Note al corso di
Algebra per Informatica
Combinatoria, Aritmetica, Polinomi, Grafi
a.a. 2023/2024

Lezione 1

Due insiemi si dicono *equipotenti* se esiste un'applicazione biettiva tra i due.
Un insieme si dice *infinito* se è equipotente a una sua parte propria.

- Assioma dell'Infinito (o di Cantor): Esiste un insieme infinito.

Un insieme ordinato si dice *ben ordinato* se ogni sua parte non vuota ammette minimo.
Un insieme si dice *naturalmente ordinato* se è ben ordinato e se ogni parte non vuota superiormente limitata ammette massimo.

Teorema 1. *(No dim.) Esiste un insieme infinito se e solo se esiste un insieme naturalmente ordinato non superiormente limitato.*

Teorema 2. *(No dim.) Tutti gli insiemi naturalmente ordinati non superiormente limitati sono isomorfi (in quanto insiemi ordinati).*

Dunque, assumendo l'assioma di Cantor, scegliamo un insieme naturalmente ordinato non superiormente limitato $(\mathbb{N}, \leq)$ e lo chiamiamo *insieme dei numeri naturali*. Il minimo di $\mathbb{N}$ lo chiamiamo 0, il minimo di $\mathbb{N} \setminus \{0\}$ lo chiamiamo 1 e così via.
Definizione: $\mathbb{N}_m := \{n \in \mathbb{N} \mid m \leq n\}$.

Principio di induzione

Teorema 3. *Principio di induzione di prima forma.*

$$(\forall x \in P(\mathbb{N}) \setminus \{\emptyset\})\big(((\forall n \in \mathbb{N})(n \in x \to n+1 \in x)) \to (x = \mathbb{N}_{min(x)})\big)$$

Dimostrazione. Sia $m = min(x)$ e per assurdo $x \neq \mathbb{N}_m$. Poiché $m = min(x)$, $x \subset \mathbb{N}_m$. Sia $y = \mathbb{N}_m \setminus x \neq \emptyset$ e sia $n = min(y)$. Certo $n \neq m$, quindi $n-1 \in x$ (Attenzione! Chi è $n-1$? È il massimo di quelli $< n$, che esiste per l'ordine naturale). Ma per ipotesi $n = (n-1)+1 \in x$, assurdo. □

Teorema 4. *Principio di induzione di seconda forma (o induzione completa).*

$$(\forall x \in P(\mathbb{N}) \setminus \{\emptyset\})\Big(\big((\forall n \in \mathbb{N})((\forall k \in \mathbb{N})(min(x) \leq k < n \to k \in x) \to n \in x)\big) \to (x = \mathbb{N}_{min(x)})\Big)$$

Dimostrazione. Sia $m = min(x)$ e per assurdo $x \neq \mathbb{N}_m$. Poiché $m = min(x)$, $x \subset \mathbb{N}_m$. Sia $y = \mathbb{N}_m \setminus x \neq \emptyset$ e sia $n = min(y)$. Se k è tale che $m \leq k < n$, allora, poiché $n = min(y)$, $k \in x$. Per la generalità di k abbiamo che

$$(\forall k)(min(x) \leq k < n \to k \in x).$$

Ma per ipotesi $n \in x$, assurdo. □

Cenni di calcolo combinatorio

Definizioni: Se $n \in \mathbb{N} \setminus 0$, dico $I_n := \{1, 2, \dots, n\}$ e $I_0 := \emptyset$. Si chiamano *segmenti iniziali* di $\mathbb{N} \setminus \{0\}$. Un insieme x si dice finito se è equipotente ad un I_n per un qualche $n \in \mathbb{N}$. n si dice *ordine* o *cardinalità* di x.

Esempio: $|a| = 0$ equivale a dire che esiste una funzione $f : a \to I_0 = \emptyset$ biettiva. Questo implica che $a = \emptyset$, altrimenti f non è una funzione.

Teorema 5. $(\forall n \in \mathbb{N})(I_n$ *non è infinito*$)$.

Dimostrazione. Si procede per induzione di prima forma. I_0 non ha parti proprie. OK. Prendo $n > 0$ e suppongo che I_n non sia equipotente ad alcuna sua parte propria. Voglio mostrare che lo stesso vale per I_{n+1}. Assumiamo allora per assurdo che esistano una $x \subset I_{n+1}$ e una funzione biettiva $f : I_{n+1} \to x$. Dividiamo in casi.

(1) Se $\neg(n+1 \in x)$, allora $f_{|I_n}$ è una funzione biettiva di I_n in $f_{|I_n}(I_n)$ che in questo caso è una parte propria di I_n perché $f(n+1) \in I_n$. Assurdo. Quindi c'è $k \in I_{n+1} : f(k) = n+1$ e, inoltre, $x \setminus \{n+1\} \subset I_n$, perché $x \subset I_{n+1}$.

(2) Se $k = n+1$,
$$f' : x \in I_n \mapsto f(x) \in x \setminus \{n+1\}$$
è biettiva tra I_n e $x \setminus \{n+1\} \subset I_n$. Assurdo. Quindi

(3) C'è un $h \in I_n : f(n+1) = h$. Allora la funzione
$$g : x \in I_n \mapsto \begin{cases} f(x), & \text{se } x \in I_n \setminus \{k\} \\ h, & \text{se } x = k \end{cases} \in x \setminus \{n+1\} \subseteq I_n$$
è biettiva. Assurdo.

□

Esempio/Teorema: se a è un insieme finito di ordine n, allora $|P(a)| = 2^n$. (Dimostrare per induzione di prima forma: Se $a \neq \emptyset$, per ogni parte p di $a \setminus \{x\}$ abbiamo una parte $p \cup \{x\}$, ossia $2^{n-1} \cdot 2$).

Definizione: Se $a_1, \dots a_n$ sono insiemi, scrivo
$$\bigcup_{i=1}^{n} a_i := a_1 \cup a_2 \cup \cdots \cup a_n$$
che poi è anche $\bigcup\{a_1, \dots a_n\}$ con l'unione unaria.

Principio di inclusione-esclusione

$$\left|\bigcup_{i=1}^{n} a_i\right| = \sum_{i=1}^{n} |a_i| - \sum_{1 \le i < j \le n} |a_i \cap a_j| + \sum_{1 \le i < j < k \le n} |a_i \cap a_j \cap a_k| - \cdots + (-1)^{n-1} |a_1 \cap \cdots \cap a_n|$$

Fare esempi del Principio di inclusione-esclusione solo per: due insiemi; tre insiemi (mediante diagrmmi di Venn).

Esercizi

(1) Dimostrare la seguente formula per induzione di prima forma
$$\sum_{i=0}^{n-1} i = n(n-1)/2.$$

(2) Dimostrare per induzione di seconda forma che

$$(\forall n \in \mathbb{N})(n \geq 12 \rightarrow (\exists a, b \in \mathbb{N})(n = 4a + 5b)).$$

(Suggerimento: cominciamo notando come la formula sia vera per $n = 12, 13, 14, 15$ e partiamo da $n > 15$).

(3) Dimostrare per induzione di prima forma che $(\forall n \in \mathbb{N} \setminus \{0\})(2^{n-1} \leq n!)$

(4) Dimostrare usando il principio di induzione di prima forma che per ogni insieme finito s vale $|P(s)| = 2^{|s|}$.

(5) Verificare mediante diagrammi di Venn il Principio di inclusione-esclusione per una coppia di insiemi a e b.

(6) Siano a e b due insiemi finiti e siano $|a| = 5$ e $|b| = 9$. Possiamo trovare la cardinalità dell'unione sapendo che $|a \cap b| = 3$? Se sì, a quanto equivale? E se $|a \cup b|$ è un multiplo di 2, quanto può valere $|a \cap b|$?

(7) Siano a, b e c insiemi finiti di ordine, rispettivamente, 2, 4 e 6. Sapendo che $a \cap b = a \cap c = \emptyset$ e che $|a \cup b \cup c| = 12$, determinare $|b \cup c|$.

Lezione 2

Definizione di *fattoriale di un numero naturale*: $0! := 1$; se $n > 0$, $n! := n \cdot (n-1)!$.

Teorema 6. *Siano a e b due insiemi finiti di ordine rispettivamente m ed n. Allora*

(1) Ci sono n^m funzioni da a a b;

Dimostrazione. Induzione su $|a|$. Base: $m = 0$, cioè, come abbiamo già visto, $a = \emptyset$. Dunque l'unica funzione può essere solo $(\emptyset \times b, \emptyset)$. Se $m > 0$, sia $x \in a$. Per ipotesi di induzione, $|Map(a \setminus \{x\}, b)| = n^{m-1}$; d'altra parte, ogni funzione in $Map(a \setminus \{x\}, b)$ può essere estesa in n modi (le immagini possibili di x) e quindi $|Map(a,b)| = |Map(a \setminus \{x\}, b)| \cdot n = n^{m-1} \cdot n = n^m$. □

(2) Esistono funzioni iniettive da a a b se e solo se $m \leq n$, nel qual caso $|In(a,b)| = n!/(n-m)!$.

Dimostrazione. Siano $\alpha \in Bi(a, I_m)$ e $\beta \in Bi(b, I_n)$.

($\rightarrow$) Sia $f \in In(a,b)$. Allora $\beta \circ f \circ \alpha^{-1} \in In(I_m, I_n)$. Se fosse $n < m$, ovvero $I_n \subset I_m$, avremmo che I_m è equipotente ad una sua parte propria, ovvero $\beta \circ f \circ \alpha^{-1}(I_m)$. Assurdo.

($\rightarrow$) Sia $m \leq n$, ovvero $I_m \subseteq I_n$, per cui possiamo prendere una $g \in In(I_m, I_n)$ (ad esempio l'immersione). Allora la funzione $\beta^{-1} \circ g \circ \alpha \in In(a,b)$.

Infine, siano $m \leq n$. Completiamo la dimostrazione per induzione di prima forma su m. Se $m = 0$, allora $a = \emptyset$ e $|In(\emptyset, b)| = 1 = n!/(n-0)!$. OK. Sia $m > 0$ e prendiamo $x \in a$. Per ipotesi di induzione abbiamo che $|In(a \setminus \{x\}, b)| = n!/(n-(m-1))!$. D'altra parte, ogni funzione in $In(a \setminus \{x\}, b)$ può essere estesa, dovendo restare iniettiva, in $n-(m-1)$ modi (le immagini possibili di x che non sono ancora state prese dagli $m-1$ elementi in $a \setminus \{x\}$) e quindi $|In(a,b)| = |In(a \setminus \{x\}, b)| \cdot (n-(m-1)) = n!/(n-(m-1)) \cdot (n-(m-1)) = n!/(n-m)!$. □

(3) Esistono funzioni suriettive da a a b sse $a = b = \emptyset$ o $0 < n \leq m$

Dimostrazione. Similmente alla dimostrazione precedente, componendo con le biezioni di a e b in I_m e I_n, rispettivamente. □

(4) Esistono funzioni biettive da a a b sse $m = n$, nel qual caso $|Bi(a,b)| = n!$.

Dimostrazione. Segue da (2) e da (3), mentre l'ordine di $|Bi(a,b)|$ si ottiene direttamente da (2) con $m = n$. □

(5) In particolare,. $|Sym(a)| = m!$.

(6) Se $m = n$, $f \in In(a,b) \leftrightarrow Bi(a,b) \leftrightarrow Su(a,b)$.

Dimostrazione. Primo $\leftrightarrow$ segue dal fatto che $Bi(a,b) \subseteq In(a,b)$ e che, in questo caso, hanno lo stesso ordine per (2) e (4). Secondo $\leftrightarrow$: f è suriettiva, quindi prendo una sezione g di f, ossia una $g : b \rightarrow a$ tale che $f \circ g = id_b$. g è iniettiva perché id_b è iniettiva (vedi un teorema passato). Quindi g per il primo $\leftrightarrow$ è biettiva, allora $f = g^{-1}$, ossia f è biettiva). □

Alcune applicazioni

Definizione: Se $t \subseteq s$, dico $\chi_{t,s} : x \in s \mapsto \begin{cases} 0, & \text{se } x \notin t \\ 1, & \text{se } x \in t \end{cases} \in \{0,1\}$ la *funzione caratteristica di t in s*.

Teorema 7. *$\varphi : t \in P(s) \mapsto \chi_{t,s} \in Map(s, \{0,1\})$ è biettiva.*

Dimostrazione. Data una $f \in Map(s, \{0,1\})$ definisco $t = \{x \in s \mid f(x) = 1\}$. Controllando su t e $s \setminus t$, si vede subito che $\chi_{t,s}$ e f hanno lo stesso grafico, per cui $\chi_{t,s} = f$. Dunque φ è suriettiva.
Per l'iniettività, siano $t, u \subseteq s$ con $t \neq u$. Senza ledere di generalità, prendo $x \in t \setminus u$. Allora $\chi_{t,s}(x) = 1 \neq 0 = \chi_{u,s}(x)$. □

Corollario (Di nuovo): Se s è finito, $|P(s)| = 2^{|s|}$ (Poiché ora sappiamo che $|P(s)| = |Map(s, \{0,1\})| = |\{0,1\}|^{|s|} = 2^{|s|}$)

Coefficienti binomiali
Siano $n, k \in \mathbb{N}$. Definisco $\binom{n}{k} := |P_k(I_n)|$ il *coefficiente binomiale n su k*. (Ovvero il numero di parti con esttamente k elementi di $\{1, \ldots, n\}$)

Teorema 8. $(\forall n \in \mathbb{N})(\sum_{k=0}^{n} \binom{n}{k} = 2^n)$

Dimostrazione. Segue dal fatto che $\{P_k(I_n) \mid k \in \{0, 1, \ldots, n\}\}$ è una partizione di $P(I_n)$. □

Teorema 9. $(\forall n, k \in \mathbb{N})(k \leq n \to \binom{n}{k} = \binom{n}{n-k})$

Dimostrazione. Ricordare che la funzione $f : x \in P(I_n) \mapsto I_n \setminus x \in P(I_n)$ è biettiva. Fissando un k, abbiamo che $\overrightarrow{f}(P_k(I_n)) = P_{n-k}(I_n)$. Dunque la funzione $g : x \in P_k(I_n) \mapsto f(x) = I_n \setminus x \in P_{n-k}(I_n)$ è biettiva e quindi $\binom{n}{k} = |P_k(I_n)| = |P_{n-k}(I_n)| = \binom{n}{n-k}$. □

Teorema 10. *(Formula ricorsiva dei coefficienti binomiali)* $(\forall n, k \in \mathbb{N})(k \leq n \to \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1})$

Dimostrazione. Prendo $1 \in I_{n+1}$. Definisco $a = \{x \in P_{k+1}(I_{n+1}) \mid n+1 \notin x\}$ e $b = \{x \in P_{k+1}(I_{n+1}) \mid n+1 \in x\}$. Ovviamente $\{a, b\}$ è una partizione di $P_{k+1}(I_{n+1})$. Quindi $|P_{k+1}(I_{n+1})| = |a| + |b|$. Ma $a = P_{k+1}(I_n)$ (perché nessun suo elemento contiene $n+1$) e $|b| = |P_k(I_n)|$, da cui la tesi. □

Visualizzazione mediante Triangolo di Tartaglia-Pascal prima con coefficienti binomiali e poi con i numeri naturali. Rivedere la formula ricorsiva: ogni coefficiente del triangolo è somma dei due coefficienti subito sopra di lui.

Teorema 11. $(\forall n, k \in \mathbb{N})(k \leq n \to \binom{n}{k} = \frac{n!}{k!(n-k)!})$

Dimostrazione. Dimostriamo la tesi usando l'induzione di seconda forma sull'insieme dei coefficienti binomiali ordinato con ordine lessicografico (formalmente, intendendo i coefficienti binomiali come coppie di numeri interi, prendo l'insieme delle coppie $\{(n,k) \in \mathbb{N} \times \mathbb{N} \mid k \leq n\}$ e lo ordino con l'ordine lessicografico, ovvero $(a,b) \leq (c,d) \longleftrightarrow (a < c \vee (a = c \wedge b \leq d))$. Esempio: $(0,0) < (0,1) < (1,0) < (1,1) < (2,0) < (2,1) < \ldots$). Dunque, per $n = k = 0$, ovvio. Allora prendo $(0,0) < (n,k)$ e suppongo vero per le coppie $< (n,k)$. Allora

$$\begin{aligned}
\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(n-k)!\,(k-1)!} + \frac{(n-1)!}{(n-1-k)!k!} \\
&= \frac{(n-1)!k}{(n-k)!k!} + \frac{(n-1)!\,(n-k)}{(n-k)!k!} \\
&= \frac{(n-1)!}{(n-k)!k!}\,(k+n-k) \\
&= \frac{n!}{(n-k)!k!}
\end{aligned}$$

□

Cenno al Teorema Binomiale (o formula di Newton): Se $(s, +, \cdot)$ è un anello unitario e $ab = ba$, allora

$$(a+b)^n = \binom{n}{0}a^n b^0 + \binom{n}{1}a^{n-1}b^1 + \cdots + \binom{n}{n-1}a^1 b^{n-1} + \binom{n}{n}a^0 b^n$$

Esercizi

(1) Siano a b e c insiemi tali che $|a| = 2$, $|b| = 4$ e $|c| = 6$. Quante sono le applicazioni iniettive da c ad a?

(2) Quante sono le applicazioni costanti da un insieme di ordine 100 ad uno di ordine 1004?

(3) Rappresentare la funzione caratteristica dell'insieme $\{0, 4\}$ nell'insieme $\{n \in \mathbb{N} \mid n^2 \leq 20\}$

(4) Sia $f : n \in \mathbb{N} \mapsto ((-1)^{n+1} + 1)/2 \in \{0, 1\}$. Di quale sottoinsieme di $\mathbb{N}$ è funzione caratteristica f?

(5) Scrivere esplicitamente la funzione caratteristica in $\mathbb{N}$ del sottoinsieme $\{n \in \mathbb{N} \mid 3|n\}$.

(6) Calcolare $\binom{7}{3}$ usando il triangolo di Tartaglia-Pascal e $\binom{7}{4}$ senza usarlo.

(7) Sia $a = \{n \in \mathbb{N} \mid n \leq 9\}$

- Qual è la cardinalità di $P_{11}(a)$?
- Qual è la cardinalità di $P_{10}(a)$?
- Quante sono le 3-parti di a?
- Qual è la cardinalità di $P_7(a)$?
- Quanti sono i sottoinsiemi di a che contengono 0 e altri tre elementi distinti di a?

(8) Dimostrare per induzione che la somma dei primi n numeri naturali è uguale a $\binom{n}{2}$.

(9) (Teorema binomiale o Formula di Newton) Sia s è un anello unitario e $a, b \in s$ tali che $ab = ba$. Dimostrare per induzione (prima forma) che

$$(a+b)^n = \binom{n}{0}a^n b^0 + \binom{n}{1}a^{n-1}b^1 + \cdots + \binom{n}{n-1}a^1 b^{n-1} + \binom{n}{n}a^0 b^n$$

Lezione 3

Aritmetica

Sia s $\mathbb{N}$ o $\mathbb{Z}$.
Definizioni

- Divide $(\forall x, y \in s)(x|y :\longleftrightarrow (\exists k \in s)(y = xk))$ (in $\mathbb{N}$ è una relazione d'ordine).
- $x \in s$. Dico $Div_{(s,\cdot)}(x) = \{y \in s \,|\, y|x\}$. $Mult_{(s,\cdot)}(x) = \{y \in s \,|\, x|y\}$. (Ometteremo il pedice quando non è ambiguo!)
- $MCD_{(s,\cdot)}(x, y) = \{d \in Div(x) \cap Div(y) \,|\, (\forall z \in Div(x) \cap Div(y))(z|d)\}$
- $mcm_{(s,\cdot)}(x, y) = \{d \in Mult(x) \cap Mult(y) \,|\, (\forall z \in Mult(x) \cap Mult(y))(d|z)\}$
- Sia $n \in \mathbb{Z}$. $-n, -1, 1, n$ vengono detti *divisori banali* di n.
- Se $n \in \mathbb{Z}$, il *valore assoluto* di n è $|n| := max(\{n, -n\})$.

Teorema 12. *Teorema divisione euclidea (o divisione con resto).*

$$(\forall m, n \in \mathbb{Z})(m \neq 0 \to (\exists!(q, r) \in \mathbb{Z} \times \mathbb{N})(n = mq + r \wedge 0 \leq r < |m|)$$

Dimostrazione. (Esistenza) Suppongo $n \geq 0$. Induzione II. $n = 0$ ovvio. Allora suppongo $0 < n$. Se $n < |m|$, $q = 0$ e $r = n$. Sia allora $n \geq |m|$. = ok. Allora $0 \leq n - |m| < n$ e per ipotesi di induzione esistono q_1, r_1: $n - |m| = mq_1 + r_1$ con $0 \leq r_1 < |m|$. Cioè

$$n = |m| + mq_1 + r_1$$

Distinguo $m > 0$ o $m < 0$ e sceglo q di conseguenza mettendo in evidenza m.
Suppongo $-n > 0$. Per prima trovo q', r': $-n = mq' + r'$ con $0 \leq r_1 < |m|$. Se $r' = 0$, pongo $q = -q'$. Sia $r > 0$. Allora

$$n = -mq' - |m| + |m| - r' = m(q' \pm 1) + (|m| - r')$$

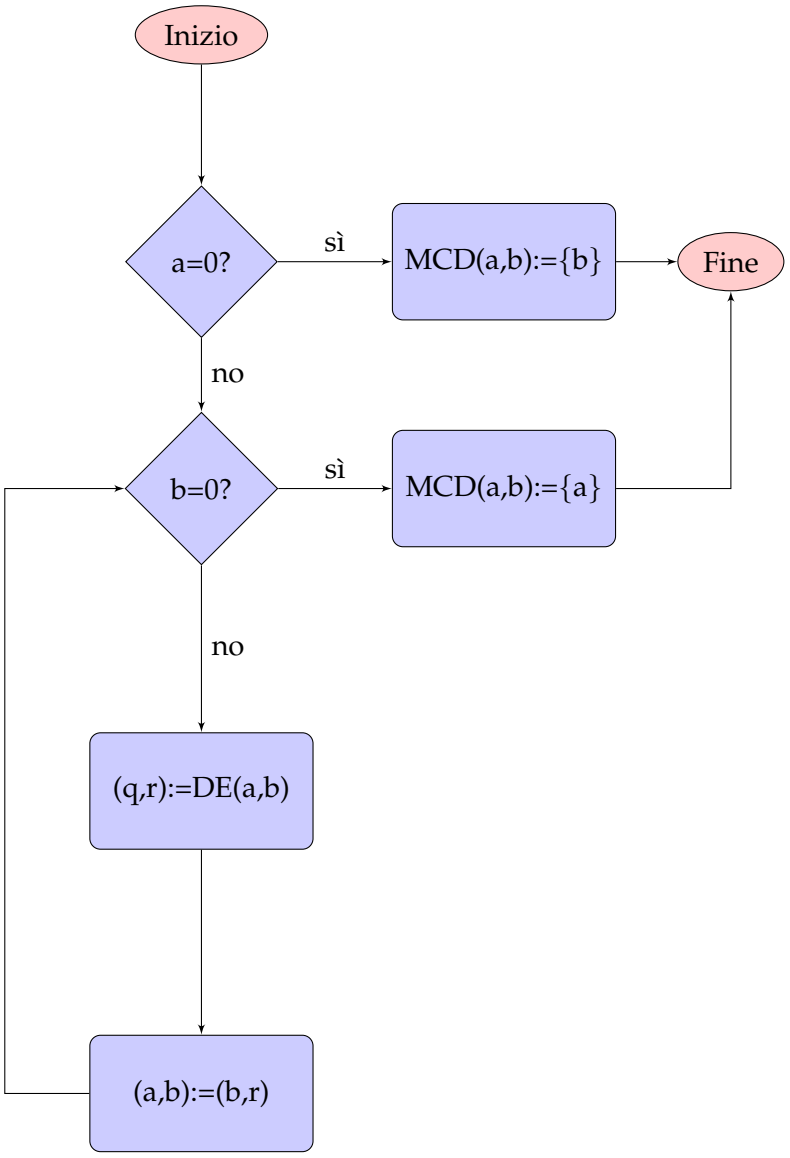
Distinguo $m > 0$ o $m < 0$ e sceglo q (mettendo in evidenza m) ed r di conseguenza.
(Unicità) Siano $q_1, q_2, r_1, r_2 : n = mq_1 + r_1$, $n = mq_2 + r_2$ e $0 \leq r_1 < |m|$, $0 \leq r_2 < |m|$.Dunque $m(q_1 - q_2) = r_2 - r_1$ e quindi

$$|m||q_1 - q_2| = |r_2 - r_1| < |m|.$$

Poiché $m \neq 0$, $|m| \neq 0$, ovvero è cancellabile in $(\mathbb{Z}, \cdot)$. Segue che $|q_1 - q_2| < 1$, dunque $|q_1 - q_2| = 0$, cioè $q_1 = q_2$, quindi anche $r_1 = r_2$. □

