

## Algoritmo di divisione euclidea

lunedì 9 novembre 2020 15:18

Notazione

$a, b \in \mathbb{Z}$  si dice che  $a$  divide  $b$  se  $\exists c \in \mathbb{Z}$  t.c.  $b = c \cdot a$   
 (o  $b$  è un multiplo intero di  $a$ )  
 si scrive  $a | b$  divisor (o  $a$  non divide)

Ese

$$2|4, 3|4, +1|2 \quad b \in \mathbb{Z} \quad a = 1 \cdot 2$$

$$2|0 \quad b \in \mathbb{Z} \quad 0 = 0 \cdot 2$$

$0|0$  perché  $0 = 0 \cdot 0$  ma % non si può fare  
 (si può "annullare")

Teorema (Divisione Euclidea)

se  $a \neq 0$ , allora un multiplo

dati  $a, b \in \mathbb{Z}$ ,  $a > 0$ , allora  $\exists! q, r \in \mathbb{Z}$  t.c.  $0 \leq r < a$  e  $b = a \cdot q + r$   
 (ve l'aveva fatto anche con)

(nulla visto che  $a > b$ )

- $q$  viene detto resto delle divisione di  $b$  per  $a$ .
- $q$  viene detto quoziente

Dimo esistenza i)  $b \geq 0$  ii)  $b < 0$

i)  $b \geq 0$  induzione su  $b$

$$\text{passo base } b=0 \quad 0 = a \cdot 0 + 0 \quad \text{condizioni soddisfatte} \quad q \in \mathbb{Z}, r \in \mathbb{Z} \text{ e } 0 \leq r < a \quad \checkmark$$

passo induttivo supponiamo che  $\forall b \leq n \exists q, r \in \mathbb{Z}$  t.c.  $0 \leq r < a$ , proviamo per  $n+1$

$$\text{TEST } n+1 = a \cdot q + r \quad \text{con } q, r \in \mathbb{Z}, 0 \leq r < a$$

$$\text{--- } n+1 < a \quad n+1 = a \cdot q + (n+1) \quad \text{cioè abbiamo scelto } q=0, 0 \leq r = n+1 < a$$

$$\text{--- } n+1 > a \quad n+1 - a \underset{0 \leq \dots \leq n}{\leq} a \Rightarrow \exists q_1, r_1 \in \mathbb{Z}, 0 \leq r_1 < a \text{ t.c. } n+1 - a = q_1 \cdot a + r_1$$

$$\Rightarrow n+1 = q_1 \cdot a + r_1 + a = (q_1 + 1) \cdot a + r_1 \quad 0 \leq r_1 < a$$

$$2) b < 0 \quad -b > 0 \stackrel{1)}{\Rightarrow} \exists q, r \in \mathbb{Z}, 0 \leq r < a \text{ t.c. } -b = a \cdot q + r$$

$$\text{--- } r=0 \text{ allora } b = a \cdot (-q)$$

$$\text{--- } r>0 \text{ allora } b = -a \cdot q - r = -a \cdot q + a - a - r = a(-q-1) + (a-r)$$

$$q' = -q - 1 \quad \text{e} \quad r' = a - r$$

$$0 \leq r' < a$$

$$b = a \cdot q' + r' \quad 0 \leq r' < a$$

Dimo unicità (si suppone che ci siano 2 scritture e si dimostra che sono uguali)

$$\text{Supponiamo } b = q_1 \cdot q_1 + r_1 \quad b = q_2 \cdot q_2 + r_2 \quad q_1, q_2, r_1, r_2 \in \mathbb{Z} \quad 0 \leq r_1, r_2 < q$$

TESI:  $q_1 = q_2, r_1 = r_2$

Supponiamo che  $r_2 \geq r_1$

$$(b=b) \rightarrow \boxed{q_1 q_1 + r_1 = q_2 q_2 + r_2} \rightarrow q(q_1 - q_2) = r_2 - r_1 \geq 0 \rightarrow q(q_1 - q_2) \geq 0$$

quindi

$$0 \leq q(q_1 - q_2) < q$$

$\in \mathbb{Z}$  i negativi non sono considerati,  
ma qualsiasi intero sia ( $1 \cdot 2, 2 \cdot 2, 3 \cdot 2 \dots$ ) allora c'è  $> 2$ , quindi  
rispetta le condizioni delle esercitazioni

$$\rightarrow q(q_1 - q_2) = 0 \Rightarrow q_1 = q_2$$

$$q_1 = q_2 \quad \cancel{q_1 q_1 + r_1} = \cancel{q_2 q_2 + r_2} \rightarrow r_1 = r_2 \quad \square$$

Esempio  $b = 26 \quad q = 13$        $26 = 1 \cdot 13 + 11$        $q = 1, r = 11 \quad 0 \leq 11 < 13$   
 $(1 \cdot 13 = 13 > 26)$

Esempio  $b = -11 \quad q = 5$        $-11 = 5 \cdot (-3) + 4 \quad q = -3, r = 4 \quad 0 \leq 4 < 5$

vergo il resto positivo!

resto non positivo

non va bene

$$-11 = 5 \cdot (-2) + (-1)$$

ma

$$0 \leq -1 < 5$$

non e' la  
scrittura  
dell'algoritmo  
euclideo

scrivere solo che

Def. (Massimo comun divisore)  $a, b \in \mathbb{Z} \quad (a, b) \neq (0, 0)$

$\text{MCD}(a, b) = \max \{ n \in \mathbb{N} \mid (n \mid a) \wedge (n \mid b) \}$  il più grande n naturale che  
divide entrambi gli interi

si denota anche (in inglese)  $\text{GCD}(a, b)$

oppure  $(a, b)$  (senza parentesi)

per la fattorizzazione  
dei numeri non  
e' efficiente  
complicato e oneroso

Oss.  $\text{mcd}(b, a) = \text{mcd}(a, b)$  commutativa

$\text{mcd}(a, b) = a \iff a \mid b$

$\text{mcd}(a, 0) = a$

$\} \quad \forall a, b \in \mathbb{Z}, (a, b) \neq (0, 0)$

l'MCD e' più  
efficiente, sfruttando  
un sistema di

$$\text{MCD}(a, b) = s$$

$$\forall a, b \in \mathbb{Z}, (a, b) \neq (0, 0)$$

K si calcola più  
efficiente, sfruttando  
un sistema di  
divisioni  
(ALGORITMO EUCLideo)

Ese  $\text{MCD}(235, 100)$  posso fattorizzare i due numeri e vedere i  
divisori comuni ma non è efficiente

$$\begin{aligned} \text{allora } 235 &= 2 \cdot 100 + 35 \quad r_1 \\ \text{divido } b \text{ per } a & \downarrow \text{ divide } a \text{ per } r_1 \\ 100 &= 2 \cdot 35 + 20 \quad r_2 \\ &\downarrow \text{ divide } r_1 \text{ per } r_2 \\ 35 &= 1 \cdot 20 + 15 \quad r_3 \\ &\downarrow \text{ divide } r_2 \text{ per } r_3 \\ 20 &= 1 \cdot 15 + 5 \quad r_4 \\ &\downarrow \text{ divide } r_3 \text{ per } r_4 \\ 15 &= 3 \cdot 5 + 0 \quad r_5 \\ &\downarrow \text{ divide } r_4 \text{ per } r_5 \\ 5 &= 0 \end{aligned}$$

} ALGORITMO

$r_4 = 0 \Rightarrow r_3$  ultimo resto  
non nullo

$$\hookrightarrow r_3 = \text{MCD}(235, 100)$$

Algoritmo Euclideo : procedimento generale

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

$$\begin{aligned} b &= a \cdot q_1 + r_1 && q_1, r_1 \in \mathbb{Z}, 0 \leq r_1 < a \quad (\text{Divisione per } a) \\ &\downarrow && \text{UNICITÀ} \\ r_1 &= 0 && \text{MCD}(a, b) = r_1 \quad (b \text{ multiplo di } a) \\ r_1 &\neq 0 && \text{la procedura continua} \end{aligned}$$

$$a = r_1 \cdot q_2 + r_2 \quad 0 \leq r_2 < r_1 \quad (\text{Divisione per } r_1)$$

$$r_2 = 0 \quad (\text{MCD}(a, b) = r_1)$$

$$r_1 = r_2 \cdot q_3 + r_3 \quad 0 \leq r_3 < r_2$$

$$r_3 = 0 \quad \dots$$

$$r_{n-1} = r_n \cdot q_{n+1} + r_n \neq 0$$

Ad un certo punto otterro'  $r_{n+1} = 0$  perché  $a > r_1 > r_2 > \dots > r_{n-2} > r_{n-1} > r_n \geq 0$   
ovvero otteno un minimo in  $\mathbb{N}$ .

SUCCESSIONE STRUTTURANTE DECRESCENTE

overo ottengo un minimo in  $N$ ,  
 overo ZERO (non possono  
 continuare in maniera stretta, senza  
 uguali orsi)

## SUCCESSIONE STRUTTURANTE DISCORSANTE

## Prov

$$z_n = \text{HCD}(a, b)$$

$$f_{CD}(a,b) = \max \{ n \in \mathbb{N} \mid (n \mid a) \wedge (n \mid b) \}$$

Dim Dimostriamo:

1)  $z_n|_x$  e  $z_n|_b$

2) se  $c \in \mathbb{N}$  t.c.  $c|a$  e  $c|b$  allora  $c|r_n$  (questo è un mox)

$$1) + 2) \rightarrow B_n = \text{rcd}(a, b)$$

$$1] \quad r_{n-2} = \underline{r_{n-1}} - q_n + r_n = r_n(q_{n+1} + 1) \quad \rightarrow r_n | r_{n-2}$$

*multiple integers*

$$r_n \cdot q_n = r_{n-2} \quad r_n | (r_n \cdot q_n)$$

Continuando così: (e ritratti rispetto agli esempi precedenti)

$$r_n | r_{n-1}, \quad r_n | r_{n-2}, \quad r_n | r_{n-3}, \dots, \quad r_n | r_1, \quad r_n | a, \quad r_n | b$$

2]  $\exists a \in N$  t.c.  $a \in A \setminus B \rightarrow a \in B$  ?

$$c \cdot a + c \cdot b \rightarrow a = c \cdot a', b = c \cdot b' \quad a', b' \in \mathbb{Z} \quad (\text{auch negativ})$$

$$b = a_1 q_1 + r_1 \rightarrow r_1 = b - a_1 q_1 = c \cdot b' - c a_1' q_1 = c(b' - a_1 q_1) \rightarrow c | r_1$$

$$R = R_1 \cdot p_2 + R_2 \rightarrow R_2 = R - R_1 \cdot p_2 = c \cdot q^1 - c \cdot R_1^1 \cdot p_2 = c(q^1 - R_1^1 \cdot p_2) \rightarrow c \mid R_2$$

Continuando così giungo a:

dei possibili prec. (ma scritti)

$$r_{n-2} = r_{n-1} \cdot q_n + r_n \rightarrow r_n = r_{n-2} - r_{n-1} \cdot q_n \quad \longrightarrow \quad c | r_n$$

(verificare anche con INDUZIONE)

四

V.50 sopra

$$\text{Eis} \quad \text{HCD}(235, 100)$$

Esempio  $\text{MCD}(363, 657)$

$$657 = 657 \cdot 1 + 306 \quad \text{R} = 0$$

$$306 = 306 \cdot 2 + 45 \quad \text{R} = 0$$

$$45 = 45 \cdot 6 + 36 \quad \text{R} = 0$$

$$36 = 36 \cdot 1 + 0 \quad \text{R} = 0$$

$$\therefore 36 = 3 \cdot 12 + 0$$

$$\rightarrow \text{R}_1 = 3 = \text{MCD}(363, 657)$$

Tale algoritmo permette di risolvere anche le equazioni omogenee (di soluzioni intere)

### Teorema (Identità di Bezout)

Dati  $a, b \in \mathbb{Z}$ ,  $(a, b) \neq (0, 0)$ , si ha  $d = \text{MCD}(a, b)$ . Allora  $\exists x, y \in \mathbb{Z}$  t.c.

