(1) In base al piccolo teorema di Fermat, per effettuare il calcolo basta conoscere il valore di $b^c \pmod{p-1}$. Questo richiede un numero di operazioni dell'ordine $O(\log c \log^2 p - 1) = O(\log^3 p)$ e fornisce un intero h compreso tra 0 e $p-1$. Per trovare $a^h \pmod p$ sono adesso necessarie ancora $O(\log^3 p)$ operazioni. In tutto, il tempo necesario é dato dalla somma di questi due tempi, che é ancora $O(\log^3 p)$.

(2) Un modulo adatto devecessere prodotto di 2 primi p e q tali che sia $pq > 22^3 = 10648$ e inoltre $p-1$ e $q-1$ non devono essere multipli di 3. Dato che $\sqrt{10648} < 104$, un modo per scegliere i due primi é quello di cercare i due piú piccoli primi maggiori di 104 che rispettino l'altra condizione. Sono adeguati 107 e 113, nel qual caso il modulo é $107 \cdot 113 = 12091$.

(3) In questo algoritmo, si scrive lo sviluppo binario dell'esponente $26 = (11010)_2$. Inoltre, si calcolano i successivi quadrati di 3 (mod 17), ciascuna volta elevando a quadrato il precedente, fino alla potenza di 2 massima contenuta in questo sviluppo (in questo caso si tratta di 2^4). Si trova

$$
\begin{aligned}
3^0 &= 1 \pmod{17}\\
3^1 &= 3 \pmod{17}\\
3^2 &= 9 \pmod{17}\\
3^4 &= 13 \pmod{17}\\
3^8 &= 16 \pmod{17}\\
3^16 &= 1 \pmod{17}.
\end{aligned}
$$

Pensando al significato della rappresentazione binaria di un numero intero, é chiaro che, a questo punto, basta moltiplicare fra di loro tutti i quadrati successivi in corrispondenza delle cifre 1 di questo sviluppo. Pertanto si ha:

$$3^{26} = 3^{2+2^3+2^4} = 9 \cdot 16 \cdot 1 = 8(\text{mod } 17).$$

(4) Sia S la somma vinta da Alvaro, espressa in milioni. Pertanto, abbiamo S intero e $0 < S < 5000$. I dati del problema equivalgono al sistema di congruenze:

$$\begin{cases} S = 6 \pmod 7 \\ S = 2 \pmod{12} \end{cases}$$

Questo sistema ha un'unica soluzione compresa tra 0 e 84 (teorema cinese del resto), che vale 62. Le altre soluzioni sono congrue a 62 modulo 84. In questo modo, la vincita minima é appunto di 62 milioni. La massima si ottiene cercando il piú grande numero minore di 5000 che sia congruo a 62 modulo 84.

(5) *quickies*

i. 2^{2000} íl piú piccolo numero con oltre 2000 cifre. Utilizzando il teorema dei numeri primi, si trova la stima $\frac{2^{2000}}{\log 2^{2000}}$ per il numero di primi minori di 2000. Quindi la probabilitá richiesta é:

$$\frac{1}{2000 \log 2} \approx 0.00072.$$

ii. Dato che $2q+1$ é primo, $\varphi(2q+1) = 2q$. Visto che q é un primo dispari e visto che la φ é moltiplicativa su numeri coprimi, si ha

$$\varphi(2q) = \varphi(2)\,\varphi(q) = 1 \cdot (q-1) = q-1,$$

Typeset by $\mathcal{AMS}$-TEX

dato che q é un numero primo.
iii. L'esponente di cifratura deve essere coprimo con $\varphi(n)$. Dato che $\varphi(43) = 42 = 2 \cdot 3 \cdot 7$ e che $\varphi(331) = 330 = 2 \cdot 3 \cdot 5 \cdot 11$, l'esponente minimo é 13.
iiii. Il fatto che n sia un modulo per RSA significa che esso é il prodotto di due primi dispari p e q. L'equazione $x^2 = 1(\text{mod } m)$ equivale al sistema di congruenze

$$\begin{cases} x^2 = 1 \pmod p \\ x^2 = 1 \pmod q \end{cases}$$

Ciascuna delle due equazioni di questo sistema ha 2 radici in $\mathbb{F}_p$. Combinando tali radici nei 4 modi possibili si ottengono tutte e sole le soluzioni modulo m.