

# Metodo Euclide esteso per il calcolo di $d$

Calcolo di  $d$  tale che  $de \equiv 1 \pmod{(p-1)(q-1)}$

*Definizione*

Colonna 1	Colonna 2	Colonna 3
<b>dividendo</b>	0	
<b>divisore</b>	1	<b>quoziente intero</b> della divisione tra dividendo e divisore
<b>resto</b> della divisione tra dividendo e divisore	0 - 1 * c	...
...	...	

*Passi successivi*

Colonna 1	Colonna 2	Colonna 3
<b>dividendo</b>	0	
<b>divisore</b>	1	<b>quoziente intero</b> della divisione tra dividendo e divisore della colonna 1
<b>resto</b> della divisione tra dividendo e divisore della colonna 1	0 - 1 * c	<b>quoziente intero</b> della divisione tra divisore e resto della colonna 1
<b>resto</b> della divisione tra divisore e resto precedenti della colonna 1	come prima operando sulle due celle precedenti della colonna 2	<b>quoziente intero</b> della divisione tra resto precedente e resto di questa riga della colonna 1
<b>resto</b> della divisione tra resto e resto precedenti della colonna 1	come prima operando sulle due celle precedenti della colonna 2	...
...	...	
<b>1</b> (se il risultato in questa colonna è 1 allora ci si ferma)	<b>d</b> ( questo sarà il d cercato) se d è negativo occorre sommare il mod indicato nell'espressione di $de \equiv 1 \pmod{(p-1)(q-1)}$ cioè $(p-1)(q-1)$	

Applichiamo quanto sopra ai seguenti dati:

$p = 3; q = 11; e = 7$   
 dividendo =  $(p-1)(q-1)$   
 divisore =  $e$

Colonna 1	Colonna 2	Colonna 3
20	0	
7	1	$c = 2$
6	-2	$c = 1$
1	3	

Quindi  $d = 3$ .

All'indirizzo <http://apuntionline.eu> in VARIE si trova il calcolo di  $d$  in js (realizzato da Capuano) e RSA.xlsx