

Note di
ARITMETICA

Mauro Saita

e-mail: maurosaita@tiscalinet.it

1

Indice

1 Numeri naturali.	3
2 Numeri interi	5
2.1 L'anello $\mathbb{Z}$ dei numeri interi.	5
2.2 La divisione in $\mathbb{Z}$: quoziente e resto	6
3 Numeri primi. Teorema fondamentale dell'aritmetica	7
3.1 Attività per il laboratorio di matematica	8
3.2 Quanto tempo serve per fattorizzare un numero?	8
3.3 Il massimo comun divisore	9
3.4 L'algoritmo di Euclide per il calcolo del massimo comun divisore di due numeri.	10
3.5 Attività per il laboratorio di matematica	12
3.6 Il teorema di Euclide	13
3.7 Curiosità sui numeri primi	14
4 Numeri figurati	15
4.1 Numeri triangolari	16
4.2 Numeri tetraedrici	18
4.3 Numeri piramidali quadratici	20
5 Aritmetica modulare. Classe di resti	22

¹Nome File: aritmetica_2016.tex

5.1	Le proprietà delle congruenze	24
5.2	Le operazioni in $\mathbb{Z}_n$: l'addizione e la moltiplicazione	24

1 Numeri naturali.

I numeri naturali sono $0, 1, 2, 3$, eccetera e si indicano con la lettera $\mathbb{N}$. Si scrive:

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}$$

In $\mathbb{N}$ sono definite due operazioni: la somma e il prodotto, non è invece possibile definire la differenza e la divisione perchè la differenza (il quoziente) di due numeri naturali non è sempre un numero naturale.

I numeri *pari* sono i numeri naturali multipli di due. Se x è un numero pari si scrive:

$$x = 2n, \quad n \in \mathbb{N}$$

I numeri *dispari* sono i numeri naturali che non sono multipli di due. Se x è un numero dispari si scrive:

$$x = 2n + 1, \quad n \in \mathbb{N}$$

Esercizio 1.1. *Dimostrare le seguenti proprietà riguardanti i numeri pari e dispari*

1. *La somma di due numeri dispari è un numero pari.*
2. *La somma di un numero pari con un numero dispari è un numero dispari.*
3. *La somma di due numeri pari è un numero pari.*
4. *Il prodotto di due numeri dispari è un numero dispari.*
5. *Il prodotto di due numeri di cui uno è pari, è pari.*

Dimostrazione dell'enunciato 2.

IPOTESI: x è un numero pari; y è un numero dispari

TESI: $x + y$ è un numero dispari

DIMOSTRAZIONE.

Per ipotesi x è un numero pari e y è un numero dispari, quindi

$$\begin{aligned} x &= 2n, \text{ con } n \in \mathbb{N} \\ y &= 2m + 1, \text{ con } m \in \mathbb{N}. \end{aligned}$$

Allora si ha:

$$x + y = 2n + (2m + 1) = (2n + 2m) + 1 = 2(n + m) + 1$$

Ovvero

$$x + y = 2(n + m) + 1$$

$n + m \in \mathbb{N}$ perchè la somma di due numeri naturali è sempre un numero naturale ($\mathbb{N}$ è *chiuso* rispetto all'operazione 'somma'). Pertanto, dall'ultima uguaglianza, si deduce che $x + y$ è dispari. ■

Esercizio 1.2. *Si consideri la differenza fra i quadrati di due numeri naturali consecutivi:*

$$\begin{array}{rcl} 1^2 - 0^2 & = & 1 \\ 2^2 - 1^2 & = & 3 \\ 3^2 - 2^2 & = & 5 \\ 4^2 - 3^2 & = & 7 \\ \dots\dots & = & \dots \end{array}$$

In questo modo si ottiene la successione dei numeri dispari. Come si può fare per dimostrare questo fatto?

Esercizio 1.3. *Provare che la differenza fra i cubi di due numeri naturali consecutivi è un numero dispari.*

Esercizio 1.4 (Gauss, ~ 1787). *Dimostrare che la somma dei primi n numeri interi positivi è data da:*

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

Esercizio 1.5. *Dimostrare che la somma dei primi n numeri dispari è uguale a n^2 .*

L'insieme dei numeri naturali è *infinito*, proprietà che nasconde qualche insidia. A titolo di esempio si veda il seguente

Problema. L'albergo più grande dell'universo ²

Tra tutti gli alberghi, il più interessante dal punto di vista dei numeri è ... un albergo immaginario, un albergo che non esiste, ma che, se esistesse, sarebbe il più grande dell'universo! Il nostro albergo immaginario dispone di un numero infinito di stanze: ci sarebbe da meravigliarsi se un potenziale cliente venisse mandato via per mancanza di camere libere. Forse anche per questo il proprietario non registra molto accuratamente gli ospiti, e quindi non sa mai con precisione quali sono le stanze libere e quelle occupate. L'altro ieri, ad esempio, si è presentato un ospite inatteso; il proprietario, pur non conoscendo qual era in quel momento la situazione delle stanze, non si è perso d'animo: ha chiesto ad ogni cliente di traslocare

²Questo problema è tratto da libro di Giuliano Spirito, "Grammatica dei numeri", Editori Riuniti.

nella stanza con il numero immediatamente maggiore (i clienti di un albergo infinito devono essere disposti ad una certa mobilità!), cosicchè la camera n. 1 fosse certamente libera. Ieri, si sono presentati all'improvviso 200 partecipanti a un convegno; di nuovo il proprietario ha fronteggiato egregiamente la situazione. Ha pregato, infatti, ogni cliente di traslocare; questa volta, però, ciascuno doveva spostarsi nella stanza il cui numero fosse il numero della camera precedente occupata maggiorato di 200. In questo modo il nostro proprietario è riuscito a liberare le prime 200 stanze per i nuovi ospiti. Ma oggi il proprietario si trova davvero in difficoltà: già l'albergo ospitava infiniti clienti, quand'ecco che si presenta una comitiva di infiniti turisti giapponesi Come farà a cavarsela in questa occasione l'albergatore?

2 Numeri interi

I numeri interi sono $0, \pm 1, \pm 2, \pm 3, \dots$ e si indicano con la lettera $\mathbb{Z}$. Si scrive:

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \dots\}$$

L'insieme $\mathbb{Z}$ contiene l'insieme $\mathbb{N}$ ($\mathbb{Z} \supset \mathbb{N}$) e, di conseguenza, anche $\mathbb{Z}$ è un insieme infinito.

2.1 L'anello $\mathbb{Z}$ dei numeri interi.

Nell'insieme $\mathbb{Z}$ dei numeri interi sono definite due operazioni fondamentali: quella di somma e quella di prodotto. Per ogni $a, b \in \mathbb{Z}$ la loro somma si denota ' $a + b$ ' e il loro prodotto si denota ' $a \cdot b$ '.

Per l'operazione ' $+$ ' di somma valgono le seguenti proprietà

1. *Proprietà commutativa* Per ogni $a, b \in \mathbb{Z}$

$$a + b = b + a$$

2. *Proprietà associativa* Per ogni $a, b, c \in \mathbb{Z}$

$$(a + b) + c = a + (b + c)$$

3. *Esistenza dell'elemento neutro della somma.* Per ogni $a \in \mathbb{Z}$ vale

$$a + 0 = 0 + a = a$$

Il numero 0 si chiama 'elemento neutro' della somma.

