Section 1.1

- 1f, 1h, 2b, 2c, 2f, 3b, 13, 14, 17b.
- Let \((x_n)_{n \geq 0}\) be a sequence given recursively as follows.
  1. \(x_0 = x_1 = 1\)
  2. \(x_{n+2} = 5x_{n+1} - 6x_n\), for all \(n \in \mathbb{N}\).

Show by strong induction that

\[x_n = 2^{n+1} - 3^n\], for all \(n \in \mathbb{N}\).

Section 1.2

- 5, 7, 9h, 11, 18, 33, 34, 38, 39, 45
- Show that \(\sqrt{7}\) is not a rational number.

Section 1.3

- 8, 10, 12, 16, 21, 25, 30, 31, 34, 36.

Section 1.4

- 5, 6, 7, 13, 15, 19, 20, 23, 25, 26.
- Let \(\sigma\) be a cycle of length \(k\) in \(S_n\). Show that
  1. \(\sigma^k = \varepsilon\).
  2. \(\sigma^s \neq \varepsilon\), for all integers \(s\) satisfying \(0 < s < k\).

- Let \(\sigma = \tau \cdot \mu\) in \(S_n\), where \(\tau\) and \(\mu\) are disjoint cycles of lengths \(p\) and \(q\) respectively. Let \(k = \text{lcm}(p, q)\). Show that
  1. \(\sigma^k = \varepsilon\).
  2. \(\sigma^s \neq \varepsilon\), for all integers \(s\) satisfying \(0 < s < k\).

Section 1.5

- Assume that Bob’s RSA-Cryptosystem public key is \((n_B = 2329, k_B = 19)\).
  1. Find Bob’s private key \(k_B'\). (Please note that \(2329 = 137 \cdot 17\).)
  2. Use Bob’s public key to encrypt the number formed by the last 3 digits of your SSN.
  3. Choose your own public and private keys and “sign” your message to Bob with the encrypted form of the number formed by the first 3 digits of your SSN, via the Diffie-Hellman signature algorithm.