VARIAE OBSERVATIONES CIRCA SERIES INFINITAS

En el 2^{0n} centenari de la mort de Leonhard Euler

per

PILAR BÀYER I ISANT

Professora de la Facultat de Matemàtiques,
Universitat de Barcelona

1. INTRODUCCIÓ

Quan hom intenta copsar la importància de l'obra de LEONHARD EULER (1707-1783) en àrees com la Teoria de Nombres o l'Àlgebra, cal tenir present que, en l'època d'EULER, aquestes branques de la Matemtica tot just estaven emergint de llur *"prehistòria"* i tenien, per tant, un caràcter moltes vegades experimental.

L'*Aritmètica* de DIOFANT D'ALEXANDRIA, per exemple, malgrat les traduccions que en feren en el món àrab, romangué ignorada a Europa fins a la segona meitat delsegle XV, i no fou fins a entrat el segle XVII que comptà amb un lector creatiu: FERMAT.

Hom pot dir que EULER fou el següent estudiós de l'obra de DIOFANT. EULER, partint de les moltes vegades enigmàtiques afirmacions de FERMAT, descrobrí multitud de propietats remarcables dels nombres enters, preparant d'una manera admirable el naixement de les *Disquisitiones Arithmeticae* de GAUSS.

Centenars i centenars d'equacions diofàntiques tractades per ell constitueixen la base de l'estudi de les formes quadràtiques, de les formes de graù superior, de les corbes el·líptiques i de nombroses recerques en Geometria algèbrica, que arriben fins als nostres dies.

Però potser el mèrit més gran d'EULER en el marc de l'Aritmètica ha d'ésser situat en el fet indiscutible que fou l'iniciador de la Teoria Analítica de Nombres. Les seves manipulacions amb sèries divergents, plenes de coratge, li permeteren intuir lligams profunds entre propietats en aparecça purament analítiques i d'altres en aparença purament algèbriques. El temps i l'esforç de nombrosos matemàtics: LEGENDRE, GAUSS, DIRICHLET, ABEL, JACOBI, KUMMER, RIEMANN, DEDEKIND, RAMANUJAN, HILBERT, HADAMARD, TAKAGI, HECKE, SIEGEL, ARTIN, WEIL, SHIMURA, IWASAWA, GROTHENDIECK, SERRE, DELIGNE, etc., feren la resta.

L'any 1770 EULER publicà el seu *Vollständige Anleitung zur Algebra*, un text certament elemental. Aquest text, junt amb la memòria de LAGRANGE *Réflexions sur la résolution algébrique des équations* (1770), el tractat de *Théorie des nombres* de LEGENDRE (1798), *les Disquisitiones Arithmeticae* de GAUSS (1801) i *la Zahlentheorie* de DIRICHLET-DEDEKIND (1863) formen el nucli de l'Àlgebra que era coneguda abans que el món matemàtic fos enriquit amb les idees de GALOIS.

Molts dels temes tractats o, millor dit, iniciats per EULER no disposaren d'un llenguatge escaient fins ben entrat el segle dinou.

2. CONTRIBUCIONS A LA TEORIA ELEMENTAL DE NOMBRES

2.1. *La descoberta per Euler del vuitè nombre perfecte*

Els grecs anomenaren perfectes els nombres que, com el 6 = 1 + 2 + 3, coincidien amb la suma de llurs parts alíquotes. Si escrivim en base dos els quatre primers nombres perfectes, coneguts ja per l'escola pitagòrica, obtenim:

	Representació decimal	*Representació binària*
P_1	6	110
P_2	28	11100
P_3	496	111110000
P_4	8128	1111111000000

i veiem, per tant, que tots són de la forma

$$2^{n-1}(1 + 2 + 4 + \ldots + 2^{n-1}) = 2^{n-1}(2^n - 1).$$

El problema, no resolt encara avui dia, de saber si existeix una infinitat de nombres perfectes és plantejat des de la matemàtica grega, i és, probablement, en gran part responsable del rigorós estudi de la divisibilitat que fa EUCLIDES en els seus *Elements*.

En el llibre IX dels *Elements* (v. [7]), EUCLIDES demostrà que tots els nombres de la forma $2^{n-1}(2^n-1)$ són perfectes, sempre que 2^n-1 sigui un nombre primer. En aquest mateix llibre EUCLIDES prova que, de nombres primers, n'existeix una infinitat.

El següent nombre perfecte $P_5 = 2^{12}(2^{13}-1) = 33.550.336$ no fou trobat fins al segle XV. CATALDI (1548-1626) allargà la llista de nombres perfectes amb dues unitats més: $P_6 = 2^{16}(2^{17}-1) = 8.589.869.056$, $P_7 = 2^{18}(2^{19}-1)$, i demostrà que tot nombre perfecte del tipus assenyalat per EUCLIDES acabava o bé amb 6 o bé amb 8.

En una carta a MERSENNE, datada el 1640, FERMAT féu tres afirmacions que considerà bàsiques per a la descoberta de nombres perfectes, i que digué que havia provat fent un esforç considerable. Aquestes eren:

1) Perquè 2^n-1 fos un nombre primer, calia que n fos primer.

2) Si p era un nombre primer, 2^p-2 era divisible per p.

3) Si 2^p-1 era compost, per a un p primer, els seus divisors propis eren del tipus $2\,kp+1$ (Per exemple $2^{11}-1 = 23\cdot 89$, el 47 divideix $2^{23}-1$ i el 223 divideix $2^{37}-1$).

Els nombres $M_p = 2^p-1$, amb p primer, són anomenats des de llavors nombres de MERSENNE.

Poc temps després, en una carta a FRENICLE DE BESSY, FERMAT afirmà que tenia una demostració del fet que, per a tot primer p i tot enter x no divisible per p, el nombre $x^{p-1}-1$ era sempre divisible per p, generalitzant així l'afirmació feta en el cas $x = 2$. Aquesta proposició és la que ha arribat als nostres dies amb el nom de *petit teorema de Fermat*. De FERMAT, però, hom no en coneix cap prova.

EULER s'interessà pel problema dels nombres perfectes durant tota la seva vida. En un treball de l'any 1732 (v. [2]) s'adonà que, si $p = 4\,m-1$ i $q = 8\,m-1$ eren primers, llavors $2^p-1 = 2^{(q-1)/2}-1$ era divisible per q; obtingué per mitjà d'aquest resultat que els nombres de MERSENNE eren compostos pels valors de p = 11, 23, 83, 131, 179, 191, 239, etc. Com que, segons observà, $223 \mid M_{37}$, 431

$|M_{43}$, 1103 $|M_{29}$ i 439 $|M_{73}$, conjecturà Euler en aquest treball que, a part dels casos esmentats, per tot altre primer $p < 50$, $2^{p-1} M_p$ era perfecte. (Posteriorment Euler afegí a la relació anterior de nombres de Mersenne compostos el M_{41} i el M_{47}). Euler justificà axí les seves afirmacions:

> *Deduxi has observationes ex theoremate quodam non ineleganti, cuius quidem demonstrationem quoque non habeo, verum tamen de eius veritate sum certissimus. Theorema hoc est: $a^n - b^n$ semper potest dividi per $n + 1$, si $n + 1$ fuerit numerus primus atque a et b non possint per eum dividi; eo autem difficiliorem puto eius demonstrationem esse, quia non est verum, nisi $n + 1$ sit numerus primus.*

El 1736 (v. [4]) Euler donà per primera vegada una demostració del petit teorema de Fermat. La demostració d'Euler en aquella ocasió fou la següent: donat un primer p, hom té que

$$2^p = (1 + 1)^p = 1 + p + \frac{p(p-1)}{2 \cdot 1} + \ldots + p + 1 = 2 + kp,$$

$$3^p = (1 + 2)^p = 1 + mp + 2^p,$$

$$3^p - 3 - (2^p - 2) = mp,$$

$$(i + a)^p = 1 + np + a^p,$$

$$(1 + a)^p - (1 + a) - (a^p - a) = np.$$

Per tant, si $a^p - a$ és divisible per p, també ho seran $(a + 1)^p - (a + 1), \ldots, (a + b)^p - (a + b)$. Com que per $a = 2$, $2^p - 2$ és divisible per p, per tot nombre x, posant $x = 2 + b$, l'expressió $x^p - x$ serà divisible per p.

El 1747 (v. [7]) Euler provà que, si $2^p - 1$ era compost, per un p primer, llavors els seus divisors propis tenien, efectivament, la forma predita per Fermat. El seu raonament fou el següent: si q és un divisor primer de $2^p - 1$, com que mcd $(2 - 1, 2^{q-1} - 1) = 2^g - 1$, on $g = \text{mcd}(p, q-1)$ i que divideix sempre $2^{q-1} - 1$, caldrà que sigui $q > 1$; però com que p és primer, cal que $p \mid q-1$. És a dir, $q = sp + 1$, però s cal que sigui parell, degut al fet que q és primer.

Fent ús novament del petit teorema de FERMAT el resultat anterior pot ésser refinat; hom pot veure així que tot divisor de M_p, per $p > 2$, és del tipus $8\,k \pm 1$ (cf. [34], Ch. 1, Th. 19).

En una carta a BERNOULLI escrita el 1772, EULER li comunicà que havia pogut establir el caràcter primer del M_{31} i, per tant, que $P_8 = 2^{30}\,M_{31}$ era el vuitè nombre perfecte. Per això EULER havia examinat tots els primers dels tipus 248 + 1 i 248 n + 63 més petits que 46.339.

Per veure fins a quin punt l'ús del petit teorema de FERMAT facilità la recerca d'aquest nombre perfecte podem fer el següent càlcul. Posem $M_p = 2^p - 1$ i $s_p = [\sqrt{M_p}]$.

Siguin $c_p = \pi(s_p)$ el nombre de primers més petits o iguals que s_p, $f_p = \pi_{2p,1}(s_p)$ el de primers més petits o iguals que s_p continguts a la progressió aritmètica $\{1 + t\,2\,p\}$, i e_p el nombre de primers de la forma anterior que, a més, poden ésser escrits com $8\,k \pm 1$. D'entrada, el nombre de divisions que EULER hauria necessitat per a establir el caràcter primer del M_{31} hauria estat $c_{31} = \pi(46.340) = 4.792$. El treball del 1747 li permetia limitar-se a un total de $f_{31} = 157$ divisions, mentre que en el procediment que finalment seguí li'n bastaren

$$e_{31} = \pi_{248,1}(s_{31}) + \pi_{248,63}(s_{31}) = 84.$$

Avui dia, en què la tasca de fer operacions ha esdevingut quelcom més fàcil, hom coneix un total de vint-i-set nombres perfectes. El darrer correspon al valor $p = 132.049$.

En el treball [14], publicat el 1760, EULER donà la cèlebre generalització del petit teorema de FERMAT. El teorema 10 d'aquest treball diu exactament:

> *Exponens minimæ potestatis χ^υ, quæ per numerum N ad χ primum divisa unitatem relinquit, vel est æqualis numero partium ad N primarum vel huius numeri semissis aliave eius pars aliquota.*

Escrivim, d'acord amb la notació introduïda per GAUSS en *les Disquisitiones,* φ (N) per indicar el nombre d'enters positius primers amb N més petits que N. En el mateix treball, EULER prova, a més a més, que φ és una funció multiplicativa, que $\varphi(p^m) = p^{m-1}(p-1)$, per un p primer, i obté, per tant, el valor de φ per a qualsevol nombre natural. Val a dir, però, que la relació

$$\sum_{d|N} \varphi(d) = N$$

és deguda a GAUSS.

Amb relació amb el petit teorema de FERMAT, seria injust no fer esment d'una demostració donada per LEIBNIZ, car és anterior a la d'EULER. L'any 1894, G. CACCA trobà a la Biblioteca de Hannover uns manuscrits de LEIBNIZ, anteriors al 1683, en els quals aquest matemàtic provava així l'esmentat resultat: sigui $x = a + b + c \ldots$, i sigui p un primer. Llavors cada coeficient multinomial que apareix en el càlcul de $x^p - \Sigma a^p$ és divisible per p; posant $a = b = c \ldots = 1$ veiem que $x^p - x$ és múltiple de p, per tot enter x.

