Cryptology Complementary TD 1

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 done more quickly?

Exercice 2. Binary Euclidean Algorithm

a. Explain how to compte the power of 2 of the gcd between two integers

b. In the setting where one of x and y is odd (suppose w.l.o.g that this is u), explain how the $\gcd(x, y)$ can be reduced to computing a $\gcd(u, v)$ where v is odd and $\max(|u|, |v|) \leq \max(|x|, |y|)/2$ only by means of subtraction and division by 2.

c. Deduce an algorithm computing the GCD of two integers.

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?