UNITELMA SAPIENZA

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI INFORMATICA

Algebra

Alessandro D'Andrea

2. L'algoritmo euclideo

Richiami

- Somma e prodotto modulo n
- L'anello $\mathbb{Z}/n$
- Alcuni elementi di $\mathbb{Z}/n$ non hanno inverso moltiplicativo
  - Se a e n non sono primi tra loro, allora $\overline{a}$ non ha inverso moltiplicativo in $\mathbb{Z}/n$.
- Oggi: **Se a e n sono primi tra loro, allora $\overline{a}$ è invertibile in $\mathbb{Z}/n$**
  - Algoritmo euclideo per il calcolo del MCD
  - Identità di Bézout

Come si calcola il MCD?

Supponiamo di dover calcolare il massimo comun divisore di 162 e 168. La tecnica che abbiamo tutti imparato consiste in

- Fattorizzare 162 e 168 in fattori primi
- Prendere ciascun fattore primo che compare in entrambe le fattorizzazioni elevato al minimo degli esponenti col quale compare
- Moltiplicare

Eseguiamo questo procedimento nel caso in questione

- $162 = 2^1 \cdot 3^4$, $168 = 2^3 \cdot 3^1 \cdot 7^1$
- Solo i primi 2 e 3 compaiono in entrambe le fattorizzazioni: 2 compare con esponente minimo 1, e 3 compare con esponente minimo 1.
- Il massimo comun divisore è $2^1 \cdot 3^1 = 6$.

Benissimo: qual è il MCD di 1352746 e 2839183?

Fattorizzare non è efficiente

Se vogliamo calcolare il MCD di 1352746 e 2839183, ci rendiamo subito conto che fattorizzare in primi i due numeri ci creerà dei problemi. Anche se possiamo utilizzare un computer, basta che i numeri siano **molto** grandi, e il tempo necessario alla fattorizzazione sarà consistente.

La fattorizzazione, tuttavia, non è essenziale al calcolo del MCD. Riprendendo l'esempio appena visto, possiamo osservare che se un numero divide 162 e 168, divide sicuramente anche la loro differenza $168 - 162 = 6$. Il MCD dovrà quindi necessariamente essere un divisore di 6.

L'algoritmo euclideo per il calcolo del MCD utilizza in modo analogo le proprietà algebriche della divisibilità per fornire una procedura alternativa rapida che prescinde dalla fattorizzazione dei due numeri.

Proprietà della divisibilità

Prima di descrivere l'algoritmo euclideo, preoccupiamoci di capire per quale motivo funzioni. In ciò che segue, a, b, d sono numeri interi. Vi ricordo che d divide a, se $a = dn$ per qualche intero n.

- Se d divide a, d divide tutti i multipli di a.
- Se d divide sia a che b, allora d divide anche $a \pm b$.
- Se d divide sia a che b, allora d divide anche $a \pm qb$.

L'algoritmo euclideo si basa sulla divisione euclidea, cioè la divisione con resto. Se a, b sono numeri interi, possiamo sempre trovare un intero q tale che

$$a = qb + r,$$

dove r è il resto della divisione, e soddisfa $0 \leq r < b$.

Ad esempio, dovendo dividere 14 per 4, si ottiene $14 = 3 \cdot 4 + 2$.

Divisione euclidea e divisibilità

Dati due interi a, b, eseguiamo la divisione euclidea

$$a = qb + r.$$

Se d divide sia a che b, allora divide sicuramente anche $r = a - qb$.

Viceversa, supponiamo che d divida sia b che r. Procedendo a ritroso, d deve dividere anche $a = qb + r$. In altre parole essere un divisore comune di a e b è lo stesso che essere un divisore comune di b ed r.

