

*Polinomi, campi e duelli: le  
equazioni polinomiali tra storia e  
matematica*

- Gerarchia delle cose che esistono:
  - 1) Dio.
  - 2) Entità spirituali superiori
  - 3) Uomo
  - 4) Natura
- Gerarchia delle discipline:
  - 1) Teologia.
  - 2) Filosofia o “scientia”.
  - 3) Storia.
  - 4) Matematica.
  - 5) Tecnologia, macchine, arti, alchimia.



Filippo Calandri, *Aritmetica* (c.1485)

Sono due torre una piso di  
lasse d'altezza. Si latere a di  
torre et distanza delle due torre  
è di cento braccia: quanto distan-  
za è a una fonte d'acqua interme-  
zia che maneggi due uccelli del-  
le due torre: si calcola de pari nata  
permette almeno ad una fonte  
qualche latere fonte: fissa per  
la acquisita fonte: fissa per  
multiplicata latere della torre  
seconda per la fonte: non si faccia  
per la fonte: se si moltiplica  
per la fonte: per multiplicata latere della

*Sono due torre in uno piano, che l'una è alta 60 bracia, l'altra è alta 80 bracia, et da l'una torre a l'altra è 100 bracia; et in tra queste due torre è una fonte d'aqua in tal luogho che movendosi due uccelli di sudette torre, et volando di pari volo, giungono a un'otta a detta fonte; vo' sapere quanto la detta fonte sarà presso a ciascuna torre. Fa' così: prima ultipli cha l'altezza della torre ognuna per sé, cioè prima 80 vie 80 fa 6400, poi 60 vie 60 fa 3600, tralo di 6400, resta 2800; poi multipricha la distantia che è dal'una torre a l'altra, cioè 100 bracia vie 100 fa 10000 et questo agugni con 2800 fa 12800 et questo parti per 200, cioè per 2 volte la distanza che è fra l'una torre e l'altra, che ne viene 64 bracia. E tanto sarà dalla fonte alla torre delle 60 bracia, et alla torre delle 80 bracia sarà presso a 36 braccia.*



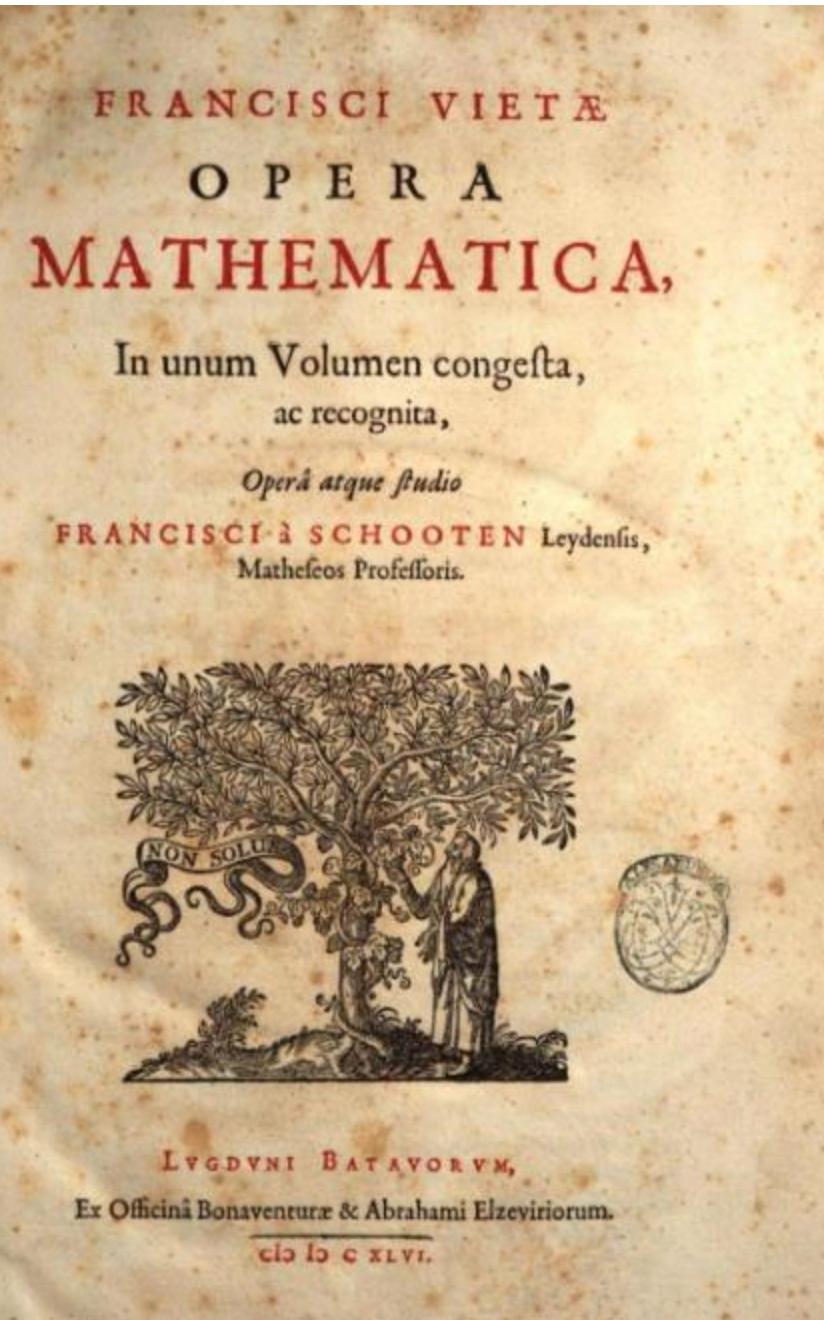
Filippo Calandri, *Aritmetica* (c.1485)

*Sono due torre in uno piano, che l'una è alta 60 bracia, l'altra è alta 80 bracia, et da l'una torre a l'altra è 100 bracia; et in tra queste due torre è una fonte d'aqua in tal luogho che movendosi dua ucelli di sudette torre, et volando di pari volo, giungono a un'otta a detta fonte; vo' sapere quanto la detta fonte sarà presso a ciascuna torre. Fa' così: prima ultipli cha l'altezza della torre ognuna per sé, cioè prima 80 vie 80 fa 6400, poi 60 vie 60 fa 3600, tralo di 6400, resta 2800; poi multipricha la distantia che è dal'una torre a l'altra, cioè 100 bracia vie 100 fa 10000 et questo agugni con 2800 fa 12800 et questo parti per 200, cioè per 2 volte la distanza che è fra l'una torre e l'altra, che ne viene 64 bracia. E tanto sarà dalla fonte alla torre delle 60 bracia, et alla torre delle 80 bracia sarà presso a 36 braccia.*

$a = 60$ ,  $b = 80$ : altezze delle due torri ( $b > a$ )       $d = 100$ : distanza tra le due torri

la distanza della fonte dalla base della prima torre (di altezza  $a$ ) è

$$\frac{b^2 - a^2 + d^2}{2d} = \frac{80^2 - 60^2 + 100^2}{200} = \frac{6400 - 3600 + 10000}{200} = \frac{12800}{200} = 64$$



François Viète (1540-1603)

Dantur.

P R O P O S I T I O   V I .

**D**uarum magnitudinum aggregato differentiam earundem addere.

*re.*  
Sit  $A + B$  addenda  $A - B$ : summa fit  $A$  bis. Vnde

T H E O R E M A .

Aggregatum duarum magnitudinum adjunctum differentiæ earundem, æquale est duplo magnitudinis majoris.

P R O P O S I T I O   V I I .

