Niels Henrik Abel (1802-1829)

LA TEORIA DE NOMBRES EN EL SEGLE XIX

per

Pascual Llorente

Considerant globalment la història de les matemàtiques durant el segle XIX, hom hi pot observar tres característiques destacades:

1) Un desenvolupament extraordinari de cada una de les branques.
2) Un procés d'abstracció creixent.
3) Una actitud cada cop més crítica respecte al rigor.

La primera d'aquestes característiques és determinada quantitativament al paràgraf inicial de la famosa *Història de la Teoria de Nombres* de L. E. Dickson: "Els esforços de Cantor i dels seus col·laboradors ens mostren que una història cronològica de les matemàtiques anteriors al segle XIX pot ésser escrita en quatre grans volums. Hom ha estimat que en caldrien uns quinze per tal de cobrir de la mateixa manera aquesta darrera centúria, de tan extensa que és la literatura matemàtica d'aquest període".[1]

Un exemple del procés d'abstracció ens ha estat donat pel Dr. Pere Menal en la conferència precedent, en la qual ha mostrat com els matemàtics del segle XIX anaren elaborant el concepte de grup abstracte.

Quant a la preocupació pel rigor, hom no es refereix només al rigor de les demostracions sinó, també, al de la fonamentació de les matemàtiques, cosa que, junt amb el procés d'abstracció assenyalat, ha produït una formalització creixent de les teories matemàtiques.

Aquesta tercera característica, vinculada al que hom sol anomenar "crisi dels fonaments", potser és la més coneguda, degut als usos ideològics a què ha estat sotmesa sovint.

En la present conferència ens proposem demostrar que la teoria de nombres és una de les branques de les matemàtiques on aquestes tres característiques són més clarament manifestes.

Suposarem que el lector/oïdor només té idees aproximades sobre la teoria de nombres i que no en coneix l'estat actual. Això, certament, és una limitació molt forta per a poder assolir el nostre propòsit i ens obliga a desenvolupar el tema prescindint, tant com puguem, de tecnicismes matemàtics.

1. Ens referim a l'obra en tres volums *History of the Theory of Numbers* de Leonard Eugene Dickson, Vol. 1 (1919), Vol. II (1920) i Vol III (1923), reeditada per Chelsea, Nova York, 1966. La cita correspon al començament del prefaci del Vol. I (la traducció és nostra).

És clar, doncs, que aquesta conferència no vol ésser un informe matemàtic del desenvolupament de la teoria de nombres durant el segle XIX, cosa que hom pot trobar en altres treballs.[2] Ací només mirarem d'assenyalar alguns *fets històrics* i d'il·lustrar-los amb uns quants, no gaires, fets matemàtics.

Sabem que sentir parlar de problemes, conceptes, teories i resultats desconeguts sol causar una certa incomoditat, i encara més sentir judicis valoratius que s'hi refereixin. Com que la lògica restricció d'extensió que imposa una conferència ens priva de desenvolupar la matemàtica que caldria per a evitar-ho, ens hem limitat a afegir algunes notes al text, en les quals el lector interessat podrà trobar aclariments complementaris i referències bibliogràfiques precises.

Finalment, cal dir que en la redacció present ha estat mantingut l'estil, un pèl lliure i col·loquial, emprat en la conferència. Potser en una altra ocasió tindrem l'oportunitat d'ocupar-nos més extensament d'alguns dels molts problemes i idees que ací només són plantejats o suggerits.

1. Desenvolupaments durant el segle XIX

Un cop d'ull a allò que avui és anomenat "Teoria de Nombres" ens pot deixar sorpresos, potser, de veure la gran varietat dels problemes propis d'aquesta branca de les matemàtiques i la igualment extraordinària diversitat dels mètodes que han estat elaborats a partir de la consideració d'aquests problemes.

Ací el terme "mètodes" no es refereix pas a un conjunt d'algorismes o de regles mecàniques per a resoldre problemes, sinó a conjunts d'idees, conceptes i resultats adequats al tractament de diversos problemes. La majoria d'aquests *mètodes* han anat donant lloc a *teories* relativament independents, per bé que profundament relacionades entre elles. Podem mencionar-ne la teoria de les congruències, la teoria dels nombres algèbrics, la teoria analítica de nombres, la teoria d'aproximació diofàntica i la geometria de nombres, entre altres. És notable que pràcticament tots aquests mètodes i teories siguin deguts als treballs dels matemàtics del segle XIX.

Entre els problemes propis de la teoria de nombres destaquen els *problemes diofàntics,* que consisteixen en la recerca de les solucions enteres d'equacions algèbriques

$$f(X_1, X_2, ..., X_k) = 0$$

amb coeficients enters.

2. Per exemple, de Jean Dieudonné i col·laboradors, *Abregé d'histoire des mathématiques 1700-1900,* Hermann, París, 1978, Vol. I, Cap. 5, pp. 165-334. O bé, d'un altre estil, L.E. Dickson, *op. cit.*

Donada una tal equació diofàntica, el primer problema és el de determinar si té o no té solució, el segon problema consisteix a determinar el nombre de solucions (en particular, si aquest nombre és finit o si el problema té infinites solucions) i el tercer problema és el de trobar les solucions.

Un exemple interessant és donat per la família d'equacions diofàntiques

$$E_n : X^n + Y^n = Z^n.$$

L'equació E_2 es vincula al problema de determinar els triangles pitagòrics (triangles rectangles de costats enters) i l'estudi se'n remunta a l'època dels babilonis. Aquest problema diofàntic té infinites solucions i està completament resolt.

La situació de les equacions E_n amb $n > 2$ és ben diferent. El comunament anomenat *Darrer Teorema de Fermat* assegura que aquestes equacions no tenen solucions enteres positives. Aquest teorema conjectural enunciat per Fermat cap a l'any 1630 és encara un problema obert. Tot i que la importància que pugui tenir com a resultat matemàtic és molt relativa (ja ni parlem de la seva "utilitat" o "aplicabilitat"), l'esforç acomplert pels matemàtics per tal d'intentar resoldre aquest problema ha produït un desenvolupament important de la teoria de nombres. Aquest exemple, que no és ni de bon tros únic en la història de les matemàtiques, hauria de fer reflexionar tots aquells que sostenen una avaluació purament pragmàtica de la recerca i l'ensenyament matemàtics.

La història de la teoria de nombres del segle XIX comença, indubtablement, amb Carl Friedrich Gauss i la seva famosa obra *Disquisitiones Arithmeticae*,[3] publicada l'any 1801. En aquesta obra Gauss considera els mateixos problemes que preocuparen els seus predecessors immediats: divisibilitat, llei de reciprocitat quadràtica, formes quadràtiques... però ho fa d'una manera essencialment nova. Aquests problemes no poden ésser considerats "heretats" car Gauss, a molts, hi arribà ignorant els treballs i els resultats que hom havia produït anteriorment. La novetat del tractament és deguda al fet que Gauss fou capaç d'elaborar els conceptes i les notacions adequats per a abordar cada un d'aquests problemes. És amb ell que comença el procés d'abstracció i de generalització que no solament permetrà que hom doni resposta a moltes de les qüestions plantejades sinó que, a més, generarà una problemàtica nova.

Diguem, de passada, que a les *Disquisitiones Arithmeticae* hom troba la primera exposició sistemàtica de l'aritmètica i que hi és publicada, per primer cop, una demostració del Teorema Fonamental de l'Aritmètica.[4]

Gauss comença les *Disquisitiones* definint el concepte de *congruència*

3. Original en llatí. Traduït a l'anglès per la Yale University Press, 1966.
4. Vegeu el llibre de G. H. Hardy i E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 1968 (1.ª edició, 1938), p. 10.

tal com ho fem actualment. D'aquesta manera s'inicia la *teoria de congruències* que, en gran part, Gauss mateix desenvolupa en aquesta obra.

El Teorema de Fermat, aleshores ja conegut i al qual Gauss arriba independentment i per altres consideracions, pot ésser expressat així:

si p és primer i $p \nmid a$, *aleshores* $a^{p-1} \equiv 1 \pmod p$.

En aquest cas, sigui *e* el menor enter positiu tal que $a^e \equiv 1 \pmod p$. Direm que *a* és una *arrel primitiva de p* si $e = p - 1$. Gauss dóna una nova demostració del resultat següent:

tot primer té una arrel primitiva,[5]

i s'ocupa de l'important problema de trobar mètodes eficients per a determinar-les. Aquest i altres problemes sobre arrels primitives no han pogut ésser resolts satisfactòriament, encara.

La teoria de congruències es desenvolupa notablement durant el segle XIX i aquests desenvolupaments culminen, en cert sentit, quan Hensel introdueix, l'any 1897, els *nombres p-àdics.*[6]

L'aplicació d'aquesta teoria a la resolució de problemes diofàntics se segueix de la següent observació: si $f(x_1, \ldots, x_k) = 0$, llavors $f(x_1, \ldots, x_k) \equiv 0 \pmod m$ per tot $m > 1$. La recíproca no és certa en general, però la implicació anterior dóna, si més no, condicions necessàries de resolubilitat.[7]

Un resultat que atragué poderosament l'atenció de Gauss fou la Llei de Reciprocitat Quadràtica.[8] Tant l'estudi d'aquesta llei com el de les seves

5. Aquest resultat fou enunciat per Lambert el 1769. El nom d'*arrel primitiva* hi fou introduït per Euler el 1773 quan en donà una demostració errònia. La primera demostració correcta fou feta per Legendre el 1785. Vegeu el llibre de William J. LeVeque, *Fundamentals of Number Theory*, Addison-Wesley, 1977, p. 96.
6. Hom pot trobar una exposició elemental de la teoria de congruències a la majoria de textos de teoria de nombres. En particular a G. H. Hardy i E. M. Wright, *op. cit.*, caps. V, VI, VII i VIII i a W. J. LeVeque, *op. cit.*, caps. 3 i 4. En aquesta darrera obra també hi ha definits els nombres p-àdics. Pel que fa als desenvolupaments durant el segle XIX vegeu L. E. Dickson, *op. cit.*, Vol. I.
7. Pel que fa a l'aplicació dels mètodes de congruències a la resolució de problemes diofàntics hom pot consultar L. J. Mordell, *Diophantine Equations*, Academic Press, Londres-Nova York, 1967, i també Z. I. Borevich i I. R. Shafarevich, *Number Theory*, Academic Press, Nova York, 1966 (original rus, 1964), cap. 1. En aquesta darrera obra també hi ha una introducció excel·lent als nombres p-àdics i a llurs aplicacions.
8. Sigui p un primer senar i sigui *a* un enter tal que $p \nmid a$. Direm que *a* és un *residu quadràtic* de p si l'equació congruencial $x^2 \equiv a \pmod p$ té solució.

   El *símbol de Legendre* $\left(\frac{a}{p}\right)$ val 1 si *a* és residu quadràtic de p i val -1 en el cas contrari.

   La Llei de Reciprocitat Quadràtica assegura que si $p = 2P + 1$ i $q = 2Q + 1$ són primers, llavors

$$\left(\frac{p}{q}\right) = (-1)^{PQ} \left(\frac{q}{p}\right).$$

   Euler enuncia un resultat essencialment equivalent a aquest el 1744-46, però diu explícitament que no l'ha pogut pas demostrar. Legendre enuncia la Llei de Reciprocitat Quadràtica el 1785 i en dóna una demostració, però incorrecta. Hom pot trobar més dades sobre la història anterior al segle XIX de la Llei de Reciprocitat Quadràtica a W. J. LeVeque, *op. cit.*, pp. 107-108. Tal com veurem tot seguit el jove Gauss també participà en aquesta història.

generalitzacions possibles ocupen un lloc destacat en el desenvolupament de la teoria de nombres durant el segle XIX.

Gauss descobrí la Llei de Reciprocitat Quadràtica empíricament i ignorant completament els treballs anteriors. El 1795, poc abans de complir divuit anys d'edat, escriu: "Durant tot un any aquest teorema m'ha turmentat i ha absorbit els meus millors esforços, fins que a la fi n'he obtingut una demostració". Aquesta primera demostració, que publica a les *Disquisitiones* (Art. 125-145), és feta per inducció i resulta, segons H.J.S. Smith, "repulsiva"; al cap d'uns anys Dirichlet en donà una versió més clara. En les mateixes *Disquisitiones* (Art. 262) publica una segona demostració, emprant la seva teoria de les formes quadràtiques. Gauss troba que aquest teorema és sorprenent i profund i arriba a considerar-lo una "joia de l'aritmètica superior". Durant la seva vida ens en dóna, pel cap baix, sis demostracions diferents.[9]

La història vinculada a la Llei de Reciprocitat Quadràtica és molt rica i interessant. Només cal dir que en el transcurs del segle XIX hom en donà unes cinquanta demostracions diferents.[10]

Tal com són definits els residus quadràtics hom pot definir els residus k-èsims, per tot $k > 2$, i llavors cercar les possibles lleis de reciprocitat corresponents.

