NUMERI NATURALI E INTERI

1.L’insieme dei numeri naturali

1.1 Le operazioni fra numeri naturali: addizione e moltiplicazione
1.2 L’ordinamento
1.3 Sottrazione e divisione
1.4 Divisibilità nell’insieme dei naturali
1.5 L’elevamento a potenza
1.6 Rappresentazione decimale dei numeri naturali
1.7 Numeri primi
1.8 Massimo comun divisore e minimo comune multiplo

2. L’insieme dei numeri interi

2.1 Operazioni fra numeri interi: addizione, moltiplicazione, sottrazione
2.2 L’ordinamento
2.3 Divisione fra numeri interi: la divisione con resto (divisione euclidea)
2.4 L’elevamento a potenza fra numeri interi

3. Note:
3.1 Il linguaggio matematico: espressioni simboliche
3.2 Verifiche e dimostrazioni

1. L'INSIEME DEI NUMERI NATURALI

Accettiamo qui una nozione intuitiva di numero naturale: quella che ci viene dall'esperienza di *contare* oggetti. In altre parole i numeri naturali sono: 1, 2, 3, …eccetera. E' chiaro a tutti cosa significa quell'eccetera: anche se la nostra esperienza ci permette di contare solo un numero finito di oggetti, fin dalle elementari abbiamo intuito che fissato un numero naturale è sempre possibile pensarne uno più grande.

La nozione di numero naturale si può fondare in modo rigoroso facendo ricorso agli assiomi di Peano (analogamente a quanto si fa in geometria elementare per fondare l'idea di punto, retta, piano).

L'insieme dei numeri naturali è di solito indicato con il simbolo N o anche con {1, 2, 3, …}.

Osservazione: Il numero 0 è un numero naturale? Per alcuni matematici sì, per altri no (ed ogni posizione ha delle giustificazioni sensate). Questa mancanza di accordo non crea problemi, purché venga esplicitata fin dall'inizio la scelta che si fa, e soprattutto purché ci si comporti poi in modo coerente con tale scelta.
La scelta che faremo qui è di considerare 0 un numero naturale. Per noi quindi N = {0, 1, 2, 3, …}.

1.1 Le operazioni nell'insieme dei numeri naturali: addizione e moltiplicazione

Nell'insieme N sono definite due operazioni: l'addizione e la moltiplicazione.
Precisiamo cosa si intende per 'operazione' in un insieme A: è una legge che associa a due (o eventualmente a più) elementi dell'insieme un elemento anch'esso dell'insieme A.

L'addizione e la moltiplicazione sono quindi operazioni nell'insieme N perché a due numeri naturali associano un numero naturale (chiamato *somma* nel caso dell'addizione, *prodotto* nel caso della moltiplicazione) .

Consideriamo queste operazioni note a livello intuitivo (anch'esse si potrebbero definire rigorosamente a partire dagli assiomi di Peano).

L' operazione di addizione gode delle seguenti proprietà:
a1) Proprietà commutativa

Per qualsiasi m,n appartenenti a **N**: $m+n=n+m$

Osservazione: al posto di 'per qualsiasi' o 'per ogni' si può usare il simbolo $\forall$ (detto quantificatore universale)
Osservazione: al posto di 'appartenenti' o 'appartengono a' si può usare il simbolo $\in$.
a2) Proprietà associativa

$\forall\, m,n,h \in \mathbf{N}$: $(m+n)+h=m+(n+h)$.

Osservazione: la proprietà associativa dell'addizione rende superflue le parentesi quando si devono addizionare diversi addendi.
a3) Esistenza dell'*elemento neutro,* cioè di un elemento e con la proprietà che $a + e = e + a = a$ $\forall a \in$ N.
L'elemento neutro per l'addizione è il numero 0, infatti per esso vale:

$\forall a \in \mathrm{N}\ \ a + 0 = 0 + a = a$.

Osservazione: Questa proprietà naturalmente si perde se si fa la scelta di non considerare 0 un elemento dell'insieme N.

L' operazione di moltiplicazione gode delle seguenti proprietà:
m1) Proprietà commutativa:

$\forall\, m,n \in \mathbf{N}$: $m \cdot n = n \cdot m$

m2) Proprietà associativa:

$\forall\, m,n,h \in \mathbf{N}$: $(m \cdot n) \cdot h = m \cdot (n \cdot h)$

Osservazione: la proprietà associativa della moltiplicazione rende superflue le parentesi quando si devono moltiplicare diversi fattori.

m3) Esistenza dell'*elemento neutro.*

L'elemento neutro per la moltiplicazione è il numero 1, infatti per esso vale:

$\forall a \in \mathrm{N} \quad a \cdot 1 = 1 \cdot a = a$

C'è infine una proprietà – la proprietà *distributiva* – che lega moltiplicazione e addizione:

d) Proprietà distributiva della moltiplicazione rispetto all'addizione:

$\forall\ a, b, c \in \mathrm{N}$: $\quad a \cdot (b + c) = a \cdot b + a \cdot c$

1.2 L'ordinamento in N

Come sappiamo i numeri naturali si possono ordinare, cioè dati due numeri naturali *m* e *n* diversi, o $m > n$, o $n > m$.