Dal momento che l'insieme dei divisori comuni di a e b coincide con l'insieme dei divisori comuni di b ed r, il massimo tra i divisori comuni di a e b dovrà essere uguale al massimo tra i divisori comuni di b ed r. In altre parole

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

Algoritmo euclideo

Dovendo calcolare il MCD di due numeri dati a e b, una strategia astuta può essere quella di eseguire la divisione euclidea tra i due numeri, calcolando il resto r. Allora $\text{MCD}(a, b) = \text{MCD}(b, r)$, ed r è certamente più piccolo di a.

Si può allora reiterare la procedura eseguendo la divisione euclidea tra b ed r. I resti diventano ogni volta più piccoli, e dopo un numero finito di passi, il resto dovrà essere 0.

A quel punto, il calcolo del MCD sarà semplice: $\text{MCD}(n, 0) = n$.

Proviamo con un esempio!

Un esempio di calcolo del MCD

Calcoliamo il MCD di 168 e 162. Eseguendo la divisione euclidea, si ottiene

$$168 = 1 \cdot 162 + 6,$$

e il resto è quindi 6. Pertanto $\mathrm{MCD}(168, 162) = \mathrm{MCD}(162, 6)$.
Possiamo eseguire una nuova divisione euclidea

$$162 = 27 \cdot 6 + 0,$$

e il nuovo resto è 0. Pertanto $\mathrm{MCD}(162, 6) = \mathrm{MCD}(6, 0)$.
Ma $\mathrm{MCD}(6, 0)$ è chiaramente uguale a 6. In conclusione

$$\mathrm{MCD}(168, 162) = \mathrm{MCD}(162, 6) = \mathrm{MCD}(6, 0) = 6.$$

Facile e rapido! Proviamo con numeri più grandi.

Un altro esempio

Calcoliamo il MCD tra 2839183 e 1352746 (aiutandoci con una calcolatrice). Eseguiremo divisioni euclidee una dopo l'altra. L'ultimo resto non nullo sarà il MCD desiderato.

$$
\begin{aligned}
2839183 &= 2 \cdot 1352746 + 133691 \\
1352746 &= 10 \cdot 133691 + 15836 \\
133691 &= 8 \cdot 15836 + 7003 \\
15836 &= 2 \cdot 7003 + 1830 \\
7003 &= 3 \cdot 1830 + 1513 \\
1830 &= 1 \cdot 1513 + 317 \\
1513 &= 4 \cdot 317 + 245 \\
317 &= 1 \cdot 245 + 72 \\
245 &= 3 \cdot 72 + 29 \\
72 &= 2 \cdot 29 + 14 \\
29 &= 2 \cdot 14 + 1 \\
14 &= 14 \cdot 1 + 0
\end{aligned}
$$

Per la cronaca: $1352746 = 2 \times 676373$, mentre 2839183 è primo!

Efficienza dell'algoritmo - I

Nel caso appena visto, il numero di divisioni non è stato eccessivo, ma è bene sapere quanto rapidamente l'algoritmo euclideo arrivi a conclusione.

Non è difficile mostrare come il numero di divisioni necessarie al calcolo di MCD(a, b) sia al più $\lceil \log_\phi b \rceil$, dove $\phi = (1 + \sqrt{5})/2 \simeq 1.681$.

In termini più concreti, se b è un numero con n cifre decimali, ce la caviamo con al più $\lceil \log_\phi(10) \cdot n \rceil \simeq 4.785 \cdot n$ divisioni.

Efficienza dell'algoritmo - II

Per cultura generale, il caso più sfortunato è quello di due numeri di Fibonacci consecutivi:

$$
\begin{aligned}
55 &= 1 \cdot 34 + 21 \\
34 &= 1 \cdot 21 + 13 \\
21 &= 1 \cdot 13 + 8 \\
13 &= 1 \cdot 8 + 5 \\
8 &= 1 \cdot 5 + 3 \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 1 + 1 \\
2 &= 1 \cdot 1 + 0
\end{aligned}
$$

Se, per rendere i resti piccoli più rapidamente, accettate che possano essere negativi, il numero di divisioni euclidee necessarie scende a circa $\log_\gamma b$, dove $\gamma = 1 + \sqrt{2}$; in altre parole, a circa 2.6125 volte il numero di cifre decimali di b.

