Publicacions de la Societat Catalana de Matemàtiques
Vol. 6

Tres perles de la Teoria de Nombres

A. I. Khintxin

PRÒLEG

El text que teniu a les mans és una joia clàssica de la literatura matemàtica. El mateix context de la seva creació té una qualitat literària especial: un soldat de l'exèrcit rus que combatia els nazis a la Segona Guerra Mundial, de nom Serioja, convalescent de les seves ferides a un hospital, prega a un professor seu, Aleksandr Khintxin, que li faci arribar lectures matemàtiques mentre duri la seva recuperació.

Emocionat per aquesta petició, Khintxin recull tres problemes que li semblen atractius i estimulants, apropiats a les condicions singulars del cas. El resultat és una petita obra mestra que ha inspirat molts matemàtics des d'aleshores, tant pel seu contingut com per l'estil clar i transparent de la seva exposició.

D'una banda, Khintxin escull tres problemes que avui, seixanta-cinc anys més tard, segueixen sent objecte d'un gran interès matemàtic, cosa que reflecteix l'encert de la seva tria. El primer dels tres problemes és el teorema de Van der Waerden sobre l'existència de progressions aritmètiques arbitràriament llargues en alguna part de qualsevol partició arbitrària dels enters. Aquest teorema és el punt de partida del que s'anomena *teoria aritmètica de Ramsey*, i està estretament relacionat amb el teorema de Szemerédi, de 1970, sobre l'existència de progressions aritmètiques arbitràriament llargues en qualsevol conjunt d'enters de densitat positiva, o el més recent teorema de Green i Tao, de 2005, que assegura el mateix per al conjunt dels nombres primers. El segon problema tracta el teorema de Mann, que estableix que la densitat d'un conjunt suma és més gran o igual que la suma de densitats dels sumands, originat en els treballs de Schnirelmann que van fer el primer avenç significatiu en la conjectura de Goldbach (cada enter parell és la suma de dos primers) i que ha obert una àrea que gaudeix de gran activitat avui dia, l'anomenada *combinatòria additiva*. L'obra s'acaba amb el problema de Waring, resolt inicialment per Hilbert, que assegura que cada enter és la suma de potències k–èssimes d'enters en un nombre màxim que només depèn de k, una generalització del teorema de Lagrange, que diu que cada nombre és la suma de com a molt quatre quadrats. Tan la

resolució de Hilbert del problema de Waring, com les que van seguir de Hardy i Littlewood i de Vinogradov, van ser de naturalesa analítica. La que es presenta aquí, deguda a Linnik, és de caire combinatori.

De l'altra, l'autor fa de cadascun dels tres problemes una exposició que, sent elemental, és a dir, sense exigir un coneixement matemàtic professional, té una intensitat matemàtica del més alt nivell. El discurs està curosament construït amb una clara finalitat didàctica, i constitueix encara avui un exemple admirable de comunicació matemàtica.

Aquesta és una traducció fidel no només al text sinó també a l'organització del material, a la notació i, tant com ha estat possible, a l'estil peculiar de l'original, en la confiança que en la versió catalana mantingui la seva frescor i la seva eficàcia expositiva.

Aina Lladó
Estellencs, agost de 2009

PREFACI

Aquesta petita obra està dedicada a tres teoremes de l'aritmètica que, malgrat la seva aparent simplicitat, han estat l'objecte de l'esforç de molts investigadors matemàtics. Les demostracions que es presenten aquí fan servir eines completament elementals (tot i que no són gaire simples).

El llibre pot ser seguit per estudiants de primers cursos d'universitat i està dirigit a un ampli cercle d'amants de les matemàtiques.

TRES PERLES DE LA TEORIA DE NOMBRES

Per començar, una carta (en lloc d'un preàmbul)

24 de març de 1945

Benvolgut Serioja,

La carta que m'enviares des de l'hospital em va produir un gran plaer per partida triple. En primer lloc, el teu prec perquè t'envïi "algunes petites perles matemàtiques" m'indica que realment estàs millorant, i no només ho estàs intentant, com un brau guerrer, per ajudar a alleujar l'ansietat dels teus amics. Aquest va ser el meu primer plaer.

A més, em va donar ocasió per reflexionar sobre com és que en aquesta guerra tants lluitadors joves com tu es deleixen tan apassionadament per dedicar-se a la seva ocupació preferida –l'ocupació que ja apreciaven abans de la guerra, i de la qual la guerra els va separar– durant la més petita treva. No hi havia res de semblant a l'anterior Guerra Mundial. En aquell temps qualsevol home jove, a l'arribar al front, sentia invariablement que la seva vida s'havia interromput, que el que havia estat fins aleshores la substància de la seva vida havia esdevingut una llegenda irrealitzable. Ara, en canvi, n'hi ha que escriuen dissertacions durant els intervals entre batalles, i les defensen a la seva tornada durant una breu llicència. No és perquè senten amb tot el seu ser que els seus assoliments tant en la guerra com en les seves ocupacions preferides – ciència, art, activitat pràctica– són dues línies d'una mateixa i gran causa? Si és així, no és aquest sentiment, potser, un dels orígens de les victòries de què nosaltres, aquí a casa, gaudim de manera tan entusiasta? Aquest pensament em gratifica molt, i aquest va ser el meu segon gran plaer.

I així vaig començar a pensar sobre què et podia enviar. No et conec del tot –només vares venir a les meves classes durant un any. De tota manera, m'ha quedat una ferma convicció sobre la profunditat i serietat de la teva actitud cap a la ciència, i per tant no vull enviar-te uns trencaclosques amb poca substància científica. D'altra banda, sabia que la teva preparació no és gaire bona –només vares assistir un any a classe a la universitat, i durant tres anys de servei ininterromput al front amb prou feines deus haver tingut temps d'estudiar. Després de deliberar alguns

dies, he fet una elecció. Has de jutjar per tu mateix si és una elecció feliç o no. Personalment, considero que els tres teoremes d'aritmètica que t'envio són perles genuïnes de la nostra ciència.

De tant en tant apareixen problemes curiosos i notables en l'aritmètica, aquesta antiga però sempre jove branca de les matemàtiques. El seus continguts són tan elementals que qualsevol estudiant d'escola els pot entendre. Normalment, tenen a veure amb la demostració d'alguna simple llei que governa el món dels nombres, una llei que resulta ser correcta en tots els casos especials que s'han pogut comprovar. Ara, el problema és provar que el seu enunciat és correcte en tots els casos. I malgrat l'aparent simplicitat del problema, la seva solució fa anys que resisteix, i de vegades segles, els esforços dels matemàtics més importants de cada època. Has d'admetre que això és ben temptador.

He triat tres d'aquests problemes per a tu. Tots tres han estat resolts recentment, i en la seva història hi ha dos fets comuns remarcables. Primer, els tres problemes han estat resolts pels mètodes aritmètics més elementals (de tota manera, no confonguis elemental amb simple; ja t'adonaràs que les solucions dels tres problemes no són gaire simples, i et caldrà un esforç no pas petit de la teva part per entendre'ls i assimilar-los bé). En segon lloc, els tres problemes han estat resolts per matemàtics joves i novells, amb prou feines de la teva edat, després d'una sèrie d'atacs infructuosos per part de "venerables"savis. No és això una espurna plena de promeses per a futurs investigadors com tu? Quina crida més encoratjadora per a una dedicació a la ciència!

La feina d'exposar aquests teoremes em va obligar a penetrar més profundament en l'estructura de les seves demostracions magnificents, i em va proporcionar un gran plaer.

Aquest ha estat el meu tercer gran plaer.

Et desitjo el millor dels èxits, en el combat i en la ciència.

Afectuosament,
Aleksandr Khintxin

Capítol 1:
El teorema de Van der Waerden sobre progressions aritmètiques

§ 1

A l'estiu del 1928 vaig passar diverses setmanes a Göttingen. Com era habitual, hi havien arribat molts investigadors estrangers per passar-hi el semestre d'estiu. Vaig fer coneixença amb molts d'ells i, de fet, amb uns quants vàrem arribar a establir una bona amistat. Quan hi vaig arribar, el tema del dia era el brillant resultat d'un jove holandès, Van der Waerden, que en aquell temps era encara un jove principiant que avui dia, però, és un matemàtic reconegut. Aquest resultat acabava de ser obtingut allà, a Göttingen, de fet només uns dies abans de la meva arribada. Gairebé tots els matemàtics que em vaig trobar me'n varen parlar amb entusiasme.

El problema tenia la història següent. Un dels matemàtics d'allí (he oblidat el seu nom) va trobar-se amb el problema següent en el seu treball científic: imagina que divideixes el conjunt dels nombres naturals de manera completament arbitrària en dues parts (per exemple, entre nombres parells i imparells, o entre nombres primers i nombres compostos, o de qualsevol altra manera). Es pot afirmar aleshores que en alguna de les dues parts s'hi poden trobar progressions aritmètiques de llargada arbitràriament gran? (per llargada d'una progressió aritmètica vull dir aquí, i en tot el que segueix, simplement la quantitat de termes que conté). Tothom a qui es plantejava la qüestió veia el problema a primera vista bastant senzill; la seva resposta afirmativa semblava ser gairebé evident. Els primers intents de resoldre-la, però, varen dur a no res. I com que els matemàtics de Göttingen i els seus convidats estrangers estaven tradicionalment en contacte permanent els uns amb els altres, aquest problema, d'una resistència provocadora, va esdevenir aviat l'objecte d'un interès matemàtic general. Tothom el va considerar, des de l'acadèmic més venerable fins al jove estudiant. Després de diverses setmanes d'esforços extenuants, el problema va cedir finalment a l'atac d'un jove que havia vingut a Göttingen a estudiar, l'holandès Van

der Waerden. Hi vaig fer coneixença i ell personalment em va explicar la seva solució al problema. Era elemental però de cap manera simple. El problema va resultar ser profund, la seva simplicitat aparent era fictícia.

Fa poc M. A. Lukomskaia (de Minsk) va descobrir i em va enviar una demostració considerablement més simple i transparent del teorema de Van der Waerden que, amb el seu amable permís, t'exposaré a continuació.

§ 2

En realitat Van der Waerden va provar més del que calia. En primer lloc, va suposar que els nombres naturals estan dividits no en dues sinó en un nombre arbitrari, diguem k, de classes (conjunts). En segon lloc, resulta que no cal descompondre tota la successió de nombres naturals per garantir l'existència d'una progressió aritmètica de llargada donada l (arbitràriament gran) en almenys una d'aquestes classes; n'hi ha prou amb un segment prou llarg. La llargada $n(k,l)$ d'aquest segment és una funció dels nombres k i l. Per descomptat no té importància d'on traiem aquest interval dins del conjunt de nombres naturals, sempre que contingui $n(k,l)$ nombres consecutius.

Així doncs, el teorema de Van der Waerden es pot enunciar de la manera següent:

Siguin k i l dos nombres naturals arbitraris. Aleshores hi ha un nombre natural $n(k,l)$ tal que si un segment arbitrari de llargada $n(k,l)$ dels nombres naturals es parteix de manera arbitrària en k parts (alguna de les quals pot ser buida), aleshores trobem en almenys una de les parts una progressió aritmètica de llargada l.

Aquest enunciat és trivialment cert per a $l = 2$. Per veure-ho, n'hi ha prou amb posar $n(k,2) = k+1$; en efecte, si un conjunt de $k+1$ nombres es parteix en k parts, certament una d'elles conté més d'un nombre, i un parell arbitrari de nombres naturals forma una progressió aritmètica de llargada 2, cosa que prova el teorema en aquest cas. Provarem el teorema per inducció sobre l. Així doncs, suposarem d'ara en endavant que el teorema es verifica per a algun nombre $l \geq 2$ i per a valors arbitraris de k, i provarem que manté la seva validesa per al nombre $l+1$ (i naturalment també per a tots els valors de k).

§ 3

D'acord amb les nostres hipòtesis, doncs, per a cada nombre natural k hi ha un nombre natural $n(k,l)$ tal que, si un segment arbitrari de llargada $n(k,l)$ de nombres naturals es parteix de manera arbitrària en k classes, hi ha una progressió aritmètica de llargada l en almenys una d'aquestes classes. Hem de provar llavors que, per a cada natural k, existeix també un nombre $n(k,l+1)$. Resolem aquest problema *construint* efectivament aquest nombre $n(k,l+1)$. Amb aquesta finalitat posem

$$q_0 = 1, n_0 = n(k,l)$$

i definim els nombres $q_1, q_2, \ldots, n_1, n_2, \ldots$ successivament de la manera següent: si q_{s-1} i n_{s-1} ja estan definits per a algun $s > 0$, posem

$$q_s = 2n_{s-1}q_{s-1}, \quad n_s = n(k^{q_s}, l), \quad (s = 1, 2, \ldots). \tag{1}$$

Els nombres q_s i n_s estan òbviament ben definits per a qualsevol valor de $s \geq 0$. Ara afirmem que podem prendre q_k per a $n(k,l+1)$. Hem de provar, doncs, que si un segment de llargada q_k de nombres naturals es parteix de qualsevol manera en k classes, aleshores hi ha una progressió aritmètica de llargada $l+1$ en almenys una d'aquestes classes. La resta del capítol es dedica a demostrar aquesta afirmació.

En el que segueix escrivim per brevetat $l+1 = l'$.

§ 4

Suposem doncs que el segment Δ de llargada q_k de la successió de nombres naturals es parteix de manera arbitrària en k classes. Diem que dos nombres a i b de Δ són del mateix *tipus* si a i b pertanyen a la mateixa classe, i aleshores escrivim $a \approx b$. Direm que dos segments de Δ de la mateixa llargada, $\delta = (a, a+1, \ldots, a+r)$ i $\delta' = (a', a'+1, \ldots, a'+r)$, són del mateix tipus si $a \approx a'$, $a+1 \approx a'+1, \ldots, a+r \approx a'+r$, i aleshores escrivim $\delta \approx \delta'$. La quantitat de possibles tipus diferents per als nombres de Δ és evidentment k. Per a segments de la forma $(a, a+1)$ (és a dir, per a segments de llargada 2) el nombre de tipus possibles és k^2; i en general, per a segments de llargada m és k^m (per descomptat, no tots els tipus han d'aparèixer necessàriament en el segment Δ).

Com que $q_k = 2n_{k-1}q_{k-1}$ (d'acord amb (1)), el segment Δ es pot veure com una successió de $2n_{k-1}$ subsegments de llargada q_{k-1}. Aquests

subsegments, com acabem de veure, poden tenir fins a $k^{q_{k-1}}$ tipus diferents. La meitat esquerra del segment Δ conté n_{k-1} d'aquests subsegments, on $n_{k-1} = n(k^{q_{k-1}}, l)$ d'acord amb (1). Pel significat del nombre $n(k^{q_{k-1}}, l)$, podem afirmar que la meitat esquerra del segment Δ conté una progressió aritmètica de l d'aquests subsegments del mateix tipus,

$$\Delta_1, \Delta_2, \ldots, \Delta_l$$

de llargada q_{k-1}; aquí, per brevetat, diem que segments de la mateixa llargada Δ_i formen una progressió aritmètica si llurs nombres inicials formen una tal progressió. A la diferència entre els nombres inicials de dos segments consecutius de la progressió $\Delta_1, \Delta_2, \ldots, \Delta_l$ li diem la diferència d_1 d'aquesta progressió. Naturalment la diferència entre els segons (o tercers, o quarts) nombres de dos d'aquests segments consecutius és igualment d_1.

A aquesta progressió de segments hi afegim ara el terme $l+1$, $\Delta_{l'}$ (recordem que $l' = l+1$), que pot estendre's més enllà de la meitat esquerra del segment Δ, però que en qualsevol cas pertany encara tot sencer al segment Δ. Els segments $\Delta_1, \Delta_2, \ldots, \Delta_l, \Delta_{l'}$ formen doncs una progressió aritmètica de llargada $l' = l+1$ i diferència d_1 de segments de llargada q_{k-1} cadascun, dels quals $\Delta_1, \Delta_2, \ldots, \Delta_l$ són del mateix tipus. No sabem res del tipus del darrer segment $\Delta_{l'}$.

Això completa el primer pas de la nostra construcció. Estaria bé que te'l tornessis a repassar abans que continuem.

