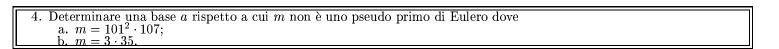
1.	Mostrare ch	e 825265 =	$5 \cdot 7$	· 17 ·	19 · 73 è un	numero di	Carmichael

2. Si calcoli il seguente simbolo di Jacobi (senza fattorizzare!)

3. Sia m in intero positivo disparie composto. Sia

$$C(m) = \{a \in U(\mathbf{Z}/m\mathbf{Z}) \mid m \text{ e}' \text{ uno pseudo primo in base } a\}.$$

- a. Mostrare che C(m) è un gruppo; b. Dimostrare che se esiste una base rispetto a cui m non è uno pseudo primo allora ne esistono almeno  $\varphi(m)/2$ ; c. Mostrare che  $|C(m)| \geq 2$ . d. Calcolare C(15).



5. (Quickies): Scrivere solo la risposta delle seguenti domande:
i. Quale è la probabilità che 50 iterazioni di Solovay-Strasen dichiarino primo un numero composto?
ii Dire quali dei seguenti numero sono basi rispetto a cui 25 è uno pseudo primo Euleriano: 1, -1, 2, 5, 7, 10, 3

i. ii. bigskip