Si bé a l'Aritmètica de NICÒMAC (~ 100 a. de C.) hom ja afirma que tot nombre perfecte és del tipus trobat per EUCLIDES, no fou fins a un treball pòstum d'EULER [19] que fou demostrat que tot nombre perfecte *parell* era de la forma $2^{p-1}(2^p - 1)$.

En un altre treball pòstum [20] EULER demostrà així mateix que, si existís un nombre perfecte imparell, aquest seria del tipus

$$q^{4d+1} p_1^{2\alpha_1} \ldots p_s^{2\alpha_s}, \text{ on els } p_i \ (1 \leq i \leq s)$$

són nombres primers diferents de 2, i q és un primer de la forma $4n + 1$.

Fins avui hom no ha trobat cap nombre perfecte imparell. Se sap, però, que no n'hi ha cap de més petit que 10^{50}.

2.2 *Nombres de Fermat. Arrels primitives*

> *Cum autem numeros a binario quadratice in se ductos et unitate auctos esse semper numeros primos apud me cons-*

tet et iam dudum Analystis illius theorematis veritas fuerit significata, nempe esse primos 3, 5, 17, 257, 65537, etc. in infinit, nullo negotio etc."

P. DE FERMAT, [16].

Els anomenats nombres de FERMAT són els de la forma $F_n = 2^{2^n} + 1$. Amb $0 \leq n \leq 4$ aquests nombres són primers. En una carta a FRENICLE, datada el 1640, FERMAT afirmà la seva creença que tots aquests nombres serien primers, si bé aquest cop admeté que, d'quest resultat, no en tenia cap demostració. El 1654 demanà a PASCAL que s'encarregués de l'estudi d'aquesta qüestió.

GOLDBACH, en una carta a EULER de l'any 1729, cridà l'atenció d'aquest sobre la conjectura de FERMAT. EULER demostrà primerament que si a, b eren nombres enters primers entre ells, llavors tot divisor de $a^{2^n} + b^{2^n}$ o bé era 2, o bé tenia la forma $2^{n+1}k + 1$. Així tot factor del F_5 seria del tipus $64k + 1$; fent $k = 10$ trobà la descomposició (v. [2])

$$F_5 = 2^{32} + 1 = 641 \cdot 6700417,$$

contradint d'aquesta manera l'afirmació feta per FERMAT.

Fins avui hom no ha trobat cap altre nombre de FERMAT primer. Com sabem, aquests nombres intervenen en les construccions amb regle i compàs per mitjà del resultat, descobert i provat per GAUSS, que diu que un polígon de F_n costats podia ésser construït amb regle i compàs quan F_n era primer. GAUSS afirmà, sense donar-ne demostració, que el recíproc era també cert: perquè un polígon de m costats fosconstruíble, calia que m fos producte d'una potència de dos per primers del tipus F_n, dos a dos diferents.

La demostració esmentada de GAUSS és basada en l'estudi dels períodes de les equacions ciclotòmiques. En la introducció de l'Art. 7 de les *Disquisitiones*, GAUSS afirma que els principis de la seva teoria s'apliquen no solament a les funcions circulars (sin, cos, etc.) *"sed pari successu ad multas alias functiones transcendentes applicari possunt, e.g. ad eas quæ ab integrali*

$$\int \frac{dx}{\sqrt{1-x^4}}$$

pendent". Vint-i-cinc anys després, ABEL i JACOBI donaren un fort impuls a l'estudi de les funcions el·líptiques. Amb aquests mitjans, ABEL provà en els números 2 i 3 del Journal de Crelle el resultat intuït per GAUSS: Si $m = 2^a p_1 \cdot \ldots \cdot p_t$, on p_i ($1 \leq i \leq t$) són primers de FERMAT dos a dos diferents, llavors la lemniscata podia ésser dividida en m parts iguals fent ús del regle i el compàs. (Aquest teorema té també una estreta relació amb l'estudi de les extensioins "abelianes"). El recíproc del teorema d'ABEL, així com el de GAUSS, és tanmateix cert. ROSEN [32] n'ha publicat recentment una demostració. L'article de ROSEN constitueix una deliciosa introducció a l'estudi de l'aritmètica de les corbes el·líptiques.

Una altra contribució destacable d'EULER en el camp de la Teoria elemental de Nombres és la relacionada amb el Teorema de WILSON. E. WARING, l'any 1770, fou el primer d'enunciar que $1 + (p - 1)!$ era sempre divisible per p, atribuint aquesta descoberta a SIR JOHN WILSON (1741-1793). No obstant això, en els manuscrits de LEIBNITZ abans esmentats, hom hi troba també una afirmació equivalent. El primer de publicar una demostració del teorema de WILSON fou LAGRANGE, derivant-lo del petit teorema de FERMAT. El 1773 EULER publicà una demostració del teorema de WILSON que, si bé no és del tot completa, és molt interessant. EULER fa ús, per primera vegada en aquesta demostració, de l'existència d'una arrel primitiva mòdul p (amb el llenguatge actual, d'un generador del grup cíclic F_p^*). Aquest concepte havia estat introduït per LAMBERT;la denominació d'arrel primitiva és deguda a EULER,però la demostració de la seva existència per EULER fou defectuosa. Suposant provat que una tal arrel a existia, EULER procedí com segueix per demostrar el teorema de WILSON: quan dividim $1, a, a^2, \ldots, a^{p-2}$ per p, les restes que obtenim són $1, 2, 3, \ldots, p-1$, en un determinat ordre. Així $a^{(-1)(p-2)/2}$ tindrà la mateixa reta mòdul p que $(p-1)!$ Sigui $p > 2$, i posem $p = 2n + 1$. Com que la resta de a^n és -1, llavors $a^n a^{2n(n-1)}$ i per tant $(p - 1)!$ tenen resta $- 1$.

El 1772 EULER afirmà que no coneixia cap regla per al càlcul general d'arrels primitives, però donà una taula amb totes les arrels primitives de p, amb p primer ≤ 41.

En les *Disquisitions Arithmeticæ* GAUSS donà dues demostracions de l'existència d'arrels primitives per un mòdul p primer i veié que, donat un mòdul m, aquest admetia arrels primitives si i només si $m = 2, 4, p^{\alpha}$ o bé $2\,p^{\alpha}$, amb p primer imparell.

Un resultat curiós és que si $F_n = 2^{2^n} + 1$ és primer ($n \geq 1$), llavors el 3 és una arrel primitiva per a F_n.

Una conjectura no demostrada d'E. ARTIN afirma que tot enter $a \ddagger -1$, no quadrat, és una arrel primitiva per a infinits primers. Una forma més precisa d'aquesta conjectura, deguda també a ARTIN, diu que si $a \ddagger b^n$, per $n > 1$, i si $\upsilon_a(N)$ indica el nombre de primers $\leqslant N$ per als quals a és una arrel primitiva modul p, llavors

$$\upsilon_a(N) \sim 0.3739558\, \pi(N).$$

Com hem vist, $p \mid 2^{p-1} - 1$ sempre. Diguem de passada que la congruència $p^2 \mid 2^{p-1} - 1$ està lligada amb el primer cas del Teorema de FERMAT. Si examinem tots els primers $p < 100.000$ veurem que per tots, menys per $p = 1093$ i $p = 3511$, es verifica que $p^2\ 2^{p-1} - 1$. A. WIEFERICH demostrà l'any 1909 que, perquè l'equació $x^p + p^p = z^p$ tingués solucions enteres amb $p \times xyz$, calia que $p^2 \times 2^{p-1} - 1$. Fent servir aquest i d'altres criteris del mateix estil, D.H. i EMMA LEHMER provaren el 1941 que el primer cas del Teorema de FERMAT era cert per a tot primer $p < 253.747.889$.

2.3 *Aplicacions de les fraccions contínues*

Diversos problemes de l'*Aritmètica* de DIOFANT condueixen a l'estudi d'equacions del tipus $A\,x^2 + B\,x + C = y^2$. El cèlebre problema dels bous del Sol d'ARQUÍMEDES (v. [7]) porta també, en la seva anàlisi última, a l'estudi de l'equació $y^2 - A\,x^2 = 1$ amb $A = 4.7229.494$. En els segles VII i XII, BRAHMEGUPTA i BHÁSCARA, respectivament, feren diverses temptatives per resoldre l'equació $x^2 - A\,y^2 = 1$.

FERMAT, el 1657, afirmà que l'esmentada equació posseïa una infinitat de solucions enteres, i el 1659 digué que ho podia provar amb el seu mètode de descens. Desafià tanmateix amb aquest problema els matemàtics anglesos LORD BROUNCKER i JOHN WALLIS, els quals en donaren solucions parcials.

La idea de fer ús de les fraccions contínues per a atacar aquest problema sembla deguda a EULER. El 1759 EULER començà a ocupar-se de l'equació $x^2 - Ay^2 = 1$, anomenant-la equació de Pell, nom que ha perdurat fins als nostres dies. La idea d'EULER fou la següent: si (x, y) és una solució en els enters de l'equació $x^2 - A y^2 = 1$, llavors

$$\frac{x^2}{y^2} = A + \frac{1}{y^2},$$

per tant

$$\frac{x}{y} > \sqrt{A} \text{ i } \frac{x}{y} + \sqrt{A} > 2\sqrt{A}.$$

Si escrivim l'equació de Pell en la forma

$$\left(\frac{x}{y} - \sqrt{A}\right)\left(\frac{x}{y} + \sqrt{A}\right) = \frac{1}{y^2},$$

veiem que

$$\left|\frac{x}{y} - \sqrt{A}\right| = \frac{1}{y^2\left|\frac{x}{y} + \sqrt{A}\right|} < \frac{1}{2y^2\sqrt{A}},$$

és a dir, x/y cal que sigui una reduïda del desenvolupament en fracció contínua de $\sqrt{A}$.

De totes maneres, demostrar que una tal equació té sempre solucions enteres amb $y \neq 0$ no fou fet fins a LAGRANGE el 1770. Aquest teorema és, de fet, el primer cas conegut del teorema de DIRICHLET relatiu a l'existència d'elements unitaris en els cossos de nombres.

El 1737 EULER demostrà que e i e^2 eren irracionals, també mitjançant l'ús de les fraccions contínues. La fórmula remarcable descoberta per ell: $e^{ix} = \cos x + i \sin x$ (v. [8], Ch. VIII, § 138) li permeté d'obtenir la igualtat $e^{i\pi} = -1$, posant un lligam entre π i e que féu possible deduir moltes propietats de l'un d'aquest nombres en funció de les de l'altre. Així, el 1761 LAMBERT pogué provar la irracionalitat de π, la de e^x, i la de tg x, per $x \neq 0$ racional. El perfeccionament del mètode seguit per EULER i LAMBERT portà LIOUVILLE, el 1844, a la descoberta dels nombres transcendents.

Potser val la pena esmentar, de passada, que les notacions π, e, i i (per a representar la unitat imaginària) foren així mateix introduïdes per EULER.

3, 14159 26535 89793 23846 26433
83279 50288 41971 69399 37510
58209 74944 59230 78164 06286
20899 86280 34825 34211 70679
82148 08651 32723 06647 09384 46

Pour abréger j'écrirai π *au lieu de ce nombre, de sorte que* π = à la demi circonférence d'un cercle dont le rayon = 1.

L. EULER.

Des Quantités transcendantes qui naissent du Cercle [8], Ch. VIII, § 126.

