Appunti su Principio di Induzione e Congruenze

Carmine Frascella

frascella@mail.dm.unipi.it

Indice

* * *

Desidero ringraziare il prof. Emanuele Callegari e la prof.ssa Giuseppina Serafica per la possibilità che mi hanno concesso quest'anno in questo stage. Ringrazio inoltre il mio caro amico Stefano Scalese per l'aiuto profuso, in via del tutto disinteressata. Per dubbi, chiarimenti o segnalazioni su eventuali errori in questi appunti, la mia mail è in copertina. Questi appunti sono stati redatti in LaTeX.

Capitolo 1

Introduzione

Iniziamo subito con alcune nozioni insiemistiche:

- $\mathbb{N}$ è l'insieme dei **naturali**. Conveniamo che lo 0 appartenga a $\mathbb{N}$, cosicchè:
$$\mathbb{N} = \{0, 1, 2, 3, ...\}$$
- L'insieme dei numeri naturali, 0 escluso, verrà indicato con $\mathbb{N}^+$;
- L'insieme dei numeri **relativi** si indica con $\mathbb{Z}$:
$$\mathbb{Z} = \{\ldots - 2, -1, 0, 1, 2, \ldots\}$$
- Altri insiemi sono l'insieme dei numeri **razionali** $\mathbb{Q}$, dei **reali** $\mathbb{R}$, dei **complessi** $\mathbb{C}$. In questi appunti però $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ non verranno menzionati, o comunque molto meno rispetto a $\mathbb{N}$ e $\mathbb{Z}$, che dovrebbero essere insiemi abbastanza familiari.

Esponiamo ora parte della notazione che si incontrerà in questi appunti.

- La seguente scrittura:
$$\sum_{i=1}^{n} i = 1 + 2 + 3 + \ldots + n$$
si legge **sommatoria** di i per i che va da 1 a n. È una scrittura che useremo spesso, conviene assimilarla;

- In modo analogo, la seguente scrittura:

$$\prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$$

si legge **produttoria** di i per i che va da 1 a n.

Riassumiamo adesso alcune nozioni di calcolo combinatorio.

- Le **disposizioni** di n oggetti *in classe* k, che indicano il numero di insiemi *ordinati* di k elementi ottenibili a partire da un insieme di n elementi, si indica con:

$$D_{n,k} = n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$$

- Le **permutazioni** di n oggetti , che indicano il numero di modi in cui si possono ordinare gli n elementi, si indica con:

$$P_n = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = D_{n,n}$$

- Per usare una notazione più sintetica, definiamo il **fattoriale** di $n \in \mathbb{N}$ in questo modo:

$$n! = P_n = D_{n,n} = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = \prod_{i=1}^{n} i$$

Notiamo che $(n+1)! = (n+1)n!$ (ciò è evidente). Conveniamo inoltre che $0! = 1$, $n! = 0$ se n è negativo;

- Le **combinazioni** di n oggetti *in classe* k, che indicano il numero di insiemi *non ordinati* di k elementi ottenibili a partire da un insieme di n elementi, si indica con:

$$C_{n,k} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k \cdot (k-1) \cdot \ldots \cdot 2 \cdot 1} = \frac{D_{n,k}}{P_k}$$

- Per usare una notazione più sintetica, definiamo, dati due numeri $n, k \in \mathbb{N}$, con $n \geq k$ per semplicità, il **coefficiente binomiale** di n e k come:

$$\binom{n}{k} = C_{n,k}$$

Esercizio 1. Si provi a dimostrare che:

- $\binom{n}{k} = \frac{n!}{k!(n-k)!}$;
- $\binom{n}{0} = \binom{n}{n} = 1$;
- $\binom{n}{1} = \binom{n}{n-1} = n$;
- $\binom{n}{k} = \binom{n}{n-k}$;
- $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

Suggerimenti: per il primo si usi la definizione di coefficiente binomiale, e poi si moltiplichi e divida per *un qualcosa* per giungere alla tesi; per il secondo e il terzo, il risultato si ottiene direttamente dalla definizione (questi sono risultati che useremo in seguito); per il quarto, invece, si usi esplicitamente la definizione di coefficiente binomiale. Il terzo è già un quesito un attimino più impegnativo, si provi a risolverlo una volta raggiunta un po' di dimestichezza con i coefficienti binomiali.

Capitolo 2

Principio di Induzione

2.1 Prima formulazione

Proposizione 2.1.1. *Il* ***principio d'induzione*** *asserisce che se* $\mathcal{P}$ *è una proprietà che vale per* $n_0 \in \mathbb{N}$*, e se* $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ *per* $n \geq n_0$*, allora* $\mathcal{P}$ *vale* $\forall\ n \in \mathbb{N}$*, con* $n \geq n_0$*.*

In altri termini, se $\mathcal{P}$ *è una proprietà tale che:*

- $\mathcal{P}(n_0)$ *è vera per un qualche* $n_0 \in \mathbb{N}$*;*
- $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ *per* $n \geq n_0$*,*

allora $\mathcal{P}$ *è vera per ogni* $n \in \mathbb{N}, n \geq n_0$*.*

2.2 Seconda formulazione

Proposizione 2.2.1. *Se* $\mathcal{P}$ *è una proprietà che vale per* $n_0 \in \mathbb{N}$*, e se* $\mathcal{P}(n_0), \ldots, \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ *per* $n \geq n_0$*, allora* $\mathcal{P}$ *vale* $\forall\ n \in \mathbb{N}$*, con* $n \geq n_0$*.*

In altri termini, se $\mathcal{P}$ *è una proprietà tale che:*

- $\mathcal{P}(n_0)$ *è vera per un qualche* $n_0 \in \mathbb{N}$*;*
- $\mathcal{P}(n_0), \ldots, \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ *per* $n \geq n_0$*,*

allora $\mathcal{P}$ *è vera per ogni* $n \in \mathbb{N}, n \geq n_0$*.*

Questa formulazione è comunenemente denominata *induzione forte*.

2.3 Schema generale di una dimostrazione per induzione

Generalmente una dimostrazione per induzione consta di due parti fondamentali: uno o più **casi base**, e uno o più **passi induttivi**.

Si inizia dunque dimostrando che la proprietà è vera per uno o più valori iniziali a noi noti. Negli esercizi più semplici, il caso base spesso consta di una sola verifica: tuttavia, vi sono casi dove ne sono necessarie più di una. Vedremo alcuni esercizi di questo tipo.

Si procede quindi dimostrando che, assunta vera la proprietà per un generico numero $n \geq n_0$ (questa è comunemente chiamata *ipotesi induttiva*) o per più numeri, la proprietà vale per $n + 1$ (o, in particolari casi, per una serie di numeri maggiori di quelli presi in considerazione nell'ipotesi induttiva).

2.4 Sommatorie e Produttorie

Cominciamo con una serie di esercizi base per familiriarizzare con i concetti espressi nella prima parte.

Esercizio 2. Dimostrare che:

$$\sum_{i=0}^{n} i = 0 + 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

Dimostrazione. A proposito di quest'esercizio, c'è un curioso aneddoto. Pare che C.F.Gauss, noto matematico tedesco, all'età di otto anni avesse determinato questa formula per risolvere alla svelta un quesito che era stato posto dal suo maestro per tenerlo a bada per un po': il maestro, ignaro del genio che si nascondeva in lui, gli chiese la somma dei numeri da 1 a 100, convinto di tenerlo occupato per molto tempo.

Procediamo ora con lo svolgimento dell'esercizio: in questo caso possiamo dimostrare che la proprietà è vera per 0, per poi procedere con il passo induttivo.

Dunque:

$$\sum_{i=0}^{0} i = 0 = \frac{0 \cdot (0+1)}{2} = 0,$$

dunque la proprietà è vera per 0.