4. *Esistenza dell'elemento opposto.* Per ogni elemento $a \in \mathbb{Z}$ esiste un elemento $b \in \mathbb{Z}$, detto *opposto* di a , per il quale si ha

$$a + b = b + a = 0$$

L'opposto di a è il numero $b = -a$.

Per l'operazione ' $\cdot$ ' di prodotto valgono le seguenti proprietà

1. *Proprietà commutativa* Per ogni $a, b \in \mathbb{Z}$

$$a \cdot b = b \cdot a$$

2. *Proprietà associativa* Per ogni $a, b, c \in \mathbb{Z}$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

3. *Esistenza dell'elemento neutro del prodotto.* Per ogni $a \in \mathbb{Z}$ vale

$$a \cdot 1 = 1 \cdot a = a$$

Il numero 1 si dice *elemento neutro del prodotto*.

Infine, valgono le leggi distributive: per ogni $a, b, c \in \mathbb{Z}$,

$$(a + b) \cdot c = a \cdot c + b \cdot c \quad \text{e} \quad c \cdot (a + b) = c \cdot a + c \cdot b.$$

Riassumendo: in $\mathbb{Z}$ sono definite le operazioni di somma e prodotto; per tali operazioni valgono le proprietà sopra enunciate. Tutto ciò si sintetizza dicendo che $\mathbb{Z}$ è un *anello commutativo*.

2.2 La divisione in $\mathbb{Z}$: quoziente e resto

Teorema 2.1. Algoritmo della divisione *Dati due interi a, b , con $b > 0$, esistono e sono unici due interi q, r per i quali:*

- $a = bq + r$
- $0 \leq r < b$

Se a e b sono interi, diciamo che b *divide* a , e scriviamo $b \backslash a$, se esiste un intero h per il quale

$$a = hb.$$

Quindi, b *divide* a se il resto della divisione di a per b è zero. Diremo allora che b è un *divisore* di a e che a è un *multiplo* di b .

Esercizio 2.2. *Determinare quoziente e resto delle seguenti coppie di numeri:*

a]	$a = 28$	$b = 7$;	e]	$a = 15$	$b = 6$;	i]	$a = -15$	$b = 6$;
b]	$a = 31$	$b = 9$;	f]	$a = 23$	$b = 15$;	l]	$a = -20$	$b = 4$;
c]	$a = 75$	$b = 2$;	g]	$a = 88$	$b = 11$;	m]	$a = -9$	$b = 4$;
d]	$a = 30$	$b = 6$;	h]	$a = -27$	$b = 8$;	n]	$a = -23$	$b = 15$;

Esercizio 2.3. *Provare che il prodotto di due numeri pari consecutivi è divisibile per 8.*

3 Numeri primi. Teorema fondamentale dell'aritmetica

Abbiamo appena visto che se a e b sono due interi con $b > 0$ esistono sempre, e sono unici, il quoziente q e il resto r della divisione di a per b .

Se il resto di tale divisione è zero (cioè $r=0$) abbiamo ovviamente $a = bq$ e in questo caso diciamo che b è un divisore di a .

Per esempio, il numero 15 ammette esattamente 4 divisori (1,3,5,15), il numero 360 ammette esattamente 24 divisori. Naturalmente ogni numero intero ammette sempre due divisori positivi, 1 e il numero n stesso. I numeri interi che ammettono esattamente due divisori positivi rivestono un ruolo particolarmente importante in diversi ambiti della matematica.

Diamo allora la seguente importante

Definizione 3.1. *Un intero $p > 1$ si dice primo se i suoi unici divisori positivi sono 1 e p ; diciamo che un intero $m > 1$ è composto se non è primo.*

Un primo fatto che evidenzia l'importanza dei numeri primi è questo: ogni intero $n > 1$ si può sempre esprimere come prodotto di numeri primi.

Per esempio, consideriamo il numero 2860. È facile convincersi che $2860 = 2 \cdot 5 \cdot 286 = 2 \cdot 5 \cdot 2 \cdot 143$. I numeri 2 e 5 sono primi; se 143 fosse primo la scomposizione in fattori primi sarebbe ultimata, ma $143 = 11 \cdot 13$ e i numeri 11 e 13 sono primi. Allora abbiamo $2860 = 2^2 \cdot 5 \cdot 11 \cdot 13$.

In generale, ogni intero n maggiore di 1, o è primo, e in tal caso la sua fattorizzazione coincide con il numero stesso, oppure è composto, e allora ammette almeno un divisore d (diverso da 1 e n) per il quale $n = qd$. Ora, se q e d sono primi abbiamo trovato la fattorizzazione di n , altrimenti, applicando il ragionamento appena esposto ai numeri q e d , otteniamo la fattorizzazione cercata e cioè

$$n = p_1 \cdots p_h \tag{3.1}$$

dove gli interi p_i sono primi non necessariamente distinti.

Si potrebbe inoltre dimostrare (ma noi non lo facciamo) che $\forall n \in \mathbb{Z}$ con $n > 1$ la scrittura 3.1 è *unica* a meno dell'ordine dei fattori.

Questo significa che qualunque intero $n > 1$ è completamente caratterizzato dai numeri primi che lo compongono. Per esempio 2580 è caratterizzato da una propria sequenza di numeri primi che è diversa da quella di tutti gli altri, e precisamente $2580 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 43$.

Le considerazioni sopra esposte costituiscono il

Teorema 3.2. (Teorema fondamentale dell'aritmetica) *Ogni intero $n > 1$ può essere scritto come prodotto*

$$n = p_1 \cdots p_h$$

dove gli interi $p_1 \cdots p_h$ sono primi e $h \geq 1$. Questa espressione è unica, a meno dell'ordine dei fattori primi.

Esercizio 3.3. *Scrivere il più piccolo numero n che abbia come divisori distinti da 1 e da n stesso, i numeri 3, 5, 7.*

Esercizio 3.4. *Sia n un intero maggiore di uno e sia $n = p_1^{s_1} \cdot p_2^{s_2} \cdots p_h^{s_h}$ la sua fattorizzazione in numeri primi. Stabilire quanti sono i divisori di n .*

3.1 Attività per il laboratorio di matematica

Esercizio 3.5. *Pensare un algoritmo che consenta di decidere se un numero n è primo o composto. Scrivere il diagramma di flusso e la relativa pseudocodifica.*

Per la risoluzione del precedente esercizio può essere utile il seguente risultato.

Proposizione 3.6. *Se $n \in \mathbb{N}$ è composto allora ammette almeno un divisore proprio minore o uguale di $\sqrt{n}$.*

Dimostrazione.

Per ipotesi n è composto, allora possiamo scrivere: $n = ab$ dove $a \in \mathbb{Z}$ e $b \in \mathbb{Z}$.

I numeri a e b non possono essere entrambi maggiori o entrambi minori di $\sqrt{n}$, altrimenti il loro prodotto sarebbe maggiore oppure minore di n . Possiamo pertanto concludere che se n è composto deve avere un divisore proprio compreso tra 2 e $\sqrt{n}$.