2.4. *El cas n = 3 de l'equació de Fermat i altres equacions diofàntiques*

Es sey demnach p nich durch 3 theilbar und also unsere beyden Factoren

$$\frac{p}{4} \textit{ und } pp + 3\,qq$$

untheilbar unter sich, so müßte ein jeder für sich ein Cubus seyn. Laßt uns dahero pp + 3qq zu einem Cubo machen, welches geschieht wann man, wie oben gezeigt worden, setzt

$$p + q\sqrt{-3} = (t + u\sqrt{-3})^3 \text{ und}$$

$$p - q\sqrt{-3} = (t - u\sqrt{-3})^3.$$

Damit dadurch werde $pp + 3\,qq = (tt + 3\,uu)^3$ *und also ein Cubus.*

L. EULER
[16], Cap. 15, § 243.

Particularment interessant és l'estudi fet per EULER del cas $n = 3$ de l'equació de FERMAT $x^n + y^n = z^n$. Els càlculs que féu a fi de provar-hi la no existncia de solucions enteres el portaren a una equació diofàntica del tipus $p^2 + 3\,q^2 = r^3$. D'ací deduí EULER, sense donar-ne demostració (la frase "*wie oben gezeigt worden*" no s'ha acabat mai de comprendre) que calia que existissin enters t, u tals que

$$p + q\sqrt{-3} = (t + u\sqrt{-3})^3.$$

Sembla que Euler emprà, per a arribar a aquesta conclusió, certes propietats, de la divisibilitat a l'anell $Z[\sqrt{-3}]$. És en aquesta omissió d'EULER on es troba la idea germinal que conduí, primer KUMMER i després DEDEKIND, a l'estudi de l'aritmètica dels cossos de nombres (cf. [5]).

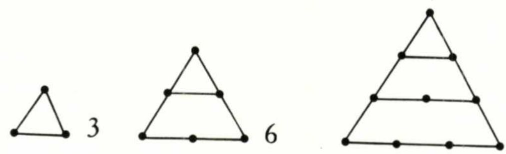
Les aportacions d'EULER a la resolució de les equacions diofàntiques foren constants al llarg de tota la seva vida. Resolgué problemes proposats per DIOFANT, com el següent: calcular tots els nombres racionals x, y, z per als quals $x\,y + x + y$, $x\,z + x + z$ i $y\,z + y + z$ són quadrats. Donà, per exemple, fórmules paramètriques per al càlcul de totes les solucions enteres d'equacions com $x^3 + y^3 = z^3 + w^3$, $x^4 + y^4 = z^4 + w^4$. Trobà totes les solucions enteres d'equacions del tipus $x^3 + A\,y^3 = B$, $y^2 = x^3 + k$, per valors particulars d'A, B i de k.

Casos particulars d'equacions diofàntiques de la forma $y^2 = 4\,x^3 - A\,x - B$, on A i B són racionals, també havien estat tractats per FERMAT. Ambdós matemàtics, EULER i FERMAT, sabien que si (a, b) i (c, d) eren punts racionals de la corba corresponent, la recta que els unia (o la tangent, si coincidien) tallava la corba novament en un punt racional. Partint d'un punt racional $x_1 = (a, b)$, hom obtenia d'aquesta manera un punt racional x^2, i el procés podia ésser iterat. EULER coneixia que, seguint aquest procediment, en certs casos hom obtenia una infinitat de punts racionals i, en certs altres, hom n'obtenia només un nombre finit, però no va saber pas com distingir-los per endavant!

2.5 *Aportacions d'Euler al programa de Bachet*

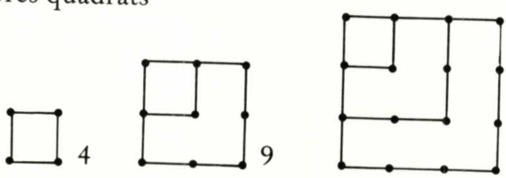
Als pitagòrics, moguts per llur interès pel concepte de nombre i per la geometria, hom deu la noció de nombre poligonal. Els nombres triangulars, quadrats, pentagonals, etc., són obtinguts tal com ho van indicant les figures:

Nombres triangulars



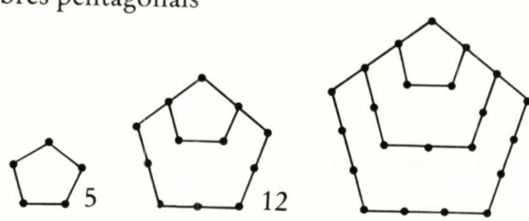
• 1 3 6 10 15 21 . . .

Nombres quadrats



• 1 4 9 16 25 36 . . .

Nombres pentagonals



• 1 5 12 22 35 51 . . .

En general, els nombres n-gonals vénen donats per les successives sumes dels termes d'una progressió aritmètica n – 2.

C.G. BACHET, editor de l'*Aritmètica de DIOFANT*, remarcà que aquest, en el llibre IV, 31, feia servir aparentment que tot enter era expressable com la suma de quatre quadrats. Ell mateix comprobà aquest resultat per tots els sencers ≤ 325, i en cridà l'atenció de FERMAT. FERMAT respongué així a BACHET:

> *Jo vaig ser el primer de descobrir el bell i general teorema que diu que tot nombre és, o bé triangular, o és suma de dos o de tres nombres triangulars; tot nombre és, o bé un quadrat, o és suma de dos, tres o quatre quadrats; tot nombre és, o bé pentagonal, o és suma de dos, tres, quatre o cinc nombres pentagonals; i així fins a l'infinit, tant si es tracta de nombres hexagonals, heptagonals o poligonals. Ací no en puc donar la demostració, puix que depèn de nombrosos i abstrusos misteris dels nombres; tinc, però, la intenció de dedicar un llibre sencer a aquest tema i portar a terme en aquesta part de l'aritmètica avenços espectaculars, que van més enllà dels límits coneguts fins ara.*

No cal dir, coneixent FERMAT, que el llibre no sortí mai.

EULER publicà nombrosos treballs sobre els nombres poligonals. El 1749, i després de set anys de temptatives, reeixí a provar el resultat, predit també per FERMAT, que tot nombre primer $p = 4n + 1$ era suma de dos quadrats.

El 1770 (cf. [11], II, Chap. VIII, p. 279), LAGRANGE, basantse en idees d'EULER, donà la primera demostració de l'anomenat teorema de BACHET, segons el qual tot enter n era suma de quatre quadrats.

Poc temps després EULER simplificà de manera considerable la demostració de LAGRANGE del teorema dels quatre quadrats i provà que el teorema per als nombres triangulars era equivalent al fet que tot enter $m = 8n + 3$ era suma de tres quadrats.

LEGENDRE afinà aquest resultat provant, el 1785, que tot enter que no fos del tipus $4^r(8n + 7)$ era suma de tres quadrats.

Pels voltants del 1754 EULER introduí la noció de resta quadràtica: un nombre a és anomenat una resta quadràtica mòdul p si existeix un enter x per al qual $x^2 - a$ és divisible per p. Fent ús dels símbols introduïts per LAGRANGE el 1808, això s'escriu:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{si a és resta quadràtica mòdul p} \\ -1 & \text{si no ho és,} \end{cases}$$

quan p és un primer que no divideix a.

El 1758 EULER obtingué el següent criteri: donat un primer p i un enter a no múltiple de p, llavors a

$$a^{\frac{1}{2}(p-1)} - 1$$

és divisible per p si i només a és resta quadràtica mòdul p, abreujadament:

$$a^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right) \ (\text{mòdul p}).$$

Usant propietats de les restes quadràtiques, concretament que

$$\left(\frac{-1}{p}\right) = +1 \ \text{ si } \ p = 4n + 1,$$

EULER donà en el seu *Opuscula Analytica* [18] una nova demostració del fet que tot primer p = 4 n + 1 era suma de dos quadrats. El treball [17] és particularment interessant, car EULER hi fa una afirmació que es deduïria de seguida de la llei de reciprocitat quadràtica, i que diu que no sap pas com demostrar:

> *Huius elegantissimi theorematis demonstratio adhuc desideratur, postquam a pluribus iamdudum frustra est investigata... . Quocirca plurimum is praestitisse censendus est, cui successerit demonstrationem huius theorematis invenire.*
>
> L. EULER [17] p. 216.

La cèlebre llei de reciprocitat quadràtica:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4},$$

p, q primers imparells, descoberta per LEGENDRE, no esdevingué un teorema fins a les *Disquisitiones* de GAUSS, on en donà diferents demostracions. A l'Art. 151 d'aquest llibre, GAUSS comentà així una pretesa demostració donada per LEGENDRE d'aquesta llei:

> *Le Gendre etiam demonstrationen tentanit, de qua quum perquam ingeniosa sit in Sect. seq. fusius loquemur. Sed quoniam in ea plura sine demonstratione supposuit (uti ipse fatetur p. 520. Nous avons supposé seulement etc.), quae partim a nemine hucusque sunt demonstrata, partim nostro quidem indicio sine theor. fund. ipso demonstrari nequent, via quam ingressus est, ad scopum deducere non posse videtur, nostraque demonstratio pro prima erit habenda.*

L'omissió de LEGENDRE a què GAUSS fa referència en el comentari anterior no és sinó un cas particular del que esdevindria el teorema de la progressió aritmètica de DIRICHLET (cf. Cap. II, 2.1 d'aquets treball).

En els Art. 291-293 de les *Disquisitiones* GAUSS demostrà novament, fent servir la teoria de les formes quadràtiques ternàries, que tot enter de la forma $8n + 3$ era suma de tres quadrats imparells i calculà el nombre de maneres en les quals un enter n podia ésser descompost com la suma de nombres triangulars. Aquest nombre depèn, en última instància, del nombre de factors primers de n, i del nombre h de classes de formes quadràtiques de discriminaant $-n$. Aquestes recerques foren prosseguides per DIRICHLET, EISENSTEIN I JACOBI, i donaren naixença a una de les aplicacions més boniques de la teoria de les funcions el·líptiques.

La primera demostració de l'afirmació de FERMAT, que tot nombre era suma de m nombres m-gonals, la donà CAUCHY l'any 1813-15. La demostració de CAUCHY fou simplificada per LEGENDRE. LEGENDRE demostrà, a més, que tot enter $> 28(m-2)^3$ era suma de quatre nombres m-gonals, si m era imparell, i que tot enter $> 7(m-2)^3$ ho era de cinc, si m era parell.

3. La fonamentació per Euler de la teoria analítica de nombres

3.1. *La introducció de la funció zeta*

> *Si ex serie numerorum primorum sequens formetur expressio*
>
> $$\frac{2^n \cdot 3^n \cdot 5^n \cdot 11^n \cdot etc}{(2^n-1)(3^n-1)(5^n-1)(7^n-1)(11^n-1)\,etc.},$$
>
> *erit eius valor æqualis summæ huius seriei*
>
> $$1+\frac{1}{2^n}+\frac{1}{3^n}+\frac{1}{4^n}+\frac{1}{5^n}+\frac{1}{6^n}+\frac{1}{7}+etc.$$
>
> L. Euler, [6] Theorema 8.

Dels cursos de càlcul tots sabem que la sèrie harmònica

$$\sum_{n=1}^{\infty} \frac{1}{n^s}$$

és convergent per $s > 1$ i divergent en el cas contrari. Anticipant-nos a la notació introduïda per Riemann posem

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

sense precisar, de moment, on pertany la variable s.

El càlcul de $\zeta(2)$ apareix proposat en el text de Pietro Mengoli *Novæ Quadraturæ Arithmeticæ*, del 1650. Wallis, Leibniz, els Bernoulli, Goldbach i Stirling s'ocuparen d'aquest problema, donant-ne tots solucions aproximades. GOLDBACH comunicà en una carta a DANIEL BERNOULLI que podia demostrar que

$$1\frac{16}{25} = 1{,}64 < \zeta(2) < 1\frac{2}{3} = 1{,}66.$$

EULER i DANIEL BERNOULLI havien conviscut a Sant Petersburg en el període que va del 1727 al 1733. Sembla que EULER esdevingué interessat en aquest problema a través de D. BERNOULLI. En aquesta època, manipulant una mica en la sèrie

$$\frac{\log(1-x)}{x} = -\sum_{n=1}^{\infty} \frac{x^{n-1}}{n}$$

(cf. [4]), EULER arribà a la identitat

$$\zeta(2) = (\log 2)^2 + \sum_{n=1}^{\infty} \frac{1}{2^n n^2}.$$

L'avantatge d'aquesta expressió és que la sèrie

$$\sum_{n=1}^{\infty} 1/2^n n^2$$

convergeix més de pressa del que ho fa la sèrie que defineix $\zeta(2)$. Mitjançant l'expressió

$$\log 2 = -\log\left(1-\frac{1}{2}\right) = \sum_{n=1}^{\infty} \frac{1}{n\,2^n} \sim 0{,}693147$$

$$\sum_{n=1}^{\infty} \frac{1}{n^2\,2^n} \sim 0{,}951787,$$

EULER arribà al resultat aproximat $\zeta(2) \sim 1{,}644934$.