El 1831 Gauss, estudiant la Llei de Reciprocitat Biquadràtica ($k = 4$), introdueix l'anell $Z[i]$ d'*enters de Gauss*: això fou el començament de l'estudi de la *teoria de nombres algèbrics*. Al cap de pocs anys, el 1844, Eisenstein, en els seus treballs sobre la *Llei de Reciprocitat Cúbica* ($k = 3$), introdueix l'anell $Z[\rho]$, on ρ és una arrel cúbica primitiva de 1. No és només per raons tècniques que foren introduïts aquests *anells d'enters algèbrics*, sinó perquè les corresponents lleis de reciprocitat hi tenen llur validesa i hi adquireixen tot llur sentit.

Durant el segle XIX els matemàtics avançaren treballosament en l'estudi de les lleis de reciprocitat. A més de Gauss i Eisenstein, destaquen per llurs contribucions Jacobi, Dirichlet i, sobretot, Kummer. En llurs treballs, a més de la teoria de nombres algèbrics, van desenvolupant la *teoria de ciclotomia* (arrels de la unitat) i també empren la teoria de les funcions el·líptiques.[11]

L'estudi de les lleis de reciprocitat entra en una nova fase quan Hilbert i Weber inicien, cap a la fi del segle XIX, l'estudi de la *teoria de cossos de classes*.

9. En el *Report on the Therory of Numbers* de H. J. S. Smith, Chelsea publ. Co., Nova York, 1965 (original, 1894), p. 59, hom esmenta sis demostracions de Gauss: dues a les *Disquisitiones* (1801), dues del 1808 i dues del 1817; totes són en aquesta obra. A W. J. LeVeque, *op. cit.*, p. 108, hom esmenta vuit demostracions donades per Gauss; d'aquesta obra hem tret la cita de Gauss inclosa al text.
10. Vegeu P. Bachman, *Niedere Zahlentheorie*, 2 Vol., Teubner, Leipzig, 1902 (reimprès en un volum per Chelsea Publ. Co., Nova York, 1968).
11. Sobre aquests desenvolupaments hom pot consultar H. J. S. Smith, *op. cit.*

La teoria de nombres algèbrics és una de les branques més desenvolupades de la teoria de nombres. Bàsicament consisteix en l'estudi de l'aritmètica dels anells d'enters dels cossos de nombres.[12]

Ja hem vist que aquest estudi comença amb els treballs de Gauss i d'Eisenstein relatius a les lleis de reciprocitat. Les investigacions de Kummer sobre les lleis de reciprocitat i sobre el Darrer Teorema de Fermat són les que donen un impuls considerable al desenvolupament d'aquesta teoria. També són importants les aportacions de Dirichlet, Dedekind, Kronecker i Hilbert, que publica, el 1896, la seva famosa *Zahlbericht,* autèntica posta al dia de la teoria de nombres algèbrics i punt de partença del desenvolupament posterior d'aquesta.

Uns altres problemes típics de la teoria de nombres són els que tenen l'origen en la consideració del conjunt dels nombres primers, que, ja ho demostrà Euclides, és infinit. A fi d'explicar la natura d'aquests problemes no hi ha res de més adequat que reproduir les següents paraules d'Euler: "Fins ara els matemàtics han intentat debades descobrir un ordre en la seqüència dels nombres primers i tenim tota la raó de creure que en això hi ha algun misteri que la ment humana no arribarà a penetrar mai. Per tal que ens en convencem basta que donem una ullada a la taula dels nombres primers, que hi ha qui s'ha molestat a calcular fins als 100.000, i veiem que no hi ha ordre ni regla. Això encara és més sorprenent pel fet que l'aritmètica ens dóna regles definides amb les quals podem continuar la seqüència dels primers tan lluny com vulguem, sense notar, emperò, cap mena de rastre d'ordre. Jo mateix em trobo molt lluny d'aquesta meta..."[13] Malgrat el pessimisme aparent d'Euler, veurem com els matemàtics del segle XIX arribaren a donar algunes respostes concretes a aquestes qüestions.

Cap a la fi del segle XVIII, Legendre abandona l'intent clàssic d'explicar l'estructura dels nombres primers i es pregunta si existeix alguna regularitat global, en mitjana, de llur creixement. Per això, considera la funció $\pi(x)$ del nombre de primers p tals que $1 < p < x$. A partir d'algunes evidències numèriques conjectura, el 1785, que

$$\pi(x) \approx A\ x\ /\ (B \log x + C)$$

on A, B i C són constants numèriques i *log* és la funció *logaritme natural.* El 1798 fa la conjectura més precisa determinant que $A = B = 1$ i que $C = 1{,}08366$.

12. El lector interessat pot consultar qualsevol text sobre Teoria de Nombres Algèbrics, en particular el de Z. I. Borevich i I. R. Safarevich, *op. cit.*
13. Euler comença així l'exposició del seu treball: "Descobriment d'una llei extraordinària dels nombres concernint la suma de llurs divisors". Per a l'original en francès vegeu l'*Opera Omnia* d'Euler, sèr. 1, Vol. II, pp. 241-253. La versió del text és treta del llibre *Matemáticas y razonamiento plausible* de George Polya, Ed. Tecnos, Madrid, 1966 (traducció de l'original *Mathematics and Plausible Reasoning,* Vol. I i II, Princeton Univ. Press, 1954), p. 133.

Independentment, Gauss, el 1792 (quan tenia catorze anys), estudiant una taula de primers, conjectura que

$$\pi(x) \approx \int_2^x \frac{dt}{\log t} = \mathrm{li}(x) \qquad \text{(logaritme integral).}^{14}$$

Les conjectures anteriors impliquen l'anomenat

$$\textit{Teorema dels nombres primers:} \lim_{x \to \infty} \pi(x) \cdot \frac{\log x}{x} = 1.$$

L'estudi d'aquest teorema conjectural ocupà molts matemàtics durant tot el segle XIX. En particular Čebyšev, Sylvester i Riemann, que el 1859 publica un dels treballs més importants de la teoria de nombres primers, en el qual introdueix la funció $\zeta(s)$ (*funció zeta de Riemann*). Finalment, el 1896, Hadamard i Ch. de la Vallée Poussin demostren, independentment l'un de l'altre, el teorema.

El fet que la demostració del Teorema dels Nombres Primers sigui analítica no ens ha pas de sorprendre, car la formulació ja n'és analítica. Sí que pot ésser sorprenent, però, la quantitat d'anàlisi que calgué desenvolupar a fi de fer possible aquesta demostració. Recordem que amb aquest propòsit Hadamard elaborà la seva teoria de les funcions enteres.

