UNIVERSITÀ DEGLI STUDI ROMA TRE
FACOLTÀ DI SCIENZE MM.FF.NN.

Tesi di Laurea di primo livello in Matematica

di

Francesca Carlucci

ALGORITTO di BERLEKAMP

Relatore

Prof. Francesco Pappalardi

Il candidato Il Relatore

ANNO ACCADEMICO 2010-2011

maggio 2012

L'esperienza più bella che possiamo avere è il mistero. È l'emozione fondamentale alla base della vera arte e della vera scienza.
Chi non sa cos'è e non sa più sognare o meravigliarsi, è come morto, e il suo sguardo è spento.

Albert Einstein

Indice

Capitolo 1

Introduzione

1.1 Fattorizzazione dei polinomi

Ogni polinomio non costante su un campo finito può essere espresso come prodotto di polinomi irriducibili.Nel caso dei campi finiti si utilizzano algoritmi per fattorizzare polinomi di grado positivo molto importanti per la teoria dei codici. Al di là del regno dei campi finiti si presentano vari problemi computazionali in algebra e teoria dei numeri che dipendono in un modo o in un altro dallla fattorizzazione di polinomi su campi finiti.

Citiamo la fattorizzazione dei polinomi sull'anello degli interi, la decomposizione di primi razionali nel campo dei numeri algebrici, il calcolo del gruppo di Galois per un'equazione oltre il razionale, e la costruzione di estensioni di campi.

La scelta dell'algoritmo piú adatto per un problema specifico di fattorizzazione dipende dalla grandezza del campo su cui si intende lavorare. Nella prima parte descriverò l'algoritmo di Berlekamp su 'piccoli campi finiti e nella seconda quello per grandi campi finiti.

L'algoritmo consiste principalmente nella costruzione di un opportuna matrice contenente coefficenti ottenuti a partire da quelli del polinomio da fattorizzare e nel calcolo del massimo comun divisore tra polinomi.

Esso é stato il principale algoritmo per la fattorizzazione di polinomi fino alla

realizzazione dell' algoritmo di Cantor-Zassenhaus nel 1981 da cui é stato ormai soppiantato in molte applicazioni.Tuttavia il metodo di Berlekamp é ancora implementato in molti sistemi di algebra computazionale ,tra cui PARI-GP, infatti é di semplice realizzazione e impone poche ipotesi sul polinomio da fattorizzare.

Capitolo 2

Teoremi utili

2.1 Base dell' algoritmo

Per mostrare l'algoritmo di fattorizzazione é sufficente considerare solo polinomi monici; il mio obiettivo é quindi quello di esprimere un polinomio monico $f \in F_q[x]$di grado positivo in forma

$$\mathbf{f} = f_1^{e_1} \cdots f_k^{e_k} \tag{2.1}$$

Teorema 1. *Ogni polinomio $f \in F_q[x]$ di grado positivo può essere scritto nella forma*

$$\mathbf{f} = a p_1^{e_1} \cdots p_k^{e_k} \tag{2.2}$$

dove $a \in F_q$, $p_1 \cdots p_k \in F_q[x]$sono distinti polinomi irriducibili monici e $e_1, \cdots, e_k$ sono interi positivi.

É inoltre possibile semplificare il lavoro dimostrando che il problema puó essere ridotto alla fattorizzazione di un polinomio senza radici multiple il che vuol dire con $e_1 = e_2 = \cdots = e_{k-1} = e_k = 1$

Teorema 2. *L'elemento $b \in F$ é una radice multipla di $f \in F[x]$ se e solo se esso é una radice sia di f che della sua derivata f'*

A dimostrazione calcoliamo il massimo comun divisore di $f(x)$ e della sua derivata $f'(x)$ utilizzando l'algoritmo Euclideo

$$\mathbf{d}(x) = MCD(f(x), f'(x)) \tag{2.3}$$

Se $d(x) = 1$ allora sappiamo che $f(x)$ non ha fattori ripetuti per il teorema 2.
Se $d(x) = f(x) \Rightarrow f'$(x)=0 quindi $f(x) = g^p(x)$ dove $g(x)$é un opportuno polinomio in $F_q(x)$ e p é la caratteristica di $F_q(x)$.Se necessario possiamo continuare con il processo di riduzione applicandolo su $g(x)$.
Se $d(x) \neq 1$ e $d(x) \neq f(x)$ allora $d(x)$ é un fattore non banale di $f(x)$ e $\frac{f(x)}{d(x)}$ non ha fattori comuni la scomposizione di $f(x)$ é ottenuta fattorizzando $d(x)$ e $\frac{f(x)}{d(x)}$ separatamente.
Nel caso in cui $d(x)$ ha fattori multipli si ripeterá un nuovo processo di riduzione. Applicandolo piú di una volta il problema originale é ridotto a quello di fattorizzare un certo numero di polinomi senza fattori ripetuti.Le fattorizzazioni canoniche di questi polinomi portano direttamente a quella del polinomio originale.
Limitiamo dunque la nostra attenzione a polinomi senza fattori ripetuti.

Teorema 3. *Se $f \in F_q[x]$ é monico $h \in F_q[x]$ é tale che $h^q \equiv h \mod f$*

$$\mathbf{f}(x) = \prod_{c \in F_q} MCD(f(x), h(x) - c) \tag{2.4}$$

In generale la (2.4) non dá una completa fattorizzazione di f
Se $h(x) \equiv$ c mod f(x) per qualche $c \in F_q$ allora il Teorema 3 fornisce una fattorizzazione banale di f quindi di nessuna utilitá.Tuttavia diciamo che h é una f-riduzione polinomiale se h é tale che il Teorema sudetto dá una fattorizzazione

non-banale.

Ogni h con $h^q \equiv hmodf$ e $0 \lneq deg(h) \lneq deg(f)$ é sicuramente una f-riduzione.

É quindi chiaro che la fattorizzazione di un polinomio per la (2.4)dipende dal calcolo di φ massimi comun divosori é quindi fattibile su piccoli campi finiti F_q.

Definizione 1. *Siano* $f(x) = (a_0x^n + a_1x^{n-1} + \cdots + a_n) \in K[x]$ *e* $g(x) = (b_0x^m + b_1x^{m-1} + \cdots + b_m) \in K[x]$ *due polinomi di grado rispettivamente* n *ed* m *con* $n, m \in N$*.La risultante* $R(f, g)$ *dei due polinomi é definita dal determinante della matrice di* $(m + n)$ *righe:*

$$R(f,g) = \begin{pmatrix} a_0 & a_1 & \cdots & a_n & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & 0 & a_0 & a_1 & \cdots & \cdots & a_n \\ b_0 & b_1 & \cdots & b_m & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_m & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & \cdots & b_m \end{pmatrix} \tag{2.5}$$

Se il grado $deg(f) = n$ *,* $a_0 \neq 0$ *e* $f(x) = (x - \alpha_0) \cdots (x - \alpha_n)$ *é lo spezzamento del polinomio* f *sul campo* K *allora* $R(f, g)$ *é dato dalla formula*

$$\mathbf{R}(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i). \tag{2.6}$$

In questo caso abbiamo naturalmente $R(f, g) = 0$ *se e soltanto se* f *e* g *hanno una radice in comune cioé se e soltanto se* f *e* g *hanno un divisore comune in* $K[x]$ *di grado positivo.*

Teorema 4. *Per* $n \geq 0$ *siano* $a_0, a_1, \cdots, a_n$ $n + 1$ *elementi distinti di* F*,e siano* $b_0, b_1, \cdots, b_n$ $n + 1$ *elementi arbitrari di* F*.Allora esiste esattamente un polinomio*

$f \in F[x]$ di grado $\leq n$ tale che $f(a_i) = b_i$ per $i = 0, 1, \cdots, n$. Questo polinomio é dato da

$$\mathbf{f}(x) = \sum_{i=0}^{n} b_i \prod_{k=0, k\neq i}^{n} (a_i - a_k)^{-1}(x - a_k). \tag{2.7}$$

