Università degli Studi di Torino

Dipartimento di Matematica Giuseppe Peano

Scuola di Scienze della Natura

Corso di Laurea in Matematica

Tesi di Laurea Triennale

Sulla Fattorizzazione di Polinomi su Campi Finiti

Relatore: Prof.ssa Lea Terracini

Candidato: Vittorio Valent

2016/2017

Indice

Introduzione

L'obiettivo di questa dissertazione è dare una piccola rassegna di alcuni dei primi, e più celebri, algoritmi di fattorizzazione di polinomi a coefficienti in campi finiti.

Il problema della fattorizzazione, anche detta scomposizione in fattori primi, lo si incontra già nei primi anni di scuola (scuole medie per gli interi e superiori per i polinomi) ed è piuttosto semplice da comprendere: dato un numero si vuole trovare quei numeri che moltiplicati tra loro danno come risultato il numero da cui si è partiti. Se vogliamo, ad esempio, fattorizzare 45 possiamo scrivere che $45 = 9 \times 5$. Ora 5 è un numero primo, mentre 9 non lo è: infatti abbiamo $9 = 3 \times 3$ dove 3 è un numero primo. Allora diciamo che la fattorizzazione (unica) di 45 è $3 \times 3 \times 5$. In modo analogo possiamo fattorizzare polinomi: una delle regole di scomposizione di polinomi più famose asserisce che $(x^2 - c^2) = (x + c)(x - c)$. Se infatti moltiplichiamo i fattori ottenuti risulta $(x + c)(x - c) = (x^2 + xc - xc - c^2) = (x^2 - c^2)$, dove quest'ultimo è proprio il polinomio da cui siamo partiti.

Si potrebbe a questo punto pensare che il problema descritto sia banale e di poco interesse matematico, se non a livello elementare. Ma la complessità del problema diventa presto manifesta: sappiamo infatti fattorizzare (anche a mano, come abbiamo fatto con 45 e $(x^2 - c^2)$) numeri e polinomi di poche cifre e di grado basso. Al crescere della taglia dei numeri in gioco, del grado dei polinomi e della cardinalità del campo finito dove questi sono definiti il problema diventa di difficile risoluzione, persino per i moderni calcolatori. Sugli interi la fattorizzazione resta un problema *quasi* impossibile: non esistono infatti algoritmi efficienti per fattorizzare numeri grandi. Con qualche strumento di algebra e di teoria dei campi possiamo invece implementare degli algoritmi di fattorizzazione di polinomi che possano terminare in un tempo accettabile. Ora la difficoltà della scomposizione sugli interi, la quale garantisce, per altro, la sicurezza della maggior parte della crittografia a chiave pubblica, non è oggetto di questa tesi; ci occuperemo invece di fattorizzare polinomi. Scomporre in fattori irriducibili questi oggetti è utile infatti per creare codici correttori, nella fattispecie codici ciclici, e per lo studio delle ricorrenze lineari sui campi finiti.

Cercheremo di costruire dunque dei procedimenti, i quali si possano implementare al calcolatore, che preso in input un polinomio e il campo finito dove vogliamo fattorizzarlo, restituisca (possibilmente in modo *deterministico*) in output la sua fattorizzazione unica. Questo non sarà sempre possibile: l'algoritmo per la ricerca delle radici risulterà, in effetti, un algoritmo *probabilistico*: uno dei possibili output sarà `nessuna risposta` .

Per arrivare ai risultati esposti nel Capitolo 3 verranno sviluppati definizioni e teoremi i quali saranno i principali strumenti per costruire gli algoritmi.
Il primo capitolo sarà interamente dedicato a definire gli oggetti e le strutture algebriche con cui lavoreremo e saranno anche esposti diversi risultati di algebra di base (senza dimostrazione) utili a provare gli asserti dei capitoli successivi.
Nel secondo capitolo si troveranno i principali teoremi e proposizioni relativi alla Teoria dei Campi di Galois e ai polinomi definiti su questi ultimi. Essendo questi gli strumenti definitivi per lo studio e la costruzione degli algoritmi di fattorizzazione, essi saranno

(quasi) tutti dimostrati.
Il terzo ed ultimo capitolo è dedicato all'argomento principale della tesi: la presentazione e la discussione di tre diversi algoritmi di fattorizzazione. Il primo è l'Algoritmo di Berlekamp, sviluppato da Elwyn R. Berlekamp nel 1967. Esso rappresenta uno dei primissimi algoritmi atti a questo scopo ed usa principalmente strumenti di algebra lineare e calcolo del massimo comune divisore tra polinomi. Vedremo in seguito l'Algoritmo di McEliece, sviluppato sempre nel 1967 da Robert J. McEliece alla JPL. Esso si discosta dall'algoritmo precedente per l'uso di alcune proprietà delle tracce su campi finiti ed un utilizzo massiccio del calcolo del massimo comune divisore. L'ultimo algoritmo, denominato Algoritmo di Ricerca delle Radici (talvolta abbreviato R.d.R.), è adatto invece a trovare radici di un polinomio su un campo finito di cardinalità grande. Infine vi sarà un breve confronto qualitativo tra questi algoritmi e sarà data (senza dimostrazione) la loro efficienza.

Capitolo 1

Fondamenti di Algebra

Questo primo capitolo è dedicato ad una rapida esposizione di alcuni risultati di base sull'algebra delle strutture di gruppi, anelli e campi. Vedremo come, astraendo le principali operazioni aritmetiche e sostituendo agli usuali numeri dei simboli come ad esempio le lettere, si potrà lavorare in una generalità maggiore della semplice aritmetica elementare. Partendo quindi da strutture definite da assiomi molto semplici dimostreremo risultati importanti e utili a provare diverse proposizioni nei capitoli successivi, in particolare relative alla Teoria dei Campi.
Poiché i risultati che seguiranno in questo capitolo sono sì importanti ma semplici da dimostrare e intuitivi, verrà omessa la dimostrazione di alcuni.

1.1 Gruppi, anelli e campi

Definiamo in primo luogo una struttura algebrica formata da un insieme e un'operazione: la struttura di gruppo.

Definizione 1.1. Si dice *gruppo* un insieme G dotato di un'operazione binaria $*$ che rispetti le seguenti proprietà:

1. $*$ è associativa, cioè per ogni $a, b, c \in G$ si ha che $a * (b * c) = (a * b) * c$;
2. esiste in G un elemento e tale che per ogni $a \in G$ $a * e = e * a = a$. In tal caso e è detto *identità*[1] ;
3. per ogni $a \in G$ esiste $a^{-1} \in G$ tale che $a * a^{-1} = a^{-1} * a = e$. In tal caso a^{-1} è detto *inverso* di a.

Il gruppo è detto *abeliano* (o *commutativo*) se

4. Per ogni $a, b \in G$ si ha che $a * b = b * a$.

La struttura di gruppo si indica con la notazione $(G, *)$.

Si osserva immediatamente che gli assiomi precedenti garantiscono, in un gruppo G, l'unicità dell'identità e degli inversi. In seguito useremo la notazione ab per indicare $a * b$ in un gruppo generico moltiplicativo. Nei gruppi abeliani additivi useremo scrivere $a + b$ invece di $a * b$ e $-a$ al posto di a^{-1}. Useremo inoltre le seguenti notazioni:

$$a^n = aa \cdots a \qquad (a \text{ moltiplicato per se stesso } n \text{ volte})$$
$$na = a + a + \ldots a \qquad (a \text{ sommato a se stesso } n \text{ volte})$$

[1] In alcuni testi si chiama anche *unità*, qui viene usato il termine identità per non creare confusione con la definizione di unità come elemento divisore dell'identità.

Seguendo una notazione standard, abbiamo le seguenti regole:

Notazione Moltiplicativa	*Notazione Additiva*
$a^{-n} = (a^{-1})^n$	$(-n)a = n(-a)$
$a^n a^m = a^{n+m}$	$na + ma = (n+m)a$
$(a^n)^m = a^{nm}$	$m(na) = (mn)a$

Definizione 1.2. Un gruppo moltiplicativo G è detto *ciclico* se esiste un elemento $a \in G$ tale che per ogni $b \in G$ si trova un intero j tale per cui $b = a^j$. In tal caso a si dice *generatore* del gruppo ciclico G e scriviamo $G = \langle a \rangle$ (G è *generato* da a).

Osserviamo che ogni gruppo ciclico è abeliano, infatti dato g generatore si ha che per ogni $a, b \in G$ e per qualche i, j interi $ab = g^i g^j = g^{i+j} = g^{j+i} = g^j g^i = ba$.

Definiamo ora un importante tipo di relazione algebrica binaria, la cosiddetta *relazione di equivalenza*.

Definizione 1.3. Sia S un insieme, $\sim$ si dice relazione di equivalenza se gode delle seguenti proprietà:

1. per ogni $x \in S$ si ha che $x \sim x$; (riflessività)
2. per ogni $x, y \in S$ si ha che $x \sim y \Rightarrow y \sim x$; (simmetria)
3. per ogni $x, y, z \in S$ si ha che $x \sim y, y \sim z \Rightarrow x \sim z$. (transitività)

Osserviamo che, data $\sim$ relazione di equivalenza, gli insiemi del tipo

$$[x] = \{y \in S : x \sim y\}$$

formano una partizione di S al variare di $x \in S$. $[x]$ si dice *classe di equivalenza di x*.

Definizione 1.4. Dati due interi a e b e un intero positivo n diciamo che a è congruente a b modulo n, scrivendo $a \equiv b \mod (n)$, se $n|a-b$, cioè se $a = b + kn$ per qualche k (equivalentemente a e b danno lo stesso resto quando divisi per n). Si verifica facilmente che la congruenza modulo n è una relazione di equivalenza su $\mathbb{Z}$.

Osservazione 1.5. Date $a, b \in \mathbb{Z}$ si ha che

$$[a+b] = [a] + [b]$$

Definizione 1.6. In virtù dell'osservazione precedente possiamo dare una buona definizione del gruppo (ciclico additivo) delle classi di equivalenza in $\mathbb{Z}$ modulo n:

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$$

Definizione 1.7. Una mappa $f : G \longrightarrow H$, dove $(G, *)$ e $(H, \star)$ godono della struttura di gruppo, è detto *morfismo* di G in H se $f(a*b) = f(a) \star f(b)$ per ogni $a, b \in G$. Inoltre se f è suriettivo e iniettivo f si dice *isomorfismo*.

Definizione 1.8. Sia $f : G \longrightarrow H$ un morfismo. Definiamo nucleo di f come

$$\ker f = \{a \in G : f(a) = e'\}$$

dove e' è l'identità in H.

Proposizione 1.9. *Sia $f : G \longrightarrow H$ un morfismo. Allora f è iniettivo se e solo se* $\ker f = \{e\}$*, dove e è l'identità di G.*

Enunciamo (e dimostriamo) ora un risultato di importanza cardinale: il Teorema Cinese dei Resti.