In altre parole l'insieme N è dotato di un ordinamento (o relazione d'ordine). Questo ordinamento si può definire a partire dall'operazione di addizione nel modo seguente:

Definizione: Siano $m, n \in N$. Diremo che $n \leq m$ se esiste $k \in N$ tale che $m = n + k$.

Osservazione: Partendo dalla definizione data di $\leq$ possiamo definire la relazione $<$.

Diciamo che $a < b$ se $a \leq b$ e $a \neq b$.

Osservazione: $a \leq b$ significa *a* è minore oppure uguale a *b*.

Quindi le seguenti disuguaglianze sono vere:

$5 \leq 5$

$1 \leq 5$

Presi due numeri naturali *m* e *n* qualsiasi, si verifica una e una sola delle seguenti condizioni:

$m = n$

$m > n$

$n > m$

Si dice anche che l'insieme N è un insieme (totalmente) ordinato, cioè è un insieme in cui è definita una relazione d'ordine (totale).

Una *relazione d'ordine* in un insieme A è una relazione che verifica le seguenti proprietà:

1) $a \leq a \ \forall a \in A$ (proprieta' riflessiva)

2) se $a \leq b$ e $b \leq a$ allora $a = b$ (proprietà antisimmetrica)

3) se $a \leq b$ e $b \leq c$ allora $a \leq c$ (proprietà transitiva).

Se inoltre vale anche la proprietà:

4) $\forall a, b \in A$ vale una sola delle seguenti relazioni:

$a < b$; $b < a$; $a = b$ (tricotomia)

allora la relazione si dice di ordine *totale.*

1.3 Sottrazione e divisione fra numeri naturali

Forse vi siete chiesti perché abbiamo parlato di due operazioni soltanto, e abbiamo trascurato sottrazione e divisione.

Il fatto è che sottrazione e divisione si definiscono a partire da addizione e moltiplicazione: la sottrazione come *operazione inversa* dell'addizione, la divisione come *operazione inversa* della moltiplicazione.

Più precisamente:

A partire dall'addizione si può definire la *sottrazione* fra due numeri *m* e *n* (che si indica con il segno ' –') come l'operazione che ai numeri *m* e *n* associa quel numero *x* (detto *differenza* di *m* e *n*) tale che:

$n + x = m$

Analogamente a partire dalla moltiplicazione di può definire la *divisione* fra due numeri naturali *m* e *n* (che si indica con il segno ' :') come l'operazione che ai numeri *m* e *n* associa quel numero *x* tale che:

$n \cdot x = m$

A differenza dell'addizione e della moltiplicazione, queste operazioni non sono 'interne' a N, perché in generale presi due numeri naturali qualsiasi non è possibile farne la sottrazione o la divisione rimanendo dentro N (cioè avendo come risultato ancora numeri naturali).

Ad esempio se *m* = 5 e *n* = 7 non c'è nessun numero naturale *x* che sommato a 7 dia 5.

Se *m* = 7 e *n* = 2, non esiste nessun numero *x* naturale tale che $2 \cdot x = 7$

1.4 Divisibilità nell'insieme dei naturali

Quest'ultimo esempio ci porta a definire un'altra relazione d'ordine in N: quella di *divisibilità.*

Definizione: Se *m* e *n* sono due numeri naturali per cui esiste $k \in N$ tale che:

$n \cdot k = m$

si dice che *m* è multiplo di *n* (o che '*n* è divisore di *m*', o che '*n* divide *m*').

Osservazione: al posto di 'esiste' si può usare il simbolo ∃ (detto quantificatore esistenziale)

1.5 Potenze

A partire dalla moltiplicazione si definisce intuitivamente l'operazione di *potenza di base il numero naturale a ed esponente il numero naturale n>0:*

$$a^n = \underbrace{a \cdot a \cdot a .... \cdot a}_{n \text{ volte}}$$

Osservazione: L'operazione di elevamento a potenza non gode né della proprietà associativa né di quella commutativa. (Dimostralo)

Proprietà delle potenze:

p1) $\forall\ a,m,n \in N: \quad a^m \cdot a^n = a^{m+n}$

p2) Se $n > m$ e $a \neq 0$ $\dfrac{a^n}{a^m} = a^{n-m}$

p3) $\forall\ a,m,n \in N$**:** $\quad (a^m)^n = a^{m \cdot n}$

p4) $\forall\ a,b,n \in N\ (ab)^n = a^n b^n$

1.6 Rappresentazione decimale dei numeri naturali

I numeri naturali sono di solito rappresentati da una sequenza finita di *cifre*. Nella scrittura in base dieci (o decimale) le cifre sono dieci: 0; 1; 2; 3; 4; 5; 6; 7; 8; 9.

La scrittura 2107, ad esempio, significa: $2 \cdot 10^3 + 1 \cdot 10^2 + 0 \cdot 10^1 + 7 \cdot 10^0$.

La scrittura 217 significa invece $2 \cdot 10^2 + 1 \cdot 10^1 + 7 \cdot 10^0$.

