COSTRUZIONE DEI GRAFI DI $\mathbb{Z}_n^*$. UN LABORATORIO PLS IN UNA CLASSE TERZA DEL LICEO SCIENTIFICO

GIANCARLO FIORINI & ALESSANDRO ZACCAGNINI

1. INTRODUZIONE

In questo articolo descriviamo l'esperienza fatta durante l'Anno Scolastico 2013–2014 con alcuni studenti delle classi terze del Liceo Scientifico "Attilio Bertolucci" di Parma, nell'ambito del Piano Nazionale Lauree Scientifiche (PLS). Il nucleo del gruppo è costituito dalle ragazze che nell'Anno Scolastico precedente hanno partecipato, giovanissime, al laboratorio PLS sul Teorema di Pitagora, mostrando un certo gusto artistico: si è dunque privilegiato un argomento che si presta ad una trattazione "grafica" che permette di far emergere aspetti artistici in senso lato, come apparirà chiaro dai diagrammi che si trovano nelle prossime pagine. Riteniamo che sarebbe stato un peccato disperdere (o frustrare) questo gruppo, che, fra l'altro, è riuscito a far coagulare intorno a sé un discreto numero di altri studenti per un totale di circa 15.

Il nostro obiettivo a lungo termine era quello di proporre un argomento propedeutico alla Crittografia: si veda per esempio Languasco & Zaccagnini [4] per un'esperienza ben rodata nelle classi quarte. Naturalmente, il testo appena citato è improponibile, *in toto*, a questo livello. In definitiva, sia il gruppo che l'argomento erano ben collaudati: in fondo la novità piú appariscente consiste nell'aver cominciato (con metà programma) in una classe terza. Ci sembrava giusto proporre un problema impegnativo ma stimolante, con un obiettivo ambizioso ma del tutto realistico: anche se la scelta può apparire azzardata, in realtà avevamo buoni motivi per essere ottimisti e il risultato finale sembra averci dato ragione.

Veniamo dunque alla scelta dell'argomento proposto: in due parole, si tratta di determinare la struttura moltiplicativa di $\mathbb{Z}_n$ per valori relativamente piccoli di n. Rimandiamo la descrizione dettagliata del percorso didattico al prossimo paragrafo §2. Tra le nostre motivazioni per la scelta dell'argomento proposto agli studenti ci sono le seguenti: uso esclusivo di carta e matita, almeno all'inizio, possibilità di esplorare vari casi semplici e di fare esperimenti numerici, osservare fenomeni, congetturare risultati, e in definitiva scoprire enunciati plausibili, ma tutt'altro che banali. Le congetture possono essere, parzialmente, verificate scegliendo valori diversi del parametro intero n. Possiamo dire di aver suggerito una introduzione molto concreta alla teoria dei gruppi abeliani finiti, in cui gli studenti sono incoraggiati a "sporcarsi le mani," rompendo anche con la tradizionale e datata visione della matematica come scienza "ipotetico-deduttiva" ma sottolineandone l'aspetto sperimentale e, perché no, ludico. La matematica discreta richiede tecniche e idee diverse dalla matematica tradizionalmente insegnata nelle scuole superiori, e si presta ad esperimenti numerici, congetture. Si noti che si tratta, in definitiva, di matematica ad un tempo elementare (iterazione delle moltiplicazioni, divisione con resto e poco altro) e profonda.

Un altro obiettivo è stato quello di far nascere l'esigenza di utilizzare strumenti piú veloci e precisi della carta e della matita. Per prima cosa una calcolatrice tascabile, poi un vero e proprio linguaggio di programmazione come può essere `pari/gp`, un'estensione del C++, che però ha un'interfaccia che ne permette un uso interattivo, come "calcolatrice programmabile" evoluta. In un liceo scientifico vi sono spesso resistenze all'uso delle macchine: nel laboratorio

Data: 22 ottobre 2018.

in esame, gli studenti hanno presto sentito l'esigenza di strumenti piú veloci e precisi di loro stessi.

Ci sono altri aspetti che vogliamo, sia pur concisamente, sottolineare.

- Come in "Game of Life" di John H. Conway, abbiamo un insieme di "regole" molto semplici, che però danno origine a risultati complessi, inaspettati e belli da vedere.
- Non c'è un'unica risposta giusta: il grafo può essere disegnato in tanti modi equivalenti.
- Anche nei casi apparentemente meno interessanti, quelli per cui $\mathbb{Z}_n^*$ è ciclico, il grafo può essere presentato in modo da ricordare degli arabeschi: si veda, ad esempio, la Figura 8 e l'Appendice B.
- Gli studenti sembrano aver apprezzato il fatto che il problema proposto era reale (cioè non "artificiale" o "semplificato"), concreto e impegnativo.

La presentazione dei risultati è avvenuta il giorno 4 giugno 2014 durante il tradizionale appuntamento di fine anno, organizzato presso il Dipartimento di Matematica e Informatica dell'Università di Parma, nel quale gli studenti che hanno partecipato ai laboratori PLS tengono in prima persona un seminario. In un secondo momento, gli studenti hanno realizzato un modello concreto di $\mathbb{Z}_{91}^*$ utilizzando palline di polistirolo colorate, sostegni di filo d'acciaio e vinavil. Per prima cosa hanno sviluppato il progetto dei quattro "piani" del grafo, tappezzando le pareti della loro aula con la "tavola pitagorica" modulo 91 e tutti gli altri schemi necessari alla progettazione del modello. Una volta fatto questo, hanno separatamente costruito i quattro livelli del grafo, ciascuno colorato di un colore diverso, e infine li hanno montati uno alla volta.

Un sentito ringraziamento va a tutti gli studenti che si sono impegnati a fondo nel laboratorio che abbiamo loro suggerito.

Discutiamo del problema in astratto nel §2; nel successivo §3 diamo la parola agli studenti e riportiamo i loro esperimenti e le loro scoperte. Nel §4 costruiamo in dettaglio il grafo planare di $\mathbb{Z}_{35}^*$, e nel §5 parliamo di altre applicazioni possibili di queste tecniche. Nel §6, invece, presentiamo la costruzione del grafo di $\mathbb{Z}_{63}^*$, il "primo" non planare, suggerendo alcune possibili realizzazioni concrete. Gli ultimi paragrafi §§7–9 sono dedicati a proposte, spunti, approfondimenti, letture ulteriori. In appendice riportiamo la semplice costruzione di $\mathbb{Z}_{15}^*$, che può essere considerato un esercizio di riscaldamento, e una breve discussione dei gruppi ciclici. Quella che presentiamo qui è la versione integrale dell'articolo [3], con ulteriori esempi svolti in dettaglio, le figure a colori ed altro materiale.

2. Il problema matematico

Per prima cosa, abbiamo proposto di indagare la struttura di $\mathbb{Z}_n$ per diversi valori relativamente piccoli di n, prima dal punto di vista additivo, poi da quello moltiplicativo, con la costruzione della relativa "tavola pitagorica." Siamo dunque passati al problema matematico che era il nostro vero obiettivo, e cioè la determinazione del grafo che dà la struttura di $\mathbb{Z}_n^*$, usando come strumento principale la determinazione dell'orbita (o ciclo) di ciascuno dei suoi elementi. Per fare questo, abbiamo suggerito alcuni valori di n scelti in un insieme di valori significativi, di grandezza tale da rendere possibile fare i calcoli con carta e penna, oppure con l'ausilio di una calcolatrice tascabile o una di quelle che si trovano fra le applicazioni nei telefoni cellulari o simili dispositivi portatili. Naturalmente, il problema è stato proposto in forma diversa: per la precisione abbiamo proposto di procedere in questo modo

(1) Studio delle proprietà moltiplicative degli elementi di $\mathbb{Z}_n$ e loro classificazione per alcuni valori piccoli ma significativi di n. Introduzione di $\mathbb{Z}_n^*$.
(2) Determinazione dell'orbita di ogni elemento m di $\mathbb{Z}_n^*$, e cioè l'insieme $\langle m\rangle = \{m^i : i \in \mathbb{N}\} \subseteq \mathbb{Z}_n^*$. Ulteriore classificazione degli elementi di $\mathbb{Z}_n^*$ in base al loro ordine, cioè $|\langle m\rangle|$.

(3) Riflessione sul fatto che le orbite hanno elementi in comune, e che alcune ne contengono altre.
(4) Determinazione delle orbite massimali, che non possono essere ampliate ulteriormente.
(5) "Saldatura" delle orbite, operazione che permette di presentare il gruppo $\mathbb{Z}_n^*$ in modo visibile.

L'obiettivo non dichiarato di un approccio "sperimentale" a questo problema è la possibile scoperta di proprietà importanti dei gruppi $\mathbb{Z}_n^*$ quali il Piccolo Teorema di Fermat, il Teorema di Eulero, il Teorema di Gauss, cose che si è puntualmente, anche se parzialmente, verificata.

Per concretezza, illustreremo dettagliatamente i passaggi della costruzione vera e propria nel caso in cui $n = 35$ nel §4, con possibili estensioni nel §5. Nel §6 diamo per sommi capi la costruzione, piuttosto impegnativa, del grafo di $\mathbb{Z}_{63}^*$, che richiede l'uso della terza dimensione. Prima però diamo i valori effettivamente usati in classe nel §3, con i commenti relativi e una discussione delle criticità emerse, lasciando la parola agli studenti e ai loro esperimenti, le loro scoperte e i loro problemi.

3. Il diario degli incontri

Dopo una introduzione alle classi di resto modulo n abbiamo analizzato alcuni insiemi $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. In particolare abbiamo calcolato $a^i \bmod n$ ($\forall i \in \mathbb{Z}_n$). Visti i valori che si ottengono, abbiamo eliminato, inizialmente, 0 ed 1. I calcoli sono stati effettuati con la calcolatrice con evidenti problemi di tempo e di facilità di errore. A questo punto sono state introdotte le proprietà delle congruenze:

$$\forall c \in \mathbb{Z} \text{ si ha} \quad a \equiv b \bmod n \quad \Longrightarrow \quad a+c \equiv b+c \bmod n, \quad ac \equiv bc \bmod n.$$

Applicando tali proprietà abbiamo reso piú rapido il calcolo. Vediamo di seguito le tabelle relative ai valori di $n = 8, 11, 12, 16, 21, 26, 31, 37$ studiati in classe.

3.1. $n = 8$. Si veda la Figura 1, parte sinistra. Osservazione: le potenze dei numeri 3, 5, 7 si ripetono in modo ciclico mentre per gli altri numeri ciò non avviene.

	0	1	2	3	4	5	6	7
2	1	2	4	0	0	0	0	0
3	1	3	1	3	1	3	1	3
4	1	4	0	0	0	0	0	0
5	1	5	1	5	1	5	1	5
6	1	6	4	0	0	0	0	0
7	1	7	1	7	1	7	1	7

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

Figura 1. A sinistra la tavola delle potenze in $\mathbb{Z}_8$, a destra in $\mathbb{Z}_{11}$.

3.2. $n = 11$. Si veda la Figura 1, parte destra. Osservazioni:

- le potenze dei numeri 2, 6, 7, 8 ripetono tutti i numeri dell'insieme
- le potenze dei rimanenti numeri si ripetono ciclicamente
- le potenze dei numeri 3, 4, 5, 9 ripetono, oltre al numero 1, i numeri stessi anche se in ordini diversi
- il numero 10 ripete sé stesso e l'unità
- tutti i numeri elevati alla potenza 10 sono congruenti a 1.

3.3. $n = 12$. Si veda la Figura 2, parte sinistra. Osservazioni:

- le potenze dei numeri 5, 7, 11 si ripetono ciclicamente
- le potenze dei numeri 2, 3, 8 ripetono una sequenza che contiene il numero 1 solo all'inizio e i numeri ripetuti sono due.