**D**uarum magnitudinum aggregato differentiam earundem subducere.

*cere.*  
Sit ex  $A + B$  auferenda  $A - B$ : residua fit  $B$  bis. Vnde

# Al-Khwarizmi *Al-jabr w'al-muqabala*

## I sei tipi di equazioni algebriche di primo e di secondo grado

➤ quadrati uguale a cose       $ax^2 = bx$

➤ quadrati uguale a numero       $ax^2 = c$

➤ cose uguale a numero       $ax = c$

➤ quadrati e cose uguale a numero

$$ax^2 + bx = c$$

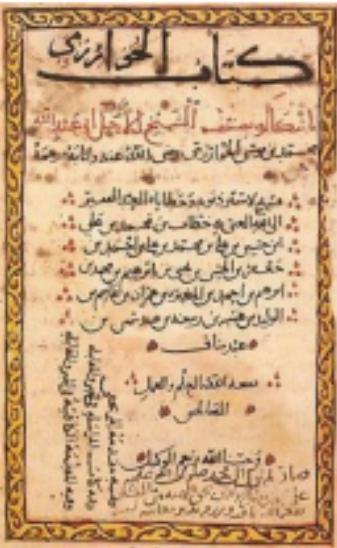
➤ quadrati e numero uguale a cose

$$ax^2 + c = bx$$

➤ cose e numero uguale a quadrati

$$bx + c = ax^2$$

con  $a, b, c$  numeri positivi



## La regola per risolvere l'equazione

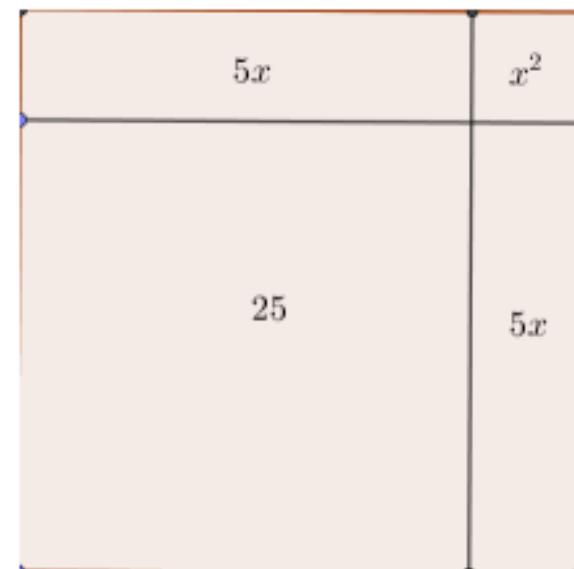
$$x^2 + 10x = 39$$

$$x = \sqrt{\left(\frac{10}{2}\right)^2 + 39} - \frac{10}{2} = 3$$

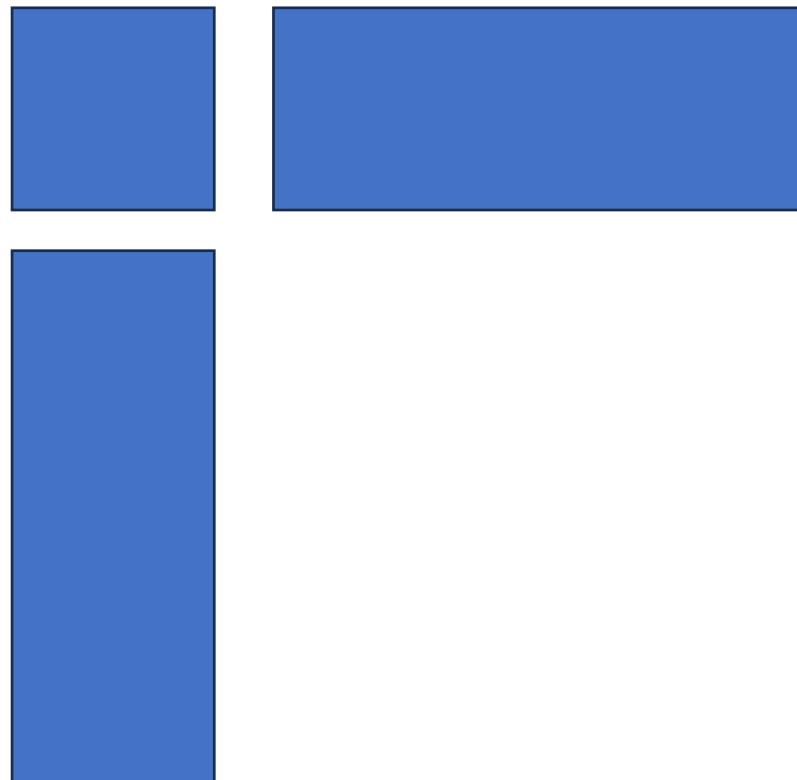
$$x^2 + px = q \quad p, q > 0$$

$$x = \sqrt{\left(\frac{p}{2}\right)^2 + q} - \frac{p}{2}$$

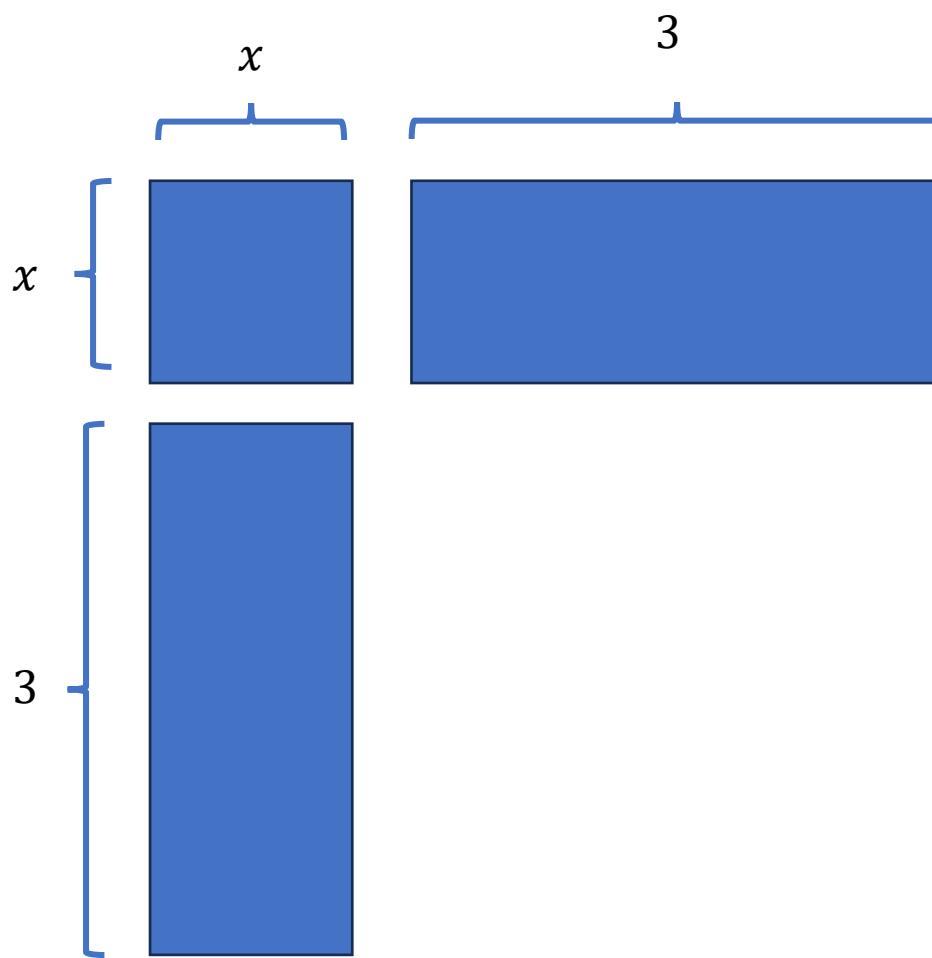
## Il completamento del quadrato



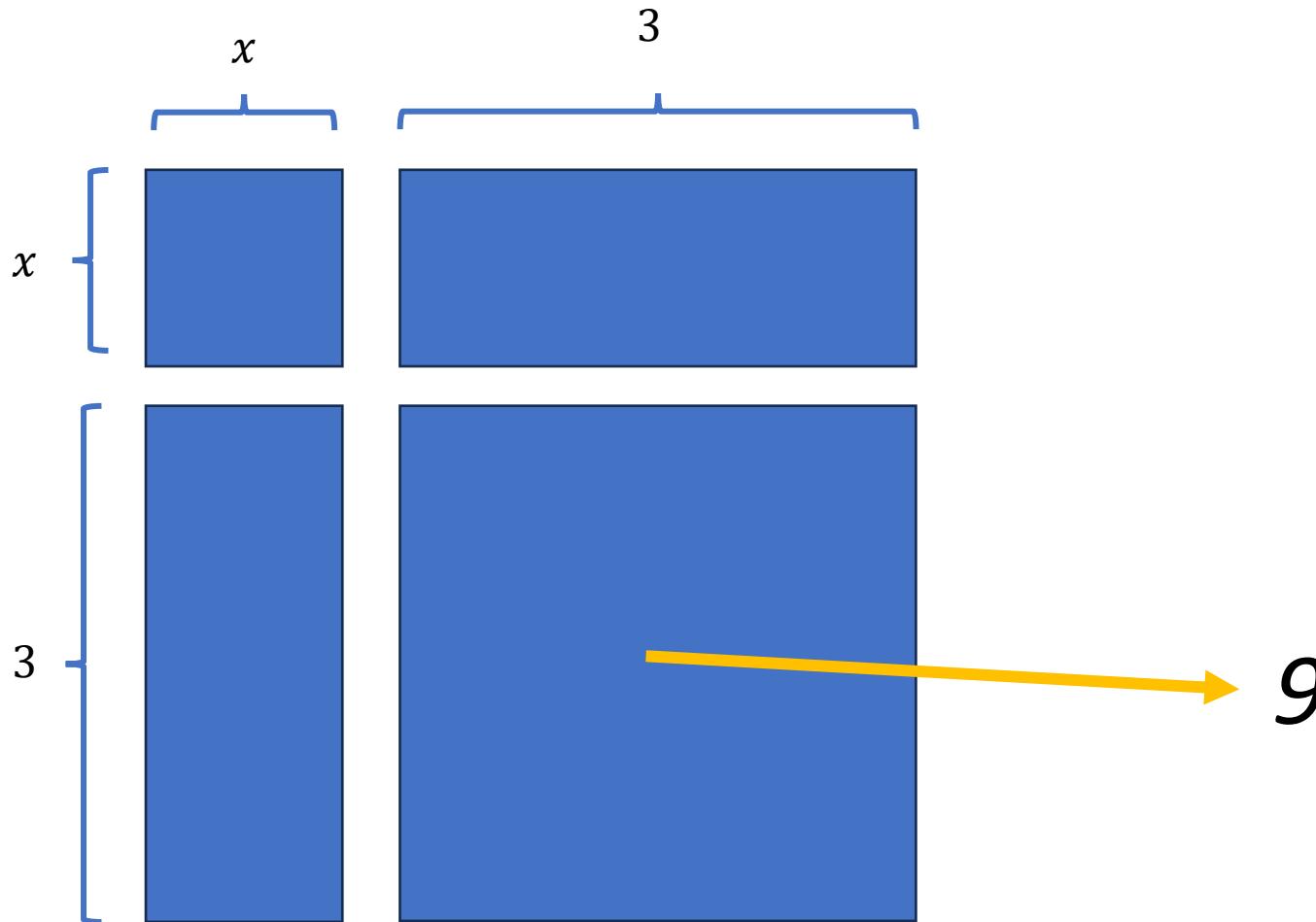
$$x^2 + 6x = 16$$

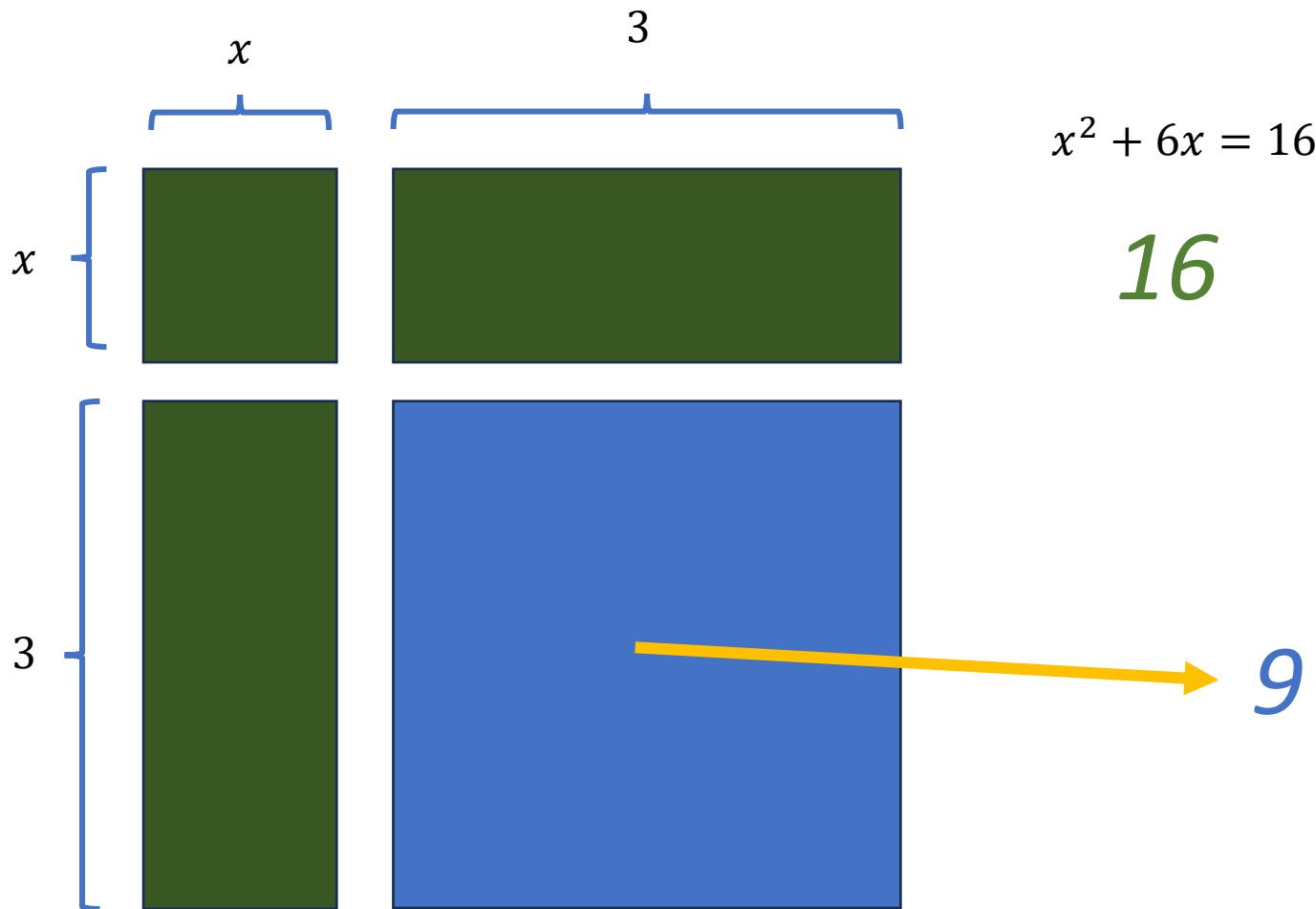


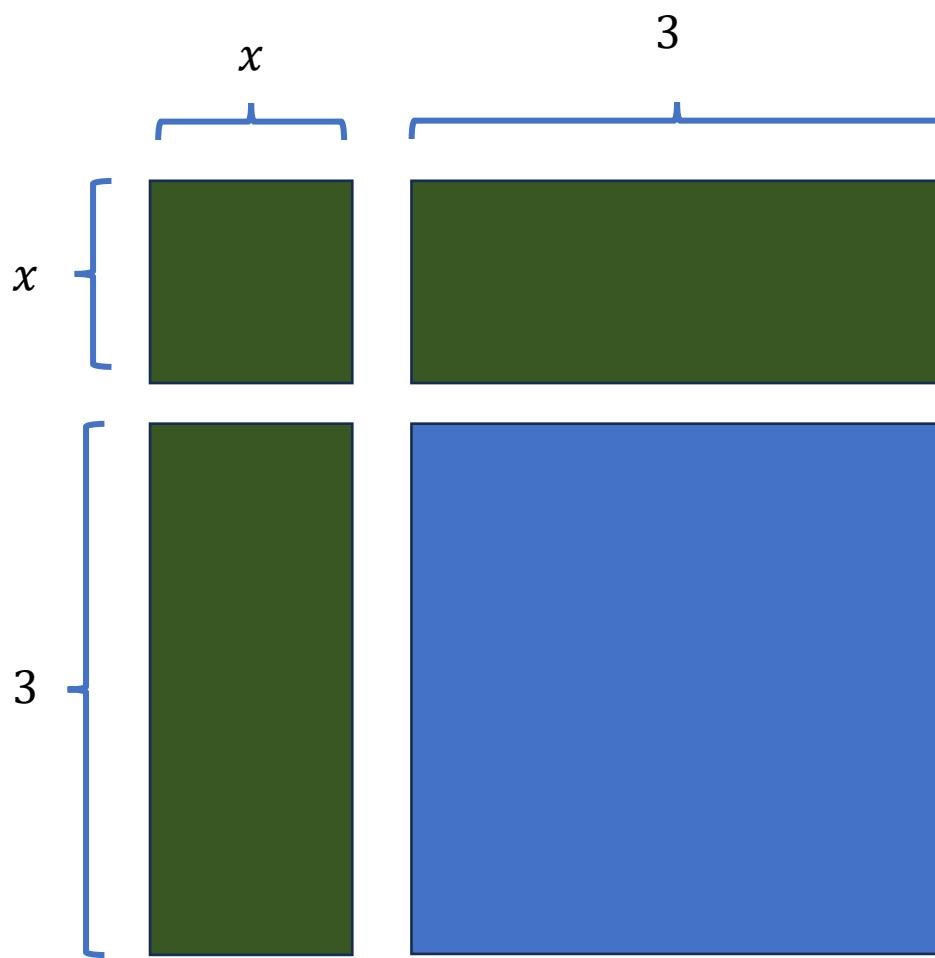
$$x^2 + 6x$$



$$x^2 + 6x$$







25

5

$$x+3=5$$

$$x=2$$

$$x^2 + 6x = 16$$

$$x^2 + 6x - 16 = 0$$

$$x_{1,2} = \frac{-6 \pm \sqrt{36 + 64}}{2} = \frac{-6 \pm 10}{2} =$$

2

-8

Scipione del Ferro  
(1465-1526)

Insegna a Bologna dal 1496.

Riesce a trovare una soluzione generale per i problemi cubici *depressi*.

$$x^3 + ax^2 + bx + c = 0$$



$$x^3 + bx + c = 0$$

Antonio Maria del Fiore  
(?-?)



Niccolò Tartaglia  
(1499-1557)

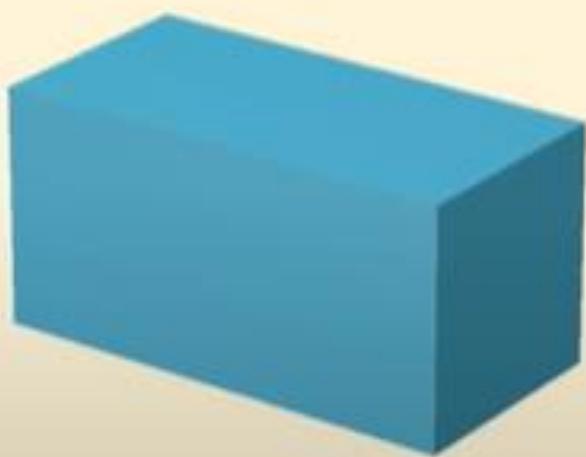
Vero nome: Niccolò Fontana

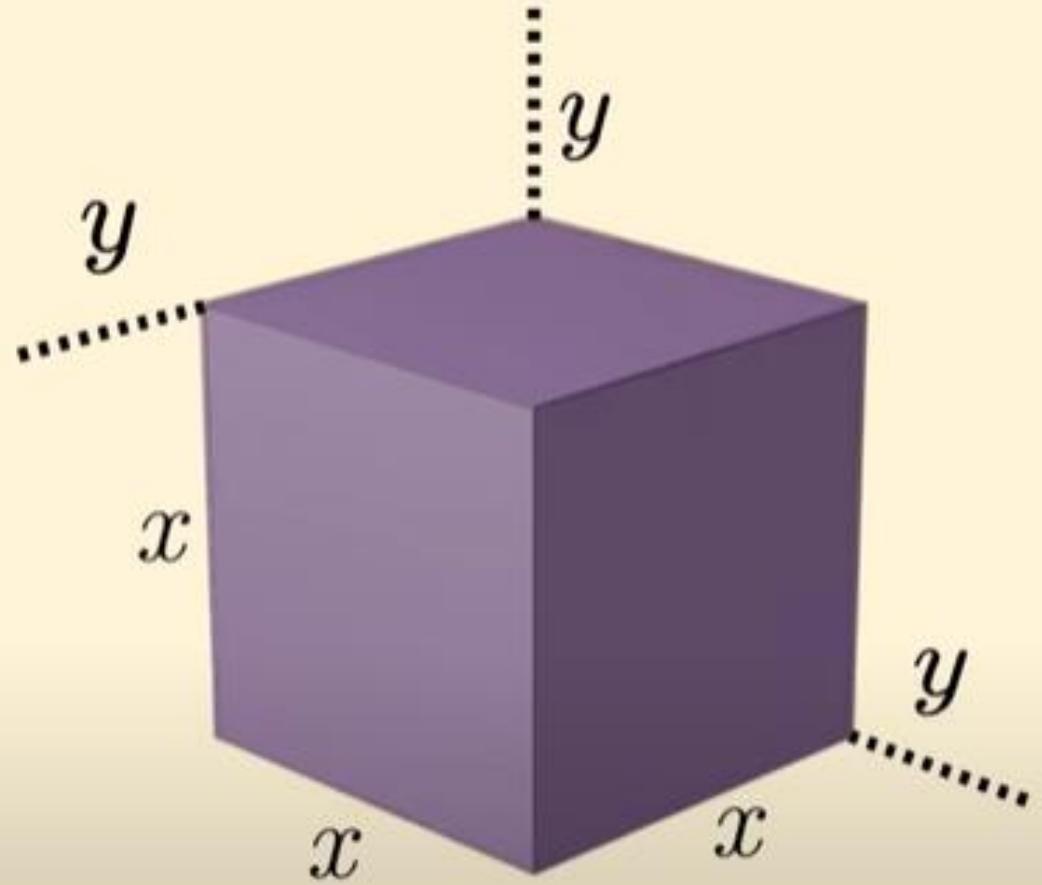
Sacco di Brescia 1512: viene ferito al cranio e alla mascella

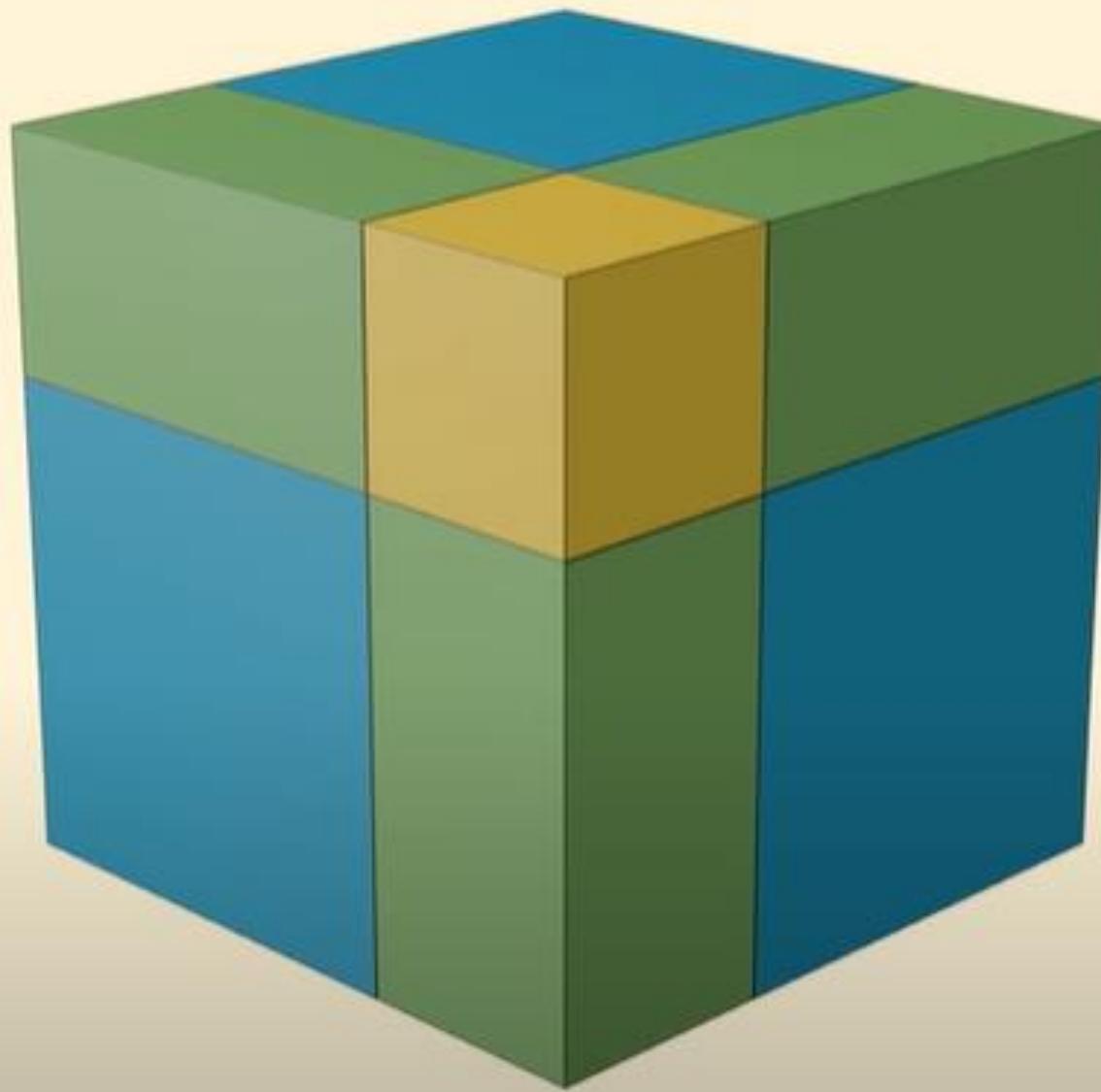
Nel 1521 diventa docente di matematica a Verona

