1. Puisque $65\,792 = \underset{\overset{\shortparallel}{2^8}}{256} \cdot 257$ et que $256 \wedge 257 = 1$,

on sait d'après le théorème des restes chinois que

$$x^2 + 28x + 3 \underset{65\,792}{\equiv} 0 \iff \begin{cases} x^2 + 28x + 3 \underset{256}{\equiv} 0 \\ x^2 + 28x + 3 \underset{257}{\equiv} 0 \end{cases}$$

A) Résolution de $x^2 + 28x + 3 \underset{257}{\equiv} 0$

Il s'agit d'une équation du second degré dans un anneau $(\mathbb{Z}/257\mathbb{Z})$ dans lequel 2 est inversible ;

on peut donc procéder de la façon habituelle

et calculer $\Delta = 28^2 - 4 \cdot 1 \cdot 3 = 772 \underset{257}{\equiv} 1$

de sorte que $\Delta \underset{257}{\equiv} (\pm 1)^2$

On trouve donc comme solutions

$$x \underset{257}{\equiv} \frac{-28 \pm 1}{2} \equiv \begin{cases} 129 \cdot -29 \equiv 114 \\ 129 \cdot -27 \equiv 115 \end{cases}$$

(puisque $2 \cdot 129 = 258 \underset{257}{\equiv} 1$)

(et comme 257 est premier, ce sont les deux seules solutions modulo 257 puisque $\mathbb{Z}/257\mathbb{Z}$ est un corps et qu'une équation algébrique ne peut y avoir plus de solutions que son degré).

B) Résolution de $x^2 + 28x + 3 \underset{256}{\equiv} 0$

Cette fois $\Delta = 772 \underset{256}{\equiv} 4 = (\pm 2)^2$,

MAIS malheureusement, 2 n'étant pas inversible dans $\mathbb{Z}/256\mathbb{Z}$, on ne peut pas utiliser la formule usuelle.

Ceci dit, on peut tout de même ré-écrire l'équation sous la forme

$$\underbrace{x^2 + 28x + 14^2}_{(x+14)^2} \underset{256}{\equiv} 14^2 - 3 = 193,$$

il suffit donc de déterminer des racines carrées de 193 dans $\mathbb{Z}/256\mathbb{Z}$.

Ce qui n'est pas si aisé ...

Lemme : $(\mathbb{Z}/256\mathbb{Z})^\times = \{ \varepsilon \cdot 5^k \mid \varepsilon = \pm 1 \text{ et } 0 \leqslant k < 64 \}$.

En effet : on sait que $(\mathbb{Z}/256\mathbb{Z})^\times$ est un groupe à $\Phi(256) = \frac{256}{2} = 128$ éléments. Commençons par calculer l'ordre multiplicatif de 5 : d'après le théorème de Lagrange, on sait qu'il divise 128, il est donc de la forme 2^k avec $k \leqslant 7$.

Or on peut calculer facilement (par mises au carré successives) les puissances qui nous intéressent :

$$5^2 = 25$$

$$5^4 = (5^2)^2 = 25^2 = 625 \underset{256}{\equiv} 113$$

$$5^8 = (5^4)^2 \underset{256}{\equiv} 113^2 \equiv 225$$

$$5^{16} = (5^8)^2 \equiv 225^2 \equiv 193 \quad \text{(ah ! tiens)}$$

$$5^{32} = (5^{16})^2 \equiv 193^2 \equiv 129$$

$$5^{64} = (5^{32})^2 \equiv 129^2 \equiv 1 \, ,$$

l'ordre de 5 est donc 64, les 64 éléments de la forme 5^k $(k < 64)$ sont donc distincts.

Ceux de la forme -5^ℓ $(\ell < 64)$ aussi, et ces deux familles sont disjointes : en effet,

si on avait $-5^\ell = 5^k$

alors $-1 \equiv 5^{k-\ell} \in \langle 5 \rangle$;

mais alors $1 = (-1)^2 \equiv 5^{2(k-\ell)}$

on doit donc avoir $2(k-\ell) \underset{64}{\equiv} 0$

donc $k-\ell \underset{64}{\equiv} 0$ ou 32 ;

or on a remarqué plus haut que ni 5^0 ni 5^{32} n'était congru à -1.

