formen un grup multiplicatiu d'ordre $2^m - 1$. Per tant, si $d \in \mathbb{F}_{2^m}$ tindrem $d^{2^m-1} = 1$ i

$$d = d^{2^m} = \left(d^{2^{m-1}}\right)^2$$

i la unicitat ve de la fórmula de la potència del binomi en característica dos que ja hem esmentat abans. Podem donar el tema per resolt o, per ser més exactes, tenim el problema reduït a trobar algorismes eficients per calcular potències grans d'elements de $\mathbb{F}_{2^m}$.

Parlem ara dels **cossos finits de característica senar** i, per simplicitat, reduïm-nos al cas dels cossos primers $\mathbb{F}_p$. Com hem observat abans, per trobar $\sqrt{b}$ sempre podríem anar

elevant al quadrat cadascun dels elements del cos fins que en trobem un que doni b o acabem els elements i vegem que b no té arrel quadrada al cos. Però, si p és molt gran, això és irrealitzable i ens hem de preguntar si hi ha algorismes eficients per trobar arrels quadrades a $\mathbb{F}_p$ ($p \neq 2$). Tot això és objecte important d'estudi a la criptografia.

Determinar si un element té arrel quadrada. La resposta és senzilla i ja la va trobar Euler el 1748. Ja sabem que tots els elements $\neq 0$ de $\mathbb{F}_p$ són zeros del polinomi $x^{p-1} - 1$. Aquest polinomi descompon com

$$(x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1).$$

Cada element diferent de zero té dues arrels quadrades. Això vol dir que a $\mathbb{F}_p$ hi ha exactament $(p+1)/2$ elements que són quadrats i $(p-1)/2$ elements que no són quadrats. Clarament, si $a = b^2$, aleshores $a^{(p-1)/2} = 1$. Com que un polinomi no pot tenir més arrels que el grau, deduïm que si a és un quadrat, aleshores $a^{(p-1)/2} = -1$. En conclusió, tenim el criteri d'Euler per decidir si un element de $\mathbb{F}_p$ és un quadrat o no:

$$a^{\frac{p-1}{2}} = 1 \iff a \text{ és un quadrat a } \mathbb{F}_p.$$

En resum, podem donar per resolt el problema de saber si un element de $\mathbb{F}_p$ té arrel quadrada.[9] Quan sapiguem que en té, el problema —molt més difícil— és trobar-la.

Trobar l'arrel quadrada. Suposem que tenim $a \in \mathbb{F}_p^*$ que ja sabem que té arrel quadrada: $a = b^2$ per un cert b que no coneixem. Ja hem vist que $a^{(p-1)/2} = 1$. Hi ha un cas trivial:

Si $p \equiv 3 \mod 4$*, les arrels quadrades de* a *són* $b = \pm a^{(p+1)/4}$*. Això és evident:*

$$\left(\pm a^{\frac{p+1}{4}}\right)^2 = b^{p+1} = b^2 = a.$$

Tema resolt.

Quan $p \equiv 1 \mod 4$ la situació és molt més complicada. Els dos algorismes clàssics són el de Cipolla del 1904 i el de Tonelli del 1891. Els dos tenen en comú que necessiten disposar d'un element de $\mathbb{F}_p$ que **no** sigui un quadrat. Com que exactament la meitat dels elements de $\mathbb{F}_p^*$ són quadrats i l'altra meitat són no-quadrats, es procedeix escollint elements a l'atzar fins que en trobem un que no sigui quadrat. Es diu que són algorismes *probabilístics* però això és una mica imprecís perquè l'arrel quadrada que es troba és 100% segura.

[9] Tanmateix, recordem que el problema és sempre la computabilitat efectiva i, per tant, cada vegada que trobem un mètode per resoldre el problema hauríem d'estudiar la seva complexitat computacional. No entrarem en aquest tema, però en aquest cas concret, elevar a a aquesta potència necessita un temps que és polinòmic en $\log(p)$. Hi ha un mètode molt més ràpid que es basa en la famosa *llei de reciprocitat quadràtica* demostrada per Gauss a les seves *Disquisitiones Arithmeticae* del 1801. És l'algorisme d'Eisenstein del 1844 que requereix poc menys que l'algorisme d'Euclides de la divisió entera.

Calcular una 2-arrel. Recordem que, en el cas de característica 2 havíem reduït l'equació de segon grau al càlcul de l'arrel quadrada (que ja hem resolt) i al càlcul de $\mathfrak{R}(b)$ que és, per definició, una solució de $x^2 + x = b$ —anomenada una 2-arrel de b. Ens limitarem a donar una idea de la solució.

Considerem la funció $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ definida $f(x) := x^2 + x$. Observem:

- $\mathbb{F}_{2^m}$ és un $\mathbb{F}_2$-espai vectorial de dimensió m.
- $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ és $\mathbb{F}_2$-lineal.
- Per tant, trobar $f^{-1}(b)$ és un *problema d'àlgebra lineal* en un $\mathbb{F}_2$-espai vectorial de dimensió m i, encara que m sigui gran, és molt més petit que 2^m.
- Per resoldre aquest problema lineal necessitem una base de $\mathbb{F}_{2^m}$.

En conclusió: necessitem mètodes eficients de trobar $\mathbb{F}_2$-bases de $\mathbb{F}_{2^m}$ i, a continuació, resoldre un sistema lineal.

3.4 Els cossos de nombres

Plantegem-nos com podem trobar una arrel quadrada en un cos de nombres i quin interès pot tenir fer-ho. Sobre aquestes preguntes només podem dir que la possibilitat de fer càlculs algebraics en cossos de nombres és un camp de recerca molt important que, en particular, té aplicacions a la criptografia i també, com veurem, a la geometria de les construccions amb regle i compàs.

Per tenir un exemple al cap, imaginem-nos que volem resoldre això:

$$\begin{aligned} z^2 = &- 104346\sqrt{-2\sqrt{-4583}-1}\sqrt{\sqrt{-4583}-2\sqrt{-2\sqrt{-4583}-1}-3} \\ &- 136710\sqrt{-4583}\sqrt{\sqrt{-4583}-2\sqrt{-2\sqrt{-4583}-1}-3} \\ &+ 91630\sqrt{-4583}\sqrt{-2\sqrt{-4583}-1} - 155682\sqrt{-2\sqrt{-4583}-1} \\ &+ 7903\sqrt{-4583} - 275363067 \end{aligned}$$

D'entrada, diguem que no estem parlant de calcular el valor aproximat del terme de la dreta i treure'n l'arrel quadrada aproximada —cosa que tampoc no està gens clar com podríem fer si tenim en compte que d'arrels quadrades n'hi ha dues. Estem parlant de trobar el valor **exacte** de z com a element d'un determinat cos de nombres implícit en l'enunciat.

Si ens hi fixem, en l'expressió anterior apareixen fins a tres arrels quadrades diferents:

$$a = \sqrt{-4583}$$
$$b = \sqrt{-2\sqrt{-4583} - 1} = \sqrt{-2a - 1}$$
$$c = \sqrt{\sqrt{-4583} - 2\sqrt{-2\sqrt{-4583} - 1} - 3} = \sqrt{a - 2b - 3}$$

i, per tant, l'àmbit on treballem és el cos de nombres $\mathbb{Q}(a, b, c)$ i la solució la busquem, doncs, en aquest mateix cos de nombres. Segon els *teorema de l'element primitiu* podem escriure $\mathbb{Q}(a, b, c) = \mathbb{Q}(\theta)$ per un cert θ (no únic) perfectament computable. En el nostre exemple, `sagemath` ens dóna que podem prendre θ com una arrel de $x^8 + 12x^6 + 9228x^4 - 91504x^2 + 20903232$ i això ens pot reduir el problema de trobar z a resoldre un sistema d'equacions quadràtiques sobre $\mathbb{Q}$. Tanmateix, els algorismes que utilitza `sagemath` per trobar z són extraordinàriament eficients i gairebé instantàniament ens dóna

$$z = \pm \left(-279\sqrt{\sqrt{-4583} - 2\sqrt{-2\sqrt{-4583} - 1} - 3} + 187\sqrt{-2\sqrt{-4583} - 1} + 245\sqrt{-4583} \right).$$

Relacionem tot això amb les construccions amb regle i compàs. Per fer-ho, llegim la primera frase de *La Geometrie* de Descartes:

> *«Tous les Problesmes de Geometrie se peuuent facilement reduire a tels termes, qu'il n'est besoin par aprés que de connoistre la longeur de quelques lignes droites, pour les construire.»*

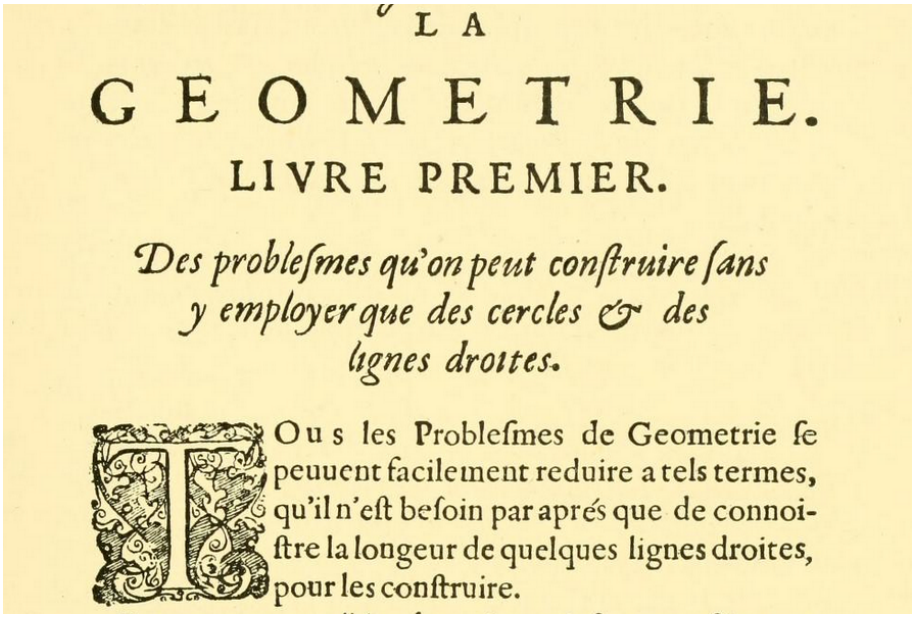
Aquesta frase —que, segons Descartes, redueix la geometria a l'aritmètica— ha tingut una importància històrica immensa, transcendental. Tanmateix, si la llegim avui amb ull crític és possible que la trobem poc acurada. Efectivament, les coordenades cartesianes redueixen la geometria a fer càlculs «aritmètics» amb coordenades i equacions.... **sempre que aquests càlculs els puguem fer de manera exacta** (i Descartes no podia!).

