

El triangle de Pascal-Tartaglia i les seves importants derivacions

J. M. Matabosch i Castell

1 Per què triangle de Pascal-Tartaglia?

TARTAGLIA (1500(?)-1557) va escriure el “Tractat general sobre el nombre i la mesura” que es publicà en part després de la seva mort (entre 1556 i 1560). En aquesta obra del matemàtic italià, apareixia una “taula” que, com veurem després, és l’antecedent immediat del “Triangle de Pascal” que es donà a conèixer cent anys després (1665). Comprovarem que PASCAL (1623-1662) es limità a disposar els nombres que Tartaglia presentava en la seva taula rectangular, en forma triangular.

Per moltes altres raons que no esmentarem aquí, és més just que del “Triangle Aritmètic” com el batejà Pascal, se’n digui “Triangle de Pascal-Tartaglia” resumit: T.P-T.

2 Els xinesos i l’escaquer

Avui sabem que els matemàtics xinesos dels primers 500 anys d. C., havien fet grans avanços (havien calculat π amb 6 decimals exactes i coneixien el Teorema de Pitàgores).

TXU-XIII-KEI va donar a conèixer els coeficients de les successives potències del binomi $(a + b)^n$ segons la figura següent.

$$\begin{array}{rcccccc} (a + b)^0 & = & & & & & 1 \\ (a + b)^1 & = & & & 1 & & 1 \\ (a + b)^2 & = & & & 1 & 2 & 1 \\ (a + b)^3 & = & & & 1 & 3 & 3 & 1 \\ (a + b)^4 & = & & & 1 & 4 & 6 & 4 & 1 \\ (a + b)^5 & = & 1 & 5 & 10 & 10 & 5 & 1 \end{array}$$

Fig. 2.1

La Fig. 2.1 disposada en un escaquer (amb els quadrats tots “blancs”) dóna la Fig. 2.2.

la mateixa obra hi ha un problema de parelles de conills que partint d'una primera parella i segons una "regla" de desenvolupament biològic de la "conillada", proporciona una taula com la de la Fig. 3.4:

	Parelles de conills que hi hauran
Comença	1
Fi 1er mes	2
Fi 2on mes	3
Fi 3er mes	5
Fi 4rt mes	8
Fi 5è mes	13
Fi 6è mes	21

Fig. 3.4

A Ramon Llull se'l considera un dels primers tractadistes coneguts del que actualment se'n diu algorísmica o "computabilitat". La importància de Llull, la posà en evidència LEIBNIZ (1646-1716), també filòsof i matemàtic, indicant la gran aportació de l'obra lul·liana "Ars Magna".

Els "Nombres de Fibonacci" o "Sucessió de Fibonacci" com és coneguda la taula de Fig. 3.4, és una successió recurrent i com a tal calculable mitjançant un algorisme. La "regla" aritmètica és: "El primer nombre, F_1 , de Fibonacci és donat: és 1. Els altres són la suma dels dos anteriors". Per tant: el segon, F_2 , serà: $0+1=1$. El tercer, F_3 , serà: $1+1=2$. El quart $F_4 = 1+2=3$; etc. Veure Fig. 9.1.

4 Tartaglia

Abans hem dit que Tartaglia, nascut 400 anys després de fer-se el "Liber Abaci" va presentar una "taula": Veure la Fig. 4.1.

	(a)	(b)	(c)	(d)	(e)
1	1	1	1	1	1
1	2	3	4	5	
1	3	6	10	15	
1	4	10	20	35	
1	5	15	35	70	
1	6	21	56	126	
1	7	28	84	210	

Fig. 4.1

La “regla” de formació d’aquesta taula és:
 “El primer element de la 1^a columna (a) és donat: és 1. Els altres elements són la suma de dos elements: l’element del costat esquerra més l’element superior”.

5 Triangle de Pascal-Tartaglia (T. P-T)

L’any 1665, es publicà el llibre “Tractat sobre el Triangle Aritmètic” de Pascal, mort tres anys abans. El “Triangle Aritmètic” es veu en la Fig. 5.1.

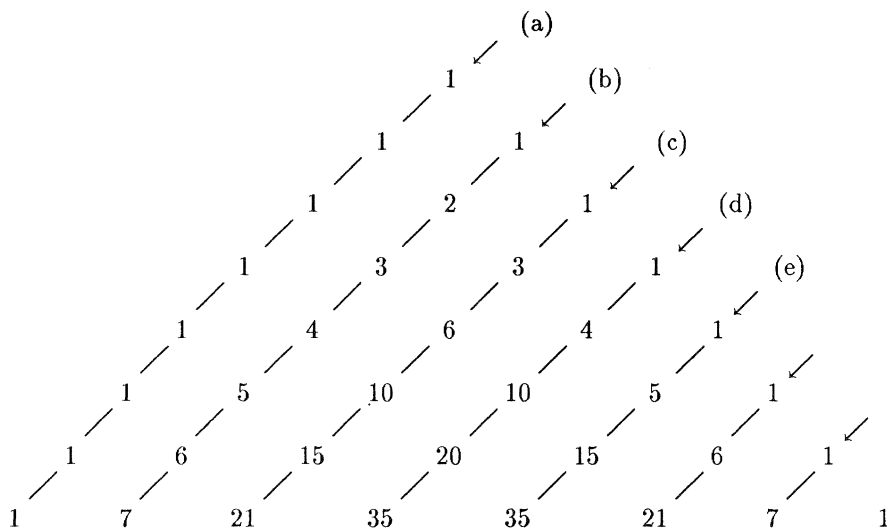


Fig. 5.1

Es pot observar que les columnes (a), (b), (c), (d) i (e) de la Fig. 5.1, són les mateixes columnes inclinades 45° de la Fig. 4.1. De fet el “Triangle Aritmètic” és la “Taula de Tartaglia” inclinada 45° .

La regla d’obtenció dels diferents elements del triangle de la Fig. 5.1, s’anomenen “lleis de Pascal”. Veure Fig. 5.2.

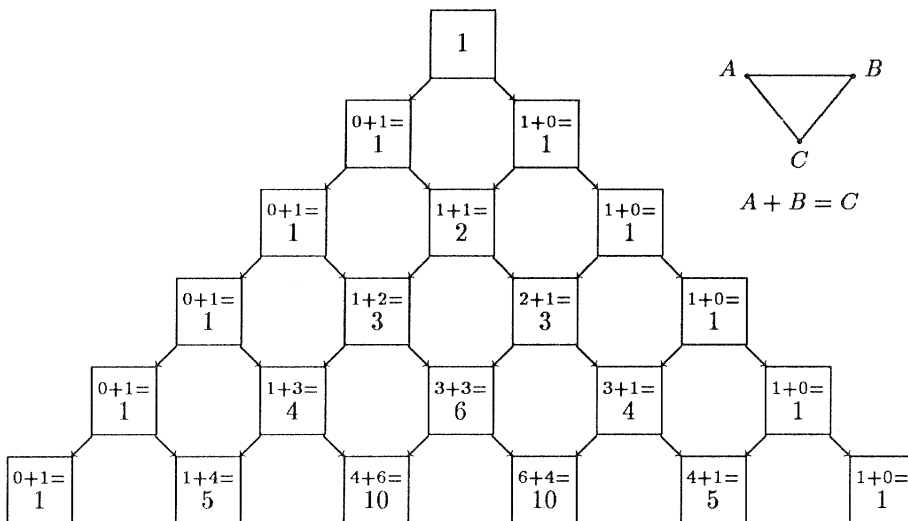


Fig. 5.2

Per millor emprar aquest Triangle, es desplacen cap a l'esquerra totes les files horitzontals fins a deixar els primers elements (els "uns") encolumnats: veure la Fig. 5.3.

1					
0+1= 1	1+0= 1				
0+1= 1	1+1= 2	1+0= 1			
0+1= 1	1+2= 3	2+1= 3	1+0= 1		
0+1= 1	1+3= 4	3+3= 6	3+1= 4	1+0= 1	
0+1= 1	1+4= 5	4+6= 10	6+4= 10	4+1= 5	1+0= 1

Fig. 5.3

Observem que la Fig. 5.3, és la "taula de Tartaglia", amb les columnes (a), (b), (c), (d), (e), ... començant un espai per sota de l'inici de la columna del costat esquerra. (Veure la Fig. 4.1).

6 Notació moderna $\binom{n}{v}$, deguda a Euler (1707-1783)

En aquesta notació n , és la "ene" de nombre i v és la "ve" de vegada. Aquestes són les lletres que farem servir a partir d'ara.