Esercizio 3.7. *Pensare un algoritmo che consenta di fattorizzare un numero intero $n > 0$. Scrivere diagramma di flusso relativa pseudocodifica.*

3.2 Quanto tempo serve per fattorizzare un numero?

L'algoritmo trovato in laboratorio per la fattorizzazione di un intero positivo presenta alcuni limiti. Esso può servire per fattorizzare numeri di poche cifre ma diventa inutilizzabile per numeri grandi, con più di 100 cifre. La ragione di questo fatto non dipende dalla particolare soluzione trovata: ancora oggi *non si conoscono algoritmi efficienti per la fattorizzazione di numeri interi molto grandi*. Nella seguente tabella sono riportati i tempi di fattorizzazione di interi molto grandi avendo a disposizione le migliori tecnologie odierne.³

³I dati riportati nella seguente tabella sono stati ottenuti con l'Intelligenza Artificiale (settembre 2026)

Numeri interi	tempi per un test di primalità	tempi per la fattorizzazione
interi di 100 cifre	< di un millisecondo	2 ore
interi di 200 cifre	un secondo	3 – 15 anni
interi di 250 cifre	qualche secondo	50 – 100 anni
interi di 1000 cifre	alcuni minuti	miliardi di miliardi di anni

3.3 Il massimo comun divisore

Dati due interi a e b , non entrambi nulli, il loro massimo comun divisore, che si denota con

$$MCD(a, b)$$

è il maggiore tra i divisori comuni di a e b .

In altri termini diciamo che il $MCD(a, b)$ è un numero d caratterizzato dalle due seguenti proprietà:

- d è un divisore di a e b .
- Se d' è un divisore comune di a e b allora $d' \leq d$.

Ad esempio:

1) $MCD(12, 8) = 4$;

2) $MCD(-12, 8) = 4$;

3) $MCD(15, 0) = 15$ e, in generale, $MCD(a, 0) = |a|$, per ogni $a \neq 0$;

4) $MCD(8, 9) = 1$. Due numeri, come 8 e 9, il cui massimo comun divisore è 1, si dicono *primi tra loro*.

Una proprietà molto importante del massimo comun divisore che utilizzeremo più avanti è la seguente:

Il massimo comun divisore di due numeri a e b si può sempre scrivere come combinazione lineare, a coefficienti interi, di a e b e cioè :

$$MCD(a, b) = ha + kb$$

per opportuni interi h e k .

Per esempio il $MCD(12, 8)$ si può scrivere nel seguente modo:

$$MCD(12, 8) = +1 \cdot 12 - 1 \cdot 8.$$

In particolare, se a e b sono primi fra loro, allora esistono due interi h e k per i quali

$$ha + kb = 1. \quad (3.2)$$

3.4 L'algoritmo di Euclide per il calcolo del massimo comun divisore di due numeri.

Conosciamo già un metodo per determinare il massimo comun divisore di due numeri. Per esempio, se si deve calcolare il $MCD(a, b)$ con $a = 24$ e $b = 80$ si deve prima *fattorizzare in numeri primi* il numero a e il numero b . Con facili conti, si ottiene $a = 2^3 \cdot 3$ e $80 = 2^2 \cdot 3^2 \cdot 5$. Il $MCD(a, b)$ si ottiene moltiplicando tra loro *i fattori primi comuni ad a e b presi una sola volta con il minimo esponente*. Nel nostro caso si ottiene: $MCD(a, b) = 2^2 \cdot 3 = 12$. Il metodo qui ricordato è corretto e, naturalmente, si può utilizzare tutte le volte che si vuole!

Tuttavia, se si vuole determinare il $MCD(a, b)$ di due numeri molto grandi, per esempio se

$$a = 52384119910237 \text{ e } b = 1246789762374$$

è facile convincersi che la nostra tecnica non è poi così comoda. Essa, infatti prevede la scomposizione in numeri primi dei due numeri dati e, come sottolineato nel paragrafo precedente, questa operazione nasconde molte insidie.

Come fare, allora? È possibile determinare il massimo comun divisore di due numeri senza doverli preventivamente scomporre in fattori primi? La risposta è affermativa: Euclide, più di 2300 anni fa, scoprì un bellissimo algoritmo che inserì nel Libro 7 degli *Elementi* (circa 300 a.C.).

L'algoritmo di Euclide. Siano a e b due interi positivi di cui si vuole determinare il loro massimo comun divisore. Sappiamo allora che esistono e sono unici due numeri q e r per i quali si ha:

$$a = bq + r \quad \text{dove} \quad 0 \leq r < b$$

L'idea di Euclide si basa su questa semplice considerazione:

$$MCD(a, b) = MCD(b, r) \quad (3.3)$$

DIMOSTRAZIONE:

Se un intero d divide sia a che b , allora divide anche la differenza $a - qb = r$; quindi d è anche un divisore comune di b e r .

Viceversa, se d divide sia b che r , allora divide anche la somma $qb + r = a$; quindi d è anche un divisore comune di a e b .

Dunque i divisori comuni di a e b sono esattamente i divisori comuni di b e r , e pertanto $MCD(a, b) = MCD(b, r)$. $\square$

Se si vuole determinare il $MCD(a, b)$ nel caso in cui $a = 2406$ e $b = 654$, mediante divisioni successive si costruisce la seguente tabella:

a	b	$a = bq + r$	q	r
2406	654	$2406 = 3 \times 654 + 444$	3	444
654	444	$654 = 1 \times 444 + 210$	1	210
444	210	$444 = 2 \times 210 + 24$	2	24
210	24	$210 = 8 \times 24 + 18$	8	18
24	18	$24 = 1 \times 18 + 6$	1	6
18	6	$18 = 3 \times 6 + 0$	3	0

Allora il $MCD(2406, 654) = 6$. Infatti, applicando ripetutamente l'uguaglianza 3.3, abbiamo:

$$\begin{aligned}
 MCD(2406, 654) &= MCD(654, 444) \\
 MCD(444, 210) &= MCD(210, 24) \\
 MCD(24, 18) &= MCD(18, 6) \\
 MCD(6, 0) &= 6
 \end{aligned}$$

Quanto all'ultima uguaglianza, si ricordi che per ogni intero positivo a ,

$$MCD(a, 0) = a.$$

Quindi *l'ultimo resto non nullo è il massimo comun divisore* di a e b .

In termini generali, l'algoritmo di Euclide per la ricerca del massimo comun divisore di due interi a , b , consiste nell'effettuare le divisioni successive:

$$\begin{aligned}
 a &= q_1 b + r_1 & (0 \leq r_1 < b) \\
 b &= q_2 r_1 + r_2 & (0 \leq r_2 < r_1) \\
 r_1 &= q_3 r_2 + r_3 & (0 \leq r_3 < r_2) \\
 \dots & & \dots \\
 r_{n-2} &= q_n r_{n-1} + r_n & (0 \leq r_n < r_{n-1}) \\
 r_{n-1} &= q_{n+1} r_n + 0
 \end{aligned}$$

Si osservi che i successivi resti che si ottengono sono non negativi e decrescono strettamente:

$$r_1 > r_2 > r_3 > \dots > r_{n-1} > \dots$$

Quindi dopo un numero finito di passi si arriva a un resto nullo. Applicando ripetutamente l'uguaglianza 3.3, abbiamo:

$$\begin{aligned}
 MCD(a, b) &= MCD(b, r_1) \\
 MCD(b, r_1) &= MCD(r_1, r_2) \\
 MCD(r_1, r_2) &= MCD(r_2, r_3) \\
 &\vdots \quad \ddots \quad \vdots \\
 MCD(r_{n-2}, r_{n-1}) &= MCD(r_{n-1}, r_n) \\
 MCD(r_{n-1}, r_n) &= MCD(r_n, 0) = r_n.
 \end{aligned}$$

Quindi l'ultimo resto r_n non nullo è il massimo comun divisore di a e b .

