UNITELMA SAPIENZA

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI INFORMATICA

Algebra

Alessandro D'Andrea

3. Teorema cinese dei resti

Richiami

- $\mathbb{Z}/n$ è un anello
- $\overline{a}$ è invertibile in $\mathbb{Z}/n$ se e solo se $\text{MCD}(a, n) = 1$
- Se $\text{MCD}(a, n) = 1$, l'inverso di $\overline{a}$ in $\mathbb{Z}/n$ si trova con l'identità di Bézout, che si calcola con l'algoritmo euclideo
- Oggi: **Congruenze lineari in una incognita e sistemi di congruenze lineari in una incognita**
  - Come riconoscere quando una congruenza ammette soluzione ed eventualmente trovarle
  - Teorema cinese dei resti

Congruenze lineari

Risolvere una congruenza lineare significa trovare tutti i valori (interi) di x tali che

$$ax \equiv b \mod n,$$

dove a, b, n sono interi dati. Una riformulazione equivalente è

$$\overline{ax} = \overline{b} \text{ in } \mathbb{Z}/n.$$

La seconda formulazione mostra che se x è soluzione della congruenza lineare, sono soluzioni anche tutti gli altri elementi della sua classe di congruenza.

Il nostro obiettivo in questa lezione è stabilire quali congruenze lineari ammettano soluzione, e determinare eventualmente tutte le soluzioni.

Se $\overline{a}$ è invertibile in $\mathbb{Z}/n$..

C'è un caso in cui sappiamo già come procedere. Se dobbiamo risolvere

$$ax \equiv b \mod n,$$

e capita che $\mathrm{MCD}(a, n) = 1$, allora $\overline{a}$ è invertibile in $\mathbb{Z}/n$. Moltiplicando entrambi i membri per il suo inverso $\overline{h}$, si ottiene

$$\begin{aligned}
a\,x &\equiv b && \mod n; \\
\overline{a}\,\overline{x} &= \overline{b} && \text{in } \mathbb{Z}/n; \\
\overline{h}\,\overline{a}\,\overline{x} &= \overline{h}\,\overline{b} && \text{in } \mathbb{Z}/n; \\
\overline{x} &= \overline{h}\,\overline{b} && \text{in } \mathbb{Z}/n; \\
x &\equiv h\,b && \mod n.
\end{aligned}$$

Compatibilità - I

La congruenza

$$2x \equiv 3 \mod 6$$

sicuramente non ha soluzione.

In effetti, $2x$ è sicuramente pari, mentre 3 è dispari. La loro differenza è allora dispari, e non può essere un multiplo di 6.

Il nostro obiettivo è quello di generalizzare questa osservazione al caso di una congruenza qualsiasi

$$ax \equiv b \mod n.$$

Compatibilità - II

Dovendo risolvere una congruenza lineare

$$ax \equiv b \mod n,$$

calcoliamo $d = \text{MCD}(a, n)$.

Un intero x è soluzione se $ax - b$ è un multiplo di n. Ma n è un multiplo di d, quindi $ax - b$ deve essere un multiplo di d.

Tuttavia, d divide anche a, e quindi anche il suo multiplo ax. In conclusione, se la congruenza ammette una soluzione x, allora d deve dividere b.

Compatibilità - III

Affinché la congruenza $ax \equiv b \mod n$ ammetta soluzioni, $\mathrm{MCD}(a, n)$ deve dividere b. In altre parole, se $\mathrm{MCD}(a, n)$ non divide b, allora la congruenza non può avere soluzioni.

Ad esempio, la congruenza

$$12x \equiv 16 \mod 18$$

sicuramente non ammette soluzioni. Infatti, il MCD tra 12 e 18 è $\mathrm{MCD}(12, 18) = 6$ che non divide 16.

Riduzione a forma normale

Che cosa possiamo dire di una congruenza

$$ax \equiv b \mod n$$

quando $d = \mathrm{MCD}(a, n)$ divide b? d divide tutti e tre gli interi a, b, n.
Quindi $a = dA, b = dB, n = dN$.
La congruenza si riformula come:

$$\begin{aligned} ax - b \quad & \text{è un multiplo di } n, \\ dAx - dB = d(Ax - B) \quad & \text{è un multiplo di } dN; \\ Ax - B \quad & \text{è un multiplo di } N. \end{aligned}$$

La congruenza iniziale ha le stesse soluzioni della congruenza

$$Ax \equiv B \mod N,$$

che si ottiene dividendo tutti e tre i coefficienti per $d = \mathrm{MCD}(a, n)$.

Due esempi - I

Risolvere

$$12x \equiv 17 \mod 21.$$

Calcoliamo $\mathrm{MCD}(12, 21) = 3$. E' vero che 3 divide 17? No. Allora la congruenza non ha soluzioni.

Risolvere

$$12x \equiv 18 \mod 21.$$

Calcoliamo $\mathrm{MCD}(12, 21) = 3$. E' vero che 3 divide 18? Sì. Allora la congruenza è equivalente a

$$4x \equiv 6 \mod 7,$$

che si ottiene dividendo tutto per 3.

Due esempi - II

Ma

$$4x \equiv 6 \mod 7$$

è una congruenza che sappiamo risolvere!

