(1)

(2) Se $m = 3 \pmod 4$, allora $(m-1)/2$ é dispari. Dunque, é sufficiente vedere che $a^{(m-1)/2} = \pm 1 \pmod m$, il che é ovvio dalla definizione di pseudo-primo di Eulero.

(3) Applicando il teorema di Pocklington-Lucas si ottiene immediatamente la conclusione. Un altra possibilitá é quella di ragionare sulla cardinalitá sul gruppo delle unitá di $\mathbb{Z}/(2q+1)\mathbb{Z}$ (in questo modo non ńecessario utilizzare una delle ipotesi).

(4) i. Le soluzioni sono quattro, ovvero $8, 18, 47, 57$ (o anche $\pm 8, \pm 18$), per il teorema cinese del resto.

ii. Dato che $65 - 1$ é una potenza di 2, 65 é pseudo-primo forte in ciascuna delle quattro basi trovate al punto i. Tuttavia, se prendiamo come a_1 e a_2 due di queste quattro basi (evitando di usare 8 e -8 oppure 18 e -18 !), il prodotto $a_1 \cdot a_2$ non é pseudo-primo forte.

iii. Oltre a quelle banali 1 e -1, quelle trovate al punto i. sono le uniche basi rispetto alle quali 65 é pseudo-primo forte. Infatti $65 - 1$ é potenza di 2, se avessimo una ulteriore base siffatta, allora, dopo aver effettuato un certo numero di elevamenti al quadrato successivi a partire da tale base, dovremmo imbatterci in uno dei quattro numeri sopra trovati, che sono gli unici il cui quadrato é $-1 \pmod{65}$. Ma nessuno di quei quattro numeri é un quadrato, quindi non vi sono altre basi rispetto alle quali 65 é uno pseudo-primo forte. Pertanto $|S(65) = 6|$. Inoltre, osserviamo che, per la parte ii., $S(65)$ non é un gruppo.

(5) *quickies* i. Vedere le definizioni.

ii. Se cerchiamo due fattori non banali non troppo distanti, possiamo prendere in considerazione numeri del tipo $10^5 + x$ e $10^5 + y$, dato che il numero dato é compreso tra 10^{10} e $2 \cdot 10^{10}$. Eseguendo i prodotti si trova che $xy = 57$ e che $x + y = 22$. Pertanto due fattori non banali sono 100019 e 100003.

iii. Si puó ragionare come in ii., con la differenza che il secondo fattore deve essere del tipo $3 \cdot 10^5 + y$, quindi $xy = 21$ e $3x + y = 16$. I due fattori che si trovano in questo modo sono 100003 e 300007.