§ 5

Ara seguim amb el segon pas. Prenem un qualsevol dels primers l termes de la progressió de segments que acabem de construir. Diguem que prenem Δ_{i_1}, de manera que $1 \leq i_1 \leq l$; Δ_{i_1} és un segment de llargada q_{k-1}. El tractem de la mateixa manera que hem fet abans amb el segment Δ. Com que $q_{k-1} = 2n_{k-2}q_{k-2}$, la part esquerra del segment Δ_{i_1} es pot veure com una successió de n_{k-2} subsegments de llargada q_{k-2}. Per a subsegments d'aquesta llargada hi ha $k^{q_{k-2}}$ tipus possibles i, d'altra banda, $n_{k-2} = n(k^{q_{k-2}}, l)$ d'acord amb (1). Per tant, la part esquerra de Δ_{i_1} ha de contenir una progressió de l d'aquests subsegments del mateix tipus, $\Delta_{i_1 i_2}$ $(1 \leq i_2 \leq l)$ de llargada q_{k-2} cadascun. Sigui d_2 la diferència d'aquesta progressió (és a dir, la distància entre els nombres inicials de dos subsegments consecutius). A aquesta progressió de segments hi afegim el terme $(l+1)$, $\Delta_{i_1 i_{l'}}$, del tipus del qual, és clar, no sabem res. El

segment $\Delta_{i_1 i_{l'}}$ no té per què pertànyer ja a la part esquerra de Δ_{i_1}, però òbviament pertany al segment Δ_{i_1}.

Ara refem la nostra construcció, que hem completat fins ara només en un dels segments Δ_{i_1}, de manera anàloga en tots els altres segments Δ_{i_1} $(1 \leq i_1 \leq l')$. Obtenim així un conjunt de segments $\Delta_{i_1 i_2}$, $(1 \leq i_1 \leq l', 1 \leq i_2 \leq l')$ amb dos subíndexs. És clar que dos d'aquests segments qualssevol amb subíndexs que no passin de l són del mateix tipus:

$$\Delta_{i_1 i_2} \approx \Delta_{i'_1 i'_2} \ (1 \leq i_1, i_2, i'_1, i'_2 \leq l).$$

Sense cap dubte veus ara que aquest procés es pot continuar. El completem fins a k vegades. Els resultats de la nostra construcció després del primer pas eren segments de llargada q_{k-1}, després del segon pas, segments de llargada q_{k-2}, etc. Després del pas k-èssim, per tant, els resultats de la nostra construcció són segments de llargada $q_0 = 1$, és a dir, són simplement nombres del nostre segment original Δ. Tot i així els denotem com abans per

$$\Delta_{i_1 i_2 \ldots i_k} \ (1 \leq i_1, i_2, \ldots, i_k \leq l').$$

Per a $1 \leq s \leq k$ i $1 \leq i_1, i_2, \ldots i_s, i'_1, i'_2, \ldots i'_s \leq l$ tenim

$$\Delta_{i_1, i_2, \ldots i_s} \approx \Delta_{i'_1, i'_2, \ldots i'_s}. \tag{2}$$

Fem ara dues observacions que són importants en el que segueix:

1. A (2), si $s < k$ i $i_{s+1}, i_{s+2}, \ldots, i_k$ són subíndexs arbitraris extrets de la seqüència $1, 2, \ldots, l, l'$, aleshores el nombre $\Delta_{i_1, i_2, \ldots i_s, i_{s+1}, \ldots, i_k}$ apareix en el segment $\Delta_{i_1, i_2, \ldots i_s}$ a la mateixa posició que el nombre $\Delta_{i'_1, i'_2, \ldots i'_s, i_{s+1}, \ldots, i_k}$ ho fa en el segment $\Delta_{i'_1, i'_2, \ldots i'_s}$. Com que aquests dos segments són del mateix tipus, d'acord amb (2), es dedueix que
$$\Delta_{i_1, i_2, \ldots i_s, i_{s+1}, \ldots, i_k} \approx \Delta_{i'_1, i'_2, \ldots i'_s, i_{s+1}, \ldots, i_k}, \tag{3}$$
sempre que $1 \leq i_1, i_2, \ldots i_s, i'_1, i'_2, \ldots i'_s \leq l$ i $1 \leq i_{s+1}, i_{s+2}, \ldots, i_k \leq l'$ $(1 \leq s \leq k)$.
2. Per a $s \leq k$ i $i'_s = i_s + 1$, els segments $\Delta_{i_1 \ldots i_{s-1} i_s}$ i $\Delta_{i_1 \ldots i_{s-1} i'_s}$ són òbviament consecutius en el pas s de la nostra construcció. Per tant, per a subíndexs arbitraris $i_{s+1} \ldots i_k$, els nombres $\Delta_{i_1 \ldots i_{s-1} i_s i_{s+1} \ldots i_k}$ i $\Delta_{i_1 \ldots i_{s-1} i'_s i_{s+1} \ldots i_k}$ apareixen en la mateixa posició en aquests dos segments, de manera que (amb $i'_s = i_s + 1$),
$$\Delta_{i_1 \ldots i_{s-1} i'_s i_{s+1} \ldots i_k} - \Delta_{i_1 \ldots i_{s-1} i_s i_{s+1} \ldots i_k} = d_s. \tag{4}$$

§ 6

Ara estem a prop del nostre objectiu. Considerem els $k+1$ nombres següents del segment Δ:

$$\begin{cases} a_0 = \Delta_{l'l'l'\ldots l'}, \\ a_1 = \Delta_{1l'l'\ldots l'}, \\ a_2 = \Delta_{11l'\ldots l'}, \\ \ldots \\ a_k = \Delta_{111\ldots 1}. \end{cases} \tag{5}$$

Com que el segment Δ està partit en k classes i tenim $k+1$ nombres a (5), dos d'aquests nombres pertanyen a la mateixa classe. Siguin a_r i a_s $(r<s)$ aquests dos nombres, de manera que

$$\Delta_{\underbrace{1\ldots 1}_{r}\underbrace{l'\ldots l'}_{k-r}} \approx \Delta_{\underbrace{1\ldots 1}_{s}\underbrace{l'\ldots l'}_{k-s}}. \tag{6}$$

Considerem els $l+1$ nombres

$$c_i = \Delta_{\underbrace{1\ldots 1}_{r}\underbrace{i\ldots i}_{s-r}\underbrace{l'\ldots l'}_{k-s}} \ (1 \le i \le l'). \tag{7}$$

Els primers l nombres d'aquest grup (és a dir, aquells amb $i<l'$) pertanyen a la mateixa classe d'acord amb (3). El darrer $(i=l')$, però, és de la mateixa classe que el primer d'acord amb (6). En conseqüència tots els $l+1$ nombres de (7) són del mateix tipus i, per provar la nostra afirmació, només ens queda veure que aquests nombres formen una progressió aritmètica, és a dir, que la diferència $c_{i+1}-c_i$ $(1 \le i \le l)$ no depèn de i.

Posem per brevetat $i+1=i'$. A més, sigui

$$c_{i,m} = \Delta_{\underbrace{1\ldots 1}_{r}\underbrace{i'\ldots i'}_{m}\underbrace{i\ldots i}_{s-r-m}\underbrace{l'\ldots l'}_{k-s}} \quad (0 \le m \le s-r),$$

de manera que $c_{i,0}=c_i$, $c_{i,s-r}=c_{i+1}$ i, per tant,

$$c_{i+1}-c_i = \sum_{m=1}^{s-r}(c_{i,m}-c_{i,m-1}).$$

D'acord amb (4) tenim

$$\begin{aligned} c_{i,m}-c_{i,m-1} &= \Delta_{\underbrace{1\ldots 1}_{r}\underbrace{i'\ldots i'}_{m}\underbrace{i\ldots i}_{s-r-m}\underbrace{l'\ldots l'}_{k-s}} - \Delta_{\underbrace{1\ldots 1}_{r}\underbrace{i'\ldots i'}_{m-1}\underbrace{i\ldots i}_{s-r-m+1}\underbrace{l'\ldots l'}_{k-s}} \\ &= d_{r+m}. \end{aligned}$$

Així doncs, la diferència

$$c_{i+1} - c_i = d_{r+1} + d_{r+2} + \ldots + d_s,$$

és efectivament independent de i, cosa que completa la demostració de la nostra afirmació.

Ja veus ara com pot ser de complicada de vegades una construcció completament elemental. I encara aquest no és un cas extrem: en el capítol següent trobaràs una altra construcció tan elemental com aquesta que és considerablement més complicada. D'altra banda, no es pot descartar que el teorema de Van der Waerden admeti una demostració encara més simple, i qualsevol investigació en aquesta direcció ha de ser benvinguda.

Capítol 2:
La hipòtesi de Landau–Schnirelmann i el teorema de Mann

§ 1

Probablement deus haver sentit parlar del teorema de Lagrange, que diu que *cada nombre natural és la suma de com a molt quatre quadrats*. En altres paraules, cada nombre natural és un quadrat d'un altre nombre o bé és la suma de dos d'aquests, o bé és la suma de tres o quatre d'aquests nombres quadrats. Per al propòsit que segueixo ens convé entendre de forma una mica diferent el contingut d'aquest teorema. Escrivim la seqüència de tots els quadrats perfectes, començant pel zero:

$$S = \{0, 1, 4, 9, 16, 25, \ldots\}. \tag{8}$$

Aquesta és una certa seqüència de nombres. Imagina quatre còpies idèntiques d'aquesta seqüència S: S_1, S_2, S_3, S_4. Ara triem un nombre arbitrari de cada còpia, $a_i^2 \in S_i$, $1 \leq i \leq 4$, i sumem aquests quatre nombres. La suma resultant

$$n = a_1^2 + a_2^2 + a_3^2 + a_4^2 \tag{9}$$

pot ser

1. zero (si $a_1 = a_2 = a_3 = a_4 = 0$);
2. el quadrat d'un nombre natural (si en alguna representació (9) del nombre n tres d'aquests nombres són zero i el quart és diferent de zero);
3. la suma de dos quadrats de nombres naturals (si en alguna representació (9) del nombre n algun parell d'aquests nombres són zero i els altres dos són diferents de zero);
4. la suma de tres quadrats de nombres naturals (si en alguna representació (9) del nombre n algun d'aquests nombres és zero i els altres tres són diferents de zero);

5. la suma de quatre quadrats de nombres naturals (si en alguna representació (9) del nombre n els quatre nombres són diferents de zero);

Així el nombre resultant n és o bé zero o bé és un nombre natural que es pot representar com a suma de com a molt quatre quadrats, i és clar que en sentit contrari cada nombre natural es pot obtenir mitjançant el procés que hem descrit.

Ara ordenem, per ordre de magnitud, tots els nombres naturals n que es poden obtenir d'aquesta manera (i.e., com a suma de quatre nombres triats respectivament de les seqüències S_1, S_2, S_3, S_4), en la seqüència

$$0, n_1, n_2, n_3, \ldots \tag{10}$$

(on $0 < n_1 < n_2 < n_3 < \ldots$, de manera que si alguns dels nombres que apareixen en l'ordenació són iguals, només un d'ells apareix en (10)). El teorema de Lagrange simplement assegura que la seqüència (10) conté tots els nombres naturals, és a dir, que $n_1 = 1$, $n_2 = 2$, $n_3 = 3$, etc.

Ara generalitzarem el nostre procés. Siguin k seqüències d'enters monòtones creixents que comencen amb zero.

$$A^{(1)} \qquad 0, a_1^{(1)}, a_2^{(1)}, \ldots, a_m^{(1)}, \ldots, \tag{11}$$

$$A^{(2)} \qquad 0, a_1^{(2)}, a_2^{(2)}, \ldots, a_m^{(2)}, \ldots, \tag{12}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots \tag{13}$$

$$A^{(k)} \qquad 0, a_1^{(k)}, a_2^{(k)}, \ldots, a_m^{(k)}, \ldots \tag{14}$$

Triem de manera arbitrària un sol nombre de cada seqüència $A^{(i)}$ ($1 \leq i \leq k$) i sumem aquests k nombres. La totalitat dels nombres obtinguts d'aquesta manera, ordenats segons les seves magnituds, porta a una nova seqüència del mateix tipus,

$$0, n_1, n_2, \ldots, n_m, \ldots, \tag{15}$$

que anomenarem la *suma* de les seqüències donades $A^{(1)}, A^{(2)}, \ldots, A^{(k)}$:

$$A = A^{(1)} + A^{(2)} + \ldots + A^{(k)} = \sum_{i=1}^{k} A^{(i)}.$$

El contingut del teorema de Lagrange ens diu que la suma $S+S+S+S$ conté la seqüència completa dels nombres naturals.

Potser has sentit parlar del famós teorema de Fermat, que diu que *la suma $S + S$ conté tots els nombres primers tals que la seva resta al dividir-los per quatre és 1* (és a dir, els nombres $5, 13, 17, 29, \ldots$). Potser també saps que el famós matemàtic soviètic Ivan Matveievitx Vinogradov va provar el següent notable teorema, en què molts dels més grans matemàtics dels dos segles anteriors havien estat treballant sense èxit.

Si denotem per P la seqüència

$$0, 2, 3, 5, 7, 11, 13, 17, \ldots \tag{16}$$

de tots els nombres primers començant per zero, aleshores la suma $P + P + P$ conté tots els nombres senars suficientment grans.

He citat aquí tots aquests exemples només amb un propòsit molt modest: familiaritzar-te amb el concepte de suma de seqüències de nombres i fer-te veure com alguns teoremes clàssics de teoria de nombres es poden formular de forma simple i convenient amb l'ajut d'aquest concepte.

§ 2

Tal com indubtablement deus haver observat, en tots els exemples mencionats estàvem interessats a mostrar que la suma d'un cert nombre de seqüències representa una seqüència que conté completament o bé quasi completament una certa classe de nombres (per exemple, tots els nombres naturals, tots els nombres senars suficientment grans, i altres de semblants). En tots els altres problemes similars, el propòsit de la investigació és provar que la suma de les seqüències de nombres representa un conjunt de nombres que és d'alguna manera "dens"en la seqüència dels nombres naturals. Sovint és el cas que aquest conjunt conté la seqüència completa dels nombres naturals (com vàrem veure en el primer exemple). El teorema de Lagrange diu que la suma de les quatre seqüències S conté la seqüència completa dels nombres naturals. Ara és costum anomenar la seqüència A una *base d'ordre k* (de la seqüència dels nombres naturals) si la suma de k seqüències idèntiques de A conté tots els nombres naturals. El teorema de Lagrange aleshores estableix que la seqüència S de quadrats perfectes és una base d'ordre quatre. Més tard es va provar que la seqüència de cubs perfectes forma una base d'ordre nou. Una petita reflexió mostra que cada base d'ordre k és també una base d'ordre $k + 1$.

En aquests i en molts altres exemples, la "densitat"de la suma que es vol conèixer queda determinada per propietats particulars de les seqüències que s'han sumat conjuntament, és a dir, per l'especial naturalesa aritmètica dels nombres que formen aquestes seqüències (sent aquests nombres naturals o bé quadrats perfectes, o bé primers, o també altres de naturalesa similar). Fa setze anys el distingit estudiant soviètic Lev Genrikhovitx Schnirelmann va proposar la qüestió següent: fins a quin punt la densitat de la suma de diverses seqüències depèn només de la densitat dels sumands, independentment de la seva naturalesa aritmètica. Aquest problema va resultar ser no només profund i interessant, sinó també útil per al tractament d'alguns problemes clàssics. Durant els quinze anys que ens precedeixen ha rebut l'atenció de molts estudiants d'elit, i ha donat lloc a una rica literatura.

Abans de poder establir problemes de forma precisa en aquest camp i escriure la paraula "densitat"sense cometes, és evident que primer ens hem de posar d'acord sobre quin nombre (o nombres) hem de fer servir per mesurar la "densitat"de les nostres seqüències (tal com en física les paraules "calent" i "fred"no adquireixen un significat científic precís fins que no hem après a mesurar la temperatura).

Una mesura molt convenient de la "densitat"d'una seqüència de nombres, que ara es fa servir per a tots els problemes científics del tipus que ens ocupa, va ser proposada per L. G. Schnirelmann. Sigui

$$0, a_1, a_2, \ldots, a_m, \ldots \tag{17}$$

una seqüència de nombres, on, com és habitual, tots els a_n són nombres naturals i $a_n < a_{n+1}$ $(n = 1, 2, \ldots)$. Denotem per $A(n)$ la quantitat de nombres naturals en la seqüència $A(n)$ que no excedeixen n (el zero no està comptat), de manera que $0 \leq A(n) \leq n$. Aleshores es compleix la desigualtat

$$0 \leq \frac{A(n)}{n} \leq 1.$$

La fracció $\frac{A(n)}{n}$, que naturalment per a diferents valors de n pren diferents valors, es pot interpretar, de manera òbvia, com un tipus de densitat mitjana de la seqüència (A) en el segment de 1 a n de la seqüència de nombres naturals. Seguint el suggeriment de Schnirelmann, la fita inferior més gran de tots els possibles valors d'aquesta fracció s'anomena la *densitat* de la seqüència (A) (dins de la seqüència completa dels nombres naturals). Denotarem aquesta densitat per $d(A)$.

