Solution de la feuille 3 bis

1. D'après le théorème des restes chinois, le morphisme canonique

$$(\mathbf{Z}/n\mathbf{Z})^\times \to (\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/p_m^{\alpha_m}\mathbf{Z})^\times$$

est un isomorphisme. Ceci nous incite à commencer par traiter le cas où $n = p^\alpha$ pour un certain p impair et $\alpha \geqslant 1$. Dans ce cas, d'après l'exercice 4 de la feuille 3, le groupe $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ est cyclique. Soit a un générateur de ce groupe. L'ordre de cet élément est alors égal au cardinal du groupe $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Donc d'après le lemme suivant on en déduit que pour tout $k \in \{0, \ldots, \varphi(p^\alpha) - 1\}$, l'ordre de a^k est

$$\frac{(p-1)p^{\alpha-1}}{\operatorname{pgcd}((p-1)p^{\alpha-1}, k)}.$$

Lemme. *Soit G un groupe et $x \in G$ un élément d'ordre n. Alors l'ordre de x^k est égal à $\frac{n}{\operatorname{pgcd}(n,k)}$.*

Ainsi, pour tout k impair, le pgcd au dénominateur sera impair, et donc l'ordre de a^k sera pair car $p-1$ est pair. Ainsi l'ordre de a^k est pair au moins pour tous les exposants k impairs appartenant à $\{0, \ldots, \varphi(p^\alpha) - 1\}$. En résolvant l'inéquation

$$0 \leqslant k = 2j + 1 \leqslant (p-1)p^{\alpha-1} - 1$$

on trouve $\varphi(p^\alpha)/2$ valeurs de j possibles, et donc au moins la moitié des éléments de $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ sont d'ordre pair.

Revenons au cas général $n = \prod_{i=1}^m p_i^{\alpha_i}$. Si $a \in (\mathbf{Z}/n\mathbf{Z})^\times$, on note $(a_1, \ldots, a_m)$ son image via le morphisme canonique dans $(\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/p_m^{\alpha_m}\mathbf{Z})^\times$. Alors pour tout $k \in \mathbf{Z}$,

$$\begin{aligned} a^k \equiv 1 \,(\mathrm{mod}\, n) &\iff \forall i \in \{1, \ldots, m\},\ a_i^k \equiv 1 \,(\mathrm{mod}\, n) \iff \forall i \in \{1, \ldots, m\}, \operatorname{ord}(a_i) \mid k \\ &\iff \operatorname{ppcm}(\operatorname{ord}(a_1), \ldots, \operatorname{ord}(a_m)) \mid k \end{aligned}$$

ce qui montre que l'ordre de a est le ppcm des ordre des a_i. En particulier, l'ordre de a est impair si et seulement si tous les ordres de a_i sont impairs. Donc

$$\begin{aligned} \#\{a \in (\mathbf{Z}/n\mathbf{Z})^\times \text{ d'ordre impair}\} &= \#\{(a_1, \ldots, a_m) \in \prod_{i=1}^m (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times \text{ tous d'ordre impair}\} \\ &\leqslant \prod_{i=1}^m \frac{\varphi(p_i^{\alpha_i})}{2} \end{aligned}$$

d'après le cas des puissances de premiers. Par multiplicativité de l'indicatrice d'Euler, cette dernière majoration est égale à $\varphi(n)/2^m$ et le résultat voulu en découle.

2. À nouveau, on utilise le théorème des restes chinois car $x \in \mathbf{Z}/n\mathbf{Z}$ satisfait $x^2 = 1$ si et seulement si son image $(x_1, \ldots, x_m)$ via le morphisme canonique satisfait $x_1^2 = 1, \ldots, x_m^2 = 1$. Or d'après le fait que l'on a admis, dans chaque facteur de la forme $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$, l'équation $x^2 = 1$ n'a que deux solutions, par exemple car dans un groupe cyclique d'ordre pair il n'y a qu'un seul sous-groupe d'ordre 2. Comme -1 et 1 sont deux solutions distinctes (p impair), les solutions modulo n sont les antécédents des éléments de la forme $(\varepsilon_1, \ldots, \varepsilon_m)$ de $\prod_{i=1}^m (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times$ où pour les ε_i appartiennent à $\{-1, 1\}$. Il y a donc 2^m solutions.