Problemi:

1) Scrivete il numero la cui cifra delle unità è *p*, quella delle decine è *q* e quella delle centinaia è *r*.
2) Scrivete il numero la cui cifra delle unità è *p*, quella delle decine è *q* e quella delle migliaia è *r*.
3) Scrivete il numero la cui cifra delle unità è *p*, quella dei decimi è *q* e quella dei centesimi è *r*.
4) Scrivete il più grande numero di tre cifre con le seguenti caratteristiche: una delle tre cifre è 4 e la somma delle restanti cifre è 8.
5) Scrivete il più grande numero di 4 cifre per cui la somma delle cifre delle unità e delle decine sia il doppio della somma delle cifre delle centinaia e delle migliaia.
6) È dato un numero intero *p* la cui rappresentazione in base dieci è di due cifre. La somma delle due cifre di *p* è 10, il numero ottenuto scambiando le cifre supera *p* di 36. Trovate *p*.
7) Che cosa succede se, nella stessa situazione del problema precedente, la somma delle cifre è 14 invece che 10?
8) È possibile che esista un numero di due cifre *p*, tale che il numero ottenuto scambiando le cifre sia il doppio di *p*?

1.7 Numeri primi

Definizione: Un intero positivo è detto *primo* se ha esattamente 2 divisori positivi.

In altri termini, sono primi gli interi positivi diversi da 1 e divisibili soltanto per sé stessi e per 1.

Esempi

- 2 è primo perché ha esattamente 2 divisori positivi: 1 e 2.
- 0 non è primo perché non è positivo.
- 18 non è primo perché ha più di 2 divisori positivi; infatti ne ha 6 (quali?).

È spesso utile rappresentare i numeri interi come prodotto di potenze di numeri primi. Questa rappresentazione, detta *scomposizione in fattori primi*, è possibile in ogni caso, ed è unica, come assicurato dal teorema che segue.

TEOREMA FONDAMENTALE DELL'ARITMETICA: Ogni intero positivo ha una e una sola scomposizione in fattori primi.

Dimostrazione
Dimostriamo per assurdo:
immaginiamo che esistano dei numeri interi positivi con due fattorizzazioni e sia m il minimo di tali numeri interi:

$$\text{m} = p_1 \cdot p_2 \cdot \ldots\ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s \quad (1)$$

in cui le p e le q sono primi. Cambiando se necessario l'ordine delle p e delle q, possiamo supporre che

$$p_1 \le p_2 \le \ldots\ldots \le p_r \qquad \text{e} \qquad q_1 \le q_2 \le \ldots \le q_s .$$

Ora p_1 non può essere uguale a q_1 perché altrimenti si potrebbe semplificare dai due membri dell'uguaglianza (1) il primo fattore e si otterrebbero due scomposizioni essenzialmente diverse in fattori primi di un numero naturale intero minore di m, contro l'ipotesi che m sia l'intero più piccolo per cui questo è possibile.

Quindi o è $p_1 < q_1$ oppure $q_1 < p_1$.

Supponiamo $p_1 < q_1$ (per l'altro caso è sufficiente scambiare le lettere p e q in ciò che segue). Formiamo il numero:

$$m' = m - (p_1 \cdot q_2 \cdot .... \cdot q_s) \quad (2)$$

Sostituendo a m le due espressioni dell'uguaglianza (1) si ottiene:

$$m' = p_1 \cdot p_2 \cdot ..... \cdot p_s - p_1 \cdot q_2 \cdot .... \cdot q_s = p_1(p_2 \cdot ..... \cdot p_r - q_2 \cdot .... \cdot q_s) \quad (3)$$

$$m' = q_1 \cdot q_2 \cdot ..... \cdot q_s - p_1 \cdot q_2 \cdot .... \cdot q_s = (q_1 - p_1)(q_2 \cdot q_3 \cdot .... \cdot q_s) \quad (4)$$

Essendo $p_1 < q_1$ segue dalla (4) che m' è un numero intero positivo e dalla (2) che m' è minore di m.

Quindi la scomposizione in fattori primi di m' deve essere unica , a parte l'ordine dei fattori.

Ma dalla (3) risulta che p_1 è un fattore di m' perciò nella (4) p_1 deve comparire come un fattore o di $(q_1 - p_1)$ o di $q_2 \cdot q_3 \cdot .... \cdot q_s$

(ciò dalla supposta unicità della scomposizione in fattori primi di m').

Il secondo caso è impossibile perché tutte le q sono maggiori di p_1.

Quindi p_1 deve essere un fattore di $(q_1 - p_1)$, cosicché deve esistere un intero h per cui che

$$(q_1 - p_1) = p_1 \cdot h \quad \text{ovvero} \quad q_1 = p_1(h+1).$$

Ma da questo risulta che p_1 è un fattore di q_1 contro l'ipotesi che q_1 sia primo.

Questa contraddizione mostra l'assurdità delle ipotesi iniziali e completa la dimostrazione del teorema.

Esempi

- $600 = 2^3 \cdot 3 \cdot 5^2$
- $68 = 2^2 \cdot 17$

Problemi:

1) Sono dati due numeri naturali, *x* e *y*. Si sa che *y*=*x*+1 e che *x*, *y* sono entrambi primi. Trovate *x* e *y*.
2) Sapendo che $M = 3^7 \cdot 5^{11} \cdot 7^2 \cdot 11^4 \cdot 19^{31}$, rivete la scomposizione in fattori primi di M^2.
3) *M* è lo stesso del problema precedente. Secondo voi compare il fattore 2 nella scomposizione in fattori primi di *M*+1?

