Extra 1: aritmetica modulare

Saturday, October 10, 2020 7:17 PM

img2020...

8 ottobre 2020

si intende positivi (1)

Ultima lezione.

- Se $n>0$ è un intero, allora esistono $p_1, \dots, p_k$ primi

tali che $n = p_1 p_2 \cdots p_k$.

Attenzione! $n=1$ fornisce $k=0$ (il prodotto vuoto fa 1).

Se non vi piace, mettete $n>1$.

Inoltre $p_1 p_2 \cdots p_k = q_1 \cdots q_\ell$ (tutti i fattori sono primi positivi)

$\Rightarrow k=\ell$ e $p_i = q_i$ $\forall i$ a meno di riordinare i fattori a 2° membro.

In generale si preferisce scrivere

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

dove i p_i sono primi (positivi) distinti e $\alpha_i \geq 1$.

Passando dalla fattorizzazione unica in $\mathbb{N}$ a quella in $\mathbb{Z}$ succedono cose un po' strane:

(1) Gli invertibili vanno trattati a parte. (In $\mathbb{Z}$, sono ± 1).
e creano una forma di indeterminazione in tutte le altre definizioni.

NB: In un anello, a divide u invertibile $\Rightarrow a$ invertibile

Dim: $a \mid u$ vuol dire $u = ax \Rightarrow 1 = a(x u^{-1}) \Rightarrow a$ invertibile.

Mantra: 1 è invertibile, inverso di invertibile è invertibile, prodotto di invertibili è invertibile, divisore di invertibile è inv.
u è inv. $\iff (u) = (1)$

(2) Se p è primo, non lo è più di ogni pu, dove u è invertibile.
In $\mathbb{Z}$, $\pm p$ sono da considerare entrambi primi, ed essenzialmente LO STESSO PRIMO! Il termine corretto è "primi associati".

Def di primo: $p \mid ab \Rightarrow p \mid a$ opp $p \mid b$ si riformula con
$ab \in (p) \Rightarrow a \in (p)$ o $b \in (p)$. Poiché $(p) = (-p)$ non c'è modo di favorire p rispetto a $-p$.

③ Poiché nei ragionamenti di divisibilità elementi associati non sono distinguibili, il "MASSIMO" di MCD va riformulato in altro modo.

"MASSIMO" = ogni altro divisore comune divide il MCD.

$MCD(12,15)=3$ si può scrivere anche $MCD(12,15)=(-3)$ poiché le due affermazioni si traducono $(12)+(15)=(3)=(-3)$.

④ Dal punto di vista della divisibilità, 0 è l'elemento PIÙ GRANDE DI TUTTI: $2\,|\,4\,|\,8\,|\,16\,|\,32\,|\,\dots\,|\,0$.

Pertanto $MCD(0,0)=0$ ha senso, anche se 0 sembra, numericamente, più piccolo.

Congruenze e invertibilità modulo N.

Def: $a\equiv b \bmod N \iff b-a\in(N)$.

È una relazione di equivalenza! (sull'insieme $\mathbb{Z}$).

$a\equiv a \bmod N \iff 0\in(N)$

$a\equiv b \bmod N \iff b-a\in(N)$

$b\equiv a \bmod N$? $\qquad\qquad a-b\in(N)$

$\qquad\qquad\qquad\qquad = -(b-a)$

$a\equiv b \bmod N \quad b-a\in(N)$

$b\equiv c \bmod N \iff c-b\in(N)$

$a\equiv c \bmod N$? $\qquad c-a=(c-b)+(b-a)\in(N)$

Sono le proprietà di sottogruppo e quindi funzionano!

Quante classi di congruenza mod N ho? ③

Casi non interessanti

- $N=0$. La rel. è l'uguaglianza $a\equiv b \bmod(0) \iff a=b$. Ho infinite classi di equivalenza. L'insieme quoziente è (essenzialmente) $\mathbb{Z}$.

- $N=1$ Ogni intero è equivalente a ogni altro.
  Ho una unica classe di equivalenza.

- $N=2$: $a \equiv b \bmod 2 \iff b-a$ è pari $\iff a$ e b hanno la stessa parità.

2 classi di congruenza
$[0] = \{\text{pari}\}$ $[1] = \{\text{dispari}\}$.

