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 correct[1] (write YES/NO). If not, give a brief justification (at most 10 words).

p	q	e	d	correct?	justify if not correct
3	5	3	3	YES	
13	9	7	55	NO	9 is not prime
13	11	7	103	YES	
17	17	3	171	NO	p and q should be different
11	13	25	37	NO	25 is not relatively prime to $(p-1)(q-1)$

[1] To clarify, correctness refers only to mathematical correctness, namely whether the decryption function is the inverse of the encryption function. This should not be confused with security.

Problem 2: Solve the recurrence equation $T_n = 3T_{n-1} - T_{n-2}$, for $T_0 = 0$, $T_1 = 1$. Follow the steps below.

(a) Characteristic polynomial and its roots:

$$x^2 - 3x + 1 \quad = \quad 0$$

The roots are $r_1 = \frac{1}{2}(3 + \sqrt{5})$ and $r_2 = \frac{1}{2}(3 - \sqrt{5})$.

(b) General solution:

$$T_n \quad = \quad \alpha_1 \cdot \left(\frac{3 + \sqrt{5}}{2} \right)^n + \alpha_2 \cdot \left(\frac{3 - \sqrt{5}}{2} \right)^n$$

(c) Equations for initial conditions and its solution:

$$\begin{aligned} \alpha_1 + \alpha_2 \quad &= \quad 0 \\ \alpha_1 \cdot \tfrac{1}{2}(3 + \sqrt{5}) + \alpha_2 \cdot \tfrac{1}{2}(3 - \sqrt{5}) \quad &= \quad 1 \end{aligned}$$

Solution: $\alpha_1 = 1/\sqrt{5}$, $\alpha_2 = -1/\sqrt{5}$.

(d) Final answer:

$$T_n \quad = \quad \frac{1}{\sqrt{5}} \left(\frac{3 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{3 - \sqrt{5}}{2} \right)^n$$