1 Introducció

Els nombres naturals sorgeixen de la necessitat de l'home de comptar. S'anomenen així perquè van ser els primers que emprà l'ésser humà per comptar objectes. El conjunt dels nombres naturals es simbolitza amb la lletra $\mathbb{N}$ i és $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$.

Usem els nombres naturals per posicionar elements dintre d'una successió ordenada (gràcies a la relació d'ordre que hi podem definir) i per mesurar la grandària dels conjunts finits, això és, comptar els objectes dels conjunts finits (cardinalitat).

Hi ha matemàtics, sobretot els de Teoria de Nombres, que prefereixen no incloure el zero (0) en la definició de nombre natural. Altres, més propers a la Lògica i a la Teoria de Conjunts, sí ho fan. En aquesta exposició considerarem que $0 \in \mathbb{N}$.

Encara que el concepte intuïtiu de nombres naturals és immediat i gairebé innat, la seva definició no és senzilla. El concepte de nombre natural està relacionat amb els agregats d'objectes. Es pot dir que dos conjunts tenen el mateix nombre d'objectes si es pot establir una correspondència un a un entre els elements d'un conjunt i els de l'altre. El concepte de nombre natural correspon a la abstracció d'allò que tenen en comú tots els conjunts amb el mateix nombre d'objectes; no és ni els objectes en sí, ni el conjunt, ni les xifres que es fan servir per representar tots els conjunts amb el mateix nombre d'objectes, sinó el concepte abstracte que hi ha al darrere d'aquesta idea.

Des del punt de vista matemàtic, la definició abstracta de nombre natural passa per un enfocament axiomàtic mitjançant els *postulats de Peano* o un enfocament constructivista de Zermelo a partir de la teoria de conjunts.

2 Construcció de $\mathbb{N}$

2.1 Definició axiomàtica

Fou Dedekind al s.XIX el primer qui va assentar les bases per a una definició rigorosa dels nombres naturals, fent servir uns postulats que més tard Peano precisaria dins d'una lògica de segon ordre.

Construïm $\mathbb{N}$ com un conjunt infinit d'elements, tots ells diferents, anomenats *nombres naturals*: $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$, que verifiquen els següents axiomes (postulats de Peano):

- **Axioma 1.** $0 \in \mathbb{N}$
- **Axioma 2.** Existeix una funció $s(n)$ que assigna a cada $n \in \mathbb{N}$ el seu *següent*, que també notarem com $s(n) = n^*$, i que verifica $a = b \Rightarrow s(a) = s(b)$.
- **Axioma 3.** El 0 no és següent de cap nombre natural: $\forall n \in \mathbb{N}\ s(n) \neq 0$.
- **Axioma 4 (injectivitat de s).** Si $s(a) = s(b)$ llavors $a = b$.
- **Axioma 5 (principi d'inducció completa).** Si $K \subset \mathbb{N}$ és tal que $0 \in K$ i $\forall n \in K\ s(n) \in K$ llavors $K = \mathbb{N}$.

D'aquests postulats se'n desprenen dues propietats elementals:

Proposició. *Tot natural és diferent del seu següent:* $n \neq n^*\ \forall n \in \mathbb{N}$.

Demostració: Apliquem el 5è axioma: sigui $K = \{n \in \mathbb{N} \mid n \neq n^*\}$ i volem veure que $K = \mathbb{N}$. Pel 3r axioma deduïm que $0 \neq 0^*$, per tant $0 \in K$. Ara sigui $n \in K$ i volem veure que $n^* \in K$. En efecte, $n \in K \Rightarrow n \neq n^*$, i pel 4t axioma deduïm que $n^* \neq (n^*)^*$, això és, $n^* \in K$. Per tant, $K = \mathbb{N}$. $\square$

Proposició. *Tot natural, excepte el* 0*, té un "anterior", això és,* $\forall n \in \mathbb{N},\ n \neq 0 \Rightarrow \exists m \in \mathbb{N}$ *tal que* $m^* = n$.

Demostració: De nou per inducció: $K = \{0\} \cup \{n \in \mathbb{N} \mid \exists m \in \mathbb{N} \text{ t.q. } m^* = n\}$. Trivialment $0 \in K$, i si $n \in K$ és evident que també $n^* \in K$, doncs l'anterior de n^* és el propi n. Per tant, $K = \mathbb{N}$. $\square$

2.2 Definició constructiva

A principis del s.XX Zermelo va demostrar l'existència dels naturals dintre de la seva teoria de conjunts fent ús de l'axioma d'infinitud, que, amb una modificació d'aquest feta per Fraenkel, permet construir el conjunt dels naturals com ordinals.