$a \equiv r \bmod N$

In generale? $a = bN + r$ $\quad 0 \le r < N$ $\quad N > 1$

(N)

$r \in \{0, 1, 2, \dots, N-1\}$.

Ogni elemento è in una delle classi $[0], [1], [2], \dots [N-1]$ che si chiamano CLASSI DI RESTO.

e sono tutte diverse

$[a] = [b] \iff b-a \in (N)$ ma $|b-a| < N$ non può essere multiplo di N, a meno che $b-a=0$.
$a-b \in (N)$
$0 \le a, b < N$

$\mathbb{Z}/\equiv \bmod N$ possiede N elementi $(N>0)$.

Di solito si indica $\mathbb{Z}/(N)$. ← si legge "ho reso tutti gli elementi di (N) uguali a 0".

NB: So sommare e moltiplicare gli elementi di $\mathbb{Z}/(N)$. (4)

Idea $[a]+[b] \overset{\text{def}}{=} [a+b]$ è ben definita?

$a+hN + b + kN = (a+b) + (h+k)N$ ✓

$[a] \cdot [b] \overset{\text{def}}{=} [ab]$

$(a+hN)(b+kN) = ab + aKN + bhN + hkN^2 =$

$= ab + (ak + bh + hkN)N$ ✓,

Queste operazioni soddisfano le proprietà che soddisfano in $\mathbb{Z}$.
(com., ass., distrib, esistenza di 0 e 1, esistenza di inv.

addittivo)

Es In $\mathbb{Z}/(5)$ $\quad -[1]=[-1]=[4]$

$[2]+[4]=[6]=[1]$ //

$[a]=[b]$ in $\mathbb{Z}/(N) \iff a \equiv b \bmod N.$

$\mathbb{Z}/(N)$ è un anello commutativo con unità.

Importante Non è necessariamente un dominio d'integrità

In $\mathbb{Z}/(6)$ $\quad [2]\cdot[3]=[0]$, ma $[2]\neq[0]$, $[3]\neq[0]$.

$\mathbb{Z}/(5)$ è un dominio d'integrità. ANZI È UN CAMPO!

$[1]\cdot[1]=[1] \quad [2]\cdot[3]=[1] \quad [4]\cdot[4]=[1]$

Ogni elemento $\neq[0]$ ha un inverso moltiplicativo.

Quali sono gli elementi invertibili di $\mathbb{Z}/(N)$? (5)

- Se $MCD(a,N)=1$, allora $[a]$ è invertibile in $\mathbb{Z}/(N)$

Dim: Bézout!

$1 = ha+kN$

$\Rightarrow \quad ha \equiv 1 \bmod N$

$\iff [ha]=[1]$ in $\mathbb{Z}/(N)$

$\iff [h][a]=[1]$ in $\mathbb{Z}/(N)$.

- Se $MCD(a,N)\neq 1$, allora $[a]$ non è invertibile in $\mathbb{Z}/(N)$.

Dim: se esiste $[h]$ t.c. $[a][h]=[1]$, allora

$ha \equiv 1 \bmod N$ cioè $ha-1=kN$ per qualche $k\in\mathbb{Z}$

$\Rightarrow 1 = ha-kN.$

$\ldots \Rightarrow d|1$

Se $MCD(a,N)=d$, allora $d \mid ta$, $a \mid kN$ — [illegible]

$d \neq 1$ conduce a un assurdo.

- $[a]$ è invertibile in $\mathbb{Z}/(N) \iff MCD(a,N)=1$

Conseguenza: se N è composto, $\mathbb{Z}/(N)$ non è un dominio d'integrità: $N=ab \Rightarrow [a]\cdot[b]=[0]$

$[0]^{*}$ $[0]^{*}$

Però, se $N=p$ è primo, $\mathbb{Z}/(p)$ è addirittura un campo!

$[a] \neq [0] \Rightarrow MCD(a,p)=1 \Rightarrow [a]$ invertibile

$1 \leq a \leq p-1$ (RICORDARE: campo $\Rightarrow$ dominio d'integrità)

Applicazioni

(6)

Risoluzione di congruenze lineari

$$ax \equiv b \mod (N)$$

Se per caso $MCD(a,N)=1$ lo so risolvere.

Se $[a]\cdot[k]=[1]$ allora

$[a]\cdot[x]=[b]$

$[k][a][x]=[k][b]$

$[1]$ $[x]=[bk]$ $\quad x \equiv bk \mod N.$

Es: $3x \equiv 4 \mod 5$. l'inverso di 3 mod 5 è 2

$3 \cdot 2 \equiv 1 \mod 5$.

$2 \cdot 3x \equiv 2 \cdot 4 \mod 5$

$x \equiv 8 \equiv 3 \mod 5$

Verifica $3 \cdot 3 = 9 \equiv 4 \mod 5$. ☺.

E se $MCD(a,N) \neq 1$?

x	$2x$
0	0
1	2

mod 6

Es: $2x \equiv 3 \mod 6$ non ha soluzione!

2	4
3	0
4	2
5	4

$2x \equiv 4 \mod 6$

$x \equiv 2 \mod 6$ ma anche $x \equiv 5 \mod 6$???

Fatto $ax \equiv b \mod N$ ha soluzione $\Longrightarrow$ $MCD(a,N)$ divide b.

Dim: Diciamo $d = MCD(a,N)$.

Se x_0 è una soluzione, allora $ax_0 \equiv b \mod N$

$\Rightarrow$ $b - ax_0 = hN \Rightarrow b = ax_0 + hN$.

Ma $d|a$, $d|N \Rightarrow d \mid ax_0 + hN = b$.

È vero anche il viceversa

Premessa: Se $MCD(a,N) = d$ allora $MCD(a/d, N/d) = 1$.

$ax \equiv b \mod N$ ha soluzione non appena $MCD(a,N)$ divide b

Dim: $ax \equiv b \mod N$ esattamente quando esiste $h \in \mathbb{Z}$ tale che $b - ax = hN \Rightarrow b = ax + hN$.

Ora $d = MCD(a,N)$ divide b. Scrivo $b/d = B$, $a/d = A$ sono interi

$d \cdot B = d \cdot Ax + d \cdot hN/d$

$B = Ax + hN/d$

$\Rightarrow Ax \equiv B \mod N/d$

Quindi $ax \equiv b \mod N$ è equivalente a $\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{N}{d}$ e $MCD\left(\frac{a}{d}, \frac{N}{d}\right) = 1$

Ora so risolvere!

(8)

Es: $2x \equiv 4 \mod 6$ $MCD(2,6)$ divide 4? sì!
$MCD(2,6) = 2$

$\Updownarrow$

$x \equiv 2 \mod 3$

(In effetti avevo $x \equiv 2, 5 \mod 6$, cioè $x \equiv 2 \mod 3$).

Riassunto: Devo risolvere $ax \equiv b \mod N$.

$MCD(a,N) = d$ divide b
- no: La congruenza non ammette soluzioni in $\mathbb{Z}$
- sì: risolvo $\frac{a}{d} x \equiv \frac{b}{d} \mod \frac{N}{d}$ che ha soluzione unica mod N/d (o in altre parole, ho d soluzioni in $\mathbb{Z}/(N)$).

Rimangono due cose prima di procedere oltre

1. Piccolo teorema di Fermat
2. Teorema cinese dei resti.

(9)

Piccolo teorema di Fermat.

Premessa.
$$(x+y)^2 = x^2 + 2xy + y^2$$
$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

$(x+y)^n = ?$

Risposta: $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$

$\binom{n}{i}$ è un coefficiente binomiale $= \frac{n!}{i!(n-i)!}$

si dimostra per induzione.

```
        1
       1 1
      1 2 1
     1 3 3 1
    1 4 6 4 1
  1 5 10 10 5 1
```

Es: $(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$.

tutti multipli di 5. È un caso?

Sì (1 4 6 4 1) non sono tutti multipli di 4.

No $\binom{p}{i}$ è sempre multiplo di p se — p è primo — $i \neq 0, p$.

$\binom{p}{i} = \frac{p!}{i!(p-i)!}$ ← qui compare un fattore p primo ← qui no.

Piccolo teorema di Fermat. Se p è primo, allora

$a^p \equiv a \mod p$ per ogni $a \in \mathbb{Z}$.

Oss: $p=2$ ovvio. $p>2$ basta dimostrarlo per $a \in \mathbb{N}$.

Dimostro p divide $a^p - a$ per induzione su a. (10)

$a=0$ p divide $0^p - 0 = 0$ ok.

Passo induttivo

So che $a^p - a$ è multiplo di p. È vero che $(a+1)^p - (a+1)$ è ancora multiplo di p?

$(a+1)^p - (a+1) =$

$= \left(a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \dots + \binom{p}{p-1} a + 1 \right) - a - 1$

multiplo di p — multipli di p — -1

OK.

Teorema cinese dei resti

Tra 1000 e 2000 soldati in piazza d'armi.

In FILA PER 3! (ne avanza 1)
IN FILA PER 5! (non ne avanzano)
IN FILA PER 7! (ne avanza 1)
IN FILA PER 11! (ne avanzano 3)

Quanti sono?

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 0 \mod 5 \\ x \equiv 1 \mod 7 \\ x \equiv 3 \mod 11 \end{cases}$$

$x = 1 + 3h$. Sostituisco in $x \equiv 0 \mod 5$ (11)

$1 + 3h \equiv 0 \mod 5$

$3h \equiv 4 \mod 5$ moltiplico per 2

$h \equiv 3 \mod 5$

$h = 3 + 5k$. Risostituisco $x = 1 + 3(3+5k) =$

$= 10 + 15k.$

Sostituisco in $x \equiv 1 \mod 7$.

$10 + 15k \equiv 1 \mod 7$

$k \equiv 5 \mod 7$ $\quad k = 5 + 7\ell$

$x = 10 + 15(5 + 7\ell) = 85 + 105\ell.$

Sostituisco in $x \equiv 3 \mod 11$

$85 + 105\ell \equiv 3 \mod 11$

$105\ell \equiv -82 \mod 11$

$6\ell \equiv 6 \mod 11$

$\ell \equiv 1 \mod 11 \qquad \ell = 1 + 11m.$

$x = 85 + 105(1 + 11m) =$

$= 190 + 1155m$

$x \equiv 190 \mod 1155$

$x = 190, 1345, 2500$

Sono 1345.

Funziona sempre?

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases} \qquad MCD(m,n) = 1. \quad (2)$$

ammette sempre UN'UNICA soluzione modulo mn.

2 dimostrazioni.

(1) faccio come prima e aiuto di fondo

(2) $\mathbb{Z}/(mn) \xrightarrow{f} \mathbb{Z}/(m) \times \mathbb{Z}/(n)$

$[x]_{mn} \longmapsto ([x]_m, [x]_n)$

f è iniettiva. $([x]_m, [x]_n) = ([y]_m, [y]_n)$

vuol dire $\begin{cases} x \equiv y \mod m \\ x \equiv y \mod n \end{cases} \Rightarrow m, n$ dividono $y - x$

$\Rightarrow mn$ divide $y - x \Rightarrow x \equiv y \mod mn$

$MCD(m,n) = 1$

$\Downarrow$

$[x]_{mn} = [y]_{mn}.$

$\mathbb{Z}/(\quad) \hookrightarrow \mathbb{Z}/(\quad) \times \mathbb{Z}/(\quad)$, che $\mathbb{Z}/(\quad) \times \mathbb{Z}/(\quad)$ hanno mn

Ma sia $\varphi(mn)$ [illegible] $\varphi(m)$ $\varphi(n)$ elementi

$\Rightarrow$ f è anche suriettiva! FINE.

Osservazione: vedremo in seguito che f è un isomorfismo di anelli.

Ultime osservazioni

- La divisibilità si verifica a partire dalla fattorizzazione in primi

Se sappiamo che a divide b, allora $b = ac$ per qualche c

Se $a = u p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ e $c = v q_1^{\beta_1} q_2^{\beta_2} \cdots q_e^{\beta_e}$, allora

$$b = ac = (uv)\, p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \cdots q_e^{\beta_e}$$

Pertanto (a meno di associati) i primi che compaiono in a devono comparire anche in b, con un'esponente maggiore o uguale (potrebbero comparire anche nella fattorizzazione di c).

È vero anche il viceversa: se tutti i primi che compaiono nella fattorizzazione in primi di a compaiono anche in b, li raccolgo tutti a sinistra e quello che mi rimane è un c tale che $b = ac$.

Ne segue che l'MCD(a,b) una volta note le fattorizzazioni, si ottiene prendendo i primi in comune (sempre a meno di associati) al minimo esponente nelle due fattorizzazioni e moltiplicando