Aritmetica

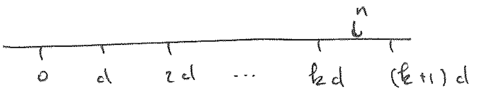
$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ gli interi

Def. Siano $a, b \in \mathbb{Z}$ con $a \neq 0$
Diciamo che a divide b se esiste un $c \in \mathbb{Z}$ tale che $b = ac$.
Se a divide b diciamo che a è un divisore di b e b è un multiplo di a

Notazione: $a \mid b$ se a divide b ; $a \nmid b$ se a non divide b

Esempi: $3 \mid 12$, $3 \nmid 7$

Esempio: Siano $n, d \in \mathbb{Z}$ con $n, d > 0$
Quanti interi positivi meno o uguale a n sono divisibile per d?



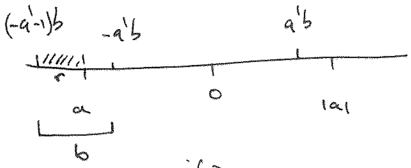
$n = kd + r$ con $0 \leq r < d$ $\quad k = \lfloor \frac{n}{d} \rfloor$

Notazione: per $x \in \mathbb{R}$ $\lfloor x \rfloor$ = l'intero più grande $\leq x$.

Teorema. Sia $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $b \neq 0$.
Allora esiste un unico $q \in \mathbb{Z}$ e $r \in \mathbb{Z}$ tale che $a = qb + r$ e $0 \leq r < b$.

Dim Esistenza: 1) $a \geq 0$ se $a < b$ prendo $q = 0$ e $r = a$
se $a \geq b$ prendo $q = \lfloor \frac{a}{b} \rfloor$ e $r = a - qb$

2) $a < 0$, allora esistono q', r' con $|a| = q'b + r'$ e $0 \leq r' < b$



se $r' = 0$ allora $|a| = q'b$ e $a = (-q')b$. prendo $q = -q'$ $r = 0$
se $r' \neq 0$ allora $a = -q'b - r' = -q'b - r' - b + b = (-q'-1)b + (-r'+b)$
prendo $q = -q' - 1$ e $r = -r' + b$

unicità: se $a = qb + r$ con $0 \leq r < b$ e $a = q'b + r'$ con $0 \leq r' < b$ allora
$(q - q')b + (r - r') = 0$ cioè $(q - q')b = r' - r$ ma $-b < r' - r < b$
quindi $r = r'$ e $q = q'$.

Si dice q il quoziente e r è il resto.

OSS Siano $a, b, c \in \mathbb{Z}$
(1) se $a \mid b$ e $a \mid c$ allora $a \mid (b + c)$
(2) se $a \mid b$ allora $a \mid bd$ per tutti $d \in \mathbb{Z}$
(3) se $a \mid b$ e $b \mid c$ allora $a \mid c$.

Siano $a, b \in \mathbb{Z}$. Cerchiamo i multipli e divisori comuni di a e b.

<u>Def</u> siano $a, b \in \mathbb{Z}$.
Un intero d si dice divisore comune di a e b se $d|a$ e $d|b$.

se $a \neq 0$ o $b \neq 0$ il divisore comune più grande si dice
il massimo comune divisore di a e b. notazione: $\operatorname{mcd}(a,b)$.

a e b si dicono relativamente primi se $\operatorname{mcd}(a,b) = 1$.

<u>oss</u> $\operatorname{mcd}(a,b) \geq 1$ perchè $1|a$ e $1|b$ quindi 1 è un divisore comune di a e b.

Esempio: Trovare $\operatorname{mcd}(24, 36)$.
divisori di 24 : 1, 2, 3, 4, 6, 8, 12, 24
36 : 1, 2, 3, 4, 6, 9, 12, 18, 36
$\operatorname{mcd}(24,36) = 12$.

<u>oss</u> se $a \neq 0$ o $b \neq 0$. $\operatorname{mcd}(a,b) = \operatorname{mcd}(a,-b) = \operatorname{mcd}(-a,b) = \operatorname{mcd}(-a,-b)$.
Quindi per calcolare il massimo comune divisore è sufficiente di avere un algoritmo che lo fa per $a \geq 0$ e $b \geq 0$.

<u>Algoritmo di Euclide.</u>

esempio: Calciamo $\operatorname{mcd}(91, 287)$.

$287 = 91 \cdot 3 + 14$.

Sia d un divisore comune di 287 e 91. allora $d|287$ e $d|91$ quindi $d|287 - 91 \cdot 3$

Quindi $d|14$ e $d|91$.

Ogni divisore di 91 e 14 divide anche $91 \cdot 3 + 14 = 287$ e 91

Quindi $\operatorname{mcd}(287, 91) = \operatorname{mcd}(91, 14)$.

$91 = 14 \cdot 6 + 7$. $7 = 91 - 14 \cdot 6$ quindi ogni divisore comune di 91 e 14 divide 7 e 14
$91 = 14 \cdot 6 + 7$ quindi ogni divisore comune di 14 e 7 divide 91 e 14

Quindi $\operatorname{mcd}(91, 14) = \operatorname{mcd}(14, 7)$.

$14 = 7 \cdot 2$ quindi $\operatorname{mcd}(14, 7) = 7$.

<u>Lemma</u> Siano $a, b \in \mathbb{Z}$ con $ab \neq 0$. Sia $q, r \in \mathbb{Z}$ con $a = bq + r$. Allora $\operatorname{mcd}(a,b) = \operatorname{mcd}(b,r)$

Dim. Sia d un divisore comune di a e b
allora d divide $a - bq = r$ cioè $d|b$ e $d|r$.
Sia e un divisore comune di b e r
allora e divide $bq + r = a$ cioè $e|a$ e $e|b$.
Quindi $\{$divisori comuni di a e $b\} = \{$divisori comuni di b e $r\}$.
In particolare $\operatorname{mcd}(a,b) = \operatorname{mcd}(b,r)$.

L'algoritmo di Euclide:

Input: $a, b \in \mathbb{Z}$ con $a \geq b > 0$

Output: mcd (a,b).

sia $r_0 = a$ e $r_1 = b$.

$$r_0 = r_1 q_1 + r_2 \qquad 0 \leq r_2 < r_1$$
$$r_1 = r_2 q_2 + r_3 \qquad 0 \leq r_3 < r_2$$
$$\vdots \qquad\qquad \vdots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n \qquad 0 \leq r_n < r_{n-1}$$
$$r_{n-1} = r_n q_n \qquad \text{resto } 0.$$

si osserva che $a = r_0 > r_1 > r_2 > \cdots \geq 0$ quindi la procedura termina.

Inoltre $\text{mcd}(a,b) = \text{mcd}(r_1, r_2) = \text{mcd}(r_2, r_3) = \cdots = \text{mcd}(r_{n-2}, r_{n-1}) = \text{mcd}(r_{n-1}, r_n) = r_n$.

Esempio di un programma.

Input $a, b \in \mathbb{Z}$, $a \geq b > 0$

```
x: a;
y: b;
while y ≠ 0
    DO  r:= il resto della divisione di x per y;
        x: y;
        y: r;
    OD;
mcd(a,b) := x;
```

si può usare l'algoritmo di Euclide anche per scrivere il mcd (a,b) come combinazione lineare di a e b. Cioè scrivere mcd (a,b) nella forma $ax + by$ per certo $x, y \in \mathbb{Z}$.

<u>Esempio</u>: calcolare mcd $(480, 175)$

$$480 = 175 \cdot 2 + 130$$
$$175 = 130 \cdot 1 + 45$$
$$130 = 45 \cdot 2 + 40$$
$$45 = 40 \cdot 1 + 5$$
$$40 = 5 \cdot 8 + 0 \qquad \text{mcd}(480, 175) = 5$$

$$\begin{aligned}
5 &= 45 - 40 \cdot 1 \\
&= 45 - (130 - 45 \cdot 2) \cdot 1 \\
&= 45 \cdot 3 - 130 \cdot 1 \\
&= (175 - 130 \cdot 1) \cdot 3 - 130 \cdot 1 \\
&= 175 \cdot 3 - 130 \cdot 4 \\
&= 175 \cdot 3 - (480 - 175 \cdot 2) \cdot 4 \\
&= 175 \cdot 11 - 480 \cdot 4
\end{aligned}$$

Quindi $5 = 175 \cdot 11 + 480 \cdot (-4)$

(controllo $5 = 1925 - 1920$ ok!)

<u>In generale</u>: calcolare mcd (a,b) $a = r_0$ $b = r_1$

$$r_0 = r_1 q_1 + r_2$$
$$r_1 = r_2 q_2 + r_3$$
$$\vdots$$
$$r_{n-4} = r_{n-3} q_{n-3} + r_{n-2}$$
$$r_{n-3} = r_{n-2} q_{n-2} + r_{n-1}$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n$$
$$r_{n-1} = r_n q_n + 0 \qquad \text{mcd}(a,b) = r_n.$$

$$\begin{aligned}
r_n &= r_{n-2} - r_{n-1} q_{n-1} \\
&= r_{n-2} - (r_{n-3} - r_{n-2} q_{n-2}) q_{n-1} \\
&= r_{n-2} (1 + q_{n-2} q_{n-1}) - r_{n-3} q_{n-1} \\
&= (r_{n-4} - r_{n-3} q_{n-3})(1 + q_{n-2} q_{n-1}) - r_{n-3} q_{n-1} \\
&\;\;\vdots \\
&= r_1 (\cdots\cdots) + r_0 (\cdots\cdots)
\end{aligned}$$

Abbiamo trovato una soluzione dell'equazione $175x + 480y = 5$ con $x, y \in \mathbb{Z}$.
Ma non è l'unica soluzione

Infatti se $d = ax + by$ allora $d = a(x + tb) + b(y - ta)$ per ogni $t \in \mathbb{Z}$.

Attenzione! L'algoritmo di Euclide funziona se $a > 0$ e $b > 0$

Però anche se $a \leq 0$ o $b \leq 0$ si può scrivere $\mathrm{mcd}(a,b)$ come combinazione lineare di a e b.

Perchè:

se $a = 0$ e $b \neq 0$ $\quad \mathrm{mcd}(a,b) = |b|$ e $|b| = 0 \cdot a + 1 \cdot b$ se $b > 0$
$= 0 \cdot a + (-1) \cdot b$ se $b < 0$

se $a \neq 0$ e $b = 0$ $\quad \mathrm{mcd}(a,b) = |a|$ e $|a| = 1 \cdot a + 0 \cdot b$ se $a > 0$
$= (-1)a + 0 \cdot b$ se $a < 0$

se $a \neq 0$ e $b \neq 0$ $\quad$ sia $d = \mathrm{mcd}(a,b) = \mathrm{mcd}(|a|, |b|)$. Allora esistono $x', y' \in \mathbb{Z}$ con $d = x'|a| + y'|b|$.

Sia $x = \frac{|a|}{a} x'$ e $y = \frac{|b|}{b} y'$ (cioè $\begin{cases} x = x' \text{ se } a > 0 \text{ e } x' = -x \text{ se } a < 0 \\ y = y' \text{ se } b > 0 \text{ e } y' = -y \text{ se } b < 0 \end{cases}$)

Allora $d = xa + yb$.

Esempio.

scrivere $\mathrm{mcd}(-91, 287)$ come combinazione lineare di -91 e 287.

$\mathrm{mcd}(-91, 287) = \mathrm{mcd}(91, 287)$

$287 = 91 \cdot 3 + 14$
$91 = 14 \cdot 6 + 7$
$14 = 7 \cdot 1 + 0$

Quindi $\mathrm{mcd}(-91, 287) = 7$

$$7 = 91 - 14 \cdot 6$$
$$= 91 - (287 - 91 \cdot 3) \cdot 6$$
$$= 91 \cdot 19 - 287 \cdot 6$$

Quindi $7 = 91 \cdot 19 + 287(-6)$, adesso metto i segni giusti:

$$7 = (-91)(-19) + 287(-6).$$

Quindi una soluzione di $-91x + 287y = 7$ è $x = -19$ e $y = -6$.

OSS. Siano $a, b \in \mathbb{Z}$ con $a \neq 0$ e $b \neq 0$

Sono equivalenti

(1) $d = \text{mcd}(a,b)$

(2) d è un divisore comune positivo di a e b tale che ogni divisore comune c di a e b divide d.

(3) d è il numero positivo più piccolo che si può scrivere come $xa + yb$ con $x, y \in \mathbb{Z}$.

Dim

(1) $\to$ (2) Sia $d = \text{mcd}(a,b)$

Esistono $x, y \in \mathbb{Z}$ tale che $d = xa + yb$. Se $c \in \mathbb{Z}$ con $c \mid a$ e $c \mid b$, allora $c \mid d$.

(2) $\to$ (1). Sia d un divisore comune di a e b tale che ogni divisore comune di a e b divide d.

$\text{mcd}(a,b)$ è un divisore comune di a e b, quindi $\text{mcd}(a,b) \mid d$. cioè $\text{mcd}(a,b) \leq d$

Però $\text{mcd}(a,b)$ è il divisore comune più grande di a e b. Quindi $d \leq \text{mcd}(a,b)$.

Perciò $d = \text{mcd}(a,b)$.

(1) $\leftrightarrow$ (3) Sia $d = \text{mcd}(a,b)$ e sia e il numero positivo più piccolo che si può scrivere come $xa + by$ con $x, y \in \mathbb{Z}$. Allora $e = x_0 a + y_0 b$ per certo $x_0, y_0 \in \mathbb{Z}$

Quindi $d \mid e$, cioè $d \leq e$. Però $d = x'a + y'b$ per certo $x', y' \in \mathbb{Z}$

quindi $e \leq d$. Perciò $e = d$.

OSS: Due interi a, b sono relativamente primi se e solo se esistono $x, y \in \mathbb{Z}$ tale che $xa + yb = 1$.

Dim: Dalla osservazione precedente con $d = 1$.

OSS Siano $a, b, c \in \mathbb{Z}$ con a e b relativamente primi

se $a \mid bc$ allora $a \mid c$

Dim: Esistono $x, y \in \mathbb{Z}$ tale che $xa + yb = 1$. Quindi $xac + ybc = c$.

$a \mid xac$ e $a \mid bc$ quindi $a \mid c$.

Esempio: $a = 6$ $b = 10$ $c = 3$ $6 \mid 30$ però $6 \nmid 3$ Quindi $\text{mcd}(a,b) \neq 1$

OSS Siano $a, b \in \mathbb{Z}$ non entrambi 0 Sia $d = \text{mcd}(a,b)$. Allora $\text{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Dim: Esistono $x, y \in \mathbb{Z}$ tale che $ax + by = d$. Quindi $\left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y = 1$.

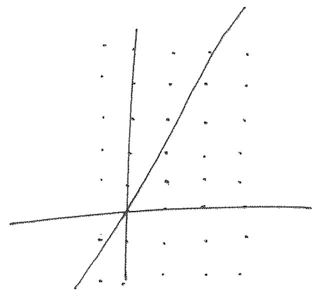
Segue che $\text{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Equazioni diofantee lineari

Def Siano $a,b,c \in \mathbb{Z}$ l'equazione $ax+by=c$ (con $x,y\in\mathbb{Z}$) si dice un equazione diofantea lineare. Se $c=0$ si dice anche che è omogeneo.

Cerchiamo le soluzioni di questo tipo di equazioni

$\mathbb{Z}\times\mathbb{Z} \subseteq \mathbb{R}\times\mathbb{R}$



Esempio $3x+5y=1$ $x=-8$ $y=5$
altri?

$3x+5y=0$

x	y
-5	3
5	-3
10	-6
15	-9
$\vdots$	$\vdots$

altri?

Caso 1 1) se $a=0$ e $b\neq 0$ l'equazione $ax+by=c$ ha solo soluzioni se $b|c$. In quel caso le soluzioni sono $\begin{cases} x=n \\ y=c/b \end{cases}$ $n\in\mathbb{Z}$.

2) se $a\neq 0$ e $b=0$ l'equazione $ax+by=c$ ha solo soluzioni se $a|c$. In quel caso le soluzioni sono $\begin{cases} x=c/a \\ y=n \end{cases}$ $n\in\mathbb{Z}$.

Dim 1) l'equazione è $0x+by=c$ cioè $by=c$. Questa ha solo soluzioni se $b|c$ e in quel caso le soluzioni sono $\begin{cases} x=n \\ y=c/b \end{cases}$ $n\in\mathbb{Z}$.

2) Simile.

Esempi: $5x=10$ allora $x=2$ soluzioni $\begin{cases} x=2 \\ y=n \end{cases}$ $n\in\mathbb{Z}$.

$5y=3$ non ha soluzioni

Caso 2 Siano $a,b\in\mathbb{Z}$ con $a\neq 0$ e $b\neq 0$ e $\mathrm{mcd}(a,b)=1$. Le soluzioni di $ax+by=0$ sono $\begin{cases} x=-bn \\ y=an \end{cases}$ $n\in\mathbb{Z}$.

Dim. Sia $n\in\mathbb{Z}$ se $x=-bn$ e $y=an$ allora $a(-bn)+b(an)=0$ quindi questi sono soluzioni dell'equazione. Adesso dobbiamo dimostrare che non ci sono altri:
Sia $x_0,y_0\in\mathbb{Z}$ con $ax_0+by_0=0$. Allora $ax_0=-by_0$, quindi $a|-by_0$. Dato che $\mathrm{mcd}(a,b)=1$ segue che $a|y_0$. Quindi esiste un $n\in\mathbb{Z}$ con $y_0=an$. In particolare $ax_0=-by_0=-abn$, cioè $x_0=-bn$.

Esempio: $16x+9y=0$ ha soluzioni. Le soluzioni sono $\begin{cases} x=-9n \\ y=16n \end{cases}$ $n\in\mathbb{Z}$.

$3x+5y=0$. Le soluzioni sono $\begin{cases} x=-5n \\ y=3n \end{cases}$ $n\in\mathbb{Z}$.

Caso 3 Siano $a, b \in \mathbb{Z}$ con $a \neq 0$ e $b \neq 0$. Sia $d = \mathrm{mcd}(a,b)$.

Le soluzioni di $ax+by=0$ sono $\begin{cases} x = -\frac{bn}{d} \\ y = \frac{an}{d} \end{cases}$ $n \in \mathbb{Z}$.

Dim. Dimostriamo che le equazioni diofantee lineari $ax+by=0$ e $\frac{a}{d}x + \frac{b}{d}y = 0$ hanno le stesse soluzioni.

Sia $A = \{(x', y') \in \mathbb{Z}\times\mathbb{Z} \mid ax'+by'=0\}$, l'insieme delle soluzioni di $ax+by=0$

sia $B = \{(x', y') \in \mathbb{Z}\times\mathbb{Z} \mid \frac{a}{d}x' + \frac{b}{d}y' = 0\}$, l'insieme delle soluzioni di $\frac{a}{d}x + \frac{b}{d}y = 0$.

Sia $(x_0, y_0) \in A$, allora $\frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{1}{d}(ax_0+by_0) = \frac{1}{d}0 = 0$, quindi $(x_0,y_0) \in B$

Sia $(x_0, y_0) \in B$, allora $ax_0+by_0 = d\left(\frac{a}{d}x_0 + \frac{b}{d}y_0\right) = d.0 = 0$, quindi $(x_0, y_0) \in A$.

Quindi $A = B$.

Osserviamo che $\mathrm{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, quindi dal caso precedente le soluzioni di $\frac{a}{d}x + \frac{b}{d}y = 0$ sono $\begin{cases} x = -\frac{bn}{d} \\ y = \frac{an}{d} \end{cases}$ $n \in \mathbb{Z}$. Quindi questi sono anche le soluzioni di $ax+by=0$.

Esempio. $6x+10y=0$, $\mathrm{mcd}(6,10)=2$, quindi le soluzioni sono quelli di $3x+5y=0$. Le soluzioni sono $\begin{cases} x = -5n \\ y = 3n \end{cases}$ $n \in \mathbb{Z}$.

Caso 4 (il caso generale).

Siano $a, b, c \in \mathbb{Z}$ con $a \neq 0$ e $b \neq 0$. Sia $d = \mathrm{mcd}(a,b)$.

1) se $d \nmid c$ allora l'equazione $ax+by=c$ non ha soluzioni

2) se $d \mid c$ allora le soluzioni dell'equazione $ax+by=c$ sono

$\begin{cases} x = \frac{x'c - bn}{d} \\ y = \frac{y'c + an}{d} \end{cases}$ $n \in \mathbb{Z}$, dove x', y' è una soluzione di $ax+by = d$.

Dim 1) Supponiamo che $(x_0, y_0) \in \mathbb{Z}\times\mathbb{Z}$ è una soluzione di $ax+by=c$

Allora $ax_0+by_0 = c$, $d \mid a$ e $d \mid b$. Quindi $d \mid ax_0+by_0$, cioè $d \mid c$

una contraddizione. Quindi non esistono soluzioni.

2). Prima vogliamo descrivere le soluzioni

Sia $A = \{(x', y') \in \mathbb{Z}\times\mathbb{Z} \mid ax'+by'=c\}$, l'insieme delle soluzioni di $ax+by=c$.

Sia $(x_0, y_0) \in A$. Definiamo $B = \{(x_0+\tilde{x}, y_0+\tilde{y}) \in \mathbb{Z}\times\mathbb{Z} \mid a\tilde{x}+b\tilde{y}=0\}$

quindi ad ogni soluzione di $ax+by=0$ abbiamo sommato x_0 e y_0.

Dimostriamo che $A = B$.

Sia $(x', y') \in A$ e consideriamo $(-x_0+x', -y_0+y')$

Allora $a(-x_0+x') + b(-y_0+y') = -(ax'+by') + (ax_0+by_0) = -c+c = 0$

quindi $(-x_0+x', -y_0+y')$ è una soluzione dell'equazione $ax+by=0$.

Inoltre $x' = x_0 + (-x_0+x')$ e $y' = y_0 + (-y_0+y')$. Quindi $(x', y') \in B$.

Sia $(x', y') \in B$. Allora $x' = x_0 + \hat{x}$ e $y' = y_0 + \hat{y}$ per certo $\hat{x}, \hat{y}$ con

$a\hat{x} + b\hat{y} = 0$. $ax'+by' = a(x_0+\hat{x}) + b(y_0+\hat{y}) = (ax_0+by_0) + (a\hat{x}+b\hat{y}) = c+0 = c$

Quindi $(x', y') \in A$.

Segue che $A = B$.

Le soluzioni di $ax+by=0$ sono $\begin{cases} \hat{x} = -\frac{bn}{d} \\ \hat{y} = \frac{an}{d} \end{cases}$ $n \in \mathbb{Z}$.

cerchiamo una soluzione di $ax+by=c$.

con aiuto del algoritmo di Euclide posso trovare $x', y' \in \mathbb{Z}$ con

$ax'+by' = d$. Allora $\frac{c}{d}(ax'+by') = c$ cioè $a\left(\frac{cx'}{d}\right) + b\left(\frac{cy'}{d}\right) = c$

Quindi $\left(\frac{cx'}{d}, \frac{cy'}{d}\right)$ è una soluzione di $ax+by=c$.

Esempio: $28x + 21y = 14$

1) calcolo il mcd di 28 e 21: $28 = 21 \cdot 1 + 7$, $21 = 7 \cdot 3 + 0$; $\operatorname{mcd}(28,21) = 7$; $7 \mid 14$ ci sono soluzioni.

2) soluzioni di $28x+21y=0$: $4x+3y=0$ le soluzioni sono $\begin{cases} \hat{x} = -3n \\ \hat{y} = 4n \end{cases}$ $n \in \mathbb{Z}$.

3) una soluzione particolare di $28x+21y=14$:

$7 = 28 - 21 \cdot 1$
$= 28 \cdot 1 + 21 \cdot (-1)$

quindi $7 = 28(1) + 21 \cdot (-1)$
$14 = 28(2) + 21(-2)$

una sol. è $\begin{cases} x_0 = 2 \\ y_0 = -2 \end{cases}$

4) Le soluzioni di $28x+21y=14$ sono $\begin{cases} x = 2-3n \\ y = -2+4n \end{cases}$ $n \in \mathbb{Z}$.

Esempio: $28x - 21y = -14$.

$\operatorname{mcd}(28,-21) = \operatorname{mcd}(28,21) = 7$ (vedi sopra) $7 \mid -14$ ci sono soluzioni

le soluzioni di $28x-21y=0$: $4x-3y=0$ le soluzioni sono $\begin{cases} \hat{x} = 3n \\ \hat{y} = 4n \end{cases}$ $n \in \mathbb{Z}$.

una soluzione particolare di $28x-21y=-14$:

$7 = 28 \cdot 1 - 21 \cdot 1$ Quindi $-14 = 28(-2) - 21(-2)$

una soluzione è $\begin{cases} x_0 = -2 \\ y_0 = -2 \end{cases}$

Le soluzioni di $28x-21y=-14$ sono $\begin{cases} x = -2+3n \\ y = -2+4n \end{cases}$ $n \in \mathbb{Z}$

Esempio

$25x - 15y = 35$

1) $\text{mcd}(25,-15) = \text{mcd}(25,15)$

$25 = 15 \cdot 1 + 10$
$15 = 10 \cdot 1 + 5$
$10 = 5 \cdot 2 + 0$ $\quad \text{mcd}(25,-15) = 5 \quad 5 \mid 35$ ci sono soluzioni

2) soluzioni di $25x - 15y = 0$
$5x - 3y = 0$ le soluzioni sono $\begin{cases} \hat{x} = 3n \\ \hat{y} = 5n \end{cases} \quad n \in \mathbb{Z}$

3) una soluzione di $25x - 15y = 35$

$5 = 15 - 10 \cdot 1$
$= 15 - (25 - 15 \cdot 1) \cdot 1 = 15 \cdot 2 - 25 \cdot 1$
$= 25(-1) + 15 \cdot (2) = 25(-1) - 15(-2)$

quindi $5 = 25(-1) - 15(-2)$ $\quad 35/5 = 7$
$35 = 25(-7) - 15(-14)$ $\quad$ una soluzione è $\begin{cases} x_0 = -7 \\ y_0 = -14 \end{cases}$

Le soluzioni di $25x - 15y = 35$ sono $\begin{cases} x = -7 + 3n \\ y = -14 + 5n \end{cases} \quad n \in \mathbb{Z}.$

Esempio

$6x - 9y = -21$

1) $\text{mcd}(6,-9) = \text{mcd}(6,9)$

$9 = 6 \cdot 1 + 3$
$6 = 3 \cdot 2 + 0$ $\quad \text{mcd}(6,-9) = 3 \quad 3 \mid -21$ ci sono soluzioni

2) soluzioni di $6x - 9y = 0$
$2x - 3y = 0$ le soluzioni sono $\begin{cases} \hat{x} = 3n \\ \hat{y} = 2n \end{cases} \quad n \in \mathbb{Z}$

3) una soluzione di $6x - 9y = -21$

$3 = 9 - 6 \cdot 1$ quindi $3 = 6(-1) + 9(1)$
quindi $3 = 6(-1) - 9(-1)$ $\quad \frac{-21}{3} = -7$
quindi $-21 = 6(7) - 9(7)$ $\quad$ una soluzione è $\begin{cases} x_0 = 7 \\ y_0 = 7 \end{cases}$

Le soluzioni di $6x - 9y = -21$ sono $\begin{cases} x = 7 + 3n \\ y = 7 - 2n \end{cases} \quad n \in \mathbb{Z}.$

<u>oss</u> si può controllare la correttezza della risposta!

Numeri primi

Def Un intero p, con $p>1$, si dice primo se i suoi soli divisori positivi sono 1 e p.

Esempio $2, 3, 5, 7$ sono primi
$91 = 7 \cdot 13$ non è primo
1 non è primo.

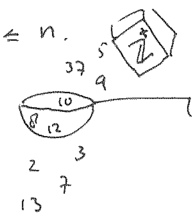
OSS Sia $a \in \mathbb{Z}$, $a > 1$. Sia p il divisore positivo più piccolo di a con $p > 1$.
Allora p è primo.

Dim. Sia $b \in \mathbb{Z}$, $b > 1$ un divisore di p. Allora $b \mid p$ quindi $b \mid a$.
Quindi $b \leq p$ e $p \leq b$. Cioè $p = b$. Quindi p è primo.

Teorema. Il numero dei primi è infinito.

Dim. Supponiamo di no. Cioè supponiamo che ci sono solo un numero finito di primi. Diciamo $p_1, \dots, p_s$. Sia $m = p_1 \cdot p_2 \cdot \dots \cdot p_s + 1$. Allora $m \in \mathbb{Z}$, $m > 1$, e per ogni i con $1 \leq i \leq s$ $p_i \nmid m$ (perché altrimenti $p_i \mid m - p_1 \cdots p_s$ cioè $p_i \mid 1$). Sia p il divisore positivo più piccolo di m con $p > 1$. Allora p è un primo e $p \mid m$. Quindi p è un primo diverso da $p_1, \dots, p_s$. Una contraddizione.

Come si può generare una lista di primi $\leq n$.



Algoritmo (Il crivello di Eratostene)
Input: $n \in \mathbb{Z}$, $n > 1$.
Output: tutti i primi $\leq n$.

```
L := [2, 3, ...., n];
M := ∅;
while  L ≠ ∅
   DO  sia m il numero più piccolo in L;
       aggiungere m ad M;
       cancelare tutti i multipli di m in L;
   OD;
M;
```

OSS Tutti i primi $\leq n$ sono in M. Inoltre ad ogni passo m è un primo:
sia a il divisore più piccolo di m con $a > 1$. Allora a è primo.
Se $a < m$ allora m è un multiplo di un primo $< m$, e di conseguenza sarebbe già cancelato. Quindi $a = m$ e m è primo.
Quindi l'algoritmo è coretto.

OSS il "bucco" tra due primi consecutivi può essere abitrariamente grande.

Dim Sia $m \in \mathbb{Z}$, con $m \geq 1$. Allora $(m+1)! = 1.2.3.\dots.m.(m+1)$, quindi $(m+1)!$ è divisibile per $2, 3, 4, \dots, m, m+1$

Quindi
$$\left.\begin{array}{ll} (m+1)!+2 & \text{non è primo} \\ (m+1)!+3 & \text{non è primo} \\ \vdots & \\ (m+1)!+m & \text{non è primo} \\ (m+1)!+(m+1) & \text{non è primo} \end{array}\right\}$$
sono m numeri consecutivi tra cui non c'è un primo.

Alcuni primi famosi

Def. Un numero primo di Mersenne è un numero primo esprimibile come 2^n-1, con n un intero positivo.

Mersenne (1588-1648)

Per $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, 2^n-1 è primo e per tutti gli altri valori di $n \leq 257$ 2^n-1 non è primo.

Questo risultato è <u>falso</u>: per $n = 67$ e 257 2^n-1 non è primo
per $n = 61, 89, 107$ 2^n-1 è primo.

OSS $(x^2-1) = (x+1)(x-1)$ quindi $2^8-1 = (2^4+1)(2^4-1)$ quindi 2^8-1 non è primo.

$(x^n-1) = (x-1)(x^{n-1}+x^{n-2}+\dots+x+1)$ quindi se prendo $x = 2^a$ e $n = b$ per certo $a, b \in \mathbb{Z}$ con $a \geq 0$ e $b \geq 1$ allora la formula diventa.

$(2^{ab}-1) = (2^a-1)(2^{a(b-1)}+2^{a(b-2)}+\dots+2^a+1)$.

In particolare, se $a>1$ e $b>1$ allora $2^{ab}-1$ non è primo.

Quindi se n non è primo allora 2^n-1 non è primo.

Per sapere quale è il numero primo più grande che conosciamo vedi per esempio "the prime pages" (link sul sito).

Teorema: Il numero di primi nell'intervallo $[1, n]$ è approssimamente $\frac{n}{\log n}$

OSS Siano $b, c, p \in \mathbb{Z}$. Se p è primo e $p \mid bc$, allora $p \mid b$ o $p \mid c$

Dim se $p \nmid b$ allora $\mathrm{mcd}(p, b) = 1$ quindi $p \mid c$.

Corollario Sia p un primo e $b_1 \dots b_s \in \mathbb{Z}$ tale che $p \mid b_1 \cdots b_s$. Allora esiste un i con $1 \le i \le s$ con $p \mid b_i$.

Teorema Sia $a \in \mathbb{Z}$, $a > 1$, allora a si può scrivere come prodotto di un numero finito di primi. Cioè $a = p_1 \cdots p_s$ dove $p_1, \dots, p_s$ sono primi. Inoltre, fino al ordine dei fattori questa scrittura è unica.

Esempio

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

$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3 \cdot 37 \cdot 3 \cdot 3 = 3^3 \cdot 37$$

$$641 = 641$$

Il teorema dice: $a = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ con $p_1, \dots, p_t$ primi distinti $p_1 < p_2 < \dots < p_t$ $a_1 \geq 1, \dots, a_t \geq 1$ e questa scrittura è unica.

Questa si dice la fattorizzazione di a in primi.

La dimostrazione del teorema facciamo più tardi.

Problema come trovare una fattorizzazione in primi.

OSS Se n è un intero positivo, e n non è primo allora esiste un primo p con $p \mid n$ e $p \le \sqrt{n}$.

Dim. Se n non è primo allora $n = a \cdot b$ per certo $a, b \in \mathbb{Z}$ con $1 < a \le b < n$. Se $a > \sqrt{n}$ allora $n = ab \geq aa > \sqrt{n} \cdot \sqrt{n} = n$ una contradizione. Quindi $a \le \sqrt{n}$. Prendiamo adesso un primo p con $p \mid a$. Allora $p \mid n$ e $p \le \sqrt{n}$.

Esempio 101 è primo perchè: se no allora esiste un primo $p \le \sqrt{101} < 11$ con $p \mid 101$. I primi < 11 sono $2, 3, 5$ e 7, ma nessuno di questi divide 101.

Esempio Trovare la fattorizzazione in primi di 7007.

$\sqrt{7007} < 84$. Cerco un primo < 84 che divide 7007

comincio: $\cancel{2}, \cancel{3}, \cancel{5}, 7$ $\quad 7007 = 7 \cdot 1001$

cerco un primo p con $7 \leq p \leq \sqrt{1001} < 32$ che divide 1001

$7 \quad 1001 = 7 \cdot 143$

cerco un primo p con $7 \leq p \leq \sqrt{143} < 12$ che divide 143

$\cancel{7}, 11 \quad 143 = 11 \cdot 13$

cerco un primo p con $11 \leq p \leq \sqrt{13} < 11$ che divide 13

non esiste quindi 13 è primo.

Quindi $7007 = 7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$

Def Siano $a, b \in \mathbb{Z}$ con $a \neq 0$ e $b \neq 0$.
Un intero c si dice *multiplo comune* di a e b se $a|c$ e $b|c$.
Il multiplo comune di a e b positivo più piccolo si dice
minimo comune multiplo. Notazione $mcm(a,b)$.

Esempio $\quad 15 : 15, 30, 45, 60, 75, 90, \ldots \qquad mcm(15,18) = 90$
$\qquad\quad 18 : 18, 36, 54, 72, 90, \ldots$

OSS Siano $a, b \in \mathbb{Z}$, $a > 1$, $b > 1$.
Se $a = p_1^{a_1} \cdots p_n^{a_n}$ con $a_1, \ldots, a_n \geq 0$ e $b = p_1^{b_1} \cdots p_n^{b_n}$ con $b_1, \ldots, b_n \geq 0$
e $p_1 \cdots p_n$ primi distinti. Allora

$$mcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$ e

$$mcm(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}.$$

Dim. Per ogni $1 \leq i \leq n$, sia c_i tale che $p_i^{c_i} \mid mcd(a,b)$ ma $p_i^{c_i+1} \nmid mcd(a,b)$,
cioè $mcd(a,b) = p_1^{c_1} \cdots p_n^{c_n}$, e sia $e_i = \min(a_i, b_i)$. Allora
$p_i^{c_i} \mid mcd(a,b)$ quindi $p_i^{c_i} \mid a$ e $p_i^{c_i} \mid b$. Quindi $c_i \leq a_i$ e $c_i \leq b_i$
e in particolare $c_i \leq \min(a_i, b_i) = e_i$. In oltre $p^{e_i} \mid a$ e $p^{e_i} \mid b$
quindi $p^{e_i} \mid mcd(a,b)$, cioè $e_i \leq c_i$. Segue che $e_i = c_i$.
La dimostrazione per il $mcm(a,b)$ è simile.

Esempio $\quad 120 = 2^3 \cdot 3^1 \cdot 5^1$
$\qquad\quad 500 = 2^2 \cdot 3^0 \cdot 5^3$

$mcd(120, 500) = 2^2 \cdot 3^0 \cdot 5^1 = 20$
$mcm(120, 500) = 2^3 \cdot 3^1 \cdot 5^3 = 3000$

OSS Siano $a, b \in \mathbb{Z}$, $a > 1$, $b > 1$. Allora $\text{mcd}(a,b) \cdot \text{mcm}(a,b) = a \cdot b$

In particolare $\text{mcm}(a,b) = \frac{a \cdot b}{\text{mcd}(a,b)}$ e posso calcolare $\text{mcm}(a,b)$ senza usare la fattorizzazione in primi.

Dim Basta osservare che nella notazione dell'osservazione precedente che $\min(a_i, b_i) + \max(a_i, b_i) = a_i + b_i$.

Def Sia $a \in \mathbb{Z}$, $a > 1$ e p un primo. Sia p^c la potenza di p più alta che divide a. Il numero c viene denotato con $\text{ord}_p(a)$.

Quindi $a = \prod_{p \text{ primo}} p^{\text{ord}(a)}$

Esempio $6600 = 2^3 \cdot 3 \cdot 5^2 \cdot 11$

$\text{ord}_2(6600) = 3$, $\text{ord}_3(6600) = 1$, $\text{ord}_5(6600) = 2$, $\text{ord}_7(6600) = 0$, $\text{ord}_{11}(6600) = 1$, e $\text{ord}_p(6600) = 0$ per ogni $p > 11$.

—||—

Siano $A, B, C, \dots, X, Y, Z \in \mathbb{Z}$. Se il numero

$$
\begin{aligned}
(K+2)\{ & 1 - [WZ + H + J - Q]^2 - [(GK + 2G + K + 1)(H + J) + H - Z]^2 - \\
& [2N + P + Q + Z - E]^2 - [16(K+1)^3(K+2)(N+1)^2 + 1 - F^2]^2 - \\
& [E^3(E+2)(A+1)^2 + 1 - O^2]^2 - [(A^2-1)Y^2 + 1 - X^2]^2 - \\
& [16 R^2 Y^4 (A^2-1) + 1 - U^2]^2 - \\
& [((A + U^2(U^2-A))^2 - 1)(N + 4DY)^2 + 1 - (X + CU)^2]^2 - \\
& [N + L + V - Y]^2 - [(A^2-1)L^2 + 1 - M^2]^2 - [AI + K + 1 - L + I]^2 - \\
& [P + L(A - N - 1) + B(2AN + 2A - N^2 - 2N - 2) - M]^2 - \\
& [Q + Y(A - P - 1) + S(2AP + 2A - P^2 - 2P - 2) - X]^2 - \\
& [Z + PC(A - P) + T(2AP - P^2 - 1) - PM]^2 \}
\end{aligned}
$$

è positivo, allora questo numero è primo, e ogni primo si può trovare in questo modo.

Però quasi mai questo numero è positivo.......

Si osserva che, per essere positivo ogni delle 14 termine $[\dots]^2$ deve essere 0.

Sia n un intero $n \geq 2$, allora n è "prodotto" di numeri primi

$P(n)$: n è "prodotto" di numeri primi

$P(2)$: 2 è primo, quindi "prodotto" di numeri primi.

Supponiamo $n > 2$ e che $2, 3, \ldots, n-1$ sono prodotti di numeri primi, dimostriamo che n è prodotto di numeri primi

consideriamo n.

1) se n è primo, allora n è prodotto di numeri primi, quindi $P(n)$ è vero.

2) se n non è primo allora esiston $a, b \in \mathbb{Z}$ $2 \leq a, b < n$ con $n = a \cdot b$

Dato che $2 \leq a \leq n-1$ segue dalla nostra ipotesi d'induzione che a è prodotto dei primi e simile b è prodotto di primi. Quindi $n = a \cdot b$ è prodotto di numeri primi. Quindi $P(n)$ è vero.

segue dal principio d'induzione che ogni intero $n \geq 2$ è prodotto di numeri primi

si osserva che con la prima forma del principio d'induzione sarebbe molto più difficile da dimostrare.

Abbiamo che ogni intero $n \geq 2$ si può scrivere come prodotto di numeri primi

cioè $n = p_1 \cdot \ldots \cdot p_r$ con $p_1, \ldots, p_r$ numeri primi

Ma vale anche che fino all'ordine dei fattori questa scrittura è unica.

$P(n)$: la fattorizzazione di n in numeri primi è unica

$P(2)$ 2 è primo, quindi la scrittura è unica

supponiamo che per $2, 3, \ldots, n-1$ la fattorizzazione i numeri primi è unica e $n > 2$.

Da dimostrare che anche n ha una fattorizzazione unica in numeri primi

1) se n è primo, allora la fattorizzazione è unica.

2) se n non è un numero primo allora n ha una fattorizzazione in numeri primi

$n = p_1 \cdots p_s$ $p_1, \ldots, p_s$ numeri primi e $s \geq 2$. supponiamo che c'è un altro

$n = q_1 \cdots q_r$ $q_1, \ldots, q_r$ numeri primi e $r \geq 2$.

p_1 è primo e $p_1 \mid n$ quindi $p_1 \mid q_1 \cdots q_r$ e quindi $p_1 \mid q_i$ per certo i, ma q_i è primo

quindi $p_1 = q_i$. Allora $\frac{n}{p_1} = p_2 \cdots p_s = q_1 \cdots q_{i-1} q_{i+1} \cdots q_r$ e $2 \leq \frac{n}{p_1} < n$

quindi $\frac{n}{p_1}$ ha una fattorizzazione unica in numeri primi. Cioè $r = s$

e i fattori $p_2, \ldots, p_s$ sono gli stessi come $q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_r$ fino al ordine

Ma $n = p_1 (p_2 \cdots p_s) = q_1 \cdots q_{i-1} q_i q_{i+1} \cdots q_r$. Quindi i fattori sono gli stessi fino al ordine.

Segue dal principio d'induzione che ogni intero $n \geq 2$ ha una fattorizzazione in numeri primi e fino al ordine dei fattori questa fattorizzazione è unica.