Corrigé de l'exercice 7 (TD5)

1. On a $ed \equiv 1 \bmod \varphi(n)$, donc $\varphi(n)$ divise $B = ed - 1$. Les questions suivantes montrent comment la connaissance d'un multiple de $\varphi(n)$ et de n suffit pour factoriser n.

2. Comme $a^{p-1} \equiv 1 \bmod p$ et $p-1$ divise m, on a $a^m = \left(a^{p-1}\right)^{\frac{m}{p-1}} \equiv 1 \bmod p$. De même, $a^m \equiv 1 \bmod q$. Par unicité dans le théorème chinois, on a donc $a^m \equiv 1 \bmod n$.
   Partant de $a^m - 1 \equiv 0 \bmod p$, comme $a^m - 1 = \left(a^{\frac{m}{2}} - 1\right)\left(a^{\frac{m}{2}} + 1\right)$, on a $a^{\frac{m}{2}} - 1 \equiv 0 \bmod p$ ou $a^{\frac{m}{2}} + 1 \equiv 0 \bmod p$ (parce que p est premier, donc $(\mathbb{Z}/p\mathbb{Z})^*$ est intègre). De même modulo q. On en déduit,

$$\begin{cases} a^{\frac{m}{2}} \equiv 1 \bmod p \\ a^{\frac{m}{2}} \equiv 1 \bmod q \end{cases}, \text{ ou } \begin{cases} a^{\frac{m}{2}} \equiv 1 \bmod p \\ a^{\frac{m}{2}} \equiv -1 \bmod q \end{cases}, \text{ ou } \begin{cases} a^{\frac{m}{2}} \equiv -1 \bmod p \\ a^{\frac{m}{2}} \equiv 1 \bmod q \end{cases},$$

$$\text{ou } \begin{cases} a^{\frac{m}{2}} \equiv -1 \bmod p \\ a^{\frac{m}{2}} \equiv -1 \bmod q \end{cases}.$$

   Par le théorème chinois, chacun de ces systèmes correspond à une seule valeur possible pour $a^{\frac{m}{2}} \bmod n$, donc à quatre valeurs au total. Pour le premier et le dernier système, 1 et -1 fournissent les mêmes congruences, donc par *unicité* dans le théorème chinois ces cas-là correspondent à $a^{\frac{m}{2}} \equiv \pm 1 \bmod n$. Pour les deux autres systèmes, on a $a^{\frac{m}{2}} \pm 1 \not\equiv 0 \bmod n$ donc $\operatorname{pgcd}(n, a^{\frac{m}{2}} \pm 1) \neq n$. Comme, de plus, $a^{\frac{m}{2}} \pm 1 \equiv 0 \bmod p$ ou q, et que p, q divisent n, on en déduit que n et $a^{\frac{m}{2}} \pm 1$ ne sont pas premiers entre eux. Autrement dit, $\operatorname{pgcd}(n, a^{\frac{m}{2}} \pm 1) \notin \{1, n\}$, et par définition ce pgcd divise n, donc son calcul fournit un diviseur non trivial de n (en temps polynomial).
   Les trois prochaines questions servent à démontrer que les éléments a qui conviennent sont assez nombreux (plus de la moitié des éléments). L'ensemble H regroupe les éléments qui ne nous permettent pas de factoriser n, et qu'on veut donc éviter.

3. D'une part, $H \subseteq (\mathbb{Z}/n\mathbb{Z})^*$ est non vide, car $\bar{1} \in H$. D'autre part, si $\bar{a}, \bar{b} \in H$, alors $(ab)^{\frac{m}{2}} = a^{\frac{m}{2}} b^{\frac{m}{2}} \equiv (\pm 1)(\pm 1) \equiv \pm 1 \bmod n$, donc $\overline{ab} \in H$. Enfin, si $\bar{a} \in H$, il est évident que $\left(a^{-1}\right)^{\frac{m}{2}} \equiv \pm 1 \bmod n$, donc $\bar{a}^{-1} \in H$, et H est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$.

4. Comme $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique, il existe un élément b_0 d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^*$. De même, il existe un élément b_1 d'ordre $q-1$ dans $(\mathbb{Z}/q\mathbb{Z})^*$, et alors b_1^2 est d'ordre $\frac{q-1}{2}$. Par le théorème chinois, il existe $\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^*$ dont les images modulo p et q sont respectivement b_0 et b_1^2, d'où le résultat.

