UNIVERSITÀ DEGLI STUDI DI MESSINA

Campi Finiti
con applicazioni alla crittografia

Luca Amata

Anno Accademico 2020 - 2021

Indice

Capitolo 1

Campi Finiti

In questo capitolo si dà una generale classificazione dei Campi Finiti sui quali vengono dimostrate alcune proposizioni caratterizzanti facendo uso dei richiami algebrici precedenti. Sono presenti alcuni esempi esplicativi. Infine sono presenti alcune applicazioni di tipo algebrico-informatico.

La trattazione di questo capitolo comprende nozioni basilari di algebra presenti in [1], in [2], in [3], in [4].

1.1 Struttura dei campi finiti

Per poter caratterizzare i campi finiti è essenziale un risultato relativo al *sottocampo fondamentale*. Nel seguito della trattazione si considereranno sempre campi con $1 \neq 0$, cioè non banali. Inoltre dato un naturale $n \geq 2$ verrà indicato con il simbolo $\mathbb{Z}_n$ il gruppo quoziente delle classi resto modulo n, $\mathbb{Z}/n\mathbb{Z}$; quindi $\mathbb{Z}_p$ con p primo indica il campo finito di ordine p, infatti nel nostro caso non può sorgere ambiguità con l'anello degli interi $p-$adici $\mathbb{Z}_p$. Si ricordano alcune definizioni.

Definizione 1.1.1. Dato un anello $A \neq 0$, si consideri l'insieme

$$C = \{m \in \mathbb{N} \ : \ m > 0 \ \wedge \ ma = \underbrace{a + \cdots + a}_{m \text{ volte}} = 0, \ \forall a \in A\}.$$

Se $C \neq \emptyset$ sia $n = \min C$ (esiste per il Principio del Buon Ordinamento), allora n si dirà *caratteristica* dell'anello A, $n = char(A)$. Se $C = \emptyset$ si dirà che $char(A) = 0$.

Nel caso di anelli unitari valgono delle condizioni che semplificano il calcolo della caratteristica.

Proposizione 1.1.2. *Sia A un anello con unità 1_A e di caratteristica n.*

i) n è il più piccolo intero positivo tale che $n1_A = 0$ oppure è 0.

ii) La mappa $\varphi : \mathbb{Z} \to A$ tale che $m \mapsto m1_F$ è un omomorfismo di anelli il cui nucleo è $\ker\varphi = \{kn \ : \ k \in \mathbb{Z}\} = (n)$.

iii) Se A non possiede zero-divisori (e in particolare se è un dominio) allora n è zero oppure è un numero primo.

Dimostrazione.

i) Se per assurdo esistesse $0 < k < n$ tale che $k1_A = 0$, allora $\forall a \in A$ si avrebbe $ka = k(1_A a) = (k1_A)a = 0a = 0$ contraddicendo la minimalità di n per tale proprietà.

ii) Verificare che la mappa φ è un omomorfismo di anelli è immediato (proprietà associativa). Il suo nucleo è $\ker\varphi = \{m \in \mathbb{Z} \ : \ 0 = \varphi(m) = m * 1_F\} = \{m \in \mathbb{Z} \ : \ n|m\} = (n)$, poiché n è la caratteristica (minimo). Se $n = 0$, cioè 1 è aperiodico, si osserva subito che $\ker\varphi = \{0\} = (0)$.

iii) Se per assurdo n non fosse primo allora potremmo scrivere $n = kr$ con $1 < k, r < n$. Quindi si avrebbe $0 = n1_A = (kr)1_A = (k1_A)(r1_A)$ e non esistendo in A zero-divisori per ipotesi allora $k1_A = 0$ oppure $r1_A = 0$, ma in ogni caso si contraddirebbe il punto *ii*); quindi n deve essere primo.

□

Definizione 1.1.3. Sia F un campo e sia P l'intersezione di tutti i sottocampi di F. P è detto *sottocampo fondamentale o minimo*.

Si può subito osservare che, per come è stato costruito, il sottocampo fondamentale non contiene sottocampi non banali.

Proposizione 1.1.4. *Siano F un campo e P il suo sottocampo fondamentale. Se $char(F) = p$, primo, allora $P \cong \mathbb{Z}_p$. Se $char(F) = 0$ allora $P \cong \mathbb{Q}$.*

Dimostrazione. Si osserva innanzitutto che 0_F e 1_F appartengono a tutti i sottocampi di F, quindi apparterranno anche a P. Ovviamente per le proprietà di campo, anche gli elementi del tipo $m1_F$, $m \in \mathbb{Z}$, apparterranno a P. Bisogna quindi provare che se $char(F) = p$ allora $P = \{m1_F \ : \ m \in \mathbb{Z}\}$ e se $char(F) = 0$ allora $P = \{(m1_F)(n*1_F)^{-1} \mid m, n \in \mathbb{Z},\ n \neq 0\}$. Dalla proposizione precedente sappiamo che l'omomorfismo $\varphi : \ \mathbb{Z} \to P$ tale che $m \mapsto m1_F$ ha nucleo $\ker\varphi = (n)$, $n = char(P)$. Se $n = p$ allora dal primo teorema di omomorfismo per anelli segue quindi che $\mathbb{Z}/\ker\varphi \cong Im(\varphi) \subset P$ cioè $\mathbb{Z}_p \overset{\sim}{\subset} P$. Ma poiché P non ha sottocampi propri allora deve essere $\mathbb{Z}_p \cong P$. Se $n = 0$ allora φ è iniettivo (il nucleo è proprio (0)) e si può considerare il morfismo $\overline{\varphi} : \ \mathbb{Q} \to P$ definito da $\overline{\varphi}(mn^{-1}) = (m1_F)(n1_F)^{-1}$. Si prova facilmente che anch'esso è iniettivo. Quindi vale l'immersione $\mathbb{Q} \overset{\sim}{\subset} P$ e per la minimalità di P si ha che $\mathbb{Q} \cong P$. □

Segue un risultato che dà informazioni sulla struttura dei campi finiti.

Corollario 1.1.5. *Ogni campo finito F ha caratteristica $char(F) = p$, con p primo, e cardinalità $|F| = p^n = q$, con $n \geq 1$ intero.*

Dimostrazione. Poiché F è finito si può considerare $\mathbb{Z}_p$ come suo sottocampo fondamentale, dove p è proprio la caratteristica F. Quindi F può essere visto come una sua *estensione*, cioè come spazio vettoriale di dimensione finita n su $\mathbb{Z}_p$. Quindi $F_{\mathbb{Z}_p} \cong \left(\underbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{n \text{ volte}}\right)_{\mathbb{Z}_p}$ e di conseguenza $|F| = p^n$. □

Sia quindi F un campo finito con $|F| = q = p^n$, p primo e $n \geq 1$. Allora ogni elemento $a \in F$ è tale che $a^{q-1} = 1$ poiché $q-1$ è la cardinalità del gruppo moltiplicativo del campo. Quindi $a^{q-1} - 1 = 0$ e includendo anche l'elemento nullo si può scrivere $a(a^{q-1} - 1) = 0$ da cui si ottiene che $a^q - a = 0$, per ogni

$a \in F$. Quindi sicuramente ogni elemento è radice del polinomio $x^q - x$ di $F[x]$. In tale campo allora si può scrivere che $x^q - x = \prod_{a \in F} (x - a)$. È possibile fare alcune considerazioni per invertire tale risultato.

