

NAME:

SID:

Problem 1: Below you are given five choices of parameters p, q, e, d of RSA. For each choice tell whether these parameters are correct¹ (write YES/NO). If the parameters are correct, compute the encryption of $M = 3$. If the parameters are incorrect, give a brief explanation why (at most 10 words).

p	q	e	d	correct?	Encrypt $M = 3$ if correct. Justify if not correct.
5	21	7	23		
13	7	5	29		
11	11	9	89		
7	17	11	37		
3	7	5	5		

¹To clarify, correctness refers only to mathematical correctness, namely whether the parameters satisfy the assumptions from the algorithm.

Problem 2: Solve the recurrence equation $Q_n = 2Q_{n-1} + 4Q_{n-2}$, for $Q_0 = 0$, $Q_1 = 2$. Follow the steps below.

(a) Characteristic polynomial and its roots:

(b) General solution:

(c) Equations for initial conditions and its solution:

(d) Final answer: