EL TRACTAT D'EULER DE LA DOCTRINA DELS NOMBRES, EXPOSADA EN SETZE CAPÍTOLS

Una comparativa amb el Disquisitiones Arithmeticae de Gauss[1]

Josep Pla i Carrera
jpla@ub.edu

1.- Introducció.

El text manuscrit de Leonhard Euler, *Tractatvs de nvmerorvm doctrina capita sedecim quae svpersvnt* [*Tractat de la doctrina dels nombres, exposada en setze capítols*] fou escrit, molt probablement entre els anys 1748 i 1750, i publicat a *Commentationes Arithmeticae*, volum segon, Ginebra 1849, 503–575, essent-ne l'editor Rudolf Fueter. Li correspon l'índex d'ENESTRÖM E792.

És un intent de l'il·lustríssim[2] matemàtic suís, Leonhard Euler, d'elaborar un text que assentés les bases conceptuals –com havia fet ja en l'anàlisi matemàtica amb l'elaboració de l'*Introductio in Analysin Infinitorum* [1748]–, peró dedicat ara a l'*aritmètica* o *teoria de nombres*, com l'anomenà Euler, l'any 1758, a E279, pàgina 39.

És, doncs, molt probable que aquest text no fos conegut per l'insigne matemàtic alemany Carl Friedrich Gauss. Això no obstant no és greu perquè, de fet, el text és, en certa forma, una recopilació dels resultats assolits en d'altres treballs aritmètics del matemàtic que eren ben coneguts pel *prínceps matematicorum*.

---

1 Llegit, a l'Aula Capella, el dia 20 de Setembre de 2007, al *Congrés Internacional 300 aniversari de Leonhard Euler (1707-2007)*, celebrat els dies 20 i 21 de setembre de 2007, a l'Escola Tècnica Superior d'Enginyeria Industrial de Barcelona.

2 La idea se'm va ocórrer quan preparava la conferència que havia de donar a la "Desena Trobada Matemàtica" de la Societat Catalana de Matemàtiques de l'IEC, el 15 de juny de 2007, amb el títol *Euler versus Gauss*. L'estic redactant en forma d'opuscle. De fet, en ell, es fa una anàlisi crítica de les cites que Gauss fa d'Euler al *Disquisitiones*, i dels dèbits que, focalitzant els quatre primers capítols, té dels resultats d'Euler, i també les mancances que s'hi constaten.

El fet que el *Tractat* –així l'anomenaré d'ara endevant– sigui, encara que de forma incipient, un text de recopilació, és tanmateix, com n'indica el títol, un Tractat. Per tant està elaborat de forma més sistemàtica que no pas un article i té una voluntat d'exposició global, concatenada i coherent. Això em va fa pensar en l'interès que pot tenir fer una anàlisi comparativa del *Tractat* d'Euler amb les quatre primeres seccions dels *Disquisitiones Arithmeticae* [1801] de Gauss, que és considerat –amb raó– el Tractat més notable d'aritmètica de l'època.[2] Com sabem el *Disquisitiones Arithmeticae* –d'ara endevant l'abreujaré *DA*– recull els resultats més notables del segle XVIII i assenta les bases per al desenvolupament de l'aritmètica en el segles XIX i XX.[3]

Val la pena indicar, ja des d'ara mateix, que l'estil formal d'ambdós autors és òbviament completament diferent, tant per la manera com redacten els textos matemàtics com pels més de cinquanta anys que hi ha entre l'un i l'altre amb tot el que això suposava a mitjans del segle xviii.

També cal recordar que, tant DICKSON (1919), principalment al volum primer, com WEIL (1984), esmenten el *Tractat*, però ho fan molt de passada i mai comparant-lo amb el text de Gauss.[4] El text de Dickson, com és prou conegut, és una exposició detallada de les aportacions en teoria de nombres des de l'antiguitat fins a finals del segle xix. En canvi, el de Weil és una exposició històrica, però amb relectura personal de l'autor. Tanmateix no arriba a Gauss. Tampoc en la resta de textos citats a la bibliografia complementària –alguns d'ells, d'un gran valor per copsar el pensament d'Euler i d'altres per copsar el pensament d'ambdós matemàtics– els autors s'entretenen, però, en aquesta anàlisi.

