

$$f(0)=0$$

$$f(1)=1$$

$$f(2)=2$$

$$f(x)=2x+1$$

$$f(x+1)=f(x)+f(1)=2x+2$$

$$f(x+2)=f(x)+f(2)=2x$$

$$f(2x)=f(2)f(x)=2f(x)=2x$$

$$f(2x+1)=2x+1$$

$$f(2x+2)=2x+2$$

$$g(0)=0$$

$$g(1)=1$$

$$g(2)=2$$

$$g(x)=x+2$$

$$g(x+y)=g(x)+g(y)=x+y$$

$$g(x+2)=x+4$$

$$g(2x)=g(2)g(x)=2g(x)=2x+2$$

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

$$g(2x+2)=2x+4$$

OSSERVAZIONE: $x \in K$ NON È UN GENERATORE DI $K \setminus \{0\}$. INFATTI, IL

SOTTOGRUPPO DEL GRUPPO MOLTIPLICATIVO $K \setminus \{0\}$ GENERATO DA x È

$$\langle x \rangle = \{x, 2x, 3x, \dots\} \subset K \setminus \{0\}$$

LEMMA: SE K È UN ANELLO COMMUTATIVO DI CARATTERISTICA PRIMA p ,

$$\text{ALLORA } (x+y)^{p^h} = x^{p^h} + y^{p^h} \quad \forall x, y \in K, h \geq 1$$

DIM (PER INDUZIONE)

SIA $h=1$, $p > k > 0 \Rightarrow p$ DIVIDE TUTTI I COEFFICIENTI BINOMIALI $\binom{p}{k} = \frac{p!}{k!(p-k)!}$

PERCHÉ NON DIVIDE $k!(p-k)!$ ALLORA $(x+y)^p = \sum_{k=0}^p \binom{p}{k} x^k y^{p-k} = x^p + y^p$

h�1) ...

DAL LEMMA PRECEDENTE SEGUO CHE, SE K È UN CAMPO DI CARATTERISTICA p ,

LA FUNZIONE $\Phi: K \rightarrow K$ $x \mapsto x^p$ È UN MORFISMO DI CAMPI. INFATTI

$$\Phi(x+y) = (x+y)^p = x^p + y^p = \Phi(x) + \Phi(y)$$

$\forall x, y \in K$

$$\Phi(xy) = (xy)^p = x^p y^p = \Phi(x)\Phi(y)$$

$K = \mathbb{F}_p^n \Rightarrow \Phi$ È UN AUTOMORFISMO, ESSENDO UN MORFISMO INIEZIONE

FROBENIUS.

DA UN CAMPO DI CARDINALITÀ FINITA IN SE STESSO, DETTO AUTOMORFISMO DI

TEOREMA: IL GRUPPO DEGLI AUTOMORFISMI DI \mathbb{F}_{p^n} $\text{Aut}(\mathbb{F}_{p^n})$ È CICLO DI

CARDINALITÀ n GENERATO DALL'AUTOMORFISMO DI FROBENIUS

LEMMA 8a: SIA F UN CAMPO. IL POLINOMIO $x^d - 1$ DIVIDE IL POLINOMIO

$$x^n - 1 \text{ IN } F[x] \Leftrightarrow d \text{ DIVIDE } n$$

DIM

$$n = qd + r, 0 \leq r \leq d \Rightarrow \text{IN } F[x] \quad (x^n - 1) = (x^d - 1) x^{nd} + (x^{n-2d} + \dots +$$

$$+ x^{n-(q-1)d} + x^r) + (x^r - 1) \Rightarrow \left(\frac{x^d - 1}{x^{n-1}} \right) \Leftrightarrow r=0 = x^r - 1 \text{ POLINOMIO NUOVO}$$

DA QUESTO TIPO DI FATTORELLAZIONE SI OTTIENE CHE, CALCOLANDO IN P , SE

$p^d - 1$ DIVIDE $p^n - 1$ ALLORA d DIVIDE n

COROLARIO 8b: d DIVIDE $n \Leftrightarrow x^{pd} - x$ DIVIDE $x^{pn} - x$ IN $\mathbb{F}_p[x]$

DIM

\Rightarrow DAL LEMMA PRECEDENTE $x^d - 1$ DIVIDE $x^n - 1$. CALCOLANDO IN P SI

OBTIENE CHE P^{d-1} DIVIDE $P^n - 1 \Rightarrow X^{P^{d-1}-1} \text{ DIVIDE } X^{P^n-1}-1$

$\Leftrightarrow X^{P^{d-1}-1} \text{ DIVIDE } X^{P^n-1}-1 \Rightarrow P^{d-1} \text{ DIVIDE } P^{n-1} \Rightarrow \frac{d}{n}$

PROPOSIZIONE 8C: TUTTI E SOLI I SOTTOCAMPI DI \mathbb{F}_{p^n} SONO I CAMPI \mathbb{F}_{p^d}
Dove d DIVIDE n

$\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n} \Rightarrow$ TUTTE LE RADICI DI $X^{p^d} - X$ IN \mathbb{F}_{p^d} SONO RADICI DI

$X^{p^n} - X$ IN $\mathbb{F}_{p^n} \Rightarrow X^{p^d} - X \text{ DIVIDE } X^{p^n} - X \Rightarrow \frac{d}{n} \Rightarrow \frac{X^{p^d} - X}{X^{p^n} - X}$ E L'

INSIEME DELLE RADICI DI $X^{p^d} - X$, CHE È UN CAMPO \mathbb{F}_{p^d} , STA IN \mathbb{F}_{p^n}

FINORA, DATO UN NUMERO PRIMO p ED UN NUMERO NATURALE $n \neq 0$, ABBIAMO

COSTRUITO UN CAMPO DI CARDINALITÀ p^n PRENDENDO UN POLINOMIO

IRRIDUCIBILE $Q \in \mathbb{F}_p[x]$ E, FACENDO IL QUOTIENTE $\frac{\mathbb{F}_p[x]}{\langle Q \rangle}$. IN QUESTO

MODO, DUE CAMPI COSTRUITI AVENTI LA STESSA CARDINALITÀ SONO ISOMORFI

OSSERVAZIONI:

1) SIA K UN CAMPO FINITO. QUAL È LA CARATTERISTICA DI K ?

PRENDIAMO IL SOTOGRUPPO $\langle 1_K \rangle \subseteq K$. POICHÉ $\langle 1_K \rangle$ È FINITO,

$\exists n > 1 | \langle 1_K \rangle \cong \mathbb{Z}_n$. POICHÉ GLI ELEMENTI DI $\langle 1_K \rangle$ SONO

ELEMENTI DI UN CAMPO, NON POSSONO ESSERE DIVISORI DI ZERO

$\rightarrow n$ È UN NUMERO PRIMO \Rightarrow UN CAMPO FINITO HA CARATTERISTICA

PRIMA p E CAMPO FONDAMENTALE \mathbb{F}_p

2) SIA K UN CAMPO FINITO. ABBIAMO VISTO CHE \exists I PRIMI $I F_p \subseteq K$.

Inoltre, il gruppo moltiplicativo $K \setminus \{0\}$ è unico. $K \setminus \{0\} = \langle \alpha \rangle$

$\Rightarrow K = I F_p \langle \alpha \rangle$. SE IL GRADO DI α SU $I F_p$ È n , $|K| = p^n \Rightarrow$ OGNI

CAMPO FINITO HA CARDINALITÀ p^n PER QUALCHE P PRIMO E $n \neq 0$

3) SIANO K_1, K_2 CAMPI FINITI DI CARDINALITÀ p^n . SIA $K_1 = I F_p \langle \alpha \rangle$,

DOVE α È UN GENERATORE DEL GRUPPO $K_1 \setminus \{0\}$ E GRADO n SU K_1 .

SIA $Q \in I F_p[x]$ IL SUO POLINOMIO MINIMO $\Rightarrow \deg(Q) = n \Rightarrow Q$ IRRIDUCIBILE

- K_1, K_2 CAMPI DI SPEZZAMENTO DI $x^{p^n} - x \in I F_p[x]$
- OGNI POLINOMIO IRRIDUCIBILE DI GRADO n IN $I F_p[x]$ È FATTORE DI $x^{p^n} - x$
- IL POLINOMIO Q HA RADICE IN K_2 INDICATA CON β .
- L'ASSEGNAZIONE $\alpha \mapsto \beta$ DEFINISCE UN MORFISMO DI CAMPI DA K_1

IN K_2 . POICHÉ UN MORFISMO DI CAMPI È SEMPRE INIETTIVO, E POICHÉ

TALE MORFISMO È SUBETTIVO AVENTE K_1 E K_2 LA STESSA CARDINALITÀ

ABBIAMO CHE $K_1 \cong K_2$

ALGORITMO DI BERLEKAMP

TEOREMA 9a: SIANO $f(x) \in I F_p[x]$ DI GRADO $d > 1$ E $h(x) \in I F_p[x]$

DI GRADO $1 \leq \deg(h) \leq d$ | $f(x)$ DIVIDE $h(x) - h(x^p)$.

ALLORA $f(x) = \text{MCD}\{f(x), h(x)\} \cdot \text{MCD}\{f(x), h(x)-1\} \cdots$ IN $\mathbb{F}_p[x]$

• $\text{MCD}\{f(x), h(x)-(p-1)\}$ È UNA FATTORIZZAZIONE NON BANALE DI $f(x)$

DIM

SUPPONIAMO CHE $\frac{f(x)}{h(x)^p - h(x)}$. IL POLINOMIO $x^p - x \in \mathbb{F}_p[x]$ SI

FATTORIZZA COME $x^p - x = x(x-1)(x-2) \cdots (x-(p-1))$

$h(x) \neq x$

$$\Rightarrow h(x) - h(x) = h(x)[h(x)-1][h(x)-2] \cdots [h(x)-(p-1)]$$

$\text{MCD}\{h(x)-i, h(x)-j\} = 1 \forall i \neq j \in \mathbb{F}_p$. INFATI, SE

$$h(x)-i = D(x)H_i(x) \quad \left. \begin{array}{l} \\ h(x)-j = D(x)H_j(x) \end{array} \right\} =$$

$\text{MCD}\{h(x)-i, h(x)-j\} = D(x) \Rightarrow$

$$\Rightarrow D(x)[H_i(x) - H_j(x)] = j-i \in \mathbb{F}_p \Rightarrow (i \neq j \Rightarrow \deg(D)=0).$$

| NOLTRÉ, $\text{MCD}\{a, b\} = 1 \Rightarrow \text{MCD}\{r, ab\} = \text{MCD}\{r, a\} \cdot \text{MCD}\{r, b\}$.

PER INDUZIONE, $\text{MCD}\{r, \prod_{i=1}^k a_i\} = \prod_{i=1}^k \text{MCD}\{r, a_i\}$. POICHÉ

$$\frac{f(x)}{h(x)^p - h(x)}, f(x) = \text{MCD}\{f(x), h(x)^p - h(x)\}. | \text{NOLTRÉ, SE } i \neq j =$$

$$\Rightarrow \text{MCD}\{h(x)-i, h(x)-j\} = 1 \text{ SI HA } f(x) = \text{MCD}\{f(x), h(x)^p - h(x)\}$$

$$= \text{MCD}\{f(x), h(x)[h(x)-1][h(x)-2] \cdots [h(x)-(p-1)]\} =$$

$$= \text{MCD}\{f(x), h(x)\} \cdot \text{MCD}\{f(x), h(x)-1\} \cdots \text{MCD}\{f(x), h(x)-(p-1)\}.$$

$$\deg(h-1) < \deg(h) \Rightarrow \text{MCD}\{h, h-1\} \neq f(x) \forall i \in \mathbb{F}_p \Rightarrow \text{NESSA}$$

FATTORIZZAZIONE PRECEDENTE APPARISCE SOLO POLINOMI DI GRADO $< d \Rightarrow$ È

(UNA FATTORIZZAZIONE NON BANALE DI $f(x)$)

MOSTRIAMO CHE UN POLINOMIO $h(x) \in F_p[x]$, CHE SODDISFA LE CONDIZIONI

DEL TEOREMA, ESISTE SEMPRE. SIA $h(x) = b_0 + b_1 x + \dots + b_{d-1} x^{d-1} \in F_p[x]$

Allora $h^p(x) = b_0^p + b_1 x^p + \dots + b_{d-1} x^{p(d-1)}$ PERCHÉ ABBIAMO

MOSTRATO CHE $(x+y)^p = x^p + y^p$ E, INNANZITUTTO, $(\sum_{i=1}^k x_i)^p = \sum_{i=1}^k x_i^p$.

MA $b_i^p = b_i \quad \forall 0 \leq i \leq d-1 \Rightarrow h^p(x) = b_0 + b_1 x^p + \dots + b_{d-1} x^{p(d-1)}$

$\Rightarrow h(x) \text{ MOD } f(x) = b_0 (\text{MOD } f) + b_1 (x^p \text{ MOD } f) + \dots$

$+ b_{d-1} (x^{p(d-1)} \text{ MOD } f)$

SIA $x^{ip} = f(x) q_i(x) + r_i(x)$, $\deg(r_i(x)) < d$, $0 \leq i \leq d-1$.

$[h^p(x) - h(x)] \text{ MOD } f = 0 \text{ MOD } f \Leftrightarrow h^p(x) \text{ MOD } f = h(x) \text{ MOD } f$

$\Leftrightarrow b_0 r(x) + b_1 r_1(x) + \dots + b_{d-1} r_{d-1}(x) = b_0 + b_1 x + \dots + b_{d-1} x^{d-1}$

\Rightarrow ABBIAMO UN SISTEMA LINEARE DI d EQUAZIONI NELLE INCognITE b_0, b_1, \dots, b_{d-1}

... b_{d-1} . BISOGNA VERIFICARE CHE ESISTANO SOLUZIONI NON NULLI. SIA

$f(x) = P_1(x) \dots P_k(x)$ UNA FATTORIZZAZIONE DI $f(x) \in F_p[x]$ IN FACTORI

IRRIDUCIBILI. SUPPONIAMO CHE f NON ABbia FACTORI MULThPi GRAZIE AD

UN TEOREMA (SIA K UN CAMPO)

DETERMINA

- $f(x) \in K[x]$ HA UN FACTOR MULThPi $\Rightarrow \text{MCD}\{f, f'\} \neq 1$

- $(K \text{ HA CARATTERISTICA } 0) \vee (K \text{ CAMPO FINITO DI CARATTERISTICA } p \wedge \lambda \text{ MCD}\{f, f'\} \neq 1) \Rightarrow f(x) \text{ HA UN FACTOR MULThPi}$

Abbiamo una versione in $\text{IFP}[x]$ del teorema unisce dei resti

$\text{MCD}\{\mathbb{P}_i(x), \mathbb{P}_j(x)\} = 1 \quad \forall 1 \leq i \leq k, 1 \leq j \leq k, i \neq j$

$$\Rightarrow \frac{\text{IFP}[x]}{\langle P_1 \rangle} \underset{\substack{\text{ISOMORFISMO} \\ \text{O, ANCHE}}}{\sim} \frac{\text{IFP}[x]}{\langle P_1(x) \rangle} \times \dots \times \frac{\text{IFP}[x]}{\langle P_k(x) \rangle}. \text{ DATO } (\lambda_1, \dots, \lambda_k) \in \text{IFP}^k$$

ESISTE UN'UNICA CLASSE $[h(x)] \in \frac{\text{IFP}[x]}{\langle P_1 \rangle}$ TALE CHE

$$[h(x)] = [\lambda_i] \text{ IN } \frac{\text{IFP}[x]}{\langle P_{i(x)} \rangle} \quad \left. \begin{array}{l} \\ \vdots \\ \end{array} \right\} \Rightarrow \frac{h(x) - \lambda_i}{P_i(x)} \quad \forall 1 \leq i \leq k$$

$$[h(x)] = [\lambda_k] \text{ IN } \frac{\text{IFP}[x]}{\langle P_{k(x)} \rangle} \quad \left. \begin{array}{l} \\ \vdots \\ \end{array} \right\} \Rightarrow \frac{h(x) - \lambda_k}{P_k(x)} \quad \forall 1 \leq i \leq k$$

$$\Rightarrow \frac{h(x)(h(x)-1)\dots(h(x)-(P-1))}{P} = h(x) - h(x)$$

ESEMPIO: FATTOREZZIAMO $f := x^5 + x^2 + 2x + 1 \in \text{IF}_3[x]$

PRIMA VERIFICHIAMO CHE $\text{MCD}\{f, f'\} = \{x^5 + x^2 + 2x + 1, 5x^4 + 2x +$

$$+ 2\} = \{x^5 + x^2 + 2x + 1, 2x^4 + 2x + 2\} = 1$$

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

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

$$\begin{array}{r}
 -2x^3 \\
 +2x+2 \\
 \hline
 -2x^3 - 2x^2 \\
 \hline
 2x^2 + 2x + 2
 \end{array}
 \left| \begin{array}{c} x+1 \\ \hline -2x^2 \end{array} \right.$$

$$\begin{array}{r}
 2x^2 + 2x + 2 \\
 \hline
 2x^2 + 2x \\
 \hline
 2
 \end{array}
 \left| \begin{array}{c} x+1 \\ \hline 2x \end{array} \right.$$

$\frac{x^2}{x+1}$ HA RESTO 0. ESSENDO IL NUMERATORE UNA COSTANTE, MCD È R, $R^3 = 1 \checkmark$

ORA SI CALCOLANO I RESTI

- $x^{3(5-1)} = x^2 = (x^2 + 2) \text{ MOD } R$
- $x^{3 \cdot 3} = x^9 = (2x^4 + x^3 + x^2 + 2x + 2) \text{ MOD } R$
- $x^{3 \cdot 2} = x^6 = (2x^3 + x^2 + 2x) \text{ MOD } R$
- $x^3 = x^3 \text{ MOD } R$
- $1 = 1 \text{ MOD } R$

$$\Rightarrow b_0 + b_1 x^3 + b_2 (2x^3 + x^2 + 2x) + b_3 (2x^4 + x^3 + x^2 + 2x + 2) + b_4 (x^2 + 2) = b_0 + b_1 x + b_2 x^2 + b_3 x^3 + b_4 x^4 \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} 2b_3 + 2b_4 = 0 \\ 2b_2 + 2b_3 - b_1 = 0 \\ b_2 + b_3 + b_4 - b_2 = 0 \\ b_1 + 2b_2 = 0 \\ 2b_3 - b_4 = 0 \end{cases} \Leftrightarrow \begin{cases} b_3 = 2b_4 \\ b_1 + b_2 + b_3 = 0 \\ b_1 = b_2 \end{cases}$$

$$\Leftrightarrow b_1 = b_2 = b_3 = 2b_4 \Rightarrow (b_0, b_1, b_2, b_3, b_4) = (0, 1, 1, 1, 2),$$

OSSIA $h(x) = x + x^2 + x^3 + 2x^4 \Rightarrow f(x) = \text{MCD}\{f, x + x^2 + x^3 + 2x^4\} \cdot (x^2 + 2x + 1)$

$$\cdot \text{MCD}\{f, 1 + x^2 + x^3 + 2x^4\} \cdot \text{MCD}\{f, 2 + x^2 + x^3 + 2x^4\} = (1 + x^2)(x^3 +$$

TEOREMA gb: SIA $f(x) \in F_p[x]$, $\deg(f) = d \in \mathbb{N}$ $f(x) = P_0(x)P_1(x)\dots P_k(x)$
MOURELLA 1

UNA FATTORIZZAZIONE IN FACTORI IRREDUCIBILI NON BANALI (GRADO ≥ 1) AVVENTI

SIANO

$$\begin{cases} r_0 = 1 \text{ MOD } f(x) \\ r_1 = x^p \text{ MOD } f(x) \\ r_2 = x^{2p} \text{ MOD } f(x) \\ \vdots \\ r_{d-1} = x^{(d-1)p} \text{ MOD } f(x) \end{cases}$$

CON $\deg(r_i) \leq d \quad \forall 0 \leq i \leq d-1$

DEFINIAMO LA MATEICE $A \in M_{d \times d}(F_p)$ I cui ELEMENTI A_{ij} SONO I

COEFFICIENTI DEL TERMINE DI GRADO i DEL POLINOMIO $r_j(x)$. AD ESEMPIO,

$$f(x) = x^5 + x^2 + 2x + 1 \in F_3[x] \rightarrow A = \begin{vmatrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 \end{vmatrix}$$

E LA MATEMATICA $A - I$ È LA MATEMATICA DEL SISTEMA $(A - I)\vec{b} = \vec{0}$

TEOREMA: IL NUMERO DI FATTORI IRREDUCIBILI K NELLA FATTORIZZAZIONE

DI f È UGUALE ALLA DIMENSIONE DEL NUOVO $A - I$ $K = d - r_k(A - I)$, DOVE

IL RANGO È CALCOLATO SUL CAMPO \mathbb{F}_p

DIM

OSSERVIAMO INNANZITUTTO CHE $\dim(\ker(A - I)) \geq 1$. INFATTI, LA d -TUPLA

$(b_0, 0, \dots, 0)$ È SEMPRE SOLUZIONE DEL SISTEMA $\forall b \in \mathbb{F}_p$. ABBIANO VISTO

CHE L'INSIEME $H := \{h \in \mathbb{F}_p[x] \mid \deg(h) \leq d \wedge \frac{f}{h^p - h}\}$ È UNO SPAZIO

VEKTORIALE SUL CAMPO \mathbb{F}_p ISOMORFO A $\ker(A - I)$. SIA K IL NUMERO DI

FATTORI IRREDUCIBILI NON BANALI DI f AVVENTI MOLTEPUANZA 1. DIMOSTRIAMO

CHE LO SPAZIO VETTORIALE \mathbb{F}_p^K È ISOMORFO AD H . ABBIANO GIÀ DIMOSTRATO

CHE $\forall (b_1, \dots, b_K) \in \mathbb{F}_p^K$ TROVIAMO UN UNICO ELEMENTO DI H USANDO IL

