Società Italiana di Storia delle Matematiche - APS

Dalla storia della matematica all'aula

L'Aritmetica modulare: una proposta laboratoriale ispirata al Liber Abbaci di Fibonacci.

Silvia Cerasaro
Dipartimento di Matematica
Università Tor Vergata- Roma

Università di Roma
Tor Vergata

Cos’è l’aritmetica modulare?

Ramo della matematica che sfrutta il concetto di **Congruenza lineare**

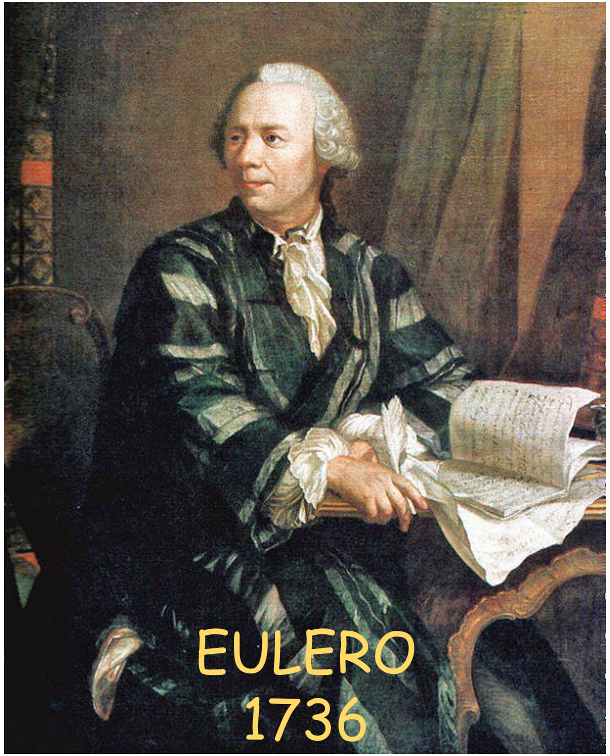
$$a \equiv b \bmod n \Leftrightarrow a = q \times n + b, \text{ con } a,b,n \text{ interi}$$

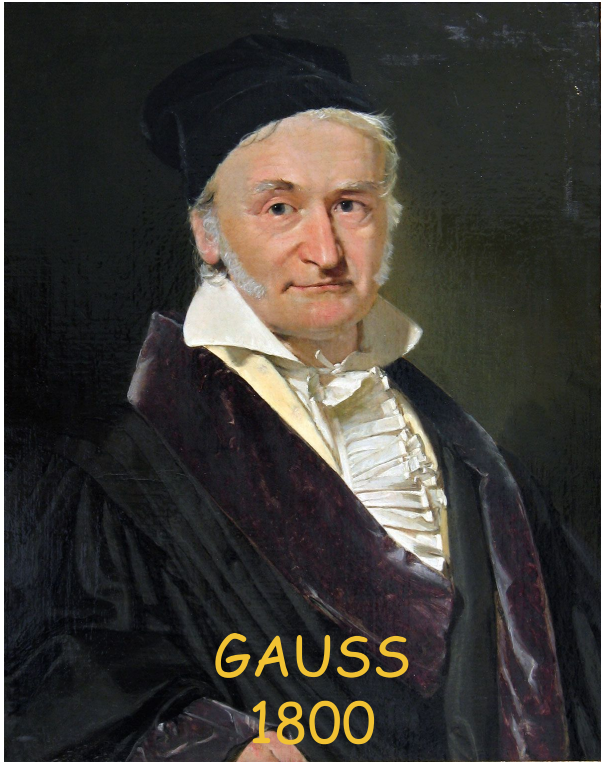
Nell’aritmetica dell’orologio:

21 ≡ 9 mod 12 se 21 = 1x12+9

16 ≡ 4 mod 12 se 16 = 1x12+4

Matematici che trattarono l’aritmetica modulare

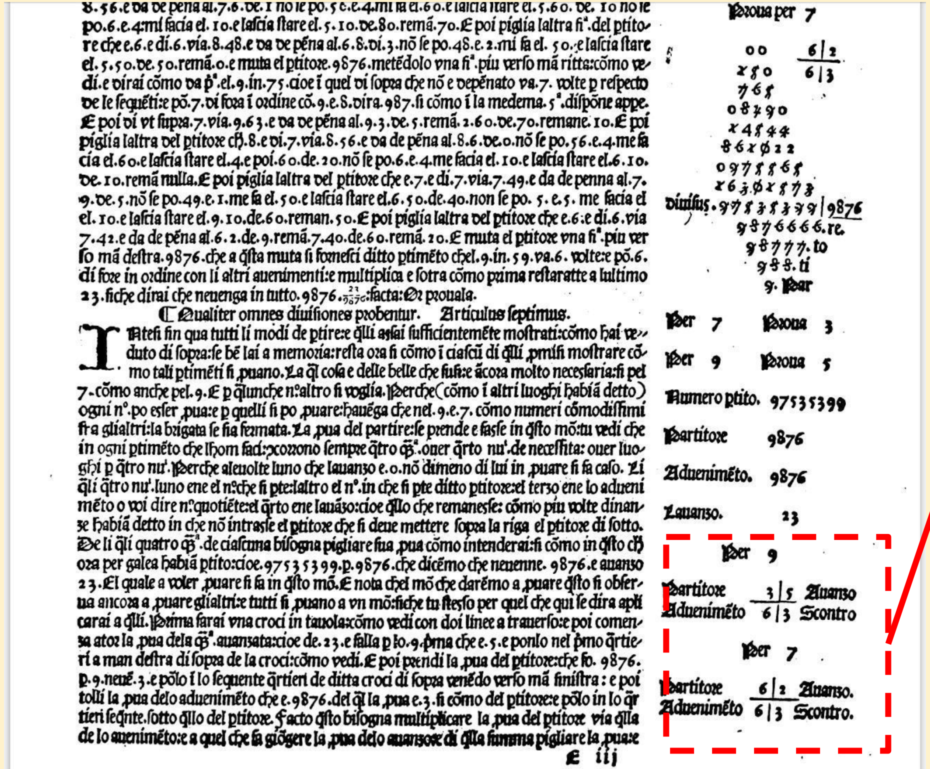


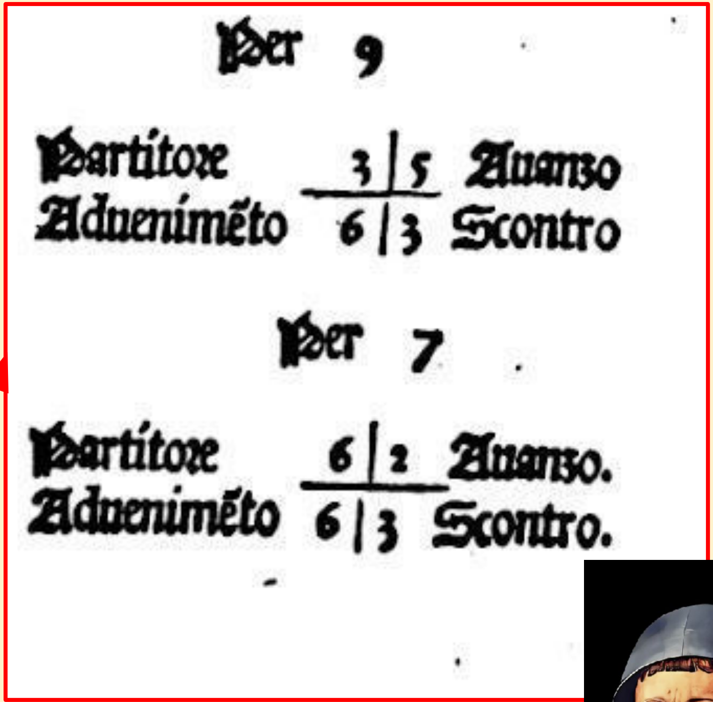


$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^{\phi(n)} \equiv 1 \bmod n$$