En el treball [5] *Inventio summæ cuiusque seriei ex dato termino generali,* publicat el 1736, si bé hom creu que fou escrit abans del 1734, EULER obtingué l'aproximació

$$\zeta(2) = 1{,}6449340668482264364 7$$

a partir de la descomposició

$$\zeta(2) = \sum_{n=1}^{10} \frac{1}{n^2} + \sum_{n=11}^{\infty} \frac{1}{n^2}.$$

La suma del primers termes la calculà a mà, i la resta l'aproximà mitjançant una fórmula deduïda per ell per al càlcul de

$$\sum_{m=1}^{n} m^k \qquad (k \geqslant 1).$$

En aquesta fórmula intervenen els nombres de BERNOULLI B_2, B_4, ... , què, com sabem, tenen per funció generatriu la donada per

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n x^n}{n!} \; (|x| < 2\pi).$$

Però l'èxit rotund en aqueta qüestió l'obtingué EULER en el treball [3] del 1734. Partint de la funció

$$f(x) = 1 - \frac{\sin x}{\sin \alpha}.$$

on α és fix i diferent d'un múltiple de π, i mitjançant el desenvolupament del sin x, EULER escriví:

$$f(x) = 1 - \frac{x}{\sin \alpha} + \frac{x^3}{3!\sin \alpha} - \ldots.$$

Considerant ara el terme de la dreta com un polinomi de grau infinit, EULER el descompongué tenint en compte les seves arrels. Si aquestes són a_1, a_2, . . . , a_n, . . . , posà

$$f(x) = \left(1 - \frac{x}{a_1}\right)\left(1 - \frac{x}{a_2}\right) \ldots \left(1 - \frac{x}{a_n}\right) \ldots = \prod_{k=1}^{\infty}\left(1 - \frac{x}{a_k}\right)$$

De la definició de f (x) se segueix que les arrels vénen donades per

$$x = \begin{cases} 2\pi n + \alpha \\ 2\pi n + \pi - \alpha. \end{cases}$$

per n = 0, ± 1, ± 2, … . Per tant

$$f(x) = \sum_{n=-\infty}^{\infty} \left(1 - \frac{x}{2\pi n + \alpha} \right) \left(1 - \frac{x}{2\pi n - \pi - \alpha} \right) =$$

$$R \left(1 - \frac{x}{\alpha} \right)$$

$$\prod_{n=1}^{\infty} \left(1 - \frac{x}{(2n-1)\pi - \alpha} \right) \left(1 + \frac{x}{(2n-1)\pi + \alpha} \right)$$

$$\left(1 - \frac{x}{2n\pi + \alpha} \right) \left(1 + \frac{x}{2n\pi - \alpha} \right).$$

Per calcular el terme de la dreta EULER introdueix funcions elementals simètriques d'infinits termes:

$$\sigma_m = \sum_{i_1 \dots i_m} a_{i_1} \dots a_{i_m}.$$

Si

$$S_m = \sum_{i=1}^{\infty} a_i^m,$$

escriu, per analogia amb les fórmules de NEWTON,

$$S_1 = \sigma_1 \quad , \quad S_2 = \sigma_1^2 - 2\,\sigma_2 \quad , \quad S_3 = \sigma_1^3 - 3\,\sigma_{1\,\sigma 2} + 3\,\sigma_3, \dots$$

Tenint en compte que en el nostre cas $\sigma_2 = o$, hom obté

$$\frac{1}{\sin \alpha} = \frac{1}{\alpha} +$$

$$\sum_{n=1}^{\infty} \left(\frac{1}{(2n-1)\pi - \alpha} - \frac{1}{(2n-1)\pi + \alpha} + \frac{1}{2n\pi + \alpha} - \frac{1}{2n\pi - \alpha} \right),$$

$$\frac{1}{\sin^2 \alpha} = \frac{1}{\alpha^2} +$$

$$\sum_{n=1}^{\infty} \left(\frac{1}{((2n-1)\pi - \alpha)^2} + \frac{1}{((2n-1)\pi + \alpha)^2} + \frac{1}{(2n\pi + \alpha)^2} + \frac{1}{(2n\pi - \alpha)^2} \right),$$

$$\frac{1}{\sin^3 \alpha} - \frac{1}{2 \sin \alpha} = \frac{1}{\alpha^3} +$$

$$\sum_{n=1}^{\infty} \left(\frac{1}{((2n-1)\pi - \alpha)^3} - \frac{1}{((2n-1)\pi + \alpha)^3} + \frac{1}{(2n\pi + \alpha)^3} - \frac{1}{(2n\pi - \alpha)^3} \right).$$

Fent ara $\alpha = \pi/2$, EULER obté les identitats

$$\frac{4}{\pi} \left(1 - \frac{1}{3} + \frac{1}{5} \ldots \right) = 1,$$

$$\frac{8}{\pi^2} \left(1 + \frac{1}{3^2} + \frac{1}{5^2} + \ldots \right) = 1,$$

$$\frac{32}{\pi^3} \left(1 - \frac{1}{3^3} + \frac{1}{5^3} - \frac{1}{7^3} + \ldots \right) = 1.$$

Però, puix que tal com observa EULER

$$\zeta(2) = \left(1 + \frac{1}{3^2} + \frac{1}{5^2} + \ldots \right) + \frac{1}{4} \zeta(2),$$

la segona de les identitats abans esmentades li permet finalment d'arribar al resultat exacte

$$\zeta(2) = \frac{\pi^2}{6}\,.$$

(Amb arguments similaars dedueix així mateix que $\zeta(4) = \pi^4/90$).

DANIEL BERNOULLI criticà en dos punts la demostració anterior. D'una part féu notar a EULER que no era del tot evident que tots els zeros de la funció $\sin z = \sin \alpha$ fossin reals, i, d'altra part, no acceptava el fet que hom descompongués les sèries infinites com si fossin polinomis.

La qüestió relativa als zeros fou provada més endavant per EULER, i quant a les objeccions fetes sobre el seu mètode, aquest en reafirmà el 1740 la validesa, inaugurant d'aquesta manera l'ús en l'Anàlisi dels produtes infinits i la factorització de funcions trascendents.

El 1737, després d'haver aconseguit calcular $\zeta(2)$, EULER insistí de nou sobre les propietats de la funció $\zeta(s)$. En el treball anomenat

$$\zeta(s) = \frac{2^s \cdot 3^s \cdot 5^s \cdot 7^s \cdot 11^s \ldots}{(2^s-1)(3^s-1)(5^s-1)(7^s-1)(11^s-1)\ldots},$$

coneguda com la descomposició en producte d'EULER (v. [6]). Aquesta descomposició és clau puix que posa en evidència el paper que juguen els primers en l'estudi de la funció ζ. De les conseqüències que hom n'obté, les quals arriben fins als nostres dies, en parlarem una mica més endavant.

Tots els estudiants coneixen la demostració feta per EUCLIDES del fet que existeixen infinits primers, però val a dir que un dels resultats que més transcendència ha tingut en el camp de la Teoria de Nombres ha estat la redescoberta feta per EULER del teorema d'EUCLIDES. EULER, en el seu *Introductio in analysin infinitorum*, del 1748, (v. [8]), procedeix d'aquesta manera, provant que el conjunt de tots els primers és infinit. Donat que és

$$\sum_{n=1}^{\infty} \frac{1}{n} = \Pi \left(1 - \frac{1}{p} \right)^{-1},$$

quan p descriu tots els primers (la qual cosa resulta de la descomposició de tot nombre natural com a producte de primers de manera única), si el conjunt de primers fos finit, llavors el terme de la dreta representaria una quantitat finita, mentre que el de l'esquerra seria infinit. Aquesta prova, indubtablement més "*difícil*" que la donada per EUCLIDES, té l'encís d'establir un lligam entre un fet de naturalesa algèbrica, l'existència d'infinits primers, i un fet de naturalesa analítica, la divergència de la sèrie harmònica, i ha estat, hom pot dir, la idea germinal de l'ús de tècniques analítiques en Teoria de Nombres.

Com una primera aplicació de les idees introduïdes per EULER esmentarem la demostració de DIRICHLET del teorema de la progressió aritmètica.

En l'*Opuscula analtica* EULER havia afirmat que en tota progressió aritmètica que comencés per 1, s'hi trobaven infinits primers. LEGENDRE havia també fet servir, en una pretesa demostració de la llei de reciprocitat quadràtica, que en tota progressió aritmètica { a + dm } en què mcd (a, m) = 1 hi havia infinits primers. DIRICHLET, a fi de provar que la sèrie

$$\sum_{p \equiv a \pmod m} \frac{1}{p}$$

era divergent, introduí les funcions aritmètiques de valors complexos anomenades caràcters (en la terminologia actual correspon als caràcters del grup abelià finit $(Z/mZ)^*$). A partir d'un caràcter χ formà la sèrie

$$L(\chi, s) = \sum_{s=1}^{\infty} \frac{x(n)}{n^s} \ (\mathrm{Re}(s) > 1),$$

veient que admetia una descomposició en "producte d'EULER":

$$L(\chi, s) = \Pi \left(1 - \frac{\chi(p)}{p^s} \right)^{-1}.$$

El punt difícil de la demostració del teorema de la progressió aritmètica és veure que L $(\chi, 1) \neq 0$, quan χ és un caràcter real diferent del caràcter unitat. Aquest fet fou provat per DIRICHLET mitjançnt la teoria de classes de formes quadràtiques binàries de GAUSS.

3.2. *L'equació funcional de la zeta*

> *Peut-on penser quelque chose de plus affreux que dire que $0 = 1 - 2^n + 3^n - 4^n +$ etc., où n est un entier positif?*
>
> N. ABEL.

L'any 1749, en el treball titulat *Remarques sur un beau rapport entre les séries des puissances tant directes que réciproques*, presentat a l'Acadèmia de Berlín (v. [15]), EULER intuí l'equació funcional satisfeta per la funció ζ, anticipant-se així més de cent anys a les idees de RIEMANN.