Capitolo 3

Algoritmo di Berlekamp

3.1 Fattorizzazione su PICCOLI campi finiti

L algoritmo di Berlekamp per la costruzione di polinomi di f-riduzione fa uso del teorema cinese dei resti per i polinomi.
Supponiamo che f non ha fattori ripetuti in modo che

$$\mathbf{f} = f_1 \cdots f_k \tag{3.1}$$

é il prodotto di distinti polinomi monici e irriducibili su F_q.
Se $(c_1 \cdots c_k)$ é una k-upla di elementi di F_q il teorema cinese dei resti implica che ci sia un unico $h \in F_q$ con

$$\mathbf{h} \equiv c_i mod f_i(x) \forall 1 \leq i \leq k deg(h) \lneq deg(f) \tag{3.2}$$

il polinomio $h(x)$soddisfa l equazione

$$\mathbf{h}^q(x) \equiv c_i^q = c_i \equiv h(x) mod f_i(x) con 1 \leq i \leq k \tag{3.3}$$

e quindi

$$\mathbf{h}^q(x) \equiv h(x) mod f(x) condeg(h) \lneq deg(f) \tag{3.4}$$

d'altra parte se h é soluzione della (3.4)allora l'identitá

$$\mathbf{h}^q(x) - h(x) = \prod_{c \in F_q} h(x) - c \tag{3.5}$$

implica che ogni fattore irriducibile di f divide uno dei polinomi $h(x) - c$.
Tutte le soluzioni della (3.4)soddisfano l'equazione

$$\mathbf{h}(x) \equiv c_i mod f_i con 1 \leq i \leq k \tag{3.6}$$

per qualche k-upla $(c_1 \cdots c_k)$ di elementi di F_q.Di conseguenza ci sono esattamente q^k soluzioni della (3.4).
Troviamo queste soluzioni attraverso la riduzione di (3.4) ad un sistema di equazioni lineari con $n = deg(f)$ costruiamo una matrice $n * n$ $B = (b_{ij})$ con $0 \leq ij \leq n-1$ calcolando le potenze$x^{iq} mod f(x)$.
Sia quindi

$$\mathbf{x}^{iq} = \sum_{j=0}^{n-1} b_{ij} x^j mod f(x) per 0 \leq i \leq n-1 \tag{3.7}$$

abbiamo allora che $h(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in F_q[x]$ é soluzione della (3.4) se e soltanto se

$$(a_0, a_1, \cdots, a_{n-1})B = (a_0, a_1, \cdots, a_{n-1}). \tag{3.8}$$

Ció deriva dal fatto che vale se e solo se
$h(x) = \sum_{j=0}^{n-1} a_j x^j = \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} a_i b_{ij} x^j \equiv \sum_{i=0}^{n-1} a_i x^{iq} = h^q(x) mod f(x)$
il sistema (3.8)puó essere quindi scritto come

$$(a_0, a_1, \cdots, a_{n-1})B - I = (0, 0, \cdots, 0). \tag{3.9}$$

Dove I é la matrice identitá inF_q.
Dalle considerazioni fatte il sistema (3.9) ha q^k soluzioni.
La dimensione dello spazio nullo della matrice$B-I$ é k,il numero dei fattori monici distinti irriducibili e il rango della matrice $B - I$ é $(n - k)$.
Dato che il polinomio costante $h_1(x) = 1$ é sempre una soluzione della (3.4) il vettore $(1, 0, \cdots, 0)$ é sempre soluzione dellla (3.9).Esisteranno $h_2(x), \cdots, h_k(x)$ polinomi di grado minore o uguale a $n - 1$ in modo che i vettori corrispondenti a $(h_1(x), h_2(x), \cdots, h_k(x))$ formino una base per lo spazio nullo di $B - I$.
I polinomi $h_2(x), \cdots, h_k(x)$ sono di grado positivo e sono una f-riduzione.
In questo approccio un ruolo fondamentale é svolto dalla determinazione del rango r della matrice$B - I$.
Abbiamo $r = n-k$ in modo che una volta che il rango r é stato strovato sappiamo che il numero di fattori irriducibili monici e distinti é dato da $k = n - r$.Sulla base di queste informazioni siamo in grado di decidere quando la procedura di fattorizzazione puó essere fermata.Il rango di$B - I$ puó essere determinato usando operazioni sulle righe e sulle colonne per ridurre la matrice a gradini.É consigliabile utilizzare solo operazioni colonna:cosí ci é permesso di moltiplicare ogni colonna della matrice $B - I$ per un elemento non nullo di F_q ed aggiungere il multiplo di qualche colonna ad una differente colonna.Il rango r é il numero di colonne diverse da zero nella forma a gradini.
Avendo trovato r sappiamo $k = n - r$.
Se $k = 1$ sappiamo che f é irriducibile su F_q e la procedura termina.
In questo caso le uniche soluzioni di(3.4)sono i polinomi costanti e lo spazio nullo