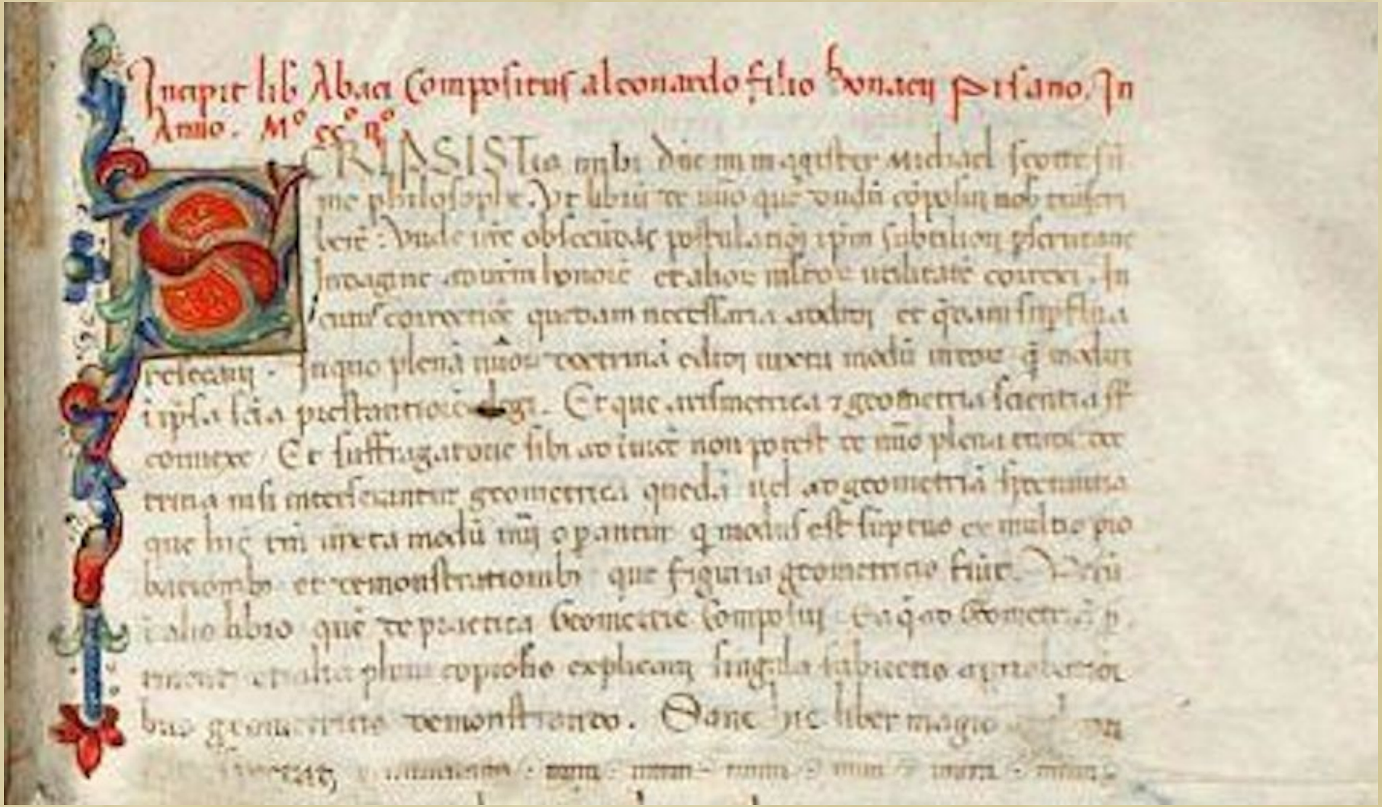
L’aritmetica modulare prima dei “grandi matematici”





Summa de arithmetica, geometria, proportioni et proportionalita , Pacioli, (1494)

Liber Abbaci di Leonardo Pisano Fibonacci



A. C. Leonardus pisanus ...
Est Abbatie florentine

B 73

SCRIPSISTIS mihi domine mi magister Michael Scotte summe
me philosophe. Ut librum de numero quem dudum composui vobis transcri
berem: Unde vestre obsecundans postulationi ipsum subtiliori perscrutans
indagine ad vestrum honorem et aliorum multorum utilitatem correxi. In
cuius correctione quedam necessaria addidi et quedam superflua
resecavi. In quo plenam numerorum doctrinam edidi iuxta modum Indorum quem modum
in ipsa scientia prestantiorem elegi. Et quia arismetrica et geometria scientia sunt
connexe. Et suffragatorie sibi ad invicem non potest de numero plena tradi doc
trina nisi interserantur geometrica quedam vel ad geometriam spectantia
que hic tamen iuxta modum numeri operantur quem modus est sumptus ex multis pro
bationibus et demonstrationibus que figuris geometricis fiunt. Verum
in alio libro quem de practica geometrie composui. Ea que ad geometriam per
tinent et alia plura copiosius explicavi singula subiectis approbationi
bus geometricis demonstrando. Sane hic liber magis ... ad ...
... theoricam ...

... quam ad practicam. Unde qui per eum huius scientie practicam bene scire voluerit oportet eos continuo usu et exer
citio diuturno in eius practicis perstudere quod scientia per practicam versa in habitum memoria et intellectus adeo concordent
cum manibus et figuris quod quasi uno impulsu et anhelitu in uno et eodem instanti circa idem per omnia naturaliter
consonent et tunc cum fuerit discipulus habitudinem consecutus gradatim poterit ad perfectionem huius facile perve
nire. Et ut facilior pateret doctrina huius librum per XV distinxi capitula ut quicquid de his lector voluerit
possit levius invenire. Porro si in hoc opere reperitur insufficientia vel defectus illud emendationi vestre subicio.

Cum genitor meus a patria publicus scriba in duana bugee pro pisanis mercatoribus ad eam
confluentibus constitutus preesset me in pueritia mea ad se venire faciens inspecta utilitate
et commoditate futura ibi me studio abbaci per aliquot dies stare voluit et doceri.
Ubi ex mirabili magisterio in arte per novem figuras Indorum introductus scientia artis in tantum mihi pre ceteris
placuit et intellexi ad illam quod quicquid studebatur ex ea apud egyptum syriam greciam siciliam et provin
ciam cum suis variis modis ad que loca negotiationis tam postea peragravi per multum studium et disputa
tionis didici conflictum. Sed hoc totum etiam et algorismum atque artem pictagore quasi errorem computavi respec
tu modi Indorum. Quare amplectens strictius ipsum modum Indorum et attentius studens in eo ex proprio sensu
quedam addens et quedam etiam ex subtilitatibus euclidis geometrice artis apponens summam huius libri quam in
telligibilius potui in XV capitulis distinctam componere laboravi fere omnia que inserui certa probatione ostendens. ut
extra perfecto pre ceteris modo hanc scientiam appetentes instruantur et gens latina de cetero sicut hactenus absque illa
minime inveniatur. Si quid forte minus aut plus iusto vel necessario intermisi mihi deprecor indulgeatur
cum nemo sit qui vitio careat et in omnibus undique sit circumspectus. Explicit prologus. Incipiunt capitula.