Esercizio 3.8. Utilizzando l'algoritmo di Euclide calcolare il $MCD(a, b)$ nei seguenti casi:

$$\begin{array}{lll}
 1] a = 128 \ b = 72; & 2] a = 84 \ b = 56; & 3] a = 484 \ b = 30; \\
 4] a = 402 \ b = 93; & 5] a = 85 \ b = 20; & 6] a = 60 \ b = 5;
 \end{array}$$

3.5 Attività per il laboratorio di matematica

Esercizio 3.9. Realizzare un foglio elettronico per il calcolo del massimo comun divisore tra due numeri che utilizzi l'algoritmo di Euclide.

È facile constatare, dopo aver eseguito qualche test, la straordinaria efficienza dell'algoritmo di Euclide. A titolo di curiosità si segnala il seguente importante risultato

Teorema 3.10. (Teorema di Lamé⁴) Siano a e b due interi positivi con $a \geq b$. Allora il numero di divisioni eseguite dall'algoritmo di Euclide per trovare il $MCD(a, b)$ è minore o uguale a cinque volte il numero di cifre di b .

Esercizio 3.11. Siano a e b due interi. Dopo aver verificato che vale la seguente uguaglianza

$$a \cdot b = MCD(a, b) \cdot mcm(a, b)$$

realizzare un foglio di calcolo che determini il minimo comune multiplo di due numeri interi assegnati.

Esercizio 3.12. Con l'ausilio di un foglio elettronico determinare i numeri primi compresi tra 1 e 100 utilizzando il cosiddetto "crivello di Eratostene".

⁴Gabriel Lamé (1795-1870) è considerato da Gauss il più importante matematico francese del suo tempo.

3.6 Il teorema di Euclide

Affrontiamo ora il seguente

Problema 3.13. *Quanti sono i numeri primi?*

Rispondere a questa domanda non è facile perché gli interi positivi sono infiniti. È possibile però calcolare quanti sono i numeri primi in alcuni intervalli prestabiliti di numeri interi. Si osservi la seguente tabella

<i>Intervallo</i>	<i>numeri primi compresi</i>	<i>densità</i>
1 – 1000	168	16,8
1000 – 2000	135	13,5
2000 – 3000	127	12,7
3000 – 4000	120	12,0
4000 – 5000	119	11,9
29000 – 30000	92	9,2
999000 – 1000000	65	6,5

È curioso osservare che la densità dei numeri primi va lentamente diminuendo! Questo significa che via via che ci si allontana dallo zero diventa sempre più difficile trovare un numero primo.

Si potrebbe addirittura pensare che i numeri primi siano in numero finito ma non è così: Euclide (III sec. a.C.) ha infatti dimostrato⁵ il seguente celebre teorema:

Teorema 3.14 (Euclide). *L'insieme dei numeri primi è infinito.*

Dimostrazione. Ragioniamo per assurdo. Supponiamo che l'insieme dei numeri primi sia finito:

$$\{2, 3, 5, \dots, p\},$$

dove p è il più grande di tutti i numeri primi. Moltiplichiamo tra loro tutti questi numeri e aggiungiamo 1 al risultato. Otteniamo così il numero

$$N = 2 \cdot 3 \cdot 5 \cdots p + 1.$$

Questo numero N non è divisibile per 2, perché la sua espressione ci dice che, dividendolo per 2, si ottiene il resto 1. Per lo stesso motivo, N non è divisibile per 3, né per 5, ..., né per p . Abbiamo così trovato un numero che non è divisibile per nessuno dei numeri primi $2, 3, 5, \dots, p$.

Questo fatto può significare due cose:

⁵Nel libro IX, proposizione 20 degli *Elementi* Euclide afferma “I numeri primi sono più di una qualsiasi assegnata moltitudine di numeri primi”.

- 1) N è primo, ma ciò è assurdo perché $N > p$;
 2) N è costituito da numeri primi che non appartengono alla collezione $\{2, 3, 5, \dots, p\}$, ma ciò è assurdo perché la collezione $\{2, 3, 5, \dots, p\}$ doveva esaurire tutti i numeri primi.

Dunque, l'insieme dei numeri primi è infinito. $\square$

Sottolineiamo che l'argomentazione del teorema di Euclide permette di concludere che la successione dei numeri primi è infinita ma *non fornisce una legge per determinare nuovi numeri primi*.

Consideriamo infatti i seguenti elenchi di numeri primi:

$$\{2\}, \quad \{2, 3\} \quad \{2, 3, 5\} \quad \{2, 3, 5, 7\} \quad \{2, 3, 5, 7, 11\} \quad \{2, 3, 5, 7, 11, 13\}$$

Allora i numeri

$$\begin{aligned} 2 + 1 \\ 2 \cdot 3 + 1 \\ 2 \cdot 3 \cdot 5 + 1 \\ 2 \cdot 3 \cdot 5 \cdot 7 + 1 \\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 \end{aligned}$$

sono primi, mentre il numero

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$$

non è primo e i suoi fattori primi 59 e 509 non appartengono all'insieme

$$\{2, 3, 5, 7, 11, 13\}.$$

3.7 Curiosità sui numeri primi

I numeri primi hanno da sempre affascinato i matematici e, fin dall'antichità, essi hanno cercato di indagarne tutti i segreti. Oggi sono molte le informazioni che possediamo a loro riguardo, ma questo non deve far credere che ogni domanda riguardante i numeri primi abbia trovato una risposta soddisfacente. Ad esempio i due problemi qui sotto riportati attendono ancora una risposta!

I numeri primi gemelli

La successione dei numeri primi mette in evidenza coppie di numeri primi che differiscono di 2. Per esempio, 5, 7; oppure 11, 13; 17, 19 e così via. Questi numeri si dicono *numeri primi gemelli*.

La domanda è questa: quante sono le coppie di numeri primi di questo tipo? In altre parole, quanti sono i numeri primi gemelli?

La congettura di Goldbach

Ogni numero pari, maggiore di due, si può scrivere come somma di due numeri primi. Per esempio, $8 = 5 + 3$; $12 = 7 + 5$; $16 = 13 + 3$ e così via.

Fino ad oggi nessuno è riuscito a dimostrare che questa affermazione è vera, e nemmeno si è riusciti a mostrare, con un controesempio, che è falsa.

4 Numeri figurati

L'idea è quella di trovare forme geometriche che contraddistinguano particolari successioni numeriche in modo tale da dedurre le proprietà aritmetiche dei numeri da proprietà di carattere geometrico. Lo slogan di questa sezione è:

*studiare l'aritmetica servendosi
della geometria.*

Iniziamo con il trovare una forma geometrica per rappresentare i numeri pari e i numeri dispari.

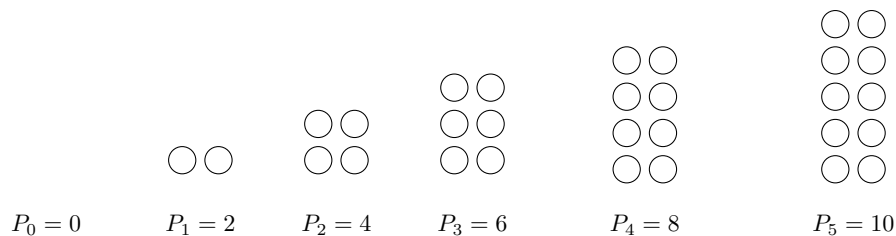


Figura 1: Rappresentazione geometrica dei numeri pari (P_n)

I numeri *pari* sono *rettangoli di base due*. Il primo numero pari, lo zero, si può pensare come un rettangolo di base due e altezza nulla.