Procediamo ora con il passo induttivo. Notiamo che:

$$\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + (n+1),$$

e ciò è banale: la somma dei primi $(n+1)$ numeri naturali può essere vista come la somma dei primi n, sommata all'$(n+1)$-esimo.
Per ipotesi induttiva:

$$\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} +(n+1) = \frac{n(n+1)}{2} + (n+1)$$

Ricordiamo che il nostro obiettivo è quello di dimostrare, assumendo vero che:

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2},$$

la seguente uguaglianza:

$$\sum_{i=0}^{n} i = \frac{(n+1)((n+1)+1)}{2} = \frac{(n+1)(n+2)}{2}$$

Notiamo ora che:

$$\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)+2n+2}{2} =$$
$$= \frac{n(n+1)+2(n+1)}{2} = \frac{(n+2)(n+1)}{2},$$

e ciò è quanto volevamo dimostrare. □

Esercizio 3. Dimostrare che:

$$\sum_{i=1}^{n}(2i-1) = 1+3+\ldots+(2n-1) = n^2$$

Dimostrazione. Dimostriamo il caso base, assumendo $n = 1$:

$$\sum_{i=1}^{1}(2i-1) = 1 = 1^2,$$

cosicchè il caso base è dimostrato. Passiamo ora al passo induttivo. La nostra ipotesi induttiva è che l'uguaglianza sussista per n:

$$\sum_{i=1}^{n}(2i-1) = n^2$$

Il nostro obiettivo è il seguente:

$$\sum_{i=1}^{n+1}(2i-1) = (n+1)^2$$

Ma:

$$\sum_{i=1}^{n+1}(2i-1) = \sum_{i=1}^{n}(2i-1) + (2(n+1)-1) = \sum_{i=1}^{n}(2i-1) + (2n+2-1) =$$

$$= \sum_{i=1}^{n}(2i-1) + (2n+1) = n^2 + 2n + 1 = (n+1)^2,$$

come volevasi dimostrare. □

Esercizio 4. Dimostrare che:

$$\sum_{i=1}^{n} i^3 = 1 + 2^3 + \ldots + n^3 = \frac{n^2(n+1)^2}{4} = \left(\sum_{i=1}^{n} i\right)^2$$

Dimostrazione. Lasciamo la verifica della validità della proposizione per $n = 1$ per esercizio. Passiamo ora al passo induttivo. La nostra ipotesi induttiva è che l'uguaglianza sussista per n:

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$$

Il nostro obiettivo è il seguente:

$$\sum_{i=1}^{n+1} i^3 = \frac{(n+1)^2(n+2)^2}{4}$$

Ma:

$$\sum_{i=1}^{n+1} i^3 = \sum_{i=1}^{n} i^3 + (n+1)^3 = \frac{n^2(n+1)^2}{4} + (n+1)^3 =$$

$$= \frac{n^2(n+1)^2 + 4(n+1)^3}{4} = \frac{n^2(n+1)^2 + 4(n+1)(n+1)^2}{4} =$$

$$= \frac{(n^2+4n+4)(n+1)^2}{4} = \frac{(n+2)^2(n+1)^2}{4},$$

come volevasi dimostrare. □

Esercizio 5. Dimostrare che:

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Dimostrazione. Lasciamo per esercizio la dimostrazione del caso base. Quanto al passo induttivo, lo schema dovrebbe ora essere familiare. Una volta fissata l'ipotesi induttiva e l'obiettivo da raggiungere, si ha:

$$\sum_{i=1}^{n+1} i^2 = \sum_{i=1}^{n} i^3 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 =$$

$$\frac{n(n+1)(2n+1)}{6} + (n+1)^2 =$$

$$= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} = \frac{n(n+1)(2n+1) + 6(n+1)(n+1)}{6} =$$

$$= \frac{(2n^2 + n + 6n + 6)(n+1)}{6} =$$

$$= \frac{(2n^2 + 7n + 6)(n+1)}{6} = \frac{(n+2)(2n+3)(n+1)}{6},$$

ossia la tesi. □

Osservazione 1. Nell'esercizio appena svolto, il termine a secondo membro è a priori una frazione. È sicuro che in realtà quello è sempre un intero?

Esercizio 6. Dimostrare che $\sum_{k=1}^{n} \frac{1}{4k^2+1} = \frac{n}{2n+1}$.

Esercizio 7. Dimostrare che $\sum_{k=1}^{n} \frac{k}{2^k} = 2 - \frac{n+2}{2^n}$.

Il secondo esercizio può essere un esempio per mostrare che, nonostante la parte *difficile* di una dimostrazione per induzione sia il passo induttivo, il caso base è essenziale, e non dev'essere omesso assolutamente. Per esempio, la seguente uguaglianza:

$$\sum_{k=1}^{n} \frac{k}{2^k} = 7 - \frac{n+2}{2^n},$$

simile a quella dell'esercizio 2, è falsa, perchè ad esempio se si sostituisce 1 ad n (caso base) si ottiene:

$$\frac{1}{2} = 7 - \frac{3}{2} = \frac{11}{2},$$

evidentemente falso.

Eppure, se si prova a dimostrare questa *non*-uguaglianza per induzione, dimenticando il caso base e passando direttamente al passo induttivo, tutto torna. Provare per credere. Entrambe le parti di una dimostrazione per induzione, quindi, sono necessarie.

Esercizio 8. Dimostrare che, se $n \geq 2$:

$$\prod_{k=2}^{n}\left(1-\frac{1}{k^2}\right)=\frac{1+n}{2n}$$

Dimostrazione. Dimostriamo il caso base:

$$\prod_{k=2}^{2}\left(1-\frac{1}{k^2}\right)=1-\frac{1}{4}=\frac{3}{4}=\frac{1+2}{4}$$

Supponiamo ora vero che:

$$\prod_{k=2}^{n}\left(1-\frac{1}{k^2}\right)=\frac{1+n}{2n}$$

Allora:

$$\prod_{k=2}^{n+1}\left(1-\frac{1}{k^2}\right)=\prod_{k=2}^{n}\left(1-\frac{1}{k^2}\right)\cdot\left(1-\frac{1}{(n+1)^2}\right)=\frac{1+n}{2n}\cdot\left(1-\frac{1}{(n+1)^2}\right)=$$

$$=\frac{1+n}{2n}-\frac{1+n}{2n(n+1)^2}=\frac{(1+n)^3-(1+n)}{2n(n+1)^2}=\frac{1+3n+3n^2+n^3-1-n}{2n(n+1)^2}=$$

$$=\frac{n^3+3n^2+2n}{2n(n+1)^2}=\frac{n(n+1)(n+2)}{2n(n+1)^2}=\frac{n+2}{2(n+1)}$$

Allora:

$$\prod_{k=2}^{n+1}\left(1-\frac{1}{k^2}\right)=\frac{n+2}{2(n+1)}=\frac{(n+1)+1}{2(n+1)}$$

□

Esercizio 9. Dimostrare che:

$$\sum_{k=1}^{n}\left(\frac{1}{k(k+1)}\right)=\frac{n}{n+1}$$

Dimostrazione. Il caso base è lasciato per esercizio. Quanto al passo induttivo, assumiamo che:

$$\sum_{k=1}^{n}\left(\frac{1}{k(k+1)}\right)=\frac{n}{n+1}$$

Allora:

$$\sum_{k=1}^{n+1}\left(\frac{1}{k(k+1)}\right)=\sum_{k=1}^{n}\left(\frac{1}{k(k+1)}\right)\cdot\left(\frac{1}{(n+1)(n+2)}\right)=$$

$$=\frac{n}{n+1}\cdot\frac{1}{(n+1)(n+2)}=\frac{n(n+2)-1}{(n+1)(n+2)}=\frac{n^2+2n+1}{(n+1)(n+2)}=$$

$$=\frac{(n+1)^2}{(n+1)(n+2)}=\frac{(n+1)}{(n+2)}$$

□

Esercizio 10. Dimostrare che $\sum_{k=1}^{n}k(k+1)=\frac{n(n+1)(n+2)}{3}$. È sicuro che il termine a secondo membro sia un intero?

