① dimmo fq 3 mod 5

es. $\begin{cases} 3X \equiv 1 \pmod 5 \\ X \equiv 3^{-1} \equiv 2 \pmod 5 \end{cases}$ $mcd(3,5)=1$

lavorare in $\mathbb{Z}_p$ p primo

insieme (+,×) operazioni

Campo Field { (1) addizione (2) sottrazione (3) moltiplicazione (4) divisione per elementi non zero

leggi (a) associativa $(xy)z = x(yz)$; $(x+y)+z = x+(y+z)$
(c) commutativa → $xy = yx$ → $x+y = y+x$
(d) distributiva → $x(y+z) = xy+xz$
tra le operazioni di addizione e moltiplicazione

insiemi comuni:
- numeri reali
- numeri complessi
- numeri razionali
- interi mod p (primo)

l'insieme degli interi non è un campo in quanto $\frac{2}{3}$ non è un intero

ESEMPIO

$$GF(2^2) \equiv GF(4) = \{0, 1, X, X^2\}$$

$$GF(2^2) = \mathbb{Z}_2[X] \pmod{X^2+X+1}$$

Elementi E_1 0
E_2 1
E_3 X
E_4 $1+X=X^2$

$X \cdot X \equiv X^2 \equiv X+1 \pmod{X^2+X+1}$

leggi

(2)

1. $0+x=x$
2. $x+x=0$
3. $1\cdot x=x$
4. $1+x=x^2$
5. addizione moltiplicazione sono commutative e associative, vale la legge di distributività $x(y+z)=xy+xz$ $\forall x,y,z$

$GF(4)=\{0,1,x,1+x\}$

$x^3=x\cdot x^2=x(1+x)=x+x^2=x+1+x=1$

allora $x^2=x^{-1}$ cioè x^2 è il moltiplicativo inverso di x.

un campo è un insieme che contiene gli elementi 0 e 1 ($1 \neq 0$) e che soddisfa le

1. proprietà di addizione e moltiplicazione
   a. $0 + x = x$, $\forall x$
   b. $1 \cdot x = x$, $\forall x$
   c. commutative, associative e distributive

associative
$(a + b) + c = a + (b + c)$

commutativa
$a \times b = b \times a$

distributiva
$x(y+z) = xy + xz$
$(x+y)z = xz + yz$

2. esiste l'addittivo inverso
   $x + (-x) = 0$
3. esiste il moltiplicativo inverso
   $x \cdot x^{-1} = 1$

---

un campo è chiuso per sottrazione
$x - y = x + (-y)$

Insieme delle matrici con coefficienti reali (4)

$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $_{2\times 2}$ non è un campo

(1) moltiplicazione non commutativa

$A \cdot B \neq B \cdot A$

(2) $M^{-1} = ?$ se $\det M = 0$

Insieme dei numeri reali ≥ 0 non è un campo

$x \in R_{\geq 0}$

add OK
mult OK
divisione NO
sottrazione

$5 - 7 = (-2)$ $\quad -2 \notin R_{\geq 0}$

Per ogni potenza p^n (p primo e $n > 0$ intero) c'è un solo campo finito con esattamente p^n elementi.

Se $n > 1$ gli interi $\bmod p^n$ non sono un campo $\quad px \equiv 1 \pmod{p^n}$ non ha soluzione quindi non è un campo finito

$GF(p^n)$ non sono gli interi mod p^n, ma vanno costruiti diversamente.

$\mathbb{Z}_2[x]$ è l'insieme di tutti i polinomi

$$a(x) = \sum_{i=0}^{n-1} a_i x^i$$

polinomio monico se $a_{n-1} = 1$ x^{n-1}

di grado $n-1$ essendo n intero >0

essendo $a_i \in \mathbb{Z}_2 = \{0,1\}$

$\mathbb{Z}_2[x]\left(\text{mod } a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0\right)$ in genere $a_n = 1$ Polinomio monico

è un campo $GF(2^n)$

se e solo se il polinomio di grado n è irriducibile

es. $n=2$ polinomi $\mathbb{Z}_2[x]$ per $n=2$

grado 0 $\begin{cases} 0 \\ 1 \end{cases}$ non di grado $n-1$ gli elementi

grado 1 $\begin{cases} x \\ 1+x \end{cases}$

quelli di

grado 2 $\begin{cases} x^2 \longrightarrow x \cdot x \text{ riducibile} \\ (1+x^2) \rightarrow (1+x)(1+x) = 1+x^2 \text{ riduc} \\ x+x^2 \rightarrow x(1+x) \text{ riducibile} \\ 1+x+x^2 \quad \underline{\text{IRRIDUCIBILE}} \end{cases}$

Allora $GF(2^2) = \mathbb{Z}_2[x] \pmod{x^2+x+1}$

$\{0, 1, x, x+1\}$ sono i resti quando si divide il polinomio irriducibile x^2+x+1

addizione, sottrazione, moltiplicazione $\pmod{x^2+x+1}$

Irriducibile significa che il polinomio $r(x)$ (di grado n) $\Rightarrow r(x) \neq f(x)g(x)$ in $\mathbb{Z}_2[x]$ non si può fattorizzare con polinomi di grado inferiore $f(x)$ e $g(x)$ (di grado $1 \div n-1$.)

PROCEDURA

Campo finito con p^n elementi

p primo $n \geq 1$ intero

$\mathbb{Z}_p$ interi mod p.

1. $\mathbb{Z}_p[x]$ è l'insieme dei polinomi con coefficienti mod p
2. Scegli $r(x)$ polinomio irriducibile mod p di grado n
3. $GF(p^n)$ è $\mathbb{Z}_p[x]$ mod $r(x)$ è un campo a p^n elementi.

$r(x), f(x), g(x) \in \mathbb{Z}_2[x]$

ESEMPIO moltiplicazione inverso di

$a(x) = x^2 + 1$ in $GF(2^8) = \frac{\mathbb{Z}_2[x]}{(\text{mod } x^8 + x^4 + x^3 + x + 1)}$

$r_0 = m(x)$ $r_1 = a(x)$	Inizia una divisione	0 1
$x^8 + x^4 + x^3 + x + 1 = (x^6 + x^4 + x)(x^2 + 1) + 1$		$-(x^6 + x^4 + x) + 0 =$ $= x^6 + x^4 + x$

$a^{-1} = x^6 + x^4 + x$

infatti

$$(x^6 + x^4 + x)(x^2 + 1) \equiv x^8 + x^6 + x^3 + x^6 + x^4 + x \equiv$$

$$\equiv x^8 + x^4 + x^3 + x \equiv 1 \quad (\text{mod } x^8 + x^4 + x^3 + x + 1)$$

OK

$a(x) = x^2 + 1 \equiv 00000101 \equiv \{05\}_{hex}$

$a^{-1}(x) = x^6 + x^4 + x \equiv 01010010 = \{52\}_{hex}$

ESEMPIO

Verifichiamo l'ordine dell'elemento $(x+1)$ del campo $\mathbb{Z}_2[x]/(x^3+x+1)$.

L'ordine è $2^3-1=7$; infatti:

$$(x+1)^7 \bmod (x^3+x+1) = 1$$

Applichiamo S&M

	1, resto $(x+1)$
1	$1^2 \cdot (x+1) \equiv x+1$
1	$(x+1)^2(x+1) \equiv (x^2+1)(x+1)$ $\equiv x^3+x^2+x+1 \equiv x^2$ $\pmod{x^3+x+1}$
1	$(x^2)^2 \cdot (x+1) \equiv x^5+x^4 \equiv 1$

$$\begin{array}{r|l} & 1 \\ x^3+x+1 & x^3+x^2+x+1 \\ & x^3+x+1 \\ \hline & x^2 \end{array}$$

$$\begin{array}{r|l} & x^2+x+1 \\ x^3+x+1 & x^5+x^4 \\ & x^5+x^3+x^2 \\ \hline & x^4+x^3+x^2 \\ & x^4+x^2+x \\ \hline & x^3+x \\ & x^3+x+1 \\ \hline & 1 \end{array}$$

OK

Logaritmi discreti

$$b(x) = a(x)^{k} \pmod{r(x)}$$

noti $a(x)$ e $b(x)$ determinare k

es. in $GF(4)$ $\quad a(x) = x = \alpha(x)$

$$b(x) = 1$$

$$k = 3$$

$$x^3 \equiv 1 \pmod{x^2+x+1}$$

Fattorizzazione di polinomi

Indico con $\mathbb{Z}_p[x]$ l'insieme di tutti i possibili polinomi della variabile x

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1 x + a_0 = \sum_{i=0}^{n-1} a_i x^i$$

di grado $(n-1)$ essendo n intero >0.

se $a_{n-1} = 1$ POLINOMIO MONICO

Ogni polinomio di massimo grado $(n-1)$ è rappresentato dal vettore a n elementi

$$(a_{n-1}, a_{n-2}, \dots, a_1, a_0)$$

essendo i coefficienti

$$a_i \in \mathbb{Z}_p \; ; \; 0 \le a_i \le p-1$$

Il numero di polinomi di grado $(n-1)$ è

$$p^n$$

e cioè il modo di comporre il vettore a n elementi con elementi scelti tra p diversi.