Identità di Bézout - I

L'algoritmo euclideo può essere però sfruttato anche per ricavare altre informazioni.

Una delle informazioni occulte possedute dall'algoritmo euclideo è il fatto che il MCD di a e b si ottiene sempre prendendo la differenza tra un multiplo di a e un multiplo di b.
Vediamo un esempio. Calcoliamo il MCD di 26 e 14:

$$\begin{aligned} 26 &= 1 \cdot 14 + 12 \\ 14 &= 1 \cdot 12 + 2 \\ 12 &= 6 \cdot 2 \quad + 0 \end{aligned}$$

Si vede che $2 = \text{MCD}(26, 14)$. Dalla seconda divisione si ricava $2 = 14 - 12$. Ad ogni modo, dalla prima divisione si ha $12 = 26 - 14$. Sostituendo,

$$2 = 14 - 12 = 14 - (26 - 14) = 2 \cdot 14 - 26.$$

Identità di Bézout - II

Vediamo un altro esempio con $a = 25, b = 16$

$$\begin{aligned} 25 &= 1 \cdot 16 + 9 \\ 16 &= 1 \cdot 9 + 7 \\ 9 &= 1 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

e procediamo a ritroso per esprimere $\mathrm{MCD}(25, 16) = 1$.

$$\begin{aligned} & & 1 &= 1 \cdot 7 - 3 \cdot 2 & & \\ 2 = 9 - 7 \quad &\Longrightarrow & 1 &= 1 \cdot 7 - 3 \cdot (9 - 7) &&= -3 \cdot 9 + 4 \cdot 7 \\ 7 = 16 - 9 \quad &\Longrightarrow & 1 &= -3 \cdot 9 + 4 \cdot (16 - 9) &&= 4 \cdot 16 - 7 \cdot 9 \\ 9 = 25 - 16 \quad &\Longrightarrow & 1 &= 4 \cdot 16 - 7 \cdot (25 - 16) &&= -7 \cdot 25 + 11 \cdot 16. \end{aligned}$$

Ricapitolando, se $d = \mathrm{MCD}(a, b)$, allora esistono degli interi h, k tali che $d = ha + kb$. Questa relazione è detta Identità di Bézout.

Elementi invertibili di $\mathbb{Z}/n$

Abbiamo finalmente un modo di stabilire quando un elemento $\overline{a}$ sia invertibile in $\mathbb{Z}/n$.

Se MCD$(a, n) \neq 1$, abbiamo già visto che $\overline{a}$ sicuramente non possiede un inverso moltiplicativo.

Se invece MCD$(a, n) = 1$, allora per l'identità di Bézout esistono h, k interi tali che $ha + kn = 1$. Ma allora

$$ha \equiv 1 \mod n,$$

poiché la differenza tra ha e 1 è un multiplo di n. In altre parole

$$\overline{h} \cdot \overline{a} = \overline{1} \text{ in } \mathbb{Z}/n,$$

e quindi non solo $\overline{a}$ è invertibile in $\mathbb{Z}/n$, ma sappiamo anche come trovare il suo inverso $\overline{h}$.

Esempio di calcolo dell'inverso

Ad esempio, poiché

$$1 = \mathrm{MCD}(25, 16) = -7 \cdot 25 + 11 \cdot 16,$$

l'inverso moltiplicativo di $\overline{16}$ in $\mathbb{Z}/25$ è $\overline{11}$. In effetti $16 \cdot 11 = 176 = 3 \cdot 25 + 1 \equiv 1 \mod 25$.

Allo stesso modo, l'inverso moltiplicativo di $\overline{25}$ in $\mathbb{Z}/16$ è $\overline{-7} = \overline{9}$. In effetti $25 \cdot 9 \equiv 9 \cdot 9 = 81 = 5 \cdot 16 + 1 \equiv 1 \mod 16$.