De fet, en aquest article –com en l'exposició que vaig fer– només puc oferir un apunt de la recerca que encara estic efectuant. Això no obstant, em va semblar molt important i interessant fer-ne partícips als assistents al Congrés i ara m'ho sembla també estendre-ho a tots aquells que llegiran les ponències d'aquell Congrés Internacional. Això fa que l'exposició sigui una exposició viva.

3 No oblido pas els dos volums del matemàtic francès Adrien-Marie LEGENDRE, *Essai d'une Thérie des nombres* (1798). També sóc conscient de l'interès que tindria repetir aquesta comparativa entre el text d'Euler i el de Legendre.

4 Voldria indicar que André WEIL, a Weil (1984), cita els paràgrafs 256-259; 284-307; 229-230; 407-410 i 456-457, del *Tractat*, respectivament, a les pàgines 192; 288; 206; 209; 209, 209.

2.- Índex del Tractat d'Euler.

Atès que, com ja he dit, aquest article és solament un apunt, considero que val la pena recordar totes les qüestions que Euler analitza el en *Tractat*. I, atesa la claredat dels títols dels capítols, m'ha semblat que n'hi havia ben bé prou amb reproduir l'índex dels setze capítols.

Capítol	Títol	Paràgrafs	Pàgines
1	Dels nombres compostos	1–54	503–508
2	Dels nombres que són divisors	55–81	508–511
3	De la suma dels nombres divisors	82–110	511–514
4	Dels nombres primers i compostos entre si	111–139	515–518
5	Dels residus obtinguts per divisió	140–166	519–521
6	Dels residus, per divisió, dels termes d'una progressió aritmètica	167–191	521–523
7	Dels residus, per divisió, dels termes d'una progressió geomètrica	192–242	523–530
8	Dels potències dels nombres que, dividits per nombres primers, proporcionen la unitat	243–263	530–532
9	Dels divisors dels nombres de la forma $a^n \pm b^n$	264–283	533–535
10	Dels residus que s'obtenen, per divisió amb nombres primers, dels quadrats	284–369	535–546
11	Dels residus que s'obtenen, per divisió amb nombres primers, dels cubs	370–410	546–551
12	Dels residus que s'obtenen, per divisió amb nombres primers, dels biquadrats	411–461	552–558
13	Dels residus que s'obtenen, per divisió amb nombres primers dels supersòlids	462–500	558–563
14	Dels residus, per divisió amb nombres compostos [d=2(2p + 1)], dels quadrats	501–539	565–570
15	Dels divisors dels nombres de la forma $xx + yy$	540–569	570–573
16	Dels divisors dels nombres de la forma $xx + 2yy$	570–586	5736

3.- Comentaris succints.

Ara farem una anàlisi succinta comparativa dels sis primers capítols del *Tractat* i de les *Disquisicions* corresponents.

Capítol 1.

&13. *Introdueix els residus respecte d'un divisor a. Són els nombres més petits que a*:1, 2, *K*, *a*–1.

> **Comparar-ho amb *DA* &4 a**
> Cada nombre tindrà, doncs, un residu tant en la successió 0, 1, 2, 3*k*, *m*–1 com en la 0, –1, –2, –3*k*, –(*m*–1) els quals anomenarem els *residus mínims*; i és clar que, llevat que el residu fos 0, sempre se'n donen dos, un *positiu*, l'altre, *negatiu*.

&14 i **15**. Si $\alpha < a$, els nombres α, $a + \alpha$, $2a + \alpha$, $3a + \alpha$, $4a + \alpha$, etc. proporcionen el residu α, i tots els nombres $a - \alpha$, $2a - \alpha$, $3a - \alpha$, $4a - \alpha$, etc. proporcionen el mateix residu $-\alpha$.

&16. Tot nombre *b* o és múltiple de *a* o $b < a$, o es troba entre dos múltiples consecutius de *a*. És a dir, $ka < b < (K + 1)a$.

> **Comparar-ho amb *DA* &3**
> TEOREMA. *Proposats m nombres enters consecutius, a, a+1, a+2, K, a+m – 1 i un altre A un i solament un d'aquells serà congru amb aquest segon segons el mòdul m.*

&31 i **32**. Introdueix els *nombres primers.*

&32. Recorda el *garbell d'Eratòstenes.*

&34. Recorda el *teorema d'Euclides*: Tot nombre factoritza en nombres primers.