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

	0	1	2	3	4	5	6	7	8	9
2	1	2	4	8	0	0	0	0	0	⋯
3	1	3	9	11	1	3	9	11	1	⋯
4	1	4	0	0	0	0	0	0	0	⋯
5	1	5	9	3	1	5	9	3	1	⋯
6	1	6	4	8	0	0	0	0	0	⋯
7	1	7	1	7	1	7	1	7	1	⋯
8	1	8	0	0	0	0	0	0	0	⋯
9	1	9	1	9	1	9	1	9	1	⋯
10	1	10	4	8	0	0	0	0	0	⋯
11	1	11	9	3	1	11	9	3	1	⋯
12	1	12	0	0	0	0	0	0	0	⋯
13	1	13	9	5	1	13	9	5	1	⋯
14	1	14	4	8	0	0	0	0	0	⋯
15	1	15	1	15	1	15	1	15	1	⋯

FIGURA 2. A sinistra la tavola delle potenze in $\mathbb{Z}_{12}$, a destra in $\mathbb{Z}_{16}$.

3.4. $n = 16$. Poi abbiamo $n = 16$ (cfr Figura 2, a destra). Osservazioni:

- le potenze dei numeri 3, 5, 7, 9, 11, 13, 15 si ripetono ciclicamente
  - 3, 5, 11, 13 con periodo 4
  - 7, 9, 15 con periodo 2
- l'unione dei vari cicli coincide con i numeri del punto precedente.

3.5. $n = 21$. Per $n = 21$ si veda la Figura 3. Osservazioni

- le potenze dei numeri 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20 si ripetono ciclicamente
  - 2, 10, 11, 17, 19 con periodo 6
  - 4, 5, 16 con periodo 3
  - 8, 13, 20 con periodo 2
- l'unione dei vari cicli coincide con i numeri del punto precedente.

3.6. $n = 26$. Si veda la Figura 4. Osservazioni

- le potenze dei numeri 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 si ripetono ciclicamente
  - 7, 11, 15, 19 con periodo 12
  - 17, 23 con periodo 6
  - 5, 21 con periodo 4
  - 3, 9 con periodo 3
  - 25 con periodo 2.

3.7. $n = 31$. Si veda la Figura 5. Osservazioni

- le potenze di tutti i numeri si ripetono ciclicamente
  - 3, 11, 12, 13, 17, 21, 22, 24 con periodo 30
  - 7, 9, 10, 14, 18, 19, 20, 28 con periodo 15
  - 15, 23, 27, 29 con periodo 10
  - 6, 26, con periodo 6

	0	1	2	3	4	5	6	7	8
2	1	2	4	8	16	11	1	$\cdots$	
3	1	3	9	6	18	12	15	3	$\cdots$
4	1	4	16	1	$\cdots$				
5	1	5	4	1	$\cdots$				
6	1	6	15	6	15	$\cdots$			
7	1	7	7	7	7	$\cdots$			
8	1	8	1	8	$\cdots$				
9	1	9	18	15	9	18	15	$\cdots$	
10	1	10	16	13	4	19	1	$\cdots$	
11	1	11	16	8	4	2	1	$\cdots$	
12	1	12	18	6	9	3	15	12	$\cdots$
13	1	13	1	13	$\cdots$				
14	1	14	7	14	$\cdots$				
15	1	15	15	$\cdots$					
16	1	16	4	1	$\cdots$				
17	1	17	16	20	4	5	1	$\cdots$	
18	1	18	9	15	18	$\cdots$			
19	1	19	4	13	16	10	1	$\cdots$	
20	1	20	1	20	1	$\cdots$			

FIGURA 3. La tavola delle potenze in $\mathbb{Z}_{21}$.

  - 2, 4, 8, 16 con periodo 5
  - 5, 25 con periodo 3
  - 30 con periodo 2
- $\forall\, a \in \mathbb{Z}_{31},\ a^{30} \equiv 1 \mod 31$.

Dall'analisi delle tabelle si è osservato che per i numeri primi tutti i numeri dell'insieme si ripetono ciclicamente mentre per gli altri solo i numeri primi col numero della classe si ripetono ciclicamente. Di conseguenza abbiamo creato nuove classi residuali chiamate $\mathbb{Z}_n^*$ e contenenti solo i numeri primi con n. Queste nuove classi hanno la caratteristica di essere tutte cicliche (le loro potenze si ripetono periodicamente tornando sempre al punto di partenza, e cioè 1) e i periodi dei numeri che la compongono sono tutti i divisori della cardinalità della classe.

L'esecuzione dei calcoli con penna, carta e calcolatrice tascabile è stata lunga e difficoltosa e con un'alta probabilità di errore. Per il calcolo del resto della divisione $\frac{a}{b} = k$ con $k \in \mathbb{R}$, non essendo in possesso della funzione Mod, abbiamo moltiplicato la parte decimale di k per b. In tal modo abbiamo notato che per numeri elevati la calcolatrice non restituisce un resto intero ma approssimato. Ad esempio

$$2^{30} : 31 = 1073741824 : 31 = 34636833.032258 \qquad \text{e}$$
$$0.032258 \cdot 31 = 0.999998.$$

Se il tedio prodotto dai numerosi calcoli ci ha indotti, in alcuni casi, ad abbandonarli, ci ha anche costretti ad escogitare operazioni, metodi, "scappatoie" per poterli ridurre al minimo. In tale direzione, dunque, abbiamo osservato che:

Osservazione 1. *Se n è un numero primo ed abbiamo superato la metà delle potenze senza avere mai trovato resto* 1*, allora sicuramente troveremo* 1 *per il resto di* a^{n-1} *e non prima.*

La spiegazione di questo risultato ci è rimasta oscura fino a che non abbiamo notato un altro fatto rilevante. Innanzitutto non tutti i numeri appartenenti a $\mathbb{Z}_n$ sono "significativi." Alcuni

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	1	2	4	8	16	6	12	24	22	18	10	20	14	2	$\cdots$
3	1	3	9	1	$\cdots$										
4	1	4	16	12	10	14	4	$\cdots$							
5	1	5	25	21	1	$\cdots$									
6	1	6	10	8	22	2	12	20	16	18	4	24	14	6	$\cdots$
7	1	7	23	5	9	11	25	19	3	21	17	15	1	$\cdots$	
8	1	8	12	18	14	8	$\cdots$								
9	1	9	3	1	$\cdots$										
10	1	10	22	12	16	4	14	10	$\cdots$						
11	1	11	17	5	3	7	25	15	9	21	23	19	1	$\cdots$	
12	1	12	14	12	$\cdots$										
13	1	13	13	$\cdots$											
14	1	14	14	$\cdots$											
15	1	15	17	21	3	19	25	11	9	5	23	7	1	$\cdots$	
16	1	16	22	14	16	$\cdots$									
17	1	17	3	25	9	23	1	$\cdots$							
18	1	18	12	8	14	18	$\cdots$								
19	1	19	23	21	9	15	25	7	3	5	17	11	1	$\cdots$	
20	1	20	10	18	22	24	12	6	16	8	4	2	14	20	$\cdots$
21	1	21	25	5	1	$\cdots$									
22	1	22	16	14	22	$\cdots$									
23	1	23	9	25	3	17	1	$\cdots$							
24	1	24	4	18	16	20	12	2	22	8	10	6	14	24	$\cdots$
25	1	25	1	$\cdots$											

FIGURA 4. La tavola delle potenze in $\mathbb{Z}_{26}$.

di essi si comportano in modo "strano" e cioè ripetono ciclicamente una serie di numeri senza ripetere il numero 1 (vedi §5.1). Questi numeri hanno la caratteristica di non essere primi con n. Abbiamo, quindi, creato la classe $\mathbb{Z}_n^*$ contenente solo i numeri primi con n, come già ricordato sopra. In seguito alla necessità di procedere piú rapidamente alla costruzione di ulteriori classi è stato introdotto il linguaggio `pari/gp`. Questo linguaggio può essere utilizzato anche come una potente calcolatrice. Le prime operazioni usate sono state le seguenti:

`+`	somma	`*`	prodotto
`-`	sottrazione	`\`	divisione intera
`/`	divisione sotto forma di frazione	`^`	potenza
`gcd(a, b)`	Massimo Comun Divisore	`%`	modulo
`./`	divisione con decimali		

Nonostante la potenza di questa nuova calcolatrice, per ottenere rapidamente le tabelle da studiare scritte in un formato facile da analizzare, sono stati necessari altri strumenti: le "strutture di controllo" in modo da poter costruire degli algoritmi.

- Selezione binaria:
  `if(<condizione>,<istr. se vero>,<istr. se falso>)`
- Ciclo iterativo:
  `for(<var>=<inizio>,<fine>,<istruzioni>)`

Ecco una sequenza di istruzioni utilizzate prima di giungere alla sintesi finale. In queste istruzioni sono state inserite anche le funzioni con parametri.

```
gp> for(i=0, 29, print(13^i % 30))
```

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
2	1	2	4	8	16	1	⋯																								1
3	1	3	9	27	19	26	16	17	20	29	25	13	8	24	10	30	28	22	4	12	5	15	14	11	2	6	18	23	7	21	1
4	1	4	16	2	8	1	⋯																							⋯	1
5	1	5	25	1	⋯																									⋯	1
6	1	6	5	30	25	26	1	⋯																						⋯	1
7	1	7	18	2	14	5	4	28	10	8	25	20	16	19	9	1	⋯													⋯	1
8	1	8	2	16	4	1	⋯																							⋯	1
9	1	9	19	16	20	25	8	10	28	4	5	14	2	18	7	1	⋯													⋯	1
10	1	10	7	8	18	25	2	20	14	16	5	19	4	9	28	1	⋯													⋯	1
11	1	11	28	29	9	6	4	13	19	23	5	24	16	21	14	30	20	3	2	22	25	27	18	12	8	26	7	15	10	17	1
12	1	12	20	23	28	26	2	24	9	15	25	21	4	17	18	30	19	11	8	3	5	29	7	22	16	6	10	27	14	13	1
13	1	13	14	27	10	6	16	22	7	29	5	3	8	11	19	30	18	17	4	21	25	15	9	24	2	26	28	23	20	12	1
14	1	14	10	16	7	5	8	19	18	4	25	9	2	28	20	1	⋯													⋯	1
15	1	15	8	27	2	30	16	22	4	29	1	⋯																		⋯	1
16	1	16	8	4	2	1	⋯																							⋯	1
17	1	17	10	15	7	26	8	12	18	27	25	22	2	3	20	30	14	21	16	24	5	23	19	13	4	6	9	29	28	11	1
18	1	18	14	4	10	25	16	9	7	2	5	28	8	20	19	1	⋯													⋯	1
19	1	19	20	8	28	5	2	7	9	16	25	10	4	14	18	1	⋯													⋯	1
20	1	20	28	2	9	25	4	18	19	8	5	7	16	10	14	1	⋯													⋯	1
21	1	21	7	23	18	6	2	11	14	15	5	12	4	22	28	30	10	24	8	13	25	29	20	17	16	26	19	27	9	3	1
22	1	22	19	15	20	6	8	21	28	27	5	17	2	13	7	30	9	12	16	11	25	23	10	3	4	26	14	29	18	24	1
23	1	23	2	15	4	30	8	29	16	27	1	⋯																		⋯	1
24	1	24	18	29	14	26	4	3	10	23	25	11	16	12	9	30	7	13	2	17	5	27	28	21	8	6	20	15	19	22	1
25	1	25	5	1	⋯																									⋯	1
26	1	26	25	30	5	6	1	⋯																						⋯	1
27	1	27	16	29	8	30	4	15	2	23	1	⋯																		⋯	1
28	1	28	9	4	19	5	16	14	20	2	25	18	8	7	10	1	⋯													⋯	1
29	1	29	4	22	16	30	2	27	8	15	1	⋯																		⋯	1
30	1	30	1	⋯																										⋯	1

