Ricerca Matematica per apprendisti: la teoria per far bottega

Pasqualina 'Lilli' Fragneto & Luca Magri

I matematici risolvono problemi
Siracusa 2016


Esperienza
Strumenti
Problema

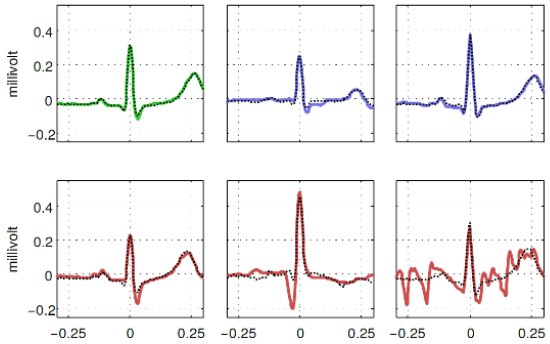
AST Applied Math Team

Che cosa facciamo?

- Innovazione e sviluppo su **problemi** industriali
- Studio di **strumenti** matematici per l'analisi e l'elaborazione di dati provenienti da applicazioni industriali
- Condivisione della nostra **esperienza** con gli altri gruppi di AST e il mondo della ricerca

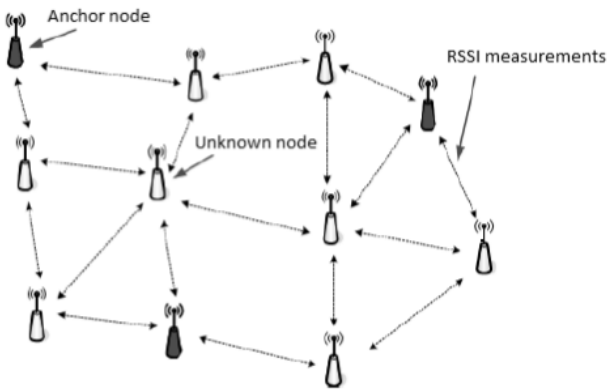
AST Applied Math Team

Detezione di anomalie

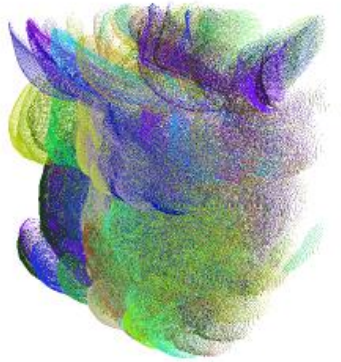


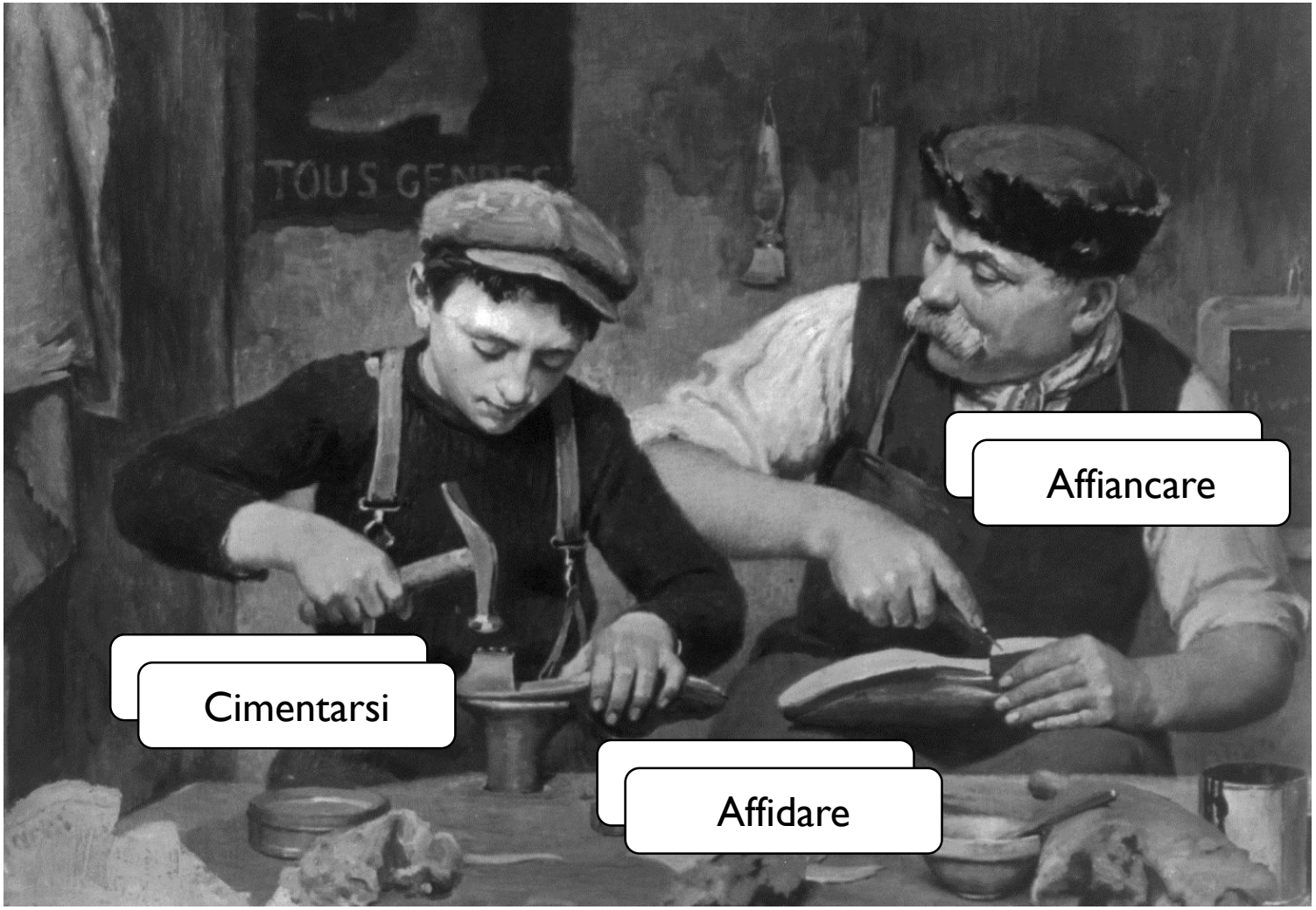
Identificazione facciale

Localizzazione



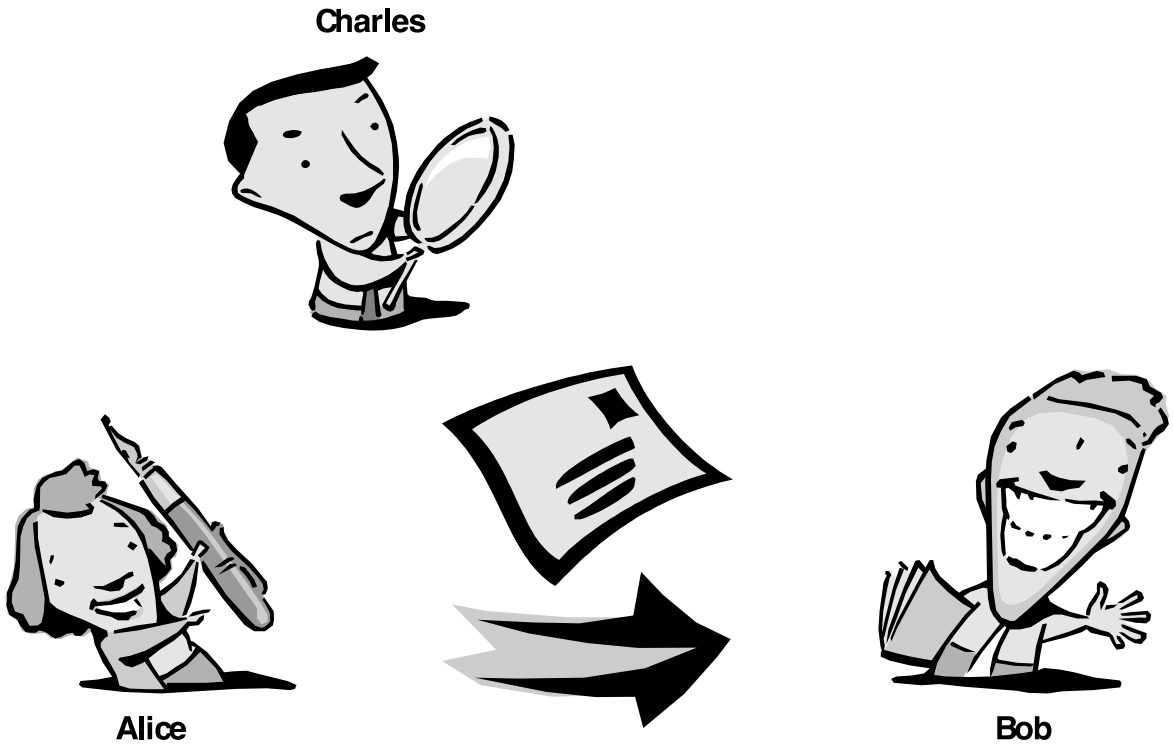
Registrazione 3D




Affiancare
Cimentarsi
Affidare

La crittografia a chiave pubblica

Il problema consiste nel far comunicare in modo sicuro due entità.



Chiarezza del problema

- **Protocolli**
- Sistema
- Aritmetica modulare
- Linguaggio hardware

Cosa garantisce un protocollo crittografico

1. Autenticazione
2. Confidenzialità
3. Integrità
4. Non ripudio

Formalismo matematico

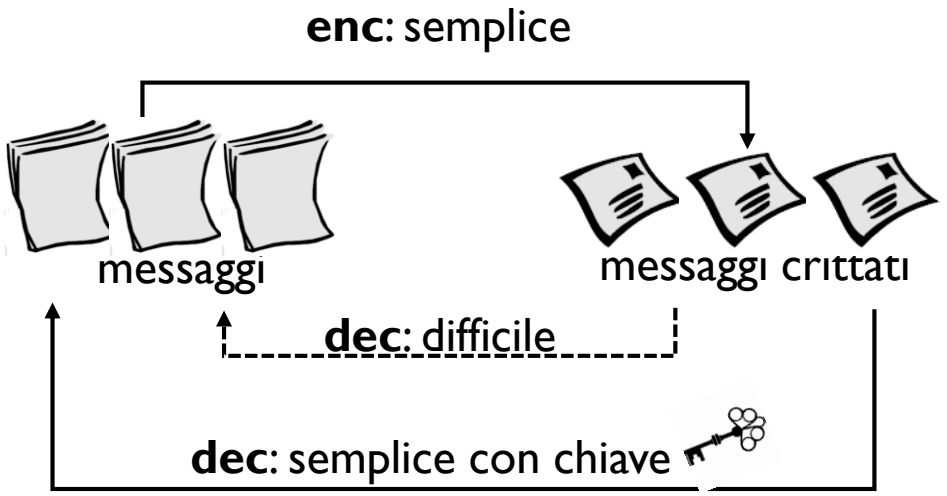
Protocolli

Sistema

Aritmetica modulare

Linguaggio hardware

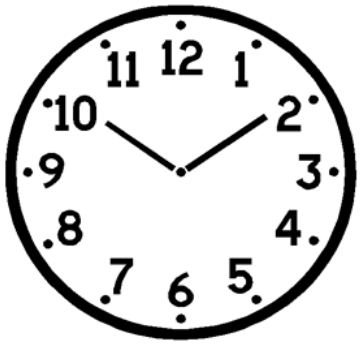
Riscriviamo il problema in "matematichese"



Idea: funzioni unidirezionali con botola

1. Fattorizzazione di interi
2. Logaritmo discreto
3. Logaritmo discreto su curve ellittiche

Consapevolezza tecnica



- Protocolli
- Sistema
- **Aritmetica modulare**
- Linguaggio hardware

(Ri)impariamo a contare in (GF(5) , + , *)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

−	0	1	2	3	4
0	0	4	3	2	1
1	1	0	4	3	2
2	2	1	0	4	3
3	3	2	1	0	4
4	4	3	2	1	0

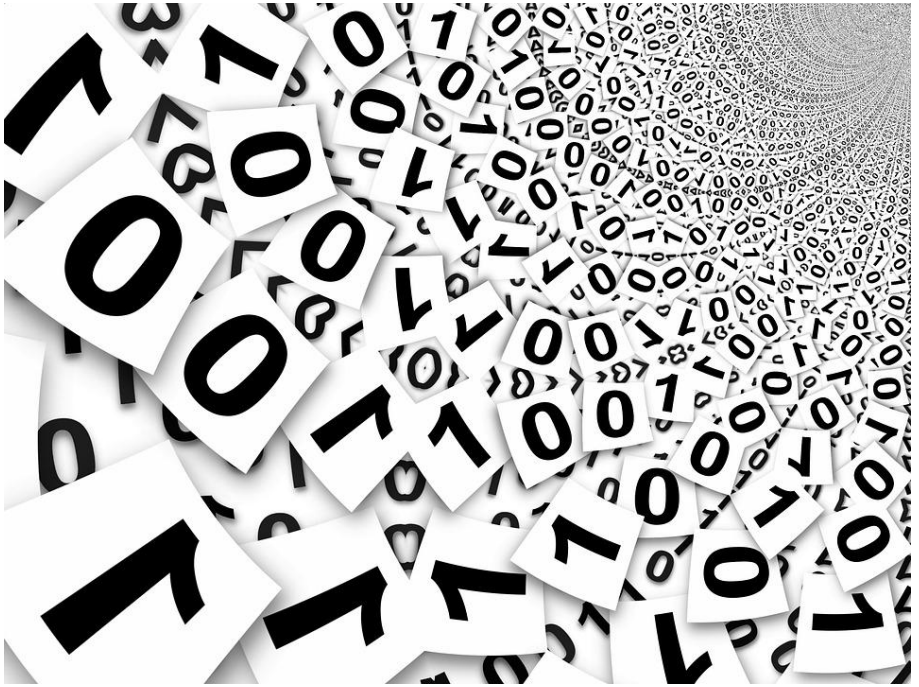
*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

/	1	2	3	4
1	1	3	2	4
2	2	1	4	3
3	3	4	1	2
4	4	2	3	1

Connessione con la realtà

- Protocolli
- Sistema
- Aritmetica modulare
- **Linguaggio hardware**

Affrontiamo il problema della rappresentazione



Sintesi della soluzione

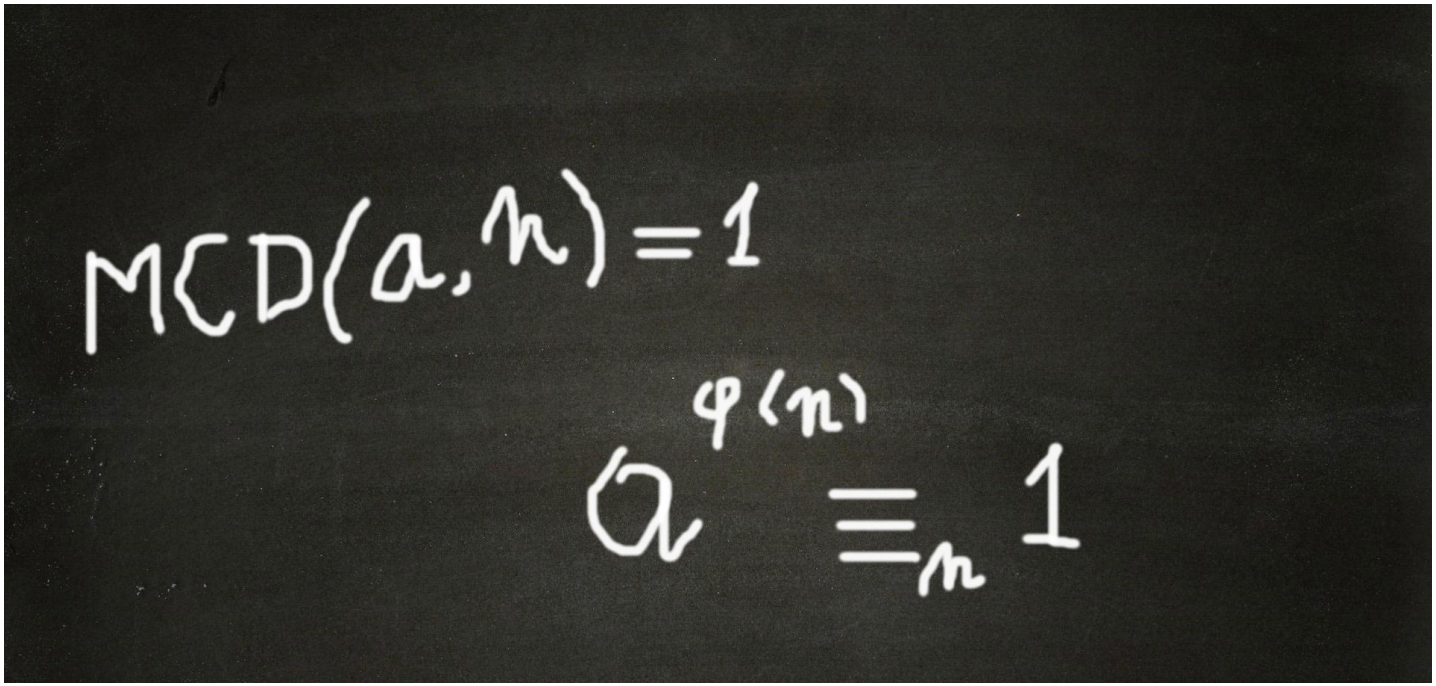
1. Sceglie due interi p, q e calcola
   $n = p*q$
2. Definisce la coppia di chiavi
   $k_p = (n, e)$ e $k_s = d$ (t.c. $e*d \equiv_{\varphi(n)} 1$)

3. Invia la chiave $k_p = (n, e)$

4. Preleva la chiave $k_p = (n, e)$
5. Rappresenta il messaggio m in GF(n)
6. Calcola c := **enc**(m)
   $c = m^e \bmod n$
7. Invia c

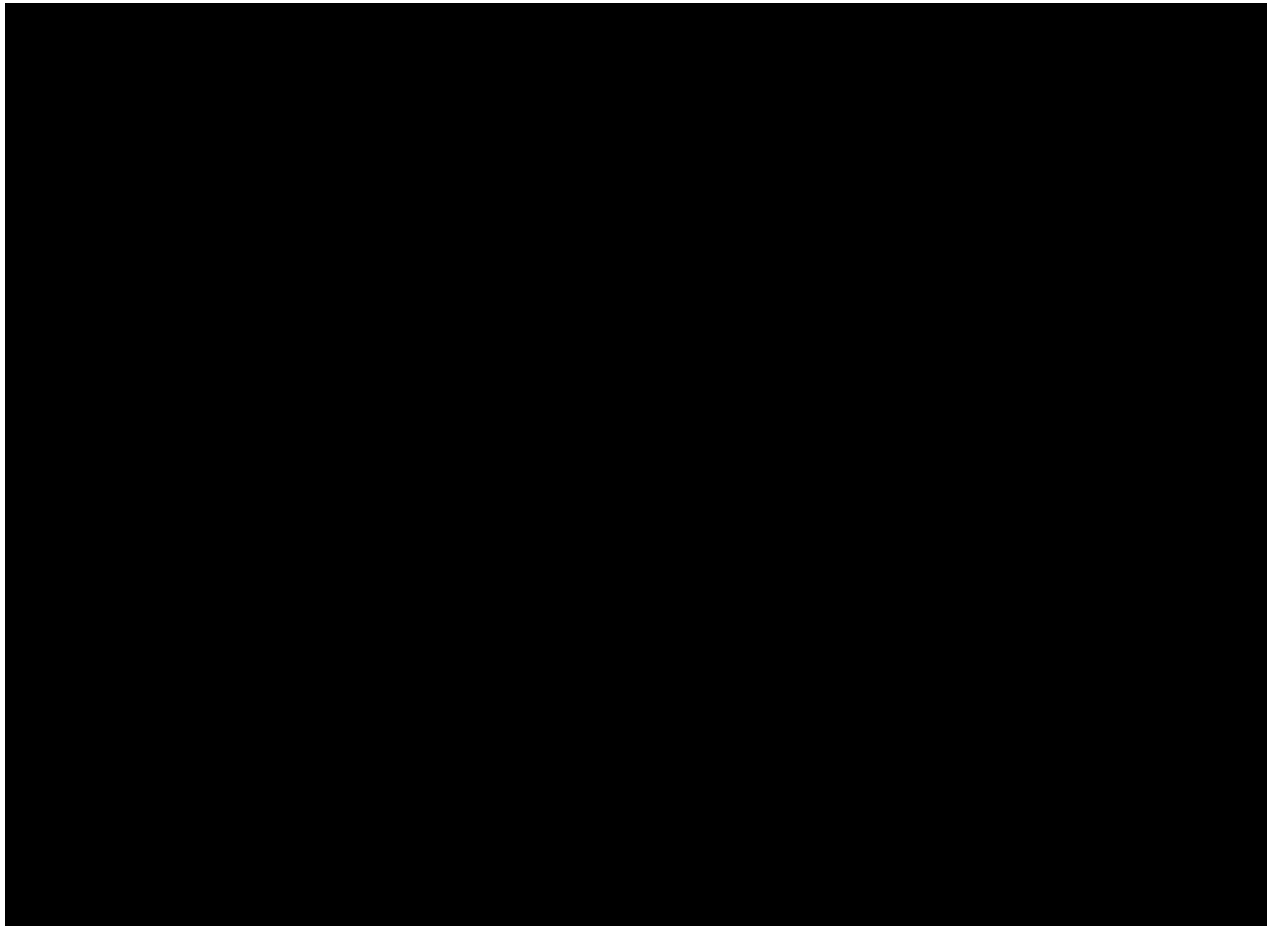
8. Preleva il messaggio cifrato c
9. Calcola **dec**(c)
   $c^d \equiv_n m^{ed} \equiv_n m^{k*\varphi(n)+1} \equiv_n m$

Dimostrazione del teorema di Eulero

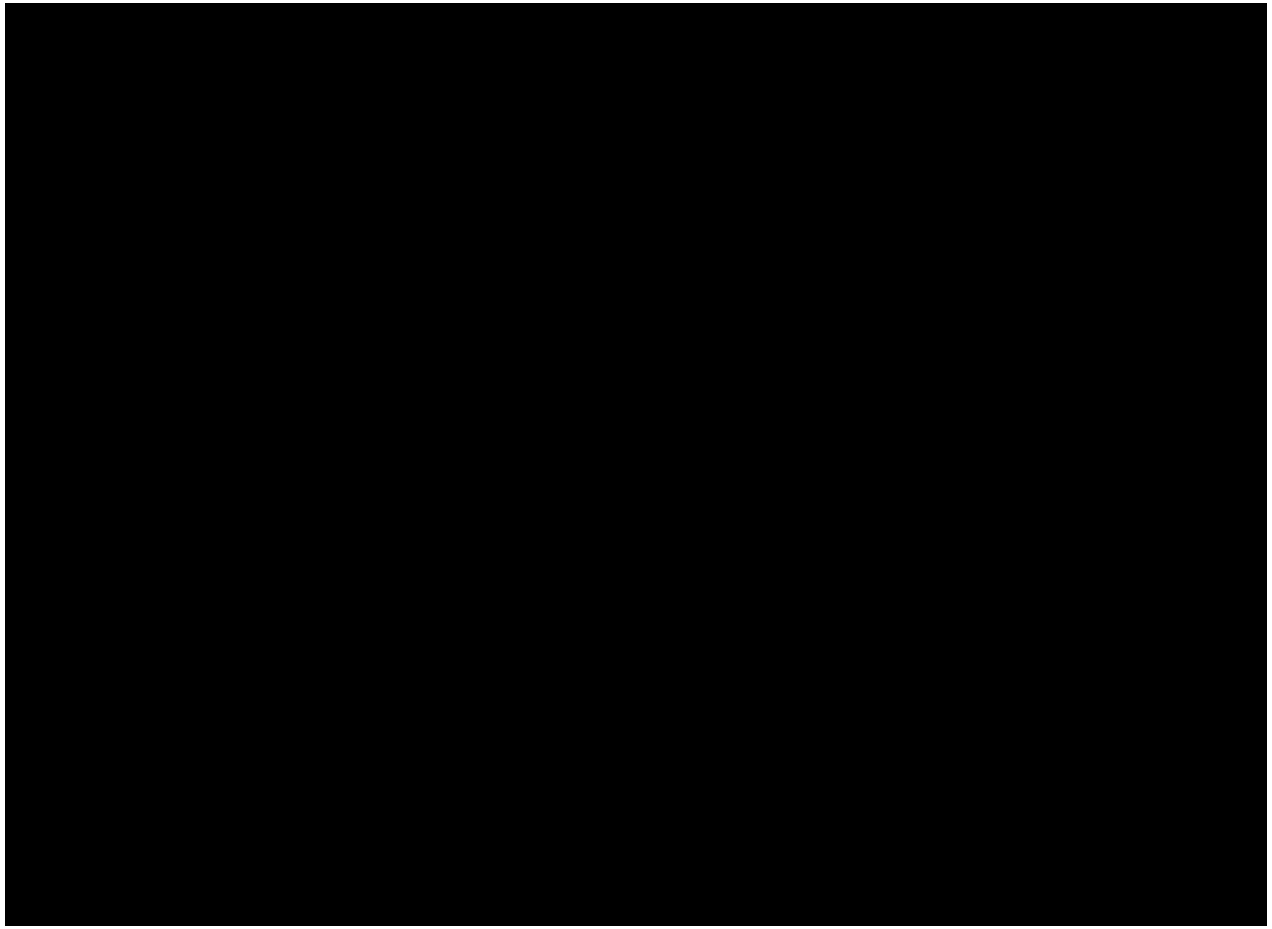


(unico momento di lezione frontale)

Arte della restituzione



Arte della restituzione



Arte della restituzione