

I gioielli della Matematica
Illustrare dimostrazioni combinatorie
in Teoria Elementare dei Numeri
per mezzo di anelli e orecchini

Alessandro Zaccagnini

MaddMaths!
Università di Parma

Roma, 17 novembre 2023

- 1 Preliminari
- 2 Il Teorema di Wilson
- 3 Il Piccolo Teorema di Fermat
- 4 Rappresentazione grafica di gruppi finiti
 - Il gruppo $\mathbb{Z}_n$
 - La tavola pitagorica in $\mathbb{Z}_{12}$
 - La periodicità delle potenze in $\mathbb{Z}_n^*$
 - La tavola pitagorica in $\mathbb{Z}_{15}$
- 5 Costruzione del grafo che rappresenta $\mathbb{Z}_{15}^*$
 - Determinazione delle catene
 - Saldatura delle catene
- 6 Costruzione del grafo che rappresenta $\mathbb{Z}_{35}^*$
 - Determinazione delle catene
 - Saldatura delle catene
 - Completamento della costruzione
- 7 Altri esempi
- 8 Riferimenti

I laboratori

Tratterò due esperienze didattiche nell'ambito del Piano Nazionale Lauree Scientifiche

La prima è stata fatta nell'anno 2013–2014 con studenti di alcune terze classi del Liceo Scientifico “Attilio Bertolucci” di Parma, con la collaborazione di Giancarlo Fiorini

La seconda nell'anno 2022–2023 con studenti del terzo e quarto anno del Liceo Classico “G. B. Romagnosi” di Parma, con la collaborazione di Caterina Cozzani e Roberta Sandri

In entrambi i casi, l'obiettivo è quello di visualizzare proprietà matematiche o dimostrazioni mediante la costruzione di oggetti concreti

Qui ci limitiamo a vedere una parte di ciascuno di questi laboratori

I dettagli sono stati pubblicati o lo saranno a breve

La moltiplicazione come fonte di complessità

Il filo conduttore di questi laboratori è la visualizzazione delle proprietà della moltiplicazione

La moltiplicazione è un'operazione *complessa*, perché rimescola gli interi molto più di quanto faccia l'addizione

La complessità della moltiplicazione è all'origine della difficoltà del problema della fattorizzazione, e quindi, in ultima analisi, della sicurezza di crittosistemi quali RSA, ma non solo

Ne ho parlato per esempio in un articolo per “MaddMaths!” in cui ho trattato la moltiplicazione in $\mathbb{N}$, ed il grafo corrispondente

- 1 Preliminari
- 2 Il Teorema di Wilson**
- 3 Il Piccolo Teorema di Fermat
- 4 Rappresentazione grafica di gruppi finiti
 - Il gruppo $\mathbb{Z}_n$
 - La tavola pitagorica in $\mathbb{Z}_{12}$
 - La periodicità delle potenze in $\mathbb{Z}_n^*$
 - La tavola pitagorica in $\mathbb{Z}_{15}$
- 5 Costruzione del grafo che rappresenta $\mathbb{Z}_{15}^*$
 - Determinazione delle catene
 - Saldatura delle catene
- 6 Costruzione del grafo che rappresenta $\mathbb{Z}_{35}^*$
 - Determinazione delle catene
 - Saldatura delle catene
 - Completamento della costruzione
- 7 Altri esempi
- 8 Riferimenti

Il Teorema di Wilson

Teorema (Wilson)

$n \geq 2$ è primo se e solo se $(n - 1)! \equiv -1 \pmod{n}$

Esempio

$$\begin{aligned}
 (11 - 1)! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \\
 &= 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 \\
 &\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 10 \\
 &\equiv -1 \pmod{11}
 \end{aligned}$$

L'equazione $x \equiv x^{-1} \pmod{11}$ equivale a $x^2 \equiv 1 \pmod{11}$ e dunque ha due sole soluzioni, $x = 1$ ed $x = 10$

Quindi possiamo associare ciascun fattore del prodotto $10!$, tranne 1 e 10, con il suo reciproco

La condizione di Wilson

Attenzione

$(10 - 1)! \equiv 0 \pmod{10}$, poiché $10 = 2 \cdot 5$ e questi sono fattori in $9!$

La condizione di Wilson è **necessaria e sufficiente** per la primalità ma richiede il calcolo di $(n - 1)!$

Esercizio

Si dimostri che se $n \geq 6$ è composto, allora $(n - 2)! \equiv 0 \pmod{n}$

Si faccia attenzione al caso $n = p^2$

Dimostrazione del Teorema di Wilson

Dimostrazione.

L'applicazione $f: \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*$ definita da $x \mapsto x^{-1}$ è una biiezione
 I suoi punti fissi sono $x = 1$ ed $x = -1 = p - 1$, perché p è primo
 Dunque

$$(p-1)! \equiv \prod_{a \in \mathbb{Z}_p^*} a \equiv (p-1) \prod_{a=2}^{p-2} a \equiv p-1 \equiv -1 \pmod{p}$$

poiché nel prodotto a destra ogni fattore è **distinto** dal suo reciproco □

C'è un'altra dimostrazione che dipende dal Teorema di Fermat

La dimostrazione combinatoria

Dimostreremo che se p è un numero primo allora

$$(p-1)! - (p-1) \quad \text{è divisibile per } p$$

Costruiremo tutti gli orecchini formati da p perline di p colori distinti, nei quali la prima perline ha un colore fissato, nero nei nostri esempi

Il numero totale è $(p-1)!$

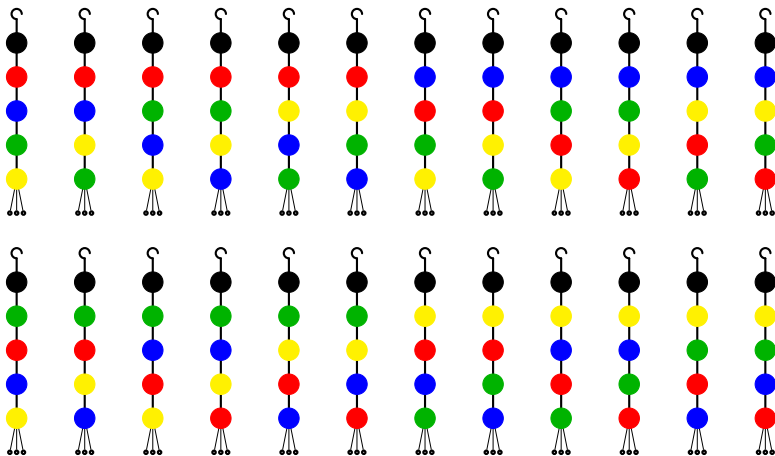
Suddivideremo questi orecchini in famiglie, utilizzando una certa trasformazione biiettiva dell'insieme