Algoritmo delle divisioni successive (o Algoritmo di Euclide)

Dati $a, b \in \mathbb{Z}$ non entrambi nulli (che insieme è MCD(0,0)?), voglio trovare $MCD_{(\mathbb{Z},\cdot)}(a, b)$. Poiché sappiamo che $MCD_{(\mathbb{Z},\cdot)}(a, b) = \{MCD_{(\mathbb{N},\cdot)}(a, b), -MCD_{(\mathbb{N},\cdot)}(a, b)\}$, possiamo cercarlo solo in $\mathbb{N}$. Dunque suppongo $m, n \in \mathbb{N}$. Dico $DE(x, y) = (q, r)$ della divisione euclidea.



Poiché i resti della divisione euclidea sono strettamente decrescenti e sempre maggiori o uguali a 0, l'algoritmo ha termine, ovvero, ponendo $b = r_0$, esiste un $t \in \mathbb{N} \setminus \{0\}$ tale che $r_{t-1} \neq 0$ e $r_t = 0$. Ovvero

$$\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
r_2 &= r_3 q_4 + r_4 \\
&\vdots \\
r_i &= r_{i+1} q_{i+2} + r_{i+2} \\
&\vdots \\
r_{t-4} &= r_{t-3} q_{t-2} + r_{t-2} \\
r_{t-3} &= r_{t-2} q_{t-1} + r_{t-1} \\
r_{t-2} &= r_{t-1} q_t + 0
\end{aligned}$$

Pongo $d = r_{t-1}$ e vedo che divide tutti i resti e che quindi è un divisore comune di a e b. Prendo poi un divisore comune di a e b e noto che divide tutti i resti, tra cui anche d.
Esempio: 111 e 17.

(1) DE(111,17)=(6,9).

(2) DE(17,9)=(1,8).

(3) DE(9,8)=(1,1).

(4) DE(8,1)=(8,0).

(5) (a,b)=(1,0). Dunque $1 \in MCD(111, 17)$.

Esempio: 1111231 e 111123.

(1) DE(1111231,111123)=(10,1).

(2) DE(111123,1)=(111123,0).

(5) (a,b)=(1,0). Dunque $1 \in MCD(1111231, 111123)$.

Teorema 13. *(Teorema di Bézout)* $(\forall (a,b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0,0)\})((\forall d \in MCD(a,b))((\exists u, v \in \mathbb{Z})(d = au + bv))))$

Dimostrazione. Parto dall'algoritmo euclideo e lo estendo. Voglio provare qualcosa in più: ogni resto si scrive come combinazione di a e di b. Sia k il minimo controesempio in $\mathbb{N}$ tra tutti i pedici i dei resti r_i che (per assurdo) non si possono scrivere come $au + bv$ per qualche $u, v \in \mathbb{Z}$. Sia $r_0 = b$. Certo $r_0 = a0 + b \cdot 1$ e $r_1 = a \cdot 1 + b(-q_1)$, quindi $k > 1$. Poiché k è il minimo controesempio, la tesi è vera per tutti i pedici naturali minori di k, ossia vale che per ogni $i \in \{1, \dots, k-1\}$ trovo $u_i, v_i \in \mathbb{Z}$ tali che $r_i = au_i + bv_i$. Allora

$$r_k = r_{k-2} - r_{k-1}q_k = au_{k-2} + bv_{k-2} - (au_{k-1} + bv_{k-1})q_k = a(u_{k-2} - u_{k-1}) + b(v_{k-2} - v_{k-1}).$$

Assurdo. □

Esercizi

(1) Calcolare il numero dei divisori positivi di 2, di 8 e di 60. Calcolare il numero dei divisori interi degli stessi numeri.

(2) Trovare, mediante il Teorema della divisione euclidea, coefficienti e resti delle seguenti coppie di numeri: $(10, 5)$, $(21, 4)$, $(-21, 4)$, $(11, 2)$, $(-11, 2)$.

(3) Trovare, se possibile, $MCD(0, 0)$ e $mcm(0, 0)$.

(4) Utilizzare l'algoritmo delle divisioni successive per trovare, in $\mathbb{Z}$, $MCD(72, 402)$, $MCD(141, 39)$, $MCD(182, 104)$, $MCD(1111231, 111123)$.

(5) Per ogni coppia (a, b) di numeri dell'esercizio precedente scegliere un $d \in MCD(a, b)$ ed utilizzare la dimostrazione del Teorema di Bézout per trovare due interi u e v tali che $d = au + bv$. [Si tratta del cosiddetto "Algoritmo delle divisioni successive esteso"]

(6) Esiste un numero u tale che $2u - 1$ è multiplo di 3? Trovarlo.

(7) Esiste un numero u tale che $79u - 1$ è multiplo di 23?

Lezione 4

Un corollario al Teorema di Bézout.

Teorema 14. *(Lemma di Euclide) Per ogni $a, b, c \in \mathbb{Z}$, se a e b sono coprimi e $a|bc$, allora $a|c$.*

Dimostrazione. Per ipotesi $(\exists h \in \mathbb{Z})(ah = bc)$ e $1 \in MCD(a, b)$. Per Bézout esistono u, v tali che $1 = au + bv$. Allora $c = acu + bcv = acu + ahv$ e quindi $a|c$. □

Definizione: $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ si dice *primo* se $(\forall a, b \in \mathbb{Z})(p|ab \to p|a \vee p|b)$

Teorema 15. *Un $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ è primo se e solo se possiede solo i divisori banali e non è invertibile (ovvero è irriducibile).*

Dimostrazione. ($\to$) Sia a un divisore di p e scriviamo $p = ab$. Allora, per ipotesi, $p|a \vee p|b$. Suppongo senza ledere di generalità $p|a$. Allora trovo k tale che $a = pk$. Dunque $p = pkb$ e $kb = 1$. Poiché gli invertibili di $\mathbb{Z}$ sono -1 e 1, segue che $b = \pm 1$ e $aa = \pm p$. Dunque p ha solo i divisori banali.
($\leftarrow$) Sia p diviso soltanto dai suoi divisori banali. Suppongo $p|ab$ ossia $(\exists h \in \mathbb{Z})(ab = ph)$. Voglio $p|a \vee p|b$, allora suppongo $\neg(p|a)$. Dunque p e a sono coprimi e quindi $p|b$ per il Lemma di Euclide. Dunque p è primo. □

Possiamo ora dimostrare il Teorema fondamentale dell'aritmetica, che è anche un'interessante applicazione di entrambi i principi di induzione.

Teorema 16. *(Teorema fondamentale dell'aritmetica) Sia $m \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Allora esistono $p_1, \dots, p_r$ primi tali che $m = p_1 \dots p_r$. Inoltre, se $m = q_1 \dots q_s$, $r = s$ ed esiste una funzione biettiva σ di $\{1, \dots, r\}$ tale che, per ogni $i \in \{1, \dots, r\}$, $p_i = \pm q_{\sigma(i)}$.*

Dimostrazione. (Esistenza della decomposoizione) Supponiamo prima $m \in \mathbb{N}$. 2 è primo: (perché $|$ è d'ordine su $\mathbb{N}$ e 2 è minimale o anche perché se a e b sono dispari lo è anche ab). Procediamo per induzione di seconda forma su m. Se $m = 2$ OK. Sia $m > 2$ e supponiamo vera la tesi per tutti i k tali che $2 \leq k < m$. Se m è primo, ovvio. Sia allora m non primo. Per il teorema precedente m ha divisori non banali. Sia $a \in \mathbb{N} \setminus \{1, m\}$ tale che $m = ab$ per un certo $b \in \mathbb{N}$. Segue che anche b non è un divisore banale, altrimenti lo sarebbe anche a. Ma allora $1 < a, b < m$ e per a e b vale l'ipotesi di induzione, per cui sono primi o prodotto di primi. Quindi lo stesso vale per m e per il principio di induzione di seconda forma la tesi vale per ogni $m > 1$.
Se $m < 1$, allora la tesi vale per $-m$, cioè esistono $p_1, \dots, p_r$ primi tali che $-m = p_1 \dots p_r$. Quindi $m = (-p_1) \dots p_r$ e segue la tesi anche per i negativi.

(Essenziale unicità) Siano $p_1 \cdots p_r = m = q_1 \cdots q_s$ due decomposizioni di m. Procediamo per induzione di prima forma su r. Se $r = 1$, abbiamo $p_1 = m = q_1 \cdots q_s$. Ma p_1 è primo quindi divide, senza ledere di generalità, q_1. Ma anche q_1 è primo, per cui possiede solo i divisori banali, per cui $q_1 = \pm p_1$. Cancellandoli, segue che $\pm 1 = q_2 \cdots q_s$, per cui $s = 1$, perché nessun primo può dividere 1. Sia $r > 1$ e supponiamo l'asserto vero per $r - 1$. Come prima, possiamo assumere che $q_1 = \pm p_1$ e quindi $p_1 \cdots p_r = m = \pm(p_1) q_2 \cdots q_s$. Da ciò segue che $p_2 \cdots p_r = m = \pm q_2 \cdots q_s$. Dall'ipotesidi induzione segue allora $r - 1 = s - 1$ (da cui ovviamente $r = s$) ed esiste $\tau : \{2, \dots, r\} \to \{2, \dots, r\}$: $p_i = \pm q_{\tau(i)}$ per $i \in \{2, \dots, r\}$. Allora definiamo $\sigma : \{1, \dots, r\} \to \{1, \dots, r\}$ tale che $\sigma(1) = 1$ e $\sigma(i) = \tau(i)$ se $i \in \{2, \dots, r\}$. Dunque σ è la funzione che cercavamo e abbiamo la tesi. □

Esercizi

(1) Trovare $a, b, c \in \mathbb{Z}$ per cui non valga il Lemma di Euclide.

(2) Quante scomposizioni in fattori primi ha il numero 12? Descrivere esplicitamente una permutazione degli indici di due sue diverse scomposizioni.

(3) Quante scomposizioni in fattori primi ha il numero 31?

(4) Quali sono i divisori banali di 31 in $\mathbb{Q}$?

Lezione 5

Congruenze modulo m

Sia $m \in \mathbb{Z}$. Sia $\equiv_m$ la relazione binaria su $\mathbb{Z}$ definita da $(\forall m, n \in \mathbb{Z})(a \equiv_m b \iff m|(b-a))$. Si vede facilmente che è di equivalenza. Questa relazione si chiama *congruenza modulo m*.
Esempi: $\equiv_0$ è la relazione di uguaglianza, $\equiv_1$ è la relazione totale; due interi sono in relazione $\equiv_2$ se e solo se sono entrambi pari o entrambi dispari. Ovviamente $\equiv_m = \equiv_{-m}$

Definizioni:

- Se $m \in \mathbb{Z}$, $\mathbb{Z}_m := \mathbb{Z}/\equiv_m$.
- Se $a, m \in \mathbb{Z}$, $a + m\mathbb{Z} := [a]_m := [a]_{\equiv_m}$.

Esplicitamente, $[a]_m = \{a + mk \mid k \in \mathbb{Z}\}$.
-Operazione (parziale) mod (o %): se $(\forall (a, m) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})(a \mathrm{mod} m = min([a]_m \cap \mathbb{N}))$.
$a \mathrm{mod} m$ sempre $< |m|$. È proprio il resto della divisione euclidea. A volte si scrive anche $\mathrm{rest}(a, m)$ o anche $a\%m$.

Descrizione esplicita di $\mathbb{Z}_m$:

Teorema 17. *Sia $m \in \mathbb{Z} \setminus \{0\}$. Allora $\mathbb{Z}_m = \{[0]_{|m|}, [1]_{|m|}, \ldots, [|m|-1]_{|m|}\}$. In particolare, $|\mathbb{Z}_m| = m$.*

Dimostrazione. Suppongo $m > 0$, tanto $\equiv_m = \equiv_{-m}$. Sia a un qualunque intero e siano $(q, r) = DE(a, m)$. Allora $a = mq + r$, cioè $a \equiv_m r$. Quindi $[a]_m = [r]_m$. Dunque i numeri si ripartiscono nelle classi che hanno per rappresentanti i resti. Dimostriamo che sono distinte. Siano $0 \leq i \leq j \leq m-1$ tali che $[i]_m = [j]_m$. Allora $0 \leq j - i \leq j < m$, ma $m|(j-i)$ e quindi $i = j$. □

Vogliamo ora mettere delle operazioni su $\mathbb{Z}_m$.
In generale. Sia $s \neq \emptyset$ e $*$ un'operazione binaria interna su s. Una relazione di equivalenza $\sim$ su s si dice *compatibile a sinistra* con $*$ se $(\forall a, b, c \in s)(a \sim b \to c * a \sim c * b)$. Rispettivamente *a destra*.
Sia $s \neq \emptyset$ e siano $*_1, \ldots, *_n$ n operazioni binarie interne su s. Una relazione di equivalenza $\sim$ su s si dice una *congruenza in* $(s, *_1, \ldots, *_n)$ se $(\forall a, b, c, d \in s)((\forall i \in \{1, \ldots, n\})((a \sim b \wedge c \sim d) \to a *_i c \sim b *_i d))$.
Sia $(s, *_1, \ldots, *_n)$ e sia $\sim$ congruenza. Allora è possibile definire, per ogni $i \in \{1, \ldots, n\}$,

$$(*_i)_\sim : ([x]_\sim, [y]_\sim) \in s/\sim \times s/\sim \mapsto [x *_i y]_\sim \in s/\sim.$$

La funzione $\pi : x \in s \mapsto [x]_\sim \in s/\sim$, ovvero quella che ad ogni elemento di s associa la sua classe di equivalenza modulo $\sim$, si chiama *epimorfismo canonico di* $(s, *_1, \ldots, *_n)$ *su* $(s/\sim, (*_1)_\sim, \ldots, (*_n)_\sim)$. Si verifica immediatamente che π è un omomorfismo. Dunque $(s/\sim, (*_1)_\sim, \ldots, (*_n)_\sim)$ eredita associatività, commutatività, elementi neutri, simmetrici e distributività. In particolare, quozienti di semigruppi, monoidi, gruppi (eventualmente abeliani), anelli (eventualmente commutativi o unitari) sono strutture dello stesso tipo.

Teorema 18. *Sia $s \neq \emptyset$, siano $*_1, \ldots, *_n$ n operazioni binarie interne su s e sia $\sim$ una relazione di equivalenza su s. Allora $\sim$ è una congruenza in $(s, *_1, \ldots, *_n)$ se e solo se è compatibile a destra e a sinistra con ogni operazione di $(s, *_1, \ldots, *_n)$.*

Dimostrazione. Possiamo supporre una sola operazione *. ($\to$) Prendo nella definizione $c \sim c$ e $a \sim b$. ($\leftarrow$) Prendo a, b, c, d ed assumo $a \sim b \wedge c \sim d$. Compatibilità a destra: allora $a * c \sim b * c$. Compatibilità a sinistra: allora $b * c \sim b * d$. Infine, per transitività, $a * c \sim b * d$. □

Si dimostra facilmente che, per ogni $m \in \mathbb{Z}$, $\equiv_m$ è una congruenza in $(\mathbb{Z}, +, \cdot)$. Dunque, possiamo costruire gli anelli quoziente di $(\mathbb{Z}, +, \cdot)$, ovvero gli $(\mathbb{Z}_m, +, \cdot)$ dove, con abuso di notazione, $+$ e $\cdot$ sono le operazioni indotte dall'epimorfismo canonico di $\mathbb{Z}$ su $\mathbb{Z}_m$.

La struttura degli anelli quoziente di $(\mathbb{Z}, +, \cdot)$:

Teorema 19. *Se $m \in \mathbb{Z} \setminus \{0\}$, sono equivalenti:*

(1) $\mathbb{Z}_m$ è un campo;

(2) $\mathbb{Z}_m$ è un dominio di integrità;

(3) m è primo.

Dimostrazione. (1)→(2) è ovvio. (2)→(3) Notiamo in primo luogo che in un dominio di integrità ci sono almeno due elementi distinti, per cui $m > 1$. Sia $m = ab$. Allora $[a]_m[b]_m = [0]_m$. Ma $(Z_m, +, \cdot)$ è integro, ossia $[a]_m = [0]_m \vee [b]_m = [0]_m$, ovvero m divide o a o b, ovvero m è primo.
(3)→(1) Ricordiamo che se m è primo ha solo i divisori banali. Allora se prendo un n naturale tale che $1 \leq n < m$, $MCD(n, m) = \{-1, 1\}$ ossia, per il Teorema di Bézout, esistono gli interi u, v tali che $1 = nu + mv$, cioè $[n]_m[u]_m = [1]_m$ ed ogni elemento non nullo è invertibile. □

Esercizi

(1) Elencare tutti gli elementi dell'insieme $[41]_5 \cap \{n \in \mathbb{Z} \mid n^2 \leq 20\}$.

(2) Definire un'operazione binaria interna $\overline{+}$ a $\mathbb{Z}_0$ tale che sia possibile costruire un'isomorfismo tra $(\mathbb{Z}_0, \overline{+})$ e $(\mathbb{Z}, +)$.

(3) Calcolare 101mod10, $101\%(-1)$ e 30093mod3.

(4) Verificare se $\mathbb{Z}_3 = \{[30]_3, [2]_3, [11]_3, [-8]_3\}$.

(5) Verificare se $\mathbb{Z}_5 = \{[30]_5, [2]_5, [11]_5, [-8]_5, [3]_5\}$.

(6) Calcolare 484289374098279340!mod3879374.

(7) Sia $*$ l'operazione binaria di $\mathbb{Z}$ definita da $(\forall a, b \in \mathbb{Z})((2 \not| b \to a * b = a + b) \wedge (2|b \to a * b = a + b/2))$. Dimostrare che $\equiv_2$ non è una congruenza rispetto a $*$.

(8) Sia $*$ l'operazione binaria di $\mathbb{Z}$ definita da $(\forall a, b \in \mathbb{Z})(a * b = 2ab)$. Dimostrare che $\equiv_2$ è una congruenza rispetto a $*$.

(9) Sia $*$ l'operazione binaria di $\mathbb{Z} \times \mathbb{Z}$ definita da $(\forall a, b, c, d \in \mathbb{Z})((a, b) * (c, d) = (a + b, c + d))$ e sia $\sim$ una relazione di equivalenza su $\mathbb{Z} \times \mathbb{Z}$ definita da $(\forall a, b, c, d \in \mathbb{Z})((a, b) \sim (c, d) \leftrightarrow (2|ab - cd))$. Dimostrare che $\sim$ è una relazione di equivalenza che non è una congruenza rispetto a $*$.

(10) La relazione di equivalenza $\sim$ in $P(\mathbb{Z})$ definita da $(\forall x, y \in P(\mathbb{Z})(x \sim y \leftrightarrow x \cap \mathbb{N} = y \cap \mathbb{N}))$ è una congruenza in $(P(\mathbb{N}, \cap, \cup)$? E quella definita da $(\forall x, y \in P(\mathbb{Z})(x \sim y \leftrightarrow x \cup \mathbb{N} = y \cup \mathbb{N}))$?

(11) Elencare i divisori dello zero e gli invertibili dei seguenti anelli: $(\mathbb{Z}_4, +, \cdot)$, $(\mathbb{Z}_8, +, \cdot)$ e $(\mathbb{Z}_9, +, \cdot)$.

Lezione 6

Equazioni diofantee

Siano $a, b, c \in \mathbb{Z}$ e sia $ed[a,b,c] : (m,n) \in \mathbb{Z} \times \mathbb{Z} \mapsto am + bn - c \in \mathbb{Z}$. $ed[a,b,c]$ si dice *equazione diofantea* di primo grado con due incognite di termini a, b, c. Per essere sintetici sarà scritta come

$$ax + by = c$$

Una coppia di interi m, n si dice *soluzione* dell'equazione diofantea se $ed[a,b,c](m,n) = 0$, ovvero se $am + bn = c$.

Teorema 20. *Siano $a, b \in \mathbb{Z} \setminus \{0\}$ e $d \in MCD(a,b)$. Le seguenti sono equivalenti:*

(1) Il Teorema di Bézout;

(2) a e b sono coprimi se e solo se esistono u, v tali che $1 = au + bv$;

(3) in $(\mathbb{Z}, +)$, $\langle a, b \rangle = d\mathbb{Z}$;

(4) l'equazione diofantea $ax + by = c$ ammette soluzioni se e solo se $d|c$.

Dimostrazione. (1)→(2) (→) Segue subito dal Teorema di Bézout prendendo $d = 1$. (←) Se m è un divisore comune ad a e a b, allora m divide anche $au + bv = 1$. Quindi a e b sono coprimi.
(2)→(3) ($\subseteq$) Certo $a, b \in d\mathbb{Z}$, per cui il sottogruppo $\langle a, b \rangle$ di $(\mathbb{Z}, +)$ generato da a e b è contenuto in $d\mathbb{Z}$. ($\supseteq$) Scrivo $a = a_1 d$ e $b = b_1 d$. Se ci fosse un divisore comune a a_1 e b_1, d non sarebbe in $MCD(a,b)$, allora a_1 e b_1 sono coprimi e trovo u, v: $1 = a_1 u + b_1 v$. Da ciò $d = au + bv$. Dunque $d \in \langle a, b \rangle$, ossia $d\mathbb{Z} \subseteq \langle a, b \rangle$.
(3)→(4) (→) Per ipotesi, esistono u, v: $au + bv = c$, quindi $c \in \langle a, b \rangle$. Per (3), $c \in d\mathbb{Z}$, ossia $d|c$. (←) $d|c$, quindi $c \in d\mathbb{Z} = \langle a, b \rangle$, allora esistono u, v: $au + bv = c$
(4)→(1) Ovvio con $d = c$. □

Teorema 21. *Sia $ax + by = c$ un'equazione diofantea con soluzione (x_0, y_0) e sia $d \in MCD(a,b)$. Allora $\{(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k) \mid k \in \mathbb{Z}\}$ è l'insieme delle soluzioni.*

Dimostrazione. Che gli elementi di quell'insieme siano soluzioni è immediato, per sostituzione. Sia d'altronde (x, y) una soluzione generica dell'equazione. Dunque $ax + by = c = ax_0 + by_0$. Divido per d e ottengo che $\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$. Ma a/d e b/d sono coprimi, dunque, per il Lemma di Euclide, dividono $(x - x_0)$ e $(y - y_0)$, rispettivamente, cioè

$$(\exists h, k \in \mathbb{Z}) \begin{cases} h\frac{a}{d} = y_0 - y \\ k\frac{b}{d} = x - x_0 \end{cases}$$

Sostituendo in $\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$ otteniamo $h = k$ e quindi la tesi. □

Equazioni congruenziali

Sia $m \neq 0$ e siano $a, b \in \mathbb{Z}$ e sia $ec[a,b,m] : [n] \in \mathbb{Z}_m \mapsto [an - b]_m \in \mathbb{Z}_m$. $ec[a,b,m]$ si dice *equazione congruenziale* di primo grado in una incognita di termini a, b e modulo m. Per essere sintetici sarà scritta come

$$ax \equiv_m b$$

Un intero n si dice *soluzione* dell'equazione congruenziale se $ec[a,b,m]([n]) = [0]_m$, ovvero se $an \equiv_m b$.
Note:

- Se n è soluzione, le soluzioni sono tutti e soli gli elementi di $[n]_m$.
- $4x \equiv_2 3$ è un esempio di equazione congruenziale senza soluzioni.

- L'equazione congruenziale $ax \equiv_m b$ ha soluzioni se e solo se l'equazione diofantea $ax + my = b$ ha soluzioni.

Da quest'ultima osservazione, ricaviamo il seguente

Teorema 22. *Siano $a, b \in \mathbb{Z}$, $m \in \mathbb{Z} \setminus \{0\}$ e $d \in MCD(a, m)$. $ax \equiv_m b$ ha soluzioni se e solo se $d|b$*

Il seguente corollario ha dimostrazione immediata.

Corollario 23. *Sia $m \in \mathbb{Z} \setminus \{0\}$. $[a]_m$ è invertibile in $(\mathbb{Z}_m, +, \cdot)$ se e solo se a e m sono coprimi.*

Corollario 24. *Sia $m \in \mathbb{Z} \setminus \{0\}$. $[a]_m$ è invertibile se e solo se non è divisore dello zero nell'anello $(\mathbb{Z}_m, +, \cdot)$.*

Dimostrazione. ($\rightarrow$) Per assurdo, se è $[a]_m$ è un divisore dello zero c'è $[b]_m \neq [0]_m$ tale che $[ab]_m = [0]_m$, ma $[a]_m$ è invertibile e dunque, moltiplicando ambo i lati per il suo inverso, otteniamo $[b]_m = [0]_m$. ($\leftarrow$) Sia $[a]_m$ non invertibile. Allora a e m non sono coprimi, quindi prendo $1 \neq d \in MCD(a, m)$ e scrivo $a = a'd$. Quindi $[m/d]_m \neq [0]_m$ e $[a]_m[m/d]_m = [a(m/d)]_m = [a'm]_m = [0]_m$. Dunque $[a]_m$ è un divisore dello zero. □

Risoluzione e semplificazione di equazioni congruenziali
Siano $a, b \in \mathbb{Z}$, $m \in \mathbb{Z} \setminus \{0\}$ e diciamo e l'equazione congruenziale $ax \equiv_m b$. Vogliamo trovare le soluzioni.

- Se $a' \in [a]_m$ e $b' \in [b]_m$, l'equazione $a'x \equiv_m b'$ ha lo stesso insieme di soluzioni di e, dunque scegliamo $a' = a\%m$ e $b' = b\%m$.

  Esempio: $100x \equiv_{11} 2$ e $1x \equiv_{11} 2$.

- Per ogni $k \in \mathbb{Z} \setminus \{0\}$, l'equazione $akx \equiv_{mk} bk$ ha lo stesso insieme di soluzioni di e.

  Esempio: $-4x \equiv_3 -1$ $4x \equiv_3 1$

- Se esiste $k \in \mathbb{Z}$ tale che $a = a'k$, $b = b'k$ e $m = m'k$, l'equazione $a'x \equiv_{m'} b'$ ha lo stesso insieme di soluzioni di e.

  Esempio: $2x \equiv_6 4$ e $x \equiv_3 2$.

- Per ogni l coprimo con m, l'equazione $alx \equiv_m bl$ ha lo stesso insieme di soluzioni di e. (Questo succede perché $[l]_m$ è invertibile e quindi $[alx]_m = [bl]_m \leftrightarrow [ax]_m = [b]_m$).

  Esempio: $5x \equiv_{19} 3$ e $4 \cdot 5x \equiv_{19} 4 \cdot 3$ (che è a sua volta equivalente a $x \equiv_{19} 11$).

Dunque, per trovare le soluzioni, bisogna:

(1) Ridurre a e b a numeri tra 0 e $m - 1$.

(2) Prendere un $d \in MCD(a, m)$. Se $d \not| b$, non abbiamo soluzioni. Se $d|b$, andiamo avanti.

(3) $d|b$, quindi scrivere $a = a'd$, $b = b'd$ e $m = m'd$ e considerare l'equazione $a'x \equiv_{m'} b'$.

(4) Trovare l'inverso di $[a']_{m'}$ con l'algoritmo delle divisioni successive esteso. Lo chiamo $[l]_{m'}$

(5) La soluzione è $[b'l]_{m'}$. (Dunque è sempre una classe di resto modulo m/d)

Esercizi

(1) Trovare elementi invertibili, cancellabili e divisori dello zero di $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_{10}$, $\mathbb{Z}_{12}$. Degli elementi invertibili, scrivere esplicitamente gli inversi. Quali dei precedenti anelli sono campi e quali no?

(2) Descrivere l'insieme delle soluzioni delle seguenti equazioni diofantee:

- $2x + 3y = 7$;
- $-4x - 6y = -14$;
- $2x + 4y = 5$.

(3) Descrivere l'insieme delle soluzioni delle seguenti equazioni congruenziali:

- $12x \equiv_7 3$;
- $12x \equiv_9 3$;
- $12x \equiv_9 9$;
- $12000x \equiv_{60} 120$;
- $-101 \equiv_{505} 404$

(4) Esiste una coppia di numeri interi u, v tali che $41u + 29v = 19$?

(5) Sia $g = \langle x \rangle$ un gruppo ciclico di ordine 19. Esiste una potenza di x^5 che sia uguale ad x? Qual è l'ordine del sottogruppo $\langle x^5 \rangle$?

(6) Se ora sono le 5 del pomeriggio, che ore saranno tra $12001 + 47^{202}(5^{36} - 15 \cdot 64)$ ore?

Lezione 7

Polinomi

Sia A un anello commutativo unitario. Dico $0 := 0_A$, ovvero l'elemento neutro di $(A, +)$.
Definizioni varie.

- Una funzione da $\mathbb{N}$ ad A viene detta *successione*, più brevemente $(a_n)_{n\in\mathbb{N}}$ intendendo che $(\forall n \in \mathbb{N})(f(n) = a_n)$.
- Dico $(a_n)_{n\in\mathbb{N}}$ un *polinomio a coefficienti in A* se $(\exists k \in \mathbb{N})((\forall n \geq k)(a_n = 0))$.
- gli a_i si dicono *coefficienti* di f.
- Dico $A[x]$ *l'insieme dei polinomi a coefficienti in A*.
- $f : n \in \mathbb{N} \mapsto 0 \in A$ viene detto *polinomio nullo* o anche 0.
- Se $f \in A[x] \setminus \{0\}$, definisco $gr(f) := min(\{k \in \mathbb{N} \mid ((\forall n > k)(a_n = 0))\})$. $gr(f)$ è detto *grado di f*.
- Se $f = (a_n)_{n\in\mathbb{N}} \in A[x] \setminus \{0\}$, $a_{gr(f)}$ è detto *coefficiente direttore* di f (scritto brevemente come $cd(f)$) e a_0 viene detto *termine noto*.
- Estendiamo queste definizioni anche al polinomio nullo: $cd(0) := 0$ (lo 0 di $\mathbb{N}$, ovviamente) e $gr(0) = -\infty$ (l'ordinamento di $\mathbb{N} \cup \{-\infty\}$ estende $(\mathbb{N}, \leq)$ e $-\infty$ è più piccolo di tutti).
- Se $a_{gr(f)} = 1$, f è detto *monico*.

Diamo ad $A[x]$ una struttura di anello.

- Definisco la somma tra polinomi come $(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} := (a_n + b_n)_{n\in\mathbb{N}}$. Il prodotto come $(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} := (\sum_{i+j=n} a_i b_j)_{n\in\mathbb{N}}$

  [Verificare per esercizio che $(A[x], +, \cdot)$ è unanello commutativo unitario verificando che l'unità è il polinomio $(1, 0, 0, 0, \ldots)$ e trovando esplicitamente gli opposti).]
- $(A[x], +, \cdot)$ si dice *anello dei polinomi a coefficienti in A*.
- I *polinomi costanti* sono quelli del tipo $(a, 0, 0, \ldots)$ con $a \in A$.
- La funzione $a \in A \mapsto (a, 0, 0, \ldots) \in A[x]$ è un monomorfismo tra anelli.
- Dunque, per ogni $a \in A$, pongo $a := (a, 0, 0, \ldots)$, identificando così con A l'insieme dei polinomi costanti.
- $x := (0, 1, 0, 0, \ldots)$.
- Facile provare per induzione che $x^n = (\underbrace{0, \ldots, 0}_{n \text{ volte}}, 1, 0, 0, \ldots)$.
- Anche facile che $ax^n = (a, 0, 0, \ldots) \cdot (\underbrace{0, \ldots, 0}_{n \text{ volte}}, 1, 0, 0, \ldots) = (\underbrace{0, \ldots, 0}_{n \text{ volte}}, a, 0, 0, \ldots)$.
- Dunque, se $gr(f) = m$ e $f = (a_0, \ldots, a_m, 0, \ldots)$, ottengo subito che $f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ (e $a_n \neq 0$ per la definizione di grado).
- Dalla distributività seguono le proprietà di somma e prodotto di due polinomi, ovvero che, se $m = gr(f)$, $n = gr(g)$ e $M = max\{m, n\}$, allora

- $f+g = \sum_{i=0}^{M}(a_i+b_i)x^i$;
- $fg = \sum_{i=0}^{m+n}(\sum_{j=0}^{i} a_j b_{i-j})x^i$.

Esempi: $\mathbb{Z}[x]$, $\mathbb{Z}_m[x]$ (con $m \in \mathbb{Z}$), $\mathbb{Q}[x]$.

Vediamo ora come si comportano i gradi dei polinomi quando andiamo a sommarli o a moltiplicarli. Siano $f, g \in A[x] \setminus \{0\}$ polinomi. Allora

- se $gr(f) = gr(g)$ e $cd(f) = -cd(g)$, allora $gr(f+g) < gr(f) = gr(g)$;
- altrimenti $gr(f+g) = max\{gr(f), gr(g)\}$.

Circa il prodotto, le cose dipendono molto dall'anello A. In $\mathbb{Z}_4$, ad esempio, $gr([1]_4 + [2]_4 x) = 1$ ma $gr(([1]_4 + [2]_4 x)^2) = 0$. Questo succede perché il coefficiente direttore del polinomio preso in esame non è cancellabile. Le seguenti proprietà che legano la cancellabilità ai gradi dei polinomi sono di facile verifica.

(1) se $cd(f)cd(g) = 0$, allora $gr(fg) < gr(f) + gr(g)$

(2) se $cd(f)cd(g) \neq 0$, allora $gr(fg) = gr(f) + gr(g)$ e $cd(fg) = cd(f)cd(g)$ (Questa è la *Formula di addizione dei gradi*, brevemente *f.a.g.*).

(3) se $cd(f)$ è cancellabile, anche f è cancellabile. In particolare, per f vale f.a.g.
Dimostrazione. $cd(f)$ cancellabile implica $cd(f)$ non divisore dello zero, quindi (2) implica $(\forall g \in A[x])$(per f e g vale f.a.g.), cioè f non è un divisore dello zero, cioè f non è cancellabile. □

(4) $A[x]$ è dominio di integrità se e solo se lo è A. (Perché, come già sappiamo, integro se e solo se non ci sono divisori dello zero non nulli)

(5) Sia $f \in A[x]$. Se $cd(f)$ è cancellabile e $gr(f) > 0$, allora f non invertibile.
Dimostrazione. Per assurdo, prendo $g = f^{-1}$. Per (2) ho $gr(f) + gr(g) = gr(fg) = gr(1) = 0$ e quindi $gr(f) = 0$, assurdo. □

(6) Se A è un dominio di integrità, $\mathcal{U}(A[x]) = \mathcal{U}(R)$. (direttamente da (5))
Controesempio a (5) e (6): $([1]_4 + [2]_4 x)([1]_4 + [2]_4 x)$.

(7) x non è mai invertibile (segue da (3) e (5)). In particolare, $A[x]$ non è mai un campo.

Teorema 25. *(Teorema della Divisione lunga) Sia A un anello commutativo unitario. Allora*

$$(\forall f, g \in A[x])(cd(g) \in \mathcal{U}(A) \to (\exists!(q,r) \in A[x] \times A[x])(f = gq + r \wedge gr(r) < gr(g))).$$

Dimostrazione. (Esistenza) Poniamo $m := gr(g)$ e $n := gr(f)$. Se $n < m$, ovvio con $q = 0$ e $r = f$. In particolare, il teorema è verificato per $f = 0$. Sia allora $n \geq m$. Pongo $a := cd(f)$ e $b := cd(g)$. Procediamo per induzione di seconda forma su n. Quindi suppongo vero l'asserto per i polinomi con grado $< n$. Sia $k := ab^{-1}x^{n-m}g$. Tra $ab^{-1}x^{n-m}$ e g vale f.a.g. (poiché $cd(g)$ è invertibile), quindi $gr(k) = gr(x^{n-m}) + gr(g) = n$ e $cd(k) = a$. Dico $h := f - k$. Dunque $gr(h) < n$ e per ipotesi di induzione ci sono q_1, r_1 tali che $h = q_1 g + r_1$ con $gr(r_1) < gr(g)$. Allora scrivo $f = k + h = (ab^{-1}x^{n-m} + q_1)g + r_1$ e pongo $q = ab^{-1}x^{n-m} + q_1$ e $r = r_1$. La tesi segue dal principio di induzione di seconda forma.
(Unicità) Siano (q_1, r_1) e (q_2, r_2) due coppie che verificano la tesi. Dunque $g(q_1 - q_2) = r_2 - r_1$. Allora $gr(r_2 - r_1) < m$ e, poiché per g vale f.a.g., $gr(g(q_1 - q_2)) = gr(g) + gr(q_1 - q_2) = m + gr(q_1 - q_2)$, da cui $m + gr(q_1 - q_2) < m$. Quindi $gr(q_1 - q_2) = -\infty$, ossia $q_1 = q_2$ e $r_1 = r_2$. □

L'importanza di questo teorema è nella sua dimostrazione, che fornisce l'algoritmo per effettuare la divisione tra polinomi (con buoni coefficienti direttori).

In particolare, nei campi è sempre possibile effettuare la divisione tra polinomi non nulli, sicché valgono tutti i risultati sui MCD, sul Teorema della divisione euclidea, sul Teorema di Bézout (che invece non vale in $\mathbb{Z}[x]$) e i loro corollari.

Teorema 26. *(No dim.) Se $(A, +, \cdot)$ è un anello fattoriale, anche $(A[x], +, \cdot)$ è un anello fattoriale.*

Esercizi

In questi esercizi, una volta fissato senza ambiguità un intero positivo n, denoteremo $[m]_n$ con $\overline{m}$.

(1) Se $(A, +, \cdot)$ è un anello commutativo unitario, dimostrare che anche $(A[x], +, \cdot)$ è un anello commutativo unitario.

(2) Trovare quattro polinomi $a, b, c, d \in \mathbb{Z}_8[x]$ tutti diversi tra loro, tali che $f = \overline{2}x - 1 \in \mathbb{Z}_8[x]$ si possa scrivere come $f = ab$ e $f = cd$.

(3) Sia $n > 1$ un numero intero e sia $f_n = \overline{3}x^4 + \overline{15}x^3 + \overline{60}x^2 + \overline{6}x + \overline{3} \in \mathbb{Z}_n[x]$. Qualora possibile, stabilire per quali valori di n f_n ha grado 4, per quali valori di n ha grado $-\infty$, per quali valori di n ha grado 3.

(4) Sia $f = \overline{3}x^2 + 1 \in \mathbb{Z}_{14}[x]$ e sia g un polinomio di grado 3 in $\mathbb{Z}_{14}[x]$. Possiamo dire qual è il grado di fg? E se $h = \overline{2}x^2 + 1$ possiamo dire qual è il grado di gh?

(5) Trovare un polinomio monico che sia prodotto di due polinomi non monici in $\mathbb{Z}_7[x]$

(6) Effettuare la divisione lunga tra i polinomi $4x^4 + 3x + 1$ e $x^2 + x$ in $\mathbb{Q}[x]$ e in $\mathbb{Z}[x]$.

(7) Effettuare la divisione lunga tra i polinomi $\overline{4}x^4 + \overline{3}x + \overline{1}$ e $\overline{2}x^2 + x$ in $\mathbb{Z}_2[x]$

(8) Trovare in $(\mathbb{Z}_4[x], +, \cdot)$ un polinomio invertibile e non costante.

Lezione 8

Sostituzione e radici

Diamo varie definizioni. Sia $f \in A[x]$ con $f = a_0 + a_1x + \cdots + a_nx^n$ e sia $c \in A$.

- Pongo $f(c) := a_0 + a_1c + \cdots + a_nc^n$
- Definisco *omomorfismo di sostituzione* l'applicazione $f \in A[x] \mapsto f(c) \in A$.
- Dico *applicazione polinomiale* determinata da f, l'applicazione $\overline{f} : c \in A \mapsto f(c) \in A$.
  Se $f = c \in A$, $(\forall z \in A)(f(z) = c)$. Motivo per cui sono detti "polinomi costanti."
- Un elemento c di A tale che $f(c) = 0$ si dice *radice* di f.
- Facile vedere dalle definizioni che $\overline{f+g}(c) = (\overline{f} + \overline{g})(c)$ e $\overline{fg}(c) = (\overline{f}(c)) \cdot (\overline{g}(c))$.
  Da questo segue che $(\forall k \in A[x])(f(c) = 0 \to (kf)(c) = 0)$.

Teorema 27. *(Teorema del resto) Sia A un anello commutativo unitario e siano $f \in A[x]$ e $c \in A$. Allora $f(c)$ è il resto della divisione di f per $x - c$.*

Dimostrazione. $x - c$ è monico, quindi posso applicare il Teorema della Divisione lunga. Ottengo $f = (x - c)q + r$ con $gr(r) < gr(x - c) = 1$. Da ciò segue che r è costante. Applico l'omomorfismo di sostituzione ed ho $f(c) = r(c) = r$. □

Dalla definizione di radice abbiamo subito:

Teorema 28. *(Teorema Ruffini) Sia A è un anello commutativo unitario e $f \in A[x]$ e $c \in A$. Allora c è radice di f sse $x - c$ divide f in $A[x]$.*

Ricordiamo che i domini di integrità sono sempre commutativi e unitari.

Teorema 29. *(Teorema di Ruffini generalizzato) Sia A un dominio di integrità e siano $f \in A[x]$ e $c_1, \ldots, c_n$ elementi a due a due distinti di A. Allora $c_1, \ldots, c_n$ sono tutte radici di f se e solo se $\prod_{i=0}^{n}(x - c_i)$ divide f in $A[x]$.*

Dimostrazione. $(\leftarrow)$ Ovvia.
$(\rightarrow)$ Procediamo per induzione di prima forma su n. Se $n = 1$, la tesi è quella del Teorema di Ruffini. Sia quindi $n > 1$ e supponiamo che il risultato valga per $n - 1$. Poiché $f(c_n) = 0$, per il Teorema di Ruffini esiste un polinomio q tale che $f = (x - c_n)q$. Per ogni $i \in \{1, \ldots, n - 1\}$, $0 = f(c_i) = (c_i - c_n)q(c_n)$. Ma $c_i - c_n$ non è mai nullo, perché le radici sono tutte distinte, e A è dominio di integrità, dunque $q(c_i) = 0$ per ogni $i \in \{1, \ldots, n - 1\}$. Per ipotesi di induzione, esiste $h \in A[x]$: $q = h\prod_{i=0}^{n-1}(x - c_i)$. Da qui la tesi usando il Principio di induzione di prima forma. □

Da ciò segue un semplice corollario sul grado di un polinomio con n radici in un dominio di integrità.

Teorema 30. *Se A è un dominio di integrità, $f \in A[x] \setminus \{0\}$ e n è il numero di radici di f, allora $n \leq gr(f)$.*

Dimostrazione. Sia $g = \prod_{i=0}^{n}(x - c_i)$. Per il Teorema di Ruffini generalizzato esiste $h \in A[x]$: $f = gh$. Ma A è dominio di integrità e $g \neq 0$, dunque vale f.a.g., quindi $gr(f) = gr(g) + gr(h) = n + gr(h) \geq n$ □

Dal teorema precedente non possiamo non richiedere che A sia un dominio di integrità. Infatti, $[2]_4x$ ha grado 1 pur avendo due radici in $\mathbb{Z}_4[x]$.

Teorema 31. *(Principio di identità dei polinomi) Sia A un dominio di integrità infinito. Allora $(\forall f, g \in A[x])(f = g \leftrightarrow \overline{f} = \overline{g})$.*

Dimostrazione. $(\rightarrow)$ Ovvia.
$(\leftarrow)$ $\overline{f} = \overline{g}$. In altre parole $(\forall c \in A)(f(c) = g(c))$. Se dico $h = g - f$, allora h ha infinite soluzioni e quindi può solo essere 0 per il corollario al Teorema di Ruffini generalizzato. □

Ovviamente per un A finito il Principio di identità dei polinomi non può valere, visto che esistono un numero finito di funzioni polinomiali, ma un numero infinito di polinomi.
Esempio: Ogni elemento di $\mathbb{Z}_3[x]$ è soluzione di $f = x^3 - x$, quindi $\overline{f} = \overline{0}$, ma i due polinomi sono diversi.

Fattorizzazione

Sia $(A, +, \cdot)$ un anello commutativo unitario e sia x un elemento di A. Un elemento y di A si dice *associato* ad x se x e y sono elementi associati in $(A, \cdot)$, ovvero se si dividono reciprocamente in $(A, \cdot)$. Similmente, x si dice *irriducibile* se $Div_{(A,\cdot)}(x) = BDiv_{(A,\cdot)}(x)$. Quindi, se A è un dominio di integrità, abbiamo che $assoc(x) = \{ux \mid u \in \mathcal{U}(A)\}$. Quindi tutti gli associati di x hanno lo stesso grado.
Chiaramente, se A è un campo abbiamo che $assoc(x) = \{ux \mid u \in A \setminus \{0\}\}$, sicché, in particolare,

Teorema 32. *Se A è un campo ogni polinomio non nullo su A è associato ad uno e un solo polinomio monico.*

Questo unico polinomio monico lo diremo *rappresentante monico della classe di f*.
Inoltre, da f.a.g. segue che, se A è un campo, ogni polinomio di grado 1 possiede solo i divisori banali, ovvero che ogni polinomio di grado 1 è irriducibile.

Teorema 33. *Sia A un campo ed $f \in A[x] \setminus \{0\}$. Allora esiste $c \in A$ ed esistono $p_1, \ldots, p_n \in A[x]$ irriducibili monici tali che $f = cp_1 \cdots p_n$. Inoltre, la decomposizione è unica a meno dell'ordine.*

Dimostrazione. L'unicità deriva dalla definizione di anello fattoriale (infatti $A[x]$ è fattoriale poiché lo è anche A) assieme all'unicità del rappresentante monico. Poiché l'esistenza è ovvia per i polinomi costanti, prendiamo un polinomio non costante f. Poiché $A[x]$ è fattoriale, esistono i polinomi irriducibili $q_1, \ldots, q_n$ tali che $f = q_1 \ldots q_n$. Sia, per ogni $i \in \{1, \ldots n\}$, $c_i = cd(q_i)$ e scriviamo $q_i = c_i p_i$. Chiaramente ogni p_i è monico e irriducibile perché associato all'irriducibile q_i. D'altra parte, detto $c = c_1 \ldots c_n$, abbiamo che $f = cp_1 \cdots p_n$, ovvero la tesi. □

Esercizi

(1) Scrivere $x^4 - \overline{4} \in \mathbb{Z}_5[x]$ come prodotto di polinomi monici di grado 2.

(2) Usare il Teorema di Ruffini per dimostrare che il polinomio $x^2 + 2 \in \mathbb{Z}_5[x]$ non può essere decomposto nel prodotto di polinomi di grado 1.

(3) Trovare in $\mathbb{Z}_5[x]$ due polinomi differenti che abbiano la stessa applicazione polinomiale.

(4) Trovare in $\mathbb{Z}_6[x]$ tre polinomi distinti che abbiano più radici del proprio grado.

(5) Scrivere, quando possibile, dei polinomi monici associati a $\overline{2}x^3 + \overline{2}x^2$, a $\overline{4}x^2 + \overline{8}$ e a $\overline{6}x^2 + x + \overline{2}$ in $\mathbb{Z}_9[x]$.

(6) Trovare tutti i primi p tali che $f = \overline{3}x^4 + x^3 + x + \overline{2} \in \mathbb{Z}_p$ sia divisibile in $\mathbb{Z}_p$ per $x^2 + 1$ (Suggerimento: usare la divisione lunga).

(7) Scrivere il rappresentante monico di $13x^3 + x - 12 \in \mathbb{Q}[x]$.

Lezione 9

Teorema 34. *Sia A un campo e sia $f \in A[x]$. Se $n = gr(f)$, f è irriducibile se e solo se $gr(f) > 0$ e vale una delle due proprietà seguenti (equivalenti tra loro)*

(a) $f = gh \to (gr(g) = n \; XOR \; gr(h) = n)$ *(ovvero "f non si decompone in polinomi di grado minore")*

(b) $f = gh \to (gr(g) = 0 \; XOR \; gr(h) = 0)$ *(ovvero "f non si decompone in polinomi di grado > 0")*

Dimostrazione. Mostriamo per prima cosa che le due proprietà sono equivalenti. Sia $f = gh$ con $gr(f) > 0$. Poiché A è un campo, vale sempre f.a.g., quindi $gr(g) = n \leftrightarrow gr(h) = 0$ e $gr(h) = n \leftrightarrow gr(g) = 0$, da cui l'equivalenza.
$(\leftarrow)$ $gr(f) > 0$ vuol dire che f non è invertibile e le due condizioni implicano che f ha solo i divisori banali.
$(\rightarrow)$ Supponiamo che f sia irriducibile, ovvero che f non sia invertibile ed abbia i soli divisori banali. Dunque certo $f \neq 0$ e sicuramente anche $gr(f) > 0$. Scrivo $f = gh$. Poiché vale f.a.g, f ha i soli divisori banali se e solo se $gr(g) = 0 XOR gr(h) = 0$ (se fossero entrambi 0, f sarebbe invertibile). Dunque vale la proprietà (a). □

Teorema 35. *Sia A un campo e sia $f \in A[x]$. Allora f ha radici in A se e solo se ha almeno un divisore di primo grado in $A[x]$.*

Dimostrazione. Segue dal Teorema di Ruffini e dal fatto che in un campo ogni polinomio di primo grado ha radici. □

Teorema 36. *Se A è dominio di integrità e $f \in A[x]$. Se $gr(f) > 1$ e f ha radici, allora non è irriducibile.*

Dimostrazione. La tesi segue dividendo f per $x - c$ grazie al Teorema di Ruffini. □

Da quanto detto e da f.a.g. abbiamo anche il seguente

Teorema 37. *Un polinomio di grado 2 o 3 su un campo A è irriducibile se e solo se non ha radici in A.*

Riassumiamo. Se A è un campo e $f \in A[k]$, allora:

- se $gr(f) = -\infty$, tutti gli elementi di A sono radici di f;
- se $gr(f) = 0$, f non ha nessuna radice;
- se $gr(f) = 1$, f è sempre irrididucibile e ha una sola radice;
- se $gr(f) = 2$ o 3, f irriducibile se e solo se non ha radici;
- se $gr(f) > 3$, f irriducibile implica che f non ha radici.

Esempi:

- $(x^2 + 1)(x^2 + 1) \in \mathbb{Q}[x]$ non ha radici e non è irriducibile.
- In $\mathbb{Z}[x]$, 2 non è invertibile ed è irriducibile, quindi $2x$ è di primo grado ma non irriducibile in $\mathbb{Z}[x]$. Invece in $\mathbb{Q}[x]$ lo è.

Alcuni importanti teoremi da sapere su $\mathbb{R}$ e su $\mathbb{C}$, enunciati senza dimostrazione:

- Ogni polinomio non costante in $\mathbb{C}[x]$ ha qualche radice. In particolare, gli unici polinomi irriducibili di $\mathbb{C}[x]$ sono quelli di grado 1.

- Ogni polinomio irriducibile di $\mathbb{R}[x]$ ha grado < 3.

  Dunque, i polinomi irriducibili in $\mathbb{R}[x]$ sono precisamente quelli di grado 1 e quelli di grado 2 privi di radici.

- Ogni polinomio di $\mathbb{R}[x]$ di grado dispari ha almeno una radice in $\mathbb{R}$. (Segue dal Teorema di degli zeri, anche detto Teorema di Bolzano)

- Le radici dei polinomi di grado 2 si trovano con la ben nota regola del discriminante (ponendo $\Delta = b^2 - 4ac$, il polinomio ha radici se e solo se $\Delta \geq 0$; in questo caso, le radici sono $x_1 = \frac{-b+\sqrt{\Delta}}{2a}$ e $x_1 = \frac{-b-\sqrt{\Delta}}{2a}$).

- Passiamo adesso ai polinomi su $\mathbb{Q}$.
Ovviamente, ogni polinomio in $\mathbb{Q}[x]$ è associato in $\mathbb{Q}[x]$ ad un polinomio in $\mathbb{Z}[x]$, moltiplicando per i denominatori.

Teorema 38. *(Criterio di irriducibilità di Eisenstein)(No dim.) Sia $f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. Se esiste un primo p tale che*

(1) p divide $a_0, a_1, \ldots, a_{n-1}$,

(2) $p \not| a_n$,

(3) $p^2 \not| a_0$,

allora f è irriducibile in $\mathbb{Q}[x]$.

Esempio: Per ogni n e p primo, $x^n - p$ è irriducibile in $\mathbb{Q}[x]$. In particolare, in $\mathbb{Q}[x]$ ci sono irriducibili di qualunque grado positivo.

Teorema 39. *(No dim.) Sia $f \in \mathbb{Z}[x] \setminus \{0\}$ con $cd(f) = a_n$ e $f(0) = a_0$. Se c è una radice razionale di f, abbiamo che $c = u/v$ con u e v coprimi, tali che $u|a_0$ e $v|a_n$.*

Da ciò abbiamo il seguente risultato.

Teorema 40. *Se $f \in \mathbb{Z}[x]$ è monico, allora ogni radice razionale è intera.*

Esercizi

(1) Elencare tutti i polinomi irriducibili di grado 2 e 3 su $\mathbb{Z}_2[x]$

(2) Detto $f = \overline{3}x^4 + x^3 + x + \overline{2} \in \mathbb{Z}_5$, scomporre f in polinomi irriducibili.

(3) Scrivere $x^3 - 4x^2 + 5$ come prodotto di polinomi monici irriducibili in $\mathbb{Q}[x]$

(4) Quali tra i seguenti polinomi sono irriducibili in $\mathbb{Q}[x]$, quali in $\mathbb{R}[x]$ e quali in $\mathbb{C}[x]$? $x^3 - 1$, $x^3 + 1$, $x^{13} + 3 \cdot 5^{12}$, $3x - 3$, $2(x^2 + 1)$.

(5) Mostrare che il polinomio $7x^4 + 6x^3 + 12x - 30$ è irriducibile in $\mathbb{Q}[x]$ ma non in $\mathbb{R}[x]$.

(6) È vero che tutti i polinomi costanti in $\mathbb{Z}[x]$ sono irriducibili?

(7) È vero che tutti i polinomi costanti di $\mathbb{Z}_6[x]$ sono irriducibili?

(8) Trovare una coppia di polinomi in $\mathbb{Z}_4[x]$ per i quali non valga al formula di addizione dei gradi.

Lezione 10

Grafi

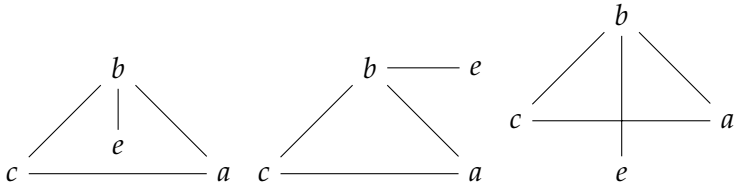
Sia v un insieme non vuoto e ρ una relazione simmetrica ed antiriflessiva su v. (v, ρ) si dice *grafo (semplice)*. Gli elementi di v si dicono *vertici* e le coppie $\{a, b\} \subseteq v$ tali che $a\rho b$ si dicono *archi* o *lati*.
Sia v un insieme non vuoto e sia $l \subseteq P_2(v) = \{\{x, y\} \mid x, y \in v \wedge x \neq y\}$. (v, l) la dico *grafo (semplice)*.
Mostrare per esercizio l'equivalenza tra le due definizioni.
Una terna di insiemi non vuoti (v, l, σ) si dice $multigrafo$ se $\sigma : l \to P_2(v)$.
Terminologia:

- Se $x, y \in v$ e $\{x, y\} \in l$, x e y si dicono gli *estremi* dell'arco $\{x, y\}$. In questo caso, diremo che x e y sono *adiacenti*. Archi che hanno un vertice in comune (ovvero gli archi con intersezione $\neq \emptyset$) si dicono *incidenti*.
- Il *grado* $d(x)$ di un vertice x è il numero di archi che lo contiene.
- Se $d(x)$ è dispari si dice che x è *dispari*, se $d(x) > 0$ è pari, x si dice *pari*, se $d(x) = 0$ x si dice *isolato* (ovvero, x non è contenuto in nessun arco).
- Un grafo si dice *completo* se tutti i suoi vertici sono a due a due adiancenti, ovvero se $l = P_2(v)$.
- Un grafo completo con n vertici viene denotato come K_n.
- $(v, P_2(v) \setminus l)$ si dice *grafo complementare* di (v, l).
- Se $v' \subseteq v$ e $l' \subseteq P_2(l')$, (v', l') si dice $sottografo$ di (v, l).
- Se l'insieme dei vertici e quello dei lati sono finiti, il (multi)grafo si dirà $finito$.

Se (v, l) e (v', l') sono due grafi, una funzione $f : v \to v'$ si dice $isomorfismo$ tra v e v' se è biettiva e $(\forall x, y \in v)(\{x, y\} \in l \leftrightarrow \{f(x), f(y)\} \in l')$.
Proprietà conservate da isomorfismi:

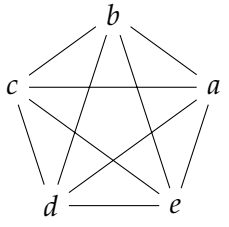
- $|v|$ e $|l|$.
- Grado di ogni vertice. (In l ci sono n archi cui x appartiene e lo stesso vale in l')

Ad esempio, le seguenti immagini sono rappresentazioni grafiche dello stesso grafo:

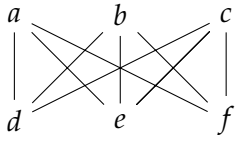


Un grafo si dice *piano* o *planare* se è rappresentabile su di un piano senza archi che si intersecano.
Esempi di due grafi non planari.

K_5:



$K_{3,3}$:



Teorema 41. *(Teorema di Kuratowski)(No dim.): Un grafo finito è planare se solo se non contiene né K_5 né $K_{3,3}$ come sottografi.*

Teorema 42. *Sia (v, l) un grafo finito. Allora* $2|l| = \sum_{x \in v} d(x)$

Dimostrazione. Sia t il numero di estremi di un qualche lato. Ogni lato ha due estremi, quindi $t = 2|l|$. D'altra parte ogni vertice x è estremo di $d(x)$ lati, per cui $t = \sum_{x \in v} d(x)$. □

Ancora definizioni.

- Siano $v_1, \ldots, v_n \in v$ tali che $(\forall i \in \mathbb{N})((1 \leq i \leq n-1) \rightarrow \{v_i, v_{i+1}\} \in l)$. Se l'insieme $\{\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\}\}$ ha ordine n, la n-upla

  $$(\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\})$$

  è detta *cammino* da v_1 a v_n di *lunghezza* n. Segue dalla definizione che tutti i lati di un cammino devono essere distinti.

- Inoltre, per ogni vertice x, si aggiunge il cammino nullo c_v da v in v di lunghezza 0.

- Un cammino di lunghezza non 0 in cui $v_1 = v_n$ si dice *circuito*.

- Definisco la seguente relazione binaria su v: $\gamma = (v \times v, g)$ dove $(v_1, v_2) \in g$ se e solo se esiste un cammino da v_1 a v_2. γ è una relazione di equivalenza.
  Dimostrazione. γ ovviamente è simmetrica ed è riflessiva grazie ai cammini nulli. Dimostriamo la transitività stando attenti all'intersezione tra i cammini. Siano $v_1 \gamma v_n$ e $w_1 \gamma w_m$ con $v_n = w_1$. Se i cammini non hanno lati in comune li concateniamo, ottenendo $v_1 \gamma w_m$. Altrimenti, sia j il minimo intero positivo tale che esista un k positivo per cui $\{v_j, v_{j+1}\} = \{w_k, w_{k+1}\}$. Allora la t-upla $(\{v_1, v_2\}, \ldots, \{v_j, v_{j+1}\}, \{w_{k+1}, w_{k+2}\}, \ldots, \{w_{m-1}, w_m\})$ è un cammino che va da v_1 a w_m e dunque γ è transitiva. □

- Una classe di equivalenza di γ si dice *componente connessa* del grafo.

- Un grafo si dice *connesso* se ha un'unica componente connessa (ovvero un'unica classe di equivalenza rispetto a γ).

- Sia (v, l, σ) un multigrafo, siano $v_1, \ldots, v_n, v_{n+1} \in v$ e sia $\{l_1, \ldots, l_n\} \subseteq l$ un insieme di archi distinti di l tali che $\sigma(l_i) = \{v_i, v_{i+1}\}$. Allora la n-upla ordinata

  $$(l_1, \ldots, l_n)$$

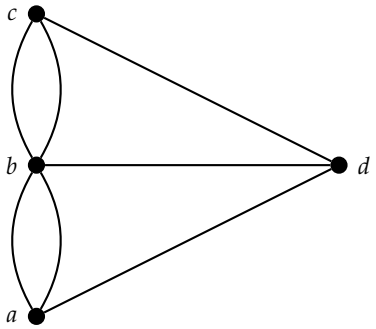
  si dice *cammino*.

- Un cammino $(l_1, \ldots, l_n)$ è detto *euleriano* se $l = \{l_1, \ldots, l_n\}$.

- Un cammino euleriano si dice *circuito euleriano* se $v_1 = v_{n+1}$.

Teorema 43. *(Teorema di Eulero)(No dim.): Sia g è un multigrafo finito privo di vertici isolati. Allora g ha un circuito euleriano sse è connesso e tutti i suoi vertici sono pari.*

Esempio: I sette ponti Königsberg (sul fiume Pregel).



Alberi e foreste

- Un grafo si dice $foresta$ se non ha circuiti;
- Un grafo connesso senza circuiti si dice *albero*.

Teorema 44. *Un grafo finito g è una foresta se e solo se per ogni coppia (x, y) di vertici distinti di g esiste al più un cammino in g da x a y.*

Dimostrazione. $(\rightarrow)$ Siano $(\{u_1, u_2\}, \{u_2, u_3\}, \ldots, \{u_{m-1}, u_m\})$ e $(\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\})$ due cammini distinti da x ad y (cioè $u_1 = v_1 = x$ e $u_m = v_m = y$). Sia $i = \{h \in \mathbb{N} \mid (\exists k \in \mathbb{N})(u_h = v_k \wedge \{u_h, u_{h+1}\} \neq \{v_k, v_{k+1}\})\}$ e sia $r = min(i)$ (c'è perché i due cammini sono distinti e quindi i non è vuoto) e sia k_r il relativo k. Sia ora $j = \{h \in \mathbb{N}_r \mid (\exists k \in \mathbb{N})(u_{h+1} = v_{k+1})\}$. $j \neq \emptyset$, perché i cammini si ricongiungono in y. Dico $s = min(j)$ ed k_s il relativo k. Certo $k_r \neq k_s$ altrimenti andiamo contro la definizione di i e j. Possiamo supporre $k_r < k_s$. Quindi il circuito è

$$(\{u_r, u_{r+1}\}, \{u_{r+2}, u_{r+3}\}, \ldots, \{u_s, u_{s+1}\}, \{v_{k_s+1}, v_{k_s}\}, \ldots, \{v_{k_r+2}, v_{k_r+1}\}, \{v_{k_r+1}, v_{k_r}\}).$$

$(\leftarrow)$ Supponiamo per assurdo che g non sia una foresta, ovvero di poter trovare un circuito

$$(\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\})$$

con $v_1 = v_n$. Poiché $n > 1$, ho che $(\{v_1, v_2\})$ e $(\{v_1, v_{n-1}, \ldots, \{v_3, v_2\}\})$ sono due cammini distinti tra i vertici v_1 e v_2, che sono distinti. Assurdo. □

Corollario 45. *Un grafo finito g è un albero se e solo se per ogni coppia (x, y) di vertici distinti di g esiste uno e un solo cammino in g da x a y.*

Visto che $K_{3,3}$ e K_5 hanno circuiti, dal Teorema di Kuratowsky otteniamo il seguente

Corollario 46. *Ogni foresta finita è un grafo planare.*

Rappresentazione radicale di un albero (fisso un vertice, detto radice, e sul livello n metto i vertici che hanno distanza n dalla radice). Dico $foglia$ dell'albero un vertice di grado 1.

Lemma 47. *Ogni albero finito con almeno due vertici ha una foglia.*

Dimostrazione. Supponiamo per assurdo che l'albero (v, l) con $|v| = n > 2$ non abbia foglie. Prendo $l_1 = \{v_1, v_2\}$. Ma $d(v_2) \geq 2$, quindi c'è $v_3 \notin \{v_1, v_2\}$ e $l_2 = \{v_2, v_3\}$. Ma $d(v_3) \geq 2$ e così via. Dunque esiste una successione $l_1, \ldots, l_n$ di lati distinti che collegano $n + 1$ vertici. Visto che $|v| = n$, qualcuno di questi deve ripetersi e quindi abbiamo trovato un circuito. Assurdo. □

Teorema 48. *Un albero di n vertici ha $n - 1$ lati.*

Dimostrazione. Procediamo per induzione di prima forma. Se $n = 1$ il risultato è ovvio. Sia allora $n > 1$ e supponiamo vero l'asserto per $n - 1$. Per il lemma precedente, l'albero ha allora una foglia x. Prendo il sottografo s di g in cui tolgo x e il suo unico ramo. s è ancora connesso e non ha circuiti, dunque è albero, dunque per induzione ha $n - 2$ lati, dunque g ne ha $n - 1$. Dal Principio di induzione di prima forma segue la tesi. □

Teorema 49. *(No dim.) Un albero finito con almeno* 2 *vertici ha almeno due foglie.*

Dimostrazione. Sia $|v| = n$. Per teorema precedente, g ha $n - 1$ lati. Quindi $\sum_{x \in v} d(x) = 2(n-1)$. Ma se ho meno di due foglie ho almeno $n - 1$ vertici di grado ≥ 2, ovvero $\sum_{x \in v} d(x) \geq 2(n-1) + 1$, assurdo. □

Se g è un grafo connesso, un sottografo s si dice *albero di supporto* o *sottoalbero massimale* se è un albero di g con lo stesso insieme di vertici di g.

Teorema 50. *(No dim.) Se $g = (v, l)$ è un grafo finito con esattamente k componenti connesse, allora $|l| \geq |v| - k$ e vale l'uguaglianza se e solo se g è una foresta.*

Dimostrazione. Per induzione su k. Se $k = 1$ prendo un albero di supporto a, per cui vale $|l_a| = |v_a| - 1$ per Teorema 48; quindi $|l_g| \geq |v_g| - 1$ (potenzialmente ci sono più lati). Sia $k > 1$ e siano s una componente connessa di g e t il sottografo costituito da tutte le altre. Come prima $|l_s| \geq |v_s| - 1$ e per induzione $|l_t| \geq |v_t| - (k-1)$. Da cui $|l| \geq |v| - k$.
È chiaro che per le foreste vale l'uguaglianza. Mostriamo ora che se vale l'uguaglianza, g è una foresta. Prendo le k componenti connesse ed ho che

$$|l| = \sum_{n=1}^{k} |l_n| \geq \sum_{n=1}^{k} (|v_n| - 1) = |v| - k = |l|$$

Se avessimo che, per un certo i, $|l_i| > |v_i| - 1$ avremmo $|l| > |l|$, dunque ogni componente connessa è un albero e g è una foresta. □

Ecco una immediata conseguenza di quest'ultimo teorema.

Corollario 51. *Le seguenti affermazioni sono equivalenti:*

(1) g è un albero;

(2) g è un grafo connesso e $|v| = |l| + 1$;

(3) g è una foresta e $|v| = |l| + 1$.

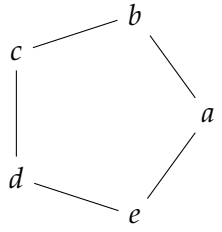
Esercizi

(1) Disegnare 7 grafi non isomorfi con 4 vertici e scrivere formalmente almeno 3 di questi.

(2) Disegnare 8 multigrafi non isomorfi con 3 vertici e scrivere formalmente almeno 3 di questi.

(3) Qual è la somma dei gradi di tutti i vertici di un grafo finito connesso senza circuiti con 7 vertici?

(4) Sia g il seguente grafo



Disegnare il grafo complementare di g.

(5) Mostrare che il grafo complementare al grafo g dell'esercizio precedente è planare disegnandone uno planare ed isomorfo ad esso.

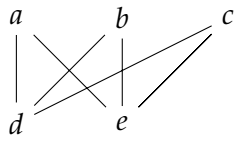
(6) Possiamo dire che il grafo complementare al grafo g dell'esercizio 4 è planare senza doverne disegnare uno? (Suggerimento: si tratta di usare la teoria)

(7) Mostrare con un esempio che esistono grafi che non sono alberi e i cui sottografi propri siano tutti alberi.

(8) Determinale tutti e soli i numeri naturali n tali che il grafo completo K_n possieda cammini euleriani.

(9) Disegnare su di un grafo completo su 7 vertici un cammino euleriano.

(10) Sia g il seguente grafo



Mostrare che g è un grafo planare.

(11) Dimostrare che un albero finito con almeno 2 vertici ha almeno due foglie.