Teorema 1.10 (Teorema Cinese dei Resti)**.** *Siano $n_1, \ldots, n_k$ interi positivi tali che $\mathrm{mcd}(n_i, n_j) = 1$ per ogni $i \neq j$ e $a_1, \ldots, a_k$ interi. Sia ancora $N = n_1 \cdot \ldots \cdot n_k$ Allora il sistema di congruenze*

$$\begin{cases} x \equiv a_1 & \mod (n_1) \\ \vdots \quad \vdots & \vdots \\ x \equiv a_k & \mod (n_k) \end{cases} \tag{1.1}$$

ammette un'unica soluzione modulo N.

Dimostrazione. Consideriamo la funzione θ così definita:

$$\begin{cases} \theta : \mathbb{Z}_N \longrightarrow \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k} \\ \theta : [a]_N \longmapsto ([a]_{n_1}, \ldots, [a]_{n_k}) \end{cases}$$

. Mostriamo che θ è un isomorfismo.

- θ è un morfismo, infatti presi $a, b \in \mathbb{Z}$ abbiamo che, secondo l'Osservazione 1.5

$$\begin{aligned} \theta([a]_N + [b]_N) &= \theta([a+b]_N) & = \\ &= ([a+b]_{n_1}, \ldots, [a+b]_{n_k}) & = \\ &= ([a]_{n_1}, \ldots, [a]_{n_k}) + ([b]_{n_1}, \ldots, [b]_{n_k}) & = \\ &= \theta([a]_N) + \theta([b]_N) \end{aligned}$$

- θ è un morfismo iniettivo: poiché gli n_i sono a due a due coprimi $([a]_{n_1}, \ldots, [a]_{n_k}) = ([0]_{n_1}, \ldots, [0]_{n_k})$ se e solo se $a = 0$, e quindi $\ker \theta = [0]$. Allora θ è iniettivo.
- θ è un morfismo suriettivo, infatti $|\mathbb{Z}_N| = N = n_1 \cdot \ldots \cdot n_k = |\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}|$, perciò dato che θ è iniettivo e ha come dominio e codominio insiemi di medesima cardinalità è automaticamente suriettivo.

Allora θ è un isomorfismo. Di conseguenza, la soluzione del sistema 1.1, visto come k-upla $([a]_{n_1}, \ldots, [a]_{n_k})$ ha una e una sola soluzione in $\mathbb{Z}_N$. □

Abbiamo visto finora come studiare un insieme e un'operazione su di esso. Tuttavia la maggior parte dei nostri sistemi numerici, si vedano i numeri interi o razionali, è dotata di due operazioni. Aggiungiamo quindi un'operazione ai nostri insiemi e passiamo alla definizione di strutture algebriche più complesse: gli anelli e i campi.

Definizione 1.11. Un *anello* è una struttura $(R, +, \cdot)$ formata dall'insieme R insieme a due operazioni $+$ e $\cdot$ tali che:

1. $(R, +)$ è un gruppo abeliano;
2. $\cdot$ è associativa, cioè per ogni $a, b, c \in R$ si ha che $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
3. Valgono le proprietà distributive, cioè per ogni $a, b, c \in R$ si ha che $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$;

Useremo spesso la notazione R invece di $(R, +, \cdot)$ per indicare un anello. Nonostante $+$ e $\cdot$ non siano necessariamente le usuali operazioni tra numeri indicheremo con 0 l'elemento neutro di R rispetto a $+$. L'inverso additivo di un elemento a sarà d'ora in poi denotato con $-a$; l'operazione $a + (-b)$ abbreviata con $a - b$; invece di $a \cdot b$ scriveremo ab. Dalla definizione di anello deduciamo che per ogni $a \in R$ vale che $a0 = 0a = 0$, pertanto per ogni $a, b \in R$ si ha che $(-a)b = a(-b) = -ab$. Introduciamo ora altre caratteristiche che un anello può avere, arrivando così alla definizione di campo.

Definizione 1.12. Dato $(R, +, \cdot)$ anello abbiamo che:

1. R si dice *anello con identità* se esiste un elemento e tale che $ae = ea = a$ per ogni $a \in R$;
2. R si dice *anello commutativo* se l'operazione $\cdot$ è commutativa;
3. R si dice *dominio di integrità* se è un anello commutativo con identità $e \neq 0$ nel quale $ab = 0$ implica che $a = 0$ oppure $b = 0$;
4. R si dice *corpo* se gli elementi non nulli di R formano un gruppo rispetto all'operazione $\cdot$;
5. un corpo commutativo si dice *campo*.

Teorema 1.13. *Ogni dominio di integrità finito è un campo.*

Dimostrazione. Siano $a_1, a_2, \ldots, a_n$ gli elementi di R dominio di integrità. Sia $a \in R$ un elemento non nullo, consideriamo allora i prodotti $aa_1, aa_2, \ldots, aa_n$. Questi devono essere tutti distinti, infatti se fosse che $aa_i = aa_j$ per $i \neq j$ avremmo che $aa_i - aa_j = a(a_i - a_j) = 0$. Poiché $a \neq 0$ deve essere che $a_i = a_j$. Inoltre per qualche i sarà che $e = aa_i = a_i a$ per commutatività. Pertanto a_i è l'inverso moltiplicativo di a. Dato che a è un generico elemento non nullo, $R \setminus \{0\}$ è un gruppo abeliano rispetto a $\cdot$ e quindi R è un campo. □

Di seguito vederemo alcune proprietà degli anelli e dei campi, soffermandoci su queste ultime. Sebbene anelli e gruppi siano strutture affascinanti e dotate di una loro teoria molto complessa, qui analizzeremo unicamente le proprietà utili ai fini della dissertazione. Introduciamo quindi il concetto di sottoanello, ideale e anello quoziente.

Definizione 1.14. Diciamo che un sottoinsieme S dell'anello R è un *sottoanello* se è a sua volta un anello rispetto alle operazioni di R.

Definizione 1.15. Un sottoanello J è detto *ideale* dell'anello R se per ogni $a \in J$ e per ogni $r \in R$ si ha che $ar \in J$ e $ra \in J$.

Definizione 1.16. Sia R un anello commutativo con identità. Un ideale J è detto *principale* se esiste $a \in R$ tale che $J = \{ra : r \in R\}$. In tal caso diciamo che J è l'ideale principale *generato da* a e lo denotiamo con (a).

Definizione 1.17. Così come nella Definizione 1.4 possiamo definire una relazione di equivalenza così data: dati due elementi $a, b \in R$ diciamo che $a \equiv b \mod J$ se e solo se $a - b \in J$.

Si verifica immediatamente che questa è una relazione di equivalenza, la quale induce pertanto un insieme delle classi di resto. Queste si denotano con $a + J = \{a + c : c \in J\}$[2]. L'insieme così ottenuto si denota con R/J; il fatto che J sia un ideale fa sì che le seguenti operazioni siano ben definite:

$$(a + J) + (b + J) = (a + b) + J \tag{1.2}$$

$$(a + J)(b + J) = (ab) + J. \tag{1.3}$$

Pertanto è immediato verificare che R/J è un anello.

Definizione 1.18. L'insieme R/J con le operazioni 1.2 e 1.3 si dice *anello quoziente* o *anello delle classi di resto modulo J*.

Teorema 1.19. *$\mathbb{Z}/(p)$, ossia l'anello delle classi di resto degli interi modulo l'ideale generato da un primo p, è un campo.*

[2]Spesso, per brevità, useremo la notazione [a]=a+J.

Dimostrazione. In virtù del Teorema 1.13 basta mostrare che $\mathbb{Z}/(p)$ è un dominio di integrità. Si ha che [1] è banalmente l'identità moltiplicativa di $\mathbb{Z}/(p)$. Siano ora $a, b \in \mathbb{Z}/(p)$ tali che $[a][b] = 0$, cioè $ab \in J$. Allora $p|ab$ e pertanto $p|a$ oppure $p|b$ (poiché p è primo). Allora abbiamo che $[a] = 0$ oppure $[b] = 0$. Quindi $\mathbb{Z}/(p)$ è finito, commutativo e non contiene zero-divisori: concludiamo pertanto che esso è un campo. □

Definizione 1.20. Sia R un anello e supponiamo esistano degli interi positivi n_i tale che $n_i r = 0$ per ogni $r \in R$. Allora il più piccolo tra gli n_i si dice *caratteristica* di R: Se non esiste nessun intero positivo n con le precedenti proprietà diciamo che R ha caratteristica 0.

Si dimostra facilmente che se R è un anello con identità allora la sua caratteristica è il più piccolo intero n tale che $n \cdot 1 = 0$.

Teorema 1.21. *Un anello R di caratteristica positiva, con identità e privo di zero-divisori deve avere come caratteristica un numero primo.*

Dimostrazione. Poiché R non contiene zero-divisori la sua caratteristica deve essere $n \geq 2$. Supponiamo che $n = hk$ con $h, k \in \mathbb{Z}$, $n > h > 1$ e $k < n$. Allora avremmo che

$$0 = ne = (hk)e = (he)(ke),$$

pertanto deve essere che $he = 0$ o $ke = 0$. Ma allora, per ogni $r \in R$, sarà che $hr = (he)r = 0$ oppure $kr = (ke)r = 0$. Allora la caratteristica di R è strettamente minore di n, in contraddizione con l'ipotesi. Concludiamo quindi che n deve essere primo. □

Corollario 1.22. *Un campo finito ha caratteristica prima.*

Teorema 1.23. *Sia R anello commutativo di caratteristica prima p. Allora*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \text{ e } (a-b)^{p^n} = a^{p^n} - b^{p^n}$$

per ogni $a, b \in R$ e per ogni $n \in \mathbb{N}$.

Dimostrazione. Siccome p e le sue potenze più piccole di n sono tutti e soli i divisori propri di p^n per ogni $n > 1$ è sufficiente dimostrare gli asserti per $n = 1$. Si ha che

$$\binom{p}{i} = \frac{p(p-1)\cdot \ldots \cdot (p-i+1)}{1 \cdot 2 \cdot \ldots \cdot i} \equiv 0 \mod p$$

per ogni $i \in \{1, \ldots, p-1\}$. Pertanto possiamo cancellare i termini dove compare il coefficiente binomiale:

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^p - ib^i = a^p + b^p$$

ed è così provata la prima identità. Per dimostrare la seconda è sufficiente osservare che

$$a^p = ((a-b)+b)^p = (a-b)^p + b^p.$$

□

Vediamo ora più nel dettaglio cosa lega le proprietà degli ideali di un anello e quelle del relativo anello quoziente. Per fare ciò introduciamo qualche definizione utile dalla teoria degli anelli.

Definizione 1.24. Sia R anello commutativo con identità. Un elemento $a \in R$ si dice *divisore* di $b \in R$ se esiste $c \in R$ tale che $ac = b$. Si dice *unità* un elemento ϵ che sia divisore dell'identità. Due elementi $a, b \in R$ si dicono *associati* se esite ϵ unità tale che $a = b\epsilon$. Un elemento $p \in R$ si dice *primo* se non è un'unità e ha come divisori solamente le unità di R e i suoi associati.