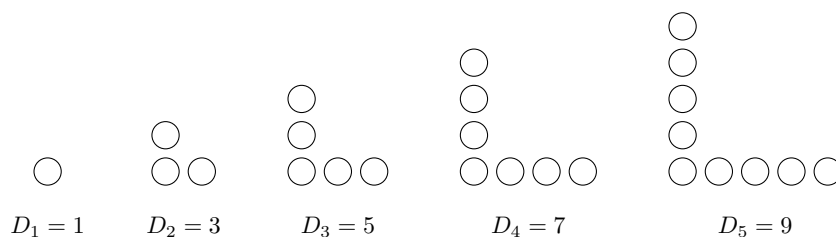


Figura 2: Rappresentazione geometrica dei numeri dispari (D_n)

I numeri *dispari* sono una *elle* formata da due segmenti della stessa lunghezza.

Ecco invece i numeri *quadrati*:

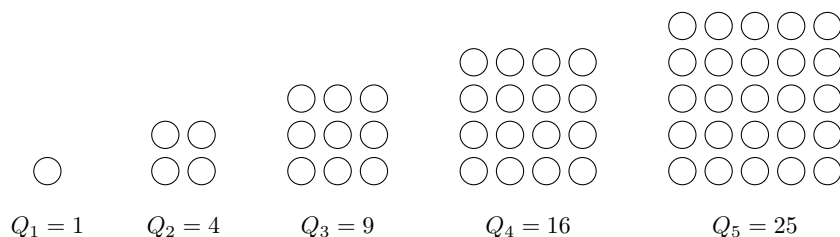


Figura 3: Rappresentazione geometrica dei numeri quadrati (Q_n)

Problema 4.1. *Dimostrare che la somma dei primi numeri dispari è uguale all'ennesimo numero quadrato, cioè*

$$1 + 3 + 5 + \dots + (2n - 1) = n^2$$

Soluzione. Basta osservare la seguente figura

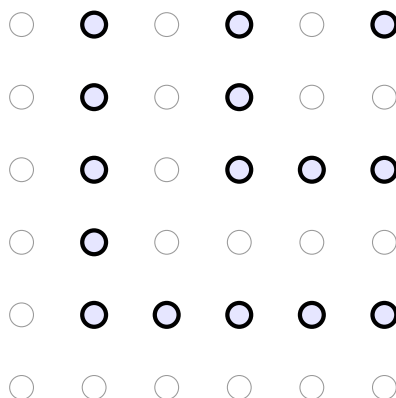


Figura 4: La somma dei primi n numeri dispari è un numero quadrato.

I numeri dispari sono stati inscatolati uno dentro l'altro in modo da formare un quadrato.

4.1 Numeri triangolari

Consideriamo ora tutti quei numeri che si ottengono sommando i primi n numeri naturali. Per esempio, 1 , $1 + 2 = 3$, $1 + 2 + 3 = 6$, $1 + 2 + 3 + 4 = 10$ eccetera. Sono i cosiddetti numeri *triangolari*.

Esercizio 4.2. *Dimostrare che la somma di due numeri triangolari consecutivi è un numero quadrato. Dimostrare cioè che $T_{n-1} + T_n = Q_n$.*

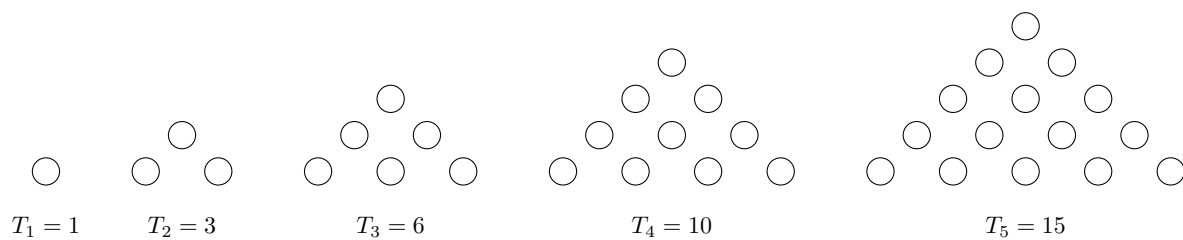


Figura 5: I primi cinque numeri triangolari.

Esercizio 4.3. *Dimostrare che $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$*

4.2 Numeri tetraedrici

I numeri tetraedrici si ottengono impilando numeri triangolari via via più grandi.

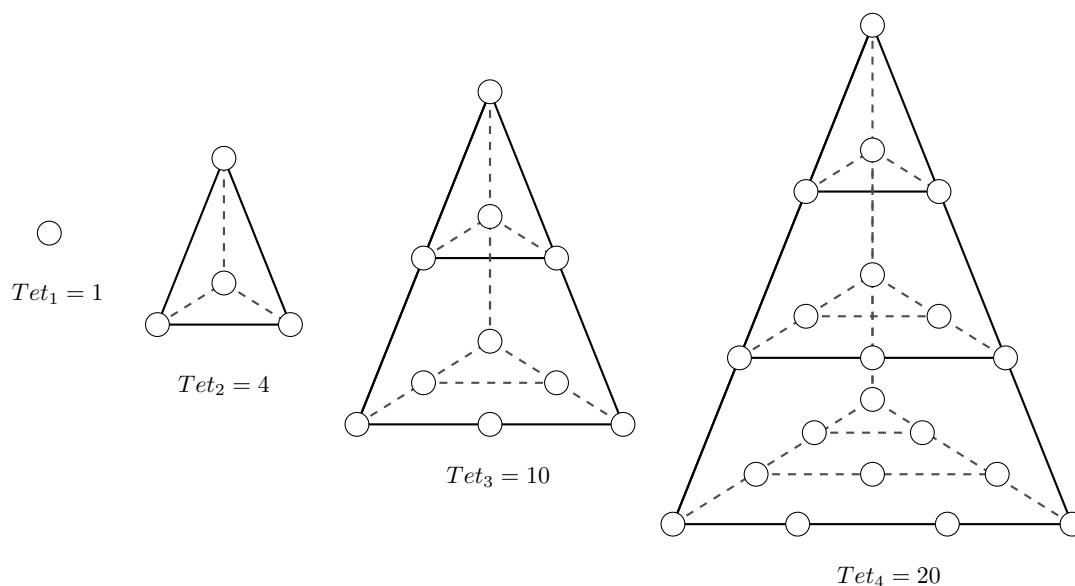


Figura 6: Scomposizione geometrica dei numeri tetraedrici (Tet_n)

Se indichiamo con $T_1, T_2, T_3 \dots$ i numeri triangolari e con $Tet_1, Tet_2, Tet_3 \dots$ i numeri tetraedrici abbiamo:

$$Tet_1 = T_1 = 1$$

$$Tet_2 = T_1 + T_2 = 1 + (1 + 2) = 4$$

$$Tet_3 = T_1 + T_2 + T_3 = 1 + (1 + 2) + (1 + 2 + 3) = 10$$

$$Tet_4 = T_1 + T_2 + T_3 + T_4 = 1 + (1 + 2) + (1 + 2 + 3) + (1 + 2 + 3 + 4) = 20$$