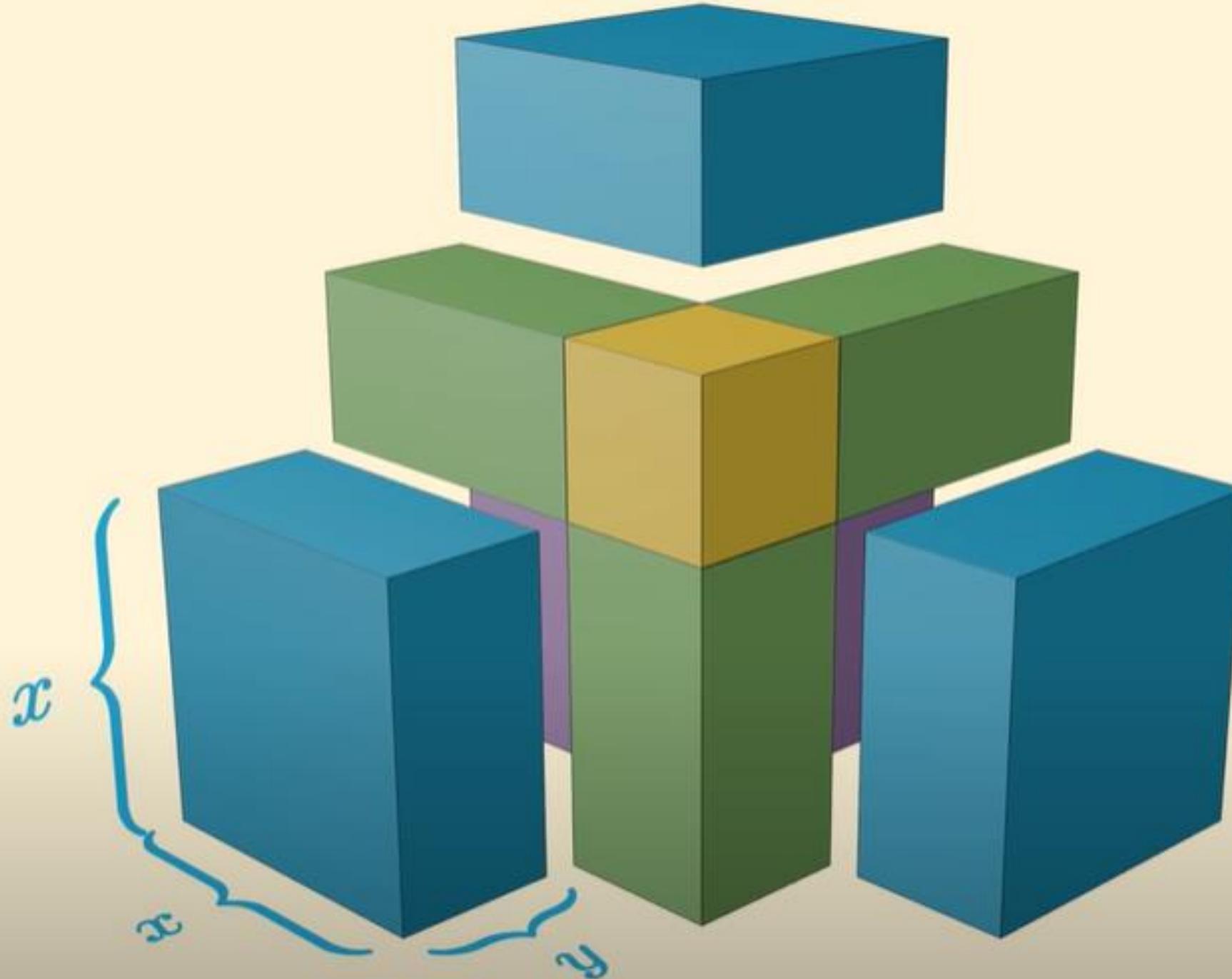
Nel 1535 viene sfidato da Antonio del Fiore

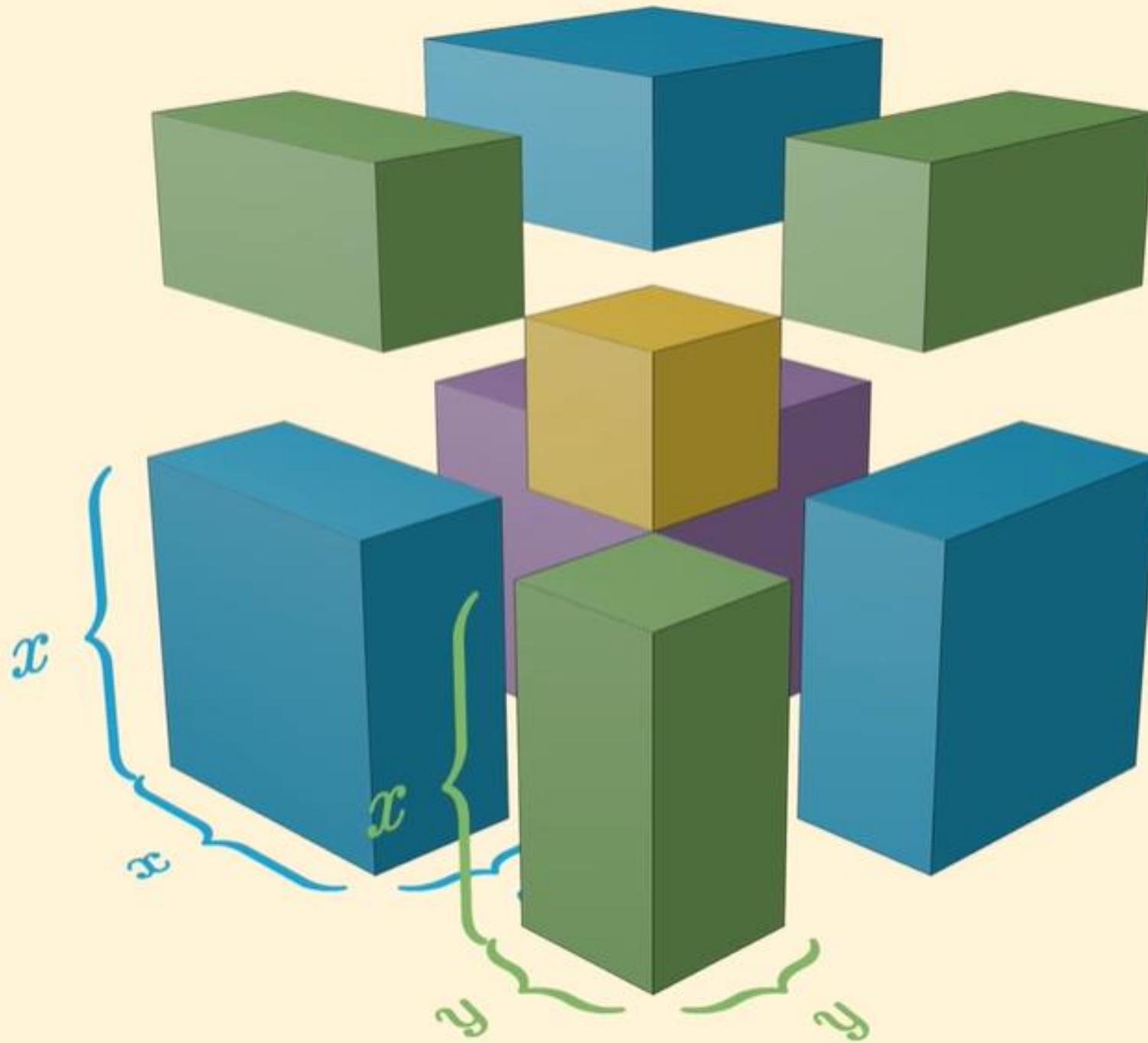
$$x^3 + 9x = 26$$

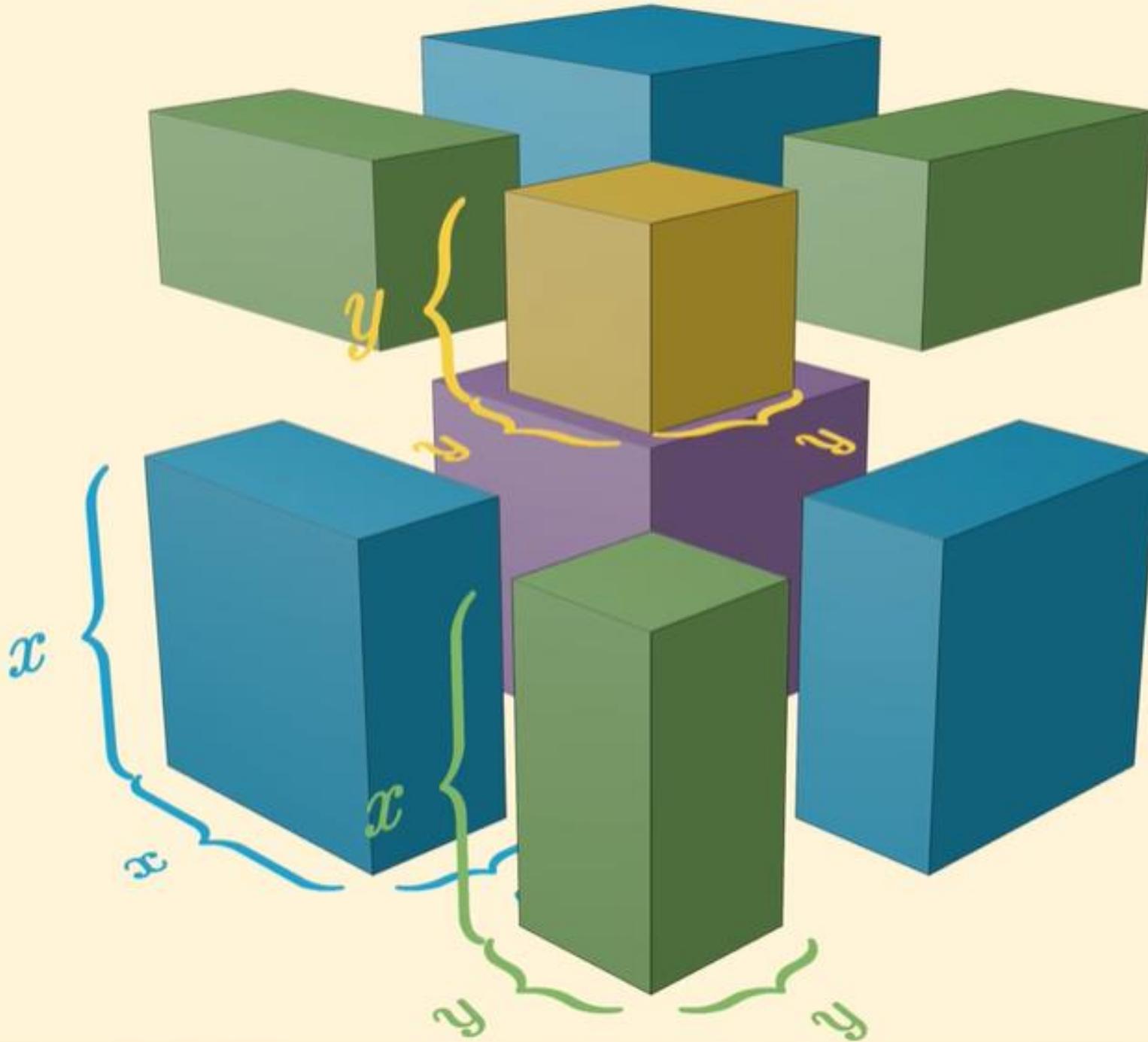


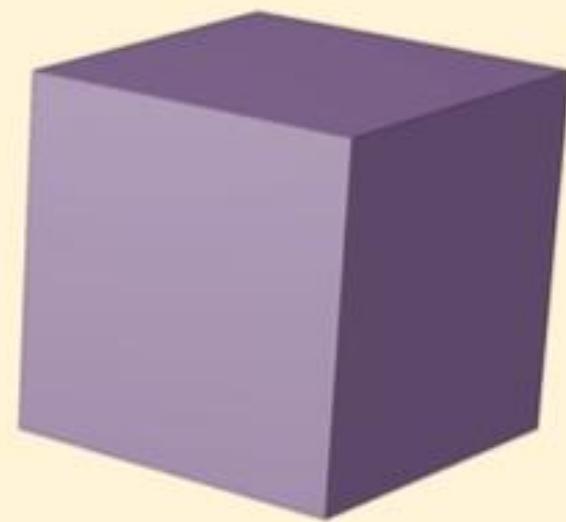
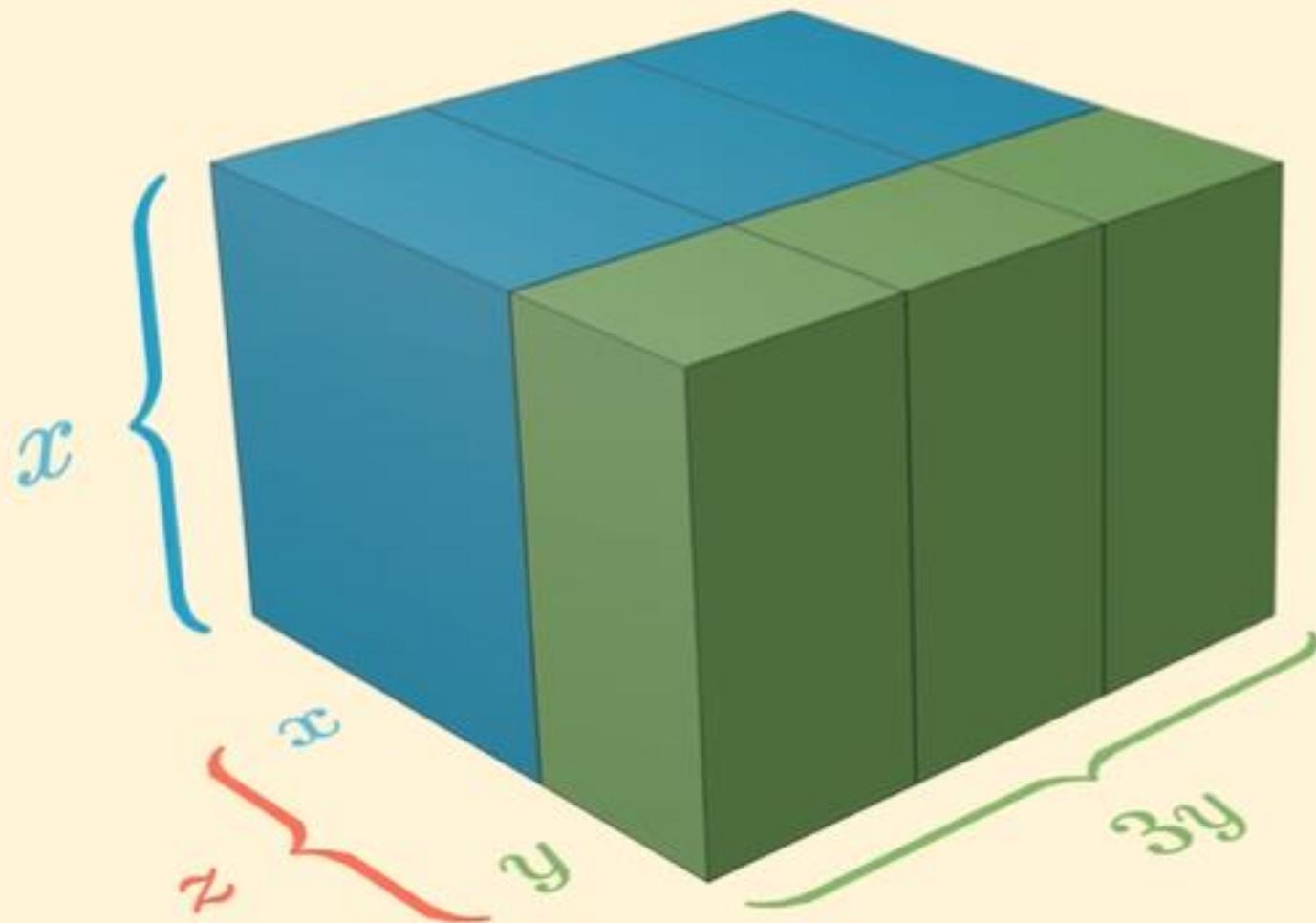