Osservazione: Forse la definizione che ricordavi di numero primo era 'Un numero si dice primo se ha come divisori solo se stesso e 1'. Con tale definizione 1 risulterebbe essere un numero primo. Questo creerebbe problemi sull'unicità della scomposizione in fattori primi, perché potremmo introdurre fra i fattori primi di un numero il numero 1 con qualsiasi esponente. Per questo motivo si preferisce non considerare il numero 1 come numero primo. Una definizione equivalente a quella che abbiamo dato e più simile a quella che probabilmente ricordavi è:

'Un numero maggiore di 1 si dice primo se ha come divisori solo se stesso e 1'.

1.8 Massimo comun divisore e minimo comune multiplo di due numeri naturali

Se due numeri naturali *a* e *b* sono entrambi divisibili per il numero naturale *k*, diciamo che *k* è un *divisore comune* di *a* e *b*.

Ad esempio i numeri 108 e 144 hanno come divisori comuni i numeri : 1, 2, 3, 4, 6, 9, 12, 18, 36.

Siccome l'insieme dei divisori comuni di due numeri *a* e *b* è un insieme finito (cioè ha un numero finito di elementi) esiste il massimo di tale insieme, cioè il più grande dei divisori comuni di *a* e *b*: tale numero si chiama ***massimo comun divisore*** (M.C.D.) dei numeri a e b. (In realtà esiste anche il minimo dell'insieme dei divisori comuni, ma è poco interessante. Perché?).

In altre parole si ha la:

Definizione: Si dice *massimo comun divisore* (M.C.D.) di due numeri *a* e *b* il più grande dei divisori comuni di *a* e *b*.

Esempi: Il M.C.D. di 108 e 144 è 36.

Si usa anche scrivere (108, 144) = 36.

Definizione: Se il M.C.D. di due numeri *a* e *b* è 1 (cioè quando 1 è l'unico divisore comune di *a* e *b*), diciamo che *a* e *b* sono *primi fra loro.*

Esempio: 74 e 75 sono primi fra loro.

Se due numeri *a* e *b* hanno entrambi come multiplo un numero *m,* si dice che *m* è *multiplo comune* dei due numeri. L'insieme dei multipli comuni di due numeri è un insieme infinito, che non ha massimo, ma ha minimo (cioè esiste il numero più piccolo dell'insieme). Tale numero si chiama ***minimo comune multiplo*** (m.c.m.) di *a* e *b*.

In altre parole si ha la:

Definizione: Si dice ***minimo comune multiplo*** (m.c.m.) di due numeri *a* e *b* il più piccolo dei multipli comuni di *a* e *b*.

Problemi:

1) Dimostrare che la relazione di divisibilità è una relazione d'ordine non totale.

Ricordiamo la definizione di *relazione d'ordine totale*.

Una *relazione d'ordine* in un insieme A è una relazione che verifica le seguenti proprietà:
1) $a \le a \ \forall a \in A$ (proprieta' riflessiva)
2) se $a \le b$ e $b \le a$ allora $a = b$ (proprietà antisimmetrica)
3) se $a \le b$ e $b \le c$ allora $a \le c$ (proprietà transitiva).
Se inoltre vale anche la proprietà:
4) $\forall a, b \in A$ vale una sola delle seguenti relazioni:
$a < b$; $b < a$; $a = b$ (tricotomia)
allora la relazione si dice di ordine *totale*.

2) Se *a* e *b* sono primi fra loro, qual è il loro m.c.m.?

Osservazione: Si può dimostrare che dati due numeri naturali *a* e *b*, il numero *m* è *minimo comune multiplo* di *a* e *b* se e solo se valgono le seguenti tre proprietà:

(i) *a* divide *m*

(ii) *b* divide *m*

(iii) ogni numero *n* che divide *a* e *b* divide anche *m*.

Problemi:

1) Cosa vuol dire 'se e solo se'?

2) Scrivi la proprietà (iii) usando il simbolismo matematico

2. L'INSIEME DEI NUMERI INTERI

Come abbiamo visto nell'insieme N dei numeri naturali non sempre è possibile fare la sottrazione. Ad esempio 3 – 5 'non si può fare', nel senso che non esiste nessun numero naturale che sommato a 5 dia 3.

Per poter eseguire tutte le sottrazioni possibili si 'estende' l'insieme N all'insieme dei numeri interi relativi, indicato con Z, o anche {…, –2, –1, 0, 1, 2, …}: l'insieme dei relativi si ottiene dall'insieme dei naturali aggiungendo gli interi 'negativi' (questa costruzione si può fare in modo rigoroso, ma a noi qui non interessa).

Possiamo anche dire che per ogni numero naturale *n* introduciamo il suo 'opposto': il numero negativo che indichiamo con - *n*. In questo modo diventa possibile eseguire la sottrazione fra due numeri interi qualunque.

Nell'insieme Z ogni numero *a* ha un *opposto*: se il numero è positivo (ad esempio *a*=5), l'opposto sarà negativo (-5); se il numero è negativo (ad esempio *a*= - 4) l'opposto sarà positivo (4). In generale l'opposto del numero *a* si indica con – *a*.

