Campi finiti - cenni

Un campo è un insieme F con due operazioni, somma $(+)$ e prodotto $\cdot$, tale che

- F è un gruppo commutativo rispetto alla somma
- $F \setminus \{0\}$ è un gruppo commutativo rispetto al prodotto
- vale la proprietà distributiva: $(a+b)c = ac + bc$ e $a(b+c) = ab + ac$

La seconda condizione implica l'esistenza di un inverso moltiplicativo per ogni $a \neq 0$ in F:

$$\forall a \in F, a \neq 0, \qquad \exists a^{-1} \in F$$
$$a \cdot a^{-1} = 1$$

Esempi: $\mathbb{Q}$ è un campo, $\mathbb{Z}$ non lo è (per esempio 2 non ha un inverso moltiplicativo in $\mathbb{Z}$).

Un campo finito è un campo con un numero finito di elementi.

- neanche $\mathbb{Z}_8$ è un campo; per esempio 2 non ha un inverso moltiplicativo in $\mathbb{Z}_8$
- infatti, moltiplicando 2 per gli elementi di $\mathbb{Z}_8$, non otteniamo mai 1

$\cdot$	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6

- si ha che $\mathbb{Z}_n$ è un campo $\iff$ n è un numero primo
- già visto: $U(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n \mid (a, n) = 1\}$
- dunque $\mathbb{Z}_n$ campo $\iff$ $U(\mathbb{Z}_n) = \mathbb{Z}_n \setminus \{0\}$ $\iff$ n primo

Teorema

1. *F un campo finito* $\Rightarrow |F| = p^m$, *p primo*
2. $\forall$ *p primo,* $\forall m \geq 1$ *esiste un unico campo finito F con p^m elementi; F si denota con $\mathbb{F}_{p^m}$ (o $GF(p^m)$)*

Per $m = 1$, $\mathbb{F}_p = \mathbb{Z}_p$
Ma come sono fatti i campi con p^m elementi, $m > 1$?

campo con 8 elementi

- Esempio: cerchiamo di costruire il campo $\mathbb{F}_8$ con 8 elementi. ($\mathbb{Z}_8$ non va bene)
- $8 = 2^3$: consideriamo $\mathbb{Z}_2[x]$, l'insieme dei polinomi a coefficienti in $\mathbb{Z}_2$
- in particolare, consideriamo l'insieme S di questi polinomi di grado *minore* di 3
- $S = \{a_2x^2 + a_1x + a_0 \mid a_i \in \mathbb{Z}_2\}$; ha 8 elementi
- esplicitamente, si ha
  $S = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$
- S "diventerà" il campo $\mathbb{F}_8$; bisogna vedere come funzionano le operazioni di somma e prodotto

somma

- l'insieme S è chiuso rispetto alla somma: la somma di due polinomi di grado minore di 3 è un polinomio di grado minore di 3.
- Ex: $(x+1)+(x^2+x) = x^2+2x+1 = x^2+1$
- S è un gruppo commutativo rispetto alla somma fra polinomi (esercizio).
- si può identificare S con $\mathbb{Z}_2^3$; il polinomio $a_2x^2+a_1x+a_0$ si identifica con la stringa $a_2a_1a_0$.
  $x+1 \to 011$, $x^2+x \to 110$
- con questa identificazione, la somma corrisponde allo XOR fra stringhe

$$\begin{aligned} (x+1)+(x^2+x) &= x^2+1 \\ 011 \oplus 110 &= 101 \end{aligned}$$

prodotto

- l'insieme S non è chiuso rispetto al prodotto: il prodotto di due polinomi di grado minore di 3 può essere un polinomio di grado maggiore o uguale a 3.
- Ex: $(x^2+1)\cdot(x^2+x) = x^4+x^3+x^2+x \notin S$
- si introduce la congruenza fra polinomi:
  $p_1(x) \equiv p_2(x) \pmod{m(x)} \iff m(x) | p_1(x)-p_2(x)$
- fra polinomi si può fare la divisione con il resto: se $p(x)$, $m(x)$ sono due polinomi, e il grado di $m(x)$ è m, allora
  $p(x) = q(x)m(x)+r(x)$, e il grado di $r(x)$ è minore di m
  inoltre $p(x) \equiv r(x) \pmod{m(x)}$
- per restare all'interno di S, il risultato della moltiplicazione va ridotto modulo un polinomio di terzo grado; si sceglie un polinomio irriducibile su $\mathbb{Z}_2$ di grado 3 (per esempio x^3+x+1).

- il risultato del prodotto va ridotto modulo $x^3 + x + 1$
- $(x^2 + 1) \cdot (x^2 + x) = x^4 + x^3 + x^2 + x =$
  $(x + 1)(x^3 + x + 1) + x + 1 \equiv x + 1$
- con questo prodotto, S diventa un campo finito: ogni elemento $\neq 0$ ha un inverso moltiplicativo.

$$\mathbb{F}_8 = \mathbb{Z}_2[x]/x^3 + x + 1$$

- ex: l'inverso di x è $x^2 + 1$;
  $x(x^2 + 1) = x^3 + x = (x^3 + x + 1) + 1 = 1$

il caso generale

Questo procedimento si generalizza: per costruire il campo $\mathbb{F}_{p^m}$:

- si considerano i polinomi a coefficienti in $\mathbb{Z}_p$;
- si sceglie un polinomio $m(x) \in \mathbb{Z}_p[x]$ di grado m, *irriducibile* su $\mathbb{Z}_p$;
- $\mathbb{F}_{p^m} = \mathbb{Z}_p[x]/m(x)$;
- la somma è la somma ordinaria fra polinomi;
- il risultato del prodotto va ridotto modulo $m(x)$.

il caso binario

- in particolare se $p = 2$, il campo $\mathbb{F}_{2^m}$ è fatto di polinomi del tipo
  $a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$, dove $a_i \in \{0, 1\}$
- si identifica $\mathbb{F}_{2^m}$ con l'insieme $\{0, 1\}^m$ delle stringhe binarie lunghe m
- $a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \leftrightarrow a_{m-1} \ldots a_1 a_0$
- la somma in $\mathbb{F}_{2^m}$ corrisponde allo XOR fra stringhe
- per quanto riguarda il prodotto, conviene lavorare sui polinomi

AES - SubBytes

- nell'AES, i plaintext sono stringhe lunghe 128 (2^7); sono pensati come 2^4 sottoblocchi di lunghezza 2^3 - cioè 16 byte
- i byte vengono trattati come elementi del campo $\mathbb{F}_{2^8} = \mathbb{Z}_2[x]/(x^8 + x^4 + x^3 + x + 1)$; (Rijndael's finite field)
- la sostituzione - Sub-bytes prende in input un byte $a_7 \ldots a_1 a_0$ e dà in output un byte $b_7 \ldots b_1 b_0$
  1. $a = a_7 x^7 + \cdots + a_1 x + a_0 \in \mathbb{F}_{2^8}$
  2. si calcola $a^{-1} = \widehat{a_7} x^7 + \cdots + \widehat{a_1} x + \widehat{a_0} \in \mathbb{F}_{2^8}$
  3. si applica una trasformazione affine a $\widehat{a_7} \ldots \widehat{a_1}\widehat{a_0}$ (della forma $x \to Ax + B$, A matrice invertibile 8×8, B matrice 8×1)
  4. il risultato dà l'output $b_7 \ldots b_1 b_0$