

Alessandro Languasco & Alessandro Zaccagnini  
 Corrigenda per “Crittografia”  
 Progetto Lauree Scientifiche (2006)

Se il numero della riga è negativo si intende che deve essere contata dal basso.

Pag.	riga.	Errata	Corrige
10.	-6.	... intero positivo ...	... intero $n \geq 2$ ...
19.	-7.	547	1547
21.	16.	$b = -58$	$v = -58$
30.	-10.	Dimostrazione della Proposizione 1.8	si veda sotto
37.	2.	... famosi pirata ...	... famosi pirati ...
44.	-12.	... Enigma. Esse ...	... Enigma. Essa ...
79.	2.	elemento	elemento non nullo

**Proposizione 1.8** *Sia  $n$  privo di quadrati e  $d, e$  tali che  $\varphi(n) | (de - 1)$ . Allora*

$$a^{de} \equiv a \pmod{n} \quad \text{per ogni } a \in \mathbb{Z}_n.$$

**Dim.** Il fatto che  $n$  sia privo di quadrati significa che  $n = \prod_i p_i$  e  $p_i \neq p_j$  per  $i \neq j$ . Allora l'ipotesi  $\varphi(n) | (ed - 1)$  equivale a  $(p_i - 1) | (ed - 1)$  per ogni  $p_i | n$ . Quindi, per la forma forte del Piccolo Teorema di Fermat 1.7, otteniamo

$$a^{de-1} \equiv a^{(p_i-1)k_i} \equiv \left(a^{(p_i-1)}\right)^{k_i} \equiv 1^{k_i} \equiv 1 \pmod{p_i}$$

per ogni  $p_i | n$ ,  $a \in \mathbb{Z}_n^*$ . Inoltre è chiaro che, se  $p_i | a$ , si ha che  $a^{de} \equiv a \pmod{p_i}$ . Possiamo quindi concludere che  $a^{de} \equiv a \pmod{p_i}$  per ogni  $p_i | n$ ,  $a \in \mathbb{Z}_n$ . Applicando il Teorema Cinese del Resto 1.5, segue che esiste una unica soluzione modulo  $n$  del sistema di congruenze  $x \equiv a \pmod{p_i}$  per ogni  $p_i | n$ . Otteniamo allora che  $a^{de}$  è l'unica soluzione cercata e quindi  $a^{de} \equiv a \pmod{n}$  per ogni  $a \in \mathbb{Z}_n$ .  $\square$