Per exemple, suposem que una certa construcció geomètrica amb regle i compàs ens produeix un triangle i volem demostrar que és isòsceles. Segon Descartes, n'hi hauria prou amb calcular les longituds del seus costats. Suposem que ho fem i veiem que els dos costats que semblen iguals tenen longituds $\sqrt{5} + \sqrt{22 + 2\sqrt{5}}$ i $\sqrt{11 + 2\sqrt{29}} + \sqrt{16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}}}$ respectivament. Aleshores, per demostrar el teorema *a la manera de Descartes* hauríem de demostrar aquesta increïble identitat:

$$\sqrt{5} + \sqrt{22 + 2\sqrt{5}} = \sqrt{11 + 2\sqrt{29}} + \sqrt{16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}}}.$$

Resulta que aquesta igualtat és certa,[10] però Descartes no tenia les eines de teoria de

[10] La identitat va ser descoberta per Daniel Shanks (*Incredible identities*, Fibon. Quart. 12 (1974), 271, 280). Vegeu també l'exercici 4.10.7 de *A Course in Computational Algebraic Number Theory* de Henri Cohen.



DE LA

GEOMETRIE.

LIVRE PREMIER.

Des problesmes qu'on peut construire sans y employer que des cercles & des lignes droites.

TOus les Problesmes de Geometrie se peuuent facilement reduire a tels termes, qu'il n'est besoin par aprés que de connoistre la longeur de quelques lignes droites, pour les construire.

cossos que calen per demostrar-la i, com que és certa, qualsevol càlcul amb decimals serà inútil per demostrar que és certa.

Un altre exemple —en un sentit contrari— podria ser aquest. L'heptàgon regular no es pot construir amb regle i compàs (Gauss 1800, Wantzel 1837) perquè la longitud ϕ del costat d'aquest heptàgon és un nombre algebraic que no es pot expressar utilitzant només sumes, restes, multiplicacions, divisions i arrels quadrades de quantitat positives. ϕ és una arrel del polinomi $x^6 - 7x^4 + 14x^2 - 7$ i té un valor aproximat de 0.86776747823. En canvi, el nombre real[11]

$$\phi' := \frac{\sqrt{18 - \sqrt{3\sqrt{8646} - 153}}}{3}$$

es pot dibuixar fàcilment amb regle i compàs i té un valor aproximat de 0.86776747821. Si fem un dibuix amb regle i compàs d'un heptàgon de costat ϕ' sobre una circumferència de radi un metre, l'error que cometrem serà d'uns 21 *picòmetres*, més o menys el radi d'un àtom d'hidrogen. A la figura 2 hi trobem aquesta construcció[12] feta amb GeoGebra i podem observar que GeoGebra considera l'heptàgon com a regular, de manera que podem inferir que GeoGebra no utilitza càlculs exactes sobre cossos de nombres.[13]

[11] Vegeu Dietmar Pfeifer, *On an Elementary Approximate Construction of The Regular Heptagon With Ruler And Compass*, Fund. J. Math. Math. Sci. 10 (2024), 87–93,

[12] La construcció es fa d'aquesta manera: el segment EB té una longitud de 79 unitats; AB és perpendicular a EB i $|AB| = 38$; AH és perpendicular a AE i $|AH| = 31$; $|HK| = 105$; $|KN| = 54$; OP passa per E i és perpendicular a EH; KQ és la bisectriu de NKO; la circumferència circumscrita té centre a K i radi $r = 54$. Fent una mica de trigonometria es dedueix que $|OQ| = |QN| = r\phi'$.

[13] Vaig preguntar els desenvolupadors de `euclidea.xyz` si utilitzaven algorismes exactes i em van contestar que treballaven amb aproximacions però van afegir-hi *«we also implemented a lot of countermeasures against*

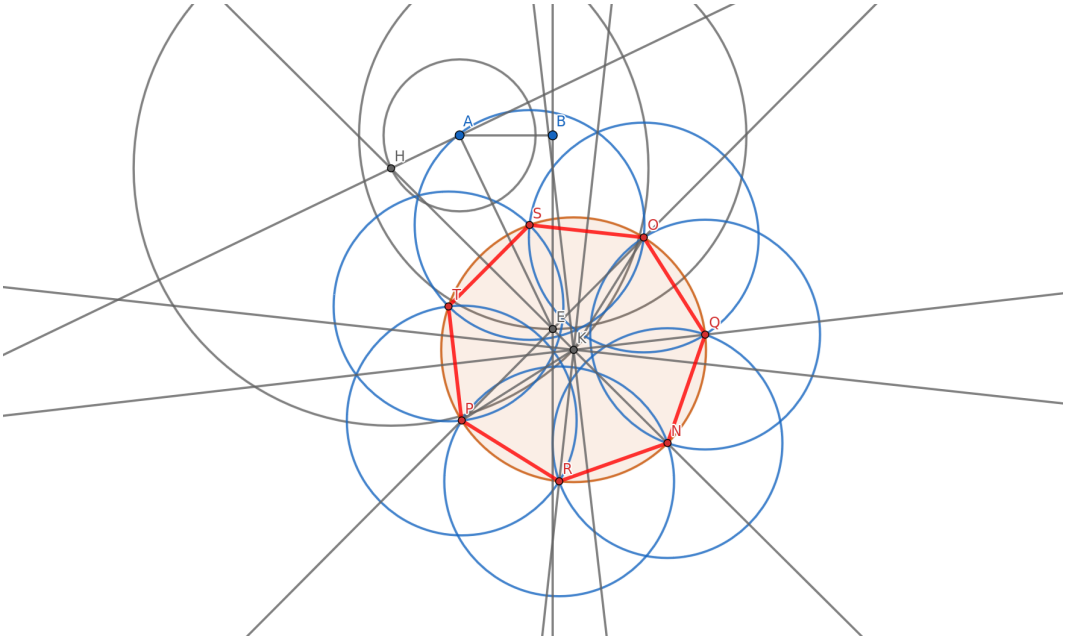


Figura 2: Construcció (Pfeifer) amb regle i compàs a GeoGebra d'un heptàgon regular amb un error $< 10^{-10}$. Les circumferències blaves «demostren» que l'heptàgon és regular.

