Liceo Matematico

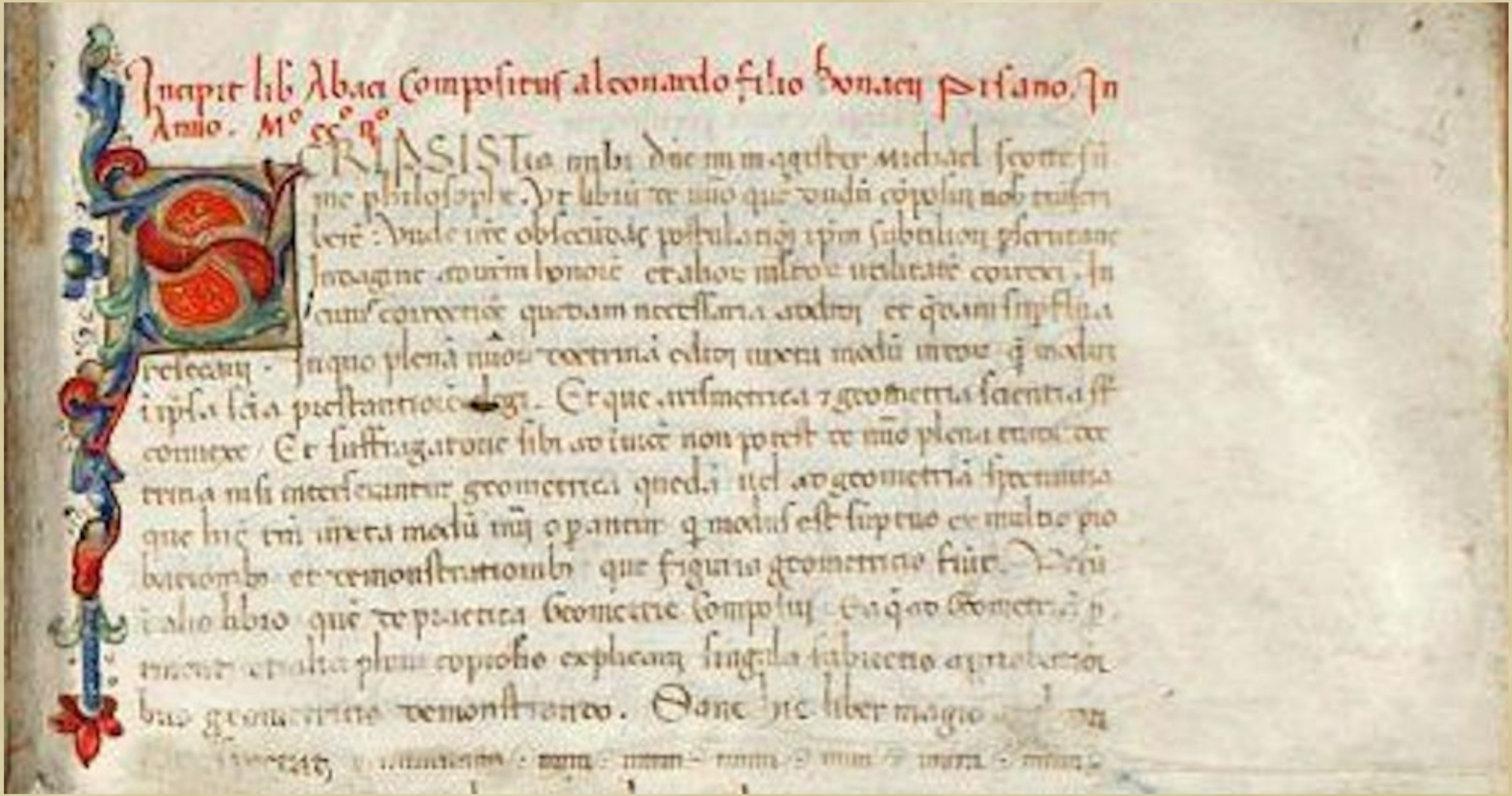
8 Marzo 2024
Dipartimento "Guido Castelnuovo"
Università La Sapienza - Roma

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

Francesca Tovena - Silvia Cerasaro
Dipartimento di Matematica
Università Tor Vergata- Roma