TEOREMA CHINSESE DEI RESTI PER L'ANELLO $\mathbb{F}_p[x] \Rightarrow$ ABBIANO DEFINITO UNA

FUNZIONE $\varphi: \mathbb{F}_p^K \rightarrow H$:

a) φ È UN MORFISMO DI SPAZI VETTORIALI

$$= \{(0, \dots, 0)\}$$

b) φ NIETTIVA: $\ker(\varphi) = \{(s_1, \dots, s_K) \in \mathbb{F}_p^K \mid s_i \bmod p_i = 0 \ \forall 1 \leq i \leq K\} =$

c) φ SURGETTIVA: $h \in H \Rightarrow h^p - h = h(h-1) \dots (h-(p-1))$. QUESTI

FATTORI SONO A COPPIE COPRIMI, QUINDI $\frac{p}{h^p - h} \Rightarrow$ UNICO $s_i \in \mathbb{F}_p$

$\forall i \in \{1, \dots, k\} \mid \frac{P_i(x)}{h - \lambda_i} \Rightarrow h \text{ È SOLUZIONE DEL SISTEMA}$

$$\left\{ \begin{array}{l} h \equiv \lambda_1 \pmod{p_1} \\ \vdots \\ h \equiv \lambda_k \pmod{p_k} \end{array} \right.$$

. ABBIAMO DIMOSTRATO CHE $\varphi: \mathbb{F}_p^k \rightarrow H$ È UN

ISOMORFISMO DI SPAZI VETTORIALI $\Rightarrow \mathbb{F}_p^k \cong H \cong \text{Ker}(A - I)$

$$\Rightarrow \dim(\text{Ker}(A - I)) = k = d - \text{rk}(A - I)$$

AD ESEMPIO, RIPRENDENDO L'ESEMPIO PRECEDENTE, TROVIAMO

FACTORI IRREDUCIBILI DI $f = \text{GRADO } f - \text{rk}(A - I) \Rightarrow 2 \times 5 - \text{rk}(A - I)$.

SE $r \in \mathbb{F}_p[x]$ HA FACTORI IRREDUCIBILI DI MOLTEPLICITÀ > 1 , PROCEDIAMO COME

SEGUE: ABBIAMO VISTO CHE $D := \text{MCD}\{r, f'\} \neq 1$. OSSERVIAMO CHE IL

POUNOMIO $\frac{f}{D}$ HA FACTORI IRREDUCIBILI TUTTI DI MOLTEPLICITÀ 1. INFATTI, SE

P_1, P_2, \dots, P_k SONO tutti DISTINTI, $f' = (P_1^{e_1}(x) \dots P_k^{e_k}(x))^l = l_1 P_1^{e_1} P_1^{e_1} P_2^{e_2} \dots P_k +$
 $+ l_2 P_1^{e_1} P_2^{e_2} P_2^{e_2} \dots P_k + \dots + l_k P_1^{e_1} P_2^{e_2} \dots P_k P_k^{e_k}$ E $D = P_1^{e_1-1} \dots P_k^{e_k-1}$

$\Rightarrow \frac{f}{D} = P_1 \dots P_k$. ALLORA FACTORIZZIAMO $\frac{f}{D}$, Poi FACTORIZZIAMO D

EVENTUALMENTE RIPETENDO IL RAGIONAMENTO CON DE D' FINO A CHE

$\text{MCD}\{D_i, D'_i\} = 1$

ESEMPIO: IN $\mathbb{F}_3[x]$ CONSIDERIAMO $f(x) = 1 + 2x + 2x^2 + x^5 + x^6 + x^7$

$f' = 2 + 4x + 5x^4 + 6x^5 + 7x^6 = 2 + x + 2x^4 + x^6 \Rightarrow \text{MCD}\{f, f'\} = 1 + 2x +$

$+ x^3 =: D \quad \frac{f}{D} = 1 + 2x^2 + x^3 + x^4$. FACTORIZZIAMO $\frac{f}{D}$ E OTTEMAMO

$\frac{f}{D} = (x+1)(1+2x+x^3)$. Poiché D non ha radici in \mathbb{F}_3 , è irriducibile.

Allora $f = \frac{f}{D} \cdot D = (x+1)(1+2x+x^3)^2$