L'insieme Z contiene come sottoinsieme l'insieme dei numeri positivi (cioè {1, 2, …}, che si possono anche scrivere {+1, +2, …}), cioè l'insieme N.

Definizione: Si chiama *valore assoluto*, o *modulo*, di un numero intero *a*, e si indica con |a|, il numero stesso se *a* è positivo o nullo, il suo opposto se *a* è negativo.

Proprietà del valore assoluto:

1) $|x| \geq 0 \qquad \forall x \in Z \qquad\qquad |x| = 0 \Leftrightarrow x = 0$

2) $|x \cdot y| = |x| \cdot |y| \qquad \forall x, y \in Z$

3) $|x + y| \leq |x| + |y| \qquad \forall x, y \in Z$ (disuguaglianza triangolare)

(dimostrarlo)

Definizione: Due numeri interi, diversi dallo zero, si dicono *concordi* se sono entrambi positivi o entrambi negativi. In caso contrario si dicono *discordi*.

2.1 Operazioni fra numeri interi

Vogliamo ora definire *addizione* e *moltiplicazione* nell'insieme Z, a partire dalle operazioni di addizione e moltiplicazione definite in N.

Si tratta quindi di definire, presi *a* e *b* interi relativi:

- la somma *a* + *b*

- il prodotto *ab*

Nel dare queste definizioni ci poniamo due vincoli:

1) vogliamo che queste operazioni, quando effettuate fra i numeri interi positivi (cioè i 'vecchi' numeri naturali) diano lo stesso risultato che davano in N.

Ad esempio vogliamo che $+7 + (+5) = +12$

e che: $(+7) \cdot (+5) = +35$.

2) Vogliamo che l'addizione e la moltiplicazione in Z godano delle stesse proprietà di cui godevano le analoghe operazioni in N, quindi:

- proprietà commutativa sia per l'addizione che per la moltiplicazione
- proprietà associativa sia per l'addizione che per la moltiplicazione
- proprietà distributiva dell'addizione rispetto alla moltiplicazione.

Si può dimostrare che assumendo questi vincoli, l'unico modo per definire addizione e moltiplicazione fra numeri interi relativi è quello che hai imparato alla scuola media, e che ricordiamo di seguito.

Addizione fra interi

- Per definire la somma $a+b$ di due numeri interi procediamo distinguendo più casi:

1) Se almeno uno dei due numeri è 0, definiamo $a+0=a$ o $b+0=b$

2) Se a e b sono entrambi positivi, li possiamo vedere come numeri naturali, e definiamo $a+b$ come era definita nei naturali.

4) Se a e b sono entrambi negativi, $-a$ e $-b$ sono positivi, quindi sappiamo quanto vale $-a+(-b)$ (vedi punto 2). Definiamo $a+b$ come l'opposto del numero (positivo) $-a+(-b)$.

3) Se a è positivo e b è negativo (cioè a e b sono discordi), distinguiamo tre casi.

Se a (cioè il numero positivo) è quello con valore assoluto maggiore definiamo la somma $a+b$ come la differenza $a-|b|$. Se b è quello con valore assoluto maggiore definiamo la somma $a+b$ come l'opposto della differenza $a-|b|$.

Analogamente se a è negativo e b è negativo (Completa tu….).

Esempi:

+5+(-4)= +1 (in quale dei precedenti casi ricade?)

Moltiplicazione fra interi

Per la moltiplicazione si procede nel seguente modo:

- il prodotto di due numeri interi **concordi *a* e *b*** si definisce come **il numero intero positivo *c*** che ha per valore assoluto il prodotto dei valori assoluti di a e di b.
- il prodotto di due numeri interi **discordi a e b** si definisce come **il numero intero negativo c** che ha per valore assoluto il prodotto dei valori assoluti di a e di b.

Ad esempio:

$(-5)\cdot(-4)=20$

$(+3)\cdot(-2)=-6$

Da quanto detto sopra risulta che il prodotto di due numeri entrambi positivi o entrambi negativi è un numero positivo, e che il prodotto di due numeri di cui uno è positivo e l'altro è negativo è un numero negativo. E' la cosiddetta 'regola dei segni', che recita così "più per più fa più; meno per meno più; più per meno meno."

Osservazione: Il prodotto di un numero intero per 0 è 0. In simboli:

$\forall a \in Z \quad a\cdot 0=0\cdot a=0$

Per dimostrarlo possiamo scrivere:

$$a \cdot 0 = a(1-1) \underbrace{=}_{\text{proprietà distributiva}} a \cdot 1 + a \cdot (-1) = a - a = 0$$

Sottrazione di numeri interi

Per come è stato definito l'insieme Z, è sempre possibile eseguire la sottrazione fra due numeri interi *a* e *b*.

Più precisamente si definisce;

$a - b = a + (-b)$, dove $-b$ è l'opposto di b.

Osservazione: Il segno '-' viene usato quindi per indicare l'opposto di un numero intero, ma anche per indicare la sottrazione fra due numeri.

Problemi:

1) Perché 'non si può dividere per zero'?