La trasformazione è periodica e il suo periodo divide p

Troveremo esattamente $p-1$ orecchini per cui il periodo vale 1

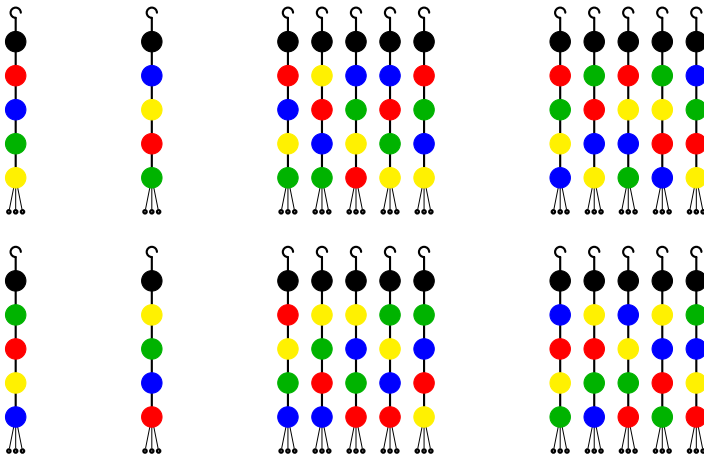
Per tutti gli altri orecchini il periodo vale p e dunque p divide $(p-1)! - (p-1)$

Gli orecchini

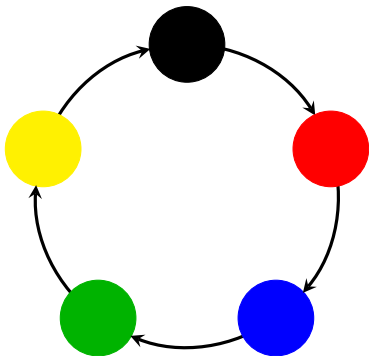


Gli orecchini che si possono realizzare con 5 perline colorate sono $4! = 24$

Gli orecchini suddivisi in classi di equivalenza

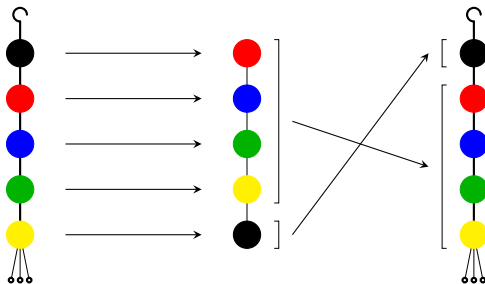


La sequenza dei colori



Come trasformare un orecchino in un altro

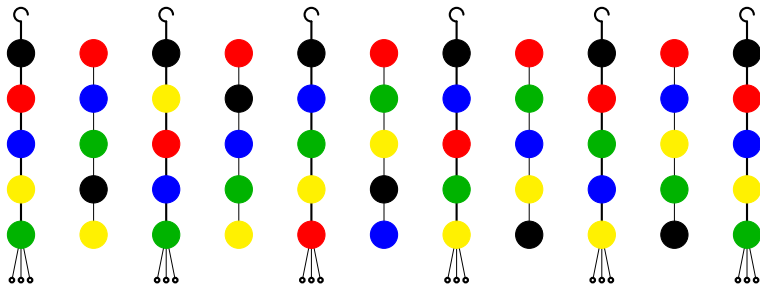
- Mandiamo ogni colore nel successivo ($N \rightarrow R \rightarrow B \rightarrow V \rightarrow G \rightarrow N$)
- Riportiamo il nero in cima senza cambiare la sequenza dei colori



Siamo tornati subito all'orecchino iniziale, al primo passo

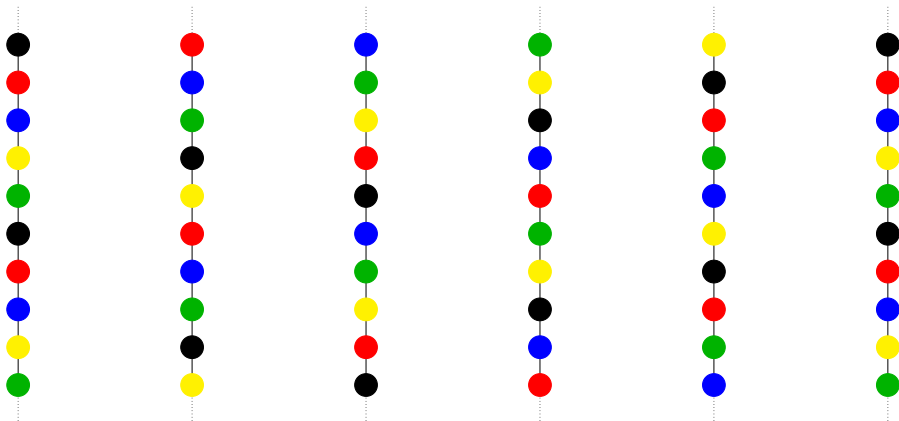
Come trasformare un orecchino in un altro

- Mandiamo ogni colore nel successivo ($N \rightarrow R \rightarrow B \rightarrow V \rightarrow G \rightarrow N$)
- Riportiamo il nero in cima senza cambiare la sequenza dei colori



Torniamo all'orecchino iniziale dopo cinque passi

La dimostrazione della periodicità della trasformazione



La dimostrazione della periodicità della trasformazione

Il periodo è $p = 5$ o un suo divisore

A sinistra replichiamo l'orecchino di partenza due volte

In orizzontale eseguiamo la trasformazione ciclica dei colori seguendo la sequenza scelta prima

L'immagine del primo orecchino si legge nella seconda colonna prendendo 5 perline consecutive partendo da una perlina nera

Siccome la sequenza si ripete dopo 5 passi, il periodo è un divisore di 5

Gli orecchini “solitari” sono $p - 1$

Gli orecchini solitari sono quelli per cui la sequenza delle perline segue quella fissata all'inizio, prendendo le perline consecutivamente, oppure saltandone sempre una, o sempre due, ...