1.1.6 Molteplicità delle radici di un polinomio

Sia K un campo. Un polinomio $f(x) \in K[x]$ di grado n nel suo campo di spezzamento L si scrive come

$$f(x) = \alpha(x - a_1)(x - a_2) \cdots (x - a_n) = \alpha(x - a_{i_1})^{t_1}(x - a_{i_2})^{t_2} \ldots (x - a_{i_r})^{t_r}$$

scritto raccogliendo per molteplicità.

Definizione 1.1.7. Una radice a_j di $f(x)$ si dice *semplice* se $t_j = 1$, *multipla* se $t_j > 1$; t_j è detta *molteplicità* della radice.

Definizione 1.1.8. È possibile definire la *derivata formale* di un polinomio. Se $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$, la sua derivata è $f'(x) = n a_n x^{n-1} + \cdots + a_2 x + a_1$. Valgono le proprietà della somma e del prodotto:

$$(f(x) + g(x))' = f'(x) + g'(x) \text{ e } (f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x).$$

Teorema 1.1.9. *Un polinomio $f(x) \in K[x]$, K campo, ha una radice multipla nel suo campo di spezzamento se e solo se $f(x)$ e $f'(x)$ hanno un divisore comune di grado maggiore di 0 in $K[x]$, cioè $(f(x), f'(x)) \neq 1$.*

Dimostrazione.
$\Rightarrow$) Se $f(x)$ ha una radice multipla in L campo di spezzamento, sia essa a, allora in $L[x]$ si può scrivere $f(x) = (x - a)^2 h(x)$. La sua derivata è quindi della forma

$$f'(x) = 2(x - a)h(x) + (x - a)^2 h'(x) = (x - a)\left(2h(x) + (x - a)h'(x)\right).$$

Si osservi che $(x - a)$ è un divisore comune fra il polinomio e la sua derivata in $L[x]$, per trovarne uno in $K[x]$ basta considerare il polinomio minimo di a, sia esso $p(x) \in K[x]$. Tale polinomio ha la proprietà $p(x) \mid f(x)$ e $p(x) \mid f'(x)$,

poiché è il *più piccolo* polinomio che ammette a come radice. Quindi in $K[x]$ vale che $(f(x), f'(x)) \neq 1$.

$\Leftarrow$) Se $(f(x), f'(x)) \neq 1$ sia allora $q(x) \in K[x]$ un loro divisore e sia a una sua radice. Se L è il campo di spezzamento di $f(x)$, allora in $L[x]$ si può scrivere $f(x) = (x-a)h(x)$. Calcolando la derivata si ottiene $f'(x) = h(x)+(x-a)h'(x)$. Per ipotesi $q(x) \mid f'(x)$ quindi a è una radice anche di $f'(x) = (x-a)g(x)$ in $L[x]$ ed è possibile scrivere

$$h(x) = f'(x) - (x-a)h'(x) = (x-a)g(x) - (x-a)h'(x).$$

Dunque si ottiene che $(x-a) \mid h(x)$. Quindi in $L[x]$ si può scrivere $f(x) = (x-a)^2 (g(x) - h'(x))$ cioè a è una radice multipla di $f(x)$ in L. □

1.1.10 Esistenza e costruzione di campi finiti

Per procedere è necessario richiamare un risultato tecnico: in un dominio con caratteristica p, primo, vale che $(a+b)^p = a^p + b^p$. Infatti per Newton

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

con i coefficienti $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Basta osservare che se $k = 0$ e $k = p$ allora $\binom{p}{k} = 1$, mentre in tutti gli altri casi $p \mid \binom{p}{k}$, poiché $k, p-k < p$ e quest'ultimo è primo; dunque tali coefficienti sono nulli nel dominio. Tale risultato si può estendere, per induzione, a $(a+b)^q = a^q + b^q$ con $q = p^n$. Infatti supponendo vero il risultato per p^{n-1} basta considerare

$$(a+b)^{p^n} = \left((a+b)^{p^{n-1}}\right)^p = \left(a^{p^{n-1}} + b^{p^{n-1}}\right)^p = a^{p^n} + b^{p^n}.$$

Teorema 1.1.11. *(di esistenza) Dati comunque un primo p ed un intero positivo n, esiste un campo con $q = p^n$ elementi, unico a meno di isomorfismi.*

Dimostrazione. Si consideri il polinomio $x^q - x \in \mathbb{Z}_p[x]$ e nel suo campo di spezzamento[1] L si consideri l'insieme $F = \{a \in L \ : \ a^q = a\}$.

[1] che sicuramente esiste per quanto dimostrato in [2], pagg.324-325

Si osservi che il polinomio scelto ha tutte le radici distinte, infatti la sua derivata formale è $qx^{q-1} - 1 = -1$ (poiché q è multiplo della caratteristica) e basta applicare il teorema 1.1.9. Tali radici sono quindi in numero di q e, per come è stato definito, anche in numero di $|F|$ quindi $|F| = q$. Inoltre si prova facilmente che F è un campo, infatti è ovviamente chiuso rispetto al prodotto: presi due elementi $a, b \in F$, $(ab)^q = a^q b^q = ab$; inoltre $(a+b)^q = a^q + b^q = a + b$ (per l'osservazione precedente). Quindi F è proprio il campo cercato. Dal teorema di unicità del campo di spezzamento di un polinomio si evince immediatamente l'unicità di F a meno di isomorfismi. □

Definizione 1.1.12. È possibile indicare ogni campo finito con la scrittura $\mathbb{F}_q$, dove $q = p^n$ con p primo e $n \geq 1$ intero. Con $\mathbb{F}_p$ si intende quindi $\mathbb{Z}_p$.

Il teorema precedente stabilisce un metodo costruttivo per determinare un campo finito, nota la cardinalità p^n. Per un'altra interessante costruzione, utile per diverse rappresentazioni degli elementi, si consideri l'anello dei polinomi $\mathbb{Z}_p[x]$ e un suo polinomio irriducibile $f(x)$ di grado n. Il quoziente $\mathbb{Z}_p[x]/(f(x))$ è un campo con p^n elementi, infatti $(f(x))$ è ideale massimale di un *P.I.D.* (quindi il quoziente non avrà ideali propri per il teorema di corrispondenza) e tutte le distinte classi del quoziente hanno come rappresentanti tutti i polinomi di grado minore di n a coefficienti in $\mathbb{Z}_p$.