Definizione 1.25. Sia R anello commutativo con identità. Un ideale non banale J di R si dice

1. *primo* se, quando $ab \in J$, allora necessariamente $a \in J$ oppure $b \in J$;
2. *massimale* se, per ogni ideale $I \supseteq J$, si ha che $I = J$ oppure $I = R$.

Inoltre, dato R dominio di integrità, diciamo che esso è un *dominio a ideali principali* (o *PID*) se tutti i suoi ideali sono principali.

Teorema 1.26. *Sia R anello commutativo con identità, J ideale di R. Allora:*

(i) J è un ideale primo se e solo se R/J è un dominio di integrità;

(ii) J è un ideale massimale se e solo se R/J è un campo;

(iii) se J è massimale allora è anche primo;

(iv) se R è un dominio a ideali principali e $J = (c)$, R/J è un campo se e solo se c è un elemento primo di R;

(v) se R è un dominio a ideali principali e J è un ideale non nullo, allora J è primo se e solo é massimale.

1.2 Anelli di polinomi

In questa sezione introduciamo degli oggetti che sono di importanza centrale al fine di questa dissertazione: i polinomi.
Dato un generico anello R e n un intero positivo, si definisce *polinomio* un'espressione della forma

$$p(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n$$

dove gli a_i sono detti *coefficienti* e sono elementi di R e la x è *l'indeterminata* e non appartiene necessariamente a R. Dato un intero positivo h ogni polinomio della forma $p(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n$ può essere scritto come $p(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n + 0 \cdot x^{n+1} + \ldots + 0 \cdot x^{n+h}$. Talvolta nella trattazione verrà sottintesa la variabile del polinomio, il quale verrà indicato con f invece di $f(x)$. Dati due polinomi

$$f(x) = \sum_{i=0}^{n} a_i x^i \text{ e } g(x) = \sum_{i=0}^{n} b_i x^i$$

su un anello R diciamo $f(x) = g(x)$ se $a_i = b_i$ per ogni $i \in \{0, 1, \ldots, n\}$.
Definiamo anche la somma tra polinomi come

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

Dati ora due polinomi

$$f(x) = \sum_{i=0}^{n} a_i x^i \text{ e } g(x) = \sum_{j=0}^{m} b_j x^j$$

definiamo il prodotto tra $f(x)$ e $g(x)$ come

$$f(x) \cdot g(x) = \sum_{k=0}^{n+m} c_k x^k, \text{ dove } c_k = \sum_{i+j=k} a_i b_i.$$

Si può dimostrare che i polinomi a coefficienti in un anello formano a loro volta un anello con queste operazioni.

Definizione 1.27. L'insieme dei polinomi a coefficienti in un anello R con le operazioni di somma e prodotto si definisce *anello di polinomi* su R e si denota con $R[x]$.

L'elemento nullo in $R[x]$ è dato dal polinomio in cui tutti i coefficienti sono l'elemento nullo di R.

Definizione 1.28. Dato un polinomio non nullo $f(x) = \sum_{i=0}^{n} a_i x^i$ tale che $a_n \neq 0$ definiamo a_n *coefficiente direttore* e a_0 *termine noto*. n è detto *grado* di f (indicato con $\deg(f)$) e, qualora a_n dovesse essere l'identità di R, il polinomio f si dice *monico*.

Teorema 1.29. *Sia R un anello. Allora si ha che:*

(i) $R[x]$ è commutativo se e solo se R è commutativo;

(ii) $R[x]$ è un anello con identità se e solo se R è un anello con identità;

(iii) $R[x]$ è un dominio di integrità se e solo se R è un dominio di integrità;

Vediamo ora alcune utili proprietà e caratteristiche degli anelli di polinomi a coefficienti in un campo generico F. In primo luogo esiste in $F[x]$ un algoritmo di divisione con resto (simile a quella definita sull'anello degli interi).

Teorema 1.30 (Algoritmo di Divisione)**.** *Dato F campo e dato $g \neq 0$ polinomio in $F[x]$ allora per ogni $f \in F[x]$ esistono due polinomi q e r tali che*

$$f = qg + r, \text{ dove } \deg(r) < \deg(g).$$

Dal fatto che esiste su $F[x]$ un algoritmo di divisione deriva il seguente Teorema.

Teorema 1.31. *$F[x]$ è un dominio a ideali principali: ogni ideale J non banale è generato da un polinomio monico univocamente identificato.*

Teorema 1.32. *Siano $f_1, \ldots, f_n$ polinomi non tutti nulli in $F[x]$. Allora esiste un unico polinomio monico $d \in F[x]$ tale che.*

(i) $d | f_i$ per ogni $i \in \{1, \ldots, n\}$;

(ii) ogni polinomio $c \in F[x]$ con la proprietà (i) divide d.

Inoltre d può essere espresso nella forma

$$d = b_1 f_1 + \ldots + b_n f_n \text{ con } b_i \in F[x]. \tag{1.4}$$

Il polinomio d è detto massimo comun divisore di $f_1, \ldots, f_n$ e viene denotato con la scrittura $d = \mathrm{mcd}(f_1, \ldots, f_n)$.

Dimostrazione. Consideriamo l'ideale J di tutti i polinomi della forma $c_1 f_1 + \ldots + c_n f_n$ con $c_j \in F[x]$. Poiché i polinomi non sono tutti nulli si ha che $J \neq \{0\}$ e pertanto è generato da un polinomio monico d. Per il Teorema 1.31 esso è univocamente determinato. Se inoltre esistesse un polinomio d_1 con le proprietà (i) e (ii) allora $d | d_1$. Al contempo $d \in d_1$ e quindi $d_1 | d$. Segue che $d = d_1$. □

Nonostante la precedente dimostrazione non sia costruttiva, esiste un algoritmo basato sull'algoritmo di divisione euclideo che permette di calcolare velocemente il massimo comun divisore tra polinomi e l'identità 1.4.

Definizione 1.33. Dati $f_1, \ldots, f_n$ polinomi in $F[x]$ diciamo che essi sono *coprimi* se $\mathrm{mcd}(f_1, \ldots, f_n) = 1$. Diciamo che essi sono *a due a due coprimi* se $\mathrm{mcd}(f_i, f_j) = 1$ per ogni $i \neq j$.

Definizione 1.34. Un polinomio $p \in F[x]$ si dice *irriducibile* su F (o *primo* in $F[x]$) se ha grado positivo e se ogni scrittura del tipo $p = b \cdot c$ con $b, c \in F[x]$ implica che b o c sia un polinomio costante.

Un polinomio si dice *riducibile* quando esso non è irriducibile. Si osservi che la riducibilità di un polinomio dipende dal campo in cui esso è definito: ad esempio il polinomio x^2-3 è irriducibile in $\mathbb{Q}[x]$, mentre si fattorizza come $x^2-3=(x-\sqrt{3})(x+\sqrt{3})$ in $\mathbb{R}[x]$.

Teorema 1.35. *Ogni polinomio $f \in F[x]$ si fattorizza in maniera unica (a meno dell'ordine dei fattori) come*

$$f = a \cdot f_1 \cdot \ldots \cdot f_k \tag{1.5}$$

dove $a \in F$ e i polinomi f_i sono irriducibili su F.

Ci riferiremo d'ora in avanti alla formula 1.5 come *fattorizzazione canonica* di f. Vediamo ora alcuni teoremi e definizioni utili alla comprensione della prossima sezione.

Teorema 1.36. *$F[x]/(f)$ è un campo se e solo se f è irriducibile su F.*

Definizione 1.37. Un elemento $b \in F$ è detto *radice* di $f \in F[x]$ se $f(b)=0$.

Una stretta correlazione tra radici e divisibilità è data dal seguente teorema.

Teorema 1.38 (Teorema di Ruffini)**.** *Un elemento $b \in F$ è una radice di $f \in F[x]$ se e solo se il polinomio $x-b$ divide f.*

Dimostrazione. Usando l'algoritmo del Teorema 1.30 scriviamo $f(x)=q(x)(x-b)+c$. Se b è una radice di f allora $f(b)=0=c$ e pertanto $x-b$ divide f. Viceversa se $x-b$ divide f si ha che $f(x)=q(x)(x-b)$; allora $f(b)=0$ e concludiamo che b è una radice di f. □

Definizione 1.39. Sia $b \in F$ radice di $f \in F[x]$. Se k è un intero positivo tale che f è divisibile per $(x-b)^k$ ma non per $(x-b)^{k+1}$ allora k si dice *molteplicità* della radice b.

Definizione 1.40. Dato un polinomio $f(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}+a_nx^n$ definito su $F[x]$ definisco la sua *derivata formale* $f'(x)=a_1+2a_2x+\ldots+(n-1)a_{n-1}x^{n-2}+na_nx^{n-1}$.

Teorema 1.41. *Un elemento $b \in F$ è radice multipla (cioè con molteplicità $k \geq 2$) di $f \in F[x]$ se e solo se b è una radice di f e di f'.*

Dimostrazione. Supponiamo che b sia una radice con molteplicità $k \geq 2$ del polinomio $f(x)$. Allora possiamo scrivere $f(x)=(x-b)^k g(x)$. Derivando otteniamo $f'(x)=k(x-b)^{k-1}g(x)+(x-b)^k g'(x)$. Sostituendo si verifica che $f(b)=f'(b)=0$. Viceversa se $f(b)=f'(b)=0$ possiamo dire che, sviluppando formalmente con Taylor in $x=b$,

$$\begin{aligned} f(x) =& f(b)+f'(b)(x-b)+\ldots+\frac{1}{k!}f^{(k)}(b)(x-b)^k+\ldots+\frac{1}{n!}f^{(n)}(b)(x-b)^n = \\ =& \frac{1}{k!}f^{(k)}(b)(x-b)^k+\ldots+\frac{1}{n!}f^{(n)}(b)(x-b)^n \end{aligned}$$

dove k è il più piccolo intero tale che $f^{(k)}(b) \neq 0$. Allora è chiaro che $k \geq 2$ è la molteplicità della radice b □

Teorema 1.42. *Sia F un campo di caratteristica p, $f(x) \in K[x]$ un polinomio non costante. Allora $f'(x) \equiv 0$ se e solo se $f(x)=g(x)^p$.*

Dimostrazione. Se $f(x)=g(x)^p$ allora $f'(x)=pg(x)^{p-1}g(x) \equiv 0$ poiché siamo in caratteristica p. Viceversa consideriamo un polinomio $f(x)=\sum_{i=0}^{n} a_i x^i$; abbiamo che $f'(x)=\sum_{i=1}^{n} i a_i x^{i-1} \equiv 0$. Allora deve essere che, per ogni i tale che $a_i \neq 0$, $i \equiv 0$, cioè $i=pb$. Si osserva allora che è possibile raccogliere un esponente p da $f(x)$ (ricordiamo che l'elevazione alla potenza p è lineare sui campi finiti a caratteristica p). □

Teorema 1.43. *Sia $f \in K[x]$ tale che* $\mathrm{mcd}(f,f')=1$. *Allora f non ha fattori ripetuti.*

Dimostrazione. Sia $f(x) = g(x)^k q(x)$ con $k \geq 2$ (cioè f ha almeno un fattore ripetuto). Allora

$$\begin{aligned} f'(x) =& 2g(x)^{k-1} g'(x)q(x) + g(x)^k q'(x) = \\ =& g(x)^{k-1}(2g'(x)q(x) + g(x)q'(x)) \end{aligned}$$

Si osservi che f ed f' hanno un fattore almeno lineare $g(x)^{k-1}$ in comune. Allora $g(x)^{k-1} | \operatorname{mcd}(f, f') \neq 1$. □

1.3 Estensioni di campi

In questa ultima sezione introduttiva analizzeremo il concetto di estensione di campo. Tali nozioni saranno fondamentali per alcuni risultati di classificazione dei campi finiti che vedremo nel prossimo capitolo.