Definició. Si K és un conjunt, definim el *següent* de K com $K^* = K \cup \{K\}$.

Amb això definim els símbols $0, 1, 2, 3, \ldots$ de la següent manera:

$0 := \emptyset \quad , \quad 1 := 0^* = 0 \cup \{0\} = \{0\} = \{\emptyset\} \quad , \quad 2 := 1^* = 1 \cup \{1\} = \{0, 1\} = \{\emptyset, \{\emptyset\}\} \quad ,$
$3 := 2^* = 2 \cup \{2\} = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \quad , \quad \ldots$

Per assegurar-nos que podem continuar amb aquest procés de forma indefinida necessitem l'Axioma de l'infinit:

Axioma de l'infinit. Existeix almenys un conjunt K que verifica $0 \in K$ i $a \in K \Rightarrow a^* \in K$. A un K d'aquestes característiques l'anomenem *conjunt recurrent*, i anomenem $\mathcal{K}$ la família de tots els conjunts recurrents.

Definició. Amb les notacions anteriors definim $\mathbb{N} = \bigcap\limits_{K \in \mathcal{K}} K$.

És immediat comprovar que $\mathbb{N} \neq \emptyset$, doncs $0 \in \mathbb{N}$ en pertànyer a tots els conjunts recurrents, i que $\mathbb{N}$ és recurrent, i a més a més, és el més petit dels conjunts recurrents. No es difícil demostrar que aquesta definició de $\mathbb{N}$ és equivalent a la construcció axiomàtica amb els postulats de Peano.

3 Suma i producte de naturals

Proposició. *Existeix una única aplicació $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, que anomenarem* suma*, que verifica les següents propietats: $\forall x, y \in \mathbb{N}$ $f(x, 0) = x$ i $f(x, y^*) = f(x, y)^*$. Notem el natural $f(x, y)$ com $x + y$.*

DEMOSTRACIÓ: Per veure'n l'existència posem $K = \{x \in \mathbb{N} \mid \exists f_x : \{x\} \times \mathbb{N} \longrightarrow \mathbb{N}\}$ on les f_x verifiquen les dues condicions de l'enunciat, i apliquem inducció completa: $0 \in K$, perquè podem definir $f_0 : \{0\} \times \mathbb{N} \longrightarrow \mathbb{N}$ com $f_0(0, y) = y$, que verifica les dues condicions inicials. A més, $x \in K \Rightarrow x^* \in K$, perquè podem definir $f_{x^*}(x^*, y) = f_x(x, y)^*$, que també verifica les dues propietats. Per tant, $K = \mathbb{N}$ i hem provat l'existència de f.

Per comprovar la unicitat suposem que existeixen dues aplicacions f, g que verifiquen les condicions de l'enunciat. Fixem $x \in \mathbb{N}$ i apliquem inducció sobre $K_x = \{y \in \mathbb{N} \mid f(x, y) = g(x, y)\}$: $0 \in K_x$ perquè $f(x, 0) = x = g(x, 0)$. A més, $y \in K_x \Rightarrow f(x, y) = g(x, y) \Rightarrow f(x, y)^* = g(x, y)^* \Rightarrow f(x, y^*) = g(x, y^*) \Rightarrow y^* \in K_x$, de manera que $K_x = \mathbb{N}$, i com això succeeix $\forall x \in \mathbb{N}$ deduïm que $f = g$. $\square$

De la definició de l'aplicació suma n'obtenim dues propietats immediates:

Proposició. *(a) $x + 1 = x^*$, (b) $x + y = 0 \Rightarrow x = 0$ i $y = 0$.*

DEMOSTRACIÓ: (a) $x + 1 = x + 0^* = (x + 0)^* = x^*$, i per veure (b) suposem que $y \neq 0$; llavors existeix a tal que $a^* = y$, i aleshores $0 = x + y = x + a^* = (x + a)^*$, impossible perquè 0 no té anterior. Per tant $y = 0$ i $0 = x + y = x + 0 = x$. $\square$

