aritmetica

liceo Lioy e liceo Pigafetta, 10 febbraio 2011

DIVISIBILITÀ

b divide a se e solo se esiste x tale che $a = b \cdot x$

Scriveremo: $b \mid a$

PROPRIETÀ

- Se $b \mid a$ e $a \mid c$ allora $b \mid c$
- Se $b \mid a$ e $b \mid c$ allora $b \mid (ax + cy)$ per ogni $x, y \in \mathbf{Z}$
  In particolare $b \mid (a + c)$ e $b \mid (a - c)$

ESEMPIO

Trovare il Massimo Comune Divisore di 10002 e 9999

Ogni divisore comune di due numeri deve essere divisore anche della loro differenza
Dunque un divisore comune di 10002 e 9999 deve dividere anche 10002 – 9999 = 3
È immediato verificare che 3 divide sia 10002 sia 9999
Perciò **MCD(10002, 9999) = 3**

UNA DEFINIZIONE IMPORTANTE

Si dice *primo* un numero naturale p, maggiore di 1, che non ammette divisori diversi da se stesso e da 1

Sono *primi* 2, 3, 5, 7, 11, …

12 è, invece, *composto* (divisibile per 1, 2, 3, 4, 6, 12)

TEOREMA DI EUCLIDE: Esistono infiniti numeri primi (per la dimostrazione si rimanda all'appendice 1)

TEOREMA FONDAMENTALE DELL'ARITMETICA: Ogni numero intero $n > 1$ può essere scomposto in modo UNICO, a meno dell'ordine, in un prodotto di primi

COROLLARIO: Se $p \mid ab$ allora $p \mid a$ o $p \mid b$

OSSERVAZIONI

Il teorema di Euclide è elegante ma non costruttivo
Numeri primi → infiniti

ma come sono "fatti"?
Non si è trovata una formula semplice che fornisca **solo** numeri primi; tanto meno una formula che fornisca **tutti** i numeri primi

Come sono distribuiti?
Sia A_n l'insieme dei numeri primi in {1, 2, 3, …, n}
Gauss, Hadamard, Poussin (miglioramenti successivi):
$A_n/n \sim 1/ln(n)$

QUESTIONI APERTE E CURIOSITÀ

- Due numeri primi p_1 e p_2 si dicono gemelli se $p_2 - p_1 = 2$
  Esempi: 11, 13; 17, 19; 41, 43 …
  Non si sa se i primi gemelli sono infiniti

- **Congettura di Goldbach**
  Ogni numero pari > 2 è somma di due numeri primi
  Esempi:
  $14 = 7 + 7$
  $24 = 11 + 13$
  $42 = 5 + 37 = 11 + 31 = 13 + 29 = 19 + 23$
  Tuttora non dimostrata

CONGRUENZE

Concetto utile per affrontare la questione della divisibilità di un numero intero n per un prefissato intero $d \neq 0$

Due numeri interi a e b sono *congrui modulo* d se, divisi per d, danno lo stesso resto
Scriveremo: $a \equiv b \pmod{d}$
Equivalentemente, $a \equiv b \pmod{d}$ se e solo se $d \mid (a - b)$
Esempi:
Le lancette dell'orologio indicano l'ora modulo 12
Il contachilometri di un'automobile segna i chilometri percorsi modulo 100 000

ESEMPI NUMERICI

2, 7, 12, 17, 22, … , – 3, – 8, … sono congrui modulo 5

3, 8, 13, 18, 23, … , – 2, – 7, … sono congrui modulo 5

0, 7, 14, 21, 28, … , – 7, – 14, … sono congrui modulo 7

4, 11, 18, 25, 32, … , – 3, – 10, … sono congrui modulo 7

AFFERMAZIONI EQUIVALENTI

- a è congruo a b modulo d
- $a = b + nd$ per qualche intero n
- d divide $a - b$

PROPRIETÀ

1. $a \equiv a \pmod{d}$
2. se $a \equiv b \pmod{d}$, allora $b \equiv a \pmod{d}$
3. se $a \equiv b \pmod{d}$ e $b \equiv c \pmod{d}$, allora $a \equiv c \pmod{d}$

→ la relazione di congruenza è una relazione di **equivalenza**

Inoltre, se $a \equiv a' \pmod{d}$
e $b \equiv b' \pmod{d}$:

4. $a + b \equiv a' + b' \pmod{d}$
5. $a - b \equiv a' - b' \pmod{d}$
6. $ab \equiv a'b' \pmod{d}$

DIMOSTRAZIONE di (4), (5), (6) (immediata)

Dalla relazione di congruenza, discende subito:

$a = a' + rd$

$b = b' + sd$

Allora:

$a + b = a' + b' + (r + s)d$

$a - b = a' - b' + (r - s)d$

$ab = a' b' + (a's + rb' + rsd)d$

CONCLUSIONE

Per ciascun intero *d*, l'insieme ***Z*** dei numeri interi viene ripartito dalla relazione di congruenza modulo *d* in classi di equivalenza

CLASSI RESTO

tra le quali sarà possibile definire delle

OPERAZIONI

naturalmente ereditate dalle analoghe operazioni in **Z**

ESEMPI di classi resto

$\boldsymbol{Z}$ (mod 5) = { $[0]_5$, $[1]_5$, $[2]_5$, $[3]_5$, $[4]_5$ }

dove:

$[0]_5 = \{0, 5, 10, 15, 20, \ldots, -5, -10, -15, \ldots\}$

$[1]_5 = \{1, 6, 11, 16, 21, \ldots, -4, -9, -14, \ldots\}$

e così via

OPERAZIONI con le classi resto

Si estendono in modo abbastanza naturale le usuali operazioni in **Z** :

$[a]_d + [b]_d = [a + b]_d$

$[a]_d \cdot [b]_d = [a \cdot b]_d$

… con alcune cautele!

ESEMPI

$[3]_6 + [10]_6 = [3]_6 + [4]_6 = [7]_6 = [1]_6$

$[5]_7[18]_7 = [5]_7[4]_7 = [20]_7 = [6]_7$

ATTENZIONE!!

$[15]_{12}[8]_{12} = [3]_{12}[8]_{12} = [24]_{12} = [0]_{12}$

Nell'aritmetica delle classi resto, **PUÒ NON VALERE** LA **LEGGE DI ANNULLAMENTO DEL PRODOTTO**

Tuttavia il problema non si pone se il numero *d* è **primo**

Casi particolari delle proprietà (4) e (6)

Per ogni $z \in Z$

- se $a \equiv b \pmod{d}$ allora $a + z \equiv b + z \pmod{d}$
- se $a \equiv b \pmod{d}$ allora $az \equiv bz \pmod{d}$

ATTENZIONE!!

La seconda proposizione in generale non si può invertire

$7 \cdot 2 = 14$

$1 \cdot 2 = 2$

$14 \equiv 2 \pmod{12}$

Tuttavia 7 NON è congruo a 1 modulo 12!

L'invertibilità non sussiste perché 2 è divisore di 12

- Altra definizione utile da ricordare:
  due interi a e b si dicono **primi tra loro** (coprimi) se
  MCD $(a , b) = 1$
  si scrive $(a, b) = 1$

Se z è primo con d, allora la proposizione si può invertire:
se $a \equiv b \pmod{d}$ se e solo se $az \equiv bz \pmod{d}$

dimostrazione (facile)

Sia $az \equiv bz \pmod{d}$
Allora d divide $az - bz = (a - b)z$
Per ipotesi $(z , d) = 1$
Dunque d divide $a - b$
$\rightarrow a \equiv b \pmod{d}$

CRITERI DI DIVISIBILITÀ

Dato un numero intero *z*, la sua rappresentazione in forma decimale è una successione di cifre $(a_n a_{n-1} \ldots a_1 a_0)$ con il seguente significato:

$z = a_0 + a_1 10 + a_2 10^2 + \ldots + a_n 10^n$

Quando z è divisibile per 2?

Proprietà delle congruenze

$10 \equiv 0 \pmod 2$

$10^2 \equiv 0 \pmod 2$

…

$10^n \equiv 0 \pmod 2$

z è divisibile per 2 se e solo se lo è l'ultima cifra a_0

Quando z è divisibile per 3?

Proprietà delle congruenze

$10 \equiv 1 \pmod 3$

$10^2 \equiv 1 \pmod 3$

…

$10^n \equiv 1 \pmod 3$

$t = a_0 + a_1 + a_2 + \ldots + a_n$

$z - t = a_1 (10 - 1) + a_2 (10^2 - 1) + \ldots + a_n (10^n - 1)$

$z - t$ è congruo con 0 modulo 3

z e t nella divisione per 3 danno lo stesso resto

z è divisibile per 3 se e solo se lo è t

z è divisibile per 3 se e solo se

$a_0 + a_1 + a_2 + \ldots + a_n$ è divisibile per 3

Quando z è divisibile per 5?

Proprietà delle congruenze

$10 \equiv 0 \pmod 5$

$10^2 \equiv 0 \pmod 5$

…

$10^n \equiv 0 \pmod 5$

$z = a_0 + a_1 10 + a_2 10^2 + \ldots + a_n 10^n$

z è divisibile per 5 se e solo se $a_0 \equiv 0 \pmod 5$, cioè se e solo se a_0 è uguale a 0 oppure a 5

Quando z è divisibile per 9?

Proprietà delle congruenze

$10 \equiv 1 \pmod 9$

$10^2 \equiv 1 \pmod 9$

…

$10^n \equiv 1 \pmod 9$

$t = a_0 + a_1 + a_2 + \ldots + a_n$

$z - t = a_1 (10 - 1) + a_2 (10^2 - 1) + \ldots + a_n (10^n - 1)$

$z - t$ è congruo con 0 modulo 9

z e t nella divisione per 9 danno lo stesso resto

z è divisibile per 9 se e solo se lo è t

z è divisibile per 9 se e solo se

$a_0 + a_1 + a_2 + \ldots + a_n$ è divisibile per 9

Quando z è divisibile per 11?

Proprietà delle congruenze

$10 \equiv -1 \pmod{11}$

$10^2 \equiv (-1)(-1) = 1 \pmod{11}$

$10^3 = (10)(10^2) \equiv (-1)(1) = -1 \pmod{11}$

$10^4 = (10^2)^2 \equiv (1)(1) = 1 \pmod{11}$ …

$t = a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^n \cdot a_n$

$z - t =$

$= a_1 (10 + 1) + a_2 (10^2 - 1) + a_3 (10^3 + 1) + a_4 (10^4 - 1) + \ldots$

$z - t$ è congruo con 0 modulo 11

z è divisibile per 11 se e solo se lo è t

z è divisibile per 11 se e solo se

$a_0 - a_1 + a_2 - a_3 \ldots + (-1)^n a_n$ è divisibile per 11

ESERCIZIO

Stabilire un criterio di

- divisibilità per 7
- divisibilità per 13

ESERCIZIO

Quanti numeri pari si possono formare con le cifre 1, 2, 3 e 7 utilizzandole tutte e ciascuna una sola volta?

2 deve essere la cifra finale
possiamo solo permutare le cifre 1, 3, 7 ai posti rispettivamente delle migliaia, centinaia e decine
per la prima cifra abbiamo 3 possibilità
per la seconda cifra ce ne restano 2
la terza cifra a questo punto è vincolata

La risposta corretta sarà 6

ESERCIZIO

Se $n > 0$ è dispari ed $r = n + 11^n$ allora:

a) r è pari

b) r è dispari

c) r^n è dispari

d) nessuna delle precedenti affermazioni è vera per tutti gli n dispari

$n \equiv 1 \pmod 2$

$11 \equiv 1 \pmod 2$

$11^n \equiv 1 \pmod 2$

$[n + 11^n] = [1] + [1] = [2] = [0]$

Dunque r è pari

ULTERIORE OSSERVAZIONE

Se $n > 0$ è dispari ed $r = n + 11^n$ allora:

a) **r è pari**
b) **r è dispari**
c) **r^n è dispari**
d) **nessuna delle precedenti affermazioni è vera per tutti gli n dispari**

Si noti che

se fosse vera (b), allora dovrebbe essere vera anche (c)

ESERCIZIO

Sia $n > 0$ è dispari e sia $r = (n + 7n^3)^n$; allora:

a) r^2 è dispari

b) r è dispari

c) r è pari

d) nessuna delle precedenti affermazioni è vera per tutti gli n dispari

Di nuovo, (a) e (b) …

?

ESERCIZIO

Due persone sono nate in anni diversi ma festeggiano il compleanno lo stesso giorno. Se oggi la somma delle loro età è dispari, quale delle seguenti affermazioni è vera?

a) la differenza delle loro età è dispari
b) il prodotto delle loro età è pari
c) la somma delle loro età tra un anno sarà pari
d) il prodotto delle loro età tra un anno sarà pari

?

La risposta corretta è evidente …

APPENDICE 1

DIMOSTRAZIONE DEL TEOREMA DI EUCLIDE:
Esistono infiniti numeri primi

Supponiamo, per assurdo, che esista un numero finito di primi: $p_1, p_2, \ldots, p_n$

Si consideri ora il numero $a = p_1p_2p_3\ldots p_n + 1$

Il numero a non è divisibile per nessuno dei $p_1, p_2, \ldots p_n$ perché dalla divisione per ciascuno di essi si ottiene sempre resto 1

Dunque a è un numero primo diverso dai precedenti

APPENDICE 2

DIMOSTRAZIONE DEL TEOREMA FONDAMENTALE DELL'ARITMETICA: ogni numero intero n > 1 può essere scomposto in modo **unico** in un prodotto di primi

Quella che segue non è la classica dimostrazione di Euclide (che si fonda sull'utilizzo dell'algoritmo della divisione nella ricerca del MCD tra due numeri naturali)

Si è preferita la seguente (molto più recente) soprattutto perché più breve

Tuttavia (chi avesse qualche curiosità è invitato al confronto) ci sembra comunque più elegante, anche se forse più sofisticata, di quella classica euclidea

DIMOSTRAZIONE

Se esiste un numero intero > 1 suscettibile di scomposizione in due prodotti di primi essenzialmente diversi, esisterà anche un minimo di tali interi; indichiamo con m tale minimo:

$m = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ (∗)

Non è restrittivo supporre che i fattori siano ordinati:

$p_1 \le p_2 \le \dots \le p_r \qquad q_1 \le q_2 \le \dots \le q_s$

p_1 deve essere diverso da q_1, perché se lo fosse allora:

$p_2 \dots p_r = q_2 \dots q_r$ (nella (∗) $p_1 = q_1$ diventa cancellabile)

e avremmo ottenuto un intero $< m$ suscettibile di scomposizione in due modi essenzialmente diversi (contro l'ipotesi che m fosse il minimo)

Quindi o vale $p_1 < q_1$ oppure $q_1 < p_1$

Supponiamo che sia vera la prima (nell'altro caso basta scambiare le lettere p e q nel ragionamento che segue)
Consideriamo il numero:
$m' = m - (p_1 q_2 q_3 \dots q_s)$

Poiché m si può scrivere in due modi diversi, si ha:
$m' = p_1 p_2 \dots p_r - (p_1 q_2 q_3 \dots q_s) = p_1 (p_2 p_3 \dots p_r - q_2 q_3 \dots q_s)$
$m' = q_1 q_2 \dots q_s - (p_1 q_2 q_3 \dots q_s) = (q_1 - p_1)(q_2 q_3 \dots q_s)$

Ma $p_1 < q_1 \rightarrow m' < m$
Allora m deve essere scomponibile in modo unico

Dunque p_1 deve comparire come fattore o in $(q_1 - p_1)$ oppure in $(q_2 q_3 \dots q_s)$

Non può comparire in $(q_2 q_3 \ldots q_s)$ perché i fattori q sono tutti primi e

$p_1 < q_1 \leq q_2 \leq \ldots \leq q_s$

Dunque p_1 deve essere un fattore di $(q_1 - p_1)$, cioè:

$q_1 - p_1 = p_1 \cdot h$ per qualche $h \in \mathbf{N}$

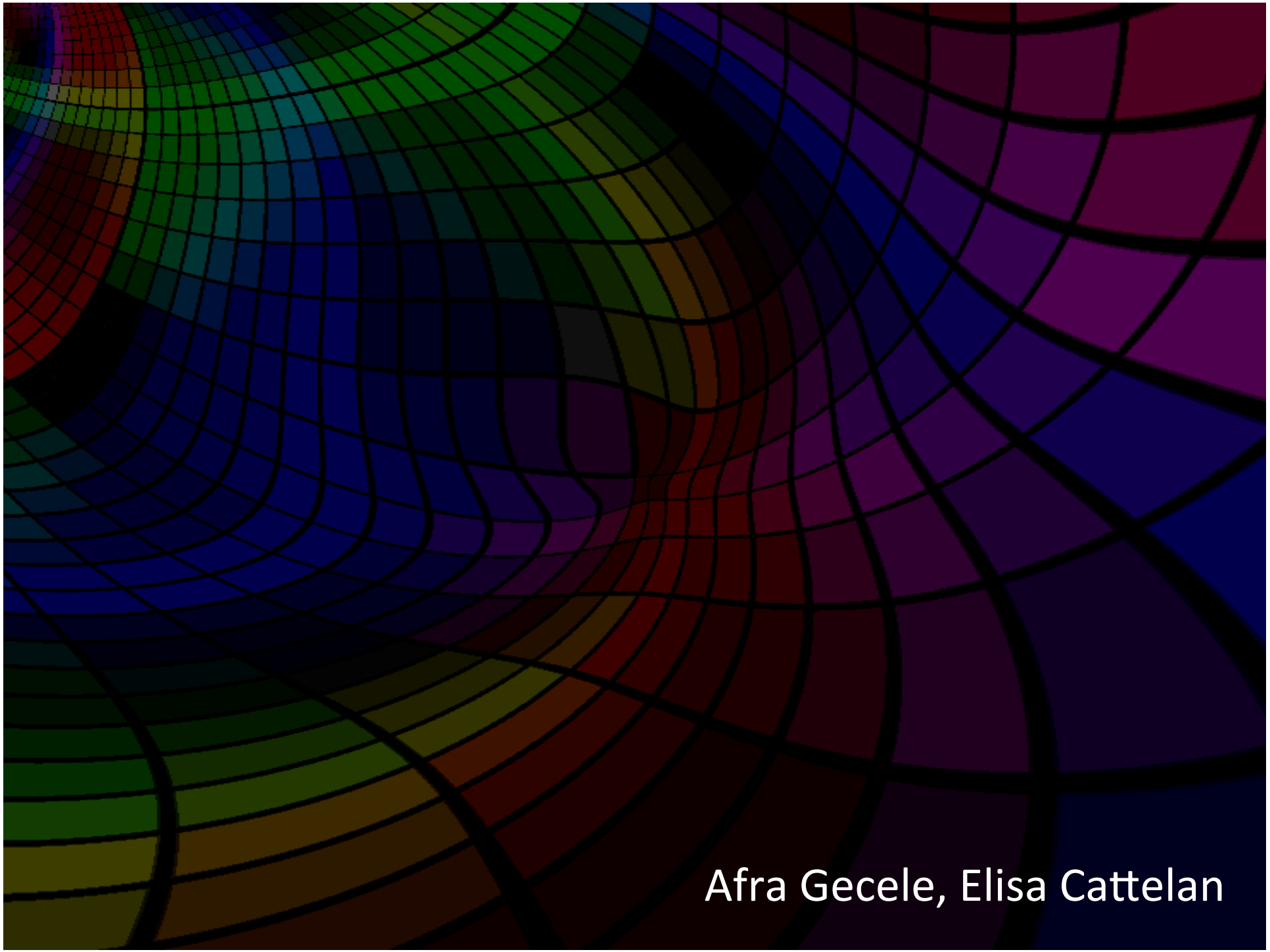
Ne segue:

$q_1 = p_1 (h + 1)$

Ma q_1 è primo, mentre qui compare *fattorizzato*

ASSURDO

Dunque ogni intero $n > 1$ deve ammettere una scomposizione in fattori primi essenzialmente **unica**


Afra Gecele, Elisa Cattelan