di $B - I$ contiene solo vettori della forma $(c, 0, \cdots, 0)$ conc $\in F_q$.
Se $k \geq 2$ prendiamo il polinomio base della f-riduzione $h_2(x)$ e calcoliamo

$$\mathbf{M}CD(f(x), h_2(x) - c) \tag{3.10}$$

$\forall c \in F_q$.Il risultato sará una fattorizzazione non banale fornita dalla (1.4).Se $h_2(x)$ non riesce a dividere $f(x)$ in k fattori calcoliamo il $MCD(g(x), h_3(x) - c)$ $\forall c \in F_q$ e tutti i fattori $g(x)$ non banali trovati fino ad ora.Questa procedura va avanti fin tanto non vengono trovati tutti i k fattori di $f(x)$.
Il processo sopra descritto deve restituire tutti i fattori infattise consideriamo due fattori distinti irriducibili e monici di $f(x)$,chiamandoli $f_1(x)$ e $f_2(x)$ per la (3.4) esistono $c_{j1}, c_{j2} \in F_q$ tale che $\forall j, 1 \leq j \leq k$

$$\mathbf{h}_j(x) \equiv c_{j1} mod f_1(x) \tag{3.11}$$

$$\mathbf{h}_j(x) \equiv c_{j2} mod f_2(x) \tag{3.12}$$

Supponiamo di avere $c_{j1} = c_{j2}$ per $1 \leq j \leq k$ poiché qualsiasi soluzione $h(x)$ della (3.4) é una combinazione lineare di $h_1(x), h_2(x), \cdots, h_k(x)$, con coefficenti in F_q esisterebbe per ogni $h(x)$ un elemento $c \in F_q$ con

$$\mathbf{h}(x) \equiv c mod f_1(x) \tag{3.13}$$

$$\mathbf{h}(x) \equiv c mod f_2(x) \tag{3.14}$$

Ma da ció che ci mostra la (3.4) in particolare esiste una sola soluzione $h(x)$ per cui vale $h(x) \equiv cmodf_1, h(x) \equiv cmodf_2$.Questa contraddizione prova che $c_{j1} \neq c_{j2}$ $\forall j\ 1 \leq j \leq k$ (infatti se $h_1(x) = 1$ avremmo $j \geq 2$).
Quindi ogni due fattori monici e irriducibili di $f(x)$ distinti sono separati da qualche polinomio $h_j(x)$.

3.2 Esempio

Fattorizziamo il polinomio $f(x) = x^8 + x^6 + x^4 + x^3 + 1$ su F_2 utilizzando l algoritmo di Berlekamp sopra descritto.
Poiché il $MCD(f(x), f'(x)) = 1$, $f(x)$ non ha fattori ripetuti.
Calcoliamo $x^{iq} modf(x)$ con $q = 2$ e $0 \leq i \leq 7$ producendo le seguenti congruenze
$x^0 = 1$
$x^2 = x^2$
$x^4 = x^4$
$x^6 = x^6$
$x^8 = 1 + x^3 + x^4 + x^6$
$x^{10} = 1 + x^2 + x^3 + x^4 + x^5$
$x^{12} = x^2 + x^4 + x^5 + x^6 + x^7$
$x^{14} = 1 + x + x^3 + x^4 + x^5$
Possiamo ora costruire la matrice dei coefficenti B:

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} \tag{3.15}$$

Calcoliamo ora la matrice B-I:

$$B - I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \tag{3.16}$$

Lavorando sulle colonne di questa matrice(per esempio sommando la seconda colonna alla quinta otteniamo la quarta) ci rendiamo conto che il rango di $B - I$ é $r = 6$;quindi $k = n - r = 8 - 6 = 2$.