FIGURA 5. La tavola delle potenze in $\mathbb{Z}_{31}$.

```
gp> f(a)=for(i=0, 29, print(a^i % 30))
gp> f(a,n)=for(i=0, n-1, print(a^i % n))
gp> f(a,n)=print1(a,"\t");
    for(i=0, n-1, print1(a^i % n, "\t")); print()
gp> g(n)=for(j=2, n-1, f(j,n))
gp> espon(n)=print1("\t");
    for(j=0, n-1, print1(j,"\t"));print();
gp> g(n)=espon(n);for(j=2, n-1, f(j,n))
```

La funzione `g(n)` ci fornisce la tabella contenente tutti i resti di

$$a^k \bmod n \qquad \forall a \in \mathbb{Z}_n \text{ con } k = 0, \ldots, n-1.$$

Ma il nostro obiettivo è di costruire la classe $\mathbb{Z}_n^*$ quindi dobbiamo considerare solo i numeri primi con n. Modifichiamo la funzione `f(a, n)`.

```
gp> f(a,n)=if(gcd(a,n)==1,print1(j,"\t");
    for(i=0, n-1, print1(a^i % n, "\t"));print())
```

L'obiettivo finale, però, è la rappresentazione della tabella in un file di testo (.txt) oppure in un foglio elettronico (.ods, .xls). Costruiamo le nuove funzioni sulla base delle precedenti assegnando la possibilità di scegliere il tipo di file e parametrizzando il nome del file. Per assolvere a tale compito costruiamo un'altra funzione.

```
gp> Znf(n,est)=Str("Z",n,".",est)
```

A questo punto scriviamo le altre funzioni.

```
gp> Zespon(n,est)=write1(Znf(n,est),"\t");
    for(j=0, n-1, write1(Znf(n,est),j,"\t"));
    write(Znf(n,est),"")
gp> Zf(a,n,est)=if(gcd(a,n)==1,write1(Znf(n,est),j,"\t");
    for(i=0, n-1, write1(Znf(n,est),a^i % n, "\t"));
    write())
gp> Z(n,est)=Zespon(n,est);for(j=2, n-1, Zf(j,n,est))
```

Nelle tabelle cosí generate è stato piú facile determinare gli ordini dei cicli, che si sono rivelati essere sottomultipli della cardinalità $\varphi(n)$ di $\mathbb{Z}_n^*$. A questo punto è risultata chiara la spiegazione dell'Osservazione 1. Anche la fase della costruzione dei grafi (descritta nei prossimi paragrafi) è stata piú agevole, pur non essendo mai facile. A questo punto abbiamo proceduto alla costruzione di grafi per mostrare la concatenazione tra i numeri della classe.

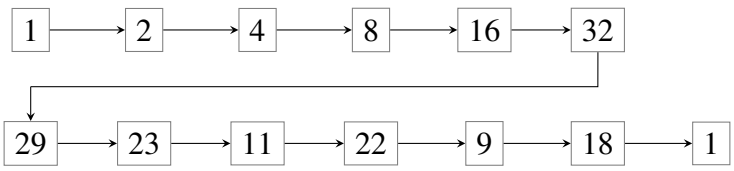
3.8. **Il punto della situazione.** Riprendiamo brevemente la parola per dire che gli studenti hanno notato che il calcolo delle potenze successive di un elemento di $\mathbb{Z}_n^*$ può essere abbreviato utilizzando una relazione di ricorrenza, come faremo qui sotto nel prossimo paragrafo. Inoltre hanno "scoperto" che, talvolta, i risultati delle calcolatrici non sono esatti ma approssimati e che calcolatrici diverse possono dare risultati diversi (il fenomeno è discusso criticamente in [8]). Infine hanno scoperto il Piccolo Teorema di Fermat e che due gruppi $\mathbb{Z}_n^*$ e $\mathbb{Z}_m^*$ con n ed m diversi fra loro possono appartenere alla stessa classe di isomorfismo, cioè, nel linguaggio usato nel laboratorio, avere lo stesso grafo.

4. La costruzione dei grafi: il caso $n = 35$

Descriveremo la costruzione del grafo relativo al gruppo $\mathbb{Z}_{35}^*$, supponendo che la relativa tavola pitagorica sia già stata creata. Nel paragrafo A diamo tutti i dettagli della costruzione, molto piú semplice, del grafo relativo a $\mathbb{Z}_{15}^*$.

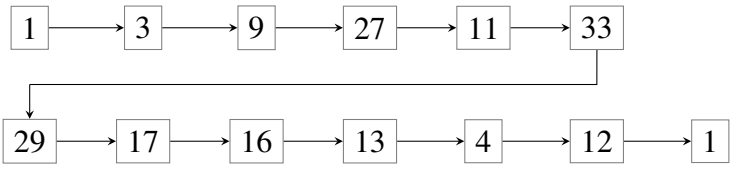
4.1. **Prima fase.** Cominciamo prendendo un elemento $m \in \mathbb{Z}_{35}^*$ e ne calcoliamo le potenze successive ridotte modulo 35. Questo primo passo può essere realizzato molto semplicemente, in generale, utilizzando la tavola pitagorica di $\mathbb{Z}_n^*$, se è già stata costruita, o mediante la relazione di ricorrenza $m^{i+1} = m^i \cdot m$ riducendo poi i risultati $\bmod n$. In questo modo i risultati intermedi non superano mai n^2.

Dato che, evidentemente, $m = 1$ non dà origine a nulla di interessante, prendiamo $m = 2$, che è primo con 35. Otteniamo dunque la "catena" (cioè, in termini algebrici precisi, l'orbita o ciclo relativo ad m)



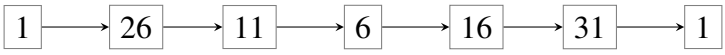
Per comodità, indichiamo l'insieme cosí trovato con $\langle 2 \rangle$ (il sottogruppo di $\mathbb{Z}_{35}^*$ generato da 2): è opportuno notare che, per esempio, $\langle 2 \rangle = \langle 18 \rangle$ poiché $18 \equiv 2^{-1} \bmod 35$. Gli studenti sono invitati a riconoscere che la catena si chiude ad anello, tornando al punto iniziale, e che questa catena non contiene *tutti* gli elementi di $\mathbb{Z}_{35}^*$. In realtà, quest'ultima cosa può accadere per alcuni n, cioè quelli per cui $\mathbb{Z}_n^*$ è un gruppo ciclico ed m è un generatore (si vedano i commenti nel §7). Stando cosí le cose, prendiamo $m \in \mathbb{Z}_{35}^* \setminus \langle 2 \rangle$ e determiniamo la relativa catena: in

pratica scegliamo il piú piccolo intero che non appartiene a $\langle 2 \rangle$, e cioè $m = 3$:



Gli studenti sono invitati a riconoscere che anche questa catena si chiude ad anello, tornando al punto iniziale, che questa catena non contiene *tutti* gli elementi di $\mathbb{Z}_{35}^*$, ma ha diversi elementi in comune con la precedente, a parte 1, come è ovvio. Questi elementi comuni (1, 4, 16, 29, 11, 9) non compaiono nello stesso ordine in cui si trovano in $\langle 2 \rangle$, ma in ordine inverso: questo sarà rilevante per la seconda fase. Prendiamo ora un nuovo elemento $m \in \mathbb{Z}_{35}^* \setminus (\langle 2 \rangle \cup \langle 3 \rangle)$: scegliamo $m = 19$ e otteniamo la catena

Poiché non abbiamo finito, prendiamo ancora un elemento $m \in \mathbb{Z}_{35}^* \setminus (\langle 2 \rangle \cup \langle 3 \rangle \cup \langle 19 \rangle)$:

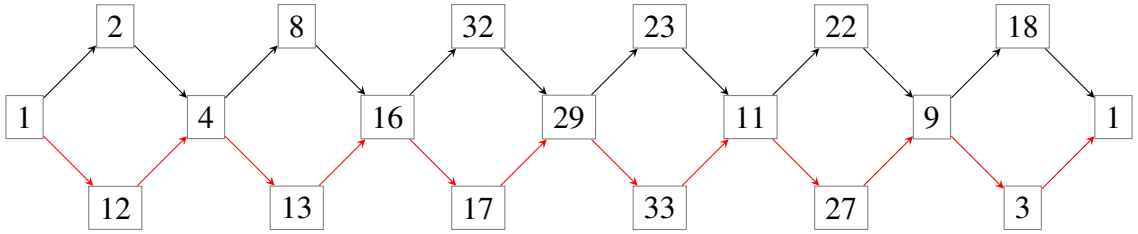


A questo punto abbiamo trovato *tutti* gli elementi di $\mathbb{Z}_{35}^*$ e quattro catene, che hanno elementi in comune ma non sono contenute una nell'altra. Ribadiamo che ciascuna catena può essere letta equivalentemente verso destra o verso sinistra: questo è un aspetto cruciale della costruzione al passo seguente.

4.2. **Seconda fase.** Resta il problema di "saldare" queste catene per ottenere una presentazione del gruppo $\mathbb{Z}_{35}^*$ che ne renda visibile la struttura emersa dai calcoli. Dal punto di vista pratico, conviene disporre per prime le catene "lunghe" e poi quelle piú corte, individuando le ripetizioni degli elementi ed eliminandole tutte fino ad ottenere il grafo cercato. Conviene cominciare incollando per primi gli elementi di molteplicità bassa, lasciando per ultimo in numero 1 che compare due volte in ciascuna catena. Notiamo esplicitamente che per fare questo dobbiamo lasciare il dominio unidimensionale usato finora, passando inizialmente a 2 ed eventualmente a 3 dimensioni.

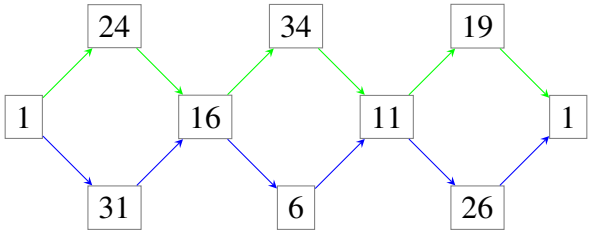
Per prima cosa saldiamo $\langle 2 \rangle$ con $\langle 3 \rangle$ (scritta al contrario), poi saldiamo $\langle 19 \rangle$ con $\langle 26 \rangle$ e infine salderemo insieme i due pezzi. I diversi colori dei segmenti orientati nei disegni che seguono servono a distinguere i fattori: il colore nero indica la moltiplicazione per 2, il rosso la moltiplicazione per 12, il verde per 24 e infine il blu per 31.

Nel disegno che segue siamo partiti dalla catena generata da 2: le frecce nere indicano la moltiplicazione per 2 in $\mathbb{Z}_{35}^*$. Questo ci dà la struttura portante a cui agganciare il resto della figura. Poi abbiamo inserito la catena generata da 12 (frecce rosse) tenendo conto del fatto che alcuni dei suoi elementi (la metà) sono già presenti nella catena precedente.

