Campi Finiti

Nomenclatura

$$a(x)=\sum_{i=0}^{n-1} a_i x^i \in \mathbb{Z}_p[x] \left(\mathrm{mod}\ r(x)=\sum_{i=0}^{n} r_i x^i\right)$$

$$GF(p^n)\equiv \mathbb{Z}_p[x]\ \mathrm{mod}\ r(x)$$

ove $a_i, r_i \in \mathbb{Z}_p$

- elementi del campo finito

$a(x)$ = polinomi di grado fino a $(n-1)$

- polinomi irriducibili (primi)

$r(x)$ = polinomi di grado n

non sono fattorizzabili in polinomi di grado inferiore in $\mathbb{Z}_p[x]$, per cui risulta

per $a(x) \neq 0$ $\quad \mathrm{mcd}(a(x), r(x)) = 1$

per $\forall a(x) \in GF(p^n) \equiv \mathbb{Z}_p[x]\ \mathrm{mod}\ r(x)$

- polinomi primitivi

alcuni $r(x)$ di grado n sono anche "primitivi"

$$p(x)=\sum_{i=0}^{n} p_i x^i \quad (p_i \in \mathbb{Z}_p)$$

i polinomi primitivi $p(x)$ di grado n sono polinomi irriducibili in $\mathbb{Z}_p[x]$ le cui n radici ottenibili come

$$p(x)=0\,,\ \text{per } x=\alpha(x) \text{ in } GF(p^n) \pmod{z(x)}$$

- sono "radici primitive"

$$\alpha(x)\in GF(p^n) \pmod{z(x)} \ :\ \alpha(x)=\sum_{i=0}^{n-1} a_i x^i \qquad a_i\in\mathbb{Z}_p$$

$\left\{\begin{array}{l}\alpha(x)\neq 0\\ \alpha(x)\neq 1\end{array}\right.$ sono elementi del campo finito "generatori" per cui

$$\left\{\alpha^k(x) \ :\ 1\le k\le p^n-1\right\}\equiv GF^*(p^n) \pmod{z(x)}$$

le potenze $\alpha^k(x)$ generano tutti gli elementi del campo (tranne lo zero). L'ordine dei polinomi generatori = radici primitive, e cioè il più piccolo esponente intero per cui $\alpha^k(x)\equiv 1 \pmod{z(x)}$, risulta $k=p^n-1$, cioè

$$\alpha^{p^n-1}(x)\equiv 1 \pmod{z(x)}$$

NOTA

Nel TRAPPE in $\mathbb{Z}_p^*$ $\alpha\leftrightarrow g$

in $GF^*(p^n)$ $\alpha(x)\leftrightarrow g(x)$

In conclusione, nel campo finito $GF(p^n)$ - definito in $\mathbb{Z}_p[x] \bmod r(x)$ ci sono

$a(x)$ - Numero degli elementi del campo $= p^n$ (elementi non zero $= p^n-1$), di grado fino a $(n-1)$

$r(x)$ - Numero dei polinomi irriducibili, di grado n

$$N_r(p,n)=\frac{1}{n}\sum_{\substack{i=1\\ i|n}}^{n}\mu\left(\frac{n}{i}\right)p^i$$

μ = funzione di Moebius

$p(x)$ - Numero dei polinomi primitivi, di grado n

$$N_p(p,n)=\frac{\phi(p^n-1)}{n}$$

$\alpha(x)$ - Numero delle radici primitive, di grado (fino a $(n-1)$)

$$N_\alpha(p,n)=\phi(p^n-1)$$

- Risulta che

$$\alpha(x)^{p^n-1}\equiv 1 \pmod{r(x)}$$

essendo p^n-1 l'"ordine" dell'elemento primitivo (minimo esponente di α per cui $\alpha^k\equiv 1 \pmod{r x}$).

- Mentre per tutti gli altri elementi $a(x)\neq\alpha(x)$ si ha:

Fermat nei campi di ordine p^n

$$a(x)^{p^n-1}\equiv 1 \pmod{r(x)}$$

esistendo certi valori $k < p^n-1$ per cui $a(x)^k\equiv 1 \pmod{r(x)}$ con k sottomultiplo di p^n-1 (essendo $mcd(a(x), r(x))=1$)

il numero di polinomi irriducibili di grado n in $\mathbb{Z}_p[x]$ è dato da

$$N_{\mathbb{I}}(p,n) = \frac{1}{n} \sum_{\substack{i=1 \\ i|n}}^{n} \mu\left(\frac{n}{i}\right) p^i$$

essendo $i|n$ gli indici interi che dividono n, e cioè tali che $\frac{n}{i} = k$, intero >0 e ove

Funzione di MOEBIUS ≡ ≡ MÖBIUS

$$\mu(n) = \begin{cases} = 0 & \text{se } n \text{ è composto da primi ripetuti} \\ = 1 & \text{se } n = 1 \\ = (-1)^k & \text{se } n \text{ è prodotto di } k \text{ primi distinti} \end{cases}$$

Per esempio $p=2$, $n=6$

Allora $i|n$ per $i = 1, 2, 3$ e 6, mentre per $i=4 \rightarrow \frac{n}{i} = \frac{6}{4} = \frac{3}{2}$ e per $i = 5 \rightarrow \frac{n}{i} = \frac{6}{5}$.

Quindi

$$N_{\mathbb{I}}(2,6) = \frac{1}{6}\left(2 - 2^2 - 2^3 + 2^6\right) = \frac{54}{6} = 9$$

infatti

$\mu\left(\frac{6}{6}\right) = \mu(1) = 1$ $\mu\left(\frac{6}{2}\right) = \mu(3) = -1$ $(k=1)$

$\mu\left(\frac{6}{3}\right) = \mu(2) = -1$ $(k=1)$ $\mu\left(\frac{6}{1}\right) = \mu(6) = 1$ $(k=2)$

FUNZIONE DI MOEBIUS

$\mu(n)$

n intero > 0

n	$\prod p_i$	k	$\mu(n)$
1	—	—	1
2	2	1	−1
3	3	1	−1
4	2x2	—	0
5	5	1	−1
6	2x3	2	+1
7	7	1	−1
8	2x2x2	—	0
9	3x3	—	0
10	2x5	2	+1
11	11	1	−1
12	3x2x2	—	0
13	13	1	−1
14	2x7	2	+1
15	3x5	2	+1
16	2x2x2x2	—	0
17	17	1	−1
18	2x3x3	—	0
19	19	1	−1
20	2x2x5	—	0
21	3x7	2	+1
22	11x2	2	+1
23	23	1	−1
24	3x2x2x2	—	0
25	5x5	—	0

FUNZIONE DI MERTENS

$$M(m) = \sum_{n \leq m} \mu(n)$$

m intero > 0

tabella riassuntiva $GF(2^n)$ $(p=2)$

n	POLINOMI PRIMITIVI $N_p(2,n)$	POLINOMI IRRIDUCIBILI $N_r(2,n)$	ELEMENTI PRIMITIVI $N_\alpha(2,n)$	ELEMENTI NON-ZERO 2^n-1	
1	1	2	1	1	
2	1	1	2	3	← PRIMO
3	2	2	6	7	← PRIMO
4	2	3	8	15	
5	6	6	30	31	← PRIMO
6	6	9	36	63	
7	18	18	126	127	← PRIMO
8	16	30	128	255	
9	48	56	432	511	
10	60	99	600	1023	
11	176	186	1936	2047	
12	144	335	1728	4095	

a parità di n: $N_p \leq N_r \leq N_\alpha$

Per ogni intero positivo n c'è sempre un polinomio primitivo di grado n su $\mathbb{Z}_p[X]$

Tutte le n radici primitive del polinomio primitivo $p(X)$ (valori $X=\alpha(X)$ per cui $p(X)=0$) sono elementi/polinomi generatori del campo finito $GF(p^n)=\mathbb{Z}_p[X] \bmod r(x)$.

Tutti i polinomi primitivi $p(X)$ di grado n su $\mathbb{Z}_p[x]$ sono irriducibili, mentre non tutti i polinomi irriducibili $r(x)$ sono anche primitivi. Le n radici primitive sono "diverse" in quanto $p(x)$ è irriducibile.

Il numero delle radici primitive $\alpha(X)$

$\alpha(X) \in GF^*(p^n)$ è

$$N_\alpha(p,n) = \phi(p^n - 1)$$

essendo $\phi(\cdot)$ la funzione di Eulero.

La dimostrazione è analoga a quella usata per calcolare il numero di radici primitive α su $\mathbb{Z}_p^*$: $N_\alpha(p) = \phi(p-1)$.

Se $\alpha(X)$ è un polinomio generatore del campo finito, allora

$$\{\alpha^i : 1 \leq i \leq p^n - 1\} \equiv GF^*(p^n)$$

$$(\bmod\ r(x))$$

Allora ogni elemento del campo $\beta(x) \in GF^*(p^n)$ si può esprimere come

$$\beta(x) \equiv \alpha^k(x) \quad \text{per } 1 \le k \le p^n-1$$
$$(\mathrm{mod}\ r(x)]$$

Sappiamo che l'ordine di $\alpha(x)$ è p^n-1

$$\alpha(x)^{p^n-1} \equiv 1 \quad \mathrm{mod}\ r(x)$$

mentre l'ordine di $\beta(x)$ è in generale

$$\beta(x)^{\frac{p^n-1}{\mathrm{mcd}(p^n-1,\, k)}} \equiv 1 \quad \mathrm{mod}\ r(x)$$

quindi β ha ordine uguale a p^n-1, se e solo se

(1) $\mathrm{mcd}(p^n-1, k)=1$, e cioè se $k \perp p^n-1$, in questo caso anche $\beta(x)$ è primitivo

Quindi le radici primitive sono tutte quelle per cui vale la (1), appunto

$$N_\alpha(p,n)=\phi(p^n-1).$$ c.v.d.

Una volta trovato il numero delle radici primitive del campo il numero dei polinomi primitivi in $\mathbb{Z}_p[x]$ è

$$N_p(p,n) = \frac{\phi(p^n-1)}{n}$$

in quanto ciascun polinomio primitivo $p(x)$ ha n radici <u>tutte diverse</u> in quanto irriducibile.

Per verificare che $\alpha(x)$ è radice primitiva valgono le stesse regole del caso $\mathbb{Z}_p$.

Posto $\quad p^n-1 = \prod_{i=1}^{m} q_i \quad q_i$ primi

allora $\alpha(x)$ è elemento primitivo del campo $GF(p^n)$, se e solo se

$$\alpha^{\frac{p^n-1}{q_i}} \not\equiv 1 \left(\bmod r(x)\right), \forall i$$

per tutti gli indici i $\quad 1 \le i \le m$

<u>Esempio</u> $GF(2^2)$; $r(x)=x^2+x+1$

$2^2-1=3=q \qquad x$ è elemento primitivo?

$x^1 \equiv x \not\equiv 1$ OK sì

ovviamente risulta $\quad x^{2^2-1} \equiv x^3 \equiv 1 \mod r(x)$

Esempio

$GF(2^3)$, $r(x) = x^2+x+1$

x è radice primitiva? $\qquad 2^3-1 = 7 = q$

$x^1 \equiv x \not\equiv 1$ ok sì

e risulta $\quad x^7 \equiv 1 \mod r(x)$

Esempio

$GF(2^4)$, $r(x) = x^4+x+1 \qquad 2^4-1 = 15 = 3\times 5$

x è radice primitiva?

$$\begin{cases} x^5 \equiv x^2+1 \not\equiv 1 \\ x^3 \equiv x^3 \not\equiv 1 \end{cases} \pmod{x^4+x+1}$$

ok!

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

e risulta $\quad x^{15} \equiv 1 \pmod{x^4+x+1}$

Se $p^n-1 = q$ primo, allora <u>TUTTI</u> gli elementi del campo $GF(p^n)$, <u>esclusi 0 e 1</u>, sono radici primitive = polinomi generatori

Infatti $\quad N_\alpha(p,n) = \phi(q) = q-1 = p^n-2$

$GF(p^n)$ è un "gruppo del primo ordine"

ESEMPIO

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

essendo x^2+x+1 polinomio irriducibile di grado 2. con due radici. Infatti $x^2+x+1=0$ in $\mathbb{Z}_2[x]$

$$GF(2^2)\begin{cases} E1=0 & 00 \\ E2=1 & 01 \\ E3=x & 10 \\ E4=x+1 & 11 \end{cases}$$

- per $x=x$ (E3) $\alpha_1(x)=x$ infatti sostituendo e tenendo conto che $x^2 \equiv x+1\ (\text{mod } x^2+x+1)$ si ha $(x+1)+x+1=0$.

- per $x=x+1$ (E4) $\alpha_2(x)=x+1$ infatti, poiché $x^2=(x+1)(x+1)=x^2+1=x\ (\text{mod } x^2+x+1)$ per cui $x+(x+1)+1=0$.

x è sempre radice primitiva dei campi $GF(p^n)$

Risulta

$$x^1 \equiv x \quad (E3)$$
$$x^2 \equiv x+1 \quad (E4)$$
$$x^3 \equiv 1 \quad (E2)$$

x genera 2^2-1 elementi del campo

$$x^K \quad 1 \leq K \leq 3 \quad (\text{mod } x^2+x+1)$$

Esempio

$\mathbb{F}_{2^3} = GF(2^3) = \mathbb{Z}_2[x] \; (\mathrm{mod}\; x^3+x+1)$ $\quad n=3$

000

$x^1 = E1 \rightarrow x$ 010

$x^2 = E2 \rightarrow x^2$ 100

$x^3 = E3 \rightarrow x+\underline{1}$ 011

$x^4 = E4 \rightarrow x^2+x$ 110

$x^5 = E5 \rightarrow x^2+x+1$ 111

$x^6 = E6 \rightarrow x^2+1$ 101

$x^7 = E7 \rightarrow 1$ 001

$p_1(x) = x^3+x+1$ è irriducibile e primitivo

ha infatti tre radici in $GF(2^3)$ che sono

$$\begin{cases} E1 = x \; ; \; E2 = x^2 \; ; \; E_4 = x^2+x \end{cases}$$

infatti, • per $\underline{x \equiv E1 = x = \alpha_1(x)}$

si ha

$$x^3 \equiv x+1 \quad (\mathrm{mod}\; x^3+x+1)$$

e allora: $(x+1)+x+1 = 0$

• per $\underline{x \equiv E2 = x^2 = \alpha_2(x)}$

si ha

$$(x^2)^2 \equiv x^2+x \quad (\mathrm{mod}\; x^3+x+1)$$
$$(x^2)^3 \equiv x^2+1$$

e allora:

$$(x^2+1)+(x^2)+1 = 0$$

• per $\underline{x \equiv E_4 \equiv x^2+x = \alpha_3(x)}$

si ha

$$(x^2+x)^2 \equiv x^4+x^2 \equiv x \quad (\mathrm{mod}\; x^3+x+1)$$
$$x(x^2+x) \equiv (x^2+x)^3 = x^2+x+1$$

e allora

$$(x^2+x+1)+(x^2+x)+1 = 0$$

l'altro polinomio minimo è:

$p_2(x) = (x^3+x^2+1)$

che ha anche radici

$$\begin{cases} E_3 = x+1 = \alpha_4(x) \\ E5 = x^2+x+1 = \alpha_5(x) \\ E6 = x^2+1 = \alpha_6(x) \end{cases}$$

$n=3$

$p=2$

per cui

$$\begin{cases} N_2(2,3) = 2 \\ N_p(2,3) = 2 \\ N_\alpha(2,3) = 6 \end{cases}$$

$p=2$
$n=4 \quad 2^4$

Esempio

$GF(2^4) = \mathbb{Z}_2[x] (\mathrm{mod}\ x^4+x+1)$

$\boxed{r(x) = x^4+x+1}$

$n=4$

$N_2(2^4) = 3$ irriducibili $(x^4+x+1); (x^4+x^3+1); (x^4+x^3+x^2+x+1)$

$N_p(2^4) = 2$ primitivi $(x^4+x+1); (x^4+x^3+1)$

$N_\alpha(2^4) = 8$ radici

$p_1(x) = x^4+x+1$

$2^n-1=15$ elementi non zero

4 Radici di (x^4+x+1)

$E1 = x^1$ — x ←○ 0010
$E2 = x^2$ — x^2 ←○ 0100
$E3 = x^3$ — x^3 1000
E4 4 — $x+1$ ←○ 0011
5 — x^2+x 0110
6 — x^3+x^2 1100
○7 — x^3+x+1 1011
8 — x^2+1 ←○ 0101
9 — x^3+x 1010
10 — x^2+x+1 0111
○11 — x^3+x^2+x 1110
12 — x^3+x^2+x+1 1111
○13 — x^3+x^2+1 1101
○14 — x^3+1 1001
E 15 — 1 0001

$p_2(x) = x^4+x^3+1$

x^{16} — x
x^{17} — x^2
x^{18} — x^3
x^{19} — $x+1$
x^{20} — x^2+x
x^{21} — x^3+x^2

il tutto $(\mathrm{mod}\ x^4+x+1)$

$\underline{E1 = x = \alpha_1} \equiv 0010$

$x^4 = x+1$

$x+1+x+1 = 0$ ok

$\underline{E2 = x^2 = \alpha_2} \equiv 0100$

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

$(x^2+1)+(x^2)+1 = 0$ ok

$\underline{E4 = x+1 = \alpha_3} \equiv 0011$

$(x+1) = x^4$

$(x+1)^4 = x^{16} = x$

$(x) + (x+1) + 1 = 0$ ok

$\underline{E8 = x^2+1 = \alpha_4} \equiv 0101$

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

$k=0,1,2,$

$(x^2+1)^4 = x^{32} \equiv x^{2+k \cdot 15} \equiv x^2$

$(x^2) + (x^2+1) + 1 = 0$ ok

$F(x) = $ [illegible]

per l'altro polinomio primitivo in $\mathbb{Z}_2[x]$ di grado $n=4$

$$p_2 = x^4+x^3+1$$

le 4 radici primitive sono quelle per cui, preso x (che è sempre radice primitiva$^{(1)}$) lo si eleva a k ove $\operatorname{mcd}(p^n-1,k)=1$ e cioè tali che $\operatorname{mcd}(15,k)=1$ per $1\leq k\leq 15$,

Il numero di tali $k \perp 15$ è $\phi(15)=8$

Per $p_1(x)$ i k delle radici sono

$$k=1,2,4,8$$

Per $p_2(x)$ i k sono

$$k=7,11,13,14$$

Per cui si ha

$$x^7 \equiv E7 \equiv x^3+x+1 \equiv \alpha_5 \equiv (1011)$$

$$x^{11} \equiv E11 \equiv x^3+x^2+x \equiv \alpha_6 \equiv (1110)$$

$$x^{13} \equiv E13 \equiv x^3+x+1 \equiv \alpha_7 \equiv (1101)$$

$$x^{14} \equiv E14 \equiv x^3+1 \equiv \alpha 8 \equiv (1001)$$

---

(1) Si osserva che $x^k \equiv x$ per $k=1$ è sempre radice primitiva per ogni $GF(p^n)$, dato che $\operatorname{mcd}(p^n-1,1)=1$.

14BIS

verifichiamo poi Fermat in GF(2^4)
Prendiamo $E3 \equiv x^3$ è un elemento del campo <u>non</u> primitivo si ha che

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

$$x^{45} \equiv 1 \pmod{x^4+x+1}$$

Infatti $x^{20} \equiv x^2+x$

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

$$x^{40} \equiv (x^2+x)(x^2+x) \equiv x^4+x^2$$

$$x^{45} \equiv (x^4+x^2)(x^2+x) \equiv x^6+x^4+x^5+x^3$$

$$x^{45} \bmod (x^4+x+1) \equiv 1$$ infatti

$$\begin{array}{r|l} & x^2+x+1 \\ \hline x^4+x+1 & x^6+x^5+x^4+x^3 \\ & x^6+x^3+x^2 \\ \hline & x^5+x^4+x^2 \\ & x^5+x^2+x \\ \hline & x^4+x \\ & x^4+x+1 \\ \hline & 1 \end{array}$$

ok!

Si osserva poi che:
l'"ordine" di x^3 è 5!

$$\frac{2^4-1}{3} = \frac{15}{3} = 5$$

infatti $x^{15} \equiv 1 \pmod{x^4+x+1}$

POLINOMI

n	primitivi	#	irriducibili	#
2	x^2+x+1	1	x^2+x+1	1
3	x^3+x+1 ; x^3+x^2+1	2	x^3+x+1 ; x^3+x^2+1	2
4	x^4+x+1 ; x^4+x^3+1	2	x^4+x+1 ; x^4+x^3+1 $x^4+x^3+x^2+x+1$	3
5	x^5+x^2+1 ; x^5+x^3+1 $x^5+x^3+x^2+x+1$ $x^5+x^4+x^3+x+1$ $x^5+x^4+x^3+x^2+1$ $x^5+x^4+x^2+x+1$	6	x^5+x^2+1 ; x^5+x^3+1 $x^5+x^3+x^2+x+1$ $x^5+x^4+x^3+x+1$ $x^5+x^4+x^3+x^2+1$ $x^5+x^4+x^2+x+1$	6

polinomi primitivi e irriducibili
di grado n
in

$\mathbb{Z}_2[X]$

Un polinomio irriducibile $r(x)$ in $\mathbb{Z}_p[x]$ di grado n è detto essere "primitivo" $r(x)=P(x)$ se l'ordine di "x modulo $r(x)$" è (p^n-1):

$$\text{se: } x^{(p^n-1)} \bmod r(x) = 1, \text{ allora } r(x)=P(x)$$

e cioè se il più piccolo intero positivo k per cui $r(x)$ "divide" (x^k-1) è $k=p^n-1$ $(k=1,2,\dots)$.

Ad esempio: $p=2$; $n=4$. Ci sono 3 polinomi irriducibili

$$r_1(x)=p_1(x)=x^4+x+1$$

$$r_2(x)=p_2(x)=x^4+x^3+1$$

che sono anche primitivi, mentre il terzo

$$r_3(x)=x^4+x^3+x^2+x+1 \neq P(x)$$

non lo è: ci sono 2 polinomi primitivi di grado $n=4$ in $\mathbb{Z}_p[x]$.

Verifichiamo $p_1(x)$.

Se $p_1(x)=x^4+x+1$ risulta

$$x^{15} \bmod (x^4+x+1)=1$$

e $x^k \bmod p_1(x) \neq 1$

per tutti i k da 1 a 14. Quindi l'ordine di x è 15 e $p_1(x)$ è primitivo.

E' facile verificare che anche $P_2(x)$ è primitivo.

verifichiamo ora: $P_3(x) = (x^4+x^3+x^2+x+1)$

Partiamo da

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

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

e troviamo subito

$$x^5 \bmod (x^4+x^3+x^2+x+1) = 1$$

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

e quindi

$P_3(x)$ divide (x^5-1) e $5<15$, quindi $P_3(x)$ non è primitivo!

$$(x^5-1) \bmod (x^4+x^3+x^2+x+1) = 0.$$

Ovviamente vale sempre che:

$$(x^{15}-1) \bmod (x^4+x^3+x^2+x+1) = 0$$

Altro esempio

$p=2$ $\quad 2^6-1=63$

$n=6$

$P(x) = x^6+x^3+1$ irriducibile: è primitivo?

$$x^9 \bmod (x^6+x^3+1) = 1$$

$$\begin{array}{r|l} & x^3+1 \\ \hline x^6+x^3+1 & x^9 \\ & x^9+x^6+x^3 \\ \hline & x^6+x^3 \\ & x^6+x^3+1 \\ \hline & 1 \end{array}$$

$9<63 \rightarrow$ NO!

Il polinomio $p(x)$ di grado n è irriducibile nel campo $\mathbb{Z}_p[x]$, mentre le radici

$$x = \alpha_i(x) \quad , \quad 1 \le i \le n$$

per cui

$$p(x) = 0$$

sono nel campo finito $GF(p^n)(\bmod\ r(x))$. Quindi $p(x)$ può essere espresso tramite gli elementi del campo finito $GF(p^n)(\bmod\ r(x))$ come

$$(1) \quad p(x) = (x-\alpha_1)(x-\alpha_2) \cdots (x-\alpha_n) \ (\bmod\ r(x))$$

$p(x)$ è infatti monico, e quindi la (1) mostra che $p(x)$ non è più irriducibile quando viene considerato al di fuori di $\mathbb{Z}_p[x]$.

Per similitudine, per esempio il polinomio

$$x^2+1$$

è irriducibile nel campo dei numeri reali, mentre è riducibile nel campo dei numeri complessi... !

$$x^2+1 = (x+j)(x-j) \qquad \pm j = \pm\sqrt{-1}$$

$$x^2 - jx + jx - j^2 = x^2+1$$

per convincersi prendiamo GF(2^4)(mod x^4+x+1)

polinomio primitivo $p_1(\alpha)=\alpha^4+\alpha+1$ $n=4$

se $p_1(\alpha)=0$; $\alpha^4=\alpha+1$ (mod $\alpha^4+\alpha+1$)

$2^4-1=15=3\times5$

mcd $(i,15)=1$ per

$i=1,2,4,8$; $i=2^k; 0\le k\le n-1$

$7, 11, 13, 14$

α

α^2

α^3

$\alpha^4=\alpha+1$ ← parto da qui

$\alpha^5=\alpha^2+\alpha$

$\alpha^6=\alpha^3+\alpha^2$

$\alpha^7=\alpha^3+\alpha+1$

$\alpha^8=\alpha^2+1$

$\alpha^9=\alpha^3+\alpha$

$\alpha^{10}=\alpha^2+\alpha+1$

$\alpha^{11}=\alpha^3+\alpha^2+\alpha$

$\alpha^{12}=\alpha^3+\alpha^2+\alpha+1$

$\alpha^{13}=\alpha^3+\alpha^2+1$

$\alpha^{14}=\alpha^3+1$

$\alpha^{15}=1$

Allora verifichiamo che

$p_1(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)=$
$=x^4+x+1$

per gli α
$\alpha^k\in GF(2^4)$

infatti

$p_1(x)=(x^2+x\alpha^5+\alpha^3)\left[(x^2+x\alpha^5+\alpha^3)+\alpha^{10}\right]$

$=(x^2+x\alpha^5+\alpha^3)^2+(x^2+x\alpha^5+\alpha^3)\alpha^{10}=$

$=(x^4+x^2\alpha^{10}+\alpha^6)+(x^2\alpha^{10}+x\alpha^{15}+\alpha^{13})=$

$=x^4+x+\alpha^6+\alpha^{13}=x^4+x+1$

ok.

Verifichiamo ora che l'altro primitivo $p_2(x)=x^4+x^3+1$

ha radici $\alpha^7;\alpha^{11};\alpha^{13};\alpha^{14}$

(mod $\alpha^4+\alpha+1$)

$$P_2(x)=(x-\alpha^7)(x-\alpha^{11})(x-\alpha^{13})(x-\alpha^{14})=$$

$$=(x^2+x(\alpha^{11}+\alpha^7)+\alpha^{18})(x^2+x(\alpha^{14}+\alpha^{13})+\alpha^{27})$$

$$=(x^2+x(\alpha^2+1)+\alpha^3)(x^2+x\alpha^2+\alpha^{12})=$$

$$=x^4+x^3\alpha^2+x^2\alpha^{12}+x^3(\alpha^2+1)+x^2\alpha^2(\alpha^2+1)+$$

$$x\,\alpha^{12}(\alpha^2+1)+x^2\alpha^3+x\alpha^5+\alpha^{15}=$$

$$=x^4+x^3(\alpha^2+\alpha^2+1)+x^2(\alpha^{12}+\alpha^4+\alpha^2+\alpha^3)+$$

$$x(\alpha^{14}+\alpha^{12}+\alpha^5)+1=x^4+x^3+x^2(0)+x(0)+1$$

$$=x^4+x^3+1$$

$\underline{\text{OK}}$

infatti

$$\alpha^{12}+\alpha^4+\alpha^3+\alpha^2=\cancel{\alpha^3}+\cancel{\alpha^2}+\cancel{\alpha}+\cancel{1}+\cancel{\alpha}+\cancel{1}+\cancel{\alpha^3}+\cancel{\alpha^2}=0$$

$$\alpha^{14}+\alpha^{12}+\alpha^5=\cancel{\alpha^3}+\cancel{1}+\cancel{\alpha^3}+\cancel{\alpha^2}+\cancel{\alpha}+\cancel{1}+\cancel{\alpha^2}+\cancel{\alpha}=0$$

OK

OPPURE

$p_2(\alpha) = \alpha^4 + \alpha^3 + 1$

$\alpha^4 = \alpha^3 + 1$

$(\mathrm{mod}\ \alpha^4 + \alpha^3 + 1)$

α

α^2

α^3

$\alpha^4 = \alpha^3 + 1$ ← parti da qui

$\alpha^5 = \alpha^3 + \alpha + 1$

$\alpha^6 = \alpha^3 + \alpha^2 + \alpha + 1$

$\alpha^7 = \alpha^2 + \alpha + 1$

$\alpha^8 = \alpha^3 + \alpha^2 + \alpha$

$\alpha^9 = \alpha^2 + 1$

$\alpha^{10} = \alpha^3 + \alpha$

$\alpha^{11} = \alpha^3 + \alpha^2 + 1$

$\alpha^{12} = \alpha + 1$

$\alpha^{13} = \alpha^2 + \alpha$

$\alpha^{14} = \alpha^3 + \alpha^2$

$\alpha^{15} = 1$

$\alpha^{16} = \alpha$

$\alpha^{17} = \alpha^2$

$\alpha^{18} = \alpha^3$

$\alpha^{19} = \alpha^3 + 1$

$\alpha^{20} = \alpha^3 + \alpha + 1$

$$p_2(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$$

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

$$(x^2 + x(\alpha^8 + \alpha^4) + \alpha^{12}) =$$

$$= (x^2 + x\alpha^{13} + \alpha^3)(x^2 + x\alpha^7 + \alpha^{12})$$

$$= x^4 + x^3\alpha^7 + x^2\alpha^{12} + x^3\alpha^{13} + x^2\alpha^{20} +$$

$$x\alpha^{25} + x^2\alpha^3 + x\alpha^{10} + \alpha^{15} =$$

$$= x^4 + x^3(\alpha^7 + \alpha^{13}) + x^2(\alpha^{12} + \alpha^{20} + \alpha^3)$$

$$+ x(\alpha^{25} + \alpha^{10}) + \alpha^{15} =$$

$$= x^4 + x^3 + x^2(0) + x(0) + 1 =$$

$$= x^4 + x^3 + 1 \text{ ok!}$$

infatti: $$\begin{cases} (\alpha + 1 + \alpha^3 + \alpha + 1 + \alpha^3) = 0 \\ (\alpha^3 + \alpha + \alpha^3 + \alpha) = 0 \end{cases}$$

$$\boxed{p(x) = \prod_{i=0}^{n-1} (x - \alpha^{2^i}) \text{ di grado } n}$$

Esercizio Cifrario di Hill in $GF(2^3) \equiv \mathbb{Z}_2[x] \pmod{x^3+x+1}$

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

Plaintext binario

$$P = (1\,0\,1)(0\,0\,1)$$

000	0
001	1
010	x
011	$x+1$
100	x^2
101	x^2+1
110	x^2+x
111	x^2+x+1

$$P = (x^2+1)(1) = P_1\ P_2$$

$$K = \begin{pmatrix} x^2 & 1 \\ x+1 & 1 \end{pmatrix}$$

Determinare il messaggio cifrato $C_1 C_2$ e effettuare la decifrazione.

(1) $\det K = x^2+x+1 \neq 0$ ok Allora risulta nei campi $GF(p^n)$ rispetto a $r(x)$ che (2) $\mathrm{mcd}(\det K, r(x)) = 1$ e quindi la (1) comporta sempre la (2). Risulta

$$\det K^{-1} \equiv \frac{1}{x^2+x+1} \equiv x^2 \pmod{x^3+x+1}$$

infatti si ha

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

e che

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

e allora posso scrivere

$$\begin{array}{l|l} & 0 \\ & 1 \\ \hline x^3+x+1=(x^2+x+1)(x+1)+x & x+1 \\ x^2+x+1=(x+1)x+1 & (x+1)^2+1= \\ & x^2+1+1=\underline{x^2} \end{array}$$

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

infatti

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

ok.

Allora

$$K^{-1}=x^2\begin{pmatrix} 1 & -1 \\ -(x+1) & x^2 \end{pmatrix}=x^2\begin{pmatrix} 1 & 1 \\ x+1 & x^2 \end{pmatrix}=$$

$$K^{-1} = \begin{pmatrix} x^2 & x^2 \\ x^3+x^2 & x^4 \end{pmatrix} = \begin{pmatrix} x^2 & x^2 \\ x^2+x+1 & x^2+x \end{pmatrix}$$

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

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

Risulta verificato che

$$K \cdot K^{-1} = \begin{pmatrix} x^2 & 1 \\ x+1 & 1 \end{pmatrix} \begin{pmatrix} x^2 & x^2 \\ x^2+x+1 & x^2+x \end{pmatrix} =$$

$$= \begin{pmatrix} x^4+x^2+x+1 & x^4+x^2+x \\ x^3+x+1 & x^3+x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

OK

Ciphering

$$C = (x^2+1, 1) \begin{pmatrix} x^2 & 1 \\ x+1 & 1 \end{pmatrix} = (x^4+x^2+x+1, x^2) = C$$

$$C \equiv (1, x^2)$$

Deciphering

$$P = (1, x^2) \begin{pmatrix} x^2 & x^2 \\ x^2+x+1 & x^2+x \end{pmatrix} =$$

$$= \Big[\underset{(x^4+x^3)}{(x^2+x^4+x^3+x^2)}, (x^2+x^4+x^3) \Big] = [x^2+1, 1] = P$$

OK

vedi retro

$$
\begin{array}{r l}
 & x+1 \\
x^3+x+1 \big) & \overline{x^4+x^3} \\
 & \underline{x^4+x^2+x} \\
 & x^3+x^2+x \\
 & \underline{x^3+x+1} \\
 & x^2+1
\end{array}
$$

$$
\begin{array}{r l}
 & x+1 \\
x^3+x+1 \big) & \overline{x^4+x^3+x^2} \\
 & \underline{x^4+x^2+x} \\
 & x^3+x \\
 & \underline{x^3+x+1} \\
 & 1
\end{array}
$$