3. On note r (resp. r_i) l'ordre de x (resp. x_i) et v (resp. v_i) la valuation 2-adique de cet ordre. On écrit $r_i = 2^{v_i} s_i$ pour un certain entier impair s_i.

   Supposons qu'il existe $i \neq j$ tel que $v_i \neq v_j$. On peut supposer, sans perte de généralité, que $v_2 > v_1$. Alors comme

   $$r = \mathrm{ppcm}(r_1, \dots, r_m) = \mathrm{ppcm}(2^{v_1} s_1, \dots, 2^{v_m} s_m) = 2^{\max v_i} \mathrm{ppcm}(s_1, \dots, s_m),$$

   on a 2^{v_2} qui divise r, et donc r est pair. De plus, $x^{r/2}$ correspond via l'isomorphisme du théorème des restes chinois à $(x_1^{r/2}, \dots, x_m^{r/2})$ et $r/2$ est un multiple de $2^{v_1} s_1$, qui est l'ordre de x_1, donc $x_1^{r/2} = 1$ donc $x^{r/2}$ correspond à un élément du produit des $(\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times$ de la forme $(1, \star, \dots, \star)$. En particulier, ce n'est pas $(-1, \dots, -1)$ donc $x^{r/2} \not\equiv -1 \pmod n$. On a donc bien montré que x satisfaisait (H).

   Si par contre tous les v_i sont égaux, montrons que x ne satisfait pas (H). Tout d'abord s'ils sont tous égaux à 0, cela veut dire que tous les ordres r_i sont impairs, et donc que leur ppcm r est impair, ce qui empêche de satisfaire (H). Si ils sont tous égaux à un certain $w \geqslant 1$, alors

   $$r = \mathrm{ppcm}(2^w s_1, \dots, 2^w s_m) = 2^w \underbrace{\mathrm{ppcm}(s_1, \dots, s_m)}_{\text{impair}}$$

   et donc $v = w$ et $s = \mathrm{ppcm}(s_1, \dots, s_m)$. Alors $x^{r/2}$ correspond à $(x_1^{r/2}, \dots, x_m^{r/2})$ via le théorème des restes chinois. Or pour tout i,

   $$x_i^{r/2} = x_i^{2^{w-1}s}$$

   qui est une racine carrée de 1 dans $\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z}$ (car $2 \times 2^{w-1}s = 2^w s$ est un multiple de $2^w s_i$ qui est l'ordre de x_i). Mais cette racine carrée n'est pas égale à 1 car sinon l'ordre de x_i, qui a valuation 2-adique égale à w, devrait diviser $2^{w-1}s$, qui a valuation $w-1$. Ainsi, d'après la question 2.(b), $x_i^{r/2} \equiv -1 \pmod{p_i^{\alpha_i}}$. Comme cela est vrai pour tout i, on en déduit que $x^{r/2} \equiv -1 \pmod n$, et donc x ne satisfait pas (H).

4. Soit $\beta \in \mathbf{N}$. On cherche à montrer que moins de la moitié (au sens large) des éléments de $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ ont un ordre r dont la valuation 2-adique est exactement égale à β.

   Comme à la question 2, si a est un générateur du groupe des inversibles, alors l'ordre de a^k est égal à

   $$\frac{(p-1)p^{\alpha-1}}{\mathrm{pgcd}((p-1)p^{\alpha-1}, k)}.$$

   Notons γ la valuation 2-adique de $p-1$. Alors

   $$v_2(\mathrm{ord}(a^k)) = \beta \iff v_2(\mathrm{pgcd}(p-1, k)) = \gamma - \beta.$$

   Ainsi, si $\beta > \gamma$, il n'y a aucun élément dont l'ordre satisfait la condition demandée (ce que l'on pouvait aussi voir comme une conséquence du fait que l'ordre de tout élément doit diviser le cardinal du groupe, qui est ici de la forme $2^\gamma u$ pour un u impair).

   Si par contre $\beta \leqslant \gamma$ alors les entiers $k \in \{0, \dots, \varphi(p^\alpha) - 1\}$ tels que $v_2(\mathrm{pgcd}(p-1, k)) = \gamma - \beta$ sont exactement les k de la forme $2^{\gamma-\beta}(2j+1)$. Leur nombre est majoré par le nombre d'entiers impairs dans $\{0, \dots, \varphi(p^\alpha) - 1)\}$ (qui correspond au cas $\beta = \gamma$), qui est précisément $\varphi(p^\alpha)/2$.