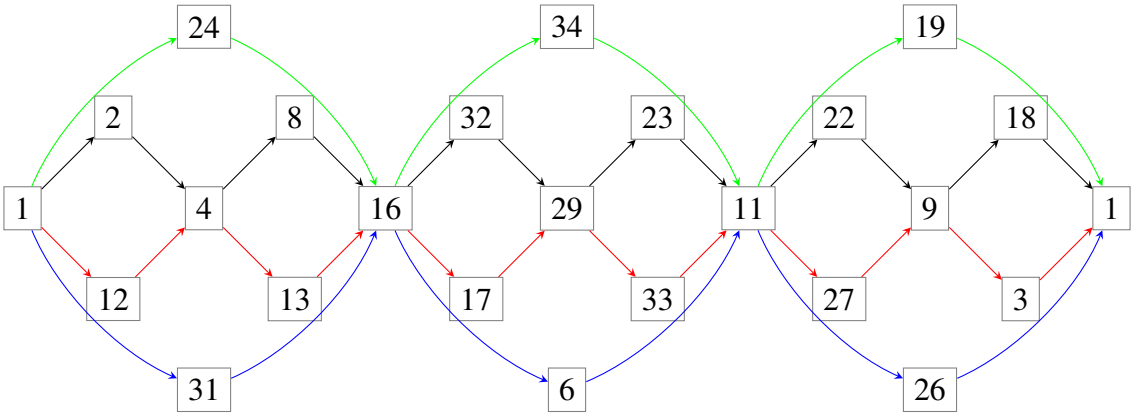


Gli ultimi due passi richiedono di inserire le catene relative a 24 (frecce verdi) e 31 (frecce blu). Saldiamo dunque le catene corte ai loro punti di contatto: per facilitare l'operazione successiva di saldatura alla struttura già trovata, montiamo le catene al contrario di come le abbiamo ottenute. Il motivo dovrebbe essere ormai chiaro: nella figura qui sopra gli elementi

di contatto sono, nell'ordine, 1, 16, 11 e di nuovo 1, e la saldatura può avvenire correttamente solo se questi elementi compaiono nello stesso ordine anche qui sotto.



Infine saldiamo i due disegni precedenti tenendo conto degli elementi comuni 1, 16 e 11:

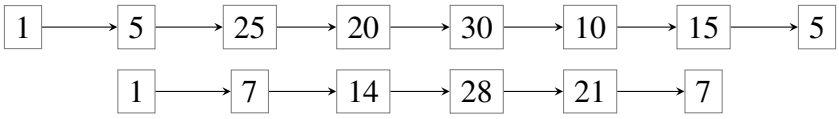


4.3. **Terza fase.** Possiamo ora concludere le operazioni "incollando" le due estremità del disegno qui sopra, che corrispondono all'elemento 1. In definitiva, possiamo presentare $\mathbb{Z}_{35}^*$ come mostrato nella Figura 6. Non è evidente a priori che la figura che otteniamo possa essere disegnata restando nel piano: in effetti, questo accade solo per alcuni valori di n.

5. Applicazioni ed estensioni

Proponiamo qui alcune possibili estensioni e applicazioni delle tecniche introdotte sopra, al di là del lavoro effettivamente svolto in classe. Parleremo degli elementi non invertibili, che finora abbiamo trascurato; dei gruppi ciclici, i meno interessanti dal nostro punto di vista perché hanno un grafo molto semplice, ma che possono essere presentati in piú modi; dell'Algoritmo di Gauss per determinare un generatore di $\mathbb{Z}_p^*$ quando p è un numero primo.

5.1. **Il ruolo degli elementi non invertibili.** Studiamo a parte quello che succede calcolando le potenze successive degli elementi non invertibili, e cioè degli $m \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$. Naturalmente possiamo supporre $m \neq 0$. Quando $n = 35$, per $m = 5$ ed $m = 7$ rispettivamente troviamo le due catene



Notiamo esplicitamente che *non è possibile* tornare ad 1 come nelle catene studiate in precedenza. Queste danno origine ai due grafici nella Figura 7.

5.2. **Esempio di gruppo ciclico: $n = 13$.** Ci limitiamo a dare un disegno di quanto accade in questa situazione, piuttosto lontana dai casi graficamente "interessanti" discussi nel resto di questo articolo: si veda la Figura 8. Una discussione piú dettagliata con presentazioni alternative si trova nel paragrafo B.

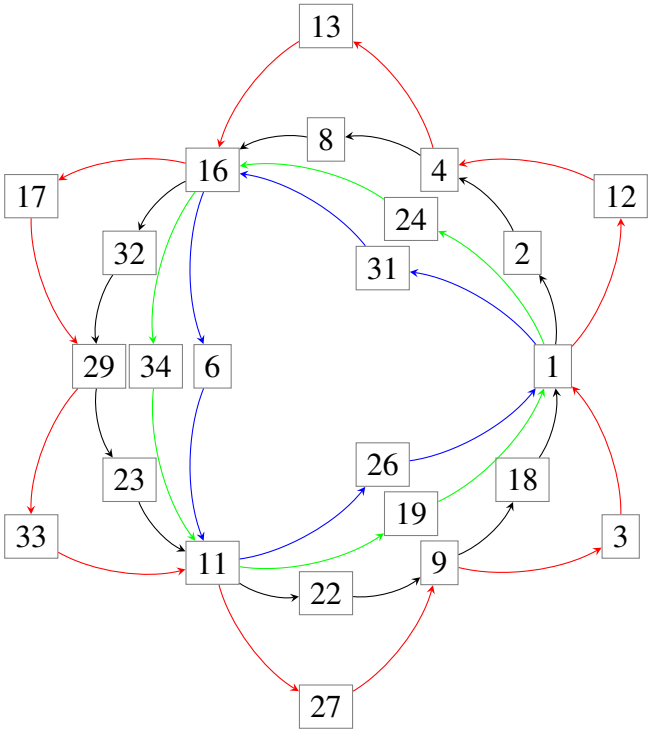


FIGURA 6. La presentazione di $\mathbb{Z}_{35}^*$. Abbiamo disposto la catena relativa a $\langle 31 \rangle$ all'interno della figura, invece che all'esterno, per motivi estetici

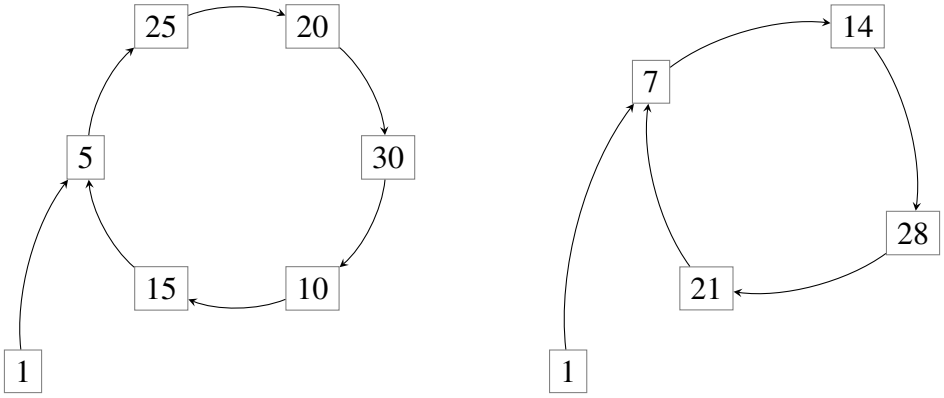


FIGURA 7. Notare la somiglianza, non casuale, con i numeri decimali periodici (con eventuale antiperiodo), con la tipica figura a forma di ρ

5.3. **Il Teorema e l'Algoritmo di Gauss.** La costruzione proposta consiste nel determinare per primi gli elementi di ordine alto, per individuare lo scheletro su cui costruire (agganciare) le altre catene di lunghezza minore. Procedendo in modo diverso, si può ricostruire l'Algoritmo di Gauss per la determinazione di un generatore di $\mathbb{Z}_p^*$ quando p è un numero primo, nel quale caso sappiamo che il gruppo è ciclico (per il Teorema omonimo). L'Algoritmo richiede la determinazione di catene come quelle descritte sopra, incollandole fra loro fino ad ottenere una catena "massimale." In un certo senso, stiamo ribaltando il punto di vista precedente: prima partivamo dalla determinazione di catene non ampliabili, mentre ora partiamo da catene che sappiamo a priori che non sono massimali. Ad ogni passo, l'algoritmo produce una catena piú lunga della precedente fino a determinarne una di lunghezza $p-1$.

Ci limitiamo ad illustrare l'Algoritmo di Gauss per mezzo di un esempio quando $p = 43$.

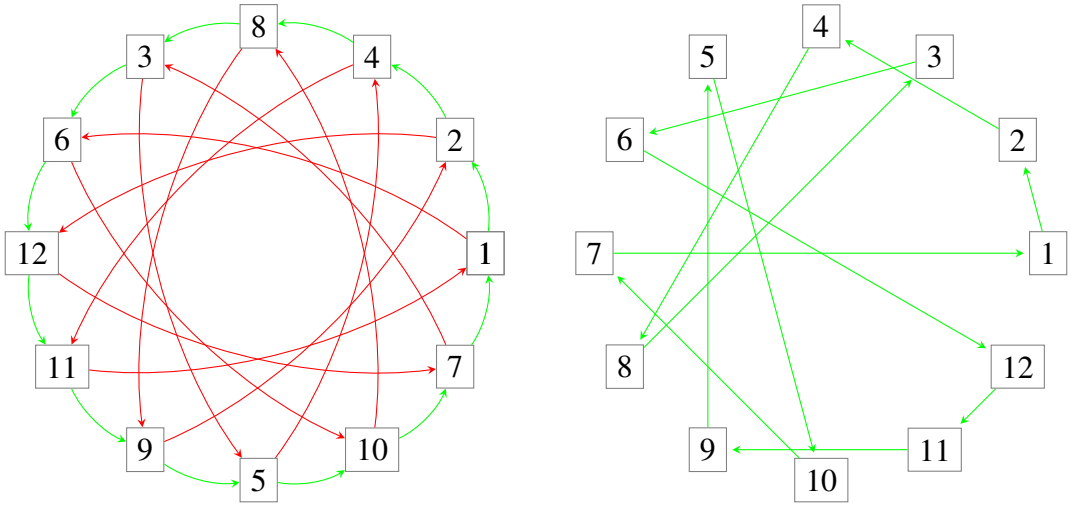
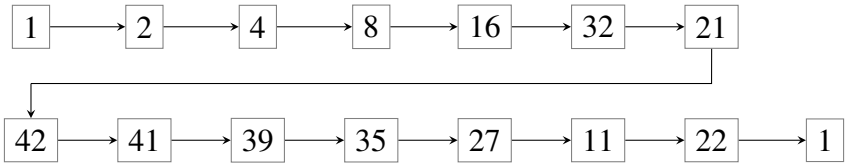
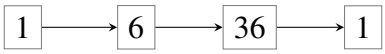


FIGURA 8. Alcuni modi per presentare il grafo del gruppo ciclico $\mathbb{Z}_{13}^*$: a sinistra, i generatori sono 2 (frecce verdi), 7 (frecce verdi, lette al contrario), 6 (frecce rosse) e 11 (frecce rosse, lette al contrario). A destra il generatore è 2, oppure 7 leggendo le frecce al contrario

Cominciamo determinando $\langle 2 \rangle$:



Poiché $\langle 2 \rangle$ non esaurisce $\mathbb{Z}_{43}^*$, prendiamo un elemento $m \in \mathbb{Z}_{43}^* \setminus \langle 2 \rangle$: in particolare scegliamo $m = 6$ e ne determiniamo la relativa catena.



La catena trovata, lungi dall'essere massimale, è addirittura piú corta della precedente. Apparentemente abbiamo fallito due volte. L'idea fondamentale dell'algoritmo di Gauss, invece, è che è possibile utilizzare l'informazione parziale ottenuta finora per determinare un elemento $a \in \mathbb{Z}_{43}^*$ con le due proprietà seguenti:

(1) $\langle a \rangle$ ha cardinalità *maggiore* di $\max\{|\langle 2 \rangle|, |\langle 6 \rangle|\}$;
(2) $\langle a \rangle \supset (\langle 2 \rangle \cup \langle 6 \rangle)$.