Università di Roma Tor Vergata

Liber Abbaci di Leonardo Pisano Fibonacci



... Leonardi pisani ...
Est Abbatie florentine

B 73

SCRIPSISTIS mihi domine mi magister Michael Scotte summe philosophe. Ut librum de numero quem dudum composui vobis transcriberem: 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 doctrina nisi interserantur geometrica quedam vel ad geometriam spectantia que hic tamen iuxta modum numeri operantur qui modus est sumptus ex multis probationibus et demonstrationibus que figuris geometricis fiunt. Verum in alio libro quem de practica geometrie composui ea que ad geometriam pertinent et alia plura copiosius explicavi singula subiectis approbationibus geometricis demonstrando. Sane hic liber magis ... spectat ...

quam ad practicam. Unde qui per eum huius scientie practicam bene scire voluerit oportet eos continuo usu et exercitio 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 anelitu in uno et eodem instanti circa idem per omnia naturaliter consonent et tunc cum fuerit discipulus habitudinem consecutus gradatim poterit ad perfectionem huius facile pervenire. Et ut facilior pateret doctrina hunc 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 provinciam cum suis variis modis. ad que loca negotiationis tam postea peragravi per multum studium et disputationis didici conflictum. Sed hoc totum etiam et algorismum atque artem pictagore quasi errorem computavi respectu 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 intelligibilius 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. Siquid 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 retineri debeant in manibus. et de introductionibus abbaci. 1

De multiplicatione integrorum numerorum. 2

De additione ipsorum ad invicem. 3

Leonardi Pisani Algorismus, Geometria
Inter Codices designatur num: 44.

[illegible] tot [illegible] iunt [illegible] pater [illegible] numeri

[illegible] millenarius [illegible] adiecta [illegible]

[illegible] rationis [illegible] numerum [illegible] figure. [illegible]

[illegible] numerum octo figurarum [illegible] 8 7 6 5 4 3 2 1 [illegible]

[illegible] 2 [illegible] 3 [illegible] parte.

[illegible] 4 [illegible] dicit mille [illegible]

[illegible] 5 [illegible] 6 [illegible] decem [illegible]

[illegible] septenario 7 [illegible] in septimo gradu decem mille milia [illegible]

[illegible] decem milia [illegible]

[illegible] duo milia [illegible] 7 [illegible] sub 4 [illegible]

[illegible] figuras

2 5 7 6 0 4 8 1 3 [illegible] ducenta [illegible]

[illegible] milia [illegible] figuras

[illegible] 1 0 0 7 5 4 3 2 8 9 0 8 1 [illegible] mille septem milia milia milia

[illegible] nonaginta [illegible] 7

[illegible] **P** [illegible]

[illegible] 15 [illegible] 6 7 8 9 3 5 7 8 4 1 0 5 2 9 6 [illegible]

figure 2 9 6 [illegible] in premisso exemplo [illegible]

[illegible] tres figuras [illegible] in principio [illegible] et sic dicas sexcenta septuaginta

octo milia milia milia milia [illegible] milia milia milia

[illegible] 7 1 0 5

milia [illegible] 2 9 6 [illegible] in principio [illegible] cum te

manet [illegible] quinque [illegible]

[illegible] cum [illegible]

P[illegible] oportet eos [illegible]

[illegible] manuum [illegible]

[illegible] manu [illegible]

[illegible] media [illegible] duo.

[illegible] media uola. [illegible] medium

[illegible] 4 [illegible] 5 [illegible] 6 [illegible] 7 [illegible]

[illegible] 8 [illegible] 9 [illegible] pollice [illegible]

[illegible] 10 [illegible] 20 [illegible] 30 [illegible]

[illegible] 40 [illegible] 50 [illegible]

[illegible] 60 [illegible] 70 [illegible]

[illegible] 80 [illegible] 90 [illegible]

[illegible] 100 [illegible] 200 [illegible] nonagesimum

[illegible] 9000 [illegible] pagina [illegible]

[illegible] 2 3 [illegible]

