Elementi di crittografia, 1^o modulo

Alessandra Cherubini*

* Dipartimento di Matematica
Politecnico di Milano
email: aleche@mate.polimi.it

1 Introduzione

La matematica che sta alla base della crittografia è la matematica combinatoria ed in particolare la teoria dei gruppi e dei campi finiti. In queste note vengono presentati alcuni elementi di tali teorie con particolare attenzione agli aspetti che trovano applicazioni in crittografia. Le note sono ad uso interno del corso e per una trattazione più sistematica e completa il lettore interessato può consultare [1]

2 Elementi di teoria dei gruppi

Una struttura algebrica (interna) è una coppia $< S, \Omega >$, dove S è un insieme, detto sostegno della struttura, Ω è un insieme finito di operazioni interne su S, assiomi (caratteristici delle varie strutture) specificano le proprietà di cui le operazioni devono godere.
Se il sostegno S della struttura è finito, si dice che la struttura è finita e il numero degli elementi di S viene indicato con $|S|$ e chiamato ordine della struttura.
Due tipi di strutture sono particolarmente importanti in crittografia: i gruppi ed i campi.

Def 2.1 (Gruppo). *Si dice* gruppo *una coppia $< G, * >$, dove G è un insieme (sostegno del gruppo), $*$ è un'operazione interna binaria su G, cioè una legge che ad ogni coppia (a, b) di elementi di G associa uno ed un solo elemento $c \in G$ (denotato $a * b$), per la quale valgono i seguenti assiomi:*

- *proprietà associativa:* $\forall a, b, c \in G \ (a * b) * c = a * (b * c)$,
- *esistenza dell'elemento neutro:* $\exists e \in G : \forall a \in G \ a * e = e * a = a$
- *esistenza dell'inverso:* $\forall a \in G \ \exists \overline{a} \in G : a * \overline{a} = \overline{a} * a = e$

Un gruppo per cui vale anche il seguente assioma

- *proprietà commutativa:* $\forall a, b \in G \ a * b = b * a$

si dice gruppo abeliano

(Vedere eventualmente le dispense del corso di Algebra e logica per le prime proprietà dei gruppi [2]).
È stato utilizzato il simbolo $*$ per indicare l'operazione binaria sul gruppo per sottolineare il fatto che l'operazione può essere qualunque, ma nel seguito useremo, se non diversamente specificato, la notazione moltiplicativa, per cui l'operazione $*$ sarà chiamata prodotto e denotata con $\cdot$ (o con il concatenamento dei due operandi), l'elemento neutro sarà chiamato unità del gruppo e a volte

denotato con 1 e l'inverso di a sarà indicato con a^{-1}.
Per i gruppi commutativi useremo invece quasi sempre la notazione additiva per cui l'operazione sarà denotata con $+$, l'elemento neutro sarà chiamato zero ed indicato con 0 e l'inverso di a sarà indicato con $-a$ e chiamato opposto di a.
Osserviamo che, grazie alla proprietà associativa, può essere definito senza problemi di parentetizzazione il prodotto di più di due elementi di G, e quindi possono essere definite le potenze ad esponente intero di un elemento $a \in G$ ponendo:

- $a^n = a \cdot a \cdot ... \cdot a$
  n volte, se $n > 0$
- $a^n = e$, se $n = 0$
- $a^n = a^{-1} \cdot a^{-1} \cdot ... \cdot a^{-1}$
  $-n$ volte, se $n < 0$

la proprietà associativa e le proprietà definitrici degli elementi neutro ed inverso garantiscono la validità delle usuali proprietà delle potenze:

- $a^n \cdot a^m = a^{n+m}$
- $(a^n)^m = a^{nm}$.

Osservate che, se si usa la notazione additiva, la potenza n-esima di un elemento a sarà indicata con na; le proprietà delle potenze si scrivono allora : $(na) + (ma) = (n + m)a$ (notate che NON è la proprietà distributiva) e $m(na) = (mn)a$ (notate che NON è la proprietà associativa, anche se ne è una immediata conseguenza).

Es 2.2 .
1. $< Z, + >$ è un gruppo commutativo.
2. L'insieme $\{A \in M_n(R) \mid det\ A \neq 0\}$ delle matrici quadrate non singolari di ordine n a coefficienti reali è un gruppo non abeliano rispetto all'usuale prodotto di matrici.
3. $< \{1, -1, i, -i\}, \cdot >$ è un gruppo abeliano finito.
4. L'insieme delle applicazioni biunivoche di un insieme X in se stesso è un gruppo non abeliano rispetto alla solita composizione di applicazioni. Se l'insieme X è finito di cardinalità n, tale gruppo è finito di ordine $n!$ e viene chiamato *gruppo simmetrico su* X ed indicato con S_n. Il gruppo simmetrico su 3 elementi è il gruppo non commutativo di ordine minimo. Siano e l'applicazione identica su un insieme di cardinalità 3, a l'applicazione che scambia i primi due elementi e lascia fermo il terzo, b l'applicazione che scambia il primo e il terzo elemento fra loro e lascia fermo il secondo, c l'applicazione che scambia gli ultimi due elementi e tiene fermo il primo, g l'applicazione che porta il primo elemento nel secondo, il secondo nel terzo ed il terzo nel primo, infine h l'applicazione che porta il primo elemento nel terzo, il secondo nel primo ed il terzo nel secondo, ovviamente e funziona da unità rispetto alla composizione di applicazioni e si ha inoltre:

	e	a	b	c	g	h
e	e	a	b	c	g	h
a	a	e	g	h	b	c
b	b	h	e	g	c	a
c	c	g	h	e	a	b
g	g	c	a	b	h	e
h	h	b	c	a	e	g

Def 2.3 (Sottogruppo). *Un sottoinsieme H di un gruppo $< G, \cdot >$ si dice* sottogruppo *di G se è a sua volta gruppo rispetto alla stessa operazione $\cdot$ definita su G.*

Osservate che per verificare se un sottoinsieme H del sostegno G di un gruppo $< G, \cdot >$ è un sottogruppo di $< G, \cdot >$ basta usare uno dei seguenti criteri

- *H è un sottogruppo di $< G, \cdot >$ sse $\forall h, k \in H$ si ha $h \cdot k \in H$ e $h^{-1} \in H$.*
  La parte "solo se" è ovvia. Dimostriamo la parte "se". L'operazione $\cdot$, essendo associativa in G, è associativa in $H(\subseteq G)$, inoltre scelto comunque $h \in H$, h^{-1} appartiene ad H per ipotesi e quindi anche $h \cdot h^{-1} = e$ appartiene ad H per ipotesi.

- *H è un sottogruppo di $< G, \cdot >$ sse $\forall h, k \in H$ si ha $h \cdot k^{-1} \in H$.*
  La parte "solo se" è ovvia. Dimostriamo la parte "se". L'operazione $\cdot$ è ovviamente associativa in H; inoltre, scelto comunque $h \in H$, $h \cdot h^{-1} = e$ appartiene ad H per ipotesi e quindi anche $e \cdot h^{-1} = h^{-1}$ appartiene ad H per ipotesi.

- *Sia H un sottoinsieme finito di G, H è un sottogruppo di $< G, \cdot >$ sse $\forall h, k \in H$ si ha $h \cdot k \in H$.*
  La parte "solo se" è ovvia. Dimostriamo la parte "se". L'operazione $\cdot$ ovviamente associativa in H, inoltre scelto comunque $h \in H$, $h^n \in H$ per tutti gli interi positivi n. Essendo H finito, le potenze positive di h non possono essere tutte distinte e dunque devono esistere due interi positivi n, m con $n \neq m$ tali che $h^n = h^m$. Supponiamo $m > n$, e sia $m = n + r$ allora $h^{n+r} = h^n \cdot h^r = h^n = h^n \cdot e$ da cui moltiplicando a sinistra per l'inverso di h^n (che nel gruppo $< G, \cdot >$ esiste) si ottiene $h^r = e$ e dunque $e \in H$ e $h^{-1} = h^{r-1} \in H$.

Es 2.4 .
1. I sottoinsiemi $\{e\}$ e G sono sottogruppi di ogni gruppo $< G, \cdot >$, detti *sottogruppi banali.*
2. L'insieme P di tutti i numeri pari è un sottogruppo del gruppo $< Z, + >$.
3. L'insieme $\{A \in M_n(R) \mid det\ A = \pm 1\}$ è un sottogruppo del gruppo $< \{A \in M_n(R) \mid det\ A \neq 0\}, \cdot >$
4. L'insieme $\{1, -1\}$ è un sottogruppo del gruppo $< \{1, -1, i, -i\}, \cdot >$.
5. I sottoinsiemi $\{e, a\}$, $\{e, b\}$, $\{e, c\}$, $\{e, g, h\}$ sono tutti i sottogruppi non banali di S_3.
6. È noto che una applicazione biunivoca su un insieme finito si può scrivere come prodotto di scambi (applicazioni che scambiano due elementi e tengono fermi gli altri). La decomposizione non è unica, ma la partità del numero di scambi di ogni fattorizzazione è funzione solo dell'applicazione data. Una permutazione si dice pari (dispari) se si decompone in un numero pari (dispari) di scambi. Sia X un insieme di cardinalità n. L'insieme delle permutazioni pari su X è un sottogruppo del gruppo simmetrico su X, che si chiama *gruppo alterno su X* (o su n elementi) e viene di solito indicato con A_n.

Def 2.5 (laterale). *Siano $< G, \cdot >$ un gruppo, H un suo sottogruppo, $g \in G$; il sottoinsieme $H \cdot g = \{h \cdot g \mid h \in H\}$ ($g \cdot H = \{g \cdot h \mid h \in H\}$) di G si chiama* laterale destro (sinistro) *di*

H in G avente come rappresentante g. Ovviamente se G fosse scritto in notazione additiva il laterale sinistro di H in G avente come rappresentante g sarebbe denotato da $H + g$ e formato dagli elementi $\{h + g \mid h \in H\}$.

Si verifica facilmente che se $H \cdot g_1 \cap H \cdot g_2 \neq \emptyset$ allora $H \cdot g_1 = H \cdot g_2$ ed inoltre se H è finito si ha $|H| = |H \cdot g|$.
(Dal corso di Algebra e logica dovreste ricordare che la relazione binaria su G, $\sim_H$, definita ponendo $g \sim_H k$ sse $g \cdot k^{-1} \in H$ è una relazione di equivalenza e che la $\sim_H$-classe di $g \in G$ è il laterale $H \cdot g$.)
Si ha dunque

Teor 2.6 (teorema di Lagrange). *Sia $< G, \cdot >$ un gruppo finito di ordine n. Un sottogruppo H di G ha ordine che divide n.*

Dim. G è unione disgiunta di un numero finito di laterali di H in G e questi laterali hanno tutti cardinalità uguale all'ordine di H, dunque si ha $|G| = r|H|$ dove r indica il numero di laterali distinti di H in G.

In generale non vale l'inverso del teorema di Lagrange (ad esempio A_4 che ha ordine 12 non ha sottogruppi di ordine 6), tuttavia sussiste il seguente:

Teor 2.7 *Sia $< G, \cdot >$ un gruppo abeliano finito di ordine n. Per ogni divisore m di n esiste almeno un sottogruppo di G di ordine m.*

2.1 Gruppi ciclici

Def 2.8 (gruppo ciclico). *Sia $< G, \cdot >$ un gruppo e $g \in G$ un qualsiasi elemento di G. L'insieme di tutte le potenze di g è un sottogruppo di G detto* sottogruppo ciclico generato da g *ed indicato in seguito con $< g >$.*
Un gruppo $< G, \cdot >$ si dice ciclico *se esiste un $g \in G$ tale che $G =< g >$. L'elemento g si chiama* generatore *di G*

Ovviamente ogni gruppo ciclico è abeliano (segue immediatamente dalle proprietà delle potenze)

Es 2.9 .
1. $< Z, + >$ è un gruppo ciclico ed un suo generatore è 1. Infatti ogni intero positivo n è 1+1+...+1 (n volte) cioè la potenza ad esponente n di 1, 0 è la potenza ad esponente 0 di 1 e ogni intero negativo $-n$ è $-1 + (-1) + ... + (-1)$ (-(-n)=n volte), cioè è la potenza di esponente $-n$ di 1. Notate che anche -1 genera $< Z, + >$
2. $< \{1, -1, i, -i\}, \cdot >$ è un gruppo ciclico generato da i, infatti $i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$ (o da $-i$).

Teor 2.10 *Ogni sottogruppo di un gruppo ciclico è ciclico.*

Dim. Sia $G =< g >$ un gruppo ciclico e sia H un sottogruppo di G. Se $H = \{e\}$ si ha ovviamente $H =< e >$. Supponiamo allora che esista in H un elemento $h \neq e$. Essendo G ciclico, esiste un intero t tale che $h = g^t$, inoltre essendo H un sottogruppo anche $h^{-1} = g^{-t}$ appartiene ad H e dunque esiste in H una potenza positiva di g. Sia allora m il minimo intero positivo tale che

$g^m \in H$ e sia g^n un generico elemento di H. Dividendo n per m si ha $n = qm+r$, dove $0 \leq r < m$, quindi $g^r = g^n \cdot (g^m)^{-q} \in H$ da cui, per come è stato definito m, segue $r = 0$ e quindi $g^n = (g^m)^q$, dunque $H =< g^m >$.

Def 2.11 (periodo di un elemento). *Considerati un gruppo $< G, \cdot >$ ed un suo elemento g si dice* periodo (o ordine) *di g, e si indica con $|g|$, il minimo intero positivo m, se esiste, tale che $g^m = e$; in tal caso si dice che l'elemento g è periodico o che ha periodo finito.*
Se tale m non esiste, cioè se non esiste alcun intero (positivo) n tale che $g^n = e$, si dice che g ha periodo 0 *(o infinito)*

Sia $< G, \cdot >$ un gruppo e sia g un suo generico elemento:

- Se $\exists t > 0 : g^t = e$, $|g|$ divide t.
  Infatti g ha ordine finito e posto $m = |g|$ si ha (dividendo t per m) $t = qm+r$, dove $0 \leq r < m$; allora $g^r = g^{t-qm} = g^t \cdot (g^m)^{-q} = e$, da cui $r = 0$.
- Se $|g| = m$, $< g >= \{g,\ g^2, ...,\ g^{m-1},\ g^m = e\}$
  Infatti se $g^r = g^s$ si ha $g^{r-s} = e$ e dunque m divide $r - s$ per cui tutte le potenze g^i con $0 < i \leq m$ sono distinte . Inoltre per ogni intero j detti rispettivamente q ed r il quoziente ed il resto della divisione di j per m si ha $g^j = g^{qm}g^r = g^r$ dove $0 \leq j < m$ ma $g^0 = g^m$ e quindi ogni potenza di g coincide con un elemento dell'insieme $\{g,\ g^2, ...,\ g^{m-1},\ g^m = e\}$.
- Sia $|G| = n$. G è ciclico sse esiste $g \in G$ tale che $|g| = n$.
- Se $|G| = n$, $\forall g \in G$ $|g|$ divide n.
  Infatti $|g| = | < g > |$ e per il Teorema di Lagrange $| < g > |$ divide $|G|$.
- Se $|G| = p$ con p primo, allora G è ciclico.
- Se $|g| = m$, $|g^h| = m/M.C.D(m, h)$.
  Infatti $(g^h)^{m/M.C.D(h,m)} = g^{mh/M.C.D(h,m)} = (g^m)^d = e$ dove $d = h/M.C.D(h, m)$. Dunque $|g^h| = r$ divide $m/M.C.D(h, m)$ ma allora $g^{rh} = e$ dunque m divide rh, assurdo.
- Se $G =< g >$ e $|G| = n$, tutti gli elementi g^h con h primo con n generano G. Quindi il numero dei possibili generatori distinti di G è $\phi(n)$.
  Infatti $|g| = n$ e $|g^h| = n/M.C.D(h, n) = n$.

Prop 2.12 *Un gruppo ciclico G di ordine n ha uno ed un solo sottogruppo di ordine m per ogni divisore m di n*

Dim. Sia $G =< g >$, posto $d = n/m$, $|g^d| = m$ e dunque $< g^d >$ è un sottogruppo di G di ordine m. Sia K un altro sottogruppo di G di ordine m, per il teorema 2.10 $K =< g^r >$ ed essendo $|K| = m$, $M.C.D(r, n) = n/m = d$, quindi $r = ld$ per qualche intero l e dunque $g^r = (g^d)^l$ da cui $K \subseteq < g^d >$, ma $|K| = | < g^d > |$, quindi $K =< g^d >$.

3 Elementi di teoria degli anelli e dei campi

Def 3.1 (anello). *Si dice* anello *una struttura algebrica $< A, +, \cdot >$ (con due operazioni binarie), tale che:*

- $< A, + >$ *è un gruppo abeliano detto* gruppo additivo dell'anello,
- $\cdot$ *è una legge di composizione interna su* A *associativa, quindi* $< A, \cdot >$ *è un semigruppo detto* semigruppo moltiplicativo dell'anello,
- *valgono le proprietà distributive di* $\cdot$ *rispetto a* $+$ *, cioè* $\forall a, b, c \in A$ *si ha* $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$.