Un cas totalment diferent és el del Teorema dels Primers en Successions Aritmètiques.[15] Aquest teorema, que fou conjecturat per Legendre el 1785, té un enunciat purament aritmètic, però fou demostrat per Dirichlet el 1837 i el 1839 amb mètodes analítics (sèries de Dirichlet, etc.). Amb aquests treballs de Dirichlet comença la *teoria analítica de nombres,* que constitueix una altra branca important de la teoria de nombres.

Els desenvolupaments anteriors han permès de plantejar i estudiar diversos problemes de la teoria de nombres algèbrics com ara el de la *densitat* de certs conjunts de primers o d'ideals primers en un cos de nombres K. Molts d'aquests problemes són relacionats amb l'estudi de les funcions $\zeta_K(s)$ (funció zeta de Riemann-Dirichlet del cos K) i en particular amb la famosa

hipòtesi de Riemann: tots els zeros complexos de la funció $\zeta(s)$ són a la recta $R(s) = 1/2$ (part real de s),

14. Gauss fou el primer que introduí la funció li(x) i s'ocupà d'aquest problema durant tota la seva vida, però mai no publicà els seus resultats. Els raonaments heurístics que, possiblement, conduïren Gauss a la seva conjectura poden ésser trobats a W. J. LeVeque, *op. cit.*, pp. 4-5.
15. Aquest teorema assegura que si $m > 1$ és un enter i a és un enter positiu coprimer amb m, llavors la successió aritmètica $\{km + a\}$ conté infinits nombres primers.
Per exemple, si considerem les successions $\{10k + a\}$, e. teorema implica que existeixen infinits nombres primers la darrera xifra dels quals és 1 (ídem, 3, 7, 9).

que és un dels problemes més importants, encara no resolts, de la teoria de nombres.

Durant el segle XIX foren acomplerts molts treballs sobre problemes diofàntics, però la majoria consistien en l'estudi d'equacions diofàntiques particulars i amb mètodes també particulars que difícilment podien ésser aplicats a altres equacions.

Un mètode general fou elaborat per Runge, el 1887, quan considerà que les equacions diofàntiques $f(X, Y) = 0$ defineixen corbes algèbriques en el pla projectiu complex i els aplicà, doncs, la teoria corresponent a aquestes corbes. Cada problema diofàntic d'aquest tipus es relaciona així amb el problema de determinar els punts de coordenades enteres (o racionals) d'una certa corba algèbrica. D'aquesta manera comença una relació mútua entre la teoria de nombres i la *geometria algèbrica* que ha estat molt fructífera i que continua essent un objecte de recerca important avui en dia.

Un altre mètode general d'abordar problemes diofàntics és la *teoria d'aproximació diofàntica*, que s'inicia, en la seva versió moderna, amb els treballs de Dirichlet del 1842 i que constitueix una altra de les grans branques de la teoria de nombres.

Bàsicament, aquesta teoria consisteix en l'estudi de l'aproximació d'un nombre real per nombres racionals. Com que els racionals són *densos* en els reals, és clar que aquesta aproximació sempre es pot fer tan precisa com es vulgui, però allò que hom estudia és l'existència de "bones aproximacions" d'un real per racionals amb el denominador relativament petit.

Il·lustrem amb un exemple la manera com aquest tipus de problema és presentat, i aplicat a les equacions diofàntiques: sigui a un enter positiu lliure de quadrats; si $(p;q)$ és una solució de l'equació diofàntica $X^2 - aY^2 = 1$, llavors

$$\left| \frac{p}{q} - \sqrt{a} \right| < \frac{1}{2q^2}$$

És a dir que el nombre racional p/q aproxima el nombre real $\sqrt{a}$ amb un error menor que la inversa del doble del quadrat del seu denominador.

El mètode més antic d'estudi d'aquest tipus de problemes d'aproximació diofàntica, i el que permeté d'obtenir els primers resultats, és el de les *fraccions contínues*. Durant el segle XVIII comença un estudi més sistemàtic vinculat a la resolució numèrica d'equacions. Tal com hem dit, la teoria moderna comença amb Dirichlet el 1842, sense emprar fraccions contínues i incloent el problema de l'aproximació simultània de diversos nombres reals.

El 1844, Liouville prova el teorema següent:

"Si α és una arrel d'un polinomi irreductible de grau $n > 1$ amb coefi-

cients enters, llavors existeix una constant $k = k(\alpha)$ tal que

$$\left| \frac{p}{q} - \alpha \right| > \frac{k}{q^n}$$

per tot nombre racional p/q."

Aquest resultat fou emprat per Liouville per a avançar en un altre dels problemes de la teoria de nombres que hem esmentat: l'estudi dels nombres transcendents.

Un primer problema consisteix a demostrar l'existència de nombres transcendents. Això potser pot semblar-nos trivial. En efecte, no és pas difícil de demostrar que el conjunt dels nombres algèbrics és numerable i, doncs, com que el conjunt dels nombres complexos és no numerable, tenim que el conjunt dels nombres transcendents és no numerable! Aquesta demostració, que ens pot semblar "clara i contundent", fou donada per Cantor el 1874. Però pateix d'una deficiència seriosa: tot i que demostra que "quasi tots" els nombres complexos són transcendents, no permet de donar-ne ni un exemple concret.

El teorema enunciat abans diu que els nombres algèbrics no tenen "aproximacions molt bones" per racionals, i aquesta limitació permeté a Liouville de construir famílies de nombres transcendents concrets.

El 1737 Euler ja havia demostrat que e i e^2 són nombres irracionals, i el 1761 Lambert demostrà que π és irracional. Tots dos empraren en llurs proves les fraccions contínues. El problema de saber si aquests nombres eren o no algèbrics, emperò, romania obert.

Hermite, el 1873, demostra que e és transcendent i finalment Lindemann, el 1882, demostra que π també ho és, cosa que posa el punt final al vell problema de la quadratura del cercle.[16]

Un altre mètode important neix de la fèrtil observació de Minkowski que certs problemes poden ésser presentats més intuïtivament considerant figures en l'espai euclidià n-dimensional. L'any 1896 demostra el famós *Teorema del Cos Convex*, que ha tingut tan útils aplicacions en la teoria dels nombres algèbrics.

