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: $x \rightarrow^f y \rightarrow^g z \Rightarrow g(f(x)) = z \Rightarrow gof(x) = z$

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

$$n = mq + r$$
$$0 \leq n < |m|$$

(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)

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

$$
\Downarrow
$$

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

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:

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

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

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

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

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

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:

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