Di grande importanza pratica è il caso $p=2$

$$\mathbb{Z}_2[x]$$

è l'insieme di tutti i polinomi con $a_i \in \mathbb{Z}_2 = (0,1)$

Tra polinomi $f(x) \in \mathbb{Z}_p[x]$

si definiscono le operazioni di

- addizione
- sottrazione
- moltiplicazione
- divisione

tenendo conto per la manipolazione dei coefficienti sempre operare modulo p.

Ad esempio $f(x) \in \mathbb{Z}_2[x]$

$f(x) = x^6 + x^3 + 1 \qquad g(x) \in \mathbb{Z}_2[x]$

$g(x) = x + 1$

$f(x) + g(x) = (x^6 + x^3 + x + 2) \bmod 2$

$= x^6 + x^3 + x \pmod 2$

$$\boxed{f(x) - g(x) = x^6 + x^3 + x = f(x) + g(x)}$$

si può fare con' grado max $= 6 = (n-1)$

$\deg\{f(x)\} = 6$

$\deg\{g(x)\} = 1$

Vediamo un esempio

$x^6 + x^3 + 1 \equiv 1001001$ EXOR ⊕

e poi

$x + 1 \equiv 0000011$

1001016

$1001010 \equiv x^6 + x^3 + x$

Prodotto

$$(x^3+x+1)(x+1) = (x^4+x^3+x^2+2x+1) \bmod 2$$
$$= x^4+x^3+x^2+1$$

Divisione

$$\frac{x^4+x^3+1}{x^2+x+1} = x^2+1+\frac{x}{x^2+x+1}$$

infatti

$$\begin{array}{r|l} & x^2+1 \\ \hline x^2+x+1 & x^4+x^3+1 \\ & x^4+x^3+x^2 \\ \hline & x^2+1 \\ & x^2+x+1 \\ \hline & x \end{array}$$

allora

$$\frac{f(x)}{r(x)} = q(x) + \frac{t(x)}{r(x)}$$

e cioè se $m(x) = x^2+x+1$, allora

$$f(x) = q(x)\, r(x) + t(x)$$

e cioè se $r(x)$ fosse una specie di polinomio modulo

$$t(x) = f(x) \bmod r(x)$$

nel caso di sopra

$$r(x) = x^2+x+1 = z(x)$$

$$f(x) = x^4+x^3+1$$

$$q(x) = x^2+1$$

$$t(x) = x = t(x)$$

allora

$$x^4+x^3+1 = (x^2+1)(x^2+x+1)+x$$

posso con perfetta analogia all'aritmetica modulare dei numeri interi sostituire che si può scrivere

$$x = (x^4+x^3+1) \bmod (x^2+x+1)$$

ovvero applicare la congruenza

$$x^4+x^3+1 \equiv x \pmod{x^2+x+1}$$

Si sostituiscono allora le operazioni nell'insieme di polinomi modulari

$$f(x) \in \frac{\mathbb{Z}}{2}[x] \pmod{x^2+x+1}$$

Rispetto al polinomio di secondo grado $n=2$

$$x^2+x+1$$

l'insieme

$$\mathbb{Z}_2[x]^{(\text{mod } x^2+x+1)}$$

è fatto dai 4 polinomi di grado $\max = 1$ $(n-1=1)$

$$(0;\ 1;\ x;\ x+1)$$

e questo un "campo finito" e cioè posso definire i moltiplicatori inversi per tutti gli elementi non nulli, se e solo se, il polinomio modulo x^2+x+1 di grado $n=2$

è IRRIDUCIBILE (equivalente di "primo") e cioè non risulta composto dal prodotto di polinomi di grado inferiore, al massimo $n-1 (=1$ in questo caso $n=2)$.

Per esempio $x^2+1 \equiv (x+1)(x+1)$

è RIDUCIBILE in $\mathbb{Z}_2[x]$, in quanto

$$(X+1)(X+1) = (X^2+2X+1) \bmod 2 = X^2+1$$

invece

$\Sigma(X) = X^2+X+1$ è IRRIDUCIBILE IN $\mathbb{Z}_2[X]$.

allora consideriamo il campo finito

$$GF(p) = \mathbb{Z}_p[X] \bmod \Sigma(X)$$

essendo $\Sigma(X)$ irriducibile in $\mathbb{Z}_p[X]$ e i suoi elementi.