Poiché $k \neq 1$ il polinomio $f(x)$ é riducibile su F_2.

I vettori $(1, 0, 0, 0, 0, 0, 0, 0)$ e $(0, 1, 1, 0, 0, 1, 1, 1)$ formano una base dello spazio nullo $B - I$ e i polinomi corrisondenti sono

$$h_1(x) = 1 \qquad\qquad h_2(x) = x + x^2 + x^5 + x^6 + x^7$$

Calcoliamo il $MCD(f(x), h_2(x) - c)\ \forall c \in F_2$

$MCD(f(x), h_2(x)) = MCD(x^8 + x^6 + x^4 + x^3 + 1, x + x^2 + x^5 + x^6 + x^7) = x^6 + x^5 + x^4 + x + 1$

e

$MCD(f(x), h_2(x) - 1) = MCD(x^8 + x^6 + x^4 + x^3 + 1, 1 + x + x^2 + x^5 + x^6 + x^7) = x^2 + x + 1$

Quindi la fattorizzazione canonica desiderata é

$f(x) = g_1(x)g_2(x) = (x^6 + x^5 + x^4 + x + 1)(x^2 + x + 1)$

3.3 Fattorizzazione su GRANDI campi finiti

Se F_q é un campo finito con q un gran numero di elementi,l'applicazione del metodo sopra descritto nella pratica diventa complicata poiché la(2.4) ci richiede di determinare il calcolo di q massimi comun divisori.Per rendere fattibile l?utilizzo delle f-riduzioni su campi finiti di grandi dimensioni é necessario trovare un modo per ridurre gli elementi $c \in F_q$ per i quali deve essere calcolato il MCD nella (2.4).Naturalmente nel contesto di fattorizzazione consideriamo q come "GRANDE se sostanzialmente q é piú grande del grado del polinomio da fattorizzare.

Sia f un polinomio monico in F_q senza fattori ripetuti,sia $deg(f) = n$ e sia k il numero dei fattori irriducibili monici distinti di f.Supponiamo che $h \in F_q[x]$ soddisfa

$$h^q \equiv hmodf \qquad\qquad 0 \lneq deg(h) \lneq n$$

in modo che h é una f-riduzione.Dal momento che i vari massimo comun divisori nella (2.4) sono primi relativamente a coppie é chiaro che al piú k di questi MCD sono $\neq 1$.Lo scopo ora é trovare una caratterizzazione a priori di quei $c \in F_q$ per cui $MCD(f(x), h(x) - c) \neq 1$.

Una caratterizzazione tale puó essere ottenuta utilizzando la teoria delle risultanti

trattata nella Definizione 1.

Sia $R(f(x), h(x)-c)$ la risultante di $f(x)$ e $h(x)-c$ allora il $MCD(f(x), h(x)-c) \neq 1$ se e solo se $R(f(x), h(x)-c) = 0$.Siamo cosí condotti a considerare

$$\mathbf{F}(y) = R(f(x), h(x) - y) \tag{3.17}$$

che dalla rappresentazione della risultante come determinante,é visto come un polinomio di grado$\leq n$.Abbiamo $MCD(f(x), h(x) - c) \neq 1$ se e solo se c é una radice di $F(y)$ in F_q.

Il polinomio $F(y)$ puó essere calcolato dalla definizione che comporta la determinazione di un determinante di grado $lneq2n - 1$;tuttavia é preferibile usare il seguente metodo.

Scegliamo $n + 1$ elementi distinti $c_0, c_1, \cdots, c_n \in F_q$ e calcoliamo le risultanti $r_i = R(f(x), h(x) - c_i)$ per $0 \leq i \leq n$;l' unico polinomio $F(y)$ di grado $\leq n$ con $F(c_i) = r_i$ per $0 \leq i \leq n$ é ottenuta dalla formula di interpolazione di Lagrange(Teo 4).Questo metodo ha il vantaggio che se un solo r_j é uguale a zero si ottiene automaticamente le radici del polinomio $F(y)$ in F_q. In ogni caso,il problema di isolare gli elementi $c \in F_q$ con il $MCD(f(x), h(x)-c) \neq 1$ é ora ridotto a trovare le radici di un polinomio in F_q.

3.4 Esempio

Fattorizziamo $f(x) = x^6 - 3x^5 + 5x^4 - 9x^3 - 5x^2 + 6x + 7$ su F_{23}.Poiché $MCD(f(x), f'(x)) = 1$,$f(x)$ non ha fattori ripetuti.Procediamo con l'algoritmo di Berlekamp e calcoliamo $x^{23i} mod\ f(x)$ per $0 \leq i \leq 5$.Costruiamo la matrice $B\ 6 * 6$

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & -1 & 8 & -3 & -10 \\ -10 & 10 & 10 & 0 & 1 & 9 \\ 0 & 7 & 9 & -8 & 10 & -11 \\ 11 & 0 & -4 & 7 & 7 & 2 \\ -3 & 0 & -10 & 9 & 2 & -10 \end{pmatrix} \tag{3.18}$$

$$B - I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & -1 & -1 & 8 & -3 & 10 \\ -10 & 10 & 9 & 0 & 1 & -9 \\ 0 & 7 & 9 & -9 & 10 & -11 \\ 11 & 0 & -4 & 7 & 6 & 2 \\ -3 & 0 & -10 & 9 & 2 & -10 \end{pmatrix} \tag{3.19}$$

Riducendo la matrice in una forma a gradini se ne deduce che il rango di $B - I$ é $r = 3$ cosí che il polinomio f ha $k = n - r = 6 - 3 = 3$ distinti fattori monici e irriducibili in $F_{23}[x]$.

Una base per lo spazio nullo di $B - I$ é data dai vettori $h_1 = (1, 0, 0, 0, 0, 0)$, $h_2 = (0, 4, 2, 1, 0, 0)$, $h_3 = (0, -2, 9, 0, 1, 1)$ i quali corrispondono ai polinomi $h_1(x) = 1$, $h_2(x) = x^3 + 2x^2 + 4x$, $h_3(x) = x^5 + x^4 + 9x^2 - 2x$.Consideriamo il polinomio f-riducente $h_2(x)$ e calcoliamo

$$\mathbf{F}(y) = R(f(x), h_2(x) - y) = \tag{3.20}$$

$$F(y) = \begin{pmatrix} 1 & -3 & 5 & -9 & -5 & 6 & 7 & 0 & 0 \\ 0 & 1 & -3 & 5 & -9 & -5 & 6 & 7 & 0 \\ 0 & 0 & 1 & -3 & 5 & -9 & -5 & 6 & 7 \\ 1 & 2 & 4 & -y & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 4 & -y & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 4 & -y & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 4 & -y & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 4 & -y & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & -y \end{pmatrix} \tag{3.21}$$

In questo caso é fattibile un diretto calcolo di $F(y)$ e otteniamo $F(y) = y^6 + 4y^5 + 3y^4 - 7y^3 + 10y^2 + 11y + 7$.Poiché f ha tre fattori monici irriducibili in $F_{23}[x]$ il polinomio F puó avere al piú tre distine radici in F_{23} che sono -3, 2 e 6.
Inoltre

$$\mathbf{M}CD(f(x), h_2(x) + 3) = x - 4, \tag{3.22}$$

$$\mathbf{M}CD(f(x), h_2(x) - 2) = x^2 - x + 7, \tag{3.23}$$

$$\mathbf{M}CD(f(x), h_2(x) - 6) = x^3 - 2x^2 + 4x - 6, \tag{3.24}$$

Cosí allora $f(x) = (x-4)(x^2 - x + 7)(x^3 - 2x^2 + 4x - 6)$ é la fattorizzazione canonica di$f(x)$ su $F_{23}[x]$