Aritmetica

L'aritmetica è lo studio dei numeri nell'insieme $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$

In questo insieme abbiamo due operazioni:

- Addizione, identificata dal segno +
- Moltiplicazione, identificata dal segno ·

Queste operazioni seguono due proprietà:

- Associatività, $\forall a, b, c \in \mathbb{Z}\ (a + b) + c = a + (b + c)$ e $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- Commutatività, $a + b = b + a$ e $a \cdot b = b \cdot a$

Inoltre esiste la **proprietà distributiva della moltiplicazione rispetto alla somma**:

$$\forall a, b, c \in \mathbb{Z}$$

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

Ognuna di queste operazione ha un elemento neutro(ossia un elemento tale che

$a + 0 = a$ e $a \cdot 1 = a$):

- Per l'addizione è l'elemento 0
- Per la moltiplicazione è l'elemento 1

Invertibilità

Ogni elemento ha un inverso, detto opposto, rispetto all'addizione, definito come

$-a$ tale che $a + (-a) = 0$

Per la moltiplicazione, l'esistenza dell'inverso non è garantita in $\mathbb{Z}$, difatti in $\mathbb{Z}$ l'unico elemento che ha un inverso è ± 1 che ha come inverso se stesso.

Ordinamento di $\mathbb{Z}$

L'insieme $\mathbb{Z}$ ha un sottoinsieme che è quello dei numeri naturali $\mathbb{N} = \{0, 1, 2, 3, ...\}$ ossia i numeri positivi.

$\mathbb{Z}$ Si può ordinare con quest'ordine: $a \leq b$ se $b - a \in \mathbb{N}$

Divisibilità

Dati 2 interi a,b diciamo che a divide b, scritto come a | b, se esiste $c \in \mathbb{Z}$ tale che $b = ac$

Da questo ne possiamo dedurre le seguenti proprietà:

- $\forall n \in \mathbb{Z},\ n \mid \pm n)$
- $\forall n \in \mathbb{Z},\ n \mid 0)$
- 0 è l'unico multiplo di se stesso
- ±1 dividono tutti i numeri interi
- Se n|a e n|b, allora n|a+b e n|a-b
- Se n|a, allora n|ab. Non è detto che n|b
- Ogni numero ha come divisore ±se stesso e ±1
- 0 ha come divisore tutti i numeri in $\mathbb{Z}$

Irriducibilità

Dato $n \neq 0$, n si dice **irriducibile** se ha come divisori solamente ±se stesso e ±1, altrimenti dice **riducibile**

Numeri primi

Dato $n \neq \pm 1$ e $n \neq \pm n$, n si dice primo ⇔ n|ab implica n|a e n|b.

Inoltre, un numero è primo ⇔ è irriducibile.

Insieme dei divisori

Denotiamo come D_n l'insieme di tutti i divisori del numero n.

Se a|n, allora $|a| \leq |n|$

Quest'insieme sarà sempre finito.

L'unica eccezione è $D_0 = \mathbb{Z}$ e quindi $|D_0| = \infty$

Massimo comune divisore

Dati due insiemi dei divisori, la loro intersezione non potrà mai essere vuota perchè, come abbiamo detto prima, tutti i numeri hanno come divisori ±se stesso e ±1.

Data l'intersezione d'insiemi dei divisori, possiamo calcolare il massimo comune divisore, cioè tra il massimo divisore comune tra gli insiemi dei divisori.

Viene denotato come $MCD(a,b)$ oppure (a,b)

Proprietà del MCD

- Se m|n, allora $MCD(m,n) = |m|$
- $(m,0) = |m|$

Divisione euclidea

La divisione euclidea è la divisione con resto ed è definita dal seguente teorema:

Siano $a,b \in \mathbb{Z}$ con $b \neq 0$ dove a è il **dividendo** e b è il **divisore**, esistono e sono unici due interi $q,r \in \mathbb{Z}$, q detto **quoziente** e r il **resto**, tali che $a = (b \cdot q) + r$ con $0 < r < |b|$

Adesso vediamo due applicazioni dell'algoritmo di divisione che abbiamo appena visto.

Notazione posizionale

La notazione posizione è il sistema che usiamo per rappresentare numeri naturali i cui valori dipendono dalla posizione delle cifre.

Sia $B \geq 2$ un numero intero che chiamiamo **base**, e sia C un insieme di simboli chiamate **cifre** che rappresentano i numeri in quell'insieme $\{0,...,b-1\}$

Chiamiamo notazione posizionale di un numero in base b, una successione di cifre che rappresentano $n = C_k, C_{k-1}, ..., C_0$ dove n in base 10 equivale a

$$n = \left\{c_{kb}^{k} + c_{k-1}b^{k-1} + ... + c_1 b^1 + c_0 b^0\right\}$$

Esempio con $b = 2$ e $c = \{0,1\}$

Base 2	Base 10
0	0
1	1
10	2
11	3
100	4
...	...