In altre parole, le potenze consecutive di a "interpolano" sia le potenze di 2 che quelle di 6. Per la precisione, l'ordine di a è il minimo comune multiplo degli ordini di 2 e di 6 (e dunque vale 42): l'ipotesi $m \in \mathbb{Z}_{43}^* \setminus \langle 2 \rangle$ serve a garantire che questo minimo comune multiplo sia maggiore in senso stretto dei due ordini calcolati in precedenza.

L'elemento a può essere calcolato a partire da 2 e da 6 prendendone opportune potenze. Ricicliamo dunque l'intera informazione trovata in precedenza. In questo caso particolare, l'algoritmo di Gauss fornirebbe il generatore $12 \equiv 2 \cdot 6 \bmod 43$: qui abbiamo scelto il generatore $34 \equiv 12^5 \bmod 43$ per coerenza con la figura. Il piú piccolo generatore, in realtà, è 3. In generale, è necessario iterare piú volte questa costruzione, ottenendo ad ogni passo elementi di ordine sempre piú grande, fino ad ottenere un generatore.

5.4. **Alcuni valori interessanti.** Proponiamo alcuni valori interessanti di n con i grafi relativi. Il caso $n = 15$ è illustrato a sinistra nella Figura 10 e non sono necessari particolari commenti. Per $n = 24$ si veda la parte destra della Figura 10; questo è il caso piú lontano dalla ciclicità:

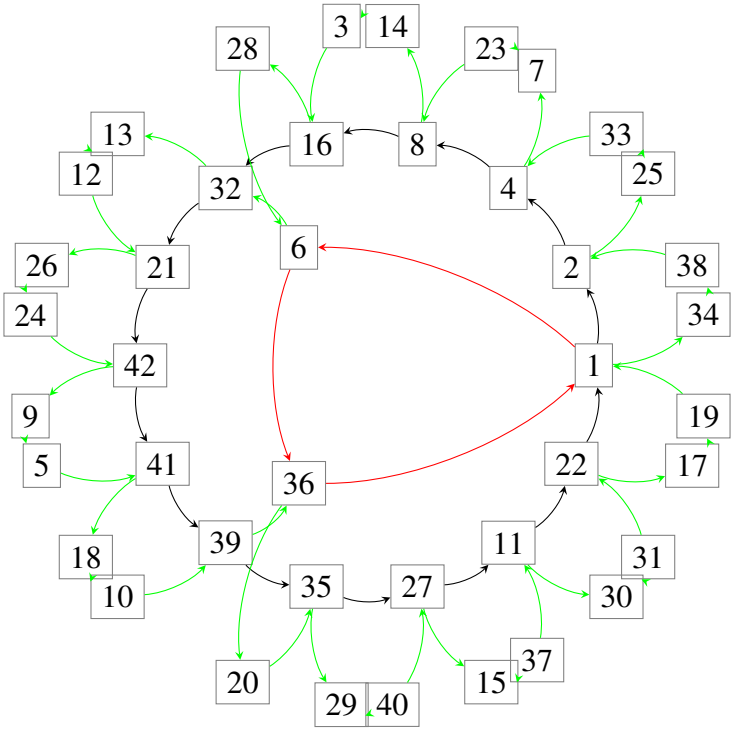


FIGURA 9. La costruzione di un generatore di $\mathbb{Z}_{43}^*$ mediante l'Algoritmo di Gauss. Le potenze di 34 (indicate dalle frecce verdi) "interpolano" sia quelle di 2 (frecce nere) sia quelle di 6 (frecce rosse)

tutti gli elementi di $\mathbb{Z}_{24}^*$ hanno ordine 1 o 2. Quando $n = 36$ (cfr la Figura 11 a sinistra) si può notare che $\mathbb{Z}_{36}^* \simeq \mathbb{Z}_{21}^*$, e quindi hanno lo stesso grafo (a parte le etichette dei nodi). Il valore $n = 40$, nella parte destra della Figura 11, dà un grafico simile a quello relativo ad $n = 24$.

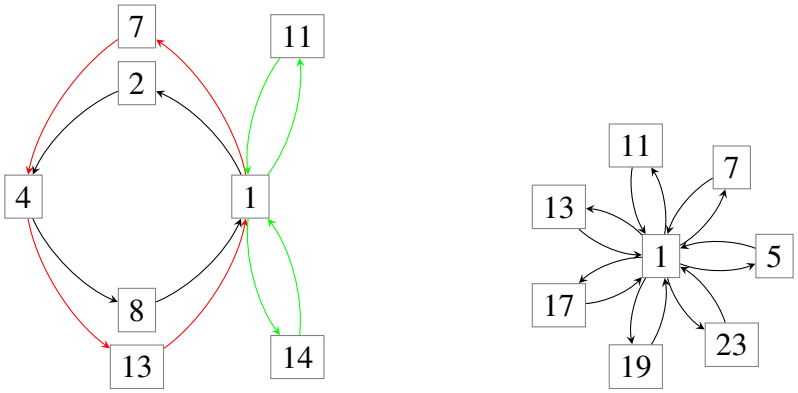


FIGURA 10. A sinistra il grafo di $\mathbb{Z}_{15}^*$, a destra quello di $\mathbb{Z}_{24}^*$.

6. LA COSTRUZIONE DEL GRAFO DI $\mathbb{Z}_{63}^*$

In questo paragrafo proponiamo una costruzione piuttosto impegnativa, quella del grafo di $\mathbb{Z}_{63}^*$ che non è planare (vedi Shanks [6] §33, p.84): i suoi quattro lobi sono isomorfi a $\mathbb{Z}_{21}^*$ (che a sua volta è isomorfo a $\mathbb{Z}_{36}^*$: si veda la parte sinistra della Figura 11) e possono essere disegnati su quattro piani incidenti in una retta passante per i punti 1, 62, 8, 55 (le radici quadrate dell'unità in $\mathbb{Z}_{63}^*$). In questo modo si eliminano le auto-intersezioni.

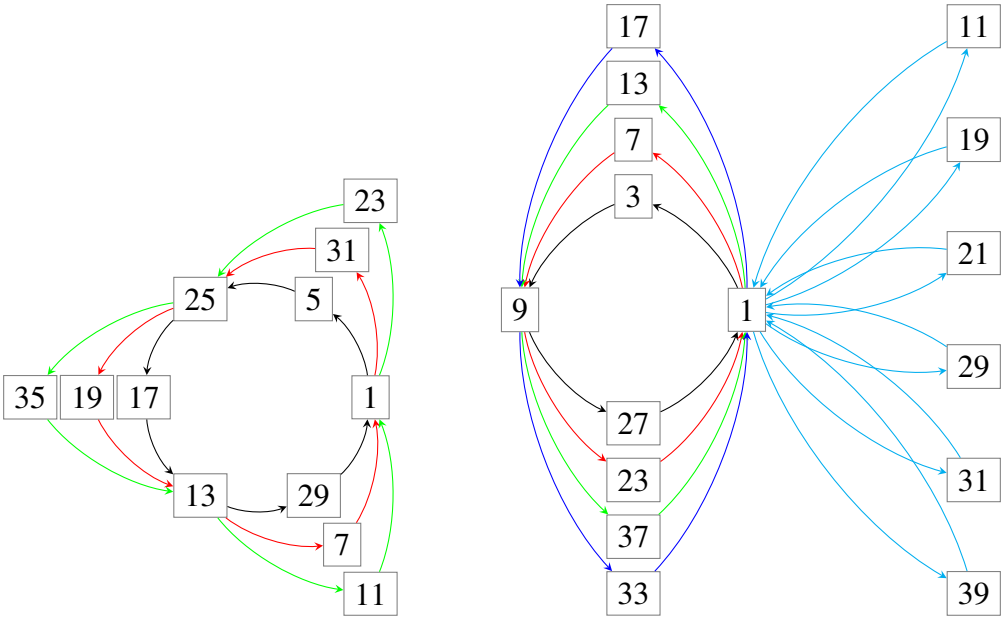


FIGURA 11. A sinistra il grafo di $\mathbb{Z}_{36}^*$, a destra quello di $\mathbb{Z}_{40}^*$.

Per prima cosa nella Figura 12 diamo il grafo in questione completo, costruito in modo da evidenziare le quattro componenti date in dettaglio nella Figura 13. Poi diamo il grafo suddiviso nei suoi quattro lobi, in grafici distinti e nelle Figure 14 e 15 due diversi metodi per incollare le 4 figure in modo da ottenere un modello tridimensionale del grafo. Infine, la Figura 16 mostra il primo passo della costruzione vera e propria.

Per passare dal grafo bidimensionale della Figura 12 a quello tridimensionale senza auto-intersezioni, proponiamo di disegnare i quattro schemi della Figura 13, chiusi ad anello, su quattro fogli di carta lucida, avendo cura di mettere nella stessa posizione i numeri "comuni" indicati sopra: si veda la Figura 16. Infine incolliamo i 4 piani cosí ottenuti secondo lo schema della Figura 14 o della Figura 15. Sono state indicate due soluzioni possibili, perché la prima è quella piú logica, ma in pratica richiede di tagliare i piani e riincollarli, mentre la seconda richiede solo incollamenti senza tagli.

7. COMMENTI E PROPOSTE; SPUNTI DI RIFLESSIONE

Elenchiamo alcuni punti significativi per la riflessione degli studenti, nonché una discussione dei valori "piccoli" di n, fino a 50, che possono essere utilmente sfruttati in classe. Si veda anche il §5.4 per i grafi relativi ad alcuni casi concreti.

7.1. **Il ruolo di 0.** Per quali n la tavola pitagorica in $\mathbb{Z}_n \setminus \{0\}$ non contiene 0? Per quali n la tavola delle potenze degli elementi non nulli di $\mathbb{Z}_n$ non contiene 0?

7.2. **Valori distinti delle potenze di un elemento e loro periodicità.** Se $d \mid \varphi(n)$, quanti valori diversi può assumere x^d per $x \in \mathbb{Z}_n^*$?

Se $m \in \mathbb{Z}_n^*$, allora la successione $x_k = m^k \bmod n$ è periodica (con eventuale antiperiodo). Infatti, $m^k \bmod n$ può assumere solo un numero *finito* di valori diversi. Se $m^k \equiv m^j \bmod n$ e $k > j \geq 0$ allora

$$m^{k-j} \equiv m^k \cdot \left(m^j\right)^{-1} \equiv 1 \bmod n.$$

Dunque esiste un intero positivo $i = k - j$ tale che $m^i \equiv 1 \bmod n$, e, in definitiva, non c'è antiperiodo. La periodicità di questa successione è, essenzialmente, lo stesso fenomeno che riscontriamo nella divisione fra interi, che dà origine a numeri decimali periodici. L'assenza

