CRITERIO DI ESISTENZA DI SOLUZIONI PER CONGRUENZE DI PRIMO GRADO: TEST DI PRIMALITÁ

TEOREMA

Se il modulo m è un numero primo tutte le classi di resto di $\mathbb{Z}_m$ sono invertibili. Tale anche l'inverso!

Ponendo $m = 2k+1$ si ha:

$$\mathbb{Z}_{m=2k+1} = \left\{ [0]_{2k+1}, [1]_{2k+1}, \dots, [2k]_{2k+1} \right\}$$

Se tutte le classi di resto di $\mathbb{Z}_{2k+1}$ sono invertibili per opportuni valori di $K \Rightarrow 2k+1 = m$ è primo!!! Si deve imporre che tutte le classi di resto siano invertibili ossia:

$$\begin{cases} [\overline{1 \cdot x_1}]_{2k+1} = [\overline{1}]_{2k+1} \\ [\overline{2 \cdot x_2}]_{2k+1} = [\overline{1}]_{2k+1} \\ \vdots \\ [\overline{2k\, x_{2k}}]_{2k+1} = [\overline{1}]_{2k+1} \end{cases} \quad (1)$$

Si deve imporre che:

$$(1 \text{ ---- } 2k) \cdot x_{2k} \;\Big|\; \frac{2k+1}{(q_1 \text{ --- } q_{2k})}$$

$r=1$

da (1) e dalla divisione fatta accanto si ottiene:

$$\begin{cases} i\,x_i - (2k+1)\,q_i = 1 \\ \vdots \\ 2k\,x_{2k} - (2k+1)\,q_{2k} = 1 \end{cases}$$

$\Rightarrow$

$MCD(i, 2k+1) = 1$

$MCD(i+1, 2k+1) = 1$

$MCD(2k, 2k+1) = 1$

(2)

↓

fino a k e poi ~~fino~~ poco

scorrere i da 1 a $2k$

VERIFICA DEL SISTEMA (2) CON UN NUMERO PRIMO E DI UN NUMERO NON PRIMO:

$k=6,\ m=2k+1=13$

$k=4,\ m=2k+1=9$

$MCD(1,13)=1$
$MCD(2,13)=1$
$MCD(3,13)=1$
$=\ (4,13)=1$
$=\ (5,13)=1$
$=\ (6,13)=1$
$=\ (7,13)=1$
$=\ (8,13)=1$
$=\ (9,13)=1$
$=\ (10,13)=1$
$=\ (11,13)=1$
$MCD(12,13)=1$

$MCD(1,9)=1$
$MCD(2,9)=1$
$MCD(3,9)=3$
$MCD(4,9)=1$
$MCD(5,9)=1$
$MCD(6,9)=3$
$MCD(7,9)=1$
$MCD(8,9)=1$

VORREI SAPERE SE IL TEST COSÍ RICAVATO IN CUI FISSATO K SI DEVE PROCEDERE A VERIFICARE ~~OPPURE~~ IN EQ. CON L'ALGORITMO DI EUCLIDE È ~~VANTAGGIOSO~~ ITERATIVAMENTE ~~SIMILE AL~~ VANTAGGIOSO RISPETTO ~~AL~~ LIVELLO ~~RISPETTO AL VERIFICARE LIVELLO~~ ~~DI ERADO~~ SE AVENDO ~~AVENDO~~ ALTRI TEST

N.B. ~~IL MCD TRA UN DISPARI E UN PARI È SEMPRE 1~~

Secondo voi l'algoritmo presentato è computazionalmente meglio degli altri testati precedentemente? Si può semplificare?

N.B.

Comunque sia con un programma che fa l'algoritmo di Euclide si può testare come vanno le cose!!!