(1) Dato che il numero n é privo di fattori quadratici, si tratta di verificare che, per ciascun primo p che divide n, si ha che $p-1|n-1$.

(2) Si tratta di applicare ripetutamente la legge di reciprocitá quadratica, ogni volta operando una riduzione della parte superiore modulo la parte inferiore del simbolo di Jacobi, e poi liberandosi di volta in volta delle potenze di 2 che dividono la parte in alto.

(3) In effetti, $C(m)$ é un sottogruppo di $U(\mathbb{Z}/m\mathbb{Z})$. Per provare il punto a. basta vedere che $C(m)$ é chiuso per il prodotto, il che é immediato. Inoltre, per il teorema di Lagrange sui gruppi finiti, $C(m)|U(\mathbb{Z}/m\mathbb{Z})=\varphi(m)$. Pertanto, se $C(m)$ é sottogruppo proprio di $U(\mathbb{Z}/m\mathbb{Z})$, allora $C(m)\leqslant\varphi(m)/2$. Questo prova b. Per la parte c. basta osservare che 1 e -1 sono comunque in $C(m)$. Infine, $C(15)=\{1,4,11,14\}$.

(4) Per la parte a. basta prendere il numero $1+101\cdot 107$. Per la parte b, risolvere il sistema di congruenze:

$$\begin{cases} x=2 \pmod 3 \\ x=1 \pmod{35} \end{cases}$$

(5) *quickies*

i. Se un numero ćomposto, la probabilitá che superi un test di Solovay-Strasen é non maggiore di $1/2$, dato che esistono sempre basi per le quali il numero non é pseudo-primo di Eulero, e moltiplicando una base che permette il superamento del test con una che non lo permette, si trova un numero rispetto al quale il numero dato non é pseudo-primo di Eulero. Quindi la probabilitá richiesta ńon maggiore di $1/2^{30}$.

ii. Sono: $1,-1,7$. Si tratta solo di applicare la definizione.