Elementi di teoria dei numeri

$\mathbb{N} = \{0, 1, \dots\}$ naturali , $\mathbb{Z} = \{\dots -2, -1, 0, 1, 2, \dots\}$ interi

$|a|$ valore assoluto di a $\quad |a| = \begin{cases} a & \text{se } a \geq 0 \\ -a & \text{se } a < 0 \end{cases}$

$|\{1, 2, 3, 5\}|$ cardinalità , # elementi insieme

a, d interi, d divide a se $\exists$ intero k : $a = kd$

notazione $d \mid a$ e $d \nmid a$

a è un multiplo di d , d è un divisore di a

$d \mid a$ se e solo se $-d \mid a$ $\Rightarrow$ divisori interi non negativi

d divisore di a , compreso tra 1 e $|a|$

Ogni intero d divide 0. L'intero 0 divide solo se stesso.

Esempio. Divisori di 24: $1, 2, 3, 4, 6, 8, 12$ e 24

1 e 24 divisori banali, detti "fattori"

Un intero $a > 1$ solo con divisori banali, primo

Un intero $a > 1$ con divisori non banali, composto

Esempio. $2, 3, 5, 7, 11, 13, 17, 19, \ldots$ sono primi

<u>Teorema della divisione.</u> $\forall\, a \in \mathbb{Z}$ ed n intero positivo esistono e sono unici interi q, r, tali che

$$a = q \cdot n + r \qquad \text{e} \qquad 0 \le r < n$$

quoziente resto

$a = q \cdot n + r \qquad q = \left\lfloor \frac{a}{n} \right\rfloor \qquad r = a \bmod n$

$a = \left\lfloor \frac{a}{n} \right\rfloor \cdot n + a \bmod n \,, \qquad a \bmod n = a - \left\lfloor \frac{a}{n} \right\rfloor \cdot n$

$n \mid a$ se e solo se $a \bmod n = 0$

Teorema (Infinità dei primi) Esistono infiniti numeri primi.

Relazioni di equivalenza

E insieme, $\quad E \times E$ (prodotto cartesiano) tutte le coppie poss.

Relazione su $E \longrightarrow$ qualsiasi sottoinsieme $S \subseteq E \times E$

Relazioni di equivalenza soddisfano le proprietà

1) Riflessiva: $\forall a \in E$, $(a,a) \in S$

2) Simmetrica: $\forall a, b \in E$, se $(a,b) \in S$ allora $(b,a) \in S$

3) Transitiva: $\forall a, b, c \in E$, se $(a,b) \in S$, $(b,c) \in S$, allora $(a,c) \in S$

Indichiamo con $\sim$ una rel. di eq. su E

$x \sim a$ per dire (x,a) app. alla relazione

l'insieme $[a] = \{x \in E : x \sim a\}$ insieme degli x in relazione con a

Teorema. $\forall a, b \in E$, se $a \in [b]$ allora $[a] = [b]$

Discende che in una rel. di equ.

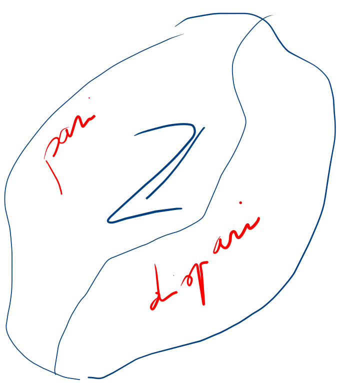
1) ciascuna classe non è vuota (prop. riflessiva)

2) ogni el. appartiene ad un'unica classe

3) le classi partizionano E

4) un elemento di una classe è un rappresentante della classe

Congruenze



a divisibile per 2, pari

non divisibile per 2, dispari

$\mathbb{Z}$ partizionato in multipli di 2 e non

Potremmo usare 3, 4, ... e partizionare in multipli e non

Possiamo raffinare la partizione raggruppando i non multipli in base al resto

Dati interi a, b e n intero positivo se

$$(a \bmod n) = (b \bmod n) \quad \text{scriveremo} \quad a \equiv b \bmod n$$

e diremo che a è congruente a b modulo n

Lemma. $a \equiv b \bmod n$ se e solo se $n \mid (b-a)$

La relazione di congruenza mod n su $\mathbb{Z}$ è una rel di equ.