In termini formali, gli orecchini solitari corrispondono alle “progressioni aritmetiche” modulo p , di ragione 1, oppure 2, oppure 3, ..., oppure $p - 1$

Questo spiega perché gli orecchini solitari sono esattamente $p - 1$

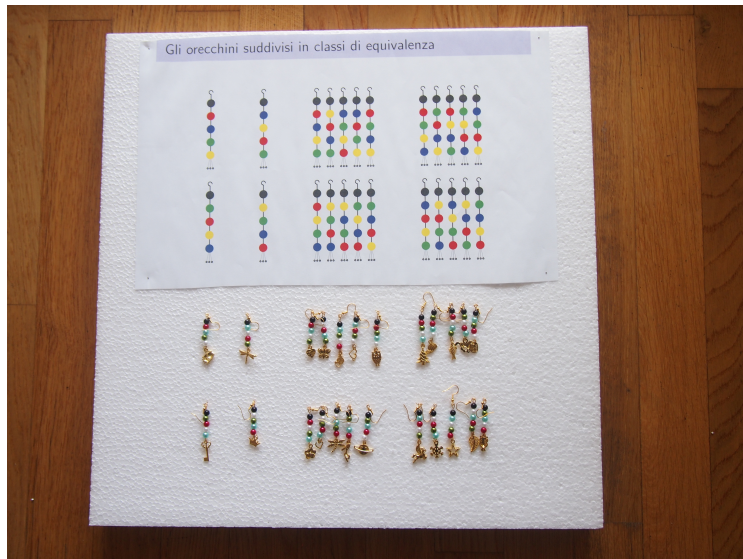
I pannelli preparati per Lucca Comics & Science



I pannelli preparati per Lucca Comics & Science



I pannelli preparati per Lucca Comics & Science

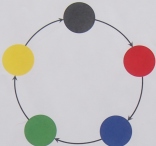


I pannelli preparati per Lucca Comics & Science



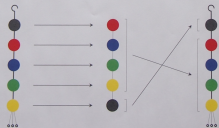
I pannelli preparati per Lucca Comics & Science

La sequenza dei colori



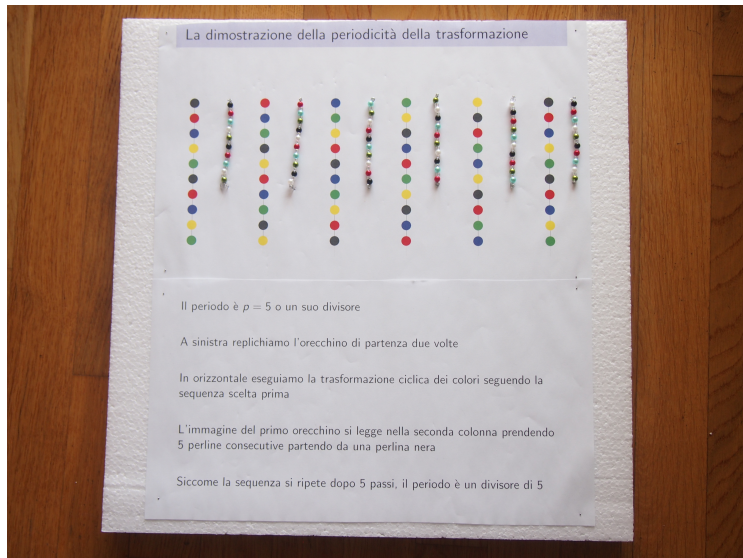
Come trasformare un orecchino in un altro

- Mandiamo ogni colore nel successivo ($N \rightarrow R \rightarrow B \rightarrow V \rightarrow G \rightarrow N$)
- Riportiamo il nero in cima senza cambiare la sequenza dei colori

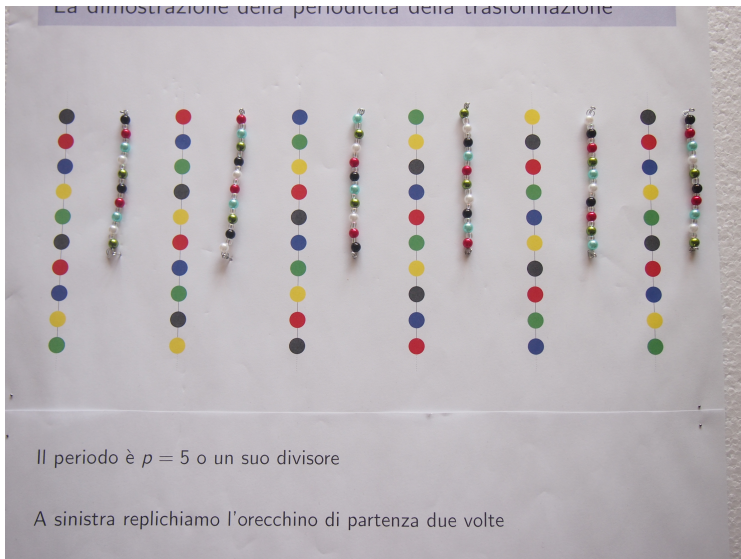


Siamo tornati subito all'orecchino iniziale, al primo passo

I pannelli preparati per Lucca Comics & Science



I pannelli preparati per Lucca Comics & Science



- 1 Preliminari
- 2 Il Teorema di Wilson
- 3 Il Piccolo Teorema di Fermat
- 4 Rappresentazione grafica di gruppi finiti
 - Il gruppo $\mathbb{Z}_n$
 - La tavola pitagorica in $\mathbb{Z}_{12}$
 - La periodicità delle potenze in $\mathbb{Z}_n^*$
 - La tavola pitagorica in $\mathbb{Z}_{15}$
- 5 Costruzione del grafo che rappresenta $\mathbb{Z}_{15}^*$
 - Determinazione delle catene
 - Saldatura delle catene
- 6 Costruzione del grafo che rappresenta $\mathbb{Z}_{35}^*$
 - Determinazione delle catene
 - Saldatura delle catene
 - Completamento della costruzione
- 7 Altri esempi
- 8 Riferimenti

Il Teorema di Fermat

Teorema (Fermat)

Se p è un numero primo e $p \nmid a$, allora

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

Esempio

$10^6 \equiv 1 \pmod{7}$: questo equivale alla periodicità dello sviluppo decimale di $1/7$

$$\frac{1}{7} = 0.\overline{142857} = \frac{142857}{999999} \iff 7 \mid 999999 = 10^6 - 1$$