Se esiste un elemento neutro rispetto all'operazione $\cdot$*, l'anello si chiama* anello con unità.
Se $\cdot$ *gode della proprietà commutativa, l'anello si dice* anello commutativo.

Es 3.2 .
1. L'insieme delle matrici quadrate di ordine n ad elementi reali è un anello con unità rispetto agli usuali somma e prodotto di matrici.
2. L'insieme degli interi relativi rispetto agli usuali somma e prodotto è un anello commutativo con unità.
3. I polinomi a coefficienti reali nell'indeterminata x, rispetto alle usuali operazioni di somma e prodotto di polinomi costituiscono un anello commutativo con unità.

Le seguenti proprietà sono di immedita verifica.
Dato un anello $< A, +, \cdot >$ e detti 0 e $-a$ rispettivamente l'elemento neutro e l'inverso rispetto alla somma di a si ha:

- $\forall a \in A$, $a \cdot 0 = 0 \cdot a = 0$
- $\forall a, b \in A$, $a \cdot (-b) = (-a) \cdot b = -(ab)$

Def 3.3 (divisori dello 0). *Siano* $< A, +, \cdot >$ *un anello e* $a, b \in A$. *Se* $a \neq 0$ *e* $b \neq 0$ *ma* $a \cdot b = 0$ *gli elementi* a, b *si dicono* divisori dello 0 *in* A.

Prop 3.4 *Un anello* $< A, +, \cdot >$ *è privo di divisori dello zero se e solo se in esso valgono le leggi di cancellazione, cioè se ognuna delle relazioni* $a \cdot b = a \cdot c$, $b \cdot a = c \cdot a$ *con* $a, b, c \in A$ *ed* $a \neq 0$ *implica* $b = c$.

Dim. Sia $< A, +, \cdot >$ privo di divisori dello zero e sia $a \cdot b = a \cdot c$ con $a, b \in A$ ed $a \neq 0$, allora si ha $a \cdot b + (-a \cdot c) = 0$ cioè $a \cdot (b + (-c)) = 0$, pertanto $b + (-c) = 0$ (altrimenti a e $b + (-c)$ sarebbero divisori dello zero). Analogamente si prova che $b \cdot a = c \cdot a$ con $a \neq 0$ implica $b = c$. Viceversa, sia $< A, +, \cdot >$ un anello in cui valgono le leggi di cancellazione e supponiamo $a \cdot b = 0$ con $a \neq 0$, allora, essendo $a \cdot b = a \cdot 0$, per cancellazione si ottiene $b = 0$, per cui a, b non sono divisori dello zero.

Def 3.5 (corpo, campo). *Si dice* corpo *un anello in cui gli elementi diversi dallo* 0 *formano gruppo rispetto a* $\cdot$.
Un corpo in cui $\cdot$ *gode della proprietà commutativa si dice* campo.

Es 3.6 I numeri razionali, reali e complessi rispetto alle usuali operazioni di somma e prodotto sono campi.

I corpi sono privi di divisori dello 0, ma ci sono anelli privi di divisori dello 0 che non sono corpi, come ad esempio $< Z, +, \cdot >$. Tuttavia si ha

Prop 3.7 *Ogni anello finito $< A, +, \cdot >$ privo di divisori dello zero è un corpo.*

Dim. Sia $< A, +, \cdot >$ un anello finito privo di divisori dello 0. Sia $a \in A$, $a \neq 0$ consideriamo $\{a^n \mid n > 0\}$. Ovviamente per ogni $n > 0$ si ha $a^n \neq 0$ altrimenti A avrebbe divisori dello zero. Essendo A finito, esistono $n, m > 0$ tali che $a^{n+m} = a^n$ da cui $a^n \cdot a^m = a^n \cdot e$ e per le leggi di cancellazione $a^m = e$ da cui $a^{-1} = a^{m-1}$, quindi ogni elemento di A diverso dallo zero ha inverso in A e dunque A è un campo.

Si potrebbe dimostrare che *non esistono corpi finiti che non siano campi (teorema di Wedderburn).*
Un esempio di corpo che non sia campo è il seguente: si consideri come sostegno del corpo l'insieme K di tutti gli elementi della forma $ai + bj + ck + d$ con $a, b, c, d \in R$, si definiscano la somma di due elementi di questo tipo come la somma di polinomi nelle variabili i, j, k , ed il prodotto di due elementi di questo tipo come il prodotto di polinomi, in cui si tiene conto delle relazioni $i^2 = j^2 = k^2 = -1, i \cdot j = k, j \cdot k = i, k \cdot i = j, j \cdot i = -k, k \cdot j = -i, i \cdot k = -j$. Rispetto alla somma e al prodotto così definiti K è un corpo, detto *corpo dei quaternioni* , ma non un campo.

Def 3.8 (Sottoanello, ideale). *Un sottoinsieme H di un anello $< A, +, \cdot >$ si dice* sottoanello *di A se è a sua volta anello rispetto alle stesse operazioni $+, \cdot$ definite su A.*
Un sottoanello I di un anello $< A, +, \cdot >$ si dice ideale *di A se presi comunque $a \in A$ e $i \in I$ si ha $a \cdot i, i \cdot a \in I$.*

Si hanno i seguenti criteri

- *H è un sottoanello di $< A, +, \cdot >$ sse $\forall h, k \in H$ si ha $h - k \in H$ e $h \cdot k \in H$.*
  La parte "solo se" è ovvia. Per la parte "se", la prima condizione garantisce che H è un sottogruppo rispetto alla somma, la seconda che l'operazione $\cdot$ è una legge di composizione interna per H.
- *I è un ideale di $< A, +, \cdot >$ sse $\forall h, k \in I$ e $\forall a \in A$ si ha $h - k \in I$, $a \cdot i \in I$, $i \cdot a \in I$.*

Es 3.9 .
1. I sottoinsiemi $\{0\}$ e A sono ideali dell'anello $< A, +, \cdot >$, detti *ideali impropri o banali.*
2. L'insieme P di tutti i numeri pari è un ideale dell'anello $< Z, +, \cdot >$.
3. Sia $a \in R$, l'insieme $\{f(x) \in R[x] \mid f(a) = 0\}$ è un ideale di $< R[x], +, \cdot >$.
4. Siano $< A, +, \cdot >$ un anello commutativo, $a \in A$, l'insieme $\{x \cdot a + na \mid x \in A, n \in Z\}$ è un ideale di $< A, +, \cdot >$, detto *ideale principale generato da a.*

Osserviamo inoltre che:
se A è un anello con unità, l'unico ideale di A che contiene l'unità è l'ideale improprio A.
Infatti se I è un ideale di A e l'unità e di A appartiene ad I, $\forall a \in A$ si ha $a \cdot e = a \in I$.
Quindi *un corpo K non contiene ideali propri.*
Sia infatti I un ideale di K non ridotto al solo 0 e sia $i \in I$, $i \neq 0$, allora esiste $i^{-1} \in K$ e $i^{-1} \cdot i = e \in I$, da cui $I = K$.

Def 3.10 (Caratteristica). *Siano* $< A, +, \cdot >$ *un anello,* $a \in A$. *Si dice* caratteristica di a *il periodo di* a *nel gruppo additivo* $< A, + >$ *(notate che nel caso in cui il periodo di* a *non sia finito si dice che* a *ha caratteristica* 0*). Se in* $< A, +, \cdot >$ *tutti gli elementi hanno caratteristica finita (cioè diversa da* 0*) ed esiste un massimo* r *delle caratteristiche degli elementi di* A*, si dice che* A *ha caratteristica* r *altrimenti si dice che* A *ha caratteristica* 0.

È facile osservare che

- *Un anello finito* $< A, +, \cdot >$ *ha caratteristica diversa da* 0.
  Infatti tutti i suoi elementi hanno caratteristica che divide l'ordine di A (per il teorema di Lagrange), quindi l'insieme delle caratteristiche degli elementi di A ammette un massimo, che è la caratteristica di A.
- *Se* $< A, +, \cdot >$ *è un anello finito privo di divisori dello* 0*, tutti i suoi elementi diversi da* 0 *hanno la stessa caratteristica e questa è un numero primo* p.
  Ogni elemento di $A - \{0\}$ ha caratteristica diversa da 0, sia allora $s \neq 0$ la caratteristica di $a \in A - \{0\}$. Sia $b \in A - \{0\}$, da $0 = sa$ si deduce $0 = 0 \cdot b = (sa)b = a(sb)$ da cui, essendo A privo di divisori dello 0, si ottiene $sb = 0$, quindi b ha caratteristica finita $r \leq s$, ora da $rb = 0$ si ottiene $0 = 0 \cdot a = (rb)a = b(ra)$ quindi $r = s$. Sia ora $r = nm$ con m, n interi positivi minori di r, da $0 = ra = nma = n(ma)$ essendo $ma \in A$ si deduce o che $ma = 0$ il che è assurdo perché a avrebbe caratteristica minore di r o che $ma \in A - \{0\}$ ha caratteristica minore di r, il che è ancora assurdo.

Ricordiamo brevemente le nozioni di anello quoziente ed omomorfismo fra anelli

Def 3.11 (laterale di un ideale). *Siano* $< A, +, \cdot >$ *un anello,* I *un suo ideale,* $a \in A$*; il sottoinsieme* $I + a = \{i + a \mid i \in I\}$ *di* A *si chiama* laterale *di* I *in* A *avente come rappresentante* a*. Ovviamente tale laterale coincide col laterale del sottogruppo additivo* I *nel gruppo additivo dell'anello* $< A, + >$.

Prop 3.12 *Siano* $< A, +, \cdot >$ *un anello ed* I *un suo ideale, allora* $< A/I, +, \cdot >$ *dove* $A/I = \{I + a \mid a \in A\}$, $(I + a_1) + (I + a_2) = I + (a_1 + a_2)$ *e* $(I + a_1) \cdot (I + a_2) = I + (a_1 \cdot a_2)$*, è un anello, detto anello quoziente di* A *rispetto ad* I.

Def 3.13 (omomorfismo). *Siano* $< A, +, \cdot >$ *e* $< R, \oplus, * >$ *due anelli, una applicazione* $f : A \longrightarrow R$ *tale che* $\forall a, b \in A$ *si abbia* $f(a + b) = f(a) \oplus f(b)$ *e* $f(a \cdot b) = f(a) * f(b)$ *si dice* omomorfismo *di* $< A, +, \cdot >$ *in* $< R, \oplus, * >$*. Un omomorfismo in cui* f *è una corrispondenza biunivoca si dice* isomorfismo *di* $< A, +, \cdot >$ *su* $< R, \oplus, * >$.

Osserviamo che, dati un anello $< A, +, \cdot >$ ed un suo ideale I, la proiezione canonica p di A su A/I risulta un omomorfismo fra anelli.

Def 3.14 (nucleo di un omomorfismo di anelli). *Siano* $< A, +, \cdot >$ *e* $< R, \oplus, * >$ *due anelli, ed* $f : A \longrightarrow R$ *un omomorfismo di* $< A, +, \cdot >$ *in* $< R, \oplus, * >$*. Detto* z *lo zero di* $< R, \oplus, * >$ *cioè l'elemento neutro del gruppo additivo* $< R, \oplus >$ *, l'ideale* $f^{-1}(z)$ *si chiama* nucleo di f.

Sussiste il seguente

Teor 3.15 (I teorema di isomorfismo per gli anelli). *Siano* $< A, +, \cdot >$ *e* $< R, \oplus, * >$ *due anelli, ed* $f : A \longrightarrow R$ *un omomorfismo di* $< A, +, \cdot >$ *in* $< R, \oplus, * >$*. Detto* I *il nucleo di* f*,* $f(A) = \{x \in R \mid \exists a \in A : \ x = f(a)\}$ *l'immagine di* A *in* R *(che è un sottoanello di* R*) e* p *la proiezione canonica di* $< A, +, \cdot >$ *su* $< A/I, +, \cdot >$ *, esiste un e un solo isomorfismo* h *di* $< A/I, +, \cdot >$ *su* $< f(A), \oplus, * >$ *tale che* $p \cdot h = f$*, definito ponendo* $h(I + a) = f(a)$ *per ogni* $a \in A$.

4 Cenni di aritmetica modulare

Abbiamo osservato che il gruppo $< Z, + >$ è ciclico, quindi per il teorema 2.10 ogni suo sottogruppo è ciclico. Quindi tutti e soli i sottogruppi propri di $< Z, + >$ sono del tipo $H_n = \{hn \mid h \in Z\}$ con $n > 1$. Consideriamo l'insieme dei laterali di H_n in $< Z, + >$, i laterali distinti di H_n in Z sono H_n, $H_n + 1$,...,$H_n + (n-1)$ e coincidono con le classi di equivalenza delle relazioni su Z così definite: $a \equiv b \ (mod\ n)$ sse esiste $h \in Z$ tale che $a - b = hn$.
Tale relazione è chiamata *relazione di congruenza modulo n*. Le classi di equivalenza rispetto a questa relazione sono chiamate *classi di resti modulo n* e denotate con $[0], [1], ..., [n-1]$. (Ricordate $[i] = H_n + i$). L'insieme delle classi di resti modulo n è di solito indicato con Z_n. Definiamo in Z_n una operazione di somma ponendo $[r] + [s] = [r + s]$.
Tale operazione è ben definita, infatti da $[r] = [t]$ e $[s] = [z]$ segue $r \equiv t,\ s \equiv z \ (mod\ n)$ cioè $r - t = hn,\ s - z = kn$ per opportuni $h, k \in Z$ da cui, sommando membro a membro, le due uguaglianza si ottiene $(r + s) - (t + z) = (h + k)n$ ovvero $[r + s] = [t + v]$.
La somma di classi di resti gode ovviamente delle proprietà associativa e commutativa.
La classe $[0]$ è l'elemento neutro rispetto alla somma ed ogni classe $[r]$ ammette come opposto (inverso rispetto alla somma) la classe $[-r]$.
Dunque $< Z_n, + >$ è un gruppo abeliano.

Es 4.1 *Supponiamo $n = 6$, le classi di resto modulo 6 sono $[0], [1], [2], [3], [4], [5]$ e la loro somma è data dalla seguente tavola*

	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Oltre l'operazione di somma, fra classi di resti modulo n può essere definito il seguente prodotto: $[r] \cdot [s] = [rs]$.
È facile osservare che il prodotto è ben posto, infatti $[r] = [t]$ e $[s] = [z]$ implicano $r - t = hn$ e $s - z = kn$ da cui moltiplicando ambo i membri della prima per s e della seconda per t e sommando membro a membro si ha $rs - tz = (hr + kt)n$ cioè $[rs] = [tz]$. Inoltre il prodotto gode delle proprietà associativa e commutativa e la classe$[1]$ è elemento neutro rispetto alla somma.
Infine valgono le proprietà distributive del prodotto rispetto alla somma.
Dunque $< Z, +, \cdot >$ è un anello commutativo con unità.

Es 4.2 *Di seguito presentiamo la tavola moltiplicativa di Z_6*

	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Prop 4.3 *Se $n = p$ con p numero primo, l'anello $< Z_p, +, \cdot >$ è un campo.*

Questo si può dimostrare tenendo conto della proposizione 3.7, visto che $< Z_p, +, \cdot >$ non ha divisori dello 0. Oppure si può fare una verifica diretta, provando che ogni $[r] \neq [0]$ ammette inverso in $Z_p^= Z_p - \{0\}*$. Essendo $M.C.D\{r,p\} = 1$, esistono infatti due interi λ e μ tali che $1 = r\lambda + p\mu$ da cui $1 \equiv r\lambda(mod\ p)$ cioè $[1] = [r][\lambda]$.

Da questo segue il seguente teorema

Teor 4.4 (Piccolo teorema di Fermat). *Siano p un numero primo ed a un qualsiasi numero intero non divisibile per p. Allora p divide $a^{(p-1)} - 1$.*

Dim. La classe di resti $[a]$ appartiene al gruppo $< Z_p^*, \cdot >$ e quindi ha periodo r che divide l'ordine $p-1$ del gruppo. Dunque $p - 1 = qr$ e quindi $[a]^{p-1} = [a]^{qr} = ([a]^q)^r = [1]$ da cui $[a]^{p-1} - [1] = [a^{p-1} - 1] = [0]$ e quindi $a^{p-1} - 1$ un multiplo di p.