Els passos seguits per EULER en aquesta ocasió són tan bells que no podem menys de detallar-los una mica. A partir de la identitat

$$1 + x + x^2 + \ldots + x^n + \ldots = \frac{1}{1-x} \qquad (*)$$

(certa per $|x| < 1$) EULER dedueix, fent $x = -1$, que

$$1 - 1 + 1 - 1 + \ldots = \frac{1}{2}.$$

Aplicant a (*) l'operador

$$x \frac{d}{dx}$$

obté

$$x + 2x^2 + 3x^3 + \ldots = \frac{x}{(1-x)^2},$$

que, per x = – 1, li dóna

$$1-2+3-4+\ldots=\frac{1}{4}\,.$$

Aplicant novament el mateix operador obté

$$x+2^2x^2+3^2x^3+\ldots=\frac{x(1+x)}{(1-x)^3},$$

i, fent x = – 1,

$$1-2^2+3^2-\ldots=0.$$

D'altra part, tenint en compte els valors de $\zeta(2)$ i $\zeta(4)$ esmentats en el paràgraf anterior, pot posar

$$1-2+3-4+\ldots=\frac{1}{4}=\frac{2}{\pi^2}\left(1+\frac{1}{3^2}+\frac{1}{5^2}+\ldots\right),$$

$$1-2^3+3^3-4^3+\ldots=-\frac{1}{8}=\frac{-2\cdot 3'.}{4}\left(1+\frac{1}{3^4}+\frac{1}{5^4}+\ldots\right).$$

A partir d'ací, Euler dedueix les següents identitats:

$$\frac{1-2+3-4+5-6+\ldots}{1-\frac{1}{2^2}+\frac{1}{3^2}-\frac{1}{4^2}+\frac{1}{5^2}-\frac{1}{6^2}+\ldots}=\frac{1\cdot(2^2-1)}{(2-1)\,\pi^2},$$

$$\frac{1^2-2^2+3^2-4^2+5^2-6^2+\ldots}{1-\frac{1}{2^3}+\frac{1}{3^3}-\frac{1}{4^3}+\frac{1}{5^3}-\frac{1}{6^3}+\ldots}=0,$$

$$\frac{1^3-2^3+3^3-4^3+5^3-6^3+\ldots}{1-\frac{1}{2^4}+\frac{1}{3^4}-\frac{1}{4^4}+\frac{1}{5^4}-\frac{1}{6^4}+\ldots}=-\frac{1\cdot 2\cdot 3\,(2^4-1)}{(2^3-1)\,\pi^4},$$

$$\frac{1^4-2^4+3^4-4^4+5^4-6^4+\ldots}{1-\frac{1}{2^5}+\frac{1}{3^5}-\frac{1}{4^5}+\frac{1}{5^5}-\frac{1}{6^5}+\ldots}=0,$$

i conjectura que, si

$$\Phi(s)=\sum_{n=1}^{\infty}\frac{(-1)^n}{n^s},$$

llavors,

$$\frac{\Phi(1-n)}{\Phi(n)}=\begin{cases}\dfrac{(-1)^{(n/2)+1}(2^n-1)(n-1)!}{(2^{n-1}-1)\pi^n}, & \text{si n és parell,}\\[2ex] 0, & \text{si n és imparell,}\end{cases}$$

sempre que sigui $n \geq 2$. Per $n = 1$ veu que

$$\frac{1-1+1-1+\ldots}{1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\ldots}=\frac{1}{2\ln 2}.$$

Les fórmules anteriors són reinterpretades mitjançant la fórmula única

$$\frac{\Phi(1-n)}{\Phi(n)}=\frac{-(n-1)!\,(n^n-1)}{(n^{n-1}-1)\pi^n}\cos\frac{\pi n}{2}.$$

EULER conjectura llavors que

$$\frac{\Phi(1-s)}{\Phi(s)}=\frac{-\Gamma(s)(2^s-1)\cos\pi s/2}{(2^{s-1}-1)\pi^s}$$

és cert per "tot s". *(Cette conjecture paroîtra sans doute fort hardie...).* Observa que per s → la fórmula de la dreta té per límit exactament 1/2 1n 2 i comprova que ambdós termes coincideixen quan

$$s = \frac{1}{2} \quad \text{i} \quad s = \frac{3}{2}.$$

(Notem que Φ (s) convergeix per $s > 0$).

Puix que

$$\Phi(s) = (1 - 2^{1-s})\, \zeta(s),$$

la fórmula predita per EULER es pot escriure com

$$\zeta(1-s) = \pi^{-s}\, 2^{1-s}\, \Gamma(s) \cos \frac{\pi s}{2}\, \zeta(s).$$

Observem que, en aquestes fórmules, hi intervé la funció gamma, una altra creació euleriana.

3.3. *Un incís en la funció gamma*

> *Quamobrem huius progressiones 1, 2, 6, 24, 120, 720, etc, terminus generalis est*
>
> $$\int dx\, (-lx)^n.$$
>
> EULER, [1].

En el treball [1] del 1730, EULER estengué la funció factorial n!, definida per als valors naturals de n, a tots els nombres reals més grans que – 1, observant que

$$n! = \int_0^1 (-\log x)^n\, dx,$$

(puix que la integral de la dreta convergeix per n real i $n > -1$).

GAUSS, en un treball del 1813 anomenat *Circa seriem infinitam*, introduí la notació

$$\Pi(s) = \int_0^\infty e^{-x} x^s \, dx \quad (s > -1)$$

per expressar la integral euleriana anterior. De fet $\Pi(s)$ és definida per tot nombre complex s tal que Re (s) > 1.

La representació següent era també familiar a EULER:

$$\Pi(s) = \lim_{n \to \infty} \frac{n!\,(n+1)^s}{(n+1)(n+2)\ldots(n+s)} .$$

Aquesta fórmula té l'avantatge que té sentit per tot s, real o complex, llevat dels valors de s que anul·len el denominador. Amb altres paraules, l'expressió

$$\Pi(s) = \sum_{n=1}^{\infty} \left(1 + \frac{s}{n}\right)^{-1} \left(1 + \frac{1}{n}\right)^{s}$$

estén la funció Π a una funció meromorfa del pla, sense zeros i amb pols en els enters negatius $s = -1, -2, -3, \ldots$. Hom demostra que

$$\Pi(s) = s\,\Pi(s-1)$$

(equació funcional) i que

$$\Pi(s) = 2^s\,\Pi\left(\frac{3}{2}\right)\Pi\left(\frac{s-1}{2}\right)\Pi^{-1/2},$$

que és l'anomenada relació de LEGENDRE. La notació $\Gamma(s)$ per representar $\Pi(s-1)$ és tanmateix deguda a LEGENDRE, i és la que s'imposà a la fi del segle XIX.

3.4. *Evolució subsegüent de les idees d'Euler: la memòria de Riemann*

Bernhard Riemann (1826-1866), amb motiu del seu nomenament de membre de l'Acadèmia de Ciències de Berlín en la branca de Físiques i Matemàtiques, ocorregut el 1859, presentà una memòria titulada *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse* [31], on establí les bases de l'estudi de la funció zeta i posà de relleu la importància d'aquesta en l'estudi de les lleis que regeixen la distribució dels nombres primers.

Partint de la igualtat descoberta per Euler

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \Pi \left(1 - \frac{1}{p^s} \right)^{-1},$$

Riemann representa per ζ (s) la funció de *variable complexa* definida en els valors de s que fan aquestes expressions convergents; és a dir per s complex amb Re (s) > 1.

Substituint nx per x en la representació integral de la funció Γ, obté

$$\frac{\Gamma(s)}{n^s} = \int_0^{\infty} e^{-nx} s^{s-1} \, dx,$$

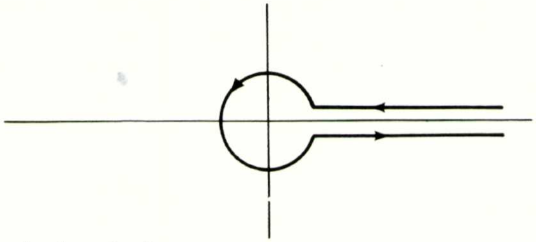
per s > 0, n = 1, 2, 3, … . Sumant aquestes expresions per tot n, Riemann arriba a l'expressió

$$\Gamma(s)\zeta(s) = \int_0^{\infty} \frac{x^{s-1}}{e^x - 1} \, dx,$$

per s > 1. A partir d'ací, i calculant la integral

$$\int_{+\infty}^{+\infty} \frac{(-x)^{s-1}}{e^x - 1} \, dx$$

al llarg del camí indicat en la figura



RIEMANN troba la relació

$$2\,i \sin(\pi s)\,\Gamma(s)\,\zeta(s) = \int_{-\infty}^{+\infty} \frac{(-x)^{s-1}}{e^x - 1}\,dx,$$

la qual fàcilment es transforma en

$$\zeta(s) = \frac{\Gamma(1-s)}{2\pi i} \int_{-\infty}^{+\infty} \frac{(-x)^{s-1}}{e^x - 1}\,dx.$$

Ara bé, les fórmules anteriors son vàlides "per tot s". En efecte, com que e^x creix molt més de pressa que x^s quan $x \to \infty$, la integral és convergent per a tot s real o complex i defineix una funció analítica complexa (puix que la convergència és uniforme sobre els compactes). La funció ζ *definida* mitjançant la relació anterior és, per tant, una funció analítica del pla complex, llevat potser dels punts s = 1, 2, 3, ..., on la funció $\Gamma(1-s)$ té pols. Com que aquesta funció coincideix amb

$$\sum_{n=1}^{\infty} n^{-s}$$

per a valors reals de $s > 1$, ho fa, per prolongació analítica, per a tot s situat al semiplà $\mathrm{Re}(s) < 1$. Com que l'expressió de $\zeta(s)$ en producte d'EULER posa en evidència que $\zeta(s)$ no té cap singularitat per $\mathrm{Re}(s) > 1$, i, d'altra part

$$\lim_{s \to 1} \zeta(s) = \infty,$$

veiem que ζ (s) és una funció meromorfa del pla complex amb un únic pol en el punt s = 1, el qual és simple, puix que el de la Γ ho era. Aquest procés de prolongació analítica, més semblant a l'emprat en el cas de la Γ i que difereix del procés fet a trossets, considerant cadenes de discs, propi de WEIERSTRASS, és el que permet a RIEMANN de substituir les manipulacions d'EULER amb sèries divergents per càlculs amb funcions que estam "veritablement definides". Val a dir, però, que un altre intent "d'explicar" el resultats d'EULER, potser més a prop del seu esperit, ha estat fet en els nostres dies mitjançant tècniques d'Anàlisi no estàndard.

La funció així obtinguda és coneguda amb el nom de funció ζ de RIEMANN.

La representació integral de la ζ, canviant ara el sentit del camí d'integració, i tenint en compte que les úniques singularitats de la integral es troben en els punts $x = \pm 2\pi in$, permet a RIEMANN, fent ús de la fórmula integral de CAUCHY, de veure que

$$2 \sin (\pi s)\, \Gamma (s)\, \zeta (s) = (2\pi)\, \Sigma\, n^{s-1} [(-i)^{s-1} + i^{s-1}];$$

és a dir, de demostrar la igualtat

$$\zeta(s) = \Gamma(1-s)\,(2\pi)^{s-1}\, 2 \sin \left(\frac{\pi s}{2} \right) \zeta(1-s),$$

que és l'equació funcional predita per EULER.

Si definim, d'acord amb RIEMANN,

$$\xi(s) = s\,(s-1)\,\pi^{-s/2}\, \Gamma \left(\frac{s}{2} \right) \zeta(s),$$

obtenim que ξ (s) és una funció entera que satisfà l'equació funcional

$$\xi(s) = \xi(1-s).$$

Mitjançant l'equació funcional veiem que ζ (s) s'anul·la quan s = – 2 n, n natural, i que $\zeta (s) \neq 0$ per tot altre valor de s situat en el semiplà Re (s) < 0. En conseqüència, els únics zeros de ζ, a part dels trivials, es troben a la franja $0 \leqslant \mathrm{Re}(s) \leqslant 1$, anomenada la "banda crítica" i simètricament situats respecte a la recta Re (s) = 1/2. RIEMANN afirma en la seva memòria que és molt probable que tots els zeros no trivials tinguin, efectivament, part real igual a 1/2. Com sabem, aquesta afirmació és l'anomenada *hipòtesi de Riemann*, avui en dia encara no demostrada.

Un teorema degut a HARDY prova que la funció ζ té una infinitat de zeros amb part real 1/2. Se sap que els primers tres milions i mig de zeros de la zeta tenen part real 1/2. Un cèlebre resultat de N. LEVINSON del 1974 afirma que almenys una tercera part dels zeros de la funció zeta a la banda crítica tenen la part real predita per RIEMANN.

2.5. *Lligam de la funció zeta amb el teorema dels nombres primers*

Suma seriei reciprocæ numerorum primorum

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \text{etc.}$$

est infinite magna, infinities tamen minor quam summa seriei harmonicæ

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \textit{etc.}$$

Atque illius summa est huius summæ quasi logarithmus.

EULER, [6] Theorema 19.