Ci rimane da verificare come si fa la moltiplicazione tra due polinomi $g(X)$ e $f(X)$ di grado minore $n-1$, essendo $\Sigma(X)$ di grado n, nel campo finito.

Ad es. $g(X), f(X) \in \mathbb{Z}_2[X] \bmod (X^2+X+1)$

Prendiamo ad esempio $g(X)=X$ e $f(X)=X$, cioè $X \cdot X = X+1$

Infatti: $X \cdot X = X^2$, allora $X^2 \bmod (X^2+X+1) = X+1$, infatti

$$x^2+x+1 \;\big|\; x^2 \qquad 1$$
$$x^2+x+1$$
$$x+1$$

Quindi

$$x^3 \equiv x \cdot x^2 \equiv x \cdot (x+1) \equiv x^2+1 \equiv 1 \pmod{x^2+x+1}$$

infatti

$$x^2+x+1 \;\big|\; x^3 \qquad x+1$$
$$x^3+x^2+x$$
$$x^2+x$$
$$x^2+x+1$$
$$1$$

quindi $x \cdot x^2 \equiv 1$

$$x^2 \equiv x^{-1} \pmod{x^2+x+1}$$

$$GF(2^8) \equiv \mathbb{Z}_2[x] \bmod (x^8+x^4+x^3+x+1)$$

$x(x) = x^8+x^4+x^3+x+1$ è "primo" in $\mathbb{Z}_2[x]$

Polinomi $\in GF(2^8)$ sono 256 polinomi di grado max 7

esempio $x^7+x^6+x^3+x+1$ polinomio

11001011 byte

trovare l'inverso. Per prima calcolare

$$mcd(x^7+x^6+x^3+x+1,\ x^8+x^4+x^3+x+1) = 1$$

in quanto $x^8+x^4+x^3+x+1$ è irriducibile: primo

Divido

$$\begin{array}{r|l} x^7+x^6+x^3+x+1 & x+1 \\ \hline x^8+x^4+x^3+x+1 & \\ x^8+x^7+x^4+x^2+x & \\ \hline x^7+x^3+x^2+1 & \\ x^7+x^6+x^3+x+1 & \\ \hline x^6+x^2+x & \end{array}$$

Poi faccio

$$x^6+x^2+x \;\big|\; x^7+x^6+x^3+x+1 \quad (x+1)$$

$$x^7+x^3+x^2$$

$$x^6+x^2+x+1$$

$$x^6+x^2+x$$

$$1$$

STOP

Allora

$r_0 = r(x) = x^8+x^4+x^3+x+1$

$r_1 = a(x) = x^7+x^6+x^3+x+1$

$q_1 = x+1$

$r_2 = x^6+x^2+x$

$q_2 = x+1$

$r_3 = 1$ STOP.

$3 = MAX$

$t_0 = 0 \; ; \; t_1 = 1$

$t_2 = t_0 - q_1 t_1$

$t_3 = t_1 - q_2 t_2$

$t_3 = a^{-1}$

$$t_2 = 0 - (x+1)\cdot 1 = x+1$$

$$t_3 = 1 - (x+1)(x+1) = x^2+x+1+1 = x^2 = a^{-1}$$

$$a^{-1}(x) = x^2$$

Infatti

$$x^2 \cdot (x^7+x^6+x^3+x+1) = x^9+x^8+x^5+x^3+x^2 = 1 \pmod{x^8+x^4+x^3+x+1}$$

ict CONSULTING

10

$$
\begin{array}{r|l}
x^8+x^4+x^3+x+1 & x+1 \\
\cline{2-2}
x^9+x^8+x^5+x^3+x^2 & \\
x^9+x^5+x^4+x^2+x & \\
\cline{1-1}
x^8+x^4+x^3+x & \\
x^8+x^4+x^3+x+1 & \\
\cline{1-1}
1 & \\
\cline{1-1}
\end{array}
$$

0 ↑

ict CONSULTING

ESISTENZA DI CAMPI FINITI $GF(p^n)$

in $\mathbb{Z}_p[x]$ c'è almeno 1 polinomio irriducibile per ogni grado $n \geq 1$

Quindi c'è un campo finito con p^n elementi per tutti i primi p e tutti gli interi $n \geq 1$.

