Question 4

Trouvez les clefs publique et privée RSA avec les nombres premiers $p = 43$ et $q = 37$. En utilisant la valeur $e = 13$, montrez toutes les étapes de l'algorithme d'Euclide étendu permettant de trouver d (j'utilise ici les même noms de variables qu'en classe). Donnez toutes les étapes de vos calculs. Vous devez me donner la séquence de tous les appels récursifs, les paramètres utilisés et les valeurs de retour.

Avec les données du problème, nous avons les informations suivantes:

$$\begin{aligned} p &= 43 \\ q &= 37 \\ e &= 13 \\ n &= p * q = 43 * 37 = 1591 \\ \phi(n) &= (p-1)(q-1) = (43-1)(37-1) = 42 * 36 = 1512 \end{aligned}$$

Puisque la fonction d'Euclide étendu est récursive, nous devons déterminer les valeurs de chaque appel. Pour la première itération, nous savons que:

$$\begin{aligned} a &= 13 \\ b &= 1512 \end{aligned}$$

Pour les prochaines itérations, on obtient a et b de la manière suivante:

$$\begin{aligned} a &= b \\ b &= a (mod\, b) \end{aligned}$$

Nous répétons cette étape jusqu'à ce que b = 0, ce qui donne le tableau suivant:

itération	a	b	a (mod b)
1	13	1512	13
2	1512	13	4
3	13	4	1
4	4	1	0
5	1	0	-

Ensuite, nous devons trouver la valeur qui est retournée à chaque itération. Nous savons que la valeur retournée par l'itération où b = 0 est:

$$(t, x, y) = (a, 1, 0)$$

Pour les autres itérations, la valeur retournée est:

$$(t, x, y) = (t', y', x' - \lfloor a/b \rfloor * y')$$

Où (t',x',y') sont déterminés par la récursion de l'algorithme

Ce qui donne le tableau suivant:

itération	t	x	y	$(x' - \lfloor a/b \rfloor * y') = y$
5	1	1	0	-
4	1	0	1	$(1 - \lfloor 4/1 \rfloor * 0) = 1$
3	1	1	-3	$0 - \lfloor 13/4 \rfloor * 1) = -3$
2	1	-3	349	$(1 - \lfloor 1512/13 \rfloor * -3) = 349$
1	1	349	-3	$(-3 - \lfloor 13/1512 \rfloor * 349) = -3$

De ce qu'on a vu en classe (d = x), on peut alors dire que d = 349. On peut vérifier cette affirmation en testant la formule suivante:

$$\begin{aligned} e * x \ (mod\ \phi(n)) &= 1 \\ 13 * 349 \ (mod\ 1512) &= 1 \\ 4537 \ (mod\ 1512) &= 1 \end{aligned}$$

Donc,

$$d = 349$$