Algebraic Algorithms for Cryptology TD 2

Exercice 1. Euclidean Algorithm

a. Apply the Euclidean Algorithm to compute the inverse of 21 modulo 40.

b. Consider the polynomials $P = X^4 + X^3 + 2X^2 + 2$ et $Q = X^3 + X + 1$. over the field $\mathbb{Z}/3\mathbb{Z}$.

1. Compute their GCD and the corresponding Bézout coefficients.
2. How could we have done more quickly?

Exercice 2. Binary Euclidean Algorithm

We will study an alternative way to compute recursively the GCD of two integers by focusing on the least significant bits instead of the most significant ones, as in the Extended Euclidean algorithm.

a. Explain how to count the multiplicity of 2 in the GCD between two integers

b. Explain how to recursively compute the GCD using only subtraction and division by 2, when:

1. one of the two input is even
2. both input are odd

c. Show that every second call, the largest of the two input is less than halved.

d. What is its arithmetic cost?

Exercice 3. Chinese Remainder Theorem: the pirates

A group of 17 pirates stole a treasure composed by golden coins of equal value. The decide to share them equally and leave the remainder to the cook. He would then receive 3 coins.

However the pirates get into a dispute and six of them are killed. The cook will then receive 4 coins. Later on, the ship sunk, and only the treasure, six pirates and the cook are saved. The cook would then receive 5 coins.

a. What is the least amount of coins which the Cook may hope to get, once he decides to poison the rest of the crew?