Esercizio 11. Dimostrare che $\sum_{k=1}^{n}k\cdot k!=(n+1)!-1$.

2.5 Divisibilità

Ora un esercizio abbastanza semplice sulla divisibilità tra numeri.

Esercizio 12. Dimostrare che, per ogni $n\geq 1$, n^3+2n è divisibile per 3.

Dimostrazione. Il caso base è semplice: 3 è certamente multiplo di 3. Supponiamo ora che la regola valga per n:

$$3\mid n^3+2n$$

Allora:

$(n+1)^3-2(n+1)=n^3+3n^2+3n+1+2n+2=(n^3+2n)+(3n^2+3n+3)$

Essendo 3 un divisore sia del primo che del secondo addendo (il primo per ipotesi induttiva, il secondo per evidenti motivi), conveniamo che
$3\mid(n+1)^3+2(n+1)$. □

Esercizio 13. Dimostrare che per ogni $n\geq 1$, il numero n^3+5n è divisibile per 6.

Esercizio 14. Dimostrare che per ogni $n\geq 1$, il numero 10^n-1 è divisibile per 9.

Esercizio 15. Dimostrare che per ogni $n\geq 1$, il numero $7^{3^n}-1$ è divisibile per 3^{n+1} (abbastanza più difficile: provarci).

2.6 Binomio di Newton

Passiamo ora a qualche esercizio un po' più impegnativo. Cominciamo da un'uguaglianza tanto nota quanto importante, conosciuta come formula del **binomio di Newton**.

Esercizio 16. Dimostrare che, dati $a, b \in \mathbb{N}, n \in \mathbb{N}^+$, vale:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Dimostrazione. L'uguaglianza è vera per $n = 1$. Infatti:

$$a + b = (a+b)^1 = \sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k = \binom{1}{0} a^{1-0} b^0 + \binom{1}{1} a^{1-1} b^1 = a + b$$

Passiamo ora al passo induttivo. Supponiamo vera la proprietà per n:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Allora:

$$(a+b)^{n+1} = (a+b)(a+b)^n = (a+b) \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \right)$$

Ora:

$$(a+b) \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \right) = \left(\sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k \right) + \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1} \right)$$

Dobbiamo ora sommare tra loro i termini simili. Consideriamo il generico termine $a^{n+1-k} b^k$, e determiniamo il suo coefficiente. Nella prima sommatoria il suo coefficiente è $\binom{n}{k}$; nella seconda esso è $\binom{n}{k-1}$. Noi vorremmo che sia $\binom{n+1}{k}$. Ma:

$$\binom{n}{k} + \binom{n}{k-1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} =$$

$$= \frac{n!}{k!(n-k+1)!} \cdot (n-k+1+k) =$$

$$= \frac{n!}{k!(n-k+1)!} \cdot (n+1) = \frac{(n+1)!}{k!(n-k+1)!} = \binom{n+1}{k},$$

e con ciò l'esercizio è concluso. □

Osservazione 2. Dato $n \in \mathbb{N}$ (evitiamo $n = 0$ per non cadere nel banale), è vero che:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Come si può dimostrare quest'asserzione usando il binomio di Newton?
Suggerimento: in effetti, $\binom{n}{k} = \binom{n}{k} 1^{n-k} 1^k$. Ora il metodo dovrebbe essere più chiaro...

Questo esercizio è strettamente imparentato con la nozione di **insieme delle parti** $\mathcal{P}(X)$ di un insieme X. L'insieme delle parti di un insieme e' l'insieme che contiene tutti i sottoinsiemi distinti di X. Ad esempio:

$$X = \{1, 2, 3\}$$

$$\mathcal{P}(X) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Si noti che il numero di elementi di X è 3, il numero di elementi di $\mathcal{P}(X)$ è $8 = 2^3$. Ciò non è affatto un caso. Infatti:

$$| X |= n \Rightarrow | \mathcal{P}(X) |= 2^n,$$

tanto che spesso si sostituisce la notazione $\mathcal{P}(X)$ con 2^X. Provare dunque a dimostrare che, se $| X |= n$, allora $| 2^X |= 2^n$. In effetti, per ogni elemento $x \in X$, si hanno due possibilità: o si inserisce x nel sottoinsieme, oppure no. E se per ogni elemento si hanno due possibilità... formalizzare quest'intuizione.

2.7 Disuguaglianze

Il principo di induzione è spesso usato per risolvere alcune **disuguaglianze**. Cominciamo subito con una nota disuguaglianza, la **disuguaglianza di Bernoulli**.

Esercizio 17. Dimostrare che, se $x \in \mathbb{N}$:

$$(1 + x)^n \geq 1 + nx$$

Dimostrazione. È abbastanza chiaro che l'induzione vada eseguita su n, visto che x è fissato una volta per tutte. Per $n = 0$ si ottiene l'uguaglianza, dunque *a fortiori* la disuguaglianza debole. Passiamo al passo induttivo. Per ipotesi induttiva sappiamo che:

$$(1 + x)^n \geq 1 + nx$$

Vogliamo dimostrare che:

$$(1+x)^{n+1} \geq 1 + (n+1)x$$

Ma:

$$(1+x)^{n+1} = (1+x)(1+x)^n \geq (1+x)(1+nx) =$$
$$= 1 + (n+1)x + nx^2 \geq 1 + x + nx = 1 + (n+1)x,$$

dato che $nx^2 \geq 0$. Dunque la tesi. □

Osservazione 3. In realtà x può essere un qualsiasi numero reale strettamente maggiore di -1. La dimostrazione è la stessa, e procedendo si nota che $(1+x) > 0 \Leftrightarrow x > -1$, e ciò serve per poter imporre la disuguaglianza. La comprensione del caso in cui $x \in \mathbb{N}$ è comunque pienamente sufficiente per i nostri scopi.

Esercizio 18. Dimostrare che $2^n > n^2$ per ogni $n \geq 5$.

Esercizio 19. Dimostrare che $n^2 > 2n + 1$ per ogni $n \geq 3$.

Esercizio 20. Dimostrare che:

$$n! \geq 2^{n-1} \text{ per ogni } n \in \mathbb{N}^+$$

Dimostrazione. Per $n = 1$ l'affermazione è chiaramente vera. Supponiamo allora che $n! \geq 2^{n-1}$. Allora:

$$(n+1)! = (n+1)n! \geq (n+1)2^{n-1} \geq 2 \cdot 2^{n-1} = 2^n,$$

dunque la dimostrazione è conclusa. □

2.8 Induzione forte

Risolveremo ora un esercizio mediante *induzione forte*. Il **Teorema fondamentale dell'Aritmetica** afferma che per ogni numero naturale esiste un'unica scomposizione in fattori primi. In realtà verrà dimostrata solo l'esistenza della fattorizzazione, non l'unicità.

Esercizio 21. Dimostrare che ogni numero naturale $n \geq 2$ si può esprimere come prodotto di numeri primi, se non è esso stesso un numero primo.

