Metodo Euclide esteso per il calcolo di *d*

Calcolo di **d** tale che **d**e ≡ 1 mod(p-1)(q-1)

Definizione

Colonna 1	*Colonna 2*	*Colonna 3*
dividendo	0	
divisore	1	**quoziente intero** della divisione tra dividendo e divisore
resto della divisione tra dividendo e divisore	0 - 1 * c	…
…	…	

Passi successivi

Colonna 1	*Colonna 2*	*Colonna 3*
dividendo	0	
divisore	1	**quoziente intero** della divisione tra dividendo e divisore della colonna 1
resto della divisione tra dividendo e divisore della colonna 1	0 - 1 * c	**quoziente intero** della divisione tra divisore e resto della colonna 1
resto della divisione tra divisore e resto precedenti della colonna 1	come prima operando sulle due celle precedenti della colonna 2	**quoziente intero** della divisione tra resto precedente e resto di questa riga della colonna 1
resto della divisione tra resto e resto precedenti della colonna 1	come prima operando sulle due celle precedenti della colonna 2	**…**
…	…	
1 (se il risultato in questa colonna è 1 allora ci si ferma)	**d** (questo sarà il d cercato) se d è negativo occorre sommare il mod indicato nell'espressione di de ≡ 1 mod(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