Syllabus for CS111 Quiz 3

Topics:

- The RSA
  - Explain the principle of public-key cryptosystems
  - Explain the RSA (initialization, encryption, decryption)
  - Suppose that Bob chooses \( p = 5, q = 11 \). Show some correct values of \( e \) (public exponent) and \( d \) (secret exponent). Give three correct pairs.
  - Bob uses \( P = (143,19) \) as his public key and \( S = 21 \) as his secret key. Is Bob’s system correct?
  - Suppose Bob chooses \( p = 7, q = 13, e = 11 \). Determine \( d \). If Alice wants to send \( M = 10 \) to Bob, what is the ciphertext?

- Fermat’s Theorem. Using the theorem to compute powers and inverses.
- Linear homogeneous recurrences equations
  - Give the recurrence relation for Fibonacci numbers. (Should also be able to prove that \( F_n \) grows exponentially with \( n \).)
  - Setting up recurrence equations.
    - Example: One female rabbit produces 3 female rabbits per week, starting the 2nd week after its born. You receive one newly-born female rabbit for your birthday. How many female rabbits will you have after \( n \) weeks? (These are genetically modified female rabbits that do not need male rabbits for reproduction.)
    - Example: We tile an \( n \)-by-1 strip using 1-by-1, 2-by-1 and 3-by-1 tiles. Let \( t_n \) be the number of such tilings. Give a recurrence for \( t_n \).
    - Example: Modify the last problem by allowing tiles of two colors, say red and green. Give a recurrence for the number of such tilings.
  - Solving linear homogeneous recurrence equations.
    - Example: Solve: \( f_n = 5f_{n-1} - 6f_{n-2} \), with initial conditions \( f_0 = 1, f_1 = 2 \). Show your work.
    - Example: Determine the general solution of the recurrence \( h_n = 5h_{n-1} - 3h_{n-2} - 9h_{n-3} \).
  - Linear non-homogeneous recurrences equations.