Definizione 1.44. Dato un campo F e K un suo sottoinsieme diciamo che, in analogia con quanto detto su gruppi e anelli, K è un *sottocampo* di F se è anch'esso un campo con le operazioni di F e F di dice *estensione (di campo)* di K. Se $K \neq F$ diciamo che K è un *sottocampo proprio* (o *non banale*) di F. Un campo non contenente sottocampi propri si dice *campo primo.*

Ad esempio tutti i campi finiti di ordine p, con p primo, sono campi primi. Il campo $\mathbb{Q}$ dei numeri razionali è un esempio di campo primo infinito. In particolare, dato un campo F e una collezione non vuota di suoi sottocampi K_i, $\cap K_i$ è ancora un sottocampo di F. Intersecando tutti i sottocampi di F otteniamo il suo *sottocampo primo*, il quale è naturalmente un campo primo.
Dalla definizione di campo primo passiamo ad un importante risultato di classificazione dei campi.

Teorema 1.45. *Sia F un campo. Allora il suo sottocampo primo è isomorfo a:*

- $\mathbb{F}_p$ *se ha caratteristica p;*
- $\mathbb{Q}$ *se ha caratteristica 0.*

Definizione 1.46. Sia K sottocampo di F e sia $\theta \in F$. Dico che $L = K(\theta)$ è l'*estensione semplice di K mediante l'aggiunta di θ*, definita come l'intersezione di tutti i sottocampi di F contenenti sia K che l'elemento θ. L risulta così essere il più piccolo sottocampo di F contenente sia K che θ.

Definizione 1.47. Sia K sottocampo di F e sia $\theta \in F$. Se θ soddisfa un'equazione polinomiale del tipo $a_0 + a_1\theta + \ldots + a_n\theta^n = 0$ con $a_i \in K$ non tutti nulli (cioè se θ è la radice di un polinomio non nullo in $K[x]$) diciamo che θ è *algebrico* su K. Un'estensione L di K si dice *estensione algebrica* se ogni elemento di L è algebrico su K.

Definizione 1.48. Sia $\theta \in F$ algebrico su K sottocampo di F. Sia g il polinomio (monico) che genera l'ideale $J = \{f \in K[x] : f(\theta) = 0\} = (g)$. Diciamo che g è il *polinomio minimo* di θ su K. Se $\deg(g) = n$ diciamo che n è il *grado (di estensione)* di θ su K.

Teorema 1.49. *Sia $\theta \in F$ algebrico su K sottocampo di F. Sia g il suo polinomio minimo. Allora:*

(i) g è irriducibile su $K[x]$;

(ii) per ogni $f \in K[x]$ si ha che $f(\theta) = 0$ se e solo se g divide f;

(iii) g è il polinomio di grado minimo avente come radice θ in $K[x]$.

Dimostrazione. Si osservi che (i) e (ii) seguono direttamente dalla Definizione 1.49 e dal Teorema 1.31. Sia ora $h(x) \in K[x]$ un polinomio monico tale che $h(\theta) = 0$. Per il punto (ii) si ha che g divide h, pertanto $\deg(h) \geq \deg(g)$. □

Definizione 1.50. Sia L un'estensione di K. Se L, considerata come spazio vettoriale su K, ha dimensione finita allora L è detta *estensione finita* di K. La dimensione di L come spazio vettoriale si dice *grado* di L su K e si indica con $[L : K]$.

Teorema 1.51. *Sia L un'estensione finita di K e M un'estensione finita di L. Allora M è un'estensione finita di K e vale che*

$$[M : K] = [M : L][L : K].$$

Teorema 1.52. *Ogni estensione finita di K è algebrica su K*

Dimostrazione. Data L estensione finita abbiamo che $[L : K] = m$. Per $\theta \in L$ gli $m + 1$ elementi $1, \theta, \ldots, \theta^m$ sono linearmente indipendenti su K, pertanto abbiamo che esistono $a_j \in K$ non tutti nulli tali che $a_0 + a_1\theta + \ldots + a_m\theta^m = 0$. Questo implica che θ è algebrico su K e quindi lo è anche L come estensione di campo. □

Ci poniamo ora il problema di capire quando un'estensione semplice è finita (e quindi algebrica). Il seguente Teorema mostra come, aggiungendo un elemento $\theta \in F$ al campo K di cui F è estensione, otteniamo un'estensione semplice $K(\theta)$ la quale è anche finita.

Teorema 1.53. *Sia F estensione di K e sia $\theta \in F$ elemento algebrico di grado n su K. Sia g il polinomio minimo di θ su K. Allora:*

(i) $K(\theta)$ è isomorfo a $K[x]/(g)$;

(ii) $[K(\theta) : K] = n$ e $\{1, \theta, \ldots, \theta^{n-1}\}$ è una base per $K(\theta)$ su K;

(iii) Ogni $\alpha \in K(\theta)$ è algebrico su K e il suo grado su K divide n.

Definizione 1.54. Sia $f \in K[x]$ un polinomio e F estensione di K. Diciamo che f si *spezza* in F se può essere scritto nella forma

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$$

dove a è il coefficiente direttore di f e $n = \deg(f)$. Il più piccolo campo in cui f si spezza è detto *campo di spezzamento* di f. In particolare il campo di spezzamento di f è $K(\alpha_1, \ldots, \alpha_n)$.

Enunciamo (ma non dimostriamo) ora un importante risultato sui campi di spezzamento, il quale sarà molto utile nella classificazione dei campi finiti.

Teorema 1.55 (Esistenza e Unicità del campo di spezzamento)**.** *Sia K un campo e f un polinomio in $K[x]$. Allora esiste il campo di spezzamento di F e questo è unico a meno di isomorfismo.*

Capitolo 2

Campi Finiti

Questo secondo capitolo è dedicato ad alcuni risultati della Teoria dei Campi. Gli enunciati contenuti in questo capitolo saranno fondamentali per la dimostrazione dei teoremi che supportano gli algoritmi di fattorizzazione. Data l'importanza di questi risultati e la loro stretta correlazione con gli oggetti principali della dissertazione, la maggior parte degli enunciati sarà corredata da una dimostrazione. La prima sezione contiene dei risultati di completa classificazione dei campi finiti, la seconda si occuperà invece di alcune funzioni particolari definibili su questi ultimi. La terza sezione riveste un ruolo di rilievo in quanto fornisce gli strumenti necessari ad affrontare il terzo ed ultimo capitolo di questa tesi.

2.1 Classificazione dei Campi Finiti

Vediamo di seguito come i campi finiti siano completamente classificati secondo la loro cardinalità.

Lemma 2.1. *Sia F un campo finito, sia K un sottocampo di F con q elementi. Allora F ha esattamente q^m elementi, dove $m = [F : K]$.*

Dimostrazione. Sappiamo che F è uno spazio vettoriale $m-$dimensionale su K. Pertanto ogni $a \in F$ può essere scritto come $a = a_1e_1 + \ldots + a_me_m$ dove $\{e_1, \ldots, e_m\}$ è una base per F su K e $a_i \in K$. Poiché gli elementi di K sono esattamente q, quelli di F sono tutte e sole le combinazioni di q elementi su m posti, cioè q^m. □

Teorema 2.2. *Sia F un campo finito. Allora in F ha p^n elementi, dove il numero primo p è la caratteristica di F e n è il grado di estensione di F sul suo sottocampo primo.*

Dimostrazione. Per il Corollario 1.22 la caratteristica di F deve essere un certo numero primo p. Allora, per il Teorema 1.45, il sottocampo primo K di F deve essere isomorfo a $\mathbb{F}_p$. La tesi segue quindi dal Lemma 2.1. □

Lemma 2.3. *Sia F un campo finito con q elementi, allora per ogni $a \in F$ vale che $a^q = a$.*

Dimostrazione. Per $a = 0$ l'identità è banale. Poiché $K \setminus \{0\}$ è un gruppo ciclico rispetto alla moltiplicazione di ordine $q - 1$ si ha che $a^{q-1} = 1$. Essendo $a \neq 0$ otteniamo la tesi moltiplicando a destra e a sinistra per a. □

Lemma 2.4. *Sia F un campo finito con q elementi e K un suo sottocampo, allora il polinomio $x^q - x$ in $K[x]$ si fattorizza in $F[x]$ come*

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a)$$

e F è il campo di spezzamento di $x^q - x$ su K.

Dimostrazione. Sappiamo che il suddetto polinomio ha al più q radici su F, inoltre, per il Lemma 2.3, tutti gli $a \in F$ soddisfano la relazione $a^q = a$, cioè $a^q - a = 0$. Pertanto tutti gli elementi di F sono radici di $x^q - x$ e questo polinomio non si spezza in nessun campo più piccolo. □

Teorema 2.5 (Esistenza e Unicità di Campi Finiti)**.** *Per ogni primo p e ogni intero positivo n esiste un campo finito con p^n elementi. Inoltre, ogni campo finito con $q = p^n$ elementi è isomorfo al campo di spezzamento di $x^q - x$ su $\mathbb{F}_p$.*

Dimostrazione. (*Esistenza*) Sia $q = p^n$, $f(x) = x^q - x$ in $\mathbb{F}_p[x]$ e F il suo campo di spezzamento su $\mathbb{F}_p$. Poiché $f' = -1$, per il Teorema 1.41 non ha radici multiple, quindi $\mathbb{F}$ è un campo e ha esattamente q elementi. Per il Teorema 1.55 abbiamo allora l'esistenza. (*Unicità*) Sia F un campo finito di ordine $q = p^n$. Per il Teorema 2.2 F ha caratteristica p e quindi contiene il sottocampo $\mathbb{F}_p$. Per il Lemma 2.4 F è il campo di spezzamento di f su $\mathbb{F}_p$. Per il Teorema 1.55 abbiamo allora l'unicità.

□

Teorema 2.6 (Criterio per Sottocampi)**.** *Sia $\mathbb{F}_q$ un campo finito con $q = p^n$ elementi. Allora ogni sottocampo di $\mathbb{F}_q$ ha ordine p^m, dove m è un intero positivo che divide n. Viceversa se m divide n esiste esattamente un sottocampo di $\mathbb{F}_q$ con p^m elementi.*

Dimostrazione. Abbiamo già visto che se K è un sottocampo di $\mathbb{F}_{p^n}$ allora ha necessariamente p^m elementi. Per il Lemma 2.1 m è un divisore di n.
Viceversa, dato m intero positivo divisore di n, abbiamo che $f(x) = x^{p^m} - x$ divide $g(x) = x^{p^n} - x$, pertanto tutte le radici di f sono anche radici di g. Quindi il campo di spezzamento di g su $\mathbb{F}_p$ contiene il campo di spezzamento di f su $\mathbb{F}_p$. Per l'unicità del campo di spezzamento vista nel Teorema 1.55 il sottocampo fissato dalle radici di $f(x) = x^{p^m} - x$ su $\mathbb{F}_{p^n}$ è unico. □

Lemma 2.7. *Sia $f \in \mathbb{F}_q[x]$ un polinomio monico irriducibile su $\mathbb{F}_q$ di grado m. Allora f divide $x^{q^n} - x$ se e solo se m divide n.*

Dimostrazione. Supponiamo che f divida $x^{q^n} - x$. Sia α una radice di f nel campo di spezzamento di f su $\mathbb{F}_q$. Abbiamo allora che $\alpha^{q^n} = \alpha$, cioè $\alpha \in \mathbb{F}_{q^n}$. Segue quindi che $\mathbb{F}_q(\alpha)$ è un sottocampo di $\mathbb{F}_{q^n}$. Ma poiché $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, per il Teorema 1.51 abbiamo che m divide n.
Viceversa, se m divide n, per il Teorema 2.6 abbiamo che $\mathbb{F}_{q^m}$ è un sottocampo di $\mathbb{F}_{q^n}$. Se α è una radice di f sul suo campo di spezzamento rispetto a $\mathbb{F}_q$, quindi $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e di conseguenza $\mathbb{F}_q(\alpha) = F_{q^m}$. Pertanto $\alpha \in \mathbb{F}_{q^n}$ e $\alpha^{q^n} = \alpha$. Allora α è una radice di $x^{q^n} - x$ e la tesi segue dal Teorema 1.49 (ii). □

Teorema 2.8. *Per ogni campo finito $\mathbb{F}_q$ il gruppo moltiplicativo $\mathbb{F}_q^*$ degli elementi non nulli è ciclico.*

Definizione 2.9. Dato il campo finito $\mathbb{F}_q$, un generatore del gruppo moltiplicativo $\mathbb{F}_q^*$ è detto *elemento primitivo* di $\mathbb{F}_q$.

Teorema 2.10. *Sia $\mathbb{F}_q$ campo finito e $\mathbb{F}_r$ un'estensione finita di $\mathbb{F}_q$. Allora $\mathbb{F}_r$ è un'estensione algebrica di $\mathbb{F}_q$ e ogni elemento primitivo di $\mathbb{F}_r$ estende algebricamente $\mathbb{F}_q$ in $\mathbb{F}_r$.*

Dimostrazione. Sia ζ un elemento primitivo di $\mathbb{F}_r$. Ovviamente $\mathbb{F}_q(\zeta) \subseteq \mathbb{F}_r$, inoltre $\mathbb{F}_q(\zeta)$ contiene 0 e tutte le potenze di ζ, quindi $\mathbb{F}_q(\zeta) \supseteq \{0\} \cup \mathbb{F}_r^* = \mathbb{F}_r$. Allora $\mathbb{F}_q(\zeta) = \mathbb{F}_r$. □

Corollario 2.11. *Per ogni campo finito Fq e ogni intero positivo n esiste un polinomio irriducibile in $\mathbb{F}_q[x]$ di grado n.*

Dimostrazione. Sia $\mathbb{F}_{q^n}$ un'estensione semplice di $\mathbb{F}_q$ con $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. Preso ζ elemento primitivo in $\mathbb{F}_{q^n}$ abbiamo che il suo polinomio minimo in $\mathbb{F}_q[x]$ è di grado n ed è irriducibile per il Teorema 1.49(i) e per il Teorema 1.53(ii). □

2.2 Tracce su Campi Finiti

In questa sezione definiremo una mappa da F a K, dove $F = \mathbb{F}_{q^n}$ è un'estensione del campo finito $K = \mathbb{F}_q$. Questa mappa, chiamata *traccia*, si rivelerà essere K-lineare e ci tornerà utile nella dimostrazione del Teorema 3.7 nella sezione dedicata all'algoritmo di McEliece.
Per raggiungere questo scopo è utile considerare il campo F come spazio vettoriale $n-$dimensionale su K, dove $\{\alpha_1, \ldots, \alpha_n\}$ denota una base di F su K.

Definizione 2.12. Sia $\alpha \in F = \mathbb{F}_{q^n}$ e $K = \mathbb{F}_q$. Definiamo la *traccia* di α su K come segue:

$$\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{n-1}}$$

Inoltre se K è il sottocampo primo di F, allora $\mathrm{Tr}_{F/K}(\alpha)$ si dice *traccia assoluta* di α su K e si indica con $\mathrm{Tr}_F(\alpha)$.

In altre parole, la traccia di un elemento $\alpha \in F$ su K è la somma dei coniugati di α rispetto a K. La traccia assume quindi valori in K essendo invariante rispetto all'automorfismo di Frobenius.

Teorema 2.13. *Siano $F = \mathbb{F}_{q^n}$ e $K = \mathbb{F}_q$. Allora la funzione $\mathrm{Tr}_{F/K}$ soddisfa le seguenti proprietà:*

(i) $\mathrm{Tr}_{F/K}(\alpha + \beta) = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta)$ *per ogni* $\alpha, \beta \in F$;

(ii) $\mathrm{Tr}_{F/K}(c\alpha) = c\,\mathrm{Tr}_{F/K}(\alpha)$ *per ogni* $\alpha \in F$ *e per ogni* $c \in K$;

(iii) $\mathrm{Tr}_{F/K}$ *è una trasformazione lineare suriettiva da F in K, dove sia F che K sono visti come spazi vettoriali su K;*

(iv) $\mathrm{Tr}_{F/K}(c) = nc$ *per ogni* $c \in K$;

(v) $\mathrm{Tr}_{F/K}(\alpha^q) = \mathrm{Tr}_{F/K}(\alpha)$ *per ogni* $\alpha \in F$.

Dimostrazione. (i) Applicando il Teorema 1.23 otteniamo:

$$\begin{aligned}
\mathrm{Tr}_{F/K}(\alpha+\beta) &= \alpha + \beta + (\alpha+\beta)^q + \ldots + (\alpha+\beta)^{q^{n-1}} &= \\
&= \alpha + \beta + \alpha^q + \beta^q + \ldots + \alpha^{q^{n-1}} + \beta^{q^{n-1}} &= \\
&= \alpha + \alpha^q + \ldots + \alpha^{q^{n-1}} + \beta + \beta^q + \ldots + \beta^{q^{n-1}} &= \\
&= \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta).
\end{aligned}$$

(ii) Per il Lemma 2.3 per ogni $c \in K$ vale $c^{q^j} = c$ con $j \geq 0$, pertanto:

$$\begin{aligned}
\mathrm{Tr}_{F/K}(c\alpha) &= c\alpha + (c\alpha)^q + \ldots + (c\alpha)^{q^{n-1}} &= \\
&= c\alpha + c^q\alpha^q + \ldots + c^{q^{n-1}}\alpha^{q^{n-1}} &= \\
&= c\alpha + c\alpha^q + \ldots + c\alpha^{q^{n-1}} &= \\
&= c(\alpha + \alpha^q + \ldots + \alpha^{q^{n-1}}) &= \\
&= c\,\mathrm{Tr}_{F/K}(\alpha).
\end{aligned}$$

(iii) La linearità deriva dai punti (i) e (ii). Vogliamo mostrare ora che esiste un elemento di $\alpha \in F$ tale che $\mathrm{Tr}_{F/K}(\alpha) \neq 0$. Dire che $\mathrm{Tr}_{F/K}(\beta) = 0$ significa dire che β è una radice di $x + x^q + \ldots + x^{q^{n-1}}$ in $K[x]$ il cui grado è q^{n-1}, pertanto ha al più q^{n-1} radici distinte. Poiché F ha q^n elementi distinti possiamo concludere che esiste un $\alpha \in F$ tale che $\mathrm{Tr}_{F/K}(\alpha) \neq 0$.

(iv) Per il Lemma 2.3 per ogni $c \in K$ vale $c^{q^j} = c$ con $j \geq 0$, pertanto:

$$\mathrm{Tr}_{F/K}(c) = \sum_{j=0}^{n-1} c^{q^j} = \sum_{j=0}^{n-1} c = nc$$

(v) Sempre per il Lemma 2.3 abbiamo che $\alpha^{q^n} = \alpha$, pertanto abbiamo che:

$$\begin{aligned} \mathrm{Tr}_{F/K}(\alpha^q) &= \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{n-1}} + \alpha^{q^n} && = \\ &= \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{n-1}} + \alpha && = \\ &= \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{n-1}} && = \\ &= \mathrm{Tr}_{F/K}(\alpha). \end{aligned}$$

□

2.3 Polinomi su Campi Finiti

Questa sezione è dedicata ad alcuni risultati in merito ai polinomi a coefficienti su campi finiti. Poiché questi ultimi sono gli oggetti principali degli algoritmi del capitolo successivo verrà posta particolare attenzione sulle dimostrazioni. Puntualizzo inoltre che, sebbene esista una vasta teoria su questi oggetti, in questa dissertazione vengono evidenziate solamente le proprietà utili ai fini della stessa.

Teorema 2.14. *Dato $\mathbb{F}_q$ campo finito e $n \in \mathbb{N}$ si ha che il prodotto di tutti i polinomi monici e irriducibili in $\mathbb{F}_q$, il cui grado divide n, è uguale a $x^{q^n} - x$.*

Dimostrazione. Per il Lemma 2.7 i polinomi irriducibili che compaiono nella fattorizzazione di $g(x) = x^{q^n} - x$ sono esattamente tutti quelli il cui grado divide n. Inoltre, poiché $g'(x) = -1$, per il Teorema 1.41 $g(x)$ non ha radici multiple sul suo campo di spezzamento rispetto a $\mathbb{F}_q$, quindi ogni fattore compare una volta sola (altrimenti avremmo almeno una radice multipla nel campo di spezzamento di g). □

Corollario 2.15. *Dato $h(x)$ polinomio in $\mathbb{F}_q[x]$, si ha che*

$$h(x)^q - h(x) = \prod_{a \in \mathbb{F}_q} (h(x) - a)$$

Dimostrazione. La tesi segue dalla sostituzione di $y = h(x)$ nella tesi del Teorema precedente. Otteniamo infatti che

$$y^q - y = \prod_{a \in \mathbb{F}_q} (y - a) = \prod_{a \in \mathbb{F}_q} (h(x) - a) = h(x)^q - h(x)$$

□

Capitolo 3

Algoritmi di Fattorizzazione

In questo capitolo tratteremo l'argomento principale della dissertazione: gli algoritmi di fattorizzazione per i polinomi a coefficienti in campi finiti. Per quanto visto nei capitoli precedenti, ogni polinomio a coefficienti in un campo finito si può scrivere univocamente come prodotto di fattori irriducibili. Saper fornire questa scomposizione ha notevoli applicazioni nel campo della teoria dei codici e nello studio delle ricorrenze lineari su campi finiti; pertanto dagli anni sessanta del secolo scorso in poi si sono implementati (con l'ausilio dei calcolatori) diversi algoritmi atti a questo scopo.