(Suggerimento: Abbiamo definito la *divisione* fra due numeri *m* e *n* (che si indica con il segno ' :') come l'operazione che ai numeri *m* e *n* associa quel numero *x* tale che:

$n \cdot x = m$

Quindi dividere un numero m per 0 vorrebbe dire trovare un numero x tale che…)

2.2 L'ordinamento in Z

L'ordinamento di N si estende a Z:
$... < -4 < -3 < -2 < -1 < 0 < 1 < 2 < 3 < 4 < ...$

Anche in questo caso, analogamente a quanto è stato fatto nell'insieme N, si può definire la relazione d'ordine usuale partendo dall'addizione.
Precisamente:
Definizione: Siano $a, b \in Z$. Diciamo che $a \le b$ se e solo se $\exists c \in N : a + c = b$.

Ad esempio $-5 \le -2$. Infatti è vero che $\exists c \in N : -5 + c = -2$. (Chi è *c*?)

Una definizione equivalente è:
Definizione: Siano $a, b \in Z$. Diciamo che $a \le b$ se e solo se $b - a \in N$.

Diciamo poi che $a < b$ se $a \le b$ e $a \ne b$.

Anche in Z valgono le seguenti proprietà:
1) $a \le a \ \forall a \in Z$ (proprieta' riflessiva)
2) se $a \le b$ e $b \le a$ allora $a = b$ (proprietà antisimmetrica)
3) se $a \le b$ e $b \le c$ allora $a \le c$ (proprietà transitiva).
4) Tricotomia
$\forall a, b \in Z$ vale una sola delle seguenti relazioni:
$a < b;\ b < a;\ a = b$

Cioè la relazione che abbiamo definito è una relazione d'ordine (prime tre proprietà) totale (quarta proprietà).

2.4 L'elevamento a potenza fra numeri interi

Per estendere la definizione di elevamento a potenza fra numeri interi si procede come abbiamo fatto per l'addizione e la moltiplicazione. Cioè nel definire tale operazione ci poniamo due vincoli:

1) Vogliamo che questa operazione, quando effettuata fra i numeri interi positivi (cioè i 'vecchi' numeri naturali) dia lo stesso risultato che davano in N

Ad esempio vogliamo che $(+7)^{(+2)} = +49$.

2) Vogliamo che l'elevamento a potenza in Z goda delle stesse proprietà di cui godeva l'analoga operazione in N, quindi:

Proprietà delle potenze:

p1) $\forall\ a,m,n \in N: \quad a^m \cdot a^n = a^{m+n}$

p2) Se $n > m$ e $a \neq 0$ $\dfrac{a^n}{a^m} = a^{n-m}$

p3) $\forall\, a,m,n \in N$**:** $\quad (a^m)^n = a^{m \cdot n}$

p4) $\forall\, a,b,n \in N\ (ab)^n = a^n b^n$

Si può dimostrare che assumendo questi vincoli, l'unico modo per definire l'operazione di elevamento a potenza fra numeri interi relativi è quello che hai imparato alla scuola media, e precisamente:

- Se la base a è un intero negativo, e n è un numero naturale, si definisce ancora:

$$a^n = \underbrace{a \cdot a \cdot a.... \cdot a}_{n \text{ volte}}$$

- Qualsiasi sia la base *a* diversa da zero (positiva o negativa) se l'esponente *m* è negativo, si definisce:

$$a^m = \frac{1}{a^{-m}}$$

- Inoltre si definisce:

$$a^0 = 1$$

Osservazione: Si può dimostrare che l'operazione così definita gode delle proprietà elencate sopra.

Se nella p1) sostituiamo all'insieme N l'insieme Z:

p1)' $\quad \forall\ a,m,n \in Z: \quad a^m \cdot a^n = a^{m+n}$

questa comprende anche la proprietà p2). (Perché?)

Osservazione: Non avrebbe senso definire la potenza a esponente un interno negativo come moltiplicazione ripetuta. Cosa vorrebbe dire che 3^{-4} è il prodotto di -4 fattori uguali a 3?

Osservazione: Se $a \in Z$ e $n \in N$, allora:

- se n è dispari a^n ha lo stesso segno di a;
- se n è pari, a^n è positivo, qualsiasi sia il segno di *a.*

Perché?

2.3 Divisione di numeri interi: la divisione con resto (divisione 'euclidea')

Come abbiamo visto nell'insieme dei numeri naturali, la divisione si definisce come operazione inversa della moltiplicazione.

Anche nel caso degli interi quindi si può definire la *divisione* fra due numeri interi *a* e *b* come l'operazione che ai numeri *a* e *b* associa quel numero *x* tale che:

$b \cdot x = a$

In generale presi due numeri interi qualsiasi *a* e *b*, non è detto che tale *x* esista.

A esempio se *a* = -7 e *b* = 2, non esiste nessun numero *x* intero tale che:

$b \cdot x = a$ cioè tale che $2 \cdot x = -7$

Possiamo estendere all'insieme Z la relazione di 'divisibilità' data in N.

Definizione: Se *a* e *b* sono due numeri interi per cui esiste $k \in Z$ tale che:

$b \cdot k = a$

si dice che *a* è multiplo di *b* (o che '*b* è divisore di *a*', o che '*b* divide *a*').