Dimostrazione. Per $n = 2$ l'asserto è vero, in quanto 2 è primo. Supponiamo allora che l'asserto sia vero per tutti i numeri da 2 a $n - 1$. Considerando n, le possibilità sono due:

- n è primo, e allora non c'è nulla da dimostrare;

- n non è primo, dunque è divisibile per un certo numero $k \neq 1$, $k \neq n$. Osserviamo subito che $1 < k < n$, da cui anche $n/k < n$. Allora, per ipotesi induttiva, essendo $n = k \cdot n/k$, ed essendo k e n/k numeri che ammettono una scomposizione in fattori primi, anche n ne ammette una.

□

Capitolo 3

Congruenze

3.1 Relazioni di equivalenza

Consideriamo l'insieme dei numeri relativi $\mathbb{Z}$ per semplicità.

Definizione 3.1. Definiamo allora il **prodotto cartesiano** $\mathbb{Z} \times \mathbb{Z}$ nel modo che segue:

$$\mathbb{Z} \times \mathbb{Z} = \{(a, b) \mid a \in \mathbb{Z}, b \in \mathbb{Z}\}$$

Il prodotto cartesiano $\mathbb{Z} \times \mathbb{Z}$ consiste quindi nelle coppie ordinate di numeri appartenenti a $\mathbb{Z}$. Notiamo che in generale, dati due numeri relativi a e b, si ha che $(a, b) \neq (b, a)$.

Definizione 3.2. Una **relazione binaria** su $\mathbb{Z}$ è un sottoinsieme $\mathcal{R}$ del prodotto cartesiano $\mathbb{Z} \times \mathbb{Z}$. Due numeri relativi x e y sono in relazione se e solo se:

$$(x, y) \in \mathcal{R}$$

Diremo in questo caso che x è in relazione con y, e scriveremo $x\mathcal{R}y$.

Non ci interessa però studiare relazioni qualsiasi, bensì una particolare classe di esse: le **relazioni di equivalenza**.

Definizione 3.3. Una **relazione di equivalenza** è una relazione binaria che soddisfa tre proprietà:

- **Proprietà riflessiva**: $\forall\ x \in \mathbb{Z} : (x, x) \in \mathcal{R}$;
- **Proprietà simmetrica**: $\forall\ x, y \in \mathbb{Z} : (x, y) \in \mathcal{R} \Leftrightarrow (y, x) \in \mathcal{R}$;
- **Proprietà transitiva**: $\forall\ x, y, z \in \mathbb{Z} : (x, y) \in \mathcal{R}, (y, z) \in \mathcal{R} \Rightarrow (x, z) \in \mathcal{R}$.

Tutto quanto detto finora può risultare ostico, per ora. Facciamo dunque subito un esempio molto elementare.

Esercizio 22. Definiamo su $\mathbb{Z}$ la relazione di **uguaglianza**, che afferma che:

$$x \mathcal{R} y \Leftrightarrow x = y$$

Dimostrare che la relazione di uguaglianza è una relazione di equivalenza su $\mathbb{Z}$.

Dimostrazione. Dimostriamo le tre proprietà, una ad una:

- È certamente vero che per ogni $x \in \mathbb{Z}$ si ha $x = x$. Dunque $\forall\ x \in \mathbb{Z} : (x, x) \in \mathcal{R}$;
- È altresì evidente che, presi due numeri relativi x e y, se $x = y$ allora $y = x$. Dunque la proprietà simmetrica è soddisfatta;
- È infine vero che, dati $x, y, z \in \mathbb{Z}$, se $x = y$ e $y = z$, allora $x = z$. Anche la transititività è allora dimostrata.

□

Quest'esempio è molto semplice da apprendere, ma è anche poco istruttivo, in quanto per effettuare la dimostrazioni non sono stati usati argomenti matematici particolari, in quanto tutto era molto evidente. Più avanti definiremo una relazione di equivalenza meno banale di questa.

Osservazione 4. Avendo a che fare con relazioni di equivalenza, per dire che x è in relazione con y useremo la seguente scrittura: $x \sim y$.

Osservazione 5. Abbiamo usato $\mathbb{Z}$ per semplicità. Una relazione di equivalenza, in realtà, si può istituire su qualsiasi insieme: basta solo accertarsi che sia ben fondata, cioè che rispetti le tre proprietà citate sopra.

Definizione 3.4. Dato un insieme (restringiamoci al caso $\mathbb{Z}$ per comodità), una relazione di equivalenza $\mathcal{R}$ e un elemento $x \in \mathbb{Z}$, si definisce **classe** di x il seguente insieme:

$$[x]_\sim = \{y \in \mathbb{Z} \mid x \sim y\}$$

La classe di x è dunque l'insieme dei numeri relativi che sono in relazione con x secondo la relazione di equivalenza di x.

Notiamo subito una cosa apparentemente banale ma importante: $\forall\ x \in \mathbb{Z} : (x, x) \in \mathcal{R} \Rightarrow x \in [x]_\sim$.

Esercizio 23. Qual è la classe di equivalenza di 0 secondo la relazione di uguaglianza vista prima?

Dobbiamo ora dimostrare un'ultima cosa fondamentale, prima di avvicinarci all'argomento vero e proprio.

Definizione 3.5. Data una relazione di equivalenza (che indicheremo con $\sim$) su $\mathbb{Z}$, essa genera una **partizione** di $\mathbb{Z}$ in classi. Una relazione di equivalenza partiziona un insieme in classi quando:

- Ogni classe è non vuota;
- L'unione delle classi ricopre $\mathbb{Z}$;
- Le classi sono a due a due disgiunte.

Vedremo un esempio di partizione di $\mathbb{Z}$ più avanti.

Definizione 3.6. L'insieme formato dalle classi secondo la relazione di equivalenza, viste come *elementi*, prende il nome di **insieme quoziente**, e si indica (in questo caso) con $\mathbb{Z}/\sim$.

3.2 Congruenze modulo n

Consideriamo sempre l'insieme dei relativi $\mathbb{Z}$.
Istituiamo la relazione di **congruenza modulo** n, che afferma che:

$$x \sim y \Rightarrow x - y = n \cdot k, k \in \mathbb{Z}$$

Questa è una relazione di equivalenza:

- $\forall\ x \in \mathbb{Z} : x - x = 0 = 0 \cdot n, 0 \in \mathbb{Z} \Rightarrow \forall\ x \in \mathbb{Z} : x \sim x$;
- $\forall\ x, y \in \mathbb{Z} : x \sim y \Rightarrow x - y = n \cdot k, k \in \mathbb{Z} \Rightarrow y - x = n \cdot (-k), -k \in \mathbb{Z} \Rightarrow y \sim x$;
- $\forall\ x, y, z \in \mathbb{Z} : x \sim y, y \sim z \Rightarrow x - y = n \cdot k, y - z = n \cdot h, k, h \in \mathbb{Z} \Rightarrow x - y = y - z = x - z = n \cdot (k + h), k + h \in \mathbb{Z} \Rightarrow x \sim z$.

Come sono fatte le classi di equivalenza di $\mathbb{Z}$ secondo la relazione di congruenza? Ogni classe, in effetti, è formata da tutti i numeri che, divisi per n, hanno lo stesso resto. Ecco perchè, in questo particolare caso, si parla di **classi di resto**.

Ad esempio, se n è 3, allora le classi di resto sono 3, e sono:

- La classe contenente tutti i multipli di 3 (che indichiamo con [0], visto che il resto della divisione intera di questi numeri per 3 è 0);
- La classe contenente tutti i multipli di 3 aumentati di 1 (che indichiamo con [1]);
- La classe contenente tutti i multipli di 3 aumentati di 2 (che indichiamo con [2]).

Dunque:

$$\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3 = \{[0], [1], [2]\}$$

Notiamo che il numero delle classi di $\mathbb{Z}_n$ è esattamente n, visto che i possibili resti sono esattamente n: 0, 1, ... , $n-1$.

Definizione 3.7. Definiamo ora le operazioni tra classi di congruenza. Le definizioni sono molto naturali:

- $[a] + [b] = [a + b]$;
- $[a][b] = [ab]$;
- $[a]^k = [a^k]$.

3.3 Criteri di congruenza

Cercheremo ora di dare dimostrazioni dettagliate circa alcuni criteri di congruenza che dovrebbero essere noti. Prima di cominciare, però, dobbiamo familiarizzare con la nozione di **espressione decimale**. Dato un numero $n \in \mathbb{N}$, n è costituito da diverse cifre:

$$n = a_k a_{k-1} \dots a_1 a_0$$

Dunque n ammette la seguente **espressione decimale**:

$$n = 10^k a_k + 10^{k-1} a_{k-1} \dots 10^1 a_1 + 10^0 a_0$$

Scritto in modo più compatto:

$$n = \sum_{j=0}^{k} 10^j a_j$$

Infine, affermiamo che n è divisibile per k se e solo se $[n]_k = [0]_k$.
La fattorizzazione di 10, base del nostro sistema di numerazione, è
$10 = 2 \cdot 5$. Dunque iniziamo dai criteri di congruenza del 2 e del 5, che sono sostanzialmente uguali.

Proposizione 3.3.1. *Un numero è congruo* (mod 2) *o* (mod 5) *alla sua cifra delle unità. Similmente, un numero è congruo* (mod 2^h) *o* (mod 5^h) *al numero formato dalle sue ultime h cifre.*

Dimostrazione. Notiamo subito che:

$$[10]_2 = [0]_2 \Rightarrow \forall\ j \geq 1,\ \forall\ a_k \in \mathbb{N} : [10^j]_2[a_j]_2 = [0]_2$$

$$[10]_5 = [0]_5 \Rightarrow \forall\ j \geq 1,\ \forall\ a_k \in \mathbb{N} : [10^j]_5[a_j]_5 = [0]_5$$

Dunque:

$$[n]_2 = [a_0]_2 + \sum_{j=1}^{k} [10^j]_2[a_j]_2 = [a_0]_2$$

$$[n]_5 = [a_0]_5 + \sum_{j=1}^{k} [10^j]_5[a_j]_5 = [a_0]_5$$

Dunque la proposizione è dimostrata. Nel caso generale, si ha che:

$$[10^h]_2 = [0]_2 \Rightarrow \forall\ j \geq h,\ \forall\ a_k \in \mathbb{N} : [10^j]_2[a_j]_2 = [0]_2$$

$$[10^h]_5 = [0]_5 \Rightarrow \forall\ j \geq h,\ \forall\ a_k \in \mathbb{N} : [10^j]_5[a_j]_5 = [0]_5,$$

e per il resto si procede come nel caso appena analizzato. □

I due criteri immediatamente più impegnativi sono quelli del 3 e del 9.

Proposizione 3.3.2. *Un numero è congruo* (mod 3) *o* (mod 9) *alla somma delle sue cifre.*

Dimostrazione. Si ha innanzitutto:

$$[10]_3 = [1]_3 \Rightarrow \forall\ j \geq 1,\ \forall\ a_k \in \mathbb{N} : [10^j]_3[a_j]_3 = [1^j]_3[a_j]_3 = [a_j]_3$$

$$[10]_9 = [1]_9 \Rightarrow \forall\ j \geq 1,\ \forall\ a_k \in \mathbb{N} : [10^j]_9[a_j]_9 = [1^j]_9[a_j]_9 = [a_j]_9$$

Dunque (analizziamo il caso (mod 3), l'altro è analogo):

$$[n]_3 = \sum_{j=0}^{k} [10^j]_3[a_j]_3 = \sum_{j=0}^{k} [a_j]_3,$$

ossia la tesi. □

Segue, in ordine di difficoltà, il criterio di congruenza per 11.

Proposizione 3.3.3. *Un numero è congruo* (mod 11) *alla somma alternata delle sue cifre, ottenuta iniziando da destra con il segno + (in altre parole: la cifra delle unità si somma, quella delle decine si sottrae, e così via).*

Dimostrazione. In maniera simile a prima:

$$[10]_{11} = [-1]_{11} \Rightarrow \forall\ j \geq 1,\ \forall\ a_k \in \mathbb{N} : [10^j]_{11}[a_j]_{11} =$$

$$= [(-1)^j]_{11}[a_j]_{11} = [(-1)^j a_j]_{11},$$

e la somma alternata nasce dal fatto che:

- $[(-1)^j a_j]_{11} = [-a_j]_{11}$ se $j \equiv 1 \pmod 2$ (ossia è dispari);
- $[(-1)^j a_j]_{11} = [a_j]_{11}$ se $j \equiv 0 \pmod 2$ (ossia è pari).

Dunque:

$$[n]_{11} = \sum_{j=0}^{k} [10^j]_{11}[a_j]_{11} = \sum_{j=0}^{k} [(-1)^j]_{11}[a_j]_{11} =$$

$$= \left(\sum_{\substack{j\,=\,0 \\ j \,\equiv\, 0\ (2)}}^{k} [(-1)^j]_{11}[a_j]_{11} \right) - \left(\sum_{\substack{j\,=\,0 \\ j \,\equiv\, 1\ (2)}}^{k} [(-1)^j]_{11}[a_j]_{11} \right),$$

come volevasi dimostrare. □

Discorso a parte merita il 7: il criterio di congruenza per 7 è meno intuitivo degli altri, e dunque spesso viene trascurato. In questo caso presentiamo solo un paio di enunciati equivalenti, che possono essere dimostrati per esercizio. Seguirà un criterio che non è di congruenza, ma di divisibilità.

Proposizione 3.3.4. *(Solo enunciato) Sono fatti equivalenti:*

- *Un numero è congruo* (mod 7) *alla somma alternata dei suoi gruppi di tre cifre ottenuti a partire da destra;*
- *Un numero è congruo* (mod 7) *alla somma dei suoi gruppi di sei cifre ottenuti a partire da destra.*

Il criterio di divisibilità per 7 afferma che un numero è divisibile per 7 se e solo se lo è il numero che si ottiene sottraendo il doppio della cifra delle unità al numero formato dalle cifre del numero di partenza meno quella delle unità.

Analizzando l'ultima formulazione, forse la più pratica, facciamo un esempio. Dimostriamo che 5677 è divisibile per 7:

$$5677 \equiv 567 - 2 \cdot 7 = 553 \pmod 7$$

$$5677 \equiv 553 \equiv 55 - 2 \cdot 3 = 49 \pmod 7,$$

e qui possiamo fermarci con le iterazioni, visto che sappiamo bene che 49 è divisibile per 7.

Esercizio 24. Determinare un criterio di congruenza per 13.

Esercizio 25. Determinare un criterio di congruenza per 17.

3.4 Esercizi di livello base

I primi esercizi di calcolo congruenziale sembreranno quasi fini a se stessi; tuttavia, una volta raggiunta una buona padronanza con tutto ciò, il calcolo congruenziale si rivela un'arma molto potente, almeno per quanto riguarda i problemi che riguardano le Olimpiadi di Matematica. Non ci si scoraggi, però, se all'inizio non si è capito tutto alla perfezione: l'esercizio costante e l'esperienza contano molto, in questo caso.

Esercizio 26. Se oggi è domenica, che giorno sarà tra 4321 giorni?

