Aritmetica modulare

Zn

Artmetica modulare

- L'aritmetica modulare (a volte detta aritmetica dell'orologio poiché su tale principio si basa il calcolo delle ore a cicli di 12 o 24) rappresenta un importante ramo della matematica.
- Trova applicazioni nella crittografia, nella teoria dei numeri (in particolare nella ricerca dei numeri primi), ed è alla base di molte delle più comuni operazioni aritmetiche e algebriche.
- Si tratta di un sistema di aritmetica degli interi, nel quale i numeri "si avvolgono su se stessi" ogni volta che raggiungono i multipli di un determinato numero n, detto modulo.

La relazione di congruenza

- L'aritmetica modulare si basa sul concetto di congruenza modulo n.
- Dati tre numeri interi a, b, n, con n ≠ 0, diciamo che a e b sono congruenti modulo n se la loro differenza (a − b) è un multiplo di n.
- In questo caso scriviamo $a \equiv b \pmod{n}$
- e diciamo che a è congruo a b modulo n.
- Per esempio, possiamo scrivere $38 \equiv 14 \pmod{12}$
- 38 − 14 = 24, che è un multiplo di 12.

Proprietà

- Fra le proprietà notiamo

$$a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n} \qquad \forall a, b \in \mathbb{N}, \forall k \in \mathbb{N}, \forall n \in \mathbb{N}_0$$

Moltiplicazione mod 11

	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Considerazioni

- La moltiplicazione su Z_n (con n primo) “mescola” gli elementi di Z_n
- Per ogni elemento x di Z_n esiste un inverso y tale che
  - se a * x (mod n) = b
  - allora y * b (mod n) = a
- Nell’esempio su Z_{11} l’inverso di 2 è 6
  - Prendiamo per esempio il numero 8
  - 8 * 2 (mod 11) = 5
  - 5 * 6 (mod 11) = 8

	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
6	0	6	1	7	2	8	3	9	4	10	5

Altro esempio

	0	1	2	3	4	5	6	7	8	9	10
f(x) = 5x mod n	0	5	10	4	9	3	8	2	7	1	6
$f^{-1}(x)$ = 9f(x) mod n	0	1	2	3	4	5	6	7	8	9	10

- **f(x) "mescola" l'insieme dei valori**
- **$f^{-1}(x)$ "riordina" l'insieme dei valori**
- **Le due funzioni sono moltiplicazioni modulo n**
- **5 è intesa come Ke**
- **9 è il reciproco di 5 modulo 11 è intesa come Kd**

Conseguenze

- Potremmo utilizzare quindi un semplice algoritmo (moltiplicazione modulo n) per crittare con una chiave (chiave pubblica) e decrittare con l'altra (chiave privata)
- Il problema che rimane è quello di rendere "impossibile" ottenere la chiave privata conoscendo la sola chiave pubblica