Dimostreremo che $a^p - a$ è divisibile per p

Dimostrazione del Teorema di Fermat

Lemma

Se p è un numero primo, allora $p \mid \binom{p}{k}$ per $1 \leq k \leq p-1$

$$\binom{p}{k} = p \cdot \frac{(p-1)!}{k!(p-k)!}$$

Dimostriamo che $a^p \equiv a \pmod{p}$ per ogni $a \in \mathbb{N}$

Induzione su a : per $a = 0$ è ovvio. Se $a^p \equiv a \pmod{p}$ allora

$$\begin{aligned} (a+1)^p &= a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1 \\ &\equiv a^p + 1 \equiv a + 1 \pmod{p} \end{aligned}$$

La dimostrazione combinatoria

Consideriamo le collane fatte con p perline di a colori diversi, dove p è un numero primo e a è un intero positivo

In totale abbiamo a^p collane

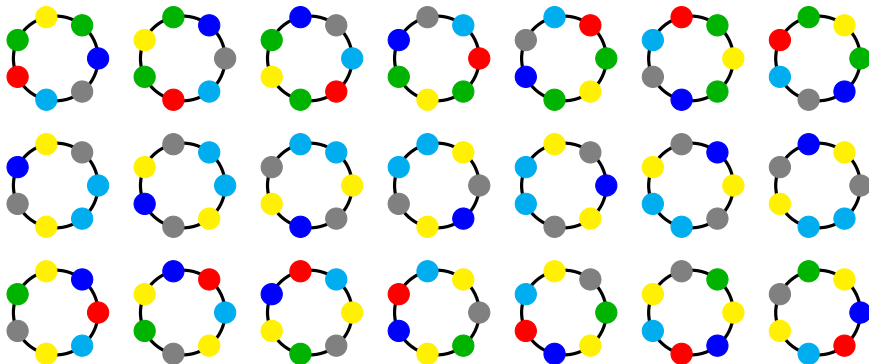
Chiameremo monocrome le a collane che hanno tutte le perline dello stesso colore: queste sono esattamente a , una per ciascun colore

Ci interessano le rimanenti $a^p - a$ collane policrome, che divideremo in classi ognuna delle quali contiene esattamente p elementi

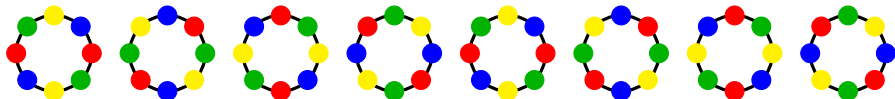
Questo dimostra che p divide $a^p - a$

Dimostrazione combinatoria del Teorema di Fermat

Suddividiamo le $6^7 - 6 = 279\,930$ collane policrome in classi, ruotandole



Le classi di equivalenza di tre collane policrome con $p = 7$ perline scelte fra $a = 6$ colori distinti. Ogni classe contiene **esattamente** 7 collane perché 7 è primo, e quindi 7 deve dividere $6^7 - 6$



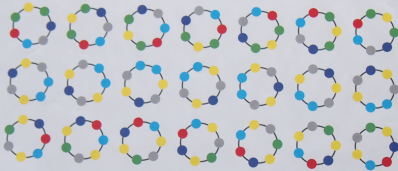
Se una collana policroma ha un numero di perline composto n , la sua classe di equivalenza può avere un numero di elementi che è un divisore proprio di n ; qui vediamo un caso in cui $n = 8$ e la classe di equivalenza di queste collane ha 4 elementi

I pannelli preparati per Lucca Comics & Science

2 Il Piccolo Teorema di Fermat

Dimostrazione combinatoria del Teorema di Fermat

Suddividiamo le $6^7 - 6 = 279\,930$ collane policrome in classi, ruotandole



Le classi di equivalenza di tre collane policrome con $p = 7$ perline scelte fra $a = 6$ colori distinti. Ogni classe contiene **esattamente** 7 collane perché 7 è primo, e quindi 7 deve dividere $6^7 - 6$.



I pannelli preparati per Lucca Comics & Science



I pannelli preparati per Lucca Comics & Science



I pannelli preparati per Lucca Comics & Science



- 1 Preliminari
- 2 Il Teorema di Wilson
- 3 Il Piccolo Teorema di Fermat
- 4 Rappresentazione grafica di gruppi finiti**
 - Il gruppo $\mathbb{Z}_n$
 - La tavola pitagorica in $\mathbb{Z}_{12}$
 - La periodicità delle potenze in $\mathbb{Z}_n^*$
 - La tavola pitagorica in $\mathbb{Z}_{15}$
- 5 Costruzione del grafo che rappresenta $\mathbb{Z}_{15}^*$
 - Determinazione delle catene
 - Saldatura delle catene
- 6 Costruzione del grafo che rappresenta $\mathbb{Z}_{35}^*$
 - Determinazione delle catene
 - Saldatura delle catene
 - Completamento della costruzione
- 7 Altri esempi
- 8 Riferimenti

Visualizzazione dei gruppi $\mathbb{Z}_n^*$

Vogliamo rappresentare una struttura molto importante in algebra mediante piccoli gioielli

In particolare, ci interessano i gruppi $\mathbb{Z}_n^*$

Costruiamo il grafo associato a $\mathbb{Z}_n^*$ studiando la tavola pitagorica $n \times n$ modulo n

Abbiamo usato un linguaggio piú semplice possibile, senza introdurre la teoria dei gruppi

Nel corso del lavoro, sono stati “scoperti” i concetti di ordine di un elemento, orbita, sottogruppo, ...

Naturalmente, sono stati “scoperti” anche i Teoremi di Fermat e di Eulero, cioè le versioni del Teorema di Lagrange valide in $\mathbb{Z}_n^*$

Operazioni modulo n

Prendiamo un intero positivo n e consideriamo l'insieme

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-2, n-1\}$$

Questi sono i possibili resti della divisione di un qualsiasi intero m per n

$$m = qn + r \quad \text{dove } q \in \mathbb{Z} \text{ ed } r \in \mathbb{Z}_n$$

$\mathbb{Z}_n$ è un insieme finito, nel quale ha senso fare addizioni e moltiplicazioni

Per la precisione, eseguiremo tutte le operazioni normalmente, ma alla fine divideremo il risultato per n trascurando il quoziente q e considerando come “risultato” il valore di r

La tavola pitagorica in $\mathbb{Z}_{12}$

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

La tavola pitagorica in $\mathbb{Z}_{12}^*$

Eliminiamo tutte le righe e le colonne che contengono qualche 0

Equivalentemente, teniamo tutte le righe e le colonne che contengono 1

1	5	7	11
5	1	11	7
7	11	1	5
11	7	5	1

In generale poniamo

$$\mathbb{Z}_n^* = \{r \in \mathbb{Z}_n : \exists a \in \mathbb{Z}_n, m \in \mathbb{Z} \text{ tali che } ar = mn + 1\}$$

Perché le due richieste qui sopra sono equivalenti?