5. Montrons d'abord que $m = \operatorname{ppcm}(p-1, q-1) = 2^{v_p} \operatorname{ppcm}(p', q')$. D'une part, p' divise $\operatorname{ppcm}(p', q')$ et donc $p - 1 = 2^{v_p} p'$ divise $2^{v_p} \operatorname{ppcm}(p', q')$. De même, $q-1$ divise $2^{v_q} \operatorname{ppcm}(p', q')$, et $2^{v_p} = 2^{v_p - v_q} 2^{v_q}$ est divisible par 2^{v_q}, donc $q-1$ divise également $2^{v_p} \operatorname{ppcm}(p', q')$. Cette dernière quantité étant un multiple commun à $p-1$ et $q-1$, elle est divisible par m (qui est le plus petit multiple commun à ces deux entiers *au sens de la divisibilité*). D'autre part, 2^{v_p} divise manifestement m (puisque m est divisible par $p - 1 = 2^{v_p} p'$), et p' divise m pour la même raison. Par le théorème de Gauss, comme p' est premier avec 2 (et donc avec 2^{v_p}), p' divise $\frac{m}{2^{v_p}}$. De même, q' divise $\frac{m}{2^{v_p}}$. Donc $\operatorname{ppcm}(p', q')$ divise $\frac{m}{2^{v_p}}$ (on utilise encore une fois le fait que le ppcm est le plus petit multiple commun *au sens de la divisibilité*), et $2^{v_p} \operatorname{ppcm}(p', q')$ divise m. On a la relation de divisibilité dans les deux sens, donc $m = 2^{v_p} \operatorname{ppcm}(p', q')$.
   Ceci étant, $\frac{m}{2} = 2^{v_p - 1} \operatorname{ppcm}(p', q')$. Pour montrer que $\bar{b}$ n'appartient pas à H, il suffit de montrer que $\bar{b}^{\frac{m}{2}}$ ne vérifie pas le premier ou quatrième système de la liste ci-dessus (puisque ces deux systèmes correspondent, on l'a vu, aux valeurs ± 1 possibles).
   Comme $b^{p-1} \equiv 1 \bmod p$, on a $b^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$. Or $\bar{b}$ est d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^*$, donc on a nécessairement $b^{2^{v_p - 1} p'} = b^{\frac{p-1}{2}} \equiv -1 \bmod p$ puis, comme p' divise $\operatorname{ppcm}(p', q')$,

$$b^{\frac{m}{2}} = b^{2^{v_p - 1} \operatorname{ppcm}(p', q')} \equiv (-1)^{\frac{\operatorname{ppcm}(p', q')}{p'}} \equiv -1 \bmod p.$$

   En effet, on élève -1 à une puissance impaire. Par un raisonnement analogue, on montre que $b^{\frac{m}{2}} \equiv 1 \bmod q$. Ceci démontre que $b^{\frac{m}{2}} \not\equiv \pm 1 \bmod n$ (sinon on aurait une contradiction en réduisant modulo p ou q), et donc que $\bar{b} \notin H$.

La probabilité que $x \in (\mathbb{Z}/n\mathbb{Z})^*$ choisi au hasard n'appartienne pas à H est égale à

$$\frac{\text{card}(\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid x \notin H\})}{\text{card}((\mathbb{Z}/n\mathbb{Z})^*)} = \frac{\text{card}((\mathbb{Z}/n\mathbb{Z})^*) - \text{card}(H)}{\text{card}((\mathbb{Z}/n\mathbb{Z})^*)} = 1 - \frac{\text{card}(H)}{\text{card}((\mathbb{Z}/n\mathbb{Z})^*)}.$$

Par le théorème de Lagrange, $\text{card}(H)$ divise $\text{card}((\mathbb{Z}/n\mathbb{Z})^*)$, donc il existe un entier naturel N tel que $\text{card}((\mathbb{Z}/n\mathbb{Z})^*) = N\text{card}(H)$. On a montré à l'instant que $H \neq (\mathbb{Z}/n\mathbb{Z})^*$, donc $N \geqslant 2$, et ceci démontre que la probabilité que $x \in (\mathbb{Z}/n\mathbb{Z})^*$ choisi au hasard n'appartienne pas à H est :

$$1 - \frac{\text{card}(H)}{\text{card}((\mathbb{Z}/n\mathbb{Z})^*)} = 1 - \frac{1}{N} \geqslant 1 - \frac{1}{2} = \frac{1}{2}.$$

À présent, on veut remédier au fait qu'on ne connaisse pas la valeur exacte de m si on n'a pas factorisé n (si bien que finalement, on ne peut pas calculer le pgcd désiré dans la deuxième question), en remplaçant $a^{\frac{m}{2}}$ par une autre puissance de a explicite.