&41. *Classifica* els nombres naturals d'acord amb el nombre de nombres primers –iguals o diferents– en què factoritzen. Aleshores diu:

Tot nombre es troba en una classe segons el nombre de primers en què factoritza.

> **Comparar-ho amb *DA* &16**
> TEOREMA. *Un nombre compost qualsevol només es pot descompondre en factors primers d'una sola manera.*

Observació. La demostració d'Euler, un xic fosca, és per *inducció incompleta*. Es basa en el *lema d'Euclides* que *enuncia*, com a *Text Afegit* [Ta], al capítol 4.[5] [Vegeu Ta4.]

> **Comparar-ho amb *DA* &13** TEOREMA **i &14**
> TEOREMA. *El producte de dos nombres positius menors que un nombre primer donat no es pot dividir per aquest primer.*
> *Si ni a ni b no es poden dividir per un nombre primer p, el producte ab tampoc no es podrà dividir per p.*

&53. Diu: "No hi ha cap llei per als nombres primers".

Capítol 2.

&76 i **77**. Compta, *per inducció*, el *nombre de divisors* d'un nombre natural.

> **Comparar-ho amb *DA* &17**
> D'aquí es pot derivar fàcilment, amb l'ajut del càlcul de combinacions que, si $A = a^\alpha b^\beta c^\gamma$ etc., on *a*, *b*, *c*, etc., designen [...] nombres primers diferents, A té $(\alpha + 1)(\beta + 1)(\gamma + 1)$ etc. divisors diferents, incloent-hi també 1 i A.

Capítol 3.

&82. Defineix la *funció suma*, $\int n$, dels divisors d'un nombre natural *n*. Ja l'havia definit a E152 i E176, coneguts per Gauss.

&96. N'estableix inductivament el *caràcter multiplicatiu*:

Si mcd(M, N) = 1, aleshores $\int(MxN) = \int Mx \int N$.

5 Són notes en les quals, en general, Euler ofereix alguns enunciats sense demostració.

&97–99. Estableix: Si p és primer i N arbitrari, aleshores $\int(p \times N) > p \times \int N$.

&107 i 108. Ho usa per caracteritzar els *nombres perfectes parells*, establint el recíproc del *teorema d'Euclides*.[6]

&109. Diu que els nombres perfectes *senars* han de ser necessàriament de la forma $(4n+1)^{4\lambda+1}\, PP$, on P és senar i $(4n+1)$ primer.

Observació. De tot això, a *DA*, no n'hi ha cap referència.

Capítol 4.

&111. Defineix els *nombres primers entre si.*

&115. Observa que, de nombres primers amb a, n'hi ha, com a màxim, $a-1$. Aleshores diu:

La tasca que val la pena fer és definir-los [comptar-los].

És a dir, introdueix la *funció* $\varphi(a)$ que compta la quantitat de nombres d, amb $1 < d < a$, primers amb a. És a dir,

$$\varphi(a) = \#\{d : 1 < d < a \text{ i } mcd(d, a) = 1\}$$

Després demostra el problema del &38 dels *DA*.

Comparar-ho amb *DA* &38

PROBLEMA. *Trobar quants nombres positius hi ha menors que un nombre positiu donat A i simultàniament primers amb ell.*

Després el demostra amb tres ítems que coincideixen amb els tres ítems &117, 124 i 133 del *Tractat* següents.

&117. Si p és primer, $\varphi(p) = p - 1$.

&124. Si p és primer, $\varphi(p^n) = p^{n-1}(p-1)$.

&133. Si $mcd(M, N) = 1$ aleshores $\varphi(MN) = \varphi(M)\varphi(N)$.

6 Vegeu EUCLIDES [III aC], llibre VIII, proposició 36, a VERA (1970), volum 1, 857-860.

Observació. La demostració d'Euler, basada en l'*indici*, és un simple *comptatge* i és molt diferent de la que ofereix a E271.

Textos afegits al marge. Són:

TA1 Si $mcd(A, B) = mcd(A, C) = 1$, aleshores $mcd(A, BC) = 1$.

Comparar-ho amb *DA* &13

TA2 Se n'obté el *lema d'Euclides*: Si p, és primer i divideix AB, aleshores p divideix A o B.

Comparar-ho amb *DA* &14

TA3 Si $mcd(A, B) = 1$, aleshores existeixen m, n que $mA - nB = k$, on k és arbitrari i, en particular, pot ser = 1.

Comparar-ho amb *DA* &27

[...] Però la congruència $ax \equiv \pm 1$, designat el mòdul per b, equival a l'equació indeterminada $ax \equiv by \pm 1$, i, certament, la manera en què aquesta s'hauria de resoldre és prou coneguda actualment.

TA4 Si $mcd(A, B) = 1$, aleshores $mcd(A^n, B^n) = 1$.

TA5 Si $mcd(A, B) = d$, aleshores $mcd\left(\frac{A}{d}, \frac{B}{d}\right) = 1$.

TA6 Si $mcd(A, B) = d$, aleshores existeix un múltiple de A que, dividit per B proporciona un nombre predeterminat C.

Capítol 5.

En aquest capítol, Euler, malgrat no introduir el concepte gaussià de *congruència mòdul d*, estableix *totes* les propietats bàsiques d'aquest concepte.

&140. El concepte de *residu* d'un nombre natural N quan el dividim per un divisor d.

Comparar-ho amb *DA* &1
Si el nombre a divideix la diferència dels nombres b, c, es diu que b i c són *congrus segons a*, si no, *incongrus*; anomenem *mòdul* aquest a. En el primer cas, cadascun dels nombres b, c, és anomenat un *residu* de l'altre; el segon, un *no-residu*.

&141 a 148. Un divisor d proporciona d *classes de nombres*, que es caracteritzen pel residu r que s'obté quan dividim els nombres naturals per d. Aquestes classes constitueixen una *partició*. Són:

$$md,\ md + 1,\ md + 2,\ md + K,\ md + (d-1)$$

Comparar-ho amb *DA* &3
TEOREMA. *Proposats m nombres enters positius, a, $a+1$, $a+2$, $a+K$, $a+m-1$ i un altre A, un i solament un d'aquells serà congru amb aquest segons el mòdul m.*

&150. Els nombres de la *classe r* són els termes de la *progressió aritmètica* r, $d + r$, $2d + r$, $3d + r$ etc., el *terme general* de la qual és contingut a la fórmula $md + r$, que anomena la classe r.

Comparar-ho amb *DA* &2
Tots els residus d'un nombre donat a segons el mòdul m estan continguts en la fórmula $a + km$, on k designa un nombre enter indeterminat.

&151 a **153**. Els residus $0 < r < d - 1$ són els *residus propis*. Podem acceptar els *residus negatius* sempre que $|r| \le \frac{1}{2}d$.

Comparar-ho amb *DA* &4
[...] Si, no tenint respecte al signe, les magnituds són diferentes, un serà $< \frac{m}{2}$; si d'altra manera, tots dos $= \frac{m}{2}$. D'on és clar que qualsevol nombre té un residu que no supera la meitat del mòdul, que s'anomenarà *[residu] mímim absolut*.

Aleshores Euler estableix les propietats bàsiques de les classes que manifesten la *compatibilitat* dels residus amb les operacions aritmètiques. Són:

&159. La *classe suma de dues classes* és la del *residu suma* dels residus sumands, un cop reduïts.

Comparar-ho amb *DA* &6
Si es tenen tants nombres A, B, C, etc., com tants altres a, b, c, etc., congrus a aquells segons un mòdul qualsevol, $A \equiv a$, $B \equiv b$, $C \equiv c$, etc., serà

$$A + B + C + etc. \equiv a + b + c + etc.$$

&160. La *classe diferència de dues classes* és la del *residu diferència* dels residus sumands, un cop reduïts.

Comparar-ho amb *DA* &6
Si $A \equiv a, B \equiv b$, serà $A - B \equiv a - b$.

Corol·lari. Dues classes r_1 i r_2 són la mateixa si [, i només si,] la diferència dels seus membres és divisible per d.

Comparar-ho amb *DA* &1 i &5
[*DA*, 1, veure el comentari a &140.]
Nombres congrus tenen els mateixos residus mínims; incongrus, diferents.

&162 i **163**. La *classe producte de dues classes* és la del *residu producte* dels residus dels factors, un cop reduïts.

Euler el demostra.

Si poso el divisor = d, al nombre A li correspon el residu α i al nombre B li correspon el residu β, al producte AB li convé el residu $\alpha\beta$, el qual si fos més gran que el divisor d, el redueixo a $\alpha\beta - d$, o bé $\alpha\beta - md$.

Si tenim que $A = md + \alpha$ i $B = nd + \beta$, fem el producte

$$AB = mnd^2 + (m\beta + n\alpha)d + \alpha\beta,$$

del qual les dues parts primeres són divisibles per d. Per tant la darrera proporciona el residu buscat.

Comparar-ho amb *DA* &7 i &8
Si $A \equiv a$ també serà $kA \equiv ka$

Si k és un nombre positiu, això només és un cas particular de la proposició de l'article precedent, posant allà $A = B = C$ etc. Si k és negatiu, $-k$ serà positiu, de manera que $-(kA) \equiv -(kB)$, d'on $kA \equiv kB$.

Si $A \equiv a$, $B \equiv b$ serà $AB \equiv ab$. Efectivament, $AB \equiv Ab \equiv ab$.

Si tenim tants nombres A ,B, C, etc., com tants altres a, b, c, etc., congrus a aquests, $A \equiv a$, $B \equiv b$, $C \equiv c$, etc. , els productes dels uns i dels altres seran congrus;

$$ABC \text{ etc.} \equiv abc \text{ etc.}$$

&164 a **166**. Val per a la *potència* k-èsima d'una classe. Obté: Si el nombre A, dividit per d, proporciona el residu α, el seu quadrat A^2, el residu α^2, el seu cub A^3, el residu α^3 i, en general, la potència A^n, dividida per d, proporcionarà el residu α^n, un cop l'hàgim reduït al mínim.

Corol·lari important. Si $A - \alpha$ és divisible per d, $A^n - \alpha^n$ també.

Comparar-ho amb *DA* &8
Si tots els membres A, B, C, etc. es prenen iguals, i també els corresponents a, b, c, etc., es té aquest teorema: *Si $A \equiv a$, i k és un enter positiu, serà $A^k \equiv a^k$*

En un afegit enuncia els resultats següents:

tA7 Si a i b tenen el mateix residu, r, na i nb tenen residu nr.

Comparar-ho amb *DA* &7

tA8 Si a i b tenen el mateix residu r, aquest hereta els divisors comuns de a i b, i recíprocament, els de b i r, ho són de a.

tA9 Si a i b són primers entre si i $a > b$, serà $a = mb + p$; i $b > p$, aleshores també $b = np + q$ i $p > q$, i així fins assolir la unitat. És a dir, Euler recorda l'*algorisme d'Euclides* quan a i b són primers entre si.

Comparar-ho amb *DA* &27
[Vegeu tA3.]

Capítol 6.

En aquest capítol, Euler estudia els termes de la *progressió aritmètica* $a + mb$ quan els dividim per un divisor d, quelcom que ja ha fet a E271.

Distingeix dos casos:

(1) Segons que $mcd(a, b) = 1$, o bé
(2) $mcd(a, b) > 1$.

&169. Observa que els *residus es repeteixen* quan $d \mid mb$, quelcom que passa, almenys, quan $m = \lambda d$. Per tant, el nombres de residus diferents possibles és *sempre* $\leq d$, si considerem també el residu $d = 0$.

De fet, un cop s'ha assolit el primer valor m que $d \mid mb$, els residus es repeteixen.

&173 a **175**. Si $mcd(a, b) = 1$, aleshores $(a + mb)_{0<m<d}$, dividit per d, proporciona d residus diferents. Són 0, 1, 2, K, d–1, en un cert ordre que es repeteix.

Comparar-ho amb *DA* &24
L'expressió $ax + b$, on a, b, denoten nombres donats, x un nombre indeterminat, o sigui, una variable, *pot resultar còngrua, segons un mòdul m primer amb a, a qualsevol nombre donat.*

&176. Hi ha, doncs, un terme $a + mb$ que proporciona un múltiple de d.

Comparar-ho amb *DA* &26
I així, per l'article 24, una congruència de primer grau $ax + b \equiv c$ sempre és resoluble quan el mòdul és primer amb a.

&178. Hi ha també un terme $a + nb$, amb $0 < n < d$ que, dividit per d, dóna 1.

Òbviament, si $mcd(a, b) = 1$, hi ha un $0 < p < d$ que pb, dividit per d, dóna 1. En efecte, el terme $(n - m)b$, dividit perd d, dóna 1. I, per tant, no hi ha res més a dir.