Disposarem els elements del T. P-T en uns eixos cartesianes (com es fan servir per senyalar les posicions de les peces en els taulers d'escacs): n , ordenades i v abscises (n i v positius sempre). Per exemple $\binom{4}{3}$ vol dir: l'element del T. P-T que es troba en la fila 4 i en la columna 3: és el 4. Veure la Fig. 6.1.

Noti's que per definició tenim:

$$\binom{n}{1} = n; \quad \binom{n}{0} = 1; \quad \binom{n}{v} = \binom{n}{n-v}.$$

Segons la notació d'Euler, com hem dit en la Fig. 5.3, la "lleï de Pascal" serà:

$$\binom{n}{v} + \binom{n}{v+1} = \binom{n+1}{v+1}.$$

$n \setminus v$	0	1	2	3	4	5	6	7	8	9	10	11	12	2^n	=
0	1													2^0	1
1	1	1												2^1	2
2	1	2	1											2^2	4
3	1	3	3	1										2^3	8
4	1	4	6	4	1									2^4	16
5	1	5	10	10	5	1								2^5	32
6	1	6	15	20	15	6	1							2^6	64
7	1	7	21	35	35	21	7	1						2^7	128
8	1	8	28	56	70	56	28	8	1					2^8	256
9	1	9	36	84	126	126	84	36	9	1				2^9	512
10	1	10	45	120	210	252	210	120	45	10	1			2^{10}	1024
11	1	11	55	165	330	462	462	330	165	55	11	1		2^{11}	2048
12	1	12	66	220	495	792	924	792	495	220	66	12	1	2^{12}	4096

Fig. 6.1

Si volem donar significat a $\binom{n}{v}$ per a $v > n$ la lleï de Pascal ens obliga a que valgui 0. Així ho suposarem d'ara en avant.

Observant la Fig. 6.2, veiem que emprant la notació d'Euler es complex, per exemple:

$$\binom{2}{1} = \binom{1}{0} \frac{2}{1}, \quad \binom{3}{2} = \binom{2}{1} \frac{3}{2}, \quad \binom{4}{2} = \binom{3}{2} \frac{4}{3}.$$

	0	1	2	3	4	5	6
0	1						
1	1	$1 \times \frac{1}{1} = 1$					
2	1	$1 \times \frac{2}{1} = 2$	$1 \times \frac{2}{2} = 1$				
3	1	$1 \times \frac{3}{1} = 3$	$2 \times \frac{3}{2} = 3$	$1 \times \frac{3}{3} = 1$			
4	1	$1 \times \frac{4}{1} = 4$	$3 \times \frac{4}{2} = 6$	$3 \times \frac{4}{3} = 4$	$1 \times \frac{4}{4} = 1$		
5	1	$1 \times \frac{5}{1} = 5$	$4 \times \frac{5}{2} = 10$	$6 \times \frac{5}{3} = 10$	$4 \times \frac{5}{4} = 5$	$1 \times \frac{5}{5} = 1$	
6	1	$1 \times \frac{6}{1} = 6$	$5 \times \frac{6}{2} = 15$	$10 \times \frac{6}{3} = 20$	$10 \times \frac{6}{4} = 15$	$5 \times \frac{6}{5} = 6$	$1 \times \frac{6}{6} = 1$

Fig. 6.2

De fet tenim la següent llei:

$$(1) \quad \binom{n+1}{v+1} = \binom{n}{v} \frac{n+1}{v+1}.$$

Ho demostrarem ara per inducció sobre n .

Per a $n = 0$, és clar. Suposem-ho cert fins $0, 1, \dots, n$. Provem-ho per a $n+1$:

Per la llei de Pascal

$$\binom{n+1}{v+1} = \binom{n}{v} + \binom{n}{v+1}.$$

per la hipòtesi d'inducció serà

$$(2) \quad \binom{n+1}{v+1} = \binom{n-1}{v-1} \frac{n}{v} + \binom{n-1}{v} \frac{n}{v+1}.$$

Tenim que:

$$\binom{n-1}{v-1} \frac{n}{v} = \binom{n}{v} = \binom{n-1}{v-1} + \binom{n-1}{v},$$

i trobem:

$$\binom{n-1}{v} = \binom{n-1}{v-1} \left(\frac{n}{v} - 1 \right) = \binom{n-1}{v-1} \frac{n-v}{v},$$

que substituint a (2) donarà:

$$\binom{n+1}{v+1} = \binom{n-1}{v-1} \frac{n}{v} + \binom{n-1}{v-1} \frac{n-v}{v} \cdot \frac{n}{v+1}.$$

Operant:

$$\binom{n+1}{v+1} = \binom{n-1}{v-1} \frac{n(n+1)}{v(v+1)} = \binom{n}{v} \frac{n+1}{v+1},$$

com voliem demostrar.