Per trovare il quinto numero tetraedrico, cioè Tet_5 , bisogna sommare tutti i numeri del seguente triangolo

$$\begin{array}{c} 1 \\ 1 + 2 \\ 1 + 2 + 3 \\ 1 + 2 + 3 + 4 \\ 1 + 2 + 3 + 4 + 5 \end{array}$$

Se sommiamo tra loro tutti gli uno poi tutti i due e così via otteniamo

$$Tet_5 = (1 \cdot 5) + (2 \cdot 4) + (3 \cdot 3) + (4 \cdot 2) + (5 \cdot 1) = 35$$

Pertanto, l'ennesimo numero tetraedrico sarà

$$\begin{aligned} Tet_n &= T_1 + T_2 + T_3 + \dots + T_n \\ &= 1 + (1 + 2) + (1 + 2 + 3) + \dots + (1 + 2 + 3 + \dots + n) \\ &= 1 \cdot n + 2 \cdot (n - 1) + 3 \cdot (n - 2) + \dots + (n - 1) \cdot 2 + n \cdot 1 \end{aligned}$$

Esercizio 4.4. *Servendosi di un foglio elettronico scrivere i primi cento numeri tetraedrici.*

Problema 4.5. *Trovare una formula chiusa per rappresentare l'ennesimo numero tetraedrico.*

Soluzione.

Per iniziare scegliamo $n = 5$ e consideriamo le tre seguenti copie di Tet_5 :

$$\begin{array}{ccc}
 1 & 1 & 5 \\
 1+2 & 2+1 & 4+4 \\
 1+2+3 & 3+2+1 & 3+3+3 \\
 1+2+3+4 & 4+3+2+1 & 2+2+2+2 \\
 1+2+3+4+5 & 5+4+3+2+1 & 1+1+1+1+1
 \end{array} .$$

Sommiamo ora tutti i termini che, nei tre triangoli, occupano la stessa posizione

$$\begin{array}{c}
 7 \\
 7+7 \\
 7+7+7 \\
 7+7+7+7 \\
 7+7+7+7+7
 \end{array} .$$

Pertanto tre copie di Tet_5 si possono ottenere così:

$$3 \cdot Tet_5 = (1+2+3+4+5) \cdot 7 = \frac{5 \cdot 6}{2} \cdot 7 \quad (4.1)$$

e infine $Tet_5 = 35$.

Ripetendo lo stesso ragionamento per Tet_n , dalla 4.1, otteniamo

$$3 \cdot Tet_n = (1+2+3+4+5+\dots+n) \cdot (n+2) = \frac{n \cdot (n+1)}{2} \cdot (n+2) \quad (4.2)$$

Quindi

L'ennesimo numero tetraedrico si può esprimere mediante la seguente formula chiusa:

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

Esercizio 4.6. *Dimostrare che la somma di tre numeri naturali consecutivi è divisibile per 6.*

4.3 Numeri piramidali quadratici

Se impiliamo numeri quadrati otteniamo i cosiddetti *numeri piramidali a base quadrata*, che indichiamo con i simboli Pir_1, Pir_2, Pir_3 etc, etc. Più precisamente, il numero Pir_n è costituito da una piramide di vertice Q_1 e dagli “strati” $Q_2, Q_3, \dots, Q_n$, di cui l’ultimo costituisce la base della piramide.

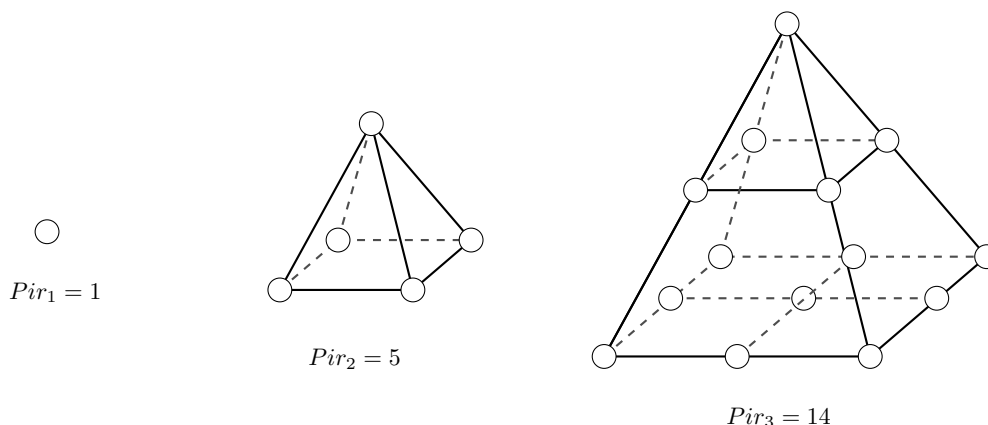


Figura 7: Scomposizione geometrica dei numeri piramidali quadratici (Pir_n)

Esercizio 4.7. *Servendosi di un foglio elettronico scrivere i primi cento numeri piramidali a base quadrata.*

Esercizio 4.8. *Dimostrare che ogni numero piramidale si può ottenere sommando due numeri tetraedrici consecutivi, cioè $Pir_n = Tet_n + Tet_{n-1}$*

Problema 4.9. *Trovare una formula chiusa per rappresentare l’ennesimo numero piramidale.*

Soluzione. Nell’esercizio 4.8 abbiamo mostrato che $Pir_n = Tet_n + Tet_{n-1}$. Dunque, abbiamo

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

In altre parole

La somma dei primi n numeri quadrati è data dalla seguente uguaglianza:

$$Pir_n = 1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{1}{6}n(n+1)(2n+1). \quad (4.3)$$

Esercizio 4.10. *Costruire, servendosi dei mattoncini per bambini, 6 copie del numero piramidale Pir_n e disponetele in modo da formare una scatola di dimensioni $n(n+1)(2n+1)$. In questo modo si dimostra, per altra via, l'uguaglianza [4.3](#).*

5 Aritmetica modulare. Classe di resti

Cominciamo con un esempio.

Consideriamo la seguente tabella ottenuta eseguendo, per ogni numero intero, la divisione per quattro.

$\mathbb{Z}$	divisione per 4	quoziente	resto
$\vdots$	$\vdots$	$\vdots$	$\vdots$
-4	-4:4	-1	0
-3	-3:4	-1	1
-2	-2:4	-1	2
-1	-1:4	-1	3
0	0:4	0	0
1	1:4	0	1
2	2:4	0	2
3	3:4	0	3
4	4:4	1	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Come già sapevamo tutti i possibili resti sono rappresentati dai numeri 0,1,2,3.

Costruiamo allora un'altra tabella avente una colonna per ogni possibile resto e poniamo in ognuna di esse tutti i numeri interi che, divisi per quattro, danno il resto corrispondente alla colonna in esame.

Quindi, poniamo in $r = 0$ tutti i numeri interi che divisi per quattro danno resto zero, in $r = 1$ tutti i numeri interi che divisi per quattro danno resto uno e così via.

$r = 0$	$r = 1$	$r = 2$	$r = 3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
-12	-11	-10	-9
-8	-7	-6	-5
-4	-3	-2	-1
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
$\vdots$	$\vdots$	$\vdots$	$\vdots$

In questo modo otteniamo una *partizione* dell'insieme $\mathbb{Z}$ in *quattro classi*, una per ogni colonna della precedente tabella.

