Cryptographie et arithmétique – Devoir maison 1

Exercice 1. Si $n \geqslant 1$, on rappelle que $\varphi(n)$ est le nombre d'éléments de $(\mathbb{Z}/n\mathbb{Z})^*$, et définit une fonction φ appelée indicatrice d'Euler.

1. Justifier que $\varphi(n) \leqslant n-1$ pour tout $n \geqslant 2$.

   On cherche une minoration de $\varphi(n)$ en fonction de n, pour tout $n \geqslant 3$. Soient p_1, …, p_r les diviseurs premiers de n, ordonnés de sorte que $p_1 < p_2 < \cdots < p_r$.

2. En exprimant $\varphi(n)$ à l'aide de p_1, …, p_r, montrer que $\varphi(n) \geqslant n \prod_{i=1}^{r} \left(1 - \frac{1}{1+i}\right)$. En déduire que $\varphi(n) \geqslant \frac{n}{r+1}$.

3. Montrer, à l'aide de la question précédente, que $\varphi(n) \geqslant \frac{n \ln(2)}{\ln(n)+\ln(2)}$.

Avec des techniques plus sophistiquées, on peut montrer qu'il existe une constante $c > 0$ telle que $\varphi(n) \geqslant \frac{c \cdot n}{\ln(\ln(n))}$ pour n assez grand.

Exercice 2. Soit $p \geqslant 5$ un nombre premier.

1. Soient a et b deux entiers. Montrer que l'équation $x^2 + ax + b \equiv 0 \mod p$ d'inconnue x admet une solution si, et seulement s'il existe un entier s tel que $a^2 - 4b \equiv s^2 \mod p$.

2. On suppose qu'il existe un entier s tel que $-3 \equiv s^2 \mod p$. Montrer qu'il existe un élément $\bar{x} \neq \bar{1}$ de $(\mathbb{Z}/p\mathbb{Z})^*$ tel que $\bar{x}^3 = \bar{1}$, et en déduire que $p \equiv 1 \mod 3$.

   On veut montrer la réciproque. Supposons que p s'écrit $p = 3q + 1$, avec q un entier.

3. Montrer qu'il existe $\bar{n} \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $n^q \not\equiv 1 \mod p$.

4. Montrer que $n^{2q} + n^q + 1 \equiv 0 \mod p$, et en déduire l'existence d'un entier s tel que $-3 \equiv s^2 \mod p$. Déterminer un tel s pour $p = 7$ et $p = 13$. Résoudre l'équation $s^2 \equiv -3 \mod 91$ d'inconnue s.