È immediato osservare che se n non è un numero primo, l'insieme $Z_n^* = Z_n - \{[0]\}$ non risulta gruppo rispetto al prodotto di classi di resti. Infatti se $n = hk$ con h, k interi positivi minori di n, si ha $[h][k] = [0]$. Tuttavia si verifica facilmente che
l'insieme $\Phi_n = \{[h] \in Z_n^* \mid M.C.D.(h,n) = 1\}$ forma un gruppo rispetto al prodotto di classi di resti.
Infatti se h, k sono primi con n, hk è primo con n e chiamato r il resto della divisione di hk per n, anche r è primo con n perché $hk = qn + r$, dunque il prodotto di due qualsiasi elementi di Φ_n sta in Φ_n. Inoltre $[1] \in \Phi_n$ e ogni $[h]$ con $M.C.D\{h,n\} = 1$ ha inverso in Φ_n, infatti esistono due interi λ e μ tali che $1 = h\lambda + n\mu$ da cui $1 \equiv h\lambda(mod\ n)$, inoltre λ è ovviamente primo con n, quindi $[\lambda]$ è l'inverso di $[h]$.
Il gruppo Φ_n ha ordine $\varphi(n)$, ove φ indica la *funzione di Eulero* che per ogni intero positivo n restituisce il numero di interi positivi minori di n primi con n. La funzione di Eulero ha alcune proprietà interessanti

- Per ogni numero primo p, $\varphi(p) = p - 1$
- Se $n = pq$ con p, q primi, $\varphi(n) = (p-1)(q-1)$
- In generale, se $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ è la decomposizione in fattori primi dell'intero n , $\varphi(n) = n(1 - \frac{1}{p_1})...(1 - \frac{1}{p_r})$

Teor 4.5 (teorema di Eulero). *Siano n un numero primo ed a un intero primo con n. Allora n divide tutti gli interi della forma $a^{\varphi(n)} - 1$.*

Dim. La dimostrazione è del tutto analoga a quella del piccolo teorema di Fermat, infatti se $M.C.D.(a,n) = 1$ la classe $[a]$ appartiene a Φ_n e quindi ha un periodo che divide l'ordine $\varphi(n)$ di Φ_n.

Ovviamente il piccolo teorema di Fermat è un immediato corollario del teorema di Eulero in quanto se n è primo $\Phi_n = Z_n^*$.

Questi teoremi (o meglio le loro dimostrazioni) offrono un metodo per calcolare l'inverso (se esiste) di una classe di resti modulo n.
Infatti per ogni $[a] \in \Phi_n$, da $[a]^{\varphi(n)} = [1]$ si ottiene $[a]^{-1} = a^{\varphi(n)-1}$.
Osservate che per calcolare l'inverso di una classe $[a] \in \Phi_n$ fino ad ora potevamo solo procedere ad una ricerca esaustiva dell'inverso fra tutti gli elementi di Φ_n e questo metodo nel caso pessimo

potrebbe richiedere di effettuare $\varphi(n)-2$ moltiplicazioni, il calcolo della potenza $(\varphi(n)-1)$-esima può essere fatto in modo più efficente facendo successive quadrature (e riduzioni modulo n) di a fino ad ottenere a^{2^i} con $i = \lfloor log_2 n \rfloor$ ed effettuando poi gli opportuni prodotti (e riduzioni modulo n) delle potenze di a così ottenute.

Es 4.6 Calcolare l'inverso di $[9]$ in Φ_{26}.
Poiché 26 è primo con 9, $[9]$ appartiene a Φ_{26}, $\varphi(26) = 12$ quindi $[9]^{-1} = [9]^{11}$, essendo $10 = 8+2+1$ abbiamo che $[9]^{11} = [9]^8[9]^2[9]$, ora $[9]^2 = [81] = [3]$, $[9]^4 = [3]^2 = [9]$, $[9]^8 = [9]^2 = [3]$, $[9]^{11} = [3][3][9]$ e quindi $[9]^{11} = [3]$.
Osservate che da $[9]^4 = [9]$ avremmo potuto dedurre (essendo in un gruppo) che $[9]^3 = [1]$ e quindi che $[9]^{-1} = [9]^2 = [3]$.
In questo caso avremmo chiaramente fatto meno calcoli con una ricerca esaustiva perché avremmo calcolato solo i due prodotti $[9][2]$ e $[9][3]$ e la seconda moltiplicazione avrebbe dato il risultato cercato, provate però a calcolare l'inverso di $[17]$.

Il calcolo della funzione di Eulero può comunque non essere semplice da calcolare per interi n grandi (richiede di conoscere i fattori primi di n), in tal caso il calcolo dell'inverso di un elemento di Φ_n può essere fatto tramite *l'algoritmo di Euclide delle divisioni successive.*

ALGORITMO DI EUCLIDE IN Z

Siano a, b due interi non entrambi nulli, ricordiamo che $d = M.C.D.(a,b)$ è un intero che divide a ed b e tale che ogni altro divisore comune di a ed b divide d.
Esiste sempre un M.C.D. di due interi non nulli, inotre se $d = M.C.D.(a,b)$ anche $-d = M.C.D.(a,b)$, per convenzione quindi si sceglie il valore positivo come M.C.D. di due interi non nulli.
L'algoritmo di Euclide fornisce $M.C.D.(a,b)$ e i due interi λ e μ tali che $M.C.D.(a,b) = \lambda a + \mu b$ e si basa sulle seguenti osservazioni di immediata verifica:

1. $a = M.C.D.(a,0)$,
2. se $b \neq 0$, $M.C.D.(a,b) = M.C.D.(b, a \ mod \ b)$, dove $a \ mod \ b$ indica il minimo intero non negativo congruo ad a modulo b.
3. $M.C.D.(a,b) = M.C.D.(b,a)$.
4. $M.C.D.(a,b) = M.C.D.(|a|,|b|)$.

Supponiamo ora (per le 1. e 4.) $0 < b < a$, sappiamo che in Z esistono (e sono unici) il quoziente q_0 ed il resto r_0 della divisione di a per b e che $0 \leq r_0 < b$. Ovviamente se $r_0 = 0$ si ha $b = M.C.D.(a,b)$.
Se $r_0 \neq 0$ siano q_1 ed r_1 il quoziente ed il resto della divisione di b per r_0 (ove $0 \leq r_1 < r_0$), se $r_1 = 0$ si ha $r_0 = M.C.D.(b,r_0) = M.C.D.(b,a) = M.C.D.(a,b)$ per le 2. e 3.
Se invece $r_1 \neq 0$, siano q_2 ed r_2 il quoziente ed il resto della divisione di r_0 per r_1 (ove $0 \leq r_2 < r_1$), se $r_2 = 0$ si ha $r_1 = M.C.D.(r_0,r_1) = M.C.D.(a,r_1) = M.C.D.(a,b)$ per la 2.
Se invece $r_2 \neq 0$, si divide r_1 per r_2 e si continua con questo procedimento di divisione fino a quando si trova un resto nullo e questo richiederà un numero finito di passi perché i resti sono una sequenza strettamente decrescente di interi non negativi.
Sia $r_{h+1} = 0$, l'ultimo resto non nullo r_h è il massimo comun divisore fra a e b, infatti per 2. $r_h = M.C.D.(r_{h-1},r_h) = M.C.D.(r_{h-2},r_h) = M.C.D.(r_{h-2},r_{h-1}) = ... = M.C.D.(a,b)$.
Nell'eseguire il procedimento abbiamo trovato la seguente catena di uguaglianze:
$a = q_0 b + r_0$,

$b = q_1 r_0 + r_1$,
$r_0 = q_2 r_1 + r_2$,
...
$r_{i-1} = q_{i+1} r_i + r_{i+1}$,
...
$r_{h-2} = q_h r_{h-1} + r_h$,
$r_{h-1} = q_{h+1} r_h$.
Dalla prima si ricava $r_0 = a - q_0 b$, che sostituita nella seconda dà $r_1 = -q_1 a + (1 + q_1 q_0)b$, di nuovo sostituendo nella terza si ottiene $r_2 = (1 + q_2 q_1)a - (q_0 + q_2 + q_2 q_1 q_0)b)$ e così continuando si trova r_h, cioè $M.C.D.(a, b)$, come combinazione lineare di a e b. Ovviamente questo permette di calcolare l'inverso di $[a] \in \Phi_n$, perché come abbiamo visto se $1 = \lambda a + \mu n$, $[a]^{-1} = [\lambda]$.

Es 4.7 Calcolare l'inverso di [9] in Φ_{26}, usando l'algoritmo di Euclide
Dividendo 26 per 9 si trova $26 = 2 \cdot 9 + 8$ e poi dividendo 9 per 8 si ha $9 = 8 \cdot 1 + 1$, dividendo 8 per 1 si avrebbe resto nullo, dunque 1 è, come sapevamo, il $M.C.D.(26, 9)$ inoltre da $9 = 8 \cdot 1 + 1$ ricaviamo $1 = 9 - 8 \cdot 1$ e da $26 = 2 \cdot 9 + 8$ otteniamo $8 = 26 - 2 \cdot 9$ che sostituita in $1 = 9 - 8 \cdot 1$ dà $1 = 9 \cdot 3 - 26$, da cui si ottiene $1 \equiv 9 \ mod \ 26$, dunque l'inverso di [9] in Φ_{26} è [3].

Osservate che nel calcolo del resto le divisioni possono essere evitate, effettuando invece sottrazioni successive.

Osservate inoltre che spesso si fa uso della notazione $m \ (mod \ n)$ per indicare che si considera il resto della divisione di m per n, ovvero un intero r con $0 \leq r \leq n - 1$ tale che le classi di resto modulo n di m ed r coincidano. Si dice che una espressione aritmetica il cui risultato è t, è calcolata modulo n se come suo risultato si prende $t \ (mod \ n)$. Dovrebbe a questo punto essere chiaro che per calcolare una espressione modulo n conviene ridurre modulo n i suoi risultati parziali, sfruttando le (a questo punto) ovvie identità:
$a+b \ (mod \ n) = (a \ (mod \ n))+(b \ (mod \ n)) \ (mod \ n)$, $ab \ (mod \ n) = (a \ (mod \ n))(b \ (mod \ n)) \ (mod \ n)$.

Ricordiamo inoltre il seguente teorema che sarà utile in seguito:

Teor 4.8 *Siano m_i, $1 \leq i \leq k$, interi positivi a due a due primi fra loro e siano c_i, $1 \leq i \leq k$, numeri interi relativi. Allora il sistema di congruenze:*
$x \equiv c_1 \ (mod \ m_1)$
$x \equiv c_2 \ (mod \ m_2)$
.....
$x \equiv c_k \ (mod \ m_k)$
ha una ed una sola soluzione $\overline{x}$ tale che $0 \leq \overline{x} \leq \prod_{1 \leq i \leq k} m_i$.

4.1 Anelli di polinomi

Consideriamo un campo K, l'insieme $K[x] = \{a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \mid a_i \in K, n \leq 0\}$ dei polinomi in x con coefficienti in K è un anello commutativo con unità privo di divisori dello $=$ rispetto alle solite operazioni di somma e prodotto di polinomi , ovvero se $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ e $g(x) = b_m x^m + b_{m-1} x^{n-1} + ... + b_1 x + b_0$ supposto $n \leq m$:

- $f(x) + g(x) = a_n x^n + ... + a_{m+1} x^{m+1} + (a_m + b_m) x^m + ... + (a_1 + b_1) x + (a_0 + b_0)$
- $f(x) \cdot g(x) = (a_n \cdot b_m) x^{n+m} + ... + (\sum_{h+k=i, \ h,k \geq 0} a_h \cdot b_k) x^i + ... + (a_0 \cdot b_0)$

L'anello così ottenuto si chiama *anello di polinomi nell'indeterminata x sul campo K*. Il coefficiente del termine di grado massimo di un polinomio $f(x)$ si chiama *coefficiente direttivo* del polinomio ed un polinomio con coefficiente direttivo uguale all'unità di K si chiama *polinomio monico*.

Prop 4.9 *Siano $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, $g(x) = b_m x^m + b_{m-1}x^{n-1} + ... + b_1 x + b_0$ due polinomi in $K[x]$ con $g(x) \neq 0$, allora esistono unici due polinomi $q(x)$ ed $r(x)$ tali che $f(x) = g(x)q(x) + r(x)$ e $gr(r(x)) < gr(g(x))$.*

Dim. Se $m > n$ allora $q(x) = 0$ e $r(x) = f(x)$ sono i polinomi cercati. Supponiamo $m \leq n$, allora $q(x)$ deve avere grado $n - m$, sia $q(x) = q_{n-m}x^m + q_{n-m-1}x^{n-m-1} + ... + q_1 x + q_0$, $r(x) = r_{m-1}x^{m-1} + r_{m-2}x^{m-2} + ... + r_1 x + r_0$. Se vogliamo che sia $f(x) = g(x)q(x) + r(x)$ i coefficienti di $q(x)$ e $r(x)$ devono soddisfare le sequenti equazioni in K:
$b_m \cdot q_{n-m} = a_n$
$b_m \cdot q_{n-m-1} + b_{m-1} \cdot q_{n-m} = a_{n-1}$
....
$b_{m-1} \cdot q_0 + b_{m-2} \cdot q_1 + ... + b_0 \cdot q_{m-1} + r_{m-1} = a_{m-1}$
....
$b_0 \cdot q_0 + r_0 = a_0$
La prima ammette l'unica soluzione $q_{n-m} = b_m^{-1}a_n$, che sostituita nella seconda permette di ricavare in modo univoco $q_{n-m-1} = b_m^{-1}(a_{n-1} - b_{m-1} \cdot b_m^{-1}a_n)$, continuando così dalle prime $n-m$ equazioni si trovano i coefficienti di $q(x)$ e dalle restanti m i coefficienti di $r(x)$.

Ovviamente l'algoritmo che si usa per calcolare quoziente e resto della divisione di $a(x)$ per $b(x)$ entrambi appartenenti a $K[x]$ non è quello descritto nella precedente dinostrazione, ma quello che siamo abituati ad usare nell'effettuare la divisione fra polinomi a coefficienti reali, l'unica cosa da tenere in considerazione è che qundo si devono fare le divisioni fra i coefficienti, tali divisioni devono essere eseguite in K (ovvero se $a, b \in K$ e $b \neq 0$, il risultato della definizione di a per b è $a \cdot b^{-1}$).
Nel seguito useremo la scrittura $a(x)$ $(mod\ b(x))$ per indicare il resto della divisione di $a(x)$ per $b(x)$, e come nel caso degli interi diremo che una espressione polinomiale il cui risultato $f(x)$ è calcolata modulo $b(x)$ se come risultato dell'espressione si prende $f(x)$ $(mod\ b(x))$.

Def 4.10 (Radice di un polinomio). *Sia $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in K[x]$. L'elemento $\alpha \in K$ si dice* radice *di $f(x)$ se $a_n \cdot \alpha^n + a_{n-1} \cdot \alpha^{n-1} + ... + a_1 \cdot \alpha + a_0 = 0$, dove ovviamente le operazioni $+, \cdot$ sono ora fatte in K.*

Prop 4.11 (Teorema di Ruffini). *Il polinomio $f(x) \in K[x]$ ha radice α se e solo se $x - \alpha$ divide $f(x)$.*

Dim. La parte "se" è ovvia. Viceversa supponiamo che $f(x)$ abbia radice α. Per la Prop 4.9 $f(x) = (x - \alpha)q(x) + r$ (con $r \in K$), da cui $f(\alpha) = (\alpha - \alpha)q(\alpha) + r$, quindi $r = 0$.

Def 4.12 (Molteplicità di una radice). *Sia $\alpha \in K$ una radice di $f(x) \in K[x]$. Si dice che α ha* molteplicità *k se $(x - \alpha)^k$ divide $f(x)$ ma $(x - \alpha)^{k+1}$ non divide $f(x)$.*

Si può provare che $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ ha la radice α con molteplicità maggiore o uguale a 2 se $x - \alpha$ divide anche la derivata $f'(x)$ di $f(x)$ definita al solito come $na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + ... + a_1$.

Def 4.13 (Polinomio irriducibile) *Un polinomio $f(x) \in K[x]$ di grado n si dice* riducibile in K *se esistono due polinomi $g(x), h(x) \in K[x]$ entrambi di grado inferiore ad n tali che $f(x) = g(x)h(x)$; altrimenti $f(x)$ si dice* irriducibile *in K.*

Ovviamente un polinomio di $K[x]$ di grado minore od eguale a 3 è riducibile in K sse ammette almeno una radice in K, invece un polinomio di grado maggiore o uguale a 4 può essere riducibile in K e non ammettere radici in K.

Es 4.14 *Il polinomio $f(x) = [1]x^4+[2]x^3+[2]x+[2] \in Z_3[x]$ non ha radici in Z_3, infatti $f([0]) = [2]$, $f([1]) = [1]$, $f([2]) = [2]$, tuttavia $f(x)$ è riducibile in Z_3 in quanto si spezza nel prodotto dei due polinomi $[1]x^2 + [1]$ e $[1]x^2 + [2]x + [2]$ entrambi irriducibili di grado 2 in Z_3.*
Notate che nel seguito quando scriveremo polinomi in $Z_p[x]$ indicheremo gli elementi di Z_p semplicemente come interi e preciseremo in che campo andiamo a considerare i coefficienti del polinomio, indicando l'anello a cui il polinomio stesso appartiene. Ad esempio il precedente polinomio $f(x)$ sarà scritto come $x^4 - 2x^3 + 2x + 2 \in Z_3[x]$.