Aquesta nova branca de la teoria de nombres, que el mateix Minkowski batejà amb el nom de *Geometria de Nombres,* ha estat desenrotllada com una branca independent que té moltes aplicacions —a la teoria de formes, a la teoria d'aproximació diofàntica, a la teoria de nombres algèbrics, etc.— i que també és estudiada pel seu interès propi.[17]

16. Una introducció a les fraccions contínues, l'aproximació diofàntica i altres temes i resultats relacionats que hem mencionat al text pot ésser trobada, per exemple, a G. H. Hardy i E. M. Wright, *op. cit.*

17. El lector interessat pot consultar l'obra original de H. Minkowski, *Geometrie der Zahlen,* Leipzig i Berlín, 1896 (reimpresa por Chelsea, Nova York, 1953) o el llibre de J. W. S. Cassels *An Introduction to the Geometry of Numbers,* Springer-Verlag, Berlín-Heidelberg, 1959, 1971.

Els paràgrafs precedents potser permeten que el lector es faci una idea de l'extraordinari desplegament de la teoria de nombres produït per l'activitat dels matemàtics del segle XIX. N'hem esmentat alguns dels problemes i dels mètodes més importants, per bé que no pas tots (igualment importants són els problemes additius, la teoria de formes, etc.). També hem anomenat alguns matemàtics dels més destacats (però no pas tots, tampoc). Ara bé, aquesta selecció de temes i d'autors, potser necessària per als nostres propòsits, no ha d'ocultar de cap de les maneres el fet que les matemàtiques siguin una producció social. Consultant la ja citada *Història de la Teoria de Nombres* de L.E. Dickson, observem que durant el segle XIX han estat publicats milers d'articles escrits per centenars de matemàtics.

Tampoc no desitgem alimentar la idea, correntment tan acceptada, que el desenvolupament de les matemàtiques sigui cosa pròpia d'aquestes i independent de la realitat sòcio-política i de les ideologies imperants en el medi en què és dut a terme. Lamentablement, el marc i el propòsit d'aquesta conferència no ens han permès d'incloure-hi aquesta mena de qüestions.

2. El procès d'abstracció

Ara considerarem la segona de les característiques generals que marquen la història de les matemàtiques del segle XIX i veurem de quina manera apareix en la teoria de nombres.

La primera cosa que hem d'assenyalar és el canvi d'actitud dels matemàtics del segle passat que els permeté d'iniciar i de desplegar el procés d'abstracció.

Tal com ja hem dit, els matemàtics anteriors al segle XIX que s'ocuparen de la teoria de nombres i, en particular, dels problemes diofàntics, s'acontentaren amb la troballa de solucions particulars d'equacions o de problemes concrets. Durant el segle XIX aquesta actitud varià notablement. Recordem que, en aquest sentit, el segle comença amb l'estudi del problema diofàntic general

$$a X^2 + b XY + c Y^2 = n$$

dut a terme per Gauss a les *Disquisitiones Arithmeticae* i acaba, per exemple, amb el plantejament del *Problema 10 de Hilbert,* que demana un mètode general que permeti de dedicir, mitjançant un nombre finit d'operacions, si un problema diofàntic donat té solució o no en té.

No hem pas de suposar, emperò, que tal canvi d'actitud fos ràpid i definitiu. En efecte, l'any 1920, Dickson encara escrivia: "Desgraciadament, seguint la manera de fer de Diophantus, molts escriptors sobre aquest tema [els problemes diofàntics] s'han acontentat amb una solució particular

del problema, obtinguda fent algunes hipòtesis que en simplifiquen l'anàlisi. [...] Els treballs que només donen solucions particulars del problema considerat tenen si més no el valor de mostrar que el problema no és impossible. Encara més, l'estudi de molts d'aquests treballs revela l'existència de molt pocs tipus de problemes diofàntics auxiliars als quals hom recorre constantment (com ara el de fer una funció quàrtica igual a un quadrat) i la solució completa dels quals permetria de fer un tractament complet d'un bon nombre de problemes, per la qual cosa se'ns presenten com objectes d'investigació particularment útils. Com que ja existeixen massa treballs sobre anàlisi diofàntica que només ofereixen solucions particulars, cal esperar que tots aquells que es dediquin al tema d'ara endavant s'abstindran de publicar res fins que no hagin obtingut la solució completa del problema considerat o, almenys, teoremes generals que s'hi refereixin. Només així el tema serà capaç de mantenir la posició que té al costat d'altres virils branques de les matemàtiques."[18]

Aquest canvi d'actitud, manifestat en l'interès per problemes i mètodes generals, ha conduït a la producció de conceptes nous, a la recerca de notacions adequades i a l'elaboració de teories més abstractes, cosa que ha generat, al seu torn, nous problemes.

Amb els desenrotllaments presentats a la secció precedent podem tenir una idea de l'abast i de la magnitud d'aquest procés durant el segle passat, que fou un procés lent i treballós, en general. Seria molt interessant i molt instructiu estudiar-ne exemples històrics concrets.

Una gran part dels conceptes fonamentals de l'àlgebra actual fou elaborada i apurada durant el procés d'abstracció dut a terme pels matemàtics del segle XIX ocupats en els problemes de la teoria de nombres.

Gauss, a les *Disquisitiones*, agafa les classes d'equivalència de formes quadràtiques binàries enteres de discriminant donat i les considera objectes, entre els quals defineix una llei de composició, i demostra (sense saber-ho) que constitueixen un grup abelià finit. També prova una sèrie de propietats que poden ésser "traduïdes" a propietats dels grups finits. No estem suggerint que en aquest treball hi hagi "implícit" el concepte de grup finit abstracte, ni que se'n "derivi naturalment". Simplement diem que Gauss, amb el seu treball, sense proposar-s'ho (i segurament sense sospitar-ho) comença el procés llarg i complex d'elaboració d'aquest concepte.

Altres conceptes algèbrics a l'elaboració dels quals contribuïren els treballs de teoria de nombres foren els de cos, anell, mòdul i ideal. Les definicions d'aquests conceptes, més o menys definitives, foren donades per Dedekind el 1871, en relació a la teoria de nombres algèbrics.

El nom dels *cossos* apareix en un treball de H. Weber del 1893, on a més considera que els "imaginaris de Galois" són cossos finits.

18. L. E. Dickson, *op. cit.*, final del Prefaci del Vol. II (la traducció és nostra).

El nom dels *anells* fou introduït per Hilbert el 1897 generalitzant la noció d'*ordre* de Dedekind.

El concepte d'*ideal* fou elaborat a través de l'estudi de la divisibilitat en anells d'enters algèbrics i dels treballs de Kronecker sobre geometria algebraica. El nom, degut a Dedekind, prové dels "nombres ideals" introduïts per Kummer en els seus treballs sobre el Darrer Teorema de Fermat.