Dimostrazione. Questo è un tipico problema che si può risolvere agevolmente con il calcolo congruenziale. Dato che i giorni della settimana sono 7, consideriamo le classi di resto modulo 7, e associamo ad ogni classe, nella nostra mente, il nome di un giorno. Dato che oggi è domenica, assegniamo alla classe 0 il nome *domenica*. In effetti, se il problema ci chiedesse *che giorno è tra* 0 *giorni?*, noi risponderemmo *domenica*. Dunque:

$$\mathbb{Z}_7 = \{[0] = [Dom], [1] = [Lun], \dots [6] = [Sab]\}$$

Allora non ci resta che capire a che classe di resto appartiene 4321. Dunque:

$$4321 = 7 \cdot 617 + 2,$$

dunque la risposta è *martedì*. □

Esercizio 27. Determinare con quale cifra termina il numero:

$$\sum_{i=1}^{94} i^2$$

Dimostrazione. In effetti il problema può essere letto in questo modo: a cosa è congrua, (mod 10), quella sommatoria? La cifra delle unità, infatti, è il resto della divisione di un numero per 10. Acquisiamo un po' di dati relativi alla cifra delle unita' dei quadrati dei vari numeri. Notiamo che la cifra delle unità di i^2 dipende esclusivamente dalla cifra delle unità di i. Dunque:

- $0^2 = 0$;
- $1^2 = 9^2 = 1$;
- $2^2 = 8^2 = 4$;
- $3^2 = 7^2 = 9$;
- $4^2 = 6^2 = 6$;
- $5^2 = 5$.

Osservazione 6. Per i più curiosi, il fatto che i numeri *complementari* abbiano lo stesso quadrato non è un caso. Perchè?

Non ci resta che *spezzare* quella somma in più parti, visto che, con le osservazioni effettuate sopra, sappiamo calcolare la somma dei numeri da 1 a 10, da 11 a 20, e così via. Per ogni gruppo di 10 numeri, infatti, si ha che la cifra delle unità della somma dei quadrati, sia essa c, è:

$$c = [0]_{10} + 2 \cdot [1]_{10} + 2 \cdot [4]_{10} + 2 \cdot [9]_{10} + 2 \cdot [6]_{10} + [5]_{10} =$$

$$= [0]_{10} + [2]_{10} + [8]_{10} + [18]_{10} + [12]_{10} + [5]_{10} = [45]_{10} = [5]_{10}$$

Allora, se chiamiamo c_{tot} la cifra cercata, si ha:

$$c_{tot} = \left[\sum_{i=1}^{94} i^2\right]_{10} = 9 \cdot \left[\sum_{i=1}^{10} i^2\right]_{10} + \sum_{i=1}^{4} i^2 = [9 \cdot 5]_{10} + [20]_{10} = [65]_{10} = [5]_{10},$$

dunque quel numero finisce con 5. □

Esercizio 28. Verificare se è vero o falso che:

$$18 \equiv 2^{192} \pmod 6$$

Dimostrazione. Innanzitutto $18 \equiv 4 \pmod 7$. Quanto a 2^{192} Analizziamo un po' a cosa sono congrue modulo 7 le varie potenze di 2. Abbiamo dunque il seguente schema:

- $2^0 \equiv 1 \pmod 7$;
- $2^1 \equiv 2 \pmod 7$;
- $2^2 \equiv 4 \pmod 7$;
- $2^3 \equiv 1 \pmod 7$;
- $2^4 \equiv 2 \pmod 7$...

Possiamo fermarci, in quanto abbiamo determinato il *periodo* delle potenze di 2 modulo 7, che è 3. Ciò vuol dire che, se $2^0 \equiv 1 \pmod 7$, allora si avrà $2^{3k} \equiv 1 \pmod 7$ per ogni $k \in \mathbb{Z}$. Più precisamente, abbiamo che, se k è l'esponente della potenza di 2, si ha:

- $2^k \equiv 1 \pmod 7 \Leftrightarrow k \equiv 0 \pmod 3$;
- $2^k \equiv 2 \pmod 7 \Leftrightarrow k \equiv 1 \pmod 3$;
- $2^k \equiv 4 \pmod 7 \Leftrightarrow k \equiv 2 \pmod 3$.

Dobbiamo dunque verificare se è vero o no che $192 \equiv 2 \pmod 3$. Dato che ciò è falso, perchè $192 = 3 \cdot 64$,concludiamo che $18 \not\equiv 2^{192} \pmod 6$. □

Esercizio 29. Verificare se è vero o falso che $4^{8888} \equiv 4 \pmod 6$.

Esercizio 30. Verificare se è vero o falso che $2^{5635} \equiv 2 \pmod 3$.

Esercizio 31. Verificare se è vero o falso che $5^{5^5} \equiv 4^4 \pmod 9$.

Esercizio 32. Verificare se è vero o falso che $3^{1234567890987654321} \equiv 3 \pmod{11}$ (ok, questo è veramente esagerato!).

3.5 Esercizi di livello medio

Seguono ora una serie di esercizi decisamente non banali per chi è alle prime armi, che uniscono un po' tutti gli argomenti visti finora. Molti di questi problemi sono tratti da testi di gare di livello provinciale delle Olimpiadi di Matematica di vari anni, dunque ovviamente non ci si aspetta che siano subito compresi a pieno. Essi però sono maggiormente istruttivi rispetto a quelli visti finora, perchè stimolano l'esecutore a ricercare anche il metodo risolutivo migliore.

Esercizio 33. Determinare il più grande intero n con questa proprietà: esistono n interi positivi distinti $a_1, \ldots a_n$ tali che, comunque se ne scelgano fra essi due distinti, nè la loro somma nè la loro differenza siano divisibili per 100.

Dimostrazione. Innanzitutto, un numero è divisibile per 100 se e solo se la sua espressione decimale termina con 00.
Dividiamo gli interi $a_1, \ldots a_n$ in gruppi come segue: in un primo gruppo mettiamo quelli la cui espressione decimale termina con 00, in un secondo gruppo quelli che terminano con 01 (o hanno una sola cifra e quella cifra è 1) oppure con 99, in un terzo quelli che hanno come ultime due cifre 02 o 98 e così via, fino ad arrivare al cinquantunesimo gruppo, in cui inseriamo quelli che terminano con le cifre 50.
Se in uno stesso gruppo vi sono due interi, allora necessariamente la loro differenza, oppure la loro somma, sarà divisibile per 100: se infatti i due interi terminano con lo stesso gruppo di due cifre, allora la loro differenza termina con 00 ed è divisibile per 100; se invece terminano con gruppi di cifre diverse, il fatto che si trovino nello stesso gruppo fa sì che la loro somma sia divisibile per 100.
Dato che abbiamo esattamente 51 gruppi, n vale al massimo 51: se infatti avessimo 52 o più interi, almeno due ricadrebbero nello stesso gruppo e, per quanto detto, la loro differenza, o la loro somma, sarebbe divisibile per 100.
D'altra parte è facile convincersi che 100, 101, ... , 150 è proprio un insieme di 51 interi positivi con la proprietà descritta nel testo, e dunque 51 è il numero richiesto. □

Esercizio 34. Consideriamo i numeri naturali da 1 a 2013. È possibile riordinare in qualche modo questi numeri, in modo che il numero ottenuto per concatenazione sia un quadrato perfetto? Ad esempio, concatenando 34 e 7 si ottiene 347. (Suggerimento: la richiesta sembra davvero assurda...)

Dimostrazione. Un tale riordinamento non esiste. Infatti, considerando il modulo 9, abbiamo che il numero ottenuto per concatenazione è congruo (mod 9) alla somma delle sue cifre. Ma in realtà possiamo affermare che quel numero è congruo alla somma dei numeri da 1 a 2013, visto che poi ognuno di questi numeri è congruo (mod 9) alla somma delle sue cifre. Ma:

$$\left[\sum_{j=1}^{2013} j\right]_9 = [3]_9,$$

e nessun quadrato perfetto è congruo a 3 (mod 9). Infatti, esso dovrebbe avere un fattore 3, ed essendo un quadrato perfetto, però, dovrebbe averne almeno due. Ma allora esso sarebbe multiplo di 9. Dunque un tale riordinamento non esiste. □

Esercizio 35. Per quanti interi relativi n si ha che $\frac{3n}{n+5}$ è intero e divisibile per 4?