De cognitione novem figurarum Yndorum et qualiter cum eis omnis numerus scribatur et qui numeri et qualiter re
tineri debeant in manibus et de introductionibus abbaci. 1
De multiplicatione integrorum numerorum. 2
De additione ipsorum ad invicem. 3

Leonardi Pisani Algorismi, Geometria
Inter Codices designatur num. 44.

[illegible]

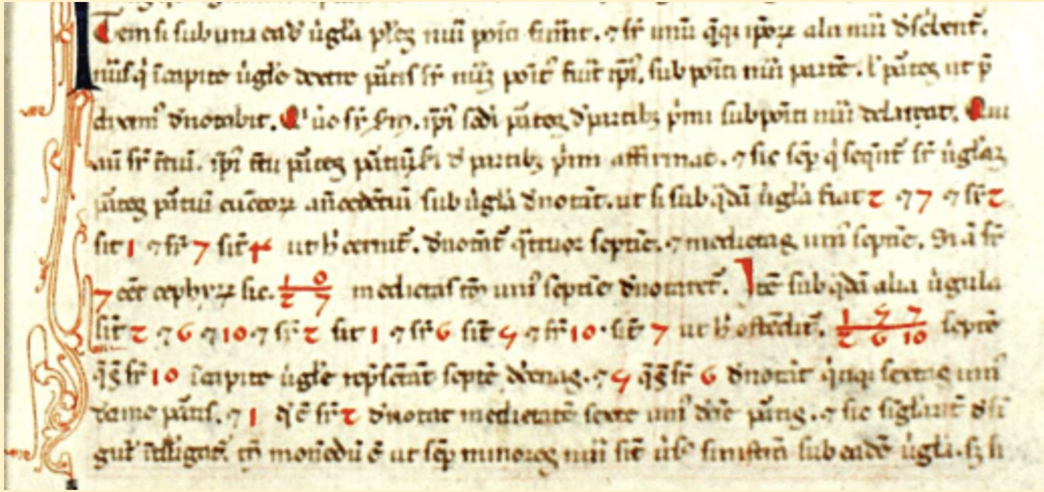
[illegible]

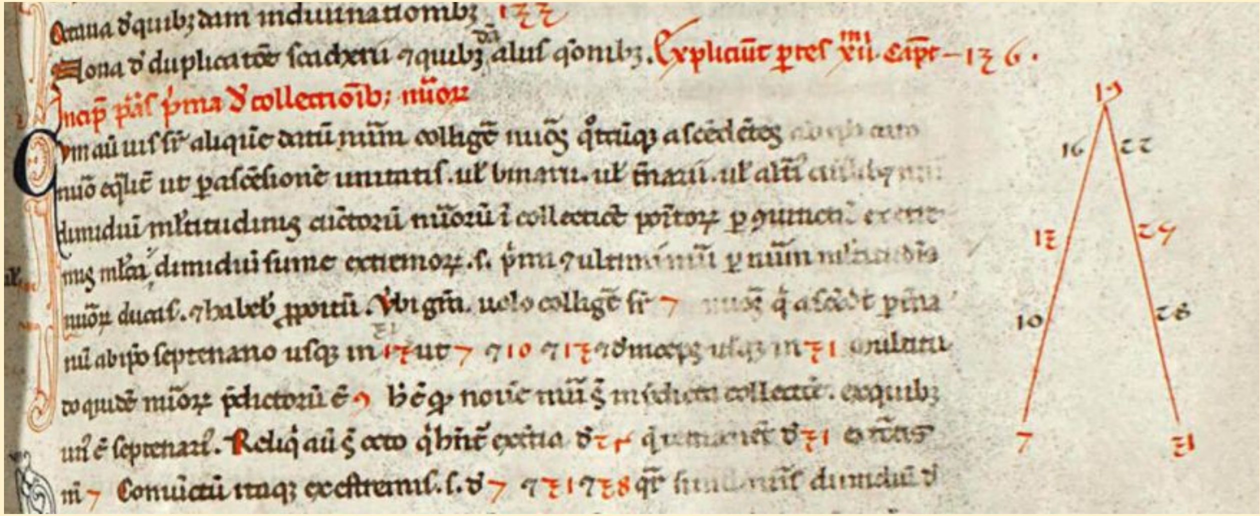
2 et	2	fiunt	4
2	3		5
2	4		6
2	5		7
2	6		8
2	7		9
2	8		10
2	9		11
2	10		12
Ianua ternarii.			
3 et	3	fiunt	6
3	4		7
3	5		8
3	6		9
3	7		10
3	8		11
3	9		12
3	10		13
Ianua quaternarii			
4 et	4	fiunt	8
4	5		9
4	6		10
4	7		11
4	8		12
4	9		13
4	10		14
Ianua quinarii			
5 et	5	fiunt	10
5	6		11
5	7		12
5	8		13
5	9		14
5	10		15
Ianua senarii			
6 et	6	fiunt	12
6	7		13
6	8		14
6	9		15
6	10		16

7	7		14
7	8		15
7	9		16
7	10		17
8 et	8	fiunt	16
8	9		17
8	10		18
9 et	9	fiunt	18
9	10		19
10 et	10	fiunt	20
20 et	20	fiunt	40
20	30		50
20	40		60
20	50		70
20	60		80
20	70		90
20	80		100
20	90		110
30 et	30	fiunt	60
30	40		70
30	50		80
30	60		90
30	70		100
30	80		110
30	90		120
40 et	40	fiunt	80
40	50		90
40	60		100
40	70		110
40	80		120
40	90		130
50 et	50	fiunt	100
50	60		110
50	70		120
50	80		130
50	90		140

