Algoritmo euclideo esteso

$(a, b) \rightarrow \quad \alpha a + \beta b = MCD(a, b)$

N.B Se abbiamo una soluzione ne troviamo infinite.

$$(\alpha + kb)\, a + (\beta - ka)\, b = \alpha a + \beta b$$

se (α, β) soluzione $\Rightarrow (\alpha + kb,\ \beta - ka)$ soluzione $\forall k$

N.B: Se (α, β) e $(\bar{\alpha}, \bar{\beta})$ soluzioni di $ax + by = MCD(a,b)$

$\Rightarrow (\alpha - \bar{\alpha},\ \beta - \bar{\beta})$ è soluzione di $ax + by = 0$

$\Rightarrow a(\alpha - \bar{\alpha}) + b(\beta - \bar{\beta}) = 0$

$b \mid \alpha - \bar{\alpha} \Rightarrow \bar{\alpha} = kb + \alpha$
$a \mid \beta - \bar{\beta} \Rightarrow \bar{\beta} = ha + \beta$ ma sostituendo

si vede che deve essere $h = -k$ $\square$

$$MCD(a, b) \leq \min(|a|, |b|)$$

$\Rightarrow$ in $\alpha a + \beta b = MCD(a, b)$ abbiamo $\alpha\beta \leq 0$

```
function my_xgcd(x,y)
    local U=[oneunit(x),zero(x),x]
    local V=[zero(y),oneunit(y),y]
    while V[3]!=zero(x)
        q=U[3]÷V[3]
        U,V=V,U-V*q
        @show U,V
    end
    U
end
```

$(1 \; 0 \; x)$

$(0 \; 1 \; y)$

q = quoziente di u_3 / v_3

$u \leftarrow V, \quad V \leftarrow u - V \cdot q$

$V_3 \leftarrow u_3 \,\%\, v_3$

$x, y = y, x$

$y < x \qquad (x, y) \Rightarrow (y, x \,\%\, y)$

$u = (u_1 \; u_2 \; u_3)$

$v = (v_1 \; v_2 \; v_3)$

$u_1 x + u_2 y = u_3$

$v_1 x + v_2 y = v_3$

sempre

STEP 1

$1 \cdot x + 0 \cdot y = x$

$0 \cdot x + 1 \cdot y = y$

$u^i = (\alpha_i \; \beta_i \; u_3^i)$

$v^i = (\gamma_i \; \delta_i \; v_3^i)$

e supponiamo

$\alpha_i x + \beta_i y = u_3^i$

$\gamma_i x + \delta_i y = v_3^i$

STEP FINALE

$\alpha \cdot x + \beta \cdot y = \boxed{MCD(x,y)}$

$u^{i+1} = v^i = (\gamma_i \; \delta_i \; v_3^i)$ ✓

$v^{i+1} = u^i - v^i (u_3^i \div v_3^i) = q$

$= (\alpha_i - q\gamma_i, \; \beta_i - q\delta_i, \; u_3^i - q v_3^i)$

$x(\alpha_i - q\gamma_i) + y(\beta_i - q\delta_i) = u_3^i - q v_3^i$

$(\alpha_i x + \beta_i y) - q(\gamma_i x + \delta_i y) =$

$= u_3^i - q v_3^i$ ok

L'algoritmo euclideo esteso è efficiente e corretto

Risolvere esplicitamente una eq. del tipo

$$ax + by = c \qquad (*)$$

negli interi.

1) $(*)$ è compatibile $\Leftrightarrow$ $MCD(a,b) \mid c$

2) Se $(*)$ è compatibile sia $S = MCD(a,b)$ $c = c'S$

→ Risolviamo $a\bar{x} + b\bar{y} = S$ $(*')$ con alg. euclideo esteso. → (x', y') la soluzione trovata

→ Troviamo una soluzione particolare

$$(x'', y'') = c'(x', y') \text{ di } (*)$$

→ Osserviamo che $\forall$ soluzione (α, β) di

$$ax + by = c$$

si scrive come soluzione part. calcolata dell'eq.

+ soluzione della eq. omogenea associata

$$ax + by = 0$$

→ $\forall$ soluzione è del tipo $(x'' + kb, y'' - ka)$

$k \in \mathbb{Z}$

□

$(\mathbb{Z}_n, \cdot)$

$[a] \in \mathbb{Z}_n$ quando $\exists [\beta] \in \mathbb{Z}_n$ tale che $[a] \cdot [\beta] = [1]$?

$\Leftrightarrow MCD(a,n)=1$

prodotto fra classi di resto

$$[a]_n \cdot [\beta]_n := [a\beta]_n$$

$q \in [a] \Rightarrow q = a + k_n$

$b \in [\beta] \Rightarrow b = \beta + hn \Rightarrow q \cdot b = (a+kn)(\beta+hn) =$

$= a\beta + n(k\beta + khn + ha)$

$\in [a\beta]$.

N.B $[a]\cdot[1] = [a]$ el neutro

$[a][\beta] = [\beta][a] = [\beta a]$ comm.

$([a]\cdot[\beta])[\gamma] = ([a\beta]\cdot[\gamma]) = [(a\beta)\gamma] =$

$= [a(\beta\gamma)] = [a]\cdot([\beta]\cdot[\gamma])$ ass.

Quando c'è l'inverso??

$n=2$ $[2]$ — $[1] = [1]$

$[2] = [0]$

$[3] = [2] = [6]$

$[0] = [0]$

$[a]\cdot[\beta] = [1] \Leftrightarrow a\beta \in [1] \Leftrightarrow$

$\Leftrightarrow a\beta = 1 + kn \Leftrightarrow$

$\Leftrightarrow a\beta - kn = 1$

ammette sol. date a ed n $\Leftrightarrow MCD(a,n)=1$ ed allora

il β dato dall'alg. euclideo esteso corrisponde proprio all'

classe inversa di $[a]$

$$\mathbb{Z}_n^* := \{ [a]_n \in \mathbb{Z}_n \mid \exists \beta : [a \cdot \beta] = 1 \} =$$

$$= \{ [a]_n \mid MCD(a,n) = 1 \}$$

OSS. $(\mathbb{Z}_n^*, \cdot)$ è un gruppo abeliano.

Si pone $\varphi(n) := |\mathbb{Z}_n^*|$

↓ funzione phi di Eulero.

Caso particolare $n = p$ numero primo.

$$\rightarrow \mathbb{Z}_p^* = \{ [a] \mid MCD(a,p) = 1 \} =$$

$$= \mathbb{Z}_p \setminus \{[0]\}.$$

ma allora $(\mathbb{Z}_p, +, \cdot)$ è un campo!

1) $(\mathbb{Z}_p, +)$ gruppo commutativo

2) $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ gruppo commutativo

$$([a] + [\beta]) \cdot [\gamma] = [a+\beta] \cdot [\gamma] =$$

$$= [(a+\beta)\gamma] = [a\gamma + \beta\gamma] =$$

$$= [a\gamma] + [\beta\gamma] = [a][\gamma] + [\beta][\gamma]$$

Esempi $\mathbb{F}_2 = \mathbb{Z}_2$

pongo $\mathbb{F}_p := \mathbb{Z}_p$ con p primo

$\mathbb{F}_3 = \mathbb{Z}_3$ $\quad$ $\mathbb{F}_{11} = \mathbb{Z}_{11}$

Teorema: Il gruppo moltiplicativo $\mathbb{F}^*$ di un campo finito $\mathbb{F}$ è ciclico di ordine $(p-1)$.

commento: Anche in $\mathbb{Z}_p^*$ con p "abbastanza grande" DLOG è difficile. $\quad \downarrow \; p \simeq 2^{200}$

Lemma: Sia G gruppo abeliano $\alpha, \beta \in G$ con $o(\alpha) = a$, $o(\beta) = b$ e $MCD(a,b) = 1$. Allora $o(\alpha\beta) = a \cdot b$.

DIM

$$(\alpha\beta)^{ab} = \alpha^{ab}\beta^{ab} = (\alpha^a)^b (\beta^b)^a = 1 \cdot 1 = 1$$

$$\Rightarrow \; o(\alpha\beta) \mid ab$$

supponiamo $\exists c$ tale che $1 \leq c < ab$ con

$$(\alpha\beta)^c = 1 \qquad (\alpha\beta)^c = \alpha^c \beta^c = 1$$

$$\Rightarrow \; \alpha^c = \beta^{-c} \Rightarrow o(\alpha^c) \mid a \qquad o(\alpha^c) = o(\beta^{-c}) \mid b$$

Ma allora $o(\alpha^c) \mid MCD(a,b) = 1 \Rightarrow \alpha^c = 1 = \beta^{-c}$

$\Rightarrow a \mid c$ e $b \mid c \Rightarrow ab \mid o(\alpha\beta) = c$ ↯ perché $c < ab$

$\Rightarrow o(\alpha\beta) = ab$.

DIM (Teorema). Sia $\alpha \in \mathbb{F}^*$ con $|\mathbb{F}| = p^n$ con $o(\alpha) = m$ massimo fra tutti i

possibili ordini di elementi di $\mathbb{F}^*$

In particolare $r \mid p^n - 1$

Inoltre $\forall \beta \in \mathbb{F}^*$ abbiamo $o(\beta) \mid r$ perché altrimenti $o(\alpha\beta) > r$ nel senso che

$\exists i : \beta^i$ ha ordine coprimo con r

e dunque $o(\alpha\beta^i) = o(\alpha) \cdot o(\beta^i) = r \cdot o(\beta^i) > r$.

$\Rightarrow \beta^r = 1$ cioè β è radice del polinomio $(x^r - 1)$

In un campo un polinomio di grado r ha al più r radici distinte.

ma $\forall \beta \in \mathbb{F} \setminus \{0\}$ è radice di $(x^r - 1)$

$\Rightarrow$ deve essere $r \geq p^n - 1$ & $r \mid p^n - 1$

$\Rightarrow r = p^n - 1$

e dunque $\exists \alpha \in \mathbb{F}^*$ con

$o(\alpha) = |\mathbb{F}^*| \Rightarrow \mathbb{F}^* = \langle \alpha \rangle$ □

Un $\alpha \in \mathbb{F}$ tale che $\langle \alpha \rangle = \mathbb{F}^*$ è detto elemento primitivo di $\mathbb{F}$.

NB: $|\mathbb{F}|$ potenza di primo $|\mathbb{F}^*|$ no!!

$\mathbb{Z}_p \to p$ tali che $p-1$ abbia almeno un fattore primo grande

□

DH → "sicuri" usando STS + $\mathbb{Z}_p^*$ come gruppo ciclico con $p > 8^{309}$

N.B: in $\mathbb{Z}_p^*$ le operazioni di prodotto ed inverso sono "veloci".

CRITTOSISTEMA A CHIAVE PUBBLICA (El Gamal)

$G = \langle g \rangle$

gruppo ciclico in cui DLOG È DIFFICILE

ALICE

$m \in G$

BOB

$\beta \in \mathbb{N}$ chiave privata.

$b = g^\beta$ chiave pubblica

b NOTO A TUTTI

$k \in \mathbb{N}$ nonce.

$(x, y) = (g^k, b^k m)$ ⟶ (x, y)

calcola $x^{-\beta} \cdot y =$

$= g^{-k\beta} \cdot g^{\beta k} m = m$

OSSERVIAMO CHE DA y NON È POSSIBILE RICAVARE ALCUNA INFORMAZIONE SU m

$y = b^k m = h m$ con $h \in G$.

$\forall m' \in G$; $m' = m' y^{-1} y$ quindi: "decrittando y" con le chiave $(m' y^{-1})$ voi ottenete m'

Sulla "seconda componente" El Gamal sarebbe un cryptosistema perfetto nel senso che EVE che intercetta il messaggio non acquisisce alcuna informazione su quale $m \in G$ ALICE voleva codificare perché $\forall m' \in G \ \exists$ almeno una "chiave" h che codifica m' come $y \to h = (m')^{-1} y$

D'altra canto ALICE risolvente anche la prima componente $\Rightarrow$ il cryptosistema non è perfetto.

OSS II: Se EVE SA RISOLVERE DLOG $\Rightarrow$ SA FORZARE EL GAMAL

Eve : $(x, y) \to (g^k, y)$ e trova $k \to$ calcola $(b^k)^{-1}$

$(b^k)^{-1} y = b^{-k}(b^k m) = m.$

Proprietà importanti

1) Un messaggio può essere codificato in più modi differenti:

$m \lessdot (g^k, b^k m)$
$(g^h, b^h m)$

2) El Gamal è omomorfico nel senso che se

$m \longmapsto (x, y) = (g^k, b^k m)$
$n \longrightarrow (x' y') = (g^h, b^h n)$
$\Big\rangle (\bar{x}, \bar{y}) = (xx', yy') =$
$= (g^{h+k}, b^{h+k} mn)$ codifica di mn.