Problem 1: In the RSA, suppose that Bob chooses $p = 3$ and $q = 43$. (a) Determine three correct values of the public exponent e. Justify briefly their correctness (at most 20 words.)

We have $\phi(n) = (p-1)(q-1) = 2 \cdot 42 = 84$. The value of e should satisfy: $\gcd(e, 84) = 1$. Possible solutions are e.g. $e = 5$, $e = 11$ or $e = 13$.

(b) For one of the e's you selected, compute the secret exponent d. Show your work.

For $e = 5$, we compute $d = 5^{-1} \pmod{84}$. Since $84 + 1 = 5 \cdot 17$, we get $d = 17$.

Problem 2: Grabbits are genetically modified rabbits that live forever and reproduce asexually on a precise schedule: each grabbit gives birth to three grabbits every Wednesday starting two weeks after birth. So if you start with 1 newly born grabbit, after one week you will still only have 1 grabbit. After two weeks you will have 4 grabbits, namely your first grabbit plus its 3 offspring. In general, how many grabbits will you have after n weeks if you start with one newly born grabbit? Set up a recurrence relation for this problem and solve it.

(a) Let G_n be the number of grabbits after n weeks. Then G_n includes the G_{n-1} grabbits that were alive in week $n-1$ plus the newly born grabbits. The number of new grabbits is $3G_{n-2}$, because only the grabbits that were around two weeks earlier can have offspring, and each of them gives birth to 3 grabbits. So the recurrence relation is:

$$\begin{aligned} G_n &= G_{n-1} + 3G_{n-2} \\ G_0 &= 1 \\ G_1 &= 1 \end{aligned}$$

(b) Characteristic polynomial and its roots:

$$x^2 - x - 3 = 0$$

so $x_{1,2} = \frac{1 \pm \sqrt{13}}{2}$.

(c) General form of the solution:

$$G_n = \alpha_1 (\tfrac{1+\sqrt{13}}{2})^n + \alpha_2 (\tfrac{1-\sqrt{13}}{2})^n$$

(d) Initial condition equations:

$$\begin{aligned} \alpha_1 + \alpha_2 &= 1 \\ \alpha_1(\tfrac{1+\sqrt{13}}{2}) + \alpha_2(\tfrac{1-\sqrt{13}}{2}) &= 1 \end{aligned}$$

and their solution:

$$\alpha_1 = \tfrac{1+\sqrt{13}}{2\sqrt{13}} \quad \alpha_2 = \tfrac{-1+\sqrt{13}}{2\sqrt{13}}$$

(e) Final answer: The number of grabbits after n weeks is:

$$\begin{aligned} G_n &= \tfrac{1+\sqrt{13}}{2\sqrt{13}} (\tfrac{1+\sqrt{13}}{2})^n + \tfrac{-1+\sqrt{13}}{2\sqrt{13}} (\tfrac{1-\sqrt{13}}{2})^n \\ &= \tfrac{1}{\sqrt{13}} [(\tfrac{1+\sqrt{13}}{2})^{n+1} - (\tfrac{1-\sqrt{13}}{2})^{n+1}] \end{aligned}$$