1 First week

2^A: insieme delle parti di A $\Rightarrow$ $2^{\wedge \# A}$ = elenco delle parti di A

Relazioni: dati 2 insiemi X e Y, e un sottoinsieme $\mathcal{R}$(X,Y) è detto relazione tra X e Y e scriveremo x$\mathcal{R}$y, x,y$\in$ $\mathcal{R}$

Funzione: siano dati X,Y e dia f una relazione tra X e Y, f $\subset X \times Y$. diremo che f è una funzione da X in Y se vale:

$$\forall x \in X : \exists ! y \in Y t.c. (x, y) \in f$$

Dominio: insieme delle x che vanno in Y

Codomidio: insieme delle y che hanno corrispondenza in X

Legge: proprietà che definisce una relazione da X a Y

Insieme di tutte le funzioni: Y^X corrisponde a tutte le funzioni con leggi diverse ma con stessi insiemi di partenza ed arrivo

Funzione identità: $id_X(X) = X$

Composizione di funzioni: $x \to^f y \to^g z \Rightarrow g(f(x)) = z \Rightarrow gof(x) = z$

Iniettiva: ad ogni f(x) corrisponde un solo y
Surgettiva: ad ogni y corrisponde un f(x)
Bigiettiva: sia iniettiva che suriettiva

Inversa: se f è biettiva, allora esiste $g = f^{-1}$

2 Second week

Sistemi equipotenti: X e Y sono equipotenti ($X \sim Y$) se hanno la stessa cardinalità e la funzione $f : X \to Y$ è bigiettiva (o invertibile)

insiemi cardinali: sono gli insiemi in formato {0,1,...,n} equipotenti all'insieme dato, si rapprensentano $|A|$ e definiscono una cardinalità pari a n+1

TEOREMA: X e Y sono equipotenti se e solo se i loro insiemi cardinali sono uguali

$$|X| = |Y|$$

Numeri naturali: sono definiti dagli assiomi di Peano:

- 0 è un numero naturale
- esiste una funzione successivo $\mathbb{N} \to \mathbb{N}$
- succ(n) $\in \mathbb{N} \backslash \{0\}$, cioé il successivo di ogni naturale è diverso da 0
- vale principio d'induzione

Principio d'induzione: con $A \subset \mathbb{N}$

- base induttiva: $0 \in A$
- passo induttivo: $\forall n \in \mathbb{N}, n \in A \Rightarrow succ(n) \in A$, allora $A = \mathbb{N}$

Principio induttivo di prima forma:
Prendiamo una proposizione P(n) e supponiamo che rispetti 2 condizioni:

- la base induttiva: P(0) è vera
- il passo induttivo: $\forall n \in \mathbb{N}$, P(n) è vera (ipotesi induttiva), allora P(succ(n))

Se rispetta queste condizioni allora implica $\forall n \in \mathbb{N}$, P(n)

Teorema di ricorsione: Sia X un insieme, esite una funzione $f : \mathbb{N} \to X$ t.c.:

$$f(0) = c$$
$$f(succ(n)) = h(n, f(n))$$

Addizione: tramite il teorema di ricorsione definiamo la funzione $m \to n + m$:

$$n + 0 = n$$
$$n + succ(m) = succe(n) + m$$

Moltiplicazione: tramite il teorema di ricorsione definiamo la funzione $m \to nm$:

$$n \cdot 0 = 0$$
$$n(m + 1) = mn + n$$

Ordinamento dei naturali: può essere totale o parziale

Ordine parziale: è una relazione $\mathcal{R} \subset X \times X$ e rispecchia le seguenti proprità:

- riflessiva: $x\mathcal{R}x, \forall x \in X$
- antisimmetrica: $x\mathcal{R}yey\mathcal{R}x \Rightarrow x = y, \forall x, y \in X$
- transitiva: $x\mathcal{R}y \ e \ y\mathcal{R}z \Rightarrow x\mathcal{R}z, \forall x, y, z \in X$

Ordinamento totale: come l'ordinamento parziale, ma con la proprietà aggiunta:

- tricotomia: $x\mathcal{R}y \ o \ y\mathcal{R}x \, \forall x, y \in X$

insiemi ordinati: se $\mathcal{R}$ è parziale o totale, dirò che $(X, \mathcal{R})$ è parzialmente o totalmente ordinato

Principio d'induzione shiftato di prima forma: identico alla prima forma ma la base invece che 0, parte da $k \leq n$

- base induttiva: P(k) è vera
- passo induttivo: $\forall n \geq k$, P(n) è vera $\Rightarrow$ P(n+1)

3 third week

exercises

4 forth week

Insiemi finiti: Indicando con I_n un insieme che va da 0 a n, diremo che l'insieme X è finito se essite $n \in \mathbb{N}$ t.c. $I_n \sim X$. Se non esiste lo definiremo insieme infinito.

Teorema di lemma dei cassetti: Siano X e Y due insiemi rispettivamente $X \sim I_n$ e $Y \sim I_m$ con $n < m$ allora la funzione $f(x):\ Y \to X$ non è iniettiva

Cardinalità: Sia X un insieme finito. Definiamo cardinalità n t.c. I_n sia equipotente a X. Definiamo I_n come insieme cardinalità associato a X

Proposizione: Sia A insieme finito e $B \subseteq A$, allora $|B| \leq |A|$

Osservazione: Qualsiasi $f(x) : \mathbb{N} \to \mathbb{N}/\{0\}$ è bigiettiva

Minimo: Sia A un insieme e $z \in A$. Se $\forall x \in A, z \leq x$, allora definiremo z come **minimo** di A:

$$z = min(A)$$

Buon ordinamento: Un ordinamento totale è definito **ben ordinato** se ogni sottoinsieme di $(Z, \leq)$ ammette un minimo

Assioma di buon ordinamento: L'ordinamento $(\mathbb{N}, \leq)$ è ben ordinato e l'ordinamento $\leq$ è **usuale** su $\mathbb{N}$ (cioé se $\exists k\ t.c.\ n + k = m$ allora $n \leq m$)

Principio di induzione (2$^a forma$): prendiamo una famiglia di preposizioni $P(n)$ e supponiamo rispetti le 2 condizioni:

- la base induttiva: $P(0)$ è vera
- il passo induttivo: $\forall n \in \mathbb{N}, \forall k \in \mathbb{N}\ t.c.\ 0 \leq k \leq n$, $P(k)$ è vera (ipotesi induttiva), allora P(n)

Se rispetta questa condizioni allora implica $\forall n \in \mathbb{N},\ P(n)$

Divisione euclidea: Siano $n, m \in \mathbb{Z} t.c. m \neq 0 \exists! q, r \in \mathbb{Z} t.c :$

$$\begin{gathered} n = mq + r \\ 0 \leq n < |m| \end{gathered}$$

(si definiscono q quoziente e r resto della divisione di n per m)

5 fifth week

Rappresentabilità: Sia $b \in \mathbb{N}$, diremo che $n \in \mathbb{N}$ è rappresentabile in base b se esistono $k \in \mathbb{N}$ e $\varepsilon 0, \varepsilon 1, ..., \varepsilon k \in I_b$ $t.c$:

$$n = \sum_{i=0}^{k} \varepsilon_i b^i \qquad \text{con } I_b = \{0, 1, ..., b-1\}$$

Teorema della rappresentazione dei naturali in base arbitraria: Sia $b \in \mathbb{N}, b \geq 2$, allora $\forall n \in \mathbb{N},\ n$ è rappresentabile in base b in maniera univoca

Divisibilità: Dati $n, m \in \mathbb{Z}$ si dice che n è **divisore** di m (o m è multiplo di n) se $\exists k \in \mathbb{Z}$ $t.c.$ $m = nk$ e scriveremo $n|m$

Proprità della divisibilità:

- se $n|m$ e $m|q$ allora $n|q$
- se $n|m$ e $m|n$ allora $n = \pm m$

Massimo Comune Divisore: Dati $m, n \in \mathbb{Z}$ si dice $d \in \mathbb{Z},\ d > 0$ massimo comune divisore se:

- $d|n$ e $d|m$
- $\exists c \in \mathbb{Z}$ $t.c.$ $c|n$ $c|m$ $c|d$

proposizione: se d e d^I sono mcd tra m e n allora $d = d^I$

Teorema: dati $n, m \in \mathbb{Z} \neq 0$, esiste mcd unico indicato con (n, m)

Lemma utile: dati $n, m, c \in \mathbb{Z} \neq 0$ e $c|n$ $c|m$, allora $\forall x, y \in \mathbb{Z}$ vale:

$$c|xn + ym$$

Corollario: Siano $n, m \in \mathbb{Z} \neq 0$ se sia $d := (n, m)$ allora esistono $x, y \in \mathbb{Z}$ $t.c$:

$$d = xn + ym$$

Numeri coprimi: dati $n, m \in \mathbb{Z}$, si dicono coprimi fra di loro se $(n, m) = 1$

proposizione: sia $d = n, m$ allora $(\frac{n}{d}, \frac{m}{d}) = 1$

Algoritmo di Euclide:

$$
\begin{array}{ccc}
n = q_1 m + r_1 & & r_1 = n - q_1 m \\
m = q_2 r_1 + r_2 & & r_2 = m - q_2 r_1 \\
r_1 = q_3 r_2 + r_3 & & r_3 = r_1 - q_3 r_2 \\
\cdot & & \cdot \\
\cdot & \Rightarrow & \cdot \\
\cdot & & \cdot \\
r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} & & r_{k-1} = r_{k-3} - q_{k-1} r_{k-2} \\
r_{k-2} = q_k r_{k-1} + r_k & & r_k = r_{k-2} - q_k r_{k-1} \\
r_{k-1} = q_{k+1} r_k + 0 & & = xn + ym
\end{array}
$$

Es:

$$(48,28)$$

$$
\begin{array}{ccc}
48 = 28 \cdot 1 + 20 & & \\
28 = 20 \cdot 1 + 8 & & 4 = 20 - 2 \cdot 8 \\
20 = 8 \cdot 2 + 4 & \Rightarrow & 8 = 28 - 20 \cdot 1 \\
8 = \underline{4} \cdot 2 + 0 & & 20 = 48 - 28 \cdot 1 \\
MDC = 4 & &
\end{array}
$$

$$
\begin{gathered}
\Downarrow \\
4 = 20 - 2(28 - 20 \cdot 1) = 3 \cdot 20 - 2 \cdot 28 \\
4 = 3(48 - 28 \cdot 1) - 2 \cdot 28 \\
= \underline{3 \cdot 48 - 5 \cdot 28}
\end{gathered}
$$

6 Sixth week

Proprietà dei coprimi: Siano $n, m, q \in \mathbb{Z}$ e n o $m \neq 0$ e $(n, m) = 1$:

- Se $n|mq$ allora $n|q$
- Se $n|q$ e $m|q$ allora $nm|q$

Numeri primi: $p \in \mathbb{Z}$ si dice **primo** se $p \geq 2$ e i suoi divisori sono quelli banali ($\pm 1|p,\ \pm p|p$). p è primo se $\forall n, m$ e $p|nm$ allora $p|n \bigvee p|m$

Minimo Comune Multiplo: dati $n, m \in \mathbb{Z}$ si dice M minimo comune multiplo di n e m se:

- $n|M$ e $m|M$
- $\exists c\ t.c.\ n|c, m|c, M|c$

Unicità mcm: dati $n, m \in \mathbb{Z}$ e M, M^1 sono mcm di n e m, allora $M = M^1$

Denotazione mcm: mcm di n e m si scrive $[n, m]$

Teorema d'esistenza: siano $n, m \in \mathbb{Z}$ allora $\exists [n, m]$ e se $n \bigvee m \neq 0$ allora:

$$[n, m] = \frac{nm}{(n,m)}$$

Teorema fondamentale dell'aritmetica: $\forall n \in \mathbb{N}, n \geq 2$, n è uguale a un prodotto di numeri primi, anche ripetuti:

$$n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_k$$

La fattorizzazione di questo prodotto è univoca

Corollario: i numeri primi sono infiniti

Congruenza: dati $a, b \in \mathbb{Z}$ diremo che a è congruo a b modulo n ($a \equiv b\ mod\ n$) se

$$n|a - b$$

Proprietà congruenza:

- riflessiva: $a \equiv a\ mod\ n \quad \forall a, n \in \mathbb{Z}$

- simmetrica: $a \equiv b \ mod \ n$ allora $b \equiv a \ mod \ n \quad \forall a, b, n \in \mathbb{Z}$
- transitiva: $a \equiv b \ mod \ n$ e $b \equiv c \ mod \ n$ allora $a \equiv c \ mod \ n \quad \forall a, b, c, n \in \mathbb{Z}$

equivalenza: una relazione $\mathcal{R}$ binaria su l'insieme X si dice relazione d'equivalenza su X se:

- è riflessiva: $\forall x \in X, \ x\mathcal{R}x$
- è simmetrica: $\forall x, y \in X, \ x\mathcal{R}y$ allora $y\mathcal{R}x$
- è transitiva: $\forall x, y, z \in X, \ x\mathcal{R}y$ e $y\mathcal{R}z$ allora $x\mathcal{R}z$

7 seventh week

Classi d'equivalenza: sia X, $x \in X$ e $\sim$ una relazione d'equivalenza su X. Chiameremo classe d'equivalenza di x in X rispetto a $\sim$ il sottoinsieme di X i quali elementi y sono equivalenti a x:

$$[x]_{\sim} = \{y \in x | y \sim x\}$$

Insieme quoziente: chiameremo insieme quoziente di X modulo $\sim$ l'insieme delle classi d'equivalenza contenute in X:

$$X/\sim = \{y \in \ x | y \sim x\}$$

Proprietà classi d'equivalenza:

- $\forall x \in X, \ x \in [x]$
- $\forall x, y \in X, \ [x] = [y] \Leftrightarrow x \sim y$
- $\forall x, y \in X, \ [x] \cap [y] \neq 0 \Rightarrow [x] = [y]$

Classi di congruenza: Dati $a, n \in \mathbb{Z}$ definiamo la classe di congruenza di a modulo n l'insieme delle x congruenti ad $a \ mod \ n$:

$$[a]_n = \{x \in \mathbb{Z} | x \equiv a \ mod \ n\}$$

Indicheremo l'insieme quoziente $\mathbb{Z} \ mod \ \sim_n$ come $\mathbb{Z}/_n\mathbb{Z}$ e ha come elementi le classi di congruenza $[a]_n$ che appartengono alle partizioni di $\mathbb{Z}$ $(2^{\mathbb{Z}})$, quindi:

$$[a]_n = \{a + kn | k \in \mathbb{Z}\}$$

Es:
$\mathbb{Z}/_3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$

Prop: Sia $a \in \mathbb{Z}$ e sia r il resto di $\frac{a}{n}$, allora $a \equiv r\ (mod\ n)$, oppure:

$$[a]_n = [r]_n$$

Criterio di divisibilità: dati $a, n \in \mathbb{Z}$ con $n \neq 0$, diremo che a è multiplo di n se:

$$[a]_n = [0]_n$$

Notazione: dato $a \in \mathbb{Z}$ e $x \in [a]_n$ ($[a]_n = [x]_n$), diremo che x è **rappresentante della classe** $[a]_n$. Se x è di tipo resto, allora x è **rappresentante canonico**

gli elementi di $\mathbb{Z}/_n\mathbb{Z}$ si chiamano **classi di resto** modulo n

Struttura algebrica: esistono due operazioni di somma e moltiplicazione tra insiemi quozienti:

- Somma: $[a]_n + [b]_n = [a+b]_n$
- Moltiplicazione: $[a]_n \cdot [b]_n = [a \cdot b]_n$

Prop: dati $a, a^1, b, b^1 \in \mathbb{Z}$ tc $[a]_n = [a^I]_n$ e $[b]_n = [b^I]_n$ allora:

- Somma: $[a+b]_n = [a^I + b^I]_n$
- Moltiplicazione: $[a \cdot b]_n = [a^I \cdot b^I]_n$

Oss: Sia $a \in \mathbb{Z},\ m \in \mathbb{N},\ m > 0$. Allora:

$$[a]_n^m = [a_1]_n \cdot [a_2]_n \cdot ... \cdot [a_m]_n \cdot = [a^m]_n$$

8 eight week

Teorema cinese del resto: Siano $n, m > 0$ e siano $a, b \in \mathbb{Z}$. Consideriamo il seguente sistema di congruenze:

$$\begin{cases} x \in \mathbb{Z} \\ x \equiv a(mod\ n) \\ x \equiv b(mod\ m) \end{cases} \quad \text{o} \quad \begin{cases} x \in \mathbb{Z} \\ [x]_n = [a]_n \\ [x]_m = [b]_m \end{cases}$$

Sia S l'insieme delle soluzioni dei precedenti Sistemi

$$S = \langle x \in \mathbb{Z} | x \equiv a(mod\ n)\ e\ x \equiv b(mod\ m) \rangle$$

Il precedente sistema è **compatile** (ammette soluzioni) se e soltanto se:

$$(n, m) | a - b$$

Se $S \neq \varnothing$ e $c \in S$, allora $S = [c]_{[n,m]} \in \mathbb{Z} = \langle c + k_{[n,m]} \in \mathbb{Z} | k \in \mathbb{Z} \rangle$

Es:

$$\begin{cases} x \equiv 9(mod\ 162) \\ x \equiv -9(mod\ 114) \end{cases}$$

1 - Compatibilità

$$\begin{aligned} (162, 114) = 6 \quad \Rightarrow \quad & (162, 114)|9 - (-9) = 6|18 = 3 \\ & \Rightarrow 9 - (-9) = 3(162, 114)_{(1)} \end{aligned}$$

2 - Calcolo di una soluzione
Algoritmo di Euclide:

$$\begin{array}{c|c} 162 = 114 + 48 & 48 = 162 - 114 \\ 114 = 2 \cdot 48 + 18 & 18 = 114 - 2 \cdot 48 \\ 48 = 2 \cdot 18 + 12 & 12 = 48 - 2 \cdot 18 \\ 18 = 12 + 6 & 6 = 18 - 12 \\ 12 = 2 \cdot 6 + 0 & \end{array} \quad \Rightarrow \quad \begin{array}{c} = 18 - (48 - 2 \cdot 18) = 3 \cdot 18 - 48 \\ = 3(114 - 2 \cdot 48) - 48 = 3 \cdot 114 - 7 \cdot 48 \\ = 3 \cdot 114 - 7(162 - 114) = 10 \cdot 114 - 7 \cdot 162 \\ 6 = 10 \cdot 114 - 7 \cdot 162 \\ (162, 114) = 10 \cdot 114 - 7 \cdot 162_{(2)} \end{array}$$

Da (1) e (2) segue che

$$9-(-9)=3(162,114)=3(10\cdot 114-7\cdot 162)$$
$$9-(-9)=30\cdot 114-21\cdot 162_{(3)}$$

$$9+21\cdot 162=-9+30\cdot 114 \Rightarrow 3411$$

$c=3411$ è una soluzione del sistema

3 - Calcolo di S
Teorema cinese del resto:

$$S=[c]_{[162,114]}=[3411]_{[162,114]}$$

$$[162,114]=\frac{162\cdot 114}{(162,114)}=3078 \quad \Rightarrow \quad S=[3411]_{[3078]}=[333]_{[3078]}$$

$$\Rightarrow S=\langle 333+3078k\in\mathbb{Z}|k\in\mathbb{Z}\rangle$$

Bonus:
Esiste soluzione di S divisibile da 17?

metodo 1

$$\begin{cases} x\equiv 333(mod\ 3078) \\ x\equiv 0(mod\ 17) \end{cases}$$

$$(3078,17)|333-0$$

$$1|333$$

è divisibile quindi accetta soluzione

metodo 2

$$[333+3078k]_{17}=[333]_{17}+[3078]_{17}[k]_{17}$$
$$[10]_{17}+[1]_{17}[k]_[17]=[10+k]_{17}$$
$$\Rightarrow k=7$$

9 neinth week

Elementi invertibili modulo n: Siano $a, n \in \mathbb{Z}$ con $n > 0$. Diremo che a è invertibile modulo n o equivalentemente che $[a]_n$ è invertibile in $\mathbb{Z}/_n\mathbb{Z}$ se esiste $x \in \mathbb{Z}$ tc:

$$ax \equiv 1(mod\ n) \Leftrightarrow [a]_n[x]_n = [1]_n$$

In questo caso diremo che x è un'inversa di $a(mod\ n)$ e $[x]_n$ è una classe inversa di $[a]_n$ in $[Z]/_n\mathbb{Z}$

Lemma: Supponiamo che a sia invertibile modulo n, ovver $[a]_n$ sia invertibile in $[Z]/_n\mathbb{Z}$. Allora esiste un unico $[x]_n \in [Z]/_n\mathbb{Z}$ tale che:

$$[a]_n[x]_n = [x]_n[a]_n = [1]_n$$

Equivalentemente $[x]_n$ è l'unica classe inversa di $[a]_n$ in $[Z]/_n\mathbb{Z}$. Tale classe $[x]_n$ viene detta inversa e viene indicata con il simbolo $[a]_n^{-1}$

Prop: $a \in \mathbb{Z}$ è invertibile $mod\ n \Leftrightarrow (a, n) = 1$, in questo caso esiste $x, y \in \mathbb{Z}$ tali che:

$$xa + yn = 1$$
$$(Algoritmo\ di\ euclide)$$

Allora

$$[a]_n^{-1} = [x]_n$$

Es:
11 $inv(mod\ 30)$

$(11, 30) = 1 \Rightarrow \exists[11]_{30}^{-1}$

alg. euclide:
$1 = 11 \cdot 11 + (-4)30$

$[1]_{30} = [(11)(11) + (-4)(30)] = [11]_{30}[11]_{30} + [-4]_{30}[0]_{30} = \underline{[11]_{30}}[11]_{30} \Rightarrow [11]_{30}^{-1} = [11]_{30}$

Def: Dato $n \in \mathbb{Z}, n > 0$, indichiamo con $(\mathbb{Z}/_n\mathbb{Z})^*$ il sottoinsieme di $\mathbb{Z}/_n\mathbb{Z}$ formato da tutti gli interi modulo n invertibili

invertibili, cioé mcd è uguale a 1

Prop: Sia p numero primo, allora vale:

$$(\mathbb{Z}/_n\mathbb{Z})^* = \{[1]_p, [2]_p, ..., [p-1]_p\} = \mathbb{Z}/_p\mathbb{Z}\backslash\{[0]_p\}$$

Prop: Sia $a \in \mathbb{Z}$ e r sia il resto di a/n, allora:

$$a \equiv n(mod\ n)$$

oppure

$$[a]_n = [r]_n$$

Criterio di divisibilità: dati $a, n \in \mathbb{Z}$ con $n \neq 0$, diremo che a è multiplo di n se:

$$[a]_n = [0]_n$$

notazione: dato $a \in \mathbb{Z}$ e $x \in [a]_n$ ($[a]_n = [x]_n$), diremo che x è *rappresentante della classe* $[a]_n$. Se x è di tipo resto, allora x è *rappresentante canonico*

Gli elementi di $\mathbb{Z}/_n\mathbb{Z}$ si chiamano *classi di resto modulo n*

Struttura algebrica: Esistono due operazioni di somma e moltiplicazione tra insiemi quozienti:
Somma: $[a]_n + [b]_n = [a+b]_n$
Moltiplicazione: $[a]_n \cdot [b]_n = [ab]_n$

Prop: dati $a, a^I, b, b^I \in \mathbb{Z}$ tali che $[a]_n = [a^I]_n$ e $[b]_n = [b^I]_n$, allora:

- $[a+b]_n = [a^I + b^I]_n$
- $[ab]_n = [a^I b^I]_n$

Oss: Sia $a \in \mathbb{Z},\ m \in \mathbb{N},\ m > 0$. Allora:

$$[a]_n^m = [a^m]_n$$

10 tenth week

Il teorema di Fermat-Eulero
Definiamo la funzione $\phi : \mathbb{N}/\{0\} \to \mathbb{N}$, detta *funzione phi di eulero*, ponendo:

$$\phi(n) := |\{a \in \mathbb{Z} \,|\leq a \leq n,\ (a,n) = 1\}| \qquad \forall n \in \mathbb{N}/\{0\}$$

Oss: la funzione ϕ è moltiplicativa sulle coppie coprime:

$$\phi(n \cdot m) = \phi(n) \cdot \phi(m) \qquad \forall n, m \in \mathbb{N}/\{0\}\ tc\ (n,m) = 1$$

Sia p un numero primo e sia $m \in \mathbb{N}/\{0\}$. Considero $n = p^m$, allora $\phi(n) = \phi(p^m)$ che vale:

$$\phi(p^m) = p^m - p^{m-1} \qquad \forall p \text{ primo e } \forall m \in \mathbb{N}/\{0\}$$

Formula generale: Sia $n \geq 2$ e $n = p_1^{m_1} \cdot p_2^{m_2} \cdot ... \cdot p_k^{m_k}$ per qualche numero primo $p_1, p_2, ..., p_k$ con $p_i \neq p_j \forall i \neq j$ e $m_1, ..., m_k \in \mathbb{N}/\{0\}$. Allora:

$$\phi(n) = \phi(p_1^{m_1} \cdot ... \cdot p_k^{m_k}) = (p_1^{m_1} - p_1^{m_{1-1}}) \cdot ... \cdot (p_k^{m_k} - p_k^{m_{k-1}})$$

Lemma: Dato $n > 0$, vale:

$$|(\mathbb{Z}/_n\mathbb{Z})^*| = \phi(n)$$

Lemma: Dati $\alpha, \beta \in (\mathbb{Z}/_n\mathbb{Z})^*$, valgono le seguenti affermazioni:

- $\alpha\beta \in (\mathbb{Z}/_n\mathbb{Z}), \quad (\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}$
- $\alpha^{-1} \in (\mathbb{Z}/_n\mathbb{Z}), \quad (\alpha^{-1})^{-1} = \alpha$

Teorema: Sia $n > 0$. Per ogni $\alpha \in (\mathbb{Z}/_n\mathbb{Z})^*$, vale:

$$\alpha^{\phi(n)} = [1]_n \text{ in } \mathbb{Z}/_n\mathbb{Z}$$

Equivalentemente, per ogni $a \in \mathbb{Z}$ tale che $(a,n) = 1$

$$a^{\phi(n)} \equiv 1 (mod\ n)$$

Corollario: Se p è un numero primo e $a \in \mathbb{Z}$ tale che $(p,a) = 1$, allora:

$$\text{Con } n = p \Rightarrow a^{p-1} \equiv 1 (mod\ p)$$

Crittografia RSA

Fissiamo $n > 0$. Per ogni $c \in \mathbb{N}/\{0\}$, definiamo la funzione:

$$\begin{aligned} P_c : (\mathbb{Z}/_n\mathbb{Z})^* &\to (\mathbb{Z}/_n\mathbb{Z})^* \\ \alpha &\to \alpha^c \end{aligned}$$

Ovvero $P_c(\alpha) := \alpha^c \quad \forall \alpha \in (\mathbb{Z}/_n\mathbb{Z})^*$. La funzione P_c è ben definita, ovvero, se α è una classe di congruenza e n invertibile, allora anche α^c è invertibile

Teorema della crittografia RSA

Sia $c \in \mathbb{N}/\{0\}$ tale che $(c, \phi(n)) = 1$ e sia $d \in \mathbb{N}/\{0\}$ un inverso di c modulo $\phi(n)$ (ovver $d > 0$ e $d \in [c]^{-1}_{\phi(n)}$), allora P_c è una funzione invertibile e vale $P_c^{-1} = P_d$

$$P_d = P_c^{-1} \Leftrightarrow \begin{array}{ll} p_d(P_c(\alpha)) = \alpha & \forall \alpha \in (\mathbb{Z}/_n\mathbb{Z})^* \\ p_c(P_d(\beta)) = \beta & \forall \beta \in (\mathbb{Z}/_n\mathbb{Z})^* \end{array}$$

Corollario: Siano $a, c \in \mathbb{Z}$ tale che $(a, n) = 1$ e $c > 0$. Considero la seguente congruenza in $x \in \mathbb{Z}$

$$x^c \equiv a(mod\ n)$$

Sia S l'insieme delle soluzioni della precedente congruenza, ovvero:

$$S := \{x \in \mathbb{Z} \mid x^c \equiv a(mod\ n)\}$$

allora se $(c, \phi(n)) = 1$ e $d > 0$ con $d \in [c]^{-1}_{\phi(n)}$, Allora

$$S = [a^d]_n = \{a^d + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}$$

Crittografia a chiave pubblica

Supponiamo che A voglia comunicare con B mediante RSA:
B pubblica $c, n \in \mathbb{Z}/\{0\}$, c chiave di codifica e n modulo tale che $(c, \phi(n)) = 1$. A userà l'alfabeto $(\mathbb{Z}/_n\mathbb{Z})^*$. Se A comunica $\alpha \in (\mathbb{Z}/_n\mathbb{Z})^*$, allora calcola α^c e lo invierà. Allora B $(c, \phi(n)) \to d > 0, d \in [c]^{-1}_{\phi(n)}$ con d chiave di decifratura. Quindi $\beta \to \beta^d = \alpha$

11 Eleventh week

Grafi: Dato un insieme V, indichiamo $\binom{V}{2}$ l'insieme i cui elementi sono tutti sottoinsiemi di V con 2 elementi, ovvero:

$$\binom{V}{2} := \{A \in 2^V \mid |A| = 2\}$$

Vale la formula:

$$|\binom{V}{2}| = \binom{|V|}{2} = \frac{|V|!}{2!(|V|-2)!} = \frac{|V|(|V|-1)}{2}$$

Def: Un grafo G è una coppia (V, E), dove V è un'insieme non vuoto detto *insieme dei vertici di* G e E è un sottoinsieme di $\binom{V}{2}$ detto *insieme dei lati di* G.
Se $G = (V, E)$ è un grafo ed $e = \{v_1, v_2\} \in E$, cioé un lato di G, allora diciamo che v_1 e v_2 sono degli estremi di e

Se G è un grafo, allora $V(G)$ indica l'insieme dei vertici e $E(G)$ l'insieme dei lati di G. Se $G = (V, E)$ è un grafo ed $e = \{v_1, v_2\} \in E$, cioé un lato di G, allora diciamo che v_1 e v_2 sono gli *estremi* di e ed anche che e congiunge v_1 e v_2

Esempi notevoli

- Per ogni $n \in \mathbb{N}$, definiamo il *cammino* P_n di lunghezza n come il seguente grafo

$$V(P_n) = \{0, 1, ..., n\} \ E(P_n) := \varnothing \text{ se } n = 0$$
$$E(P_n) := \{\{i, i+1\} \in \binom{V(P_n)}{2}\}$$

- P_∞ il cammino infinito
- Per ogni $n \in \mathbb{N}$ con $n \geq 3$, il *ciclo* di lunghezza n è definito:

$$V(C_n) = \{1, 2, ..., n\} \ E(C_n) = \{\{i, i+1\} \in \binom{V(C_n)}{2}\} \cup \{\{1, n\}\}$$

- Per ogni $n \in \mathbb{N},\ n \geq 1$, il *grafo completo* di n vertici, denotato con k_n, è definito:

$$V(k_n)_: = \{1, 2, ..., n\},\ E(kn) := \binom{V(kn)}{2}$$

Sottografi e sottografi indotti
Siano $G = (E, V)$ e $G^I = (E^I, V^I)$ due grafi. Diremo che G^I è un sotto grafo di G se $V^I \subset V$ e $E^I \subset E$

Se G^I è sottografo di G vale:

$$E^I = \{e \in E \mid e = \{v_1, v_2\}, v_1 \in V^I, v_2 \in V^I\}$$

allora G^I si dice *sotto grafo* di G *indotto* da V^I e si indica con il simbolo $G[V^I]$ 13/05/21

Morfismi
Siano $G = (V, E)$ e $G^I = (V^I, E^I)$ due grafi, e $f : V \to V^I$ una funzione iniettiva. Allora si dice morfismo da G a G^I se vale:

$$\forall v_1, v_2 \in V,\ \{v_1, v_2\} \in E \Rightarrow \{f(v_1), f(v_2)\} \in E^I$$

Se $f : V \to V^I$ è un morfismo da G a G^I, allora scriveremo $f : G \to G^I$

Oss: Siano $G = (V, E)$ e $G^I = (V^I, E^I)$ due grafi, sia $f : G \to G^I$. Per ogni $e = \{v_1, v_2\} \in E$, allora:

$$f(e) = \{f(v_1, v_2)\} \in \binom{V^I}{2}$$

Definiamo $f(E) := \{f(e) \in \binom{V^I}{2} \mid e \in E\}$, segue che:

$$f(E) \subset E^I$$

Dunque f è un morfismo solo se $f(E) \subset E^I$

Isomorfinsmo
Diciamo che f è un isomorfinsmo da G in G^I se:

- f è bigiettiva
- f è morfismo da G in G^I
- $f^{-1} : V(G) \to V(G)$ è un morfismo da G^I in G. Se esiste un isomorfismo, allora G si dice isomorfo a $G^I \Rightarrow G \cong G^I$

Prop: Siano G, G^I due grafi e $f : V \to V^I$ una funzione. f è isomorfismo da G in G^I se e solo se:

- f è bigiettiva
- $f(E) = E^I$, ovvero $\forall e \in \binom{V}{2},\ e \in E \Leftrightarrow f(e) \in E^I$

Passeggiate, cammini e cicli
Sia G una successione finita ordinata di vertici di G. Allora si dice:

- Passeggiata in G, se $n = 0$ oppure $n \geq 1$ e $\{v_i, v_{i+1}\} \in E \quad \forall i \in \{0, 1, ..., n-1\}$
- Cammino in G, se è una passeggiata in G e $v_i \neq v_j \quad \forall i, j \in \{0, 1, ..., n\}$
- Ciclo in G se è una passeggiata in G, $v_0 = v_n$ e $n \geq 3$, $v_i \neq v_j$

Se $(v_0, v_1, ..., v_n)$ è una passeggiata in G, allora n è detto lunghezza, $n = l(G)$

Def
Sia G un grafo e siano $v, w \in V$. Sono *congiungibili* in G con passeggiata se esiste una passeggiata in G della seguente forma: $(v_0, v_1, ..., v_n)$

12 Dodicesima settimana

Congiungibilità
Sia $G = (V, E)$ e siano $v, w \in V$. Diciamo che v e w sono congiungibili con un cammino se esiste un cammino $(v_0, v_1, ..., v_n)$ tale che $v_0 = v$ e $v_n = w$

Prop: Sia $G = (V, E)$ e siano $v, w \in V$. Allora v e w sono congiungibili con un cammino se e soltanto se lo sono con una passeggiata

Oss: Dato un grafo $G = (V, E)$ e $v, w \in V$ diciamo che v e w sono congiungibili se lo sono per cammini o passeggiate

Prop: Sia $G = (V, E)$ e sia $\sim$ la relazione binaria su V indetta dalla nozione di congiungibilità in G: $\sim \in \mathcal{P}(V \times V)$ è definita ponendo $v \sim w$ se v è congiungibile a w in G. Allora $\sim$ è una relazione di equivalenza in V. Allora $\sim$ è una relazione di equivalenza in V

Def: Sia $G = (V, E)$ e sia $\sim$ la relazione di congiungibilità su V, indichiamo con $\{V_i\}_{i\in I}$ l'insieme di tute le $\sim$ classi d'equivalenza.I sotto grafi $\{G[V_i]\}_{i\in I}$ indotti da G su V_i si dicono *componenti connesse* di G

Grafi connessi
Un grafo si dice *connesso* se possiede una sola componente connessa. Altrimenti si definisce *sconnesso*

Oss:

- Sia G un grafo, allora G è connesso se e solo se ogni coppia di vertici di G è congiungibile in G
- Ogni componente connessa di G^I di G è un grafo connesso

Prop: Siano G e G^I due grafi e sia $f : G \to G^I$ un morfismo. Valgono:

- se $v, w \in V(G)$ tale che v è raggiungibile a w in G, allora $f(w)$ e $f(v)$ sono congiungibili in G^I
- Se f è un isomorfinsmo, allora $v \sim w$ in $G \Leftrightarrow f(v) \sim f(w)$ in G^I

Corollario: Siano G e G^I due grafi isomorfi, siano $\{G_i\}_{i\in I}$ le componenti connesse di G e $\{G^I_j\}_{j\in I}$ le componenti connesse di G^I. Allora G e G^I hanno lo stesso numero di componenti connesse e tali componenti sono 2 a 2 isomorfe. Più precisamente, $\exists\varphi : I \to J$ una bigezione talche che $G_i \cong G^I_{\varphi(i)} \quad \forall i \in I$

Corollario: Due grafi isomorfi sono entrambi connessi o non connessi

Relazione fondamentale tra gradi dei vertici e numero dei lati di un grafo finito

Def: Un grafo G è detto finito se ha un numero finito di vertici

Oss: Un grafo finito possiede anche un numero finito di lati.
Viceversa è falso, esistono grafi con infiniti vertici e finiti lati.

Def: Sia G un grafo finito e sia $v \in V$. Definiamo il grado $deg_G(v)$ di v in G ponendo:

$$deg_G(v) := |\{e \in E \mid v \in E\}|$$

(o numero di lati che escono da v)

20/05/21

Prop: Sia $G = (V, E)$ un grafo finito. Allora:

$$\sum_{v \in V} \; deg_G(v) = 2|E|$$

lemma delle strette di mano: In un grafo finito, il numero di vertici di grado dispari è pari

Def: Sia $G = (V, E)$ un grafo finito con n vertici, definiamo con *score* di G, con il simbolo $score(G)$, come la n-upla di interi equali ai gradi dei vertici di G.
Diremo che lo score è in *forma canonica* se la successione è ordinata in modo non decrescente

Prop: Siano G e G^I due grafi isomorfi, vale:

$$score(G) = score(G^I)$$

Il contrario è falso, esistono grafi non isomorfi ma con score pari.

Grafi 2-connessi e grafi di Hamilton

Def: Sia $G = (V, E)$ un grafo finito con almeno 2 vertici e sia $v \in V$. definitamo $G - v$ il grafico ottenuto da G rimuovendo v, ponendo:

$$V(G - v) := V/\{v\}, \quad E(G - v) := \{e \in E, v \notin V\}$$

Def: un grafo G si dice *2-connesso* se ha almeno 3 vertici e $\forall v \in V(G)$, $G - v$ è connesso

Lemma: ogni grafo 2-connesso è anche connesso. il contrario non vale.

Def: Sia G un grafo. UN ciclo in G che attraversa tutti i vertici di G è detto *ciclo Hamiltoniano.* Se G ammette almeno un ciclo Hamiltoniano è detto *grafo Hamiltoniano*

Oss: Un Hamiltoniano è sempre un grafo finito e ha almeno 3 vertici

Lemma: Un grafo Hamiltonianoè anche 2-connesso

13 thirteenth week

Foglia: sia $G = (V, E)$ un grafico e sia $v \in V$. Diciamo che v è una *foglia* di G se $deg_G(v) = 1$

Lemma: Un grafo 2-connesso o hamiltoniano non possiede foglie

Lemma: Siano G e G^I due grafi isomorfi. Valgono le seguenti affermazioni:

- G è 2-connesso solo se lo è anche G^I
- G è Hamiltoniano solo se lo è anche G^I

Note: per determinare l'isomorfismo di un grafo, possiamo verificare alcune caratteristiche:

- $score(G) = score(G^I)$
- G e G^I sono entrambi connessi o meno. Il numero di componenti connesse è lo stesso
- entrambi sono 2-connessi o meno
- entrambi sono Hamiltoniani o meno
- hanno lo stesso numero di sottocili
- scelto un vertice di G di grado k, allora tutti k vertici collegati a $f(v)$ devono avere lo stesso score di quelli collegati a v

Se tutte queste regole sono rispettate non per forza i due grafi sono isomorfi. Il modo pià accurato per determinare l'isomorfismo è di generarne uno a mano

Lemma: Sia $n \in \mathbb{N}$ con $n \geq 1$, allora se $G = (V, E)$ è un grafo con n vertici, vale:

$$deg_G(v) \leq n - 1 \qquad \forall v \in V$$

Corollario: Sia $n \in \mathbb{N}$ con $n \geq 1$ e sua $d = (d_1, ..., d_n) \in \mathbb{N}^n$ ordinato. Se $d_n > n - 1$ allora nessun grafo avrà d come score (ost 1)

Oss: Siano $n, m \in \mathbb{N}/\{0\}$ e sia $d \in \mathbb{N}^{n+m}$ in forma $(0_1, ..., 0_m, d_1, ..., d_n)$ ordinata. Definiamo d^I come d senza gli zero. Anche d^I è score del grafo

Lemma: Siano $n, k \in \mathbb{N}/\{0\}$ tale che $k < n$ e $h := n - k$ e d score in forma $(d_1, ..., d_h, n - 1_1, ..., n - 1_k)$ ordinata. Se $d_1 < k$ allora d non è score di un grafo (ost 2) 27/05

Lemma: Sia $n \in \mathbb{N}$ con $n \geq 3$, sia $d = (d_1, ..., d_n) \in \mathbb{N}^n$ ordinato e sia L:

$$L := |\{i \in \{1, ..., n-2\} \mid d_i \geq 2\}|$$

Se $L < d_{n-1} + d_n - n$, allora d non è score di un grafo (ost3)

Lemma: Sia $n \in \mathbb{N}/\{0\}$ e $d \in \mathbb{N}^n$ un vettore ordinato tale che $d_1 \leq ... \leq d_n \leq 2$. Vale:

- se $d = (0_1, ..., 0_{n-1}, 2)$ oppure $n \geq 2$ e $d = (0_1, ..., 0_{n-2}, 2, 2)$, allora non è un grafo
- Se $d = (0, ..., 0)$ allora d è lo score di un grafo con n vertici isolati. Se esiste $m \in \mathbb{N}$ tale che $n \geq m \geq 3$ e $d = (0_1, ..., 0_{n-m}, 2_1, ..., 2_m)$ allora d è lo score del grafico con $n - m$ vertici isolati e m vertici in ciclo

Se per $k \in \mathbb{N}$ volte lo score è pari a 1 allora il grafo è formato da $k/2$ segmenti

Corollario: Se il numero di $d = 1$ è pari, allora d è lo score di un grafo solo se d non ha le forme:

$$d = (0, ..., 0, 2) \quad \text{oppure} \quad d = (0, ..., 0, 2, 2)$$

Teorema dello score
Sia $n \in \mathbb{N}$ con $n \geq 2$ e $d \in \mathbb{N}^n$ tale che $d_1 \leq ... \leq d_n \leq n - 1$. definiamo il vettore ponendo:

$$d_i^I \begin{cases} d_i & se\ i < n - d_n \\ d_i - 1 & se\ i > n - d_n \end{cases} \qquad \forall i \in \{1, ..., n-1\}$$

d è lo score di un grafo solo se lo è d^I

14 fourteenth week

Alberi
Un grafo si dice albero se è connesso e senza cicli. Una foresta è un grafo senza cicli

Teorema: Sia $T = (V, E)$ un grafo. Le seguenti affermazioni sono equivalenti:

1. T è un albero
2. Per ogni $v,\ v^I \in V$, esiste un unico cammino in T che congiunge v a V^I
3. T è connesso e, per ogni $e \in E$, il grafo $T - e$ è sconnesso
4. T non ha cicli e, per ogni $e \in \binom{V}{2} \setminus E$, il grafo $T+e$, definito ponendo $T+e := (V, E \cup \{e\})$, ha almeno un ciclo
5. T è connesso e soddisfa la seguente formula di eulero:

$$|V| - 1 = |E|$$

Lemma: Sia T un albero finito avente almeno 2 vertici. Allora T ha almeno 2 foglie

Osservazione: Il precedente lemma non vale se l'albero è infinito

Teorema: La connessione di T non può essere omessa per l'applicazione della formula di eulero

Corollario: Sia $n \in \mathbb{N} \setminus \{0\}$ e sia $d \in \mathbb{N}^n$. Allora esiste un albero con score d se e solo se:

$$n - 1 = \tfrac{1}{2}\left(\sum^n d_i\right)$$