En resum: per fer realitat el somni de Descartes ens cal poder calcular arrels quadrades en cosos de nombres.

II. L'equació de tercer grau

Comencem dient que si treballem en el cos dels reals i ens interessen les solucions d'una equació de grau no excessivament gran, calculades amb un nombre de decimals més que suficient per a qualsevol aplicació tècnica, tot el que direm a continuació és superflu: qualsevol programa com `sagemath` ens resol el problema en fraccions de segon.[14] Per

cheating». En resum, malgrat que GeoGebra i Euclidea són molt útils per estudiar geometria, no podem considerar els seus dibuixos com si fossin teoremes.

[14]Hem justificat la importància de la resolució d'equacions polinòmiques en el càlcul dels valors propis dels sistemes lineals. Curiosament, aquesta afirmació no és gens encertada perquè —ves quina paradoxa!— la manera més efectiva de calcular (numèricament) els zeros d'un polinomi —i la manera com ho fan realment els ordinadors— consisteix en prendre una matriu que tingui per polinomi característic el polinomi del que volem trobar les arrels i, aleshores, calcular els valors propis d'aquesta matriu. No podem entrar a fons en la teoria dels mètodes numèrics que hi ha al darrere de l'afirmació anterior (tot això està tractat a fons en el capítol 13 del llibre *Matrices* de Denis Serre).

exemple:

```
> x = polygen(RR)
> (x^3-3*x+1).roots()
> [(-1.87938524157182, 1), (0.347296355333861, 1), (1.53208888623796, 1)]
> (x^5 - 1.34495506833944*x^4 + 0.659756735077032*x^3 - 0.143302837199138*x^2 +\
>    0.0129552063084713*x - 0.000306554042370339).roots()
> [(0.0354612649646488, 1), (0.194742530979593, 1), (0.231467267093585, 1),\
>    (0.384475149203858, 1), (0.498808856097755, 1)]
```

Si encara seguiu llegint és que us interessa alguna cosa més que les solucions aproximades que basten per a les aplicacions tècniques. Potser voldríeu solucions **exactes**, com en el cas de l'equació de segon grau. En aquest cas, us diré que les solucions exactes de $x^3 - 3x + 1$ **en el cos dels nombres reals** són:

$$x_1 = 2\cos\left(\frac{2\pi}{9}\right), \quad x_2 = 2\cos\left(\frac{8\pi}{9}\right), \quad x_3 = 2\cos\left(\frac{14\pi}{9}\right).$$

Per comprovar-ho, observem que si θ és qualsevol dels tres angles anteriors, aleshores $3\theta = 2\pi/3$ i $\cos(3\theta) = -1/2$ i si apliquem la fórmula del cosinus de l'angle triple

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

observem que, efectivament, x_1, x_2, x_3 són tres solucions diferents de l'equació de tercer grau inicial i són, per tant, totes les solucions de l'equació, expressades d'una manera *exacta* però ni *algebraica* ni *per radicals*. És això el que volem? Potser sí. Havíem demanat solucions *exactes* i aquestes ho són, encara que, potser hauríem preferit utilitzar, en lloc de la funció cosinus, les funcions arrel quadrada o arrel cúbica?

4 Resolució de la cúbica per radicals

Suposem que el cos base és $\mathbb{R}$ i volem trobar una fórmula per a les solucions de l'equació genèrica de tercer grau

$$ax^3 + bx^2 + cx + d = 0, \quad a \neq 0.$$

D'entrada, podem dividir per a i generalitzar el truc de «completar el quadrat» a un truc igualment senzill de «completar el cub». Això en el cas de l'equació de segon grau ja ens donava la *FFE*[2], però ara simplement ens reduirà el problema a resoldre aquesta equació:

$$x^3 + px + q = 0.$$

La història del descobriment al segle XVI de la solució de la cúbica *per radicals* és apassionant però no la podem incloure en aquest text.[15] El que sí que és important que

[15] Als meus estudiants els recomanava, dins de les lectures del curs, aquest vídeo del famós canal de Youtube *Veritasium*: `https://www.youtube.com/watch?v=cUzklzVXJwo`.

fem aquí és, com a mínim, sembrar el dubte sobre si és assenyat esperar que totes les equacions es puguin resoldre per radicals. Plantegem la situació d'aquesta manera:

- Hi ha dos tipus de nombres reals irracionals: els que són solució d'alguna equació polinòmica i els que no són solució de cap equació polinòmica. Els primers s'anomenen nombres algebraics, els segons s'anomenen nombres transcendents. Entre els nombres algebraics podem fer esment de

$$\sqrt{2}, \quad \varphi = \frac{1+\sqrt{5}}{2} \text{ (la raó àuria)}, \quad \cos\left(\frac{2\pi}{9}\right), \ldots$$

  Entre els transcendents podem esmentar

$$e, \quad \pi, \quad e^{\pi}, \quad \cos(1), \ldots$$

  Designem per $\mathcal{A} \subsetneq \mathbb{R}$ el subconjunt dels nombres algebraics, que es pot demostrar que formen un cos.