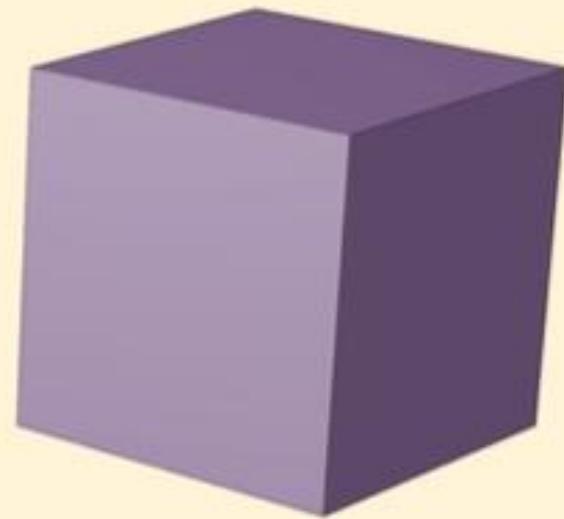
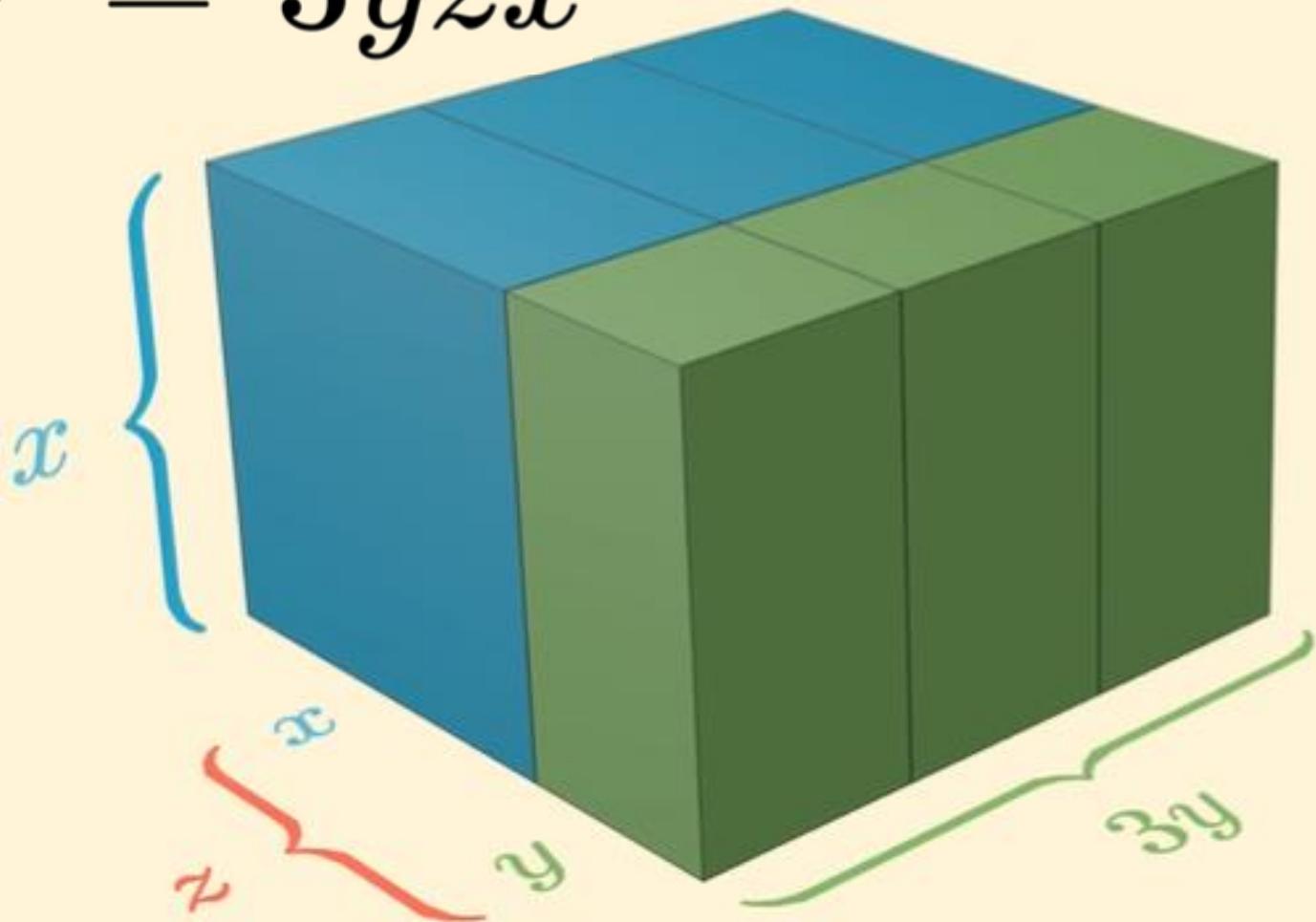






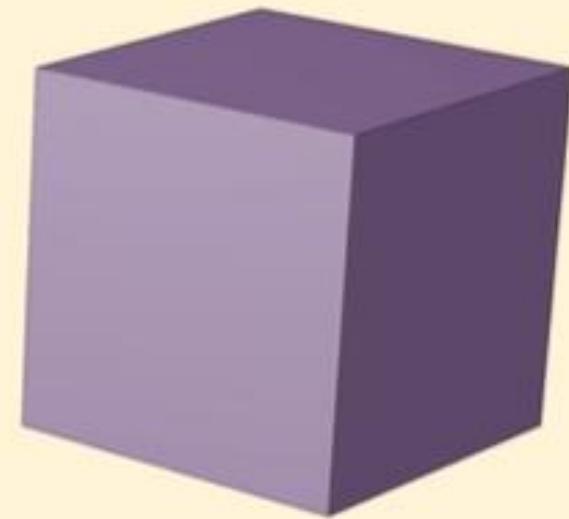
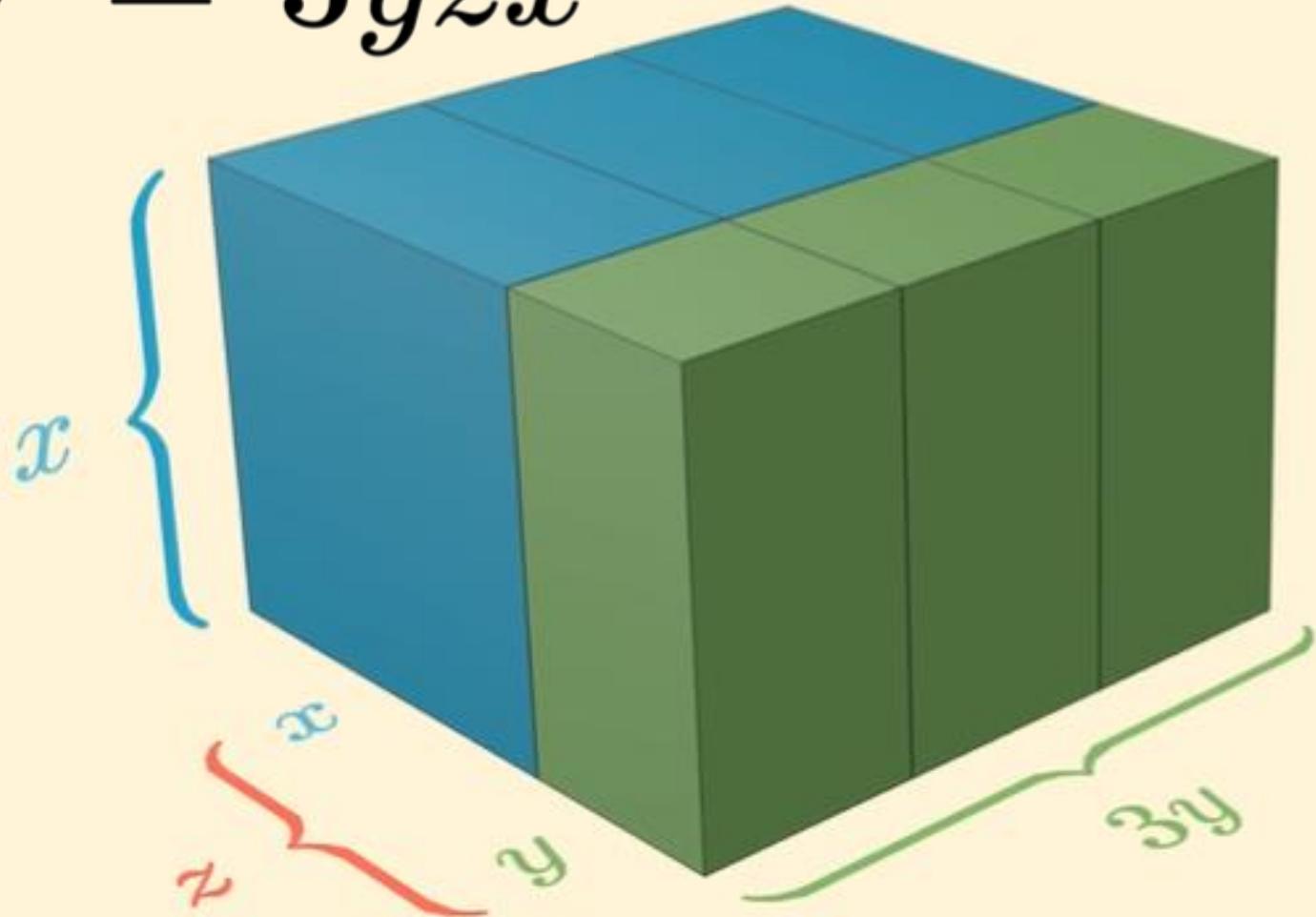


$$V = 3yzx$$



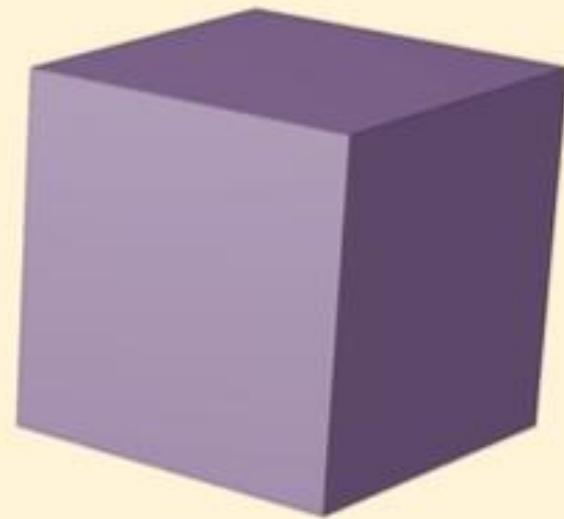
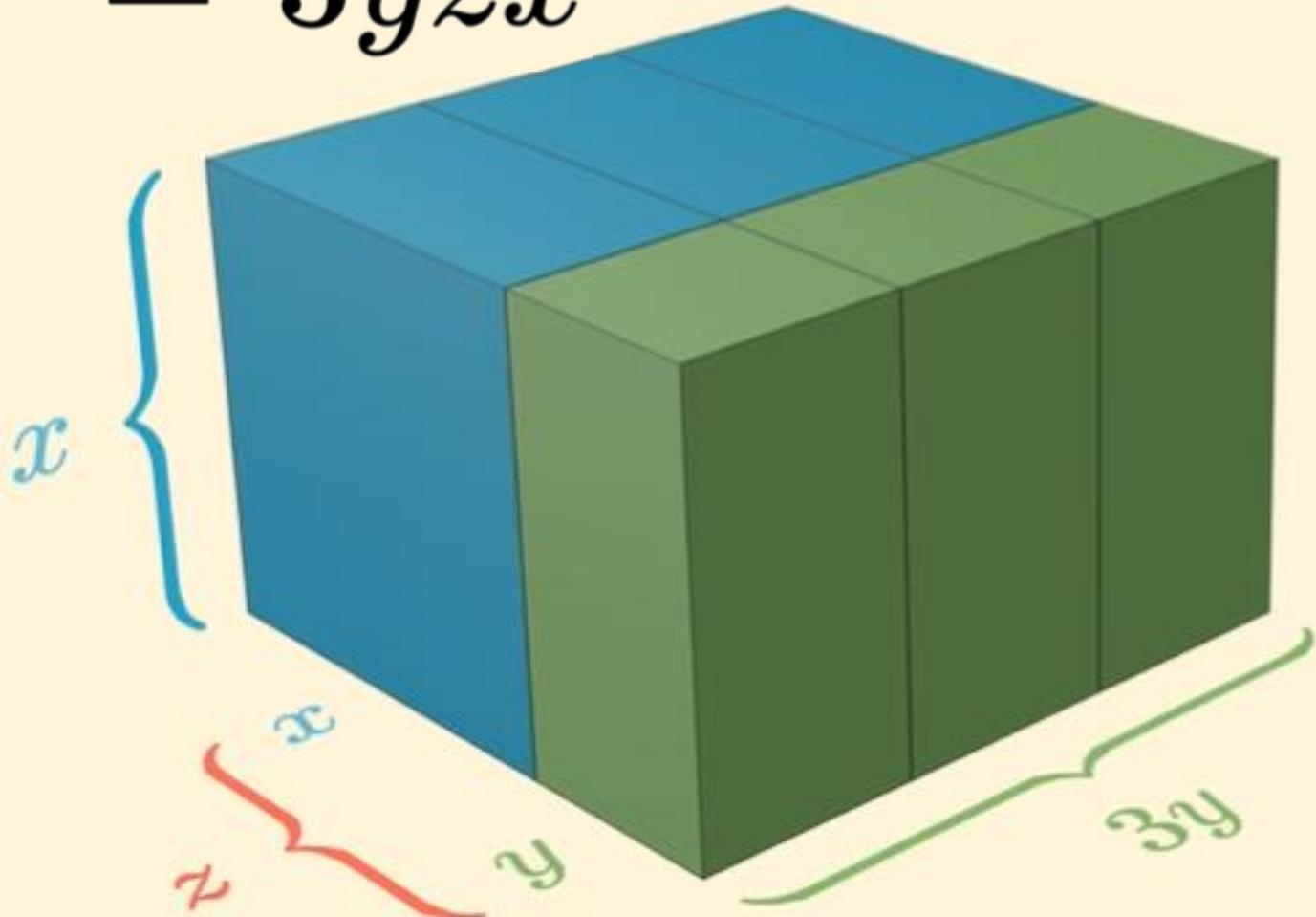
$$x^3 + 9x = 26$$

$$V = 3yzx$$



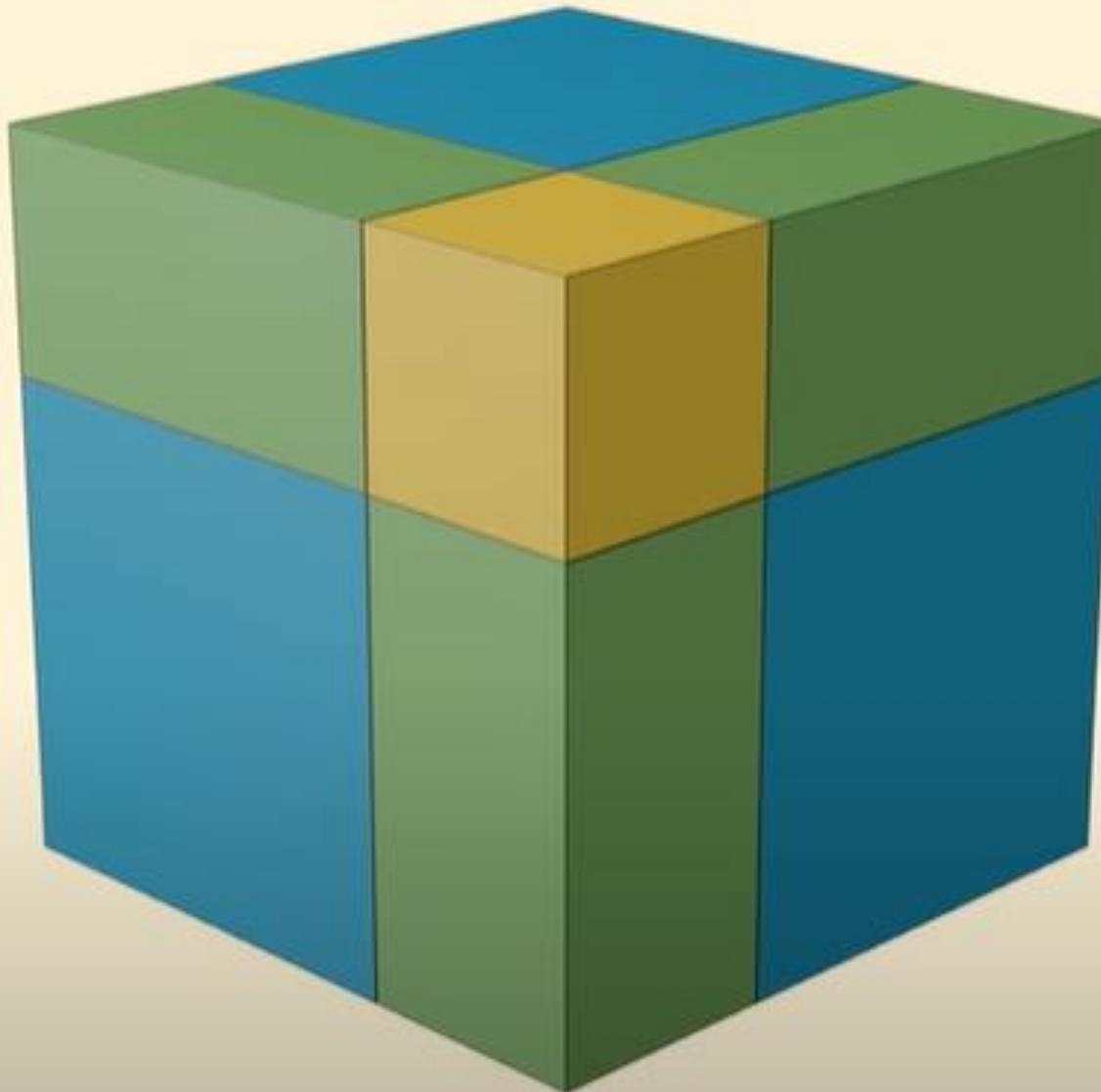
$$x^3 + 9x = 26$$

$$V = 3yzx$$



$$3yz = 9$$

$$x^3 + 9x + y^3 = 26 + y^3 \quad 3yz = 9$$



$$\underbrace{x^3 + 9x + y^3}_{z^3} = 26 + y^3 \quad 3yz = 9$$
$$= 26 + y^3$$

$$\underbrace{x^3 + 9x + y^3}_{z^3} = 26 + y^3 \quad 3yz = 9$$
$$z^3 = 26 + y^3$$

$$z = \frac{3}{y}$$

$$y^6 + 26y^3 - 27 = 0$$

Quando chel cubo con le cose appresso  
Se agguaglia à qualche numero discreto  
Trouan dui altri differenti in esso.  
Dapoi terrai questo per consueto  
Che'llor produtto sempre sia eguale  
Al terzo cubo delle cose neto,  
El residuo poi suo generale  
Delli lor lati cubi ben sottratti  
Varra la tua cosa principale.  
In el secondo de cotesti atti  
Quando che 'l cubo restasse lui solo  
Tu osseruarai quest'altri contratti,  
Del numer farai due tal part'à uolo  
Che l'una in l'altra si produca schietto

El terzo cubo delle cose in stolo  
Delle qual poi, per commun precetto  
Torrai li lati cubi insieme gionti  
Et cotal somma sara il tuo concetto.  
El terzo poi de questi nostri conti  
Se solue col secondo se ben guardi  
Che per natura son quasi congionti.  
Questi trouai, & non con pañi tardi  
Nel mille cinquecent'e, quattro e trenta  
Con fondamenti ben sald'e gagliardi  
Nella citta dal mar'intorno centa.