1) $a \equiv a \bmod n$

2) $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$

3) $\left.\begin{array}{l} a \equiv b \bmod n \\ b \equiv c \bmod n \end{array}\right\} \Downarrow$ $a \equiv c \bmod n$

$\mathbb{Z}$ partizionato in "classi di congruenza" a seconda del resto

$$[a]_n = \{ a + k \cdot n : k \in \mathbb{Z} \} \qquad \text{mod}_n$$

Esempio $\quad [3]_7 = \{ \dots, -11, -4, 3, 10, 17, \dots \}$

Una classe può essere denotata uno qualsiasi dei suoi elementi

$$[3]_7, \ [-11]_7, \ [10]_7 \ \dots$$

L'insieme di tutte le classi di equivalenza mod n

$$\mathbb{Z}_n = \{ [a]_n : 0 \leq a \leq n-1 \}$$

Usando il più piccolo el. positivo per rappr. ogni classe

$$\mathbb{Z}_n = \{ a : 0 \leq a \leq n-1 \} \leftarrow$$

$$\mathbb{Z} = \{ \dots -2, -1, 0, 1, 2, \dots \}$$

viene partizionato in

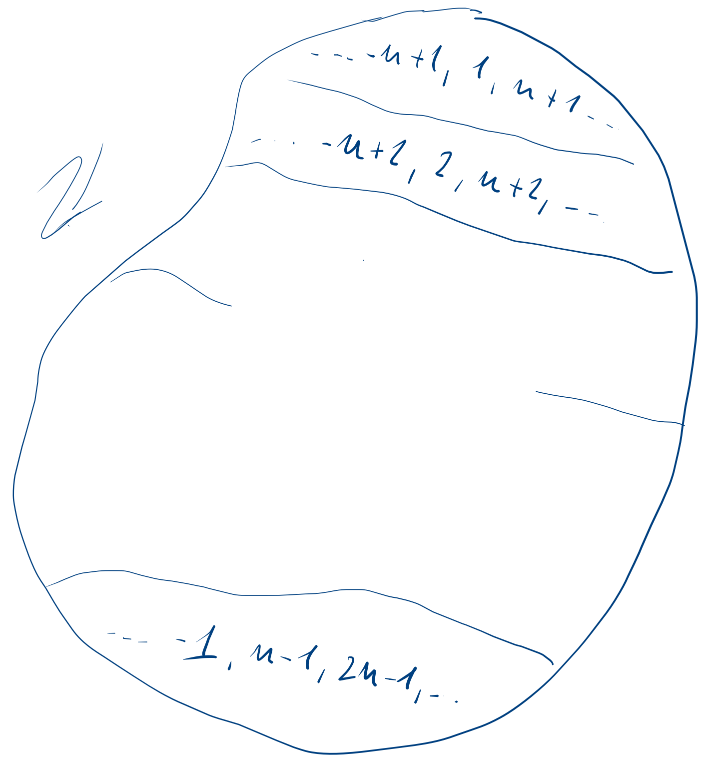
$$\mathbb{Z}_{\underline{0}} = \{ \dots -n, 0, n, \dots \}$$

$$\mathbb{Z}_{\underline{1}} = \{ \dots -n+1, \underline{1}, n+1, \dots \}$$

$$\mathbb{Z}_{\underline{2}} = \{ \dots -n+2, \underline{2}, n+2, \dots \}$$

$$\vdots$$

$$\mathbb{Z}_{\underline{n-1}} = \{ \dots -1, \underline{n-1}, 2n-1, \dots \}$$



classi disgiunte che ricoprono $\mathbb{Z}$

Osservazioni : sommo due elementi qualsiasi di due classi

$\Rightarrow$ risultato elemento della stessa classe

moltiplico due elementi qualsiasi di due classi

$\Rightarrow$ risultato elemento della stessa classe

$+$, $\cdot$ univocamente determinate dalle classi

Massimo comune divisore

a, b interi, $d \mid a$ e $d \mid b \Rightarrow d$ divisore comune di a e b

Esempio 30, 1, 2, 3, 5, 6, 10, 15 e 30 $\Rightarrow$ 1, 2, 3 e 6

24, 1, 2, 3, 4, 6, 8, 12 e 24 divisori comuni

Se $d \mid a$ e $d \mid b$, allora $d \mid (a+b)$ e $d \mid (a-b)$

Anzi, $\forall x, y \in \mathbb{Z}$, se $d \mid a$ e $d \mid b$, allora

$$d \mid (ax + by)$$

Inoltre, se $a \mid b$, allora $|a| \leq |b|$ oppure $b = 0$.

Il massimo comune divisore di due interi non entrambi nulli è il più grande divisore comune.

Notazione $\quad MCD(a,b)$ oppure $gcd(a,b)$

greatest common divisor

Teorema. Se a, b interi non entrambi nulli, allora $MCD(a,b)$ è il più piccolo intero positivo dell'insieme

$$\{a \cdot x + b \cdot y \;:\; x, y \in \mathbb{Z}\}$$

(più piccolo intero positivo combinazione lineare di a e b)

Un po' di proprietà ...

Corollario. Se a, b interi, $d \mid a$ e $d \mid b$, allora $d \mid MCD(a, b)$

Corollario. Se a, b interi, n intero non negativo, allora

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

Def. Due interi a e b relativamente primi se $MCD(a, b) = 1$

Corollario. Dati n, a, b, se $n \mid a \cdot b$ e $MCD(a, n) = 1$,

$$\Longrightarrow \quad n \mid b$$

Teorema. Dati n, a, b, se $MCD(a, n) = 1$, $MCD(b, n) = 1$

$$\Longrightarrow \quad MCD(a \cdot b, n) = 1$$

Corollario. Per tutti i primi p e tutti gli interi a, b, se $p \mid a \cdot b$, allora $p \mid a$ o $p \mid b$

Lemma. Se $a \mid p$ e $b \mid p$ e $MCD(a,b) = 1$

$$\Rightarrow \quad a \cdot b \mid p$$

Teorema (Unicità fattorizzazione) Un intero composto a può essere scritto come prodotto

$$a = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$$

in modo unico, dove, per $i = 1, \ldots, r$, gli interi p_i sono primi: $p_1 < p_2 < \ldots < p_r$ e gli e_i sono interi positivi.

Teorema: $\forall$ a intero non negativo, b positivo

$$MCD(a,b) = MCD(b, a \bmod b)$$

Sketch: $u \mid a$ e $u \mid b \Rightarrow u \mid r$

$\rightarrow$ $r = a - bq = su - (tu)q = \underbrace{(s-qt)}_{t'} \cdot u \Rightarrow u \mid r$

$u \mid b$ e $u \mid r \Rightarrow u \mid a$

$\rightarrow$ $a = b \cdot q + r = (tu)q + t'u = (tq + t')u \Rightarrow u \mid a$

$\{$divisori comuni $a, b\} \equiv \{$divisori comuni $b, r\}$

Forma algoritmica

Euclid (a, b)

if $(b = 0)$ then return a

else return Euclid $(b, a \bmod b)$

Extended_Euclid (a, b)

if $(b = 0)$ then return $(a, 1, 0)$

$(d', x', y') \leftarrow$ Extended_Euclid $(b, a \bmod b)$

$(d, x, y) \leftarrow (d', y', x' - \lfloor a/b \rfloor y')$

return (d, x, y)

Perché funziona!

Se $b = 0$, $(a, 1, 0)$ ok!

$$a = 1 \cdot a + 0 \cdot b$$

Se $b \neq 0$, (d', x', y')

con $d' = MCD(b, a \bmod b)$

$$d' = b \cdot x' + (a \bmod b) \cdot y'$$

$$d = d' = b x' + (a \bmod b) \cdot y'$$

$$= b x' + (a - \lfloor a/b \rfloor \cdot b) \cdot y'$$

$$= a y' + b (x' - \lfloor \tfrac{a}{b} \rfloor \cdot y')$$

$$= a x + b y \qquad \blacksquare$$

Gruppi

Un gruppo $(G, \oplus)$ è un insieme G con un'operazione binaria $\oplus$ per cui valgono

1. Chiusura. $\forall a, b \in G, \quad a \oplus b \in G$
2. Identità. Esiste $e \in G$: $a \oplus e = e \oplus a = a, \ \forall a \in G$
3. Associatività. $\forall a, b, c \in G, \quad a \oplus (b \oplus c) = (a \oplus b) \oplus c$
4. Reciproco. $\forall a \in G, \ \exists! \, b \in G : a \oplus b = b \oplus a = e$

Se soddisfa anche

5. Commutativa. $\forall a, b \in G, \quad a \oplus b = b \oplus a$

il gruppo si dice Abeliano

Esempi di gruppi

$(\mathbb{Z}, +)$ $\qquad$ $(n\mathbb{Z}, +)$ $\qquad$ $(\{0,1\}^n, \oplus)$

(multipli di n) $\qquad$ XOR

$(\mathbb{Z}, \cdot)$ NON è un gruppo (e.g. 2 non ha reciproco)

$(\mathbb{R}, \cdot)$ NON è un gruppo (e.g. 0 non ha reciproco)

$(\mathbb{R}\setminus\{0\}, \cdot)$ è un gruppo

Teorema (legge di cancellazione). In un gruppo $(G, \oplus)$

1. se $a \oplus b = a \oplus c \Rightarrow b = c$
2. se $b \oplus a = c \oplus a \Rightarrow b = c$

$(G, \oplus)$ se $|G| < \infty$, il gruppo si dice <u>finito</u>

$|G|$ costituisce l'ordine del gruppo

Gruppi finiti additivo e moltiplicativo modulo n

Possiamo costruire gruppi finiti su $\mathbb{Z}_n$

Osservazione: dati a, a', b e b', se

$a \equiv a' \bmod n$ e $b \equiv b' \bmod n$

allora

$(a+b) \equiv (a'+b') \bmod n$ e $a \cdot b \equiv a' \cdot b' \bmod n$

Pertanto, possiamo definire $+_n$ (somma) e $\cdot_n$ (prodotto) su $\mathbb{Z}_n$

$$[a]_n + [b]_n = [a+b]_n \qquad [a]_n \cdot [b]_n = [a \cdot b]_n$$

Teorema. $(\mathbb{Z}_n, +_n)$ è un gruppo finito abeliano

Lemma. $\forall\, a, z$ interi, n intero positivo

$$(a \cdot n + z) \equiv z \mod n$$

Lemma. Siano a ed n interi tali che $MCD(a, n) = 1$

$\forall\, k \in \mathbb{Z}$, $MCD(a + kn, n) = 1$

Sia

$$\mathbb{Z}_n^* = \{ [a]_n \in \mathbb{Z}_n : MCD(a, n) = 1 \}$$

(interi a relativamente primi con n)

Teorema $(\mathbb{Z}_n^*, \cdot_n)$ è un gruppo finito abeliano

Esempio $\mathbb{Z}_{15}^* = \{ [a]_{15} \in \mathbb{Z}_{15} : MCD(a, 15) = 1 \}$

$= \{ 1, 2, 4, 7, 8, 11, 13, 14 \}$

Nota: per dimostrare l'esistenza dei reciproci si noti che

$\forall a \; MCD(a, n) = 1 \Rightarrow$ Extend_Euclid (a, n)

dà $(d, x, y) = (1, x, y)$

$\Rightarrow 1 = a \cdot x + ny \Leftrightarrow ax = 1 - ny$

$a \cdot x \bmod n = (1 - ny) \bmod n \equiv 1 \bmod n \Rightarrow x$ è il reciproco di a

Quanti elementi ha $\mathbb{Z}_n^*$?

Un po' di esempi.

$n = p$ (primo). Allora tutti $a \in \{1, \dots, p-1\}$: $MCD(a,p) = 1$

$$\Longrightarrow \quad |\mathbb{Z}_p^*| = p-1$$

$n = p \cdot q$ (primi). Nota che se $MCD(a,n) \neq 1$, poiché $n \nmid a$ (n è più grande di a) allora $p \mid a$ o $q \mid a$

Gli a divisibili da p sono : $p, 2p, 3p, \dots (q-1)p$

" da q sono : $q, 2q, 3q, \dots (p-1)q$

Gli a restanti sono $n-1-(q-1)-(p-1) = pq-1-(q-1)-(p-1)$

$$= pq - q - p + 1$$

$$= q(p-1) - (p-1)$$

$$= (q-1)\cdot(p-1)$$

$$|\mathbb{Z}_{pq}^*| = (p-1)(q-1) \quad \Longleftarrow$$

$n = p^e$, p primo, $e \geq 1$ intero

Ragionando come prima $a \in \{1, \dots, n-1\}$ non è rel. primo a n

allora p o qualche suo multiplo divide a

Multipli di p tra 0 e $p^e - 1$

$$\underbrace{0 \cdot p,\ 1 \cdot p,\ \dots,\ (p^{e-1} - 1) \cdot p}_{\text{esattamente } p^{e-1}}$$

Pertanto

$$|\mathbb{Z}_{p^e}^*| = p^e - p^{e-1} = p^{e-1} \cdot (p-1)$$

Per un n generico vale il seguente

Siano $p_1, \dots, p_k$ primi distinti, $e_1, \dots, e_k$ interi non neg.

Sia $n = \prod_{i=1}^{k} p_i^{e_i}$. Risulta

$$\left|\mathbb{Z}_n^*\right| = \varphi(n) = \prod_{i=1} p_i^{e_i - 1}(p_i - 1)$$

funzione $\varphi(n)$ di Eulero

Nota: facile vedere che generalizza i casi precedenti

$$\left|\mathbb{Z}_{15}^*\right| = \left|\mathbb{Z}_{3\cdot 5}^*\right| = (3-1)(5-1) = 2 \cdot 4 = 8$$

Sottogruppi e proprietà

$(G, \oplus)$ gruppo, $H \subseteq G$. Se anche $(H, \oplus)$ è un gruppo, diremo che $(H, \oplus)$ è un sottogruppo di $(G, \oplus)$

$\forall a \in G$, indico $a^{(n)}$ il risultato dell'operazione iterata $n-1$ volte. Pongo $a^{(0)} = e$. $a^{(1)} = a$

Teorema. Se $(G, \oplus)$ è un gruppo finito, $\forall a \in G$ $\exists n$ tale che $a^{(n)} = e$

Teorema $(G, \oplus)$ gruppo finito, $H \subseteq G$ tale che

$\forall a, b \in H$, $a \oplus b \in H$ (H è chiuso rispetto a $\oplus$)

allora $(H, \oplus)$ è un sottogruppo di $(G, \oplus)$

Teorema di Lagrange. Se $(G, \oplus)$ è un gruppo finito ed $(H, \oplus)$ è un suo sottogruppo, allora $|H|$ è un divisore di $|G|$

Se $H \neq G$, $(H, \oplus)$ è un sottogruppo proprio di $(G, \oplus)$

Corollario Se $(H, \oplus)$ è un sottogruppo proprio di $(G, \oplus)$ allora $|H| \leq |G|/2$

Sottogruppi generati da un elemento

Abbiamo denotato con $a^{(k)}$ l'elemento ottenuto iterando $\oplus$. E.g. $a=2$ in $(\mathbb{Z}_6, +_6)$

$$a^{(1)} = 2 \qquad a^{(2)} = 4 \qquad a^{(3)} = 0$$

In generale in $\mathbb{Z}_n$ $\quad a^{(k)} = k \cdot a \bmod n$, $\quad \mathbb{Z}_n^* \quad a^{(k)} = a^k \bmod n$

(multipli) (potenze)

In futuro, quando costruiremo gruppi non numerici a seconda dei casi useremo la notazione additiva o moltiplicativa — da interpretare in relazione al contesto

$$\langle a \rangle = \{ a^{(k)} : k \geq 1 \}$$

sottogruppo generato da a, a si dice generatore del gruppo

Se G è finito, $\langle a \rangle$ è finito (al più tutto G)

Risulta $a^{(i)} \oplus a^{(j)} = a^{(i+j)} \Rightarrow \langle a \rangle$ è chiuso $\oplus$

Si definisce ordine di a, $\mathrm{ord}(a)$ il minimo $t : a^{(t)} = e$

Teorema. Per ogni $(G, \oplus)$ finito e $\forall a \in G$, $\mathrm{ord}(a)$ è uguale alla cardinalità del sottogruppo $\langle a \rangle$ che genera

Corollario. Sia $a \in G$ di ordine t.

$a^{(i)} = a^{(j)}$ se e solo se $i \equiv j \mod t$

Corollario. $(G, \oplus)$ finito con unità e, $\forall a \in G$

risulta $a^{|G|} = e$

Definizione. Se esiste $a \in G$ tale che $\langle a \rangle = G$,

allora G si dice <u>ciclico</u> e l'elemento

a <u>generatore</u> o <u>radice primitiva</u> di G

Esempi

$(\mathbb{Z}_{15}, +_{15})$ è un gruppo ciclico. 1 è un generatore

$15 \cdot 1 \equiv 0 \mod 15$ e $0 < i < 15$ risulta $i \cdot 1 = i \not\equiv 0 \mod 15$

Anche 2 è un generatore

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 1, 3, 5, 7, 9, 11, 13\}$$

Non tutti sono generatori

$$\langle 3 \rangle = \{0, 3, 6, 9, 12\}$$

$(\mathbb{Z}_n, +_n)$ è un gruppo ciclico. 1 è un generatore

$(\mathbb{Z}_p, +_n)$ è un gruppo ciclico. Ogni suo elemento è un generatore (a parte 0)

primo

Nota: vale per ogni gruppo di ordine primo

$(G, \oplus)$ ha ordine primo. Allora il Teorema

di Lagrange $\Rightarrow$ non può avere sottogruppi propri

perché p non ammette divisori non banali

$\Rightarrow$ tutti gli elementi di G a meno

dell'elemento identità sono generatori