Dal punto di vista teorico è possibile trovare un algoritmo per fattorizzare ogni polinomio di qualsiasi grado in un campo finito di qualsivoglia ordine che si concluda in un tempo finito: sono infatti finiti i polinomi di un dato grado n e lo sono pertanto gli irriducibili di grado minore o uguale a n. Di conseguenza è facile costruire un algoritmo che, dato in input un polinomio di grado n, lo fattorizzi dividendolo per tutti i possibili irriducibili di grado minore o uguale a n e trovando quindi la sua fattorizzazione canonica. Un tale algoritmo, tuttavia, risulterebbe inefficace (e molto lento) anche per campi finiti di piccolo ordine e per gradi bassi. Illustriamo in questo capitolo tre distinti algoritmi di fattorizzazione: i primi due si basano sul Teorema 3.1, il terzo si propone di trovare delle eventuali radici (e quindi, per il Teorema di Ruffini, una scomposizione parziale) di un polinomio senza dover "provare" tutti gli elementi del campo.

3.1 Algoritmo di Berlekamp

In questa sezione introduciamo l'algoritmo di Berlekamp, sviluppato da Elwyn R. Berlekamp nel 1967, insieme al Teorema di Fattorizzazione (Teorema 3.1) su cui l'algoritmo si basa.
Come già detto, ogni polinomio $f \in \mathbb{F}_q[x]$ (che supporremo, senza perdita di generalità, monico) ha una scomposizione canonica

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

dove $f_1 \dots f_k$ sono polinomi monici distinti in $\mathbb{F}_q[x]$ e $e_1 \dots e_k$ sono interi positivi e rappresentano le molteplicità con cui i fattori compaiono nella scomposizione. Sempre senza perdita di generalità possiamo supporre che f non abbia fattori ripetuti e che quindi gli e_i siano tutti uguali a 1: infatti, a questo scopo, basta calcolare il massimo comun divisore tra il polinomio e la sua derivata formale

$$d(x) = \mathrm{mcd}(f(x), f'(x)).$$

Se $d(x) = 1$ allora, per il Teorema 1.43, f non ha fattori ripetuti. Se invece $d(x) = f(x)$ allora $f'(x) = 0$ (poiché f non è il polinomio nullo). Pertanto $f(x) = g(x)^p$ (Teorema

1.42) dove p è la caratteristica di $\mathbb{F}_q$; se necessario, si applica il medesimo procedimento a g. Se infine $d(x) \neq 1$ e $d(x) \neq f(x)$ allora $d(x)$ è un fattore non banale di $f(x)$. Il problema si riconduce allora a fattorizzare $d(x)$ e $f(x)/d(x)$, dove quest'ultimo polinomio è privo di fattori ripetuti.
Iterando questo procedimento un numero sufficiente di volte ai $d(x)$ otteniamo un numero, certamente finito, di fattori non banali per f, tutti senza fattori ripetuti. Il problema è quindi facilmente riconducibile alla fattorizzazione di un polinomio i cui fattori sono tutti privi di molteplicità. Per affrontarlo con efficacia, il seguente teorema riveste un'importanza cardinale.

Teorema 3.1. *Sia $f \in \mathbb{F}_q[x]$ un polinomio monico e $h \in \mathbb{F}_q[x]$ monico tale che $h^q \equiv h \mod f$. Allora si ha che*

$$f(x) = \prod_{c \in \mathbb{F}_q} \mathrm{mcd}(f(x), h(x) - c). \tag{4.2}$$

Dimostrazione. Ciascun massimo comun divisore al secondo membro dell'equazione 4.2 divide $f(x)$. Poiché i polinomi $h(x) - c$ sono a due a due coprimi lo sono anche tutti i massimi comuni divisori con $f(x)$, pertanto il loro prodotto divide $f(x)$. Allo stesso tempo si ha che, per ipotesi, $f(x)$ divide

$$h(x)^q - h(x) = \prod_{c \in \mathbb{F}_q} (h(x) - c), \text{(Corollario 2.15)} \tag{4.3}$$

perciò f divide il secondo membro di 4.2. Poiché entrambi i polinomi coinvolti nell'equazione 4.2 sono monici e si dividono l'un l'altro, essi devono essere uguali. □

Osservazione 3.2. In generale, la relazione 4.2 non fornisce una fattorizzazione completa di f, infatti i fattori $\mathrm{mcd}(f, h(x) - c)$ potrebbero a loro volta essere fattorizzabili. Inoltre se $h(x) \equiv a \mod f$ per qualche $a \in \mathbb{F}_q$ allora applicando il Teorema 3.1 otteniamo una fattorizzazione banale per f. Osserviamo inoltre che vale il viceversa: se h conduce ad una fattorizzazione banale per f allora deve essere che tutti gli $\mathrm{mcd}(f(x), h(x) - c) = 1 \; \forall c \in \mathbb{F}_q$ e quindi $h \equiv a \mod f$

Definizione 3.3. Sia $g \in \mathbb{F}_q$ un polinomio monico che conduca ad una fattorizzazione non banale di f, allora g si dice polinomio *f-riduttore*. In particolare tutti i polinomi del tipo $h(x)^q \equiv h \mod f$ con $0 < \deg(h) < \deg(f)$ sono f-riduttori.

Per scomporre f in fattori irriducibili è di conseguenza necessario trovare dei polinomi f-riduttori, ed è a questo punto che introduciamo l'algoritmo di Berlekamp.
Se $f = f_1 \cdots f_k$ è il prodotto di polinomi monici e irriducibili su $\mathbb{F}_q$ (abbiamo già visto che questa ipotesi non toglie generalità al problema) allora, per ogni k-upla di elementi in $\mathbb{F}_q$ $c_1, \ldots, c_k$, il Teorema Cinese dei Resti (Teorema 1.10) ci garantisce l'esistenza e unicità della soluzione $h(x) \in \mathbb{F}_q[x]$ tale che $h(x) \equiv c_i \mod f_1(x)$ per $i = 1, \ldots, k$ e $\deg(h) < \deg(f)$. Allora il polinomio $h(x)$ soddisfa la condizione

$$h(x)^q \equiv c_i^q = c_i \equiv h(x) \mod f(x)$$

e pertanto

$$h(x)^q \equiv h(x) \mod f, \; con \; \deg(h) < \deg(f) \tag{4.4}$$

e quindi h è un polinomio f-riduttore. Inoltre abbiamo che, se h è soluzione di 4.4 allora ogni fattore irriducibile di f divide uno dei polinomi $h(x) - c$. Poiché tutte le soluzioni dipendono dalla scelta della k-upla $(c_1, \ldots, c_k)$ con $c \in \mathbb{F}_q$ ci sono esattamente q^k soluzioni dell'equazione 4.3.
Per trovare le soluzioni possiamo ridurre l'equazione 4.3 ad un sistema lineare, costruendo la matrice $n \times n$ $B = (b_{ij})$, $i, j = 0, \ldots, n-1$ attraverso il calcolo delle potenze x^{iq}

mod $f(x)$. In particolare sia

$$x^{iq} \equiv \sum_{j=0}^{n-1} b_{ij} x^j \mod f(x).$$

Allora abbiamo che $h(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ è soluzione di 4.3 se e solo se

$$(a_0, a_1, \ldots, a_{n-1})B = (a_0, a_1, \ldots, a_{n-1}) \tag{4.5}$$

Infatti 4.5 è equivalente a dire che

$$\begin{aligned} h(x) &= \sum_{j=0}^{n-1} a_j x^j \\ &= \sum_{j=0}^{n-1}\sum_{i=0}^{n-1} a_j b_{ij} x^j \\ &\equiv \sum_{j=0}^{n-1} a_j x^{iq} = h(x)^q \mod f(x). \end{aligned}$$

Il sistema si può anche riscrivere come

$$(a_0, a_1, \ldots, a_{n-1})(B - I) = (0, 0, \ldots, 0) \tag{4.6}$$

dove I è la matrice identica su $\mathbb{F}_q$. Cerchiamo quindi la dimensione del nucleo di $B - I$ (o, equivalentemente, la dimensione dell'autospazio relativo all'autovalore 1 di B) e una relativa base. Se $\dim(\ker(B)) = k$, allora il rango di B è $n - k$ e ci sono esattamente k fattori irriducibili non banali di f.
Osserviamo che $h_1(x) = 1$, corrispondente al vettore $(1, 0, \ldots, 0)$ è sempre soluzione del sistema 4.6. Inoltre esistono $h_2(x), \ldots, h_k(x)$ di grado minore o uguale a $n - 1$ tali che i vettori corrispondenti formino una base per il nucleo di $B - I$. Questi ultimi hanno grado positivo e sono polinomi f-riduttori.
In questo procedimento è fondamentale determinare il rango di B e quindi il numero di fattori da cercare: una volta fatto ciò, l'algoritmo esegue q massimi comuni divisori tra $f(x)$ e $h_2(x) - c$, ottenendo una fattorizzazione parziale per f. Nel caso in cui non vengano trovati tutti i k fattori non banali di f, si procede con h_3 e così via.

Osservazione 3.4. Osserviamo che il processo termina sempre con successo e fornisce la fattorizzazione completa del polinomio. Consideriamo infatti due fattori distinti di $f(x)$, ad esempio $f_1(x)$ e $f_2(x)$. Allora esistono degli elementi c_{i1} e c_{i2} in $\mathbb{F}_q$ tali che $h_i(x) \equiv c_{i1} \mod f_1(x)$ e $h_i(x) \equiv c_{i2} \mod f_2(x)$ per tutti gli $i = 1, \ldots, k$. Dire che il processo non fornisce tutti i fattori di f equivale a dire che è possibile avere $c_{i1} = c_{i2}$ per ogni $i = 1, \ldots, k$, ovvero che non esistono c_{ij} capaci di separare f_1 ed f_2. Ogni polinomio $h(x)$ soluzione di 4.4 è, tuttavia, una combinazione lineare (Per il teorema Cinese dei Resti) dei polinomi $h_1(x), \ldots, h_k(x)$; pertanto se fosse vero che $c_{i1} = c_{i2}$ per ogni $i = 1, \ldots, k$, avremmo che, per ogni $h(x)$ soluzione di 4.4, $h(x) \equiv c \mod f_1(x)$ e $h(x) \equiv c \mod f_2(x)$ per un $c \in \mathbb{F}_q$. Ma dalla costruzione delle soluzioni della 4.4 si ha l'esistenza di una soluzione $h(x) \equiv 0 \mod f_1(x)$ e $h(x) \equiv 1 \mod f_2(x)$, quindi esiste sempre un $j \in \{1, \ldots, k\}$ tale che $c_{j1} \neq c_{j2}$. Di conseguenza avremo che $h_j(x) - c_{j1}$ sarà divisibile per $f_1(x)$ ma non per $f_2(x)$. Questo mostra che ogni fattore deve essere separato da almeno uno degli $h_j(x)$, quindi l'algoritmo di Berlekamp è un procedimento deterministico.

Esempio 3.5. Usiamo l'algoritmo di Berlekamp per fattorizzare il polinomio

$$x^8 + x^6 + x^4 + x^3 + 1$$

su $\mathbb{F}_2$. Si verifica immediatamente che $\mathrm{mcd}(f(x), f'(x)) = 1$, cioè $f(x)$ non ha fattori ripetuti. Si procede quindi nel calcolare $x^{iq} \mod f(x)$ per $q = 2$ e $0 \leq i \leq 7$:

$$\begin{aligned}
x^0 &\equiv 1 && \mod f(x)\\
x^2 &\equiv x^2 && \mod f(x)\\
x^4 &\equiv x^4 && \mod f(x)\\
x^6 &\equiv x^6 && \mod f(x)\\
x^8 &\equiv 1 + x^3 + x^4 + x^6 && \mod f(x)\\
x^{10} &\equiv 1 + x^2 + x^3 + x^4 + x^5 + x^7 && \mod f(x)\\
x^{12} &\equiv x^2 + x^4 + x^5 + x^6 && \mod f(x)\\
x^{14} &\equiv 1 + x + x^3 + x^4 + x^5 && \mod f(x)
\end{aligned}$$

E con questi costruiamo la matrice B

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 0\\
1 & 0 & 1 & 1 & 1 & 1 & 0 & 0\\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 1\\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}$$

e la matrice $B - I$

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0\\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0\\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1\\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 1
\end{pmatrix}$$

La matrice $B-I$ ha rango 6, pertanto ci sono esattamente due fattori non banali di f. I vettori che generano il nucleo di B sono $(1,0,0,0,0,0,0,0)$ e $(0,1,1,0,0,1,1,1)$, associati ai polinomi $h_1(x) = 1$ e $h_2(x) = x + x^2 + x^5 + x^6 + x^7$. Poiché h_1 è la soluzione banale, calcoliamo $\mathrm{mcd}(f(x), h_2(x)) = x^6 + x^5 + x^4 + x + 1$ e $\mathrm{mcd}(f(x), h_2(x) + 1) = x^2 + x + 1$. Abbiamo quindi trovato la fattorizzazione completa:

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

3.2 Algoritmo di McEliece

In questa sezione tratteremo l'algoritmo di fattorizzazione sviluppato da Robert J. McEliece nel 1968. Esso si basa, come l'algoritmo di Berlekamp, sul Teorema 3.1 ma introduce un nuovo modo di cercare polinomi f-riduttori.
L'algoritmo mira infatti a costruire una famiglia di polinomi T_i, di cui almeno uno f-riduttore. Sia f, come sempre, un polinomio monico privo di fattori ripetuti tale che $f = f_1 \cdots f_k$ e sia $n_j = \deg(f_j)$ per $j \in \{1, \ldots, k\}$. Sia ora N il minimo intero tale che $x^{q^N} \equiv x \mod f(x)$, allora per il Teorema 2.14 $N = \mathrm{mcm}(n_1, \ldots, n_k)$; inoltre, essendo i polinomi f_i irriducibili su $\mathbb{F}_q$, N è il grado del campo di spezzamento di f rispetto a $\mathbb{F}_q$. Sia il polinomio $T(x) = x + x^q + x^{q^2} + \ldots + x^{q^{N-1}}$, definiamo allora $T_i(x) = T(x^i)$.

Lemma 3.6. *Dato T definito come prima, abbiamo che*

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

Dimostrazione.

$$\begin{aligned} T\left(\sum_{i=0}^{n-1} a_i x^i\right) &= \sum_{j=0}^{N-1} \left(\sum_{i=0}^{n-1} a_i x^i\right)^{q^j} = \\ &= \sum_{j=0}^{N-1}\sum_{i=0}^{n-1} (a_i x^i)^{q^j} = && \text{(poiché siamo in caratteristica } p) \\ &= \sum_{j=0}^{N-1}\sum_{i=0}^{n-1} a_i (x^i)^{q^j} = && \text{(poiché } a_i \in \mathbb{F}_q \text{ e l'ordine del campo è } q) \\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{N-1} a_i (x^i)^{q^j} = \sum_{i=0}^{n-1} a_i \sum_{j=0}^{N-1} (x^i)^{q^j} = \sum_{i=0}^{n-1} a_i T(x^i) && \text{(per definizione di } T) \end{aligned}$$

□

Enunciamo ora un risultato che garantisce, nel caso in cui f sia un polinomio riducibile su $\mathbb{F}_q$, di trovare dei polinomi f-riduttori tra i polinomi T_i.

Teorema 3.7. *Sia f un polinomio riducibile su $\mathbb{F}_q$, allora almeno uno dei polinomi T_i per $1 \leq i \leq n-1$ è f-riduttore.*

Dimostrazione. È immediato verificare che ogni T_i soddisfa $T_i^q \equiv T_i \mod f$. Supponiamo allora che tutti i T_i con $1 \leq i \leq n-1$ conducano ad una fattorizzazione banale di f attraverso (4.2). Esistono allora degli elementi $c_1 \dots c_{n-1}$ in $\mathbb{F}_q$ tali che $T_i(x) \equiv c_i \mod f(x)$ per ogni $1 \leq i \leq n-1$. Posto $c_0 = N$ visto come un elemento di $\mathbb{F}_q$, abbiamo che $T_i(x) \equiv c_i \mod f(x)$ per ogni $0 \leq i \leq n-1$. Sia ora

$$g(x) = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q[x]$$

di grado strettamente minore di n. Applicando T a g otteniamo, per il Lemma 3.6, che

$$T(g(x)) = T\left(\sum_{i=0}^{n-1} a_i x^i\right) = \sum_{i=0}^{n-1} a_i T(x^i) \equiv \sum_{i=0}^{n-1} a_i c_i \mod f(x).$$

Poniamo

$$c(g) = \sum_{i=0}^{n-1} a_i c_i \in \mathbb{F}_q,$$

pertanto abbiamo che

$$T(g(x)) \equiv c(g) \mod f_j(x) \text{ per } 1 \leq j \leq k. \tag{4.7}$$

Poiché $N = \mathrm{mcm}(n_1, \dots, n_k)$ almeno uno degli N/n_j non è divisibile per $p = \mathrm{char}(\mathbb{F}_q)$. Supponiamo, a meno di riordinare i fattori, che sia N/n_1. Sia θ_1 una radice di f_1 sul campo di spezzamento di f_1 su $\mathbb{F}_q$. Sia $\mathbb{F}_1$ il suddetto campo di spezzamento. Per il Teorema 2.13(iii) esiste un polinomio $g_1 \in \mathbb{F}_q[x]$ tale che

$$\mathrm{Tr}_{F_1/\mathbb{F}_q}(g_1(\theta_1)) = 1. \tag{4.8}$$

Poiché assumiamo che $k \geq 2$ (altrimenti il polinomio sarebbe irriducibile) possiamo applicare il Teorema Cinese dei Resti per ottenere un polinomio g tale che

$$g \equiv g_1 \mod f_1, g \equiv 0 \mod f_2. \tag{4.9}$$

Allora si ha che anche g soddisfa per 4.8 e 4.9

$$\mathrm{Tr}_{F_1/\mathbb{F}_q}(g(\theta_1)) = 1,$$

infine dai Teoremi 2.13(iii) e 2.13(iv) deduciamo che

$$\mathrm{Tr}_{F_1/\mathbb{F}_q}(g(\theta_1)) = N/n_1.$$

Per la definizione di traccia ed elemento θ_1 segue che

$$T(g(x)) \equiv N/n_1 \mod f_1(x).$$

Tuttavia la seconda congruenza in 4.9 porta a dire che

$$T(g(x)) \equiv 0 \mod f_2(x).$$

Ma poiché $N/n_1 \neq 0$ in $\mathbb{F}_q$ abbiamo una contraddizione alla 4.7. L'assurdo nasce quindi supponendo che nessun T_i sia f-riduttore, allora almeno uno dei T_i è f-riduttore. □

Osserviamo che anche l'algoritmo di McEliece è un algoritmo deterministico: la costruzione esplicita dei T_i porta ad avere almeno una fattorizzazione non banale, pertanto l'algoritmo termina (eventualmente applicandolo ai polinomi trovati) in un numero finito di passi.

Esempio 3.8. Cerchiamo la fattorizzazione canonica su $\mathbb{F}_2$ del polinomio

$$x^7 + x^5 + x^4 + x + 1.$$

Si verifica che $\mathrm{mcd}(f(x), f'(x)) = 1$, pertanto $f(x)$ non ha fattori ripetuti. Cerchiamo ora N tale che $x^{2^N} \equiv x \mod f(x)$.

$$\begin{aligned}
x &\equiv x && \mod f(x)\\
x^2 &\equiv x^2 && \mod f(x)\\
x^4 &\equiv x^4 && \mod f(x)\\
x^8 &\equiv x^6 + x^5 + x^2 + x && \mod f(x)\\
x^{16} &\equiv x^3 + x + 1 && \mod f(x)\\
x^{32} &\equiv x^6 + x^2 + 1 && \mod f(x)\\
x^{64} &\equiv x^6 + x + 1 && \mod f(x)\\
x^{128} &\equiv x^6 + x^4 + x^2 + x + 1 && \mod f(x)\\
x^{256} &\equiv x^5 + 1 && \mod f(x)\\
x^{512} &\equiv x^6 + x^3 + x^2 && \mod f(x)\\
x^{1024} &\equiv x && \mod f(x)
\end{aligned}$$

Allora $N = 10$ ed è dato il polinomio

$$T_1(x) = \sum_{j=0}^{9} x^{2^j} \equiv x^6 + x^2 + x + 1 \mod f(x).$$

Poiché T_1 non è una costante modulo $f(x)$ esso è un polinomio f-riduttore. Calcoliamo quindi

$$\begin{aligned}\mathrm{mcd}(f(x), T_1(x)) &= \mathrm{mcd}(x^7 + x^5 + x^4 + x + 1, x^6 + x^2 + x + 1) = \\ &= x^5 + x^4 + x^3 + x^2 + 1\end{aligned}$$

$$\begin{aligned}\mathrm{mcd}(f(x), T_1(x) - 1) &= \mathrm{mcd}(x^7 + x^5 + x^4 + x + 1, x^6 + x^2 + x) = \\ &= x^2 + x + 1\end{aligned}$$

Allora abbiamo che

$$f(x) = (x^5 + x^4 + x^3 + x^2 + 1)(x^2 + x + 1).$$

Osserviamo che il secondo fattore non ha radici in $\mathbb{F}_2$ e quindi è irriducibile. Inoltre, poiché $N = 10$ è il minimo comune multiplo dei gradi dei fattori irriducibili di $f(x)$, una qualsiasi fattorizzazione non banale del primo fattore porterebbe ad un diverso valore di N; quindi anche il primo fattore è irriducibile su $\mathbb{F}_2$. Quella trovata è pertanto la fattorizzazione canonica di f.