In ogni caso è possibile fra due numeri interi effettuare la 'divisione con resto'. Si tratta semplicemente della divisione che ognuno di noi ha imparato ad eseguire alla scuola elementare fra un numero a – detto dividendo – e un numero b diverso da 0- detto divisore- ottenendo un quoziente e un resto.
In termini teorici, questo corrisponde al seguente teorema (di cui omettiamo la dimostrazione).

TEOREMA (DIVISIONE EUCLIDEA)
Per ogni coppia di interi *m, n,* con $n \neq 0$, esistono e sono unici gli interi *q, r* tali che $m = nq + r$ e $0 \leq r < |n|$.

Esempi:

- Se *m*=19, *n*=5, allora *q*=3, *r*=4
Si può scrivere:
$19 = 3 \cdot 5 + 4$

- Se *m* = –21, *n* = 6, allora *q* = –4, *r* = 3
Si può scrivere:

$-21 = 6 \cdot (-4) + 3$

Problemi:

1) Nell'enunciato del teorema:
- quale lettera designa il *dividendo*?
- quale lettera designa il *divisore*?
- quale lettera designa il *quoziente*?
- quale lettera designa il *resto*?

2) Calcolate quoziente e resto della divisione euclidea di 53 per 3

3) Calcolate quoziente e resto della divisione euclidea di –53 per 3

4) Calcolate quoziente e resto della divisione euclidea di 53 per –3

5) Perché è necessaria la condizione $n\neq 0$? Che cosa potrebbe succedere se non fosse verificata?

6) Secondo te sarebbe meglio aggiungere la condizione $n\leq m$?

7) Che cosa succede se $m=0$?

8) Che cosa succederebbe se eliminassimo le due condizioni su r?

9) *Che cosa succederebbe se al posto delle condizioni $0\leq r<n$ mettessimo $-n<r\leq 0$?

Definizione: Se, dati m, n con $n\neq 0$ si ottiene $r=0$ come resto della divisione euclidea, cioè se esiste un intero q tale che $m=n\cdot q$, si dice che m è divisibile per n (o che "n è un divisore di m" o "n divide m" o "m è un multiplo di n").

Esempi

- 54 è divisibile per 6 perché il resto della divisione di 54 per 6 è 0.
- –17 non è divisibile per 4 perché il resto della divisione di –17 per 4 è 3.

Attenzione!
La divisibilità è una relazione e dà origine a una formula, la divisione è un'operazione e dà origine a un termine. Quindi "12 è divisibile per 3" è un'affermazione vera. "12 diviso 3 dà 4 come quoziente e resto 0" è un'altra affermazione vera. "12 diviso 3" non è un'affermazione, può essere un modo alternativo di rappresentare il numero 4.

Osservazione: Il teorema precedente ci suggerisce modi per rappresentare particolari classi di numeri interi. Come possiamo rappresentare un generico numero dispari? Dato che i numeri dispari sono tutti e soli quelli la cui divisione euclidea per 2 dà come resto 1, possiamo rappresentare un generico numero dispari con la scrittura $2k+1$, dove k può variare negli interi. Analogamente, un generico numero pari sarà rappresentato dalla scrittura $2k$. Per sapere se un numero è pari o dispari ci serve soltanto il suo resto nella divisione euclidea per 2, non il quoziente.

Problemi:

1) Quale scrittura potrebbe rappresentare un generico multiplo di 3?
2) La scrittura $10k$ va bene per rappresentare un generico multiplo di 5?
3) Qual è l'insieme descritto dall'espressione $3k+2$, al variare di k negli interi?

4) Tre studenti devono stabilire se è vero che 10^{30} è divisibile per $10^{20}+1$. Il primo studente dice: "Non è vero perché i fattori primi di 10^{30} sono 2 e 5, mentre $10^{20}+1$ non è multiplo né di 2 né di 5." Il secondo studente dice: "È vero perché se provi con la calcolatrice ti dà un risultato esatto: 10^{10}." Il terzo studente dice: "Non è possibile saperlo, sono numeri troppo grandi". Secondo te, chi ha ragione? Perché? È possibile che abbiano tutti ragione? In caso contrario, dove sbagliano quelli che sbagliano?

5) Uno studente deve risolvere il problema: se $m = 3^2 \cdot 5^4 \cdot 7^{19} \cdot 11^5 \cdot 19^{20}$, è vero che $m+5$ è multiplo di 10? Lo studente pensa: "Sicuramente la rappresentazione in base dieci di m ha un 5 come cifra delle unità." Secondo te, è vero quello che pensa lo studente? È utile per rispondere al problema?

6) Di un numero intero n si sa che è divisibile per 7 ed è divisibile per 9. Si può concludere che n è divisibile per 63?

7) Di un numero intero k si sa che è divisibile per 4 ed è divisibile per 6. Si può concludere che è divisibile per 24?

3. NOTE

3.1 Il linguaggio matematico: espressioni simboliche

Finora abbiamo utilizzato espressioni matematiche senza pensarci troppo sopra. Adesso proviamo a guardarle un po' meglio. Le espressioni (tradizionalmente denominate 'algebriche' nel caso contengano lettere) si dividono in due categorie: quelle che rappresentano oggetti o funzioni (dette anche *termini*) e quelle che esprimono proprietà o relazioni (dette anche *formule*). I termini sono il corripondente simbolico dei nomi, o delle costruzioni che nel linguaggio verbale svolgono le funzioni dei nomi. Le formule sono il corrispondente simbolico delle *proposizioni* (o *enunciati*). In matematica si usano espressioni sia simboliche sia verbali, a volte anche mescolate insieme.