Quando chel cubo con le cose  
 apresso  
 Se aguaglia a qualche numero  
 discreto  
 Trovan dui altri differenti in  
 esso.  
 Dapoi terrai questo per  
 consueto  
 Che'el lor produtto sempre sia  
 eguale  
 Al terzo cubo delle cose neto.  
 El residuo poi suo generale  
 Delli lor lati cubi ben sottratti  
 Varrà la tua cosa principale.

$$x^3 + px = q$$

$$u^3 - v^3 = q$$

$$u^3v^3 = \left(\frac{p}{3}\right)^3$$

$$x = u - v$$

In el secondo de codesti atti  
 Quando chel cubo restasse lui solo  
 Tu osserverai quest'altri contratti:  
 Del numer farai due tal parti a volo  
 Che l'una in l'altra si produca schietto  
 El terzo cubo delle cose in stolo.  
 Delle qual poi, per commun preceitto  
 Torrai li lati cubi insieme gionti  
 Et cotal summa sarà il tuo concetto.

$$x^3 = px + q$$

$$u^3 + v^3 = q$$

$$u^3v^3 = \left(\frac{p}{3}\right)^3$$

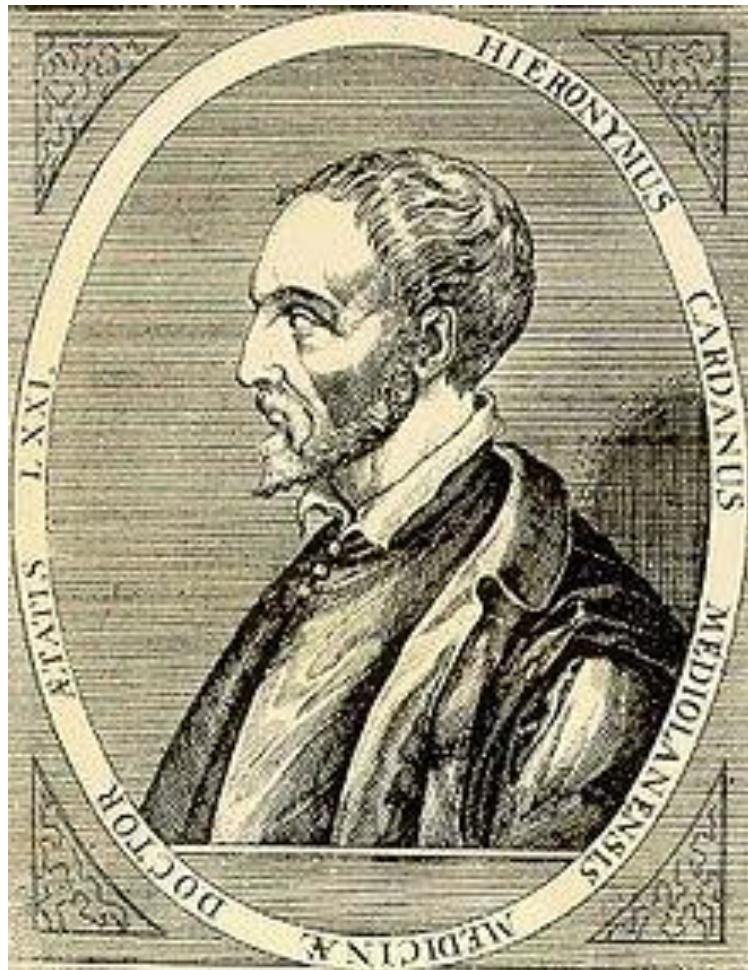
$$x = u + v$$

$$x^3 + q = px$$

Venezia 1534



Santa Maria dei Servi a Bologna

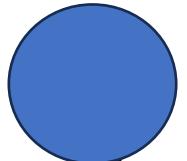


Gerolamo Cardano  
(1501-1576)

Figlio illegittimo di Fazio Cardano,  
nobile.

Studia medicina a Pavia e poi si  
trasferisce a Padova

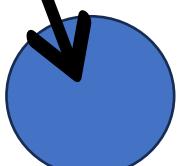
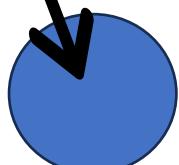
La sua vita è costellata di difficoltà  
lavorative, spesso risolte grazie  
all'aiuto della famiglia Borromeo.

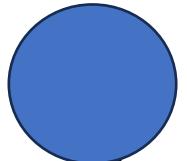


**2 Gennaio 1539**

Cardano scrive a Tartaglia per avere la formula risolutiva.

Tartaglia si rifiuta.

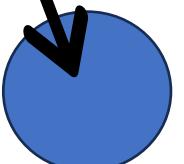




**2 Gennaio 1539**

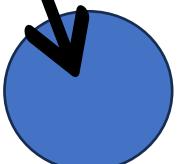
Cardano scrive a Tartaglia per avere la formula risolutiva.

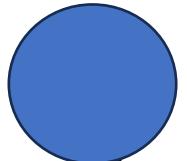
Tartaglia si rifiuta.



**12 febbraio 1539**

Cardano risponde arrabbiato a Tartaglia.





**2 Gennaio 1539**

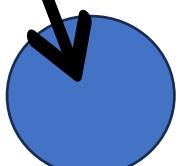
Cardano scrive a Tartaglia per avere la formula risolutiva.

Tartaglia si rifiuta.



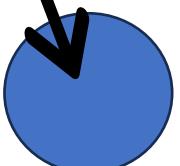
**12 febbraio 1539**

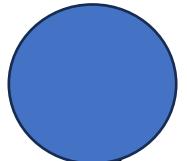
Cardano risponde arrabbiato a Tartaglia.



**13 marzo 1539**

Cardano invita Tartaglia a Milano.





**2 Gennaio 1539**

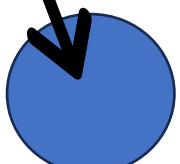
Cardano scrive a Tartaglia per avere la formula risolutiva.

Tartaglia si rifiuta.



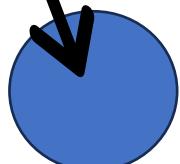
**12 febbraio 1539**

Cardano risponde arrabbiato a Tartaglia.



**13 marzo 1539**

Cardano invita Tartaglia a Milano.



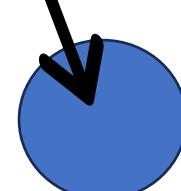
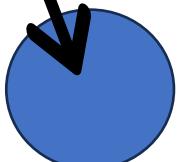
**25 marzo 1539**

Tartaglia arriva a Milano e soggiorna da Cardano.



**1539**

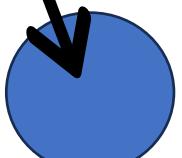
Per tutto l'anno i due restano in corrispondenza.





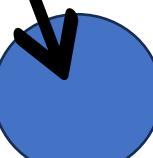
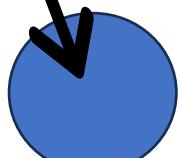
1539

Per tutto l'anno i due restano in corrispondenza.



1544

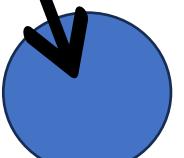
Cardano pubblica l'*Ars Magna*.





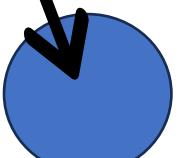
**1539**

Per tutto l'anno i due restano in corrispondenza.



**1544**

Cardano pubblica l'*Ars Magna*.



**12 febbraio 1547**

Ferrari sfida Tartaglia, a cui viene dato un mese per accettare.





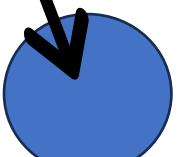
**1539**

Per tutto l'anno i due restano in corrispondenza.



**1544**

Cardano pubblica l'*Ars Magna*.



**12 febbraio 1547**

Ferrari sfida Tartaglia, a cui viene dato un mese per accettare.



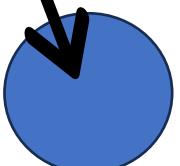
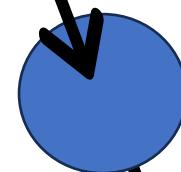
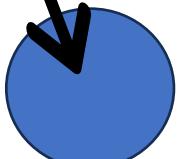
**Febbraio 1547**

Tartaglia accetta ma solo se parteciperà anche Cardano.



**Marzo 1547**

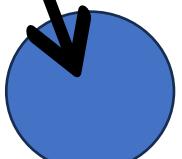
Ferrari manda una lettera in cui dice che ha saputo della soluzione di Del Ferro e che Tartaglia non ha diritti di priorità.





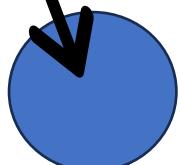
**Marzo 1547**

Ferrari manda una lettera in cui dice che ha saputo della soluzione di Del Ferro e che Tartaglia non ha diritti di priorità.



**27 aprile 1547**

Tartaglia insiste che debba partecipare Cardano. Propone 31 quesiti.





**Marzo 1547**

Ferrari manda una lettera in cui dice che ha saputo della soluzione di Del Ferro e che Tartaglia non ha diritti di priorità.



**27 aprile 1547**

Tartaglia insiste che debba partecipare Cardano. Propone 31 quesiti.



**Aprile 1547**

Ferrari risponde con una lettera ingiuriosa e propone anche lui 31 quesiti.





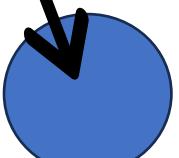
**Marzo 1547**

Ferrari manda una lettera in cui dice che ha saputo della soluzione di Del Ferro e che Tartaglia non ha diritti di priorità.



**27 aprile 1547**

Tartaglia insiste che debba partecipare Cardano. Propone 31 quesiti.



**Aprile 1547**

Ferrari risponde con una lettera ingiuriosa e propone anche lui 31 quesiti.



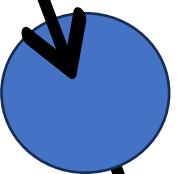
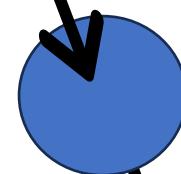
**23 giugno 1547**

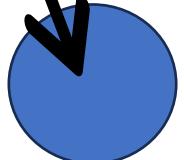
Tartaglia risolve quasi tutti i quesiti.



**10 agosto 1547**

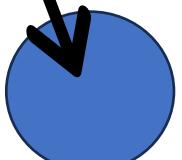
Ferrari lancia una nuova sfida.





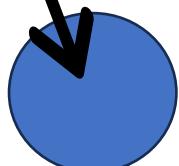
**10 agosto 1547**

Ferrari lancia una nuova sfida.



**Fine agosto 1547**

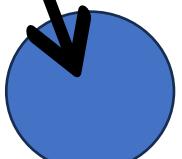
Tartaglia risolve tutti i problemi proposti e anche quelli vecchi.





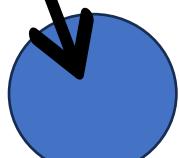
**10 agosto 1547**

Ferrari lancia una nuova sfida.



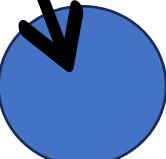
**Fine agosto 1547**

Tartaglia risolve tutti i problemi proposti e anche quelli vecchi.



**ottobre 1547**

Ferrari lancia una nuova sfida e finalmente risolve i 31 quesiti proposti da Tartaglia.





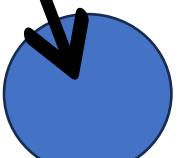
**10 agosto 1547**

Ferrari lancia una nuova sfida.



**Fine agosto 1547**

Tartaglia risolve tutti i problemi proposti e anche quelli vecchi.



**ottobre 1547**

Ferrari lancia una nuova sfida e finalmente risolve i 31 quesiti proposti da Tartaglia.



**Ottobre 1647**

Tartaglia, stufo, lancia una sfida pubblica, con o senza Cardano.



La disputa si svolse a Milano il 10 Agosto 1548.

Tartaglia perde la sfida e anche il lavoro, cadendo nell'anonimato.

Ferrari diventa famosissimo e ottiene numerose offerte di lavoro.

HIERONYMI CAR  
DANI, PRÆSTANTISSIMI MATHE-  
MATICI, PHILOSOPHI, AC MEDICI,  
ARTIS MAGNÆ,  
SIVE DE REGVLIS ALGEBRAICIS,  
Lib.unus. Qui & totius operis de Arithmetica, quod  
OPVS PERFECTVM  
in scriptis est in ordine Decimus.

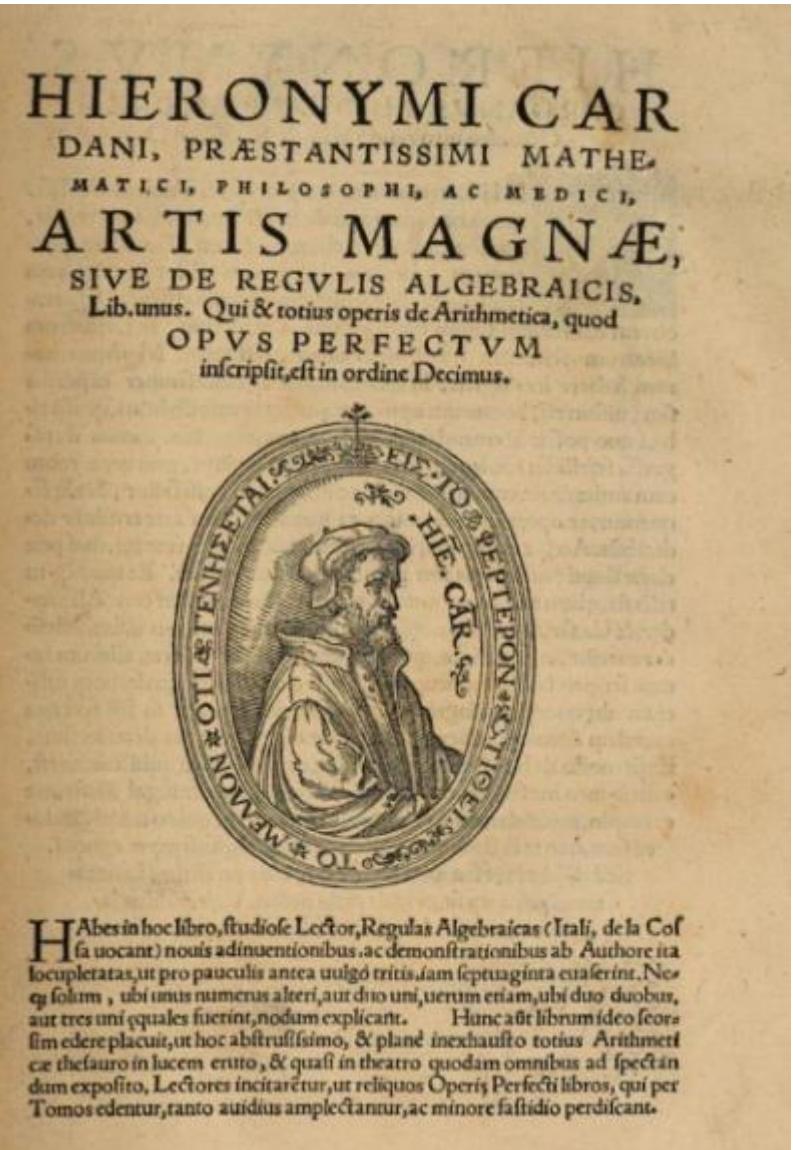


**H**abes in hoc libro, studiose Lector, Regulas Algebraicas (Itali, de la Cos-  
ta uocant) nouis adiuventionibus, ac demonstrationibus ab Authore ita  
locupletatas, ut pro pauculis ante uulgo tritis, iam septuaginta exaserint. Ne-  
c quod solum, ubi unus numerus alteri, aut duo uni, uerum etiam, ubi duo duobus,  
aut tres uni squales fuerint, nodum explicant. Hunc ait liberum ideo scori-  
fim edere placuit, ut hoc abstrusissimo, & planè inexhausto totius Arithmeti-  
ce thefauro in lucem eruto, & quasi in theatro quadam omnibus ad spectan-  
dum exposito, Lectores incitaretur, ut reliquos Operis Perfecti libros, qui per  
Tomos edentur, tanto audiūs amplectantur, ac minore fastidio perdiscant.

gerit, nihil nō intelligere posse se credat. Huius emulatiōe Nicolaus Tartalea Brixellensis, amicus noster, cū in certamē cū illius discipulo Antonio Maria Florido uenisset, capitulum idem, ne uinceretur, inuenit, qui mihi ipsum multis precibus exoratus tradidit. Deceptus

m	qualitatem	capitu
d	5 p: R: 45	
e	5 — 12 — 15	
i	7 3	
	25 45	
	175 — 135	
	40	

res 1 p: R<sub>2</sub> 5  
qd. 6 p: R<sub>2</sub> 20  
cub. 16 p: R<sub>2</sub> 320  
ati, & numeri, etiam



Scipione del Ferro, di Bologna, tempo fa ha risolto in modo estremamente elegante e ammirabile il caso del cubo e della cosa uguale a numero [cubica deppressa]. Tale arte, superando ogni umana sottigliezza e lo splendore di ogni ingegno mortale, testimonia il valore della sua mente, ed è cosa tanto meravigliosa che chi l'ha inventata può vantarsi di nessuno lo supererà. Suo emulo è il mio amico Nicolò Tartaglia, di Brescia, che in una disputa che sostenne con Antonio Maria del Fiore, discepolo di Scipione del Ferro, trovò anch'egli la soluzione e me la comunicò dietro mia supplica, senza dimostrazione, che ho riportato in diversi casi con l'aiuto del mio ex allievo Ludovico Ferrari. Parte di questo è merito suo, mentre il resto è opera mia.