Dimostrazione. Sostituendo $m = n + 5$, lespressione data diventa:

$$\frac{3m - 15}{m} = 3 - \frac{15}{m}$$

Affinchè la frazione sia intera, allora, m deve essere un divisore di 15, per cui le possibilità sono solo ± 1, ± 3, ± 5 e ± 15. Di queste, le uniche per cui lespressione è un multiplo di 4 sono 1, -3, 5 e -15, per cui gli n cercati sono -20, -8, -4 e 0. □

Esercizio 36. Qual è la seconda cifra (partendo da sinistra) del numero $(10^{16} + 1)(10^8 + 1)(10^4 + 1)(10^2 + 1)(10 + 1)$? Un indizio:

$$(a + b)(a - b) = a^2 - b^2, a \neq b \Rightarrow a + b = \frac{a^2 - b^2}{a - b}$$

Dimostrazione. Si possono calcolare direttamente tutte le cifre del numero.

Per mezzo dell'indizio, infatti, possiamo affermare che:

$$(10^{16}+1)(10^8+1)(10^4+1)(10^2+1)(10+1) =$$

$$= \frac{1032-1}{1016-1} \cdot \frac{1016-1}{108-1} \cdot \frac{108-1}{104-1} \cdot \frac{104-1}{102-1} \cdot \frac{102-1}{10-1} = \frac{1032-1}{10-1}$$

Ma ora $10^{32}-1$ è costituito da 32 cifre tutte uguali a 9: dunque il rapporto tra $10^{32}-1$ e 9 è costituito da 32 cifre tutte uguali a 1. dunque ogni cifra, la seconda inclusa, è uguale a 1. □

Esercizio 37. In una scatola ci sono venti palline, numerate da 1 a 20. Ciascun numero è presente in una e una sola di queste palline. Quante palline diverse dobbiamo estrarre come minimo, per essere sicuri che il prodotto dei loro numeri sia un multiplo di 12?

Dimostrazione. I multipli di 3 compresi tra 1 e 20 sono 6, dunque ci sono 14 numeri che non sono multipli di 3. Se estraessimo giusto quei 14 numeri, il loro prodotto non sarebbe un multiplo di 3 e men che meno di 12, dunque il numero n di estrazioni minime per assicurarci che il prodotto sia un multiplo di 12 è maggiore di 14. Se estraiamo 15 numeri, invece, avremo sicuramente almeno un multiplo di 3. Dato che i numeri pari compresi tra 1 e 20 sono 10, e quelli dispari 10, con 15 estrazioni ci assicuriamo almeno 5 numeri pari. Dunque il prodotto sarà un multiplo di 3 e un multiplo di $2^5 = 32$. In particolare, sarà multiplo di 3 e di 4, e dunque di 12. Ne consegue che n è proprio 15. □

Esercizio 38. In quanti modi diversi si possono mettere in fila i numeri $\{21, 31, 41, 51, 61, 71, 81\}$ in modo che, comunque se ne scelgano quattro in posti consecutivi, la loro somma sia divisibile per tre?

Dimostrazione. Per brevità indicheremo con *buono* un modo di ordinare i numeri $a_1, \ldots, a_7$ assegnati che soddisfi le caratteristiche richieste. Cerchiamo di stabilire alcune proprietà degli ordinamenti *buoni*:

1. Perchè un ordinamento sia *buono* non è importante quali siano i numeri scelti dall'insieme assegnato ma soltanto qual è il resto della loro divisione per 3;

2. Il resto di ciascuno degli elementi di un ordinamento buono $(a_1, \ldots, a_7)$ è determinato completamente una volta scelto quello dei primi quattro elementi.

   Infatti, dato che l'ordinamento è *buono*, sia $(a_2, \ldots, a_5) = (a_1, \ldots, a_4) + \\ +(a_5 - a_1)$ che $(a_1, \ldots, a_4)$ sono divisibili per tre.

Allora anche $(a_5 - a_1)$ deve esserlo. Questo significa che a_5 ed a_1, se divisi per 3, danno lo stesso resto.

Analogamente possiamo dire la stessa cosa per le coppie a_2, a_6 e a_3, a_7.

3. Il resto della divisione per tre di un numero intero può essere soltanto 0, 1 o 2. Per brevità parleremo di numeri di tipo 0, 1 o 2 a seconda di quale delle tre possibilità si presenti. La somma di quattro numeri è divisibile per tre soltanto se (a meno dell'ordine) i quattro numeri sono di questi tipi: 0, 0, 0, 0 oppure 1, 2, 0, 0 oppure 1, 2, 1, 2. Nell'insieme a nostra disposizione abbiamo però soltanto 3 numeri di tipo 0, $(21, 51, 81)$, soltanto due $(31, 61)$ di tipo 1 e soltanto due $(41, 71)$ di tipo 2.

   Questo esclude la prima e la terza possibilità. Quest'ultima perchè in base alla proprietà 2 dovremmo necessariamente proseguire con altri elementi di tipo 1 o 2, che però non abbiamo a disposizione.

4. Non tutti gli ordinamenti di 1, 2, 0, 0 sono possibili: ancora per la proprietà 2 non possono esserci due numeri di tipo 0 nei primi tre posti. Se così non fosse troveremo ancora due numeri di tipo 0 negli ultimi tre posti per un totale di quattro, ma ne abbiamo a disposizione soltanto tre.

   Di conseguenza il numero al quarto posto deve essere per forza di tipo 0 e i tipi degli elementi a_1, a_2, a_3 devono essere identici a quelli degli elementi a_5, a_6, a_7 rispettivamente.

A questo punto siamo in grado di calcolare quanti sono gli ordinamenti *buoni*:

- L'elemento al quarto posto può essere scelto solo tra 21, 51, 81, ovvero in tre modi diversi;
- Ai primi tre posti ci deve essre un numero di tipo 0, uno di tipo 1 e uno di tipo 2. I modi possibili di ordinare i tipi di numero sono 6;
- Per ciascuno dei tipi dei primi tre elementi della sequenza è possibile scegliere tra due numeri diversi dell'insieme. Quindi per ciascuno dei modi di ordinare i tipi ci sono $2 \cdot 2 \cdot 2 = 8$ modi diversi di scegliere;
- Una volta fatte le scelte ai punti precedenti, gli elementi agli ultimi tre posti sono univocamente determinati.

Riepilogando, il numero di ordinamenti *buoni* è:

$$3 \cdot 6 \cdot 8 = 144$$

□

3.6 Esercizi di livello avanzato

Quelli che seguono sono tre esercizi tratti da vari testi delle edizioni nazionali delle Olimpiadi di Matematica, che si tengono ogni anno a Cesenatico, in Emilia-Romagna. Ogni anno, questi problemi sono letti dai 300 ragazzi più bravi d'Italia, dunque la loro difficoltà è indubbia. Questi problemi non devono spaventare, ma devono aiutare a capire *in tenera età* cosa vuol dire affrontare una gara nazionale, e come ci si pone davanti a questa. Spero che questi appunti abbiano stimolato la voglia, perlomeno, di leggere i tre quesiti che seguono, e comprendere le soluzioni presentate. Premetto che non ci si aspetta assolutamente che uno studente alle prime armi sappia risolvere in maniera agevole questi problemi, però ci si aspetta che uno studente alle prime armi sia perlomeno curioso.

Esercizio 39. **(Cesenatico 2011, es. 2)** Una sequenza di interi positivi $a_1, a_2, \ldots, a_n$ è detta *scaletta* di lunghezza n se è composta da n numeri consecutivi, in ordine crescente.