En el treball [6] del 1737 EULER demostra que la sèrie

$$\Sigma \, \frac{1}{p},$$

formada amb els recíprocs dels nombres primers, és divergent. D'altra part, com que la sèrie

$$\Sigma \frac{1}{n^2}$$

convergeix, EULER fa el comentari que hi ha "*més primers que quadrats*" (*. . . sequitur infinities plures esse numeros primos quam quadratos in serie omnium omnino numerorum*).

L'afirmació d'EULER va però més enllà de la de la simple divergència de la sèrie $\Sigma\, p^{-1}$. A partir de la igualtat

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p} \left(1 - \frac{1}{p} \right)^{-1},$$

EULER dedueix que

$$\log \left(\sum_{n=1}^{\infty} \frac{1}{n} \right) = \Sigma \log \left(1 - p^{-1} \right)^{-1}$$

$$= \Sigma \left(p^{-1} + \frac{1}{2} p^{-2} + \frac{1}{3} p^{-3} + \ldots \right)$$

$$= \Sigma \frac{1}{p} + \text{conv.}$$

Ara bé, fent "x = 1" en el desenvolupament

$$\log \frac{1}{1-x} = x + \frac{x^2}{2} + \frac{x^3}{3} + \ldots$$

obté

$$\log \frac{1}{1-1} = \log \infty = 1 + \frac{1}{2} + \frac{1}{3} + \ldots .$$

Així la sèrie

$$\Sigma \frac{1}{n}$$

"divergeix com el logaritme" i EULER pot posar

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \ldots \log(\log \infty).$$

Si interpretem aquesta igualtat en la forma

$$\sum_{p<x} \frac{1}{p} \equiv \log(\log x) \quad (x \to \infty),$$

donat que

$$\log(\log x) = \int_1^{\log x} \frac{du}{u} = \int_e^x \frac{dv}{v \log v},$$

ens ve a dir que la densitat dels primers al voltant d'un punt v ve a ésser igual a 1/log v.

EULER havia expressat el seu pessimisme sobre el fet que hom pogués tenir coneixements precisos sobre les lleis que regeixen el comportament dels primers, sense sospitar que ell estava introduïnt les eines més útils per a llur estudi futur. A la introducció del seu treball [9] escriví:

> *Les mathématiciens on tâché jusqu'ici en vain de découvrir quelque ordre dans la progression des nombres premiers, et l'on a lieu de croire que c'est un mystère auquel l'esprit humain ne saurait jamais pénétrer. Pour s'en convaincre, on n'à qu'à qu'à jeter les yeux sur les tables des nombres pemiers que quelques-uns se sont donné la peine de continuer au-delà de cent mille et l'on s'apercevra d'abord qu'il n'y règne aucun ordre ni règle.*

L'any 1785, LEGENDRE, en el seu *Essai sur la théorie des nombres,* introduí la notació

$$\pi(x) = \sum_{p \leqslant x} 1$$

per representar la funció que, a un nombre x, li fa correspondre el nombre de nombres primers inferiors o iguals a x, fent la important conjectura

$$\pi(x) \approx \frac{x}{\log x - 1{,}08366}\,.$$

Independentment, GAUSS, l'any 1972, és a dir quan tenia quinze anys, suggerí que la densitat mitjana dels nombres primers al voltant d'un nombre x vindria donada per l/log x, proposant la fórmula

$$\int_2^x \frac{du}{\log u} = \mathrm{Li}(x) - \mathrm{Li}(2)$$

per a la funció π (x).

No és clar, tant en un cas com en l'altre, quin era el significat precís que aquests autors donaven a l'expressió "una fórmula per a π (x)". Una simple integració per parts dóna que

$$\int_2^x \frac{du}{\log u} = \frac{x}{\log x} + 0\left(\frac{x}{\log^2 x}\right)$$

i, per tant, les fórmules proposades per GAUSS i LEGENDRE són asimptòticament equivalents. L'esforç necessari fet per ambdós autors per arribar a les conjectures anteriors fou enorme. Hom sap (v. [18]) que GAUSS construí una taula amb tots els primers fins a $3 \cdot 10^6$, comptà quants n'hi havia a cada miler i comparà els resultats obtinguts amb els valors presos per la funció Li (x).

En dos importants treballs [39], [40] publicats el 1848 i el 1850, respectivament, ČEBYŠEV demostrà que si el límit

$$\lim_{x \to \infty} \frac{\pi(x) \log x}{x}$$

existia, llavors era necessàriament igual a 1 i, a més a més, que existien constants A, B per a les quals

$$A \frac{x}{\log x} \leqslant \pi(x) \leqslant B \frac{x}{\log x},$$

per tot x suficientment gran.

L'afirmació

$$\pi(x) \sim \frac{x}{\log x} \quad (x \to \infty)$$

o la seva equivalent $\pi(x) \sim \mathrm{Li}(x)$, que és coneguda com a teorema dels nombres primers, no fou provada fins l'any 1896 per HADAMARD I DE LA VALLÉE POUSSIN, de manera independent.

RIEMANN, en la memòria de l'any 1859 abans esmentada, fou el primer a descobrir la connexió que hi havia entre la distribució dels zeros de la funció ζ i el comportament de $\pi(x)$.

Si definim

$$J(x) = \frac{1}{2} \left[\sum_{p^n < x} \frac{1}{n} + \sum_{p^n \leqslant x} \frac{1}{n} \right],$$

les funcions $J(x)$ i $\pi(x)$ estan relacionades per mitjà de les igualtats:

$$J(x) = \pi(x) + \frac{1}{2}\pi(x^{1/2}) + \frac{1}{3}\pi(x^{1/3}) + \ldots + \frac{1}{n}\pi(x^{1/n}) + \ldots$$

$$\pi(x) = J(x) - \frac{1}{2} J(x^{1/2}) - \frac{1}{3} J(x^{1/3}) - \frac{1}{5} J(x^{1/5})$$

$$+ \frac{1}{6} J(x^{1/6}) + \dots + \frac{\mu(n)}{n} J(x^{1/n}) + \dots,$$

on hom dedueix la segona a partir de la primera per la fórmula d'inversió de MÖBIUS. Observem que, per cada valor de x, la fórmula que dóna π (x) conté únicament un nombre finit de sumands no nuls.

RIEMANN, fent ús de l'Anàlisi de FOURNIER, arribà en la seva memòria a la següent fórmula per a J (x):

$$J(x) = \mathrm{Li}(x) - \sum_{\rho} \mathrm{Li}(x^{\rho}) - \log 2 + \int_x^{\infty} \frac{du}{u(u^2-1)\log u} \quad (x > 1),$$

on el sumatori s'estén a tots els zeros ρ de la funció ζ situats a la banda crítica; l'ordre de sumació és el donat per $|\mathrm{Im}\,\rho|$ creixent, i cal tenir-lo en compte, puix que la sèrie no és absolutament convergent.

L'aproximació suggerida per RIEMANN

$$\pi(x) \sim \mathrm{Li}(x) + \sum_{n=2}^{\infty} \frac{\mu(n)}{n} \mathrm{Li}(x^{1/n}),$$

que hom obté per substitució dels valors de J en la fórmula que dóna π (x), és molt millor que la donada per $\pi(x) \sim \mathrm{Li}(x)$. Tot i que RIEMANN sabia que

$$\pi(x) - \sum_{n=1}^{N} \frac{\mu(n)}{n} \mathrm{Li}(x^{1/n}) = \sum_{n=1}^{N} \sum_{\rho} \mathrm{Li}(x^{\rho/n}) + \text{(termes més petits)},$$

no pogué donar cap estimació del que ell anomenà "termes periòdics":

$$\sum_{n=1}^{N} \sum_{\rho} \mathrm{Li}(x^{\rho/n}).$$

De totes maneres, la deducció donada per RIEMANN de la fórmula per a J (x), i per tant la de π (x), contenia dos punts foscos, dels quals RIEMANN era conscient (cf. [14], Ch. 1). La demostració correcta no fou aconseguida fins a quaranta anys després.

El 1893 (v. [19], HADAMARD publicà un treball sobre la representació de funcions enteres mitjançant productes infinits. Aplicant els seus resultats a la funció ξ provà la fórmula

$$\xi(s) = \xi(0) \prod_{\rho} \left(1 - \frac{s}{\rho} \right),$$

on ρ escriu tots els zeros de ξ, o, cosa que és equivalent, tots els zeros de ζ continguts a la banda crítica. Per a fer el producte infinit cal que cada arrel ρ s'aparelli amb l'arrel $1 - \rho$.

MANGOLDT, el 1895, fent servir la descomposició anterior d'HADAMARD de la funció ξ, demostrà la fórmula

$$\psi(x) = x - \Sigma \frac{x^{\rho}}{\rho} = \Sigma \frac{x^{-2n}}{2n} - \log 2\pi \quad (x > 1),$$

on

$$\psi(x) = \sum_{p^n < x} \log p$$

és l'anomenada funció de ČEBYŠEV. L'ordre de sumació a la sèrie

$$\Sigma \frac{x^{\rho}}{\rho}$$

és així mateix el donat per $|\mathrm{Im}\, \rho|$ creixent. A partir de la fórmula anterior aconseguí demostrar que la fórmula per a J (x) donada per RIEMANN era correcta. Cal, però, observar que ni la fórmula de MANGOLDT ni la de RIEMANN no eren encara suficients per a establir el teorema dels nombres primers (si hom no feia ús de la hipòtesi de RIEMANN).

Les demostracions d'HADAMARD i DE LA VALLÉE POUSSIN, del 1896, del teorema dels nombres primers parteixen de la fórmula de MANGOLDT i contenen com a resultat clau que $\zeta(1 + it) \neq 0$ per tot t ε R, t $\neq 0$.

A [42] DE LA VALLÉE POUSSIN demostrà, a més a més, que

$$\pi(x) - \mathrm{Li}(x) = O\left(x \exp\left(-c \sqrt{\log x}\right)\right),$$

essent $c > 0$ una constant; per això exhibí una regió a la banda crítica lliure de zeros, suficientment gran.

Hom pot provar també (v. [14], Ch. 5, § 5) que si θ és un nombre real per al qual $\zeta(s) \neq 0$, per tot s en el semiplà $\mathrm{Re}(s) > \theta$, llavors

$$\pi(x) - \mathrm{Li}(x) = O(x^{\theta+\varepsilon}),$$

per tot $\varepsilon > 0$. Tenint en compte el teorema D'HARDY, cal que sigui

$$\frac{1}{2} \leqslant \theta \leqslant 1.$$

Si θ fos 1, la relació anterior no ens diria res, però si hom pogués provar que $\theta < 1$, seria considerablement millor que totes les estimacions dels termes d'error obtingudes fins ara. Si la hipòtesi de RIEMANN fos certa, hom podria pendre

$$\theta = \frac{1}{2}.$$

Veiem així, de forma ben explícita, com els zeros de la funció zeta "*controlen*" el nombre de primers.

3.6. *Retorn a Euler*

Si invertim la fórmula del producte per $\zeta(s)$, obtenim, per Re (s) > 1,

$$\frac{1}{\zeta(s)} = \prod_p \left(1 - \frac{1}{p^s} \right) = 1 - \frac{1}{2^s} - \frac{1}{3^s} - \frac{1}{5^s} + \frac{1}{6^s} - \ldots$$

$$R \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s},$$

essent $\mu(n)$ la funció de Möbius. A [8], Euler esmentà la igualtat

$$0 = 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{6} - \frac{1}{7} + \frac{1}{10} - \frac{1}{11} - \frac{1}{13} + \ldots,$$

que resultaria de la identitat anterior si fos vàlid de fer-hi $s = 1$. La demostració que aquesta igualtat és certa és realment difícil; von Mangoldt, el 1897 (v. [29]), fou el primer a demostrar que la sèrie convergia i que tenia zuma zero. De la Vallée Poussin demostrà, a més, que

$$\sum_{n<x} \frac{\mu(n)}{n} = O\left(\frac{1}{\log x} \right),$$

amb connexió amb les seves recerques sobre els termes d'error en el teorema dels nombres primers (v. [42]).