Esempio 1.1.13. Per costruire il campo $\mathbb{F}_9$, cioè con $q = 9 = 3^2$, si può quindi procedere in due modi equivalenti:

i) Per il teorema, sappiamo che il campo di spezzamento del polinomio $x^9 - x \in \mathbb{Z}_3[x]$ è il campo cercato. Per ottenerlo si può considerare dapprima la scomposizione del polinomio in fattori irriducibili su $\mathbb{Z}_3$:

$$x^9 - x = x(x+1)(x-1)(x^2+1)(x^2+x-1)(x^2-x-1).$$

Il campo di spezzamento L, essendo un'estensione finita, può essere costruito estendendo il campo base con le radici del polinomio stesso.
Esaminiamo i suoi fattori irriducibili: quelli di primo grado $x, x+1, x-1$

non danno contributi, essendo le loro radici già facenti parte del campo base. Il fattore x^2+1 ammette due radici in L e siano esse α_1, α_2, si ha che $\alpha_i^2 = -1$. Il fattore x^2+x-1 ammette due radici in L e siano esse β_1, β_2, si ha che $\beta_i^2 + \beta_i = 1$. Infine, il fattore x^2-x-1 ammette due radici in L e siano esse γ_1, γ_2, si ha che $\gamma_i^2 - \gamma_i = 1$. Quindi si ottiene la catena di campi $\mathbb{Z}_3 \subseteq \{0,1,2,\alpha_1,\alpha_2,\beta_1,\beta_2,\gamma_1,\gamma_2\} \subseteq L$, con le ultime due estensioni coincidenti per la minimalità del campo di spezzamento. Sappiamo, per il teorema 1.1.11, che tale insieme deve essere chiuso rispetto alle operazioni e questi sono tutti e soli gli elementi che si possono ottenere come risultato di qualsiasi operazione.
Per fare qualche esempio si possono considerare dapprima radici di uno stesso fattore irriducibile, ad esempio è noto che $\alpha_1 + \alpha_2 = 0$ e $\alpha_1\alpha_2 = 1$ (per le proprietà dei polinomi di secondo grado) dunque $\alpha_2 = -\alpha_1 = \alpha_1^{-1}$ (sono mutuamente opposti e reciproci). Per quanto riguarda le radici del fattore x^2+x-1 si ha che $\beta_1+\beta_2 = -1$ e $\beta_1\beta_2 = -1$ dunque $\beta_2 = -1-\beta_1 = -\beta_1^{-1}$. Per il terzo fattore risulta quindi $\gamma_2 = 1-\gamma_1 = -\gamma_1^{-1}$. Avendo trovato opposti e reciproci si può procedere ad altre operazioni: α_1+1 a quale elemento corrisponde? Si ha che α_1+1 è radice del fattore x^2+x-1, infatti $\alpha_1^2 + 2\alpha_1 + 1 + \alpha_1 + 1 - 1 = -1 + 3\alpha_1 + 1 = 0$ quindi, dato che non è dato un ordine per le radici, si può fissare $\alpha_1 + 1 = \beta_1$. Così facendo è possibile trovare le tavole delle operazioni del campo.

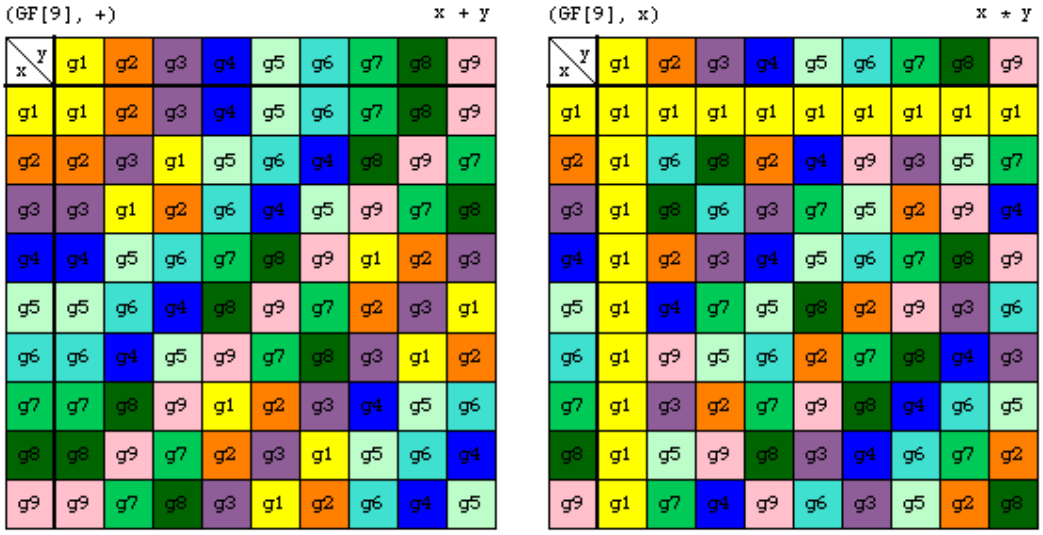
ii) Un altro metodo è quello di considerare il quoziente $\mathbb{Z}_p[x]/(f(x))$, ovviamente per scelte opportune: come campo $\mathbb{Z}_3$ e come polinomio irriducibile, ad esempio, x^2+x-1. Si ottiene quello che sappiamo essere un campo di caratteristica 3 con 3^2 elementi:

$$\begin{aligned}\mathbb{Z}_3[x]/(x^2+x-1) &= \{a+bx \ : \ a,b \in \mathbb{Z}_3, \ x^2 = -x+1\} \\ &= \{0,1,2,x,1+x,2+x,2x,1+2x,2+2x\}.\end{aligned}$$

Osserviamo come si combinano alcuni elementi tramite le operazioni, ad esempio $x^2 = -x+1 = 1+2x$ (per le proprietà di $\mathbb{Z}_3$ tutte le potenze superiori alla prima possono ricondursi al primo grado); l'elemento x^{-1}

si può trovare considerando genericamente $1 = x^{-1}x = (a+bx)x = ax + bx^2 = ax - bx + b = (a-b)x + b$ da cui deve essere $a - b = 0$ e $b = 1$, cioè $a = b$ e $b = 1$ giungendo al risultato $x^{-1} = 1 + x$. Stesso ragionamento per gli altri elementi.

Considerando $g_1 = 0, g_2 = x, g_3 = 2x, g_4 = 1, g_5 = 1+x, g_6 = 1+2x, g_7 = 2, g_8 = 2+x, g_9 = 2+2x$ si ottiene:



(a) Somma (b) Prodotto

Figura 1.1: Tavole delle operazioni

iii) Si può anche considerare un campo isomorfo cambiando semplicemente polinomio irriducibile: $\mathbb{Z}_3[x]/(x^2+1) = \{a+bx \ : \ a, b \in \mathbb{Z}_3, \ x^2 = -1\}$. Gli elementi avranno sempre la stessa rappresentazione $\{0, 1, 2, x, 1+x, 2+x, 2x, 1+2x, 2+2x\}$, ma cambierà il risultato delle operazioni (viene effettuata una permutazione sulle tavole delle operazioni). In questo caso, utilizzando lo stesso procedimento visto in precedenza, risulta ad esempio che $x^{-1} = -x$ infatti $1 = x^{-1}x = (a+bx)x = ax + bx^2 = ax - b$.

È possibile costruire praticamente un isomorfismo; indichiamo con

$$\mathbb{Z}_3[x]/(x^2+x-1) = \mathbb{Z}_3(\beta), \text{ e } \mathbb{Z}_3[x]/(x^2+1) = \mathbb{Z}_3(\alpha)$$

con β, α radici rispettivamente dei polinomi $x^2 + x - 1,\ x^2 + 1$.
Sia $\varphi :\ \mathbb{Z}_3(\beta) \longrightarrow \mathbb{Z}_3(\alpha)$ tale che $\beta \mapsto \alpha + 1$. L'elemento immagine di b deve soddisfare un preciso vincolo affinché φ sia un isomorfismo: deve continuare ad essere radice del polinomio $x^2 + x - 1$. In $\mathbb{Z}_3(\alpha)$ infatti $\alpha^2 + 2\alpha + 1 + \alpha + 1 - 1 = -1 + 3\alpha + 1 = 0$ (l'altra radice è $-\alpha + 1$). Quindi $\varphi(t + s\beta) = t + s(\alpha + 1)$ è un isomorfismo.