La costruzione delle tavole pitagoriche

Le tavole pitagoriche rilevanti sono state costruite dagli studenti

Inizialmente, hanno fatto i calcoli con carta e matita, per poi passare ad utilizzare le calcolatrici tascabili, incluse quelle dei telefoni cellulari

Questo ha portato alla scoperta di piccole differenze nei risultati, principalmente nel calcolo del resto usando la procedura

$$a/n \rightarrow \{a/n\} \rightarrow n\{a/n\} = a - n \left\lfloor \frac{a}{n} \right\rfloor$$

perché calcolatrici diverse danno luogo ad arrotondamenti leggermente diversi. Qui $\{x\}$ indica la *parte frazionaria* di x

Piano piano è sorta l'esigenza di usare calcolatrici programmabili per alleviare la noia dei calcoli, necessari per raggiungere il risultato desiderato ma molto tedious

Alla fine, gli studenti hanno imparato i rudimenti di `pari-gp`

La periodicità delle potenze in $\mathbb{Z}_p^*$ e in $\mathbb{Z}_n^*$

Teorema (Fermat)

Se p è un numero primo, ed a è un intero non divisibile per p , allora p divide $a^{p-1} - 1$

Come conseguenza, la successione $x_m = a^m \bmod p$ è periodica con periodo $p - 1$ o un suo divisore

Teorema (Eulero)

Se n è un numero intero, ed a è un intero primo con n , allora n divide $a^{\varphi(n)} - 1$, dove $\varphi(n) = |\mathbb{Z}_n^|$*

Come conseguenza, la successione $x_m = a^m \bmod n$ è periodica con periodo $\varphi(n)$ o un suo divisore

Periodicità: lo stesso fenomeno che riscontriamo nella divisione fra interi, che dà origine a numeri decimali periodici

La tavola pitagorica in $\mathbb{Z}_{15}$

1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	14	6	13	5	12	4	11	3	10	2	9	1	8
8	1	9	2	10	3	11	4	12	5	13	6	14	7
9	3	12	6	0	9	3	12	6	0	9	3	12	6
10	5	0	10	5	0	10	5	0	10	5	0	10	5
11	7	3	14	10	6	2	13	9	5	1	12	8	4
12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	13	12	11	10	9	8	7	6	5	4	3	2	1

La tavola pitagorica in $\mathbb{Z}_{15}^*$

1	2	4	7	8	11	13	14
2	4	8	14	1	7	11	13
4	8	1	13	2	14	7	11
7	14	13	4	11	2	1	8
8	1	2	11	4	13	14	7
11	7	14	2	13	1	8	4
13	11	7	1	14	8	4	2
14	13	11	8	7	4	2	1

Vogliamo trasformare questa tabella di numeri in un oggetto

Le potenze degli elementi di $\mathbb{Z}_{15}^*$

	0	1	2	3	4
1	1	1	1	1	1
2	1	2	4	8	1
4	1	4	1	4	1
7	1	7	4	13	1
8	1	8	4	2	1
11	1	11	1	11	1
13	1	13	4	7	1
14	1	14	1	14	1

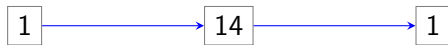
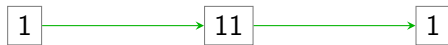
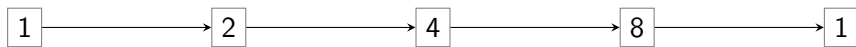
periodo 1	1			
periodo 2	4	11	14	
periodo 4	2	7	8	13

- 1 Preliminari
- 2 Il Teorema di Wilson
- 3 Il Piccolo Teorema di Fermat
- 4 Rappresentazione grafica di gruppi finiti
 - Il gruppo $\mathbb{Z}_n$
 - La tavola pitagorica in $\mathbb{Z}_{12}$
 - La periodicità delle potenze in $\mathbb{Z}_n^*$
 - La tavola pitagorica in $\mathbb{Z}_{15}$
- 5 Costruzione del grafo che rappresenta $\mathbb{Z}_{15}^*$**
 - Determinazione delle catene
 - Saldatura delle catene
- 6 Costruzione del grafo che rappresenta $\mathbb{Z}_{35}^*$
 - Determinazione delle catene
 - Saldatura delle catene
 - Completamento della costruzione
- 7 Altri esempi
- 8 Riferimenti

Determinazione delle catene quando $n = 15$

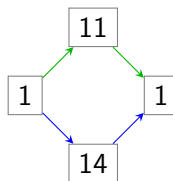
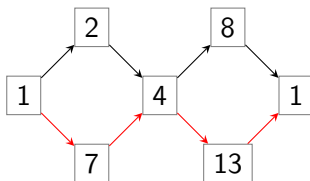
Chiameremo “catena” l'orbita di un elemento

Primo obiettivo: determinazione delle catene “massimali,” cioè che non possono essere ulteriormente estese

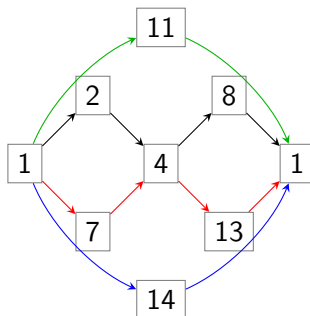


Saldatura delle catene

Secondo obiettivo: progressiva eliminazione degli elementi ripetuti (1 e 4 in questo caso), mediante “saldatura” delle catene

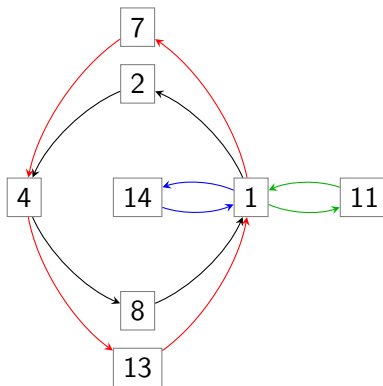


Saldiamo i due pezzi facendo corrispondere i numeri 1 a destra e sinistra



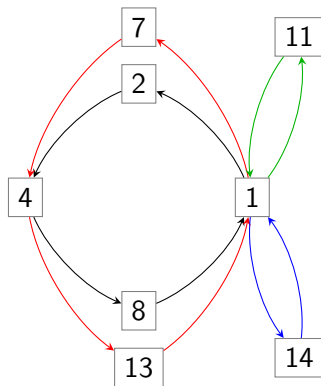
Il grafo di $\mathbb{Z}_{15}^*$

Per concludere, colleghiamo i due numeri 1



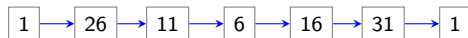
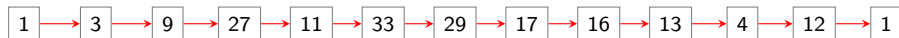
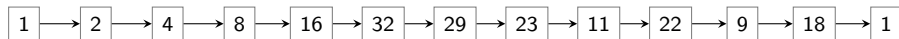
Il grafo di $\mathbb{Z}_{15}^*$

