



## Tavola n. 5.5 Soluzioni Il Teorema di Eulero

$21 = 3 \cdot 7$  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  $\text{MCD}(a, 21) = 1$

$a$	$a^{p-1} = a^2$	$a^{p-1} - 1 =$ $a^2 - 1$	divisibile per $p=3$ ?	$a^{p-1} = a^2$ in $Z_{21}$	$a^{(p-1)(q-1)}$ $= (a^2)^6$ in $Z_{21}$
2	$2 \cdot 2 = 4$	3	si	4	1
4	$4 \cdot 4 = 16$	15		16	1
5	$5 \cdot 5 = 25$	24		4	1
8	$8 \cdot 8 = 64$	63		1	1
10	$10 \cdot 10 = 100$	99		16	1
11	$11 \cdot 11 = 121$	120		16	1
13	$13 \cdot 13 = 169$	168		1	1
16	$16 \cdot 16 =$ 256	255		4	1
17	$17 \cdot 17 = 289$	288		16	1
19	$19 \cdot 19 = 361$	360		4	1
20	$20 \cdot 20 =$ 400	399		1	1