$$d = ax + by$$

SOMMA DI PRODOTTI

$a, b$  fissati

$x, y$  si possono trovare

Esempio  $a = 100, b = 235$  troviamo  $x, y \in \mathbb{Z}$  t.c.  $s = 100x + 235y$

Ricavo 5 dall'algoritmo euclideo, ovvero eseguo i passaggi al contrario [vedi ex. prec.]

$$s = 3s - 1 \cdot 30 \rightarrow \text{ero un resto} = 3s - 1(100 - 2 \cdot 35) = 3 \cdot 35 - 1 \cdot 100$$

scrivo allora il 30

dovendo espanderlo il più possibile, non conto

$$= 3(235) - 2(100) - 1 \cdot 100 = 3 \cdot 235 - 7 \cdot 100 \rightarrow x = -7 \text{ e } y = 3$$

$$\text{ovvero } = -7a + 3b$$

Se avessi dovuto trovare  $s$  dall'equazione posso andare "a tentativi" (poco efficiente)

o usare l'algoritmo euclideo.

Esempio Cerchiamo  $x, y \in \mathbb{Z}$  t.c.  $363x + 657y = 3$  dove  $s = \text{MCD}(363, 657)$

Guardo le righe prec. e giro l'espressione

$$\begin{aligned} s &= 45 - 36 = 45 - (363 - 657 \cdot 6) = -363 + 657 \cdot 7 = -363 + 7(657 - 363 \cdot 2) \\ &= 657 - 363 + (657 - (363 - 657) \cdot 2) \cdot 7 = 657 - 363 + 657 \cdot 7 - 363 \cdot 9 + 657 \cdot 14 \\ &= 657 \cdot 22 + 363(-15) \rightarrow x = -15, y = 22 \end{aligned}$$

RISOLVIMENTO EQUAZIONI LINEARI (grado=1) di forma  $ax + by = c$   $a, b, c \in \mathbb{Z}$  trovare  $x, y \in \mathbb{Z}$

1.  $\sim$  7  $\sim$   $\sim$

RISOLVENDO EQUAZIONI LINEARI (grado=1) di forma

$$ax + by = c$$

$a, b, c \in \mathbb{Z}$  trovare  $x, y \in \mathbb{Z}$

↳ Quando  $\exists$  soluzioni?

↳ se  $\exists$ , come le trovo tutte?

Prop  $a, b, c \in \mathbb{Z}$  allora

l'equazione  $ax + by = c$  ha soluzioni  $x, y \in \mathbb{Z} \iff \text{mcd}(a, b) \mid c$  (ovvero  $c$  multiplo)

Dim " $\leftarrow$ "  $\text{d} = \text{mcd}(a, b)$ ,  $d \mid c \rightarrow c = d \cdot d$ ,  $x \in \mathbb{Z}$

• per BESOUT  $\exists x, y \in \mathbb{Z}$  t.c.  $ax + by = d$

• multiplo per  $d$ :  $a(\alpha x) + b(\alpha y) = da$  ma  $d \mid c$  scelgo  $X = \alpha x, Y = \alpha y \in \mathbb{Z}$   
 $\rightarrow aX + bY = c$

" $\rightarrow$ " Sono  $x, y \in \mathbb{Z}$  una soluzione (una coppia), cioè  $\boxed{ax + by = c}$

Sia  $d = \text{mcd}(a, b)$  proviamo che  $d \mid c$

$$\alpha = \alpha d, \beta = \beta d \quad \alpha, \beta \in \mathbb{Z}$$

$$\begin{array}{rcl} \alpha d x + \beta d y & = & c \\ \downarrow & & \downarrow \\ d(\alpha x + \beta y) & = & c \\ X & & Y \end{array} \quad \rightarrow d \mid c \quad \square$$

Ese  $21x + 13y = 5$  Cerchiamo le soluzioni intere.

$$\text{mcd}(21, 13) = 1 \quad (13 \text{ è primo e } 13 \nmid 21) \rightarrow 1 \mid 5 \xrightarrow{\text{mcp}} \exists x, y \in \mathbb{Z}$$

Prima risolviamo  $21x + 13y = 1$

$$\underline{21} = 1 \cdot \underline{13} + \underline{8}$$

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$\text{BESOUT } 1 = 3 - 1 \cdot 2 = 3 - (5 - 3) = 2 \cdot 3 - 5$$

$$= (8 - 5) \cdot 2 - 5 = -3 \cdot 5 + 2 \cdot 8 = \dots$$

$$= -8 \cdot \underline{13} + 5 \cdot \underline{21}$$

$$1 = -8 \cdot 13 + 5 \cdot 21 \quad \text{mult. per } 5$$

$$5 = -8 \cdot 5 \cdot \underline{13} + 5 \cdot 5 \cdot \underline{21}$$

$$= -40 \cdot (\underline{13}) + 25 \cdot (\underline{21})$$

$$\begin{aligned} \text{soltuzione} \\ x = 25 \\ y = 40 \end{aligned}$$

$$5 = 13 - 8 = 13 - (21 - 13) = 2 \cdot \underline{13} - \underline{21} \rightarrow x' = -1, y' = 2$$

seconda  
soluzione  
(di fronte)

Come trovare tutte le soluzioni INTERE?

Come trovare tutte le soluzioni INTEREZI?

$$\boxed{ax+by=c} \quad a, b, c \in \mathbb{Z} \quad \text{ha soluzioni} \iff d = \text{mcd}(a, b) \mid c$$

Supponiamo  $d \mid c$

$$d \mid a, d \mid b \quad (\text{perche } d = \text{mcd}(a, b)) \quad a = da', \quad b = db'$$

$$a'dx + b'dy = c'd \quad d \text{ so essere} > 0 \quad \rightarrow a'x + b'y = c'$$

Tutte le soluzioni di  $a'x + b'y = c'$  sono soluzioni di  $a'x + b'y = c'$   
ma  $\text{mcd}(a', b') = 1$

Dove in poi supponiamo direttamente che  $\text{mcd}(a, b) = 1$

Prov Sia  $(x_0, y_0) \in \mathbb{Z}^2$  una soluzione di  $ax+by=c$ , dove  $a, b, c \in \mathbb{Z}$ ,  $\text{mcd}(a, b)=1$

Allora tutte le soluzioni sono delle forme:

$$(x_0 + bK, y_0 - aK) \quad K \in \mathbb{Z}$$

copia  
altamente risolto &  
percorso delle soluzioni

Come procedere per calcolare  $\boxed{ax+by=c} *$

- 1) Calcolare  $d = \text{mcd}(a, b)$  e controllare che  $d \mid c$
  - 2) Dividere \* per  $d$   $a = da'$ ,  $b = db'$
  - 3) Trovare una soluzione particolare  $(x_0, y_0)$  con Bezout
  - 4) Tutte le soluzioni sono  $\begin{cases} x = x_0 + b'k \\ y = y_0 - a'k \end{cases}$
- ove  $\text{mcd}(a', b') = 1$   
grazi

Ese  $175x + 77y = 323$

1] Calcolo  $\text{mcd}(175, 77)$

$$175 = 77 \cdot 2 + 21$$

$$77 = 21 \cdot 3 + 14$$

$$21 = 14 \cdot 1 + 7 \quad \rightarrow \text{mcd}$$

$$14 = 7 \cdot 2 + 0$$

$$\therefore d = \text{mcd}(175, 77) = 7$$

$$323 = 7 \cdot 47$$

$$7 \mid 323 \quad \checkmark$$

l'equazione ha soluzione (N.B. se ne ha 00)

2]  $175x + 77y = 323$

$$25x + 11y = 47$$

Dividiamo per 7: ora posso semplificare dividendo per il mcd.

3] Troviamo una soluzione  $(x_1, y_1)$  con Bézout

$$\begin{array}{l} 25x_1 + 11y_1 = 1 \\ 25 = 2 \cdot 11 + 3 \\ 11 = 3 \cdot 3 + 2 \\ 3 = 1 \cdot 2 + 1 \\ 2 = 2 \cdot 1 + 0 \end{array}$$

Bezout

$$\begin{aligned} 1 &= 3 - 2 = 3 - (11 - 3 \cdot 3) = 4 \cdot 3 - 11 \\ &= 4(25 - 2 \cdot 11) - 11 = 4 \cdot 25 - 3 \cdot 11 \\ (x_1, y_1) &= (4, -3) \end{aligned}$$

Una soluzione di  $25x_0 + 11y_0 = 47$  è  $x_0 = 47 \cdot x_1 = 47 \cdot 4 = 188$

(moltiplicando per 47)  
e' invece  $x_0$

$$y_0 = 47 \cdot y_1 = 47(-3) = -423$$

4] Tutte le soluzioni di  $25x + 11y = 47$  sono:

$$\begin{array}{l} x = x_0 + b'k \\ y = y_0 - a'k \end{array} \quad k \in \mathbb{Z} \quad \left\{ \begin{array}{l} x = 188 + 11k \\ y = -423 - 25k \end{array} \right. \quad k \in \mathbb{Z}$$

e . e . e . e

EQUAZIONE DIOPANTIENE LINEARE

$\downarrow$   
relative agli interi

$$(*) \quad ax + by = c$$

le soluzioni  $(x, y) \in \mathbb{Z}^2 \iff \text{MCD}(a, b) \mid c$

In tal caso

- si divide (\*) per  $d = \text{MCD}(a, b)$
- $ax + by = c$  con  $\text{MCD}(a, b) = 1$
- trovare una soluzione  $(x_0, y_0) \in \mathbb{Z}^2$  con Bézout
- tutte le soluzioni sono  $(x, y) = (x_0 + bk, y_0 - ak)$ ,  $k \in \mathbb{Z}$

$$\begin{aligned} ax + by &= c \\ a(x_0 + bk) + (y_0 - ak)b &= c \\ ax_0 + bax + by_0 - abk &= c \\ ax_0 + by_0 &= c \end{aligned}$$

Prov Aumento di variabili: Presi  $a_1, \dots, a_n, b \in \mathbb{Z}$  t.c.  $(a_1, \dots, a_n, b) \neq (0, \dots, 0)$

Allora  $a_1 x_1 + \dots + a_n x_n = b$  ha soluzioni intere  $\iff \text{MCD}(a_1, \dots, a_n) \mid b$ .

Def  $\text{MCD}(a, b, c) := \text{MCD}(a, \text{MCD}(b, c)) = \text{MCD}(\text{MCD}(a, b), c)$

"max f<sub>n</sub> ∈ N t.c.  $(n \mid a) \wedge (n \mid b) \wedge (n \mid c)$ "

$$\hookrightarrow n \mid a \iff a \equiv 0 \pmod{n} \iff a = n \cdot k \quad [\text{notazione}]$$

Def. Minimo comune multiplo:  $a, b \in \mathbb{Z}$   $\quad \text{mcm}(a, b) = \min \{n \in \mathbb{N} \mid (a \mid n) \wedge (b \mid n)\}$

Per calcolarlo si usa la formula:

$$\text{mcm} = \frac{a \cdot b}{\text{MCD}(a, b)} \rightarrow \begin{array}{l} \text{il più grande fattore} \\ \text{comune fra } a \text{ e } b \end{array}$$

## Numeri primi e fattorizzazione

Def  $a \in \mathbb{Z}$ ,  $a \neq \pm 1$ ,  $a$  si dice RIDUCIBILE se  $a = b \cdot c$  con  $b, c \in \mathbb{Z}$ ,  $b, c \neq \pm 1$

Irriducibile se si dice irriducibile o primo se non è riducibile  
(i negativi sono  $-1$  n. primo)  
(per convenzione 1 non è primo)  
per convenzione si considerano  
pochi quelli positivi)

Ese  $4 = 2 \cdot 2$  RIDUCIBILE,  $2, 3, 5, 7, 11$  sono primi (non riducibili)

Lema  $a, b \in \mathbb{Z}$ ,  $p$  è primo t.c.  $p \mid a \cdot b$ . Allora  $p \mid a$  o  $p \mid b$  (o entrambi)

DIM Supponiamo che  $p \nmid a$  e proviamo che  $p \mid b$  (per rendere la diseguaglianza vera)

LEMMA  $a, b \in \mathbb{Z}$ ,  $p \in \mathbb{P}$  primo t.c.  $p \mid a \cdot b$ . Allora  $p \mid a$  o  $p \mid b$  (o entrambi)

DIM Supponiamo che  $p \nmid a$  e proviamo che  $p \nmid b$  (per rendere la diseguazione vera) (n.b. per simmetria è il viceversa)

$p \nmid a \rightarrow \text{gcd}(p, a) = 1$  ( $p$  è primo,  $a$  e  $p$  non hanno fattori comuni altri di 1)

BY-OUT

$$\rightarrow \exists x, y \in \mathbb{Z} \text{ t.c. } ax + py = 1$$

• moltiplichiamo i vari membri per  $b$ :  $\underbrace{abx + pby = b}_{\substack{\text{multiplo di } p \\ \text{ "kp}}} \quad \underbrace{abx + pby = b}_{\substack{\text{multiplo di } p \\ \text{ "kp}}}$

$$\rightarrow kp + pby = b \rightarrow p(\kappa x + by) = b \rightarrow p \mid b \quad \square$$

$\left[ \begin{array}{l} p \mid b \Leftrightarrow b = p \cdot h \text{ con } h \in \mathbb{Z} \\ \text{quindi } p \text{ divide } b \text{ perché } b \text{ è prodotto} \\ \text{di } p \text{ per qualcosa di intero.} \end{array} \right]$

TEOREMA DI FATTORIZZAZIONE UNICA (Teorema fondamentale dell'aritmetica)

Sia  $a \in \mathbb{Z} \setminus \{0, -1, +1\}$  allora  $a$  si scrive in modo unico come prodotto di (un numero finito) di numeri primi.

Lo a meno dell'ordine  
e del segno

$$\rightarrow \begin{cases} \text{es} & -3 \cdot 2 = -2 \cdot 3 \\ \text{e} & 3 \cdot 2 = 2 \cdot 3 \end{cases}$$

Ese.  $6 = 2 \cdot 3 = 3 \cdot 2 = (-2) \cdot (-3) = (-3) \cdot (-2)$

DIM Basta dimostrarlo per  $a > 1$  (se  $a < 0$  considero  $(-a) > 0$ ,  $a = (-1) \cdot (-a)$ )

[DIM per INDUZIONE]

- PASSO BASE per  $a \in \mathbb{Z}$ ,  $a$  è primo ✓

- PASSO INDUTTIVO Supponiamo il teorema vero  $\forall a \leq a$  è divisibile per  $a+1$

$a+1$  è primo ✓

$a+1$  non è primo  $\rightarrow a+1$  è riducibile  $= b \cdot c$ ,  $b, c \in \mathbb{Z} \setminus \{ \pm 1 \}$   $\rightarrow b, c < a+1$

per NP

$$\rightarrow \text{non tutti} \quad b = p_1 \cdot \dots \cdot p_s \text{ primi}$$

$$c = p_{s+1} \cdot \dots \cdot p_t \quad (\text{non necessariamente distinti}, \quad \text{es } p_1 = p_{s+1})$$

$$\rightarrow a+1 = b \cdot c = p_1 \cdot \dots \cdot p_s \cdot p_{s+1} \cdot \dots \cdot p_t$$

primi

Questo dimostra l'esistenza dei primi

UNICITÀ:  $a+1 = p_1 \cdot \dots \cdot p_r$  primi  $a+1 = q_1 \cdot \dots \cdot q_t$  primi Tesi:  $r = t$  e  $p_1 \cdot \dots \cdot p_r = a+1 = q_1 \cdot \dots \cdot q_t \rightarrow p_1 \mid q_1 \cdot \dots \cdot q_t$  in quanto se è falso  $p_1 = q_i$

LEZIONE

PRIMO

→ per il lemma precedente  $p_1$  divide uno ( $\circ$  min) + tra  $q_1, \dots, q_t$

Diciamo che  $p_1 \mid q_i$ , un numero che divide un primo è il numero primo  $\Rightarrow 1$ , ma si non puo' essere per definizione

$$\rightarrow p_1 = q_1$$

e continuo:  $p_1 \cdot p_2 \cdot \dots \cdot p_r = p_1 \cdot q_2 \cdot \dots \cdot q_t$

procedendo in questo modo si ottiene  $p_2 = q_2, \dots, p_r = q_r$ ,  $r = t$  dopo le semplificazioni

$$\circ \quad r \leq t \quad \circ \quad t \leq r$$

$$\hookrightarrow p_r = q_r \cdot q_{r+1} \cdot \dots \cdot q_t$$

$$p_r \mid q_r \cdot \dots \cdot q_t \rightarrow p_r \mid q_r$$

$$p_r \cancel{=} p_r \cdot q_{r+1} \cdot \dots \cdot q_t$$

$$1 = \underset{y}{q_{r+1}} \cdot \dots \cdot \underset{y}{q_t} \rightarrow r = t$$

[ Il teorema della fattorizzazione è computationalmente molto complesso e dispendioso come tempo. Si usa spesso tale complessità nella crittografia ]

**TEOREMA DI EUCLIDE:** I numeri primi sono infiniti

"More than the books"

Dim Supponiamo per assurdo che  $p_1, \dots, p_n$  siano tutti e soli i numeri primi (finiti)

$$\text{Consideriamo } N = p_1 \cdot \dots \cdot p_n + 1 \in \mathbb{Z}$$

per il teorema di fattorizzazione ( $N$  non è primo perché diverso da  $p_1, \dots, p_n$ , ed  $\epsilon > 1$ )

$$\exists i \in \{1, \dots, n\} \text{ t.c. } p_i \mid N$$

$$\begin{array}{ll} \text{Supponiamo } i=1 & N = p_1 \cdot m, \quad m \in \mathbb{Z} \\ & \parallel \\ & p_1 \cdot \dots \cdot p_{n+1} \end{array}$$

$$\rightarrow p_1 \cdot m - p_1 \cdot \dots \cdot p_n = 1 \rightarrow p_1(m - p_2 \cdot \dots \cdot p_n) = 1 \rightarrow p_1 \mid 1$$

1 non è un numero per qualcosa!

! Abbiamo dimostrato che  $N$  non è divisibile per quei numeri primi, non è dato che  $N$  sia primo ma sicuramente  $\exists p \in \{p_1, \dots, p_n\}$  primo tale che  $p \mid N$ .

$$\underline{\text{Es}} \quad N = 2 \cdot 3 \cdot 5 + 1 = 31 \text{ PRIMO}$$

$N = 3 \cdot 5 + 1 = 16$  non è primo,  $2 \mid N$  ma 2 non è fra i primi divisori di  $N$

**TEOREMA (DIRICHLET)** Dati  $a, b \in \mathbb{Z}$ ,  $\text{gcd}(a, b) = 1$ . Allora  $\exists \infty$  primi della forma  $an + b$ ,  $n \in \mathbb{Z}$

nuove forme  $a_n + d$ ,  $n \in \mathbb{C}$

Esempio se primi della forma  $a_n + 1$ ,  $a_n + 3$  |  $a_{n+2}$  e 2 non sono composti, quindi  
l'unico n primo è 2

Esistono successioni di interi consecutivi che non contengono primi arbitrariamente larghi.

Ad esempio, dato  $n \in \mathbb{Z}$ ,  $n \geq 2$

$$\underbrace{n!+2}_{2|}, \underbrace{n!+3}_{3|}, \dots, \underbrace{n!+n}_{n!}$$

$n-1$  interi consecutivi composti

«ridicibili»

Def  $p$  e  $p+2$  vengono detti "primi gemelli" se  $p$  e  $p+2$  sono primi.

Esempio 3 e 5, 5 e 7, 17 e 19

$$2^{336863034885} \cdot 2^{1230000} \pm 1 \text{ primi gemelli}$$

PROBLEMI APERTI:

- Esistono primi gemelli?
- Congettura di Goldbach: ogni intero  $\geq 4$  puo' essere scritto come somma di 2 numeri primi.