Se considero il problema

$$x^3 + ax^2 + bx + c = 0$$

Facendo la sostituzione

$$x = y - \frac{a}{3}$$

Il termine di secondo grado scompare e lo studio come fosse una cubica *depressa*.

$$ax^3 + bx^2 + cx + d = 0$$

$$q = \frac{3ac - b^2}{3a^2}$$

$$p = \frac{9abc - 27a^2d - 2b^3}{27a^3}$$

$$s = \sqrt[3]{\frac{p}{2} + \sqrt{\frac{q^3}{27} + \frac{p^2}{4}}}$$

$$t = \sqrt[3]{\frac{p}{2} - \sqrt{\frac{q^3}{27} + \frac{p^2}{4}}}.$$

$$x_1 = s + t - \frac{b}{3a};$$

$$x_2 = -\frac{1}{2}(s+t) - \frac{b}{3a} + \frac{\sqrt{3}}{2}(s-t)i;$$

$$x_3 = -\frac{1}{2}(s+t) - \frac{b}{3a} - \frac{\sqrt{3}}{2}(s-t)i.$$

## I VARI «CASI» DI EQUAZIONI DI TERZO GRADO

$x^3 + ax = N$	$x^3 + ax^2 = +bx + N$
$x^3 = ax + N$	$x^3 + bx = +ax^2 + N$
$x^3 + N = ax$	$x^3 = +bx + ax^2 + N$
$x^3 = ax^2 + N$	$x^3 + N = +bx + ax^2$
$x^3 + ax^2 = N$	$x^3 + ax^2 + N = +bx$
$x^3 + N = ax^2$	$x^3 + bx + N = +ax^2$
$x^3 + ax^2 + bx = N$	

# I VARI «CASI» DI EQUAZIONI DI QUARTO GRADO

$x^4 = bx^2 + ax + N$	$x^4 + bx^2 + ax = N$
$x^4 = bx^2 + cx^3 + N$	$x^4 + cx^3 + bx^2 = N$
$x^4 = cx^3 + N$	$x^4 + bx^2 + N = ax$
$x^4 = ax + N$	$x^4 + bx^2 + N = cx^3$
$x^4 + cx^3 = bx^2 + N$	$x^4 + N = cx^3$
$x^4 + cx^3 = N$	$x^4 + N = ax$
$x^4 + ax = N$	$x^4 + N = ax + bx^2$
$x^4 + bx^2 = cx^3 + N$	$x^4 + cx^3 + N = bx^2$
$x^4 + bx^2 = ax + N$	$x^4 + ax + N = bx^2$
$x^4 + ax = +bx^2 + N$	$x^4 + N = +cx^3 + bx^2$

## Problema II capitolo XXXVII

«Dividere 10 in due parti il cui prodotto sia 40»

$$xy = 40$$

$$x + y = 10$$

## Problema II capitolo XXXVII

«Dividere 10 in due parti il cui prodotto sia 40»

$$xy = 40$$

$$x + y = 10$$

Le soluzioni sono

$$5 + \sqrt{-15}; 5 - \sqrt{-15}$$

Prendiamo il caso

$$\sqrt{-9}$$

Non può essere né 3, né -3.

Dunque per Cardano

«è di una terza natura nascosta» e «così progredisce la sottigliezza aritmetica, il cui fine è *tanto raffinato quanto inutile*»

$$x^3 = 15x + 4$$

$x = 4$  è una soluzione, infatti:

$$(4)^3 = 15 * 4 + 4$$

$$64 = 60 + 4$$

$$x^3 = 15x + 4$$

$$x = \sqrt[3]{2 - \sqrt{-121}} + \sqrt[3]{2 + \sqrt{-121}}$$



Originario di Bologna

Segue la disputa tra Tartaglia, Fiore, Cardano e Ferrari.

Decide di scrivere un'opera in 5 volumi intitolata *L'Algebra*.

Ne vengono pubblicati 3. Gli ultimi furono riscoperti all'inizio del XX secolo.

Rafael Bombelli  
(1526-1572)

# L'aritmetica con gli immaginari

$\sqrt{-1}$  è chiamata *più di meno*

$-\sqrt{-1}$  è chiamata *meno di meno*

$$(+)\times(+i) = +i$$

$$(-)\times(+i) = -i$$

$$(+)\times(-i) = -i$$

$$(-)\times(-i) = +i$$

$$\textcolor{red}{(+i) \times (+i) = -}$$

$$(+i) \times (-i) = +$$

$$(-i) \times (+i) = +$$

$$(-i) \times (-i) = -$$

$$i^2 = -1$$

## *L'Algebra* di Bombelli: libro secondo

$$x^3 = 15x + 4$$

La formula cardanica contiene la radice «*sofistica*»  $\sqrt{-121}$

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} = \sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i}$$

E' facile verificare che  $x = 4$  è una radice reale dell'equazione. Ma come ottenerla dalla formula?

Nel primo libro Bombelli si era posto il problema di «trovare il lato cubico di un *binomio*», ovvero di trasformare  $\sqrt[3]{a \pm \sqrt{-b}}$  nella forma  $u \pm \sqrt{-v}$  ( $a, b$  numeri positivi).

Bombelli osserva che allora  $u$  e  $v$  devono soddisfare le due condizioni  $\begin{cases} a = u^3 - 3uv \\ \sqrt[3]{a^2 + b} = u^2 + v \end{cases}$

Per trovare  $u, v$  propone il seguente metodo **«per pratica»:**

Quando  $a = 2$  e  $b = 121$ ,  $\sqrt[3]{a^2 + b} = \sqrt[3]{4 + 121} = 5$  e le due condizioni diventano  $\begin{cases} 2 = u^3 - 3uv \\ 5 = u^2 + v \end{cases}$

Così deve essere  $u^2$  minore di 5 e  $u^3$  maggiore di 2 e **«a tentoni»**  $u = 2$  e  $v = 1$ .

“E con questa regola – afferma Bombelli – benché non sia generale, ma più tosto pratica, sarà quasi impossibile, quando dette radici haveranno lato, non lo trovare”.

nel caso dell'equazione  $x^3 = 15x + 4$ ,

$$\sqrt[3]{2 + 11i} = 2 + i \text{ and } \sqrt[3]{2 - 11i} = 2 - i$$

$$x = \sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i} = 2 + i + 2 - i = 4$$

# Le notazioni algebriche di Bombelli

*vedere nella equazione de quella capito in un  
ad aggiughiare  $\sqrt[3]{\alpha}$   $\sqrt[3]{\beta}$  e  $\sqrt[3]{\gamma}$  piglia il te-  
s. et questo a causa del quadrato della metà  
che di questo pigliata fa radice, dirà  $\sqrt[3]{\alpha}$*

*ap  $\sqrt[3]{\alpha}$   $\sqrt[3]{\beta}$   $\sqrt[3]{\gamma}$ .*

*$\sqrt[3]{\alpha}$   $\sqrt[3]{\beta}$   $\sqrt[3]{\gamma}$   $\sqrt[3]{\alpha}$   $\sqrt[3]{\beta}$   $\sqrt[3]{\gamma}$*

$$\sqrt[3]{2 + \sqrt{0 - 121}} + \sqrt[3]{2 - \sqrt{0 - 121}}$$

cioè

$$\sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i}$$

Notazione esponenziale per le potenze  
dell'incognita

$$x^3 = 15x + 4$$

Le notazioni per le radici quadrate e  
cubiche

$$2 + \sqrt{0 - 121} \quad \text{cioè} \quad 2 + 11i$$

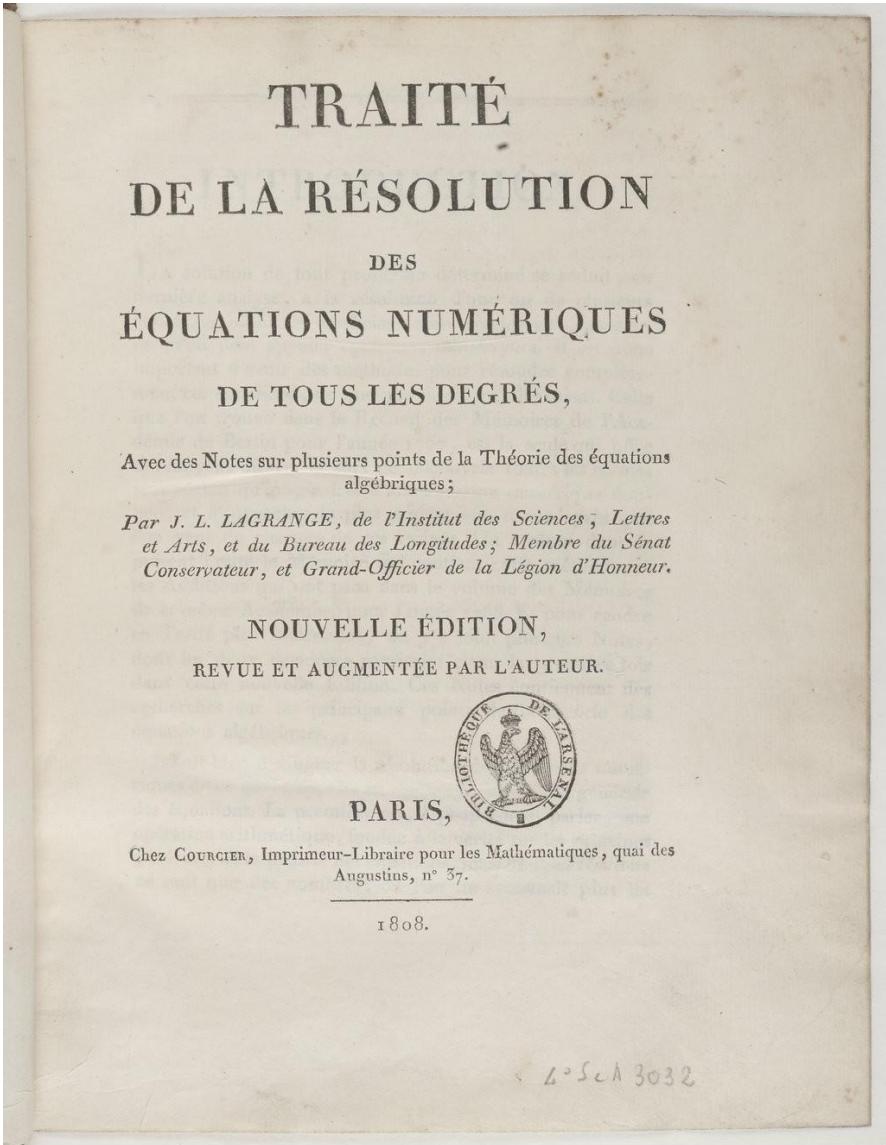


Dopo tante fatiche di molti geometri rimane solo una minima speranza di poter pervenire un giorno alla risoluzione generale delle equazioni algebriche ed appare sempre più verosimile che una tale risoluzione sia impossibile e contraddittoria. [...] per farla breve, si presuppone senza una motivazione sufficiente che la soluzione di un'equazione arbitraria si possa ridurre alla soluzione di equazioni pure. Non sarà forse difficile dimostrare rigorosamente tale impossibilità già per le equazioni di quinto grado, sulla qual cosa pro porrò con più particolari le mie argomentazioni in un altro luogo

Post tot tantorum geometrarum labores perexiguam spem superesse, ad resolutionem generalem aequationum algebraicarum unquam pervenienti, ita ut magis magisque verisimile fiat, talem resolutionem omnino esse impossibilem et contradictoriam. [...] Seu, missis verbis, sine ratione sufficienti supponitur, cuiusvis aequationis solutionem ad solutionem aequationum purarum reduci posse. Forsan non ita difficile foret, impossibilitatem iam pro quinto gradu omni rigore demonstrare, de qua re alio loco disquisitiones mea



Carl Gauss  
(1777-1855)



Source gallica.bnf.fr / Bibliothèque nationale de France



Giuseppe Luigi Lagrangia  
(1736-1813)

Nasce a Valentano (Lazio)

Si laurea nel 1788 a Modena in Filosofia e Medicina.

Nel 1797 diventa professore di Matematica a Modena.

Nel 1814 riaperta l'Università di Modena, ne divenne rettore, pur continuando ad insegnare matematica applicata, medicina e clinica medica.

Divenne presidente dell'Accademia dei XL.



Paolo Ruffini  
(1796-1822)

TEORIA GENERALE  
DELLA  
EQUAZIONI,  
*IN CUI SI DEMOSTRA IMPOSSIBILE*  
LA SOLUZIONE ALGEBRAICA DELLE  
EQUAZIONI GENERALI DI GRADO  
SUPERIORE AL QUARTO  
*D I*  
PAOLO RUFFINI.  
*PARTE PRIMA.*

BOLOGNA MDCCXCVIII.

NELLA STAMPERIA DI S. TOMMASO D' AQUINO,

Rielabora idee di Lagrange.

La dimostrazione è contestata

Ci ritorna più volte fino al 1813.

TEORIA GENERALE  
DELL'E  
EQUAZIONI,

IN CUI SI DEMOSTRA IMPOSSIBILE.  
LA SOLUZIONE ALGEBRAICA DELLE  
EQUAZIONI GENERALI DI GRADO  
SUPERIORE AL QUARTO

D I

PAOLO RUFFINI.

PARTE PRIMA.

BOLOGNA MDCCXCVIII.

NELLA STAMPERIA DI S. TOMMASO D'AQUINO,

DELLA IMMATERIALITÀ  
DELL'ANIMA,  
OPUSCOLO

DEL DOTTOR PAOLO RUFFINI

P. PROFESSORE DI MATEMATICA SUBLIME IN MODENA,  
MEMBRO DELLA LEGION D'ONORE, DELL'ISTITUTO  
NAZIONALE, DELL'ACCADEMIA DI RELIGIONE  
CATTOLICA, UNO DEI QUARANTA DELLA  
SOCIETÀ ITALIANA DELLE SCIENZE,  
EC.

Aggiugnesi la Confutazione dei Principii del Sistema  
Metafisico di Erasmo Darwin.

ALLA SANTITÀ DI NOSTRO SIGNORE

PIO SETTIMO  
FELICEMENTE REGNANTE.

