Università degli Studi di Trento
CryptoLabTN

# Groebner bases and ECDLP: involution

27 Ottobre 2017

Ceria Michela

# Indice

# ... Cos'è una curva ellittica?

**Equazione di Weierstrass**:

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

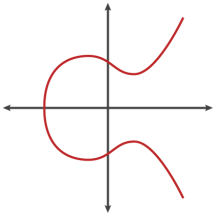
$$a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$$

**Curva ellittica**:

soluzioni di $f(x,y) = 0$

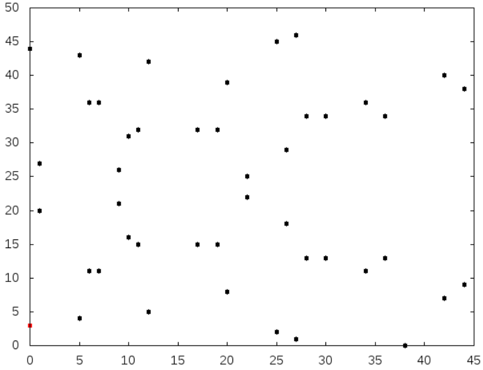
$+$

punto all'infinito $\mathcal{O}$



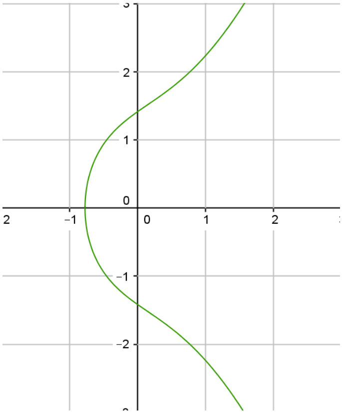
# ESEMPIO

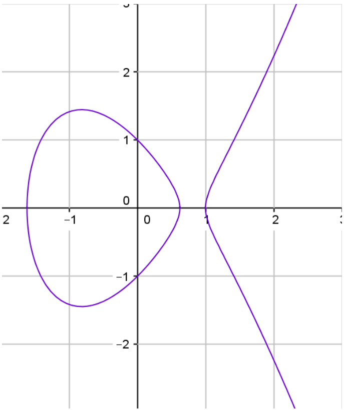
$E : y^2 = x^3 + 14x + 9$ su $\mathbb{Z}_{47}$.



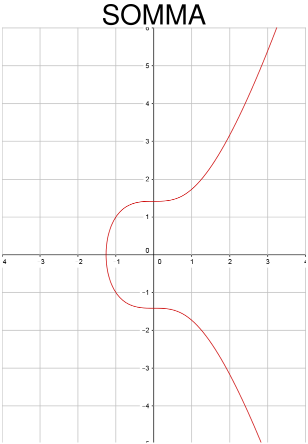

$E$ ha ordine 46.

# Curve buone



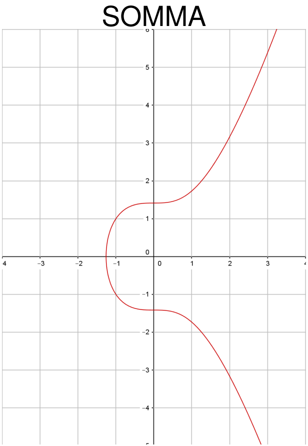



# LEGGE DI GRUPPO



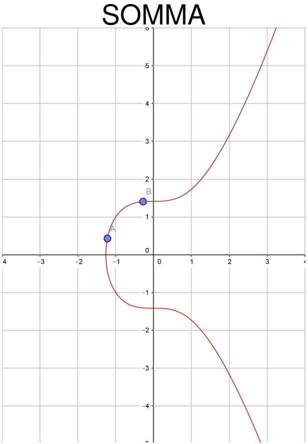

- **E** curva ellittica;
- $\mathcal{O}$ punto all'infinito su **E**;
- $A \in$ **E**;
- $A \oplus \mathcal{O} = A$.

# LEGGE DI GRUPPO



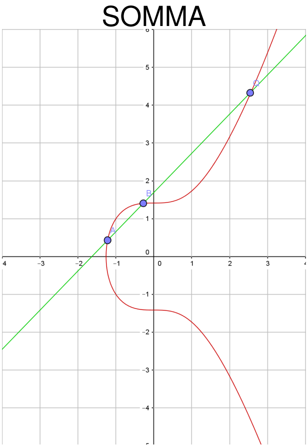

- **E** curva ellittica;
- $\mathcal{O}$ punto all'infinito su **E**;
- $A \in$ **E**;
- $A \oplus \mathcal{O} = A$.

# LEGGE DI GRUPPO



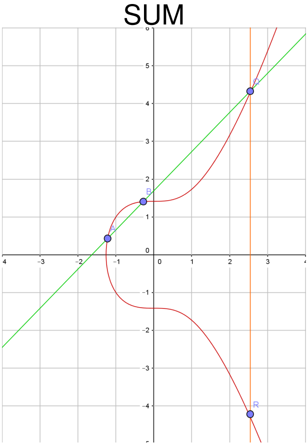

- **E** curva ellittica;
- $\mathcal{O}$ punto all'infinito su **E**;
- $A, B \in \mathbf{E}$;

# Legge di gruppo




- **E** curva ellittica;
- $\mathcal{O}$ punto all'infinito su **E**;
- $A, B \in$ **E**;
- $\ell$ retta tra $A$ e $B$;
- $Q$ terza intersezione tra **E** e $\ell$;

# LEGGE DI GRUPPO

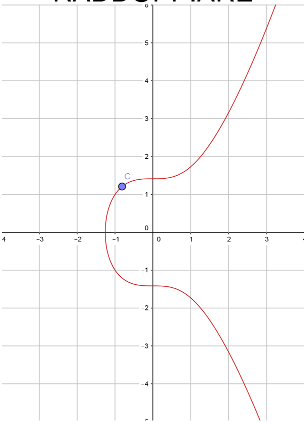



- **E** curva ellittica;
- $\mathcal{O}$ punto all'infinito su **E**;
- $A, B \in$ **E**;
- $\ell$ retta tra $A$ e $B$;
- $Q$ terza intersezione tra **E** ed $\ell$;
- $R$ punto riflesso di $Q$ rispetto all'asse $x$.

$\Longrightarrow$ $R$ è la somma $A \oplus B$.

# LEGGE DI GRUPPO

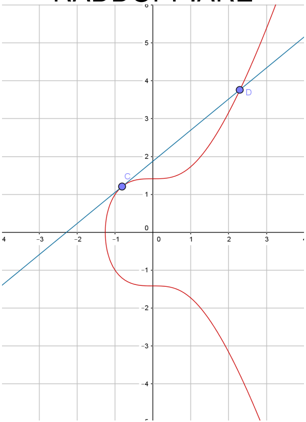
RADDOPPIARE




Se voglio calcolare $[2]C = C \oplus C$

# LEGGE DI GRUPPO

RADDOPPIARE



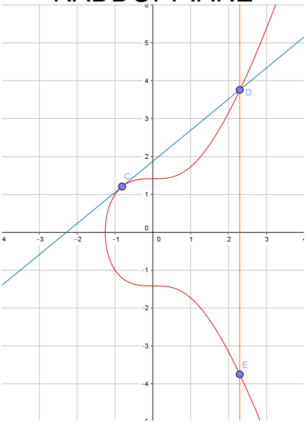

Se voglio calcolare $[2]C = C \oplus C$

$$\Downarrow$$

- $\ell$ tangente alla curva in $C$;
- $D$ intersezione tra **E** e $\ell$;

# LEGGE DI GRUPPO

RADDOPPIARE



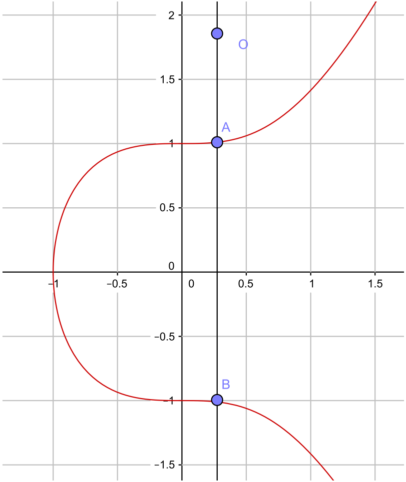

Se voglio calcolare $[2]C = C \oplus C$

$\Downarrow$

- $\ell$ tangente alla curva in $C$;
- $D$ intersezione tra **E** e $\ell$;
- $E$ punto riflesso di $D$ rispetto l'asse $x$.

$\Longrightarrow$ $E$ è il doppio... $[2]C$.

# Legge di gruppo

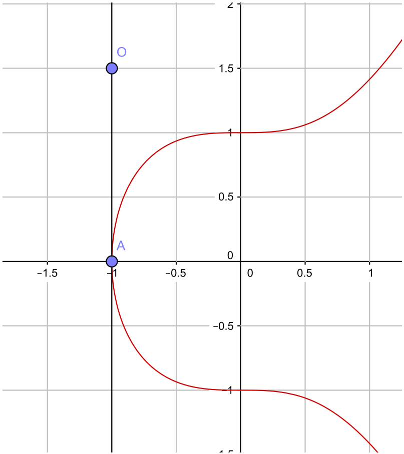



Se $A$ e $B$ sono sulla stessa retta verticale ($x_A = x_B$)

$$\Downarrow$$

- $A \oplus B = \mathcal{O}$;
- $B = -A$.

# LEGGE DI GRUPPO




Se $A$ sta sull'asse $x (y_A = 0)$

$$\Downarrow$$

- $[2]A = \mathcal{O}$;
- $A = -A$.

## Moltiplicazione per scalare ed ordine di un punto

- $k \in \mathbb{N}$:

$$\begin{aligned}[k] \quad : \quad & \mathbf{E} \to \mathbf{E} \\ & P \to [k]P = k \cdot P = \underbrace{P \oplus P \oplus \ldots \oplus P}_{k}\end{aligned}$$

- $k = 0$: $[0]P = \mathcal{O}$

- $k < 0$: $[k]P = [-k](-P)$

- Ordine di $P \in \mathbf{E}$:
  il minimo $m \in \mathbb{Z}$, $m > 0$, se esiste, t.c. $[m]P = \mathcal{O}$

  Se $m$ non esiste $\implies$ $P$ ha **ordine infinito**

# Moltiplicazione per scalare ed ordine di un punto

- $k \in \mathbb{N}$:

$$\begin{aligned} [k] \quad : \quad & \mathbf{E} \to \mathbf{E} \\ & P \to [k]P = k \cdot P = \underbrace{P \oplus P \oplus \ldots \oplus P}_{k} \end{aligned}$$

- $k = 0$: $[0]P = \mathcal{O}$

- $k < 0$: $[k]P = [-k](-P)$

- Ordine di $P \in \mathbf{E}$:
  il minimo $m \in \mathbb{Z}$, $m > 0$, se esiste, t.c. $[m]P = \mathcal{O}$

  Se $m$ non esiste $\implies$ $P$ ha **ordine infinito**

# ELLIPTIC CURVE CRYPTOGRAPHY

## ECDLP

Data una curva ellittica $E$ su un campo $\mathbb{K}$, un punto $P$ su di essa con ordine $n$ ed un altro punto $Q$ su E, vogliamo trovare $k$ t.c.

$$Q = [k]P.$$

Tale problema si chiama **ECDLP** e la sua difficoltà è fondamentale per la crittografia delle curve ellittiche

## ONE WAY

Data una curva ellittica $E$ ed un punto $P$ di ordine $n$:

- una moltiplicazione per scalare $[k]P = Q$ è **facile** da calcolare
- dato un punto $Q$, è **molto complicato** trovare $k$ t.c. $Q = [k]P$.

$\rightarrow$ **one-way function**.

# Elliptic Curve Cryptography

## ECDLP

Data una curva ellittica $E$ su un campo $\mathbb{K}$, un punto $P$ su di essa con ordine $n$ ed un altro punto $Q$ su E, vogliamo trovare $k$ t.c.

$$Q = [k]P.$$

Tale problema si chiama **ECDLP** e la sua difficoltà è fondamentale per la crittografia delle curve ellittiche

## One way

Data una curva ellittica $E$ ed un punto $P$ di ordine $n$:

- una moltiplicazione per scalare $[k]P = Q$ è **facile** da calcolare
- dato un punto $Q$, è **molto complicato** trovare $k$ t.c. $Q = [k]P$.

$\rightarrow$ **one-way function**.

# RISOLVERE ECDLP?

- **Pollard's Rho**
- **Semaev summation polynomials**
- *variazione di Amadori-Pintore-Sala*

# COME SI CALCOLA UNA BASE DI GROEBNER?

L'algoritmo classico di Buchberger è poco efficiente....

1. tecniche di Macaulay e poi Faugère, → **algebra lineare**;
2. le tecniche involutive di Janet, Gerdt–Blinkov e Seiler → **divisioni involutive**.

# MACAULAY

Dato $\mathbf{k}[x_1, ..., x_n]$ e preso un insieme di polinomi **omogenei** $H = \{h_1, ..., h_r\}$ di grado $D$

Macaulay definisce una **matrice** per rappresentare $H$, le cui colonne sono indicizzate dagli $\binom{n+D-1}{n-1}$ termini di grado $D$ in $n$ variabili e le cui righe sono indicizzate dagli elementi di $H$.

Nell'entrata $(i, j)$ della matrice viene posto il coefficiente di $f_i$ nel monomio $j$-esimo.

# Esempio

$D = 2$ in $\mathbf{k}[x, y]$ $H = \{x^2, xy - y^2\}$:

| $x^2$ | $xy$ | $y^2$ |
|---|---|---|
| 1 | 0 | 0 |
| 0 | 1 | 1 |

# Faugère... and us

**Caso non omogeneo**: $F = \{f_1, ..., f_s\} \subset \mathbf{k}[x_1, ..., x_n]$, $\deg(f_i) = d_i$, $1 \leq i \leq s$. L'algoritmo di Faugère è **induttivo** sul grado dei polinomi, a partire da $d = \min\{d_1, ..., d_s\}$.

Dato un grado $D$, costruisce una matrice per $F_D \subset F$ con i polinomi ottenuti dagli elementi di $F_{D-1}$ moltiplicati per le variabili in tutti i modi possibili. **Colonne: grado $\leq D$**.

Riduce **sottomatrici**, legate agli S-polinomi, inserendo in $F$ i nuovi elementi così trovati.

# FAUGÈRE

- **riduzione tutta insieme**
- **bound numero passi**
- **signature**
- **dipendenza dall'implementazione**
- _, *Pintore, Sala, Visconti*: algoritmo ad hoc?

# INVOLUZIONE?

*One can also seek alternatives for the use of the usual Groebner bases algorithm. For example, the concept of Involutive Bases for polynomial ideals* [...]. *The idea was derived from the theory of algebraic analysis of PDEs. By calculating the involutive basis of a system, one can study the same kind of problems addressed by Groebner bases. In fact, one can show that an involutive basis is a special, though usually redundant, form of Groebner basis. Involutive Bases algorithms have shown to be particularly efficient* [...]

# INVOLUZIONE

Una **divisione involutiva** $L$ su $\mathcal{T} = \{x_1^{\gamma_1} \cdots x_n^{\gamma_n} | \gamma = (\gamma_1, ..., \gamma_n) \in \mathbb{N}^n\}$ è una relazione $|_L$ definita, per ogni insieme finito $U \subset \mathcal{T}$, sull'insieme $U \times \mathcal{T}$ in modo tale che le relazioni seguenti valgono per ogni $u, u_1 \in U$ e $t, t_1 \in \mathcal{T}$

(i). $u \,|_L\, t \Rightarrow u \,|\, t$;

(ii). $u \,|_L\, u$ per ogni $u \in U$;

(iii). $u \,|_L\, ut, u \,|_L\, ut_1 \Leftrightarrow u \,|_L\, utt_1$;

(iv). $u \,|_L\, t, u_1 \,|_L\, t \Rightarrow$ either $u \,|_L\, u_1$ or $u_1 \,|_L\, u$;

(v). $u \,|_L\, u_1, u_1 \,|_L\, t \Rightarrow u \,|_L\, t$;

(vi). se $V \subseteq U$ and $u \in V$ allora $u \,|_L\, t$ rispetto a $U \Rightarrow u \,|_L\, t$ rispetto a $V$.

### Definition

Sia $L$ una divisione involtutiva su $\mathcal{T}$ ad $F$ un insieme finito di polinomi. Diciamo

- $p \in \mathbf{k}[x_1, ..., x_n]$ è $L$-riducibile modulo $f \in F$ se in $p$ c'è un termine $t$ tale che $\mathrm{T(f)} \mid_{\mathrm{L}} \mathrm{t}$ ed in particolare $t = \mathrm{T(f)v}$ con $v$ moltiplicativo per T(f). Da questo si ottiene la $L$-riduzione $p \to g = p - c(t, p)/Lc(f)fv$, dove $Lc(f)$ denota il coefficiente di T(f), ovvero il leading coefficient di $f$ e $c(t, p)$ il coefficiente di $t$ in $p$;

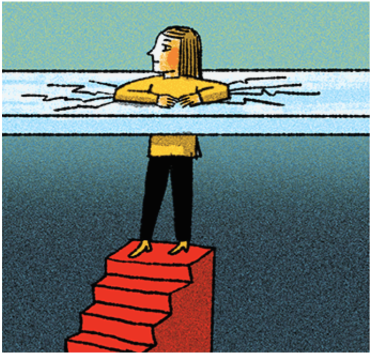
Un insieme $F$ è $L$-autoridotto se T{F} è $L$-autoridotto e ogni polinomio $f \in F$ non possiede alcun termine $L$-riducibile modulo $F$.

### Definition

Un insieme $L$-autoridotto $F$ si chiama *base involutiva* di $(F)$ se $\forall f \in F \, \forall u \in \mathcal{T}, \; NF_L(fu, F) = 0$.

Diversamente dai bound di Faugère...

- calcolo della regolarità
- test di Cartan



# DIVISIONI INVOLUTIVE RELATIVE

Sia $U \subset \mathcal{T}$ un insieme finito di termini. Diciamo che una *divisione involutiva relativa* $L$ è data su $U$ se, per ogni $u \in U$ una partizione

$$\{x_1, ..., x_n\} = M_L(u, U) \sqcup NM_L(u, U),$$

è data sull'insieme delle variabili in modo che, denotato

$$L(u, U) := \{x_1^{a_1} \cdots x_n^{a_n} \mid a_i \neq 0 \Rightarrow x_i \in M_L(u, U)\},$$

valgono le seguenti due condizioni:

1. $\mathrm{T(U)} = \bigcup_{\mathrm{u} \in \mathrm{U}} \mathrm{uL(u, U)}$;
2. $\forall u, v \in U$, $uL(u, U) \cap vL(v, U) = \emptyset$.

L'insieme $M_L(u, U)$ viene chiamato *insieme delle variabili moltiplicative relative*, $NM_L(u, U)$ viene chiamato **insieme delle variabili non moltiplicative relative**, mentre $L(u, U)$ si dice *insieme dei termini moltiplicativi relativi*.
$C_L(u, U) := uL(u, U)$:**cono relativo** di $u \in U$.

***Grazie per la cortese attenzione!***