1.1.14 Automorfismi

Definizione 1.1.15. Dato un campo F di caratteristica p, si definisce la mappa $\Phi :\ F \to F$ tale che $a \mapsto a^p$, detto l'*omomorfismo di Frobenius*.

L'omomorfismo di Frobenius è iniettivo, infatti il nucleo $\ker \Phi = \{a \in F\ :\ a^p = 0\} = \{0\}$. Per provarlo basta osservare che se $a^p = a^{p-1}a = 0$ allora deve essere $a = 0$ o $a^{p-1} = 0$; se fosse $a \neq 0$ allora $a^{p-1} = a^{p-2}a = 0$ e ancora $a^{p-2} = a^{p-3}a = 0$ fino ad esaurire le potenze e giungere alla condizione che $a = 0$. Poiché il campo è finito, $\mathbb{F}_q,\ q = p^n$, risulta anche suriettivo. Tale risultato si può generalizzare alla mappa data da $a \mapsto a^{p^r}$, $r \geq 1$, che corrisponde a composizioni dell'omomorfismo di partenza.

Dire che Φ è un automorfismo di un campo F, con $char(F) = p$, significa dire che $F = F^p$ e questa è una caratterizzazione dei *campi perfetti* che, inoltre, è equivalente ad affermare che ogni estensione algebrica di tale campo è *separabile*[2].

1.1.16 Gruppo moltiplicativo

Segue adesso un risultato molto importate che verrà utilizzato come strumento dalle successive trattazioni dell'elaborato. È necessario richiamare un importante risultato riguardante i gruppi abeliani finiti.

Proposizione 1.1.17. *Sia G un gruppo abeliano finito e $\forall p$ primo, tale che $p|\ |G|$, si ponga $\Sigma_p = \{x \in G$ che hanno ordine una potenza di $p\}$. Allora:*

[2] come si dimostra in [5], pag. 36 del cap. V

(i) ogni Σ_p *è un sottogruppo di* G*;*

(ii) G *è prodotto diretto di tutti i* Σ_p *al variare di* p *tra tutti i divisori primi di* $|G|$*, cioè risulta* $G = \Sigma_{p_1} \times \Sigma_{p_2} \times \cdots \times \Sigma_{p_k}$*;*

(iii) ogni Σ_p *è prodotto diretto di gruppi ciclici di ordine una potenza di* p*.*

Teorema 1.1.18. *Il gruppo moltiplicativo di un campo finito è ciclico.*

Dimostrazione. Sia F un campo finito e $F^* = F\backslash\{0\}$ il suo *gruppo moltiplicativo*, esso è finito e abeliano e dunque è possibile applicare la proposizione precedente e $F^* = \Sigma_{p_1} \times \Sigma_{p_2} \times \cdots \times \Sigma_{p_k}$, con p_i fattori primi distinti di $|F^*| = p^n - 1$. Per provare che F^* è ciclico basta provare che i Σ_{p_i} sono tutti ciclici. Sia p il generico elemento fra quegli p_i, si ricordi che ogni Σ_p è prodotto diretto di gruppi ciclici $\Sigma_p = \mathbb{Z}_{p^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p^{\alpha_k}}$, con $\sum_i \alpha_i = \alpha$ dove $|\Sigma_p| = p^\alpha$. Se l'ordine massimo degli elementi di Σ_p fosse $p^\beta < p^\alpha$ allora per ogni $s \in \Sigma_p$ si avrebbe $s^{p^\beta} = 1$ e ciò implicherebbe l'assurdo che il polinomio $x^{p^\beta} - 1$ abbia più radici del suo grado. Quindi tale ordine dev'essere p^α, cioè $\Sigma_p = \mathbb{Z}_{p^\alpha}$ ciclico. Essendo ciò vero per ogni Σ_{p_i}, allora F^* risulta essere prodotto diretto di gruppi ciclici di ordine coprimo. □

Si osservi che se il campo è infinito ciò non vale, un controesempio è dato da $(\mathbb{R}^*, \cdot)$ che contiene -1 di periodo 2, ma $(\mathbb{Z}, +)$ non contiene un tale elemento.

Definizione 1.1.19. Un elemento u che genera il gruppo moltiplicativo di un campo finito F è detto *elemento primitivo*.

L'elemento primitivo è tale che $F = \mathbb{Z}_p(u)$, con p primo caratteristica del campo, cioè F è *estensione semplice* del suo sottocampo minimo.

Esempio 1.1.20. Considerato il campo $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2 + 1)$ la classe $1 + x$ è un elemento primitivo del gruppo moltiplicativo. Infatti il suo ordine, che dev'essere un divisore di $|\mathbb{F}_9^*| = 8$, può essere $2, 4, 8$ (non essendo l'unità). Osserviamo che $(1 + x)^2 = 1 + 2x + x^2 = 2x \neq 1$, $(1 + x)^4 = ((1 + x)^2)^2 = (2x)^2 = x^2 = -1 \neq 1$ e $(1 + x)^8 = ((1 + x)^4)^2 = (-1)^2 = 1$.

1.1.21 Sottocampi

Poiché il campo $\mathbb{F}_q$ di cardinalità $q = p^n$ può essere considerato come campo di spezzamento del polinomio $x^q - x$, è auspicabile che una decomposizione di tale polinomio possa fornire informazioni sui sottocampi di F.

Lemma 1.1.22. *Se $m \mid n$ allora $x^{p^m} - x \mid x^{p^n} - x$.*

Dimostrazione. Si consideri l'identità, valida in un anello qualunque:

$$y^t - 1 = (y-1)(y^{t-1} + \cdots + y + 1).$$

Per ipotesi si può scrivere $n = mt$ e ponendo $y = p^m$ si ottiene

$$p^n - 1 = (p^m)^t - 1 = (p^m - 1)((p^m)^{t-1} + \cdots + p^m + 1)$$

da cui si evince che $p^m - 1 \mid p^n - 1$, quindi $\dfrac{p^n - 1}{p^m - 1}$ è un intero.
Utilizziamo l'identità iniziale nell'anello dei polinomi $\mathbb{F}_q[x]$, ponendo

$$y = x^{(p^m-1)} \text{ e } t = \frac{p^n - 1}{p^m - 1} \text{ si ha}$$

$$(x^{(p^m-1)})^{\frac{p^n-1}{p^m-1}} - 1 = (x^{(p^m-1)} - 1)((x^{(p^m-1)})^{(\frac{p^n-1}{p^m-1}-1)} + \cdots + x^{(p^m-1)} + 1),$$

$$\text{cioè } x^{(p^n-1)} - 1 = (x^{(p^m-1)} - 1)((x^{(p^m-1)})^{(\frac{p^n-1}{p^m-1}-1)} + \cdots + x^{(p^m-1)} + 1).$$

Quindi $x^{(p^m-1)} - 1 \mid x^{(p^n-1)} - 1$. Moltiplicando entrambi i membri per x si ottiene $x^{p^m} - x \mid x^{p^n} - x$. □

Teorema 1.1.23. *Un campo K è sottocampo di Fq, con $q = p^n$, se e solo se $|K| = p^m$ con $m \mid n$.*

Dimostrazione.
⇒) Sia $K \subset \mathbb{F}_q$, sicuramente $charK = p$ e quindi $\mathbb{F}_p \subset K$, si può così scrivere $|K| = p^m$ dove m è la dimensione di K su $\mathbb{F}_p$, $[K : \mathbb{F}_p]$. Per il teorema dei gradi delle estensioni finite, per il campo intermedio K, si ha $n = [\mathbb{F}_q : \mathbb{F}_p] = [\mathbb{F}_q : K][K : \mathbb{F}_p] = [\mathbb{F}_q : K]m$, dunque $m \mid n$.

⇐) Sia m intero positivo tale che $m \mid n$, per provare che esiste un sottocampo di $\mathbb{F}_q$ di cardinalità p^m si può usare il lemma precedente: $x^{p^m} - x \mid x^{p^n} - x$.

Considerando che $\mathbb{F}_q$ è il campo di spezzamento di $x^{p^n} - x$, allora essendo $x^{p^m} - x$ un suo fattore ha tutte le sue radici in $\mathbb{F}_q$. Per quanto visto nel teorema 1.1.11 sappiamo che il sottoinsieme della radici di $x^{p^m} - x$ è un campo (quindi un sottocampo di $\mathbb{F}_q$) che può essere inteso come il suo campo di spezzamento di cardinalità p^m poiché tutte le sue radici sono semplici. □

Ovviamente tale sottocampo è unico a meno di isomorfismi e mettendo assieme tutte le considerazioni finora fatte, risulta evidente che dato un campo $\mathbb{F}_q$, $q = p^n$, per qualunque intero positivo $m \mid n$ esiste un unico sottocampo di $\mathbb{F}_q$ di cardinalità p^m.

Esempio 1.1.24. Il campo $\mathbb{F}_{16}$ non ha sottocampi di cardinalità 8.
Questo caso potrebbe trarre in inganno, infatti $8 \mid 16$ cioè $2^3 \mid 2^4$, ma la condizione necessaria e sufficiente è data sulla divisibilità degli esponenti ed in questo caso $3 \nmid 4$. Infatti tutti i sottocampi di $\mathbb{F}_{16} = \mathbb{F}_{2^4}$ sono dati dagli interi positivi che dividono 4 (utilizzati come esponenti): $m = 1, 2, 4$. Quindi abbiamo i sottocampi $\mathbb{F}_{2^1} = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ (sottocampo minimo), $\mathbb{F}_{2^2} = \mathbb{F}_4$ e $\mathbb{F}_{2^4} = \mathbb{F}_{16}$ (il campo stesso).

Esempio 1.1.25. Consideriamo il campo $\mathbb{F}_{p^{30}}$, con p primo qualsiasi. I divisori positivi di 30 sono $1, 2, 3, 5, 6, 10, 15, 30$ che determinano tutti e soli i sottocampi. Le relazioni fra i sottocampi $\mathbb{F}_{p^i}$ contenuti in $\mathbb{F}_{p^{30}}$ sono mostrate nel diagramma di Hasse:

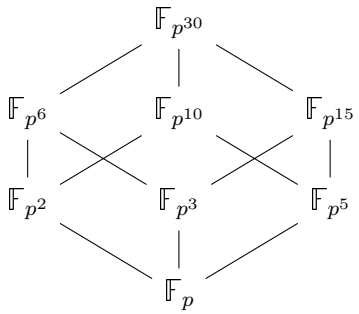


Figura 1.2: Struttura dei sottocampi di $\mathbb{F}_{p^{30}}$.

1.1.26 Polinomi irriducibili

Esiste un risultato per i polinomi irriducibili su campi finiti che permette di determinarne alcuni in modo piuttosto semplice.

Teorema 1.1.27. *In $\mathbb{F}_p[x]$ si ha che $x^{p^n} - x = \prod p(x)$, al variare di tutti i polinomi monici irriducibili $p(x)$ su F_p di grado m tale che $m \mid n$.*

Dimostrazione. Sia $p(x)$ un polinomio monico irriducibile su F_p di grado m con $m \mid n$. Per provare che $p(x) \mid x^{p^n} - x$, si consideri il campo che estende $\mathbb{F}_p$

$$E = \frac{\mathbb{F}_p[x]}{(p(x))},$$

che sappiamo contenere almeno una radice di $p(x)$, sia essa a.
Per l'irriducibilità del polinomio $p(x)$, si ha che $|E| = p^m$ ed ogni elemento di E è radice del polinomio $x^{p^m} - x$, che sappiamo essere un fattore di $x^{p^n} - x$. In particolare da questo si deduce che a è una radice di $x^{p^n} - x$. Poiché $p(x)$ è il polinomio minimo di a su F_p allora $p(x) \mid x^{p^n} - x$. Cioè ogni polinomio monico irriducibile di grado un divisore di n è un fattore di $x^{p^n} - x$.
Per mostrare che i suoi fattori sono tutti e soli polinomi di questo tipo, basta far vedere che preso un fattore monico irriducibile di $x^{p^n} - x$, sia $p(x)$, il suo grado divide n. Sappiamo che $L = \mathbb{F}_{p^n}$ è il campo di spezzamento di $x^{p^n} - x$ e preso $p(x)$ monico irriducibile di grado m che divide il polinomio, allora le radici di $p(x)$ sono anche elementi di L. In particolare sia a una di queste radici, si verifica che $\mathbb{F}_p \subset \mathbb{F}_p(a) \subset \mathbb{F}_{p^n}$ e per il teorema dei gradi si ha $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p(a)][\mathbb{F}_p(a) : \mathbb{F}_p]$ e poiché $[\mathbb{F}_p(a) : \mathbb{F}_p] = m$ allora $m \mid n$. □

Esempio 1.1.28. Il polinomio $x^9 - x \in \mathbb{Z}_3[x]$ si decompone come $x^9 - x = x(x^8 - 1) = x(x^4 - 1)(x^4 + 1) = x(x^2 - 1)(x^2 + 1)(x^2 + x - 1)(x^2 - x + 1) = x(x - 1)(x + 1)(x^2 + 1)(x^2 + x - 1)(x^2 - x + 1)$. Per scomporre il polinomio $x^4 + 1$ si può osservare che non ammette radici nel campo, dunque non contiene fattori lineari e l'unica sua decomposizione può essere del tipo $x^4 + 1 = (ax^2 + bx + c)(dx^2 + ex + f)$. Svolgendo il prodotto ed uguagliando i due membri si ottengono le soluzioni cercate.

Il seguente teorema fornisce una condizione necessaria e sufficiente per stabilire se un polinomio sia irriducibile o meno.

Teorema 1.1.29. *Un polinomio $f(x) \in \mathbb{F}_q[x]$ di grado n è irriducibile se e solo se risulta* $\text{MCD}\left(f(x), x^{q^i} - x\right) = 1$ *per ogni* $i = 1, 2, \ldots, \lfloor \frac{n}{2} \rfloor$.

Dimostrazione. Proveremo, per entrambe le implicazioni, le contronominali.
$\Rightarrow$) Supponiamo $\text{MCD}\left(f(x), x^{q^d} - x\right) \neq 1$, per almeno un valore $1 \leq d \leq \lfloor \frac{n}{2} \rfloor$, allora esiste un fattore non banale di $f(x)$ che risulta dunque riducibile.
$\Leftarrow$) Viceversa, supponiamo $f(x)$ riducibile e sia $f_1(x)$ un suo fattore monico irriducibile di grado d con $1 \leq d \leq \lfloor \frac{n}{2} \rfloor$. Per il Teorema 1.1.27 si ha che $f_1(x) | x^{q^d} - x$ da cui $f_1(x) | MCD\left(f(x), x^{q^d} - x\right)$ e quindi $\text{MCD}\left(f(x), x^{q^d} - x\right) \neq 1$. □

Esempio 1.1.30. Provare l'irriducibilità del polinomio

$$f(x) = x^7 + 2x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + x + 1 \in \mathbb{F}_3[x].$$

Si può utilizzare il teorema di caratterizzazione; poiché $n = 7$ e $q = 3$ si considerano i valori $1 \leq d \leq \lfloor \frac{7}{2} \rfloor$:

$$\text{MCD}\left(f(x), x^{3^1} - x\right), \quad \text{MCD}\left(f(x), x^{3^2} - x\right), \quad \text{MCD}\left(f(x), x^{3^3} - x\right).$$

Per il loro calcolo si può procedere utilizzando l'algoritmo euclideo (delle divisioni successive) e si verifica che tutti e tre i massimi comuni divisori sono 1.
Quindi, per la caratterizzazione, il polinomio $f(x)$ è irridubile.
Questo risultato ci permette, ad esempio, di costruire un campo di ordine 3^7:

$$\frac{\mathbb{F}_3[x]}{(f(x))} \cong \mathbb{F}_{3^7}.$$

Segue un esercizio che permette di applicare alcuni risultati precedenti.

Esercizio. Determinare in $\mathbb{F}_{81}$ il numero delle radici dei polinomi:

$$a)\ x^{80} - 1; \qquad b)\ x^{81} - 1; \qquad c)\ x^{88} - 1.$$

a) $x^{80} - 1$: Osserviamo che $|\mathbb{F}_{81}^*| = 80$ ed ogni elemento a non nullo di $\mathbb{F}_{81}$ è tale che $a^{80} = 1$. Quindi ogni elemento non nullo è radice del polinomio e il numero di tali elementi eguaglia il grado del polinomio. In effetti $\mathbb{F}_{81}$ è il campo di spezzamento di $x^{81} - x$.

b) $x^{81} - 1$: Affinché un elemento a non nullo del campo sia radice del polinomio deve verificarsi che $o(a)|81 = 3^4$ e poiché appartiene a $\mathbb{F}_{81}^*$ anche che $o(a)|80 = 2^4 \cdot 5$. L'unico caso possibile è che $o(a) = 1$ e quindi $a = 1$, unica radice in $\mathbb{F}_{81}$.

c) $x^{88} - 1$: Con lo stesso ragionamento fatto prima, affinchè a non nullo del campo sia radice del polinomio deve verificarsi che $o(a)|88 = 2^3 \cdot 11$ e $o(a)|80 = 2^4 \cdot 5$ quindi che $o(a) \in \{1, 2, 4, 8\}$. L'elemento di periodo 1 è l'unità, inoltre poichè $\mathbb{F}_{81}^*$ è ciclico sappiamo che esistono un unico sottogruppo di ordine 2, un unico di ordine 4 e un unico di ordine 8 (e sono tutti ciclici e contenuti ognuno nel successivo). Per la caratterizzazione dei gruppi ciclici, possiamo pensare a $\mathbb{Z}_8$ (in notazione additiva) che contiene un elemento di ordine 1, uno di ordine 2, due di ordine 4 e quattro di ordine 8. Sono quindi tutte e sole le radici del polinomio.

Capitolo 2

Applicazioni

2.1 Applicazioni alla Crittografia

Nel presente paragrafo sono esposti in maniera prevalentemente qualitativa alcuni concetti riguardanti tecniche di *Crittografia*. L'esposizione è mirata a definire e chiarire i concetti più astratti e teorici e procede, quindi, senza in alcun modo scendere in dettagli troppo tecnici o che riguardano la parte fisica dei dispositivi e mezzi di comunicazione. La trattazione comprende nozioni presenti fondamentalmente in [6], in [7].

Lo studio della *Crittografia*[1] risponde ad un problema della comunicazione legato alla semantica: quello di rendere illeggibili i messaggi a meno di possedere l'adeguato metodo di lettura. In generale il procedimento (algoritmo) usato è reso noto, così che chiunque possa implementarlo, e ciò che contraddistingue e rende "personale" la cifratura è la *chiave*: un parametro iniziale sul quale si basa la codifica.

Definizione 2.1.1. Un sistema crittografico è detto

a) *simmetrico*, se un'unica chiave detta *privata* è utilizzata sia dalla sorgente per codificare il messaggio, sia dai destinatari per decodificarlo. Il problema fondamentale di tale metodo è quello di comunicare in modo sicuro la chiave esclusivamente ai destinatari.

[1] la cui etimologia conduce al significato di *scrittura nascosta*

b) *asimmetrico*, se viene utilizzata una coppia di chiavi: una detta *pubblica*, usata per codificare il messaggio, e l'altra *privata*, usata per decodificare il messaggio. Tale sistema, introdotto nel 1976 da Diffie e Hellman, è quello attualmente più diffuso e poiché anche le applicazioni di tale elaborato saranno riferite ad esso è utile approfondirne la conoscenza[2].

Un concetto essenziale per utilizzare un sistema crittografico asimettrico è quello di *complessità computazionale*, cioè molto in generale su quanto sia difficile riuscire a decifrare un messaggio praticamente.

2.1.2 Complessità computazionale

Brevemente, si dirà che un algoritmo ha complessità *polinomiale* se per essere eseguito, nel peggiore dei casi, impiega un tempo[3] limitato superiormente dal valore an^b, per certi $a \in \mathbb{R}_{>0}$, $b \in \mathbb{R}_{>1}$ e n è un valore che rappresenta l'istanza iniziale del problema. Mentre ha complessità *esponenziale* se, con le stesse premesse, il limite superiore è ab^n, con analoghi parametri.
Algoritmi di complessità polinomiale, o inferiore, si dicono *computazionalmente trattabili* mentre algoritmi di complessità esponenziale sono detti generalmente *computazionalmente intrattabili*.

Alcuni problemi attualmente intrattabili molto usati in crittografia sono quello della *fattorizzazione* in primi di un numero intero (su cui è basato il sistema RSA) e quello del *logaritmo discreto*.

Esempio 2.1.3. (Problema del Logaritmo Discreto - DLP)
Dato un gruppo ciclico $G(+) = \langle g \rangle$ di ordine n, la mappa:

$$f : \mathbb{Z}_n \longrightarrow G \text{ definita da } t \longmapsto tg := \underbrace{g + \cdots + g}_{t \text{ volte}}.$$

è un isomorfismo fra $\mathbb{Z}_n(+)$ e $G(+)$. Il problema di calcolare la mappa inversa f^{-1} è detto del logaritmo discreto, cioè dato un elemento $h \in G = \langle g \rangle$ ovviamente è sempre possibile trovare un $t \in \mathbb{Z}_n$ tale che $h = tg$ e si può

[2]facendo riferimento all'articolo originale [8]
[3]dove l'unità di tempo si riconduce all'esecuzione di un'operazione elementare

scrivere, in forma simbolica, che $t = \log_g h$. Tale problema è strettamente legato alla struttura del gruppo e la sua complessità computazionale dipende quindi dal gruppo scelto.

Si prova che se $G = \mathbb{Z}_n$ allora il problema è facilmente risolvibile in un tempo polinomiale, infatti si riduce al dover calcolare[4] il valore minimo di $t \in \mathbb{Z}_{>0}$ tale che $h = tg \ (mod\ n)$ e per far ciò è possibile utilizzare l'algoritmo di Euclide esteso[5]. Tale gruppo non è quindi utilizzabile ai fini crittografici. Vedremo in seguito altri esempi significativi. □

2.1.4 Sistemi crittografici

Nei crittosistemi asimmetrici, la chiave pubblica k è resa disponibile dal proprietario a chiunque voglia codificare un messaggio, fissato un algoritmo specifico. Una buona *funzione di codifica*, φ, deve permettere di calcolare facilmente il messaggio cifrato, $c = \varphi(m, k)$, ma ovviamente deve essere "computazionalmente difficile" da invertire (funzione *one-way*) a meno di possedere informazioni addizionali (in questo caso, funzione *trapdoor-one-way*).
La conoscenza della chiave privata s deve permettere facilmente, tramite un'opportuna funzione ψ, la decodifica del messaggio cifrato, $m = \psi(c, s) = \psi(\varphi(m, k), s)$.
Verrà riportato un esempio di sistema crittografico ([10]).

Esempio 2.1.5. (Sistema di ElGamal)
Tale crittosistema implementa il protocollo di Diffie-Hellman (DHKA) per lo scambio sicuro delle chiavi e la funzione trapdoor-one-way è legata al DLP.
Sia quindi fissato un gruppo ciclico G di ordine n e dato l'alfabeto binario $\{0, 1\}$ sia $f : G \longrightarrow \{0, 1\}^r$ una funzione dal gruppo fissato all'insieme delle stringhe binarie di lunghezza r. Seguono i passaggi previsti dal sistema:

Parametri: Alice sceglie un generatore di G, g, e un numero intero casuale a tale che $1 \leq a \leq n - 1$. La coppia (ag, a), dove ag è l'elemento di G generato in notazione additiva, rappresenta la coppia di chiavi (pubblica, privata).

[4] espresso in notazione additiva

[5] esattamente limitata da $\log^2 n$, come mostrato in [9], pag. 869

Quindi Alice pubblica i parametri per la comunicazione: $(G, +, f, g, ag)$.
Codifica: Bob vuole inviare il messaggio $m \in \{0,1\}^r$ ad Alice e conosce i parametri pubblici. Fissa un intero casuale b tale che $1 \leq b \leq n-1$, calcola bg, codifica il messaggio: $c = m + f(b(ag))$ e invia ad Alice la coppia (bg, c).
Decodifica: Alice riceve (bg, c) e calcola, secondo il protocollo DHKA, che $a(bg) = (ab)g = (ba)g = b(ag)$ (è necessario conoscere la chiave privata a). A questo punto calcola $c - f(b(ag)) = m$, ottenendo il messaggio non cifrato m.

Tale sistema è sicuro fintanto che il problema DLP di ottenere a da ag e b da bg è intrattabile (senza la conoscenza delle rispettive chiavi private). Quindi, secondo il protocollo DHKA, la chiave di codifica/decodifica è proprio $b(ag)$ che sia Alice che Bob possiedono come già visto. □

2.1.6 Curve Ellittiche

Per completare la panoramica sulla crittografia è opportuno accennare alle Curve Ellittiche del piano affine, considerando quelle non singolari.

Definizione 2.1.7. Una *Curva Ellittica* E sul campo finito $\mathbb{F}_q$ può essere espressa dall'equazione: $E/\mathbb{F}_q : \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ detta forma di Weierstrass, dove $a_i \in \mathbb{F}_q$ e il discriminante è non nullo.

Esistono dei casi particolari, ad esempio quando la caratteristica del campo è 2 o 3, per i quali l'equazione di Weierstrass assume forme più semplici.

Sia $\mathrm{Supp}(E) \subset \mathbb{F}_q \times \mathbb{F}_q$ l'insieme dei punti che soddisfano l'equazione della curva ellittica non singolare $E/\mathbb{F}_q$, cioè il supporto, e $\mathcal{O}$ il punto proiettivo della curva, allora l'insieme $E(\mathbb{F}_q) := \mathrm{Supp}(E) \cup \mathcal{O}$ è un gruppo abeliano additivo il cui elemento neutro è proprio $\mathcal{O}$.

Definizione 2.1.8. Presi comunque due punti sulla curva: $P_1, P_2 \in E(\mathbb{F}_q)$, si definisce l'operazione di *gruppo sulla curva ellittica*, in notazione additiva, $P_1 + P_2 := R$ effettuando le seguenti operazioni:

1) tracciare la retta r passante per essi

2) individuare il terzo punto di intersezione $r \cap E$, sia esso P_3

3) tracciare la retta s passante per P_3 e $\mathcal{O}$

4) individuare il terzo punto di intersezione $s \cap E$, sia esso R

Per le proprietà geometriche della curva e delle operazioni effettuate si osserva che tale definizione è ben posta e dà luogo ad un gruppo abeliano. Poiché si lavora su campi finiti, anche il gruppo della curva è finito e può essere utilizzato con profitto per implementare[6] crittosistemi basati sul DLP.

Osserviamo che esistono vari casi che vale la pena di analizzare per chiarire alcune particolarità. Per far questo verrà utilizzato un esempio.

Esempio 2.1.9. Si consideri la curva ellittica $E: \ y^2 = x^3 - x + 1$ sul campo $\mathbb{F}_7$, tale curva è non singolare ed ha un unico punto improprio, $\mathcal{O}[0,1,0]$, di molteplicità 3 (flesso). Cosa succede applicando la definizione di somma ai punti di $\mathrm{Supp}(E)$.

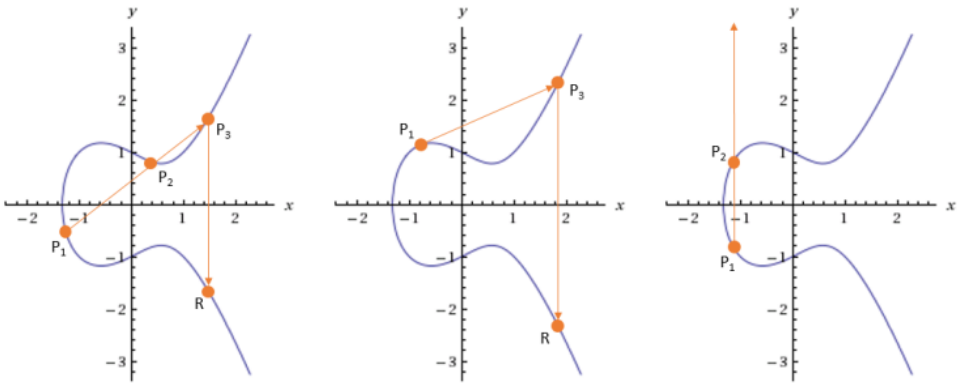
a) *Punti distinti*: $P_1, P_2 \in \mathrm{Supp}(E)$, $P_1 \neq P_2$. Può essere seguito l'algoritmo senza alcuna ulteriore precisazione.

b) *Punti coincidenti* sulla curva: $P_1, P_2 \in \mathrm{Supp}(E)$, $P_1 = P_2$. L'unica osservazione da poter fare è che trattandosi di punti coincidenti, bisogna partire dalla tangente del punto alla curva. Il resto delle operazioni procedono come descritto. Ripetendo questa operazione m volte permette di calcolare il multiplo mP del punto P.

c) *Punti allineati verticalmente* sulla curva: $P_1, P_2 \in \mathrm{Supp}(E)$, $(P_1)_x = (P_2)_x$. In questo caso la retta r fra i due punti ha come altra intersezione il punto $\mathcal{O}$ e trovare la retta s passante per $\mathcal{O}$ e se stesso significa cercare la tangente al punto improprio che avrà come intersezione $s \cap E$ lo stesso $\mathcal{O} = R$. In questo caso i due punti di dicono *opposti*.

Poiché utilizziamo il supporto della curva su di un campo finito (cioè cerchiamo i punti razionali su quel campo), l'insieme dei punti sui quali si lavora effettivamente può essere visualizzato nel seguente modo:

[6] la trattazione esaustiva si trova in [7]



(a) Elementi distinti (b) Elementi coincidenti (c) Elementi opposti

Figura 2.1: Operazione di gruppo sulla curva E

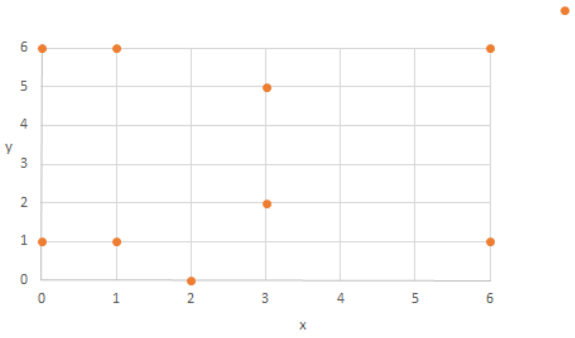


Figura 2.2: Punti del gruppo della curva

La tabella è ottenuta valutando la curva in ogni valore del campo, ottenendo così tutti i punti del supporto. Ad esempio per $x = 0$ si ottiene $y^2 = 1$ da cui $y = 1, -1 = 1, 6 \in \mathbb{Z}_7$; oppure per $x = 3$ si ottiene $y^2 = 6 - 3 + 1 = 4$ che in $\mathbb{Z}_7$ è un quadrato perfetto con radici $y = 2, 5$; infine per $x = 4$ si ha $y^2 = 1 - 4 + 1 = 5$ che non è un quadrato nel campo e dunque non esistono punti della curva con tale ascissa.

Per avere una stima, a priori, sulla cardinalità del supporto di una curva su un campo finito $E/\mathbb{F}_q$, si può tenere conto di alcune osservazioni tecniche:

- Si estende l'endomorfismo di Frobenius al gruppo $E(\mathbb{F}_q)$ definendo:
  $\Phi : \ E(\mathbb{F}_q) \to E(\mathbb{F}_q) \quad$ tale che $\quad \Phi(\mathcal{O}) = \mathcal{O} \quad$ e $\quad \Phi(x, y) = (x^q, y^q)$.

- La quantità $t = q+1-|E(\mathbb{F}_q)|$ è detta *traccia di Frobenius relativa a* q e soddisfa[7]: $|t| \leq 2\sqrt{q}$, che fornisce un intervallo contenente la cardinalità del gruppo $E(\mathbb{F}_q)$.
- Per ogni punto $(x, y) \in E(\mathbb{F}_q)$ vale l'identità $\Phi^2(x, y)-t\Phi(x, y)+q(x, y) = 0$ detta *equazione caratteristica di* Φ.

Osservazione: Nell'esempio 2.1.3 viene riportato che il problema del logaritmo discreto è strettamente legato al gruppo scelto e il caso esaminato non era accettabile. Se invece $G = E(\mathbb{F}_q)$, cioè il gruppo dei punti razionali di una curva ellittica definita sul campo $\mathbb{F}_q$, allora generalmente il problema del logaritmo discreto ha complessità esponenziale[8] e dunque per grandi valori di q diventa intrattabile. Tale gruppo è quindi utilizzato da vari sistemi crittografici basati sul DLP.

Conclusioni: Sistemi crittografici di tale tipo, tenendo conto della struttura di base, attuano parecchie ottimizzazioni anche per quanto riguarda la compressione dei dati crittografati. Ad esempio, poiché il gruppo della curva è costituito da punti, cioè coppie di coordinate $(x, y) \in \mathbb{F}_q^2$, alcune osservazioni permettono di considerare la sola coordinata x e con un solo bit di informazione aggiuntivo è possibile, tramite l'equazione della curva, trovare la y relativa. Altre tecniche permettono di comprimere i parametri pubblici del sistema crittografico.
Esistono inoltre crittosistemi avanzati sulle curve ellittiche che sfruttano funzioni di codifica particolari strettamente legate alla natura dei punti razionali della curva, ma non è nell'interesse dell'elaborato parlarne.

La *sicurezza* o *forza* di una codifica, cioè quanto è resistente agli attacchi di decodifica da parte di chi non conosce le chiavi, è proporzionale alla grandezza della chiave. Si dice che un crittosistema ha X *bit di sicurezza* se la sua forza è equiparabile a quella di un crittosistema simmetrico con chiave di X bit[9].

[7] quanto dimostrato nel teorema di Hasse in [11], pag.138
[8] con costante $\lceil \log q \rceil$ come dimostrato in [7], pag. 8
[9] l'attacco più efficiente è quello di provare tutte le possibili chiavi e costa circa 2^{X-1}

Ad esempio[10] un crittosistema simmetrico con chiave di 80 bit ha la stessa sicurezza di un sistema RSA con chiave 1024 bit e di un sistema su Curve Ellittiche con chiave $160 - 223$ bit.

[10]come appare in [12], pag.63

Bibliografia

[1] T. Hungerford, *Algebra*. No. 73 in Graduate Texts in Mathematics, New York: Springer-Verlag, 1974.

[2] G. Piacentini Cattaneo, *Algebra - un approccio algoritmico*. Padova: Decibel-Zanichelli, 1996.

[3] I. Herstein, *Algebra*. University Press, Roma: Editori Riuniti, 1982.

[4] Z. Wan, *Lectures on Finite Fields and Galois Rings*. World Scientific, 2003.

[5] N. Bourbaki, *Algebra*. Elements of Mathematics, Parigi: Springer-Verlag, 1990.

[6] C. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, 1948.

[7] I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*. New York, NY, USA: Cambridge University Press, 1999.

[8] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theor.*, vol. 22, pp. 644–654, Sept. 2006.

[9] T. Cormen, C. Stein, R. Rivest, and C. Leiserson, *Introduction to Algorithms*. McGraw-Hill Higher Education, 2nd ed., 2001.

[10] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of CRYPTO 84 on Advances in cryptology*, (New York), pp. 10–18, Springer-Verlag, 1985.

[11] J. Silverman, *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, 106, Springer-Verlag New York, 2009.

[12] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management - part 1: General (revised)," in *NIST Special Publication*, 2006.

Indice analitico