Gli interi 4 e 7 sono primi tra loro, quindi $\overline{4}$ è invertibile in $\mathbb{Z}/7$. Il suo inverso è $\overline{2}$. Moltiplicando entrambi i membri per 2 si ottiene

$$8x \equiv 12 \mod 7$$

cioè

$$x \equiv 5 \mod 7,$$

e la congruenza è risolta!

Strategia risolutiva

Ricapitoliamo. Per risolvere la congruenza

$$ax \equiv b \mod n,$$

calcolo $d = \text{MCD}(a, n)$ e verifico se divide b.

- Se d non divide b, la congruenza non ammette soluzioni
- Se d divide b, divido a, b, n tutti per d e ottengo una congruenza equivalente.

  In tale congruenza il coefficiente della x è invertibile, e posso trovare facilmente le soluzioni.

Risoluzione di un esercizio

Moltiplicando il numero intero x per 34, si ottiene un numero le cui ultime due cifre decimali sono 16. Che si può dire del numero x?

$$34x \equiv 16 \mod 100.$$

$\mathrm{MCD}(34, 100) = 2$. Inoltre, 2 divide 16. La congruenza è equivalente a

$$17x \equiv 8 \mod 50.$$

Ora $\mathrm{MCD}(17, 50) = 1$, quindi 17 è invertibile modulo 50. L'inverso è 3. Moltiplicando per 3 entrambi i membri

$$x \equiv 24 \mod 50.$$

Il numero x è della forma $24 + 50k$. In altre parole, le sue ultime due cifre sono 24 oppure 74. $(34 \cdot 24 = 816, 34 \cdot 74 = 2516$. Funziona!!!)

Esercizio di riepilogo

Mettete in pausa, e provate a risolvere

$$12x \equiv 21 \mod 87.$$

Passiamo ora a risolvere sistemi di congruenze lineari. Siamo interessati a sistemi di questo tipo

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n. \end{cases}$$

Teorema (cinese dei resti)

Se m, n sono primi tra loro, il sistema ammette soluzioni per ogni scelta di a, b. Una volta fissati a e b, la soluzione è inoltre unica modulo mn.

Può essere necessario saper risolvere sistemi di congruenze anche quando m, n non sono primi tra loro. Per il momento, però, limitiamoci al caso $\mathrm{MCD}(m, n) = 1$, e proviamo a capire per quale motivo il Teorema cinese dei resti sia vero.

Unicità della soluzione $\mod mn$

$\text{MCD}(m,n) = 1$. Se x_1, x_2 sono soluzioni del sistema

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n, \end{cases}$$

allora $x_1 \equiv a \equiv x_2 \mod m$ e $x_1 \equiv b \equiv x_2 \mod n$.
Questo vuol dire che $x_1 - x_2$ è un multiplo sia di m che di n, e quindi anche del prodotto mn. In conclusione $x_1 \equiv x_2 \mod mn$.

Fissati i valori di a e b, o il sistema non ha soluzioni, o le soluzioni sono tutti e soli gli interi contenuti in una singola classe di congruenza modulo mn.

Le soluzioni del sistema non cambiano sostituendo a con un altro valore che sia nella sua classe di congruenza modulo m (e analogamente per b). Posso quindi limitarmi a considerare $0 \leq a < m, 0 \leq b < n$.

Esistenza della soluzione

Ciascun intero è soluzione del sistema

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n, \end{cases}$$

per un'opportuna scelta di $0 \leq a < m, 0 \leq b < n$.

Quindi tutte le mn classi di resto modulo mn sono ottenute come soluzioni del sistema per un'opportuna scelta di a, b.

Tuttavia le possibili scelte di a, b sono in totale mn. Questo dimostra che per ogni scelta di a, b il sistema ha necessariamente soluzioni.

Un esempio pratico

Risolviamo

$$\begin{cases} x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7. \end{cases}$$

La prima congruenza ci dice che $x = 3 + 5t$ per un opportuno valore intero di t.
Sostituendo nella seconda congruenza, si ottiene $3 + 5t \equiv 2 \mod 7$, cioè

$$5t \equiv 2 - 3 \equiv 6 \mod 7.$$

Moltiplichiamo per l'inverso moltiplicativo di 5, che è 3, ottenendo

$$t \equiv 3 \cdot 5t \equiv 3 \cdot 6 = 18 \equiv 4 \mod 7.$$

Sostituendo $t = 4 + 7s$ in $x = 3 + 5t$ si ottiene

$$x = 3 + 5(4 + 7s) = 23 + 35s, \text{ cioè } x \equiv 23 \mod 35.$$

Filosofia generale

Conoscere un numero modulo mn, è equivalente a conoscerlo sia modulo m che modulo n.

Conoscere un numero modulo $m_1, m_2, \ldots, m_k$, dove gli m_i sono numeri primi tra loro, equivale a conoscerlo modulo $m_1 \cdot m_2 \cdot \cdots \cdot m_k$.

Se ho un paio di migliaia di soldati in piazza d'armi, e li conto modulo $5, 6, 7$ e 11, allora conosco il loro numero modulo $2310 = 5 \cdot 6 \cdot 7 \cdot 11$, e quindi li ho contati con precisione.

A volte, contare modulo m e modulo n è più semplice che contare modulo mn. Ne faremo esperienza in svariati esempi.