Es dedueix també:

$$\binom{n}{v} = \frac{n!}{(n-v)!v!}, \quad \text{prou coneguda.}$$

7 Binomi de Newton (1643-1727)

Es demostra que: “els $\binom{n}{v}$ són els coeficients del binomi $(a+b)^n$ ”

Al principi ja hem dit que els xinesos coneixien aquest fet.

Per simplificar, prescindirem de la part “literal” dels polinomis resultants de les potències $(a+b)^n$. Per exemple:

$$(a+b)^2 = a^2 + 2ab + b^2, \quad \text{tractarem només dels nombres: 1, 2, 1.}$$

Veiem la Fig. 7.1, els coeficients de $(a+b)^2$ i $(a+b)^3$

$$\begin{array}{r} \boxed{1} + \boxed{1} \\ \times \boxed{1} + \boxed{1} \\ \hline \boxed{1} + \boxed{1} \\ \quad \boxed{1} + \boxed{1} \\ \hline \boxed{1} + \boxed{2} + \boxed{1} \\ (a+b)^2 \end{array} \qquad \begin{array}{r} \boxed{1} + \boxed{2} + \boxed{1} \\ \times \quad \boxed{1} + \boxed{1} \\ \hline \boxed{1} + \boxed{2} + \boxed{1} \\ \quad \boxed{1} + \boxed{2} + \boxed{1} \\ \hline \boxed{1} + \boxed{3} + \boxed{3} + \boxed{1} \\ (a+b)^3 \end{array}$$

Fig. 7.1

3ra. La suma d'elements d'una fila inclinada 135° començant per $\binom{n}{0}$ es dedueix de la fórmula anterior i de la simetria entre la columna i la fila inclinada. És:

$$\sum_{w=0}^v \binom{n+w}{w} = \binom{n+v+1}{v}.$$

9 Nombres de Fibonacci en el triangle P-T.

Es demostra que la suma dels elements de la fila inclinada de 45° són els Nombres de Fibonacci, F_n :

$$F_n = \sum_{v=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-1-v}{v}$$

en la que n és qualsevol nombre sencer.

Veure la Fig. 9.1: les columnes de la "Taula de Tartaglia" decalades 2 quadres; les sumes horitzontals són els "Nombres de Fibonacci".

F_n	Σ	(a)	(b)	(c)	(d)	(e)
$F_1 =$	1					
$F_2 =$	1	1				
$F_3 =$	2	1	1			
$F_4 =$	3	1	2			
$F_5 =$	5	1	3	1		
$F_6 =$	8	1	4	3		
$F_7 =$	13	1	5	6	1	
$F_8 =$	21	1	6	10	4	
$F_9 =$	34	1	7	15	10	1

Fig. 9.1

10 Sumes de les successives potències: $\sum_{m=1}^n m^t$, sent $t > 0$

Recordant el que hem dit en l'apartat 8, fórmula (1), podem posar:

$$\sum_{m=1}^n \binom{m}{v} = \binom{n+1}{v+1} \quad (\text{observi's que } m = 1, 2, 3, \dots, n).$$

Aplicant-ho per a $v = 1$, serà:

$$\sum_{m=1}^n m = \binom{n+1}{2} = \frac{1!}{2!}(n^2 + n) = \frac{n^2}{2} + \frac{n}{2}.$$

Per a $v = 2$

$$\sum_{m=1}^n \binom{m}{2} = \binom{n+1}{2+1} = \binom{n+1}{3}, \quad \text{és a dir}$$

$$\sum_{m=1}^n (m^2 - m) = 2! \binom{n+1}{3} = \frac{2!}{3!} (n+1)n(n-1) = \frac{n^3 - n}{3},$$

$$\sum_{m=1}^n m^2 = \frac{n^3 - n}{3} + \sum_{m=1}^n m,$$

$$\sum_{m=1}^n m^2 = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}.$$

Fent el mateix també trobariem:

$$\sum_{m=1}^n m^3 = \frac{n^4}{4} + \frac{n^3}{2} + \frac{n^2}{4},$$

$$\sum_{m=1}^n m^4 = \frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30},$$

$$\sum_{m=1}^n m^5 = \frac{n^6}{6} + \frac{n^5}{2} + \frac{5n^4}{12} - \frac{n^2}{12}.$$

I en general, està clar que procedint de la mateixa manera, obtenim:

$$(1) \quad \sum_{m=1}^n m^t = \frac{n^{t+1}}{t+1} + P(n);$$

en la que $P(n)$ és un polinomi de grau inferior a $(t+1)$.