In alternativa



- 1 Preliminari
- 2 Il Teorema di Wilson
- 3 Il Piccolo Teorema di Fermat
- 4 Rappresentazione grafica di gruppi finiti
 - Il gruppo $\mathbb{Z}_n$
 - La tavola pitagorica in $\mathbb{Z}_{12}$
 - La periodicità delle potenze in $\mathbb{Z}_n^*$
 - La tavola pitagorica in $\mathbb{Z}_{15}$
- 5 Costruzione del grafo che rappresenta $\mathbb{Z}_{15}^*$
 - Determinazione delle catene
 - Saldatura delle catene
- 6 Costruzione del grafo che rappresenta $\mathbb{Z}_{35}^*$
 - Determinazione delle catene
 - Saldatura delle catene
 - Completamento della costruzione
- 7 Altri esempi
- 8 Riferimenti

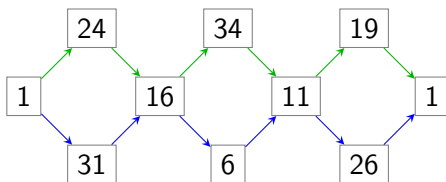
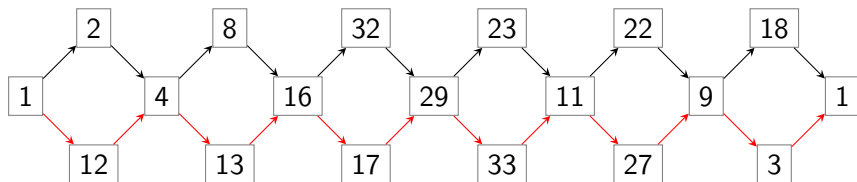
Determinazione delle catene quando $n = 35$



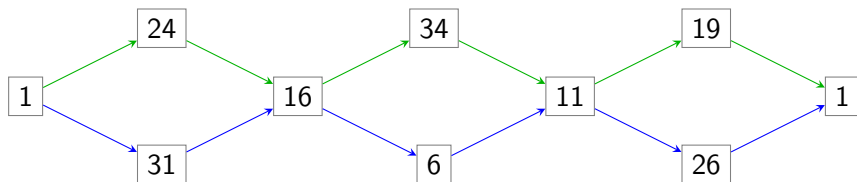
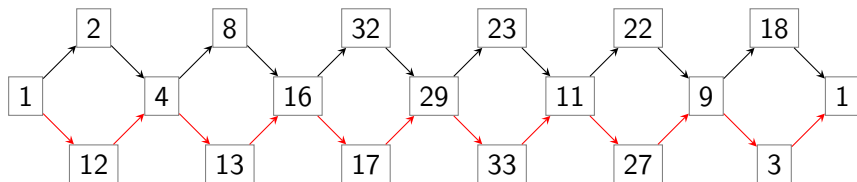
Si notino gli elementi ripetuti (1, 4, 16, 29, 11, 9) e il fatto che le catene possono essere percorse in entrambi i versi

Le potenze di 3 sono le stesse delle potenze di $3^{-1} \equiv 12 \pmod{35}$, in ordine inverso

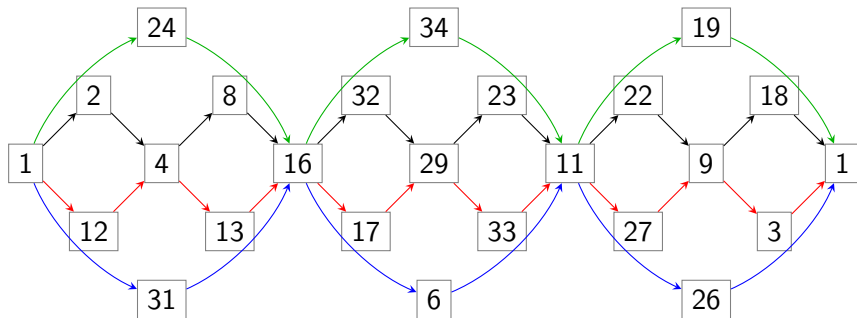
Saldatura delle catene

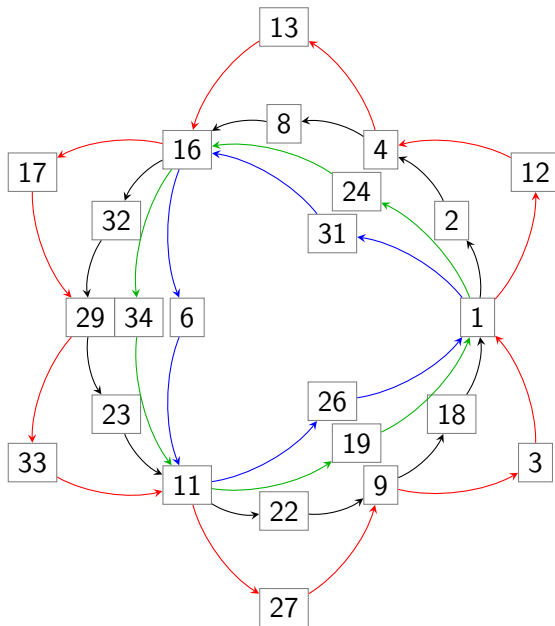


Saldatura delle catene, II



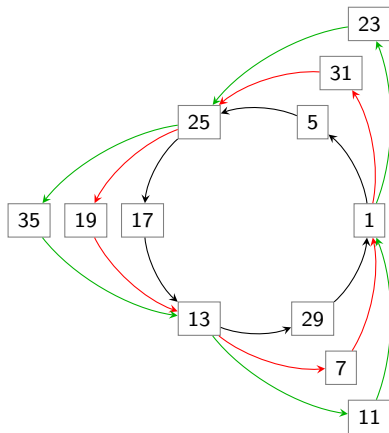
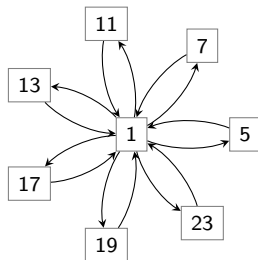
Completamento della costruzione