Esempi
Le seguenti espressioni sono termini

- $7+2$ Questa scrittura è equivalente a scritture come: 9; $2+7$; $\frac{18}{2}$; $a+9-a$
- $7+x$ Questa scrittura al variare di x negli interi rappresenta un numero intero.
- $10^7 - 7$ Questa scrittura rappresenta un numero intero. Sapreste scriverne una rappresentazione in base dieci senza l'aiuto della calcolatrice?

Le seguenti espressioni sono formule

- $7+2=9$ Questa è una formula vera.
- $8-3=6$ Questa è una formula falsa
- $5a=15$ Questa è una formula vera se $a=3$, falsa in tutti gli altri casi.
- $0<x^2+1$ Questa è una formula vera per ogni valore reale di x.

Uso delle Parentesi

Per scrivere espressioni algebriche si usano alcune convenzioni che riguardano la precedenza degli operatori. Una formula come $3+7\cdot5$ senza un criterio di lettura potrebbe essere interpretata come $(3+7)\cdot5$ oppure come $3+(7\cdot5)$. Nella scuola media abbiamo imparato che la seconda interpretazione è quella adottata universalmente in matematica. Le principali convenzioni sono:

$a\cdot b+c$ si legge come $(a\cdot b)+c$	[e non $a\cdot(b+c)$]
$-a+b$ si legge come $(-a)+b$	[e non $-(a+b)$]
$a/b\cdot c$ si legge come $(a/b)\cdot c$	[e non $a/(b\cdot c)$]
$a/b+c$ si legge come $(a/b)+c$	[e non $a/(b+c)$]
$a\cdot b^c$ si legge come $a\cdot(b^c)$	[e non $(a\cdot b)^c$]
$a+b^c$ si legge come $a+(b^c)$	[e non $(a+b)^c$]

Si usa anche dire che in mancanza di parentesi la moltiplicazione ha la precedenza sull'addizione, e l'elevamento a potenza ha la precedenza sull'addizione e sulla moltiplicazione.
Inoltre:

a^{b^c} sta per $a^{(b^c)}$ [e non per $\left(a^b\right)^c$ che equivale a a^{bc}]

3.2Verifiche e dimostrazioni

Abbiamo visto che una formula può essere verificata per tutti, alcuni o nessun valore delle lettere che vi compaiono. Il modo più immediato per verificare se una formula è vera per un certo valore di una certa lettera è di fare la sostituzione. Se però vogliamo sapere se una formula vale per un insieme infinito di valori, come ad esempio per tutti i numeri naturali, non è possibile eseguire tutte le sostituzioni necessarie. Occorre trovare altri modi. Vediamo qualche esempio.

Esempi

- Considerate la proprietà "La somma di un numero dispari col numero dispari seguente è un multiplo di 4". Facciamo qualche prova: 1+3=4; 3+5=8; 5+7=12; 7+9=16, … Possiamo essere certi che la proprietà vale in generale? In base alle sole prove eseguite, no. Possiamo però ragionare come segue. Un numero dispari generico può essere rappresentato da $2n+1$, dove n è un intero. Il dispari seguente può essere rappresentato da $2n+3$. La loro somma è $4n+4$ che è certamente un multiplo di 4, indipendentemente dal valore di n. Infatti $4n+4 = 4(n+1)$.
- La *congettura di Goldbach* (formulata nel 1742) afferma che ogni numero pari maggiore di 2 può essere rappresentato come somma di due numeri primi. In tutte le prove fatte finora, anche con calcolatori di grande potenza, per tutti i numeri pari testati si è sempre trovata una rappresentazione come somma di due primi. Tuttavia la congettura di Goldbach non è un teorema perché non c'è una dimostrazione che valga per tutti gli infiniti numeri pari maggiori di 2. Quindi, per quanto ne sappiamo oggi, un giorno qualcuno potrebbe trovare un numero pari (molto grande, evidentemente) che non è la somma di due primi, oppure qualcun altro potrebbe trovare una dimostrazione generale della congettura, trasformandola in teorema.
- È vero che, al variare di x nei naturali, l'espressione x^2+x+5 rappresenta un numero primo? L'affermazione è verificata per $x=0$, $x=1$, $x=2$, $x=3$. Uno studente pigro potrebbe accontentarsi di queste verifiche e dire "… e così via". Invece per $x=4$ si ottiene 25, che non è primo. Quindi l'affermazione non è vera in generale.

Problemi

1) Secondo voi è vera o no la proprietà: "Per ogni numero naturale x il numero naturale x^2-x+11 è primo."?
2) Secondo voi è vera o no la proprietà: "Per ogni numero naturale x il numero naturale x^2+x+41 è primo."?
3) Sapete trovare un valore intero di x per il quale il valore dell'espressione x^3+x^2+x+47 è un numero primo? E uno per cui il valore dell'espressione è un numero non primo?