La suma verifica cinc propietats fonamentals que es demostren fàcilment per inducció: per a qualssevol $a, b, c \in \mathbb{N}$ es compleixen les propietats

- *Commutativa:* $a + b = b + a$
- *Associativa:* $(a + b) + c = a + (b + c)$
- *Existència d'element neutre:* $a + 0 = 0 + a = a$
- *Llei de simplificació:* $a + c = b + c \ \Rightarrow\ a = b$
- *Llei de monotonia:* $a = b \ \Rightarrow\ a + c = b + c$

Proposició. *Existeix una única aplicació* $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, *que anomenarem* producte, *que verifica les següents propietats:* $\forall x, y \in \mathbb{N}\ f(x, 0) = 0$ *i* $f(x, y^*) = f(x, y) + x$. *Notem el natural* $f(x, y)$ *com* $x \cdot y$.

DEMOSTRACIÓ: Per veure'n l'existència posem $K = \{x \in \mathbb{N} \mid \exists f_x : \{x\} \times \mathbb{N} \longrightarrow \mathbb{N}\}$ on les f_x verifiquen les dues condicions de l'enunciat, i apliquem inducció completa: $0 \in K$, perquè podem definir $f_0 : \{0\} \times \mathbb{N} \longrightarrow \mathbb{N}$ com $f_0(0, y) = 0$, que verifica les dues condicions inicials. A més, $x \in K \ \Rightarrow\ x^* \in K$, perquè podem definir $f_{x^*}(x^*, y) = f_x(x, y) + y$, que també verifica les dues propietats. Per tant, $K = \mathbb{N}$ i hem provat l'existència de f.

Per comprovar la unicitat suposem que existeixen dues aplicacions f, g que verifiquen les condicions de l'enunciat. Fixem $x \in \mathbb{N}$ i apliquem inducció sobre $K_x = \{y \in \mathbb{N} \mid f(x, y) = g(x, y)\}$: $0 \in K_x$ perquè $f(x, 0) = 0 = g(x, 0)$. A més, $y \in K_x \ \Rightarrow\ f(x, y) = g(x, y) \ \Rightarrow\ f(x, y) + x = g(x, y) + x \ \Rightarrow\ f(x, y^*) = g(x, y^*) \ \Rightarrow\ y^* \in K_x$, de manera que $K_x = \mathbb{N}$, i com això succeeix $\forall x \in \mathbb{N}$ deduïm que $f = g$. □

Igual que en el cas de la suma, podem deduir dues propietats immediates del producte:

Proposició. *(a)* $x \cdot 1 = x$, *(b)* $x \cdot y = 0 \ \Rightarrow\ x = 0$ *ó* $y = 0$.

DEMOSTRACIÓ: (a) $x \cdot 1 = x \cdot 0^* = x \cdot 0 + x = 0 + x = x$, i per veure (b) suposem que $x \neq 0$ i $y \neq 0$; llavors existeixen a, b tals que $a^* = x$, $b^* = y$, i aleshores $0 = x \cdot y = x \cdot b^* = x \cdot b + x = x \cdot b + a^* = (x \cdot b + a)^*$, impossible perquè 0 no té anterior. La contradicció ens diu, per tant, que $x = 0$ o bé $y = 0$. □

Les propietats fonamentals del producte, totes elles demostrables per inducció, són les següents ($a, b, c \in \mathbb{N}$):

- *Commutativa:* $a \cdot b = b \cdot a$
- *Associativa:* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- *Distributiva respecte de la suma:* per la dreta, $(a + b) \cdot c = a \cdot c + b \cdot c$, i per l'esquerra, $c \cdot (a + b) = c \cdot a + c \cdot b$

- *Existència d'element neutre:* $a \cdot 1 = 1 \cdot a = a$
- *Existència d'element absorbent:* $a \cdot 0 = 0 \cdot a = 0$
- *Llei de simplificació:* $a \cdot c = b \cdot c$ i $c \neq 0 \;\Rightarrow\; a = b$
- *Llei de monotonia:* $a = b \;\Rightarrow\; a \cdot c = b \cdot c$

4 Ordre a $\mathbb{N}$

Definició. Diem que una relació binària $\mathcal{R}$ és un *ordre estricte* si verifica les propietats *antireflexiva* ($a \not\mathcal{R} a$), *antisimètrica* ($a\mathcal{R}b,\ b\mathcal{R}a \Rightarrow a = b$) i *transitiva* ($a\mathcal{R}b,\ b\mathcal{R}c \Rightarrow a\mathcal{R}c$). Diem que $\mathcal{R}$ és un *ordre total* si verifica les propietats *reflexiva* ($a\mathcal{R}a$), *antisimètrica* i *transitiva*.