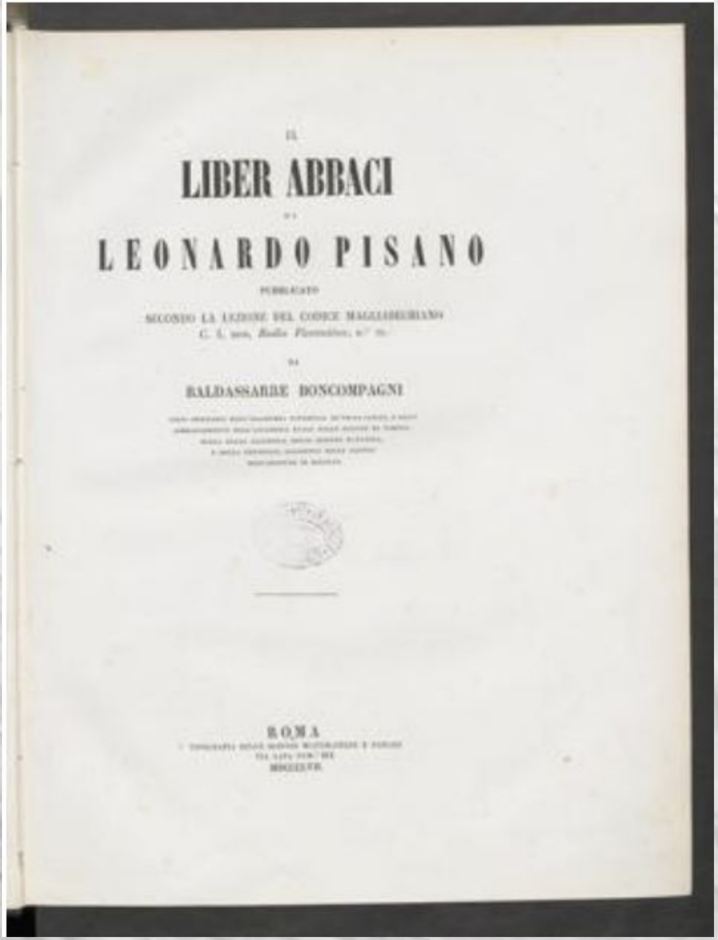
60	70		130
60	80		140
60	90		150
70 et	70	fiunt	140
70	80		150
70	90		160
80 et	80	fiunt	160
80	90		170
et		fiunt	
90	90		180
Expliciunt iunctiones			
Incipiunt multiplicationes			
De binario			
2 vices	2	fiunt	4
2	3		6
2	4		8
2	5		10
2	6		12
2	7		14
2	8		16
2	9		18
2	10		20
De ternario			
3 vices	3	fiunt	9
3	4		12
3	5		15
3	6		18
3	7		21
3	8		24
3	9		27
3	10		30
De quaternario			
4 vices	4	fiunt	16
4	5		20
4	6		24
4	7		28
4	8		32
4	9		36
4	10		40

5 vices	5	fiunt	25
5	6		30
5	7		35
5	8		40
5	9		45
5	10		50
De senario			
6 vices	6	fiunt	36
6	7		42
6	8		48
6	9		54
6	10		60
De septenario			
7 vices	7	fiunt	49
7	8		56
7	9		63
7	10		70
De octonario			
8 vices	8	fiunt	64
8	9		72
8	10		80
De nouenario			
9 vices	9	fiunt	81
9	10		90
De decenario			
10 vices	10	fiunt	100
10	20		200
Expliciunt multiplicationes			

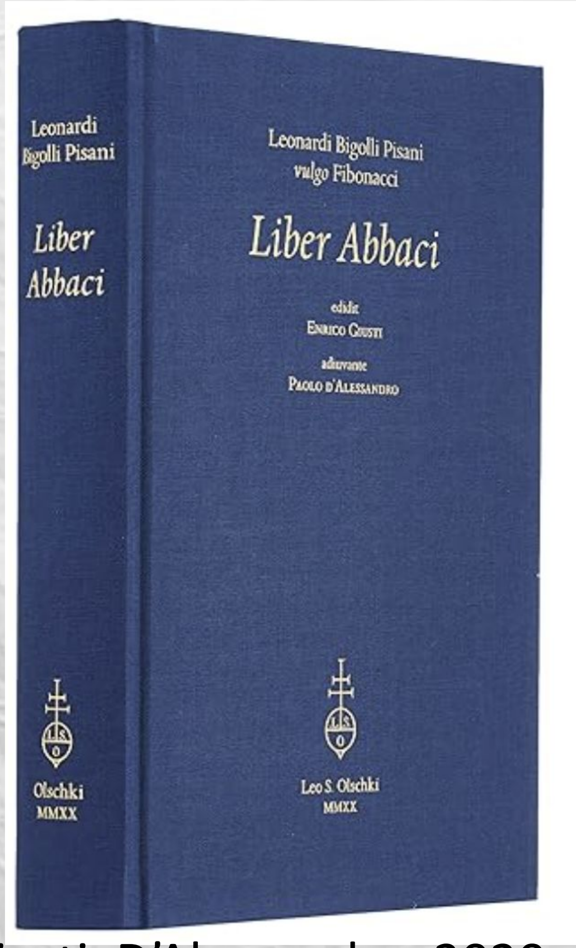




Non è presente alcun formalismo simbolico: compaiono solo numeri interi, frazioni, frazioni multiple, tabelle e diagrammi.



Boncompagni, 1857



Giusti, D'Alessandro, 2020

Traduzione in italiano presente sul sito di PROGETTO FIBONACCI

Fare matematica con un testo storico

Dalle Indicazioni Nazionali…

Lo studente avrà acquisito una visione storico-critica dei rapporti tra le tematiche principali del pensiero matematico e il contesto filosofico, scientifico e tecnologico

…acquisizione della consapevolezza del valore culturale delle discipline e della loro evoluzione storica ed epistemologica.

Attività proposte nelle classi del biennio

Uso diretto della fonte storica in classe

Guillemette, Radford, 2022

Con l’utilizzo del Liber Abbaci come fonte storica si tiene in considerazione l’**aspetto culturale** ed **epistemologico** di cui la storia stessa è portatrice; si riflette sulla lingua usata, sull’evoluzione del linguaggio specifico mentre si costruisce la conoscenza matematica [Barbin, 2022].

La storia delle matematiche facilita l’***apprendimento discorsivo***, ovvero la capacità delle persone di apportare cambiamenti storico-sociali mediante la costruzione della conoscenza [Sfard, 2015].

La fonte storica e l’uso di altri artefatti aumentano la motivazione e l’interesse all’apprendimento [Nataraj & Thomas, 2009].

Dal Liber Abbaci…

II.9

Modo uideamus si hec multiplicatio recta est: iungantur figure de superiori 98, scilicet 9 cum 8, et dematur 9, remanebunt 8. Iterum illud idem fiat de inferioribus 98, remanebunt similiter 8; et multiplicentur 8 per 8, erunt 64, de quibus extrahantur omnes nouene que sunt in eisdem 64, remanebit pro pensa 1, uel aliter: iungantur figure que sunt in predictis 64, scilicet 6 cum 4, erunt 10, de quibus demantur 9, remanebit similiter 1, postea colligantur figure, que sunt in summa multiplicationis, scilicet 9 et 6 et 0 et 4 tamen non est necesse ut figura nouenarii colligatur in aliqua persimili probatione, cum nouenarius semper erit, ut extrahi precipiatur unde colligantur 6 et 0 et 4, erunt 10, de quibus demantur 9, remanebit 1 pro pensa, sicuti remanere oportebat.

L’aritmetica modulare nel Liber Abbaci

- Usata per il controllo della correttezza di un conto (prova del nove, del sette e del tredici)
- Usata nella risoluzione di problemi sulle *Divinazioni*, nei quali Leonardo Pisano fa uso di concetti matematici elevati.

XII.8.1

Incipit pars 8ª decimi capituli de quibusdam diuinationibus.

Cvm autem quis numerum aliquem posuerit in corde suo, et uoluerit, ut illum inuenias: precipe, ut ponat dimidium ipsius numeri supra ipsum numerum; et si aliqua rupta medietas concurrerit, precipe ut faciat inde integrum. Cuius totius numeri medietatem ponat iterum supra ipsum numerum: et si aliqua medietas concurrerit, iterum in integrum restituat. Deinde interroga eum, si ex summa, quam habet, potest tibi dare

Obiettivi Specifici dell’apprendimento

- Le classi di resto modulo un intero n;
- Le operazioni con le classi di resto modulo un intero n;
- l’algoritmo di Euclide per il calcolo del MCD;
- l’identità di Bezout;
- il teorema cinese del resto.