El canvi d'actitud que hem assenyalat significa un autèntic trencament epistemològic. Aquest trencament fou produït, indubtablement, per Gauss i les seves *Disquisitiones*. A partir d'aleshores, la teoria de nombres és *tota una altra*.

Hem parlat d'uns quants fets que justifiquen la nostra afirmació. Malgrat tot, interessa aprofundir en aquest punt perquè confirmar-lo, entre altres coses, significaria una prova més contra la tesi que pretén que hi ha un progrés continu de les matemàtiques. Alhora, planteja la qüestió dels "herois" de les matemàtiques i llur corresponent visió apologètica. Per molt que destaquem la importància d'un Gauss, no ens adherim a aquest tipus de visió. No obstant això, pensem que no som al moment ni al lloc més adequats per a estendre'ns sobre tot això.

Una conseqüència del procés d'abstracció, generador de conceptes i de teories, és la necessitat de considerar problemes nous. Aquests problemes cada cop són més teòrics i difereixen dels problemes inicials en llur formulació, en llur significat i en els mètodes possibles de resolució. Per a adonar-se de la magnitud d'aquestes diferències només cal comparar els problemes que preocupaven els matemàtics del segle XVIII amb els que proposà Hilbert al Congrés Internacional de Matemàtics de París el 1900.

Això ha produït un desplaçament aparent del camp d'interès de la teoria de nombres cap a regions que poden semblar allunyades, tant pel llenguatge com per la problemàtica, d'aquelles que inicialment considerem pròpies de la teoria.

Aquest fenomen, que no és exclusiu de la teoria de nombres sinó comú a tota la matemàtica, ha continuat (i amb un ritme accelerat) fins als nostres dies, i origina dificultats manifestes a tothom que desitja introduir-se en l'estudi d'aquests temes.

Aquestes dificultats, pròpies del grau d'abstracció a què han arribat les matemàtiques en el nostre segle, són agreujades pel plantejament i l'estil que hom sol adoptar en ensenyar-les.

Més endavant insistirem sobre aquestes qüestions, però diguem ara mateix que es fa difícil imaginar que hom pugui arribar a comprendre una teoria abstracta ignorant-ne la gènesi històrica i el procés real d'abstracció que l'anà produint.

3. La qüestió del rigor

La tercera característica destacada de la història de les matemàtiques del segle XIX, ja l'hem anomenada, és la creixent preocupació pel rigor. Aquesta preocupació no té l'origen en els treballs sobre teoria de nombres sinó en els d'Anàlisi i en els de Geometria.

Pel que fa a l'Anàlisi, la qüestió del rigor ja hi era present cap al 1831 en els intents de Cauchy dirigits a obtenir definicions més precises i correctes dels conceptes fonamentals (límit, continuïtat, etc.) i hi esdevingué una veritable preocupació a partir de les dificultats que sorgiren en estudiar la convergència de les sèries trigonomètriques.

Pel que fa a la Geometria, un dels problemes que preocuparen durant molt de temps els matemàtics fou el de la possibilitat de demostrar el famós "postulat de les paral·leles" d'Euclides. Els intents d'arribar a una contradicció partint de la negació del postulat conduïren Gauss (que mai no publicà els resultats), Lobačevskij el 1829 i altres matemàtics del segle XIX al desplegament de les *geometries no-euclidianes*. Aquests treballs feren rebre un altre cop fort a la intuïció i contribuïren a enfortir la preocupació pel rigor, que no trigà a estendre's a la majoria dels matemàtics de l'època.

L'evolució de la qüestió del rigor durant el segle XIX és magníficament resumida a la següent nota històrica de Lakatos:

"Cap al 1800 el *rigor de la prova* (construcció o experiment transparent) era contraposat a l'argument confús i a la generalització inductiva. Era allò que Euler entenia per *"rigida demonstratio"*, i la idea kantiana de les matemàtiques infal·libles també era basada en aquesta concepció. Hom també pensava que hom demostra allò que hom s'ha proposat demostrar. A ningú no se li acudia que l'articulació verbal d'un experiment mental impliqués cap dificultat real. La lògica formal aristotèlica i les matemàtiques eren dues disciplines totalment separades: els matemàtics consideraven que la primera era clarament inútil. La prova de l'experiment mental subministrava convicció plena sense cap patró deductiu o estructura 'lògica'.

"Els primers temps del segle XIX, l'onada de contraexemples portà la confusió. Com que les proves eren transparents, les refutacions havien d'ésser extravagàncies miraculoses que calia segregar completament de les proves indubtables. La *revolució del rigor de Cauchy* reposava damunt la innovació heurística segons la qual el matemàtic no havia de tenir-ne prou amb la prova: calia que prosseguís i trobés què era allò que havia provat, enumerant-ne les excepcions o, més aviat, enunciant un domini segur on la prova fos vàlida. Però ni Cauchy ni Abel no veieren cap connexió entre ambdós problemes. Mai no se'ls acudí que si descobrien una excepció calia que tornessin a mirar tota la prova. (D'altres practicaven l'exclusió de monstres, l'ajust de monstres o àdhuc "feien els ulls grossos", però tots eren d'acord en el fet que la prova era tabú i que no tenia res a veure amb les "excepcions".)

"La unió, durant el segle XIX, de la lògica i les matemàtiques tingué dues deus principals: la geometria no-euclidiana i la *revolució del rigor de Weierstrass.* Ambdues produïren la integració de la prova (experiment mental) i les refutacions, i començaren a desenvolupar *l'anàlisi de la prova,* introduint gradualment patrons deductius en la prova-experiment-mental. Allò que denominem "mètode de prova i refutacions" constituí llur innovació heurística: uní la lògica i la matemàtica per primera vegada. El rigor de Weierstrass triomfà malgrat els seus reaccionaris opositors, excardinadors de monstres i ocultadors de lemes, que empraven consignes com ara "l'estupidesa del rigor", "artificialitat contra bellesa", etc. *El rigor de l'anàlisi de la prova superà el rigor de la prova,* encara que la majoria dels matemàtics en suportaven pacientment la pedanteria només en la mesura que els prometia una certesa completa.

"La teoria de conjunts de Cantor (amb una nova fornada de refutacions inesperades de teoremes "rigorosos") convertí en dogmàtica una bona part de la vella guàrdia de Weierstrass, sempre disposada a combatre els "anarquistes", excloent els nous monstres o al·ludint a "lemes ocults" en llurs teoremes, que representaven "el darrer crit del rigor", mentre continuaven flagel·lant –per reaccionaris– els de la vella escola per pecats similars.

