Tavola n. 5.5 Il Teorema di Eulero

21 = 3 • 7 è prodotto di due primi distinti $p = 3$ e $q = 7$.

Osserviamo che $p-1 = 2$ e $q-1 = 6$.

Considera gli interi a con $1<a<21$ e MCD(a, 21)=1

a	$a^{p-1} = a^2$	$a^{p-1} - 1 = a^2 - 1$ divisibile per $p=3$?	$a^{p-1} = a^2$ in Z_{21}	$a^{(p-1)(q-1)} = (a^2)^6$ in Z_{21}
2	2 • 2 =4			
4	4 • 4 = 16			
5	5 • 5 = 25			
8	8 • 8 = 64			
10	10 •10 = 100			
11	11•11 =121			
13	13 • 13 =169			
16	16 • 16 = 256			
17	17 • 17 =289			
19	19 • 19 =361			
20	20 • 20 = 400			