Per fare questa conversione usiamo l'algoritmo di divisione e dividiamo il numero per la base fino ad ottenere 0 come quoziente

Ad esempio convertendo 4 in base 2 avremo:

- $4:2 = 2r = 0$
- $2:2 = 1r = 0$
- $1:2 = 0r = 1$

Adesso leggiamo i resti dal basso verso l'alto ⇑ e otterremo il numero 100 in base 2.

Questo procedimento funzione per tutte le basi che hanno come insieme di cifre $\{0,...,b-1\}$

Convenzione

Se $b<10$ prendiamo come cifre $\{0,...,b-1\}$. Se $b>10$ usiamo le lettere per definire le cifre oltre il 10 dove A è 10 e le lettere successive crescono di +1.

Ad esempio: convers$2BA7_{13}=2\cdot 13^3+11\cdot 13^2+10\cdot 13+7$

Algoritmo di Euclide per il calcolo del MCD

L'algoritmo di Euclide per calcolare il massimo comune divisore cerca di ridurre a resto 0 una serie di divisioni applicate ad un numero naturale.

Dati $a,b\in\mathbb{Z}$, l'algoritmo di Euclide prevede di effettuare $\frac{a}{b}$, calcolare il resto r e continuare ad effettuare $\frac{divisore}{r}$ finchè non otteniamo $r=0$, quando otteniamo $r=0$ sappiamo che il massimo comune divisore è il dividendo dell'ultima divisione(il resto della penultima).

Esempio:

Calcoliamo $MCD(14575,105)$

- $14575:105=138\ r=85$
- $105:85=1\ r=20$
- $85:20=4\ r=5$
- $20:5=4\ r=0$

Abbiamo trovato $MCD(14575,105)=5$

Dimostrazione

Osserviamo che se Oss$MCD=r_n$ è l'ultimo resto di questa serie di divisioni, vuol dire che r_n sarà sicuramente un divisore di tutti i resti. Inoltre è sicuramente il massimo perchè è l'ultimo divisore che ci dà questa successione.sic

Identità di Bezout

Dati $a,b\in\mathbb{Z}$ non entrambi nulli e dato $d=MCD(a,b)$ allora esistono $A,B\in\mathbb{Z}$ non univoci tali che

$$d=Aa+Bb$$

L'algoritmo di Euclide oltre a calcola $MCD(a,b)$ ci dà anche l'identità di Bezout, ad esempio: Calcoliamo $MCD(126,35)$:

- $126:35=35\cdot 3+21$
- $35:21=21\cdot 1+14$
- $21:14=14\cdot 1+7$
- $14:7=2\cdot 7+0$

Ne ricaviamo che $MCD(126{,}35) = 7$ e ora proviamo a ricavare l'identità di Bezout:

$7 = 21 - 14 = 35 - 21 = 21 - 35 + 21 = -35 + 2 \cdot 21 = -35 + 2 \cdot 126 - 3 \cdot 35 = -35 + 2 \cdot 126 - 6 \cdot 35 = -7 \cdot 35 + 2 \cdot 126$

$-7 \cdot 35 + 2 \cdot 126$ Che è l'identità di Bezout($A = -7$ $B = 2$). Notiamo che per ricavarla abbiamo ripercorso le operazioni che abbiamo fatto per trovare l'MCD ed a ogni passo sostituiamo i numeri con quelli che abbiamo trovato nelle divisioni.

Osservazione

Ci sono ∞ coppie di valori A,B tali che $7 = 126A + 35B$

Equazioni diofantee lineari in due variabili

Le equazioni diofantee sono equazioni a coefficienti interi con soluzioni intere.

Dati A,B e C $\in\mathbb{Z}$, esistono soluzioni intere tali che $Ax + By = C$?

Non sempre queste equazioni hanno soluzioni, ad esempio $6x + 24y = 7$ non ha soluzioni intere perchè $6x + 24y$ da un numero pari $\forall x,y\in\mathbb{Z}$ mentre 7 è un numero dispari.

Grazie all'identità di Bezout però sappiamo quando un equazione diofantee lineare in due variabili ha soluzione:

Proposizione

Siano $a,b,c\in\mathbb{Z}$ con $b \neq 0$ e $d = (a,b)$ cioè $MCD(a,b)$, allora l'equazione diofantea lineare $ax + by = c$ ha soluzioni intere se e solo se $d|c$).

Fattori coprimi

Se $(a,b) = 1$, i fattori a e b si dicono coprimi. Da ciò ne ricaviamo che l'equazione $ax + by = 1$ ha soluzioni se e solo se a e b sono coprimi.

Proposizione

Supponiamo di avere $n,a,b\in\mathbb{Z}$, supponiamo che n sia coprimo di a e $n|ab$), allora $n|b$)

Sia n un numero intero $n\notin 0,1,-1$. Allora n è irriducibile se e solo se n è primo.

Teorema fondamentale dell'aritmetica

Sia n un numero intero, $n\notin 0,1,-1$. Allora esiste un'unica fattorizzazione

$$n = \pm p_1 \cdot p_2 \cdot ... \cdot p_s$$

Dove p_i sono numeri primi positivi.

Da ciò ne ricaviamo che per ogni numero naturale diverso da 0, esiste una fattorizzazione unica.

Inoltre, sappiamo che esistono infiniti numeri primi positivi.