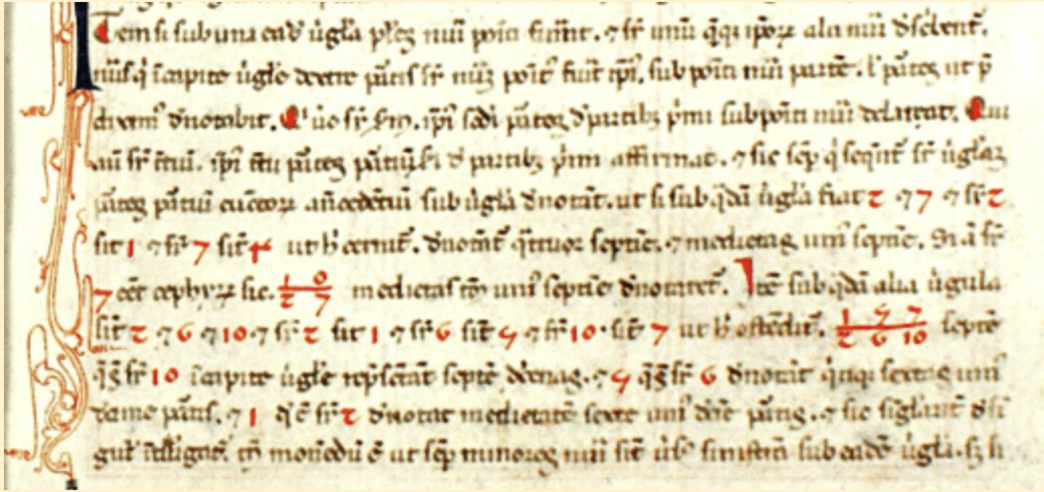
[illegible] intelligas [illegible]

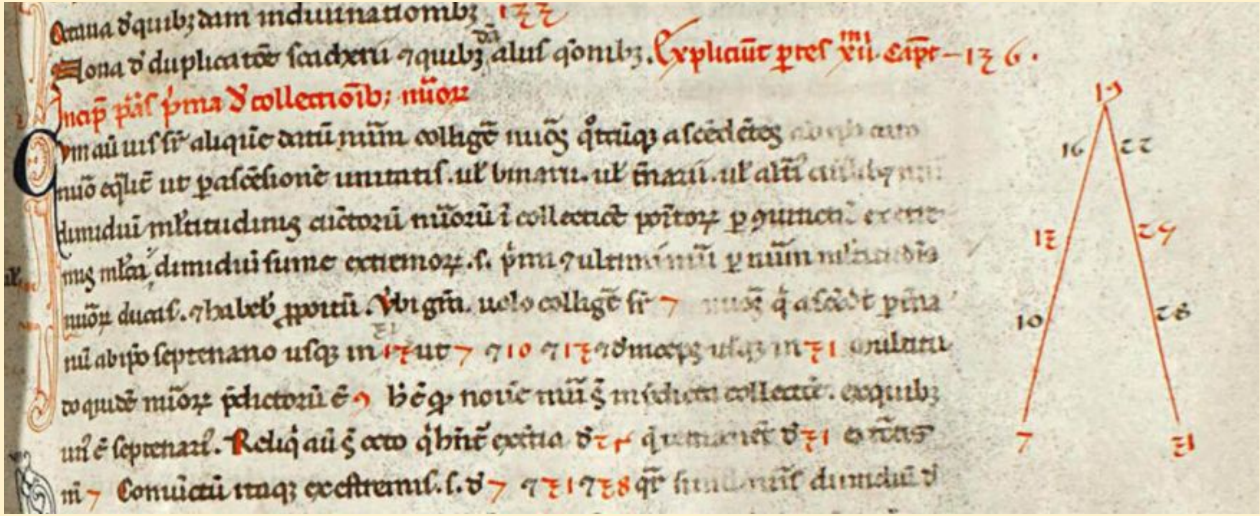
2	et 2	fiunt	4
2	3		5
2	4		6
2	5		7
2	6		8
2	7		9
2	8		10
2	9		11
2	10		12
Ianua ternarii.			
3	et 3	fiunt	6
3	4		7
3	5		8
3	6		9
3	7		10
3	8		11
3	9		12
3	10		13
Ianua quaternarii			
4	et 4	fiunt	8
4	5		9
4	6		10
4	7		11
4	8		12
4	9		13
4	10		14
Ianua quinarii			
5	et 5	fiunt	10
5	6		11
5	7		12
5	8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

FERMAT
1640

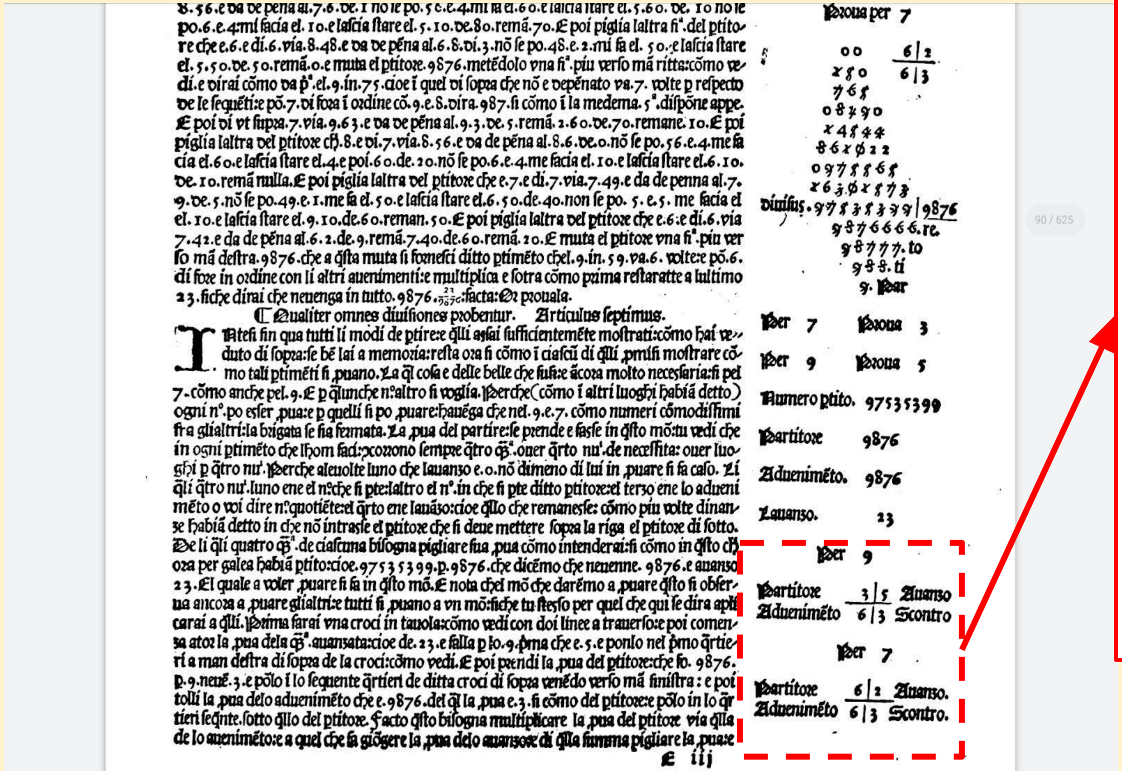
$$a^{p-1} \equiv 1 \pmod{p}$$

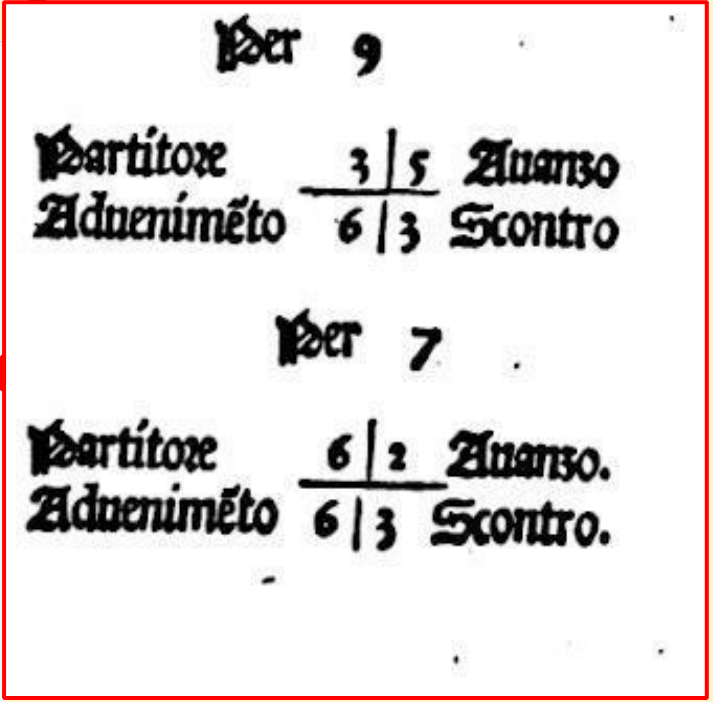
EULERO
1736

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

GAUSS
1800

L'aritmetica modulare prima dei "grandi matematici"





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

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

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

Attività proposte nelle classi del biennio

Uso diretto della fonte storica in classe

Lettura in chiave
STORICA

Liber Abbaci

Lettura in chiave
MATEMATICA

Lettura in chiave
EDUCATIVA

Guillemette, Radford, 2022

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

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].

Assume un ruolo fondamentale il DIALOGO

Attività 1: La prova del nove

(II.9 ; G: II.22) Adesso vediamo se (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.

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

Scheda 1

Leggi il seguente brano e scrivi nel linguaggio matematico che conosci quello che viene descritto. Si considera la moltiplicazione svolta nel paragrafo precedente, cioè $98 \times 98 = 9604$

(II.9 ; G: II.22) Adesso vediamo se (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.

Esercizio per gli studenti

Di cosa si tratta?

Nel seguente brano, dando per scontato dal paragrafo precedente che $37 \times 49 = 1813$, cosa si descrive?

> (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.

Cosa significa "si divida 37 per 9, cioè si addizionino le figure del 37"?

Esercizio per gli studenti

Inventa tu un esempio.

Perché la prova del nove funziona?

Rivedere il concetto di divisione tra numeri naturali

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

Quali valori può assumere il resto?

Scheda 2

Scrivi la divisione dei seguenti numeri per 9, specificando il quoziente ed il resto.

23	46	72	134	251

Quindi, $23 = 9 \times$____+____. Scrivi lo stesso per gli altri numeri.

Esercizio per gli studenti

Riporta nella seguenta tabella i numeri da 1 a 90, in base al resto della divisione per 9.

1	2	3	4	5	6	7	8	0

Esercizio per gli studenti

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

A quale classe appartiene il 335?

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

oppure

$335 = 300+30+5=(9\times33+3)+(9\times3+3)+(9\times0+5)$

Quindi, $3+3+5=11\equiv2 \mod 9$

Questo giustifica perché prendere la somma delle cifre

A quale classe di resto appartengono i seguenti numeri?

324

1256

123

995

377

Esercizio per gli studenti

Vediamo gli esempi riportati da Fibonacci…

$$98 \times 98 = 9604$$

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

$$(9 \times 10)^2 + 2 \times (9 \times 10 \times 8) + 8^2$$

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

$64 \equiv 1 \bmod 9$

Il prodotto è :

$9604=9000+600+0+4=$

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

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

Sarà possibile dedurre le seguenti regole: >>>

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

oppure 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 $a \times b = n \times q_3 + (r_1 \times r_2)$

