

## 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 solutions 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  $\alpha \geq 1$ .
  4. Let  $n = \prod_{i=1}^{\ell} p_i^{\alpha_i}$  be an odd integer, with at least two distinct prime factors (i.e.  $\ell \geq 2$ ). 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.  $\ell \geq 2$ ). For  $x \in \mathbf{Z}/n\mathbf{Z}$  we denote by  $(x_1, \dots, x_\ell)$  its image in  $\prod_{i=1}^{\ell} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})$  under the isomorphism of the Chinese Remainder Theorem.

1. Let  $x \in (\mathbf{Z}/n\mathbf{Z})^\times$ . Denote by  $r$  its multiplicative order, and by  $r_i$  the multiplicative order of each of the  $x_i$ . We write  $v$  (resp.  $v_i$ ) for the 2-adic valuation of  $x$  (resp.  $x_i$ ). Show that  $x$  does not satisfy the assumptions A1 and A2 of Shor's algorithm if and only if all  $v_i$  are equal.
2. Let  $p$  be an odd prime and  $\alpha \geq 1$  and integer. Given a non negative integer  $\beta$ , prove that the proportion of elements of  $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$  whose order has 2-adic valuation equal to  $\beta$  is less than or equal to  $\frac{1}{2}$ .
3. 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  $y \in \{0, \dots, 2^n - 1\}$  with probability

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

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  $y \in \{0, \dots, 2^n - 1\}$ .

**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/gpasm.html> (the command is `contfrac(75/14)`).