Sussiste inoltre la seguente

Prop 4.15 *Un polinomio $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in K[x]$ si scrive in uno ed un sol modo (a meno di riordino dei fattori) nella forma: $f(x) = a_n g_1(x)g_2(x)...g_r(x)$ dove $r \leq n$ e per ogni i con $1 \leq i \leq r$ il polinomio $g_i(x)$ è monico ed irriducibile in K.*

Dal teorema precedente e dal teorema di Ruffini segue facilmente che la somma delle molteplicità delle radici di un polinomio $f(x)$ è minore o uguale al grado di $f(x)$.

Def 4.16 *Siano $f(x), g(x) \in K[x]$ due polinomi non entrambi nulli. Un polinomio $d(x) \in K[x]$ che divide $f(x)$ e $g(x)$ e tale che ogni polinomio $h(x) \in K[x]$ che divida $f(x)$ e $g(x)$ divide $d(x)$, si dice* massimo comun divisore *di $f(x)$ e di $g(x)$ ($M.C.D.(f(x), g(x))$).*

Dati due polinomi $f(x), g(x) \in K[x]$ non entrambi nulli, se $d(x) = M.C.D.(f(x), g(x))$ per ogni $k \in K$, $k \neq 0$ anche $kd(x) = M.C.D.(f(x), g(x))$, si conviene quindi di prendere come $M.C.D.(f(x), g(x))$ il polinomio monico fra i massimi comuni divisori.
Ovviamente dalla Prop.4.15 segue che esiste sempre il $M.C.D(f(x), g(x))$ e che si può calcolare come prodotto dei fattori monici irriducibili comuni ad $f(x)$ e $g(x)$ presi col minimo esponente. Va tuttavia notato che fattorizzare un polinomio è in generale un procedimento costoso, quindi è opportuno riformulare anche per gli anelli di polinomi l'algoritmo di Euclide.

ALGORITMO DI EUCLIDE IN K[x]

Siano $f(x), g(x) \in K[x]$ due polinomi non entrambi nulli, l'algoritmo di Euclide fornisce $M.C.D.(f(x), g(x))$ e due polinomi $\lambda(x), \mu(x)$ tali che $M.C.D.(f(x), g(x)) = \lambda(x)f(x)+\mu(x)g(x)$ e si basa sulle seguenti osservazioni di immediata verifica:

1. $a^{-1}f(x) = M.C.D.(f(x), 0)$, dove a è il coefficiente direttivo di $f(x)$
2. se $g(x) \neq 0$, $M.C.D.(f(x), g(x)) = M.C.D.(g(x), f(x) \ mod \ g(x))$, dove $f(x) \ mod \ g(x)$ indica il resto delle divisione di $f(x)$ per $g(x)$.
3. $M.C.D.(f(x), g(x)) = M.C.D.(g(x), f(x))$.

4. $M.C.D.(f(x), g(x)) = M.C.D.(a^{-1}f(x), b^{-1}g(x))$, dove a, b sono i coefficienti direttivi rispettivamente di $f(x)$ e $g(x)$

Supponiamo sia $0 \neq g(x)$ e $gr(g(x)) \leq gr(f(x))$, sappiamo che in $K[x]$ esistono (e sono unici) il quoziente $q_0(x)$ ed il resto $r_0(0)$ della divisione di $f(x)$ per $g(x)$ e che $gr(r_0(x)) < gr(g(x))$. Ovviamente se $r_0(x)$ è il polinomio nullo si ha $b^{-1}g(x) = M.C.D.(f(x), g(x))$.
Se $r_0(0) \neq 0$ siano $q_1(x)$ ed $r_1(x)$ il quoziente ed il resto della divisione di $g(x)$ per $r_0(x)$ (ove $gr(r_1(x)) < gr(r_0(x))$); se $r_1(x)$ è il polinomio nullo si ha $r_0(x) = M.C.D.(g(x), r_0(x)) = M.C.D.(g(x), f(x)) = M.C.D.(f(x), g(x))$ per le 2. e 3.
Se invece $r_1(x)$ non è il polinomio nullo, siano $q_2(x)$ ed $r_2(x)$ il quoziente ed il resto della divisione di $r_0(x)$ per $r_1(x)$ (ove $gr(r_2(x)) < gr(r_1(x))$), se $r_2(x)$ è il polinomio nullo si ha $r_1(x) = M.C.D.(r_0(x), r_1(x)) = M.C.D.(g(x), r_1(x)) = M.C.D.(f(x), g(x))$ per la 2.
Altrimenti si divide $r_1(x)$ per $r_2(x)$ e si continua con questo procedimento di divisione fino a quando si trova un resto nullo e questo richiederà un numero finito di passi perché i gradi dei resti sono una sequenza strettamente decrescente di interi non negativi. Siano $r_{h+1} = 0$, ed $r_h(x)$ l'ultimo resto non nullo, allora $c^{-1}r_h(x)$, dove c è il coefficiente direttivo di $r_h(x)$ è il massimo comun divisore fra $f(x)$ e $g(x)$, infatti per 2. $c^{-1}r_h(x) = M.C.D.(r_{h-1}(x), r_h(x)) = M.C.D.(r_{h-2}(x), r_h(x)) = M.C.D.(r_{h-2}(x), r_{h-1}(x)) = ... = M.C.D.(f(x), g(x))$.
Nell'eseguire il procedimento abbiamo trovato la seguente catena di uguaglianze:
$f(x) = q_0(x)g(x) + r_0(x)$,
$b(x) = q_1(x)r_0(x) + r_1(x)$,
$r_0(x) = q_2(x)r_1(x) + r_2(x)$,
...
$r_{i-1}(x) = q_{i+1}(x)r_i(x) + r_{i+1}(x)$,
...
$r_{h-2}(x) = q_h(x)r_{h-1}(x) + r_h(x)$,
$r_{h-1}(x) = q_{h+1}(x)r_h(x)$.
Dalla prima si ricava $r_0(x) = f(x) - q_0(x)g(x)$, che sostituita nella seconda dà $r_1(x) = -q_1(x)f(x) + (e + q_1(x)q_0(x))g(x)$, di nuovo sostituendo nella terza si ottiene $r_2(x) = (e + q_2(x)q_1(x))f(x) - (q_0(x) + q_2(x) + q_2(x)q_1(x)q_0(x))g(x))$ dove e indica l'unità di K e così continuando si trova $r_h(x)$, e quindi $c^{-1}r_h(x)$, come combinazione lineare di $f(x)$ e $g(x)$.

4.2 Campi finiti

Vogliamo nel seguito descrivere la struttura dei campi finiti. A tal proposito elenchiamo dapprima alcune proprietà dei campi finiti

1. Ogni campo finito K ha caratteristica p con p numero primo

2. Se K è un campo finito di ordine q, per ogni $a \in K$ si ha $a^q = a$.
   Infatti il gruppo moltiplicativo di K, il cui insieme sostegno è $K - \{0\}$ ha ordine $q - 1$ e dunque il periodo di a divide $q - 1$ da cui $a^{q-1} = e$ dove e indica l'unità di K.

3. Se la caratteristica di K è p, si ha $(a \pm b)^{p^m} = a^{p^m} \pm b^{p^m}$ per ogni $a, b \in K$ e per ogni m intero non negativo.
   Infatti i coefficienti binomiali dei termini misti che si ottengono sviluppando la potenza $(a \pm b)^{p^m}$ sono tutti multipli di p.

4. Se la caratteristica di K è p, detta e l'unità di K, l'insieme $\{ne \mid 0 \leq n \leq p - 1\}$ è un sottocampo K_e di K, detto *sottocampo minimo o primo di K* (infatti ogni altro sottocampo

di K deve contenere e e quindi i suoi multipli).
Inoltre la corrispondenza $f : Z_p \to K_e$ definita ponendo $f([r]) = re$ per ogni r con $0 \leq r \leq p-1$ è una corrispondenza biunivoca fra Z_p e K_e che conserva le operazioni, per cui possiamo dire che ogni campo K di caratteristica p contiene come sottocampo, a meno di isomorfismi, cioè a meno di cambiamenti di nome, Z_p.
Ne segue che il solo campo finito di ordine p, con p primo, a meno di isomorfismi è Z_p.

Prop 4.17 *Ogni campo finito K ha ordine p^n dove p è la caratteristica di K ed n un intero positivo.*

Dim. Sia p la caratteristica di K, essendo p un numero primo, ogni elemento diverso dallo 0 del gruppo additivo di K ha ordine p. Inoltre il gruppo additivo di K è abeliano e dunque, per ogni divisore d dell'ordine m di K, esiste un sottogruppo di $< K, + >$ di ordine d, in particolare se q con $q \neq p$ fosse un fattore primo di m, il gruppo additivo $< K, + >$ avrebbe un sottogruppo H di ordine q che sarebbe ciclico. Il generatore di H avrebbe periodo q(rispetto alla somma), il che vuol dire che come elemento dell'anello avrebbe caratteristica q . Esisterebbe perciò in K un elemento di caratteristica q contro il supposto. L'unico fattore primo di m è pertanto p, da cui $q = p^n$ per qualche intero positivo n.

Ci chiediamo ora se esiste un campo di ordine p^n, per ogni numero primo p e per ogni intero positivo n.
Ovviamente se $n = 1$ un campo di ordine p esiste ed è il campo Z_p che è sostanzialmente l'unico campo di ordine p.
Supponiamo allora $n > 1$. Se esiste un campo K di ordine p^n, K deve contenere (una copia di) Z_p ed elementi non appartenenti a Z_p. Sia $\alpha \in K - Z_p$, K deve allora contenere tutti gli elementi della forma $a_n\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0$ con $a_i \in Z_p,\ 0 \leq i \leq n$, ovvero tutti i "polinomi" in α a coefficienti in Z_p. Tali elementi non possono essere tutti distinti in quanto K è finito, pertanto si avrà $b_r\alpha^r + b_{r-1}\alpha^{r-1} + ... + b_1\alpha + b_0 = c_s\alpha^s + c_{s-1}\alpha^{s-1} + ... + c_1\alpha + c_0$ per qualche coppia di interi positivi $r,\ s$ con $r \geq s$ e per $b_i, c_i \in Z_p$ con $b_i \neq c_i$ per almeno un i. Dunque esiste un polinomio $f(x) = b_r x^r + ... + b_{s+1}x^{s+1} + (b_s - c_s)x^s + ... + (b_0 - c_0) \in Z_p[x]$ che ammette α come radice. Il polinomio $f(x)$ o è irriducibile su Z_p o si decompone nel prodotto di fattori irriducibili su Z_p (Prop. 4.15) e, visto che un campo è privo di divisori dello 0, α deve essere radice di uno di questi fattori irriducibili.

Dunque
se esiste un campo K di ordine p^n, ogni elemento di $K - Z_p$ è radice di un polinomio irriducibile $f(x)$ in $Z_p[x]$.

Inoltre
l'insieme I dei polinomi a coefficienti in Z_p che ammettono α come radice è un ideale di $Z_p[x]$ ed esiste un polinomio $f(x) \in I$ irriducibile su Z_p che divide ogni polinomio di I.
La verifica che I è ideale, è standard, infatti la differenza di due polinomi di I (ovvero polinomi di $Z_p[x]$ aventi α come radice) sta in $Z_p[x]$ ed ammette α come radice, quindi sta in I, inoltre il prodotto di un qualunque polinomio di $Z_p[x]$ con un qualsiasi polinomio di I, appartiene a $Z_p[x]$ ed ammette α come radice e dunque sta in I. Tra tutti i polinomi di I sia $f(x)$ un polinomio non nullo di grado minimo in I, e sia $i(x)$ un polinomio di I, detti $q(x)$ ed $r(x)$ rispettivamente il quoziente ed il resto della divisione di $i(x)$ per $f(x)$ si ha $i(x) = q(x)f(x) + r(x)$, ovvero $r(x) = i(x) - q(x)f(x)$ quindi $r(x)$ appartiene ad I, ma avendo $r(x)$ grado inferiore ad $f(x)$ segue allora che $r(x)$ è il polinomio nullo, pertanto $i(x) = q(x)f(x)$. Quindi tutti e soli i polinomi (non nulli) di I irriducibili su Z_p sono i polinomi di grado minimo e fra di essi ne esiste uno ed uno solo che è monico.

Quindi abbiamo dimostrato il seguente

Teor 4.18 *Dato un campo finito K di caratteristica p (e quindi di ordine p^n) e considerato il suo sottocampo minimo Z_p, per ogni elemento $\alpha \in K - Z_p$ esiste unico un polinomio monico irriducibile $f(x)$ che ammette α come radice.*

Tale polinomio si chiama *polinomio minimo* di α in $Z_p[x]$.

Sia $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_1x + a_0$ il polinomio minimo di α, ogni elemento k di K della forma $b_n\alpha^n + b_{n-1}\alpha^{n-1} + ... + b_1\alpha + b_0$ con $b_i \in Z_p$, $0 \leq i \leq n$, ovvero ogni "polinomio" in α a coefficienti in Z_p, può essere scritto in uno ed un sol modo come un "polinomio" in α a coefficienti in Z_p di grado inferiore ad m. Infatti, essendo α radice di $f(x)$, sussiste in K l'identità $\alpha^m = -(a_{m-1}\alpha^{m-1} + ... + a_1\alpha + a_0)$ e quindi sostituendo iterativamente in $k = b_n\alpha^n + b_{n-1}\alpha^{n-1} + ... + b_1\alpha + b_0$ ogni occorrenza di α^m con $-(a_{m-1}\alpha^{m-1} + ... + a_1\alpha + a_0)$ si ottiene una scrittura di k come "polinomio" in α a coefficienti in Z_p di grado inferiore ad m. Supponiamo ora che ci siano due scritture diverse $d_r\alpha^r + d_{r-1}\alpha^{r-1} + ... + d_1\alpha + d_0, c_s\alpha^s + c_{s-1}\alpha^{s-1} + ... + c_1\alpha + c_0$ di k come polinomi in α a coefficienti in Z_p di grado inferiore ad m allora si avrebbe $d_r\alpha^r + d_{r-1}\alpha^{r-1} + ... + d_1\alpha + d_0 - (c_s\alpha^s + c_{s-1}\alpha^{s-1} + ... + c_1\alpha + c_0) = 0$ e dunque α sarebbe radice di un polinomio in $Z_p[x]$ con grado inferiore ad n, contro l'ipotesi che $f(x)$ sia il polinomio minimo di α in $Z_p[x]$.
Il numero di scritture distinte di elementi di K come "polinomi" in α a coefficienti in Z_p è dunque p^m ed è facile verificare che l'insieme dei "polinomi" in α a coefficienti in Z_p costituiscono un sottocampo di K che chiamiamo *estensione semplice algebrica* di Z_p mediante α ed indichiamo con $Z_p(\alpha)$.
In particolare dunque se $|K| = p^n$ ed esiste un elemento $\alpha \in K - Z_p$ il cui polinomio minimo $f(x)$ in $Z_p[x]$ ha grado n, si ha $K = Z_p(\alpha)$.

Tutto ciò che abbiamo visto sopra può sembrare poco utile allo scopo di provare l'esistenza di un campo di ordine p^n, infatti si parte sempre dall'ipotesi che un tale campo esista. Vediamo ora come procedere in generale

Def 4.19 *Siano F un campo finito, $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ un polinomio monico di grado n irriducibile su F, $a(x), b(x) \in F[x]$. Chiamiamo prodotto modulo $f(x)$ di $a(x)$ con $b(x)$, e scriviamo $a(x)b(x)$ $(mod\ f(x))$, il resto della divisione dell'usuale prodotto $a(x)b(x)$ per $f(x)$.*

Teor 4.20 *Siano F un campo finito di ordine q, $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ un polinomio monico di grado n irriducibile su F, l'insieme K dei polinomi di $F[x]$ di grado inferiore ad n rispetto alla usuale somma di polinomi ed al prodotto di polinomi modulo $f(x)$, è un campo finito di ordine q^n. Il polinomio $f(x)$ si dice polinomio generatore di K.*

Dim. Ovviamente $< K, + >$ è un gruppo abeliano. Inoltre è facile verificare che K rispetto al prodotto modulo $f(x)$ è un semigruppo abeliano, infatti il prodotto modulo $f(x)$ è un'operazione interna su K e gode delle proprietà associativa e commutativa perché è associativo e commutativo l'usuale prodotto di polinomi. Inoltre l'unità e di F è unità per K.
Resta da verificare che ogni elemento diverso da 0 ammette inverso. Sia dunque $g(x) \in K$, poiché $f(x)$ è irriducibile (ed ha grado maggiore di $g(x)$), $M.C.D.(f(x), g(x)) = e$, dove e indica l'unità di F, quindi esistono due polinomi $\lambda(x), \mu(x) \in F[x]$ tali che $e = \lambda(x)f(x) + \mu(x)g(x)$, pertanto $e = \mu(x)g(x)$ $(mod\ f(x))$ e dunque $g(x)$ ammette inverso (e tale inverso è $\mu(x)$ $(mod\ f(x))$ quindi ha grado minore di n).

Dalla distributività dell'usuale prodotto di polinomi rispetto alla somma, segue poi subito la distributività rispetto alla somma del prodotto modulo $f(x)$.
Dunque K è un campo rispetto a usuale somma di polinomi e prodotto modulo $f(x)$.
Inoltre è immediato verificare che $|K| = q^n$.

Osserviamo che il polinomio generatore $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ ammette x come radice in K. Poiché il nome della variabile in un polinomio può essere scelto arbitrariamente, per evitare ambiguità fra la variabile del polinomio e la x pensata come elemento di K chiamiamo per il momento y la variabile del polinomio f, otteniamo quindi $f(y) = y^n + a_{n-1}y^{n-1} + ... + a_1y + a_0$ e calcoliamo $f(x)$ in K, questo significa che dopo aver effettuato la sostituzione della variabile con l'elemento $x \in K$ facciamo i prodotti modulo $f(x)$, ottenendo quindi $f(x) = 0$.

Inoltre se prendiamo $F = Z_p$ il teorema precedente dice che se esiste un polinomio $h(x)$ di grado n irriducibile su Z_p, esiste anche un campo di ordine p^n, che indicheremo con $Z_p(x)$. Tale campo si costruisce a partire da Z_p usando come polinomio generatore $h(x)$ e può essere visto come l'estensione di Z_p con un elemento (simbolico) x, radice del polinomio irriducibile $h(y)$.

Es 4.21 Consideriamo il campo Z_3 ed il polinomio $f(x) = x^2 + x + 2 \in Z_3[x]$ irriducibile su Z_3. Il campo $K_1 = Z_3(x)$ ha come elementi $0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2$. La somma è la solita somma di polinomi e nel prodotto bisogna tener conto dell'identità $x^2 = -x-2 = 2x+1$, per cui si ha ad esempio $(x+2)(2x+2) = 2x^2+1 = 2(2x+1)+1 = x$. Osservate che f ammette in K_1 anche la radice $2x+2$, infatti $f(2x+2) = (2x+2)^2+(2x+2)+2 = x^2+2x+1+2x+2+2 = x^2+x+2 = 0$. Se si considera $Z_3(2x+2)$ si ottengono tutti i polinomi nell'indeterminata $2x+2$ a coefficienti in Z_3 di grado minore o uguale ad 1, cioè $0, 1, 2, 2x+2, 2x+2+1 = 2x, 2x+2+2 = 2x+1, 2(2x+2) = x+1, 2(2x+2)+1 = x+2, 2(2x+2)+2 = x$, ed è facile osservare che $Z_3(x)$ e $Z_3(2x+2)$ sono isomorfi (cioè ottenuti uno dall'altro a meno di scambio di nomi) tramite la corrispondenza $\psi : Z_3(x) \to Z_3(2x+2)$ che porta x in $2x+2$ e tiene fermi gli elementi di Z_3; la ψ cioè agisce nel seguente modo: $\psi(0) = 0,\ \psi(1) = 1,\ \psi(2) = 2,\ \psi(x) = 2x+2,\ \psi(x+1) = 2x,\ \psi(x+2) = 2x+1,\ \psi(2x) = x+1,\ \psi(2x+1) = x+2,\ \psi(2x+2) = x$.
Se poi si considera il polinomio $g(x) = x^2 + 1 \in Z_3[x]$ irriducibile su Z_3 e si costruisce il campo K_2 di ordine 9 che ha $g(x)$ come polinomio generatore, K_2 ha gli stessi elementi (e la stessa operazione di somma) di K_1, ma nel prodotto bisogna tener conto dell'identità $x^2 = -1$, per cui si ha ad esempio $(x+2)(2x+2) = 2x^2+1 = 2(-1)+1 = -1 = 2$. Si può verificare che K_1 e K_2 sono isomorfi nella corrispondenza $\theta : K_1 = Z_3(x) \to K_2$ così definita: $\theta(0) = 0,\ \theta(1) = 1,\ \theta(2) = 2,\ \theta(x) = 2x+1,\ \theta(x+1) = 2x+2,\ \theta(x+2) = 2x,\ \theta(2x) = x+2,\ \theta(2x+1) = x,\ \theta(2x+2) = x+1$.

Quanto notato nell'esempio precedente è un risultato generale, sussistono infatti le seguenti

Prop 4.22 *Sia F un campo finito. Se α e β sono radici di un polinomio $f \in F[x]$ irriducibile su F, le estensioni $F(\alpha)$ e $F(\beta)$ sono isomorfe tramite l'isomorfimo ψ che porta α in β e tiene fermi gli elementi di F.*

Prop 4.23 *Sia F un campo finito. Se $f(x), g(x) \in F[x]$ sono polinomi irriducibili su F dello stesso ordine n, le estensioni K_1 e K_2 di F ottenute usando come polinomi generatori rispettivamente $f(x)$ e $g(x)$ sono isomorfe.*

Def 4.24 (campo di spezzamento di un polinomio). *Siano F un campo, $g(x) \in F[x]$ un qualsiasi polinomio a coefficienti in F e K un'estensione di F. Se in $K[x]$ il polinomio $g(x)$ può essere scritto come $a_n(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$ e se K è il minimo campo contenente F ed $\alpha_1, \alpha_2, ..., \alpha_n$, il campo K si dice campo di spezzamento di $g(x)$ su F.*

Si può provare il seguente

Teor 4.25 *Se F è un campo e $g(x)$ è un polinomio di grado $n > 0$ a coefficienti in F, allora esiste un campo di spezzamento di $g(x)$ su F e tale campo è unico a meno di isomorfismi*

Per costruire il campo di spezzamento si considera la decomposizione di g in fattori irriducibili su F: $g(x) = a_n g_1(x)...g_r(x), 1 \leq r < n$ e poi, supposto che $g_i(x)$ sia il primo fattore con grado maggiore di 1, si costruisce K_1 che è l'estensione di F fatta usando come polinomio generatore il polinomio $< g_i(x) >$. Come abbiamo osservato precedentemente in K_1 il polinomio g_i ammette una radice θ e quindi è riducibile (e pure riducibili possono essere diventati anche altri polinomi g_j), inoltre $K_1 = F(\theta)$. Si considera quindi la nuova decomposizione di g in K_1 e si continua con lo stesso procedimento. Poiché la somma dei gradi dei fattori è n e ad ogni passo un fattore almeno riduce il suo grado, dopo un numero finito di passi si trova un campo in cui il polinomio g si spezza in fattori lineari e che risulta essere l'estensione di F mediante l'insieme delle radici di g. L'unicità, a meno di isomorfismi, è una generalizzazione (non del tutto banale) delle Prop.4.22 e 4.23.

Teor 4.26 *Per ogni intero della forma p^n, con p numero primo ed n intero positivo, esiste un campo di ordine p^n e tale campo è unico a meno di isomorfismi.*

Dim. Ogni campo finito K con $|K| = p^n$, se esiste, contiene (a meno di isomorfismi) il sottocampo Z_p (proprietà 4) e può essere pensato come una estensione di Z_p.
Poniamo $q = p^n$ e consideriamo il campo di spezzamento K del polinomio $x^q - x \in Z_p[x]$ (di cui abbiamo già provato l'esistenza).
Verifichiamo che $F = \{k \in K \mid k^q = k\}$ è un sottocampo di K. Siano infatti $a, b \in F$. Dalla 3) abbiamo $(a-b)^q = a^q - b^q = a - b$ e ovviamente si ha $(ab^{-1})^q = a^q(b^{-1})^q = ab^{-1}$ e quindi $a - b, ab^{-1} \in F$. Del resto le radici del polinomio $x^q - x$ sono tutte semplici, infatti la derivata del polinomio è $qx^{q-1} - 1 = -1$ (ricordate che siamo in caratteristica p e che q è divisibile per p) e non ha radici comuni col polinomio. Dunque $|F| = q$, inoltre F contiene Z_p e tutte le radici del polinomio $x^q - x \in Z_p[x]$, quindi coincide col suo campo di spezzamento K. Abbiamo quindi provato l'esistenza di un campo di ordine q.
Sia ora L un altro campo di ordine q, dalla 2) $\forall l \in L$ si ha $l^q = l$. Ogni elemento di L è dunque radice del polinomio $x^q - x \in M[x]$, ove M è un qualsiasi sottocampo di L, quindi il polinomio $x^q - x \in M[x]$ si spezza in prodotto di fattori lineari in $M[x]$, ove M è un qualsiasi sottocampo di L. Quindi L è il campo di spezzamento di $x^q - x$ su un qualunque sottocampo di L. In particolare, poiché L ha Z_p come sottocampo minimo, è il campo di spezzamento di $x^q - x \in Z_p[x]$ e dunque tutti i campi di ordine q sono campi di spezzamento di $x^q - x$ su $Z_p[x]$ e quindi isomorfi fra loro.

Nel seguito il campo di ordine $q = p^n$ sarà indicato con F_q e chiamato polinomio di Galois di ordine q (si usa anche spesso la notazione $GF(q)$ per indicare tale campo).

Vogliamo ora studiarne la struttura.
Per farlo proviamo una interessante proprietà di struttura dei campi finiti.

Teor 4.27 *Il gruppo moltiplicativo di ogni campo finito è ciclico.*

Dim. Sia F_q campo finito di ordine q e supponiamo $q > 2$ (se $q = 2$ il gruppo moltiplicativo del campo è costituito dalla sola unità ed è banalmente ciclico). Il gruppo moltiplicativo $F_q^* = F_q - \{0\}$ di F_q ha ordine $h = q - 1$ che non è primo. Sia dunque $h = p_1^{r_1} p_2^{r_2} ... p_m^{r_m}$ la decomposizione di h in fattori primi. Per ogni $1 \leq i \leq m$ il polinomio $x^{h/p_i} - 1$ ha al più h/p_i radici in F_q e poiché $h/p_i < h$ esiste un elemento $a_i \in F_q^*$ che non è radice di $x^{h/p_i} - 1$, poniamo $b_i = a_i^{h/p_i^{r_i}}$, si ha ovviamente

$b_i^{p_i^{r_i}} = a_i^h = 1$ e dunque il periodo di b_i è un divisore di $p_i^{r_i}$ che, essendo $b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1$, non divide $p_i^{r_i-1}$, pertanto il periodo di b_i è $p_i^{r_i}$.
Proviamo ora che $b = b_1 b_2 ... b_m$ ha periodo h. Ovviamente il periodo di b divide h, e, se lo divide propriamente, divide uno almeno degli h/p_i. Senza perdita di generalità supponiamo che il periodo di b divida h/p_1. Allora si avrebbe $1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} ... b_m^{h/p_1}$. Poiché per $2 \leq i \leq m$ il periodo $p_i^{r_i}$ di b_i divide h/p_1 abbiamo $b_i^{h/p_1} = 1$, da cui si ottiene l'assurdo $1 = b_1^{h/p_1}$. Perciò b ha periodo h e genera quindi F_q^*.

Def 4.28 (elemento primitivo). *Sia F un campo finito, un generatore del gruppo moltiplicativo $F^* = F - \{0\}$ si dice* elemento primitivo di F.

Osserviamo ora che *se H e K sono due campi finiti ed H è un sottocampo di K, allora K è un'estensione semplice algebrica di H definita da un qualunque elemento primitivo ξ di K.*
Infatti per prima cosa ξ è algebrico su H, essendo radice del polinomio $x^{|K|-1} - 1 \in H[x]$, inoltre $H(\xi) \subseteq K$ ma 0 e tutte le potenze di ξ appartengono a $H(\xi)$ perciò (essendo K^* ciclico, generato da ξ) $K \subseteq H(\xi)$ e quindi si ha subito $K = H(\xi)$.
Da questo si ricava che
esiste un polinomio minimo di ξ su H e tale polinomio è irriducibile su K.
Il polinomio minimo su K di un elemento primitivo su H si dice *polinomio primitivo* su K.
In particolare il campo F_{p^n} risulta essere estensione algebrica semplice di Z_p definita da un elemento primitivo di F_{p^n}. Tale elemento deve perciò avere un polinomio minimo di grado n su Z_p (che pe definizione è un polinomio primitivo su Z_p) e quindi esiste un polinomio irriducibile di grado n su Z_p. (Notate che ogni polinomio primitivo su un campo K è irriducibile su K ma non vale il viceversa, come vedremo più avanti).

Come conseguenza *F_{p^m} è (isomorfo ad) un sottocampo di F_{p^n} se e solo se m divide n.*
Infatti se F_{p^m} è un sottocampo di F_{p^n}, il campo F_{p^n} è isomorfo a $F_{p^m}(\xi)$ per un opportuno ξ e dunque ha ordine $(p^m)^r$ dove r è il grado del polinomio minimo di ξ. Viceversa se m divide n allora $p^m - 1$ divide $p^n - 1$ ed il polinomio $x^{p^m-1} - 1$ divide il polinomio $x^{p^n-1} - 1$ in $Z_p[x]$, quindi $x^{p^m} - x$ divide $x^{p^n} - x$ in $Z_p[x]$ e quindi ogni radice di $x^{p^m} - x$ (cioè ogni elemento del campo di spezzamento del polinomio $x^{p^m} - x$) è radice di $x^{p^n} - x$ (cioè appartiene al campo di spezzamento del polinomio $x^{p^n} - x$). Poiché nella dimostrazione del Teor 4.26 abbiamo provato che il campo di spezzamento di $x^{p^i} - x$ è isomorfo a F_{p^i} abbiamo che F_{p^m} è un sottocampo di F_{p^n}. Tra l'altro il fatto che il gruppo moltiplicativo di ogni campo finito sia ciclico, dice anche che F_{p^n} ha un solo sottocampo di ordine p^m.

In conclusione ci sono due "tipi" di campi finiti, i campi che possiamo chiamare modulari, costituiti dall'insieme delle classi di resti modulo p, con p primo, rispetto all'usuale somma e prodotto di classi di resti ed i campi, che possiamo chiamare polinomiali, che sono costititi dai polinomi a cofficienti in Z_p con p primo aventi grado minore di n rispetto alla solita somma di polinomi ed al prodotto modulo un polinomio irriducibile $f(x)$ di grado n su Z_p che viene chiamato *polinomio generatore* del campo polinomiale.
Osservate che ogni campo finito F_{p^n} con $n = mr,\ m, r > 1$ può essere anche rappresentato come estensione di F_p^r mediante un polinomio $g(x) \in F_r[x]$ di grado m irriducibile su F_p^r, o come estensione di F_p^m mediante un polinomio $h(x) \in F_m[x]$ di grado r irriducibile su F_p^m. I campi costruiti in questo modo, che sono ovviamente tutti isomorfi tra loro e ad F_{p^n}, vengono detti campi composti e questo modo di rappresentare i campi finiti può essere utile nelle applicazioni.

4.3 Basi di campi finiti

Ricordiamo alcune definizioni

Def 4.29 (spazio vettoriale) *Siano $< V, + >$ un gruppo abeliano e K un campo. V è uno* spazio vettoriale su K *se è definita una funzione $K \times V \to V$, che chiameremo prodotto esterno e indicheremo con la notazione infissa $\cdot$, con le sequenti proprietà*

1. $\forall v, w \in V$ *e* $\forall k \in K$ *si ha* $k \cdot (v + w) = k \cdot v + k \cdot w$
2. $\forall v \in V$ *e* $\forall h, k \in K$ *si ha* $(h + k) \cdot v = h \cdot v + k \cdot v$
3. $\forall v \in V$ *e* $\forall h, k \in K$ *si ha* $(hk) \cdot v = h \cdot (k \cdot v)$
4. $\forall v \in V$ *detta* 1 *l'unità di* K *si ha* $1 \cdot v = v$

Gli elementi di V si chiamano vettori e gli elementi di K scalari.

(Potreste non aver mai visto questa definizione formale, ma sicuramente tutti conoscete bene il campo vettoriale R^n sul campo reale R, costituito dalle n-uple di numeri reali. Questo esempio può servirvi da modello per quanto segue).

Def 4.30 (generatori, indipendenza lineare, base, dimensione) *Sia V uno spazio vettoriale su K. Un sottoinsieme G di V si dice* insieme di generatori di V *se per ogni $v \in V$ esistono $v_1, v_2, ...v_n \in G$ e $k_1, k_2, ..., k_n \in K$ tali che $v = k_1 \cdot v_1 + k_2 \cdot v_2 + ... + k_n \cdot v_n$. I vettori $w_1, w_2, ...w_s$ si dicono* linearmente indipendenti *se, per ogni $k_1, k_2, ..., k_s \in K$, $k_1 \cdot w_1 + k_2 \cdot w_2 + ... + k_s \cdot w_s = \underline{0}$ implica $k_1 = k_2 = ... = k_s = 0$ (dove $\underline{0}$ indica l'elemento neutro di $< V, + >$ mentre 0 indica lo zero di K). Un insieme di generatori linearmente indipendenti si dice* base *di V su K. Uno spazio vettoriale non ha un'unica base ma si può provare che o tutte le basi hanno la stessa cardinalità. La cardinalità di una base di V si dice* dimensione *di V.*

Un campo finito F_r può essere pensato come uno spazio vettoriale su un qualsiasi suo sottocampo F_q.
La somma vettoriale è la somma in F_r ed il prodotto scalare vettore è il prodotto in F_r (gli elementi di F_q stanno in F_r). Tralasciando una verifica più formale, sia $r = q^t$, ogni elemento di F_{q^t}, essendo un polinomio in x a coefficienti in F_q di grado minore di t, può essere identificato con la t-upla dei suoi coefficienti , quindi F_{q^t} può essere visto come lo spazio vettoriale, F_q^t, delle t-uple di F_q sul campo F_q (che è una ovvia generalizzazione di R^t su R). La dimensione dello spazio vettoriale F_q^t è t (il grado del polinomio generatore $f(x)$).
Infatti F_q^t, come spazio di t-uple, ha come base l'insieme dei vettori $\{e_i \mid 1 \leq i \leq t\}$ dove e_i indica il vettore la cui unica componente non nulla è la i-esima che è uguale all'unità del campo F_q.
Tale base si chiama *base canonica* dell'estensione F_{q^t} di F_q. Una base di F_{q^t} su F_q formata da elementi della forma $1, \alpha, \alpha^2, ..., \alpha^{t-1}$ si dice *base polinomiale*. Un esempio di base polinomiale è costituito da $\{1, x, x^2, ..., x^{t-1}\}$. La base canonica è una base polinomiale, infatti in notazione polinomiale, il vettore e_i diventa il polinomio x^{t-i}, ove x^0 rappresenta l'unità di F_q.

Def 4.31 (elementi coniugati) *Siano F_{q^t} un campo finito ed α un suo elemento. Gli elementi $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{t-1}}$ si chiamano i* coniugati di α rispetto a F_q.

I coniugati di α hanno lo stesso periodo di α nel gruppo moltiplicativo di F_{q^t}.
Gli elementi coniugati di α sono tutti radici del polinomio minimo $g(x)$ di α sopra F_q e sono

distinti sse $g(x)$ ha grado t.
Infatti sia $g(x) = a_s x^s + a_{s-1}x^{s-1} + ... + a_0$, per le le proprietà 3) e 2) sappiamo che $0 = g(\alpha)^{q^j} = a_s^{q^j}\alpha^{sq^j} + a_{s-1}^{q^j}\alpha^{(s-1)q^j} + ... + a_0^{q^j} a_s(\alpha^{q^j})^s + a_{s-1}(\alpha^{q^j})^{(s-1)} + ... + a_0 = g(\alpha^{q^j})$, dunque α^{q^j} è radice di $g(x)$ per ogni intero positivo j. Supponiamo $s = t$, se ci fossero $0 \leq i < j \leq t-1$ tali che $\alpha^{q^j} = \alpha^{q^i}$, si avrebbe, moltiplicando entrambi i membri per $\alpha^{q^{t-j}}$, $\alpha^{q^t} = \alpha^{q^{t-j+i}}$ e quindi, per la 2), $\alpha = \alpha^{q^{t-j+i}}$ ed α sarebbe radice del polinomio $x - x^{q^{t-j+i}} \in F_q[x]$, α apparterrebbe quindi al campo di spezzamento di $x - x^{q^{t-j+i}}$ che è il campo $F_{q^{t-j+i}}$, e allora $F_{q^t} = F_q(\alpha)$ sarebbe un suo sottocampo per cui t dovrebbe dividere $t - j + i < t$, assurdo. Se invece $s \neq t$, ovviamente s divide propriamente t (perché α appartiene a F_{q^t} e quindi $F_q(\alpha)$, che ha ordine q^s, è un sottocampo di F_{q^t}) ma allora $g(x)$ ha al più s radici e $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{t-1}}$ non possono essere distinti. Si può provare che in questo caso i coniugati di α rispetto a F_q sono gli elementi distinti $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{s-1}}$ ciascuno ripetuto t/s volte.
Se gli elementi $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{t-1}}$ costituiscono una base per F_{q^t}, pensato come spazio vettoriale su F_q, tale base si chiama *base normale di F_{q^t} su F_q*.
Si può dimostrare che *per ogni campo finito K ed ogni suo sottocampo F esiste una base normale di K su F formata da elementi primitivi di K.*
La rappresentazione degli elementi del campo finito F_{q^t} usando una sua base normale su F_q è molto conveniente quando si voglia effettuare un elevamento a potenza q di un generico elemento di F_{q^t}. Infatti sia $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{t-1}}$ una base normale e sia $\beta = a_0 \cdot \alpha + a_1 \cdot \alpha^q + a_2 \cdot \alpha^{q^2} + ... + a_{t-1}\alpha^{q^{t-1}} \in F_{q^t}$ con $a_i \in F_q$ per ogni $0 \leq i \leq t-1$; allora $\beta^q = (a_0 \cdot \alpha + a_1 \cdot \alpha^q + a_2 \cdot \alpha^{q^2} + ... + a_{t-1}\alpha^{q^{t-1}})^q = a_0^q \cdot \alpha^q + a_1^q \cdot \alpha^{q^2} + a_2^q \cdot \alpha^{q^3} + ... + a_{t-1}^q \alpha^{q^t} = a_0 \cdot \alpha^q + a_1 \cdot \alpha^{q^2} + a_2 \cdot \alpha^{q^3} + ... + a_{n-1}$ che è sostanzialmente uno shift ciclico delle componenti della t-upla formata dai coefficienti di β rappresentato nella base normale.

Es 4.32 Cerchiamo una base polinomiale ed una base normale per F_8 come estensione del campo Z_2. Costruiamo F_8 a partire dal polinomio $x^3 + x^2 + 1 \in Z_2[x]$ che è irriducibile su Z_2 (essendo di grado 3 basta verificare che non ha radici in Z_2). Gli elementi di F_8, sono allora $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$. La base polinomiale è $\{1, x, x^2\}$, questa base non è normale in quanto $x^4 = x^3 \cdot x = (x^2+1) \cdot x = x^3 + x = (x^2+1) + x \neq 1$, gli elementi coniugati di x rispetto a Z_2 sono allora $x, x^2, x^2+x+1 (= x^4)$. Verifichiamo che formano una base, si ha $1 = x + x^2 + (x^2 + x + 1)$ e dunque $x, x^2, x^2+x+1 (= x^4)$ generano 1, e di conseguenza tutti gli elementi di F_8. Gli elemanti $x, x^2, x^2+x+1 (= x^4)$ sono pertanto un insieme di generatori di F_8 formato da un numero di vettori uguale alla dimensione dello spazio vettoriale F_8 su Z_2 e dunque sono una base. Osserviamo che se vediamo F_8 come estensione del campo Z_2 effettuata attraverso il polinomio irriducibile $x^3 + x + 1 \in Z_2[x]$, l'insieme $B = \{x, x^2, x^2+x+1\}$ è ancora una base (nella definizione di base il prodotto di F_8 non è coinvolto), ma non è normale, infatti $x^4 = x^2 + x$ e $(x^2+x+1)^2 = x+1$ per cui gli elementi di B non sono coniugati. Una base normale per F_8 in questo caso sarebbe ad esempio $x^2 + x + 1, x + 1, x^2 + 1$.

Ricordiamo brevemente due criteri che permettono di stabilire se date t-uple di elementi sono rispettivamente basi e basi normali di F_{q^t} su F_q.

Prop 4.33 *Siano $\alpha_1, \alpha_2, ..., \alpha_t \in F_{q^t}$. Allora $\{\alpha_1, \alpha_2, ..., \alpha_t\}$ è una base di F_{q^t} su F_q sse*

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_t \\ \alpha_1^q & \alpha_2^q & \dots & \alpha_t^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{q^{t-1}} & \alpha_2^{q^{t-1}} & \dots & \alpha_t^{q^{t-1}} \end{vmatrix} \neq 0$$

Prop 4.34 *Sia $\alpha \in F_{q^t}$. Allora $\{\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{t-1}}\}$ è una base normale di F_{q^t} su F_q sse i polinomi $x^t - 1$ e $\alpha \cdot x^{t-1} + \alpha^q \cdot x^{t-2} + \alpha^{q^2} \cdot x^{t-3} + ... + \alpha^{q^{t-1}}$ sono relativamente primi.*

4.4 Polinomi e campi ciclotomici

Def 4.35 (campo ciclotomico, radice dell'unità). *Siano K un campo ed n un intero positivo. Il campo di spezzamento di $x^n - 1 \in K[x]$ si chiama* n-esimo campo ciclotomico su K *e si indica con $K^{(n)}$. Le radici di $x^n - 1$ in $K^{(n)}$ si chiamano* radici n-esime dell'unità su K *ed il loro insieme si indica con $E^{(n)}$.*

Osserviamo ora che un qualunque campo finito F_q è il campo di spezzamento del polinomio $x^{q-1}-1$ (pensato come polinomio a coefficienti su un qualsiasi sottocampo di F_q). Infatti ogni elemento non nullo di F_q ha (come elemento del gruppo moltiplicativo di F_q) un periodo che divide $q-1$ e dunque è una radice del polinomio $x^{q-1} - 1$. Poiché tale polinomio ha esattamente $q-1$ radici, allora le sue radici sono tutti e soli gli elementi non nulli di F_q, pertanto $x^{q-1} - 1$ si spezza su F_q ma non si può spezzare su alcun sottocampo di F_q, e pertanto si ha la seguente

Prop 4.36 *Il campo finito F_q è il $(q-1)$-esimo campo ciclotomico su un qualsiasi suo sottocampo.*

Prop 4.37 *Siano K un campo finito di caratteristica p ed n un intero positivo non divisibile per p. Allora $E^{(n)}$ è un gruppo ciclico di ordine n rispetto al prodotto definito in $K^{(n)}$.*

Dim. Poiché $x^n - 1$ non ha radici multiple in $K^{(n)}$ (in quanto la sua derivata è nx^{n-1} ed ammette solo la radice 0), $|E^{(n)}| = n$. Inoltre $E^{(n)}$ è un sottogruppo di $< K^{(n)}, \cdot >$, infatti siano $a, b \in E^{(n)}$ (cioè sia $a^n = b^n = 1$), allora $(ab^{-1})^n = a^n b^{-n} = 1$ e quindi $ab^{-1} \in E^{(n)}$. Ora usando la stessa tecnica della dimostrazione del Teor 4.27 si ottiene che $E^{(n)}$ ha un elemento di periodo n e quindi è ciclico.

Def 4.38 (radice primitiva dell'unità, polinomio ciclotomico). *Siano K un campo finito di caratteristica p ed n un intero positivo non divisibile per p. Un generatore ξ di $< E^{(n)}, \cdot >$ si chiama* radice primitiva n-esima dell'unità su K. *Si chiama* n-esimo polinomio ciclotomico su K il polinomio $Q_n(x) = \prod_{1 \le s \le n, M.C.D(n,s)=1}(x - \xi^s)$, dove ξ è una radice primitiva dell'unità.

(Le definizioni e le proprietà precedenti non richiedono in realtà di partire da un campo K finito, anzi forse vi può aiutare ricordare il concetto di radice primitiva dell'unità del campo complesso che avete visto in I anno e fare ora il parallelo con tale concetto, tuttavia, in questo contesto, possiamo limitarci a considerare K finito). È facile osservare che $Q_n(x)$ *non dipende da* ξ, infatti abbiamo visto che se a è un generatore di un gruppo ciclico di ordine n, tutti e soli i generatori del gruppo sono della forma a^s con $1 \le s \le n$ e $M.C.D(s,n) = 1$, quindi $Q_n(x)$ è il prodotto di tutti i polinomi del tipo $x - \zeta \in K^{(n)}[x]$, dove ζ è una radice primitiva n-esima dell'unità su K.
Inoltre, sempre *nell'ipotesi che K sia un campo di caratteristica p con p che non divide n il polinomio $x^n - 1 \in K[x]$ è il prodotto dei polinomi ciclotomici $Q_d(x)$ con d divisore di n.*
Infatti, detta ξ una radice n-esima primitiva dell'unità su K, si ha $x^n - 1 = \prod_{1 \le i \le n}(x - \xi^i)$, ma ξ^i ha periodo $h = n/M.C.D.(n,i)$ quindi è una radice primitiva h-esima dell'unità su K (con h che divide n) e viceversa per ogni divisore d di n, $\xi^{n/d}$ ha periodo d e quindi è una radice primitiva d-esima dell'unità. Dunque per ogni divisore d di n possiamo raggruppare tutti i polinomi $(x - \xi^j)$ con ξ^j radice primitiva d-esima dell'unità il cui prodotto è proprio $Q_d(x)$.
Utilizzando quanto sopra osservato si può allora provare che $Q_n(x) \in F[x]$ *dove F indica il sottocampo minimo di K.*

Ovviamente $Q_1(x) = x - 1 \in F[x]$. Supponiamo $Q_m(x) \in F[x]$ per ogni $m < n$, allora $\prod_{1 \leq d < n, d|n} Q_d(x) \in F[x]$ ed essendo $Q_n(x) = \frac{(x^n-1)}{\prod_{1 \leq d < n, d|n} Q_d(x)}$ con $x^n - 1 \in F[x]$ si ottiene il risultato (effettuando la divisione dei polinomi in $F[x]$).

Es 4.39 Siano p un numero primo ed n un intero positivo qualsiasi, si ha allora $Q_{p^n} = \frac{x^{p^n}-1}{Q_1(x)Q_p(x)...Q_{p^{n-1}}(x)} = 1 + x^{p^{n-1}} + x^{2p^{n-1}} + ... + x^{(n-1)p^{n-1}}$

Inoltre sempre *nell'ipotesi che K sia un campo finito di caratteristica p ed ordine q con p che non divide n, $Q_n(x)$ si spezza nel prodotto di $\varphi(n)/d$ polinomi monici distinti e irriducibili dello stesso grado d e $K^{(n)}$ è il campo di spezzamento di uno qualsiasi di tali fattori su K, e risulta essere un'estensione di grado d su K dove d è il minimo intero positivo tale che $q^d \equiv 1$ mod n.*
Infatti sia η una radice primitiva n-esima dell'unità su F_q, η appartiene al campo F_{q^k} sse $\eta^{q^k} = \eta$ cioè sse $q^k \equiv 1$ *mod* n. Pertanto detto d il minimo intero positivo per cui $q^d \equiv 1$ *mod* n, η appartiene a F_{q^d} ma non appartiene ad alcuno dei suoi sottocampi. Dunque il polinomio minimo di η su F_q ha grado d ed essendo η una generica radice di $Q_n(x)$, tutti i fattori irriducibili (in $F_q[x]$) di $Q_n(x)$ hanno grado d.
Osserviamo infine che *se n è un intero positivo e d un suo divisore con $1 \leq d < n$ allora per ogni campo K l'n-esimo polinomio ciclotomico $Q_n(x)$ su K divide $\frac{x^n-1}{x^d-1}$.*
Infatti sappiamo già che $Q_n(x)$ divide $x^n - 1 = (x^d - 1)\frac{x^n-1}{x^d-1}$, inoltre poiché le radici di $Q_n(x)$ sono le radici primitive n-esime dell'unità, essendo d un divisore proprio di n, nessuna radice di $Q_n(x)$ ha periodo d, perciò $Q_n(x)$ e $x^d - 1$ non hanno radici comuni e quindi $M.C.D.(Q_n(x), x^d - 1) = 1$ da cui segue che $Q_n(x)$ divide $\frac{x^n-1}{x^d-1}$.

4.5 Rappresentazione degli elementi dei campi finiti.

Ricapitoliamo qui i modi di rappresentare gli elementi di un campo finito F_q con $q = p^n$, dove p, numero primo, è la caratteristica di F_q e possiamo supporre $n \leq 2$ (in quanto F_p con p primo è un campo che ci è ben noto).
F_q può essere visto come un'estensione di F_p, effettuata attraverso un polinomio f di grado n irriducibile in $F_p[x]$ e quindi i suoi elementi possono essere rappresentati (in modo unico) come polinomi in x (radice di f in F_q) di grado minore ad n. La somma di elementi è in questo caso molto semplice, mentre più complicato è il prodotto (che è fatto modulo f).
A questo punto potrebbe essere comodo trovare un elemento primitivo ξ di F_q perché in tal caso gli elementi di F_q diversi da 0 potrebbero essere tutti scritti come potenze di ξ ed il prodotto di lementi risulterebbe banale. In tal caso ovviamente si può preparare una tabella di conversione fra le scritture degli elementi come polinomi e come potenze di ξ per utilizzare la notazione polinomiale nel fare la somma e quella esponenziale nel fare il prodotto. Ma come trovare un elemento primitivo?
F_q può essere anche visto come il $(q-1)$-esimo campo ciclotomico su F_p, in tal caso F_q si può costruire a partire dalla decomposizione dell'$(q-1)$-esimo polinomio ciclotomico in fattori irriducibili in F_p (che avranno tutti lo stesso grado, come abbiamo visto). Una qualsiasi radice ζ di uno qualunque di questi fattori, è anche una radice primitiva $(q-1)$-esima dell'unità su F_p e quindi è un elemento primitivo di F_q, gli elementi di F_q sono allora lo 0 e le potenze positive (fino alla $(q-1)$-esima) di ζ.
Infine gli elementi di F_q possono avere una rappresentazione matriciale. Sia $f(x) = x^n + a_{n-1}x^{n-1} + ...a_1x + a_0$ un polinomio monico di grado n su un campo, $f(x)$ può essere visto come il polinomio

caratteristico della matrice $A = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}$ detta matrice associata ad $f(x)$.
È ben noto che $f(A) = 0$ (teorema di Cayley Hamilton: ogni matrice è radice del suo polinomio caratteristico). Se f è un polinomio monico irriducibile di grado n sul campo F_p allora la matrice A assume il ruolo di radice di $f(x)$ e gli elementi di F_q possono essere scritti come polinomi in A a coefficienti in F_p di grado minore di n. I calcoli si fanno in tal caso con le solite regole di somma e prodotto di matrici. La rappresentazione matriciale può essere anche utilizzata a partire da un fattore irriducibile del $(q-1)$-esimo polinomio ciclotomico su F_p. Se infatti C è la matrice associata a tale polinomio, gli elementi di F_q possono essere visti come potenze positive (fino alla $(q-1)$-esima) di C.

Es 4.40 Rappresentiamo nei modi sopra elencati gli elementi di F_9.
Un polinomio irriducibile di grado 2 su $F_3(= Z_3)$ è x^2+1 e dunque gli elementi di F_9 possono essere rappresentati da $\{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$, la somma è la usuale somma di polinomi ed il prodotto è fatto modulo x^2+1, cioè sostituendo 2 ad x^2 nell'usuale prodotto di polinomi di $Z_3[x]$ fino ad ottenere un polinomio di grado minore o uguale a 1. Si ha dunque $x \cdot x = 2$, $x \cdot (x+1) = x+2$, $x \cdot (x+2) = 2x+2$, $(x+1) \cdot (x+1) = 2x$, $(x+1) \cdot (x+2) = 1$, $(x+2) \cdot (x+2) = x$.
L'elemento x non è primitivo su F_9, infatti $x^1 = x$, $x^2 = 2$, $x^3 = 2x$, $x^4 = 1$, quindi pe avere una rappresentazione degli elementi di F_9 come potenze dovremmo cercare un elemnto primitivo. A tal proposito ricordiamo che F_9 è l'ottavo campo ciclotomico su Z_3. Da quanto visto sopra si ha $Q_8(x) = Q^{2^3}(x) = 1 + x^{2^2}$ e $1 + x^4$ si decompone in $Z_3[x]$ nel prodotto di due polinomi irriducibili di secondo grado (2 è il minimo intero positivo d per cui $3^d \equiv 1 \; mod \; 3$), infatti $1 + x^4 = (x^2 + x + 2)(x^2 + 2x + 2)$. Sia ora ζ una radice di $x^2 + 2x + 2$, tale radice è un elemento primitivo di F_9 e gli elementi di F_9 sono $\{0, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6, \zeta^7, \zeta^8\}$. Il prodotto di due elementi si calcola facilmente (usando le proprietà delle potenze), mentre non è semplice calcolare la somma di due elementi. Per collegarci alla rappresentazione precedente in cui la somma era semplice, possiamo notare che una radice del polinomio x^2+2x+2 in tale rappresentazione di F_9 è $2+x$ (infatti $(2+x)^2 + 2(2+x) + 2 = 4 + 4x + x^2 + 4 + 2x + 2 = 4 + 4x + 2 + 4 + 2x + 2 = 0$), quindi otteniamo la seguente tabella di conversione: $\zeta = 2 + x$, $\zeta^2 = 4 + 4x + x^2 = x$, $\zeta^3 = 2x + x^2 = 2x + 2$, $\zeta^4 = 2$, $\zeta^5 = 2x + 1$, $\zeta^6 = 2x$, $\zeta^7 = x + 1$, $\zeta^8 = 1$, da cui si ottiene facilmente ad esempio $\zeta^3 + \zeta^5 = \zeta^2$.
Ora se vogliamo usare la rappresentazione matriciale, abbiamo che la matrice A associata al polinomio $x^2 + 1$, monico di grado 2 irriducibile su Z_3, è $\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$. Gli elementi di F_9 sono allora: $\{0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 2I = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, I + A = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, 2I + A = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}, 2A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, I + 2A = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, 2I + 2A = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}\}$ (ricordarsi che gli elementi delle matrici sono in Z_3). I calcoli si fanno con le solite regole di somma e prodotto di matrici.
Se vogliamo lavorare su F_9 pensandolo come ottavo campo ciclotomico su Z_3 e usando la rappresentazione matriciale, possiamo considerare la matrice C associata al polinomio $x^2 + 2x + 2$. Si ha $C = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Il campo F_9 è allora fomato da $\{0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, C = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, C^2 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, C^3 = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}, C^4 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, C^5 = \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix}, C^6 = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}, C^7 = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}, C^8 =$

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$, dove la somma si effettua come somma di matrici, ad esempio $C^2 + C^4 = C$.

4.6 Polinomi irriducibili su campi finiti

Da quanto osservato precedentemente appare chiaro che, per costruire rappresentazioni di campi finiti, serve saper costruire polinomi irriducibili (e meglio primitivi) di un generico grado n almeno su campi modulari. Abbiamo anche visto che il teorema di Ruffini ci offre la seguente condizione necessaria ma, in generale, non sufficiente per verificare l'irriducibilità di un polinomio $f(x)$ su un campo finito K:
se $f(x)$ è irriducibile su K allora per ogni $k \in K$ si ha $f(k) \neq 0$.
In generale tuttavia la ricerca di polinomi irriducibili, di polinomi minimi e di polinomi primitivi non è un compito banale.
Supponiamo per esempio di cercare una rappresentazione di F_{64}. Essendo $64 = 2^6$ il campo di ordine 64 esiste ed è un'estensione di F_2 con polinomio generatore di grado 6. Dobbiamo quindi cercare un polinomio irriducibile di grado 6 su F_2.
Tale polinomio deve avere come termine noto 1 e contenere un numero dispari di termini. Possibili candidati sono i polinomi $f_i(x) = x^6 + x^i + 1$ with $1 \leq i \leq 5$. Per $i = 2$ si ha subito $f_2(x) = (x^3 + x + 1)^2$ Con conti standard si verifica che i polinomi $f_1(x) = x^6 + x + 1$ e $f_3(x) = x^6 + x^3 + 1$ sono irriducibili su F_2. ($f_4(x)$ e $f_5(x)$ sono irriducibili o no su F_2?) Proviamo ora che $f_1(x)$ è primitivo su F_2. A tal scopo dobbiamo calcolare le potenze di x in F_{64} usando come polinomio generatore $f_1(x)$ e provare che x, radice di $f_1(x)$, ha periodo 63 (che è l'ordine di F_{64}^*). Poiché $x \in F_{64}^*$ non serve calcolare tutte le potenze di x, perché sappiamo dalla teoria dei gruppi che il periodo di x deve essere un divisore di 63, quindi basta calcolare x^7, x^9, x^{21} (è inutile calcolare x^3 perché è sicuramente diversa da 1 in quanto tutti i polinomi di grado minore di 6 sono elementi distinti di F_{64}). Dalla identità $x^6 = x + 1$ $(mod\ f_1(x))$, abbiamo $x^7 = x(x+1) = x^2 + x$, $x^9 = x^3(x+1) = x^4 + x^3$, $x^{21} = x^3(x^9)^2 = x^3(x^4 + x^3)^2 = x^3(x^8 + x^6) = x^3(x^3 + x^2 + x + 1) = x^6 + x^5 + x^4 + x^3 = x + 1 + x^5 + x^4 + x^3$, quindi essendo tutte queste potenze diverse da 1 abbiamo che 63 è il periodo di x e che dunque x è il generatore di F_{64}^*. Gli elementi di F_{64} dunque sono $\{0\} \cup \{x^j \mid 1 \leq j \leq 63\}$ che si moltiplicano agevolmente. Per fare la somma di potenze ed avere il risultato in forma di potenza (o anche in forma polinomiale come polinomio di grado inferiore a 6) invece è utile avere a disposizione la tabella di conversione di ogni potenza in forma polinomiale modulo $f_1(x)$, (ovvero esprimere ogni potenza come il polinomio di grado minore di 6, resto della divisione della potenza per $f_1(x)$).
Invece $f_3(x)$ non è primitivo. Infatti se facciamo i conti modulo $f_3(x)$, ovvero teniamo conto dell'identità $x^6 = x^3 + 1$, ricaviamo $x^9 = x^6 + x^3 = x^3 + 1 + x^3 = 1$ e quindi x, radice di $f_3(x)$, ha periodo 9 e qundi non genera F_{64}^*. Anche le altre radici di $f_3(x)$ in F_{64}^* hanno lo stesso periodo e dunque $f_3(x)$ non ha radici primitive.

Osserviamo che per decidere se un polinomio è primitivo, possiamo procedere anche in altro modo, utilizzando il seguente risultato:
Sia $f(x) \in F_q[x]$ un polinomio irriducibile su F_q di grado m, allora il periodo di ogni radice di $f(x)$ in F_{q^m} è il minimo intero positivo r tale che $f(x)$ divida $x^r - 1$.
Quindi per decidere che $f_1(x)$ è primitivo, basta dividere $x^7 - 1$, $x^9 - 1$, $x^{21} - 1$ per $f_1(x)$ e verificare che tutte le divisioni danno resto non nullo. (Abbiamo selezionato gli esponenti 7, 9, 21 perché, come già osservato i periodi di un elemento in F_{64}^* può essere solo un divisore di 63 e ovviamente $f_1(x)$ non divide $x^3 - 1$).

Ci chiediamo ora come trovare polinomi irriducibili su un campo F_q. I polinomi minimi di elementi

di una estensione F_{q^n} di F_q, sono ovviamente irriducibili su F_p, quindi supposto di conoscere un polinomio $f(x)$ irriducibile di grado n su F_q (cioè un polinomio generatore di F_{q^n}), descriviamo di seguito un metodo per costruire il polinomio minimo di un elemento di F_{q^n}.
Lavoriamo su un esempio, da cui si può facilmente inferire il metodo generale. Consideriamo al solito F_{64} e prendiamo come polinomio generatore $f_3(x)$. Sia α una radice di $f_3(x)$ (non la chiamiamo x che , come è noto, è una radice di $f_3(x)$, per evitare ambiguità fra variabile ed elemento di F_{64}), si ha allora $\alpha^6 = \alpha^3+1$. Cerchiamo il polinomio minimo $g(x)$ di $\beta = \alpha^3+\alpha$. Tale polinomio ha sicuramente grado minore di 7 e quindi ha la forma $g(x) = c_6x^6+c_5x^5+c_4x^4+c_3x^3+c_2x^2+c_1x+c_0$ (nonostante il polinomio minimo sia per definizione monico, qui abbiamo messo c_6 come coefficiente di x^6 perché così ammettiamo che il grado del polinomio minimo di β possa essere minore di 6). Imponiamo ora che β sia radice di $g(x)$. Calcoliamo le potenze di β modulo $f_3(x)$, in altre parole tenendo conto dell'identità $\alpha^6 = \alpha^3 + 1$.:
$\beta^2 = \alpha^6 + \alpha^2 = \alpha^3 + \alpha^2 + 1$,
$\beta^3 = \beta^3 = \alpha^9 + \alpha^7 + \alpha^5 + \alpha^3 = \alpha^6 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^3 = \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$,
$\beta^4 = (\beta^2)^2 = \alpha^6 + \alpha^4 + 1 = \alpha^4 + \alpha^3$,
$\beta^5 = \beta(\beta^4) = \alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 = \alpha^4 + \alpha + \alpha^3 + 1 + \alpha^5 + \alpha^4 = \alpha^5 + \alpha^3 + \alpha + 1$
$\beta^6 = (\beta^3)^2 = \alpha^{10} + \alpha^8 + \alpha^6 + \alpha^2 + 1 = \alpha^7 + \alpha^4 + \alpha^5 + \alpha^2 + \alpha^3 + 1 + \alpha^2 + 1 = \alpha^4 + \alpha + \alpha^4 + \alpha^5 + \alpha^3 = \alpha^5 + \alpha^3 + \alpha$
e quindi calcoliamo $g(\beta)$
$\alpha^5(c_6 + c_5 + c_3) + \alpha^4(c_4 + c_3 + c_2) + \alpha^3(c_6 + c_5 + c_4 + c_3 + c_2 + c_1) + \alpha^2(c_2) + \alpha(c_6 + c_5 + c_3 + c_1) + (c_5 + c_3 + c_2 + c_0)$
ed imponiamo che sia 0. Poiché $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$ sono una base di F_{64} dobbiamo trovare le soluzioni del sistema lineare omogeneo di 6 equazioni in 7 incognite
$c_6 + c_5 + c_3 = 0$
$c_4 + c_3 + c_2 = 0$
$c_6 + c_5 + c_4 + c_3 + c_2 + c_1 = 0$
$c_2 = 0$
$c_6 + c_5 + c_3 + c_1 = 0$
$c_5 + c_3 + c_2 + c_0 = 0$
che naturalmente va risolto in F_2, la matrice dei coefficienti del sistema ha rango 6 (verificare!) e la soluzione del sistema è $c_6 = c_5 = c_0 = 1,\ c_4 = c_3 = c_2 = c_1 = 0$ quindi il polinomio minimo di β è $x^6 + x^5 + 1$ e tale polinomio è ovviamente irriducibile.

Ricordate che quando si risolve un sistema lineare omogeneo a coefficienti reali in cui la matrice dei coefficienti ha rango r ed il numero delle incognite è $n > r$ si dice che il sistema ha ∞^{n-r} soluzioni, questo significa che noi possiamo trovare le soluzioni del sistema assegnando ad $n - r$ variabili un valore arbitrario, e poi calcoliamo i valori assunti dalle restanti variabili in funzione di quei valori arbitrari. Qui stiamo lavorando in F_2 e quindi i possibili valori arbitrari che possono essere assegnati ad una variabile sono solo 0 e 1, quindi un sistema lineare in cui la matrice dei coefficienti ha rango r ed il numero delle incognite è $n > r$ ha 2^{n-r} soluzioni, nel nostro caso quindi, essendo $n - r = 1$, il sistema ha 2 soluzioni, la soluzione banale e quella data. Ovviamente se vogliamo risolvere un sitema lineare omogeneo con n incognite e rango della matrice dei coefficienti $r < n$ su un campo F_q il numero di soluzioni sarà q^{n-r}.

Il polinomio irriducibile di β si può anche trovare calcolando gli elementi coniugati a β rispetto ad F_2, cioè le potenze β, β^2, β^{2^2}.... fino a trovare il minimo d per cui $\beta^{2^d} = \beta$. Il d così trovato è il grado del polinomio minimo di β che si trova come: $g(x) = (x - \beta)(x - \beta^2)...(x - \beta^{2^{d-1}})$, infatti le radici del polinomio minimo di β sono gli elementi coniugati di β ovvero le potenze β, $\beta^2, ...\beta^{2^{d-1}}$ con $\beta^{2^d} = \beta$.

Entrambi i procedimenti sono ovviamente generalizzabili ad un campo finito qualsiasi.

I metodi precedenti permettono di costruire un polinomio irriducibile di grado minore o uguale ad n su un campo F_q supponenedo di conoscere almeno un polinomio generatore di F_{q^n}, ma come si procede se si vuole trovare direttamente un polinomio generatore di F_{q^n}?
Ricordiamo che F_{q^n} è il (q^n-1)-campo ciclotomico su uno dei suoi sottocampi e che, come abbiamo già osservato, un polinomio generatore di F_{q^n} è un qualsiasi fattore irriducibile su F_q del (q^n-1)-polinomio ciclotomico.
Consideriamo ad esempio il campo F_{64} e supponiamo di voler trovare un suo polinomio generatore. Il 63-esimo polinomio ciclotomico è un polinomio di grado $\varphi(63)=\varphi(9)\varphi(7)=9(1-\frac{1}{3})6=36$ che divide $\frac{x^{63}-1}{x^9-1}=x^{54}+x^{45}+x^{36}+x^{27}+x^{18}+x^9+1$ e $\frac{x^{63}-1}{x^{21}-1}=x^{42}+x^{21}+1$ e quindi divide il loro M.C.D.; essendo
$x^{54}+x^{45}+x^{36}+x^{27}+x^{18}+x^9+1=(x^{12}+x^3)(x^{42}+x^{21}+1)+(x^{36}+x^{33}+x^{27}+x^{24}+x^{18}+x^{12}+x^9+1$
si può decidere subito che il massimo comun divisore è $x^{36}+x^{33}+x^{27}+x^{24}+x^{18}+x^{12}+x^9+1$, sappiamo che tale polinomio si spezza in 6 polinomi irriducibili di grado 6 e quindi serve un algoritmo per fattorizzare i polinomi.

4.7 Fattorizzazione di polinomi su campi finiti

Il problema di fattorizzare un polinomio di $K[x]$ nel prodotto di fattori irriducibili su K, si può ridurre a quello di fattorizzare un polinomio $f(x)\in K[x]$ che

- sia monico,
- non abbia fattori multipli.

Infatti se $f(x)$ avesse come coefficiente direttivo $a\neq 1$, potremmo considerare al suo posto il polinomio $a^{-1}f(x)$ che è monico, fattorizzarlo e poi moltiplicare per a la fattorizzazione trovata. Se invece $f(x)$ avesse un fattore $h(x)$ con molteplicità $r>1$, $h(x)$ sarebbe un fattore della derivata $f'(x)$ di $f(x)$ con molteplicità $r-1$. Posto $d(x)=M.C.D.(f(x),f'(x)))$ si può considerare $f(x)=\frac{f(x)}{d(x)}d(x)$ dove $\frac{f(x)}{d(x)}$ è privo di fattori multipli e $d(x)$ ha grado minore del grado di $f(x)$. Se $d(x)$ non ha fattori multipli per fattorizzare $f(x)$ ci siamo ridotti a fattorizzare due polinomi privi di fattori multipli, altrimenti si ripete il procedimento precedente su $d(x)$ e si continua fino a quando (dopo un numero di passi minore del grado di $f(x)$) si spezza $f(x)$ in prodotto di fattori privi di fattori multipli che poi spezzeremo in fattori irriducibili.
La fattorizzazione di un polinomio sfrutta la seguente

Prop 4.41 *Se $f(x)\in F_q[x]$ è monico e privo di fattori multipli e se $h(x)\in F_q[x]$ soddisfa la condizione $h(x)^q\equiv h(x)$ $(mod\ f(z))$ (ovvero se $f(x)$ divide $h(x)^q-h(x)$), allora $f(x)=\prod_{c\in F_q} M.C.D.(f(x),h(x)-c)$.*

Dim. Ovviamente $\prod_{c\in F_q} M.C.D.(f(x),h(x)-c)$ divide $f(x)$. Del resto per ipotesi $f(x)$ divide $h(x)^q-h(x)=\prod_{c\in F_q}(f(x)-c)$ (ricordate che F_q è il campo di spezzamento del polinomio y^q-y) e dunque $f(x)$ divide $\prod_{c\in F_q} M.C.D.(f(x),h(x)-c)$, da cui segue l'uguaglianza $f(x)=\prod_{c\in F_q} M.C.D.(f(x),h(x)-c)$.

Il problema di fattorizzare $f(x)$ è così ridotto a quello di trovare i polinomi $h(x)$ tali che $h(x)^q\equiv h(x)$ $(mod\ f(z))$ con il vincolo $0<gr(h(x))<gr(f(x))=n$ (che assicura di ottenere polinomi

che danno luogo a fattorizzazioni non banali). Sia $h(x) = a_{n-1}x^{n-1} + ... + a_1x + a_0$, si ha allora $h(x)^q = (a_{n-1}x^{n-1} + ... + a_1x + a_0)^q = a_{n-1}^q x^{q(n-1)} + ... + a_1^q x^q + a_0^q = a_{n-1}x^{q(n-1)} + ... + a_1x^q + a_0$. A questo punto si esprimono le potenze x^{qi} modulo $f(x)$ calcolando così $h(x)^q \ (mod\ f(x))$ che deve coincidere con $h(x)$. Si trova in questo modo un sistema lineare omogeneo S di n equazioni che ha come n incognite i coefficienti $a_i,\ 0 \leq i \leq n-1$. Le soluzioni di S danno i coefficienti degli $h(x)$ che stiamo cercando, a partire dai quali in virtù della Prop. 4.41 possiamo ottenere una fattorizzazione di $f(x)$. Non sappiamo però se è una fattorizzazione in fattori irriducibili. A questo punto ci può aiutare un'analisi più dettagliata dei polinomi $h(x)$.
Se $f(x) = f_1(x)f_2(x)....f_k(x)$ è la fattorizzazione di $f(x)$ in fattori monici irriducibili su F_q e non ripetuti, allora presa comunque una k-upla $(c_1, c_2, ..., c_k)$ di elementi di F_q per il teorema cinese dei resti (che potete trovare su un qualunque testo di algebra) esiste un unico polinomio $a(x)$ tale che $a(x) = c_i \ (mod\ f_i(x)),\ 1 \leq i \leq k$ e $gr(a(x)) < gr(f(x))$, tale polinomio soddisfa la condizione $a(x)^q = c_i^q = c_i = a(x) \ (mod\ f(x))$. Viceversa se $b(x)$ è un polinomio tale che $b(x)^q = b(x) \ (mod\ f(x))$ e $gr(b(x)) < gr(f(x))$ allora dal fatto che $b(x)^q - b(x) = \prod_{c \in F_q}(b(x) - c)$ segue che ogni fattore irriducibile di $f(x)$ deve dividere uno dei polinomi $b(x) - c$ e quindi ogni $b(x)$ soddisfa le condizioni $b(x) = c_i \ (mod\ f_i(x)),\ 1 \leq i \leq k$ per qualche k-upla $(c_1, c_2, ..., c_k)$ di elementi di F_q. Dunque il numero di possibili polinomi $h(x)$ ovvero il numero di possibili soluzioni del sistema S è q^k, il che vuol dire che il rango delle matrice dei coefficienti di S deve essere $r = n - k$, dunque noto il rango r della matrice dei coefficienti di S si ottiene subito il numero $k = n - r$ di fattori irriducibili (distinti) di $f(x)$.

Ad esempio supponiamo di voler fattorizzare $f(x) = x^8 + x^6 + x^4 + x^3 + 1$ su F_2. Il polinomio $f(x)$ è monico, non ha fattori multipli in quanto $M.C.D.(f(x), f'(x)) = 1$. Dobbiamo calcolare $x^{2i},\ 0 \leq i \leq 7$ modulo $f(x)$. Si ha:
$x^0 = 1,\ x^2 = x^2,\ x^4 = x^4,\ x^6 = x^6$
$x^8 = x^6 + x^4 + x^3 + 1,$
$x^{10} = x^8 + x^6 + x^5 + x^2 = x^5 + x^4 + x^3 + x^2 + 1,$
$x^{12} = x^7 + x^6 + x^5 + x^4 + x^2,$
$x^{14} = x^9 + x^8 + x^7 + x^6 + x^4 = x^5 + x^4 + x^3 + x + 1,$
da qui ponendo $h(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ si ottiene: $h(x)^q = a_6x^7 + (a_6 + a_4 + a_3)x^6 + (a_7 + a_6 + a_5)x^5 + (a_7 + a_6 + a_5 + a_4 + a_2)x^4 + (a_7 + a_5 + a_4)x^3 + (a_6 + a_5 + a_1)x^2 + a_7x + (a_7 + a_5 + a_4 + a_0) \ (mod\ f(x))$ e pertanto si deve risolvere in F_2 il sistema:
$a_6 = a_7$
$a_6 + a_4 + a_3 = a_6$
$a_7 + a_6 + a_5 = a_5$
$a_7 + a_6 + a_5 + a_4 + a_2 = a_4$
$a_7 + a_5 + a_4 = a_3$
$a_6 + a_5 + a_1 = a_2$
$a_7 = a_1$
$a_7 + a_5 + a_4 + a_0 = a_0$
Le autosoluzioni di questo sistema sono:
$a_0 = 1,\ a_1 = a_2 = a_3 = a_4 = a_5 = a_6 = a_7 = 0,\ a_0 = a_3 = a_4 = 0,\ a_1 = a_2 = a_5 = a_6 = a_7 = 1.$
La prima soluzione corrisponde ad un polinomio di grado 0 e quindi non è interessante dal punto di vista di una fattorizzazione significativa. La seconda soluzione dà il polinomio $x^7 + x^6 + x^5 + x^2 + x$. A questo punto si calcolano $M.C.D.(x^8 + x^6 + x^4 + x^3 + 1, x^7 + x^6 + x^5 + x^2 + x) = x^6 + x^5 + x^4 + x + 1$ e $M.C.D.(x^8 + x^6 + x^4 + x^3 + 1, x^7 + x^6 + x^5 + x^2 + x - 1) = x^2 + x + 1$ e si ha una fattorizzazione $f(x) = (x^6 + x^5 + x^4 + x + 1)(x^2 + x + 1)$. Poiché il sistema ammette 2 soluzioni, la matrice dei coefficienti ha rango 6 e quindi 2 è il numero di fattori irriducibili di $f(x)$ e la decomposizione precedente è quindi una decomposizione in fattori irriducibili.

Osserviamo che per campi "grandi" l'algoritmo (di Berlekamp) sopra esposto è inefficiente infatti si deve calcolare un numero di *M.C.D.* uguale all'ordine del campo. Esistono tuttavia dei raffinamenti dell'algoritmo che lo rendono utilizzabile anche per campi grandi, questi raffinamenti sono basati sulla caratterizzazione degli elementi c del campo per cui $h(x) - c$ risulta primo con $f(x)$ che ci permette quindi di evitare il calcolo dei relativi *M.C.D.*. Tale caratterizzazione si può trovare in [1].

4.8 Logaritmo discreto

Siano G un gruppo ciclico finito (ad esempio il gruppo moltiplicativo di un campo finito F_q) , b un elemento generatore di G fissato (che nel caso G sia il gruppo moltiplicativo di F_q è un elemento primitivo di F_q), ed a un qualsiasi elemento di G . Si chiama *logaritmo discreto* di a (in base b) il minimo intero non negativo d tale che $a^d = b$. Ovviamente $d \leq |G| - 1$.
In generale il problema di calcolare il logaritmo discreto è più difficile computazionalmente di quello di calcolare la potenza (si è a lungo ritenuto che il costo computazionale del calcolo del logaritmo discreto in G fosse dell'ordine di $|G|^{1/2}$, mentre come già abbiamo visto il calcolo della potenza è dell'ordine di $lg\ |G|$) e questo ha reso l'elevamento a potenza su gruppi finiti uno strumento molto usato in crittografia.
Va osservato però che se $|G| - 1$ ha fattori primi piccoli il logaritmo discreto può essere calcolato in modo efficiente.
Infatti sia $|G| - 1 = \prod_{1 \leq i \leq k} p_i^{e_i}$ la fattorizzazione di $|G| - 1$ in fattori primi. Se vogliamo trovare il logaritmo discreto r di un elemento a in base b, possiamo determinare il valore di r modulo $p_i^{e_i}$ e poi usare il teorema cinese dei resti per calcolare r modulo $|G| - 1$. Sia $r = \sum_{j=0,e^i-1} s_j p_i^j \ (mod\ p_i^{e_i})$, allora $a^{(|G|-1)/p_i} = (b^{(|G|-1)/p_i})^r = (b^{(|G|-1)/p_i})^{s_0}$ dove s_0 può assumere solo p_i valori. Per calcolare s_1 ora si può considerare $d = ab^{-s_0} = b^{r_1}$ ove $r_1 = \sum_{j=1,e^i-1} s_j p_i^j \ (mod\ p_i^{e_i})$ e quindi $d^{(|G|-1)/p_i^2} = (b^{(|G|-1)/p_i^2})_1^r = (b^{(|G|-1)/p_i})^{s_1/p_i} = (b^{(|G|-1)/p_i})^{s_1}$ e così si continua fino a calcolare tutti gli s_j. (La complessità dell'algoritmo di calcolo di r seguendo questa procedura è $p_k^{1/2}(lg\ |G|)^2$ dove p_k è il massimo fattore primo di $|G| - 1$.)
Per rendere quindi sicuri gli algoritmi che usano la potenza come funzione one way bisogna considerare gruppi G tali che $|G| - 1$ abbia fattori primi grandi (sono molto usato i gruppi moltiplicativi di campi F_{2^n} con $2^n - 1$ primo).

4.9 Cenni alle curve ellittiche

Una curva ellittica su $\mathbb{R}$ (campo reale) è l'insieme dei punti (x, y) che soddisfano un'equazione della forma:
$y^2 = x^3 + ax + b$ con $a, b \in \mathbb{R}$.
Se $x^3 + ax + b$ non ha fattori ripetuti allora la curva ellittica di equazione $y^2 = x^3 + ax + b$ può essere utilizzata per costruire un gruppo abeliano.
Il gruppo ha come supporto l'insieme dei punti della curva a cui viene aggiunto uno speciale simbolo O detto punto all'infinito. Per ogni coppia di elementi P e Q (non entrambi uguali ad O) del supporto definiamo come retta PQ: la retta che congiunge P con Q se P, Q sono punti distinti della curva, la tangente alla curva in P se $P = Q$ è un punto della curva, la parallela all'asse y per P se P è un punto della curva e $Q = O$. Se la retta PQ ha con la curva un'ulteriore intersezione R' (che può anche coincidere con P o Q) si pone $P + Q = R$ dove R è il simmetrico di R' rispetto all'asse x; se la retta PQ non ha ulteriori intersezioni (cioè se PQ è parallela all'asse y) si pone $P + Q = O$ ed infine si pone per definizione $O + O = O$.
La somma gode dunque della proprietà commutativa.

Se $P = (x_P, y_P)$ e $Q = (x_Q, y_Q)$ sono due punti della curva non simmetrici rispetto all'asse x allora, chiamato m il coefficiente angolare della retta PQ, si ha $x_R = m^2 - x_P - x_Q$ e $y_R = -y_P + m(x_P - x_R)$. Ovviamente se $P \neq Q$ si ha $m = (y_P - y_Q)(x_P - x_Q)^{-1}$ se invece $P = Q$ e $y_P \neq 0$ si ha $m = (3x_P^2 + a)(2y_P)^{-1}$, coefficiente angolare della retta tangente in P alla curva. Per ragioni di simmetria se P e Q sono due punti della curva simmetrici rispetto all'asse x (incluso il caso $P = Q$ con $x_P = 0$), la retta PQ non ha ulteriori intersezioni con la curva e dunque si pone $P + Q = O$.
Una volta verificata l'associatività della somma (che richiede conti noiosi ma standard) si ha subito che O funziona da elemento neutro e che ogni P ammette un opposto (il suo simmetrico rispetto all'asse x).
Possiamo ripetere gli argomenti precedenti prendendo i coefficienti della curva su un campo finito F_q di caratteristica diversa da 2 e 3 ed otterremo un numero finito di coppie (che chiameremo punti) che soddisfano l'equazione della curva (naturalmente modulo q). Per ogni valore di x che possa essere visto come ascissa di un punto della curva ci saranno sempre due punti della curva che hanno ascissa x e le loro ordinate sono una opposta dell'altra modulo q, considerando tali punti come "simmetrici rispetto all'asse x", possiamo semplicemente estendere la definizione di somma sul supporto formato da punti di una curva ellittica su F_q e punto all'infinito O anche in questi casi.
Vanno trattati a parte i casi di campi di caratteristica 3 e 2. Trascuriamo il caso di campi di caratteristica 3 che non ha interesse paricolare dal punto di vista crittografico e consideriamo invece campi F_{2^m}.
Su un campo F_{2^m}, una curva ellittica è l'insieme delle coppie (punti) (x, y) con $x, y \in F_{2^m}$ che soddisfano un'equazione della forma $y^2 + xy \equiv x^3 + ax^2 + b \ (mod\ 2^m)$ con $a, b \in F_{2^m}$. Anche in questo caso possiamo definire un gruppo prendendo come supporto l'insieme dei punti della curva (che sono in numero finito) più un punto speciale O chiamato punto all'infinito. Chiamiamo simmetrico del punto $P = (x_P, y_P)$ il punto di coordinate $(x_P, x_P + y_P)$. Se P, Q sono punti distinti e non simmetrici allora le coordinate di $R = P+Q$ sono $x_R = m^2+m+x_P+x_Q+a,\ y_R = m(x_P+x_R)+x_R+y_P$ ove $m = (y_P - y_Q)(x_P + x_Q)^{-1}$, se invece $P = Q$ è un punto della curva e $x_P \neq 0$, le coordinate di $R = P + P = 2P$ sono $x_R = m^2 + m + a,\ y_R = x_P^2 + (m+1)x_R$ dove $m = (x_P + y_P)x_P^{-1}$. Come in tutti gli altri casi poniamo $P + Q = O$ se Q è il simmetrico di P o se $P = Q$ con $x_P = 0$ e $P + O = P$ per ogni elemento P del supporto. Il supporto equipaggiato con questa somma risulta un gruppo.

Poiché lavoriamo in notazione additiva, nei gruppi definiti sulle curve ellittiche la potenza di ordine k di un elemento P è al solito denotata con kP, se prendiamo in considerazione il sottogruppo ciclico H generato da P, possiamo definire il logaritmo discreto di $Q \in H$ in base P come il minimo intero non negativo tale che $kP = Q$. Algoritmi basati su elevamento a potenza e calcolo di logaritmo discreto in (sottogruppi ciclici di) gruppi costruiti su curve ellittiche sono utilizzati in crittografia.

References

[1] R.Lidl,H.Niederreiter, Introduction to finite fields and their applications, Cambridge University Press

[2] Dispense del corso di Algebra e logica 1 , www.mate.polimi.it.