Per ogni grado n e primo p c'è almeno un polinomio irriducibile di grado n e c'è almeno un campo finito di p^n elementi. A più polinomi irriducibili dello stesso grado corrispondono più campi finiti tutti ISOMORFI tra loro. Quindi c'è un solo campo finito di grado p^n detto

$$GF(p^n)$$

Se $n=1$

$$\mathbb{Z}_p \equiv GF(p)$$

Non esistono campi finiti con k elementi se $k \neq p^n$.

Il gruppo $\mathbb{Z}_p^*$ moltiplicativo contiene elementi che sono tutti il loro inverso ed è un gruppo ciclico di ordine $p-1$

In pratica di studiamo

$$GF(2^n) \; n \geq 1$$

Cerchiamo

$n=3$ $GF(2^3)$ la cardinalità del gruppo è $2^3 = 8$ 8 elementi

Partiamo da $\mathbb{Z}_2$ il campo dei coefficienti e da $\mathbb{Z}_2[x]$ = l'insieme di tutti i polinomi di qualsiasi grado $n \geq 1$ con coefficienti $\in \mathbb{Z}_2 = \{0, 1\}$

cerchiamo un polinomio irriducibile in $\mathbb{Z}_2[x]$ di grado massimo $n=3$.

$$f(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0$$

ove $a_i \in \mathbb{Z}_2 \ \forall i$ (sono 16 differenti polinomi)

Per essere irriducibile, deve essere $a_0 = 1$, perché se $a_0 = 0$ allora $f(x)$ si può dividere per x e quindi è riducibile.

Dei 8 quindi sono 4 i polinomi da considerare

(8 sono i polinomi con grado massimo $= 3$, con $a_3 \neq 0$)

$$\begin{cases} f_1(x) = x^3 + 1 \\ f_2(x) = x^3 + x^2 + 1 \\ f_3(x) = x^3 + x^2 + 1 \\ f_4(x) = x^3 + x^2 + x + 1 \end{cases}$$

ora $f_1(x)$ è riducibile, infatti:

$$(x^3+1) = (x+1)(x^2+x+1)$$

TUTTI I COEFFICIENTI SI RIDUCONO MOD 2! $(2x \equiv 0)$

$f_4(x)$ è riducibile, infatti

$$x^3+x^2+x+1 = (x+1)(x^2+1)$$

TUTTAVIA $f_2(x)$ e $f_3(x)$ sono IRRIDUCIBILI

$$f_2(x) = x^3 + x + 1$$

$$f_3(x) = x^3 + x^2 + 1$$

scegliamo uno dei due per costruire

polinomio irriducibile

usiamo $f_2(x) = x^3+x+1 = p(x)$ anche modulo del polinomio

e costruiamo

$$GF(2^3) \equiv \mathbb{Z}_2[x] \,/\, (x^3+x+1).$$

Gli otto elementi sono tutti i polinomi di massimo grado $(n-1)=2$ e cioè

	a_2	a_1	a_0	elemento
0	0	0	0	0
1	0	0	1	1
x	0	1	0	2
$x+1$	0	1	1	3
x^2	1	0	0	4
x^2+1	1	0	1	5
x^2+x	1	1	0	6
x^2+x+1	1	1	1	7

Per fare la somma di due elementi basta fare EXOR $\equiv \oplus$

$$\begin{array}{lccc} (\text{elemento } 3) + (\text{elemento } 6) = & 0 & 1 & 1 \\ & 1 & 1 & 0 \\ \hline (\text{elemento } 5) & 1 & 0 & 1 \end{array} \quad \oplus$$

e così $(x+1)+(x^2+x)=x^2+1$ usando le mod mod 2. $2x \equiv 0$

$E3+E6=E5$

Il prodotto $E5 \times E7$

$$(x^2+1)(x^2+x+1) = x^4+x^3+x^2+x^2+x+1 =$$

Poiché $f(x) \bmod (x^3+x+1) = f(x) \bmod (x^3+x+1)$

$f(x)=x^4+x^3+x+1$.