"Alguns matemàtics aleshores s'adonaren que la tendència al rigor de l'anàlisi de la prova, en el mètode de proves i refutacions, portava a una infinitud viciosa. Llavors començà una contrarevolució "intuïcionista": la decebedora pedanteria lògico-lingüística de l'anàlisi de la prova fou condemnada i hom inventà per a les proves normes noves i extremistes de rigor; les matemàtiques i la lògica tornaren a divorciar-se.

"Els logicistes tractaren de salvar el matrimoni i naufragaren en les paradoxes. El rigor de Hilbert convertí les matemàtiques en una teranyina d'*anàlisis de la prova,* el retorn infinit de les quals ell pretenia detenir mitjançant transparents *proves* de consistència de la seva metateoria intuïcionista. El "substrat fundacional", la regió d'incriticable familiaritat, fou desplaçada cap als experiments mentals de les matemàtiques.

"Gràcies a cada una de les "revolucions del rigor", l'anàlisi de la prova penetrà amb més profunditat dins les proves, fins al *substrat fundacional* del "coneixement bàsic familiar" on la intuïció transparent,el rigor de la prova, regnava absolutament i on la crítica era exclosa. Així, els diferents nivells de rigor només es distingeixen pel punt on tracen la línia divisòria entre el rigor de l'anàlisi de la prova i el rigor de la prova; és a dir, el punt on hauria d'aturar-se la crítica i començar la justificació. "No s'arriba mai a la certesa"; "els fonaments" mai no es troben, encara que l'*"astúcia* de la raó" converteix cada augment de *rigor* en un augment de *contingut* de l'abast de les matemàtiques."[19]

19. Imre Lakatos, *Pruebas y Refutaciones. La lógica del descubrimiento matemático,* Alianza Editorial SA (AU 206), Madrid, 1978 (traduït de l'original *Proof and Refutations. The Logic of Mathematical Discovery,* Cambridge University Press, 1976), pp. 73-74. També hi són desenvolupats altres temes tractats en aquesta secció, en particular la qüestió del rigor en l'anàlisi.

La cita anterior ha d'ésser completada i matisada amb la següent "Nota dels Editors" del llibre de Lakatos, on aquests tracten de comentar-la i fer-la més justa:

"Creiem que aquesta nota històrica minimitza una mica els èxits dels "rigoristes matemàtics". La tendència al rigor a vegades fa l'efecte que ha constituït un esforç dirigit a dos objectius distints, només un dels quals és assolible. Aquests dos objectius són, primer, els arguments i les proves rigorosament correctes (en què la veritat és transmesa infal·liblement de les premisses a les conclusions) i, segon, axiomes o primers principis rigorosament veritables (que haurien de subministrar al sistema la injecció primitiva de veritat, veritat que seria transmesa llavors al conjunt de les matemàtiques pel camí de les proves rigoroses). El primer d'aquests dos objectius fou assolible (donades, és clar, certes suposicions), mentre que el segon mostrà que era inassolible."[20]

Podem extreure de tot això una sèrie de conseqüències històriques, epistemològiques i pedagògiques. De moment només n'indicarem una que sembla evident: *el concepte de rigor no és immutable i definitiu sinó històric i variable.*

D'altra banda, hom també pot dir que la crítica matemàtica neix de necessitats concretes i que aquesta crítica ha estat la força conductora de la recerca dels fonaments de les matemàtiques.

Hem dit al començament que l'anomenada "crisi dels fonaments", produïda la segona meitat del segle XIX, potser és més coneguda degut als usos ideològics a què ha estat sotmesa sovint. Ara no insistirem en aquests *usos*, ni en l'explotació filosòfica de les ciències, ni en les diverses actituds que hom ha adoptat amb la "crisi", car aquestes qüestions ja han estat prou tractades en altres llocs[21] i no formen part dels objectius específics d'aquesta conferència. Diguem només que, davant de l'intent, generalment interessat, de presentar la imatge d'un "enfonsament" de les matemàtiques, ens sembla que basta contraposar el fet històric de llur impressionant desplegament durant aquest període per tal de posar en evidència la fal·làcia d'una visió tan tremendista.

L'actitud crítica i les successives "revolucions del rigor", pel que fa a la teoria de nombres, s'anaren desenvolupant de manera similar a com ho feren en les altres branques de les matemàtiques.

De la qüestió dels fonaments podem esmentar breument els diferents intents d'ampliar i fonamentar el concepte de nombre.

Els *nombres complexos* aparegueren per primer cop cap a l'any 1545

20. I. Lakatos, *op. cit.*, pp. 74-75.
21. Vegeu, per exemple, de Louis Althusser, *Curso de Filosofía para Científicos*, Ed. Laia, Barcelona, 1975 (traduït de *Philosophie et philosophie spontanée des savants*, Maspéro, París, 1967), especialment pp. 67 i següents.

quan Cardano féu conèixer la fórmula de resolució de l'equació de tercer grau, però no foren considerats *nombres* pels matemàtics sinó una mena d'*ens* de mística aparença. Recordem que el 1702 Leibniz expressava: "Els nombres imaginaris són un reflex delicat i admirable de l'esperit diví, gairebé una cosa amfíbia entre l'ésser i el no ésser".[22] Durant el segle XVIII no fou pas aclarit completament aquest concepte dels nombres imaginaris, malgrat que Euler en reconeix la significació fonamental en la teoria de funcions i estableix, el 1748, l'admirable relació

$$e^{ix} = \cos x + i \sin x.$$

El segle XIX els nombres complexos són definitivament acceptats (acceptació deguda, fonamentalment, als treballs on Gauss els dóna llur interpretació geomètrica) i reben llur definició formal com a parells de nombres reals, expressats amb la forma $x + iy$.

Altres *ampliacions* del concepte de nombre són les corresponents a la consideració dels nombres algèbrics i dels nombres reals i foren establertes de manera definitiva per Dedekind.

Els intents de fonamentar l'aritmètica mitjançant la lògica començaren amb els treballs de Frege (1884) i de Peano (1893), que eren el complement dels esforços de Cantor per a fonamentar-la a partir de la seva teoria de conjunts.[23]

Al capdavall, entre les contribucions importants dels matemàtics del segle XIX, podem esmentar les diverses construccions dels *nombres reals*, i molt especialment la duta a terme per Dedekind.