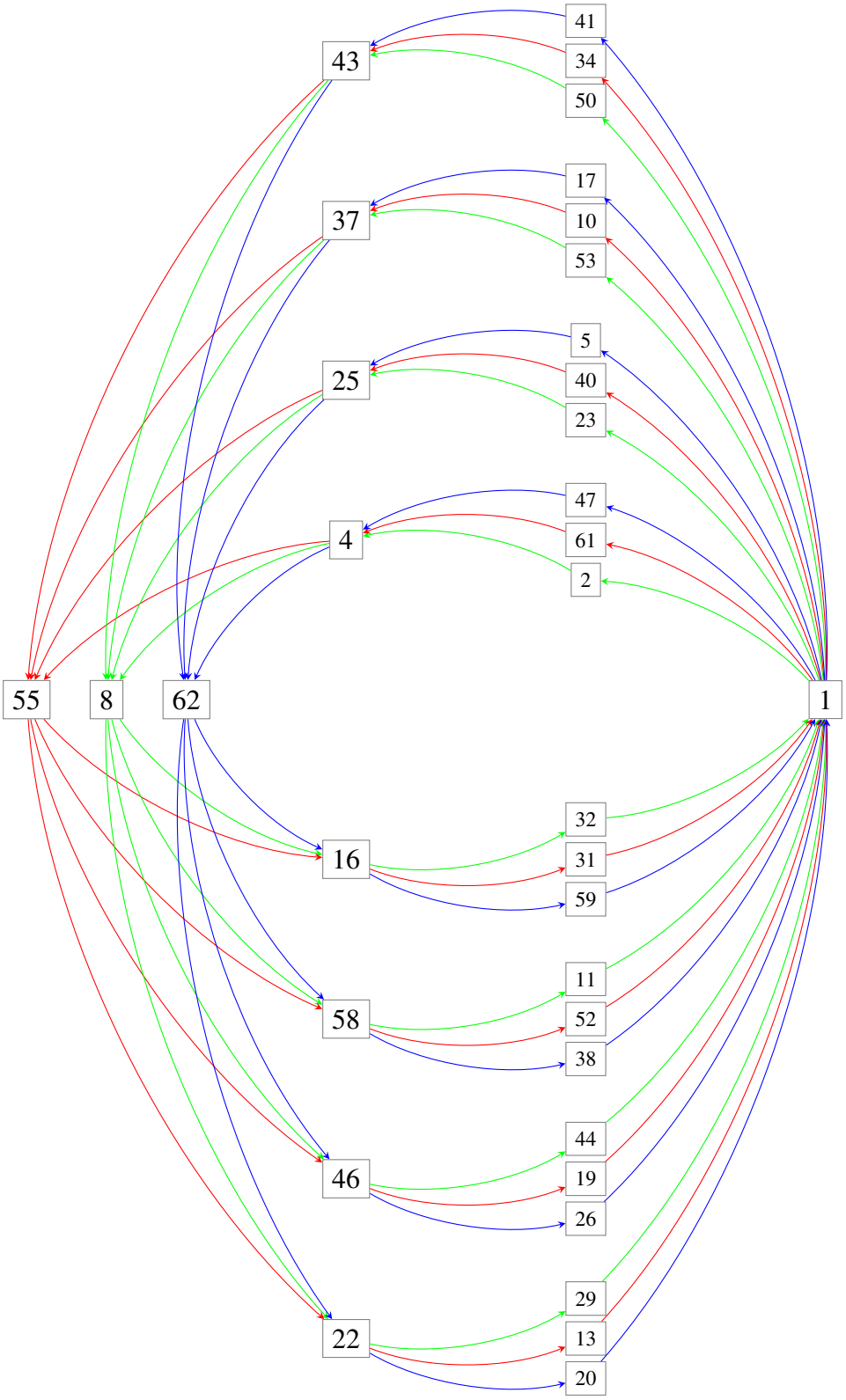


FIGURA 12. La presentazione di $\mathbb{Z}_{63}^*$

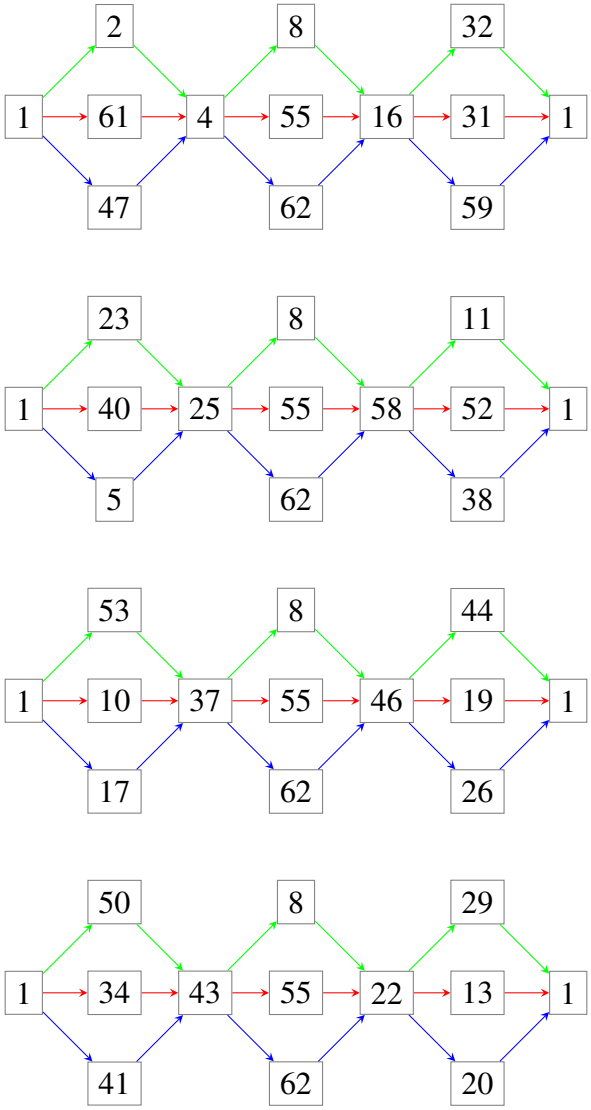


FIGURA 13. I quattro sottogruppi di $\mathbb{Z}_{63}^*$ isomorfi a $\mathbb{Z}_{36}^*$: si veda la parte sinistra della Figura 11

dell'antiperiodo è dovuta all'ipotesi che $m \in \mathbb{Z}_n^*$. In caso contrario, come abbiamo visto sopra nel §5.1, la successione è periodica ma è dotata di antiperiodo (e infatti il numero 1 non può essere ottenuto se non come valore iniziale della sequenza).

Dimostrare rigorosamente quest'ultima affermazione; verificare anche l'affermazione sulla relazione tra figura a forma di ρ e numeri "decimali" periodici; un esempio svolto si trova in [9], Figura 6.

7.3. **Catene massimali.** Vi sono valori di n per cui esistono m che danno luogo a catene "massimali" (che contengono *tutti* gli elementi di $\mathbb{Z}_n^*$). Quali sono questi valori? La risposta è data dal Teorema di Gauss generalizzato: vedi Teorema 11.3.11 di [5]). Nella Figura 17 forniamo una tabella di generatori per $\mathbb{Z}_p^*$, quando $p \leq 50$ è primo. Se p è un numero primo dispari, un generatore di $\mathbb{Z}_n^*$ per $n = p^\alpha$ o $n = 2p^\alpha$ si ottiene facilmente da g_p.

7.4. **Come condensare le informazioni.** Quando $\mathbb{Z}_n^*$ è ciclico basta un generatore; quando non lo è? In questo caso, qual è il minimo numero di generatori necessario? Tornando all'esempio

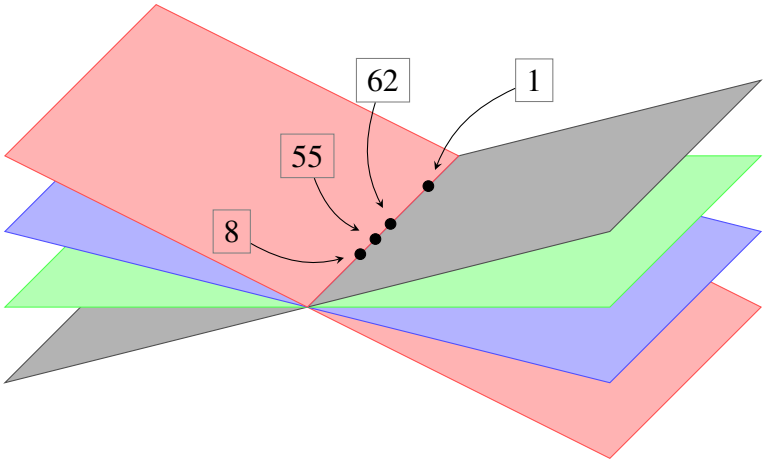


FIGURA 14. I quattro piani su cui disegnare i quattro lobi del grafo di $\mathbb{Z}_{63}^*$

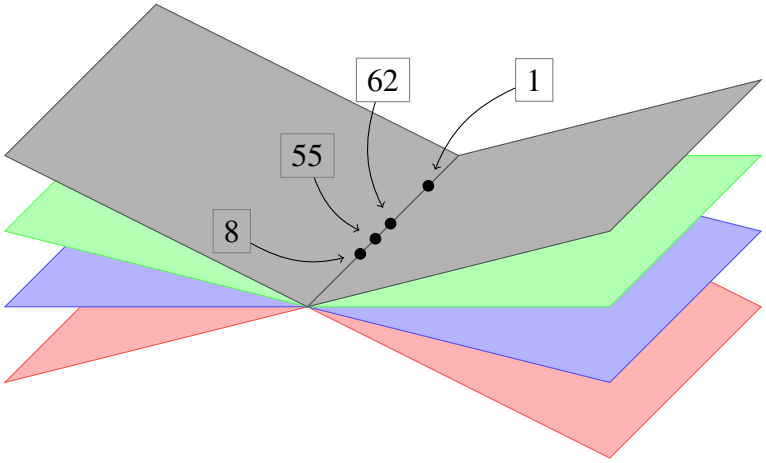
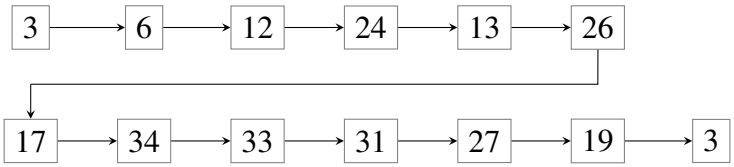


FIGURA 15. Un modo alternativo, e piú semplice in pratica, per incollare i quattro piani della Figura 14

studiato in dettaglio nel §4, si noti che, partendo da 3 invece che da 1, si ottiene la catena



In questa catena compaiono *tutti* gli elementi di $\mathbb{Z}_{35}^* \setminus \langle 2 \rangle$. In altre parole, abbiamo verificato che ogni elemento di $\mathbb{Z}_{35}^*$ può essere scritto nella forma $2^a \cdot 3^b$ dove $a \in \mathbb{Z}_{12}$ e $b \in \mathbb{Z}_2$, cioè, piú formalmente, che $\mathbb{Z}_{35}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{12}$. Il numero minimo di generatori necessario dà una misura di quanto il gruppo è lontano dall'essere ciclico, e questo si riflette sulla struttura del grafo.

7.5. **Radici quadrate.** Si studi il ruolo delle "radici quadrate" di 1, cioè degli elementi $m \in \mathbb{Z}_n^*$ che soddisfano $x^2 \equiv 1 \bmod n$. In generale, si studi il ruolo delle soluzioni delle equazioni $x^k \equiv 1 \bmod n$ per $k \mid \varphi(n)$ e si osservi che il grafo è tanto piú complicato tanto piú numerose sono le soluzioni rispetto al numero "atteso" che è k.

7.6. **Il Teorema di Eulero.** Si noti che l'ordine di ogni elemento divide il numero di elementi di $\mathbb{Z}_n^*$ (Teorema di Eulero; il Teorema di Fermat ne è un caso particolare: vedi rispettivamente

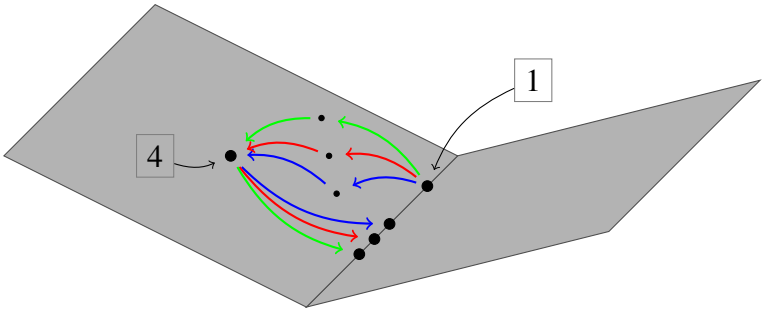


FIGURA 16. Disegno della prima metà della prima parte della Figura 13. Per maggiore chiarezza, abbiamo omesso le etichette di 8, 55, 62

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
g_p	1	2	2	3	2	2	3	2	5	2	3	2	6	3	5

FIGURA 17. g_p è il piú piccolo intero positivo che genera $\mathbb{Z}_p^*$

il Teorema 11.2.7 e il Teorema 11.2.1 di [5]). Si noti altresí che "di solito" l'ordine massimo degli elementi è molto piú piccolo. Questo rende il grafo molto "connesso."