Attività 1: La prova del nove

(II.9 ; G: II.22) Adesso vediamo se $\frac{(PdA)}{}$ questa moltiplicazione è corretta: si sommino le figure del 98 superiore, cioè 9 con 8, e si tolga il 9, rimarrà 8. Si faccia di nuovo lo stesso col 98 inferiore, rimarrà ugualmente 8 ; e si moltiplichi 8 per 8, farà 64, dal quale si tolgano tutti i gruppi di 9 che sono nello stesso 64, rimarrà come resto 1, oppure in altro modo: si sommino le figure che sono nel 64 detto sopra, cioè 6 con 4, farà 10, dal quale si tolga 9, rimarrà similmente 1, dopo si addizionino le figure che sono in cima alla moltiplicazione, cioè 9 e 6 e 0 e 4, tuttavia non è necessario che la figura delle 9 unità sia aggiunta in qualche simile prova, poiché il nove sempre è previsto che venga tolto o estratto prima si cominci sempre con il togliere o l'estrarre le 9 unità, dunque si sommino 6 e 0 e 4, farà 10, dal quale si tolga 9, rimarrà 1 per il resto, come doveva rimanere.

(II.12 ; G: II.28) E se la moltiplicazione è corretta si può sapere in questo modo: si divida 37 per 9, cioè si addizionino le figure del 37, cioè il 3 con il 7, sarà 10, dal quale leviamo 9, rimarrà 1, che si conservi ; ugualmente si addizionino le figure del 49, cioè il 4 con il 9, sarà 13, dal quale togliamo 9, rimarrà 4, che si moltiplica con l'1 conservato, sarà 4, che si conserva per la prova, e si sommino le figure che sono in cima alla moltiplicazione, cioè 1 e 8 e 1 e 3, sarà 13, dal quale si tolga 9, rimarrà 4, come occorre che rimanga come resto.

- *Tradurre dal linguaggio naturale al linguaggio matematico*
- *Riflettere sull'esempio "significativo" utilizzato per dimostrazione;*

Vediamo il primo esempio riportato da Fibonacci…

$$98 \times 98 = 9604$$

$$(9 \times 10 + 8) \times (9 \times 10 + 8) =$$

$$\cancel{(9 \times 10)}^2 + 2 \times (9 \cancel{\times 10 \times} 8) + 8^2$$

…si tolgano tutti i gruppi di 9…non è necessario che la figura delle 9 unità sia aggiunta in qualche simile prova, poiché il nove sempre è previsto che venga tolto o estratto prima si cominci sempre con il togliere o l'estrarre le 9 unità…

$64 \equiv 1 \bmod 9$

Il prodotto è :
$9604=9000+600+0+4=$

$$(9\times1000+0)+(9\times66+6)+(9\times0+0)+(9\times0+4)$$

Quindi, $9604=0+6+0+4=10\equiv 1 \bmod 9$

Perché la prova del nove funziona?

$$a = 9 \times q + r \; con \; 0 \leq r < 9$$

Esempi di esercizi

A quale classe appartiene il 335?

$335 = 9 \times 37 + 2$ quindi $335 \equiv 2 \bmod 9$

oppure

$335 = 300+30+5=(9x33+3)+(9x3+3)+(9x0+5)$

Quindi, $3+3+5=11\equiv 2 \bmod 9$

Questo giustifica perché prendere la somma delle cifre

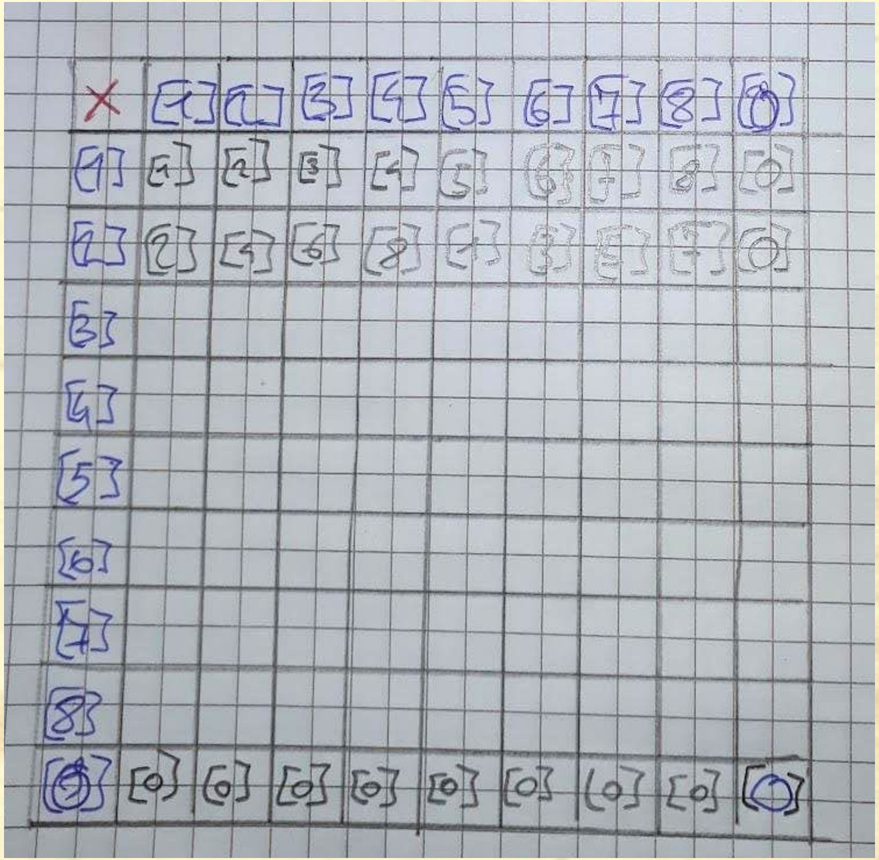
Considerare i numeri partendo dal resto della divisione per 9 e “catalogarli”, ottenendo le **classi di resto**

CLASSE 1	CLASSE 2	CLASSE 3	CLASSE 4	CLASSE 5	CLASSE 6	CLASSE 7	CLASSE 8	CLASSE 0
1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	10	77	18
19	10	20	22	23	24	25	20	27
28	29	30	31	38	33	34	35	38
37	38	39	40	41	42	43	44	45
40	47	48	49	50	51	52	53	54
55	56	57	58	59	66	61	62	63
64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81
82	83	84	85	80	87	88	89	90

Si costruiscono le tavole della somma e del prodotto.

Si individuano gli elementi neutri per le due operazioni.

Si discute l'esistenza di opposto e inverso.



Sarà possibile dedurre le seguenti regole:

Se $a = n \times q_1 + r_1$ e $b = n \times q_2 + r_2$, allora $a + b = n \times q_3 + (r_1 + r_2)$

o **se $a \equiv r_1 \bmod n$ e $b \equiv r_2 \bmod n$, allora $a + b \equiv r_1 + r_2 \bmod n$**

Se $a = n \times q_1 + r_1$ e $b = n \times q_2 + r_2$, allora $a \times b = n \times q_3 + (r_1 \times r_2)$

o **se $a \equiv r_1 \bmod n$ e $b \equiv r_2 \bmod n$, allora $a \times b \equiv r_1 \times r_2 \bmod n$**

Si procede a realizzare le tavole su un foglio di calcolo.