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

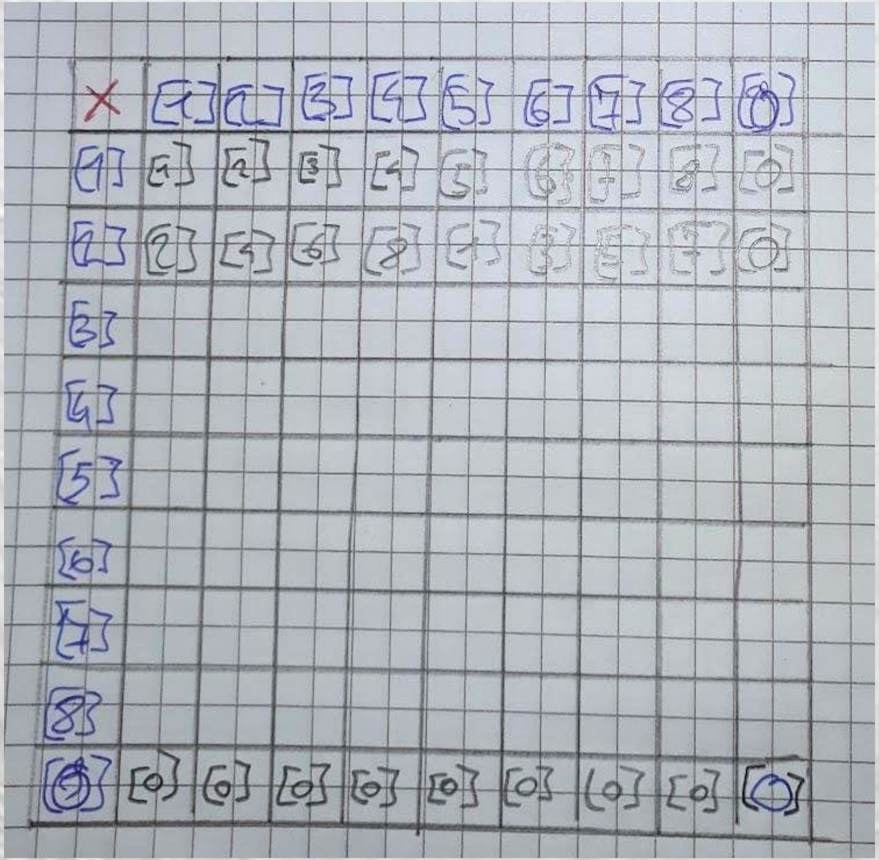
Si costruiscono le tavole della somma e del prodotto.

Si individuano gli elementi neutri per le due operazioni

Si discute l'esistenza di opposto e inverso

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

In particolare, 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
1	+	1	2	3	4	5	6	7	8	0
2	1	2	3	4	5	6	7	8	0	1
3	2	3	4	5	6	7	8	0	1	2
4	3	4	5	6	7	8	0	1	2	3
5	4	5	6	7	8	0	1	2	3	4
6	5	6	7	8	0	1	2	3	4	5
7	6	7	8	0	1	2	3	4	5	6
8	7	8	0	1	2	3	4	5	6	7
9	8	0	1	2	3	4	5	6	7	8
10	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	13
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
13	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 = 5x1+2

5 = 2x2+1

2 = 1x2+0

1 = 7x (-2)+5x3

L'inversa della classe 5 mod 7 è 3. Infatti, 5x3=15≡1 mod 7

Riflessione per lo studente…

In quale circostanza si sommano le cifre di un numero?

L'aritmetica modulare può essere utile per la comprensione dei **criteri di divisibilità** per 3 e 9,

In particolare per 11, se si recita la regola "sommo le cifre di posto pari con le opposte di posto dispari, se il resto sarà o zero o 11, allora il numero considerato è divisibile per 11".

Infatti, sappiamo *già* che $a \equiv b \bmod 11$ se $a = 11 \times n + b$.

In particolare si ha che $10 \equiv -1 \bmod 11$, $100 \equiv 1 \bmod 11$, $1000 \equiv -1 \bmod 11$, ecc..

Funziona sempre la prova del nove?

58 x 65 = 3770

4	8
2	8

58 x 65 = 3707

4	8
2	8

Condizione necessaria ma NON sufficiente...

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

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

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

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

(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($3\times5\times7$) = mod 105. Questo giustifica la scelta del 105 da parte di Fibonacci.

La soluzione è data da:

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

$$\begin{cases} \frac{N}{n_1}x_1 \equiv 1 \, mod\, 3 \\ \frac{N}{n_1}x_2 \equiv 2 \, mod\, 5 \\ \frac{N}{n_1}x_3 \equiv 3 \, mod\, 7 \end{cases}$$

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
$35 \equiv 2 \bmod 3$
$21 \equiv 1 \bmod 5$
$15 \equiv 1 \bmod 7$, 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:

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

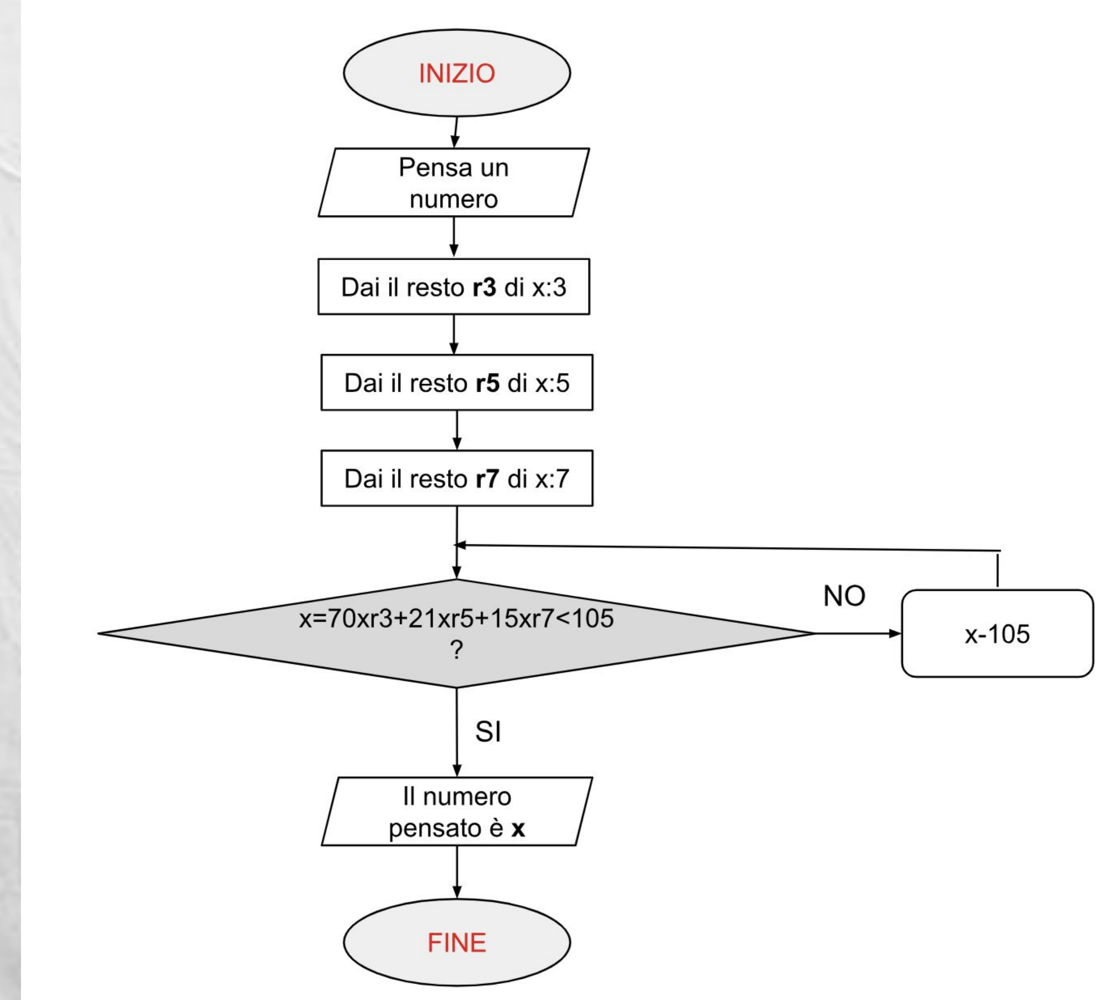
Quindi, poiché $2 \, x_1 \equiv r_3 \, mod \, 3$, cioè $x_1 \equiv 2 \, r_3 \, mod \, 3$.

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

Proporre agli studenti la risoluzione di problemi simili

(XII.8.5; *G: XII.1195***)** Prescrivi che il numero che egli tenne a memoria sia diviso per 5 e per 7 e per 9 nel modo del metodo precedente; e chiedi cosa rimanga da ciascuna divisione, una per una, e per ciascuna unità che sarà rimasta dalla divisione per 5, conserva 126; e per qualunque unità rimanente dalla divisione per sette, 225; e per ciascuna unità rimasta dalla divisione per 9, prendi 280; e sempre quando il totale sarà cresciuto, cosicché sia possibile sottrarre 315, togli via il 315 quante volte avrai potuto, e ciò che alla fine ti sarà rimasto sarà il numero cercato.

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 digitale (foglio di calcolo e Python);
2) l’insegnante come mediatore degli apprendimenti e guida verso l’autonomia;
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.

per eventuali contatti

cerasaro@axp.mat.uniroma2.it

silvia.cerasaro3@gmail.com

Grazie per l'attenzione!!!