7.7. **Funzione di Carmichael.** Il parametro che regola la connessione è il rapporto fra $\varphi(n)$ e la funzione di Carmichael $\lambda(n)$, il massimo ordine di qualche elemento di $\mathbb{Z}_n^*$. Se questo rapporto vale 1 il gruppo è ciclico. Nel nostro linguaggio, $\lambda(n)$ è la massima lunghezza di una qualche catena di $\mathbb{Z}_n^*$. Limitatamente ai valori discussi in questo articolo, abbiamo $\lambda(13) = 12$, $\lambda(15) = 4$, $\lambda(24) = 2$, $\lambda(35) = 12$, $\lambda(36) = 6$, $\lambda(40) = 4$, $\lambda(43) = 42$. Se $p > 2$ ed $\alpha \geq 1$ poniamo $\lambda\big(p^\alpha\big) = \varphi(p^\alpha) = (p-1)p^{\alpha-1}$. Inoltre, poniamo $\lambda(1) = \lambda(2) = 1$, $\lambda(4) = 2$ e $\lambda\big(2^\alpha\big) = \frac{1}{2}\varphi(2^\alpha) = 2^{\alpha-2}$ per $\alpha \geq 3$. In generale, se i p_i sono numeri primi distinti, poniamo

$$\lambda\Big(\prod_{i=1}^{k} p_i^{\alpha_i}\Big) = \operatorname{mcm}\big(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_k^{\alpha_k})\big).$$

Per il Teorema di Gauss generalizzato esiste almeno un elemento $g \in \mathbb{Z}_n^*$ di ordine esattamente $\lambda(n)$ e questo è il valore massimo possibile. Evidentemente $\lambda(n) \mid \varphi(n)$. Quando il rapporto $\varphi(n)/\lambda(n)$ è grande il grafo è molto connesso e, dal nostro punto di vista, interessante.

7.8. **Valori interessanti; isomorfismi.** Qui diamo un elenco di valori interessanti di n con un cenno alla struttura relativa: questi sono i valori di $n \leq 50$ che danno origine a gruppi non ciclici ordinati in classi di isomorfismo. I gruppi ciclici sono discussi con un esempio nel §5.2 e piú in generale nel §B.

$$\begin{aligned}
\mathbb{Z}_8^* \cong \mathbb{Z}_{12}^* &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 & \mathbb{Z}_{24}^* &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\
\mathbb{Z}_{15}^* \cong \mathbb{Z}_{16}^* \cong \mathbb{Z}_{20}^* \cong \mathbb{Z}_{30}^* &\cong \mathbb{Z}_2 \times \mathbb{Z}_4 & \mathbb{Z}_{32}^* &\cong \mathbb{Z}_2 \times \mathbb{Z}_8 \\
\mathbb{Z}_{21}^* \cong \mathbb{Z}_{28}^* \cong \mathbb{Z}_{36}^* \cong \mathbb{Z}_{42}^* &\cong \mathbb{Z}_2 \times \mathbb{Z}_6 & \mathbb{Z}_{33}^* \cong \mathbb{Z}_{44}^* &\cong \mathbb{Z}_2 \times \mathbb{Z}_{10} \\
\mathbb{Z}_{35}^* \cong \mathbb{Z}_{39}^* \cong \mathbb{Z}_{45}^* &\cong \mathbb{Z}_2 \times \mathbb{Z}_{12} & \mathbb{Z}_{40}^* \cong \mathbb{Z}_{48}^* &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4
\end{aligned}$$

Per esempio, l'isomorfismo fra $\mathbb{Z}_{24}^*$ e $\mathbb{Z}_2^3$ si realizza osservando che gli elementi di $\mathbb{Z}_{24}^*$ si scrivono in modo unico come $5^a \cdot 7^b \cdot 13^c$ con $a, b, c \in \mathbb{Z}_2$.

Notiamo esplicitamente che la parola *isomorfismo* assume un significato molto concreto e visibile! Dal punto di vista topologico astratto, il grafo di $\mathbb{Z}_n^*$ è planare per relativamente pochi

valori di n, mentre richiede dimensione 3 già per $n = 63$ oppure $n = 91$. Per questo motivo, è necessaria una grande cautela nella scelta dei valori da sottoporre agli studenti.

7.9. **Applicazioni pratiche.** A parte le applicazioni alla crittografia, queste tecniche sono usate per la generazione di sequenze *pseudocasuali* per simulare fenomeni stocastici. Notiamo l'apparente ossimoro: sequenza pseudocasuale generata da una formula deterministica. Per quanto detto sopra, è particolarmente interessante il caso in cui n è un numero primo.

8. Le basi matematiche

I fondamenti matematici di questo lavoro sono, evidentemente, i Teoremi di Fermat, Eulero e quello di Gauss generalizzato. ...

Il criterio per la tridimensionalità del grafo è enunciato nel §33, alle pagg. 96–97 di Shanks [6]. La spiegazione originale non è chiarissima. In pratica, per quanto detto sopra $\mathbb{Z}_n^*$ ha un sottogruppo ciclico massimale G_1 di ordine $m_1 = \lambda(n)$. Si prende il quoziente $\mathbb{Z}_n^*/G_1$, che ha ordine $n_1 = \varphi(n)/\lambda(n)$: questo, a sua volta, ha un sottogruppo ciclico massimale G_2 di ordine $m_2 = \lambda(n_1)$. Si itera questa costruzione fino a che uno dei quozienti è ciclico, ottenendo una sequenza di interi $m_1, m_2, \ldots, m_k$ con le proprietà che:

- $m_{i+1} \mid m_i$ per $i = 1, 2, \ldots, k-1$;
- $\mathbb{Z}_n^* \cong \mathbb{Z}_{m_k} \times \cdots \times \mathbb{Z}_{m_1}$.

Se due o piú dei numeri m_i non sono potenze di 2, allora il grafo di $\mathbb{Z}_n^*$ non è planare. In definitiva, questo è un modo alternativo per enunciare il Teorema 44.

Questa spiegazione è troppo complicata, ma l'esercizio 19S a pag. 206 può essere spiegato abbastanza bene.

9. Approfondimenti e bibliografia essenziale

La principale fonte d'ispirazione è stata il bellissimo (anche se forse un po' originale) libro di Shanks [6] e, in particolare, i diagrammi alle pagg. 83–92; per i dettagli si vedano i §§33 e 34. Vi si possono trovare i grafi relativi ai valori $n = 8$, 15, 21, 24, 54, 55, 56, 63, 64, 65, 85, 96, 105. Tutti questi grafi sono planari tranne quello per $n = 63$. Il testo che fornisce lo schema del Laboratorio PLS "Crittografia" da noi proposto solitamente nelle classi quarte è Languasco & Zaccagnini [4], integrato da Zaccagnini [7] e ora anche da [9]. Una trattazione completa, a livello universitario, si trova in Languasco & Zaccagnini [5]. L'Algoritmo di Gauss è descritto dettagliatamente in [5], pagg. 153–156. Si veda l'Appendice di Zaccagnini [8] per una discussione dei numeri decimali periodici. Il linguaggio `pari/gp` è descritto in dettaglio nel Cap. 2 di [4] e nel materiale su rete di [5]. Per testi in lingua italiana che trattano questi argomenti si vedano Childs [1] e Conway & Guy [2].

Riferimenti bibliografici

[1] L. Childs, *Algebra: un'introduzione concreta*, ETS, Pisa, 1983.

[2] J. H. Conway & R. K. Guy, *Il libro dei numeri*, Hoepli, Milano, 1999.

[3] G. Fiorini & A. Zaccagnini, *Costruzione dei grafi di $\mathbb{Z}_n^*$. Un laboratorio PLS in una classe terza del Liceo Scientifico*, A spasso per la matematica — Laboratori PLS 2014–2018 (a cura di A. Saracco e A. Zaccagnini), Dipartimento di Scienze Matematiche, Fisiche e Informatiche, Università di Parma, 2018, PLS – Parma.

[4] A. Languasco & A. Zaccagnini, *Crittografia*, Coop. Libraria Editrice Università di Padova, Padova, 2006, Progetto Nazionale Lauree Scientifiche. Sottoprogetto Matematica per il Veneto.

[5] A. Languasco & A. Zaccagnini, *Manuale di crittografia*, Ulrico Hoepli Editore, Milano, 2015. `https://www.hoepli.it/libro/manuale-di-crittografia/9788820366902.html`.

[6] D. Shanks, *Solved and Unsolved Problems in Number Theory*, fourth ed., Chelsea, New York, 1993.

1	2	3	4	6	8	9	11	12	13	16	17	18	19	22	23	24	26	27	29	31	32	33	34
2	4	6	8	12	16	18	22	24	26	32	34	1	3	9	11	13	17	19	23	27	29	31	33
3	6	9	12	18	24	27	33	1	4	13	16	19	22	31	34	2	8	11	17	23	26	29	32
4	8	12	16	24	32	1	9	13	17	29	33	2	6	18	22	26	34	3	11	19	23	27	31
6	12	18	24	1	13	19	31	2	8	26	32	3	9	27	33	4	16	22	34	11	17	23	29
8	16	24	32	13	29	2	18	26	34	23	31	4	12	1	9	17	33	6	22	3	11	19	27
9	18	27	1	19	2	11	29	3	12	4	13	22	31	23	32	6	24	33	16	34	8	17	26
11	22	33	9	31	18	29	16	27	3	1	12	23	34	32	8	19	6	17	4	26	2	13	24
12	24	1	13	2	26	3	27	4	16	17	29	6	18	19	31	8	32	9	33	22	34	11	23
13	26	4	17	8	34	12	3	16	29	33	11	24	2	6	19	32	23	1	27	18	31	9	22
16	32	13	29	26	23	4	1	17	33	11	27	8	24	2	18	34	31	12	9	6	22	3	19
17	34	16	33	32	31	13	12	29	11	27	9	26	8	24	6	23	22	4	3	2	19	1	18
18	1	19	2	3	4	22	23	6	24	8	26	9	27	11	29	12	13	31	32	33	16	34	17
19	3	22	6	9	12	31	34	18	2	24	8	27	11	33	17	1	4	23	26	29	13	32	16
22	9	31	18	27	1	23	32	19	6	2	24	11	33	29	16	3	12	34	8	17	4	26	13
23	11	34	22	33	9	32	8	31	19	18	6	29	17	16	4	27	3	26	2	13	1	24	12
24	13	2	26	4	17	6	19	8	32	34	23	12	1	3	27	16	29	18	31	9	33	22	11
26	17	8	34	16	33	24	6	32	23	31	22	13	4	12	3	29	11	2	19	1	27	18	9
27	19	11	3	22	6	33	17	9	1	12	4	31	23	34	26	18	2	29	13	32	24	16	8
29	23	17	11	34	22	16	4	33	27	9	3	32	26	8	2	31	19	13	1	24	18	12	6
31	27	23	19	11	3	34	26	22	18	6	2	33	29	17	13	9	1	32	24	16	12	8	4
32	29	26	23	17	11	8	2	34	31	22	19	16	13	4	1	33	27	24	18	12	9	6	3
33	31	29	27	23	19	17	13	11	9	3	1	34	32	26	24	22	18	16	12	8	6	4	2
34	33	32	31	29	27	26	24	23	22	19	18	17	16	13	12	11	9	8	6	4	3	2	1

FIGURA 18. La tavola pitagorica in $\mathbb{Z}_{35}^*$. Si notino le soluzioni dell'equazione $x^2 \equiv 1 \bmod 35$ sulla diagonale principale

[7] A. Zaccagnini, *Cryptographia ad usum Delphini*, Quaderno n. 459, Dipartimento di Matematica dell'Università di Parma, febbraio 2007, http://people.dmi.unipr.it/alessandro.zaccagnini/psfiles/papers/CryptoDelph.pdf.