La deduzione dell'inverso per la moltiplicazione sarà facilitata dalla scrittura attraverso una pluralità di tabelle in Z_n.

```
=SE($A4+J$1<9;$A4+J$1;$A4+J$1-9)
```

A	B	C	D	E	F	G	H	I	J	K
+	1	2	3	4	5	6	7	8	0	
1	2	3	4	5	6	7	8	0	1	
2	3	4	5	6	7	8	0	1	2	
3	4	5	6	7	8	0	1	2	3	
4	5	6	7	8	0	1	2	3	4	
5	6	7	8	0	1	2	3	4	5	
6	7	8	0	1	2	3	4	5	6	
7	8	0	1	2	3	4	5	6	7	
8	0	1	2	3	4	5	6	7	8	
0	1	2	3	4	5	6	7	8	0	

Z_9

=SE($M6*T$1<9;$M6*T$1;$M6*T$1-(int($M6*T$1/9)*9))

M	N	O	P	Q	R	S	T	U	V
x	1	2	3	4	5	6	7	8	0
1	1	2	3	4	5	6	7	8	0
2	2	4	6	8	1	3	5	7	0
3	3	6	0	3	6	0	3	6	0
4	4	8	3	7	2	6	1	5	0
5	5	1	6	2	7	3	8	4	0
6	6	3	0	6	3	0	6	3	0
7	7	5	3	1	8	6	4	2	0
8	8	7	6	5	4	3	2	1	0
0	0	0	0	0	0	0	0	0	0

Tavola moltiplicativa per Z_7

x	1	2	3	4	5	6	0
1	1	2	3	4	5	6	0
2	2	4	6	1	3	5	0
3	3	6	2	5	1	4	0
4	4	1	5	2	6	3	0
5	5	3	1	6	4	2	0
6	6	5	4	3	2	1	0
0	0	0	0	0	0	0	0

Tavola moltiplicativa per Z_{13}

x	1	2	3	4	5	6	7	8	9	10	11	12	0
1	1	2	3	4	5	6	7	8	9	10	11	12	0
2	2	4	6	8	10	12	1	3	5	7	9	11	0
3	3	6	9	12	2	5	8	11	1	4	7	10	0
4	4	8	12	3	7	11	2	6	10	1	5	9	0
5	5	10	2	7	12	4	9	1	6	11	3	8	0
6	6	12	5	11	4	10	3	9	2	8	1	7	0
7	7	1	8	2	9	3	10	4	11	5	12	6	0
8	8	3	11	6	1	9	4	12	7	2	10	5	0
9	9	5	1	10	6	2	11	7	3	12	8	4	0
10	10	7	4	1	11	8	5	2	12	9	6	3	0
11	11	9	7	5	3	1	12	10	8	6	4	2	0
12	12	11	10	9	8	7	6	5	4	3	2	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0

Tavola moltiplicativa per Z_{10}

x	1	2	3	4	5	6	7	8	9	0
1	1	2	3	4	5	6	7	8	9	0
2	2	4	6	8	0	2	4	6	8	0
3	3	6	9	2	5	8	1	4	7	0
4	4	8	2	6	0	4	8	2	6	0
5	5	0	5	0	5	0	5	0	5	0
6	6	2	8	4	0	6	2	8	4	0
7	7	4	1	8	5	2	9	6	3	0
8	8	6	4	2	0	8	6	4	2	0
9	9	8	7	6	5	4	3	2	1	0
0	0	0	0	0	0	0	0	0	0	0

…in alternativa al metodo euristico…

Identità di Bezout

Ad esempio, l'inversa della classe 5 mod 7.

Con l'algoritmo euclideo:

$7 = 5 \times 1 + 2$

$5 = 2 \times 2 + 1$

$2 = 1 \times 2 + 0$

$$1 = 7 \times (-2) + 5 \times 3$$

L'inversa della classe 5 mod 7 è 3. Infatti, $5 \times 3 = 15 \equiv 1 \bmod 7$

Funziona sempre la prova del nove?

58 x 65 = 3770

4	8
2	8

58 x 65 = 7370

4	8
2	8

Condizione necessaria ma NON sufficiente…

Cristoforo Clavio (1583)

tradotta in volgare da Lorenzo Castellano nel 1586.

Mirabile proprietà del 9.

La proua del 9. è fallace, e perche è fallace.

La proua del 7. è fallace, ma non tanto quãto quella del 9. & perche.

Certezza, che l'operatione sia bẽ fatta sarà se tutte due le proue per 9. & per 7. riescano.


ARITMETICA
PRATTICA
Composta dal molto R. P.
CHRISTOFORO CLAVIO
BAMBERGENSE
Della Compagnia di Giesù,
Et tradotta dal Latino in Italiano dal Sig.
LORENZO CASTELLANO
Patritio Romano.
Reuista dal medesimo P. CLAVIO
con alcune aggiunte.
Domus Romanae S. Mariae Magdalenae
IN VENETIA, MDCLXXVIII.
Presso Steffano Curti.
CON LICENZA DE' SVPERIORI.

Pietro Antonio Cataldi (1602)

INITIVM SAPIENTIAE EST TIMOR DOMINI.

PRIMA PARTE
DELLA PRATICA
ARITMETICA,
OVERO ELEMENTI PRATICI DELLI NVMERI ARITMETICI,
Doue si mostrano le operationi semplici d'essi numeri Aritmetici, che sono Sommare, Sottrare, Moltiplicare, & Partire;
Et questo con li suoi veri principij, diffinitioni, regole, & essempij, Modo nuouo, reale, facile, & vtilissimo;
Data hora in luce da PERITO ANNOTIO à commune beneficio, essendo non solo necessaria alli principianti delle Scienze Mathematiche, & da loro dependenti, ma anco ad ogni sorte d'Artefici, & altre persone di qual si vogli qualità.

IN BOLOGNA,
Presso gli Heredi di Giouanni Rossi. MDCII.
Con licenza de' Superiori.

Non voglio restar di dire che li pratici Aritmetici sogliono fare la prova di ciascuno delli quattro elementi, cioè del Sommare, Sottrarre, Moltiplicare & partire in un modo che chiamiamo prova del 7, overo del 9 in questo modo. Partono li numeri, che si hanno da adoperare a far la prova della operatione, che vogliono per 7, overo per 9, & dell'avvenimento non tengono conto alcuno, ma si bene all'avanzo, quale avanzo, overo zero, cioè o quando niente avanzasse, lo chiamano prova di quel numero, che haveranno partito & esse prove poi le adoperano nel modo, che conviene a volere fare la prova dell'operatione che essi hanno.