Definició. Donats $a, b \in \mathbb{N}$ diem que *a és menor que b*, i ho escrivim $a < b$, si existeix $c \in \mathbb{N}$, $c \neq 0$, tal que $a + c = b$. La definició de *a menor o igual que b* ($a \leq b$) és la mateixa però permetent que $c = 0$.

Proposició. *La relació* $<$ *és un ordre estricte a* $\mathbb{N}$*, i* $\leq$ *és un ordre total a* $\mathbb{N}$.

Demostració: La relació $<$ és antireflexiva perquè si fos $a < a$ es tindria que $a+c = a$ per a algun $c \neq 0$, però per la llei de simplificació de la suma, $a+c = a \Rightarrow c = 0$, contradicció. És antisimètrica perquè mai no es verifica l'antecedent de la definició d'antisimetria. En efecte, si fos $a < b$ i $b < a$ alhora, existirien $c, d \in \mathbb{N}$ no nuls tals que $a + c = b$, $b + d = a$, i usant les lleis de monotonia i simplificació tindríem $a+b+c+d = a+b \Rightarrow c+d = 0 \Rightarrow c = d = 0$, contradicció. Finalment, és transitiva perquè $a < b,\ b < c \Rightarrow a + x = b,\ b + y = c$ amb $x, y \neq 0 \Rightarrow a + x + y = b + y = c$ amb $x + y \neq 0 \Rightarrow a < c$.

D'altra banda, $\leq$ és reflexiva perquè $a + 0 = a \Rightarrow a \leq a$, és antisimètrica perquè $a \leq b$, $b \leq a \Rightarrow a + c = b,\ b + d = a \Rightarrow a + b + c + d = a + b \Rightarrow c + d = 0 \Rightarrow c = d = 0 \Rightarrow a = b$, i la transitivitat es demostra igual que per a $<$. $\square$

Proposició (principi del bon ordre). *El conjunt* $(\mathbb{N}, \leq)$ *és ben ordenat, això és, tot subconjunt* $C \subset \mathbb{N}$*,* $C \neq \emptyset$*, té un mínim.*

Demostració: Sigui $C \subset \mathbb{N}$ amb $C \neq \emptyset$. Si $0 \in C$ llavors 0 és mínim perquè $0 \leq c\ \forall c \in C$. Suposem doncs que $0 \notin C$. Considerem $A = \{x \in \mathbb{N} \mid x < c\ \forall c \in C\}$. És evident que $0 \in A$ perquè $0 \notin C$, i que A no pot ser un conjunt recurrent, perquè si ho fos tindríem $A = \mathbb{N} \Rightarrow C = \emptyset$ (en efecte, $c \in C \subset \mathbb{N} = A \Rightarrow c \in A \Rightarrow c < c$, absurd), i per tant existeix

$x \in A$ tal que $x^* \notin A$. Però $x \in A \Rightarrow x < c \; \forall c \in C \Rightarrow x^* \leq c \; \forall c \in C$, i no pot ser $x^* < c \; \forall c \in C$ perquè $x^* \notin A$, per tant existeix $m \in C$ tal que $m = x^* \Rightarrow m = \min(C)$. $\square$

Teorema de l'extrem. *Tot subconjunt $A \subset \mathbb{N}$, $A \neq \emptyset$ i fitat superiorment, té un màxim.*

DEMOSTRACIÓ: Sigui $S = \{x \in \mathbb{N} \mid a \leq x \; \forall a \in A\} \neq \emptyset$ el conjunt de les fites superiors d'A. Pel principi del bon ordre, existeix $m = \min(S)$ i anem a comprovar que també $m = \max(A)$. Si $m = 0$ significa que $A = \{0\}$ i $\max(A) = 0$. Si $m \neq 0$ existeix n tal que $n^* = m$ i $n \notin S \Rightarrow$ existeix un $a \in A$ tal que $n < a \Rightarrow m = n^* \leq a$. Com també tenim $a \leq m$ deduïm que $m = a$, per tant $m \in A$ i $m = \max(A)$. $\square$

5 Sistemes de numeració

Definició. Un *sistema de numeració* és un conjunt finit de símbols anomenats *dígits* o *xifres* del sistema, i un conjunt de *regles de generació* que ens permeten representar qualsevol nombre natural. El cardinal del conjunt de dígits s'anomena *base* del sistema.