A partir del que portem dit fins ara, es poden treure algunes conclusions:

La suma dels senars successius serà:

$$\sum_{m=1}^n (2m-1) = \sum_{m=1}^n 2m - \sum_{m=1}^n 1 = 2\left(\frac{n^2+n}{2}\right) - n = n^2.$$

La suma dels parells successius serà:

$$\sum_{m=1}^n 2m = 2 \sum_{m=1}^n m = 2\left(\frac{n^2+n}{2}\right) = 2 \binom{n+1}{2}.$$

Nombres “rectangulars”, “triangulars” i “quadrats”:

Amb la fórmula anterior, es troben els nombres, 2, 6, 12, 20, ... $(n^2 + n)$, que són els nombres “rectangulars”.

Els nombres “rectangular” partits per 2 són els nombres “triangulars”:

$$\binom{n+1}{2}.$$

Els nombres “quadrats” es troben com a suma dos a dos dels triangulars, o sigui dels nombres de la columna $\binom{n}{2}$ del T. P-T. Veiem-ho en la Fig. 10.1.

0	
1	$1+0=$ 1
3	$3+1=$ 4
6	$6+3=$ 9
10	$10+6=$ 16
15	$15+10=$ 25

Fig. 10.1

11 Importants derivacions del triangle Pascal-Tartaglia

11.1 Demostració de la fórmula, en notació moderna:

$$\int_0^a x^n dx = \frac{a^n + 1}{n + 1}.$$

FERMAT (1601-1665) nascut a Beaumont de Lomagne, a una trentena de quilòmetres al Nord de Toulouse, es pot considerar el matemàtic que en la seva època més bé coneixia el T. P-T i el que més “suc” en va treure. Pascal el va definir com “el primer home del món” i li escrigué en una ocasió: “Busqueu en d’altres parts qui us segueixi en les vostres invencions numèriques; pel que a mi fa us confesso que sóc molt lluny d’això: no sóc capaç més que d’admirar-les”.

Fermat, abans del 1636 ja coneixia la igualtat que hem indicat al començament d’aquest apartat.

Per situar-nos més bé en el moment en que Fermat va fer aquesta trascendental descoberta, recordem tres fets:

- 1er.** Fermat havia emprat les coordenades en els seus estudis geomètrics, abans que DESCARTES (1596-1650). Se’ls considera els inventors de la Geometria Analítica.
- 2on.** Des d’ARQUÍMEDES (287(?) -212, a. C.), passant per GALILEU (1564-1642), CAVALIERI (1598-1647) i d’altres [entre els quals l’astrònom KEPLER (1571-1630)] es preconitzava el càlcul de les longituds, superfícies

i volums a base de dividir-les i sumar tots els valors trobats. Com més petites les divisions, més exacte el resultat.

3er. Arquímedes havia calculat la superfície entre una recta i un arc de paràbola construint un triangle de superfície equivalent.

En la Fig. 11.1, tenim la gràfica d'una paràbola d'equació $y = x^2$. Hem dividit la base de longitud 1 en 10 espais iguals a 0'1.