6. On sait que $\varphi(n) = (p-1)(q-1)$, donc est divisible par $p-1$ et $q-1$. Comme B est divisible par $\varphi(n)$, on en déduit qu'il est un multiple commun à $p-1$ et $q-1$, donc m divise B (par propriété du ppcm, encore une fois, vis-à-vis de la relation de divisibilité).
Donc $\frac{B}{m}$ est un entier, qu'on peut écrire $\frac{B}{m} = 2^k l$, avec l un entier impair. Montrons que pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^*$, on a $x^{\frac{m}{2}} \equiv x^{\frac{B}{2^{k+1}}} \bmod n$. Grâce à l'unicité du théorème chinois, il suffit de démontrer cette égalité de congruence modulo p et q. Nous allons donc le démontrer en procédant suivant deux cas, selon que $x^{\frac{m}{2}} \bmod p, q$ soit égal à 1 ou -1.
   - Si $x^{\frac{m}{2}} \equiv 1 \bmod p$, alors $x^{\frac{B}{2^{k+1}}} = \left(x^{\frac{m}{2}}\right)^{\frac{B}{m2^k}} \equiv 1^l \equiv 1 \bmod p$. Donc $x^{\frac{B}{2^{k+1}}} \equiv x^{\frac{m}{2}} \bmod p$. De même modulo q.
   - Si $x^{\frac{m}{2}} \equiv -1 \bmod p$, alors $x^{\frac{B}{2^{k+1}}} \equiv (-1)^l \bmod p \equiv -1 \bmod p$ parce que l est impair. Donc $x^{\frac{B}{2^{k+1}}} \equiv x^{\frac{m}{2}} \bmod p$. De même modulo q.

   En résumé, on a l'égalité $x^{\frac{B}{2^{k+1}}} \equiv x^{\frac{m}{2}} \bmod p, q$ pour tout $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^*$, donc l'égalité est valable modulo n.

7. L'algorithme prend en entrée n, e et d. On devrait, eu égard des questions précédentes, calculer $\text{pgcd}\left(n, x^{\frac{B}{2^{k+1}}} \pm 1\right)$ avec x choisi au hasard et k la puissance de 2 dans $\frac{B}{m}$, mais on ne connaît pas k puisqu'on ne connait pas m, même si on sait que k n'excède pas la puissance de 2 dans la décomposition en facteurs premiers de B. On va donc calculer la puissance de 2 dans la décomposition en question, qu'on note k' ; puis on calcule $\text{pgcd}\left(n, x^{\frac{B}{2^{k'+1}}} - 1\right)$; si on obtient un facteur trivial de n, alors on remplace k' par $k'-1$; si on finit par avoir un facteur non trivial, on renvoie $\text{pgcd}\left(n, x^{\frac{B}{2^{k'+1}}} - 1\right)$ et $\frac{n}{\text{pgcd}\left(n, x^{\frac{B}{2^{k'+1}}} - 1\right)}$ (pour avoir l'autre facteur). En résumé, si `EuclidePGCD` est l'algorithme de calcul de pgcd et `rand` un algorithme qui tire un entier au hasard dans un intervalle, alors :
   - on prend en entrée n, e et d ;
   - soit $B := ed - 1$;
   - tant que $B \equiv 0 \bmod 2$ faire $B := B/2$ fin tant que ;
   - soit $x = \texttt{rand}(0, n-1)$;
   - tant que $(\text{pgcd}\left(n, x^B - 1\right) = 1$ ou $\text{pgcd}\left(n, x^B - 1\right) = n)$ et $B \leqslant ed - 1$ faire $B := B * 2$ fin tant que ;
   - imprimer ($\texttt{EuclidePGCD}(n, x^B - 1)$,$n/\texttt{EuclidePGCD}(n, x^B - 1)$).

8. Dans ce cas $B = 300 = 2^2 \cdot 75$. On prend des entiers au hasard assez petits pour faciliter l'exponentiation, par exemple 2. Alors, comme $2^{75} = 2^{64+8+2+1} = \left(\left(\left(\left(\left(2^2\right)^2\right)^2 \cdot 2\right)^2\right)^2 \cdot 2\right)^2 \cdot 2$, on a :

$$2^{75} = \left(\left((256 \cdot 2)^2\right)^2 \cdot 2\right)^2 \cdot 2 \equiv 43 \bmod 77 \not\equiv \pm 1 \bmod 77,$$

et $\text{pgcd}(77, 2^{75} - 1) = \text{pgcd}(77, 42) = 7$ fournit un facteur non trivial de 77.