Abans d'enunciar i provar el teorema fonamental de la numeració, que és la base dels sistemes de numeració posicionals, ens cal provar el teorema de la divisió euclidiana a $\mathbb{N}$ com a lema previ:

Teorema de la divisió euclidiana. *Donats $D, d \in \mathbb{N}$ amb $d \neq 0$, existeixen uns únics $c, r \in \mathbb{N}$, anomenats respectivament* quocient *i* residu *de la divisió entera de D per d, tals que $D = d \cdot c + r$, amb $r < d$.*

DEMOSTRACIÓ: Si $D = 0$ la demostració és evident: $c = r = 0$. Suposem $D \neq 0$ i per provar l'existència considerem el conjunt $A = \{x \in \mathbb{N} \mid d \cdot x \leq D\}$, que és no buit ($0 \in A$) i fitat superiorment ($D$ n'és una fita), per tant existeix $c = \max(A)$ que verifica $d \cdot c \leq D < d \cdot (c+1) = d \cdot c + d \Rightarrow D = d \cdot c + r$ amb $r < d$. Per veure'n la unicitat suposem que $D = d \cdot c + r = d \cdot c' + r'$ amb $r \leq r'$ i $r, r' < d$. Però $r \leq r' \Rightarrow r + h = r'$ per algun $h \in \mathbb{N} \Rightarrow d \cdot c + r = d \cdot c' + r + h \Rightarrow d \cdot c = d \cdot c' + h \Rightarrow d \cdot c' \leq d \cdot c \Rightarrow c' \leq c \Rightarrow c' + m = c$ per algun $m \in \mathbb{N} \Rightarrow d \cdot c' + d \cdot m = d \cdot c = d \cdot c' + h \Rightarrow d \cdot m = h \Rightarrow r' = r + d \cdot m$, de manera que si fos $m \neq 0$ tindríem $r' \geq d$, en contradicció amb la hipòtesi, per tant ha de ser $m = 0 \Rightarrow h = 0$ i $r = r'$, $c = c'$. $\square$

Teorema fonamental de la numeració. *Sigui $b \in \mathbb{N}$, $b > 1$. Llavors tot $n \in \mathbb{N}$, $n \neq 0$, es pot escriure de forma única com $n = n_0 + n_1 b + n_2 b^2 + \cdots + n_p b^p$ amb $n_p \neq 0$, $n_i < b$.*

DEMOSTRACIÓ: Fem la divisió euclidiana de n per b, i obtenim $n = b \cdot c_1 + n_0$ amb $n_0 < b$. Si $c_1 < b$ posem $c_1 = n_1$ i ja hem acabat. Del contrari, dividim c_1 per b i obtenim

$c_1 = b \cdot c_2 + n_1$ amb $n_1 < b$. Substituint c_1 en l'expressió anterior tenim $n = b^2 c_2 + b n_1 + n_0$. Si $c_2 < b$ hem acabat, i si no repetim el procés. Com la successió de quocients és decreixent, $c_1 > c_2 > c_3 > \cdots$ el procés acabarà i obtindrem l'expressió cercada. Per provar la unicitat de l'expressió suposem que $n = n_0 + n_1 b + \cdots + n_p b^p = n'_0 + n'_1 b + \cdots + n'_r b^r$, que podem escriure com $n = n_0 + b(n_1 + \cdots + n_{p-1} b^{p-1}) = n'_0 + b(n'_1 + \cdots + n'_{r-1} b^{r-1})$, que representen dues expressions de la divisió euclidiana de n per b. Per unicitat d'aquesta expressió deduïm que $n_0 = n'_0$ i $n_1 + n_2 b + \cdots + n_{p-1} b^{p-1} = n'_1 + n'_2 b + \cdots + n'_{r-1} b^{r-1}$, i repetim el procés amb aquesta última. Iterant-lo acabem obtenint que $n_i = n'_i$ i $p = r$. □

5.1 Breu història dels sistemes de numeració

Abans que sorgissin els nombres per a representar quantitats, l'ésser humà emprà altres mètodes per comptar, fent servir objectes com ara pedres, palets de fusta, nusos en una corda o simplement els dits. Més endavant sorgiren el símbols gràfics com senyals per comptar, com les marques en una vara o traços a la sorra. Tots aquests són exemples de sistemes de numeració no posicionals.