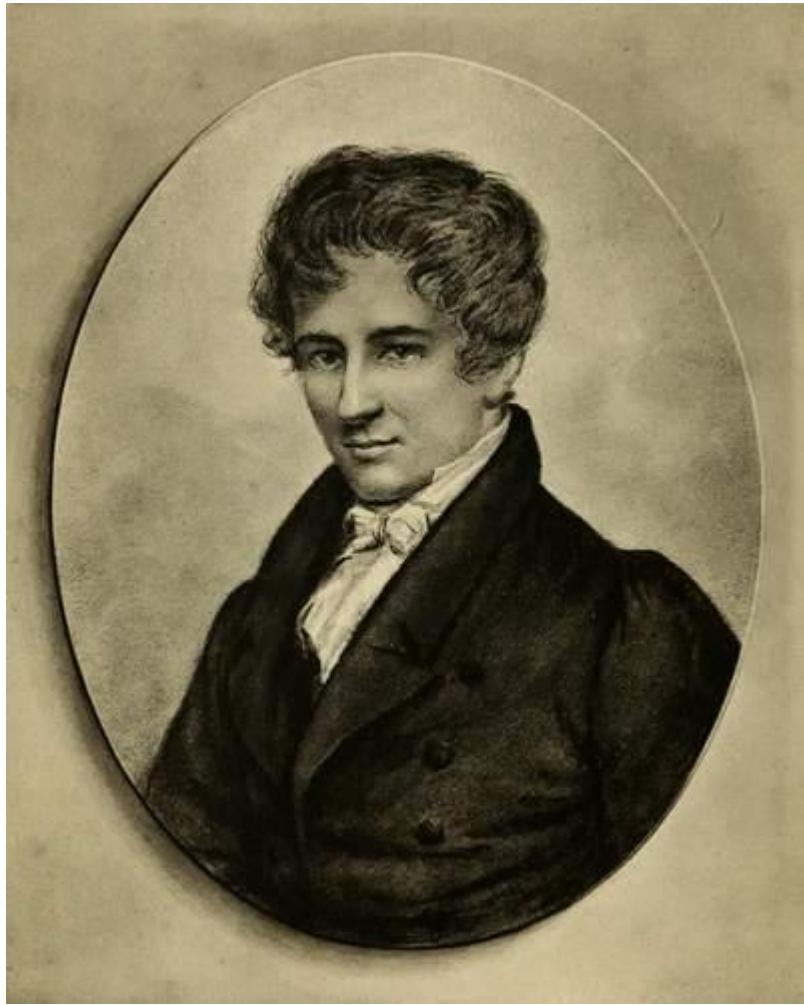
( IN MODENA )

Per gli Eredi di Bartolomeo Soliani.

MDCCCVI.



6535



Niels Abel  
(1802-1829)

Uno dei problemi più interessanti dell'algebra è quello della risoluzione algebrica delle equazioni. Quasi tutti i matematici di alto livello se ne sono occupati. Si giunse senza difficoltà all'espressione generale delle radici delle equazioni dei primi quattro gradi. [...] In tale situazione si sarebbe potuta ottenere la risoluzione [per gradi superiori al quarto] benché ciò non fosse in alcun modo sicuro; se però sfortunatamente la soluzione fosse impossibile, la si potrebbe cercare in eterno, senza trovarla. Per ottenere qualcosa di sicuro in questa materia occorre dunque seguire un'altra strada. Occorre riformulare il problema in modo che sia sempre possibile risolverlo, ciò che è sempre possibile fare per un qualunque problema. Invece di cercare una relazione di cui si ignora l'esistenza, occorre domandarsi se una tale relazione sia in effetti possibile.



Journal für die reine und angewandte Mathematik

## VII.

### DÉMONSTRATION DE L'IMPOSSIBILITÉ DE LA RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS GÉNÉRALES QUI PASSENT LE QUATRIÈME DEGRÉ.

*Journal für die reine und angewandte Mathematik*, herausgegeben von Crelle, Bd. 1, Berlin 1826.

On peut, comme on sait, résoudre les équations générales jusqu'au quatrième degré, mais les équations d'un degré plus élevé, seulement dans des cas particuliers, et, si je ne me trompe, on n'a pas encore répondu d'une manière satisfaisante à la question: "Est-il possible de résoudre en général les équations qui passent le quatrième degré?" Ce mémoire a pour but de répondre à cette question.

Résoudre algébriquement une équation ne veut dire autre chose, que d'exprimer ses racines par des fonctions algébriques des coefficients. Il faut donc considérer d'abord la forme générale des fonctions algébriques, et chercher ensuite s'il est possible de satisfaire à l'équation donnée, en mettant l'expression d'une fonction algébrique au lieu de l'inconnue.

#### § I.

*Sur la forme générale des fonctions algébriques.*

Soient  $x', x'', x''', \dots$  un nombre fini de quantités quelconques. On dit que  $v$  est une fonction *algébrique* de ces quantités, s'il est possible d'exprimer  $v$  en  $x', x'', x''', \dots$  à l'aide des opérations suivantes: 1) par l'addition; 2) par la multiplication, soit de quantités dépendant de  $x', x'', x''', \dots$ , soit de quantités qui n'en dépendent pas; 3) par la division; 4) par l'extraction de racines d'indices premiers. Parmi ces opé-



## VII.

### DÉMONSTRATION DE L'IMPOSSIBILITÉ DE LA RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS GÉNÉRALES QUI PASSENT LE QUATRIÈME DEGRÉ.

*Journal für die reine und angewandte Mathematik*, herausgegeben von Crelle, Bd. 1, Berlin 1826.

On peut, comme on sait, résoudre les équations générales jusqu'au quatrième degré, mais les équations d'un degré plus élevé, seulement dans des cas particuliers, et, si je ne me trompe, on n'a pas encore répondu d'une manière satisfaisante à la question: "Est-il possible de résoudre en général les équations qui passent le quatrième degré?" Ce mémoire a pour but de répondre à cette question.

Résoudre algébriquement une équation ne veut dire autre chose, que d'exprimer ses racines par des fonctions algébriques des coefficients. Il faut donc considérer d'abord la forme générale des fonctions algébriques, et chercher ensuite s'il est possible de satisfaire à l'équation donnée, en mettant l'expression d'une fonction algébrique au lieu de l'inconnue.

#### § I.

*Sur la forme générale des fonctions algébriques.*

Soient  $x'$ ,  $x''$ ,  $x''' \dots$  un nombre fini de quantités quelconques. On dit que  $v$  est une fonction *algébrique* de ces quantités, s'il est possible d'exprimer  $v$  en  $x'$ ,  $x''$ ,  $x''' \dots$  à l'aide des opérations suivantes: 1) par l'addition; 2) par la multiplication, soit de quantités dépendant de  $x'$ ,  $x''$ ,  $x''' \dots$ , soit de quantités qui n'en dépendent pas; 3) par la division; 4) par l'extraction de racines d'indices premiers. Parmi ces opé-



- Vita di Galois: 1811 - 1832
- Nasce a Bourg-la-Reine, nei pressi di Parigi
- Madre di una famiglia di giuristi, il padre è sindaco della città nel 1815

*Presa della Bastiglia: 1789 Battaglia di Waterloo: 1815*

## Évariste Galois



## École polytechnique

- Frequenta il Liceo Luis-le-Grand
- Inizia con un buon rendimento, ma le sue attenzioni vengono assorbite dalla politica studentesca e dalla Matematica
- A 17 anni tenta senza successo il concorso per l'ammissione all'École polytechnique
- Prende lezioni private di matematica.

- Nella primavera dello stesso anno invia due lavori all'Accademia delle Scienze; il referee è Cauchy
- Nel frattempo riesce a pubblicare il suo primo lavoro sugli annali di Matematica di Gergonne.
- Nel 1829, il padre di Galois si suicida a seguito di uno scandalo politico
- Ritenta il concorso del Politecnico, fallendolo, ma riesce ad accedere all'École Normale Supérieure

**ANALYSE ALGÉBRIQUE.**

*Démonstration d'un théorème sur les fractions continues périodiques ;*

Par M. Evariste GALOIS, élève au Collège de Louis-le-Grand.

---

On sait que si , par la méthode de Lagrange, on développe en fraction continue une des racines d'une équation du second degré, cette fraction continue sera périodique , et qu'il en sera encore de même de l'une des racines d'une équation de degré quelconque , si cette racine est racine d'un facteur rationnel du second degré du premier membre de la proposée, auquel cas cette équation aura , tout au moins , une autre racine qui sera également périodique. Dans l'un et dans l'autre cas, la fraction continue pourra d'ailleurs être immédiatement périodique ou ne l'être pas immédiatement , mais , lorsque cette dernière circonstance aura lieu, il y aura du moins une des transformées dont une des racines sera immédiatement périodique.

Or , lorsqu'une équation a deux racines périodiques , répondant à un même facteur rationnel du second degré , et que l'une d'elles est immédiatement périodique , il existe entre ces deux racines une relation assez singulière qui paraît n'avoir pas encore été remarquée , et qui peut être exprimée par le théorème suivant :

*THÉORÈME. Si une des racines d'une équation de degré quelconque est une fraction continue immédiatement périodique , cette équation aura nécessairement une autre racine également périodique*

Proprio oggi avrei dovuto presentare all'Accademia prima un rapporto sul lavoro del giovane Galois e poi una mia memoria sulla determinazione analitica delle radici primitive nella quale dimostro come sia possibile ridurre tale determinazione alla risoluzione di equazioni numeriche dotate solo di radici intere e positive. Sono tuttavia a casa, indisposto. Sono dispiaciuto di non poter partecipare alla sessione odierna e vorrei pregarla di iscrivermi a parlare per la prossima sessione sui due argomenti indicati. La prego di accettare i miei omaggi... A.-L. Cauchy

L'anno scorso, prima del 1 marzo, il Sig. Galois consegnò al Segretario dell'Istituto una memoria sulla risoluzione delle equazioni numeriche. Tale memoria avrebbe dovuto partecipare al Gran Premio di Matematica. Essa meritava il premio in quanto poté risolvere alcune difficoltà che Lagrange non era riuscito a superare. Il sig. Cauchy attribuiva sommi elogi all'autore per quanto seppe fare. E cosa è successo? La memoria è andata perduta ed il premio viene assegnato senza la partecipazione del giovane studioso.



Jean Baptiste Joseph  
Fourier

- All'inizio del 1830, Galois manda i suoi articoli a Fourier, per poter partecipare al Gran Premio di Matematica
- Fourier morirà prima di averli letti.
- Galois riesce a pubblicare tre lavori sul Bulletin des Sciences Mathématiques.



**fuciliere della  
Garde nationale**

- A 19 anni, con lo scoppio della Rivoluzione di Luglio (1830), Galois inizia ad impegnarsi politicamente
- Nel Dicembre del 1830, Galois viene espulso dalla Scuola, ed entra nella Guardia Nazionale
- Nel 1831 invia una terza versione del suo lavoro principale ad un premio di matematica
- L'articolo viene rigettato sulla base della poca chiarezza

Caro sig. Galois,

il vostro lavoro fu inviato al sig. Poisson per un parere. Egli lo ha restituito allegando un rapporto che qui cito:

“Abbiamo fatto ogni sforzo per capire le dimostrazioni del sig. Galois. I suoi argomenti non sono né abbastanza chiari né sufficientemente sviluppati per permetterci di giudicarne il rigore; non ci è stato nemmeno possibile farci un’idea sul lavoro.

L’autore afferma che le proposizioni contenute nel manoscritto sono parte di una teoria generale ricca di applicazioni. Spesso parti diverse di una teoria si chiariscono a vicenda e possono essere comprese più facilmente quando sono considerate insieme piuttosto che isolate una dall’altra. Per formarsi un’opinione bisogna quindi attendere che l’autore pubblichi un resoconto più completo di questo lavoro”.

Per questo motivo, vi restituiamo il manoscritto con la speranza che possiate trovare utili per il lavoro futuro le osservazioni del sig. Poisson.



**fuciliere della  
Garde nationale**

- Nel Maggio del 1831 propone un brindisi che viene interpretato come una minaccia a Luigi-Filippo: viene arrestato il giorno dopo
- Viene liberato a metà Giugno
- Durante i festeggiamenti del 14 luglio Galois veste l'uniforme della discolta Artiglieria della Guardia Nazionale ed è pesantemente armato; viene nuovamente arrestato
- Viene condannato a 6 mesi di prigione



***“Non ho tempo”***

- Durante l'epidemia di colera del 1832 viene trasferito in ospedale e dopo poco viene rilasciato sulla parola
- In ospedale, si innamora di Stéphanie; viene sfidato a duello dal suo fidanzato Pescheux d'Herbinville, esperto tiratore
- La notte prima del duello, in cui morirà, scrive una lettera all'amico Chavalier, nella quale spiega la sua teoria matematica

FRAN

(a)

Il y a quelques mots à compléter dans cette  
Note de l'A. P.

Car il n'a pas fini et il faut que l'équation soit  
finie, mais il n'a pas pu faire ce qu'il voulait faire.

transcription, j'espère, de ceux qui trouveront leur profit  
dans la lecture.

à effacement. E. Gallois le 29 Mai 1832.

ainsi  $F = \cup V$ , et l'on aura  
 $\phi V = \phi V^1 = \phi V^2 = \dots = \phi V^{n+1}$   
 La valeur de  $V$  pourra être déterminée également  
 2°. Considérons que la fonction  $F$  est dé-  
 terminable relativement, c'est à dire que l'on peut écrire  $F = \phi V$ ,  
 & on saura aussi  $\phi V = \phi V^1 = \phi V^2 = \dots = \phi V^{n+1}$   
 puisque l'équation de  $V$  a par la définition commun-  
 tale à  $V$  suffit à l'équation relative  $F = \phi V$ ,  
 c'est une quantité réduite. Donc la fonction  $F$   
 sera nécessairement variable par les substitutions  
 du groupe tout à done.

Alors si le groupe dont la double équation est  
 l'agent dans le théorème précédent proposé. Le  
 théorème est donc démontré.  
 Soit maintenant  $\phi V$  l'équation du groupe en question.  
 Soit  $\phi V$  l'équation que l'on a trouvée. Si le groupe est constitué  
 par les lettres  $a, b, c, d, \dots$  alors il peut y avoir  
 à considérer, moins seulement les substitutions de lettres  
 par lesquelles on passe d'une permutation à l'autre.  
 Mais l'on peut également arbitrairement faire faire  
 une permutation  $\phi$  à ces autres substitutions permutations  
 sans déranger pour toujours par les mêmes substitutions  
 de lettres. Le nouveau groupe ainsi formé parraîtra  
 comme le même proposé que le premier, puisque  
 dans le théorème précédent, il ne résulte que des  
 substitutions  $\phi$  de lettres que l'on fait faire dans l'é-  
 quation.

PROPOSITION II.

Théorème. Si l'on ajoute à une équation donnée d'un  
 système quelconque  $\phi V = \phi V^1 = \phi V^2 = \dots = \phi V^{n+1}$ , il  
 convient de faire alors l'analogie du groupe à l'équa-  
 tion ne rien pas changer, mais il se présente un  
 p. groupes appartenant à l'équation proposée respecti-  
 vement quelles sont les opérations châssées ou conservées  
 l'équation auxiliaire. 2°. ces groupes peuvent être la  
 partie remarquable, que l'on pourra de l'un à l'autre  
 en équation dans toutes les permutations de groupes une  
 même substitution de lettres.

1°. si après l'ajout de  $\phi V$ , l'équation en  $V$  n'est pas  
 plus que l'on peut faire évidemment, il est clair que  
 le groupe à l'équation ne rien pas changer. Il se présente  
 alors l'équation en  $V$  à démontrer en  
 se faisant de même opérations de la forme  $\phi$

$$\phi(V, t) \times \phi(V, t') \times \phi(V, t'') \times \dots$$

et  $t, t', t'' \dots$  sont les ~~différentes~~ valeurs de  $t$ .  
 Alors le groupe à l'équation proposée à démontrer  
 sera le groupe châssé d'un même nombre de  
 permutations, puisque à chaque valeur de  $V$  correspond  
 une permutation. Ces groupes sont respectivement l'ensemble  
 de l'équation proposée, quels que soient les opérations successives  
 sur  $t, t', t'', \dots$

## Approccio di Galois: “al contrario”

$$a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 = 0$$

Classicamente:  $a_n, a_{n-1}, \dots, a_1, a_0 \rightsquigarrow x^1, \dots, x^n$

Galois:  $x^1, \dots, x^n \rightsquigarrow a_n, a_{n-1}, \dots, a_1, a_0$

Questo approccio è  
ispirato al quello di altri  
matematici dell'epoca:

- Joseph-Louis Lagrange
- Paolo Ruffini
- Niels Henrik Abel

## Lagrange:

- Sviluppa un metodo per ottenere equazioni intermedie, poi dette “*risolventi di Lagrange*”, per risolvere equazioni.
- Nel farlo, utilizza il concetto di “*gruppo di isotropia*”, formato da tutte quelle “*permutazioni*” tra le radici di un polinomio che lo lasciano invariato.

$$I(f) = \{\sigma \text{ tali che } f(\sigma(x_1), \dots, \sigma(x_n)) = f(x_1, \dots, x_n)\}$$

## Galois:

- Il gruppo di isotropia, oggi noto come “*gruppo di Galois*”, diventa l’oggetto principale dello studio.