Per familiaritzar-te amb les propietats elementals d'aquest concepte, et recomano que et convencis a tu mateix de la validesa dels teoremes següents:

1. Si $a_1 > 1$ (és a dir, la seqüència (A) no conté la unitat), aleshores $d(A) = 0$.
2. Si $a_n = 1 + r(n-1)$ (és a dir, començant amb a_1, és una progressió aritmètica amb terme inicial 1 i diferència r), aleshores $d(A) = 1/r$.
3. La densitat de qualsevol progressió geomètrica és zero.
4. La densitat de la seqüència de quadrats perfectes és zero.
5. Per tal que la seqüència (A) contingui la seqüència completa dels nombres naturals $(a_n = n, N = 1, 2, \ldots)$, és necessari i suficient que $d(A) = 1$.
6. Si $d(A) = 0$ i A conté el número 1, i si $\epsilon > 0$ és arbitrari, aleshores existeix un nombre suficientment gran m tal que $A(m) < \epsilon m$.

Si has provat tot això, estàs suficientment familiaritzat amb el concepte de densitat per ser capaç de fer-lo servir. Ara et vull familiaritzar amb la demostració del següent notable, encara que ben simple, lema de Schnirelmann:

$$d(A + B) \geq d(A) + d(B) - d(A)d(B). \tag{18}$$

El significat d'aquesta desigualtat és clar: la densitat de la suma de dues seqüències arbitràries de nombres no és menor que la suma de les seves densitats disminuïda pel producte d'aquestes densitats. Aquesta "desigualtat de Schnirelmann"representa la primera eina, encara massa crua, per estimar la densitat d'una suma a partir de les densitats dels sumands. Aquí tenim la seva demostració. Denotem per $A(n)$ la quantitat de nombres naturals que apareixen a la seqüència A i no excedeixen n, i per $B(n)$ el nombre anàleg per a la seqüència B. Per brevetat escrivim $d(A) = \alpha$, $d(B) = \beta$, $A + B = C$, $d(C) = \gamma$. El segment $(1, n)$ de la seqüència de nombres naturals conté $A(n)$ nombres de la seqüència A, cada un dels quals apareix a la seqüència C. Siguin a_k i a_{k+1} dos nombres consecutius d'aquest grup. Entre ells hi ha $a_{k+1} - a_k - 1 = l$ nombres que no pertanyen a A. Aquests nombres són

$$a_k + 1, a_k + 2, \ldots, a_k + l = a_{k+1} - 1.$$

Alguns d'ells apareixen a C; per exemple, tots els nombres de la forma $a_k + r$, on r pertany a B (i ho escrivim de la forma següent: $r \in B$). De

tota manera, hi ha tants nombres d'aquesta última classe com nombres hi ha a B en el segment $(1, l)$, això és, $B(l)$ nombres. En conseqüència, cada segment de longitud l inclòs entre dos nombres consecutius de la seqüència A conté com a mínim $B(l)$ nombres que pertanyen a C. Per tant el nombre, $C(n)$, de nombres del segment $(1, n)$ que apareixen a C és com a mínim

$$A(n) + \Sigma B(l)$$

on el sumatori s'estén a tots els segments que estan lliures de nombres que apareixen a A. D'acord amb la definició de densitat, $B(l) \geq \beta l$, de manera que

$$C(n) \geq A(n) + \beta \Sigma l = A(n) + \beta(n - A(n)),$$

ja que Σl és la suma de les longituds de tots els segments que estan lliures d'elements que apareixen a A, el qual és simplement el nombre $n - A(n)$ de nombres del segment $(1, n)$ que no són a A. Però $A(n) \geq \alpha n$, i per tant

$$C(n) \geq A(n)(1 - \beta) + \beta n \geq \alpha n(1 - \beta) + \beta n,$$

la qual cosa ens porta a

$$C(n)/n \geq \alpha + \beta - \alpha\beta.$$

Com que aquesta desigualtat es compleix per a qualsevol nombre natural n, tenim

$$\gamma = d(C) \geq \alpha + \beta - \alpha\beta.$$

Q.E.D.

La desigualtat de Schnirelmann (18) es pot escriure de forma equivalent

$$1 - d(A + B) \leq (1 - d(A))(1 - d(B)),$$

i d'aquesta manera es pot generalitzar fàcilment al cas d'un nombre arbitrari de sumands:

$$1 - d(A_1 + A_2 + \ldots + A_k) \leq \prod_{i=1}^{k} (1 - d(A_i)).$$

Es prova per simple inducció; no has de tenir cap problema per sortir-te'n tu mateix. Si escrivim l'última desigualtat de la forma

$$d(A_1 + A_2 + \ldots + A_k) \geq 1 - \prod_{i=1}^{k} (1 - d(A_i)), \tag{19}$$

això ens permet estimar una altra vegada la densitat d'una suma a partir de la densitat dels sumands. L. G. Schnirelmann va obtenir una sèrie de resultats destacables a partir d'aquesta elemental desigualtat, i va obtenir sobretot aquest important teorema:

Cada seqüència amb densitat positiva és una base de la seqüència de nombres naturals.

En altres paraules, si $\alpha = d(A) > 0$, aleshores la suma d'un nombre suficientment gran de seqüències A conté la seqüència completa de nombres naturals. La demostració d'aquest teorema és tan simple que m'agradaria explicar-te-la, encara que això ens distregui una mica del nostre problema immediat.

Denotem, per abreujar, la suma de k seqüències per A_k, cadascuna de les quals coincideix amb A. Aleshores, gràcies a la desigualtat (19),

$$d(A_k) \geq 1 - (1 - \alpha)^k.$$

Com que $\alpha > 0$, tenim, per a una k suficientment gran,

$$d(A_k) > 1/2. \tag{20}$$

Ara es pot veure fàcilment que la seqüència A_{2k} conté la seqüència completa de nombres naturals. Aquesta és una simple conseqüència de la proposició general següent.

LEMA 1 *Si $A(n) + B(n) > n - 1$, aleshores n és a $A + B$.*

De fet, si n és a A o a B, queda tot provat. Podem suposar per tant que n no és a A ni a B. Aleshores $A(n) = A(n-1)$ i $B(n) = B(n-1)$ i en conseqüència

$$A(n-1) + B(n-1) > n - 1.$$

Ara, siguin $a_1, a_2, \ldots, a_r$ i $b_1, b_2, \ldots, b_s$ els nombres del segment $(1, n-1)$ que són a A i a B respectivament, així $r = A(n-1)$ i $s = B(n-1)$. Aleshores tots els nombres

$$a_1, a_2, \ldots, a_r,$$

$$n - b_1, n - b_2, \ldots, n - b_s$$

pertanyen al segment $(1, n-1)$. Hi ha $r + s = A(n-1) + B(n-1)$ d'aquests nombres, una quantitat més gran que $n - 1$. Per tant un dels nombres de la fila superior és igual a un dels nombres de la fila inferior. Sigui $a_i = n - b_k$. Aleshores $n = a_i + b_k$, és a dir, n és a $A + B$.

Tornant ara al nostre objectiu, tenint en compte (20), per a un n arbitrari:

$$A_k(n) > \frac{n}{2} + \frac{n-1}{2}$$

i per tant

$$A_k(n) + A_k(n) > n - 1.$$

D'acord amb el lema que acabem de provar, deduïm que n és a $A_k + A_k = A_{2k}$. Però n és un nombre natural arbitrari, i per tant el nostre teorema queda provat.

Aquest simple teorema porta a una sèrie d'aplicacions importants que apareixen en els articles de L. G. Schnirelmann. Per exemple, ell va ser el primer a provar que la seqüència P, formada per la unitat i tots els nombres primers, és una base de la seqüència de nombres naturals. La seqüència P, certament, té densitat zero, tal com Euler ja havia provat, de manera que el teorema que acabem de provar no es pot aplicar directament. Pero Schnirelmann va ser capaç de provar que $P + P$ tenia densitat positiva. Amb la qual cosa $P + P$ forma una base, i per tant P també. A partir d'aquí és fàcil inferir que un nombre natural arbitrari, amb l'excepció de l'u, pot, per a una k suficientment gran, ser representat com la suma d'almenys k primers. En aquell temps (1930) aquest resultat va ser fonamental i va provocar el màxim interès en el món científic. En aquests moments, gràcies al treball remarcable de I. M. Vinogradov, sabem considerablement més en aquesta direcció, tal com ja t'he mencionat al començament d'aquest capítol.

§ 3

En el que precedeix, el meu propòsit era el d'introduir-te pel camí més curt possible al problema d'aquesta singular i fascinant branca de la teoria de nombres, l'estudi de la qual va començar amb el destacat treball de L. G. Schnirelmann. El propòsit immediat d'aquest capítol és un problema en aquest camp, i ara procedeixo a formular-lo.

Durant la tardor de 1931, després de tornar d'un viatge, L. G. Schnirelmann ens va comunicar les seves converses amb Landau a Göttingen, i entre altres coses va dir que durant aquelles converses varen descobrir l'interessant fet que segueix: en tots els exemples concrets que varen ser capaços d'observar, era possible reemplaçar la desigualtat

$$d(A + B) \geq d(A) + d(B) - d(A)d(B),$$

que vàrem obtenir a § 2, per la desigualtat més precisa i més curta

$$d(A+B) \geq d(A) + d(B). \tag{21}$$

Això és, la densitat de la suma sempre resulta ser com a mínim tan gran com la suma de les densitats dels sumands (amb la suposició, per descomptat, que $d(A) + d(B) \leq 1$). Ells naturalment varen suposar que la desigualtat (21) era l'expressió d'una llei universal, però els primers intents per provar aquesta conjectura varen ser desafortunats. Tot d'una va ser evident que si la seva conjectura era correcta, el camí cap a la seva demostració seria bastant difícil. Arribats a aquest punt, volem fer notar que si la hipotètica desigualtat (21) representa una llei universal, aleshores aquesta llei es pot generalitzar, de manera immediata, per inducció al cas d'un nombre arbitrari de sumands; és a dir, sota la hipòtesi que

$$\sum_{i=1}^{k} d(A_i) \leq 1$$

tenim

$$d(\sum_{i=1}^{k} A_i) \geq \sum_{i=1}^{k} d(A_i). \tag{22}$$

Aquest problema no podia sinó atraure l'atenció dels investigadors, a causa de la simplicitat i elegància de l'hipotètica llei (21) d'una banda, i de l'altra degut a l'enorme contrast entre el caràcter elemental del problema i la dificultat de la seva solució que ja va fer-se evident després dels primers atacs. Jo mateix estava fascinat pel problema en aquell temps, i vaig deixar totes les meves altres investigacions per dedicar-m'hi. A començaments del 1932, després d'uns quants mesos de feina dura, vaig aconseguir demostrar la desigualtat (21) per al cas més important, $d(A) = d(B)$ (aquest cas ha de ser considerat com el més important ja que en la majoria dels problemes concrets tots els sumands són iguals). Al mateix temps vaig provar la desigualtat general (22) amb la condició que $d(A_1) = d(A_2) = \ldots = d(A_k)$ (és fàcil veure que aquest resultat no es pot deduir a partir de l'anterior per simple inducció, sinó que demana una demostració específica). El mètode que vaig fer servir era completament elemental, però molt complicat. Després vaig ser capaç de simplificar una mica la demostració.

Sigui com sigui, no era més que un cas especial. Durant molt temps em semblava que alguna millora subtil del meu mètode podia conduir

a una solució completa del problema, però tots els meus esforços en aquesta direcció varen resultar ser infructífers.

Al mateix temps, la publicació del meu treball va atraure l'atenció d'un ampli cercle d'estudiosos d'arreu del món cap a la hipòtesi de Landau-Schnirelmann. Es varen obtenir molts resultats insignificants, i va aparèixer un munt de literatura respecte a això. Alguns autors varen portar el problema del domini dels nombres naturals a altres camps. Dit d'una altra manera, el problema esdevingué un problema de "moda". Diverses societats il·lustrades oferien premis per a la seva solució. Els meus amics matemàtics d'Anglaterra em varen escriure l'any 1935 que una bona part dels matemàtics anglesos havien posposat la seva feina habitual per intentar resoldre el problema. Landau, en el seu tractat dedicat als últims avenços en teoria additiva de nombres, va escriure que "li agradaria atraure l'atenció del lector cap a aquest problema". El problema, però, era obstinat, i va malmetre durant una sèrie d'anys els esforços dels estudiants més capacitats. No va ser fins a l'any 1942 que Mann, el jove matemàtic americà, va trobar finalment una demostració completa de la desigualtat (21) (i per tant també de la desigualtat (22)). El seu mètode és completament elemental i està relacionat amb el meu treball sobre això, encara que es basa en una idea completament diferent. La demostració és llarga i molt complicada, i no em sento capaç de presentar-te-la aquí. Un any després, el 1943, Artin i Scherk varen publicar una nova demostració del mateix teorema, basada en una idea diferent. És considerablement més curta i més transparent, tot i que encara bastant elemental. Aquesta és la demostració que m'agradaria presentar-te; he escrit aquest capítol per explicar-te-la, i forma el contingut de totes les seccions que segueixen.

§ 4

Suposa que A i B són dues seqüències. Diem $A + B = C$. Escrivim $A(n)$, $d(A)$, etc., amb el seu significat habitual. Recordem que comencem totes les nostres seqüències amb zero, però que només considerem els nombres naturals que apareixen en aquestes seqüències quan calculem $A(n)$, $B(n)$, $C(n)$. Hem de provar que

$$d(C) \geq d(A) + d(B) \tag{23}$$

sempre que $d(A) + d(B) \leq 1$. Per abreujar diem $d(A) = \alpha$, $d(B) = \beta$ en el que segueix.

Lema 2 (Fonamental) *Si n és un nombre natural arbitrari, existeix un enter m $(1 \leq m \leq n)$ tal que*

$$C(n) - C(n-m) \geq (\alpha + \beta)m.$$

En altres paraules, existeix un "tros"$(n-m+1, n)$ del segment $(1, n)$ en el qual la densitat mitjana de la seqüència C és com a mínim $\alpha + \beta$.

Ara ens encarem amb dos problemes: primer, provar el lema fonamental, i segon, veure que la desigualtat (23) s'obté a partir del lema fonamental. El segon d'aquests problemes és incomparablement més fàcil que el primer, i començarem per tant amb el segon problema.

Suposa que el lema fonamental ja està provat. Això significa que en un cert "tros"$(n-m+1, n)$ del segment $(1, n)$ la densitat mitjana de la seqüència C és com a mínim $\alpha + \beta$. Pel lema fonamental, el segment $(1, n-m)$ té també un cert "tros"$(n-m-m'+1, n-m)$ en el qual la densitat mitjana de C és com a mínim $\alpha + \beta$. És clar que si continuem aquest procés, el segment $(1, n)$ queda dividit en un nombre finit de subsegments, i en cadascun d'ells la densitat mitjana de C és com a mínim $\alpha + \beta$. Per tant la densitat mitjana de C és també $\alpha + \beta$ en tot el segment $(1, n)$. Com que n era arbitrari, tenim

$$d(C) \geq \alpha + \beta. \qquad \text{Q. E. D.}$$

Així el problema es redueix a provar el lema fonamental. Ara tornem a aquesta demostració, que és llarga i complicada.

§ 5

SEQÜÈNCIES NORMALS

En tot el que segueix hem de considerar el nombre n com a fix i totes les seqüències que investiguem estaran formades pel zero i certs nombres del segment $(1, n)$. Decidim anomenar una tal seqüència N *normal*, si té la propietat següent: si els nombres arbitraris f i f' del segment $(1, n)$ no apareixen a N, el nombre $f + f' - n$ tampoc no apareix a N (on el cas $f = f'$ no està exclòs).

Si el nombre n pertany a la seqüència C, aleshores

$$C(n) - C(n-1) = 1 \geq (\alpha + \beta)1,$$

i per tant el lema fonamental és trivialment correcte ($m = 1$). Com a conseqüència, en el que segueix, assumirem –et prego que ho tinguis present– que n no pertany a C.