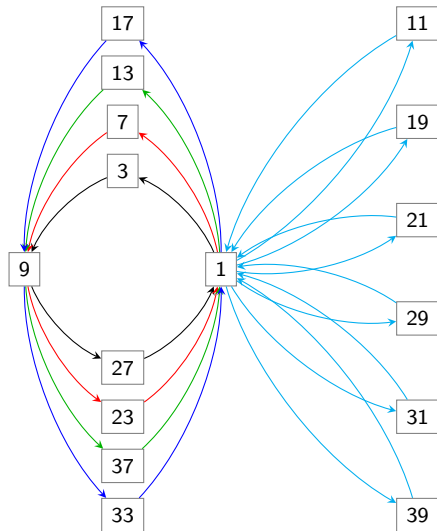


- 1 Preliminari
- 2 Il Teorema di Wilson
- 3 Il Piccolo Teorema di Fermat
- 4 Rappresentazione grafica di gruppi finiti
 - Il gruppo $\mathbb{Z}_n$
 - La tavola pitagorica in $\mathbb{Z}_{12}$
 - La periodicità delle potenze in $\mathbb{Z}_n^*$
 - La tavola pitagorica in $\mathbb{Z}_{15}$
- 5 Costruzione del grafo che rappresenta $\mathbb{Z}_{15}^*$
 - Determinazione delle catene
 - Saldatura delle catene
- 6 Costruzione del grafo che rappresenta $\mathbb{Z}_{35}^*$
 - Determinazione delle catene
 - Saldatura delle catene
 - Completamento della costruzione
- 7 Altri esempi
- 8 Riferimenti

$n = 24$ ed $n = 36$



$$n = 40$$



Dove siamo arrivati

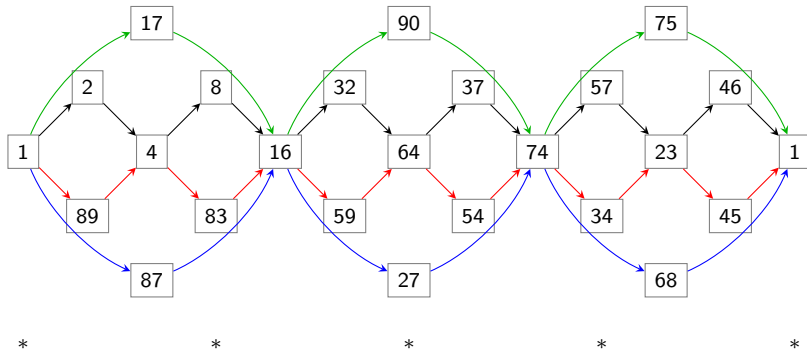
Gli studenti hanno scelto un caso piuttosto impegnativo, e cioè $n = 91$

Questo non è il più piccolo valore di n per cui il grafo non è planare, che è $n = 63$

Quando $n = 91$, si devono determinare le 4 radici quadrate dell'unità, che sono 1, 27, 64, 90, e le 8 radici quarte, che sono le precedenti e 8, 34, 57, 83

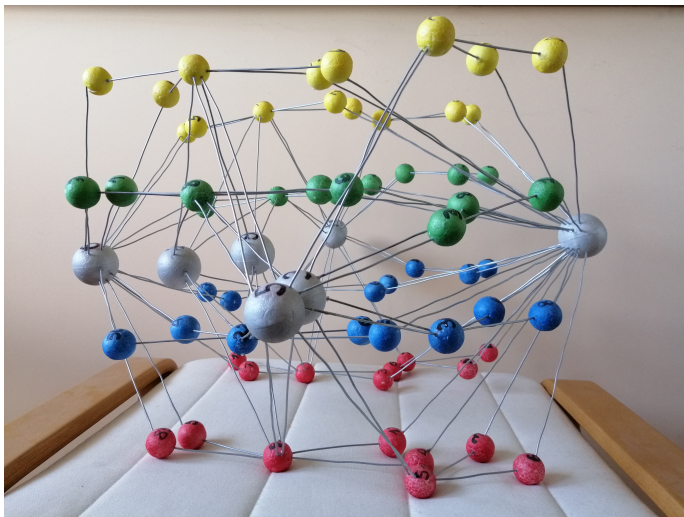
Queste servono a formare lo scheletro a cui agganciare le 4 copie (isomorfe) dei sottogruppi di $\mathbb{Z}_{91}^*$ che hanno un grafo planare

Dove siamo arrivati, II



Questo è uno dei 4 “piani” del grafo di $\mathbb{Z}_{91}^*$. Ciascun piano è isomorfo a $\mathbb{Z}_{35}^*$. I piani hanno in comune le 8 radici quarte dell’unità, che sono 1, 27, 64, 90, 8, 34, 57, 83. Per la costruzione di un modello concreto, c’è il problema tecnico di come agganciare i 4 piani agli elementi comuni

Dove siamo arrivati, III

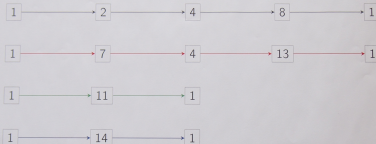


I pannelli preparati per Lucca Comics & Science

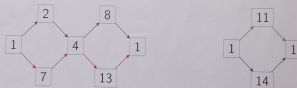
④ Rappresentazione grafica di gruppi finiti

Determinazione delle "catene" quando $n = 15$

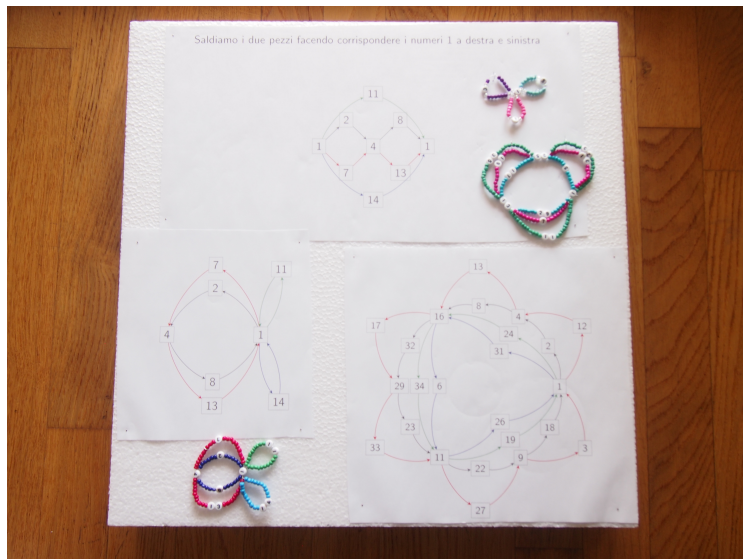
Primo obiettivo: determiniamo le catene che non possono essere ulteriormente estese