3.3 Algoritmo di Ricerca delle Radici

In questa sezione analizziamo un ultimo algoritmo: ci poniamo ora il problema di trovare le radici di un polinomio sul campo finito $\mathbb{F}_p$ nel caso in cui p è un numero primo dispari. Naturalmente se p è piccolo è sufficiente sostituire dentro il polinomio tutti gli elementi di $\mathbb{F}_p$. Il problema è concreto invece se il campo finito ha tanti elementi da rendere computazionalmente difficile applicare questo approccio di forza bruta. Cerchiamo allora un algoritmo che fornisca le radici (o, equivalentemente, i suoi fattori lineari) senza dover sostituire tutti gli elementi di $\mathbb{F}_p$ nel polinomio. In seguito vedremo un semplice algoritmo che lavora in campi finiti primi, tralasciando algoritmi molto più complessi adatti a campi finiti non primi.
In primo luogo osserviamo che è sufficiente trovare le radici di polinomi monici della forma

$$f(x) = \prod_{i=1}^{n}(x - c_i)$$

dove n è il grado del polinomio, gli $(x - c_i)$ sono tutti fattori lineari e $c_i \in \mathbb{F}_p$ le radici di f. Infatti in un campo finito di ordine p sappiamo, per il Teorema 2.14, che

$$\prod_{a \in \mathbb{F}_p}(x - a) = x^p - x.$$

Cercare le radici di $f(x)$ equivale a cercarle nel polinomio $g(x) = \mathrm{mcd}(f(x), x^p - x)$, dove quest'ultimo è chiaramente della forma richiesta. Osserviamo inoltre che se $g(x) = \mathrm{mcd}(f(x), x^p - x)$, $\deg(f) = n$ e $\deg(g) = k$ con $k \leq n$, allora f ha esattamente k radici distinte su $\mathbb{F}_p$.
Sia quindi $f(x)$ polinomio della forma richiesta con $\deg(f) = k$, $b \in \mathbb{F}_p$, consideriamo il polinomio

$$f(x - b) = \prod_{i=1}^{k}(x - b - c_i) = \prod_{i=1}^{k}(x - (b + c_i))$$

dove i c_i sono le radici di f. Sappiamo che $f(x - b)$ divide $x^p - x = x(x^{p-1} - 1) = x(x^{\frac{p-1}{2}} + 1)(x^{\frac{p-1}{2}} - 1)$. Si osservi che $-b$ è una radice di f se e solo se x è un fattore di $f(x - b)$. Infatti x è un fattore di $f(x - b)$ se e solo se 0 è una radice di $f(x - b)$; allora si ha che $f(-b) = 0$ e quindi $-b$ è una radice. Supponiamo che x non sia un fattore di

$f(x-b)$, allora abbiamo che

$$f(x-b) = \mathrm{mcd}(f(x-b), x^{\frac{p-1}{2}} + 1)\,\mathrm{mcd}(f(x-b), x^{\frac{p-1}{2}} - 1) \tag{4.10}$$

L'algoritmo procede quindi come segue. Dato un polinomio $g(x)$ di cui vogliamo trovare le radici, calcoliamo $f(x) = \mathrm{mcd}(g(x), x^p - x)$. Scegliamo un $b \in \mathbb{F}_p$ e calcoliamo $f(-b)$. Se $f(-b) = 0$ allora abbiamo trovato una radice e una fattorizzazione parziale di $f(x) = (x-b)q(x)$. Se $f(-b) \neq 0$ calcoliamo il resto di $x^{\frac{p-1}{2}}$ modulo $f(x-b)$. Nel caso improbabile che $x^{\frac{p-1}{2}} \equiv \pm 1 \mod f(x-b)$ scegliamo un altro b. Altrimenti abbiamo che l'identità 4.10 conduce ad una fattorizzazione non banale di $f(x-b)$. Sostituendo $x+b$ a x otteniamo una fattorizzazione di f. A questo punto possiamo iterare il processo fino a trovare tutte le k radici di g, dove $k = \deg(f)$.

Osservazione 3.9. Questo è di fatto un algoritmo probabilistico. Se dovessimo provare tutti i valori di $b \in \mathbb{F}_p$ allora avremmo semplicemente sostituito nel polinomio tutti gli elementi di $\mathbb{F}_p$. Esiste inoltre una versione più complessa dell'algoritmo riguardante la ricerca di radici di polinomi su un campo generico $\mathbb{F}_q$; la discussione di quest'ultimo non è tuttavia oggetto della dissertazione.

Esempio 3.10. Cerchiamo, ad esempio, le radici su $\mathbb{F}_{17}$ del polinomio

$$f(x) = x^6 - 7x^5 + 3x^4 - 7x^3 + 4x^2 - x - 2$$

Cercare le radici di $f(x)$ equivale a trovarle nel polinomio $g(x) = \mathrm{mcd}(f(x), x^{17} - x)$. Applicando l'algoritmo di Euclide otteniamo $g(x) = x^4+6x^3-5x^2+7x-2$. Per utilizzare l'algoritmo sopra descritto scegliamo $b = 0$. Osserviamo tuttavia che $x^{\frac{p-1}{2}} = x^8 \equiv 1 \mod (g(x))$, pertanto la prima scelta di b conduce ad una fattorizzazione banale di g. Passiamo dunque a $b = 1$: $g(x-1) = x^4 + 2x^3 - 3x - 2$ e $x^8 \equiv -4x^3 - 7x^2 + 8x - 5 \mod (g(x-1))$. Allora $b = 1$ porta ad una fattorizzazione non banale di g. Procedendo con l'algoritmo abbiamo che:

$$\begin{aligned}\mathrm{mcd}(g(x-1), x^8 + 1) &= \mathrm{mcd}(x^4 + 2x^3 - 3x - 2, -4x^3 - 7x^2 + 8x - 4)\\ &= x^2 - 7x + 4,\end{aligned}$$

$$\begin{aligned}\mathrm{mcd}(g(x-1), x^8 - 1) &= \mathrm{mcd}(x^4 + 2x^3 - 3x - 2, -4x^3 - 7x^2 + 8x - 6)\\ &= x^2 - 8x + 8.\end{aligned}$$

Per quanto detto sopra abbiamo trovato una fattorizzazione del polinomio

$$g(x-1) = (x^2 - 7x + 4)(x^2 - 8x + 8),$$

e quindi, calcolando $g((x-1)+1)$, anche del polinomio

$$g(x) = (x^2 - 5x - 2)(x^2 - 6x + 1) = g_1(x)g_2(x).$$

Per fattorizzare $g_1(x)$ e $g_2(x)$ ripetiamo il procedimento a questi ultimi utilizzando $b = 2$. Abbiamo che $g_1(x-2) = x^2 + 8x - 5$ e $x^8 \equiv -8x + 2 \mod (g_1(x-2))$. Inoltre

$$\mathrm{mcd}(g_1(x-2), x^8 + 1) = \mathrm{mcd}(x^2 + 8x - 5, -8x + 3) = x + 6;$$

dividendo $g_1(x-2)$ per $(x+6)$ otteniamo

$$g_1(x-2) = (x+6)(x+2)$$

e quindi la fattorizzazione

$$g_1(x) = (x+8)(x+4)$$

Passando a g_2 osserviamo che $g_2(x-2) = x^2 + 7x = x(x+7)$. Ciò implica che 0 è una radice di $g_2(x-2)$ e quindi -2 è una radice di $g_2(x)$. Abbiamo allora che

$$g_2(x) = (x+2)(x-8).$$

Combinando le precedenti fattorizzazioni concludiamo che

$$g(x) = (x+8)(x+4)(x+2)(x-8),$$

pertanto le radici di $f(x)$ su $\mathbb{F}_{17}$ sono -8 ,-4 ,-2, 8.

3.4 Breve confronto tra gli Algoritmi

In quest'ultima sezione analizziamo gli algoritmi da un punto di vista computazionale, cioè quante operazioni servono per portare a termine l'algoritmo. Tutti i risultati forniti in questa sezione non saranno corredati di dimostrazione e verranno enunciati come appendice degli algoritmi esposti nelle sezioni precedenti.

In primo luogo mettiamo a confronto l'algoritmo di Berlekamp e l'algoritmo di McEliece. Entrambi si basano sul Teorema 3.1 ma prendono strade diverse nella ricerca dei polinomi f-riduttori; il primo sfrutta l'algebra lineare e il metodo di riduzione Gaussiano, il secondo invece sfrutta la traccia sul campo di spezzamento del polinomio f. Detto n il grado del polinomio da fattorizzare e q l'ordine del campo finito, si dimostra che il primo necessita di n^3 operazioni in coordinate (ricordiamo che un polinomio di grado n si può rappresentare come un vettore di $n+1$ componenti) per la riduzione della matrice e qn^2 operazioni per eseguire i mcd. Il secondo, invece, necessita di N potenze q-esime successive che richiedono n^2N operazioni, oltre alle qn^2 per la fattorizzazione. Si dimostra che N (il minimo comune multiplo dei gradi dei fattori di f) cresce, in media, linearmente con n anche se il valore massimo cresce più velocemente di e^{n^α} con $\alpha < \frac{1}{2}$. Inoltre è spesso necessario computare diversi $T_i(x)$ prima di trovarne uno f-riduttore, quindi i due algoritmi hanno la stessa velocità di calcolo. Quello proposto da McEliece, tuttavia, è più semplice da programmare: è infatti più immediato computare le q-esime potenze successive che non la riduzione di una matrice $n \times n$.

Osserviamo infine come l'algoritmo per la ricerca delle radici utilizzi, invece di polinomi riduttori, delle costanti di riduzione le quali si cercano in maniera casuale all'interno del campo finito. Il principio di fattorizzazione in fattori lineari è infatti molto simile, anche se privo della ricerca di polinomi di riduzione particolari. L'algoritmo diventa quindi probabilistico nel senso di trovare, tra gli elementi scelti casualmente all'interno del campo finito, delle costanti di riduzione. In questa dissertazione non si è indagato sulla probabilità che, dato $f(x)$ polinomio da fattorizzare e $b \in \mathbb{F}_p$, $x^{\frac{p-1}{2}} \equiv \pm 1 \mod f(x-b)$.

Bibliografia

Lidl, R., Niederreiter, H. (1997). Finite Fields, volume 20 of Encyclopedia of Mathematics and its Applications. Cambridge, U.K., Cambridge University Press, 2nd edn.

McEliece, R. J. (1969). Factorization of polynomials over finite fields. Math. Comput., 23, (861,867).

Von Zur Gathen, J., Panario, D. (2001) Factoring Polynomials Over Finite Fields: A Survey.