$\boxed{n=11}$ $x=2;\ y=2,\ z=7$

$(2,2,7)$ $\quad 2+2+7=11$

la vedo come

$\underbrace{11}_{2}0\underbrace{11}_{2}0\underbrace{1111111}_{7}$ IDEA

Per $n=11$ è come contare le stringhe binarie di lunghezza 13 con undici "1" e due "0".

Sono $\binom{13}{2}$.

Es. n arbitrario? Quante (x,y,z) con $x+y+z=n$.

Soluzione: $\binom{n+2}{2}$

$\underbrace{\underbrace{111}_{x}0\underbrace{1111}_{y}0\underbrace{111}_{z}}_{n+2}$

Gli 1 sono $x+y+z=n$

Soluzione 2: $\binom{n}{k} = \binom{n}{n-k} = \binom{n+2}{n}$

Quante soluzioni di $x+y+z+w=17$?

$\underbrace{111111}_{x}\ 0\ \underbrace{11111111}_{y}\ 0\ \underbrace{111111111}_{z}\ 0\ \underbrace{111111}_{w}$

$\boxed{\text{PARTIZIONI}}$ $\binom{17+3}{3}$

Poker 52 carte $= 13 \times 4$

1, 2, 3 . . . . . 10 J Q K

Full $\{\underbrace{2^{\heartsuit}}\ \underbrace{2^{\diamondsuit}}\ \underbrace{2^{\spadesuit}}\ \underbrace{1^{\spadesuit}}\ \underbrace{1^{\heartsuit}}\}$

non ordinati

Quanti full?

13 valori per il tris. $\quad 13 \cdot 4 \cdot 12 \cdot \binom{4}{2}$

valori per il TRIS $\quad$ semi del TRIS $\quad$ valore coppia

Probabilità con Full $= \dfrac{\text{Casi favorevoli}}{\text{Casi possibili}} = \dfrac{13 \cdot 4 \cdot 12\binom{4}{2}}{\binom{52}{5}}$

CALCOLO COMBINATORIO

GELATI

LUN 16 Ricev. Matteo Serventi
Sala Riunioni
Ore 16 Studio 216 Mat.

22/10/14

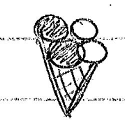
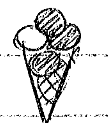
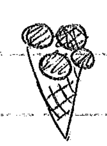
12 frutta
8 non frutta

a) In quanti possibili coni con 4 gusti? $\binom{20}{4}$

b) 4 gusti, esattamente 2 di frutta. $\binom{12}{2} \cdot \binom{8}{2}$

b) 4 gusti, almeno 2 di frutta cioè 2 o 3 o 4

$$\binom{12}{2}\binom{8}{2} + \binom{12}{3} \cdot \underbrace{\binom{8}{1}}_{8} + \binom{12}{4}\underbrace{\binom{8}{0}}_{1}$$

(?) $\binom{12}{2}\binom{18}{2}$ → SBAGLIATO: problema del doppio conteggio

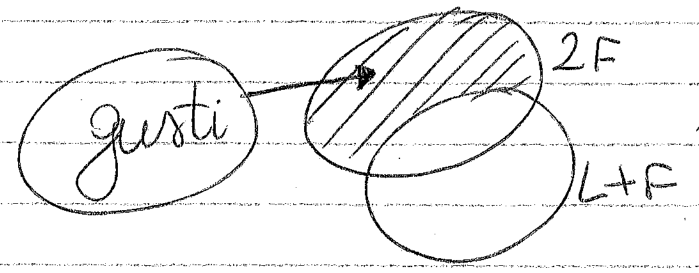
c) 4 gusti, almeno 2 frutta, ma non insieme limone e fiordilatte.

$$\left[\binom{12}{2}\binom{8}{2}+\binom{12}{3}\underbrace{\binom{8}{1}}_{8}+\binom{12}{4}\underbrace{\binom{8}{0}}_{1}\right]-$$

quelli con limone e fiordilatte

$\binom{18}{2}$ ↓ sbagliato

↳ almeno 2 di frutta



Mi interessano quelli con sia limone, sia fiordilatte, ma con almeno 2 frutti.

LIM, FIOR, FR, FR → $\binom{11}{2}$ ⊕
LIM, FIOR, FR, ¬FR → $11 \cdot 7$

(11 ↓ fr, 7 ↓ ¬fr)

Risposta

$$\left[\binom{12}{2}\binom{8}{2}+\binom{12}{3}\binom{8}{1}+\binom{12}{4}\binom{8}{0}\right]-\binom{11}{2}+11\cdot 7$$

Scelte successive
$\boxed{\text{SI MOLTIPLICA}}$

(LF) FR FR
↳ è già una scelta

$|A \cup B| = |A| + |B| - |A \cap B|$
$|A \cap B| = -|A \cup B| + |A| + |B|$

Fibonacci $F_0 = 1$, $F_1 = 1$ $\quad F_{n+2} = F_{n+1} + F_n$

F_0	F_1	F_2	F_3	F_4	F_5	F_6
0	1	1	2	3	5	8

$F_n = ?$ formula?

$F_n = n^2 + 3n + 1$?
$F_n = n^3 + 5n^2$?
$F_n = 2^n$?

Digressione DIFFERENZA CON ESPONENZIALE (non cala mai)

2^n 1 2 4 8 16 32
differenze: 1 2 4 ~~8~~ 8 16

DIFFERENZE DI FIBONACCI

F_n | 0 1 1 2 3 5 8 13
differenze: 1 0 1 1 2 3 5

il comportamento è simile a quello dell'esponenziale

$F_n = 2^n$?
3^n ?
$\emptyset$
$F_n = 3^n - 2^n$?
$F_n = 3^n - 5 \cdot 2^n$

PRE-FIBONACCI

ci occupiamo solo di (*) $F_{n+2} = F_{n+1} + F_n$

$f_0 = ?$, $f_1 = ?$

Tento $f_n = c^n$?

Come scelgo c?

$c = 2?$ $\quad 2^{n+2} \neq 2^{n+1} + 2^n$

Voglio $c^{n+2} = c^{n+1} + c^n \quad \forall n$

Divido per c^n con $c \neq 0$

$$c^2 = c + 1 \Rightarrow c^2 - c - 1 = \emptyset$$

POLINOMIO CARATTERISTICO DELLA SUCCESSIONE DI FIBONACCI $\quad p(x) = x^2 - x - 1$

Le radici di $p(x)$ sono $\dfrac{1 \pm \sqrt{1+4}}{2}$

$\alpha = \dfrac{1+\sqrt{5}}{2} \quad \beta = \dfrac{1-\sqrt{5}}{2}$

Primo Tentativo $\boxed{F_n = \alpha^n}$

Sostituisco nella ⊛

$\alpha^{n+2} = \alpha^{n+1} + \alpha^n$

Semplifico dividendo per α^n

$\alpha^2 = \alpha + 1$

$\alpha^2 - \alpha - 1 = 0 \rightarrow$ polinomio caratteristico

Se pongo $F_n = \alpha^n$ oppure $F_n = \beta^n$ la ⊛ è soddisfatta, ma non le condizioni iniziali $F_0 = 0$, $F_1 = 1$.

Provo allora con una combinazione lineare

Secondo Tentativo

$$f_n = \underbrace{A\alpha^n + B\beta^n}_{\text{PRE-FIBONACCI}}$$

Devo scegliere A, B.

La ⊛ continua ad essere soddisfatta:

$$(A\alpha^{n+2} + B\beta^{n+2}) = (A\alpha^{n+1} + B\beta^{n+1}) + (A\alpha^n + B\beta^n)$$

$$\Longleftrightarrow$$

$$A(\alpha^{n+2} - \alpha^{n+1} - \alpha^n) + B(\beta^{n+2} - \beta^{n+1} - \beta^n) = \emptyset \,?$$

$\alpha^2 = \alpha + 1 \Rightarrow \alpha^2 - \alpha - 1 = 0 \Rightarrow \alpha^{n+2} - \alpha^{n+1} - \alpha^n = 0$

Controllo le condizioni iniziali $\quad F_0 = 0 = A\alpha^0 + B\beta^0 = A + B$

$F_1 = 1 = A\alpha + B\beta = A\left(\frac{1+\sqrt{5}}{2}\right) + B\left(\frac{1-\sqrt{5}}{2}\right)$

Ottengo il sistema:

$$\begin{cases} A + B = 0 \\ A\alpha + B\beta = 1 \end{cases} \quad \begin{cases} B = -A \\ A\alpha - A\beta = 1 \end{cases} \quad \begin{cases} \ldots \\ A(\alpha - \beta) = 1 \end{cases} \quad \begin{cases} \ldots \\ A\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) = 1 \end{cases}$$

$$\begin{cases} B = \left(-\frac{1}{\sqrt{5}}\right) \\ A(\sqrt{5}) = 1 \quad A = \left(\frac{1}{\sqrt{5}}\right) \end{cases}$$

$$F_n = \left(\frac{1}{\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(-\frac{1}{\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n$$

28/10

Fibonacci $F_0=0$, $F_1=1$, $F_{n+2}=F_{n+1}+F_n$

abbiamo visto che

$$F_n=\underbrace{\left(\frac{1}{\sqrt5}\right)}_{A}\underbrace{\left(\frac{1+\sqrt5}{2}\right)}_{\alpha}^{n}+\underbrace{\left(-\frac{1}{\sqrt5}\right)}_{B}\underbrace{\left(\frac{1-\sqrt5}{2}\right)}_{\beta}^{n}$$

Dimostro $\forall n\ P(n)$: induzione su n.

Dimostriamo $P(\emptyset)$: $F_0=\left(\frac{1}{\sqrt5}\right)\alpha^0+\left(-\frac{1}{\sqrt5}\right)\beta^0=0$ $\boxed{ok}$

$P(1)$: $F_1=1$, $F_1\overset{?}{=}\left(\frac{1}{\sqrt5}\right)\alpha^1+\left(-\frac{1}{\sqrt5}\right)\beta^1=\left(\frac{1}{\sqrt5}\right)(\alpha-\beta)$

$P(2)$: $\ldots=\left(\frac{1}{\sqrt5}\right)\left(\frac{1+\sqrt5}{2}-\frac{1-\sqrt5}{2}\right)=\left(\frac{1}{\sqrt5}\right)\sqrt5=1$

$n\geq 0$

$P(n+2)$! $F_{n+2}=\left(\frac{1}{\sqrt5}\right)\alpha^{n+2}+\left(-\frac{1}{\sqrt5}\right)\beta^{n+2}$?

Cosa sappiamo?

$$F_{n+2}\overset{def}{=}F_{n+1}+F_n=\left(\frac{1}{\sqrt5}\alpha^{n+1}+\left(-\frac{1}{\sqrt5}\right)\beta^{n+1}\right)+\left(\frac{1}{\sqrt5}\alpha^{n}+\left(\frac{1}{\sqrt5}\right)\beta^{n}\right)$$

IP induttiva

P(n+1) P(n)

$$=\frac{1}{\sqrt5}\alpha^n\underbrace{(\alpha+1)}_{\alpha^2}+\left(-\frac{1}{\sqrt5}\right)\beta^n\underbrace{(\beta+1)}_{\beta^2}=\frac{1}{\sqrt5}\alpha^{n+2}+\left(-\frac{1}{\sqrt5}\right)\beta^{n+2}$$

Ho dimostrato $P(n+2)$ dando per buono $P(n+1)$ e $P(n)$.

Ho dimostrato $\forall n\ P(n+1)\wedge P(n)\to P(n+2)$

anche $P(0)$ anche $P(1)$

$\to P_0, P_1$

$P_0\wedge P_1\to P_2$

$P_1\wedge P_2\to P_n$

$P_2\wedge P_3\to P_4$

P_4

INDUZIONE FORTE

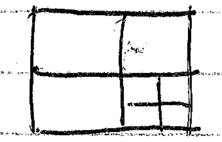
Induzione

Posso dividere un quadrato in 103 quadrati più piccoli e in n?

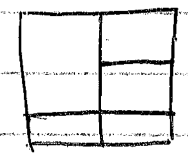
Figura ⇒ lo so.

Fare con n=7.

n=5? NO

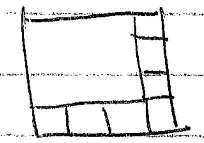


7



6

$\to P(n)\to P(n+5)$



8

$\to P(n)\to P(n+7)$

Invento l'ipotesi $P(n)\equiv$ un quadrato si può dividere in n quadrati.

L'ho verificata per n=4, 6, 7, 8.

Cerco di dimostrare $(\forall n\geq 6)\ P(n)$.

Lo faccio per induzione forte.

Prendo un $k\geq 6$ cerco di ottenere $P(k)$.

Prendo $k\geq 9$.

6 7 8 9 10 11 12 13

Per induzione forte mostro $\forall n\geq 6\ P_n$.

Ig così $n = 6, 7, 8$ li faccio a mano
Se $k \geq 9$ mostro $P(k)$, suppongo per ipotesi induttiva che siano veri $P(m)$ per $6 \leq m < k$.
Mi serve solo $m = k-3$.

$k \geq 9 \Rightarrow k-3 \geq 6$

$P(k-3)$ posso supporlo vero per ipotesi induttiva e siccome so che $\forall m (P(m) \rightarrow P(m+3))$

$P(k-3) \Rightarrow P(k)$
quindi supp. $P(k-3)$ vero ottengo $P(k)$.
Per induzione $\forall k \geq 6 \; P(k)$.
Primi 2, 3, 5, 7, 11, 13, 17, 19, 23, 29

Primi se $p > 1$ e $\forall x\, y \in \mathbb{Z} (P = xy \rightarrow x = 1 \vee y = 1)$
Quanti sono i divisori di
$\underbrace{2^{10} \cdot 3^{13} \cdot 17^{19} \cdot 13^{20}} = n$ → elenco qualunque

x divisore di y se $\exists k \in \mathbb{Z} \;\; xk = y$

Come sono fatti i divisori di n?

Sono del tipo $2^a \cdot 3^b \cdot 17^c \cdot 13^d$ con $a \leq 10, b \leq 13, c \leq 19, d \leq 20$.

E' come contare le quadruple con queste caratteristiche:
(a, b, c, d) sono $11 \cdot 14 \cdot 20 \cdot 21$

9.14 p 81 30 studenti devono essere distribuiti in 3 classi A, B, C.
Quanti modi per farlo supponendo (1) ogni classe deve contenere 10.

$$\overset{A}{\binom{30}{10}} \overset{B}{\binom{20}{10}} \overset{C}{\binom{10}{10}}$$

Se semplicemente li divido in 3 gruppi di 10 senza distribuirli nelle classi

$\langle \{\}, \{\}, \{\} \rangle$

$$\frac{\binom{30}{10}\binom{20}{10}\binom{10}{10}}{3!}$$

Quante funzioni iniettive ci sono da $[k] \rightarrow [n]$?
Ho n scelte per $f(1)$

$[k] = \{1, 2, \ldots\ldots, k\}$

$n-1$ $\quad f(2)$

$n-2$ $\quad f(3)$

$\vdots$

$n-k+1 - n-(k-1)$ $\quad f(k)$

$n(n-1)(n-2)\ldots(n-(k-1)) = \frac{n!}{(n-k)!}$ $\;\; [k] \rightarrow [n]$ iniettive

"
taglio

I sottoinsiemi di $[n]$ con k elementi

$\mathcal{P}_k([n])$ sono $\binom{n}{k} = \frac{n!}{(n-k)!\,k!}$

Chiamiamo

$C_k^n = |\mathcal{P}_k([n])| = |\{A \mid A \subseteq [n] \wedge |A| = k\}|$

$C_k^n = ?$

$I_k^n = \{f \mid f: [k] \rightarrow [n]\}$ iniettive

Per scegliere una $f: [k] \rightarrow [n]$ iniettiva posso fare così:

① Scelgo $Im(f) \subseteq [n]$ C^n_k modi

② fissata l'immagine $\{a_1,\dots,a_k\} \subseteq [n]$ scelgo dove

$f:[k] \to \{a_1 \dots a_k\}$ è iniettiva

Totale $I^n_k = C^n_k \cdot k!$

$$\frac{n!}{(n-k)!} \quad \left[\frac{n!}{(n-k)!\,k!}\right]\cdot k!$$

③ 30 studenti nelle classi A, B, C. Quanti modi?

Come contare le $f:[30]\to\{A,B,C\}$.

variante Ogni classe deve avere almeno 1 studente

$3\,3\,3 \dots 3 = 3^{30}$

S_A = le scelte in cui la classe A rimane vuota

2^{30} assegnazione: $[30]\to\{B,C\}$

$S_B = \dots = 2^{30}$ tutte le funzioni

$S_C = \dots = 2^{30}$ $f:[30]\to\{A,B,C\}$

tranne quelle $S_A\cup S_B \cup S_C$

$\underset{\text{tutte}}{3^{30}} - 2^{30}-2^{30}-2^{30}+3$

FAGIOLO: 1° giorno alto 1 cm
2° giorno $1+1/30$
3° giorno $(1+1/30) + 1/30\,(1+1/30)$
Dopo un anno è alto ≥ 40 metri.
Dopo n giorni quanto è alto?
Usiamo Bernoulli →

Bernoulli $(1+x)^n \overset{P(n)}{\geq} 1+nx$ $(x>-1)$

Induzione su n

$n=0$ $(1+x)^0 = 1 \geq 1+0x$

$n+1$ $(1+x)^{n+1} = (1+x)^n(1+x)$: $P(n)+1$

$(1+x)^n \underset{P(n)}{\geq} (1+nx)$

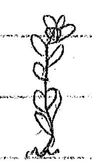
$$(1+x)^{n+1} = \underline{(1+x)^n}(1+x) \geq \underline{(1+nx)}(1+x) \overset{?}{\geq} 1+(n+1)x$$

$(1+x)^n \geq 1+nx$

$$(1+nx)(1+x) = 1+x+nx+nx^2 = 1+(n+1)x+nx^2 \geq 1+(n+1)x$$

Ho dimostrato solo:

$\forall n[P(n)\to P(n+1)]$, $P(0)$ $\xrightarrow{\text{per induzione}}$ $\forall n\, P(n)$



Fagiolo alto 1 cm.

Se al giorno n è alto x

$n+1$ è alto $x + \frac{1}{30}x = x\left(1+\frac{1}{30}\right)$ giorno n

$1 = \left(1+\frac{1}{30}\right)^0, \left(1+\frac{1}{30}\right), \left(1+\frac{1}{30}\right)\left(1+\frac{1}{30}\right) \dots \left(1+\frac{1}{30}\right)^n$ cm

$n=365$ $\left(1+\frac{1}{30}\right)^{365} \geq 1 + 365\,\frac{1}{30}$ cm

NON BASTA.

$$\left(1+\frac{1}{30}\right)^{365} \geq \left(1+\frac{1}{30}\right)^{30\cdot 12} = \left(\underbrace{\left(1+\frac{1}{30}\right)^{30}}_{\text{APPLICO BERNOULLI}}\right)^{12}$$

$$\underset{\text{Bernoulli}}{\geq} \left(1+30\,\frac{1}{30}\right)^{12} = 2^{12} = 2^6\cdot 2^6 = 64\cdot 64 = 4096$$

cm
$\Downarrow$
40 m

Quanti anagrammi di ATTILLATO? $\neq 9!$
di ALTO? 4! permutazioni di 4 elementi

LTAO
LATO

Prima faccio gli anagrammi di

$A^1 T^1 T^2 I L^1 L^2 A^2 T^3 O \neq$

$A^2 T^2 T^1 I L^2 L^1 A^1 T^3 O$

$$\frac{9!}{3!\,2!\,2!}$$ 1ª SOL

2a SOL

| A | | | | | | A | | |

$\{3,7\} \subseteq \{1,2,\dots,9\}$

modi di scegliere il ~~... delle~~ posto delle A

$$\binom{9}{2}\binom{7}{3}\binom{4}{2}\binom{2}{1}\binom{1}{1} =$$

A T L I O

$$\frac{9!}{2!\,\cancel{7!}}\;\frac{\cancel{7!}}{3!\,\cancel{4!}}\;\frac{\cancel{4!}}{2!\,\cancel{2!}}\;2! = \frac{9!}{2!\,3!\,2!}$$

$f: \mathbb{N}\times\mathbb{N} \to \mathbb{N}^{\geq 8} = \{5,6,7,8,\dots\}$

$f(x,y) = 3x+5y$ Iniettiva? NO Surgettiva? $\Updownarrow$

$\forall n \geq 8\,(\exists x,y.\ n = 3x+5y)$

$3,5 \to 3\cdot 3+5\cdot 5$
$5,3 \to 3\cdot 5+5\cdot 3$
$0,0 \to 0$
$5,0 \to 3\cdot 5+5\cdot 0$
$0,3 \to 3\cdot 0+5\cdot 3$

5 OK
$6 = 3\cdot 2+5\cdot 0$
$7 = ?$
$8 = 3\cdot 1+5\cdot 1$
$9 = 3\cdot 3+5\cdot 0$
$10 = 3\cdot 0+5\cdot 2$
$11 = 3\cdot 2+5\cdot 1$
$12 = 3\cdot 4+5\cdot 0$

$P(n): \exists x y\,[n = 3x+5y]$

$\underbrace{P(8), P(9), P(10)}$, $P(11)$, $P(12)$ a mano

$P(n) \to P(n+3)$

<u>Principio del minimo</u> Se $A \subseteq \mathbb{N}, A \neq \emptyset \Rightarrow A$ ha un minimo.

Se per assurdo la tesi fosse falsa, esisterebbe il minimo $n \geq 8$ che non riesco a scrivere nella forma $n = 3x+5y$.

$n \neq 8, 9, 10$
$n \geq 11 \Rightarrow n-3 \geq 8 \Rightarrow P(n-3)$ vera

$\uparrow$
n era il minimo

Però so che $P(n-3) \to P(n)$
Quindi è vera anche $P(n)$. ⊠

Quante $f:[20]\to[20]$

a) Assumono almeno un valore ≥ 11

b) Assumono esattamente un valore ≥ 11

...

a) Quante non assumono valori ≥ 11?

È come se $f:[20]\to[10]$ queste sono 10^{20}.

Risposta: $20^{20}-10^{20}$

b) Scelgo un numero $a \geq 11$. 10 modi

Devo mandare $[20]\to\{1,\dots,20\}\cup\{a\}=\{1,2,\dots,10,a\}$

11^{20} modi − quelle che non assumono il numero a $[20]\to[10]$

Risposta $10\cdot[11^{20}-10^{20}]$

a ...

4.8 PAG 42 $H_k=\sum_{i=1}^{k}\frac{1}{i}$

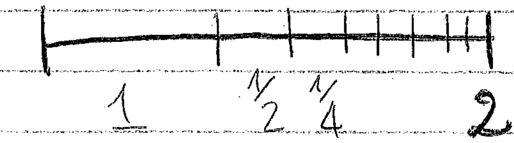
$H_5=\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}$

$H_{2^n}\geq 1+\frac{n}{2}$

$H_8=H_{2^3}\geq 1+3/2$

Digressione

$2=1+1/2+1/4+1/8+1/16\dots+1/2^n+\dots$



Serie armonica

P(0) $H_{2^0}\geq 1+0/2$

OK $H_1=\frac{1}{1}$

P(n+1)? $H_{2^{n+1}}\geq 1+\frac{n+1}{2}$

$H_{2^{n+1}}=\sum_{i=1}^{2^{n+1}}\frac{1}{i}=\sum_{i=1}^{2^n}\frac{1}{i}+\sum_{i=2^n+1}^{2^{n+1}}\frac{1}{i}$

$\underset{P(n)}{\geq}(1+n/2)+\underbrace{\frac{1}{2^n+1}+\frac{1}{2^n+2}+\dots+\frac{1}{2^n+2^n}}_{2^n}$

$2^{n+1}=2^n\cdot 2=2^n+2^n$

$\overset{?}{\geq} 1+\frac{n+1}{2}$ ||

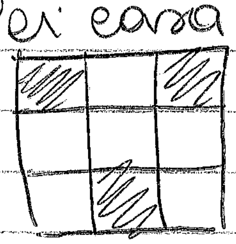
$1+n/2+1/2=1+\frac{n+1}{2}$

Capire se $\frac{1}{2^n+1}+\frac{1}{2^n+2}+\dots+\frac{1}{2^n+2^n}\geq\frac{1}{2}$?

$\geq$

$\underbrace{\frac{1}{2^n+2^n}+\frac{1}{2^n+2^n}+\dots\frac{1}{2^n+2^n}}_{2n}=2^n\left(\frac{1}{2^n\cdot 2}\right)=\frac{1}{2}$

Per casa:



Almeno una riga monocolore.

PAG 47 Trovare una formula per a_n.

$a_1=4,\ a_2=22,\ a_3=82$

$a_n=6a_{n-1}-11a_{n-2}+6a_{n-3}$

$n\geq 4$

$a_4=6\cdot 82-11\cdot 22+6\cdot 4$

Si prova $a_n=x^n$ (tentativo).

Sostituendo $x^n=6x^{n-1}-11x^{n-2}+6x^{n-3}$

$\frac{1}{x^{n-3}}$ $\quad x^3 = 6x^2 - 11x + 6$ polinomio caratteristico $p(x)$

$x^3 - 6x^2 - 11x - 6 = 0$

$(x-1)(x-2)(x-3)$

$p(3) = p(2) = p(1) = 0$

$2^{n-3}\Big(\; 2^3 = 6 \cdot 2^2 - 11 \cdot 2 + 6$

$\qquad 2^n = 6\,2^{n-1} - 11\,2^{n-2} + 6 \cdot 2^{n-3}$

Valem per il 2, 1.

Quasi quasi $2^n = a^n$, non proprio.

$a_n = A \cdot 2^n + B\,3^n + C \cdot 1^n$ Ok

$C = -2$

$A = 3$

$B = 4$

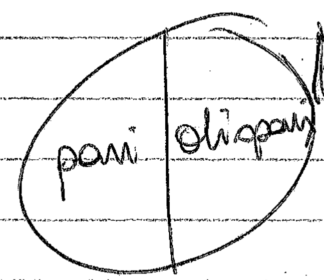
CORREZIONE COMPITO 11/11/14

• Quanti sono i sottoinsiemi di 3 elementi di $\mathbb{N}_{100}$ tali che $a+b+c$ è pari $\{a, b, c\}$

Sol $\{$PARI, PARI, PARI$\}$ oppure $\{$PARI, DISPARI, DISPARI$\}$

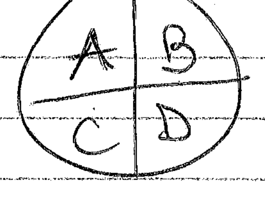
$$\binom{50}{3} + \binom{50}{1} \cdot \binom{50}{2}$$

• Quanti sono i sottoinsiemi di $\mathbb{N}_{100}$ contengono almeno 3 pari?



$$\underbrace{2^{50}}_{\text{modi di scegliere i dispari}} \cdot \Big(\underbrace{2^{50}}_{\text{pari}} - \underbrace{\binom{50}{0} - \binom{50}{1} - \binom{50}{2}}_{\text{scelta dei pari}}\Big)$$

• Quante sono i sottoinsiemi di $\mathbb{N}_{100}$ che contengono esattamente 3 pari ed esattamente un multiplo di 5.



$A = \{x : 2 \nmid x \wedge 5 \nmid x\}$ $\quad |A| = 40$

$B = \{x : 2 \mid x \wedge 5 \nmid x\}$ $\quad |B| = 40$

$C = \{x : 2 \nmid x \wedge 5 \mid x\}$ $\quad |C| = 10$

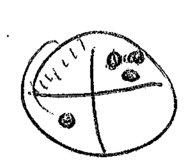
$D = \{x : 2 \mid x \wedge 5 \mid x\}$ $\quad |D| = 10$

$S \subseteq \mathbb{N}_{100}$

Il sottoinsieme può contenere

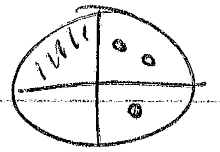
Caso 1 $\;\underbrace{\text{1 elemento di C}}_{10 \text{ modi}}$, $\overbrace{\text{3 pari in B}}^{\binom{40}{3}}$

altri da A. $\Rightarrow 2^{40}$



$10 \cdot \binom{40}{3} \cdot 2^{40}$

Caso 2



$\overset{10}{1 \text{ elemento da } D}$, $\underbrace{2 \text{ elementi da } B}_{\binom{40}{2}}$ e $\underbrace{\text{altri da } A.}_{2^{40}}$

$$10 \cdot \binom{40}{2} \cdot 2^{40}$$

Sol $\quad 10 \cdot \binom{40}{3} \cdot 2^{40} + 10 \cdot \binom{40}{2} \cdot 2^{40}$

• Quante terne ordinate (n, m, u) $n \cdot m \cdot u = 100$

Sol $\boxed{36}$

$n = 2^{a_1} \cdot 5^{b_1}$
$m = 2^{a_2} \cdot 5^{b_2}$
$u = 2^{a_3} \cdot 5^{b_3}$

$\begin{cases} a_1 + a_2 + a_3 = 2 \\ b_1 + b_2 + b_3 = 2 \end{cases}$

$100 = 2^2 \cdot 5^2$

6 scelte per gli a_i

$6 \cdot 6 = 36$

CONGRUENZE

Tra 100 giorni, che giorno è? Oggi è martedì

Ogni 7 gg è martedì

$$\begin{array}{r|l} 100 & 7 \\ 30 & 14 \\ 2 & \end{array}$$

$100 = 7 \cdot 14 + 2$

Tra $7 \cdot 14$ gg è martedì
Resto di 2 gg è giovedì

$$100 \equiv 2 \pmod 7$$

↑
congruo

100 giorni fa, che giorno era?

$$\begin{array}{r|l} -100 & 7 \\ & \end{array}$$

$100 = 7 \cdot 14 + 2$
$-100 = 7 \cdot -14 - 2$

16 settimane fa
-2 giorni = domenica

Di solito vogliamo un resto positivo:

$$0 \leq R \leq 7$$

Quindi $-100 = 7(-15) + 5 \qquad = 7(-14) - 7 + 7 - 2$

toglo una settimana in più

aggiungo dopo la settimana che avevo tolto

TEOREMA $\forall a, b \in \mathbb{Z}$ con $b > 0$ $\exists!\, q$ (quoziente), r tali che $a = b \cdot q + r$ $\qquad \begin{array}{l|l} a & b \\ q & r \end{array}$

$$\wedge \qquad 0 \leq r < b$$

1 caso $a > 0$, $b > 0$

q è un numero unico intero tale che

$$\underbrace{b \cdot q \leq a < b(q+1)}_{b}$$

$r = a - b \cdot q \qquad q = \left\lfloor \frac{a}{b} \right\rfloor$

$b(q+1) - bq = b > \qquad a - bq = r \geq 0$

$a = bq + r$

$-a = b(-q) - r$

$= b(-q) - b + (b - r)$

$= b(-q-1) + \underbrace{(b-r)}_{r'}$

$$\begin{array}{c|c} -a & b \\ \hline b-r & -q-1 \end{array} \qquad \begin{array}{c|c} a & b \\ \hline r & q \end{array}$$

<u>OSS</u> $\begin{array}{c|c} a & b \\ \hline r & q \end{array} \quad \begin{array}{c|c} a & b \\ \hline r & q' \end{array}$

$a|b$ e $c|b \Rightarrow$ stesso resto

$a = bq + r \wedge c = bq' + r \Rightarrow a - c$ multiplo di b

<u>Dim</u>

$(a-c) = (bq + r) - (bq' + r) = b(q - q')$

<u>Teo</u> Se due numeri danno lo stesso resto diviso per b. La loro differenza è multiplo di b.

<u>Viceversa</u> Se $a-c$ è multiplo di b, <u>allora</u> a e c hanno lo $\boxed{\text{stesso}}$ resto diviso per b

<u>Dim</u> $\begin{array}{c|c} a & b \\ \hline r & q \end{array} \quad \begin{array}{c|c} c & b \\ \hline r' & q' \end{array}$

$a = bq + r$

$c = bq' + r' \Rightarrow (a-c) = b(q-q') + (r-r')$

per essere un multiplo di $b \Rightarrow r = r'$

<u>Def</u> $a \equiv c \pmod b \Longleftrightarrow a$ e c danno lo stesso resto divisi per b

$\Longleftrightarrow a - c$ multiplo di b

$b | a-c$

$a \equiv c \quad (7)$

$a+2 \equiv c+2 \quad (7)$

] entrambe multiple di 7

In generale:

$a \equiv c \pmod b \Longleftrightarrow a + x \equiv c + x \pmod b$

$\Updownarrow \qquad\qquad \Updownarrow$

$b | a-c \qquad b | (a-x) - (c-x)$

$\Updownarrow$

$b | a-c$

$a \equiv c (b)$ So che $\exists q (a-c) = bq$

$\Downarrow ? \quad \Uparrow ?$ NON SEMPRE

$ka \equiv kc (b)$ $\quad ka - kc = k(a-c)$

$= kbq$

$= b(kq)$

<u>es</u> in cui non funziona $\Uparrow$?

$6 \cdot 2 \equiv 6 \cdot 3 \pmod 6$

però $2 \not\equiv 3 \pmod 6$

$2 \cdot 2 \equiv 2 \cdot 4 \pmod 4$ — il viceversa
ma $2 \not\equiv 4 \pmod 4$ — non vale sempre.

Ci sono casi in cui si può.

Caso $a \equiv 0 \ (b)$
$\Leftrightarrow b | a$

Teo Se p è primo si può dividere

$ka = kb \pmod p$

$\Downarrow$

$a \equiv b \ (p)$
se $k \not\equiv 0 \ (p)$

$0 \cdot 7 = 0 \cdot 8$
ma $7 \neq 8$

Teo $a \equiv c \ (b) \ \wedge \ a' \equiv c' \ (b)$

$\Longrightarrow a + a' \equiv c + c' \ (b)$

Dim

$a \equiv c \ (b)$

$a + a' \underset{(b)}{\equiv} c + a' \underset{(b)}{\equiv} c' + c$

Esercizio Se $a \equiv c$ e $a' \equiv c'$ allora

$a \cdot a' \equiv c \cdot c'$.

Resto di $\underline{1234567}$ mod 3/9/4/7 — 18/11/14

$7 + 6 \cdot 10 + 5 \cdot 10^2 + 4 \cdot 10^3 + 3 \cdot 10^4 + 2 \cdot 10^5 + 1 \cdot 10^6$

||| (3)

$10 \equiv 1 \ (3)$

$7 + 6 + (5+4) + 3 + (2+1)$
$\ \ \ \ \ \ \equiv 0 \ \ \ \equiv 0 \ \ \ \equiv 0 \ \ \ \equiv 0$

$\boxed{\text{MOD } 3}$

$\to 7 \equiv 1 \ (3)$ ✓

Resto r della divisione di a:b è congruo a mod b

$1 \ (3) \equiv -2 \ (3)$
minor resto positivo

$10 \equiv 1 \ (9)$ $7 + 6 + 5 + 4 + 3 + 2 + 1 \equiv 1 \ (9)$

$\boxed{\text{MOD } 9}$

$\sum_{i=0} a_i 10^i = a_0 + a_1 10 + \underbrace{a_2 10^2 + \ldots + a_m 10^m}_{\text{diventano zero perché tutti multipli di } 10^2}$

$10^2 \equiv 100 = 4 \cdot 25 = \emptyset \ (4)$

$\boxed{\text{MOD } 4}$ $\equiv a_0 + a_1 10 + a_2 10^2 (a_2 + a_3 10 + \ldots + a_m 10^{m-2})$ — raccolgo 10^2
$\underset{(4)}{\equiv} a_0 + a_1 \cdot 10$

$1234567 \equiv 67 \ (4)$
|||
$\underbrace{67 + 100 (12345)}_{\equiv 0 \ (4)}$

quindi $7 + 6 \cdot 10 \ (4) \equiv 7 + 6 \cdot 2 \ (4)$
$\downarrow$
$2 \ (4)$ — $\equiv 7 \ (4) \equiv 3 \ (4)$

$\boxed{\text{MOD 7}}$ TRUCCO $1000 = 7(143) - 1$

$1000 \equiv -1\ (7)$ in (7) i multipli di 7 contano zero

Potremo prendere 6 (positivo più piccolo)

$-1 \equiv 6\ (7)$, ma -1 è più comodo.

$$\sum_{i=0}^{m} a_i 10^i = a_0 + (a_1 \cdot 10 + a_2 \cdot 10^2) + 1000(a_3 + a_4 \cdot 10 + a_5 \cdot 10^2) + 1000^2(a_6 + a_7 \cdot 10 + a_8 \cdot 10^2) + 1000^3(\dots) \text{ etc.}$$

$$\sum_{i=0}^{\lceil m/3 \rceil} 1000^i \underbrace{(a + a\, 10 + a}_{??}$$ scritto in base 1000 → raccolgo 1000

$$\underbrace{1}\,\underbrace{234}\,\underbrace{567} \equiv 1 \cdot 1000^2 + (234)1000 + 567$$ spezzo a in blocchi di 3

$$\underset{(7)}{\equiv} (-1)^2 + 234(-1) + 567$$

$$\underset{(7)}{\equiv} 1 - 234 + 567 \equiv 334 \equiv 3 \cdot 10^2 + 3 \cdot 10 + 4$$

$$\equiv 3 \cdot 3^2 + 3 \cdot 3 + 4 \equiv 3 \cdot 2 + 2 + 4 \equiv 1 + 4 \equiv 5\ (7)$$

$\boxed{\text{MOD 11}}$ $$1234567 \underset{(11)}{\equiv} 7 + 6 \cdot 10 + 5 \cdot 10^2 + 4 \cdot 10^3 + 3 \cdot 10^4 + 2 \cdot 10^5 + 10^6$$

$10 \equiv -1\ (11)$ $$\underset{(11)}{\equiv} 7 - 6 + 5 - 4 + 3 - 2 + 1 \equiv -1 + 5 \equiv 4\ (11)$$

$\boxed{\text{MOD 10}}$ $3^{100} \bmod (10)$?

$$3^{100} = (3 \cdot 3)(3 \cdot 3)(3 \cdot 3) \dots (3 \cdot 3) \equiv 9^{50} \equiv (-1)^{50} \equiv 1$$

$9 \equiv -1\ (10)$

$a \equiv a'(c)$, $b \equiv b'(c)$ $\Rightarrow$ $a + b \equiv a' + b'(c)$, $a \cdot b \equiv a' \cdot b'(c)$

$a \equiv a'(c) \overset{?}{\Rightarrow} 2^a \equiv 2^{a'}(c)$ In generale regola sbagliata

$a \equiv a'(c) \underset{\text{sì}}{\Rightarrow} a^n \equiv a'^n\ (c)$

Ad es. $5 \equiv 2(3)$ sì! $2^5 \equiv 2^2\ (3)$ $\underline{2 \equiv 1(3)}$ NO!

$2^2 \cdot 2^2 \cdot 2^2$ con $2^2 \equiv 1$, $2^2 \equiv 1$, $2^2 \equiv 2$; $2^2 \equiv 1(3)$

(In generale non funziona)

- - - - -

$143x \equiv 7(11)$ Trovare x (TIPICO ESERCIZIO DA ESAME)

Esempio dal libro $\sqrt{1234567} \in \mathbb{N}$?

Se fosse intero, vorrebbe dire che

$\exists x \in \mathbb{N}$ tc $x^2 = 1234567 \rightarrow x^2 \equiv 1234567\ (3)$

$x^2 \equiv 1234567\ (4)$

$\vdots$

$1234567 \equiv 1\ (3)$

x^2 può essere congruo a 1? sì!

Tentativo fallito

(Dim per assurdo → cerco un caso in cui non torna)

$1234567 \equiv 3\ (4)$

x^2 può essere congruo a 3?

$\underbrace{x = 0, 1, 2, 3\ (4)}_{\text{una di queste}}$

$x \equiv 0 \Rightarrow x^2 \equiv 0^2 \equiv 0(4)$ $\underline{x \text{ è } 0 \text{ o } 1}$

$x \equiv 1 \Rightarrow x^2 \equiv 1^2 \equiv 1(4)$

$x \equiv 2 \Rightarrow x^2 \equiv 2^2 \equiv 0(4)$

$x \equiv 3 \Rightarrow x^2 \equiv 3^2 \equiv 9 \equiv 1(4)$

$\forall x \{x^2 \equiv 0 \lor x^2 \equiv 1\}\ (4)$ qualunque sia x, $x^2 \neq 1,2,3,4,5,\dots$

perché se fosse uguale, sarebbe anche $\equiv (4)$

$\left.\begin{array}{l} x^2 \equiv 0 \lor x^2 \equiv 1\ (4) \\ 1,2,3,4,5,6,7 \equiv 3(4) \end{array}\right\}$ se fossero uguali, otterrei un ASSURDO, quindi sono DIVERSI. //

MCD Massimo Comun Divisore

MCD(252,198)

1° modo Scompone in primi

$252 = 2^2 \cdot 3^2 \cdot 7$ $\quad$ $MCD(252,198) = 2 \cdot 3^2 = 18$

$198 = 2 \cdot 3^2 \cdot 11$

Scrivo (a,b) invece di $MCD(a,b)$

$(252,198) = 18$

(a,b) = max intero che divide sia a che b

$(0,0)$ = non esiste

$5|0$? sì $5 \cdot 0 = 0$

$6|0$? sì $6 \cdot 0 = 0$ $\}$ NON C'È IL MAX

(a,b) esiste se $a \neq 0 \vee b \neq 0$

$(100,0) = 100 \rightarrow$ è il max perché un $x > 100$ non dive 100

$(-100,0) = 100 \rightarrow 100/-100$? sì ma $100 > -100$

$100(-1) = -100$

$MCD(a,b) = MCD(|a|,|b|) \rightarrow$ ed è >0 (se esiste)

$MCD(6,-4) = MCD(6,4) = 2 \rightarrow$ posso prendere i positivi

$MCD(a,b) = MCD(a-b,b)$

$= MCD(a+b,b) = MCD(a+kb,b)$

qualsiasi multiplo di b

Posso aggiungere ai numeri a o b un loro multiplo e l'MCD non cambia.

ES $(252,198) = (54,198)$ $\quad$ $\begin{array}{r|l} 198 & 54 \\ 36 & 3 \end{array}$

$= (18, 36)$

$= (18, 0)$

$= 18$

Dimostro che $(a,b) = (\underbrace{a+kb}_{\text{resto di } a|b}, b) = MCD(a,b)$

$MCD(a,b) = \max\{x \mid x|a \wedge x|b\}$

$MCD(a+kb,b) = \max\{x \mid x|a+kb \wedge x|b\}$

~~Basta~~ dimostrare

$\subseteq$ $\{x \mid x|a \wedge x|b\} = \{x \mid x|a+kb \wedge x|b\}$

dimostro che l'uno è $\subseteq$ nell'altro

Prendo un x tale che $x|a \wedge x|b$

Faccio vedere che $x|a+kb$

So che $b = x \cdot ?_{①}$ $\quad$ $a = x \cdot ?_{②}$

$\Longrightarrow$

$(a+kb) = x\underbrace{(?_{②} + k?_{①})}_{?_{③}}$

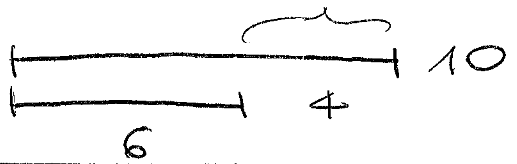
$\supseteq$ Prendo $x|a+kb \wedge x|b$

Devo far vedere che $x|a \wedge x|b$ (è vero)

So che $a+kb = ?_{①}$ $\quad$ $b = ?_{②}\, x$

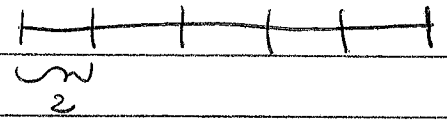
$a = \underbrace{a+kb} - \underbrace{kb} = ?_{①} x - k ?_{②} x = x(?_{①} - k?_{②})$

Geometricamente



$MCD(10,6) = MCD(10-6,6) = MCD(4,6)$

$MCD(10,6) = 2$



Teorema del Bezout

$a, b \in \mathbb{Z}$

$CL(a,b) = \{ar + bs \mid r \in \mathbb{Z}, s \in \mathbb{Z}\}$

combinazione lineare

$CL(10,6) = \{\underbrace{10+6}_{16}, \underbrace{2\cdot 10+6}_{26}, \underbrace{-1\cdot 10+6}_{-4}, \underbrace{10+2\cdot 6}_{22}, \dots\}$

$MCD(10,6) \in$ a questo insieme

$-10+2\cdot 6 = 2$ ✓

$\underbrace{MCD(a,b) \in CL(a,b)}_{\text{TEOREMA}}$

$CL^{+}(a,b) = CL(a,b) \cap \mathbb{Z}^{>0}$

Teo: allora $MCD(a,b) = \min CL^{+}(a,b)$

MCD sempre > 0.

19/11/14

MCD = massimo comun divisore

Abbrevio $MCD(a,b)$ con (a,b)

$CL(a,b) = a\mathbb{Z} + b\mathbb{Z} = \{ar+bs \mid r \in \mathbb{Z} \wedge s \in \mathbb{Z}\}$

$CL(10,6) = \{\underbrace{10\cdot 4 + 6(-1)}_{34}, \underbrace{10\cdot 2 + 6\cdot 3}_{38}, \dots\dots\}$

$(10,6) = 2 \in$

$= 10(-1)+6\cdot 2$

Teorema (Bezout) $MCD(a,b) \in CL(a,b)$

$MCD(a,b) = \min(CL(a,b) \cap \mathbb{Z}^{>0})$

Dim $d \overset{def}{=} \min(CL(a,b) \cap \mathbb{Z}^{>0})$

addirittura multiplo

Voglio dimostrare $d = MCD(a,b)$

cioè ① $d \mid a \wedge d \mid b$ ② d è il più grande tra i divisori

① e ② vero?

Come dimostro che $d \mid a$, senza sapere chi sono d e a?
Divido a per d e trovo il resto.

$\begin{array}{c|c} a & d \\ \hline r & q \end{array}$ Scrivo $\boxed{a = dq + r}$

$0 \le r < d$

d era una combinazione $\boxed{d = am + bn}$

$\Rightarrow$ anche $r \in CL(a,b)$ $r = a - dq = a - (am+bn)q$
$= a(1-m) + b(nq)$

Ma d era la più piccola combinazione lineare
$\Rightarrow r=0$ (se no se $r>0$ contraddice la minimalità di d)

Dimostrato che $d|a$ ($d|b$ uguale)

Mostro che d è il più grande. Come?

Prendo un ~~altro~~ divisore z di $a<b$ ($z|a \wedge z|b$) e cerco di dimostrare $z \leq d$.
In realtà faccio vedere che $z|d$ (e quindi $z \leq d$ se d è positivo)

Siccome $z|a \wedge z|b$
$\Rightarrow z|\underbrace{am+bn}_{=d}$ (somma di multipli di z è multiplo di z)

#

$z|a \wedge z|b \Rightarrow z \leq MCD(a,b)$
$\Uparrow$
$z|MCD(a,b)$

Es Esistono x e $y \in \mathbb{Z}$ tc $18=252x+198y$?

Sì $18=MCD(252,198) \in CL(252,198)$
cioè x, y esistono.

Q_1 Come li trovo?
Q_2 $36=252m+198n$ $\exists m,n$? Sì $m=2x$, $n=2y$

In generale: $\exists z,w$
$17=252z+198w$?

Non esistono z e $w \in \mathbb{Z}$.
Perché?

EQUAZIONI DIOFANTEE
(Diofanto)

Per assurdo esistono z e w.
Dico $18|252$, $18|198$,
quindi $18|252z+198w=17$ $\perp$ ASSURDO #

Quindi per quali numeri K esiste la soluzione dell'equazione $K=252x+198y$?

Per tutti e soli i K che sono multipli di $MCD(252,198)=18$

Dim
$MCD(252,18)=252m+198n$ (per Bezout)
Se K è MCD per (qualcosa) q.
Se $K=MCD(252,18)\cdot q \Rightarrow K=252(mq)+198(nq)$

In generale, se K non è multiplo di $MCD(252,198)$, come faccio a dimostrare che la soluzione non c'è?
In questo caso, se $K=252m+198n$
$MCD(252,198)$ divide qualunque combinazione lineare di $252,198$
$\Rightarrow$ K è multiplo di $MCD(252,198)$

IDEM se al posto di 298 e 152 ho a, b

Come trovo $\underline{x,y}$, $18=MCD(252,198)=252x+198y$

Troviamo x, y con $MCD(1020,351)=1020x+351y$

$$\begin{array}{r|l} 1020 & 351 \\ 318 & 2 \end{array} \qquad 1020=351\cdot 2+318$$

$(1020,351)=(318,351)$

$$\begin{array}{r|l} 351 & 318 \\ 33 & 1 \end{array}$$

$=(318,33)$

$$\begin{array}{r|l} 318 & 33 \\ 21 & 9 \end{array}$$

$=(21,33)$

$=(21,12)$

$=(9,12)$

$=(9,3)$

$=(0,3)=3$

Trovare (x,y) $MCD(1020, 351) = 1020x + 315y$

$\quad\quad = 3$

1020	1020	351
1020	1	0
351	0	-1
$1020 - 2 \cdot 351$ 318	1	-2
$351 - 1 \cdot 318$ 33	-1	3
$318 - 9 \cdot 33$ 21	10	-21
$33 - 21$ 12	-11	32
$21 - 12$ 9	21	-61
3		

$1020 = 1020 \cdot 1 + 351 \cdot 0$

$351 = 1020 \cdot 0 + 351 \cdot 1$

$318 = 1020 - 2 \cdot 351$

$= (1020 \cdot 1 + 351 \cdot 0)$

$2(1020 \cdot 0 + 351 \cdot 1)$

$= 1020(1 - 2 \cdot 0) + 351(0 - 2 \cdot 1)$

$3 = 12 - 9 =$

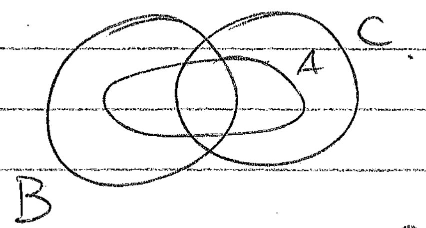
$-32 \cdot 1020 + 93 \cdot 351$

Es $a|bc \overset{?}{\Rightarrow} a|b \vee a|c$?

NO $4|6 \cdot 10 \Rightarrow$ però $4 \nmid 6 \wedge 4 \nmid 10$

Simile al problema insiemistico

$A \subseteq B \cup C \not\Rightarrow A \subseteq B \vee A \subseteq C$



Teo $a|bc \wedge (MCD(a,b) = 1) \Rightarrow a|c$

Dim $\boxed{\text{Bezout}} \Rightarrow 1 = am + bn \ (\exists m, n)$

$\Downarrow \times c$

$c = acm + bcn$

Ma $a|acm$ e $a|bcn$.

Teorema p primo, $p|bc \Rightarrow \underbrace{p|b}_{A} \vee \underbrace{p|c}_{B}$?

$(A \vee B) \equiv (\neg A \Rightarrow B)$

Basta far vedere che

se $p \nmid b \Rightarrow p|c$

Se $p \nmid b \Rightarrow MCD(p, b) = 1$

$\uparrow$

(Questo è 1 o p. Se fosse p, $p|b$)

$101 \cdot 31 = 17 \cdot 43 = n$

Se fossero uguali, $17 | 101 \cdot 31 \Rightarrow 17 | 101 \vee$

$17 | 31$

Esercizio Unicità Scomposizione in primi

$n = p_1^{a_1} \cdot \ldots \cdot p_n^{a_n} = q_1^{b_1} \cdots q_k^{b_k}$. p_i, q_i primi

(e p_i distinti tra loro
q_i ______)

$p_i^{a_i} = q_i^{b_i}$

Dato i, esiste j: A meno dell'ordine la scomposizione è la stessa.

Esercizio $a|n \wedge b|n \overset{?}{\Rightarrow} ab|n$ NO

$2|2 \wedge 2|2$ ma $2 \cdot 2 | 2$

è vero se $MCD(a,b) = 1$

$a|n \wedge b|n \wedge \boxed{(a,b) = 1} \Rightarrow ab|n$

Bezout mi dice

$1 = ax + by \ (\exists x, y)$

$\Downarrow \times n$

$m = amx + bny$ $\quad b|n \Rightarrow ab|an \Rightarrow ab|anx$

$a|n \Rightarrow ab|bn \Rightarrow ab|bny$

$ab|anx+bny$

$\quad\quad\quad\quad\ \ \| $

$\quad\quad\quad\quad\ \ n$

Teo
$(a,n)=1 \Rightarrow$ esiste l'inverso di a mod n cioè esiste un b, $ab \equiv 1 (n)$

Dim Bezout
$1 = ax + ny$
$1 \equiv ax + \cancel{ny}\ (n)$ $\quad$ x è l'inverso di a mod n

25/11/14

Teo Dati $a, b, n \in \mathbb{Z}$
$\exists x, y\ \boxed{n = ax+by}$ ← equazione lineare diofantea
$\Leftrightarrow MCD(a,b)|n$

Es $7 = 21x + 14y$
Bezout $\Rightarrow x = 1, y = -1$

$28 = 21x' + 14y'$
$x' = 4, y' = -4$

Congruenze

Dati $a, b, c \in \mathbb{Z}$ cerchiamo $x \in \mathbb{Z}$ $ax \equiv b (c)$. Quando esiste x?

Dire $ax \equiv b(c)$ equivale a dire che $ax = b$ + multiplo di c
cioè $\exists y : \underbrace{b = ax+cy}_{\text{diofantea}}$. Ci chiedevamo se $\exists x$,

$ax \equiv b(c)$
$\Leftrightarrow$
$(\exists x . \exists y\ b = ax+cy)$
$\Leftrightarrow$
$MCD(a,c)|b$

Teo Dati $a, b, c \in \mathbb{Z}$
$\exists x . ax \equiv b(c) \Leftrightarrow MCD(a,c)|b$

Es
$195x \equiv 6\ (42)$. Trovare x se esiste.
Sol $MCD(195, 42)|6$
$\quad\quad\quad\quad \|$
$\quad\quad\quad\quad 3$

Cerco x, y. $6 = 195x + 42y$ $\quad$ Trasformo in Diofantea
Prima faccio (risolvo)
$3 = 195x' + 42y'$ (*) visto che $3 = MCD(195, 42)$

	195	42
195	$195\boxed{1} + 42\boxed{0}$	
42	$195\boxed{0} + 42\boxed{1}$	
27	$195\boxed{1} + 42\boxed{-4}$	$\leftarrow 27 = 195 - 4 \cdot 42$
15	$195\boxed{-1} + 42\boxed{5}$	$15 = 42 - 27$
12	$195\boxed{2} + 42\boxed{-9}$	
$15-12=3$	$\boxed{-3}$	$\boxed{14}$

$(195, 42) = (27, 42)$
$\uparrow$
$195 - 4 \cdot 42$

Ho scoperto che $3 = 195(-3) + (42)(14)$.
Ho risolto:
$3 = 195x' + 42y'$ (*)

$6 = 195(-6) + 42(28)$
$\Downarrow$
$6 \equiv 195(-6) + \cancel{42(28)} \quad (42)$

$x = -6 \qquad x = -6 + 42k, \ x = 36$

2a sol di $195x \equiv 6(42)$ ($\mp$)

$195 \mid 42$
$27 \mid 4$

$195 = 42 \cdot 4 + 27$
$(\cancel{42 \cdot 4} + 27)x \equiv 6 \ (42)$

($\mp$) $27x \equiv 6(42)$
$\exists y \ 27x = 6 + 42y$
$\exists y \ 9x = 2 + 14y$
$9x \equiv 2(14)$
$\uparrow \cdot 3$ perché $(3, 14) = 1$

$3 \cdot 9 = 27 = 28 - 1$
$3 \cdot 9 \underset{(14)}{\equiv} \cancel{28} - 1$

$27x \equiv 6 \ (14)$
$-x \equiv 6 \ (14)$
$x \equiv -6 (14)$
$x = -6 + 14k$

Regole

① $ax \equiv b(c) \iff \frac{a}{d}x \equiv \frac{b}{d}\left(\frac{c}{d}\right)$

basta che rimangono numeri interi

② $kax \equiv kb(c) \iff ax \equiv b(c)$ se $(k, c) = 1$

③ $ax \equiv b(c) \Rightarrow kax \equiv kb(c)$

Dim $c \mid ax - b$
$\Downarrow$
$c \mid (ax-b)k$

① $ax \equiv b \ (c)$ ha soluzione
$ax = b + cy$ ha soluzione
$\frac{a}{d}x = \frac{b}{d} + \frac{c}{d}y$ ha soluzione
$\frac{a}{d}x \equiv \frac{b}{d}\left(\frac{c}{d}\right)$ ha soluzione

③ non serve

$x \equiv 6 \ (7)$ soluzione $x = 6$
$x = 6 + k7$

$\downarrow \times 7$

$7x \equiv 42(7)$

Viene $7 \cdot 2 \equiv 42 (7)$ $\quad x = 2$ Risolvo
$\ \ \ \ \ \ \ \ \text{III} \quad\quad \text{III}$
$\ \ \ \ \ \ \ \ 0 \quad\quad 0$

② Se $(k, c) = 1$ per Bezout trovo $\alpha, \beta \in \mathbb{Z}$
$1 = k\alpha + c\beta$
$1 \underset{(c)}{\equiv} k\alpha$

So che k e α sono inversi uno dell'altro modulo c

La ② dice che
$kax \equiv bk \ (c)$
$\downarrow \times \alpha$
$(\underbrace{\alpha k}_{1})ax \equiv b(\underbrace{k\alpha}_{1}) \ (c)$
$\downarrow$
$ax \equiv b \ (c)$

Esercizio
$\binom{17}{8} \equiv 0 \ (17)$

Teo p primo $\quad 0 < i < p$
$\Rightarrow$
$p \mid \binom{p}{i} \equiv \emptyset \ (p)$

Dim
$\binom{p}{i} = \frac{p!}{(p-i)!\,i!} \qquad \binom{p}{i} p!(p-i)! = p!$

ovvio che $p \mid p!$

Quindi $p \mid \binom{p}{i}(i!)(p-i)!$

Ricordiamo che $p \mid (ab)c \Rightarrow (p \mid a \vee p \mid b) \vee p \mid c$ (p primo)
$\Downarrow$
$(p \mid ab) \vee p \mid c$

$p \mid \binom{p}{i} \vee \underbrace{p \mid i!}_{\text{ASSURDO}} \vee \underbrace{p(p-i!)}_{\text{ASSURDO}}$

Siccome $0 < i < p$
$i! = i(i-1)(i-2)\dots 1$ tutti questi fattori sono $< p$, p non li divide

Se p dividesse $i!$, dividerebbe uno dei suoi fattori che è assurdo, perché $< p$.

Idem $p \nmid i! \quad p \nmid (p-i)!$ quindi $p \mid \binom{p}{i}$

Esercizio $(x+y)^p \equiv ? \ (p) \quad p$ primo

$(x+y)^p = \sum_{i=0}^{p} x^{p-i} y^i \binom{p}{i} = \binom{p}{0}x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \binom{p}{p}y^p,$

ma per $0 < i < p$, $\binom{p}{i} \equiv 0 \ (p)$

Quindi: $(x+y)^p \underset{(p)}{\equiv} \binom{p}{0}x^p + \binom{p}{p}y^p \equiv x^p + y^p$

$(x+y)^{17} \equiv x^{17} + y^{17} \ (17) \qquad 17$ primo

Es p primo
$x^p \equiv ? \ (p)$
$\searrow x$

$8^{17} \equiv ? \ (17)$
$\searrow 8$

$8^0 = 1$

Teo $x^p \equiv x \quad (p)$ $\quad$ p primo

Dim Induzione su x $(x \geq 0)$

Dim $(x+y)^p \equiv x^p + y^p \quad (p)$

$$(x+y+z)^p \equiv (x+y)^p + z^p \quad (p)$$
$$\equiv x^p + y^p + z^p \quad (p)$$

Per induzione su m, mostro che
$\underbrace{(x_1+x_2+ \ldots + x_m)^p \equiv x_1^p + x_2^p + \ldots x_m^p \quad (p)}_{Q(m)}$

$m = 1, 2, 3$ l'ho verificato

$Q(m) \Rightarrow Q(m+1)$

$$(x_1+x_2+\ldots x_m)^p \underset{Q(m)}{\equiv} x_1^p + \ldots x_m^p + x_{m+1}^p$$

x lo scriviamo come $x^p = \underbrace{1+1+1 \ldots 1}_{m \text{ volte}}$

$$\equiv 1^p + 1^p + \ldots + 1^p \quad (p)$$
$$\equiv 1 + 1 + \ldots + 1 \quad (p)$$
$$\equiv x \quad (p)$$

$x \geq 0$ $\quad$ $-x \equiv (p-x)$
$$(-x)^p \equiv (p-x)^p$$
$$\equiv (p-x)$$
$$\equiv -x \quad (p)$$

Es $x^{p-1} \equiv \, ? \quad (p)$ $\quad$ p primo

$$x \equiv x^p \equiv x^{p-1} \cdot x$$

$$x^{p-1} \equiv x^p \equiv x \quad (p)$$

$\Updownarrow$ divido per x

$$x^{p-1} \equiv 1 \quad (p)$$

se $(x,p) = 1$ sse $p \nmid x$
sse $x \not\equiv 0 \; (p)$

Teo se $x \not\equiv 0 \; (p) \Rightarrow x^{p-1} \equiv 1 \quad (p)$

$2^{1000} \equiv \, ? \quad (17)$

$2^{16} \equiv 1 \quad (17)$ $\qquad$ $1000 \,|\, 16$, $8 \,|\, 62$

$1000 = 16 \cdot 62 + 8$

$$2^{1000} = 2^{16 \cdot 62 + 8} = (2^{16})^{62} \cdot 2^8 \equiv 2^8 \quad (17)$$

congruenze Esponenziali

$2^m \equiv 3 \; (17)$ $\qquad$ si vedranno.

26/11/11

Teo PICCOLO TEOREMA DI FERMAT

p primo $\Rightarrow x^p \equiv x \quad (p)$

Grande Teo di Fermat

$x^2+y^2 = z^2 \rightarrow$ l'unica che si può svolgere (facilmente)

$3^2 + 4^2 = 5^2$

$x^3 + y^3 = z^3$ $\quad$ Dimostrazione complicata.

$x^m + y^m = z^m$

Inoltre, per il PICCOLO TEOREMA DI FERMAT,

se $\not\equiv 0\ (p) \Rightarrow x^{p-1} \equiv 1\ (p)$.

Visto che p primo, $x \not\equiv 0\ (p)$

$\Updownarrow$

x invertibile mod p $\longleftrightarrow (x,p)=1$

ES

$10 \not\equiv 0\ (12)$

$(10,12)=2$ MCD

$2^{16} \equiv 1\ (17)$	$3^{31} \equiv 3\ (31)$
$2^{17} \equiv 2\ (17)$	$3^{30} \equiv 1\ (31)$

Esercizio

Trovare gli $x \in \mathbb{Z}$.

$2^x \equiv 1\ (17)$

1 soluzione $x=16$. Altre soluzioni?

$x=k16$ con $k\in\mathbb{Z}$

Attenti!! $\underset{\substack{\shortparallel \\ 2}}{2^{17}} \not\equiv \underset{\substack{\shortparallel \\ 1}}{2^{0}}\ (17)$ nonostante $17 \equiv 0\ (17)$

$2^{32} = (2^{16})(2^{16}) \equiv 1 \cdot 1 \equiv 1\ (17)$ $2^{a+b} = 2^a \cdot 2^b$

$2^{k\cdot 16} \equiv \underbrace{2^{16}\ 2^{16} \ldots 2^{16}}_{k} \equiv 1 \cdot 1 \ldots 1 \equiv 1\ (17)$

$2^{-16} \equiv\ ?\ (17)$ $2^{-16} = \frac{1}{2^{16}} \notin \mathbb{Z}$

Diamo un significato intero a 2^{-16}. Come?

$2^{-16} = (2^{-1})^{16}$

Nell'ambito delle $\underset{(17)}{\equiv}$ a (2^{-1}) gli diamo

il significato di un inverso di 2 mod 17

?

$2^{15} \cdot 2 \equiv 2^{16} \equiv 1\ (17)$? $2 \equiv 1\ (17)$

$2^{-1} \equiv 9 \equiv 2^{15}\ (17)$

Alcune soluzioni sono:

$x=16$ (Piccolo Teorema di Fermat)

$x=16k$

$x=-16$ se diamo a 2^{-16} il significato di $(2^{-1})^{16}$

allora $2^{-1} \equiv 2^{16-1} \equiv 2^{15}$

$(2^{-1})^{16} \equiv (2^{-1})^{16} \cdot 1 \equiv (2^{-1})^{16} \cdot (2^{16}) \equiv \underbrace{(2^{-1})(2^{-1})}_{16}\ \underbrace{2 \cdot 2 \ldots 2}_{16}$

$2^{-1} = 2^{15}$ $= 2^{-1}2\ 2^{-1}2 \ldots 2^{-1}2 = \underbrace{1 \cdot 1 \ldots 1}_{16}\ 1\ (17)$

Trovare gli $x \in \mathbb{Z}$ $2^x \equiv 1\ (17)$.

Altre soluzioni?

$\mathbb{Z}/(17) = \{0,1,2,\ldots,16\}$

$2 \cdot 9 = 1$

$10+10=3$

$3 \equiv 10+10\ (17)$

$3 \equiv 10+10$ in $\mathbb{Z}/(17)$

Lavorando in $\mathbb{Z}/(17)$ calcoliamo per vari n.

$2^0 \underset{(17)}{\equiv} 1$ $2^1 = 2, 2^2$

$$\begin{array}{ccccccccc} 2^0 & 2^1 & 2^2 & 2^3 & 2^4 & 2^5 & 2^6 & 2^7 & 2^8 \; \ldots \\ \hline 2 & 2 & 4 & 8 & 16 & 15 & 13 & 9 & 1 \\ & & & & \equiv & \equiv & \equiv & & \\ & & & & -1 & -2 & -4 & & \end{array}$$

Non solo $2^{16} \equiv 1 (17)$, ma anche $2^8 \equiv 1 (17)$.
(Fermat)

Fermat ci trovava una soluzione, ma non la più piccola.

Trovare gli x con $2^x \equiv 1 (17)$. Fermat ci dava $x = 16$ ma non è detto che sia la più piccola.

Procediamo sperimentalmente.
La più piccola è $\emptyset$.
A parte $\emptyset$, è $\underbrace{1, 2, 3 \ldots\ldots 15}_{\text{tra queste}}$, ma

deve dividere 16 (quella che ci dà Fermat)
La ricerca si limita a 2, 4, 8.
2 non va bene.
Trovo che 8 va bene.

Le altre soluzioni sono i multipli della più piccola, cioè
$x = 8$, $x = 16$, $x = 16+8$ $x = 8k$ $k \in \mathbb{Z}$

La più piccola soluzione si chiama
$o(2)_{17}$ Chi è? $\boxed{8}$

$2^{x} \equiv 1 (17) \iff x$ è multiplo della soluzione più piccola
$o(2)_{17} = 8$

$\iff x \equiv 0 (8)$

Abbiamo ricondotto una congruenza esponenziale
↓
congruenza normale.

Es
$2^x \equiv 15 (17)$.
Tutte le soluzioni.

Dim $2^x = 2^5 \ (17)$ siccome $(2, 17) = 1$ (2 invertibile)

$2^x \cdot 2^{-5} = 2^5 2^{-5} \equiv 1 (17)$ esiste $(2^{-1}) \bmod 17$

$2^{\overset{y}{x-5}} \equiv 1 (17)$ ⊛

Sapevo che $2^y \equiv 1 (17)$ $\Updownarrow$ $y \equiv 0 (8)$

Quindi con $y = x-5$, ottengo ⊛ $\leftrightarrow x-5 \equiv 0 (8)$
$x \equiv 5 (8)$
$x = 5+8k$

$8^x \equiv 15 (17)$
$(2^3)^x \equiv 15 (17)$
$2^{3x} \equiv 2^5 (17)$
$2^{3x-5} \equiv 1 (17)$
$3-5 \equiv 0 (8)$
$3\boxed{x} \equiv 5 \ (8)$
$*3$ ($x \equiv 15 (8) \equiv 7 (8)$ $x = 7+8k$

① $n = ax + by$ Trovare la x.

② $ax \equiv b\ (c)$ Come si trovano

③ $a^x \equiv 1\ (m)$ tutte le soluzioni?

Es

$$10 = 40x + 50y$$

$x = -1$ $y = 1$

Le altre come si trovano?

A x posso aggiungere un multiplo di 50 $(k50)$.

A y posso sottrarre un multiplo di 40 $(-k40)$.

Ma non sono tutte.

$$n = ax + by$$

$$= a(\underbrace{x+kb}_{x'}) + b(\underbrace{y-ka}_{y'})$$

Se $\boxed{x}$ e $\boxed{y}$ risolvono la ①, anche $x' = x + Kb$, $y' = y - ka$ la risolvono.

Nel caso $10 = 40x + 50y$ ho la soluzione $x = -1 + k50$ $y = 1 - k40$

Sono tutte? NO.

Per trovarle tutte prima divido

$$10 = 40x + 50y$$

$$1 = 4x + 5y$$

dividendo per 10

Soluzioni $\begin{cases} x = -1 + k \cdot 5 \\ y = 1 - k4 \end{cases}$

$x = 4$ $y = -5$

Altre? No, sono tutte.

Come lo dimostro?

trasformo $n = ax + by$

$d = MCD(a,b)$ se $d | n \Rightarrow$ divide tutti e 3

$$n = ax + by$$

$$n' = a'x + b'y$$

Se x, y sono soluzioni lo sono anche $x + kb'$, $y - ka'$ sono tutte

$n' = n/d \in \mathbb{Z}$

$a' = a/d \in \mathbb{Z}$

$b' = b/d \in \mathbb{Z}$

Se invece $d \nmid n$, non ci sono soluzioni.

Teo $a, b \in \mathbb{Z}$

$$a' = \frac{a}{(a,b)} \quad b' = \frac{b}{(a,b)} \Rightarrow (a', b') = 1$$

Dim Se non fosse 1, $(a', b') \neq 1$ esiste $m > 1$ - $m | a'$, $m | b'$

$$m \left| \frac{a}{(a,b)} \right. \quad m \left| \frac{b}{(a,b)} \right. \rightarrow m(a,b) | a, \ m(a,b) | b$$

$n(a,b) > (a,b)$

ASSURDO

Teo $n' = a'x + b'y$

$(a', b') = 1$ allora le uniche soluzioni sono $\begin{cases} x + kb' \\ y - ka' \end{cases}$

Prendiamo una soluzione x, y di $\boxed{n' = a'x + b'y}$ e un'altra x', y' $\boxed{n' = a'x' + b'y'}$

li sottraggo

$0 = a'(x - x') + b'(y - y')$

$0 \equiv a'(x - x') (b')$

$(a', b') = 1$ a' ha un inverso k mod b'

$0 \equiv k0 \equiv ka'(x - x') \equiv x - x' (b')$

$0 \equiv x - x' (b') \vee x \equiv x' (b')$

$x' = x +$ multiplo di b'.

① 5 squadre. torneo: tutte contro tutte in 5 giornate.

Come organizzo il torneo?

1° giorno $(1,5)$ $(2,4)$ 3 riposa.

Regola: il giorno $i \leq 5$, la squadra x gioca con la squadra y, (se $x \neq y$) e se $x + y \equiv i \ (5)$

2° giorno $(2,5)$ $(3,4)$ 1 riposa.

$2 + 5 \equiv 7 \equiv 2 \ (5)$

Dimostriamo che $\forall i \leq 5$ c'è una sola squadra x che riposa. Cioè c'è una sola x tale che

$x + x \equiv i \quad (5)$

$\Updownarrow$

$2x \equiv i \ (5)$

Di x ce n'è una sola, perché 2 è invertibile mod 5.

Ad es. $2 \cdot 3 \equiv 1 (5)$

$2x \equiv i (5)$

$x \equiv \boxed{i \cdot 3} (5)$ nell'intervallo c'è un solo x.

$i = 3$ $x \equiv 9 \ (5)$
$\equiv 4$

Con 6 squadre il metodo non funziona.

La regola $x+y=i\ (6)$

$\underbrace{2}x = i\ (\underbrace{6})$ $x+x=2x \equiv 2\ (6) \leftarrow (1,4)$