1. Dimostrare che per ogni intero positivo n esistono due scalette di lunghezza n, senza elementi in comune, $a_1, a_2, \ldots, a_n$ e $b_1, b_2, \ldots, b_n$, tali che per ogni i tra 1 ed n il massimo comune divisore fra a_i e b_i è uguale a 1.

2. Dimostrare che per ogni intero positivo n esistono due scalette di lunghezza n, senza elementi in comune, $a_1, a_2, \ldots, a_n$ e $b_1, b_2, \ldots, b_n$, tali che per ogni i tra 1 ed n il massimo comune divisore fra a_i e b_i è maggiore di 1.

Dimostrazione.

1. Fissiamo n numeri consecutivi $a_1, a_2, \ldots, a_n$. Sia ora d un numero più grande di n che non abbia fattori comuni con nessuno tra $a_1, a_2, \ldots, a_n$ (ad esempio il minimo comunque multiplo aumentato di 1, oppure un numero primo più grande di a_n).

   Poniamo allora $b_1 = a_1 + d, b_2 = a_2 + d, \ldots, b_n = a_n + d$. Allora $a_1, a_2, \ldots, a_n$ e $b_1, b_2, \ldots, b_n$ sono due scalette di lunghezza n disgiunte fra loro e tali che, per ogni i tra 1 ed n, il massimo comune divisore fra a_i e b_i è uguale a 1: infatti, se esistesse un fattore comune di a_i e b_i, questo sarebbe un fattore anche di $b_i - a_i = d$, e questo è impossibile, perchè d e a_i non hanno fattori in comune.

2. Analogamente a prima fissiamo $a_1, a_2, \ldots, a_n$ consecutivi, con $a_1 > 1$; prendiamo poi un intero $d > n$ che abbia fattori in comune con ognuno

degli elementi $a_1, a_2, \ldots, a_n$ (ad esempio, il minimo comune multiplo), e fissiamo $b_1 = a_1 + d, b_2 = a_2 + d, \ldots, b_n = a_n + d$.

Ancora una volta le scalette $a_1, a_2, \ldots, a_n$ e $b_1, b_2, \ldots, b_n$ sono disgiunte fra loro, ma in questo caso a_i e b_i hanno sempre un fattore in comune: infatti a_i e d hanno sempre un fattore in comune, e quindi lo stesso è vero per a_i e $d + a_i = b_i$.

□

Esercizio 40. **(Cesenatico 2011, es. 3)** Su una lavagna sono scritti i numeri interi compresi fra 1 e 7. È possibile che non tutti i numeri da 1 a 7 siano presenti, ed è anche possibile che uno, alcuni o tutti i numeri siano ripetuti, una o più volte. Una mossa consiste nello scegliere uno o più numeri presenti sulla lavagna, purchè tutti diversi, cancellarli, e scrivere al loro posto i numeri che, unitamente a quelli cancellati, formano l'intero insieme $\{1, 2, 3, 4, 5, 6, 7\}$. Ad esempio, mosse consentite sono:

- Cancellare un 4 ed un 5, e scrivere al loro posto i numeri 1, 2, 3, 6 e 7;
- Cancellare un 1, un 2, un 3, un 4, un 5, un 6 ed un 7 senza scrivere niente al loro posto.

Dimostrare che, se è possibile trovare una sequenza di mosse che, partendo dalla situazione iniziale, porti ad avere sulla lavagna un unico numero (scritto una sola volta), allora questo numero non dipende dalla sequenza di mosse utilizzata.

Dimostrazione. Chiamiamo n_1 il numero di cifre 1 presenti in un certo momento sulla lavagna, n_2 il numero di cifre 2, e così via fino ad n_7. Ogni volta che si fa una mossa, ognuna di queste molteplicità cambia di 1 (e quindi inverte la sua parità), perchè ogni numero tra 1 e 7 viene scritto o cancellato. Supponiamo che dopo una sequenza di k mosse rimanga sulla lavagna un unico numero, diciamo x; n_x ha cambiato parità k volte ed è infine dispari; tutte le altre molteplicità, cambiando parità anchesse k volte, risultano infine uguali a zero, quindi pari.
Anche nella situazione iniziale, perciò, n_x deve avere parità diversa da ogni altra molteplicità. Non esiste quindi alcuna sequenza di mosse che porti ad avere sulla lavagna un'unica copia di un numero y diverso da x: n_y dovrebbe partire con parità diversa da tutte le altre molteplicità, ma abbiamo già stabilito che ha la stessa parità di n_z per tutti i numeri z diversi da x. □

Esercizio 41. **(Cesenatico 2012, es. 4)** Sia $x_1, x_2, x_3, \dots$ la successione definita per ricorrenza come segue:

$$\begin{cases} x_1 = 4 \\ x_n = x_1 x_2 \dots x_{n-1} + 5 \quad \forall\ n \geq 2 \end{cases}$$

(I primi termini della successione sono quindi $x_1 = 4, x_2 = 4 + 5 = 9$,
$x_3 = 4 \cdot 9 + 5 = 41, \dots$)
Trovare tutte le coppie non ordinate di interi positivi distinti (a, b) tali che $x_a \cdot x_b$ è un quadrato perfetto.

Dimostrazione. Dimostreremo che l'unica coppia che soddisfa la condizione è $(1, 2)$. Innanzitutto, questa coppia è valida, e si trova anche abbastanza intuitivamente (insomma, un po' ci si sporca le mani, prima di risolvere un problema!).

Un quadrato perfetto si può ottenere, a partire da due fattori, esclusivamente in due modi:

- Entrambi i fattori sono quadrati perfetti;
- Entrambi i fattori non sono quadrati perfetti, ma hanno tutti i fattori in comune, elevati peraltro ad una potenza dispari.

Escluderemo ora entrambi questi casi. Cominciamo col primo, il più semplice.

Notiamo subito che ogni numero della successione successivo al 9 (dunque un numero del tipo $x_k, k > 2$) è congruo 2 (mod 3), visto che esso è costituito da una produttoria di numeri tra cui è incluso il 9 (dunque multipla di 3) sommata a 5. Dato che $5 \equiv 2 \pmod 3$, si ha che:
$\forall\ k > 2 : x_k \equiv 2 \pmod 3 \Rightarrow \forall\ k > 2 : x_k$ non è un quadrato perfetto
Infatti i quadrati sono congrui a 0 o 1 (mod 3), mai a 2. Dunque, oltre a 4 e 9, la successione non presenta altri quadrati.

Escludiamo ora l'altro caso. Prendiamo due numeri qualsiasi diversi, x_a e x_b. Supponiamo $a > b$, dunque $x_a > x_b$. Consideriamo tutti i fattori primi di x_b. Risulterà che, per ogni fattore primo p di x_b, $x_a \equiv 5 \pmod p$. Dunque, a meno che $p = 5$, si ha $[5]_p \neq [0]_p$. Se dunque escludiamo il caso $p = 5$, abbiamo dimostrato che, presi due qualsiasi numeri diversi della successione, essi sono primi tra loro, dunque *a fortiori* non possono formare un quadrato perfetto, se moltiplicati tra loro (a meno che non siano già essi stessi quadrati, da cui il caso già individuato).

Dimostriamo allora per *induzione forte* che nessun numero della successione è divisibile per 5:

- 4 non è divisibile per 5, e ciò è palese;
- Supponiamo che $x_1, \dots x_{n-1}$ non siano divisibili per 5. Allora neanche il numero formato dal loro prodotto è divisibile per 5, non contenendo alcun fattore 5. Sommare 5 al numero ottenuto non cambia la sua classe di equivalenza (mod 5). Dunque x_n non è divisibile per 5.

□