$$\frac{x^4+x^3+x+1}{x^3+x+1} =$$

$$\begin{array}{r|l} x^4+x^3+x+1 & x^3+x+1 \\ \hline x^4+x^2+x & x+1 \\ \hline x^3+x^2+1 & \\ x^3+x+1 & \\ \hline x^2+x & \end{array}$$

cioè

$$x^4+x^3+x+1 = (x+1)(x^3+x+1)+x^2+x$$

e quindi in $\mathbb{Z}_2[x]/(x^3+x+1)$ si ha

$$(x^2+1)(x^2+x+1)$$

$$\equiv x^2+x = E6 \pmod{p(x)}$$

$$E5 \times E7 = E6$$

ict CONSULTING

$p = 7 = 2^n - 1 = 2^3 - 1$

Il gruppo moltiplicativo dei polinomi non di grado 0 è un gruppo ciclico di ordine 7, poiché 7 è primo, tutti gli elementi tranne elementi minimi del gruppo

per esempio l'elemento x

$$x^1 \equiv x$$
$$x^2 \equiv x^2$$
$$x^3 \equiv x+1 \quad \bmod x^3+x+1$$
$$x^4 \equiv x^2+x$$
$$x^5 \equiv x^2+x+1$$
$$x^6 \equiv x^2+1$$
$$x^7 \equiv 1$$

tutti i vari elementi escluso lo zero

Infatti

$$x \bmod x^3+x+1 = x$$

$$\frac{x}{x^3+x+1} \equiv x$$

$$\frac{x^2}{x^3+x+1} \equiv x^2$$

$$x^2 \bmod x^3+x+1 = x^2$$

ict CONSULTING (17)

$$\frac{x^3}{x^3+x+1} \equiv x+1$$

infatti

$$x^3 \,/\, x^3+x+1 \;\;\Big|\; 1$$
$$\underline{x^3}$$
$$x+1$$

e poi

$$x \cdot x^3 = x^4 =$$
$$= x \cdot (x+1) = x^2+x$$
$$x^4 \equiv x^2+x$$

e poi

$$x \cdot x^4 = x^5 =$$
$$= x(x^2+x) = x^3+x^2$$
$$x^5 = x^3+x^2 =$$
$$= x^3+x^2 \,/\, x^3+x+1 \;\;\Big|\; 1$$
$$\underline{x^3+x^2}$$
$$x^2+x+1$$

$$x^5 \equiv x^2+x+1$$

$$x \cdot x^5 = x^6 =$$
$$= x(x^2+x+1) = x^3+x^2+x$$

$$x^3+x^2+x \,/\, x^3+x+1 \;\;\Big|\; 1$$
$$\underline{x^3+x^2+x}$$
$$x^2+1$$

$$x^5 = x^2+1$$

$$x^7 = x(x^2+1) = x^3+x = \quad x^3+x \,/\, x^3+x+1 \;\;\Big|\; 1$$
$$\underline{x^3+x}$$
$$1$$

$$\equiv 1.$$ STOP

Campo finito $GF(2^3)$

$$\mathbb{Z}_2[x] / (x^3+x+1) \pmod{\quad}$$

MOLTIPLICATORI INVERSI

	W	W^{-1}
000	0	—
001	1	1
010	2	→ 5
011	3	6
100	4	7
101	5	← 2
110	6	3
111	7	4

$E2 \equiv x \equiv W$

$E5 \equiv x^2+1 \equiv W^{-1}$

EUCLIDE ESTESO

$mcd(x, x^3+x+1)$

$a(x) = x^3+x+1$

$a(x) = x$

ricerca di $a^{-1}(x)$ tale che

$$a^{-1}(x) \cdot a(x) \equiv 1 \pmod{x^3+x+1}$$

$r_0 = a(x)$

$r_1 = a(x)$

$r_0 = r_1 q_1 + r_2$

$$\begin{array}{r|l} & x^2 \\ \hline x & x^3+x+1 \\ & x^3 \\ \hline & x+1 \end{array}$$

$q_1(x) = x^2$

$r_2(x) = x+1$

$r_1 = r_2 q_2 + r_3$

$$\begin{array}{r|l} & 1 \\ \hline x+1 & x \\ & x+1 \\ \hline & 1 \end{array}$$

$q_2(x) = 1$

$r_3(x) = 1$ STOP.

$a^{-1}(x) = x^2+1$

$t_0 = 0 \; ; \; t_1 = 1$

$t_2 = t_0 - q_1 t_1 =$

$= 0 - x^2 = x^2$

$t_3 = t_1 - q_2 t_2 =$

$= 1 - 1 \cdot x^2 = x^2+1 =$

$= a^{-1}(x)$

Altro esempio

$m(x) = x^3 + x + 1$

$a(x) = x + 1$

$a^{-1}(x) = ?$

$r_0 = m(x)$

$r_1 = a(x)$

$q_1 = x^2 + x$

$r_2 = 1$. STOP

$$\begin{array}{r|l} & x^2+x \\ \hline x+1 & x^3+x+1 \\ & x^3+x^2 \\ \hline & x^2+x+1 \\ & x^2+x \\ \hline & 1 \end{array}$$