Si $d \mid (a + mb)$, amb $m < d$, aleshores $a + (m + 1)b$ i $a + (m - 1)b$, dividits per d, donen, respectivament, b i $-b$.

Comparar-ho amb *DA* &27 i &30 *Exemple*
Resta que afegim quelcom de com cal trobar la solució d'una congruència d'aquest tipus. Obser-vem, en primer lloc, que una congruència de la forma $ax + t \equiv u$, el mòdul de la qual suposem primer amb a, depèn de la $ax \equiv \pm 1$; en efecte, si $x \equiv r$ satisfà aquesta, $x \equiv \pm(u - t)r$ satisfarà aquella. Però la congruència $ax \equiv \pm 1$, designat el mòdul per b, equival a l'equació indeterminada $ax \equiv by \pm 1$, i, certament, la manera en què aquesta s'hauria de resoldre és prou coneguda actualment.

Exemple. Si es proposa la congruència $19x \equiv 1(mòd.140)$, es resol primer segons el mòdul 2, i serà $x \equiv 1(mòd.2)$. Es posa $x \equiv 1 + 2x'$, i resultarà $38x' \equiv -18(mòd.140)$, a la qual equival $19x' \equiv -9(mòd.70)$. Si aquesta és resolta novament segons el mòdul 2, resulta $x \equiv 1(mòd.2)$, i, posat $x' \equiv 1 + 2x''$, resulta $38x'' \equiv -28(mòd.70)$, o sigui $19x'' \equiv -14(mòd.35)$. Resolta aquesta segons 5, dóna $x'' \equiv 4(mòd.5)$, o sigui $x'' \equiv 4 + 5x'''$, i substituint-la, resulta $95x''' \equiv -90(mòd.35)$, o sigui $19x''' \equiv -18(mòd.7)$.
Finalment, d'aquesta se segueix $x''' \equiv 2(mòd.7)$, i, posat $x''' \equiv 2 + 7x^{iv}$, finalment es conclou que $x \equiv 59 + 140x^{iv}$; per tant, $x \equiv 59(mòd.140)$ és la solució completa de la congruència proposada.

&179. Coneguts m i p, és fàcil determinar els valors els residus dels quals són 2, 3, k. Són: $a + (m + p)b$, $a + (m + 2p)b$,...

&183. Observa que la manera de determinar el valor p s'aconsegueix resolent l'equació indeterminada .

Comparar-ho amb *DA* &27
[Vegeu el comentari de &178.]

És un resultat realment notable perquè, amb els del capítol 5, estableix que, quan d és primer, els residus es comporten algèbricament com els nombres racionals, i no solament com els nombres enters.

&187 a **&191**. Després analitza el cas $d = D\varphi$, $b = B\varphi$, on $\varphi = mcd(b, d)$. Cal tractar el cas en el qual la diferència de la progressió aritmètica és B i el

divisor D. Aleshores tindrem els D residus 0, 1, 2, K, D–1. D'aquí que el cas inicial proporcioni solament els residus 0, φ, 2φ, $K\varphi$, $(D–1)\varphi$.

És a dir, EULER redueix aquest cas al cas anterior, dividint prèviament b i d pel màxim comú divisor φ. La resta és una conseqüència immediata dels paràgrafs anteriors, convenientment adaptats.

4.- Comentaris finals.

Fins aquí –amb l'anàlisi dels sis primers capítols del text d'Euler– hem vist que hi ha una certa coincidència amb els paràgrafs && 1, 2, 3, 4, 5, 6 ,7, 8 , 13, 14, 16, 17, 24, 26, 27, 30 i 38 dels *DA*. Aquest text, molt elaborat i autocontingut, usa paràgrafs intermedis per connectar d'una manera metodològica formal gairebé impecable tots els enunciats. El text d'Euler, en canvi, és un text molt menys precís i, com és força usual en el matemàtic suís, elaborat amb una metodologia *genètica*, usant la dicotomia hilbertiana.

És realment una pena que Euler no retornés sobre aquest text, incorporant-hi d'una manera més elaborada els "afegits" i estructurant-lo d'una forma més coherent. Aquesta és una tasca que podem fer, tanmateix, nosaltres emprant els seus articles –de cada tema el més general i més acabat. S'obté aleshores una perspectiva molt més acurada de les aportacions d'EULER.