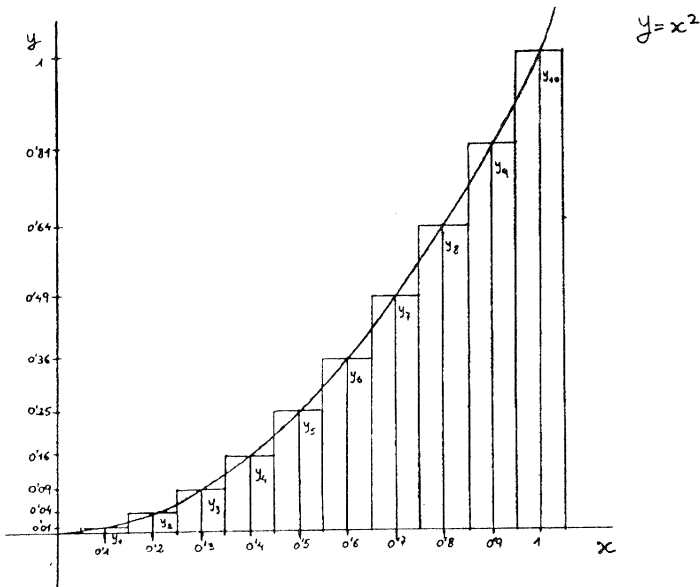


Fig. 11.1

Els rectangles tenen les superfícies següents:

Primer rectangle (d'esquerra a dreta):	$y_1 \times 0,1 = 0,01 \times 0,1 = 0,001$.
Segon rectangle	$y_2 \times 0,1 = 0,04 \times 0,1 = 0,004$.
Tercer rectangle	$y_3 \times 0,1 = 0,09 \times 0,1 = 0,009$.
⋮	
Desè rectangle	$y_{10} \times 0,1 = 1 \times 0,1 = 0,1$.

La suma dels deu rectangles és la superfície S_d :

$$S_d = 0,1(0,01 + 0,04 + 0,09 + \dots + 1) = 0,385.$$

Ara bé, pel que hem vist en l'apartat 10, tenim que la suma dels deu valors: $y_1, y_2, y_3 \dots y_{10}$, és:

$$\sum_{m=1}^{10} (0,1m)^2 = 0,1^2 \sum_{m=1}^{10} m^2 = 0,01 \left(\frac{10^3}{3} + \frac{10^2}{2} + \frac{10}{6} \right) = 0,01 \times 385 = 3,85.$$

Per tant S_d serà:

$$S_d = 0,1 \times 3,85 = 0,385.$$

Si en la Fig. 11.1 enlloc de 10 divisions en féssim 100 tindriem més precisió en el càlcul (no farem cap figura amb les 100 divisions). Tindrem, raonant igual que abans:

$$\sum_{m=1}^{100} (0,01m)^2 = 0,01^2 \sum_{m=1}^{100} m^2 = 0,0001 \left(\frac{100^3}{3} + \frac{100^2}{2} + \frac{100}{6} \right) = 33,835.$$

I la S_c , serà:

$$S_c = 0,01 \times 33,835 = 0,33835.$$

Sense saber quin és el valor de la superfície buscada, sabem, i es confirma fàcilment el mateix per una funció $y = f(x)$, que com més divisions fem més ens acostarem al valor correcte.

Suposarem ara que enlloc de divisions de 0,1 i 0,01 de la base, les farem d'un valor igual a f , sent:

$$q = \frac{1}{f} \quad (q: \text{quantitat total de divisions fetes}).$$

La superfície S_q , serà:

$$S_q = f \times \sum_{m=1}^q (fm)^2 = f^3 \sum_{m=1}^q m^2 = f^3 \left(\frac{q^3}{3} + \frac{q^2}{2} + \frac{q}{6} \right),$$

i serà:

$$S_q = f^3 \left(\frac{1}{3f^3} + \frac{1}{2f^2} + \frac{1}{6f} \right) = \frac{1}{3} + \frac{f}{2} + \frac{f^2}{6}.$$

Hem dit al començament d'aquest apartat que cal fer el màxim petites les subdivisions; el més petit és $f=0$.

Tindrem doncs:

$$S_q = \frac{1}{3}.$$

Si enlloc de trobar la superfície determinada per la paràbola i l'eix de les x (Fig. 11.1) entre $x = 0$ i $x = 1$, trobem la superfície entre $x = 0$ i $x = x$, serà:

$$q = \frac{x}{f},$$

i la superfície S_{x^2} , serà:

$$S_{x^2} = \frac{x^3}{3}.$$

Recordant l'apartat 10 fórmula (1) tindrem:

$$S_{x^t} = \frac{x^{t+1}}{t+1},$$

sent S_{x^t} la superfície compresa entre $y = x^t$ i l'eix de les x , entre $x = 0$ i $x = x$.

A Leibniz es deu el símbol actual d'integral que és una "essa" estilitzada. Per tant en notació moderna S_{x^t} serà el que hem escrit al principi d'aquest apartat.