Per començar, el lema fonamental és fàcil de demostrar en el cas en què la seqüència C és normal. De fet, denotem per m el nombre positiu més petit que no apareix a C ($m \leq n$ ja que n, per hipòtesi, no pertany a C). Sigui s un nombre enter arbitrari, comprès entre $n - m$ i n; $n - m < s < n$. Aleshores, $0 < s + m - n < m$. Afirmo que $s \in C$. Si no és el cas, el nombre $s + m - n$, a causa de la normalitat de C, no pot aparèixer a C. Però acabem de veure que aquest nombre és més petit que m, mentre que m, per definició, és l'enter positiu més petit que no apareix a C.

Per tant tots els nombres s del segment $n - m < s < n$ apareixen a C, i així

$$C(n) - C(n - m) = m - 1.$$

D'altra banda, pel lema 1, com que m no és de $C = A + B$ tenim $A(m) + B(m) \leq m - 1$. Consegüentment

$$C(n) - C(n - m) \geq A(m) + B(m) \geq (\alpha + \beta)m, \tag{24}$$

que novament prova la validesa del lema fonamental.

§ 6

EXTENSIONS CANÒNIQUES

Ara centrem la nostra atenció al cas en què la seqüència $C = A + B$ no és normal. En aquest cas afegirem al conjunt B nombres que no conté, d'acord amb un esquema molt precís, i així passarem de B a una seva extensió B_1. Aleshores, evidentment, el conjunt $C_1 = A + B_1$ serà una extensió del conjunt C. Tal com he dit abans, aquesta extensió dels conjunts B i C (el conjunt A es manté inalterat) es definirà de forma precisa; això és possible si i només si el conjunt C no és normal. Anomenarem aquesta extensió una *extensió canònica* dels conjunts B i C. Deduirem algunes propietats importants de les extensions canòniques, amb l'ajuda de les quals la demostració del lema fonamental quedarà completada.

Ara procedeixo a la definició de les extensions canòniques dels conjunts B i C. Si C no és normal, existeixen dos nombres c i c' en el segment $(0, n)$, tals que

$$c \notin C, \;\; c' \notin C, \;\; c + c' - n \in C.$$

Com que $C = A + B$, tenim

$$c + c' - n = a + b, \quad (a \in A, \; b \in B). \tag{25}$$

Sigui β_0 el nombre més petit del conjunt B que pot exercir el paper del nombre b en l'equació (25). En altres paraules, β_0 és l'enter més petit $b \in B$ que satisfà l'equació (25) per a nombres adequadament triats, $c \notin C$, $c' \notin C$, $a \in A$, en el segment $(0, n)$. Aquest nombre β_0 serà la *base* de les nostres extensions.

Així l'equació

$$c + c' - n = a + \beta_0 \tag{26}$$

ha de tenir solucions per als nombres c, c', a que satisfan les condicions

$$c \notin C, \;\; c' \notin C, \;\; a \in A,$$

on els tres nombres pertanyen al segment $(0, n)$.

Considerem tots els nombres c i c' que satisfan l'equació (26) i compleixen les condicions prèvies, per formar un conjunt C^*. Evidentment els conjunts C i C^* no tenen cap element en comú. Anomenem la seva unió (és a dir, tots els nombres de C o de C^*)

$$C \cup C^* = C_1$$

l'extensió canònica del conjunt C.

Examinem ara l'expressió $\beta_0 + n - c$. Si admetem que c recorre tots els valors dels nombres del conjunt C^* que acabem de construir, els valors d'aquesta expressió formen un cert conjunt B^*. D'acord amb l'equació (26), cadascun d'aquests nombres $\beta_0 + n - c$ ($c \in C^*$) es pot escriure de la forma $c' - a$ on $c' \in C^*$, $a \in A$.

Sigui b^* un nombre arbitrari que pertany a B^*. Com que és de la forma $\beta_0 + n - c$, és $\geq \beta_0 \geq 0$; i com que també és de la forma $c' - \alpha$ ($c' \in C^*$, $a \in A$), és $\leq c' \leq n$. Així tots els nombres del conjunt B^* pertanyen al segment $(0, n)$. A més, si $b^* \in B^*$, aleshores $b^* \notin B$, si no deduiriem a partir de $b^* = c' - \alpha$ que $c' = a + b^* \in A + B = C$, la qual cosa és falsa.

Així, el conjunt B^* es troba dins del segment $(0, n)$ i no té elements en comú amb el conjunt B. Posem

$$B \cup B^* = B_1$$

i anomenem el conjunt B_1 una extensió canònica del conjunt B.

Provem que

$$A + B_1 = C_1.$$

Per començar, sigui $a \in A$, $b_1 \in B_1$. Provarem que $a + b_1 \in C_1$. Sabent que $b_1 \in B_1$ deduïm que o bé $b_1 \in B$ o bé $b_1 \in B^*$. Si $b_1 \in B$, aleshores $a+b_1 \in A+B = C \subset C_1$. Si $b_1 \in B^*$, en canvi, aleshores o bé $a+b_1 \in C$, i per tant també pertany a C_1, o bé $a + b_1 \notin C$. En aquest cas, però (com que b_1, com a element de B^*, és de la forma $\beta_0 + n - c'$, $c' \notin C$), obtenim

$$c = a + b_1 = a + \beta_0 + n - c' \notin C.$$

Per tant

$$c + c' - n = a + \beta_0 \in A + B = C,$$

on $c \notin C$ i $c' \notin C$. Però, d'acord amb la definició del conjunt C^*,

$$c = a + b_1 \in C^* \subset C_1. \qquad \text{Q. E. D.}$$

Així hem provat que $A + B_1 \subset C_1$.

Per provar la relació inversa, suposem que $c \in C_1$, la qual cosa significa que o bé $c \in C$ o bé $c \in C^*$. Si $c \in C$, aleshores $c = a + b$, $a \in A$, $b \in B \subset B_1$. Si $c \in C^*$, aleshores, per a un cert $a \in A$, el nombre $b^* = c - a$, com ja sabem, és de B^*. Tenim $c = a + b^* \in A + B^* \subset A + B_1$. Així $C_1 \subset A + B_1$. També hem provat més amunt que $A + B_1 \subset C_1$. Consegüentment $C_1 = A + B_1$.

Ara recordem que, d'acord amb la nostra hipòtesi, $n \notin C$. És fàcil veure –i això és important– que el nombre n no apareix a l'extensió de C_1. Pensem que si $n \in C^*$, aleshores és possible, per la definició de C^*, posar $c' = n$ en l'equació (26), la qual ens diu que $c = a + \beta_0 \in A + B = C$, mentre que $c \notin C$ d'acord amb (26).

Si la seqüència estesa C_1 encara no és normal, aleshores, com que $A + B_1 = C_1$ i $n \notin C_1$, els conjunts A, B_1 i C_1 formen un triplet amb totes les propietats del triplet A, B, C que són necessàries per a una nova extensió canònica. Prenem una nova base β_1 d'aquesta extensió, definim els conjunts complementaris B_1^*, C_1^* igual que abans, i escrivim

$$B_1 \cup B_1^* = B_2, \quad C_1 \cup C_1^* = C_2.$$

Un cop més estem en condicions d'afirmar que $A+B_2 = C_2$ i $n \notin C_2$. És evident que aquest procés es pot continuar fins que una de les extensions C_h arribi a ser normal. Clarament aquest cas ha d'arribar, ja que en cada extensió afegim nous nombres als conjunts B_μ i C_μ sense sobrepassar els extrems del segment $(0, n)$.

D'aquesta manera obtenim les seqüències finites de conjunts

$$B = B_0 \subset B_1 \subset \ldots \subset B_h,$$

$$C = C_0 \subset C_1 \subset \ldots \subset C_h,$$

on cada $B_{\mu+1}$ (respectivament $C_{\mu+1}$) conté nombres que no apareixen a B_μ (C_μ) i això ens dóna el conjunt B^*_μ (C^*_μ), demanera que

$$B_{\mu+1} = B_\mu \cup B^*_\mu, \quad C_{\mu+1} = C_\mu \cup C^*_\mu \quad (0 \leq \mu \leq h-1).$$

Denotem per β_μ la base de l'extensió que porta $(B_\mu,\ C_\mu)$ dins de $(B_{\mu+1},\ C_{\mu+1})$. Tenim

$$A + B_\mu = C_\mu, \quad n \notin C_\mu \quad (0 \leq \mu \leq h).$$

Finalment, el conjunt C_h és normal, mentre que els conjunts C_μ $(0 \leq \mu \leq h-1)$ no ho són.

§ 7

PROPIETATS DE LES EXTENSIONS CANÒNIQUES

Ara hem de formular i provar en forma de tres lemes aquelles propietats de les extensions canòniques que necessitarem més endavant. Només el lema 5 tindrà aplicacions posteriors; els lemes 3 i 4 només es necessiten per provar el lema 5.

LEMA 3 $\beta_\mu > \beta_{\mu-1}$ $(1 \leq \mu \leq h-1)$*; és a dir, les bases de les extensions canòniques successives formen una seqüència monòtona creixent.*

De fet, com que $\beta_\mu \in B_\mu = B_{\mu-1} \cup B^*_{\mu-1}$, o bé $\beta_\mu \in B^*_{\mu-1}$ o bé $\beta_\mu \in B_{\mu-1}$. Si $\beta_\mu \in B^*_{\mu-1}$, aleshores β_μ és de la forma

$$\beta_\mu = \beta_{\mu-1} + n - c,$$

on $c \in C^*_{\mu-1} \subset C_\mu$ i per tant $c < n$, i així $\beta_\mu > \beta_{\mu-1}$, i el lema 3 queda provat. Si $\beta_\mu \in B_{\mu-1}$, aleshores per definició del nombre β_μ existeixen enters $a \in A$, $c \notin C_\mu$, $c' \notin C_\mu$ tals que

$$c + c' - n = a + \beta_\mu \in C_\mu.$$

Però per a $\beta_\mu \in B_{\mu-1}$, tenim

$$c + c' - n = a + \beta_\mu \in A + B_{\mu-1} = C_{\mu-1}, \tag{27}$$

on $c \notin C_{\mu-1}$, $c' \notin C_{\mu-1}$. Així, gràcies a la propietat de minimalitat de $\beta_{\mu-1}$, $\beta_\mu \geq \beta_{\mu-1}$. Si $\beta_\mu = \beta_{\mu-1}$, deduïm a partir de (27) i la definició del conjunt $C^*_{\mu-1}$ que

$$c \in C^*_{\mu-1} \subset C_\mu, \quad c' \in C^*_{\mu-1} \subset C_\mu.$$

Totes dues, però, són falses, i per tant, $\beta_\mu > \beta_{\mu-1}$.

En el que segueix denotarem per m l'enter positiu més petit que no apareix a C_h.

LEMA 4 *Si $c \in C^*_\mu$ $(0 \leq \mu \leq h-1)$ i $n - m < c < n$, aleshores $c > n - m + \beta_\mu$. Això és, tots els nombres c del conjunt C^*_μ que es troben en l'interval $n - m < c < n$ es troben sobre la part d'aquest segment que es caracteritza per les desigualtats $n - m + \beta_\mu < c < n$.*

Hem de veure que

$$c + m - n > \beta_\mu.$$

A partir de $n - m < c < n$ deduïm que

$$0 < m + c - n < m.$$

Així, per definició del nombre m,

$$m + c - n \in C_h.$$

Ara

$$C_h = C_\mu \cup C^*_\mu \cup C^*_{\mu+1} \cup \ldots \cup C^*_{h-1}.$$

Considerem dos casos,

1. Si $m + c - n \in C_\mu$, aleshores

$$m + c - n = a + b_\mu, \quad a \in A, \ \ b_\mu \in B_\mu.$$

Però $m \notin C_\mu$ i $c \notin C_\mu$ (la darrera ja que $c \in C_\mu^*$). Fent servir la propietat de minimalitat de β_μ tenim $b_\mu \geq \beta_\mu$. Si $b_\mu = \beta_\mu$, gràcies a la definició del conjunt C_μ^* tenim que $m \in C_\mu^*$, la qual cosa és falsa ja que $C_\mu^* \subset C_{\mu+1}^* \subset C_h$ i $m \notin C_h$. Com a conseqüència $b_\mu > \beta_\mu$, i per tant

$$m + c - n = a + b_\mu \geq b_\mu > \beta_\mu,$$

així el lema 4 queda provat.

2. Si $c' = m + c - n \in C_\nu^*$ $(\mu \leq \nu \leq h-1)$, aleshores, per la definició del conjunt C_ν^*, c' satisfà una equació de la forma (26),

$$c' - a = \beta_\nu + n - c'',$$

on $a \in A$, $c'' \in C_\nu^*$. Amb la qual cosa tenim $c' \geq c' - a > \beta_\nu \geq \beta_\mu$ (on la darrera desigualtat ve donada pel lema 3), i el lema 4 queda també provat.

LEMA 5 *Tenim*

$$C_\mu^*(n) - C_\mu^*(n-m) = B_\mu^*(m-1) \qquad (0 \leq \mu \leq h-1).$$

Això és, el nombre d'enters $c \in C_\mu^*$ que es troben en el segment $n - m < c < n$ és exactament el mateix que el nombre d'enters $b \in B_\mu^*$ en el segment $0 < b < m$ (de la mateixa longitud).

Examinem la relació

$$b = \beta_\mu + n - c. \tag{28}$$

Per la mateixa definició dels conjunts B_μ^* i C_μ^*, $c \in C_\mu^*$ implica $b \in B_\mu^*$, i inversament. Si, a més, $n - m + \beta_\mu < c < n$, aleshores $\beta_\mu < b < m$, i en sentit contrari. Per tant

$$C_\mu^*(n) - C_\mu^*(n - m + \beta_\mu) = B_\mu^*(m-1) - B_\mu^*(\beta_\mu).$$

Pel lema 4, $C_\mu^*(n - m + \beta_\mu) = C_\mu^*(n-m)$. D'altra banda, cada $b \in B_\mu^*$ es pot expressar en la forma (28), on $c < n$; així b excedeix β_μ^*, i consegüentment $B_\mu^*(\beta_\mu^*) = 0$. Per tant

$$C_\mu^*(n) - C_\mu^*(n-m) = B_\mu^*(m-1). \qquad \text{Q. E. D.}$$

§ 8

DEMOSTRACIÓ DEL LEMA FONAMENTAL

És molt fàcil ara provar el lema fonamental a partir dels resultats de § 5 i fent servir el lema 5 que acabem de provar.

Si apliquem el resultat de § 5 en la forma de la desigualtat (24) a les seqüències A, B_h i C_h (cosa que podem fer gràcies a la normalitat de C_h), trobem que

$$C_h(n) - C_h(n-m) \geq A(m) + B_h(m), \tag{29}$$

on m és l'enter positiu més petit que no és a C_h. Òbviament $m \notin A$ i $m \notin B_h$, per tant podem escriure $A(m-1)$ i $B_h(m-1)$ en lloc de $A(m)$ i $B_h(m)$, respectivament.

Tenim

$$C_h = C \cup C^* \cup C_1^* \cup \ldots \cup C_{h-1}^*,$$

$$B_h = B \cup B^* \cup B_1^* \cup \ldots \cup B_{h-1}^*,$$

on els conjunts que apareixen a cadascuna d'aquestes unions són disjunts dos a dos, així

$$C_h(n) - C_h(n-m) = C(n) - C(n-m) + \sum_{\mu=0}^{h-1}(C_\mu^*(n) - C_\mu^*(n-m)),$$

$$B_h(m) = B_h(m-1) = B(m-1) + \sum_{\mu=0}^{h-1} B_\mu^*(m-1);$$

per descomptat, hem posat $C_0^* = C^*$, $B_0^* = B^*$. D'acord amb (29) tenim

$$C(n) - C(n-m) + \sum_{\mu=0}^{h-1}(C_\mu^*(n) - C_\mu^*(n-m))$$

$$\geq A(m) + B(m-1) + \sum_{\mu=0}^{h-1} B_\mu^*(m-1).$$

Pel lema 5, però,

$$C_\mu^*(n) - C_\mu^*(n-m) = B_\mu^*(m-1) \qquad (0 \leq \mu \leq h-1),$$

així la desigualtat anterior esdevé

$$C(n) - C(n-m) \geq A(m) + B(m-1) = A(m) + B(m) \geq (\alpha + \beta)m,$$

la qual cosa prova el lema fonamental.

Tal com vàrem veure a § 4, això completa la demostració del teorema de Mann que resol el problema mètric fonamental de la teoria additiva de nombres.

No trobes que la construcció d'Artin i Scherk té el segell d'una obra mestra? Trobo aquest mètode, amb la seva estranya combinació d'estructura refinada i extraordinària forma elemental, especialment atractiu.

Capítol 3:
Una solució elemental del Problema de Waring

§ 1

Deus recordar el teorema de Lagrange, que vàrem discutir al començament del capítol anterior. Aquest deia que cada nombre natural es pot expressar com una suma de com a molt quatre quadrats. També et vaig mostrar com aquest teorema es pot expressar en termes completament diferents: Si quatre seqüències, cadascuna idèntica a

$$(A_2): \quad 0, 1^2, 2^2, \ldots, k^2, \ldots, \tag{30}$$

se sumen conjuntament, la seqüència resultant conté tots els nombres naturals. O fins i tot de forma més breu, la seqüència (A_2) és una base (de la seqüència dels nombres naturals) d'ordre quatre. També vaig mencionar-te que més tard s'havia provat que la seqüència de cubs

$$(A_3): \quad 0, 1^3, 2^3, \ldots, k^3, \ldots \tag{31}$$

és una base d'ordre nou. Tots aquests fets porten de manera natural a la hipòtesi que diu que per a un nombre natural arbitrari n, la seqüència

$$(A_n): \quad 0, 1^n, 2^n, \ldots, k^n, \ldots, \tag{32}$$

és una base (l'ordre de la qual òbviament depèn de n). Aquesta conjectura de fet va ser proposada per Waring ja al segle $XVIII$. De tota manera, es va veure que el problema era molt difícil, i no va ser fins a començaments d'aquest segle que la validesa de la hipòtesi de Waring va ser provada, per Hilbert (1909). La demostració del Hilbert no només és feixuga en el seu aspecte formal i es basa en teories analítiques complicades (integrals múltiples), sinó que també està mancada de transparència conceptual. L'eminent matemàtic francès Poincaré va escriure en el seu assaig sobre el treball científic creatiu de Hilbert, que tan bon punt les motivacions bàsiques que són darrere d'aquesta demostració s'entenguessin, probablement sortirien resultats aritmètics de gran

importància, com d'un calidoscopi. En un cert sentit tenia raó. Deu o quinze anys més tard, varen aparèixer noves demostracions del teorema de Hilbert obtingudes per Hardy i Littlewood a Anglaterra i per I. M. Vinogradov a la Unió Soviètica. Aquestes demostracions eren una altra vegada analítiques i formalment feixugues, però diferien favorablement de la demostració de Hilbert per la seva transparència en el mètode i en la seva simplicitat conceptual, que no deixaven res a desitjar. De fet, a causa d'això, els dos mètodes esdevingueren fonts potents de nous teoremes aritmètics.

Quan la nostra ciència, però, tracta amb un problema tan completament elemental com el problema de Waring, invariablement pretén trobar una solució que no requereixi conceptes o mètodes que transcendeixin els límits de l'aritmètica elemental. La recerca d'una demostració elemental de la hipòtesi de Waring és el tercer problema que m'agradaria comentar-te. Aquesta demostració elemental del teorema de Hilbert va ser obtinguda per primera vegada l'any 1942, pel jove estudiant soviètic I. V. Linnik.

Ja estàs acostumat al fet que "elemental"no vol dir "simple". La solució elemental del problema de Waring que va descobrir Linnik tampoc no és, tal com veuràs, gaire simple, i requerirà per part teva un considerable esforç per entendre-la i digerir-la. M'haig d'esforçar per fer que aquesta tasca, de seguir la meva exposició, et sigui tan fàcil com sigui possible. Però has de recordar que en matemàtiques (com probablement en qualsevol altra ciència) l'assimilació de qualsevol cosa realment valuosa i significativa és una tasca dura.

Les idees de Schnirelmann que et vaig descriure al començament del segon capítol tenen un paper essencial en la demostració de Linnik. Potser recordes (ho vaig mencionar aleshores) com Schnirelmann va provar el seu famós teorema que la seqüència P que inclou zero, u i tots els nombres primers és una base de la seqüència dels nombres naturals. Ell va provar que la seqüència $P + P$ té densitat positiva. Això prova immediatament l'afirmació, ja que, d'acord amb el teorema general de Schnirelmann que vam provar, cada seqüència amb densitat positiva és una base de la seqüència dels nombres naturals. El mateix mètode també és a la base de la demostració del teorema de Hilbert descoberta per Linnik. Així, tot es redueix a provar que la suma d'un nombre suficientment gran de seqüències (A_n) és una seqüència amb densitat positiva. Tot d'una que això se satisfà, podem, en virtut del mateix teorema general de Schnirelmann, veure provat el teorema de Hilbert.

§ 2

EL LEMA FONAMENTAL

Si sumem k seqüències, idèntiques a A_n, d'acord amb la regla del capítol 2, evidentment obtenim la seqüència $A_n^{(k)}$ que conté el zero i tots aquells nombres naturals que es poden expressar com a suma de com a molt k sumands de la forma x^m, on x és un nombre natural arbitrari. En altres paraules, el nombre m pertany a la seqüència $A_n^{(k)}$, si l'equació

$$x_1^n + x_2^n + \ldots + x_k^n = m \tag{33}$$

té solució en els enters no negatius x_i $(1 \leq i \leq k)$. Tal com vàrem veure a § 1, el problema és provar que, per a valors suficientment grans de k, la seqüència $A_n^{(k)}$ té densitat positiva.

Per a valors fixats de k i m, l'equació (33) es pot resoldre en general de diverses maneres diferents. En el que segueix denotarem per $r_k(m)$ el nombre d'aquestes maneres, és a dir, el nombre de sistemes d'enters no negatius $x_1, x_2, \ldots, x_k$ que satisfan l'equació (33). És clar que el nombre m és de A_n^k si i només si $r_k(m) > 0$. En el que segueix, suposarem que el nombre n ve donat i és fix, i per tant direm als nombres que només depenen de n, constants. Aquestes constants es denotaran per la lletra c o $c(n)$, on aquesta constant c pot tenir diferents valors en diferents parts de la nostra discussió, tenint només en compte que aquests valors són constants. Potser no estàs acostumat a aquest tipus de llibertat notacional, pero ràpidament et resultarà familiar. Ha demostrat ser molt convenient, i apareix més i més freqüentment en la investigació moderna.

Lema Fonamental. *Existeix un nombre natural $k = k(n)$, que depèn només de n, i una constant c, tal que, per a un nombre natural arbitrari N,*

$$r_k(m) < cN^{(k/n)-1}, \quad (1 \leq m \leq N). \tag{34}$$

Un cop més, com en el capítol precedent, estem encarats amb dos problemes: primer, provar el lema fonamental, i segon, obtenir a partir d'aquest lema la conclusió que necessitem, és a dir, que la seqüència

$A_n^{(k)}$ té densitat positiva. Novament el segon problema és considerablement més fàcil que el primer, i per tant hem de començar amb el segon problema.

De la definició del nombre $r_k(m)$, immediatament es dedueix que la suma

$$r_k(0) + r_k(1) + \ldots + r_k(N) = R_k(N)$$

representa el nombre de sistemes $(x_1, x_2, \ldots, x_k)$ de k enters no negatius per als quals

$$x_1^n + x_2^n + \ldots + x_k^n \leq N. \tag{35}$$

Cada grup de nombres per als quals

$$0 \leq x_i \leq (N/k)^{1/n} \quad (1 \leq i \leq k)$$

òbviament satisfà aquesta condició. Per satisfer aquestes desigualtats, evidentment cada x_i pot ser triat en més de $(N/k)^{1/n}$ maneres ($x_i = 0, 1, \ldots, \lfloor (N/k)^{1/n} \rfloor$).[1] Després d'una d'aquestes tries arbitràries, els nombres $x_1, x_2, \cdots, x_k$ es poden combinar, i d'aquesta manera tenim més de $(N/k)^{1/n}$ possibilitats diferents per triar el sistema complet d'enters x_i $(1 \leq i \leq k)$, de manera que se satisfà la condició (35). Això mostra que

$$R_k(N) \geq (N/k)^{1/n}. \tag{36}$$

Suposem que el lema fonamental ha estat provat, i que la desigualtat (34) se satisfà per a un N qualsevol. Ara hem de verificar que la desigualtat (34) és consistent amb la desigualtat (36) que hem demostrat, només si la seqüència $A_n^{(k)}$ té una densitat positiva. La idea que hi ha darrere de la deducció següent és molt simple: en la suma $R_k(N)$, els sumands $r_k(m)$ només són diferents de zero si m apareix a $A_n^{(k)}$. Si $A_n^{(k)}$ té densitat zero, aleshores per a valors de N grans el nombre d'aquests sumands hauria de ser relativament petit; gràcies a (34), de tota manera, cada sumand no pot ser gaire gran. Per tant la seva suma $R_k(N)$ serà relativament petita, mentre que d'acord amb (36) ha de ser més aviat gran.

Falta fer els càlculs. Suposem que $d(A_n^{(k)}) = 0$. Aleshores, per a un $\epsilon > 0$ arbitràriament petit i un N triat adequadament,

$$A_n^{(k)}(N) < \epsilon N.$$

1 Aquí $\lfloor a \rfloor$ denota l'enter més gran menor que a.

Aquí podem suposar que el nombre N és arbitràriament gran, ja que $A_n^{(k)}$ (per a una k arbitrària) conté l'enter 1 (recorda el problema 6 del capítol 2, que vares resoldre). Aplicant l'estimació (34) obtenim

$$\begin{aligned} R_k(N) &= \sum_{m=0}^{N} r_k(m) = r_k(0) + \sum_{m=1}^{N} r_k(m) \\ &< 1 + cN^{(k/n)-1} A_n^{(k)}(N) < 1 + c\epsilon N^{(k/n)}, \end{aligned}$$

i així, per a N suficientment gran,

$$R_k(N) < 2c\epsilon N^{(k/n)}.$$

Per a ϵ prou petit,

$$2c\epsilon < (1/k)^{k/n},$$

de manera que

$$R_k(N) < (N/k)^k/n,$$

que contradiu (36). Així tenim

$$d(A_n^{(k)}) > 0.$$

I, com ja sabem, això prova el teorema de Hilbert.

Veus de quina manera més simple ha sortit. Encara hem de provar, però, el lema fonamental, i per fer això hem de viatjar per una carretera llarga i difícil, com en el capítol precedent.

§ 3

LEMES SOBRE EQUACIONS LINEALS

Ara hem de tornar ben enrere. Per tant estarà bé que de moment oblidis completament el problema que tenim plantejat. Et tornaré a cridar l'atenció sobre aquest problema quan hi tornem més tard.

Ara hem de trobar algunes estimacions per al nombre de solucions d'un sistema lineal d'equacions. A més, els lemes d'aquest paràgraf tenen un interès intrínsec, independentment de la solució del problema per al qual es necessitaran.

LEMA 6 *En l'equació*

$$a_1 z_1 + a_2 z_2 = m, \tag{37}$$

siguin a_1, a_2, m enters amb $|a_2| \leq |a_1| \leq A$, i siguin a_1 i a_2 relativament primers. Aleshores el nombre de solucions de l'equació (37) que satisfan les desigualtats $|z_1| \leq A$, $|z_2| \leq A$ no és més gran que $3A/|a_1|$.

DEMOSTRACIÓ . Podem suposar que $a_1 > 0$, ja que altrament només hem de substituir z_1 per $-z_1$ a cada solució.

Siguin $\{z_1, z_2\}$ i $\{z_1', z_2'\}$ dues solucions diferents de l'equació (37). Aleshores restant les igualtats següents

$$a_1 z_1 + a_2 z_2 = m,$$

$$a_1 z_1' + a_2 z_2' = m,$$

obtenim

$$a_2(z_2' - z_2) = a_1(z_1 - z_1').$$

De manera que la part esquerra d'aquesta equació ha de ser divisible per a_1. Però[2] $(a_1, a_2) = 1$, i en conseqüència $z_2' - z_2$ ha de ser divisible per a_1. Ara bé $z_2' \neq z_2$, i per tant $|z_2' - z_2|$, és múltiple d'a_1, no és més petit que a_1. Així, per a dues solucions diferents de l'equació (37), $\{z_1, z_2\}$ i $\{z_1', z_2'\}$, hem de tenir $|z_2' - z_2| \geq a_1$.

A cada solució $\{z_1, z_2\}$ de l'equació (37), acordem que z_1 és el primer membre i z_2 el segon. És obvi que el nombre de solucions de l'equació (37) que satisfan les condicions $|z_1| \leq A$, $|z_2| \leq A$ no és més gran que el nombre t de segons membres que s'on a l'interval $\langle -A, A\rangle$. Com que hem provat que dos d'aquests segons membres estan separats almenys per una distància a_1, la diferència entre el segon membre més gran i el més petit dins de l'interval $\langle -A, A\rangle$ és com a mínim $a_1(t-1)$. D'altra banda, aquesta diferència no és més gran que $2A$, per tant

$$a_1(t-1) \leq 2A,$$

$$(t-1) \leq 2A/a_1,$$

$$t \leq (2A/a_1) + 1 \leq 3A/a_1$$

(ja que que suposem que $a_1 \leq A$ i per tant $1 \leq A/a_1$). Això prova el lema 6. □

2 (a_1, a_2) denota el màxim comú divisor entre els enters a_1, a_2.

LEMA 7 *En l'equació*

$$a_1z_1 + a_2z_2 + \ldots + a_lz_l = m, \tag{38}$$

siguin els a_i *i* m *enters que satisfan les condicions*[3]

$$|a_i| \leq A \quad (1 \leq i \leq l), \qquad (a_1, a_2, \ldots, a_l) = 1.$$

Aleshores el nombre de solucions de l'equació (38) que satisfan les desigualtats $|z_i| \leq A \quad (1 \leq i \leq l)$ *no supera*

$$c(l)A^{l-1}/H,$$

on H *és el nombre més gran entre* $|a_1|, |a_2|, \ldots, |a_l|$, *i* $c(l)$ *és una constant que depèn només de* l.

DEMOSTRACIÓ . Si $l = 2$, aleshores el lema 7 esdevé el lema 6 (amb $c(2) = 3$).

Així el lema 7 està provat per a $l = 2$. Per tant suposem que $l \geq 3$ i que la veracitat del lema 7 ja ha quedat establerta per al cas de $l - 1$ variables. Com que la numeració no és important, podem suposar que $|a_l|$ és el més gran dels nombres $|a_1|, |a_2|, \ldots, |a_l|$, és a dir, $H = |a_l|$.

Hi ha dos casos per considerar.

1. $a_1 = a_2 = \ldots = a_{l-1} = 0$.
   Com que $(a_1, a_2, \ldots, a_l) = 1$, tenim $|a_l| = 1$, per tant l'equació donada és de la forma $\pm z_l = m$. En aquesta equació cadascun dels $z_1, z_2, \ldots, z_{l-1}$ clarament pot assumir qualsevol valor enter arbitrari en l'interval $\langle -A, A\rangle$, i així com a molt $2A + 1 \leq 3A$ valors. Pel que fa a z_l, però, només pot prendre com a molt un valor. Conseqüentment el nombre de solucions de l'equació donada que satisfan les desigualtats $|z_i| \leq A$ $(1 \leq i \leq l)$ no excedeix
   $$(3A)^{l-1} = c(l)A^{l-1} = c(l)A^{l-1}/H,$$
   cosa que prova el lema 7 en aquest cas.
2. Si almenys un dels nombres $a_1, a_2, \ldots, a_{l-1}$ és diferent de zero, aleshores
   $$(a_1, a_2, \ldots, a_{l-1}) = \delta$$

3 $(a_1, a_2, \ldots, a_l)$ denota el màxim comú divisor entre els enters que estan entre parèntesis.

existeix. Denotem per H' el més gran d'entre els nombres

$$|a_i|/\delta \quad (1 \leq i \leq l-1).$$

Suposem ara que els nombres $z_1, z_2, \ldots, z_l$ satisfan l'equació donada (38) i les desigualtats $|z_i| \leq A$ $(1 \leq i \leq l)$. Diem

$$(a_1/\delta)z_1 + (a_2/\delta)z_2 + \ldots, (a_{l-1}/\delta)z_{l-1} = m', \tag{39}$$

i així

$$a_1z_1 + a_2z_2 + \ldots + a_{l-1}z_{l-1} = \delta m'.$$

Aleshores evidentment

$$\delta m' + a_l z_l = m \tag{40}$$

i

$$|\delta m'| \leq \sum_{i=1}^{l-1} |a_i||z_i| \leq l\delta H'A,$$

que implica que

$$|m'| \leq lH'A.$$

Així, si els nombres $z_1, z_2, \ldots, z_l$ satisfan l'equació (38) i les desigualtats $|z_i| \leq A$ $(1 \leq i \leq l)$, aleshores existeix l'enter m' que, amb aquests nombres, satisfà les equacions (39) i (40), on $|m'| \leq lH'A$. En l'equació (40), però, tenim clarament que $\delta \leq |a_l|$ i $(\delta, a_l) = 1$ (altrament tindríem $(a_1, \ldots, a_l) > 1$). Per tant, pel lema 6, el nombre de solucions de l'equació (40) (en les variables m', z_l) que satisfan $|m'| \leq lH'A, |z_l| \leq A \leq lH'A$ no és més gran que $3lH'A/|a_l|$. Per al mateix m', l'equació (39), d'acord amb el lema 7 per a equacions amb $l-1$ variables, té com a molt $c(l)A^{l-2}/H'$ solucions en enters z_i amb $|z_i| \leq A$.

És evident, del que hem dit fins aquí, que el nombre de solucions $\{z_1, \ldots, z_l\}$ de l'equació (38) que satisfan les desigualtats $|z_i| \leq A$ $(1 \leq i \leq l)$ no és més gran que

$$(3lH'A/|a_l|)c(l)A^{l-2}/H' = c(l)A^{l-1}/|a_l| = c(l)A^{l-1}/H,$$

i queda completada la demostració del lema 7.[4] □

4 Deus haver notat que en l'última cadena d'equacions el símbol $c(l)$ apareix en diferents llocs amb significats diferents. Ja t'he preparat abans per a aquest ús del símbol.

Ara ens dedicarem a investigar la totalitat de les equacions de la forma

$$a_1z_1 + a_2z_2 + \ldots, a_lz_l = 0, \tag{41}$$

on $|a_i| \leq A$ $(1 \leq i \leq l)$ i, com sempre, tots els a_i són enters. Sigui B un nombre positiu la relació del qual amb A queda descrita per les desigualtats $1 \leq A \leq B \leq c(l)A^{l-1}$, i sigui $l > 2$. Ara volem estimar la suma dels nombres de solucions z_i, $|z_i| \leq B$ $(1 \leq i \leq l)$, de totes les equacions (41) d'aquesta família.

1. Primer fem un examen per separat de l'equació (41) per al cas que $a_1 = a_2 = \ldots = a_l = 0$ (és un membre de la nostra família) i estimarem el nombre de solucions que satisfan les desigualtats $|z_i| \leq B$ $(1 \leq i \leq l)$. Òbviament la nostra equació se satisfà per un sistema arbitrari de nombres $z_1, z_2, \ldots, z_l$, i només hem de calcular quants d'aquests sistemes existeixen de manera que es compleixin les desigualtats $|z_1| \leq B, |z_2| \leq B, \ldots, |z_l| \leq B$. Com que l'interval $\langle -B, B\rangle$ conté com a molt $2B+1$ enters, cada z_i pot prendre com a molt $2B + 1$ valors diferents. Per tant, el nombre de sistemes $\{z_1, z_2, \cdots, z_l\}$ del tipus en què estem interessats no supera $(2B + 1)^l \leq (3B)^l = c(l)B^l$. De tota manera, segons la nostra hipòtesi, $B \leq c(l)A^{l-1}$ i, per tant, $c(l)B^l = c(l)B^{l-1}B \leq c(l)(AB)^{l-1}$. Així, per al cas en què $a_1 = a_2 = \ldots = a_l = 0$, l'equació (41) té com a molt $c(l)(AB)^{l-1}$ solucions del tipus en què estem interessats.
2. Si almenys un dels coeficients a_i és diferent de zero, el màxim comú divisor d'aquests coeficients, $(a_1, a_2, \ldots, a_l) = \delta$, existeix. Suposem primer que $\delta = 1$, i sigui H el més gran dels nombres $|a_i|$ $(i = 1, 2, \ldots, l)$. Clarament H és un nombre de l'interval $\langle 1, A\rangle$. Per tant, H es troba o bé entre A i $A/2$, o bé entre $A/2$ i $A/4$, o bé entre $A/4$ i $A/8$, etc. Per tant podem trobar un enter $m \geq 0$ tal que

   $$A/2^{m+1} < H \leq A/2^m. \tag{42}$$

   D'acord amb el lema 7, per a una equació del tipus (41) amb $\delta = 1$ i tal que H satisfà les desigualtats (42), el nombre de solucions z_i, $|z_i| \leq B$, no és més gran que

   $$c(l)B^{l-1}/H \leq c(l)B^{l-1}/(A/2^{m+1}) = c(l)B^{l-1}2^m/A.$$

   D'altra banda, a partir de (42) tenim que

   $$|a_i| \leq A/2^m (1 \leq i \leq l). \tag{43}$$

Per tant el nombre d'equacions del tipus (41) per a les quals les desigualtats (42) es compleixen és com a molt igual al nombre d'equacions del mateix tipus que satisfan les condicions (43), és a dir, com a molt

$$(2(a/2^m)+1)^l \leq (3A/2^m)^l = c(l)A^l 2^{-ml}.$$

Així, la suma del nombre de solucions $|z_i| \leq B$ de totes les equacions del tipus (41) per a les quals $\delta = 1$ i $A2^{-m+1} < H \leq A2^{-m}$ no supera

$$(c(l)B^{l-1}2^m/A) \cdot c(l)A^l 2^{-ml} = c(l)(AB)^{l-1}2^{-m(l-1)}.$$

Sumant aquesta estimació per tot $m \geq 0$, obtenim la conclusió següent: La suma dels nombres de solucions $|z_i| \leq B$ de totes les equacions (41) per a les quals $|a_i| \leq A$ $(1 \leq i \leq l)$ i $\delta = 1$ és com a molt

$$c(l)(AB)^{l-1}.$$

3. Ens falta trobar el nombre de solucions del tipus requerit per a les equacions amb $\delta > 1$. En aquest cas l'equació (41) és evidentment sinònima de l'equació

$$(a_1/\delta)z_1 + (a_2/\delta)z_2 + \ldots + (a_l/\delta)z_l = 0,$$

on

$$(a_1/\delta, a_2/\delta, \ldots, a_l/\delta) = 1,$$

i el nombre A s'ha de reemplaçar pel nombre A/δ. Tal com hem vist en l'apartat anterior, la suma del nombre de solucions $|z_i| \leq B$ de totes aquestes equacions, per a un δ donat i fix, no supera[5]

$$c(l)(AB\delta^{-1})^{l-1} = c(l)(AB)^{l-1}\delta^{-(l-1)}.$$

Ara, clarament només hem de sumar aquesta expressió per tots els valors possibles de δ $(1 \leq \delta \leq A)$.

Així, hem trobat que la suma dels nombres de les solucions buscades de totes les equacions de la forma (41), on $|a_i| \leq A$ $(1 \leq i \leq l)$ i no tots els a_i són zero, no supera el valor de

$$c(l)(AB)^{l-1}\sum_{\delta=1}^{A}\delta^{-(l-1)} < c(l)(AB)^{l-1}\frac{l-1}{l-2} = c(l)(AB)^{l-1}.$$

5 Com que ara en comptes de considerar A hem de triar el nombre més petit A/δ, és concebible que la condició $B \leq c(l)A^{l-1}$ sigui violada. De tota manera, pots verificar sense cap dificultat que en el cas anterior no hem fet servir aquesta condició en cap moment, i que el resultat del segon cas no en depèn.

[Per obtenir la primera relació fem servir la desigualtat

$$\sum_{n=1}^{A}(1/n^{q+1}) < (q+1)/q,$$

la qual és vàlida per a un nombre natural arbitrari q i per a un $A \geq 1$ arbitrari (denotem per q el nombre $l-2$, que és positiu ja que hem suposat que $l > 2$). Aquí n'hi ha una demostració simple: per a $n \geq 1$ tenim

$$\begin{aligned} n^{-q} - (n+1)^{-q} &= ((n+1)^q - n^q)/n^q(n+1)^q \\ &= (n^q + qn^{q-1} + \ldots + 1 - n^q)/n^q(n+1)^q \\ &\geq qn^{q-1}/n^q(n+1)^q > q/(n+1)^{q+1}, \end{aligned}$$

i així

$$(n+1)^{-(q+1)} < q^{-1}(n^{-q} - (n+1)^{-q}).$$

Substituint successivament $n = 1, 2, \ldots, A-1$ en aquesta desigualtat i sumant conjuntament totes les desigualtats resultants trobem que

$$\sum_{n=2}^{A} n^{-(q+1)} < q^{-1}(1 - A^{-q}) < 1/q,$$

la qual cosa implica que

$$\sum_{n=1}^{A} n^{-(q+1)} < 1 + (1/q) = (q+1)/q. \qquad \text{Q. E. D.}$$

Comparant això amb el resultat en l'anterior primer apartat, on hem obtingut una estimació per al cas $a_1 = a_2 = \ldots = a_l = 0$, arribem a la conclusió següent:

LEMA 8 *Sigui $l > 2$ i $1 \leq A \leq B \leq c(l)A^{l-1}$. Aleshores la suma del nombre de solucions $|z_i| \leq B$ $(1 \leq i \leq l)$ de totes les equacions de la forma*

$$a_1 z_1 + a_2 z_2 + \ldots + a_l z_l = 0,$$

on $|a_i| \leq A$ $(1 \leq i \leq l)$ no és més gran que

$$c(l)(AB)^{l-1}.$$

§ 4

DOS LEMES MÉS

Abans de procedir a demostrar el lema fonamental, hem d'obtenir dos lemes més d'un tipus especial. Tots dos són molt simples, tant pel que fa a la idea com a la seva forma, encara que pots tenir alguna dificultat per assimilar-los bé perquè tenen a veure amb l'enumeració de totes les combinacions possibles, la construcció de les quals és més aviat delicada. La dificultat d'aquest problema combinatori abstracte rau en la dificultat d'expressar-lo amb símbols matemàtics: s'ha d'expressar més amb paraules que amb símbols. Aquesta és, per descomptat, una dificultat de presentació, i no del tema en ell mateix, i em prendré la molèstia d'expressar tan concretament com sigui possible totes les qüestions que apareguin, així com la seva solució.

Denotarem per A una col·lecció de nombres, no tots necessàriament diferents. Si el nombre a apareix λ vegades en el conjunt A, direm que la seva multiplicitat és λ. Siguin $a_1, a_2, \ldots, a_r$ els diferents nombres que apareixen a A, i siguin $\lambda_1, \lambda_2, \ldots, \lambda_r$ les seves respectives multiplicitats (ja que A conté en total $\sum_{i=1}^{r} \lambda_i$ nombres). Sigui B una altra col·lecció del mateix tipus, que consisteix en els diferents nombres $b_1, b_2, \ldots, b_s$ amb multiplicitats respectives $\mu_1, \mu_2, \ldots, \mu_s$.

Investiguem l'equació

$$x + y = c, \tag{44}$$

on c és un nombre donat i x i y són desconeguts. Estem interessats en les solucions $\{x, y\}$ d'aquesta equació en la qual x és un dels nombres de la col·lecció A (abreujat $x \in A$) i y és un dels nombres de la col·lecció B ($y \in B$). Si els nombres $x = a_i$ i $y = b_k$ satisfan l'equació (44), això ens porta a $\lambda_i \mu_k$ solucions del nostre tipus, ja que cadascun dels λ_i "espècimens" del nombre a_i que apareixen a la col·lecció A es pot combinar amb un dels μ_k "espècimens" del nombre b_k que apareix a la col·lecció B. Però tenim[6] $\lambda_i \mu_k \leq (\lambda_i^2 + \mu_k^2)/2$. Per tant el nombre

6 "La mitjana geomètrica no és més gran que la mitjana aritmètica". Aquí hi ha la demostració més simple:

$$0 \leq (\lambda_i - \mu_k)^2 = \lambda_i^2 + \mu_k^2 - 2\lambda_i \mu_k, \quad \text{d'on} \quad 2\lambda_i \mu_k \leq \lambda_i^2 + \mu_k^2.$$

d'aquestes solucions de l'equació (44), on $x = a_i$, $y = b_k$, no és més gran que $(\lambda_i^2 + \mu_k^2)/2$. Així el nombre de totes les solucions $x \in A$, $y \in B$ de l'equació (44) no és més gran que $\sum(\lambda_i^2 + \mu_k^2)/2$. Aquí el sumatori és sobre tots els parells de subíndexs $\{i, k\}$ per als quals $a_i + b_k = c$. La nostra suma creix si sumem λ_i^2 sobre tot i i μ_k^2 sobre tot k (ja que cada b_k es pot combinar amb com a molt un a_i.) Per tant, obtenim finalment que el nombre de solucions $x \in A$, $y \in B$ de l'equació (44) no és superior al nombre

$$\frac{1}{2}(\sum_{i=1}^{r} \lambda_i^2 + \sum_{k=1}^{s} \mu_k^2).$$

D'altra banda, considerem l'equació

$$x - y = 0 \tag{45}$$

i calculem el nombre de solucions amb $x \in A$, $y \in A$. Evidentment cadascuna d'aquestes solucions és de la forma $x = y = a_i$ $(1 \le i \le r)$. Per a una i donada obtenim λ_i^2 solucions, ja que els nombres x, y poden coincidir, de manera independent, amb cadascun dels λ_i "espècimen" del nombre a_i que apareixen a A. Així, el nombre total de solucions $x \in A$, $y \in A$ de l'equació (45) és igual a $\sum_{i=1}^{r} \lambda_i^2$. Exactament de la mateixa manera, per descomptat, trobem que el nombre total de solucions $x \in B$, $y \in B$ de la mateixa equació és $\sum_{k=1}^{s} \mu_k^2$. Si comparem aquests resultats amb els que hem trobat abans arribem a la conclusió següent:

Lema 9 *El nombre de solucions de l'equació*

$$x + y = c, \quad x \in A, y \in B$$

no és més gran que la meitat de la suma del nombre de solucions de les equacions

$$x - y = 0, \;\; x, y \in A \quad \text{i} \quad x - y = 0, \;\; x, y \in B.$$

Per al cas especial en què les col·leccions A i B coincideixen obtenim el següent

Corol·lari 10 *El nombre de solucions de l'equació*

$$x + y = c, \quad x, y \in A$$

no és més gran que el nombre de solucions de l'equació

$$x - y = 0, \;\; x, y \in A.$$

Ara siguin k i s dos nombres naturals arbitraris. Posem $k2^s = l$, i investiguem l'equació

$$x_1 + x_2 + \ldots + x_l = c.$$

Siguin $A_1, A_2, \ldots, A_l$ col·leccions de nombres. Suposem que cada col·lecció A_i $(1 \leq i \leq l)$ està formada pels nombres diferents $a_{i1}, a_{i2}, \ldots$ amb multiplicitats respectives $\lambda_{i1}, \lambda_{i2}, \ldots$. Estem interessats en el nombre de solucions de l'equació

$$x_1 + x_2 + \ldots + x_l = c, \quad x_i \in A_i \quad (1 \leq i \leq l). \tag{46}$$

Si considerem

$$x_1 + x_2 + \ldots + x_{l/2} = x, \quad x_{(l/2)+1} + \ldots + x_l = y$$

($l/2$ és per descomptat un enter), aleshores l'equació donada es pot escriure de la forma

$$x + y = c,$$

i el lema 9, que acabem de provar, es pot aplicar aquí. Només hem de trobar a quin conjunt de nombres pertanyen x i y. Com que $x_i \in A_i$ $(1 \leq i \leq l)$, x pot ser un nombre arbitrari de la forma $z_1 + z_2 + \ldots + z_{l/2}$, on $z_i \in A_i$ $(1 \leq i \leq l/2)$. De manera similar y pot ser un nombre arbitrari de la mateixa forma, amb $z_i \in A_{(l/2)+i}$ $(1 \leq i \leq l/2)$.

Així, pel lema 9, el nombre de solucions de l'equació (46) no supera la meitat de la suma del nombre de solucions de l'equació

$$x - y = 0 \tag{47}$$

sota les hipòtesis següents:

1. $x = z_1 + z_2 + \ldots + z_{l/2}, \qquad y = z'_1 + z'_2 + \ldots + z'_{l/2},$

$$z_i, z'_i \in A_i \quad (1 \leq i \leq l/2); \tag{48}$$

2. x i y tenen la mateixa forma, però

$$z_i, z'_i \in A_{(l/2)+i} \quad (1 \leq i \leq l/2). \tag{49}$$

En els dos casos l'equació (47) es pot reescriure de la forma

$$(z_1 - z_1') + (z_2 - z_2') + \ldots + (z_{l/2} - z_{l/2}') = 0. \tag{50}$$

Així concloem que el nombre de solucions de l'equació (46) no supera la meitat de la suma del nombre de solucions de l'equació (50) sota les hipòtesis (48) i (49), és a dir, no supera la meitat de la suma del nombre de solucions de les equacions

$$\sum_{i=1}^{l/2}(z_i - z_i') = 0, \quad z_i, z_i' \in A_i \quad (1 \leq i \leq l/2) \tag{51}$$

i

$$\sum_{i=1}^{l/2}(z_i - z_i') = 0, \quad z_i, z_i' \in A_{(l/2)+i} \quad (1 \leq i \leq l/2). \tag{52}$$

L'equació (50) té $l/2$ sumands en el cantó esquerre, és a dir, tants com la meitat de l'equació original (46).

Diem

$$\sum_{i=1}^{l/4}(z_i - z_i') = x, \qquad \sum_{i=(l/4)+1}^{l/2}(z_i - z_i') = y,$$

i per tant portem l'equació (50) a la forma

$$x + y = 0.$$

Així podem aplicar una altra vegada el lema 9. És evident que, de la mateixa manera que hem obtingut l'equació (50) a partir de l'equació (46), ara anirem de l'equació (50) a l'equació

$$\sum_{i=1}^{l/4}(u_i + u_i' - u_i'' - u_i''') = 0, \tag{53}$$

en la qual hem de considerar la suma dels nombres de solucions d'aquesta equació sota les següents (ara quatre) hipòtesis, per a $(1 \leq i \leq l/4)$:

1. $u_i, u_i', u_i'', u_i''' \in A_i$,
2. $u_i, u_i', u_i'', u_i''' \in A_{(l/4)+i}$,
3. $u_i, u_i', u_i'', u_i''' \in A_{(l/2)+i}$,
4. $u_i, u_i', u_i'', u_i''' \in A_{(3l/4)+i}$.

Com que $l = k \cdot 2^s$, podem repetir aquest procés s vegades. Evidentment s'acaba amb l'equació

$$\sum_{i=l}^{k}(y_i^{(1)} + y_i^{(2)} + \ldots + y_i^{(2^{s-1})} - y_i^{(2^{s-1}+1)} \ldots - y_i^{(2^s)}) = 0, \qquad (54)$$

en la qual hem de considerar la suma dels nombres de solucions d'aquesta equació sota 2^s hipòtesis diferents, per a $(1 \leq j \leq 2^s)$:

1. $y_1^{(j)} \in A_1,\ y_2^{(j)} \in A_2, \ldots, y_k^{(j)} \in A_k,$
2. $y_1^{(j)} \in A_{k+1},\ y_2^{(j)} \in A_{k+2}, \ldots, y_k^{(j)} \in A_{2k},$
   .....
2^s. $y_1^{(j)} \in A_{k2^s-k+1}, \ldots, y_k^{(j)} \in A_{k2^s}.$

Si posem

$$y^{(j)} = y_1^{(j)} + y_2^{(j)} + \ldots + y_k^{(j)} \quad (1 \leq j \leq 2^s),$$

aleshores l'equació (54) s'expressa d'aquesta forma simple:

$$y^{(1)} + y^{(2)} + \ldots + y^{(2^{s-1})} - y^{(2^{s-1}+1)} - \ldots - y^{(2^s)} = 0. \qquad (55)$$

Aquí volem tractar de la suma dels nombres de solucions de l'equació (55) sota les següents 2^s hipòtesis, que difereixen l'una de l'altra en el valor del paràmetre ω $(0 \leq \omega \leq 2^s - 1)$:

$$y^{(j)} = y_1^{(j)} + y_2^{(j)} + \ldots + y_k^{(j)},$$

on

$$y_1^{(j)} \in A_{\omega k+1}, \quad y_2^{(j)} \in A_{\omega k+2}, \ldots, y_k^{(j)} \in A_{(\omega+1)k} \quad (1 \leq j \leq 2^s).$$

Així podem expressar el resultat final de la nostra deducció en la forma que dóna la proposició següent:

LEMA 11 *Si $l = k \cdot 2^s$, el nombre de solucions de l'equació* (46),

$$x_1 + x_2 + \ldots + x_l = c, \quad x_i \in A_i \quad (1 \leq i \leq l)$$

no supera la suma dels nombres de solucions de l'equació (55),

$$y^{(1)} + y^{(2)} + \ldots + y^{(2^{s-1})} - y^{(2^{s-1}+1)} - \ldots - y^{(2^s)}) = 0,$$

amb

$$y^{(j)} = y_1^{(j)} + y_2^{(j)} + \ldots + y_k^{(j)},$$

$$y_1^{(j)} \in A_{\omega k+1}, \quad y_2^{(j)} \in A_{\omega k+2}, \ldots, y_k^{(j)} \in A_{(\omega+1)k} \quad (1 \le j \le 2^s),$$

i $\omega = 0, \ldots, 2^s - 1$.

Observa la connexió entre els lemes 9 i 11 per a $k = s = 1$, $l = 2$.

Això elimina els nostres preliminars, i ara estem preparats per començar l'assalt directe al lema fonamental.

§ 5

DEMOSTRACIÓ DEL LEMA FONAMENTAL

Provarem el lema fonamental pel mètode d'inducció sobre n. En les demostracions per inducció passa sovint que la demostració es fa més fàcil si plantegem una proposició més forta que la que volem provar (i de vegades és només així que la demostració es pot arribar a completar per aquest mètode). El motiu és fàcil d'entendre. En les demostracions per inducció, la proposició es considera correcta per al nombre $n-1$, i es demostra per al nombre n. Per tant, com més forta és la proposició, més ens dóna per al cas $n-1$; per descomptat, també hem de provar més per al cas n, però en molts problemes la primera consideració acaba sent més important que la segona.

I així és, de fet, en el nostre cas ara mateix. El nostre interès immediat és el nombre de solucions de l'equació $x_1^n + x_2^n + \ldots + x_k^n = m$ $(1 \le m \le N)$ (on, d'acord amb el significat real del problema, $0 \le x_i \le m^{1/n} \le N^{1/n}$). Però x^n és el cas especial més simple d'un polinomi de grau n

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n,$$

i serà convenient per a nosaltres reemplaçar l'equació donada per una equació molt més general

$$f(x_1) + f(x_2) + \ldots + f(x_k) = m, \tag{56}$$

on les variables estan subjectes a les condicions més febles $|x_i| \le N^{1/n}$ $(1 \le i \le k)$. La demostració de la nostra proposició sobre l'equació (56) ens donarà més del que realment necessitem; però, tal com veuràs,

és precisament aquest reforç de la nostra proposició el que ens obre la possibilitat d'una demostració per inducció. Així doncs, per a $m \leq N$, denotem per $r_k(m)$ el nombre de solucions de l'equació (56) que satisfan les condicions $|x_i| \leq N^{1/n}$ $(1 \leq i \leq k)$. Per descomptat encara som lliures de disposar de manera arbitrària dels coeficients del polinomi $f(x)$ perquè la inducció es pugui dur a terme (tenint només en compte que les condicions imposades es compleixin en el cas $f(x) = x^n$). Ara provarem la proposició següent:

PROPOSICIÓ 12 *Suposem que els coeficients del polinomi $f(x)$ satisfan les desigualtats*

$$|a_i| \leq c(n)N^{i/n} \quad (0 \leq i \leq n). \tag{57}$$

Aleshores, per a un $k = k(N)$ triat de manera adequada,

$$r_k(m) < c(n)N^{(k/n)-1} \quad (1 \leq m \leq N).$$

Com que les desigualtats (57) se satisfan de forma òbvia en el cas $f(x) = x^n$ per a $c(n) = 1$, aquest teorema és realment una versió més forta del nostre lema fonamental.

Considerem primer el cas $n = 1$, $f(x) = a_0x + a_1$. Posem $k(1) = 2$, i per tant l'equació (56) pren la forma

$$a_0(x_1 + x_2) = m - 2a_1.$$

Estem interessats en solucions d'aquesta equació que compleixin les condicions $|x_1| \leq N$, $|x_2| \leq N$. Així, hi ha com a molt $2N + 1 \leq 3N$ valors possibles per a x_1. Però com a molt correspon un x_2 a cada x_1, per tant

$$r_2(m) \leq 3N,$$

la qual cosa completa la demostració de la nostra proposició per a $n = 1$ $(k = 2)$.

Ara sigui $n > 1$, i suposem que la nostra afirmació ja ha estat verificada per l'exponent $n - 1$. Posem $k(n - 1) = k'$ i triem

$$k = k(n) = 2n \cdot 2^{\lfloor 4 \log_2 k' \rfloor},$$

on l'exponent significa el màxim enter que no excedeix $4 \log_2 k'$. En el que segueix, per abreujar, posarem $\lfloor 4 \log_2 k' \rfloor - 1 = s$ i per tant

$$k = 2n \cdot 2^{s+1}. \tag{58}$$

Per estimar el nombre, $r_k(m)$, de solucions de l'equació (56), primer li apliquem el lema 9, posant

$$x = \sum_{i=1}^{k/2} f(x_i), \quad y = \sum_{i=k/2+1}^{k} f(x_i).$$

La col·lecció A (i la col·lecció B, que coincideixen en aquest cas) consisteix en totes les sumes de la forma

$$\sum_{i=1}^{k/2} f(x_i), \quad |x_i| \le N^{1/n} \quad (1 \le i \le k/2).$$

Pel corol·lari del lema 9, $r_k(m)$ no supera el nombre de solucions de l'equació $x - y = 0$, on $x \in A$, $y \in A$, és a dir,

$$x = \sum_{i=1}^{k/2} f(x_i), \quad y = \sum_{i=1}^{k/2} f(y_i),$$

$$|x_i| \le N^{1/n}, \quad |y_i| \le N^{1/n} \quad (1 \le i \le k/2).$$

En altres paraules, $r_k(m)$ no supera el nombre de solucions de l'equació

$$\sum_{i=1}^{k/2} (f(x_i) - f(y_i)) = 0, \tag{59}$$

on $|x_i| \le N^{1/n}$, $|y_i| \le N^{1/n}$ $(1 \le i \le k/2)$. Ara diem $x_i - y_i = h_i$ $(1 \le i \le k/2)$ i reemplacem el sistema de variables $\{x_i, y_i\}$ pel sistema $\{y_i, h_i\}$; ara permetem a y_i i h_i $(1 \le i \le k/2)$ prendre tots els possibles valors enters en l'interval $\langle -2N^{1/n}, 2N^{1/n} \rangle$, la qual cosa només pot incrementar el nombre de solucions de la nostra equació. Això significa que cada sumand $f(x_i) - f(y_i)$ en l'equació (59) està reemplaçat per l'expressió

$$\begin{aligned} f(y_i + h_i) - f(y_i) &= \sum_{v=0}^{n-1} a_v [(y_i + h_i)^{n-v} - y_i^{n-v}] \\ &= \sum_{v=0}^{n-1} a_v \sum_{t=1}^{n-v} \binom{n-v}{t} h_i^t y_i^{n-v-t}. \end{aligned}$$

Si canviem la variable t del sumatori posant

$$v + t = u,$$

de manera que

$$n - v - t = n - u, \qquad t = u - v,$$

obtenim

$$\begin{aligned} f(y_i + h_i) - f(y_i) &= h_i \sum_{v=0}^{n-1} a_v \sum_{u=v+1}^{n} \binom{n-v}{u-v} h_i^{u-v-1} y_i^{n-u} \\ &= h_i \sum_{u=1}^{n} y_i^{n-u} \sum_{v=0}^{u-1} a_v \binom{n-v}{u-v} h_i^{u-v-1} \\ &= h_i \sum_{u=1}^{n} a_{i,u} y_i^{n-u} = h_i \phi_i(y_i), \end{aligned}$$

on

$$\phi_i(y) = \sum_{u=1}^{n} a_{i,u} y_i^{n-u}$$

és un polinomi de grau $n-1$ amb coeficients

$$a_{i,u} = \sum_{v=0}^{u-1} a_v \binom{n-v}{u-v} h_i^{u-v-1} \qquad (1 \le i \le k/2)$$

que depenen dels nombres h_i.

Així, en les noves variables $\{y_i, h_i\}$, l'equació (59) pren la forma

$$h_1\phi_1(y_1) + h_2\phi_2(y_2) + \ldots + h_{k/2}\phi_{k/2}(y_{k/2}) = 0. \tag{60}$$

En aquesta equació els nombres h_i i y_i poden prendre valors enters arbitraris en l'interval $\langle -2N^{1/n}, 2N^{1/n} \rangle$, on hem de tenir present que els coeficients dels polinomis $\phi_i(y)$ (de grau $n-1$) depenen dels nombres h.

Apunta bé que de moment hem demostrat el següent: *El nombre $r_k(m)$ que estem estimant no supera la suma del nombre de solucions enteres y_i, $|y_i| \le 2N^{1/n}$ $(1 \le i \le k/2)$, de totes les equacions (60) que es poden obtenir a partir de tots els possibles valors dels nombres h_i, $|h_i| \le 2N^{1/n}$ $(1 \le i \le k/2)$.*

§ 6

CONTINUACIÓ

Examinem ara una de les equacions (60), és a dir, de moment mirarem els nombres h_i $(1 \leq i \leq k/2)$ com a constants. Apliquem el lema 11 a aquesta equació; els nombres $h_i\phi_i(y_i)$ tenen el paper de les variables x_i, el nombre $k/2 = 2n \cdot 2^s$ té el paper del nombre l, i diem $2n = k_o$ per abreujar. Recorda un cop més que el nombre h_i apareix a l'equació (60) no només de forma explícita sinó també a través dels coeficients dels polinomis $\phi_i(y)$. La col·lecció A_i a la qual els nombres $x_i = h_i\phi_i(y_i)$ pertanyen consisteix, en el cas present, en tots els nombres de la forma $h_i\phi_i(y_i)$, on els nombres h_i tenen valors fixats i els nombres y_i es mouen en l'interval $\langle -2N^{1/n}, 2N^{1/n}\rangle$.

D'acord amb el lema 11, el nombre de solucions de l'equació (60) que satisfan les condicions que acabem de descriure, no supera la suma dels nombres de solucions de l'equació

$$y^{(1)} + y^{(2)} + \ldots + y^{(2^{s-1})} - y^{(2^{s-1}+1)} - \ldots - y^{(2^s)}) = 0 \qquad (61)$$

sota les 2^s hipòtesis següents que corresponen als diferents valors del paràmetre $w = 0, 1, \ldots, 2^s - 1$:

$$\left.\begin{array}{l} y^{(j)} = y_1^{(j)} + y_2^{(j)} + \ldots + y_{k_o}^{(j)} \\ y_i^{(j)} \in A_{wk_o+i} \quad (1 \leq i \leq k_o) \end{array}\right\} (1 \leq j \leq 2^s),$$

on, recorda, A_r $(1 \leq r \leq 2^s)$ és la col·lecció de nombres de la forma $h_r\phi_r(y_r)$ amb h_r fixats i y_r, $|y_r| \leq 2N^{1/n}$, arbitraris.

Per al cas $w = 0$ (que triem només com a exemple), l'equació (61) es veu de forma estesa així:

$$\begin{array}{ll} & [y_1^{(1)} + y_2^{(1)} + \ldots + y_{k_o}^{(1)}] \\ + & [y_1^{(2)} + y_2^{(2)} + \ldots + y_{k_o}^{(2)}] \\ + & \cdots\cdots\cdots \\ + & [y_1^{(2^{s-1})} + y_2^{(2^{s-1})} + \ldots + y_{k_o}^{(2^{s-1})}] \\ - & [y_1^{(2^{s-1}+1)} + y_2^{(2^{s-1}+1)} + \ldots + y_{k_o}^{(2^{s-1}+1)}] \\ - & \cdots\cdots\cdots \\ - & [y_1^{(2^s)} + y_2^{(2^s)} + \ldots + y_{k_o}^{(2^s)}] = 0, \end{array}$$

o bé, reorganitzant els sumands,

$$\begin{aligned} & [y_1^{(1)} + y_1^{(2)} + \ldots + y_1^{(2^{s-1})} - y_1^{(2^{s-1}+1)} - \ldots - y_1^{(2^s)}] \\ + \quad & [y_2^{(1)} + y_2^{(2)} + \ldots + y_2^{(2^{s-1})} - y_2^{(2^{s-1}+1)} - \ldots - y_2^{(2^s)}] \\ + \quad & \cdots\cdots\cdots \\ + \quad & [y_{k_o}^{(1)} + y_{k_o}^{(2)} + \ldots + y_{k_o}^{(2^{s-1})} - y_{k_o}^{(2^{s-1}+1)} - \ldots - y_{k_o}^{(2^s)}] = 0; \end{aligned}$$

cadascun dels nombres $y_i^{(j)}$ és un nombre de la forma $h_i\phi_i(v_i^{(j)})$, on $|v_i^{(j)}| \leq 2N^{1/n}$. Per tant l'última equació es pot reescriure de la forma

$$\begin{aligned} & h_1[\phi_1(v_1^{(1)}) + \phi_1(v_1^{(2)}) + \ldots + \phi_1(v_1^{(2^{s-1})}) - \phi_1(v_1^{(2^{s-1}+1)} - \ldots - \phi_1(v_1^{(2^s)}] \\ + \quad & h_2[\phi_2(v_2^{(1)}) + \ldots - \phi_2(v_2^{(2^s)})] \\ + \quad & \cdots\cdots\cdots \\ + \quad & h_{k_o}[\phi_{k_o}(v_{k_o}^{(1)}) + \ldots - \phi_{k_o}(v_{k_o}^{(2^s)})] = 0. \end{aligned}$$

Escrivint, per simplificar,

$$\phi_1(v_1^{(1)}) + \phi_1(v_1^{(2)}) + \ldots + \phi_1(v_1^{(2^{s-1})}) - \phi_1(v_1^{(2^{s-1}+1)} - \ldots - \phi_1(v_1^{(2^s)}) = z_i$$

$$(i \leq i \leq k_o)$$

aquesta equació es pot escriure de forma bastant més curta de la manera següent:

$$h_1 z_1 + h_2 z_2 + \ldots + h_{k_o} z_{k_o} = 0. \tag{62}$$

En total tenim 2^s equacions d'aquesta classe, i la seva totalitat es pot escriure de forma compacta

$$\sum_{i=1}^{k_o} h_{wk_o+i} z_{wk_o+i} = 0 \quad (0 \leq w \leq 2^s - 1).$$

De tota manera, de moment centrarem la nostra investigació en l'equació (62), la qual es pot veure com a típica. Per estimar el nombre de solucions d'aquesta equació en la qual estem interessats, primer hem de mirar entre quins límits pot variar la quantitat $\phi_i(v_i^{(j)})$. Per això, recordem que

$$\phi_i(y) = \sum_{u=1}^{n} a_{i,u} y^{n-u},$$

on

$$a_{i,u} = \sum_{v=0}^{u-1} a_v \binom{n-v}{u-v} h_i^{u-v-1} \qquad (1 \le i \le k/2).$$

Per tant, a partir de la nostra hipòtesi $|a_v| < c(n)N^{v/n}$ i $|h_i| \le 2N^{1/n}$, es dedueix que

$$|a_{i,u}| < \sum_{v=0}^{u-1} c(n)N^{v/n}\binom{n-v}{u-v}c(n)N^{(u-v-1)/n} = c(n)N^{(u-1)/n}\sum_{v=0}^{u-1}\binom{n-v}{u-v};$$

és a dir, tenint en compte que $u \le n$,

$$|a_{i,u}| < c(n)N^{(u-1)/n}. \tag{63}$$

D'altra banda, com que $|v_i^{(j)}| \le 2N^{1/n}$, tenim $|v_i^{(j)}|^{n-u} \le c(n)\cdot N^{(n-u)/n}$ i en conseqüència

$$|a_{i,u}| \cdot |v_i^{(j)}|^{n-u} \le c(n)N^{(u-1)/n}N^{(n-u)/n} = c(n)N^{(u-1)/n}.$$

La mateixa estimació (amb un altre $c(n)$) es compleix per a tot $\phi_i(v_i^{(j)})$, ja que el nombre de termes del polinomi és igual a n. Així,

$$|\phi_i(v_i^{(j)}| < c(n)N^{(n-1)/n} \qquad (1 \le i \le k_o,\ \ 1 \le j \le 2^n).$$

Però cada z_i és la suma de $2^s = c(n)$ sumands de la forma $\pm\phi_i(v_i^{(j)})$, i per tant

$$|z_i| < c(n)N^{(n-1)/n} \qquad (1 \le i \le k_o)$$

(amb un altre $c(n)$, naturalment). Això significa que, en l'equació (62), cada z_i només pot prendre els valors que són a l'interval

$$\langle -c(n)N^{(n-1)/n}, c(n)N^{(n-1)/n}\rangle.$$

Sigui $\bar{m}$ un d'aquests nombres. L'equació $z_i = \bar{m}$ no només se satisfà d'una sola manera sinó, en general, de diverses, ja que la definició del nombre z_i és tal que un mateix valor de z_i pot ben bé resultar d'eleccions diferents dels nombres $v_i^{(j)}$ $(1 \le j \le 2^s)$. Ara hem d'estimar el nombre de solucions de la relació $z_i = \bar{m}$, és a dir, de l'equació

$$\phi_i(v_i^{(1)}) + \ldots + \phi_i(v_i^{(2^{s-1})}) - \phi_i(v_i^{(2^{s-1+1})}) - \ldots - \phi_i(v_i^{(2^s)}) = \bar{m}. \tag{64}$$

Amb aquest propòsit finalment haurem d'aplicar la llargament promesa inducció. Procedim com segueix.

Primer reescrivim l'equació (64) en la forma

$$\begin{aligned} & \phi_i(v_i^{(1)}) + \phi_i(v_i^{(2)}) + \ldots + \phi_i(v_i^{(k')}) \\ = \; & \bar{m} - \phi_i(v_i^{(k'+1)} - \ldots - \phi_i(v_i^{(2^{s-1}+1)}) + \ldots + \phi_i(v_i^{(2^s)}). \end{aligned}$$

Això és possible ja que per a $k' = k(n-1) > 1$ (i ja hem vist que $k(1) = 2$) tenim

$$2^{s-1} = 2^{\lfloor 4 \log_2 k' \rfloor - 2} > k'.$$

(Amb detall: $k' \geq 2$, $\log_2 k' \geq 1$, $3 \log_2 k' \geq 3$, $\lfloor 4 \log_2 k' \rfloor - 2 > 4 \log_2 k' - 3 \geq \log_2 k'$, $2^{s-1} = 2^{\lfloor 4 \log_2 k' \rfloor - 2} \geq k'$.)

Si denotem la part dreta de l'última equació per m', obtenim

$$\phi_i(v_i^{(1)}) + \ldots + \phi_i(v_i^{(k')}) = m'. \tag{65}$$

Triem alguns valors particulars per als nombres

$$v_i^{(j)} \qquad (k'+1 \leq j \leq 2^s)$$

(naturalment en l'interval $\langle -2N^{1/n},\ 2N^{1/n} \rangle$); aleshores m' també adquireix un valor definit. A l'equació (65), com que $\phi_i(y)$ és un polinomi de grau $n-1$, ara li apliquem el teorema que hem de provar. Hem de verificar que totes les hipòtesis necessàries es compleixen. Tenim

$$\phi_i(y) = \sum_{u=1}^{n} a_{i,u} y^{n-u},$$

on, d'acord amb (63),

$$|a_{i,u}| < c(n) N^{(u-1)/n} = c(n) (N^{(n-1)/n})^{\frac{u-1}{n-1}}, \tag{66}$$

i, com és fàcil de veure,

$$|m'| < c(n) N^{(n-1)/n}$$

(ja que $\bar{m}$ i tots els $\phi_i(y_i^{(j)})$ satisfan la desigualtat).

En virtut de la darrera desigualtat, el paper de N pot ser assumit pel nombre $c(n)N^{(n-1)/n}$; aleshores les condicions (66), que els coeficients del polinomi $\phi_i(y)$ satisfan, són precisament les condicions (57) substituint n per $n-1$. Així totes les hipòtesis efectivament es compleixen, i podem

assegurar que el nombre de solucions de l'equació (65), per a les quals $|v_i^{(j)}| \leq 2N^{1/n} = 2(N^{(n-1)/n})^{1/(n-1)}$, no supera el nombre

$$c(n)(N^{(n-1)/n})^{\frac{k'}{n-1}-1} = c(n)N^{\frac{k'-n+1}{n}}. \tag{67}$$

Aquesta estimació s'ha obtingut per a valors fixats $v_i^{(k'+1)}, \ldots, v_i^{(2^s)}$. Clarament, com a molt tenim

$$(4N^{1/n}+1)^{2^s-k'} < c(n)N^{\frac{2^s-k'}{n}} \tag{68}$$

valors d'aquests. El nombre total de solucions del nostre tipus, de l'equació (64), per tant, no excedeix el producte dels cantons drets de (67) i (68), és a dir, és com a molt

$$c(n)N^{\frac{2^s-n+1}{n}}. \tag{69}$$

Tornem ara a l'equació (62). Hem vist que cada z_i pot assumir només valors que són a l'interval $\langle -c(n)N^{\frac{n-1}{n}},\ c(n)N^{\frac{n-1}{n}}\rangle$. Ara veiem que la "multiplicitat" de cadascun d'aquests valors (és a dir, el nombre de maneres de triar $y_i^{(j)}$ de forma que l'equació sigui satisfeta) no supera el nombre (69).

Aquest resultat fa possible reduir el problema global a una estimació dels nombres de solucions d'equacions lineals. Això és perquè al final de § 5 vàrem reduir l'estimació de $r_k(m)$ a l'estimació del nombre de solucions de les equacions de la forma (60). Però tal com vàrem provar mitjançant una aplicació del lema 11, el nombre de solucions de l'equació (60), que satisfan $|y_i| \leq 2N^{1/n}$, és com a molt igual a la suma dels nombres de solucions de 2^s equacions del tipus (62), que ja són equacions lineals. En connexió amb això, hem obtingut els intervals en els quals les variables z_i poden prendre valors. Una dificultat certament nova (el preu que hem hagut de pagar per la transició a equacions lineals) és que les noves variables z_i han de ser considerades amb certes multiplicitats (per a les quals també hem determinat límits de variació).

Finalment no hem d'oblidar que tots aquests càlculs s'han fet sota la hipòtesis que els nombres h_i estan triats i són fixats. Per tant encara hem de multiplicar el resultat obtingut pel nombre de totes aquestes possibles eleccions.

El resultat final d'aquesta secció, que hem de recordar, diu: *El nostre nombre estimat $r_k(m)$ no supera la suma dels nombres de solucions en enters z_i, $|z_i| \leq c(n)N^{(n-1)/n}$, amb multiplicitats $\lambda_i \leq c(n)N^{(2^s-n+1)/n}$, d'equacions de la forma*

$$\sum_{i=1}^{k_o} h_{wk_o+i} z_{wk_o+i} = 0, \tag{70}$$

on ω recorre els valors $0, 1, \ldots, 2^s - 1$, i els nombres h_r $(1 \leq r \leq 2^s k_o)$ prenen, independentment l'un de l'altre, tots els enters de l'interval $\langle -2N^{1/n},\ 2N^{1/n} \rangle$.

I per tant veiem que ara hem obtingut una estimació per a $r_k(m)$ en la formulació de la qual el polinomi donat $f(x)$ no apareix, la qual cosa dóna a aquesta estimació un caràcter molt general.

§ 7

CONCLUSIÓ

Ara que hem reduït el problema a una estimació del nombre de solucions d'equacions lineals que són independents de la forma especial del polinomi $f(x)$, ràpidament aconseguim el nostre objectiu amb l'ajuda del lema 8.

Denotem per K qualsevol combinació particular dels nombres h_i, $|h_i| \leq 2N^{1/n}$ $(1 \leq i \leq k/2)$, i per $U_w(K)$ el nombre de solucions de l'equació (70) per a aquesta combinació fixa K i per a una w prescrita, on ens preocuparem de les solucions z_i que satisfan les desigualtats $|z_i| \leq c(n)N^{(n-1)/n}$, amb multiplicitats $\lambda_i \leq c(n)N^{(2^s-n+1)/n}$. Aleshores, d'acord amb el resultat final de la secció precedent,

$$r_k(m) \leq \sum_K [\sum_{w=0}^{2^s-1} U_w(K)],$$

on el sumatori sobre K s'estén sobre totes les combinacions K admissibles dels nombres h_i. Això es pot escriure com

$$r_k(m) \leq \sum_{\omega=0}^{2^s-1} [\sum_K U_\omega(K)].$$

De tota manera, és evident de manera immediata que, per a un w diferent les sumes $\sum_K U_w(K)$ no difereixen en absolut l'una de l'altra (ja que per un w diferent les equacions (70) no difereixen l'una de l'altra en cap sentit). Per tant podem escriure

$$r_k(m) \leq 2^s \sum_K U_o(K) = c(n) \sum_K U_o(K).$$

Aquí $U_o(K)$ és el nombre de solucions de l'equació

$$h_1 z_1 + h_2 z_2 + \ldots + h_{k_o} z_{k_o} = 0, \tag{71}$$

per a una combinació donada K dels nombres h_i, $|h_i| \leq 2N^{1/n}$ $(1 \leq i \leq k/2)$, on $|z_i| \leq c(n)N^{(n-1)/n}$ i els z_i tenen multiplicitats $\lambda_i \leq c(n) \cdot N^{(2^s-n+1)/n}$. Denotem per $U_o^*(K)$ el nombre de solucions de la mateixa equació suposant que totes les z_i són simples. Aleshores clarament

$$U_o(K) \leq [c(n)N^{(2^s-n+1)/n}]^{k_o} U_o^*(K),$$

o bé, recordant que $k_o = 2n$,

$$U_o(K) \leq c(n)N^{2(2^s-n+1)} U_o^*(K),$$

i per tant

$$r_k(m) \leq c(n)N^{2(2^s-n+1)} \sum_K U_o^*(K). \tag{72}$$

Ara observem el següent. Cada K representa una certa combinació admissible dels valors de totes les h_i $(1 \leq i \leq k/2)$; el nombre $U_o^*(K)$, en canvi, queda completament determinat pels valors del primer $k_o = 2n$ d'aquests valors $(1 \leq i \leq 2n)$, perquè només ells apareixen a l'equació (71). Per descomptat, quan triem una certa combinació fixada K, al mateix temps també definim de forma única una certa combinació K' dels valors $h_1, h_2, \ldots, h_{2n}$. Però si, al contrari, se selecciona una certa combinació K' dels nombres $h_1, h_2, \ldots, h_{2n}$, a ella li correspon no només la simple combinació K, sinó més aviat tantes maneres com existeixen de triar la resta de "suplements" h_i $(2n < i \leq k/2)$. Com que cada h_i ha de ser de l'interval $\langle -2N^{1/n},\ 2N^{1/n} \rangle$, és evident que a una combinació K' li corresponen com a molt

$$c(n)(N^{1/n})^{(k/2)-2n} = c(n)N^{(k/2n)-2}$$

combinacions K. Així

$$\sum_K U_o^*(K) \leq c(n)N^{(k/2n)-2} \sum_{K'} U_o^*(K'),$$

on $U_o^*(K')$ és el nombre de solucions enteres z_i, $|z_i| \leq c(n) \cdot N^{(n-1)/n}$ $(1 \leq i \leq 2n)$ de l'equació (71) per a la combinació donada K' dels nombres h_i, $|h_i| \leq 2N^{1/n}$ $(1 \leq i \leq 2n)$, i el sumatori s'ha d'estendre a totes aquestes combinacions. Així a partir de (72) obtenim[7]

$$\begin{aligned} r_k(m) &\leq c(n)N^{2(2^s-n+1)}N^{(k/2n)-2}\sum_{K'} U_o^*(K') \\ &= c(n)N^{2(2^{s+1}-n)}\sum_{K'} U_o^*(K'). \end{aligned} \tag{73}$$

Finalment, $\sum_{K'} U_o*(K')$ es pot estimar immediatament amb l'ajuda del lema 8, on hem de posar $l = 2n$, $A = 2N^{1/n}$, $B = c(n)N^{(n-1)/n}$; pots verificar fàcilment que totes les hipòtesis del lema 8 se satisfan. Aplicant aquest lema trobem que

$$\sum_{K'} U_o^*(K') \leq c(n)(AB)^{2n-1} = c(n)N^{2n-1}.$$

Per acabar, la desigualtat (73) ens porta a

$$r_k(m) \leq c(n)N^{2(2^{s+1}-n)}N^{2n-1} = c(n)N^{22^{s+1}-1} = c(n)N^{\frac{k}{n}-1},$$

que completa la demostració del lema fonamental i de passada el teorema de Hilbert.

Aquesta demostració, tan exquisidament elemental, indubtablement et semblarà complicada, a tu. Però només necessitaràs de dues a tres setmanes de feina amb llapis i paper per entendre-la i digerir-la completament. És conquerint dificultats d'aquesta classe que el matemàtic creix i es desenvolupa.

* * *

7 Recorda que $k = 2n \cdot 2^{s+1}$.