HAI709I : Fondements cryptographiques de la sécurité, Université de Montpellier, 2024

16/09/2024. Homework for Lecture 2.

Exercise 1. Let n be a prime number, a and b be integer numbers, and a be co-prime with n. Prove that there exists an integer c such that

$$a \cdot c = b \mod n.$$

Exercise 2. We are given a polynomial $L(x) = c_0 + c_1 x$ with integer coefficients such that

$$\begin{array}{rcl} L(3) & = & 5 \mod 7 \\ L(5) & = & 3 \mod 7. \end{array}$$

Find the values of c_0 and c_1 modulo 7.

Exercise 3. We are given polynomials $L(x) = a_0 + a_1 x$ and $R(x) = b_0 + b_1 x$ with integer coefficients. Which of the following options are possible:

(a) there is no $z \in \{0, 1, \dots, 10\}$ such that $L(z) = R(z) \mod 11$;

(b) there exists exactly one $z \in \{0, 1, \dots, 10\}$ such that $L(z) = R(z) \mod 11$;

(c) there exist exactly two $z \in \{0, 1, \dots, 10\}$ such that $L(z) = R(z) \mod 11$;

(d) there exist more than two different $z \in \{0, 1, \dots, 10\}$ such that $L(z) = R(z) \mod 11$.

Explain your answer.