Altro metodo per il calcolo di *d*

su un intervento di Jaume Bernardi e Mattia Moro

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

Ricordando che

dividendo / divisore = quoziente e resto
16 / 5 = 3 e 1

dividendo = divisore * quoziente + resto
16 = 5 * 3 + 1

divisore = (dividendo – resto) / quoziente
5 = (16 -1) / 3

Definizione

de ≡ 1 mod(p-1)(q-1)

de mod(p-1)(q-1) = 1 mod(p-1)(q-1)

de mod (p-1)(q-1) = 1

dividendo mod divisore = 1

dividendo = divisore * quoziente + resto

de = (p-1)(q-1) * ?quoziente + 1

d = ((p-1)(q-1) * ?quoziente + 1) / e

a questo punto, se trovo un ?quoziente che mi fa risultare d un intero, ho calcolato **d**.

Applichiamo quanto sopra ai seguenti dati:

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

d = ((p-1)(q-1) * ?quoziente + 1) / e

Proviamo per ?quoziente = 1
d = (20 * 1 + 1) / 7 = 21 / 7 = 3