En aquest text, a més, solament m'he fixat en els sis primers capítols. A partir del setè Euler s'interessarà pels *residus quadràtics* –i també pels cúbics i els quàrtics– i mirarà de resoldre els dos problemes que menen al *teorema fonamental* –en la terminologia de Gauss–; és a dir, el *teorema de reciprocitat quadràtica*. Aquests problemes són:

(1) Quins nombres primers p admeten una representació quadràtica –és a dir, són de la forma $p = a^2 + kb^2$, amb a, b, primers entre si?
(2) Com són els nombres primers p que divideixen una forma del tipus $a^2 + kb^2$, $k = 2, 3$?

Certament que aquesta qüestió està molt ben tractada en els textos COX, (1989), capítol primer, i KNOEBEL; LAUBENBACHER; LODDER; PENGELLEY (2007), capítol quart. Tanmateix, com ja he dit abans, no estan vinculats al *Tractat* sinó al desenvolupament conceptual global del pensament d'Euler

en relació amb aquesta qüestió –les *formes quadràtiques*– que tant de fruit van produir en l'obra de Lagrange, Legendre i, sobretot, Gauss.

No sembla, doncs, que no tingui interès acabar l'anàlisi del *Tractat* i la comparació amb els *DA* i en això estic dedicant una part del temps. Aquestes pàgines són una primera aproximació a allò que es pot aconseguir.

5. Bibliografia

Bibliografia primària.

EULER, Leonhard (1750-51) "De nvmeris amicabilvs", *Opuscula varii argumentii*, volum *2* (1950), 23-107. [E152].

EULER, Leonhard (1750-51) "Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs", *Commentationes arithmeticae collectae*, vol. *2* (1849), 639-647. [E176].

EULER, Leonhard (1760-61) "Theoremata arithmetica nova methodo demonstrata", *Novi Commentarii academiae scientiarum Petropolitanae*, vol. *8* (1763), 74-104. [E271].

EULER, Leonhard (1758) "De resolvtione formvlarvm quadricarvm indeterminatarvm per nvmeros integros", *Novi Commentarii academiae scientiarum Petropolitanae*, *9* (1760), 3-39. [E279].

EULER, Leonhard (1748-1750) "Tractatus de nvmerorvm doctrina capita sedecim quae svpersvunt", *Commentationes arithmetiae collectae*, *2* (1849), 503-75. [E792].

GAUSS, Carl Friedrich (1801) *Disquisitiones Arithmeticae*, Lipsiae, Gerhard Fleisher. Traducció catalana de Griselda PASCUAL. Barcelona, Societat Catalana de Matemàtiques, 1996.

LEGENDRE, Adrien-Marie (1798) *Essai d'une Thérie des nombres* (1798), París. Firmin-Didot. Reeditat a París, Librairie Scientifique et Technique Albert Blanchard, 1955.

Bibliografia secundària.

COX, David A. (1989) *Primes of the Form $x^2 + ny^2$*, Nova York, John Wiley & Sons, Inc.

DICKSON, Leonard Eugene (1919) *History of the Theory of Numbers*, Tres volums, Washington, D.C. Carnegie Institute of Washington. Reeditats a Nova York, Dover Publications, Inc. 2005.

DUNHAM, William (1999) *Euler. Tha Master of Us All*, Washington, D.C., The Mathematical Association of America. N'existeix una traducció castellana a la col·lecció *La Matemática en sus personajes*, Madrid, Nívola.

DUNHAM, William (editor) (2007) *The Genius of Euler*. *Reflections on His Life and Work*, Washington, D.C., The Mathematical Association of America.

KNOEBEL, Arthur; LAUBENBACHER, Reinhard; LODDER, Jerry; PENGELLEY, David (2007) *Mathematical Masterpieces. Further Chronicles by the Explorers*, Nova York, Springer.

LEMMERMEYER, Franz (1991) *Reciprocity Laws,* Nova York, Springer.

SANDIFER, C. Edward (2007a) *The Early Mathematics of Leonhard Euler*, Washington, D.C., The Mathematical Association of America.

SANDIFER, C. Edward (2007b) *How Euler Did It*, Washington, D.C., The Mathematical Association of America.

VARDARAJAN, V.S. (2006) *Euler Through Time: A New Look at Old Themes*, Nova York, American Mathematical Society.

WEIL, André (1984) *Number Theory: An Approach through History from Hammurapi to Legendre*, Boston, Birkhäuser Verlag.