Les recerques d'Euler sobre els valors

$$\zeta(2) = \frac{\pi^2}{6}, \zeta(4) = \frac{\pi^4}{90}$$

foren continuades. En el 1755 [13] Euler enuncià que

$$\zeta(2n) = -\frac{(2\pi i)^{2n} B_{2n}}{2(2n)!},$$

donant una taula per als valors dels nombres de Bernoulli que arribava fins al

$$B_{30} \left(B_o = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 + - \frac{1}{30}, \text{etc}\right).$$

Per obtenir aquesta fórmula avui dia hom avalua la funció ζ als enters negatius:

$$\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1},$$

per $n \geqslant 1$, i el resultat predit per EULER resulta llavors de l'equació funcional.

RIEMANN, en la seva memòria, no donà cap expressió per a $\zeta(-n)$, però esmentà que $\zeta(-2) = \zeta(-4) = \ldots = 0$, cosa que en resulta com a conseqüència.

Sobre els valors que pren la funció zeta als enters positius imparells hom sap molt poca cosa. Hom ha provat recentment que $\zeta(3)$ és irracional.

El resultat d'EULER fou generalitzat per SIEGEL (v. [35] i [36]), que provà que les funcions zeta dels cossos totalment reals sempre prenen valors racionals sobre els enters negatius. Aquests són nuls i solament si $-n$ és parell. Això permet de deduir certes propietats de congruència lligant aquests valors, les quals són la base de la construcció, per interpolació, de les funcions zeta p-àdiques de KUBOTA I LEOPOLDT, en el cas abelià [24], i DE SERRE en el cas general [33].

Esmentarem finalment que la natura dels valor presos per la funció zeta als enters parells > 0 i als enters imparells $\leqslant 0$ queda "*explicada*" dins la teoria general de *motius* de GROTHENDIECK i DELIGNE(cf. [10]).

4. ELS ORÍGENS DE LA TEORIA DE PARTICIONS

> *Qui autem actu omnes partitiones dinumerare voluerit, non solum in immensum laborem se immergit, sed omni etiam attentioine adhibita vix cavebit, ne turpiter decipiatur.*
>
> L. EULER, [9].

En una carta datada el 1669, LEIBNIZ preguntà a BERNOULLI si no s'havia preocupat mai d'investigar de quantes maneres diferents un nombre podia ésser escrit com la suma de dos, de tres, o de més nombres. Hi comentà que, si bé el problema li semblava difícil de resoldre, el creia important. Aquest tema fascinà EULER, que, amb tota justícia, pot ésser considerat el fundador de la teoria corresponent. En el treball [9] del 1750, *De partitione numerorum*, i en una sèrie de treballs posteriors, EULER s'ocupà del problema i obtingué una sèrie d'identitats remarcables.

Donat un sencer positiu n, indiquem per p (n) el nombre de maneres en què podem escriure n com a suma de nombres positius $\leqslant$ n. Ex. p (4) = 5, p (5) = 7, puix que

$$4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1,$$

$$5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1$$
$$= 1 + 1 + 1 + 1 + 1\,.$$

Posem p (0) = 1; EULER considerà la sèrie

$$\sum_{n=0}^{\infty} p(n)\, x^n$$

i s'adonà que

$$\prod_{m=1}^{\infty} \frac{1}{1-x^m} = \sum_{n=0}^{\infty} p(n)\, x^n \qquad (\text{per } |x| < 1).$$

La igualtat anterior es pot veure, formalment, de la següent manera. Desenvolupant el producte mitjançant sèries de potències obtenim

$$\prod_{m=1}^{\infty} \frac{1}{1-x^m} = (1 + x + x^2 + \ldots)(1 + x^2 + x^4 + \ldots)(1 + x^3 + x^6 + \ldots)\ldots\,.$$

Si multipliquem els termes de la dreta i els agrupem segons les potències de x, com si fossin polinomis, obtenim una sèrie del tipus

$$1 + \sum_{k=1}^{\infty} a(k)\, x^k.$$

Suposant que prenem el terme x^{k_1} de la primera sèrie, el terme x^{k_2} de la segona, ..., i el terme x^{mk_m} de la m-èsima sèrie, on cada $k_i \geq 0$, llur producte donarà:

$$x^{k_1}\, x^{2k_2} \cdot \ldots \cdot x^{mk_m} = x^k,$$

essent $k = k^1 + 2k_2 + \ldots + m\, k_m$. Això també pot ésser escrit en la forma

$$k = (1 + 1 + \overset{(k_1}{\ldots} + 1) + (2 + 2 + \overset{(k_2}{\ldots} + 2) \ldots + (m + m + \overset{(k_m}{\ldots} + m).$$

Veiem d'aquesta manera que cada paartició de k donarà lloc a m d'aquests termes i, per tant, el coeficient a (k) de x^k coincidirà amb p (k). Fàcilment el raonament anterior és trasformat en un de rigorós, si $|x| < 1$.

Com a conseqüència d'una fórmula similar a l'anterior EULER trobà la següent relació recurrent per al càlcul de p (n):

$$p(n) - p(n-1) - p(n-2) + p(n-5) + p(n-7) + \ldots = 0.$$

Si invertim el producte anterior, obtenim

$$\prod_{m=1}^{\infty} (1 - x^m) = 1 + \sum_{n=1}^{\infty} (p_1(n) - p^0(n))\, x^n,$$

on p_1 (n) indica el nombre de particions de n en un nombre parell de parts desiguals, i p_o (n) el nombre de particions de n en un nombre imparell de parts desiguals. EULER demostrà que la desigualtat

$p_1(n) \ddagger p_0(n)$ estava estretament relacionada amb els nombres pentagonals. Si

$$\omega(n) = \frac{3n^2 - n}{2}$$

indica el n-èsim nombre pentagonal, i posem

$$\omega(-n) = \frac{3n^2 + n}{2},$$

llavors el cèlebre teorema D'EULER sobre els nombres pentagonals s'expressa mitjançant la igualtat:

$$\prod_{m=1}^{\infty} (1 - x^m) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \ldots$$

$$= 1 + \sum_{n=1}^{\infty} (-1)^n (x^{\omega(n)} + x^{\omega(-n)})$$

$$= \sum_{n=-\infty}^{\infty} (-1)^n x^{\omega(n)}.$$

Com moltes altres funcions aritmètiques, per exemple

$$\tau(n),\ c(n),\ \sigma^k(n),\ \zeta(-2n-1),$$

la funció p (n) pot ésser definida mitjançant els coeficients de formes modulars. Si fem

$$\eta(z) = e^{\pi i z/12} \prod_{m=1}^{\infty} (1 - e^{2\pi i m z}),\ \mathrm{Im}\, z > 0,$$

obtenim una funció analítica en el semiplà superior que satisfà l'equació funcional (v. [3])

$$\eta\left(\frac{az+b}{cz+d}\right) = \omega\sqrt{cz+d}\quad \eta(\zeta),$$

per Im $z > 0$, essent ω una determinada arrel 24 de la unitat que depèn de a, b, c i d, però que no depèn de z. A menys de productes per escalars $\eta(24z)$ és l'única forma parabòlica de pes 1/2 amb nivell < 900. La funció de partició es recupera mitjançant la fórmula

$$\eta^{-1}(z) = \sum_{n=0}^{\infty} p(n)\, e^{e\pi i [n-1/24] z}.$$

Després d'EULER la contribució més important a l'estudi de la funció de partició p(n) fou la feta per RAMANUJAN. El 1917, G. H. HARDY i S RAMANUJAN, mitjançant l'anomenat mètode del cercle, feren una estimació de la integral

$$p(n) = \frac{1}{2\pi i} \int_{C_r} \frac{F(z)}{z^{n+1}}\, dz,$$

on

$$F(z) = \prod_{m=1}^{\infty} (1 - z^m)^{-1},$$

i C_r és el cercle $|z| = r$ amb $r < 1$, i obtingueren així la fórmula asimptòtica:

$$p(n) = \frac{e^{K\sqrt{n}}}{4\sqrt{3}\, n} \left(1 + 0 \left(\frac{1}{\sqrt{n}} \right) \right).$$

(El mètode del cercle posteriorment emprat per HARDY I LITTLEWOOD en relació amb el problema de WARING). Una fórmula exacta per a p (n) fou obtinguda per RADEMACHER el 1937 (v [30]).

Una de les descobertes més importants fetes per RAMANUJAN sobre p (n) és la de les congruències que aquesta funció satisfà. MAC MAHON, per mitjà de la fórmula d'EULER del càlcul recurrent de p (n), havia construït una taula amb els valors de p (n) per a $n \leqslant 200$. Per observació directa de la taula RAMANUJAN intuí que

$$p(5m + 4) \equiv 0 \qquad (\text{mòd } 5),$$

$$p\,(7\,m + 5) \equiv 0 \qquad (\text{mòd } 7),$$

$$p\,(11\,m + 6) \equiv 0 \qquad (\text{mòd } 11).$$

Fent servir, d'una part, la funció generatriu donada per EULER per a p (n) i, d'altra part, la fórmula obtinguda per JACOBI

$$\prod_{m=1}^{\infty} (1 - x^m)^3 = \frac{1}{2} \sum_{-\infty}^{\infty} (-1)^n (2\,n + 1)\, x^{n(n+1)/2},$$

on els índexs

$$\frac{1}{2}\, n\,(n + 1)$$

descriuen tots els nombres triangulars, RAMANUJAN acconseguí demostrar les dues primeres congruències.

Més endavant, RAMANUJAN formulà la conjectura següent:

Si

$$\delta = 5^a \cdot 7^b \cdot 11^c \qquad \text{i} \qquad 24\,\lambda \equiv 1 \ (\text{mò } \delta)$$

llavors

$$p\,(m\,\delta + \lambda) \equiv 0 \qquad (\text{mòd } \delta).$$

Un moment de reflexió posa en evidència que n'hi ha prou provant la conjectura per als valors de

$$\delta = 5^a,\ 7^b \text{ i } 11^c.$$

La conjectura anterior fou lleugerament corregida per WATSON l'any 1938, car la corresponent afirmació, tal com la feia RAMANUJAN, en el cas $\delta = y^b$, no era del tot correcta. En la seva forma definitiva les congruències quedaren finalment demostrades en el treball [2] d'O.L ATKIN, del 1967.

La recerca de congruències entre els valors presos per funcions aritmètiques ha estat constant des dels temps de RAMANUJAN fins als nostres dies (cf., per exemple, [27]). El 1967 SERRE enuncià una conjectura, provada més endavant per DELIGNE, que associava a certes formes parabòliques

$$f = \sum_{n=1}^{\infty} \tau(n)\, e^{2\pi i n z}$$

de pes *enter* k un sistema de representacions l-àdiques:

$$\rho_{\ell}: \mathrm{Gal}\,(K_{\ell} \mid Q) \to GL_2\,(Z^l),$$

tals que

$$\mathrm{Tr}\,(\rho_l\,(F_p)) = \tau\,(p),$$

$$\det\,(\rho_l\,(F_p)\,) = p^{k-1},$$

per tot primer p ‡ l. Ací K_l indica l'extensió maximal de Q no ramificada fora de l i F_p, l'element de FROBENIUS de p. Un estudi de Im ρ_li en particular de les seves reduccions mòdul l ha permès a SWINNERTON-DYER (v. [38]) explicar el *perquè* de les congruències per certes funcions (cas dse la τ), caracteritzant tots els primers per als quals n'hi podia haver.