[8] A. Zaccagnini, *La calcolatrice e le sue limitazioni*, L'Educazione Matematica, Anno XXVII, Serie VII **2** (2007), 35–45.

[9] A. Zaccagnini, *Riesame critico delle operazioni elementari*, Uno sguardo matematico sulla realtà — Laboratori PLS 2010–2014 (a cura di M. Belloni e A. Zaccagnini), Dipartimento di Matematica e Informatica, Università di Parma, 2014, PLS – Parma, pp. 71–91.

APPENDICE A. LA COSTRUZIONE DEL GRAFO DI $\mathbb{Z}_{15}^*$

Diamo qui di seguito la costruzione del grafo di $\mathbb{Z}_{15}^*$ in tutti i dettagli, a partire dalle "tavole pitagoriche" nelle Figure 19 e 20, proseguendo con la determinazione delle potenze degli elementi di $\mathbb{Z}_{15}^*$ (Figura 21) e concludendo con la costruzione delle relative catene (Figura 22). Il grafo è stato presentato nella parte sinistra della Figura 10.

APPENDICE B. GRUPPI CICLICI

Per forza di cose abbiamo trascurato i gruppi ciclici, ma possono dare origine a grafi molto belli se presentati opportunamente, per esempio disponendone gli elementi nell'ordine "naturale" $1, 2, \ldots, p-1$. Abbiamo già dato il grafo di $\mathbb{Z}_{13}^*$ nella Figura 8 e di $\mathbb{Z}_{43}^*$ nella Figura 9 associata alla dimostrazione del Teorema di Gauss. Qui diamo i grafi di $\mathbb{Z}_{29}^*$ nella Figura 24, di $\mathbb{Z}_{31}^*$ nelle Figure 25 e 26, e infine una presentazione alternativa di $\mathbb{Z}_{43}^*$ nella Figura 27.

GF: LICEO SCIENTIFICO "ATTILIO BERTOLUCCI," VIA TOSCANA 10/A, 43122 PARMA.

E-MAIL: FIOREGIAN@LIBERO.IT

AZ: DIPARTIMENTO DI SCIENZE MATEMATICHE, FISICHE E INFORMATICHE, UNIVERSITÀ DEGLI STUDI DI PARMA, PARCO AREA DELLE SCIENZE 53/A, 43124 PARMA.

E-MAIL: ALESSANDRO.ZACCAGNINI@UNIPR.IT

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

FIGURA 19. 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

FIGURA 20. La tavola pitagorica in $\mathbb{Z}_{15}^*$

	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

FIGURA 21. Le potenze degli elementi di $\mathbb{Z}_{15}^*$

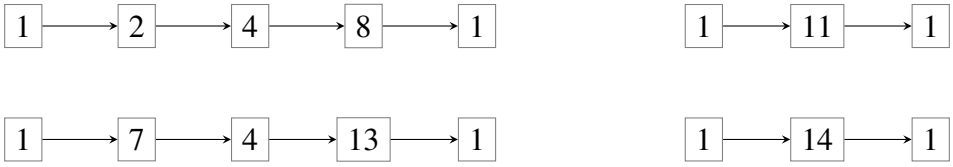


FIGURA 22. Determinazione delle catene quando $n = 15$

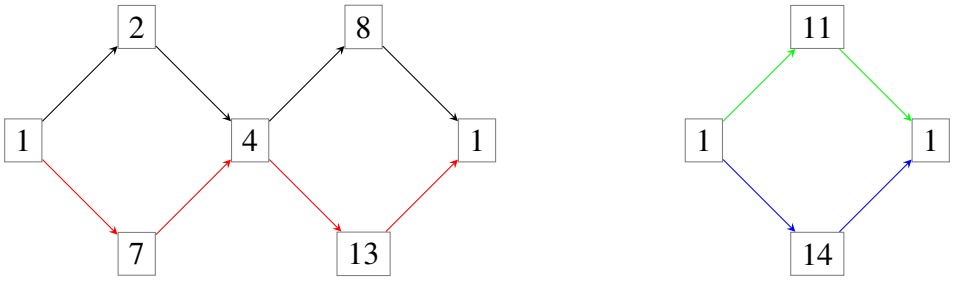


FIGURA 23. Saldatura delle catene

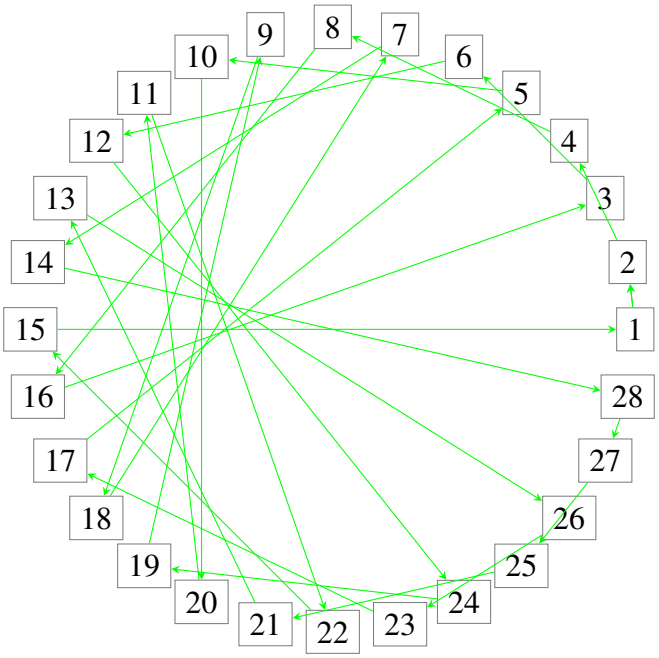


FIGURA 24. Il gruppo ciclico $\mathbb{Z}_{29}^*$ è generato da 2

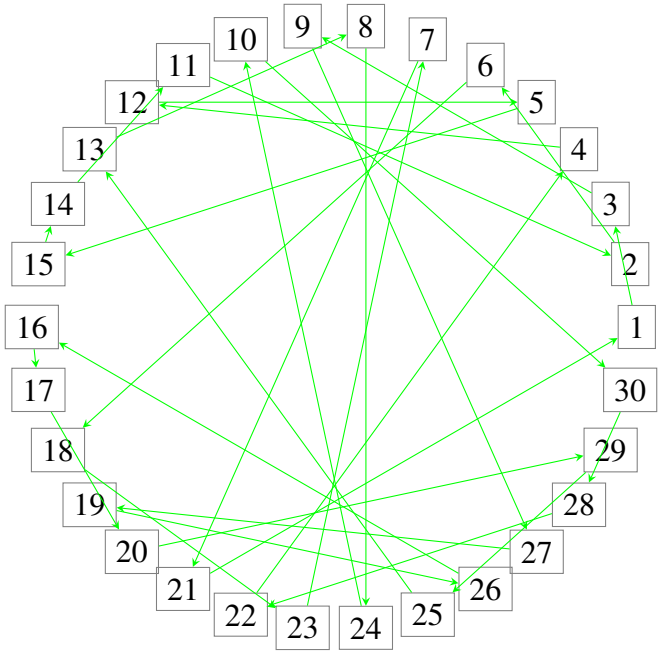


FIGURA 25. Il gruppo ciclico $\mathbb{Z}_{31}^*$ è generato da 3

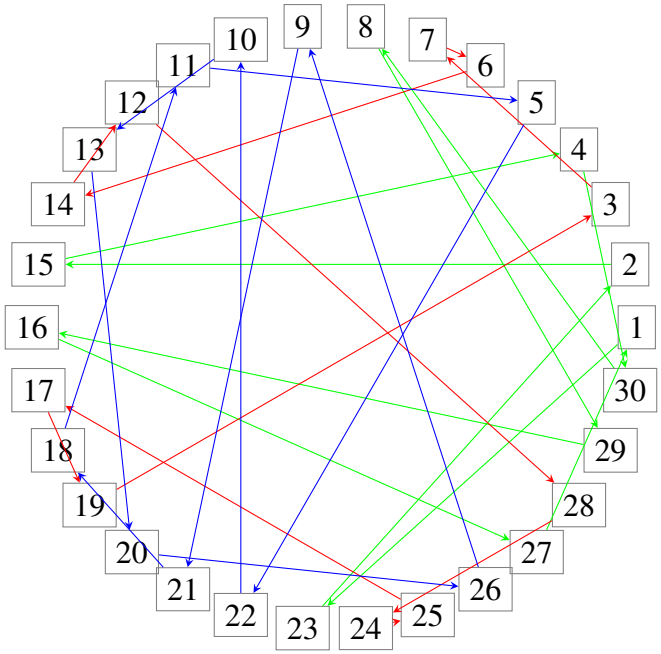


FIGURA 26. Le potenze di 23 generano un sottogruppo ciclico di $\mathbb{Z}_{31}^*$ di indice 3: vi sono dunque 3 "classi laterali" indicate dai colori diversi

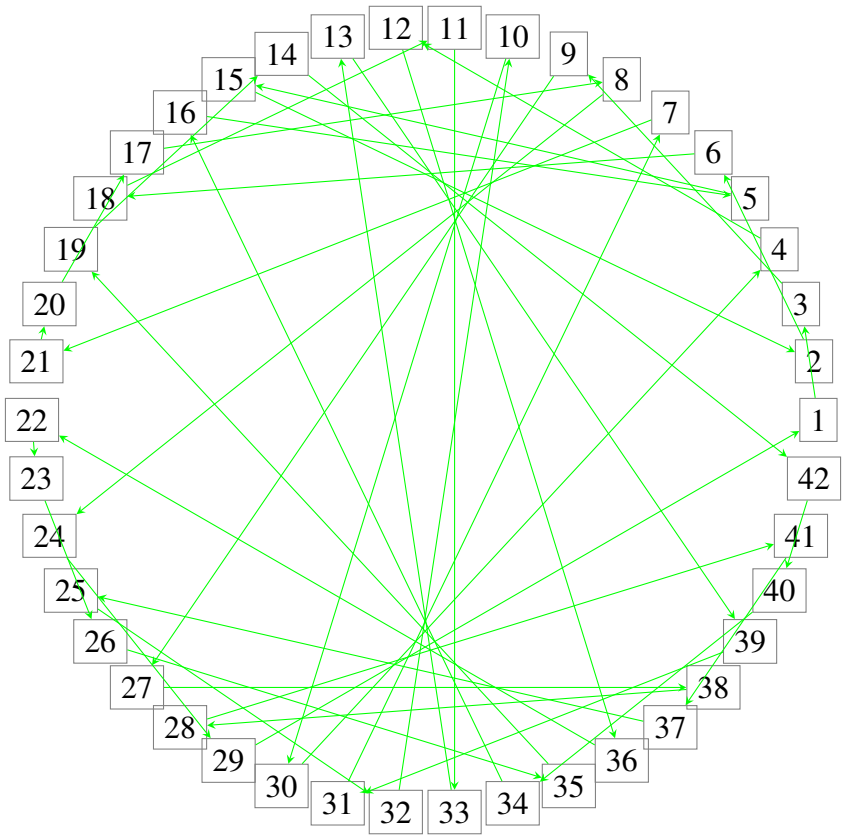


FIGURA 27. Il gruppo ciclico $\mathbb{Z}_{43}^*$ è generato da 3