Feuille 3 bis

Exercice 1. (Probabilité de succès d'une partie de l'algorithme de Shor).
Soit $n \geqslant 3$ un entier impair, dont la factorisation en produit de nombres premiers est notée

$$n = \prod_{i=1}^{m} p_i^{\alpha_i}.$$

1. Montrer que la proportion d'éléments du groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ ayant un ordre pair est au moins égale à $1 - \frac{1}{2^m}$.
2. Combien l'équation $x^2 = 1$ a-t-elle de solutions dans $\mathbf{Z}/n\mathbf{Z}$?

   Pour $x \in (\mathbf{Z}/n\mathbf{Z})^\times$, on pourra noter $(x_1, \ldots, x_m)$ son image dans $\prod_{i=1}^m (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times$ (à travers l'isomorphisme du théorème des restes chinois). On dit que x satisfait l'hypothèse (H) si l'ordre (multiplicatif) de x, noté r, est pair, et si $x^{r/2} \not\equiv -1 \pmod n$.

3. Montrer qu'une condition nécessaire et suffisante pour que x satisfasse (H) est qu'il existe $i \neq j$ tels que les ordres de x_i et de x_j aient des valuations 2-adiques distinctes.
4. Dans le cas où $n = p^\alpha$ (avec p premier impair et $\alpha \geqslant 1$), montrer que la proportion d'éléments $x \in (\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ dont l'ordre a une valuation 2-adique donnée est majorée par $\frac{1}{2}$.
5. En déduire que la proportion d'éléments x de $(\mathbf{Z}/n\mathbf{Z})^\times$ satisfaisant (H) est supérieure ou égale à $1 - \frac{1}{2^{m-1}}$.
6. En déduire un algorithme probabiliste renvoyant deux diviseurs non-triviaux (éventuellement égaux) de n avec une certaine probabilité que l'on peut minorer explicitement.