Poniamoci ora la seguente domanda.

Dati due qualsiasi numeri interi x e y come possiamo stabilire se appartengono o meno alla stessa classe?

La risposta è semplice: occorre dividere i due numeri x e y per quattro e verificare se hanno lo stesso resto. In caso affermativo i due numeri prescelti appartengono alla stessa classe, altrimenti no.

Riflettiamo un poco su ciò che abbiamo appena imparato: la costruzione delle due precedenti tabelle e la successiva partizione dell'insieme $\mathbb{Z}$ sono state possibili perché, all'inizio di questo paragrafo, abbiamo scelto di dividere tutti gli interi per il numero $n = 4$.

In realtà questa scelta non era obbligata; per esempio, se avessimo diviso tutti gli interi per $n = 7$ avremmo ancora ottenuto una partizione di $\mathbb{Z}$ in classi, quelle corrispondenti a tutti i possibili resti della divisione per sette e cioè 0, 1, 2, 3, 4, 5, 6.

Insomma, tutto ciò che abbiamo fin qui esposto ed in particolare, la partizione di $\mathbb{Z}$ in classi di equivalenza è realizzabile scegliendo un qualunque intero $n > 0$; ovviamente quello che cambia sono le classi!.

Queste considerazioni ci inducono a dare la seguente importante

boxedminipage [t]13cm

Definizione 5.1. *Dati due numeri x e y appartenenti a $\mathbb{Z}$ ed un intero $n > 0$ diciamo che “ x è congruo a y modulo n ” e scriviamo*

$$x \equiv y \pmod{n}$$

se e solo se x e y divisi per n danno lo stesso resto.

è boxedminipage

La relazione di congruenza che abbiamo appena introdotto⁶ suddivide l'insieme $\mathbb{Z}$ dei numeri interi in n classi che chiamiamo *classi di resti modulo n* . Scriveremo così:

$$[0], [1], [2], \dots, [n-1]$$

Indichiamo inoltre con $\mathbb{Z}_n$ l'insieme costituito da queste classi di resti e cioè:

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

Esercizio 5.2. *Determinare le classi che si ottengono dalle seguenti congruenze:*

$$\begin{array}{ll} a] & x \equiv y \pmod{4}; \\ b] & x \equiv y \pmod{5}; \end{array} \qquad \begin{array}{ll} c] & x \equiv y \pmod{8}; \\ d] & x \equiv y \pmod{12}. \end{array}$$

⁶Si può dimostrare che la definizione 5.1 è equivalente alla seguente: “se a e b sono interi, diciamo che x è congruo a y modulo n , e scriviamo $x \equiv y \pmod{n}$ (o anche $x \equiv_n y$) se e solo se la differenza $x - y$ è un multiplo di n .”

Esercizio 5.3. *Nell'insieme $\mathbb{Z}$ dei numeri interi verificare se sono vere o false le seguenti congruenze, giustificando le risposte.*

$$\begin{array}{ll} a] & 10 \equiv 13 \pmod{3}; \\ b] & 2 \equiv 8 \pmod{5}; \\ c] & 20 \equiv 4 \pmod{6}; \end{array} \qquad \begin{array}{ll} d] & 100 \equiv 1 \pmod{9}; \\ e] & 25 \equiv 5 \pmod{3}; \\ f] & 17 \equiv 5 \pmod{4}. \end{array}$$

5.1 Le proprietà delle congruenze

Per una “congruenza” valgono le seguenti proprietà.

1. Per ogni $x \in \mathbb{Z}$, $x \equiv x \pmod{n}$ (proprietà riflessiva)

2. Per ogni $x, y \in \mathbb{Z}$,
se $x \equiv y \pmod{n}$ allora $y \equiv x \pmod{n}$ (proprietà simmetrica)

3. Per ogni $x, y, z \in \mathbb{Z}$,
se $x \equiv y \pmod{n}$ e $y \equiv z \pmod{n}$
allora $x \equiv z \pmod{n}$ (proprietà transitiva)

Esercizio 5.4. *Dimostrare le precedenti proprietà argomentando in modo chiaro e dettagliato.*

5.2 Le operazioni in $\mathbb{Z}_n$: l'addizione e la moltiplicazione

In quale modo si possono sommare gli elementi di $\mathbb{Z}_5$? E in quale modo si possono moltiplicare?

Procediamo così:

$$\begin{array}{ll} [0] + [1] = [0 + 1] = [1] & [0] \cdot [1] = [0 \cdot 1] = [0] \\ [0] + [2] = [0 + 2] = [2] & [0] \cdot [2] = [0 \cdot 2] = [0] \\ [0] + [3] = [0 + 3] = [3] & [0] \cdot [3] = [0 \cdot 3] = [0] \\ \dots \dots \dots & \dots \dots \dots \\ [1] + [1] = [1 + 1] = [2] & [1] \cdot [1] = [1 \cdot 1] = [1] \\ \dots \dots \dots & \dots \dots \dots \\ [2] + [4] = [2 + 4] = [6] = [1] & [2] \cdot [4] = [2 \cdot 4] = [8] = [3] \end{array}$$

Questo ultimo caso è un poco diverso dagli altri; infatti, essendo $6 = 5 \cdot 1 + 1$, abbiamo $[6] = [1]$. Analogamente $8 = 5 \cdot 1 + 3$ e quindi $[8] = [3]$.

A questo punto siamo in grado di costruire la tabella della somma e quella del prodotto in $\mathbb{Z}_5$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

In generale definiamo l'addizione e la moltiplicazione in $\mathbb{Z}_n$ nel seguente modo:

Definizione 5.5. Se $[a]$ e $[b]$ sono due classi di resti modulo n , poniamo

$$[a] + [b] = [a + b] \quad e \quad [a] \cdot [b] = [a \cdot b]$$

In questa definizione $[a]$ e $[b]$ sono classi di equivalenza individuate da un rappresentante (a e b rispettivamente); perché la nostra definizione sia sensata dobbiamo verificare che *il risultato della somma non dipende dal particolare rappresentante che abbiamo scelto per le due classi di resti che fanno da addendi (o da fattori)*. In altre parole occorre verificare che

$$\text{se } a' \equiv a \quad e \quad b' \equiv b \quad \text{allora} \quad a' + b' \equiv a + b \quad e \quad a' \cdot b' \equiv a \cdot b$$

Per non complicare troppo la nostra trattazione omettiamo, per il momento, queste verifiche.

Il problema che ora ci poniamo è il seguente: *dovendo eseguire dei calcoli in $\mathbb{Z}_n$, possiamo utilizzare tutte quelle proprietà algebriche che contraddistinguono gli ordinari insiemi numerici?* In altre parole, *quali proprietà caratterizzano la somma e il prodotto in $\mathbb{Z}_n$?*

Cominciamo allora ad occuparci dell'addizione.

In $\mathbb{Z}_n$ valgono le seguenti importanti proprietà

1. Proprietà commutativa:

$$\text{per ogni } [a], [b] \in \mathbb{Z}_n \quad [a] + [b] = [b] + [a]$$

2. Proprietà associativa:

$$\text{per ogni } [a], [b], [c] \in \mathbb{Z}_n \quad ([a] + [b]) + [c] = [a] + ([b] + [c])$$

3. Esistenza dell'elemento neutro:

$$\text{per ogni } [a] \in \mathbb{Z}_n \text{ abbiamo } [a] + [0] = [0] + [a] = [a]$$

Questo significa che la classe individuata dal numero zero non produce alcun effetto se sommata ad una qualsiasi altra classe. Per questa ragione chiamiamo la classe $[0]$ *elemento neutro rispetto alla somma*.