5. D'après la question 3, l'ensemble des $x \in (\mathbf{Z}/n\mathbf{Z})^\times$ qui ne satisfont pas (H) est en bijection (via le théorème des restes chinois) avec

   $$\bigsqcup_{x_1 \in (\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z})^\times} \left\{(x_1, x_2, \dots, x_m) \in \prod_{i=1}^m (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times \mid \forall i \geqslant 2,\ v_2(\mathrm{ord}(x_i)) = v_2(\mathrm{ord}(x_1))\right\}$$

Or chacun des ensembles de l'union disjointe est de cardinal inférieur ou égal à

$$\prod_{i=2}^{m} \frac{\varphi(p_i^{\alpha_i})}{2}$$

d'après la question 4. Donc l'ensemble des x ne satisfaisant pas (H) est de cardinal majoré par

$$\varphi(p_1^{\alpha_1}) \times \prod_{i=2}^{m} \frac{\varphi(p_i^{\alpha_i})}{2} = \frac{\varphi(n)}{2^{m-1}}$$

et le résultat en découle en passant au complémentaire.

6. On considère l'algorithme suivant :

   Soit x pris suivant la loi uniforme sur $\{1, \dots, n-1\}$.
   Si $\text{pgcd}(x, n) > 1$ on renvoie $\text{pgcd}(x, n)$ et $n/\text{pgcd}(x, n)$.

   Sinon, x définit une classe inversible modulo n.

   — On calcule son ordre multiplicatif r.

   — Si r est impair, on a perdu, l'algorithme renvoie **échec**.

   — Si r est pair, on calcule $x^{r/2} \pmod n$, et si c'est -1, on a perdu, l'algorithme renvoie **échec**. Si par contre $x^{r/2} \not\equiv -1 \pmod n$, on renvoie $\text{pgcd}(x^{r/2} - 1, n)$ et $\text{pgcd}(x^{r/2} + 1, n)$.

Expliquons pourquoi cet algorithme renvoie deux diviseurs non-triviaux de n (lorsqu'il ne renvoie pas **échec**).
Dans le cas où $\text{pgcd}(x, n) > 1$, il est clair que l'algorithme renvoie deux diviseurs de n, strictement compris entre 1 et n (les deux diviseurs peuvent éventuellement être égaux).
Dans l'autre cas, si x satisfait (H) alors l'algorithme renvoie $d := \text{pgcd}(x^{r/2} - 1, n)$ et $d' := \text{pgcd}(x^{r/2} + 1, n)$. Ce sont clairement deux diviseurs de n. Montrons que d est strictement compris entre 1 et n (l'argument est très similaire pour d'). Si d était égal à 1, alors comme

$$x^r \equiv 1 \pmod n$$

(par définition de l'ordre r), l'entier n divise $x^r - 1 = (x^{r/2} - 1)(x^{r/2} + 1)$, et est premier avec le premier facteur, donc divise le second. Mais ceci contredit (H). D'autre part, si d était égal à n, alors n diviserait $x^{r/2} - 1$, ce qui contredirait la minimalité de r.

Enfin, estimons la probabilité qu'en entier pris uniformément dans $\{1, \dots, n-1\}$ conduise à renvoyer **échec**. Cette probabilité est

$$\frac{\#\{x \in \{1, \dots, n-1\} \cap (\mathbf{Z}/n\mathbf{Z})^\times \text{ ne satisfaisant pas } (H)\}}{n-1} \leqslant \frac{\varphi(n)}{2^{m-1}(n-1)}$$

Donc la probabilité d'échec de l'algorithme est d'autant plus petite que m est grand (i.e. que n a beaucoup de facteurs premiers distincts) et que $\varphi(n)$ est petit devant $n-1$ (ce qui se produit aussi quand n est composé de beaucoup de petits facteurs premiers). C'est cohérent, l'algorithme a plus de chances de trouver des diviseurs quand l'entier n en a beaucoup, donc quand il est produit de plein de petits facteurs premiers.

Notons que comme $\varphi(n) \leqslant n-1$, la probabilité d'échec est toujours majorée par $\frac{1}{2^{m-1}} \leqslant \frac{1}{2}$ pour un entier ayant au moins deux facteurs premiers.