(*) Qualche professore riguarda come inutili le riprove, o verificazioni nei calcoli, sostenendo che il miglior modo di preservarli dagli errori è quello di raddoppiare di attenzione e di diligenza. Ma noi, per lunga esperienza, crediamo al contrario che la più grande attenzione, e la più provata abilità, non bastano ad assicurare l' esattezza di un calcolo, quando anche si eseguisse ripetutamente, perchè nel ripetere il calcolo si ripetono non di raro anche gli errori commessi. Per la qual cosa, lodevole, e da adottarsi sempre che si può, è il sistema di pervenire per diverse vie allo stesso risultamento di calcolo; e le ripruove, che invertono per lo più l' andamento delle operazioni primitive, non che essere utili, sono spesso necessarie. S' intende bene che il calcolatore debba usarne con giudizio, e sarebbe strano se in un lungo calcolo non si procedesse innanzi senza far prima le ripruove di tutte le operazioni intermedie. L' attenzione prolungata si stanca, e le ripruove la soccorrono di tratto in tratto, assicurando il già fatto, e dando lena a riprendere come da capo il lavoro.


C08557

ELEMENTI

DI

ARITMETICA

DI

F. AMANTE.

SESTA EDIZIONE.

Amante, F. (1852), p. 20

Attività 2:
su alcune divinazioni

(XII.8.4; *G: XII.1191*) Divida il numero cercato per 3, e per 5, e per 7, e sempre chiedi quanto rimase di ciascuna divisione. Tu invero serba 70 da ciascuna unità che sarà avanzata dalla divisione per 3, e per ciascuna unità che sarà avanzata dalla divisione per 5 trattieni 21, e per ciascuna unità che sarà avanzata dalla divisione per sette ritieni 15. E ogni volta che il totale avrà superato 105, togli via di lì 105, e ciò che ti sarà rimasto sarà il numero separato. Per esempio: sia posto che dalla divisione per tre resti 2; per i quali trattieni due volte settanta, cioè 140, da cui togli 105, ti resterà 35. E dalla divisione per 5 resta 3, da cui trattieni tre volte 21, cioè 63, sommalo con il predetto 35, farà 98. E dalla divisione per 7 resta 4, per questo serberai quattro volte 15, cioè 60, sommalo al 98 predetto, farà 158, da cui togli 105, ti resterà 53, che era il numero cercato. Da questo metodo procede davvero una migliore decriptazione, naturalmente se qualcuno avrà conosciuto questo metodo insieme a te, e qualcuno gli avrà detto privatamente [un numero], allora quel tuo compagno, non interrogato, divida tacitamente il numero a lui detto per 3, e per 5, e per 7 per il metodo detto prima, e quanto sarà rimasto da quella divisione te lo dica in ordine, e così potrai sapere il numero che gli fu detto in privato

Dal linguaggio naturale a quello matematico..

Sia x il numero pensato. Si divida x rispettivamente per 3, 5 e 7.

Sia r_3 il resto della divisione per 3;

Sia r_5 il resto della divisione per 5;

Sia r_7 il resto della divisione per 7.

Allora $\boxed{x = (70r_3 + 21r_5 + 15r_7) - n105}$ fino a quando $x \leq 105$

Perché vale la formula usata da Fibonacci?

$$\boxed{x = (70r_3 + 21r_5 + 15r_7)}$$

$70 \equiv 0 \; mod \; (5, 7)$ e $70 \equiv 1 \; mod \; 3$

$21 \equiv 0 \; mod \; (3, 7)$ e $21 \equiv 1 \; mod \; 5$

$15 \equiv 0 \; mod(3, 5)$ e $15 \equiv 1 \; mod \; 7$

Inoltre poiché

$21r_5$ e $15r_7 \equiv 0 \; mod \; 3$, $x \equiv r_3 \; mod \; 3$

$70r_3$ e $15r_7 \equiv 0 \; mod \; 5$, $x \equiv r_5 \; mod \; 5$

$70r_3$ e $21r_5 \equiv 0 \; mod \; 7$, $x \equiv r_7 \; mod \; 7$

(XII.8.4; *G: XII.1191*) Divida il numero cercato per 3, e per 5, e per 7, e sempre chiedi quanto rimase di ciascuna divisione. Tu invero serba 70 da ciascuna unità che sarà avanzata dalla divisione per 3, e per ciascuna unità che sarà avanzata dalla divisione per 5 trattieni 21, e per ciascuna unità che sarà avanzata dalla divisione per sette ritieni 15. E ogni volta che il totale avrà superato 105, togli via di lì 105, e ciò che ti sarà rimasto sarà il numero separato. Per esempio: sia posto che dalla divisione per tre resti 2; per i quali trattieni due volte settanta, cioè 140, da cui togli 105, ti resterà 35. E dalla divisione per 5 resta 3, da cui trattieni tre volte 21, cioè 63, sommalo con il predetto 35, farà 98. E dalla divisione per 7 resta 4, per questo serberai quattro volte 15, cioè 60, sommalo al 98 predetto, farà 158, da cui togli 105, ti resterà 53, che era il numero cercato. Da questo metodo procede davvero una migliore decriptazione, naturalmente se qualcuno avrà conosciuto questo metodo insieme a te, e qualcuno gli avrà detto privatamente [un numero], allora quel tuo compagno, non interrogato, divida tacitamente il numero a lui detto per 3, e per 5, e per 7 per il metodo detto prima, e quanto sarà rimasto da quella divisione te lo dica in ordine, e così potrai sapere il numero che gli fu detto in privato

Leonardo usa il Teorema Cinese del Resto…

$$\begin{cases} x \equiv 1 \; mod \; 3 \\ x \equiv 2 \; mod \; 5 \\ x \equiv 3 \; mod \; 7 \end{cases}$$

Poiché il MCD(3,5)=MCD(3,7)=MCD(5,7)=1, esiste una unica soluzione del sistema modulo($3 \times 5 \times 7$) = mod 105. Questo giustifica la scelta del 105 da parte di Fibonacci.

La soluzione è data da:

$\boxed{x = \frac{N}{n_1}x_1 + \frac{N}{n_2}x_2 + \frac{N}{n_3}x_3}$ con $N = n_1 \times n_2 \times n_3$ e x_1, x_2, x_3 soluzioni di

$$\begin{cases} \frac{N}{n_1}x_1 \equiv r_3 \, mod \, 3 \\ \frac{N}{n_2}x_2 \equiv r_5 \, mod \, 5 \\ \frac{N}{n_3}x_3 \equiv r_7 \, mod \, 7 \end{cases}$$

cioè, poiché $n_1 = 3$, $n_2 = 5$, $n_3 = 7$, si ha:

$$\begin{cases} 35\,x_1 \equiv 1\ mod\ 3 \\ 21\,x_2 \equiv 2\ mod\ 5 \\ 15\,x_3 \equiv 3\ mod\ 7 \end{cases}$$

Poiché
$35 \equiv 2$ mod 3
$21 \equiv 1$ mod 5
$15 \equiv 1$ mod 7, allora si ha:

$$\begin{cases} 2\,x_1 \equiv 1\ mod\ 3 \\ x_2 \equiv 2\ mod\ 5 \\ x_3 \equiv 3\ mod\ 7 \end{cases}$$

Poiché la classe inversa di 2 mod 3 è 2, si ha

$$\begin{cases} x_1 = 2 \\ x_2 = 2 \\ x_3 = 3 \end{cases}$$

Quindi

$x = 35 \times 2 + 21 \times 2 + 15 \times 3 = 157 \equiv 52 \, mod \, 105$

Perché Fibonacci scrive $x = 70r_3 + 21r_5 + 15r_7$ mentre dal teorema cinese del resto si ha $x = 35\,x_1 + 21\,x_2 + 15\,x_3$?

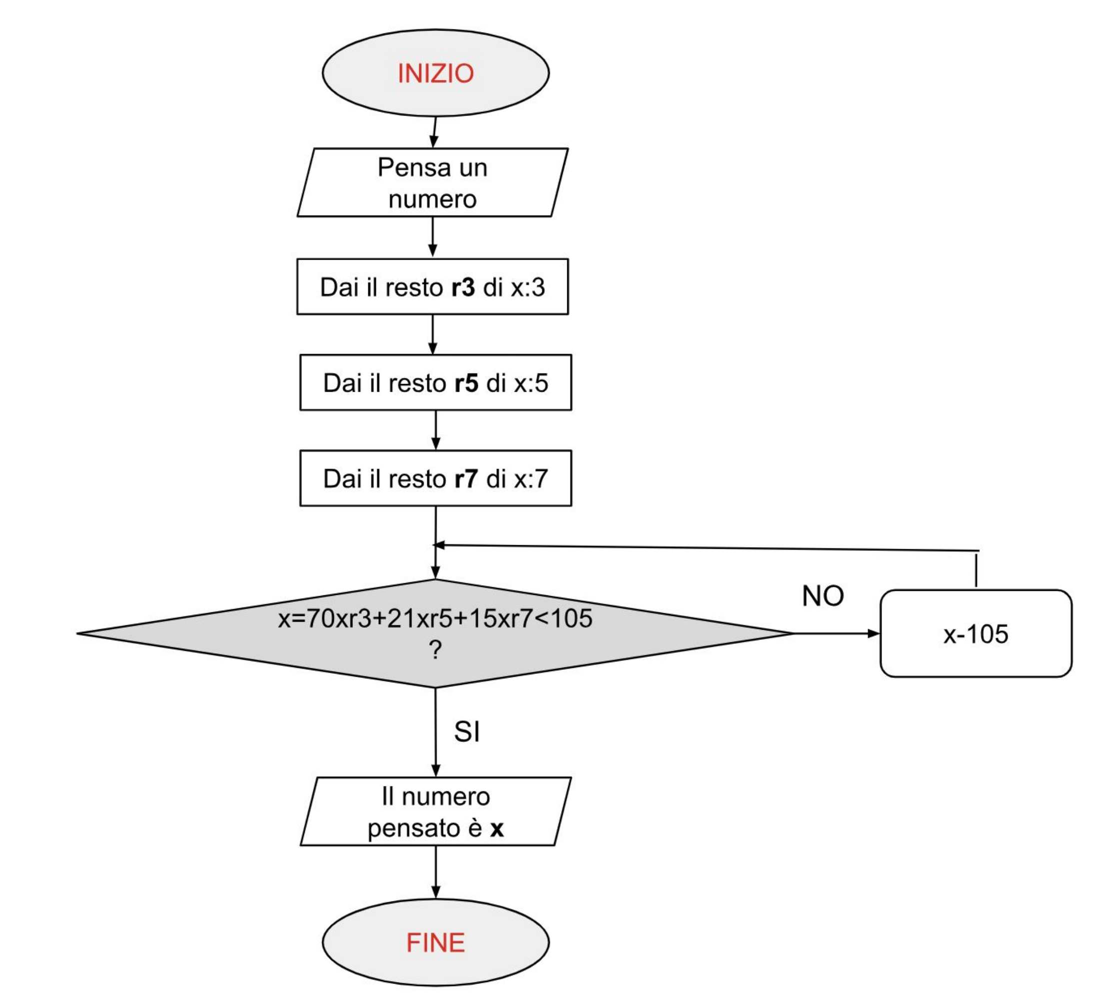
Per poterlo capire, si sfrutta nuovamente il teorema cinese del resto, ottenendo:

$$\begin{cases} 2\,x_1 \equiv r_3 \, mod \, 3 \\ x_2 \equiv r_5 \, mod \, 5 \\ x_3 \equiv r_7 \, mod \, 7 \end{cases}$$

Quindi, poiché $2\,x_1 \equiv r_3 \, mod \, 3$, cioè $x_1 \equiv 2\,r_3 \, mod \, 3$.

Allora $70r_3 = 35\,x_1 = 35 \times 2\,r_3$.

Programmare su Python



File Edit Format Run Options Window Help

```python
print("Pensa ad un numero")
r3 = int(input("Inserisci il resto del numero che hai pensato diviso 3: "))
r5 = int(input("Inserisci il resto del numero che hai pensato diviso 5: "))
r7 = int(input("Inserisci il resto del numero che hai pensato diviso 7: "))

x = (70 * r3)+(21 * r5)+(15 * r7) #procedimento seguito da Fibonacci
y = x - 105 #comando per avere un numero mod 105
if x < 105:
    print( "il numero che hai pensato è: ", x)
else:
    while y>105:
        y= y - 105 #corpo del ciclo per ottenere un numero <105
    print("il numero che hai pensato è: ", y)
```

```
Pensa ad un numero
Inserisci il resto del numero che hai pensato diviso 3: 1
Inserisci il resto del numero che hai pensato diviso 5: 2
Inserisci il resto del numero che hai pensato diviso 7: 3
il numero che hai pensato è:  52
```

Conclusioni

I significati matematici coinvolti causano un *remplacement* [Barbin, 2022], cioè vengono sostituiti e rimpiazzati.

Le risorse a disposizione sono state:

1) i differenti artefatti presentati, ovvero
   - quello storico (il Liber Abbaci);
   - quello "concreto", quali le tabelle dell'addizione e della moltiplicazione;
   - quello digitale (foglio di calcolo e Python);
2) l'insegnante come mediatore degli apprendimenti e guida verso l'autonomia (colleghi di Latino);
3) i compagni, nei dialoghi tra pari, utili alla costruzione della conoscenza.

Bibliografia

Ambrosetti, N. (2012), *L'eredità arabo-islamica nelle scienze e nelle arti del calcolo dell'Europa medievale* , 1-407

Barbin, É. (2022). On the role and scope of historical knowledge in using the history of mathematics in education. ZDM–Mathematics Education, 54(7), 1597-1611

Boncompagni, B. (Ed.). (1857). Liber abbaci (Vol. 1). Tipogr. delle Scienze Matematiche e Fisiche

Corry, L., (2020), *Breve storia dei numeri,* Hoepli Editore

Dascal M., (2007), *Gottfried Wilhelm Leibniz, The art of controversies,* Springer

Fibonacci L., traduzione del *Liber Abbaci,* presente sul sito https://www.progettofibonacci.it/index.html

Giusti, E., & d'Alessandro, P. (2022). Leonardi Bigolli Pisani vulgo Fibonacci. Liber Abbaci. Sudhoffs Archiv, 106(1), 123-124

Guillemette, D. e Radford, L. (2022). Storia della matematica nel contesto della formazione degli insegnanti di matematica: una prospettiva dialogica/etica. ZDM–Educazione alla matematica , 54 (7), 1493-1505

Sfard, A. (2015), *Apprendimento, comunicazione e matematica. Il saggio manuale dell'apprendimento* , 129-138.

Grazie per l'attenzione!!!

per eventuali contatti

cerasaro@axp.mat.uniroma2.it

silvia.cerasaro@gmail.com