Répondez directement sur l'énoncé en **détaillant vos calculs** et **justifiant vos raisonnements**.

Nom: **CORRIGÉ**

1. À l'aide de l'algorithme d'Euclide, résoudre la congruence $2096\,x \underset{97627}{\equiv} 1$.

Idée : on fabrique par combinaisons linéaires successives des congruences de la forme

$$\ell_i : a_i \underset{97627}{\equiv} 2096\,x_i$$

jusqu'à obtenir celle qu'on cherche (qui existe forcément puisque $2096 \wedge 97627 = 1$).

Par exemple :

	i	a_i	x_i
	1	97627	0
	2	2096	1
$\ell_1 - 46\ell_2$	3	1211	-46
$\ell_2 - \ell_3$	4	885	47
$\ell_3 - \ell_2$	5	326	-93
$\ell_4 - 2\ell_3$	6	233	233
$\ell_5 - \ell_4$	7	93	-326
$\ell_6 - 2\ell_5$	8	47	885
$\ell_7 - \ell_6$	9	46	-1211
$\ell_8 - \ell_7$	10	1	2096

et la dernière ligne nous apprend que $x \underset{97627}{\equiv} 2096$.

2. À l'aide du théorème des restes chinois et de la factorisation $97627 = 233 \cdot 419$, confirmer votre réponse en 1.

Soit $\varphi : \mathbf{Z}_{97627} \to \mathbf{Z}_{233} \times \mathbf{Z}_{419}$ l'isomorphisme donné par le théorème des restes chinois.

On a, dans $\mathbf{Z}_{97627}$,

$$\begin{aligned}
2096 \cdot x = 1 &\iff \varphi(2096 \cdot x) = \varphi(1) \\
&\iff \varphi(2096) \cdot \varphi(x) = \varphi(1) \\
&\iff (-1, 1) \cdot \varphi(x) = (1, 1) \\
&\iff \varphi(x) = (-1, 1)^{-1} \\
&\iff \varphi(x) = (-1, 1) \\
&\iff x = \varphi^{-1}(-1, 1) = 2096.
\end{aligned}$$

3. Combien existe-t-il de racines primitives dans $\mathbf{Z}_{19}$? Construire une des tables de logarithmes possibles.

D'après un résultat vu en classe, on sait qu'il y a au moins une racine primitive dans $\mathbf{Z}_{19}$, de sorte que $\mathbf{Z}_{19}^{\times} \cong \mathbf{Z}_{18}$. Les racines primitives étant les éléments générateurs pour ce groupe, on conlut qu'il y en a

$$\phi(18) = \phi(2) \cdot \phi(9) = 1 \cdot (9-3) = 6.$$

Pour trouver une première racine primitive, on calcule les puissances d'un élément pris au hasard, par exemple $\alpha = 2$:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
α^i	1	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10

Puisque ces 18 puissances sont toutes distinctes, on remarque que $\mathrm{ord}_{19}(2) = 18$ et donc que 2 est une racine primitive. Les 5 autres sont de la forme 2^i avec $i \wedge 18 = 1$, soit

$$13,\ 14,\ 15,\ 3,\ 10.$$

4. Résoudre, avec un minimum de calculs, l'équation $9x^2 + x + 2 = 0$ dans $\mathbf{Z}_{19}$.

Puisque $2 \in \mathbf{Z}_{19}^{\times}$, on peut utiliser la formule usuelle et dire que les racines sont de la forme

$$x = \frac{-1+\delta}{2 \cdot 9}$$

où

$$\delta^2 = \Delta = 1^2 - 4 \cdot 9 \cdot 2 = 1 - 2^2 \cdot 2^8 \cdot 2^1 = 1 - 2^{11} = 1 - 15 = 5 = 2^{16} = (\pm 2^8)^2 = (\pm 9).$$

On trouve donc

$$x = \frac{-1 \pm 9}{2 \cdot 9} = \frac{-1 \pm 9}{-1} = 10 \text{ ou } -8 = 10 \text{ ou } 11.$$