Procédons maintenant à déterminer les racines carrées r de 193 dans $\mathbb{Z}/256\mathbb{Z}$.

Écrivant $r = \pm 5^k$, on cherche donc à résoudre $r^2 \equiv 193$

soit $\underset{\substack{\parallel \\ 5^{2k}}}{(\pm 5^k)^2} \underset{256}{\equiv} 5^{16}$;

ceci n'est possible que si $2k \underset{64}{\equiv} 16$ soit $k \underset{32}{\equiv} 8$

ou $k \underset{64}{\equiv} 8$ ou 40.

On trouve donc 4 racines carrées :

$r_1 = 5^8 \equiv 225$, $r_2 = -5^8 \equiv 31$,

$r_3 = 5^{40} = 5^{32} \cdot 5^8 = 129 \cdot 225 \equiv 97$,

$r_4 = -5^{40} \equiv 159$.

Revenant à $(x+14)^2 \underset{256}{\equiv} 193$, on trouve donc 4 solutions

$x \equiv r_i - 14 \underset{256}{\equiv} 211, 17, 83, 145$

(À ce stade, c'est sans doute une bonne idée de prendre le temps de vérifier que ce sont bien des solutions à notre congruence de départ $x^2 + 28x + 3 \underset{256}{\equiv} 0$)

c) Application des restes chinois

Revenant à la congruence initiale modulo 65 792, on sait donc qu'elle admet exactement 8 solutions.

Explicitement : puisque $1 \cdot 257 - 1 \cdot 256 = 1$,

(relation de Bézout)

on sait que $\begin{cases} x \underset{256}{\equiv} a \\ x \underset{257}{\equiv} b \end{cases} \Leftrightarrow x \underset{65\,792}{\equiv} 257a - 256b$

Avec cette formule on trouve

(a, b)	$x \bmod 65\,792$
$(17, 114)$	40 977
$(83, 114)$	57 939
$(145, 114)$	8081
$(211, 114)$	25 043
$(17, 115)$	40 721
$(83, 115)$	57 683
$(145, 115)$	7825
$(211, 115)$	24 787

2. Soient p et q des nombres premiers tels que

$p = 2q + 1$ (on appelle alors q un nombre premier de Sophie Germain)

On sait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe à

$\Phi(p) = p - 1 = 2q$ éléments, et qu'il existe au moins un élément primitif α (démontré en classe).

On a alors un isomorphisme
$$\begin{aligned} \mathbb{Z}/2q\mathbb{Z} &\longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \, ; \\ k &\longmapsto \alpha^k \end{aligned}$$

les éléments primitifs sont ceux qui sont de la forme α^k avec k générateur de $\mathbb{Z}/2q\mathbb{Z}$, i.e. relativement premier à $2q$. Il y en a donc

$$\Phi(2q) = \Phi(2)\,\Phi(q) = q - 1 \, .$$

Par exemple : pour $p = 11$, $q = 5$, on s'attend à trouver 4 éléments primitifs dans $\mathbb{Z}/11\mathbb{Z}$. Puisque

$$3^5 \underset{11}{\equiv} 1 \, , \quad 4^5 \underset{11}{\equiv} 1 \, , \quad 5^5 \underset{11}{\equiv} 1 \, , \quad 9^5 \underset{11}{\equiv} 1 \quad \text{et} \quad 10^2 \underset{11}{\equiv} 1 \, ,$$

ce sont forcément ceux qui restent : $\underset{2^9}{\overset{}{2}}$, $\underset{2^9}{\underset{\equiv}{6}}$, $\underset{2^7}{\underset{\equiv}{7}}$, $\underset{2^3}{\underset{=}{8}}$