Exercise sheet 3: Shor's algorithm

Exercise 1.

1. Determine all the elements of even order of $(\mathbf{Z}/15\mathbf{Z})^\times$.
2. Which ones of them also satisfy the assumption A2 of Shor's algorithm?

Exercise 2.

1. Let p be an odd prime number. Show that at least half of the elements of $(\mathbf{Z}/p\mathbf{Z})^\times$ have even order.
2. Let p be an odd prime number. Show that the equation $x^2 = 1$ only has two solution in $(\mathbf{Z}/p\mathbf{Z})^\times$.
3. Prove that the same answers hold in $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ when p is an odd prime and $\alpha \geqslant 1$.
4. Let $n = \prod_{i=1}^{\ell} p_i^{\alpha_i}$ be an odd integer, with at least two distinct prime factors (i.e. $\ell \geqslant 2$). Show that the proportion of elements of $(\mathbf{Z}/n\mathbf{Z})^\times$ that have even order is greater than or equal to $1 - \frac{1}{2^\ell}$.
5. How many square roots of 1 are there in $(\mathbf{Z}/n\mathbf{Z})^\times$?

Exercise 3. Let $n = \prod_{i=1}^{\ell} p_i^{\alpha_i}$ be an odd integer, with at least two distinct prime factors (i.e. $\ell \geqslant 2$). We denote by $\mathcal{R} := \{z \in (\mathbf{Z}/n\mathbf{Z})^\times \mid z^2 \equiv 1 \pmod n\}$ the set of square roots of 1 modulo n.

1. Let $s \geqslant 1$ and $y \in (\mathbf{Z}/n\mathbf{Z})^\times$. Show that the cardinality of the set $\{x \in (\mathbf{Z}/n\mathbf{Z})^\times \mid x^s \equiv y^s \pmod n\}$ does not depend on y.
2. Prove that if there exists $x_0 \in (\mathbf{Z}/n\mathbf{Z})^\times$ such that $x_0^s \equiv -1 \pmod n$, then for all $z \in \mathcal{R}$ there exists $y \in (\mathbf{Z}/n\mathbf{Z})^\times$ such that $z \equiv y^s \pmod n$.
3. For $s \geqslant 1$, denote by $\mathcal{S}_s := \{x \in (\mathbf{Z}/n\mathbf{Z})^\times \mid x^s \in \mathcal{R} \setminus \{1\}\}$ and by $\mathcal{S}'_s := \{x \in (\mathbf{Z}/n\mathbf{Z})^\times \mid x^s \in \mathcal{R} \setminus \{-1, 1\}\}$. Show that
$$\frac{|\mathcal{S}'_s|}{|\mathcal{S}_s|} \geqslant 1 - \frac{1}{2^\ell - 1}.$$
4. Prove that the proportion of invertible residue classes modulo n that satisfy the assumptions A1 and A2 of Shor's algorithm is greater than or equal to $1 - \frac{1}{2^{\ell-1}}$.

Exercise 4. In order to apply Shor's algorithm to factor $N = 21$, we choose $n = 9$ so that $2^n = 512 > N^2 = 441$. We also need to pick an element of $(\mathbf{Z}/21\mathbf{Z})^\times$, let's say $a = 2$. One can check that its order r is equal to 6.
In the lecture, we showed that the output of Shor's period-finding algorithm is $y \in \{0, \ldots, 2^n - 1\}$ with probability

$$p(y) = \begin{cases} \dfrac{1}{2^{2n}} \displaystyle\sum_{x=0}^{r-1} (J_x + 1)^2 & \text{if } 2^n \mid ry \\ \dfrac{1}{2^{2n}} \displaystyle\sum_{x=0}^{r-1} \left(\dfrac{\sin\left(\frac{\pi r y (J_x+1)}{2^n}\right)}{\sin\left(\frac{\pi r y}{2^n}\right)} \right)^2 & \text{otherwise;} \end{cases}$$

where $J_x := \lfloor \frac{2^n - 1 - x}{r} \rfloor$. Using the software of your choice, draw the plot of $p(y)$ as a function of $y \in \{0, \ldots, 2^n - 1\}$.

Exercise 5. Determine the convergents of the continued fraction representation of $\frac{75}{14}$.
You can check your result using PARI-GP: https://pari.math.u-bordeaux.fr/gpwasm.html
(the command is `contfrac(75/14)`).