4. Esistenza dell'inverso rispetto alla somma:

per ogni elemento $[a] \in \mathbb{Z}_n$ esiste un elemento che denotiamo con $[-a]$, detto *inverso di $[a]$ rispetto alla somma* o più semplicemente *opposto di $[a]$* , per il quale

$$[a] + [-a] = [-a] + [a] = [0]$$

Le proprietà sopra esposte ci consentono di affermare che l'insieme $\mathbb{Z}_n$ è un *gruppo commutativo* (o anche *gruppo abeliano* ⁷) rispetto alla somma.

Dobbiamo però fare attenzione, perchè la somma in $\mathbb{Z}_n$ può riservare qualche sorpresa. Per esempio, in $\mathbb{Z}_4$ abbiamo:

$$[2] + [2] = [0]$$

Quindi, il luogo comune secondo il quale *in matematica, due più due fa sempre quattro* risulta, in questo caso, palesemente falso!

Esercizio 5.6. *Eseguire le seguenti somme mod n :*

$$\begin{array}{ll} a) & 4 + 3 = \dots\dots \pmod{3}; \\ b) & 4 + 3 = \dots\dots \pmod{4}; \\ c) & 4 + 3 = \dots\dots \pmod{5}; \end{array} \quad \begin{array}{ll} d) & 2 + 5 = \dots\dots \pmod{2}; \\ e) & 2 + 5 = \dots\dots \pmod{3}; \\ f) & 2 + 5 = \dots\dots \pmod{6}; \end{array}$$

Esercizio 5.7. *Verificare che $\mathbb{Z}_4$ è un gruppo abeliano rispetto alla somma. (Costruire la tabella relativa alla somma in $\mathbb{Z}_4$ e poi verificare le quattro proprietà sopra enunciate).*

Per quanto riguarda il *prodotto* sussistono invece le seguenti proprietà:

1. Proprietà commutativa:

$$\text{per ogni } [a], [b] \in \mathbb{Z}_n \quad [a] \cdot [b] = [b] \cdot [a]$$

2. (Proprietà associativa:

$$\text{per ogni } [a], [b], [c] \in \mathbb{Z}_n \quad ([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$$

3. Esistenza dell'elemento neutro:

per ogni $[a] \in \mathbb{Z}_n$ abbiamo

$$[a] \cdot [1] = [1] \cdot [a] = [a]$$

Questo significa che la classe individuata dal numero uno non produce alcun effetto se moltiplicata per una qualsiasi altra classe. Per questa ragione chiamiamo la classe $[1]$ *elemento neutro rispetto al prodotto*.

Come avrete notato non abbiamo incluso tra le proprietà del prodotto quella relativa all'esistenza dell'inverso. Infatti, in certe classi di resti, non tutti gli elementi ammettono inverso rispetto al prodotto. Per esempio, dalla tabella relativa alla moltiplicazione in $\mathbb{Z}_6$

⁷Dal nome del matematico norvegese N. H. Abel (1802-1829).

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

ci accorgiamo subito che le classi $[2]$, $[3]$ e $[4]$ non hanno inverso.

In generale, vale infatti il seguente

Teorema 5.8. *Un elemento $a \in \mathbb{Z}_n$ è invertibile se e solo se a è primo con n , cioè se e solo se $\text{MCD}(a, n) = 1$. In particolare, se p è un numero primo, allora ogni elemento non nullo di $\mathbb{Z}_p$ è invertibile.*

Dimostrazione. Supponiamo che $[a] \in \mathbb{Z}_n$ sia invertibile, vale a dire supponiamo che esista una classe $[b]$ in $\mathbb{Z}_n$ per la quale $[a] \cdot [b] = 1$ in $\mathbb{Z}_n$. Questo significa che, in $\mathbb{Z}$, $ab - 1 = hn$ per qualche intero h , ovvero che

$$ab - hn = 1.$$

Da quest'ultima uguaglianza segue che ogni intero che divide sia a che n deve dividere anche 1, e quindi il massimo comun divisore di a e n è 1.

Viceversa, se a e n sono primi tra loro, allora esistono interi x, y per i quali $ax + ny = 1$. (Si veda 3.2). Allora $ax = 1$ in $\mathbb{Z}_n$, ovvero a è invertibile in $\mathbb{Z}_n$, con inverso x . $\square$

Osservazione

Ricordiamo la definizione della funzione φ di Eulero: per ogni intero m , $\varphi(m)$ è il numero degli interi t , $1 \leq t \leq m$, che sono primi con m . Dunque, per il teorema precedente, il numero degli elementi invertibili di $\mathbb{Z}_m$ è $\varphi(m)$.

Esercizio 5.9. *Eseguire le seguenti moltiplicazioni mod n :*

$$\begin{array}{ll} a) & 4 \cdot 3 = \dots \pmod{3}; \\ b) & 4 \cdot 3 = \dots \pmod{4}; \\ c) & 4 \cdot 3 = \dots \pmod{5}; \end{array} \quad \begin{array}{ll} d) & 2 \cdot 5 = \dots \pmod{2}; \\ e) & 2 \cdot 5 = \dots \pmod{3}; \\ f) & 2 \cdot 5 = \dots \pmod{6}; \end{array}$$

Esercizio 5.10. *Determinare gli inversi di tutti gli elementi di $\mathbb{Z}_5$ diversi da $[0]$.*

Esercizio 5.11. *Stabilire se la seguente affermazione è vera o falsa e motivare la risposta: “in $\mathbb{Z}_n$ vale la legge di annullamento del prodotto” e cioè*

$$\text{per ogni } [a], [b] \in \mathbb{Z}_n \text{ se } [a] \cdot [b] = [0] \text{ allora } [a] = [0] \text{ oppure } [b] = [0].$$

Soluzione. L'affermazione è falsa infatti in $\mathbb{Z}_n$, esistono classi diverse da zero il cui prodotto è la classe zero. Per esempio in $\mathbb{Z}_6$ abbiamo $[2] \cdot [3] = [0]$ ed anche $[3] \cdot [4] = [0]$.

Esercizio 5.12. *Stabilire se la seguente affermazione è vera o falsa e motivare la risposta: “in $\mathbb{Z}_n$ vale la legge di cancellazione del prodotto” e cioè*

$$\text{per ogni } [a], [b], [c] \in \mathbb{Z}_n \text{ se } [a] \cdot [c] = [b] \cdot [c] \text{ allora } [a] = [b].$$

Esercizio 5.13. *Verificare che il polinomio $p(x) = x^4 - 117x + 39$ non ammette radici intere.*

Esercizio 5.14. *Servendosi di un foglio elettronico, determinare le seguenti classi di resti: $\mathbb{Z}_2$, $\mathbb{Z}_6$ e $\mathbb{Z}_{11}$.*

Esercizio 5.15. *Utilizzando Excel, costruire la tavola della moltiplicazione per le classi di resto $\text{mod}(26)$. Individuare gli elementi invertibili e per ognuno di essi determinare l'inverso.*