UNITELMA SAPIENZA

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI INFORMATICA

Algebra

Alessandro D'Andrea

1. Aritmetica modulare

Programma del corso

- **Gruppi finiti**
  - Aritmetica modulare
  - Alcuni risultati elementari di teoria dei gruppi
  - Applicazioni: crittografia RSA – un algoritmo di primalità
- **Algebra lineare**
  - Sistemi di equazioni lineari
  - Operatori lineari, spazi vettoriali, geometria affine
  - Applicazioni: *page-rank* – compressione immagini

Congruenze modulo 10

L'aritmetica degli interi modulo 10 considera solo la cifra delle unità, e ignora tutte le altre.

- Gli unici numeri che consideriamo sono $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$
- $3 + 8 = 1$, $6 \cdot 7 = 2$
- $-4 = 6$, $3 - 9 = 4$
- La divisione è problematica: $2/6 = 2?$ $7?$, $1/2 = ?$

Definizione formale: due numeri a, b sono congrui, o congruenti, modulo 10 se la loro differenza $b - a$ è multipla di 10. Si scrive $a \equiv b \mod 10$. Ad esempio

$$137 \equiv 27 \mod 10, \qquad 26 \equiv -14 \mod 10.$$

Somma e prodotto mod 10

La cifra delle unità di una somma (o di un prodotto) dipende solamente dalle cifre delle unità degli addendi (o dei fattori).

$$6+5=11, \qquad 16+75=91, \qquad -24+215=191.$$

$$4\cdot 9=36, \qquad 14\cdot 29=406, \qquad (-16)\cdot(-11)=176.$$

Scriviamo: $6+5\equiv 1 \mod 10$, $4\cdot 9\equiv 6 \mod 10$.

Valgono le solite proprietà

$$a+b\equiv b+a, \quad a\cdot b\equiv b\cdot a, \quad a(b+c)\equiv ab+ac \mod 10.$$

$$(a+b)+c\equiv a+(b+c), \qquad (a\cdot b)\cdot c\equiv a\cdot(b\cdot c) \mod 10.$$

$$0+a=a, \quad 0\cdot a\equiv 0, \quad 1\cdot a\equiv a, \quad 2\cdot 5=0 \mod 10.$$

L'anello $\mathbb{Z}/10$

La notazione non è univoca. Spesso si rappresenta con $\overline{a}$ l'intera classe di congruenza dell'intero a. Ad esempio

$$\overline{2} = \{\ldots, -28, -18, -8, 2, 12, 22, 32, 42, \ldots\},$$

e si eseguono le operazioni direttamente tra classi di congruenza:

$$\overline{4} + \overline{8} = \overline{2}, \qquad \overline{7} \cdot \overline{8} = \overline{6}.$$

Questo ha esattamente lo stesso significato di

$$4 + 8 = 2 \mod 10, \qquad 7 \cdot 8 = 6 \mod 10.$$

L'insieme delle classi di congruenza modulo 10, con le sue operazioni di somma e prodotto, si indica con $\mathbb{Z}/10$. $\mathbb{Z}/10$ è un anello.

Che cos'è un anello?

Un anello è un insieme A sul quale sono definite due operazioni:

- la somma $(a, b) \mapsto a + b$
- il prodotto $(a, b) \mapsto a \cdot b$

commutative e associative. L'operazione di somma deve rendere A un gruppo abeliano: deve possedere un elemento neutro (che si indica con 0)

$$a + 0 = 0 + a = a \quad \text{per ogni } a \in A;$$

e ogni elemento $a \in A$ deve possedere un inverso additivo, che si indica con $-a$:

$$a + (-a) = (-a) + a = 0.$$

L'operazione di prodotto deve distribuire inoltre rispetto alla somma

$$a(b + c) = ab + ac, \qquad (a + b)c = ac + bc.$$

Anche il prodotto possiede un elemento neutro, che si indica con 1. Sono anelli $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ e, come abbiamo imparato, anche $\mathbb{Z}/n$.

L'anello $\mathbb{Z}/n$

In quello che abbiamo visto, 10 non riveste un ruolo speciale, e possiamo ripetere l'intera costruzione usando qualsiasi intero $n > 1$.

- $a \equiv b \mod n$ esattamente quando n divide $b - a$
  - $a \equiv a \mod n$
  - $a \equiv b \mod n \implies b \equiv a \mod n$
  - $a \equiv b \mod n, b \equiv c \mod n \implies a \equiv c \mod n$
- Se $a \equiv a' \mod n$, $b \equiv b' \mod n$, allora
  - $a + a' \equiv b + b' \mod n$
  - $a \cdot a' \equiv b \cdot b' \mod n$.