# Lagrange cerca un metodo unico per risolvere le equazioni di vari gradi

si accorge che è possibile scrivere i coefficienti di un polinomio in funzione delle sue radici, in modo particolare:

$$\begin{aligned}x^2 + \textcolor{red}{px} + \textcolor{blue}{q} &= (x - \alpha)(x - \beta) \\&= x^2 - (\alpha + \beta)x + \alpha\beta\end{aligned}$$

I coefficienti sono  
funzioni simmetriche  
delle radici

$$\textcolor{red}{p} = -(\alpha + \beta)$$

$$\textcolor{blue}{q} = \alpha\beta$$

## Esempio del metodo di Lagrange:

Cerchiamo le radici del polinomio:  $x^2 + px + q = (x - \alpha)(x - \beta)$

poniamo:

$$r_1 = \alpha + \beta \quad (= -p)$$
$$r_2 = \alpha - \beta$$

Mentre  $r_2$  non è fissato dalle *permutazioni* delle radici, lo è  $r_2^2$

$$\begin{aligned} r_2^2 &= (\alpha - \beta)^2 = \alpha^2 + \beta^2 - 2\alpha\beta \\ &= \alpha^2 + 2\alpha\beta + \beta^2 - 2\alpha\beta - 2\alpha\beta \\ &= (\alpha + \beta)^2 - 4\alpha\beta = p^2 - 4q = \Delta \end{aligned}$$

Otteniamo quindi le radici dal seguente sistema:

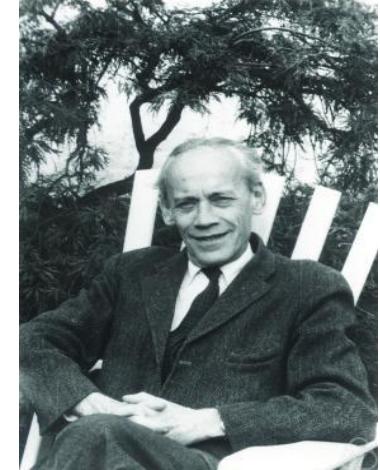
$$\begin{cases} \alpha + \beta = -p \\ \alpha - \beta = \sqrt{\Delta} \end{cases}$$

$$\rightsquigarrow \begin{cases} 2\alpha = -p + \sqrt{\Delta} \\ 2\beta = -p \pm \sqrt{\Delta} \end{cases} \rightsquigarrow x_{1,2} = \frac{-p \pm \sqrt{\Delta}}{2}$$

Questo approccio si estende al grado 3° e al 4°, ma non al 5°

# Teoria di Galois

- Riordinata da Joseph Liouville, 14 anni dopo la morte di Galois
- Sviluppata in forma moderna da Dedekind, Kronecker e Artin, alla fine del 1800
- I polinomi sono messi in relazione con **campi**, che a loro volta sono messi in relazione con **gruppi**



# Teoria di Galois

## Teorema

*Un polinomio è risolubile per radicali se, e solo se, il suo gruppo di Galois è risolubile*

Un problema di equazioni e numeri viene riformulato in un problema di studio di proprietà di particolari strutture: i gruppi

# Cosa sono i campi?

Esempi:

$\mathbb{Q}$   $\mathbb{R}$   $\mathbb{C}$

Non è un campo:

$\mathbb{Z}$

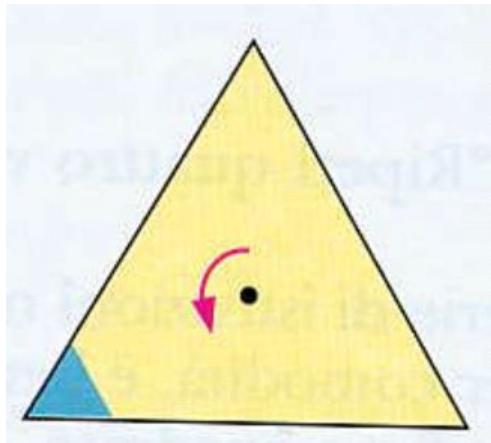
- Chi sono i numeri complessi? Sono i numeri reali con l’“aggiunta” dell’elemento  $i$ , dove  $i$  è radice di  $X^2 + 1$
- Nello stesso modo, possiamo costruire altri campi aggiungendo radici di polinomi

# Cos'è un gruppo?

$S(n)$

$(G, \cdot, e_G)$

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \dots\}$

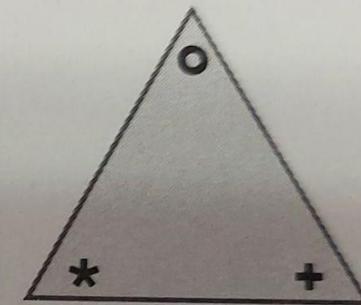
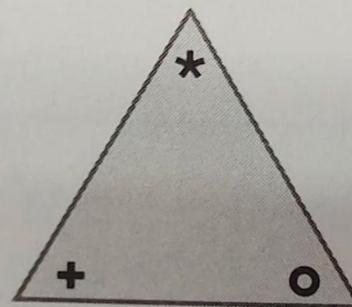
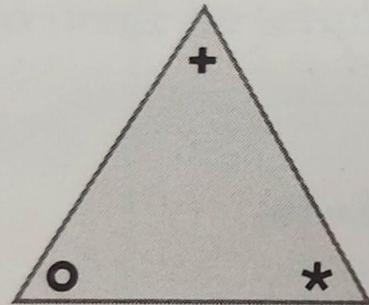


$\mathbb{R} \setminus \{0\}$

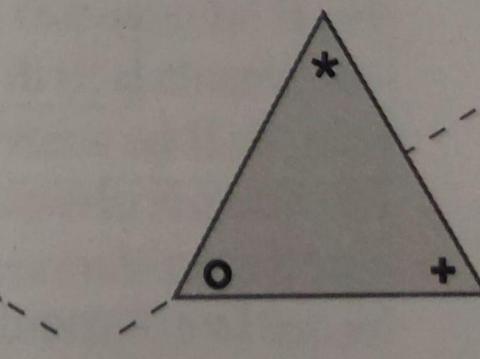
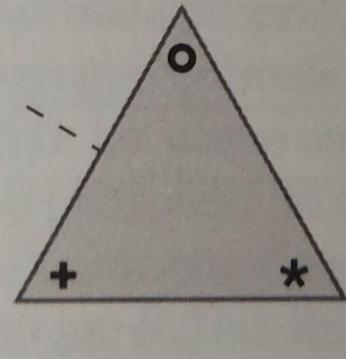
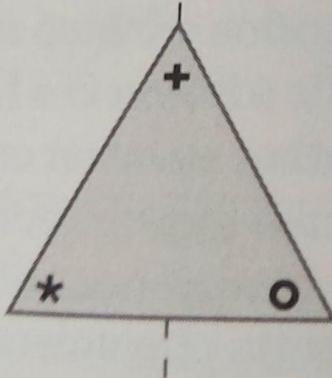


# Gruppo diedrale $D_3$

Tre rotazioni

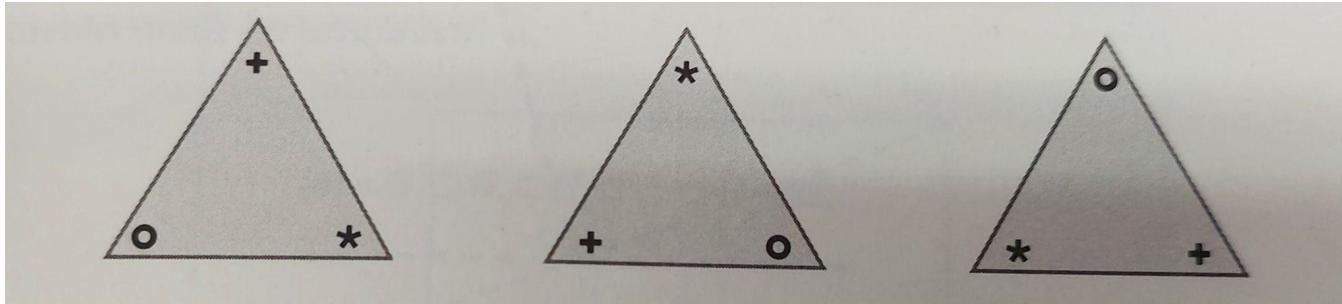


Tre riflessioni

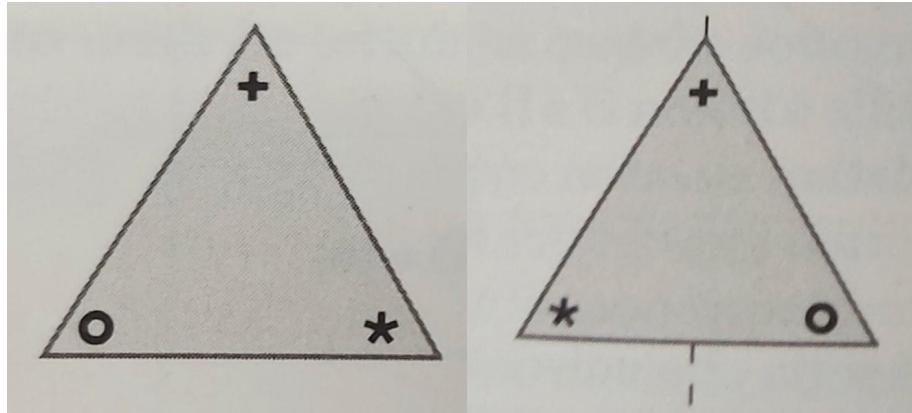


# Sottogruppi di $D_3$

Il sottogruppo delle rotazioni  $C_3$



I sottogruppi delle riflessioni,  $C_2$



# Congruenze modulari: $\mathbb{Z}_5$

- Prendiamo l'insieme dei numeri interi

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \dots\}$$

- Consideriamo la divisione col resto per 5 di ciascuno dei numeri interi
- Li possiamo raggruppare in 5 sottoinsiemi, in base al loro resto:

$$\bar{0} = \{0, \pm 5, \pm 10, \pm 15, \dots\}$$

$$\bar{1} = \{1, \pm 6, \pm 11, \pm 16, \dots\}$$

$$\bar{2} = \{2, \pm 7, \pm 12, \pm 17, \dots\}$$

$$\bar{3} = \{3, \pm 8, \pm 13, \pm 18, \dots\}$$

$$\bar{4} = \{4, \pm 9, \pm 14, \pm 19, \dots\}$$

# Congruenze modulari: $\mathbb{Z}_5$

$$\bar{0} = \{0, \pm 5, \pm 10, \pm 15, \dots\}$$

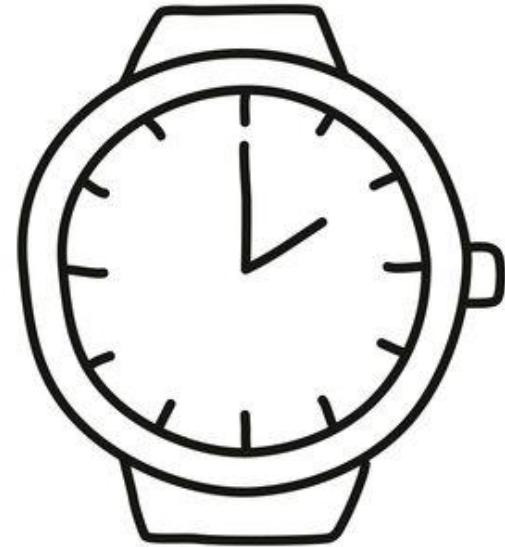
$$\bar{1} = \{1, \pm 6, \pm 11, \pm 16, \dots\}$$

$$\bar{2} = \{2, \pm 7, \pm 12, \pm 17, \dots\}$$

$$\bar{3} = \{3, \pm 8, \pm 13, \pm 18, \dots\}$$

$$\bar{4} = \{4, \pm 9, \pm 14, \pm 19, \dots\}$$

- Legge di composizione:  $\bar{a} + \bar{b} = \overline{\text{resto modulo 5 di } a + b}$
- Nel concreto:  $\bar{3} + \bar{4} = \bar{2}$

$Z_{12} \cong$ 

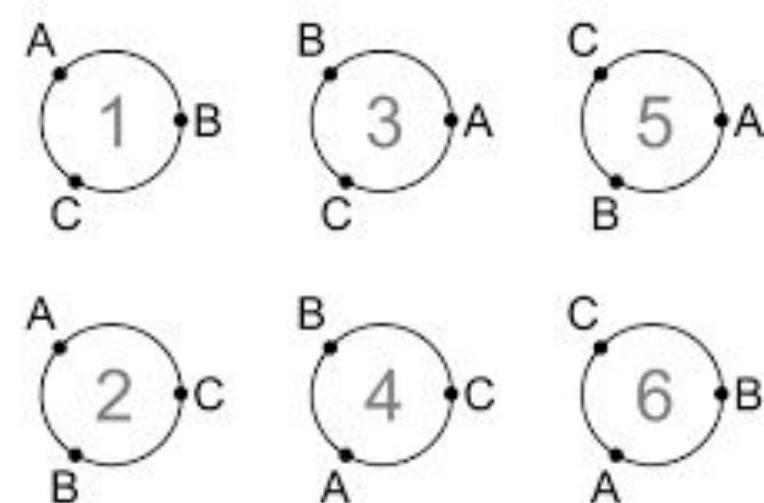
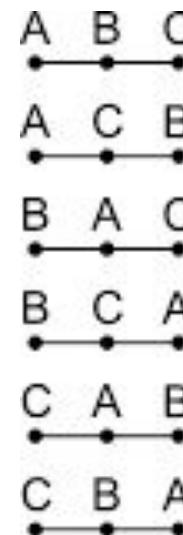
- $6:00 + 1 \text{ ora} = 7:00$
- $11:00 + 3 \text{ ore} = 2:00$
- $10:00 + 14 \text{ ore} = 10:00 + 2 \text{ ore} = 0:00$

Se stessimo usando un orologio digitale, chi sarebbe la n in  $Z_n$ ?

# Le permutazioni: $S(n)$

- Gli elementi di questo gruppo sono “tutti i possibili modi di riordinare n oggetti messi in fila”
- Se pensiamo a  $S(3)$  come tutti i possibili modi di riordinare 1 2 3, abbiamo che i suoi elementi sono:  
1 2 3, 1 3 2, 2 1 3, 2 3 1, 3 1 2, 3 2 1

- **Curiosità:** Ogni gruppo può essere visto come un sottogruppo di  $S(n)$ , per un certo n



# Le permutazioni: $S(n)$

Come vengono scritte le permutazioni dai matematici? In  $S(3)$ :  
Identità, (12), (13), (23), (123), (132)

- Identità = tutto resta fermo
- (12) = L'1 è scambiato con il 2
- (1 2 3) = L'1 va in 2, il 2 va in 3, il 3 va in 1

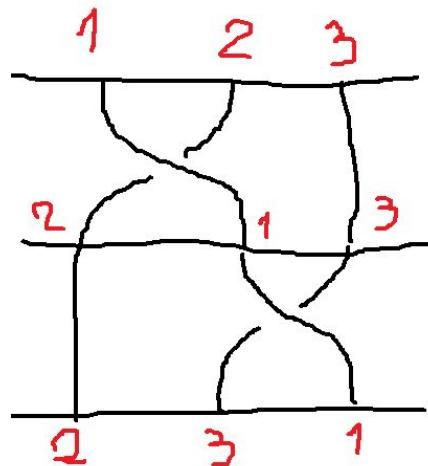
## Esempio concreto:

10 amici decidono di sedersi intorno ad un tavolo.  
Ogni possibile modo in cui gli amici possono sedersi corrisponde ad un elemento di  $S(9)$

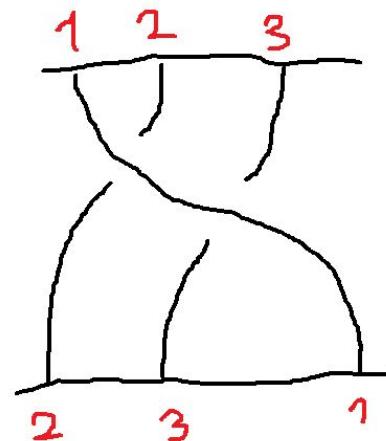
# Composizione di permutazioni

$$\{1, 2, 3\} \xrightarrow{(12)} \{1, 2, 3\} \xrightarrow{(23)} \{1, 2, 3\} =$$

$$= \{1, 2, 3\} \xrightarrow{(132)} \{1, 2, 3\}$$



=



# Gruppi risolvibili

$\{e\} = G_1 \subset G_2 \subset G_3 \subset \dots \subset G_n = G$

con certe proprietà

S(2), S(3), S(4) : Risolvibili

Da S(5) in poi: No

# La teoria di Galois nell'attualità

## Crittografia

- I sistemi crittografici digitali usano proprietà dei campi finiti, detti “Campi di Galois” in onore del matematico francese
- Questi non sono altro che gli  $\mathbb{Z}_p$  visti precedentemente, con la moltiplicazione definita in modo simile all’addizione
- Questi sistemi (ad esempio RSA) sfruttano le proprietà dei campi finiti e la difficoltà nel fattorizzare i prodotti di numeri primi molto grandi

# La teoria di Galois nell'attualità

Classificazione dei gruppi finiti semplici (finita nel 2004)

- gruppo ciclico di ordine primo, cioè un gruppo finito semplice commutativo
- gruppo alterno almeno di quinto grado, cioè il gruppo delle permutazioni pari di un insieme di almeno cinque elementi
- gruppo lineare classico (proiettivo lineare speciale, simplettico, ortogonale o gruppo unitario su un campo finito)
- gruppo di tipo Lie. Includerebbe per esempio il gruppo di Tits.
- gruppi sporadici, che non rientrano in nessuna famiglia particolare e sono 26

Il più grande gruppo sporadico, detto il “gruppo mostro”, ha cardinalità  
808017424794512875886459904961710757005754368000000000  
 $\approx 8 \cdot 10^{53}$

# Ringraziamenti e fonti

Sono stati consultati i seguenti libri

- Cardano, il trionfo delle equazioni di terzo grado
- Galois, l'invenzione della teoria dei gruppi

di Fernando Corbalán

e diapositive e dispense dei corsi universitari di

- Alessandra Fiocca
- Riccardo Rosso
- Fabio Stumbo

L'argomento della presentazione è stato ispirato dal video

- How Imaginary Numbers Were Invented  
di Derek Muller