Amb relació amb la teoria de particions, una altra relació fou descoberta i provada per EULER referent a la funció suma de divisors. L'any 1751, a [11], EULER havia observat que la funció ∫ n, igual a la suma de les parts alíquotes d'un nombre n (normalment representada avui dia per σ (n)) satisfeia la igualtat:

$$\begin{aligned} \int n &= \int (n-1) + \int (n-2) - \int (n-5) - \int (n-7) \\ &+ \int (n-12) + \int (n-15) - \int (n-22) - \int (n-26) \\ &+ \int (n-35) + \int (n-40) - \int (n-51) - \int (n-57) \\ &+ \int (n-70) + \int (n-77) - \int (n-92) - \int (n-100) + \text{etc.}, \end{aligned}$$

on $\int 0$ es fa igual a n sempre que surti a la fórmula. EULER observa la semblança d'aquesta expressió amb el seu teorema sobre els nombres pentagonals

$$\Pi\,(1 - x^x) = 1 - x - x^2 + x^5 + x^7 - x^{12} - c^{15} +$$

$$+ x^{22} + x^{26} - x^{35} - x^{40} + \text{etc.}$$

En el treball esmentat es dedica, partint de la certesa de la fórmula per a $\int n$, a obtenir una sèrie de notables identitats i fa, tot seguit, el comentari següent:

> *Ce raisonnement, quoi qu'il soit encore fort éloigné d'une démonstration parfaite, ne laissera pas pourtant de lever plusieurs doutes sur la fa forme bizarre de l'expression que je viens d'expliquer.*

Tres anys després, el 1754 (v. [12]), EULER pogué demostrar que la fórmula per a $\int n$ era, efectivament, correcta. El seu treball, curt però de difícil contingut, fou qualificat com *ein Meisterstück* per JACOBI.

BIBLIOGRAFIA

[1] *De progressionibus seu quarum termini generales algebraice dari nequeunt.* Commentaarii academiæ scientiarum Petropolitanæ 5 (1730/1), 1738, p. 36-57. Opera Omnia, Series I, v. XIV: Commentationes Analyticæ, p. 1-24.

[2] *Observationes de theroremate quodam Fermatiano aliisque ad numeros primos spectantibus.* Comment. acad. scient. Petrop. 6 (1732/3), 1738, 103-107. Opera Omnia, Series I, v. II: Commentatioines Aritmeticæ, p. 1-5

[3] *De summis serierum reciprocarum.* Comment. acad. scient. Petrop. 7 (1734/5), 1740, p. 123-134.

[4] *Theorematum quorundam ad numeros primos spectantium demonstratio.* Comment. acad. scient. Petrop. 8 (1736), 1741, p. 141-146. Opera Omnia, Series I, v. II: Comment. Arith., p. 33-37.

[5] *Inventio summæ cuiusque seriei ex dato termino generali.* Comment. acad. scient. Petrop. 8 (1736), 1741, p. 9-22. Opera Omnia, Series I, v. XIV: Comment. Anal., p. 108-123.

[6] *Variæ observationes circa series infinitas.* Comment. acad. scient. Petrop. 9 (1737), 1744, p. 160-188. Series I, v. XIV: Comment. Anal., p. 216-244.

[7] *Theoremata circa divisores numerorum.* Novi comment.acad. scient. Petrop. 1 (1747/8), 1750, p. 20-48. Opera Omnia, Series I, v. II: Comment. Arith., p. 62-85.

[8] *Introductio in Analysin Infinitorum.* Lauana, 1748. Opera Omnia, Series I, v. VIII. Introduction à l'analyse infinitesimale. Bachelier, París, 1835.

[9] *De partitione numerorum.* Novi comment. acad. scient. Petrop. 3 (1750/51), 1753, p. 125-169. Opera Omnia, Series I, v. II: Comment. Arith., p. 254-294.

[10] *Carta a Goldbach.* Abril 12, 1749. Novi comment. acad. scient. Petrop. 5 (1751), 1754-5. Opera Omnia, Series I, v. II: Comment. Arith. p. 210.

[11] *Découverte d'une loi tout extraordinaaire des nombres par rapport à la somme de leurs diviseurs.* Bibliothèque impartiale 3, 1751, p. 10-31. Opera Omnia, Series 'I, vol II: Comment. Arith, p. 254-294.

[12] *Demonstratio theorematis circa ordinem in summis divisorum observatum.* Novi coment. acad. scient. Petrop. 5 (1754/5), 1760, p. 75-83. Opera Omnia, Seires I, v. II: Comment. Arithu. p. 390-398.

[13] *Institutiones calculi differentialis.* Acad. imp. scient. Petrop. St. Petersburg, 1755. Opera Omnia, Series I, v. X.

[14] *Theoremata arithmetica nova methododemonstrata.* Novi comment. acad. scient. Petrop. 8 (1760/1), 1763, p. 74-104. Opera Omnia, Series I, v. II: Comment. Arithu., p. 531-555.

[15] *Remarques sur un beau rapport entre les séries des puissances tant directes que réciproques.* Mémoires de l'acad. des sciences de Berlin 17 (177761), 1768, p. 83-106. Opera Omnia, Series I, v. XV, p. 70-90.
[16] *Vollständige Anleitung zur Algebra.* St. Petersburg, 1770. Opera Omnia, Series I, v. I.
[17] *Decriteriis æquationis $fx^2 + gy^2 = hz^2$ utrumque resolutionem admittat necne.* Opuscula analytica. St. Petersburg, 1783.
[18] *Opuscula analytica.* St. Petersburg, 1783.
[19] *De numeris amicabilibus.* Comm. Arith. 2, 1849, p. 630. Opera postuma 1, p. 14-15.
[20] *Tractatus de numerorum doctrina.* Comm. Arith., 2, p. 514. Opera postuma 1, p. 14-15.

Altres autors

[1] APOSTOL, T.M.: *Introduction to Analytic Number Theory.* Under. Texts in Maths. Springer, Nova York, 1976.
[2] ATKIN, A.O.L.: *Proof of a conjecture of Ramanujan.* Glasgow Math. J. 8 (1976), 14-32.
[3] AYOUB, R.: *An Introduction to the Analytic Theory of Numbers.* Math. Surveys 10. AMS, Rhode Island, 1963.
[4] AYOUB, R.: *Euler and the zeta function.* Amer. Math. Monthly 81 (1974), 1067-1086.
[5] BAYER, P.: *El Teorema de Fermat.* Publ. Mat. U.A.B. 2 (1976), 94-110.
[6] CATALDI, P..: *Trattato de numeri perfetti di Pierto Antonio Cataldo.* Bolonya, 1603.
[7] CIENTÍFICOS GRIEGOS I, II. Aguilar, Madrid, 1970.
[8] *Complex Analysis.* The Open University, unit 15: Number Theory. The Open University Press., Milton Keynes, 1975.
[9] DAVIS, P.J.: *Leohnard Euler's integral: A historical profile of the gamma function.* Amer. Math. Monthly 66 (1959), 849-869.
[10] DELIGNE, P.: *Valeurs de fonctions L et périodes d'intégrales. A Automorphic forms, representations and L-functions.* Proceed. Symp. Pure Math. 33. AMS, Thode Island, 1979.

[11] Dickson, L.F.: *History of the theory of Numbers I, II, III.* Carnegie Institute of Washington, 1919, 1920, 1923. Chelsea, Nova York, 1971.

[12] Dieudonné, J.: *Abrégé d'histoire des Mathématiques 1700-1900,* I, II. Hermann, París, 1975.

[13] Dirichlet, L.P.G., Dedekind, R.: *Vorlesungen über Zahlentheorie.* Braunschweig, 1863. Chelsea, Nova York, 1968.

[14] Edwards, H.M.: *Riemann's zeta function.* Acad. Press, Nova York, 1968.

[15] Ellison, W.J., Mèndes France, M.: *Les nombres premiers.* Hernann, Paarís, 1975.

[16] Fermat, P.: *Varia Opera Math. d. Petri de Fermat.* Tolosæ, 1679. œuvres de Fermat I, II. París, 1891, 1894.

[17] Gauss, C.F.: *Disquisitiones arithmeticæ.* Leipzig, 1801. Untersuchungen über höhere Arithmetik. Chelsea, 1889; reimp. 1965.

[18] Gauss, C.F.: *Carta a Enke del 24 Dec. 1849.* Werke II, 444-447. Königlichen Gesellschaft der Wissenschaften zu Göttinge.

[19] Hadamard, J.: *Étude sur les Propriétés des Fonctions Entières et en Particulier d'une Fonction Considérée par Riemann.* J. Math. Pures Appl. 9 (19893), 171-215.

[20] Hadamard, J.: *Sur la distribution des zeros de la fonction* $\zeta(s)$ *et ses consequences arithmétiques.* Bull. Soc. Math. France 24 (1896), 199-220.

[21] Hardy, G.H., Wright E.M.: *An Introduction to the Theory of Numbers.* Clarendon Press, Oxford, 1938.

[22] Hardy, G.H.: Ramanujan, *twelve lectures on subjects suggested by his life and work.* Chelsea, Nova York, 1940.

[23] Jacobi, C.G.J.: *Gesammelte werke.* G. Reiner, Berlín, 1881-1891.

[24] Kubota, T., Leopoldt, H.W.: *Eine p-adische Theorie der Zetawerte.* J. Reine Angew. Math. 214-215 (1964), 328-339.

[25] Lagrange, J.L.: *Réflexions sur la résolution algébrique des équations.* Akad. Wiss., Berlín, 1770-71.

[26] LEGENDRE, A.M.: *Essai sur la Théorie des Nombres.* Duprat, París, 1978. Blanchard, París, 1955.
[27] LE VEQUE, W.J.: *Reviews in Number Theory 4.* AMS, Rhode Island, 1974.
[28] VON MANGOLDT, H.: *Zu Riemann's Abhandlung "Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse".* J. Reine Angew. Math. 114 (1895), 255-305.
[29] VON MANGOLDT, H.: *Beweis der Gleichung* $\Sigma\, k^{\infty} = 1\, u\, (k)/k = 0$. S.B. Kgl. Preuss. Akad Wiss., Berlín (1897), 835-852.
[30] RADEMACHER, H.: *On the partition function p (n).* Proc. London Mathu. Soc. 43 (1937), 241-254.
[31] RIEMANN, B.: *Ueber die Anzhl der Primzahlen unter einer gegebener Grösse.* Monaatsber. Akad. Berlin (1859), 671-680.
[32] ROSEN, M.: *Abel's theorem oin the lemniscate.* Amer. Math. Monthly 88 (1981).
[33] SERRE, J.P.: *Formes modulaires et fonctions zêta p-adiques. A Modular Functions of One Variable III.* Lect. Notes 350. Springer, Berlín, 1973.
[34] SHANKS, D.: *Solved and unsolved problems in Number Theory.* Spartan, Nova York, 1962.
[35] SIEGEL, C.L.: *Über die analytische Theorie der quadratischen Formen III.* Ann. of Mathu. 38 (1937), 212-291. Gesam. Abh I, 469-548.
[36] SIEGEL, C.L.: *Berechnung von Zetafunktionen on ganzzahligen Stellen.* Gött. Nach 10 (1969), 87-102.
[37] SIMÓ, C.: *Els nombres primers.* Bullt. Soc. Cat. de Ciències 1 (1979), 25-677.
[38] SWINNERTON-DYER, HU.P.F.: *On l-adic representations and congruences for coefficients of modular forms. A Modular Functions of One Variable III.* Lect. Notes 350. Springer, Berlín, 1973.
[39] TCHEBYCHEF, P.L.: *Sur la fonction qui détermine la totalité des nombres premiers inferieurs à une limite donnée (1848).* J. Math. Pures Appl. 17 (1852).
[40] TCHEBYCHEF, P.L.: *Mémoire sur les nombres premiers (1850).* J. Math. Pures Appl. 17 (1852).

[41] DE LA VALLÉE POUSSIN, C.J.: *Recherches analytiques sur la théorie des nombres (première parti).* Ann. Soc. Sci. Bruxelles 20 (1896), 183-256.

[42] DE LA VALLÉE POUSSIN, C.J.: *Sur la fonction ζ (s) de Riemann et le nombre de nombres premiers inférieurs a une limite donnéee.* Mém. Courronnes et Autres Mém. Publ. Acad. Roy. Sci., des Lettres Beaux-Arts Belg. 59 (1899-1900).