11.2 Teorema de Fermat ("Petit Teorema")

$$(1) \quad a^p \equiv a \pmod{p}.$$

Si mirem en la Fig. 6.1, columna de la dreta, veurem els resultats de 2^p per a $p = 3, 5, 7$ i 11 , que compleixen les respectives congruències, indicades per (1):

$$\begin{array}{lll} 2^3 & = & 8 \qquad \qquad 8 \equiv 2 \pmod{3}, \\ 2^5 & = & 32 \qquad \qquad 32 \equiv 2 \pmod{5}, \\ 2^7 & = & 128 \qquad \qquad 128 \equiv 2 \pmod{7}, \\ 2^{11} & = & 2048 \qquad \qquad 2048 \equiv 2 \pmod{11}. \end{array}$$

Anem ara a deduir la següent congruència:

$$(a+b)^{p^k} \equiv a^{p^k} + b^{p^k} \pmod{p}.$$

Desenvolupant com hem dit en l'apartat 7:

$$\begin{aligned} (a+b)^{p^k} &= \binom{p^k}{0} a^{p^k} b^0 + \binom{p^k}{1} a^{p^k-1} b^1 + \dots + \binom{p^k}{p^k} a^0 b^{p^k}, \\ (a+b)^{p^k} &= a^{p^k} + p^k a^{p^k-1} b + \dots + b^{p^k}. \end{aligned}$$

Veiem que tots els sumands excepte el primer i el darrer, són divisibles per p :
Fent $k = 1$, tindrem:

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

Fent $a = 0, 1, 2, \dots, n$ i $b = 1$, tenim:

$$(n + 1)^p \equiv n^p + 1^p \pmod{p} \equiv n + 1 \pmod{p}.$$

I queda demostrada per inducció, la (1).

Fàcilment es dedueix:

$$(2) \quad a^{p-1} \equiv 1 \pmod{p}, \quad (\text{sent } (a, p) = 1).$$

Aquesta darrera fórmula és d'ús molt freqüent i d'ella es dedueix la fórmula, més general, del:

Teorema d'Euler:

$$a^{\varphi(m)} \equiv 1 \pmod{m}, \quad (\text{sent } (a, m) = 1)$$

en la que m és un nombre compost:

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_n^{\alpha_n} \quad (p_1, p_2 \dots p_n : \text{ nombres primers}).$$

i la "funció d'Euler" $\varphi(m)$, denota el nombre de sencers $1 \leq K \leq m$ primers amb m . És ben conegut que $\varphi(m)$ val:

$$\varphi(m) = p_1^{\alpha_1-1}(p_1 - 1) \cdot p_2^{\alpha_2-1}(p_2 - 1) \dots p_n^{\alpha_n-1}(p_n - 1).$$

Segons hem dit a (2): $a^{p-1} \equiv 1 \pmod{p}$, vol dir:

$a^{p-1} = cp + 1$, que elevat a p , és:

$$a^{p(p-1)} = (cp + 1)^p.$$

Aplicat el desenvolupament del binomi a aquesta fórmula,

$$\binom{p}{0} c^p p^p + \binom{p}{1} c^{p-1} p^{p-1} + \dots + \binom{p}{p} c^0 p^0 \equiv 1 \pmod{p^2}.$$

I en general:

$$a^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^\alpha}.$$

Pel que hem dit abans:

$$\begin{array}{l} a^{\varphi(m)} \equiv 1 \pmod{p_1^{\alpha_1}} \quad \text{i per tant} \quad a^{\varphi(m)} - 1 \equiv 0 \pmod{p_1^{\alpha_1}}, \\ a^{\varphi(m)} \equiv 1 \pmod{p_2^{\alpha_2}} \quad \text{i per tant} \quad a^{\varphi(m)} - 1 \equiv 0 \pmod{p_2^{\alpha_2}}, \\ \vdots \\ a^{\varphi(m)} \equiv 1 \pmod{p_n^{\alpha_n}} \quad \text{i per tant} \quad a^{\varphi(m)} - 1 \equiv 0 \pmod{p_n^{\alpha_n}}. \end{array}$$

També serà:

$$a^{\varphi(m)} - 1 \equiv 0 \quad [\text{mòd}(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_n^{\alpha_n})], \quad \text{i:}$$

$a^{\varphi(m)} \equiv 1 \pmod{m}$, com es volia demostrar.