Exercise 1.

(a) Compute the multiplicative inverse of 357 modulo 1234 (357\(^{-1}\) mod 1234).

(b) A polynomial \(a(x)\) is a multiplicative inverse of \(b(x)\) modulo \(m(x)\) such that 
\(b(x) \cdot a(x) \equiv 1 \mod m(x)\). In \(\mathbb{Z}_2(x)\), where 
\(m(x) = x^5 + x^3 + 1\), compute the multiplicative inverse of \(b(x) = x^3 + x + 1\).

Hint: + is the modulo 2 addition.

Hint: Apply the Extended Euclidean Algorithm (Section 6.3 in the script).

Exercise 2. Let \(a, b, c, d \in \mathbb{Z}\). \(a\) is said to divide \(b\) if (and only if) there exists some \(k \in \mathbb{Z}\) such that \(a \cdot k = b\). Notation: \(a \mid b\). Prove the following implications:

(a) \(a \mid b\) and \(b \mid c\) \(\Rightarrow\) \(a \mid c\).

(b) \(a \mid b\) and \(c \mid d\) \(\Rightarrow\) \((ac) \mid (bd)\).

(c) \(a \mid b\) and \(a \mid c\) \(\Rightarrow\) \(a \mid (xb + yc) \forall x, y \in \mathbb{Z}\).

Exercise 3. Use the Ceasar cipher with key \(k = 13\) to encrypt the word

CRYPTOGRAPHY

Hint: first, map the characters to their numeric representation, e.g., 'C' \(\rightarrow\) 3.