Secondo obiettivo: eliminiamo gli elementi ripetuti, cioè 1 e 4, mediante "saldatura" delle catene



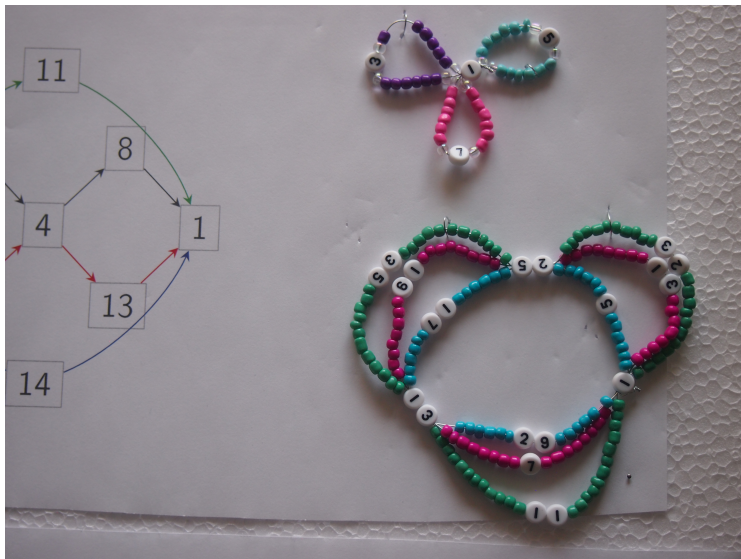
I pannelli preparati per Lucca Comics & Science



I pannelli preparati per Lucca Comics & Science



I pannelli preparati per Lucca Comics & Science



Gli oggetti costruiti dai ragazzi del Liceo Classico



- 1 Preliminari
- 2 Il Teorema di Wilson
- 3 Il Piccolo Teorema di Fermat
- 4 Rappresentazione grafica di gruppi finiti
 - Il gruppo $\mathbb{Z}_n$
 - La tavola pitagorica in $\mathbb{Z}_{12}$
 - La periodicità delle potenze in $\mathbb{Z}_n^*$
 - La tavola pitagorica in $\mathbb{Z}_{15}$
- 5 Costruzione del grafo che rappresenta $\mathbb{Z}_{15}^*$
 - Determinazione delle catene
 - Saldatura delle catene
- 6 Costruzione del grafo che rappresenta $\mathbb{Z}_{35}^*$
 - Determinazione delle catene
 - Saldatura delle catene
 - Completamento della costruzione
- 7 Altri esempi
- 8 Riferimenti

Bibliografia

La prima parte di questa conferenza è illustrata in dettaglio in Cozzani, Sandri & Zaccagnini [1], in fase di completamento; vedi anche l'articolo su "MaddMaths!" [2]

La seconda parte è descritta in dettaglio in Fiorini & Zaccagnini [3] (vedi la versione estesa), dove diamo la costruzione passo per passo del grafo di $\mathbb{Z}_{63}^*$

Un'idea simile, ma in $\mathbb{N}$ anziché in $\mathbb{Z}_n^*$, è descritta nell'articolo [4], apparso su "MaddMaths!" all'inizio del 2020

Sul mio canale YouTube potete trovare i video relativi ad alcune dimostrazioni dei Teoremi di cui abbiamo parlato oggi; si vedano [5], [6], [7], [8]

- [1] Caterina Cozzani, Roberta Sandri, & Alessandro Zaccagnini.

Collane, orecchini e scatolette — Costruzione di oggetti matematici con materiali della vita quotidiana.

Accettato per la pubblicazione – In preparazione, 2024.

- [2] A. Zaccagnini.

Collane, orecchini e ... numeri.

Sito web MaddMaths!, 2022.

<https://maddmaths.simai.eu/divulgazione/collane-e-orecchini/>.

- [3] G. Fiorini & A. Zaccagnini.

Costruzione dei grafi di $\mathbb{Z}_n^*$. Un laboratorio PLS in una classe terza del Liceo Scientifico.

In A. Saracco e A. Zaccagnini, a cura di, *A spasso per la Matematica — PLS 2014–2018*, pages 51–73 & 97–102. CLEUP, Padova, 2018.

Dipartimento di Scienze Matematiche, Fisiche e Informatiche, Università di Parma.

Versione integrale <https://people.dmi.unipr.it/alessandro.zaccagnini/psfiles/papers/fz-integrale.pdf>.

[4] A. Zaccagnini.

Operazioni: elementari, ma non troppo!

Sito web MaddMaths!, 2020.

<https://maddmaths.simai.eu/divulgazione/focus/operazioni-elementari/>.

[5] A. Zaccagnini.

Operazioni: elementari ma non troppo!, 2022.

Conferenza tenuta a Parma l'11.3.2022. Video su YouTube.

<https://youtu.be/r4jf39tYkSw>.

[6] A. Zaccagnini.

Come riconoscere i numeri primi? Il teorema di Wilson, 2020.

Video-pillola su YouTube. <https://youtu.be/mubwg24FJzE>.

[7] A. Zaccagnini.

Il piccolo Teorema di Fermat, 2021.

Video-pillola su YouTube. <https://youtu.be/Zd0BG9ccAN8>.

[8] A. Zaccagnini.

La dimostrazione combinatoria del Teorema di Wilson, 2022.

Video-pillola su YouTube. <https://youtu.be/ctJcNeeEHpY>.

Grazie!

Alessandro Zaccagnini

Dipartimento di Scienze Matematiche, Fisiche e Informatiche

Università di Parma

Parco Area delle Scienze, 53a

Campus Universitario

43124 Parma

`alessandro.zaccagnini@unipr.it`

`https://people.dmi.unipr.it/alessandro.zaccagnini/`

`https://www.youtube.com/c/AlessandroZaccagnini`

`https://twitter.com/AleZaccagnini66`