$t_0 = 0$

$t_1 = 1$

$t_2 = t_0 - q_1 t_1 =$

$= 0 - (x^2+x) \cdot 1 = x^2 + x$

$a^{-1} = x^2 + x$

Infatti

$1 \cdot a^{-1} \equiv 1 \pmod{x^3+x+1}$

$(x+1)(x^2+x) = x^3 + x^2 + x^2 + x =$

$= x^3 + x$

$(x^3+x) \bmod (x^3+x+1) = 1$ c.v.d.

$$\begin{array}{r|l} & 1 \\ \hline x^3+x & x^3+x+1 \\ & x^3+x \\ \hline & 1 \end{array}$$

ESEMPIO

$GF(2^8) \equiv \mathbb{Z}_2[x] / (x^8 + x^4 + x^3 + x + 1)$ mod

$a(x) = x^2 + 1$

$r_0 = a(x)$

$r_1 = a(x)$

$t_2 = t_0 - q_1 t_1$

$t_0 = 0, \; t_1 = 1$

$q_1 = x^6 + x^4 + x$

$$
\begin{array}{r|l}
x^8 + x^4 + x^3 + x + 1 & x^2 + 1 \\
\hline
x^8 + x^6 & x^6 + x^4 + x \\
\hline
x^6 + x^4 + x^3 + x + 1 & \\
x^6 + x^4 & \\
\hline
x^3 + x + 1 & \\
x^3 + x & \\
\hline
1 &
\end{array}
$$

$$t_2 = 0 - (x^6 + x^4 + x) = x^6 + x^4 + x = a^{-1}$$

$a(x) = x^2 + 1 \equiv 00000101 = \{05\}_{hex}$

$a^{-1}(x) = x^6 + x^4 + x \equiv 01010010 = \{52\}_{hex}$

ALTRO INVERSO → $\mathbb{Z}_2[x]/(x^8+x^4+x^3+x+1)$ mod

$a(x) = x^2+x+1$

$a^{-1}(x)$?

$r_0 = a(x)$

$r_1 = q(x)$

$q_1 = x^6+x^5+x^3$

$r_2 = x+1$

$q_2 = x$

$r_3 = 1$. STOP $3 = MAX$

$$x^2+x+1 \;\big|\; x^8+x^4+x^3+x+1 \quad \Big|\; x^6+x^5+x^3$$

$x^8+x^7+x^6$

$x^7+x^6+x^4+x^3+x+1$

$x^7+x^6+x^5$

$x^5+x^4+x^3+x+1$

$x^5+x^4+x^3$

$x+1$

$$x+1 \;\big|\; x^2+x+1 \quad \Big|\; x$$

x^2+x

1

$t_0 = 0$, $t_1 = 1$

$t_2 = t_0 - q_1 t_1 = 0-(x^6+x^5+x^3) = x^6+x^5+x^3$

$t_3 = t_1 - q_2 t_2 =$

$= 1-(x)(x^6+x^5+x^3) = x^7+x^6+x^4+1 = q^{-1}$

Infatti

$(x^7+x^6+x^4+1)(x^2+x+1) =$

$x^9+x^8+x^6+x^2+x^8+x^7+x^5+x+x^7+x^6+x^4+1 =$

$= x^9+x^5+x^4+x^2+x+1$

$$x^8+x^4+x^3+x+1 \;\big|\; x^9+x^5+x^4+x^2+x+1 \quad \Big|\; x$$

$x^9+x^5+x^4+x^2+x$

1. c.v.d.

Moltiplicazione in $\mathbb{Z}_2[x]/(x^8+x^4+x^3+x+1)$

$m(x) = x^8+x^4+x^3+x+1 \equiv$

$\equiv 100011011$ [9 BIT]

Moltiplichiamo 11001011 [8B]

$(x^7+x^6+x^3+x+1)\ m(x) =$

$= x^8+x^7+x^4+x^3+x =$

$= (x^7+x^3+x^2+1) + (x^8+x^4+x^3+x+1)$

$\equiv (x^7+x^3+x^2+1) \bmod (x^8+x^4+x^3+x+1)$

[8 BIT]

11001011 → SHIF LEFT & APPEND A "0"

FINESTRA A 8 BIT

→ 110010110 (9 BITS)

→ SUBTRACT $x^8+x^4+x^3+x+1$

→ 110010110 ⊕

100011011

010001101

$(x^7+x^3+x^2+1)$

- QUINDI L'ALGORITMO GF(2^8) PER LA MOLTIPLICAZIONE PER X, E'