Ad esempio, $1 \equiv 15 \equiv 120 \mod 7$. Calcoliamo anche un prodotto:

$$16 \cdot 12 \equiv 2 \cdot 5 \equiv 10 \equiv 3 \mod 7.$$

Possiamo anche scrivere $\overline{16} \cdot \overline{12} = \overline{2} \cdot \overline{5} = \overline{10} = \overline{3}$ a patto che sia chiaro che tutto si trova in $\mathbb{Z}/7$.

Risoluzione di equazioni - I

Prima di andare avanti, ho bisogno di una premessa. Quando abbiamo bisogno di risolvere un'equazione, effettuiamo manipolazioni che non cambiano l'insieme delle soluzioni.
Ad esempio, se abbiamo l'equazione

$$A = B,$$

come sua conseguenza abbiamo anche

$$2A = 2B.$$

Questo vuol dire che se la prima equazione è soddisfatta, lo è anche la seconda, cioè che ogni soluzione della prima equazione è soluzione anche della seconda.
Tuttavia anche la prima equazione è una conseguenza della seconda, poiché si ottiene dalla seconda moltiplicando per $1/2$. Pertanto le due equazioni sono equivalenti, e hanno lo stesso insieme di soluzioni.

Risoluzione di equazioni - II

Le manipolazioni lecite, nella risoluzione di equazioni, sono tutte di questo tipo, cioè invertibili. Ad esempio, dall'equazione

$$A - B = C$$

segue l'equazione

$$A = C + B$$

sommando ad entrambi i membri B; pertanto la seconda equazione è una conseguenza della prima. Tuttavia, anche la prima è una conseguenza della seconda: la ottengo sommando ad entrambi i membri $-B$.

In conclusione, ogni soluzione della prima equazione è anche soluzione della seconda, e viceversa: le due equazioni hanno le stesse soluzioni.

Somma e prodotto in $\mathbb{Z}/5$

Calcoliamo le tavole di addizione e moltiplicazione nell'anello $\mathbb{Z}/5$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Si vede immediatamente che ogni classe diversa da $\overline{0}$ possiede un inverso moltiplicativo! Non abbiamo quindi problemi a risolvere equazioni di primo grado in $\mathbb{Z}/5$. Ad esempio, se $2x \equiv 3 \mod 5$, basta moltiplicare entrambi i membri per l'inverso di $\overline{2}$, che è $\overline{3}$, per ottenere

$$x \equiv 3 \cdot (2x) \equiv 3 \cdot 3 \equiv 4 \mod 5.$$

Somma e prodotto in $\mathbb{Z}/6$

La situazione in $\mathbb{Z}/6$ è completamente diversa:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Si vede subito che solo $\overline{1}$ e $\overline{5}$ possiedono un inverso moltiplicativo, e quindi la strategia di moltiplicare per l'inverso non è sempre applicabile alla risoluzione di una congruenza lineare.

Ad esempio, l'equazione $2x \equiv 3 \mod 6$ non ha soluzione in $\mathbb{Z}/6$.

Perché $\overline{2}$ non ha inverso in $\mathbb{Z}/6$?

Se x è un inverso moltiplicativo di $\overline{2}$ in $\mathbb{Z}/6$, allora

$$2x \equiv 1 \mod 6.$$

In altre parole, la differenza $2x - 1$ è multipla di 6. Ma questo non può accadere, perché tutti i multipli di 6 sono pari, mentre $2x - 1$ è dispari!

Questo ragionamento si applica all'elemento $\overline{a} \in \mathbb{Z}/n$ ogni volta che a ed n abbiano un fattore in comune: supponiamo che $d \neq 1$ divida sia a che n. Se x è un inverso moltiplicativo di $\overline{a}$ in $\mathbb{Z}/n$, allora

$$ax \equiv 1 \mod n.$$

In altre parole $ax - 1$ è multiplo di n; ma poiché d divide n, è anche multiplo di d. Questo è impossibile, perché ax è multiplo di d, e quindi $ax - 1$ non può esserlo!

Invertibili di $\mathbb{Z}/n$

In conclusione, se a ed n non sono primi tra loro, sicuramente $\overline{a}$ non possiede un inverso moltiplicativo in $\mathbb{Z}/n$.

Vedremo nella prossima lezione che se a ed n sono primi tra loro, $\overline{a}$ ha sempre un inverso moltiplicativo in $\mathbb{Z}/n$. Per trovarlo, avremo bisogno di imparare l'algoritmo euclideo per il calcolo del massimo comun divisore.

Come verifica di quello che abbiamo imparato, calcolate le tavole di addizione e moltiplicazione di $\mathbb{Z}/7$ e $\mathbb{Z}/8$, e controllate quali elementi abbiano inverso moltiplicativo.