No creiem que calgui explicitar aquí la construcció dels nombres reals per mitjà de *talles*, però sí que ens sembla que convé que ens referim a certes interpretacions "històriques" que, d'alguna manera, minimitzen l'aportació autènticament innovadora del treball de Dedekind. Per exemple, el col·lectiu *Nicolas Bourbaki* en els seus *Elements d'Història de les Matemàtiques*, quan considera la teoria de les magnituds d'Eudoxi (desenvolupada als llibres V i X dels *Elements* d'Euclides), declara: "És fàcil de veure que d'aquest fonament axiomàtic deriva necessàriament la teoria dels nombres reals". Lamentablement, el significat d'expressions del tipus de "deriva necessàriament", "se'n segueix naturalment", etc. (tan sovint emprades per certs expositors), mai no és aclarit suficientment. Tota vegada, la frase

22. Aquesta cita de Leibniz i la resta d'aquesta nota històrica sobre els nombres complexos són tretes de l'excel·lent llibre de Félix Klein, *Matemática Elemental desde un punto de vista superior*, Vol. I.

23. Sobre aquest punt pot ésser interessant d'analitzar la dualitat ordinal-cardinal del concepte de nombre natural i la manera com aquesta es manifesta en les diverses fonamentacions d'aquest. Hom trobarà una discussió d'aquesta qüestió i les seves correspondències psicològiques a, de Jean Piaget i E. W. Beth, *Epistemología matemática y psicología*, Ed. Crítica (Grijalbo), Barcelona, 1980, pp. 283-296.

anterior de Bourbaki sembla que ens vulgui fer fixar en una espècie d'ineptitud comuna a tots els matemàtics des d'Eudoxi fins a Dedekind. Aquest error "històric" de Bourbaki esdevé més difícil d'admetre si tenim present que el mateix Dedekind respongué clarament a aquesta mena d'interpretacions i objeccions quan li foren formulades per R. Lipschitz (vegeu les cartes del 10 i del 27 de juny de 1876 de Dedekind a Lipschitz).[24]

Aquesta preocupació pel rigor de les demostracions i dels fonaments que estem comentant, juntament amb el procés d'abstracció que hem considerat en la secció precedent, han produït una formalització cada cop més gran de les teories matemàtiques.

De fet, el desplegament del procés de formalització i el refermament de la visió formalista de les matemàtiques (fins que n'ha esdevingut l'"estil dominant") corresponen a la història del segle XX. No obstant això, pot ésser interessant que assenyalem un parell de fets històrics que contenen conseqüències pedagògiques importants.

En primer lloc, volem insistir en el fet que la formalització és una etapa necessària i útil del procés de producció dels coneixements matemàtics, però una *etapa posterior,* tant històricament com en la pràctica concreta i real dels matemàtics.

Quan hom pretén capgirar aquest procés, com ho propugnen els formalistes-estructuralistes, apareixen una sèrie de problemes que poden arribar a produir un cert grau d'"alienació" en l'activitat dels matemàtics.

Recordem la caracterització següent, donada per D. Lehman: "Les propietats que ha de posseir una "bona" estructura són les d'ésser tot alhora prou general per a comprendre *situacions molt vàries,* prou rica per a donar lloc a *teoremes no trivials* i prou potent per a ésser *manejable tècnicament*".[25] Sembla natural, doncs, que quan hom ensenya una estructura n'hagi de mostrar, a més del procés que l'originà, que efectivament posseeix aquestes propietats.

D'altra banda, volem fer fixar l'atenció en el fet que moltes vegades la presentació formalitzada no significa cap avançament real en la resolució d'un problema concret. La "claredat" aparent de la nova formulació en un

24. Hi ha extractes d'aquestes cartes al final del llibre de Michel Fichant i Michel Pécheux, *Sobre la historia de las ciencias,* Siglo XXI, Mèxic, 1971-1978 (traduït de l'original *Sur l'histoire des sciences,* Maspéro, París, 1969), on també hi ha una discussió més àmplia d'aquest punt.
Tractem ara d'aclarir el sentit de les cometes que afecten els adjectius "històriques", "històric", emprats al text (a la vora d'"interpretacions" i d'"error" respectivament). Tals *interpretacions* i *errors,* que sovintegen en l'obra esmentada de Bourbaki (i en altres "Històries"), no són en realitat *històrics* sinó *epistemològics* (o bé, potser, ideològics) i provenen d'una visió particular de les matemàtiques i de llur història. No fa cap falta insistir en el fet que la nostra discrepància té l'origen en una concepció epistemològica molt diferent de la bourbakinista.

25. D. Lehmann, *Matemática y dogmática.* Informe presentat a la Societat Matemàtica de França el febrer de 1972, i inclòs al llibre *La enseñanza de las matemáticas modernas,* Alianza Editorial (AU 207), Madrid, 1978. La cita del text hi és a la p. 369.

llenguatge més concís i que ens és més habitual ens pot fer enganyar en aquest sentit.

Vegem-ne un exemple. La consideració de diversos problemes de la teoria de nombres en els quals hom aplica raonaments de *divisibilitat* ha conduït al concepte abstracte de *congruència* que, com hem vist, permet, entre altres coses, reformular el Teorema de Fermat i el concepte d'arrel primitiva. En una segona etapa del procés d'abstracció i formalització hom elabora les estructures algèbriques i la teoria de congruències pot ésser expresada en termes dels anells $\mathbb{Z}_n$ (quocients de l'anell $\mathbb{Z}$ dels enters racionals). En particular, tenim que si p és primer, $\mathbb{Z}_p$ és un cos i els seus elements no nuls constitueixen un grup multiplicatiu cíclic de $p - 1$ elements. Això implica immediatament tant el Teorema de Fermat com el fet que cada primer té una arrel primitiva. Presentats així aquests resultats poden semblar-nos clars i àdhuc trivials. Però l'estructura *no dóna rés més* i el problema de determinar efectivament les arrels primitives continua sense resolució satisfactòria.

Amb aquests comentaris no volem pas minimitzar l'aportació fonamental que significà el procés de formalització dut a terme pels matemàtics del nostre segle ni suggerir que no hagi d'ésser incorporat a l'ensenyament. Només volem expressar la nostra convicció segons la qual és un error pedagògic presentar les matemàtiques *cap per avall,* és a dir, en un sentit oposat al de llur desplegament històric veritable. Que, per exemple, hom no ha de començar un primer curs d'àlgebra explicant la teoria de les categories, o de fer creure als estudiants del batxillerat que els nombres enters són certes classes d'equivalència de parells ordenats de nombres naturals.