1. Sposta gli 8 bit di una posizione a sinistra e aggiungi uno '0' come ultimo bit
2. Se il primo bit è 0, STOP.
3. Se il primo bit è 1, XOR 100011011

- PER X^3 si fa tre volte. PER X^n si fa n volte
- PER UN POLINOMIO

ad es: $X^h + X^k + X^j$ $\quad h>k>j$

si fa prima h volte e si ottiene il primo termine
poi fa ancora k " " " secondo "
e infine si fa j " " " terzo termine.
e infine si fa EXOR ⊕ dei 3 termini

$GF(2^8)$ $\qquad x^8+x^4+x^3+x+1 = z(x)$

(1) $\quad x^8 \bmod z(x) = [z(x) - x^8] = x^4+x^3+x+1$

$GF(2^n)$ $x^n \bmod z(x) = [z(x) - x^n]$

$$f(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

$$x \cdot f(x) \equiv (b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \pmod{z(x)}$$

se $b_7 = 0$ allora
il polinomio è di grado 7 ed è già
un elemento appartenente al campo

Se $b_7 = 1$ allora si deve applicare la (1)

$$x \cdot f(x) \equiv (b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0) + (x^4+x^3+x+1)$$

la MOLTIPLICAZIONE PER X È UNO SCORRIMENTO A SINISTRA DI UN BIT SEGUITO DA XOR CON (00011011) che rappresenta (x^4+x^3+x+1)

$X \equiv (0000\,0010) = \{02\}$

$f(X) \equiv (b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0)$

$$X \bullet f(X) = \begin{cases} b_6 b_5 b_4 b_3 b_2 b_1 b_0 0 & (\text{se } b_7 = 0) \\ (b_6 b_5 b_4 b_3 b_2 b_1 b_0 0) \oplus (0\,0\,0\,1\,1\,0\,1\,1) & (\text{se } b_7 = 1) \end{cases}$$

SHIFT LEFT AND APPEND '0'

$\{02\} \bullet \{87\}$ $\quad \{87\} \equiv (1000\,0111) \quad b_7 = 1$

0000 1110 SHIFT LEFT

$\oplus$ 0001 1011

0001 0101

$\{03\} \bullet \{6E\} = \{6E\} \oplus (\{02\} \bullet \{6E\})$

$\{6E\} \equiv (0\,110\,1110)$

$\{03\} = 0000\,0011 = X + 1$

$\{03\} \bullet \{6E\} = (\{02\} \bullet \{6E\}) \oplus (\{6E\})$

$\{02\} \bullet \{6E\} = 1101\,1100 \quad b_7 = 0$

$\oplus$ 0110 1110 $\{6E\}$

1011 0010

ESEMPIO

$f(x) = x^6 + x^4 + x^2 + x + 1$

$g(x) = x^7 + x + 1$

$P(x) = x^8 + x^4 + x^2 + x + 1$

$f(x) \cdot g(x) \equiv x^7 + x^6 + 1 \pmod{P(x)}$

$f(x) = 01010111$

$g(x) = 10000011$

ESEGUO LE MOLTIPLICAZIONI PER X DI $f(x)$

$f(x) \cdot x = m_1(x)$

① $(01010111) \cdot (00000010) = \boxed{10101110}$

infatti $b_7 = 0 \rightarrow \underline{10101110}$ $f(x)$ shift left 1

$f(x) \cdot x^2$

② $(01010111) \cdot (00000100) = 01000111$

$x f(x)$ SL

$01011100 \oplus$

00011011

01000111

$x^2 f(x)$ SL

③ $(01010111) \cdot (00001000) = 10001110$ x^3

④ $(01010111) \cdot (00010000) =$ x^4

$$= \begin{array}{r} 00011100 \\ 00011011 \\ \hline 00000111 \end{array} \oplus$$

(5) $(01010111) \bullet (00010000) = 00001110$ $\quad \times 5$

(6) $(01010111) \bullet (01000000) = 00011100$ $\quad \times 6$

(7) $(01010111) \bullet (10000000) = \boxed{00111000}$ $\quad \times 7$

Perciò

$(01010111) \bullet (10000011) =$

$(01010111) \bullet [(00000001) \oplus (00000010) \oplus (10000000)] =$

$= (01) \otimes (1) \otimes (7) = (01010111) \oplus (10101110) \oplus (00111000) =$

$= 11000001 \equiv x^7 + x^6 + 1$

OK