- També podem considerar tots els nombres reals que es poden expressar a partir dels nombres racionals amb les operacions de suma, resta, multiplicació, divisió i arrel n-èsima (de nombres positius), per tot n. Designem $\mathcal{R}$ el conjunt de tots aquests nombres. Es pot demostrar que tots aquests nombres són algebraics i, evidentment, formen un cos. Tenim

$$\mathcal{R} \subseteq \mathcal{A} \subsetneq \mathbb{R}$$

  i no tenim cap motiu per pensar que $\mathcal{R} = \mathcal{A}$. En canvi, si *totes* les equacions polinòmiques es poguessin resoldre *per radicals*, això implicaria $\mathcal{R} = \mathcal{A}$.

El problema de decidir si totes les equacions polinòmiques es poden resoldre per radicals o no va ser un problema molt important que va restar obert durant molts anys. La resposta a aquest problema es va veure que era negativa. En particular, $\mathcal{R} \neq \mathcal{A}$ i un exemple de nombre algebraic que **no** es pot expressar per radicals és, precisament, $\cos(2\pi/9)$. O potser sí que es pot? Ho estudiem a continuació.

Tres matemàtics italians del segle XVI —Scipione del Ferro, Niccolò Tartaglia, Gerolamo Cardano— van trobar un mètode per resoldre *per radicals* l'equació de tercer grau (sobre el cos dels nombres reals). Amb la notació actual i, sobre tot, amb la utilització dels nombres negatius, la solució d'aquests matemàtics és relativament senzilla d'explicar: ve donada per la famosa *Fórmula de Cardano*:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Observem que aquesta fórmula ens dóna un únic valor —els altres dos s'obtindrien utilitzant aquesta arrel per factoritzar el polinomi de tercer grau i, a continuació, resoldre

una equació de segon grau. Com justifiquem aquesta fórmula? Calia ser un geni per *descobrir-la*, però no cal ser un geni per *comprovar-la*: n'hi ha prou amb fer uns petits càlculs rutinaris. Tenim, doncs, una *FFE*^{3} que ens demostra que (sempre sobre els reals) les equacions de tercer grau es poden resoldre per radicals.[16] Posem-la a la pràctica en un parell d'exemples.

- $x^3+x-2=0$. Comencem amb un exemple senzill, per agafar pràctica. Sabeu quines són les solucions? És mot senzill

$$x^3+x-2=(x-1)(x^2+x+2).$$

  Tenim una única solució que és $x=1$ i la fórmula de Cardano ens l'hauria de trobar. Provem-ho:

$$x=\sqrt[3]{1+\sqrt{\frac{28}{27}}}+\sqrt[3]{1-\sqrt{\frac{28}{27}}}=\sqrt[3]{1+\frac{2}{9}\sqrt{21}}+\sqrt[3]{1-\frac{2}{9}\sqrt{21}}.$$

  Per tant, com que ja sabem que l'única solució de l'equació és $x=1$, necessàriament s'ha de complir aquesta curiosa —i, a primera vista, una mica increïble— identitat:

$$\sqrt[3]{1+\frac{2}{9}\sqrt{21}}+\sqrt[3]{1-\frac{2}{9}\sqrt{21}}=1.$$

  Aquests tipus d'identitats amb radicals poden ser molt difícils de demostrar.[17] Us atreviu amb aquesta? La solució és *«adonar-se»* que

$$\left(\frac{1}{2}\pm\frac{\sqrt{21}}{6}\right)^3=1\pm\frac{2}{9}\sqrt{21}.$$

  La conclusió de tot això seria que de la fórmula de Cardano —a diferència de la fórmula de l'equació de segon grau— val més oblidar-se'n.

- x^3-3x+1. Aquesta equació ja ha sortit abans i, de fet, ha anat sortint al llarg d'aquest text. És una equació històricament significativa i ja és hora que expliquem per què. Recordem que les solucions d'aquesta equació són, exactament:

$$x_1=2\cos\left(\frac{2\pi}{9}\right),\quad x_2=2\cos\left(\frac{8\pi}{9}\right),\quad x_3=2\cos\left(\frac{14\pi}{9}\right).$$

[16] Observem que si volem treballar amb altres cossos, aquesta fórmula encara és més *sospitosa* que la *FFE*^{2}. D'entrada, els denominadors que hi apareixen ens diuen que hem de descartar els cossos de característica 2 i 3, però encara hi ha un altre detall molt important: hi apareixen arrels cúbiques i, en un cos general, d'arrels cúbiques n'hi poden haver fins a tres i, per tant, la fórmula de Cardano ens donaria nou solucions possibles, mentre que l'equació original només en pot tenir, com a màxim, tres. Això és molt curiós perquè fa un moment hem *comprovat* que els valors de la fórmula de Cardano són solucions de l'equació. Tenim, doncs, una contradicció i, inevitablement, en la comprovació de la fórmula de Cardano devem haver aplicat alguna propietat que només és vàlida als nombres reals. Descobrir on hem aplicat aquesta propietat seria molt interessant, però ara no tenim temps de fer-ho.

[17] Qui era un mestre en intuir identitats complicades amb radicals era el famós *Ramanujan*. En els seus quaderns n'hi havia algunes de ben inversemblants, que han tingut interessats els experts durant anys.

Observem que $2\pi/9$ és un angle de 40 graus. Si poguéssim **trisecar l'angle** amb regle i compàs, com que és trivial construir amb regle i compàs un triangle equilàter, podríem construir amb regle i compàs un angle de 40 graus i, per tant, un segment de longitud x_1. Però ja hem dit que amb regle i compàs només podem construir segments de longituds que siguin nombres enters combinats amb operacions de sumes, restes, multiplicacions divisions i arrels quadrades. En conclusió:

> *Si x_1 no es pot expressar amb sumes, restes, multiplicacions, divisions i arrels quadrades, aleshores l'angle no es pot trisecar, en general.*

La fórmula de Cardano ens ha d'expressar x_1 a partir de radicals ... però surten arrels cúbiques. Per tant, no ens serveixen per dibuixar un angle de 40 graus. De fet, es pot demostrar que la trisecció de l'angle amb regle i compàs és impossible, veient que és impossible expressar x_1 només amb arrels quadrades. Però aquest fet no el podrem demostrar avui.

Apliquem, doncs, la fórmula de Cardano a $x^3 - 3x + 1$. Obtenim que la solució és...

$$x = \sqrt[3]{\frac{-1+\sqrt{-3}}{2}} + \sqrt[3]{\frac{-1-\sqrt{-3}}{2}}$$

Això és absurd! A l'equació de segon grau, quan obteníem valors impossibles —arrels quadrades de nombres negatius— volia dir que l'equació no tenia solució, però ara sabem segur que aquesta equació té solució. En té tres i sabem els seus valors numèrics. **Què està passant?** La fórmula de Cardano està malament?!? Ens estem equivocant en algun lloc?!? Però abans hem comprovat que la fórmula de Cardano dóna realment solucions de l'equació! Potser l'hi hauríem de preguntar al Cardano directament?!?

Aquesta situació —coneguda com el *casus irreducibilis*— va confondre profundament el mateix Cardano i altres matemàtics de l'època. De fet, si coneixem la teoria dels *nombres complexos*, aquesta situació aparentment paradoxal queda immediatament resolta:

- La fórmula de Cardano és correcta i ens dóna una solució expressada amb radicals, en els nombres complexos.
- El valor x que dóna la fórmula de Cardano és suma de dos nombres complexos no reals, però x és **real** perquè els dos nombres complexos són *conjugats*. De fet, $x \approx 1.532$ i coincideix amb la solució $2\cos(2\pi/9)$ que havíem trobat abans.[18]
- Tota aquesta situació posa de manifest que l'àmbit naturals per estudiar les solucions d'una equació polinòmica és el dels *nombres complexos*, **encara que només ens interessin les arrels reals**.

[18] Aquí estem obviant el fet que, quan treballem sobre els complexos, els nombres diferents de zero tenen *tres* arrels cúbiques diferents i, aleshores, la fórmula de Cardano no ens dóna una solució de l'equació, sinó que ens les dóna totes tres (no pas nou, perquè no totes les combinacions d'arrels cúbiques són vàlides).

- Efectivament, la fórmula de Cardano ens demostra que totes les cúbiques es poden resoldre per radicals *sobre els nombres complexos*.

- L'exemple que acabem d'estudiar suggereix que, en canvi, no totes les cúbiques es poden resoldre per radicals si exigim de romandre sempre dins dels nombres reals. Es pot demostrar que és impossible expressar les solucions de l'equació $x^3 - 3x + 1 = 0$ utilitzant només nombres reals, arrels cúbiques i arrels quadrades de nombres positius.

És a dir: Cardano i els altres matemàtics de l'època que van estudiar l'equació de tercer grau tenien al seu davant els **nombres complexos**, havien arribat a una situació absurda que només el nombres complexos podien dilucidar ... però no van ser capaços de concebre els nombres complexos en la seva plenitud.[19]

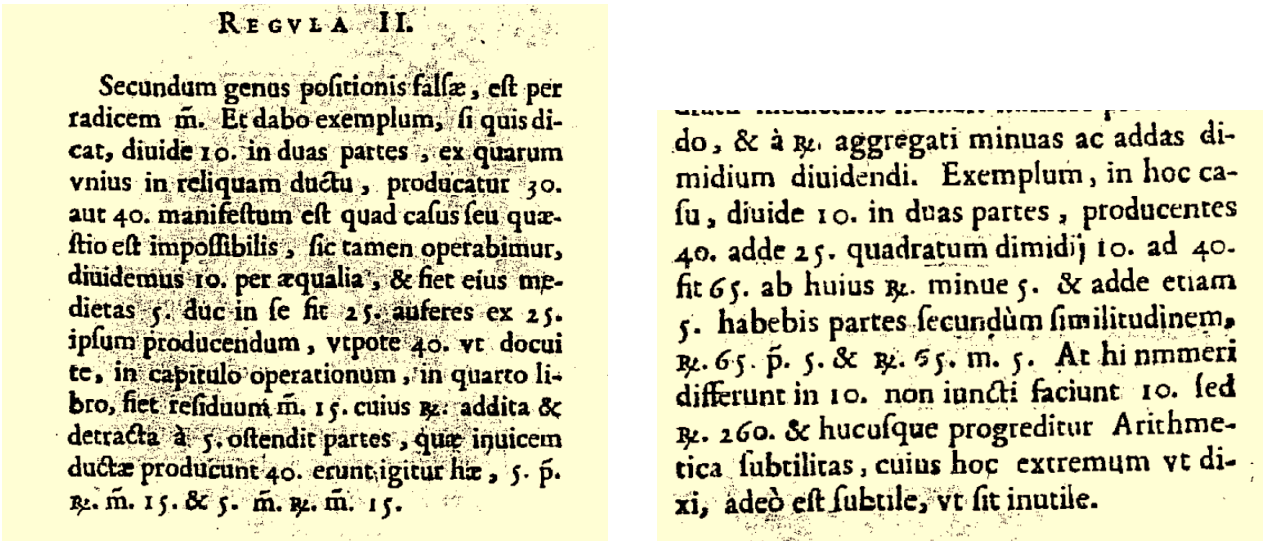
Tanmateix, hem d'admirar Cardano perquè, en la seva obra monumental *Ars Magna* del 1545 hi trobem, a banda de la resolució de les cúbiques i les quàrtiques —que atribueix inequívocament a Scipione del Ferro i Niccolò Tartaglia:

- El concepte d'*arrel múltiple* d'un polinomi.

- La utilització sistemàtica dels nombres negatius. Malgrat això, el fet que Cardano, en lloc d'estudiar l'única equació de tercer grau $x^3 + px + q = 0$ n'estudiï tretze (i vint per a l'equació de quart grau), mostra que admetia els nombres negatius, però no s'hi sentia prou còmode.

- L'acceptació de les arrels quadrades de nombres negatius i la possibilitat de fer operacions aritmètiques amb quantitats que les incloguin. Aquest fet històricament transcendental apareix al capítol XXXVII de l'*Ars Magna* on diu, textualment, *«Secundum genus positionis falsæ, est per radicem m̃»* —que T. R. Witmer tradueix per *The second species of negative assumption involves the square root of a negative*— i a continuació planteja un exercici que ens duria a una equació de segon grau amb solucions $5 \pm \sqrt{-15}$ i demostra que són solucions veient que $(5+\sqrt{-15})(5-\sqrt{-15}) = 40$. Malgrat tot, al final de l'exercici fa el comentari *«Arithmetica subtilitas, cuius hoc extremum vt dixi, adeò est subtile, vt sit inutile»*, que T. R. Witmer tradueix *So progresses arithmetic subtlety the end of which, as is said, is as refined as it is useless*.

[19] Al llarg de la història de la ciència hi ha hagut molts casos com aquest. Un exemple molt interessant —que té una certa semblança amb el de l'equació de tercer grau i els nombres complexos— és el de la *teoria de la relativitat*: al 1887 l'experiment de Michelson-Morley va crear un problema teòric immens a la física, i des d'aquell mateix moment diversos físics (com Lorentz) i matemàtics (com l'eminent Poincaré) van trobar les fórmules que podien resoldre el problema; tenien —com Cardano amb els complexos i l'equació de tercer grau— la teoria de la relativitat al davant dels seus ulls, però va caldre esperar l'espurna de geni d'Einstein perquè es fes la llum. *[Això és una sobre-simplificació: quan ja estaven redactades aquestes notes vaig llegir el recent llibre de Jean-Marc Ginoux «Poincaré, Einstein and the Discovery of Special Relativity» (Springer 2024) que, presumiblement, dilucida completament aquesta etapa de la història de la ciència.]*



REGVLA II.

Secundum genus poſitionis falſæ, eſt per radicem m̃. Et dabo exemplum, ſi quis dicat, diuide 10. in duas partes, ex quarum vnius in reliquam ductu, producatur 30. aut 40. manifeſtum eſt quad caſus ſeu quæſtio eſt impoſſibilis, ſic tamen operabimur, diuidemus 10. per æqualia', & fiet eius medietas 5. duc in ſe fit 25. auferes ex 25. ipſum producendum, vtpote 40. vt docui te, in capitulo operationum, in quarto libro, fiet reſiduum m̃. 15. cuius R̃. addita & detracta à 5. oſtendit partes, quæ inuicem ductæ producunt 40. erunt igitur hæ, 5. p̃. R̃. m̃. 15. & 5. m̃. R̃. m̃. 15.

do, & à R̃. aggregati minuas ac addas dimidium diuidendi. Exemplum, in hoc caſu, diuide 10. in duas partes, producentes 40. adde 25. quadratum dimidij 10. ad 40. fit 65. ab huius R̃. minue 5. & adde etiam 5. habebis partes ſecundùm ſimilitudinem, R̃. 65. p̃. 5. & R̃. 65. m. 5. At hi nmmeri differunt in 10. non iuncti faciunt 10. ſed R̃. 260. & hucuſque progreditur Arithmetica ſubtilitas, cuius hoc extremum vt dixi, adeò eſt ſubtile, vt ſit inutile.

Figura 3: Cardano, *Ars Magna*, cap. XXXVII

I què fa Cardano en el *casus irreducibilis*? Doncs hi passa d'esquitllentes: cap ni una de les cúbiques que resol (excepte les que tenen solucions enteres) dóna un terme negatiu dins de l'arrel quadrada. Si ens limitem a les cúbiques reduïdes (sense terme quadràtic) aquestes són les 40 equacions que resol Cardano en cadascun dels capítols com a exemples de les seves regles de resolució:

XI. $x^3 + 6x = 20$, $x^3 + 3x = 10$, $x^3 + 6x = 2$.

XII. $x^3 = 6x + 40$, $x^3 = 6x + 6$.

XIII. $x^3 = 10x + 12$, $x^3 + 12 = 10x$, $x^3 + 3 = 8x$, $x^3 = 8x + 3$, $x^3 + 60 = 46x$.

XV. $x^3 = 84 + 12x$, $x^3 + 9 = 12x$.

XVII. $x^3 + 6x = 178$, $x^3 = 21x + 380$, $x^3 + 9 = 10x$.

XVIII. $x^3 + 3x = 4$, $x^3 + 4 = 6x$, $x^3 = 22x + 36$, $x^3 + 8x = 9$, $x^3 = 3x + 2$.

XIX. $35 + x^3 = 32x$.

XX. $x^3 = 84x + 889$.

XXI. $x^3 + 64 = 36x$, $x^3 = 36x + 55$.

XXII. $x^3 + 8 = 8x$, $8x + 7 = x^3$.

XXV. $x^3 = 20x+32$, $x^3+24 = 32x$, $x^3 = 10x+24$, $x^3 = 19x+30$, $x^3 = 7x+90$, $x^3 = 16x+21$, $x^3 = 4x+15$, $x^3 = 14x+8$, $x^3+12 = 34x$, $16x = x^3+21$, $19x = x^3+18$, $18x = x^3+8$, $15x = x^3+18$, $x^3+48 = 25x$.

Les de color vermell són les que no tenen cap arrel racional i són, per tant, les úniques en les que la fórmula de Cardano és realment necessària. N'hi ha set. Les de color blau són les que tenen discriminant positiu i, per tant, la fórmula de Cardano involucra arrels de nombres negatius. Per entendre millor els prejudicis i les limitacions de Cardano, estudiem com resol, en el capítol XXV, l'equació $x^3 = 20x + 32$. De fet, dóna una regla *particular* –que vol dir que potser no és útil en tots els casos— per resoldre equacions de la forma $x^3 = px + q$ (amb $p, q > 0$, és clar).

En primer lloc observem que $x = -2$ és una solució evident de l'equació i, per tant, podem escriure

$$x^2 - 20x - 32 = (x + 2)(x^2 - 2x - 16)$$

amb la qual cosa les arrels són -2 i $1 \pm \sqrt{17}$. Observem també que, si apliquem directament la fórmula de Cardano a l'equació, apareixen arrels quadrades de nombres negatius i no anem enlloc.

Què és el que fa Cardano? En primer lloc, podem estar segurs que Cardano veu que -2 és una arrel però, com que es tracta d'un nombre negatiu, considera que no és una arrel vàlida i en vol trobar una de positiva. El que proposa, quan es tracta d'equacions de la forma $x^3 = px + q$ és de buscar —*a ull*, s'entén— una solució del sistema $p = a + b$, $q = a\sqrt{b}$. Un cop trobats valors de a i b que compleixin el sistema, Cardano diu que la solució de l'equació inicial és

$$x = \frac{\sqrt{b}}{2} + \sqrt{a + \frac{b}{4}}.$$

Per a nosaltres, l'explicació de la validesa d'aquesta regla és senzilla: el sistema que proposa Cardano que resolguem a ull és equivalent a trobar un $c = \sqrt{b}$ que compleixi $-y^3 + py - q = 0$. És a dir, és equivalent a trobar una arrel $-c$ de l'equació inicial. Si ara dividim $x^3 - px - q$ per $x + c$ tindrem l'equació de segon grau que compleixen les altres dues arrels i la regla de Cardano es redueix a la fórmula de les equacions de segon grau.

En resum, a Cardano li faltava, d'una banda, tenir més confiança en la *validesa* dels nombres negatius i, de l'altra, conèixer la relació entre les arrels d'un polinomi i la descomposició en factors (és a dir, Vieta). Malgrat tot, el contingut monumental de l'*Ars Magna* fa pensar que Cardano sí que coneixia tot això però, per alguna mena de prejudici, no ho va voler escriure sobre el paper.[20]

Quan l'autor d'aquest petit treball de caire docent va explicar aquests temes als seus alumnes de primer curs del grau de matemàtiques, vam acabar la classe fent un viatge en el temps i parlant amb Cardano a veure si li podem donar la petita empenta que li faltava per poder entendre què passa amb els negatius i, sobretot, amb els *«secundum genus positionis falsæ»*, és a dir, amb les arrels quadrades dels negatius. La discussió va ser tan interessant com, probablement, inútil i, inevitablement, va anar a parar a qüestions filosòfiques, principalment *què significa que un objecte matemàtic existeix*. Cardano,

[20] Aquesta situació fa pensar en l'obra d'Arquimedes de la que hem parlat a la pàgina 4.

potser per influència de Plató —que va dir *«la geometria tracta d'allò que sempre és»*— acceptava l'existència del que es pot representar geomètricament, i només del que es pot representar geomètricament. Nosaltres li vam replicar que l'arrel quadrada de -1 sí que tenia una representació geomètrica —un gir de noranta graus que, fet dues vegades ($\equiv$ elevat al quadrat) es -1 ($\equiv -I$)— però per aquest camí no ens vam entendre: la distància que ens separava era massa gran. Aleshores, vam argumentar en la línia de dir que *La Ilíada* bé que crèiem que existia, però comparar la Ilíada amb $\sqrt{-1}$ tampoc no el va convèncer gens. Finalment, li vam dir que *«en matemàtiques, existeix tot allò que no és contradictori»*, Cardano es va escandalitzar profundament i va acusar els matemàtics del futur —nosaltres— de *«pensar-nos que som Déu»*. Li vam replicar *«una mica sí que ho som»* i vam retornar al nostre temps. Abans de marxar, un dels estudiants va voler fer-se una selfie amb Cardano: