Appunti di Lezione: Strutture Discrete

Parte II: Fondamenti di Teoria dei Numeri e metodologie di dimostrazione

V. Cutello

Contenuti I

Contenuti II

- Inverso modulare

4. **Applicazioni dell'Aritmetica modulare**
   - La prova del 9
   - Codici ISBN e Carte di Credito
   - Cifrari monoalfabetici a trasposizione
   - Hashing

5. **Teoria dei numeri e problemi aperti**
   - Numeri primi di Mersenne e numeri perfetti
   - Numeri primi gemelli
   - La congettura di Goldbach

6. **Caso studio: La congettura di Collatz**

STRUTTURE DISCRETE

PARTE 2: Fondamenti di Teoria dei Numeri e metodologie di dimostrazione

1: Numeri interi

Insiemi numerici

Ricordiamo gli insiemi numerici

- $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$ "numeri interi naturali"
- $\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$ "numeri interi relativi"
- $\mathbb{Q} = \{\frac{n}{m} : n, m \in \mathbb{Z}\}$ "numeri razionali"
- $\mathbb{R} = \{x : x \text{ razionale o irrazionale } \}$ "numeri reali"
- $\mathbb{C} = \{x : x \text{ reale o immaginario } \}$ "numeri complessi"

Vale la catena di inclusioni strette

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Insiemi numerici

Mentre la prima inclusione stretta è ovvia

$$\mathbb{N} \subset \mathbb{Z}$$

soffermiamoci un pochino sulle altre 3

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

- Esempio di numero razionale non intero: $\frac{1}{2}$
- Esempio di numero reale non razionale: $\sqrt{2}$ (ci ritorniamo a breve)
- Esempio di numero complesso non reale: i, ovvero il numero immaginario che gode della proprietà: $i^2 = -1$.

I pitagorici e $\sqrt{2}$

La scuola pitagorica fu fondata da Pitagora a Crotone intorno al 530 a.C.

Era nei fatti una setta mistica oltre che, ovviamente, una scuola di matematica, filosofia etc.

- Gli allievi matematici erano la cerchia più stretta dei seguaci.
- Vivevano all'interno della scuola ed erano obbligati al celibato.
- Solo loro potevano ascoltare le lezioni di Pitagora e parlare con lui.
- A loro era imposto l'obbligo del segreto, in modo che gli insegnamenti impartiti e le scoperte fatte non diventassero di pubblico dominio.

I pitagorici e $\sqrt{2}$

- Ai Pitagorici, oltre al famoso teorema, si deve anche la scoperta dei numeri irrazionali. Ovvero, nello specifico, che il lato di un quadrato e la sua diagonale erano incommensurabili. In altre parole, non vi era una unità di misura unica tale da poter misurare in quantità intere di essa sia il lato che la diagonale.
- Ricordiamo, che la lunghezza della diagonale di un quadrato il cui lato misura 1, è uguale a $\sqrt{2}$.
- Per i Pitagorici, che credevano che tutto fosse misurabile, fu una scoperta sconvolgente e venne tenuta rigorosamente segreta. Si dice che uno dei seguaci, Ippaso, che voleva tornare in Grecia e divulgare il segreto, fu ucciso proprio per evitare tale divulgazione.
- $\sqrt{2}$, la cui irrazionalità dimostreremo tra un po', viene anche detto *numero di Pitagora* o *costante di Pitagora*.

Operazioni sui numeri interi

- Sull'insieme $\mathbb{N}$ sono definite 2 operazioni
  - **Somma**: $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ che ad ogni coppia di numeri (n, m) associa il numero $n + m \in \mathbb{N}$.
  - **Prodotto**: $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ che ad ogni coppia di numeri (n, m) associa il numero $n \cdot m \in \mathbb{N}$.
- Sull'insieme $\mathbb{Z}$ sono definite 3 operazioni
  - **Somma** e **Prodotto** come definite per $\mathbb{N}$.
  - **Differenza**: $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ che ad ogni coppia di numeri (n, m) associa il numero $n - m \in \mathbb{Z}$.
- Notate come non abbiamo definito, in maniera diretta, la differenza tra numeri interi naturali $\mathbb{N}$. Essa risulta comunque definita qualora la differenza di due numeri relativi, che risultano essere anche naturali, risulti essere a sua volta un numero naturale.
- Non abbiamo definito in maniera diretta neppure la divisione tra numeri interi relativi $\mathbb{Z}$. Lo faremo presto in maniera indiretta.

Valore assoluto

Il *Valore Assoluto* (o modulo) di un intero relativo $n \in \mathbb{Z}$ è l'intero $|n| \geq 0$ definito come

$$|n| = \begin{cases} n, & \text{se } n \geq 0 \\ -n, & \text{se } n < 0 \end{cases}$$

Alcune Proprietà

Per ogni $n, m \in \mathbb{Z}$ abbiamo

- $|n| = 0$ se e solo se $n = 0$
- $|n \cdot m| = |n| \cdot |m|$
- $n + |n| \geq 0$ ed in particolare $n + |n| = 0$ se e solo se $n \leq 0$.

Definizione assiomatica dei numeri interi naturali

Il matematico e logico piemontese Giuseppe Peano (1858-1932), lo stesso che introdusse i simboli insiemistici classici, dà una definizione assiomatica dell'insieme dei numeri naturali $\mathbb{N}$.

- Esiste un numero naturale 0.
- Ogni numero naturale a ha un numero naturale successore, denotato come $S(a)$.
- Non esiste un numero naturale il cui successore è 0.
- Numeri naturali distinti hanno successori distinti: se $a \neq b$, allora $S(a) \neq S(b)$.

NOTA

Avendo definito la funzione $+$ abbiamo che

- $S(0) = 1$
- Per ogni numero naturale a, $S(a) = a + 1$
- Infine, dato un numero naturale n ed il suo successore $S(n)$ diciamo che n è il predecessore di $S(n)$, denotato con $P(S(n))$.
- Quindi, ogni numero naturale n, tranne lo 0, ha un predecessore che è il numero $n - 1$.

Assioma del buon ordinamento

- Utilizzando la funzione successore, possiamo, come sappiamo, introdurre una relazione d'ordinamento sui numeri naturali $<$ ($\leq$) definita, per ogni coppia $a, b \in \mathbb{N}$ come

$$\begin{aligned} a &\leq a \\ a &< S(a) \\ a &< b \quad \text{se esiste } c \in \mathbb{N} \text{ tale che } a < c \text{ e } c < b \end{aligned}$$

- A questo punto, possiamo introdurre il seguente assioma

Assioma del buon ordinamento

Se S è un qualunque insieme non vuoto di numeri naturali, allora in S esiste un elemento minimo, ovvero esiste $s \in S$ tale che $s \leq t$ per ogni $t \in S$.

Proprietà formali di somma e prodotto

Ribadiamo le proprietà formali

- Proprietà della somma
  - **Commutatività:** per ogni $a, b \in \mathbb{Z}$, si ha $a + b = b + a$.
  - **Associatività:** per ogni $a, b, c \in \mathbb{Z}$, si ha $a + b + c = a + (b + c) = (a + b) + c$.
  - **Elemento neutro:** il numero 0 è l'elemento neutro della somma, ovvero per ogni $a \in \mathbb{Z}$, si ha $a + 0 = 0 + a = a$.
- Proprietà del prodotto
  - **Commutatività:** per ogni $a, b \in \mathbb{Z}$, si ha $a \cdot b = b \cdot a$.
  - **Associatività:** per ogni $a, b, c \in \mathbb{Z}$, si ha $a \cdot b \cdot c = a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
  - **Distributività:** per ogni $a, b, c \in \mathbb{Z}$, si ha $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.
  - **Elemento neutro:** il numero 1 è l'elemento neutro del prodotto, ovvero per ogni $a \in \mathbb{Z}$, si ha $a \cdot 1 = 1 \cdot a = a$.
  - **Elemento zero:** iper ogni $a \in \mathbb{Z}$, si ha $a \cdot 0 = 0 \cdot a = 0$; e, inoltre, se $a \cdot b = 0$ allora $a = 0$ oppure $b = 0$.

Proprietà formali di somma e prodotto: Esempi

- Ricordiamo che il calcolo avviene rispettando le priorità degli operatori: il prodotto ha una priorità più alta della somma e differenza che hanno la stessa priorità; e
- utilizzando l'associatività a sinistra, che risulta particolarmente importante per la differenza. Quindi

$$a - b - c = (a - b) - c \quad \textbf{e NON} \quad a - b - c = a - (b - c).$$

- Esempi.
  - $10 + 3 \cdot 5 - 5 = 10 + 15 - 5 = 25 - 5 = 20.$
  - $20 - 3 \cdot 5 - 5 = 20 - 15 - 5 = 5 - 5 = 0$
  - $5 - 1 - 2 + 3 = 4 - 2 + 3 = 2 + 3 = 5$

Principio di Induzione

- Peano introdusse un ulteriore assioma nella sua definizione dell'insieme dei numeri naturali. Tale assioma viene chiamato "Principio di induzione"
  - Se una proprietà P è posseduta dal numero 0 e
  - la proprietà P è posseduta anche dal successore di ogni numero naturale che possiede la proprietà P, allora
  - la proprietà P è posseduta da tutti i numeri naturali.
- Il principio di induzione, di cui adesso dimostriamo la validità, ci sarà utile nella dimostrazione di molte proprietà di strutture discrete.

NOTA

Il primo caso, si chiama caso base e, se ci si riferisce agli interi positivi, si utilizza il numero 1 al posto del numero 0.

Principio di Induzione

- Possiamo dimostrare il Principio di Induzione

Teorema

Sia P una affermazione riguardante i numeri naturali. Se

(a) *$P(0)$ è vera, ed inoltre*

(b) *per ogni numero naturale n se $P(n)$ è vera allora è vera anche $P(n+1)$*

possiamo concludere che P è vera per ogni numero naturale.

Principio di Induzione: dimostrazione

Dimostrazione:

Ragioniamo per assurdo e supponiamo falsa la tesi, ossia supponiamo che esista almeno un naturale n per cui $P(n)$ è falsa. Costruiamo il seguente insieme:

$$S = \{n : n \in \mathbb{N}, \text{ e } P(n) \text{ è falsa } \}$$

Per la nostra ipotesi di assurdo S non è vuoto. Per l'Assioma del Buon Ordinamento esiste in S esiste un elemento minimo s. Per definizione di S, $P(s)$ è falsa. Dalle ipotesi sappiamo che $s \neq 0$ poiché $P(0)$ è vera. Quindi poiché $S \subset \mathbb{N}$, deve essere $s > 0$. Allora esiste il suo predecessore, il numero naturale $s - 1$.
Dal momento che $s - 1 < s$ abbiamo che $s - 1 \notin S$ quindi $P(s - 1)$ è vera.
Ma questo implica, per il caso (b) che $P(s)$ è vera. Quindi abbiamo una contraddizione.
$\triangle$

Principio di Induzione: Seconda forma

- Il principio di induzione si può esprimere e dimostrare in una seconda forma. La seguente
  - Se una proprietà P è posseduta dal numero 0 e
  - Se, fissato un numero n, la proprietà P è vera per tutti i numeri che precedono n, allora
  - la proprietà P è posseduta da tutti i numeri naturali.

NOTA

La dimostrazione della validità del Principio di Induzione nella seconda forma è totalmente analoga a quella già vista.

Principio di Induzione: Esempi ed esercizi

- Dimostrare per induzione che
  1. per ogni intero $n \geq 4$ si ha $n! > 2^n$
  2. dato un insieme finito A allora $|\mathcal{P}(A)| = 2^{|A|}$;
  3. dato un intero $n \geq 1$ si ha che $1 + 2 + \cdots + (n-1) + n = \frac{n(n+1)}{2}$.
  4. dato $x \neq 1$, si ha per ogni $n \geq 0$ (progressione geometrica):

$$\sum_{i=0}^{n} x^i = \frac{1 - x^{n+1}}{1 - x}$$

Principio di Induzione: Esempio 2

- Dimostriamo per induzione che dato un insieme finito A allora $|\mathcal{P}(A)| = 2^{|A|}$.
- Utilizzeremo l'induzione sulla cardinalità di A.
  - Caso base: $|A| = 0$ (e quindi $A = \emptyset$) abbiamo $\mathcal{P}(A) = \{\emptyset\}$ e quindi $|\mathcal{P}(A)| = 1 = 2^0$.
  - Passo induttivo: supponiamo l'asserto sia vero per tutti gli insiemi A tali che $0 < |A| = n - 1$ e dimostriamolo per n. Sia allora A un insieme tale che $|A| = n$ e sia $a \in A$. L'insieme $A' = A \setminus \{a\}$ ha una cardinalità di $n - 1$ elementi e quindi $|\mathcal{P}(A')| = 2^{n-1}$. Ovviamente, $\mathcal{P}(A') \subset \mathcal{P}(A)$ ed inoltre, possiamo dire che gli elementi di $\mathcal{P}(A) \setminus \mathcal{P}(A')$ sono tutti i sottoinsiemi di A che contengono a. Questi elementi sono esattamente tanti quanti sono gli elementi di $\mathcal{P}(A')$, infatti la funzione

$$f_a : \mathcal{P}(A') \to \mathcal{P}(A) \setminus \mathcal{P}(A')$$

    che associa ad ogni elemento $X \in \mathcal{P}(A')$ l'elemento $X \cup \{a\}$ è una corrispondenza biunivoca.
  - Quindi $|\mathcal{P}(A)| = 2 \cdot |\mathcal{P}(A')| = 2 \cdot 2^{n-1} = 2^n$.

Principio di Induzione: Formula di Gauss, esempio 3

Dimostriamo per induzione che dato un intero $n \geq 1$ si ha che $1 + 2 + \cdots + (n-1) + n = \frac{n(n+1)}{2}$.

- Il caso base è $n = 1$ e per $n = 1$ la formula è vera perché $1 = \frac{1(1+1)}{2}$.
- Passo induttivo: supponiamo l'asserto sia vero per n e dimostriamolo per $n+1$. Essendo vero per n abbiamo

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Allora

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2(n+1)}{2}.$$

Notiamo che $n(n+1) + 2(n+1) = n^2 + 3n + 2 = (n+1) \cdot (n+2)$ e l'asserto è dimostrato.

Funzioni "floor" e "ceiling"

Sia x un numero reale, definiamo i 2 seguenti valori:

- "Floor": il più grande numero intero minore o uguale ad x è detto "floor" e denotato con $\lfloor x \rfloor$
- "Ceiling": il più piccolo numero intero maggiore o uguale ad x è detto "ceiling" e denotato con $\lceil x \rceil$

Esempi:

x	$\lfloor x \rfloor$	$\lceil x \rceil$
$3,8$	3	4
$-3,8$	-4	-3
3	3	3
-3	-3	-3

Divisione tra interi

- Introduciamo adesso l'operazione di divisione tra interi relativi, utilizzando le operazioni di somma e prodotto definite su $\mathbb{Z}$. Abbiamo il seguente teorema.

Teorema

Dati due interi $a, b \in \mathbb{Z}$ con $b \neq 0$, chiamati rispettivamente dividendo e divisore, esistono unici due interi relativi q, r, denominati rispettivamente quoziente e resto, tali che $a = q \cdot b + r$ con $0 \leq r < |b|$.

Modulo: Il resto r è anche detto modulo della divisione e viene comunemente denotato con $a \bmod b$.
"Floor": Nel caso in cui a e b siano positivi, il quoziente q è l'intero più grande che è minore o uguale al rapporto (divisione) $\frac{a}{b}$ ossia al "floor" $\lfloor \frac{a}{b} \rfloor$

Divisione tra interi

Si noti che nel teorema definiamo il resto sempre positivo.
Per dimostrare il teorema agiremo per casi:

1. Nel primo caso assumiamo che il dividendo a ed il divisore b siano entrambi non negativi
2. Nel secondo caso assumiamo che il dividendo a sia negativo ma il divisore b positivo
3. Nel terzo caso assumiamo che il dividendo a sia positivo e il divisore b negativo
4. Nel quarto caso assumiamo che il dividendo a ed il divisore b siano entrambi negativi

Ed infine, dimostreremo l'unicità di quoziente e resto.

Divisione tra interi: primo caso

- Assumiamo allora che a, b siano entrambi non negativi ed in particolare $b \neq 0$.
- Consideriamo il seguente insieme di numeri interi non negativi

$$S = \{a - kb : k \in \mathbb{N}, a - kb \geq 0\}$$

- L'insieme è non vuoto, perché per $k = 0$ abbiamo che $a \in S$. Per l'assioma del buon ordinamento, l'insieme S ha un minimo, indichiamolo con $r \geq 0$. Denotiamo con q il valore di k tale che $r = a - qb$ da cui $a = qb + r$.
- Notiamo subito che se $r = a - qb$ è il minimo di S allora q è il massimo intero in $\mathbb{N}$ tale che $a - qb \geq 0$, ossia $q = \lfloor \frac{a}{b} \rfloor$. Infatti, se esistesse $k > q$ tale che $a - kb \geq 0$ avremmo

$$(a - qb) - (a - kb) = (k - q)b \geq 0$$

perché $b > 0$ e $k > q$. Ma questo contraddirebbe l'ipotesi che $a - qb$ è il minimo di S.

Divisione tra interi: primo caso

- Viceversa, se q è il massimo intero in $\mathbb{N}$ tale che $a - qb \geq 0$, allora per ogni $k \in \mathbb{N}$ se $a - kb \geq 0$ abbiamo che $q \geq k$ e quindi

$$(a - kb) - (a - qb) = (q - k)b \geq 0$$

perché $b > 0$ e $q \geq k$, e tale diseguaglianza dimostra che $a - qb$ è il minimo in S.

- Dato che $r = a - qb$ è il minimo in S, dobbiamo dimostrare che $r < b$.
- Supponiamo per assurdo che sia $0 < b \leq r$. In particolare, avremmo $r = b + h$ per qualche $h \geq 0$. Quindi

$$a = qb + r = qb + b + h = (q + 1)b + h$$

ed allora $h = a - (q+1)b \in S$ ossia $h = a - (q+1)b < a - qb = r$ che contraddice l'ipotesi che r era il minimo di S.

Divisione tra interi: primo caso

Esempi

- $a = 1$, $b = 10$: abbiamo $q = \lfloor \frac{1}{10} \rfloor = 0$ e $1 = 0 \cdot 10 + 1$.
  Quindi quoziente $q = 0$ e resto $r = 1$, ovvero $1 \bmod 10 = 1$.
- $a = 19$, $b = 10$: abbiamo $q = \lfloor \frac{19}{10} \rfloor = 1$ e $19 = 1 \cdot 10 + 9$ e infatti $2 \cdot 10 > 19$.
  Quindi quoziente $q = 1$ e resto $r = 9$, ovvero $19 \bmod 10 = 9$.
- $a = 14$, $b = 4$: abbiamo $q = \lfloor \frac{14}{4} \rfloor = 3$ e $14 = 3 \cdot 4 + 2$ e infatti $4 \cdot 4 > 14$.
  Quindi quoziente $q = 3$ e resto $r = 2$, ovvero $14 \bmod 4 = 2$.
- $a = 23$, $b = 5$: abbiamo $q = \lfloor \frac{23}{5} \rfloor = 4$ e $23 = 4 \cdot 5 + 3$.
  Quindi quoziente $q = 4$ e resto $r = 3$, ovvero $23 \bmod 5 = 3$.
- $a = 29$, $b = 7$: abbiamo $q = \lfloor \frac{23}{5} \rfloor = 4$ e $29 = 4 \cdot 7 + 1$.
  Quindi quoziente $q = 4$ e resto $r = 1$, ovvero $29 \bmod 7 = 1$.

Divisione tra interi: secondo caso

- Assumiamo allora che $b > 0$ mentre $a < 0$.
- Consideriamo il valore assoluto $|a| > 0$. Dal momento che $a < 0$ ne segue che $|a| = -a$.
- Per quanto visto nel primo caso, esistono q' ed $0 \leq r' < b$ tali che

$$|a| = q'b + r' \text{ e quindi } -a = q'b + r'$$

da cui otteniamo

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

- Se $r' = 0$ abbiamo finito. Se $r' > 0$ abbiamo $0 < b - r' < b$ e possiamo riscrivere l'uguaglianza come

$$a = (-q')b + (-r') = (-q')b - b + b + (-r') = (-q' - 1)b + (b - r')$$

prendendo come quoziente $q = -q' - 1$ e come resto $r = b - r'$ il secondo caso del teorema è dimostrato.

Si può verificare facilmente che anche nel secondo caso, come nel primo, $q = \lfloor \frac{a}{b} \rfloor$.

Divisione tra interi: secondo caso

Esempi

- $a = -1, b = 10$: per $a = 1$ abbiamo $q' = 0$ e $r' = 1$.
  Quindi per $a = -1$ abbiamo $q = 0 - 1 = -1$ e $r = 10 - 1 = 9$
  Infatti, $-1 = (-1) \cdot 10 + 9$ e quindi $-1 \bmod 10 = 9$.
- $a = -19, b = 10$: per $a = 19$ abbiamo $q' = 1$ e $r' = 9$.
  Quindi per $a = -19$ abbiamo $q = -1 - 1 = -2$ e $r = 10 - 9 = 1$.
  Infatti, $-19 = -2 \cdot 10 + 1$ e quindi $-19 \bmod 10 = 1$.
- $a = -14, b = 4$: per $a = 14$ abbiamo $q = 3$ e $r = 2$.
  Quindi per $a = -14$ abbiamo $q = -3 - 1 = -4$ e $r = 4 - 2$.
  Infatti $-14 = -4 \cdot 4 + 2$ e quindi $-14 \bmod 4 = 2$.
- $a = -23, b = 5$: per $a = 23$ abbiamo $q = 4$ e $r = 3$.
  Quindi per $a = -23$ abbiamo $q = -4 - 1 = -5$ e $r = 5 - 3 = 2$.
  Infatti $-23 = -5 \cdot 5 + 2$ e quindi $-23 \bmod 5 = 2$.
- $a = -29, b = 7$: per $a = 29$ abbiamo $q = 4$ e $r = 1$.
  Quindi per $a = -29$ abbiamo $q = -4 - 1 = -5$ e $r = 7 - 1 = 6$.
  Infatti $-29 = -5 \cdot 7 + 6$ e quindi $-29 \bmod 7 = 6$.

Divisione tra interi: terzo caso

- Assumiamo adesso che $b < 0$ e $a > 0$.
- Consideriamo il valore assoluto $|b| > 0$ e sappiamo che $|b| = -b$.
- Per quanto visto nel primo caso, esistono q' ed $0 \leq r' < |b|$ tali che

$$a = q'|b| + r' \text{ e quindi } a = q'(-b) + r'$$

da cui otteniamo

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

- Prendendo come quoziente $q = -q'$ e come resto $r = r'$ il terzo caso del teorema è dimostrato.

Divisione tra interi: terzo caso

Esempi

- $a = 1, b = -10$: per per $b = 10$ abbiamo $q' = 0$ e $r' = 1$.
  Quindi per $b = -10$ abbiamo $q = -q' = 0$ e $r = r' = 1$
  Infatti, $1 = 0 \cdot (-10) + 1$ e quindi $1 \bmod (-10) = 1$.
- $a = 19, b = -10$: per $b = 10$ abbiamo $q = 1$ e $r = 9$.
  Quindi per $b = -10$ abbiamo $q = -1$ e $r = 9$
  Infatti, $19 = -1 \cdot (-10) + 9$ e quindi $19 \bmod (-10) = 9$.
- $a = 14, b = -4$: per $b = 4$ abbiamo $q = 3$ e $r = 2$.
  Quindi per $b = -4$ abbiamo quoziente $q = -3$ e resto $r = 2$.
  Infatti $14 = -3 \cdot (-4) + 2$ e quindi $14 \bmod (-4) = 2$.
- $a = 23, b = -5$: per $b = 5$ abbiamo quoziente $q = 4$ e resto $r = 3$
  Quindi per $b = -5$ abbiamo $q = -4$ e $r = 3$.
  Infatti $23 = -4 \cdot (-5) + 3$ e quindi $23 \bmod (-5) = 3$.
- $a = 29, b = -7$: per $a = 29$ abbiamo $q = 4$ e $r = 1$.
  Quindi per $b = -7$ abbiamo $q = -4$ e $r = 1$
  Infatti $29 = -4 \cdot (-7) + 1$ e quindi $29 \bmod (-7) = 1$.

Divisione tra interi: quarto caso

- Assumiamo adesso che $b < 0$ e $a < 0$.
- Consideriamo i valori assoluti $|a| > 0$ e $|b| > 0$ e quindi $|a| = -a$ e $|b| = -b$.
- Per quanto visto nel primo caso, esistono q' ed $0 \leq r' < |b|$ ovvero $0 \leq r' < -b$ tali che

$$|a| = q'|b| + r'$$

- Utilizzando i valore di q' e r' ed agendo come nel secondo caso, abbiamo

$$a = (-q' - 1)|b| + |b| - r' = (q' + 1)b - b - r'$$

- Prendendo come quoziente $q = q' + 1$ e come resto $r = -b - r'$ il quarto caso del teorema è dimostrato.

Divisione tra interi: quarto caso

Esempi

- $a = -1$, $b = -10$: per per $a = 1$ e $b = 10$ abbiamo $q' = 0$ e $r' = 1$.
  Quindi per $a = -1$ e $b = -10$ abbiamo $q = q' + 1$ e $r = -b - r' = 10 - 1 = 9$
  Infatti, $-1 = 1 \cdot (-10) + 9$ e quindi $-1 \bmod (-10) = 9$.
- $a = -19$, $b = -10$: per $a = 19$ e $b = 10$ abbiamo $q = 1$ e r$r = 9$.
  Quindi per $a = -19$ e $b = -10$ abbiamo $q = 2$ e $r = 10 - 9 = 1$
  Infatti, $-19 = 2 \cdot (-10) + 1$ e quindi $-19 \bmod (-10) = 1$.
- $a = -14$, $b = -4$: per $a = 14$ e $b = 4$ abbiamo $q = 3$ e $r = 2$.
  Quindi per $a = -14$ e $b = -4$ abbiamo quoziente $q = 4$ e resto $r = 2$.
  Infatti $-14 = 4 \cdot (-4) + 2$ e quindi $-14 \bmod (-4) = 2$.
- $a = -23$, $b = -5$: per $a = 23$ e $b = 5$ abbiamo $q = 4$ e $r = 3$
  Quindi per $a = -23$ e $b = -5$ abbiamo $q = 5$ e $r = 5 - 3 = 2$.
  Infatti $-23 = -5 \cdot (-5) + 2$ e quindi $-23 \bmod (-5) = 2$.

Divisione tra interi: unicità

Dimostriamone l'unicità di quoziente e resto ragionando per assurdo, ossia supponiamo che esistano $a, b \in \mathbb{Z}$ ed esistano $q_1 \neq q_2$ e $r_1 \neq r_2$ tali che, $0 \leq r_1 < |b|$, $0 \leq r_2 < |b|$ e

$$\begin{aligned} a &= bq_1 + r_1 \text{ e} \\ a &= bq_2 + r_2 \end{aligned}$$

Sottraendo membro a membro otteniamo

$$0 = b(q_1 - q_2) + (r_1 - r_2) \quad \text{ovvero} \quad b(q_2 - q_1) = r_1 - r_2$$

e passando ai valori assoluti

$$|b(q_2 - q_1)| = |b||(q_2 - q_1)| = |r_1 - r_2|$$

Distinguiamo i 2 casi

1. $r_1 \geq r_2$ e
2. $r_1 < r_2$

Teorema di Unicità Quoziente e Resto

1. Supponiamo allora $r_1 \geq r_2$
   - $|r_1 - r_2| = r_1 - r_2 \leq r_1 < |b|$. Quindi
   - $|b| > r_1 - r_2 = |r_1 - r_2| = |b||(q_2 - q_1)|$ da cui otteniamo
   - $1 > |(q_2 - q_1)| \geq 0$ e quindi, essendo q_1 e q_2 numeri interi, ne deduciamo che $|(q_2 - q_1)| = 0$ ovvero $q_1 = q_2$.
   - Dal momento che $b(q_2 - q_1) = r_1 - r_2$ ne deduciamo anche che $r_1 = r_2$.
2. Il caso $r_1 < r_2$ si dimostra in maniera analoga (**esercizio**)

Divisione tra interi: riepilogo

Riepilogando, dati due interi $a, b \in \mathbb{Z}$ con $b \neq 0$, per trovare quoziente e resto r positivo della divisione $\frac{a}{b}$ agiamo così:

1. Troviamo il $q' = \lfloor \frac{|a|}{|b|} \rfloor$ ovvero il massimo intero q' tale che $|a| - q|b| \geq 0$ e fissiamo $r' = |a| - q'|b|$. Se $a, b \geq 0$ poniamo $q = q'$ e $r = r'$.
2. Se $a < 0$ e $b > 0$ poniamo $q = -q' - 1$ e $r = b - r'$.
3. Se $a > 0$ e $b < 0$ poniamo $q = -q'$ e $r = r'$.
4. Se $a < 0$ e $b < 0$ poniamo $q = q' + 1$ e $r = -b - r'$.

In pratica, notiamo come nel caso $b < 0$ sia sufficiente solamente cambiare il segno del quoziente, una volta trovato il quoziente considerando a come dividendo e $|b|$ come divisore. Vediamo altri esempi.

Esempi

- $|a| = 13, |b| = 10 : q' = 1$ e $r' = 3$, quindi
  - per $a = 13$ e $b = 10$ abbiamo $q = q', r = r', 13 = 1 \cdot 10 + 3$ e quindi $13 \bmod 10 = 3$;
  - per $a = 13$ e $b = -10$ abbiamo $q = -q', r = r'$, $13 = -1 \cdot (-10) + 3$ e quindi $13 \bmod (-10) = 3$;
  - per $a = -13$ e $b = 10$ abbiamo $q = -q' - 1, r = b - r'$, $-13 = -2 \cdot 10 + 10 - 3$ e quindi $-13 \bmod 10 = 7$;
  - per $a = -13$ e $b = -10$ abbiamo $q = q' + 1, r = -b - r'$, $-13 = 2 \cdot (-10) + 10 - 3$ e quindi $-13 \bmod (-10) = 7$.
- Notiamo che, in particolare, per ogni coppia di interi positivi n e m tali che $n < m$ abbiamo
  - $n \bmod m = n$;
  - $n \bmod (-m) = n$;
  - $-n \bmod m = m - n$;
  - $-n \bmod (-m) = m - n$;
- quindi, per esempio, $-1 \bmod 10 = 9 \bmod 10 = 9$, oppure $-2 \bmod 7 = 5 \bmod 7 = 5$ etc.

Divisione tra interi: programmazione

- I linguaggi di programmazione differenziano l'operazione di divisione tra reali e tra interi.
- Per esempio
  - Se abbiamo la dichiarazione float x, y, z; con valori $x = 3$ e $y = 2$ allora l'istruzione "$z = x/y$;" assegnerà alla variabile z il valore 1.5.
  - Se abbiamo la dichiarazione $intx, y, z$; con valori $x = 3$ e $y = 2$ allora l'istruzione "$z = x/y$;" assegnerà alla variabile z il valore 1 ovvero il quoziente della divisione intera x/y.
  - L'operatore % assegna ad una variabile intera il resto di una divisione intera. Quindi, nell'esempio sopra $z = x\%y$ assegnerà alla variabile z il valore 1.

Definizione di divisibilità

Diamo la seguente

Definizione di Divisibilità

Dati due interi relativi $n, m \in \mathbb{Z}$ si dice che m è un divisore di n se esiste un intero relativo $k \in \mathbb{Z}$ tale che $n = k \cdot m$.
In altre parole, m è un divisore di n se il resto della divisione di n per m è uguale a zero.
In tale caso, useremo la notazione $m \mid n$. Se m non è un divisore di n useremo la notazione $m \nmid n$.

Sinonimi standard

- m è un divisore di n
- n è un multiplo di m

Esempi:
$2 \mid 8; -5 \mid 15; 5 \nmid 16; 3 \nmid -7$

Alcune definizioni ben conosciute

- Un numero n si dice pari se il resto della sua divisione per 2 è uguale ad 0 (può essere solo 0 oppure 1). Quindi, un numero n è pari se esiste un intero k tale che $n = 2k$.
- Un numero n che non è pari si dice dispari, ed in tal caso, visto che il resto della sua divisione per 2 è uguale ad 1, esiste un intero k tale che

$$n = 2k + 1.$$

Adesso che sappiamo cosa sono i numeri pari ed i numeri dispari, possiamo provare una proprietà apparentemente strana dei numeri dispari, ossia che la somma dei primi n numeri dispari è uguale a n^2.

Somma dei primi n numeri dispari

Dimostriamo che la somma dei primi n numeri dispari è uguale ad n^2 utilizzando l'assioma di induzione.

- Caso base: $n = 1$ e la somma in questo caso è proprio $1 = 1^2$.
- Supponiamo allora che la somma dei primi $n - 1$ numeri dispari sia uguale a $(n-1)^2$.
- Come sono fatti i primi n numeri dispari? Sono della forma $2k + 1$ per $0 \leq k \leq n - 1$. Infatti, abbiamo
  $1 = 2 \cdot 0 + 1; 3 = 2 \cdot 1 + 1; 5 = 2 \cdot 2 + 1$ etc.
- In particolare, l'ennesimo numero dispari sarà allora uguale a $2(n-1) + 1$. Se lo aggiungiamo a $(n-1)^2$ otteniamo

$$(n-1)^2 + 2(n-1) + 1 = n^2 - 2n + 1 + 2n - 2 + 1 = n^2$$

che dimostra la proprietà.

Prime proprietà della divisibilità

Teorema

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

(Somma) *Se $a \mid b$ e $a \mid c$ allora $a \mid (b + c)$.*

(Prodotto) *Se $a \mid b$ allora $a \mid bc$.*

(Transitività) *Se $a \mid b$ e $b \mid c$ allora $a \mid c$.*

Dimostrazione:

Somma

Dato che $a \mid b$ esiste x tale che $b = ax$, e dato che $a \mid c$ esiste y tale che $c = ay$.
Quindi $b + c = ax + ay = a(x + y)$ e ponendo $z = x + y$ abbiamo trovato un intero tale che $b + c = az$ dimostrando che $a \mid (b + c)$.

Prodotto

Dato che $a \mid b$ esiste x tale che $b = ax$, quindi $bc = axc$ il che dimostra che $a \mid bc$.

Transitività

Dato che $a \mid b$ esiste x tale che $b = ax$, e dato che $b \mid c$ esiste y tale che $c = yb$.
Quindi $by = axy$ ossia $c = axy$ e ponendo $z = xy$ abbiamo trovato un intero tale che $c = az$ dimostrando che $a \mid c$.

$\triangle$

Proprietà della divisibilità

Come conseguenza del teorema appena dimostrato abbiamo il seguente

COROLLARIO

(Quadrato) *Se* $a \mid b$ *allora* $a \mid b^2$

(Combinazione lineare) *Se* $a \mid b$ *e* $a \mid c$ *allora* $a \mid (hb + kc)$ *per ogni* $h, k \in \mathbb{Z}$.

Dimostrazione:

Il primo caso è una banale conseguenza del caso "prodotto".
Per il secondo caso, abbiamo che se $a \mid b$ allora $a \mid hb$ per ogni $h \in \mathbb{Z}$ e, se $a \mid c$, allora $a \mid kc$ per ogni $k \in \mathbb{Z}$. Quindi, $a \mid (hb + kc)$
$\triangle$

Proprietà della divisibilità

Proprietà del numero 0

Teorema

Ogni intero relativo $a \in \mathbb{Z}$, è divisore di 0, *ovvero* 0 *è multiplo di qualunque numero intero relativo, cioè* $a \mid 0$. *Il numero* 0 *è divisore solo di se stesso.*

Dimostrazione:

- Per ogni $a \in \mathbb{Z}$ abbiamo $a \cdot 0 = 0$. Quindi, $a \mid 0$.
- Se $0 \mid a$ allora esiste x tale che $0 \cdot x = a$. Ma $0 \cdot x = 0$ e quindi $a = 0$.

$\triangle$

Proprietà della divisibilità

Proprietà antisimmetrica

Teorema

Siano $a, b \in \mathbb{Z}$, se $a \mid b$ e $b \mid a$ allora $|a| = |b|$, ossia $a = \pm b$.

Dimostrazione:

- Dalle ipotesi abbiamo che $b = ax$ e $a = by$. Quindi, $a = axy$.
- Abbiamo allora che $a(xy - 1) = 0$ che implica che $a = 0$ oppure $xy = 1$.
- Se il prodotto fra interi è nullo almeno uno dei fattori deve essere nullo. Quindi
  - Se $a = 0$ quindi $b = 0y = 0$ e la proprietà è dimostrata
  - Se $xy = 1$ allora o sono entrambi uguali ad 1 o entrambi uguali a -1. Quindi $y = \pm 1$ e $a = \pm b$.

$\triangle$

Proprietà della divisibilità

Divisori banali

Teorema

Siano $a \in \mathbb{Z}$, *allora* $\pm a \mid a$ *e* $\pm 1 \mid a$.

- La dimostrazione è molto semplice (esercizio).
- Questi divisori sono detti i divisori banali del numero a.

Minimo Comune Multiplo

Richiamiamo per completezza la definizione di Minimo Comune Multiplo (MCM) tra interi relativi

Definizione (MCM)

Siano $a, b \in \mathbb{Z}$ non entrambi nulli, si chiama Minimo Comune Multiplo fra a e b un terzo intero $m \in \mathbb{N}$ (quindi positivo) tale che m è il più piccolo multiplo sia di a che di b. Ovvero,

- $a \mid m$ *e* $b \mid m$ *cioè a, b sono entrambi divisori di m*
- *Se x è un multiplo comune di a e b, ovvero* $a \mid x$ *e* $b \mid z$*, allora* $m \mid x$ *cioè m divide ogni altro multiplo comune di a e b*

Massimo Comune Divisore

Diamo la definizione di Massimo Comune Divisore (MCD) tra interi relativi

Definizione (MCD)

Siano $a, b \in \mathbb{Z}$ non entrambi nulli, si chiama Massimo Comune Divisore fra a e b un terzo intero $d \in \mathbb{Z}$ tale che:

- *$d \mid a$ e $d \mid b$ cioè d è un divisore sia di a che di b*
- *Se x è un divisore comune di a e b, ovvero $x \mid a$ e $x \mid b$, allora $x \mid d$ cioè d è multiplo di ogni altro divisore comune di a e b*

Osservazione

Il Massimo Comune Divisore fra due interi relativi è unico a meno del segno. Se d è un Massimo Comune Divisore fra due interi $a, b \in \mathbb{Z}$ allora $-d$ è anch'esso un Massimo Comune Divisore fra a, b ma è l'unico altro MCD.

Per convenzione, si stabilisce che il MCD tra due due interi relativi è il MCD di segno positivo.

Algoritmo di Euclide

Il calcolo del MCD tra due numeri,
per come lo abbiamo imparato a scuola, è un po' complicato,
e, come vedremo, anche "costoso" computazionalmente.

Negli "Elementi" di Euclide, il matematico greco noto soprattutto per i suoi lavori in geometria, tra la fine del IV e l'inizio del III secolo avanti Cristo, è presente un algoritmo per il calcolo del MCD molto più semplice, oggi, da "implementare" visto che è basato su divisioni successive.

L'algoritmo si basa su questa osservazione (che è anche la dimostrazione per induzione della sua correttezza). Siano $a, b \in \mathbb{N}$ e sia $b \leq a$. Allora

(Caso Base) se $b = 0$ allora il $MCD(a, b) = a$. Altrimenti

(Passo Induttivo) visto che $a = qb + r$ con $0 \leq r < b$ allora

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

Notiamo che se $b \mid a$ allora $a = qb$ ed il resto della divisione $r = 0$ e quindi $MCD(a, b) = MCD(b, 0) = b$ per il caso base. Quindi, se $b \mid a$ otteniamo in un passo che $MCD(a, b) = b$.

Algoritmo di Euclide

Dimostriamo allora che se $a = qb + r$ con $r \neq 0$ e $0 < r < b$ allora

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

- Se d è un divisore di a e b allora esistono h e k tali che $a = hd = qkd + r$. Quindi $r = d(h - qk)$ e quindi d è anche un divisore di r.
- Viceversa, se d è un divisore di b e di r allora esistono h e k tali che $a = qb + r = qkd + hd$ e quindi d è un divisore di a visto che $a = d(qk + h)$ e

Algoritmo di Euclide

Il seguente codice "C", nelle due versione iterativa e ricorsiva, calcola il MCD tra due numeri interi qualunque, nell'ipotesi che $a \geq b$.

Versione Iterativa

```
int Euclide(int a, int b)
{
 int r;
 while (b! = 0)
 {
     r = a%b;
     a = b ;
     b = r;
 }
 return a;
}
```

Versione Ricorsiva

```
int Euclide(int a, int b)
{
 if (b==0) return a
 else return Euclide(b, a%b)
}
```

Algoritmo di Euclide: Esempio

Come si intuisce, l'algoritmo di Euclide genera implicitamente una sequenza $x_1, x_2, x_3, \ldots, x_n, 0$ dove $x_1 = a = max(a, b)$, $x_2 = b = min(a, b)$, e, per ogni k, x_{k+1} è il resto della divisione tra x_{k-1} e x_k.
Calcoliamo, come esempio, il $MCD(330, 156)$

- $x_1 = 330$, $x_2 = 156$
- $x_3 = 330\%156 = 18 \Rightarrow 330 = 2 \cdot 156 + 18$
- $x_4 = 156\%18 = 12 \Rightarrow 156 = 8 \cdot 18 + 12$
- $x_5 = 18\%12 = 6 \Rightarrow 18 = 1 \cdot 12 + 6$
- $x_6 = 12\%6 = 0 \Rightarrow 12 = 2 \cdot 6 + 0$

Quindi $MCD(330, 156) = 6$.

Notiamo che $330/6 = 55 = 5 \cdot 11$ e $155/6 = 26 = 2 \cdot 13$ e quindi il risultato è corretto.

Algoritmo di Euclide: Esempio

Dall'esempio, notiamo anche che andando a ritroso

$$\begin{aligned} 6 &= 18 - 12 = \\ &= 18 - (156 - 8 \cdot 18) = -156 + 9 \cdot 18 = \\ &= -156 + 9 \cdot (330 - 2 \cdot 156) = \\ &= -19 \cdot 156 + 9 \cdot 330 \end{aligned}$$

Quanto appena visto, suggerisce una dimostrazione costruttiva del seguente teorema che ci dice che il *MCD* tra due numeri si può sempre scrivere come una loro combinazione lineare

Teorema

Siano $a, b \in \mathbb{N}$ *non entrambi uguali a* 0, *allora esistono* $h, k \in \mathbb{Z}$ *tali che*

$$MCD(a, b) = a \cdot h + b \cdot k$$

Algoritmo di Euclide: terminazione e complessità

- Ci rimane da dimostrare che l'algoritmo di Euclide termina (ovvero non entra in un loop infinito) e capire quante iterazioni (o chiamate ricorsive) l'algoritmo compie prima di terminare.
- Ricordiamo che l'algoritmo *Euclide(a, b)* termina quando $b = 0$ e che dopo la prima iterazione sicuramente $b < a$.
- Ad ogni iterazione del ciclo "while" (o chiamata ricorsiva), si passa dalla coppia di parametri a, b alla coppia di parametri $b, a\%b$. Quindi
  - Se $b \leq a/2$ dopo l'iterazione, il primo parametro si è dimezzato;
  - se $b > a/2$ allora il quoziente q della divisione a/b è necessariamente uguale ad 1 ed il resto $r = a\%b = a - b < a/2$. Quindi, nel caso in questione, dopo 2 iterazioni (chiamate ricorsive) avremo che il primo parametro sarà più piccolo di $a/2$.
- Possiamo concludere allora che il numero massimo di iterazioni (chiamate ricorsive) è ovviamente $2 \cdot \log_2 a$.

Numeri Primi

Diamo adesso una delle definizioni più importanti in Teoria dei Numeri.

Definizione (Numero Primo)

Si definisce Numero Primo un intero relativo $p \in \mathbb{Z}$, tale che p ha come unici divisori quelli banali e tale che $p \neq \pm 1$.

Osservazione Tradizionalmente, comunque, la definizione di Numero Primo si limita agli interi naturali. E quindi, definiamo come numeri primi gli elementi della successione

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots$$

Ritorneremo presto a parlare dei numeri primi.

Numeri coprimi

Definizione (Numeri Coprimi)

Due numeri $a, b \in \mathbb{Z}$ *si dicono coprimi se* $MCD(a, b) = 1$.

- Sappiamo allora che esistono $h, k \in \mathbb{Z}$ tali che $a \cdot h + b \cdot k = 1$.
- Vale anche il viceversa, ovvero il seguente teorema

Teorema

Siano $a, b \in \mathbb{N}$ *non entrambi uguali a* 0, *se esistono* $h, k \in \mathbb{Z}$ *tali che* $a \cdot h + b \cdot k = 1$ *allora* $MCD(a, b) = 1$.

Dimostrazione:

Sia $d = MCD(a, b)$. Quindi, $d \mid a$ e $d \mid b$ ma allora $d \mid (a \cdot h + b \cdot k)$. Ma l'unico divisore positivo di 1 è proprio 1 stesso e quindi $d = 1$.
$\triangle$

Numeri coprimi

- Come conseguenza del teorema precedente abbiamo le seguenti proprietà
  - **(P1)** Due numeri interi consecutivi sono coprimi
  - **(P2)** Siano $a, b, c \in \mathbb{Z}$ tali che $c \mid a \cdot b$ e c, a coprimi. Allora $c \mid b$.
  - **(P3)** Siano $a, b, c \in \mathbb{Z}$ tali che $a \mid c$ e $b \mid c$, se a e b sono coprimi allora $a \cdot b \mid c$.
- Notiamo che nei casi (P2) e (P3) l'ipotesi di coprimalità è fondamentale. Infatti
  - Nel caso (P2), abbiamo che $9 \mid 3 \cdot 6$ ma $9 \nmid 3$ e $\nmid 6$ e infatti non è coprimo con nessuno dei 2.
  - Nel caso (P3), abbiamo che $4 \mid 12$ e $6 \mid 12$ ma $24 \nmid 12$ e infatti 4 e 6 non sono coprimi.

Numeri coprimi: dimostrazioni proprietà

- Dimostriamo (P1)
  - Siano n e $n+1$ due numeri interi consecutivi, allora per $h = 1$ e $k = -1$ abbiamo $1 = h \cdot (n+1) + k \cdot n$
- Dimostriamo (P2)
  - Siano $a, b, c \in \mathbb{Z}$ tali che $c \mid a \cdot b$ e c, a coprimi. Quindi, esiste h tale che $hc = ab$ ed esistono k, k' tali che $1 = ka + k'c$. Moltiplicando per b ambo i termini dell'ultima uguaglianza otteniamo $b = kab + k'cb$ da cui $b = khc + k'cb = c(kh + k'b)$ e quindi $c \mid b$.
- Dimostriamo (P3)
  - Siano $a, b, c \in \mathbb{Z}$ tali che $a \mid c$ e $b \mid c$, ed a e b coprimi. Allora esistono h, k, h', k' tali che $c = ah$, $c = bk$, e $1 = ah' + bk'$. Moltiplicando per c ambo i termini dell'ultima uguaglianza otteniamo $c = ah'c + bk'c = ah'bk + bk'ah = ab(h'k + k'h)$ e quindi $ab \mid c$.

Numeri Primi e Fattorizzazione degli Interi

Come corollario immediato della Proprietà P2 abbiamo che se un numero primo p divide un prodotto $a \cdot b$ allora divide almeno uno dei due fattori del prodotto.
Il teorema fondamentale che riguarda i numeri primi è il seguente teorema di fattorizzazione.

Teorema (Fattorizzazione degli Interi)

Ogni intero $n > 1$ si può esprimere come prodotto di numeri primi positivi ed in modo unico a meno dell'ordine dei fattori.

Nota Unicità significa che se

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

con p_i e q_j numeri primi positivi allora $r = s$ e p_i=q_i se opportunamente ordinati.

Numeri Primi e Fattorizzazione degli Interi

Dimostriamo il teorema di fattorizzazione in due passi distinti.

1. Prima dimostriamo che dato un qualunque intero naturale $n > 1$ esiste una fattorizzazione di n;
2. successivamente, dimostriamo che tale fattorizzazione è unica.

Esistenza: Dimostrazione:
Se, per assurdo, esistessero interi > 1 che non siano prodotto di numeri primi positivi, potremmo costruire l'insieme

$$S = \{n : n \in \mathbb{N}, \text{ non prodotto di numeri primi}\}$$

Per l'assioma di buon ordinamento, possiamo scegliere il minimo dell'insieme S, denotiamolo con s. Per definizione, s non è primo perché se lo fosse sarebbe prodotto (con un solo fattore) di primi positivi (se stesso) e quindi non sarebbe in S. Quindi, s ha divisori diversi da quelli banali e quindi almeno un divisore positivo $1 < d < s$. Allora, esiste $c \in \mathbb{N}$ tale che $s = d \cdot c$, e anche $1 < c < s$. Poiché, c ed d sono minori di s, che ricordiamo è il più piccolo elemento in S, allora c e d sono prodotti di primi positivi, e quindi anche s lo è.
$\triangle$

Numeri Primi e Fattorizzazione degli Interi

Unicità: Dimostrazione:

Sia

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

con p_i e q_j numeri primi positivi. Dobbiamo dimostrare che $r = s$ e che possiamo riordinare i fattori primi ed avere p_i=q_i per ogni i. Dimostriamolo per induzione su r.

- Caso base: $r = 1$. Se $n = p_1$ allora n è primo, e quindi non ha divisori diversi da quelli banali, ossia se stesso e ± 1. Quindi, da $p_1 = q_1 \cdot q_2 \cdot \ldots \cdot q_s$ otteniamo che $s = 1$ e $q_1 = p_1$.
- Caso induttivo: supponiamo la tesi sia vera per r e dimostriamola per $r + 1$. Se

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r \cdot p_{r+1} = q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

abbiamo che q_1 è un divisore di $p_1 \cdot p_2 \cdot \ldots \cdot p_r \cdot p_{r+1}$ e quindi, per quanto precedentemente visto, deve dividere almeno uno dei fattori. Ma sono tutti fattori primi, quindi, q_1 deve essere uguale ad almeno uno dei fattori, che, a meno di riordinare il prodotto, possiamo assumere sia p_1. Dividendo membro a membro per p_1 otteniamo $p_2 \cdot \ldots \cdot p_r \cdot p_{r+1} = q_2 \cdot \ldots \cdot q_s$.

△

Numeri Primi e Fattorizzazione degli Interi

Unicità: Dimostrazione:

- Caso induttivo(cont.): Dal momento che

$$p_2 \cdot \ldots \cdot p_r \cdot p_{r+1} = q_2 \cdot \ldots \cdot q_s$$

  e i fattori del primo membro sono r possiamo applicare l'ipotesi induttiva.
- Abbiamo allora che il numero dei fattori a primo membro è uguale al numero dei fattori a secondo membro, ossia $r = s - 1$ e quindi $r + 1 = s$ ed inoltre i fattori $p_2, \ldots, p_r, p_{r+1}$ coincidono con i fattori $q_2, \ldots, q_s$ a meno dell'ordine.
- Poiché anche $p_1 = q_1$ il teorema è dimostrato.

$\triangle$

Teorema di Euclide

Un altro teorema, tradizionalmente attribuito ad Euclide, è il seguente

Teorema

I numeri primi sono infiniti.

Dimostrazione:

Limitiamoci a dimostrare che i numeri primi positivi sono infiniti.
Supponiamo per assurdo che siano finiti e quindi esiste n tale che i numeri primi siano

$$p_1 = 2, p_2 = 3, \ldots, p_n.$$

Consideriamo allora i numeri positivi

$$h = p_1 \cdot p_2 \cdot \ldots \cdot p_n \text{ e } k = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$$

Per quanto già visto, h e k essendo il secondo il successore del primo, sono coprimi. Notiamo che k non può essere primo perché è diverso da $p_1 = 2, p_2 = 3, \ldots, p_n$ che abbiamo supposto essere tutti i numeri primi. Se non è primo, dal Teorema sulla fattorizzazione sappiamo che k si può scrivere in modo unico come prodotto di primi positivi. Ma questi primi positivi devono essere compresi tra $p_1 = 2, p_2 = 3, \ldots, p_n$ e quindi non sarebbe coprimo con h.
△

Densità dei primi

I primi non solo sono infiniti, ma sono distribuiti in maniera tale da essere molto frequenti. Infatti, vale il seguente teorema

Teorema

Sia $n \in \mathbb{N}$ e sia $\pi(n)$ il numero di "numeri primi" minori od uguali ad n. Allora

$$\lim_{n\to\infty} = \frac{\pi(n)}{\frac{n}{\ln n}} = 1$$

Il teorema ci garantisce che esistono due costanti c_1 e c_2 tali che

$$c_1 \frac{n}{\ln n} \leq \pi(n) \leq c_2 \frac{n}{\ln n}$$

Quindi, per ogni n circa abbiamo una stima di circa $\frac{n}{\ln n}$ numeri primi più piccoli di n. Esempi

- per $n = 100$ stimati $\frac{100}{\ln 100} = \frac{100}{4{,}6} \approx 22$, effettivi 25
- per $n = 1000$ stimati $\frac{1000}{\ln 1000} = \frac{1000}{6{,}9} \approx 145$, effettivi 168
- per $n = 10000$ stimati $\frac{10000}{\ln 10000} = \frac{10000}{9{,}2} \approx 1085$, effettivi 1229

Postulato (Teorema) di Bertrand

Una dimostrazione indiretta del fatto che i numeri primi siano infiniti è data dal Postulato di Bertrand, conosciuto anche con il nome di Teorema di Bertrand-Chebyshev

Teorema

Per ogni $n \geq 2$ esiste un numero primo p tale che $n < p < 2n$.

Test di primalità

- Come verificare se un numero n è primo?
- Ovviamente, verificando che non abbia divisori diversi da quelli banali. Ciò si può fare, in maniera ottimizzata, controllando tutti i numeri interi compresi tra 2 e $\sqrt{n}$.
- Infatti, se il più piccolo divisore di un numero n, denotiamolo con h, fosse maggiore di $\sqrt{n}$ avremmo

$$n = h \cdot q > \sqrt{n} \cdot \sqrt{n} = n$$

  e quindi un assurdo, poiché anche q essendo anch'esso divisore sarebbe più grande di n.
- Il metodo è corretto ma non è molto efficiente, specialmente se si tiene conto che in molte applicazioni di crittografia oggi si usano numeri primi a più di 100 cifre.
- Altri metodi più veloci esistono, ma esulano dallo scopo di questo corso.

Il crivello di Eratostene

- Se abbiamo necessità di calcolare tutti i numeri primi minori od uguali ad un numero prefissato n possiamo utilizzare un algoritmo antico e molto semplice, dovuto al matematico greco Eratostene di Cirene (276-194 AC) noto anche per aver misurato per primo con ottima approssimazione le dimensioni della Terra.
- Come funziona l'algoritmo? Supponiamo di voler calcolare tutti i numeri primi compresi tra 2 e n. Allora procediamo in questo modo
  - Scriviamo in sequenza tutti i numeri naturali compresi tra 2 e n.
  - Partiamo dal numero 2, e cancelliamo dalla sequenza tutti i multipli di 2;
  - Ad ogni passo successivo, prendiamo il primo tra i numeri che seguono che non è stato cancellato e cancelliamo tutti i suoi multipli
  - Quando abbiamo cancellato tutti i multipli del numero più grande che sia minore o uguale a $\sqrt{n}$ ci fermiamo.
- Tutti i numeri rimasti sono primi compresi tra 2 e n.

Il crivello di Eratostene: Esempio

- Supponiamo di voler calcolare tutti i numeri primi compresi tra 2 e 100.
- Partiamo con tutti i numeri naturali in sequenza

2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41
42	43	44	45	46	47	48	49	50	51
52	53	54	55	56	57	58	59	60	61
62	63	64	65	66	67	68	69	70	71
72	73	74	75	76	77	78	79	80	81
82	83	84	85	86	87	88	89	90	91
92	93	94	95	96	97	98	99	100	

Il crivello di Eratostene: Esempio

- Cancelliamo allora tutti i multipli di 2

2	3		5		7		9		11
	13		15		17		19		21
	23		25		27		29		31
	33		35		37		39		41
	43		45		47		49		51
	53		55		57		59		61
	63		65		67		69		71
	73		75		77		79		81
	83		85		87		89		91
	93		95		97		99		

Il crivello di Eratostene: Esempio

- Cancelliamo adesso tutti i multipli di 3, il più piccolo dei numeri non cancellati più grandi di 2.

2	3	5	7			11
	13		17		19	
	23	25			29	31
		35	37			41
	43		47		49	
	53	55			59	61
		65	67			71
	73		77		79	
	83	85			89	91
		95	97			

Il crivello di Eratostene: Esempio

- Continuiamo con i multipli di 5

2	3		5		7				11	
	13				17		19			
	23						29		31	
					37				41	
	43				47		49			
	53						59		61	
					67				71	
	73				77		79			
	83						89		91	
					97					

Il crivello di Eratostene: Esempio

- Completiamo cancellando tutti i multipli di 7 l'ultimo numero rimasto che è più piccolo di $10 = \sqrt{100}$
- otteniamo così i 25 numeri primi compresi tra 2 e 100.

2	3		5		7				11
	13				17		19		
	23						29		31
					37				41
	43				47				
	53						59		61
					67				71
	73						79		
	83						89		
					97				

Criteri di divisibilità

Esistono delle regole molto semplici per verificare, in alcuni casi speciali, se un numero a divide un numero b. Molte di queste si imparano già nei primi anni di scuola. Rivediamo alcune di esse, che riguardano numeri primi ed un numero "speciale", come vedremo, ovvero il numero 9. Cominciamo da quelle più semplici e conosciute.

Div. per 2 Un numero n è divisibile per 2 se e solo se è pari, ovvero se la sua cifra delle unità è una delle seguenti $0, 2, 4, 6, 8$.

Div. per 3 Un numero n è divisibile per 3 se e solo se la somma delle sue cifre è un numero divisibile per 3. In questo caso, notiamo che la somma delle cifre di un numero n è un numero ovviamente più piccolo di n stesso, e se iteriamo il procedimento di sommare la somma delle cifre, si arriverà presto ad uno dei seguenti numeri $3, 6, 9$. Vediamo 3 esempi di numeri divisibili per 3

- Esempio: 1590 la somma delle cifre è $1 + 5 + 9 = 15$ e reiterando $1 + 5 = 6$.
- Esempio: 283197 la somma delle cifre è $2 + 8 + 3 + 1 + 9 + 7 = 30$ e reiterando $3 + 0 = 3$.
- Esempio: 12342222 la somma delle cifre è $1 + 2 + 3 + 4 + 2 + 2 + 2 + 2 = 18$ e reiterando $1 + 8 = 9$.

Div. per 5 Un numero n è divisibile per 5 se e solo se la sua cifra delle unità è 0 oppure 5.

Divisibilità per 7

Un po' meno semplice e di sicuro meno conosciuto è il criterio di divisibilità per 7. Dato un numero intero n dividiamolo per 10. Sia q il quoziente della divisione per 10 e r il resto. Quindi

$$n = 10q + r.$$

Dimostriamo il seguente

Teorema

n è divisibile per 7 se e solo se $q - 2r$ è divisibile per 7.

Dimostrazione:

Supponiamo n sia divisibile per 7. Allora esiste h tale che $n = 7h$. D'altro canto, dividendo n per 10 otteniamo $n = 10q + r$. Quindi, abbiamo

$$\begin{aligned} 7h &= 10q + r \text{ sottraendo } 21r \text{ da entrambi i membri otteniamo} \\ 7h - 21r &= 10q - 20r \text{ e quindi} \\ 7(h - 3r) &= 10(q - 2r) \end{aligned}$$

Quindi, il numero primo 7 divide il prodotto $10(q - 2r)$ e dal momento che non divide 10 allora divide $q - 2r$.

△

Divisibilità per 7

Dimostrazione cont.

Viceversa, supponiamo $q - 2r$ sia divisibile per 7. Allora esiste k tale che $q - 2r = 7k$ e quindi $q = 7k + 2r$. Allora

$$n = 10q + r = 10(7k + 2r) + r = 70k + 21r = 7(10k + 3r)$$

$\triangle$

Vediamo degli esempi

- 84 : abbiamo $8 - 2 \cdot 4 = 0$ e quindi 84 è divisibile per 7.
- 161 : abbiamo $16 - 2 \cdot 1 = 14 = 7 \cdot 2$ e quindi 161 è divisibile per 7.
- 581 : abbiamo $58 - 2 \cdot 1 = 56 = 7 \cdot 8$ e quindi 581 è divisibile per 7.
- 2247 : abbiamo $224 - 2 \cdot 7 = 210 = 7 \cdot 30$ e quindi 2247 è divisibile per 7.

Divisibilità per altri primi

In maniera analoga a quanto dimostrato per 7, dato un numero n e la sua divisione per 10 che produce quoziente q, ovvero il numero ottenuto dal numero dato n non scrivendo la cifra delle unità, e resto r, ovvero la cifra della unità, abbiamo il seguente teorema che ci dà un criterio di divisibilità per i primi $13, 17, 19$ e 23. Ripetiamo anche il caso 7 per maggiore chiarezza.

Teorema

Un numero intero $n = 10 \cdot q + r$ è divisibile per p se e solo se $q + a \cdot r$ è divisibile per p, dati i seguenti valori combinati di p e a

p	a
7	-2
13	4
17	-5
19	2
23	7

La dimostrazione del teorema per ognuno dei 5 ulteriori casi è analoga al caso 7.

Divisibilità per altri primi

Dato un numero intero $n = 10 \cdot q + r$ e presi q quoziente della divisione per 10 ovvero numero ottenuto da n omettendo la cifra delle unità, ed r resto della divisione per 10 ovvero cifra delle unità, abbiamo allora che

- 13 divide n se $q + 4r$ è divisibile per 13
- 17 divide n se $q - 5r$ è divisibile per 17
- 19 divide n se $q + 2r$ è divisibile per 19
- 23 divide n se $q + 7r$ è divisibile per 23

Prendiamo come esempio il numero 96577 e abbiamo $q = 9657$ e $r = 7$.

- $q + 4r = 9657 + 28 = 9685$; $968 + 20 = 988$, $98 + 32 = 130$ ed infine $13 + 0 = 13$ e quindi 96577 è divisibile per 13;
- $q - 5r = 9657 - 35 = 9622$; $962 - 10 = 952$, $95 - 10 = 85$ ed infine $8 - 25 = -17$ e quindi 96577 è divisibile anche per 17;
- $q + 2r = 9657 + 14 = 9671$; $967 + 2 = 969$, $96 + 18 = 114$ ed infine $11 + 8 = 19$ e quindi 96577 è divisibile anche per 19;
- $q + 7r = 9657 + 49 = 9706$; $970 + 42 = 1012$, $101 + 14 = 115$, ed infine $11 + 35 = 46 = 2 \cdot 23$ e quindi 96577 è divisibile anche per 23

Divisibilità per 11

Per il numero 11 una regola simile a quelle già viste è la seguente $n = 10q + r$ è divisibile per 11 se e solo se $q - r$ è divisibile per 11. Tale regola è equivalente alla seguente più facile da usare e ricordare. Guardiamo i multipli di 11

- $11, 22, 33, 44, 55, 66, 77, 88, 99$ (2 cifre)
- $110, 121, 132, 143, 154, 165, 176, 187, 198, 209, 220, 231, \ldots$ (3 cifre)
- $1001, 1012, 1023, 1034, 1045, 1056, \ldots$ (3 cifre)

In pratica, se a è la somma delle cifre di posto dispari e b è la somma delle cifre di posto pari, la loro differenza è divisibile per 11. Vediamo altri esempi

- 2805 $a = 2 + 0 = 2$ e $b = 8 + 5 = 13$ quindi $a - b = -11$ ed il numero è divisibile per 11
- 14894 $a = 1 + 8 + 4 = 13$ e $b = 4 + 9 = 13$ quindi $a - b = 0$ ed il numero è divisibile per 11

Casi particolari se il numero ha un numero pari di cifre:

- Tutti i numeri dove le cifre si susseguono a coppie uguali, es. 112233 sono divisibili per 11
- Numeri palindromi, ossia numeri che letti da sinistra a destra o da destra a sinistra sono uguali, esempio 12344321

Radice numerica

Diamo la seguente definizione

Definizione (Radice Numerica)

Dato $n \in \mathbb{N}$ la radice numerica di n, denotiamola con $\rho(n)$ è la somma delle sue cifre reiterata sino ad ottenere una sola cifra.

Vediamo degli esempi

- $198 : 1 + 9 + 8 = 18 \to 1 + 8 = 9$ e quindi $\rho(198) = 9$.
- $239 : 2 + 3 + 9 = 14 \to 1 + 4 = 5$ e quindi $\rho(239) = 5$.
- $1137 : 1 + 1 + 3 + 7 = 12 \to 1 + 2 = 3$ e quindi $\rho(1137) = 3$.

Quindi, un numero n è divisibile per 3 se e solo se $\rho(n) = 3$ oppure $\rho(n) = 6$, oppure ancora $\rho(n) = 9$.

Divisibilità per 9

- Un numero n è divisibile per 9 se e solo se la somma delle sue cifre è un numero divisibile per 9, ossia se e solo se $\rho(n) = 9$.
- Negli esempi visti prima, allora, solo 198 è divisibile per 9, mentre sia 198 che 1137 sono divisibili per 3.
- Il numero 9 è la cifra più alta del nostro sistema di numerazione in base 10. Questo ci dice che le cifre di tutti i numeri che precedono una potenza di 10 sono tutte uguali a 9. In particolare, per ogni intero $i > 0$, $10^i - 1$ e il numero composto da i cifre tutte uguali a 9. Per esempio $10^1 - 1 = 9$, $10^2 - 1 = 99$, $10^3 - 1 = 999$, etc.
- Per quanto detto prima, allora, $10^i - 1$ è divisibile per 9 per ogni $i > 0$.

In particolare, se indichiamo con b_i il numero intero con i cifre tutte uguali ad 1 abbiamo che $10^i - 1 = 9 \cdot b_i$. A causa di tale caratteristica, vale la proprietà descritta nel seguente teorema.

Teorema (Divisibilità per 9)

Sia n un numero naturale e sia m la somma delle sue cifre. Allora $n - m$ è divisibile per 9.

Altra proprietà del 9

Dimostrazione:

Il numero n è caratterizzato dalla seguente

$$n = \sum_{i=0}^{k} a_i \cdot 10^i$$

dove a_0 sono le unità, a_1 le decine, ed in generale a_i il coefficiente della potenza 10^i. Quindi, $a_0, a_1, \ldots, a_k$ sono le cifre che rappresentano il numero. Otteniamo allora che

$$n - m = \sum_{i=0}^{k} a_i \cdot 10^i - \sum_{i=0}^{k} a_i = \sum_{i=0}^{k} a_i \cdot (10^i - 1) = \sum_{i=0}^{k} a_i \cdot 9 \cdot b_i = 9 \cdot \sum_{i=0}^{k} a_i \cdot b_i$$

$\triangle$

Vediamo degli esempi

- 199 non è divisibile per 9 però $199 - 19 = 180$ è divisibile per 9;
- 640 non è divisibile per 9 però $640 - 10 = 630$ è divisibile per 9;
- 1129 non è divisibile per 9 però $1129 - 13 = 1116$ è divisibile per 9

Problemi implementativi e matematici

Proponiamo come esercizi implementativi i seguenti

- Implementare il test di primalità come funzione "**bool Primo(int x)**" che prende in input un intero naturale, verifica che sia maggiore di 1 e ritorna vero se il numero è primo e falso altrimenti. La funzione implementa la ricerca di divisori sino alla $\sqrt{x}$ e termina immediatamente quando trova un divisore, oppure quando supera il valore di $\sqrt{x}$
- Come secondo esercizio implementativo, implementare il crivello di Eratostene. La funzione che implementerete usa come parametro un intero n e poi utilizza un array dinamica per memorizzare tutti i numeri primi minori di n calcolati.
- Il terzo esercizio è matematico: adesso che sappiamo cosa sono i numeri pari, e cos'è il MCD di due numeri possiamo dimostrare che $\sqrt{2}$ non è un numero razionale. La dimostrazione di questo esercizio è data nei lucidi successivi.

$\sqrt{2}$ non è razionale.

Dimostriamo adesso, ragionando per assurdo, che $\sqrt{2}$ non è un numero razionale.

- Assumiamo quindi che esistano 2 numeri naturali, a e b tali che $\sqrt{2} = \frac{a}{b}$.
- Assumiamo che la frazione sia ridotta, ovvero che il $MCD(a, b)$ sia 1. Se non fosse così, potremmo dividere numeratore e denominatore per il loro MCD ed ottenere lo stesso valore.
- Allora, almeno uno dei 2 numeri deve essere dispari.
- Elevando al quadrato otteniamo

$$2b^2 = a^2$$

- Quindi, il quadrato di a è pari, ed allora anche a è pari, ovvero esiste k tale che $a = 2k$.
- Avremmo allora

$$2b^2 = a^2 = 4k^2 \quad \text{e quindi} \quad b^2 = 2k^2$$

- Allora, anche b è pari, che contraddice la nostra ipotesi iniziale.

Esercizi divisibiltà

Vediamo con un esempio come svolgere gli esercizi.
Es.: 525 :

- divisibile per 3 (somma delle cifre $= 12$),
- divisibile per 5 (termina con 5),
- divisibile per 7 ($52 - 10 = 42$ multiplo di 7),
- non divisibile per 9 (somma delle cifre non è multiplo di 9),
- non divisibile per 11 (somma cifre di posto dispari 10 e posto pari 2),
- non divisibile per 13 ($52 + 20 = 72$ non multiplo di 13 perché $7 + 8 = 15$),
- non divisibile per 17 ($52 - 25 = 27$ non multiplo di 17),
- non divisibile per 19 ($52 + 10 = 62$ non multiplo di 19 perché $6 + 4 = 10$),
- non divisibile per 23 ($52 + 35 = 87$ non divisibile per 23 perché $8 + 49 = 57$ non è multiplo di 23).

Esercizi divisibilità

Per ognuno dei seguenti, verificare quali criteri di divisibilità si possono applicare tra quelli visti per $2, 3, 5, 7, 9, 11, 13, 17, 19, 23$.
Verificare anche che numeri consecutivi sono coprimi.

- 119, 120,
- 195, 196,
- 231, 232
- 399, 400,
- 437, 438,
- 532, 533

STRUTTURE DISCRETE

PARTE 2: Fondamenti di Teoria dei Numeri e metodologie di dimostrazione

2: Aritmetica Modulare

Congruenze

- L'aritmetica modulare riguarda il calcolo sui resti delle divisioni tra interi rispetto ad un divisore fissato.
- L'idea centrale è quella delle congruenze, ovvero considerare "equivalenti" interi che hanno lo stesso resto rispetto ad un divisore fissato.
- Ricordiamo che per il Teorema della Divisione dati comunque due interi relativi $n, m \in \mathbb{Z}$, $m \neq 0$, esistono unici q (quoziente) ed r (resto) della divisione intera, tali che $n = qm + r$ e in particolare il resto r verifica la proprietà che $0 \leq r < |m|$ ed è denotato con $n \bmod m$. Quindi, $n = qm + n \bmod m$.
- n viene comunemente detto "base" mentre m viene detto "modulo".

Congruenza modulo m

Fissiamo un intero relativo m. Nell'insieme $\mathbb{Z}$ degli interi relativi definiamo una relazione, detta congruenza modulo m, in questo modo:

- un intero $a \in \mathbb{Z}$ è in relazione con $b \in \mathbb{Z}$ se $m \mid (a - b)$ ovvero $a - b$ è un multiplo di m.
- Equivalentemente, a è in relazione con b se $a \bmod m = b \bmod m$. Infatti, se $a \bmod m = b \bmod m = r$ abbiamo $a = q_1 m + r$ e $b = q_2 m + r$ per qualche $q_1, q_2 \in \mathbb{Z}$ e quindi $a - b = (q_1 - q_2)m$ è un multiplo di m.
- Se ciò si verifica cioè se a e b sono in relazione si scrive

$$a \equiv b (\bmod\ m)$$

  e si dice che a è congruo b modulo m.
- Se ciò non si verifica, cioè a non è congruo b modulo m si scrive

$$a \not\equiv b (\bmod\ m)$$

- Da quanto detto abbiamo ovviamente che $a \equiv a (\bmod\ m)$ per ogni a e per ogni m.

Congruenze: Esempi

- $12 \equiv 9 (\mod 3)$: infatti $12 \mod 3 = 0$ e $9 \mod 3 = 0$ entrambi per il primo caso del teorema della divisione
- $-15 \equiv 9 (\mod 4)$: infatti per il secondo caso del teorema della divisione, $-15 \mod 4 = 1$ mentre per il primo caso, $9 \mod 4 = 1$
- $7 \not\equiv 1 (\mod 4)$ infatti $7 \mod 4 = 3$ mentre $1 \mod 4 = 1$
- $-7 \equiv 1 (\mod 4)$ infatti $-7 \mod 4 = 1$

Congruenze

- Notiamo che per ogni $a \in \mathbb{Z}$ ed ogni $m \in \mathbb{N}$ abbiamo che

$$a \equiv a \bmod m (\bmod\ m)$$

- Infatti, per il teorema della divisione abbiamo $a = qm + r$ con $0 \leq r < |m|$ ovvero $a = qm + a \bmod m$.
- Quindi,

$$a - (a \bmod m) = qm$$

Congruenze

La relazione di congruenza modulo m è una relazione d'equivalenza, ed ovviamente, ciò implica che abbiamo una infinità di relazioni di equivalenza, visto che possiamo variare m nell'insieme $\mathbb{Z}$.
Dimostriamo che è una relazione di equivalenza

Riflessiva: Per ogni $a \in \mathbb{Z}$ è vero che $a \equiv a (\mathrm{mod}\ m)$? Si, perché $0 = a - a$ è multiplo di m (lo 0 è multiplo di qualunque numero.)

Simmetrica: Se $a \equiv b (\mathrm{mod}\ m)$ allora $a - b = km$ per qualche $k \in \mathbb{Z}$ e quindi, moltiplicando per -1 otteniamo $b - a = (-k)m$ ossia $b \equiv a (\mathrm{mod}\ m)$

Transitiva: Se $a \equiv b (\mathrm{mod}\ m)$ e $b \equiv c (\mathrm{mod}\ m)$ abbiamo che esistono $h, k \in \mathbb{Z}$ tali che $a - b = hm$ e $b - c = km$. Sommando membro a membro le ultime due uguaglianze otteniamo: $a - c = (h + k)m$ e quindi $a \equiv c (\mathrm{mod}\ m)$.

Nota: Come conseguenza del teorema della divisione, la congruenza modulo m coincide con la congruenza modulo $-m$.
Infatti se $a \equiv b (\mathrm{mod}\ m)$ allora $a - b = km$ con $k \in \mathbb{Z}$ e quindi $a \equiv b (\mathrm{mod}(-m))$ poiché $a - b = (-k)(-m)$.
Ci limiteremo a studiare allora le congruenze con $m \geq 0$.

Congruenze e classi di equivalenza

Visto che la relazione di congruenza modulo m è una relazione d'equivalenza vediamo quali sono le classi di equivalenza in cui viene partizionato $\mathbb{Z}$ dalla relazione di congruenza modulo m.
In particolare, vediamo alcune congruenze notevoli.

Congruenza modulo 0

$$a \equiv b (\mathrm{mod}\ 0) \text{ se e solo se } a - b = k \cdot 0 \text{ ovvero } a - b = 0 \text{ quindi se } a = b.$$

La relazione di congruenza modulo 0 coincide con la relazione di uguaglianza. Se a è un intero relativo la sua classe di equivalenza modulo 0 è $\{a\}$. Ogni classe contiene un solo elemento. $\mathbb{Z}$ viene partizionato in infinite classi ognuna contenente un solo numero.

Congruenze e classi di equivalenza

Congruenza modulo 1

$$a \equiv b \pmod 1 \text{ se e solo se } a - b = k \cdot 1 \text{ ovvero } a - b \text{ è multiplo di } 1.$$

Ma ogni numero è multiplo di 1 quindi ogni numero a è in relazione modulo 1 con ogni altro intero relativo b. Esiste quindi un'unica classe di equivalenza modulo 1 contenente tutti gli interi cioè $\mathbb{Z}$.

Congruenza modulo 2

$$a \equiv b \pmod 2 \text{ se e solo se } a - b = k \cdot 2 \text{ ovvero } a - b \text{ è un numero pari}$$

Allora, se a è pari, abbiamo $a = 2 \cdot h$ per qualche h e quindi $b = 2h - 2k = 2(h - k)$ è pure pari. Notiamo anche che se a è pari, allora $a - 0 = k \cdot 2$ e quindi $a \equiv 0 \pmod 2$ per ogni a numero pari.
Se invece a è dispari, abbiamo $a = 2 \cdot h + 1$ per qualche h e quindi $b = 2h - 2k + 1 = 2(h - k) + 1$ è pure dispari.
Esistono quindi due classi di equivalenza modulo 2 una contenente tutti i numeri pari e l'altra contenente tutti i numeri dispari.

Congruenze e classi di equivalenza

Dato un intero $m \geq 0$, indicheremo con $[a]_m$ la classe rappresentata dall'intero a nella relazione di congruenza modulo m, cioè

$$[a]_m = \{b \in \mathbb{Z} : a \equiv b (\mathrm{mod}\, m\}.$$

Dimostriamo adesso il seguente teorema (che estende quanto visto per il caso $m = 2$.)

Teorema

Fissato un intero $m > 1$, le classi di equivalenza della relazione di congruenza modulo m sono in numero di m e sono esattamente: $[0]_m$, $[1]_m$, $[2]_m$, $\ldots [m-1]_m$.

Dimostrazione:

Sia $a \in \mathbb{Z}$ e sia r il resto della divisione intera di a per m, ovvero, applicando l'algoritmo di divisione

$$a = qm + r \text{ con } 0 \leq r < m.$$

Dal momento che $a - r = qm$ abbiamo che $a \equiv r (\mathrm{mod}\ m)$.
Quindi, dal momento che r può assumere solo i valori che vanno da 0 a $m-1$ le classi di equivalenza sono solo quelle dell'enunciato del teorema.
$\triangle$

Congruenze e classi di equivalenza

Dimostrazione cont.

Dimostriamo adesso che le classi $[0]_m$, $[1]_m$, $[2]_m$, $\ldots [m-1]_m$, sono tutte distinte. Ragioniamo per assurdo e supponiamo che esistano $x, y \in \mathbb{Z}$, $x \neq y$ e $0 \leq x, y < m-1$ tali che $[x]_m = [y]_m$. Senza perdita di generalità supponiamo che $x > y$. Dall'ipotesi possiamo scrivere $x - y = km$ cioè $x - y$ è un multiplo di m. Da $0 \leq x, y < m-1$ e $x > y$ segue che $0 < x - y < m - 1$, che è una contraddizione visto che non esistono multipli di m in tra 0 e $m-1$.
$\triangle$

Come abbiamo appena dimostrato le classi della relazione di congruenza modulo m sono esattamente $[0]_m$, $[1]_m$, $[2]_m$, $\ldots [m-1]_m$, ovvero le classi caratterizzate da tutti i possibili resti della divisione di un intero per m. Queste classi allora si chiamano anche classi resto modulo m.

Esempio

Sia $m = 5$ (congruenza modulo 5). Le classi resto modulo 5 sono $[0]_5, [1]_5, [2]_5, [3]_5, [4]_5$.

Congruenze Aritmetiche

- Dato $a \in \mathbb{Z}$ come facciamo a stabilire in quale classe resto sta?
- La risposta ci viene fornita dal teorema appena dimostrato: $[a]_m = [r]_m$ dove r è il resto della divisione di a per m.
- Quindi se $m = 5$ e $a = 22$ allora eseguendo la divisione abbiamo $22 : 5 = 4$ con resto di 2, ottenendo che $[22]_5 = [2]_5$.
- Notiamo che in classe $[0]_5$ ci sono tutti i multipli di 5 ed in generale in $[0]_m$ ci sono tutti i multipli di m.

Invarianza rispetto a somma e prodotto

Vale il seguente teorema.

Teorema

Dato $m \in \mathbb{N}$ e dati $a, b \in \mathbb{Z}$ tali che $a \equiv b \pmod{m}$, allora comunque prendiamo $c, d \in \mathbb{Z}$ tali che $c \equiv d \pmod{m}$ abbiamo

1. $a + c \equiv b + d \pmod{m}$
2. $a \cdot c \equiv b \cdot d \pmod{m}$

Dimostrazione:

Per ipotesi esistono $k_1, k_2 \in \mathbb{Z}$ tale che $a - b = k_1 m$ e $c - d = k_2 m$. Quindi,

1. $(a + c) - (b + d) = (a - b) + (c - d) = (k_1 + k_2)m$ che dimostra la proprietà.
2. Abbiamo $a = b + k_1 m$ e $c = d + k_2 m$, quindi $ac - bd = (b + k_1 m)(d + k_2 m) - bd = bk_2 m + dk_1 m + k_1 k_2 m^2 = (bk_2 + dk_1 + k_1 k_2 m)m$ che dimostra la proprietà.

△

Invarianza rispetto a somma e prodotto

Come caso particolare del teorema abbiamo
Invarianza rispetto alla somma: Se sommiamo ad ambo i membri di una congruenza uno stesso numero intero, la congruenza non cambia. Cioè, per ogni $a, b, c \in \mathbb{Z}$ se

$$a \equiv b (\mathrm{mod}\ m) \text{ allora } a + c \equiv b + c (\mathrm{mod}\ m)$$

Invarianza rispetto al prodotto: Se moltiplichiamo ambo i membri di una congruenza per uno stesso numero intero, la congruenza non cambia. Cioè, per ogni $a, b, c \in \mathbb{Z}$ se

$$a \equiv b (\mathrm{mod}\ m) \text{ allora } ac \equiv bc (\mathrm{mod}\ m)$$

Invarianza rispetto a somma e prodotto

Come conseguenza dell'invarianza rispetto a somma e prodotto, dati $a, b, m \in \mathbb{N}$ e visto che $a \equiv a \bmod m (\bmod\ m)$ e $b \equiv b \bmod m (\bmod\ m)$ allora valgono le seguenti proprietà

(P1) $(a+b) \equiv (a \bmod m + b \bmod m)(\bmod\ m)$ ossia
$(a+b) \bmod m = (a \bmod m + b \bmod m)(\bmod\ m)$

(P2) $(a \cdot b) \equiv (a \bmod m \cdot b \bmod m)(\bmod\ m)$ ossia
$(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m))(\bmod\ m)$

Come conseguenza della proprietà P2 abbiamo

(P3) Dati $a, n, m \in \mathbb{N}$, $a^n \equiv (a \bmod m)^n (\bmod\ m)$

(P4) Dati $a, b, h, k, m \in \mathbb{N}$ allora $a^h \cdot b^k \equiv (a^h \bmod m) \cdot (b^k \bmod m)(\bmod\ m)$ ossia
$a^h \cdot b^k \bmod m = (a \bmod m)^h \cdot (b \bmod m)^k \bmod m$

Invarianza rispetto a somma e prodotto: Esempi

Esempi

1. $60 \bmod 7 = (50 + 10) \bmod 7$. Quindi, per la proprietà P1 abbiamo
   $60 \bmod 7 = ((50 \bmod 7) + (10 \bmod 7)) \bmod 7 = (1 + 3) \bmod 7 = 4$
2. $60 \bmod 7 = (6 \cdot 10) \bmod 7$. Quindi, per la proprietà P2 abbiamo
   $60 \bmod 7 = ((6 \bmod 7) \cdot (10 \bmod 7)) \bmod 7 = (6 \cdot 3) \bmod 7 = 18 \bmod 7 = 4$
3. Calcoliamo $13^2 \bmod 10$. Per la proprietà P3 abbiamo
   $13^2 \bmod 10 = (13 \bmod 10)^2 \bmod 10 = 3^2 \bmod 10 = 9 \bmod 10 = 9$.
   Verifichiamo, $13^2 = 169$ ed il resto della divisione per 10 è proprio 9.
4. Calcoliamo $41503 \bmod 5$. Abbiamo $41503 = 121 \cdot 343 = 11^2 \cdot 7^3$ e quindi per la proprietà P4:
   $41503 \bmod 5 = (11^2 \bmod 5) \cdot (7^3 \bmod 5) \bmod 5 =$
   $= (11 \bmod 5)^2 \cdot (7 \bmod 5)^3 \bmod 5 = 1 \cdot 2^3 \bmod 5 = 8 \bmod 5 = 3$

Invarianza rispetto a somma e prodotto: Esempi

Esempi

1. Calcoliamo $3^{10} \bmod 11$. Dal momento che $3^{10} = 3^4 \cdot 3^6$ per la proprietà P2 abbiamo $3^{10} \bmod 11 = (3^4 \bmod 11) \cdot (3^6 \bmod 11) \bmod 11$. Quindi

$$3^{10} \bmod 11 = (3^4 \bmod 11) \cdot (3^6 \bmod 11) \bmod 11 =$$
$$(81 \bmod 11) \cdot (3^6 \bmod 11) \bmod 11 = 4 \cdot (3^6 \bmod 11) \bmod 11$$

Ma, $3^6 = 3^3 \cdot 3^3$ e applicando ancora la proprietà P2, abbiamo $3^6 \bmod 11 = ((3^3 \bmod 11) \cdot (3^3 \bmod 11)) \bmod 11 = (27 \bmod 11)^2 \bmod 11$. Quindi,

$$3^{10} \bmod 11 = 4 \cdot (27 \bmod 11)^2 \bmod 11 = 4 \cdot 5^2 \bmod 11 =$$
$$4 \cdot 25 \bmod 11 = 100 \bmod 11 = 1.$$

Verifichiamo, $3^{10} = 59049$ e quindi $3^{10} - 1 = 59048 = 11 \cdot 5368$

2. Calcoliamo $2^{20} \bmod 11$. Abbiamo

$$2^{20} \bmod 11 = (2^5)^4 \bmod 11 = 32^4 \bmod 11 = (32 \bmod 11)^4 \bmod 11 =$$
$$10^4 \bmod 11 = (10^2)^2 \bmod 11 = (100 \bmod 11)^2 \bmod 11 = 1 \bmod 11 = 1$$

Verifichiamo, $2^{20} = 1048576$ e quindi $2^{20} - 1 = 1048575 = 11 \cdot 95325$

Invarianza rispetto a somma e prodotto

Il viceversa delle proprietà viste, vale però solo per la somma. Infatti,

Invarianza rispetto alla somma: Se sottraiamo ad ambo i membri di una congruenza uno stesso numero intero, la congruenza non cambia. Cioè, per ogni $a, b, c \in \mathbb{Z}$ se

$$a \equiv b (\mathrm{mod}\ m) \text{ allora } a - c \equiv b - c (\mathrm{mod}\ m)$$

vale, banalmente, visto che abbiamo dimostrato il risultato per interi relativi, e quindi in particolare $c \in \mathbb{Z}$

Invarianza rispetto al prodotto: Se dividiamo ambo i membri di una congruenza per uno stesso numero intero, la congruenza potrebbe non valere più. Ecco un esempio

$$2 \cdot 3 \equiv 2 \cdot 1 (\mathrm{mod}\ 4) \text{ MA } 3 \not\equiv 1 (\mathrm{mod}\ 4)$$

Invarianza rispetto alla somma: conseguenze

Una immediata conseguenza dell'invarianza rispetto alla somma è la seguente

Teorema

Per ogni $m \in \mathbb{N}$, $m > 1$, una qualunque sequenza di m interi consecutivi contiene esattamente un intero divisibile per m.

Dimostrazione:

Consideriamo allora m interi consecutivi, dove il più piccolo è n per qualche $n \in \mathbb{Z}$. Gli m interi della sequenza sono ovviamente

$$n, n+1, n+2, \ldots, n+m-1$$

Come abbiamo già dimostrato, le classi di equivalenza della relazione di congruenza modulo m sono $[0]_m$, $[1]_m$, $[2]_m$, $\ldots$ $[m-1]_m$, ed in particolare la classe $[0]_m$ contiene tutti gli interi divisibili per m ovvero tutti i multipli di m.
L'intero n sta allora in una di queste classi. Supponiamo stia nella classe $[i]_m$ per $0 \leq i \leq m-1$. Quindi $n \equiv i \pmod{m}$ ed allora $n+1 \equiv i+1 \pmod{m}$ ovvero $n+1 \in [i+1]_m$.
$\triangle$

Invarianza rispetto alla somma: conseguenze

Dimostrazione cont.

Notiamo allora che se $i = 0$ ovvero $n \in [0]_m$ abbiamo dimostrato il teorema. Se invece $i > 0$, visto che $0 < i < m$ incrementando i esattamente $m - i$ volte, con $m - i < m$ iil valore m e quindi otteniamo che $n + (m - i) \equiv i + (m - i) (\mathrm{mod}\ m)$ ossia $n + (m - i) \equiv m (\mathrm{mod}\ m) \equiv 0 (\mathrm{mod}\ m)$. In conclusione, $n + (m - i)$ è il numero multiplo di m nella sequenza di m numeri consecutivi.

$\triangle$

Possiamo allora dire

- Dati 2 numeri consecutivi, almeno uno dei due numeri è divisibile per 2. E questo già lo sapevamo.
- Dati 3 numeri consecutivi, esattamente uno dei tre numeri è divisibile per 3 ed almeno uno è divisibile per 2. Quindi, il prodotto di 3 numeri consecutivi è sempre divisibile per 6.
- Dati 5 numeri consecutivi, esattamente uno dei cinque numeri è divisibile per 5, almeno uno è divisibile per 3 ed almeno 2 sono divisibili per 2. Quindi, il prodotto di 5 numeri consecutivi è sempre divisibile per 60
- etc.

Invarianza rispetto alla somma: Esercizi

(E1) Comunque prendiamo $n > 1$, si ha $n^3 - n \equiv 0 (\mod 6)$ ovvero comunque prendiamo $n > 1$, $n^3 - n$ è un multiplo di 6.

Per dimostrare l'esercizio notiamo che $n^3 - n = n(n^2 - 1)$. Ma $n^2 - 1 = (n-1) \cdot (n+1)$. Quindi,

$$n^3 - n = n \cdot (n-1) \cdot (n+1) = (n-1) \cdot n \cdot (n+1)$$

ovvero è il prodotto di 3 interi consecutivi e quindi è divisibile per 6.

(E2) Se abbiamo tre numeri consecutivi $n, n+1, n+2$, con $n > 3$, tali che n e $n+2$ sono entrambi primi, allora $n+1$ è un multiplo di 6.

Per dimostrare l'esercizio, ci ricordiamo che dati 3 numeri consecutivi almeno uno deve essere pari, ossia divisibile per 2. Dal momento che n e $n+2$ sono primi, tale numero pari deve necessariamente essere $n+1$. Analogamente, dal momento che uno dei tre numeri deve essere divisibile per 3, tale numero deve necessariamente essere $n+1$. Quindi, $n+1$ è divisibile sia per 2 che per 3 ed è quindi divisibile per 6.

Invarianza rispetto al prodotto: Esercizi

- Se vogliamo calcolare $11^{333} \bmod 10$, dal momento che $11 \equiv 1 (\mathrm{mod} 10)$ abbiamo che
$$11^{333} \equiv 1^{333} (\mathrm{mod} 10) \equiv 1 (\mathrm{mod} 10)$$
quindi $11^{333} \bmod 10 = 1$.
- Calcoliamo adesso $9^{333} \bmod 10$. Per il secondo caso del teorema della divisione abbiamo che $-1 \bmod 10 = 9$ e quindi $9 \equiv (-1) (\mathrm{mod} 10)$. Quindi,
$$9^{333} \equiv (-1)^{333} (\mathrm{mod} 10) \equiv (-1) (\mathrm{mod} 10) \equiv 9 (\mathrm{mod} 10)$$
e concludiamo che $9^{333} \bmod 10 = 9$.
- Calcoliamo adesso $48^{10} \bmod 10$. Abbiamo che $48 \bmod 10 = 8 = (-2) \bmod 10$. Quindi
$$48^{10} \equiv (-2)^{10} (\mathrm{mod} 10) \equiv 1024 (\mathrm{mod} 10) \equiv 4 (\mathrm{mod} 10)$$
e concludiamo che $48^{10} \bmod 10 = 4$.

Divisione modulare

Abbiamo visto che due interi naturali $a, b \in \mathbb{N}$ non entrambi uguali a 0, sono coprimi, ovvero $MCD(a, b) = 1$, se e solo se esistono $h, k \in \mathbb{Z}$ tali che $a \cdot h + b \cdot k = 1$. Come sappiamo, per i numeri razionali esiste un concetto di "inverso" ovvero preso $a \in \mathbb{Q}$, $a \neq 0$, esiste $x \in \mathbb{Q}$ tale che $a \cdot x = 1$. L'elemento x viene chiamato "inverso di a" e denotato con il simbolo a^{-1}. Il seguente teorema introduce una nozione simile per l'aritmetica modulare.

Teorema (Esistenza dell'inverso modulare)

Siano $a, b \in \mathbb{N}$ entrambi maggiori di zero. Allora, esiste un elemento $x \in \mathbb{N}$ tale che $a \cdot x \equiv 1 \pmod{b}$ se e solo se a e b sono coprimi.

L'elemento x, denotato con $a^{-1} \bmod b$ o semplicemente a^{-1} viene detto "inverso di a modulo b".

Esempi:

- $a = 5, b = 3 : a^{-1} = 2$, infatti $2 \cdot 5 \bmod 3 = 10 \bmod 3 = 1$.
- $a = 9, b = 7 : a^{-1} = 4$, infatti $4 \cdot 9 \bmod 7 = 36 \bmod 7 = 1$.
- $a = 9, b = 11 : a^{-1} = 5$, infatti $5 \cdot 9 \bmod 11 = 45 \bmod 11 = 1$.
- $a = 14, b = 6$: notiamo che i multipli di 14 quando divisi per 6 danno i seguenti resti $14 \bmod 6 = 2, 28 \bmod 6 = 4, 42 \bmod 6 = 0, 56 \bmod 6 = 2, 70 \bmod 6 = 4, 80 \bmod 6 = 0, \ldots$ e quindi, come dice il teorema, l'inverso di 14 modulo 4 non esiste.

Divisione modulare

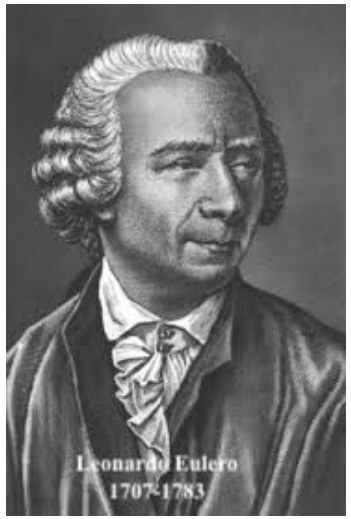
Dimostriamo il teorema

Dimostrazione:

- Caso $\Rightarrow$: supponiamo a, b siano coprimi. Esistono h, k tali che $ha + kb = 1$. Quindi, $ha = 1 - kb$ e quindi, dal momento che $(1 - kb) \bmod b = 1$ abbiamo che $ha \equiv 1 (\bmod\ b)$ e $h = a^{-1}$ modulo b.
- Caso $\Leftarrow$: supponiamo esista x tale che $xa \equiv 1 (\bmod\ b)$. Dalla definizione di congruenza, ciò implica che esiste k tale che $xa - 1 = kb$ e quindi $xa + (-k)b = 1$ ovvero $MCD(a, b) = 1$ e quindi a, b coprimi.

$\triangle$

Eulero



Eulero fu uno dei più grandi matematici del diciottesimo secolo e probabilmente uno dei più grandi della storia.

Fu un fisico, astronomo, logico ed ingegnere ed autore di numerose e fondamentali scoperte in molti settori della matematica tra cui il calcolo infinitesimale, la teoria dei grafi e la teoria dei numeri.

Qui, introduciamo una definizione in teoria dei numeri che ha notevoli applicazioni.

Funzione di Eulero

- Sia n un intero positivo, cioè $n > 0$.
- Vogliamo contare quanti sono i numeri che precedono n e che siano coprimi con n.
- Definiamo allora la funzione

$$\phi(n) = |\{x : x \in \mathbb{N}, 0 < x \leq n \text{ e } MCD(n, x) = 1\}|$$

Esempi:

- $n = 1 : \phi(1) = 1$ poiché $0 < 1 \leq 1$ e $MCD(1, 1) = 1$.
- $n = 2 : \phi(2) = 1$ poiché $0 < 1 \leq 1$ e $MCD(2, 1) = 1$, mentre $MCD(2, 2) = 2$.
- $n = 3 : \phi(3) = 2$ poiché $MCD(3, 1) = 1$, e $MCD(3, 2) = 1$
- $n = 4 : \phi(4) = 2$ poiché $MCD(4, 1) = 1$, e $MCD(4, 3) = 1$
- $n = 5 : \phi(5) = 4$ poiché $MCD(5, x) = 1$, per $x = 1, 2, 3, 4$.

Formula generale

- Proviamo a costruire una formula generale per il calcolo di $\phi(n)$.
- Lo faremo analizzando alcuni casi speciali.
- Cominciamo con il caso più semplice

Formula di Eulero: Caso 1

Se n è un numero primo tutti i predecessori di n sono ad esso coprimi, e quindi $\phi(n) = n - 1$.

Esempi:

- $phi(2) = 1$
- $phi(3) = 2$
- $phi(5) = 4$
- $phi(7) = 6$
- $phi(11) = 10$
- $phi(13) = 12$

Formula generale

Formula di Eulero: Caso 2

Analizziamo il caso n potenza di numero primo, ovvero $n = p^k$ dove $k \geq 2$ e p è primo.

- I divisori di n sono $p, p^2, \ldots, p^k$ quindi se un numero x non è coprimo con n deve essere un multiplo di p.
- I multipli di p sono: $p, 2p, 3p, \ldots, p^{k-1}p$ e sono ovviamente p^{k-1}
- Quindi, i numeri coprimi con $n = p^k$ sono $\phi(n) = \phi(p^k) = n - p^{k-1} = p^k - p^{k-1}$

Esempi:

- $\phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$ e precisamente $1, 3, 5, 7$
- $\phi(3^3) = 3^3 - 3^2 = 27 - 9 = 18$ e precisamente $1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26$
- $\phi(5^3) = 5^3 - 5^2 = 125 - 25 = 100$

Formula generale

Formula di Eulero: Caso 3

Analizziamo il caso n prodotto di due numero primi distinti, ovvero $n = p_1 \cdot p_2$ con p_1, p_2 entrambi primi

- Tra gli interi $1, 2, 3, \ldots p_1 \cdot p_2 = n$ ci sono p_2 multipli di p_1, ossia $p_1, 2p_1, 3p_1, \ldots, p_2 \cdot p_1$ e, analogamente p_1 multipli di p_2.
- Tolti i multipli di p_1 e di p_2 tutti gli altri interi sono ovviamente coprimi con n
- Il totale dei multipli di p_1 e p_2 è $p_1 + p_2 - 1$ (non vogliamo contare $p_1 \cdot p_2$ due volte)
- Quindi

$$\phi(n) = n - p_1 - p_2 + 1 = p_1 p_2 - p_1 - p_2 + 1 = (p_1 - 1) \cdot (p_2 - 1)$$

Esempi:

- $\phi(2 \cdot 3) = 1 \cdot 2 = 2$ e precisamente $1, 5$
- $\phi(3 \cdot 5) = 2 \cdot 4 = 8$ e precisamente $1, 2, 4, 7, 8, 11, 13, 14$

Formula generale

Formula di Eulero: Numeri coprimi

Il caso 3 può essere generalizzato, come nel seguente teorema (che non dimostriamo)

Teorema

Sia $n = h \cdot k$ dove h e k sono interi maggiori di zero e coprimi tra di loro. Allora $\phi(n) = \phi(h) \cdot \phi(k)$

Esempi:

- $\phi(4 \cdot 9) = \phi(2^2) \cdot \phi(3^2) = 2 \cdot 6 = 12$ e precisamente $1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35$
- $\phi(5 \cdot 8) = \phi(5) \cdot \phi(2^3) = 4 \cdot (8 - 4) = 16$ e precisamente $1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39$

Formula generale: Teorema

Utilizzando il Teorema di Fattorizzazione degli Interi possiamo ricavare la formula generale per il calcolo della funzione ϕ di Eulero.

Teorema

Sia $n > 1$, consideriamo la sua fattorizzazione $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$ Allora

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdot (p_2^{k_2} - p_2^{k_2-1}) \cdot \ldots \cdot (p_m^{k_m} - p_m^{k_m-1})$$

Dimostrazione:

Dimostriamo il teorema per induzione sul numero dei fattori primi presenti nella fattorizzazione di n.

Caso Base: se $m = 1$ allora $n = p_1^{k_1}$ ed il teorema è vero per il Caso 2 visto precedentemente.

$\triangle$

Formula generale: Teorema

Dimostrazione cont.

Passo induttivo: Supponiamo il teorema sia vero per ogni intero n' la cui fattorizzazione presenta al più $m-1$ numeri primi diversi. Se denotiamo con $n' = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_{m-1}^{k_m-1}$ abbiamo

$$n = n' \cdot p_m^{k_m}.$$

Per l'ipotesi induttiva, abbiamo che

$$\phi(n') = (p_1^{k_1} - p_1^{k_1-1}) \cdot (p_2^{k_2} - p_2^{k_2-1}) \cdot \ldots \cdot (p_{m-1}^{k_{m-1}} - p_{m-1}^{k_{m-1}-1})$$

ed inoltre, per il caso 2 abbiamo che $\phi(p_m^{k_m}) = p_m^{k_m} - p_m^{k_m-1}$. Dal momento che n' e $p_m^{k_m}$ sono coprimi, per il teorema su enunciato, che generalizza il Caso 3, abbiamo

$$\begin{aligned} \phi(n) &= \phi(n') \cdot \phi(p_m^{k_m}) = \\ &= (p_1^{k_1} - p_1^{k_1-1}) \cdot (p_2^{k_2} - p_2^{k_2-1}) \cdot \ldots \cdot (p_{m-1}^{k_{m-1}} - p_{m-1}^{k_{m-1}-1}) \cdot (p_m^{k_m} - p_m^{k_m-1}) \end{aligned}$$

ed il teorema è dimostrato.
$\triangle$

Esempi:

- $\phi(42) : 42 = 2 \cdot 3 \cdot 7$ Quindi $\phi(42) = 1 \cdot 2 \cdot 6 = 12$.
- $\phi(220) : 220 = 4 \cdot 5 \cdot 11 = 2^2 \cdot 5 \cdot 11$ e quindi $\phi(220) = 2 \cdot 4 \cdot 10 = 80$.

Teorema di Eulero

Il seguente teorema, detto Teorema di Eulero, dimostra come la funzione ϕ di Eulero si possa applicare alla esponenziazione modulare.

Teorema

Siano $n, m > 0$, *se* $MCD(n, m) = 1$ *allora*

$$n^{\phi(m)} \equiv 1 (\text{mod } m)$$

Vediamo alcuni esempi.

- $n = 12, m = 5 : 12^4 \equiv 1 (\text{mod } 5)$ infatti $12^4 = 20736$ e $20736 \text{ mod } 5 = 1$.
- $n = 21, m = 20 : \phi(20) = \phi(4 \cdot 5) = \phi(4) \cdot \phi(5) = 8$ e quindi $21^8 \equiv 1 (\text{mod } 20)$ e infatti $21^8 = 37.822.859.361$ e dal momento che $37.822.859.361 = 20 \cdot 1.891.142.968 + 1$ abbiamo che $21^8 \text{ mod } 20 = 1$.

Dimostrazione del Teorema di Eulero

Per dimostrare il Teorema di Eulero procediamo per passi.

Lemma (E1)

Sia $m > 1$, e sia $C_m = \{x : 0 < x < m, MCD(x, m) = 1\}$. Allora,

(a) *per ogni $x \in C_m$ esiste $y \in C_m$ tale che $x \cdot y \equiv 1 (\mod m)$*

(b) $C_m^{-1} = \{x^{-1} \mod m : x \in C_m\} = C_m$.

Dimostrazione:

Dimostriamo il punto (a). Come conseguenza del teorema di esistenza dell'inverso modulare, tutti gli elementi di C_m che sono, per definizione, coprimi con m ammettono un inverso modulo m. Quindi per ogni $x \in C_m$ esiste y' tale che $x \cdot y' \equiv 1 (\mod m)$ ossia $(x \cdot y') \mod m = 1$. Per la proprietà P2 sul prodotto, abbiamo
$(x \cdot y') \mod m = (x \mod m) \cdot (y' \mod m) \mod m = 1$.
Inoltre, dal momento che $x < m$ abbiamo $x \mod m = x$ e quindi
$(x \cdot y') \mod m = x \cdot (y' \mod m) \mod m = (x \cdot y) \mod m = 1$ dove $y = y' \mod m$.
Per la definizione di modulo $y < m$ ed inoltre, visto che y possiede un inverso, ossia x, y è coprimo con m. Quindi, $y \in C_m$ ed il punto (a) è dimostrato.
$\triangle$

Dimostrazione del Teorema di Eulero

Dimostrazione cont.

La dimostrazione del punto (a) ci dice che per ogni elemento $x \in C_m$ il suo inverso modulo m x^{-1} appartiene anch'esse a C_m.
Quindi $C_m^{-1} \subseteq C_m$ e di conseguenza $|C_m^{-1}| \leq |C_m|$.
Dimostriamo adesso il punto (b) semplicemente dimostrando che 2 elementi diversi di C_m hanno 2 diversi inversi modulari.
Infatti, questo dimostrerebbe che la funzione che associa ad ogni $x \in C_m$ il suo inverso, è una funzione iniettiva, e di conseguenza $|C_m| \leq |C_m^{-1}|$, che ci porterebbe a concludere non solo che $|C_m| = |C_m^{-1}|$ ma anche che $C_m^{-1} = C_m$ essendo C_m^{-1} un sottoinsieme con la stessa cardinalità dell'insieme finito C_m.
Supponiamo per assurdo che esistano $x, y, z \in C_m$ tali che $x \cdot z \equiv y \cdot z \equiv 1 (\mod m)$.
Assumiamo che $x \neq y$ e, senza ledere la generalità del discorso, $x > y$.
Quindi, $x \cdot z = qm + 1$ e $y \cdot z = q'm + 1$ da cui $z(x - y) = m(q - q')$ e dal momento $z \in C_m$ abbiamo che m e z sono coprimi, allora m deve dividere $x - y$. Ma $x - y < m$ e quindi m non può essere un divisore di $x - y$. Abbiamo trovato una contraddizione e quindi non esistono $x, y, z \in C_m$ tali che $x \cdot z \equiv y \cdot z \equiv 1 (\mod m)$.
$\triangle$

Lemma E1: esempi

Vediamo degli esempi

- Per $m = 5$ abbiamo $C_5 = \{1, 2, 3, 4\}$ e $1^{-1} \bmod 5 = 1$, $2^{-1} \bmod 5 = 3$, $3^{-1} \bmod 5 = 2$, $4^{-1} \bmod 5 = 4$.

  Quindi, $C_5^{-1} = \{1, 3, 2, 4\}$.
- Per $m = 10$ abbiamo $C_{10} = \{1, 3, 7, 9\}$ e $1^{-1} \bmod 10 = 1$, $3^{-1} \bmod 10 = 7$, $7^{-1} \bmod 10 = 3$, e $9^{-1} \bmod 10 = 9$.

  Quindi, $C_{10}^{-1} = \{1, 7, 3, 9\}$
- Per $m = 12$ abbiamo $C_{12} = \{1, 5, 7, 11\}$ e $1^{-1} \bmod 12 = 1$, $5^{-1} \bmod 12 = 5$, $7^{-1} \bmod 12 = 7$, e $11^{-1} \bmod 12 = 11$.

  Quindi, $C_{12}^{-1} = \{1, 5, 7, 11\}$.

Dimostrazione del Teorema di Eulero

Dimostriamo adesso il seguente

Lemma (E2)

Siano $n, m > 1$, tale che $MCD(n, m) = 1$. Sia $C_{n,m} = \{(n \cdot x) \bmod m : x \in C_m\}$. Allora,

$$C_{n,m} = C_m$$

Dimostrazione:

Dimostriamo prima che $C_{n,m} \subseteq C_m$ e poi che $C_m \subseteq C_{n,m}$.

- Sia $k \in C_{n,m}$, allora esiste $x \in C_m$ tale che $k = (n \cdot x) \bmod m$, con $0 \leq k < m$. Se fosse $k = 0$ esisterebbe q tale che $n \cdot x = qm$, cioè m dividerebbe n oppure x, ma ciò non è possibile dal momento che $MCD(n, m) = 1$ e $MCD(x, m) = 1$. Quindi, $k > 0$ e dall'ipotesi $MCD(n, m) = 1$ esiste l'inverso di n modulo m (n^{-1}) e per il Lemma E1 esiste anche l'inverso di x modulo m (x^{-1}). Quindi, esiste l'inverso di $n \cdot x$ modulo m che è $n^{-1} \cdot x^{-1}$. Ne segue che $(n \cdot x) \bmod m$ è coprimo con m e di conseguenza, visto che $(n \cdot x) \bmod m < m$, appartiene a C_m.
- Dimostriamo adesso che $C_m \subseteq C_{n,m}$. Sia $x \in C_m$, l'intero $n^{-1}x \bmod m$ ha un inverso modulo m che è $n \cdot x^{-1}$ e quindi è coprimo con m e, essendo minore di m appartiene a C_m. Quindi, $x = n \cdot n^{-1}x \bmod m \in C_{n,m}$.

△

Lemma E2: esempi

Vediamo degli esempi

- Per $m = 5$ e $n = 13$ abbiamo che $MCD(13, 5) = 1$, inoltre $C_5 = \{1, 2, 3, 4\}$ e $C_{13,5} = \{1 \cdot 13 \bmod 5, 2 \cdot 13 \bmod 5, 3 \cdot 13 \bmod 5, 4 \cdot 13 \bmod 5\}$. Abbiamo
  - $1 \cdot 13 \bmod 5 = 13 \bmod 5 = 3$; $2 \cdot 13 \bmod 5 = 26 \bmod 5 = 1$;
  - $3 \cdot 13 \bmod 5 = 39 \bmod 5 = 4$; $4 \cdot 13 \bmod 5 = 52 \bmod 5 = 2$.

  Quindi, $C_{13,5} = \{3, 1, 4, 2\} = C_5$.
- Per $m = 10$ e $n = 13$ abbiamo $C_{10} = \{1, 3, 7, 9\}$ e $C_{13,10} = \{1 \cdot 13 \bmod 10, 3 \cdot 13 \bmod 10, 7 \cdot 13 \bmod 10, 9 \cdot 13 \bmod 10\}$. Abbiamo
  - $1 \cdot 13 \bmod 10 = 13 \bmod 10 = 3$; $3 \cdot 13 \bmod 10 = 39 \bmod 10 = 9$;
  - $7 \cdot 13 \bmod 10 = 91 \bmod 10 = 1$; $9 \cdot 13 \bmod 10 = 117 \bmod 10 = 7$.

  Quindi, $C_{13,10} = \{3, 9, 1, 7\} = C_{10}$.
- Per $m = 12$ e $n = 13$ abbiamo $C_{12} = \{1, 5, 7, 11\}$ e $C_{13,12} = \{1 \cdot 13 \bmod 12, 5 \cdot 13 \bmod 12, 7 \cdot 13 \bmod 12, 11 \cdot 13 \bmod 12\}$. Abbiamo
  - $1 \cdot 13 \bmod 12 = 13 \bmod 12 = 1$; $5 \cdot 13 \bmod 12 = 65 \bmod 12 = 5$;
  - $7 \cdot 13 \bmod 12 = 91 \bmod 12 = 7$; $9 \cdot 13 \bmod 12 = 117 \bmod 12 = 9$.

  Quindi, $C_{13,12} = \{1, 5, 7, 9\} = C_{12}$.

Dimostrazione del Teorema di Eulero

Possiamo adesso dimostrare il Teorema di Eulero.
Siano $n, m > 1$, tale che $MCD(n, m) = 1$. Vogliamo dimostrare che $n^{\phi(m)} \equiv 1 (\mathrm{mod}\ m)$.
Dalla definizione di $\phi(m)$ abbiamo che $|C_m| = \phi(m)$.
Inoltre, per il Lemma E1 sappiamo che $C_m^{-1} = \{x^{-1} \bmod m : x \in C_m\} = C_m$ e quindi abbiamo

$$\prod_{x \in C_m} x = \prod_{y \in C_m^{-1}} y$$

da cui otteniamo

$$\prod_{x \in C_m} x \cdot \prod_{x \in C_m} x = \prod_{x \in C_m} x \cdot \prod_{y \in C_m^{-1}} y \equiv 1 \ (\mathrm{mod}\ m)$$

visto che possiamo riscrivere il prodotto come segue

$$\prod_{x \in C_m} x \cdot \prod_{y \in C_m^{-1}} y = \prod_{x \in C_m} x \cdot x^{-1} \bmod m.$$

Dimostrazione del Teorema di Eulero, cont.

Per il Lemma E2 sappiamo che $C_{n,m} = \{(n \cdot x) \bmod m : x \in C_m\} = C_m$. Quindi,

$$\prod_{x \in C_m} x = \prod_{z \in C_{n,m}} z = \prod_{x \in C_m} (n \cdot x) \bmod m$$

Per la proprietà P2 abbiamo che

$$\left(\prod_{x \in C_m} (n \cdot x) \bmod m \right) \bmod m = \left(\prod_{x \in C_m} n \cdot x \right) \bmod m = \left(n^{\phi(m)} \prod_{x \in C_m} x \right) \bmod m$$

Quindi

$$\left(\prod_{x \in C_m} x \right) \bmod m = \left(n^{\phi(m)} \prod_{x \in C_m} x \right) \bmod m$$

Ossia, abbiamo la seguente congruenza

$$n^{\phi(m)} \cdot \prod_{x \in C_m} x \equiv \prod_{x \in C_m} x \pmod{m}$$

Dimostrazione del Teorema di Eulero, cont.

Moltiplicando entrambi i membri della congruenza per lo stesso valore $\prod_{x \in C_m} x$ la congruenza si mantiene

$$n^{\phi(m)} \cdot \prod_{x \in C_m} x \cdot \prod_{x \in C_m} x \equiv \prod_{x \in C_m} x \cdot \prod_{x \in C_m} x \pmod{m}$$

Ma, come abbiamo visto, $\prod_{x \in C_m} x \cdot \prod_{x \in C_m} x \equiv 1 \pmod{m}$ e quindi

$$n^{\phi(m)} \cdot \prod_{x \in C_m} x \cdot \prod_{x \in C_m} x \equiv n^{\phi(m)} \cdot 1 \equiv \prod_{x \in C_m} x \cdot \prod_{x \in C_m} x \equiv 1 \pmod{m}$$

Ossia,

$$n^{\phi(m)} \equiv 1 \pmod{m}.$$

Il piccolo teorema di Fermat

Una delle conseguenze del Teorema di Eulero viene comunemente conosciuta come il "piccolo Teorema di Fermat."

Pierre de Fermat fu uno dei più importanti matematici della prima metà del XVII. E' universalmente conosciuto per un teorema in teoria dei numeri, che pensò di avere dimostrato (ma molto probabilmente si sbagliava) e che fu dimostrato più di 300 anni dopo nel 1994 da un matematico inglese, Andrew Wiles nel 1994.

Quel teorema, conosciuto come "Ultimo Teorema di Fermat" afferma che non esistono soluzione intere positive all'equazione

$$a^n + b^n = c^n$$

per $n > 2$, in altre parole che il Teorema di Pitagora si fermava ai quadrati e non si estendeva ai cubi, etc. Come vedremo in seguito, attraverso la corrispondenza con Blaise Pascal, un altro grande matematico francese, Fermat fu anche uno dei fondatori della teoria della probabilità.

Il piccolo teorema di Fermat

Il cosiddetto "Piccolo Teorema di Fermat", che è una diretta conseguenza del teorema di Eulero, è il seguente:

Teorema

Se p è primo e $MCD(a, p) = 1$, ovvero a non è un multiplo di p, allora $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

Esempi:

- $p = 3, a = 10 : 10^2 \bmod 3 = 100 \bmod 3 = 1$ e quindi $10^2 \equiv 1 (\mathrm{mod} 3)$.
- $p = 5, a = 12 : 12^4 \bmod 5 = 20736 \bmod 5 = 1$ e quindi $12^4 \equiv 1 (\mathrm{mod} 5)$.
- $p = 17, a = 40 : 40^{16} \bmod 17 = 1$ e quindi $40^{16} \equiv 1 (\mathrm{mod} 17)$.

Altra conseguenza del Teorema di Eulero

Ecco un altra conseguenza del teorema di Eulero

Teorema

Se $MCD(a, n) = 1$*, allora per ogni* $x > 0$

$$a^x \equiv a^{x \bmod \phi(n)} (\bmod\ n)$$

Dimostrazione:

Se calcoliamo la divisione intera $x/\phi(n)$ otteniamo quoziente q e resto $r = x \bmod \phi(n)$ e quindi $x = q \cdot \phi(n) + x \bmod \phi(n)$. Allora,

$$a^x = a^{q \cdot \phi(n) + x \bmod \phi(n)} = (a^{\phi(n)})^q \cdot a^{x \bmod \phi(n)}$$

Ma $MCD(a, n) = 1$ e quindi per il teorema di Eulero $a^{\phi(n)} \equiv 1 (\bmod\ n)$ da cui otteniamo

$$(a^{\phi(n)})^q \cdot a^{x \bmod \phi(n)} \equiv (1)^q \cdot a^{x \bmod \phi(n)} (\bmod\ n) \equiv a^{x \bmod \phi(n)} (\bmod\ n)$$

$\triangle$

Esempi

Vediamo alcuni esempi.

- Supponiamo di voler calcolare $12^{50} (\text{mod } 5)$. Dal momento che $MCD(12, 5) = 1$ allora abbiamo che

$$12^{50} \equiv 12^{50 \text{ mod } \phi(5)} (\text{mod } 5) \equiv 12^{50 \text{ mod } 4} (\text{mod } 5) \equiv 12^2 (\text{mod } 5) \equiv 4 (\text{mod } 5)$$

  quindi $12^{50} (\text{mod } 5) = 4$.

- Calcoliamo adesso $3^{100} \cdot 7^{200} \text{ mod } 10$. Abbiamo $10 = 2 \cdot 5$ e quindi $\phi(10) = 1 \cdot 4 = 4$. Quindi

$$3^{100} \cdot 7^{200} \text{ mod } 10 = (3^{100} \text{ mod } 10) \cdot (7^{200} \text{ mod } 10) \text{ mod } 10$$

  Visto che 3 e 10 sono coprimi abbiamo $3^{100} \equiv 3^{100 \text{ mod } \phi(10)} (\text{mod } 10) \equiv 3^{100 \text{ mod } 4} (\text{mod } 10)$ quindi,

$$3^{100} \equiv 3^0 (\text{mod } 10) \equiv 1 (\text{mod } 10)$$

  ed inoltre, visto che 7 e 10 sono coprimi abbiamo $7^{200} \equiv 7^{200 \text{ mod } \phi(10)} (\text{mod } 10) \equiv 7^{200 \text{ mod } 4} (\text{mod } 10)$ quindi

$$7^{200} \equiv 7^0 (\text{mod } 10) \equiv 1 (\text{mod } 10)$$

  Quindi, $3^{100} \cdot 7^{200} \text{ mod } 10 = 1 \cdot 1 = 1$.

Calcolo dell'inverso modulare

- Abbiamo visto che se n ed m sono coprimi, allora esiste l'inverso di n modulo m ossia esiste k tale che $n \cdot k \equiv 1 \pmod{m}$
- Per calcolare l'inverso modulare possiamo usare il teorema di Eulero che ci dice che se n ed m sono coprimi allora $n^{\phi(m)} \equiv 1 \pmod{m}$ e quindi $n \cdot n^{\phi(m)-1} \equiv 1 \pmod{m}$ ossia $n^{\phi(m)-1}$ è l'inverso di n modulo m.
- Notiamo anche che
  - possiamo normalizzare l'inverso, ovvero trovare un inverso compreso tra 0 e $m-1$ calcolando $n^{\phi(m)-1} \bmod m$
  - k è l'inverso di n modulo m, se e solo se k è ovviamente anche l'inverso di $n \bmod m$.
- Quindi se n ed m sono coprimi, l'inverso di n modulo m è

$$(n \bmod m)^{\phi(m)-1} \bmod m$$

Esempi sul calcolo dell'inverso modulare

- Troviamo l'inverso di 11 modulo 7. Dal momento che 7 e 11 sono coprimi, l'inverso esiste. 7 è primo, quindi $\phi(7) = 6$. Inoltre, $11 \mod 7 = 4$. Calcoliamo

$$\begin{aligned} 4^5 \bmod 7 &\equiv (4^2)^2 \cdot 4 \equiv (16 \bmod 7)^2 \cdot 4 (\bmod 7) \\ &\equiv 2^2 \cdot 4 (\bmod 7) \equiv 16 \bmod 7 \equiv 2 \end{aligned}$$

  Quindi, l'inverso di 11 modulo 7 è 2 ed infatti

$$2 \cdot 11 = 22 \equiv 1 (\bmod 7)$$

- Troviamo l'inverso di 30 modulo 11. Dal momento che 30 e 11 sono coprimi, l'inverso esiste. 11 è primo, quindi $\phi(11) = 10$. Inoltre, $30 \mod 11 = 8$. Calcoliamo

$$\begin{aligned} 8^9 \bmod 11 &\equiv (8^2)^4 \cdot 8 \equiv (64 \bmod 11)^4 \cdot 8 (\bmod 11) \\ &\equiv 9^4 \cdot 8 \equiv (9^2)^2 \cdot 8 \equiv (81 \mod 11)^2 \cdot 8 (\bmod 11) \\ &\equiv 16 \cdot 8 \equiv (16 \bmod 11) \cdot 8 \equiv 40 \bmod 11 = 7 \end{aligned}$$

  Quindi, l'inverso di 30 modulo 11 è 7 ed infatti

$$7 \cdot 30 = 210 \equiv 1 (\bmod 11)$$

  poiché $210 = 19 \cdot 11 + 1$.

Esempi sul calcolo dell'inverso modulare

- Troviamo l'inverso di 45 modulo 16. Dal momento che $45 = 3^2 \cdot 5$ e $16 = 2^4$ sono coprimi, l'inverso esiste. Come sappiamo $\phi(16) = 2^4 - 2^3 = 8$. Inoltre, $45 \mod 16 = 13$. Calcoliamo

$$\begin{aligned} 13^7 \mod 16 &\equiv (13^2)^3 \cdot 13 \equiv (169 \mod 16)^3 \cdot 13 (\mod 16) \\ &\equiv 9^3 \cdot 13 (\mod 16) \equiv (81 \mod 16) \cdot 9 \cdot 13 (\mod 16) \\ &\equiv 1 \cdot 9 \cdot 13 (\mod 16) = 117 \mod 16 = 5 \end{aligned}$$

  poiché $117 = 7 \cdot 16 + 5$. Quindi, l'inverso di 45 modulo 16 è 5 ed infatti

$$45 \cdot 5 = 225 = 14 \cdot 16 + 1$$

- Troviamo l'inverso di 70 modulo 9. Dal momento che $70 = 2 \cdot 5 \cdot 7$ e $9 = 3^2$ sono coprimi, l'inverso esiste. Inoltre, $\phi(9) = \phi(3^2) = 3^2 - 3 = 6$. Infine, $70 \mod 9 = 7$. Calcoliamo

$$\begin{aligned} 7^5 \mod 9 &\equiv (7^2)^2 \cdot 7 \equiv (49 \mod 9)^2 \cdot 7 (\mod 9) \\ &\equiv 4^2 \cdot 7 (\mod 9) \equiv (16 \mod 9) \cdot 7 (\mod 9) \equiv 49 \mod 9 = 4 \end{aligned}$$

  Quindi, l'inverso di 70 modulo 9 è 4 ed infatti

$$4 \cdot 70 = 280 \equiv 1 (\mod 9)$$

  poiché $280 = 31 \cdot 9 + 1$.

Esercizi

Trovare i seguenti inversi modulari

- Inverso di 49 modulo 23
- Inverso di 51 modulo 16
- Inverso di 63 modulo 10
- Inverso di 72 modulo 5
- Inverso di 83 modulo 10
- Inverso di 97 modulo 11
- Inverso di 100 modulo 23

Esercizi

Calcolare i seguenti (giustificare i risultati proposti)

- $9^{100} \bmod 8 \rightarrow$ **Risultato:** 1
- $15^{80} \bmod 16 \rightarrow$ **Risultato:** 1
- $13^{40} \bmod 19 \rightarrow$ **Risultato:** 4
- $11^{57} \bmod 23 \rightarrow$ **Risultato:** 17
- $7^{50} \bmod 11 \rightarrow$ **Risultato:** 1
- $40^{60} \cdot 60^{40} \bmod 31 \rightarrow$ **Risultato:** 1
- $29^{101} \bmod 31 \rightarrow$ **Risultato:** 29

Applicazioni dell'Aritmetica modulare

Sono tante le applicazioni dell'aritmetica modulare sia nel campo matematico ma anche, e soprattutto, nel campo informatico, con particolare riferimento sia alla gestione dei dati che alla sicurezza. Ne presenteremo alcune nel seguito:

- La prova del 9
- Codici ISBN e carte di credito
- Cifrari a trasposizione
- Hashing

La prova del 9

La prova del nove è una verifica di correttezza del risultato di una operazione aritmetica tra numeri interi, attraverso il raffronto delle radici numeriche degli operandi e del risultato. Tale tecnica ci consente di verificare, però, solo se abbiamo sbagliato i conti. Chiariamo meglio. Ricordando la definizione di radice numerica, vale il seguente teorema che non dimostriamo

Teorema

Dati $n, m \in \mathbb{N}$, *abbiamo che*

- $\rho(n \cdot m) = \rho(\rho(n) \cdot \rho(m))$
- $\rho(n + m) = \rho(\rho(n) + \rho(m))$

Esempi:

- $123 \cdot 347 = 42671$ Giusto? Vediamo, $\rho(123) = 6$ e $\rho(347) = 5$ quindi $\rho(\rho(123) \cdot \rho(347)) = \rho(30) = 3$, mentre $\rho(42671) = \rho(20) = 2$. Quindi calcolo sbagliato. E in effetti, $123 \cdot 347 = 42681$ e $\rho(42681) = 3$.
- $123 + 347 = 472$ Giusto? Vediamo, $\rho(123) = 6$ e $\rho(347) = 5$ quindi $\rho(\rho(123) + \rho(347)) = \rho(11) = 2$, mentre $\rho(472) = \rho(13) = 4$. Quindi calcolo sbagliato. E in effetti, $123 + 347 = 470$ e $\rho(470) = \rho(11) = 2$.

Perché si chiama prova del 9? Perché la radice numerica si ottiene eliminando i 9 dalle somme. Per esempio $3 + 4 + 7 = 14$ e se sottraiamo 9 o sommiamo le cifre otteniamo lo stesso risultato 5.

La prova del 9

Il problema della prova del nove è che ci dice con esattezza se un calcolo è sbagliato ma non ci garantisce che sia corretto.
Esempi:

- Come abbiamo visto $123 \cdot 347 = 42681$. Ma che succede se sbagliamo i conti e scriviamo $123 \cdot 347 = 42771$? Vediamo, $\rho(123) = 6$ e $\rho(347) = 5$ quindi $\rho(\rho(123) \cdot \rho(347)) = \rho(30) = 3$, ma anche $\rho(42771) = \rho(21) = 3$. Quindi calcolo sbagliato, la prova del 9 ci dice però giusto.
- Quindi è affidabile solo quando ci dice che abbiamo sbagliato. Ovvero vale la seguente regola
- *Se i due numeri sono diversi allora il risultato è errato. Se i due numeri sono uguali allora il risultato può essere corretto*

La prova del 9 si basa sull'aritmetica modulare ed il calcolo modulo 9 perché vale il seguente

Teorema

Dato $n \in \mathbb{N}$, *abbiamo che*

$$n \equiv \rho(n) (\mathrm{mod}\ 9)$$

Quindi, il teorema ci dice che ogni numero è congruente alla somma delle sue cifre, e quindi alla sua radice numerica, modulo 9. In virtù di tale teorema, e delle regole di invarianza della congruenza rispetto alla somma ed al prodotto, abbiamo la regola del 9.

La prova del 9

Dimostrazione:
Per il Teorema di divisibilità del 9 sappiamo che dato $n \in \mathbb{N}$, se m è la somma delle sue cifre allora $n - m$ è divisibile per 9, ossia esiste un k tale che $n - m = 9k$. Quindi, ottengo che $n \equiv m (\mod 9)$.
Reiterando, se m' è la somma delle cifre di m otteniamo
$m \equiv m' (\mod 9)$ ossia

$$n \equiv m (\mod 9) \equiv m' (\mod 9)$$

Fermiamo il processo di somma delle cifre quando otteniamo un numero con una sola cifra, la radice numerica, ed otteniamo

$$n \equiv \rho(n) (\mod 9)$$

$\triangle$

La prova del 9

Osserviamo allora che se consideriamo la successione delle radici numeriche, abbiamo i seguenti valori

n	$\rho(n)$	n	$\rho(n)$	n	$\rho(n)$
1	1	10	1	19	1
2	2	11	2	20	2
3	3	12	3	21	3
4	4	13	4	22	4
5	5	14	5	23	5
6	6	15	6	24	6
7	7	16	7	25	7
8	8	17	8	26	8
9	9	18	9	27	9

Quindi per le radici numeriche abbiamo sequenze $1, 2, \ldots 9$, che si ripetono e per ogni n possiamo notare che $\rho(n) = 9$ solo sui multipli di 9.

Codice ISBN

Il codice ISBN (dall'inglese International Standard Book Number,) è un codice identificativo internazionale standard per i libri. Oggi, è una sequenza numerica di 13 cifre, mentre prima del 2007 era costituita da 10 cifre, dove l'ultimo carattere poteva anche essere la lettera maiuscola X. I primi caratteri del codice identificano varie cose tra cui la casa editrice, etc. L'ultimo carattere è un carattere di controllo che verifica la correttezza formale del codice. Vediamo come funziona.

ISBN-10 Se le cifre sono $a_{10}, a_9, \ldots, a_1$ (qui, il carattere "X" sta a denotare il numero 10) il codice è formalmente corretto se

$$a_1 + 2a_2 + 3a_3 + \ldots + 9a_9 + 10a_{10} \equiv 0 (\mathrm{mod} 11)$$

Allora, per esempio

- Il codice 2468864212 è corretto? Abbiamo

  $$10 \cdot 2 + 9 \cdot 4 + 8 \cdot 6 + 7 \cdot 8 + 6 \cdot 8 + 5 \cdot 6 + 4 \cdot 4 + 3 \cdot 2 + 2 \cdot 1 + 2 = 264$$

  il numero è divisibile per 11 quindi è un codice ISBN-10 corretto.
- Il codice 2468864211 non è invece un codice ISBN-10 corretto.

Codice ISBN

ISBN-13 Se le cifre sono $a_1, a_2, \ldots, a_{13}$ il codice è formalmente corretto se

$$a_1 + 3a_2 + a_3 + 3a_4 \ldots + a_9 + 3a_{10} + a_{11} + 3a_{12} + a_{13} \equiv 0 (\mathrm{mod}\, 10)$$

Allora, per esempio

- Il codice 2468864211129 è corretto? Abbiamo $2 + 12 + 6 + 24 + 8 + 18 + 4 + 6 + 1 + 3 + 1 + 6 + 9 = 100$ ed è un codice ISBN-13 corretto.
- Il codice 2468864211128 corrisponde al numero 99 e quindi non è corretto.

Codice Carta di Credito

Anche il codice numerico a 16 cifre delle carte di credito si basa sull'aritmetica modulare. Per verificarne la correttezza "aritmetica" ci si basa sulla formula di Luhn, che è la seguente

- Assumiamo che le 16 cifre siano le seguenti (a gruppi di 4): $a_1 b_1 a_2 b_2$, $a_3 b_3 a_4 b_4$, $a_5 b_5 a_6 b_6$, $a_7 b_7 a_8 b_8$.
- Si moltiplicano le cifre $a_1, a_2, \ldots, a_7, a_8$ per 2 ottenendo quindi $2a_1, 2a_2, \ldots, 2a_7, 2a_8$. Se qualcuno di questi 8 numeri dovesse essere maggiore di 9 (e quindi a 2 cifre) lo si sostituisce con la somma delle sue cifre. In altre parole, consideriamo le 8 cifre della radice numerica: $\rho(2a_1), \rho(2a_2), \ldots, \rho(2a_7), \rho(2a_8)$.
- Si calcola la somma (formula di Luhn)

$$S = \sum_{i=1}^{8} \rho(2a_i) + \sum_{i=1}^{8} b_i$$

- Il codice numerico della carta di credito è formalmente corretto se

$$S \equiv 0 (\mathrm{mod}\ 10)$$

ossia se il numero ottenuto con la formula di Luhn è un multiplo di 10.

Codice Carta di Credito

Esempi: verifichiamo i seguenti codici

- 1234-5678-8765-4321
  - Le cifre di posto dispari, quelle che abbiamo denotato con a_i sono allora $1, 3, 5, 7, 8, 6, 4, 2$ moltiplicando per 2 e sommando le cifre dei risultati a più di una cifra otteniamo i numeri: $2, 6, 1, 5, 7, 3, 8, 4$ la cui somma è 36
  - Le cifre di posto pari, quelle che abbiamo denotato con b_i sono allora $2, 4, 6, 8, 7, 5, 3, 1$ e la somma da come risultato di nuovo 36. Quindi, non è un numero di carta di credito corretto, visto che il risultato finale $36 + 36 = 72$ non è un multiplo di 10.
- 1111-1212-1212-1212
  - Le 8 cifre di posto dispari, quelle che abbiamo denotato con a_i sono tutte uguali ad 1 e ci danno la somma 16.
  - Le 8 cifre di posto pari, quelle che abbiamo denotato con b_i sono $1, 1, 2, 2, 2, 2, 2, 2$ e la somma da come risultato 14. Quindi, la sequenza è un numero di carta di credito corretto, visto che il risultato finale $16 + 14 = 30$ è un multiplo di 10.

Il cifrario di Cesare

- Una delle maggiori applicazioni dell'aritmetica modulare (e della Teoria dei Numeri in generale) è nel campo della Crittografia.
- La complessità degli algoritmi crittografici esula dagli obiettivi di questo Corso
- Ma come esempio, vediamo qui una tecnica di crittografia che utilizzava Giulio Cesare per comunicare con i suoi generali.
- Con l'alfabeto moderno di 26 lettere, il Cifrario di Cesare, funzionerebbe così
- Si ignorano gli spazi tra parole, ed ogni lettera dell'alfabeto presente nel messaggio, si sposta di 3 posizioni in avanti, come vedete nella tabella sotto

a	b	c	d	e	f	g	h	i	j	k	l	m
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
d	e	f	g	h	i	j	k	l	m	n	o	p

n	o	p	q	r	s	t	u	v	w	x	y	z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
q	r	s	t	u	v	w	x	y	z	a	b	c

- Quindi, per esempio, il messaggio "ce la faremo" diventa : "fhldiduhpr"
- Per decifrare il messaggio si fa il processo inverso.

ROT-13

- Il cifrario di Cesare è un esempio di cifrario a sostituzione monoalfabetica, ossia un sistema crittografico che utilizza un alfabeto per il testo in chiaro e una permutazione dello stesso per il testo cifrato.
- Un altro esempio di cifrario a sostituzione monoalfabetica, è ROT-13, un sistema semplice usato sul web per offuscare parole o frasi, abbastanza diffuso nei newsgroup.
- ROT-13 è una semplice variate del Cifrario di Cesare dove invece di spostare le lettere di 3 posizioni, le si sposta di 13 posizioni, ed in questo modo cifratura e decifratura si possano fare allo stesso modo.
- Ecco la tabella del ROT-13

a	b	c	d	e	f	g	h	i	j	k	l	m
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
n	o	p	q	r	s	t	u	v	w	x	y	z

n	o	p	q	r	s	t	u	v	w	x	y	z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
a	b	c	d	e	f	g	h	i	j	k	l	m

Implementazione cifrari a trasposizione

- Vediamo adesso come implementare un cifrario a trasposizione, tipo il Cifrario di Cesare o ROT-13.
- Si associa ad ogni lettera dell'alfabeto $\{a, b, c, \ldots, z\}$ il numero corrispondente all'ordine alfabetico, ma partendo da zero.
- Quindi, ad a associamo 0, a b associamo 1 e così via sino a z alla quale associamo il numero 25.
- Si decide quale chiave utilizzare, ovvero nello specifico un numero intero $0 < k < 26$. In pratica, questo numero è la chiave segreta che serva per criptare e decriptare il messaggio.
- Dato un messaggio $\mathcal{M}$ da criptare, lo riscriviamo come sequenza dei numeri associati alle lettere
- Sia allora il messaggio il $\mathcal{M} = m_1 m_2 \cdots m_s$, da cifrare.
- Applichiamo ad ogni lettera la funzione

$$f(m_i) = m_i + k \mod 26.$$

- Quindi il messaggio cifrato è

$$f(\mathcal{M}) = f(m_1)f(m_2)\cdots f(m_s)$$

- Per decifrare il messaggio si usa la funzione

$$g(m_i) = m_i - k \mod 26.$$

Gestione dei dati e la tecnica Hashing

- Immaginate il problema di avere una struttura dati per gestire le automobili in circolazione in Italia.
- Ogni automobile è univocamente identificata dal suo numero di targa (2 lettere, 3 cifre, 2 lettere).
- In questo modo, il numero totale di targhe possibili è più di 456 milioni (impareremo presto a calcolarlo).
- Il parco auto in Italia, però, è di circa 50 milioni. Dobbiamo quindi utilizzare una struttura ben più grande, sprecando un'enorme quantità di spazio?
- Risposta no. Se n sono le auto, possiamo utilizzare una struttura dati con n ingressi, ed associare ad ogni auto, identificata dal numero di targa convertito in intero a, il numero $h(a) = a \bmod n$.
- Una funzione di questo tipo è detta funzione di "hashing".
- In altri corsi ne vedrete i dettagli, e scoprirete cosa fare in caso di "collisioni", ossia 2 numeri che hanno lo stesso valore di hashing.

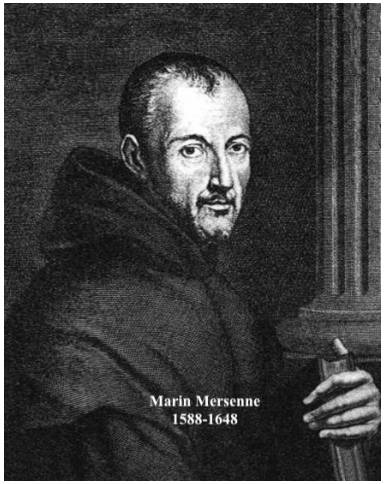
Teoria dei numeri

- Molti sono i problemi della teoria dei numeri, che è quel ramo della matematica pura che si occupa delle proprietà dei numeri interi, che possono essere facilmente compresi e che sono ancora aperti (persino da secoli ormai).
- Abbiamo già visto comunque molti risultati del campo, come le proprietà della divisibilità, l'algoritmo di Euclide, la fattorizzazione di interi in numeri primi, lo studio delle congruenze. E poi ancora, il piccolo teorema di Fermat e il teorema di Eulero (che è una sua generalizzazione), e la funzione ϕ di Eulero e le sue proprietà.
- Vedremo qui alcuni dei problemi aperti più famosi, molti dei quali avranno a che vedere con proprietà e congetture riguardanti i numeri primi.

Sequenze numeriche

- Le definizioni che daremo daranno adito a sequenze numeriche e molti dei problemi aperti saranno del tipo: "questa sequenza numerica è infinita?"
- Sul web trovate un sito dedicato alle sequenze di interi: "The On-Line Encyclopedia of Integer Sequences" all'indirizzo "http://oeis.org/"
- OEIS è una collezione vastissima di sequenze numeriche, e per ogni sequenza numerica vengono descritte le proprietà e sono anche date tutte le informazioni storiche.
- Le sequenze sono tutte catalogate e ben identificate, per esempio la sequenza dei numeri primi $\mathbb{P}$ è la sequenza "A000040" che trovate all'indirizzo "http://oeis.org/A000040"
- In quanto segue, quando appropriato, citeremo anche la sequenza che si trova su OEIS.

Numeri primi di Mersenne



Marin Mersenne fu un matematico, teologo e filosofo francese che studiò e propose una lista di numeri primi speciali.

- I numeri primi di Mersenne sono numeri primi della forma

$$M_p = 2^p - 1.$$

- Esempi: i primi 5 primi di Mersenne
  - $M_2 = 2^2 - 1 = 3$
  - $M_3 = 2^3 - 1 = 7$
  - $M_5 = 2^5 - 1 = 31$
  - $M_7 = 2^7 - 1 = 127$
  - $M_{13} = 2^{13} - 1 = 8191$
- Sequenza su OEIS "A000668"
- Dagli esempi visti, sembra che l'esponente p debba necessariamente essere primo. In effetti è così.

Numeri primi di Mersenne

- Se infatti consideriamo $2^n - 1$ ed n non è primo, ossia $n = hk$ per $h, k \geq 2$ allora abbiamo (verificare i conti come esercizio)

$$2^{hk} - 1 = (2^h - 1)(1 + 2^h + 2^{2h} + 2^{3h} + \ldots 2^{h(k-1)})$$

  e quindi $2^{hk} - 1$ non è primo.
- Inoltre, $2^{11} - 1 = 2048 - 1 = 2047 = 23 \cdot 89$ non è primo. Quindi, $2^p - 1$ con p primo, non è necessariamente un numero primo.
- Ad oggi, si conoscono solo 51 numeri primi di Mersenne, il più grande dei quali scoperto poco più di un anno fa, grazie al progetto GIMPS (Great Internet Mersenne Prime Search), basato su tecniche di calcolo distribuito, è un primo con più di 24 milioni di cifre

$$M_{82589933} = 2^{82589933} - 1$$

- Ci sono risultati antichi e importanti che legano i numeri primi di Mersenne ai numeri "perfetti", ma rimane irrisolto il problema fondamentale ovvero se i primi di Mersenne sono infiniti.

Numeri perfetti: funzione "Sigma"

- Dato un numero $n \in \mathbb{N}$, definiamo la seguente funzione

$$\sigma(n) = \sum_{0<d,d|n} d$$

- Quindi la funzione "sigma" ci restituisce la somma di tutti i divisori positivi di un numero n.
- Notiamo allora che
  $\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 7, \sigma(5) = 6, \sigma(6) = 12$ etc.
- Sono tante le proprietà della funzione σ, che è stata oggetto di studio da sempre, una di queste proprietà, semplice ed immediata è che se p è primo, allora $\sigma(p) = p + 1$.

Numeri perfetti

- Un numero $n \in \mathbb{N}$ si dice perfetto se $\sigma(n) = 2n$, ovvero, visto che n è un divisore di se stesso, se il numero n è uguale alla somma di tutti i suoi divisori propri.
- Il primo numero perfetto è 6, infatti $6 = 1 + 2 + 3$ e $\sigma(6) = 1 + 2 + 3 + 6 = 12$.
- I successivi 2 sono 28 e 496.
- I primi a studiare i numeri perfetti furono i pitagorici. Pitagora si accorse di una proprietà che fu poi dimostrata da Euclide, ossia che se $2^n - 1$ è un numero primo, allora

$$2^{n-1} \cdot (2^n - 1)$$

  è perfetto.
- Successivamente, Eulero dimostrò che tutti i numeri perfetti pari devono essere di tale forma.
- Infatti, $6 = 2^1 \cdot (2^2 - 1), 28 = 2^{3-1} \cdot (2^3 - 1), 496 = 2^{5-1} \cdot (2^5 - 1)$

Numeri perfetti

- Allora i numeri perfetti pari sono strettamente legati ai primi di Mersenne.
- Infatti, ne conosciamo soltanto 51 (tanti quanti i numeri di Mersenne conosciuti).
- Sequenza su OEIS "A000396"
- Primo problema notevole che è ancora irrisolto per i numeri perfetti: "Esistono numeri perfetti dispari?"
- Così come per i numeri di Mersenne, anche per i numeri perfetti, il problema aperto più importante è se siano infiniti oppure no.

Numeri perfetti

- Ultima e curiosa considerazione: tutti i numeri perfetti pari terminano con un 6 oppure con un 8. Infatti, essendo della forma $2^{n-1}(2^n - 1)$ abbiamo che i due fattori
  - 2^{n-1} potenza di 2 termina con $2, 4, 6, 8$ perché pari. Notiamo che nessuna potenza di 2 può terminare con 0 perché altrimenti sarebbe divisibile per 10 e quindi anche 5 sarebbe un suo fattore primo.
  - Allora, $2^n - 1$ termina con $1, 3, 7$ perché non può terminare con 5 perché $2^n - 1$ è primo.
  - Notiamo che se 2^{n-1} termina con 2 allora $2^n - 1$ termina con 3; se termina con 4 allora $2^n - 1$ termina con 7; se termina con 6 allora $2^n - 1$ termina con 1; e infine se termina con 8 allora $2^n - 1$ termina con 5 e non è primo.
  - Quindi ci sono solo tre coppie possibili per le unità di 2^{n-1} e $2^n - 1$, ossia $(2, 3)$, $(4, 7)$ e $(6, 1)$ ed in tutti e 3 i casi, il loro prodotto da 6 o 8 come cifra delle unità.

Numeri primi gemelli

- Ad Euclide si deve anche la definizione di un problema che rimane ancora irrisolto e che riguarda i numeri primi gemelli.
- Due numeri primi p_1 e p_2 si dicono gemelli se la loro differenza è uguale a 2 ovvero se $|p_1 - p_2| = 2$.
- Esempi di coppie di numeri primi gemelli:
  $(3, 5), (5, 7), (11, 13), (17, 19)$ etc.
- Dati due primi gemelli $p_1 < p_2$, il numero $p_1 + 1$ è detto separatore della coppia di primi gemelli.
- Se $p_1 > 3$ abbiamo già dimostrato che il separatore di una coppia di primi gemelli è un multiplo di 6.
- La sequenza dei separatori di numeri gemelli su OEIS è "A014574"
- Così come per i numeri di Mersenne e per i numeri perfetti, il problema aperto più importante riguardo ai primi gemelli, proposto da Euclide, è se siano infiniti oppure no.

Numeri primi gemelli: generalizzazione

- I numeri primi gemelli sono coppie di numeri primi la cui differenza è 2.
- Ovviamente, la differenza di 2 numeri primi consecutivi maggiori di 2 non può essere un numero dispari, perché entrambi dispari.
- Numeri primi consecutivi che distano 4, per esempio 13 e 17 sono detti "primi cugini."
- Per ogni intero pari $2k$, allora, possiamo estendere la congettura sui numeri primi gemelli come segue
  - Per ogni intero $k \geq 1$, esistono infinite coppie di numeri primi consecutivi la cui differenza è $2k$?
- Tale congettura fu proposta nel 1849 dal matematico francese Alphonse de Polignac, e, ovviamente, ad oggi rimane non dimostrata.

La congettura di Goldbach

- La congettura di Goldbach (matematico prussiano) viene formulata nel modo in cui la conosciamo da Eulero, nel 1742, in risposta ad un quesito di Goldbach.
- La congettura afferma semplicemente che ogni numero pari maggiore di 4 può essere scritto come somma di due numeri primi.
- Esempi:
  - $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7 = 5 + 5$, $12 = 5 + 7$
  - $14 = 3 + 11 = 7 + 7$, $16 = 3 + 13 = 5 + 11$, $18 = 5 + 13 = 7 + 11$
- Ovviamente, ad oggi, la congettura non è stata dimostrata, né é stato trovato un numero pari che non si possa scrivere come somma di due numeri primi.

La congettura di Goldbach

- Dal momento che i numeri pari sono tutti i numeri $2k$ per $k \geq 1$, se $p_1 + p_2 = 2k$ allora $k = \frac{p_1+p_2}{2}$.
- Questa semplice considerazione ci permette di dare due definizioni equivalenti della congettura:

  G1 Per ogni intero $x \geq 2$, esiste un intero $d \geq 0$, tale che

  $$x - d \text{ e } x + d, \text{ sono entrambi primi.}$$

  G2 Equivalentemente, per ogni intero $x \geq 2$, esistono due numeri primi p_1 e p_2 tali che

  $$x = \frac{p_1 + p_2}{2}$$

- Notiamo che se l'intero x è primo, allora nel primo caso possiamo prendere $d = 0$ e nel secondo caso $p_1 = p_2 = x$.

La congettura di Goldbach

- I separatori dei numeri primi gemelli sono un insieme di interi per cui la congettura di Goldbach vale.
- Abbiamo però anche un insieme infinito di interi per cui la congettura è verificata: la sequenza di "Interprimi", ovvero gli interi che sono il punto di mezzo di due primi consecutivi.
- Se denotiamo con $\mathcal{P} = \{p_1, p_2, p_3, \ldots\}$ l'insieme infinito di numeri primi, la sequenza di interprimi è definita come

$$\begin{aligned} \mathcal{I} &= \{\frac{p_n + p_{n+1}}{2} : p_n, p_{n+1} \in \mathcal{P}, n \geq 2\} = \\ &= \{4, 6, 9, 12, 15, 18, 21, 26, 30, 34, \ldots\} \end{aligned}$$

- Quindi, $\mathcal{I}$ contiene tutti gli insiemi definiti dalla congettura di Polignac per ogni intero $k \geq 1$, incluso ovviamente l'insieme dei numeri primi gemelli.
- Notiamo subito che $\mathcal{I}$ non contiene interi come, per esempio, 8 e 10 perché non sono punto di mezzo di primi consecutivi.
- Quindi $\mathcal{P} \cup \mathcal{I} \subset \mathbb{N}$.
- La sequenza di interprimi su OEIS è "A024675"

La congettura di Goldbach

- Grazie alla potenza di calcolo dei computer moderni, la congettura di Goldbach è stata verificata sino ad interi pari a circa 10^{17}.
- Perché si è convinti della sua veridicità?
- Perché per il teorema sulla densità dei numeri primi, sappiamo che dato $n \in \mathbb{N}$ e la funzione $\pi(n)$ che rappresenta il numero di primi più piccoli di n, abbiamo che $\pi(n) \sim \frac{n}{\ln n}$
- Quindi, per ogni n abbiamo circa

$$\frac{1}{2}\frac{n}{\ln n} \cdot \left(\frac{n}{\ln n} + 1\right)$$

  coppie di primi più piccoli di n (appena parleremo di calcolo combinatorio capiremo perché).
- Risulta abbastanza semplice verificare che, per esempio per $n \geq 14$

$$n < \frac{n^2}{2\ln^2 n}$$

- quindi abbiamo un numero sufficiente di coppie per verificare la congettura.

La congettura di Goldbach: distanza

- La definizione della congettura nella forma equivalente G1 ci permette di associare ad ogni intero n, un intero $d(n)$ che è il minimo valore d tale che $n-d, n+d$ sono entrambi primi. Chiamiamola "distanza di Goldbach".
- Tale associazione ovviamente è possibile farla per tutti gli interi se e solo se la congettura è vera.
- In ogni caso, ai numeri primi sarà associato ovviamente il valore 0, ai separatori di primi gemelli il valore 1
- Quindi: $d(2) = 0$, $d(3) = 0$, $d(4) = 1$, $d(5) = 0$, $d(6) = 1$, $d(7) = 0$, $d(8) = 3$, $d(9) = 2$, $d(10) = 3$, etc.
- Abbiamo allora la sequenza $0, 0, 1, 0, 1, 0, 3, 2, 3, \ldots$ che su OEIS è la sequenza numero "A047160"

La congettura di Goldbach: distanza

- Se indichiamo con $\mathbb{G}_k$ la sequenza di interi che ha distanza di Goldbach uguale a k allora abbiamo
  - $\mathbb{G}_0 = \mathbb{P}$ ovvero la sequenza dei numeri primi;
  - $\mathbb{G}_1 = \{4, 6, 12, 18, 30, 42, 60, 72, 102, 108, \ldots\}$ è la sequenza dei separatori dei primi gemelli, tutti multipli di 6 tranne il 4;
  - $\mathbb{G}_2 = \{9, 15, 21, 39, 45, 69, 81, 93, 99, 105, 111, \ldots\}$ sequenza OEIS numero A072569
  - $\mathbb{G}_3 = \{8, 10, 14, 16, 20, 26, 34, 40, 44, 50, 56, 64 \ldots\}$ sequenza OEIS numero A087695
  - $\mathbb{G}_4 = \{27, 33, 57, 63, 75, 93, 135, 153, 177, 237 \ldots\}$
- Notiamo subito che dato un qualunque n vale la seguente proprietà

  (P) n e $d(n)$ sono coprimi. Infatti, se $h > 1$ fosse un divisore comune a n e $d(n)$ allora h dividerebbe sia $n - d(n)$ che $n + d(n)$ che invece abbiamo supposto essere primi.

La congettura di Goldbach: distanza

- Se le sequenze $\mathbb{G}_k$ sono una partizione di $\mathbb{N} \setminus \{0, 1\}$ allora la congettura di Godlbach è vera.
- Date le sequenze $\mathbb{G}_k$ sono molte le cose che non sappiamo (ed in realtà sappiamo molto poco). Ne citiamo 2
  - Esistono sequenze infinite? Non sappiamo, per esempio, se i primi gemelli sono infiniti, e quindi non sappiamo se in particolare $\mathbb{G}_1$ è infinita.
  - Esistono sequenze vuote? Ovvero esistono dei valori di d tali che per nessun intero n $n - d$ e $n + d$ sono entrambi primi?

La congettura di Collatz

- La congettura di Collatz, conosciuta anche come congettura $3x + 1$, fu enunciata per la prima volta nel 1937 da un matematico tedesco, Lothar Collatz.
- La congettura lega la teoria dei numeri ad un problema di terminazione di un algoritmo iterativo.
- L'algoritmo è basato sulla seguente funzione

$$f(n) = \begin{cases} 1 \text{ se } n = 1 \\ \frac{n}{2} \text{ se } n \text{ è pari} \\ 3n + 1 \text{ se } n \text{ è dispari} \end{cases}$$

La congettura di Collatz

- L'algoritmo è il seguente

Algoritmo di Collatz
Leggi un intero $x \geq 1$
while $(x > 1)$ **do**
if $x \mod 2 == 0$ $x = x/2$;
else $x = 3 * x + 1$;
end_while

- Problema irrisolto: l'algoritmo si ferma sempre oppure esiste un x partendo dal quale non si raggiunge mai il valore 1 ?

Traiettorie dei numeri

- Notiamo che per ogni n dato come input all'algoritmo, viene generata una sequenza di interi, chiamata anche traiettoria di n
- Esempi:
  - $n = 1 :\rightarrow 1$
  - $n = 2 :\rightarrow \mathbf{2}, 1$
  - $n = 3 :\rightarrow 3, 10, 5, \mathbf{16}, 8, 4, 2, 1$
  - $n = 4 :\rightarrow \mathbf{4}, 2, 1$
  - $n = 5 :\rightarrow 5, \mathbf{16}, 8, 4, 2, 1$
  - $n = 6 :\rightarrow 6, 3, 10, 5, \mathbf{16}, 8, 4, 2, 1$
  - $n = 7 :\rightarrow 7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, \mathbf{16}, 8, 4, 2, 1$
  - $n = 8 :\rightarrow \mathbf{8}, 4, 2, 1$
  - $n = 9 :\rightarrow 9, 28, 14, 7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, \mathbf{16}, 8, 4, 2, 1$
  - $n = 10 :\rightarrow 10, 5, \mathbf{16}, 8, 4, 2, 1$
- Abbiamo così una funzione $c(n)$ che associa ad ogni intero n il numero di elementi della traiettoria, e quindi abbiamo una sequenza numerica

$$0, 1, 7, 2, 5, 8, 16, 3, 19, 6, 14, 9, 9, 17, 17, 4, 12, 20, \ldots$$

che è la sequenza di OEIS numero "A006577".

Traiettorie dei numeri

- Notiamo che per alcuni interi la lunghezza della traiettoria è maggiore del numero stesso, come per esempio $3, 6, 7, 9$
- La sequenza di tali numeri è la seguente, sequenza OEIS numero "A228014"

$$3, 6, 7, 9, 11, 14, 15, 18, 19, 27, 31, 41, 47, 54, 55,$$
$$62, 63, 71, 73, 82, 83, 91, 94, 95, 97, 108, 109, 110, \ldots$$

- Per ogni traiettoria, possiamo anche verificare qual è il valore del massimo elemento raggiunto.
- Per esempio, per 3 e 5 abbiamo come valore massimo 16 mentre per 7 abbiamo come valore massimo 52.
- La seguente sequenza, OEIS numero "A025586", ci da il massimo valore delle traiettorie per ogni n

$$n = 1 - 16: \quad \rightarrow \quad 1, 2, 16, 4, 16, 16, 52, 8, 52, 16, 52, 16, 40, 52, 160, 16,$$
$$n = 17 - 32: \quad \rightarrow \quad 52, 52, 88, 20, 64, 52, 160, 24, 88, 40, 9232, 52, 88, 160, 9232, 32 \ldots$$

Traiettorie dei numeri

- Per $n = 27$ e $n = 31$ il valore massimo raggiunto è 9232 che è più grande del quadrato dei due numeri. Infatti $27^2 = 729$ e $31^2 = 961$.
- Abbiamo anche la sequenza di interi n la cui traiettoria ha come valore massimo un numero maggiore o uguale n^2, sequenza OEIS numero "A225038"

$$1, 3, 7, 27, 31, 41, 47, 54, 55, 62, 63, 71, 73, 82, 83, 91, 94, 95,$$
$$6631675, 7460635, 319804831, 379027947, 426406441, 479707247 \ldots$$

- Infine, segnaliamo la sequenza di interi n tali che il valore massimo raggiunto dalla loro traiettoria, supera tutti quelli precedenti, ossia stabilisce un nuovo record.
- Per esempio, per 3 abbiamo valore massimo 16, il record successivo è stabilito da 7 con 52 e poi 15 con 160 e così via. La sequenza OEIS corrispondente è la numero "A006884"

$$1, 2, 3, 7, 15, 27, 255, 447, 639, 703, 1819, 4255, 4591, 9663, 20895, 26623,$$
$$31911, 60975, 77671, 113383, 138367, 159487, 270271, 665215, 704511, \ldots$$

Traiettorie dei numeri

- Una prima semplificazione ed ottimizzazione della congettura di Collatz, è la seguente:

Algoritmo di Collatz semplificato

Leggi un intero $x \geq 1$
while $(x > 1)$ **do**
    if $x \mod 2 == 0$ $x = x/2$;
    else $x = (3 * x + 1)/2$;
end_while

- Visto che, essendo x dispari, sicuramente $3x + 1$ è pari, possiamo direttamente assegnare come nuovo valore ad x il valore $(3x + 1)/2$. In questo modo, le traiettorie per ogni numero si accorciano
  - $n = 1 :\rightarrow 1$
  - $n = 2 :\rightarrow 2, 1$
  - $n = 3 :\rightarrow 3, 5, 8, 4, 2, 1$
  - $n = 4 :\rightarrow 4, 2, 1$
  - $n = 5 :\rightarrow 5, 8, 4, 2, 1$
  - $n = 6 :\rightarrow 6, 3, 5, 8, 4, 2, 1$
  - $n = 7 :\rightarrow 7, 11, 17, 26, 13, 20, 10, 5, 8, 4, 2, 1$

Traiettorie dei numeri

- Data la definizione della congettura di Collatz, possiamo riformularla anche come segue: dato un intero $n \geq 1$ l'algoritmo raggiunge sempre una potenza di 2?
- In questo modo, le traiettorie per ogni numero si accorciano, anche se ovviamente non cambiano i valori massimi raggiunti
  - $n = 1 :\rightarrow 1$
  - $n = 2 :\rightarrow \mathbf{2}$
  - $n = 3 :\rightarrow 3, 10, 5, \mathbf{16}$
  - $n = 4 :\rightarrow \mathbf{4}$
  - $n = 5 :\rightarrow 5, \mathbf{16}$
  - $n = 6 :\rightarrow 6, 3, 10, 5, \mathbf{16}$
  - $n = 7 :\rightarrow 7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, \mathbf{16}$
  - $n = 8 :\rightarrow \mathbf{8}$
  - $n = 9 :\rightarrow 9, 28, 14, 7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, \mathbf{16}$
  - $n = 10 :\rightarrow 10, 5, \mathbf{16}$
  - $n = 11 :\rightarrow 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, \mathbf{16}$
  - $n = 12 :\rightarrow 12, 6, 3, 10, 5, \mathbf{16}$
  - $n = 13 :\rightarrow 13, 40, 20, 10, 5, \mathbf{16}$
  - $n = 14 :\rightarrow 14, 7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, \mathbf{16}$
  - $n = 15 :\rightarrow 15, 46, 23, 70, 35, 106, 53, 160, 80, 40, 20, 10, 5, \mathbf{16}$

Traiettorie dei numeri

- Se teniamo conto solo delle iterazioni della funzione di Collatz sino a raggiungere una potenza di 2 abbiamo una nuova funzione $c(n)$ che associa ad ogni intero n tale numero di iterazioni, e quindi abbiamo una sequenza numerica

$$0, 0, 3, 0, 1, 4, 12, 0, 15, 2, 10, 5, 5, 13, 13, 0, 8, 16, 16, \ldots$$

  che è la sequenza di OEIS numero "A208981".
- Se dagli esempi visti state congetturando che tutti i numeri non potenze di 2 più grandi di 8 raggiungono sempre il numero 16 vediamo subito che la congettura è falsa
- Per esempio, la traiettoria del numero 21 è: $21, 64$, mentre la traiettoria del numero 85 è $85, 256$.
- In generale, se $h > 3$ è un numero pari, allora $2^h \equiv 1 (\mathrm{mod}\ 3)$ (lo dimostriamo a seguire) e quindi $2^h - 1$ è divisibile per 3. Quindi, possiamo scrivere $2^h - 1 = 3k$ ed inoltre sappiamo che k non è pari, perché altrimenti avremmo $k = 2s$ e quindi $2^h - 1 = 2 \cdot 3s$ che non è possibile perché $2 \cdot 3s$ ed il suo successore 2^h sono coprimi.
- Quindi, partendo da k la sequenza di Collatz ci porta subito a $3k + 1 = 2^h$.
- Per esempio, $21 = (2^6 - 1)/3 = (64 - 1)/3$ e $85 = (2^8 - 1)/3 = (256 - 1)/3$.

Traiettorie dei numeri

- Dimostriamo adesso che se h è pari allora $2^h \equiv 1 (\mod 3)$
- Partiamo dalla semplice congruenza $2 \equiv -1 (\mod 3)$ che è banalmente vera visto che $2 + 1 = 3 \equiv 0 (\mod 3)$.
- Per la proprietà di invarianza rispetto al prodotto, ottengo allora che per ogni $k \geq 1$, $2^k \equiv (-1)^k (\mod 3)$.
- Per k pari otteniamo quanto volevamo dimostrare visto che in quel caso $(-1)^k = 1$.

La Congettura di Collatz

- Sebbene la congettura sia stata formulata nel 1937, gran parte del lavoro "sperimentale" per provare a risolverla è incominciato nel 1970.
- Ad oggi, la congettura è stata verificata per tutti gli $n < 10^{18}$
- Per sottolinearne la difficolta, riporto quanto detto da uno dei più grandi matematici esperti di Strutture Discrete, Paul Erdos: "La matematica non è ancora pronta per tali problemi."
- Ciò detto, possiamo divertirci a giocare con le sequenze e magari trovarne di nuove e interessanti.

FINE SECONDA PARTE

Fondamenti di Teoria dei Numeri e metodologie di dimostrazione