Cap a l'any 3.000 a.C. a Mesopotàmia apareixen els primers vestigis de nombres, com a símbols en forma de cunya gravats sobre taulells de fang mitjançat un palet esmolat (sistema de numeració babilònic, escriptura cuneïforme). Més tard, l'imperi Grec i l'imperi Romà també adoptarien sistemes de numeració d'aquest tipus però amb gràfics diferents: lletres de l'alfabet i algun altre símbol (sistemes semiposicionals).

Amb aquests sistemes de numeració no posicionals o semiposicionals és molt complicat dissenyar algorismes de càlcul. Per exemple, les operacions mercantils es feien molt farragoses. És per això que s'establiren de forma general els sistemes posicionals.

El sistema de numeració que emprem actualment a Europa i que és el més estès prové de l'indoaràbic. Fou un sistema posicional de base 10 i comprenia el concepte de zero. La seva aparició constituí un dels grans avenços de la matemàtica. Va tenir el seu origen a l'Índia entre els segles V i VIII (tot i que s'especula que pogués tenir els seus orígens a la Xina), s'expandí pel món islàmic i d'aquí, a través d'al-Andalus, a la resta d'Europa.

Altres sistemes de numeració que hi ha hagut al llarg de la història, cronològicament:

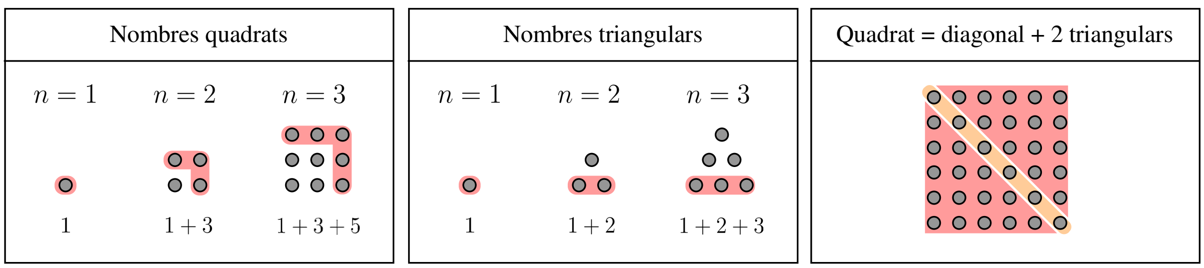
- 3.000 a.C - **Egipci** - Additiu, no posicional, amb símbols per a les potències de 10.
- 2.500 a.C - **Babilònic** - Semiposicional, de base 10, additiu fins al 60 i posicional per a nombres superiors.

- 1.500 a.C - **Xinès** - Híbrid additiu/multiplicatiu, no posicional. Símbols de l'1 al 10 i potències de 10.
- 1.000 a.C - **Maia** - Posicional de base 20 amb 5 com base auxiliar.
- 600 a.C - **Grec** - Additiu, no posicional. Símbols 1,2,3,...,10,20,30,...,100,200,300,...

En l'actualitat, els sistemes binari, octal i hexadecimal (bases 2, 8 i 16 respectivament) són de gran importància en l'àmbit de la informàtica.

5.2 Els nombres figurats com a recurs didàctic

Un *nombre figurat* és un nombre natural representat gràficament mitjançant un patró geomètric discret (punts). El gràfic en mostra uns exemples:



Aquestes disposicions geomètriques sovint ens permeten trobar fórmules interessants. Per exemple, amb els nombres quadrats es veu clarament que la suma dels n primers nombres senars és n^2:

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

També, veiem que un nombre triangular d'ordre n és $1+2+\cdots+n$, i si ens adonem que un nombre quadrat d'ordre n està format per la seva diagonal i dos triangulars d'ordre $n - 1$ (els que queden a banda i banda de la diagonal), obtenim la fórmula de la suma dels $n - 1$ primers nombres naturals:

$$n^2 = n + 2(1 + 2 + \cdots + n - 1) \;\Rightarrow\; 1 + 2 + \cdots + n - 1 = \frac{n^2 - n}{2}.$$