Corrigé du Partiel du 9 novembre 2022, 11h30-13h

Exercice 1.

1. Modulo 89, on a $9 \cdot 10 \equiv 90 \equiv 1$ et $3^4 \equiv 9^2 \equiv 81 \equiv -8$ donc
$$8 \cdot 9 \cdot 10 + 3^4 \equiv 8 \cdot 1 - 8 \equiv 0. \pmod{89}$$

2. On calcule bêtement modulo 17
$$\begin{aligned} 8! &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \equiv (2 \cdot 8) \cdot (3 \cdot 6) \cdot 4 \cdot (5 \cdot 7) \\ &\equiv (-1) \cdot 1 \cdot 4 \cdot 1 \equiv -4, \end{aligned} \pmod{17}$$
d'où
$$8!^2 \equiv (-4)^2 = 16 \equiv -1. \pmod{17}$$

3. On utilise le fait que $k \equiv -(n-k)$ modulo n, ce qui donne modulo n
$$\begin{aligned} \left(\frac{n-1}{2}\right)!^2 &\equiv \left(\frac{n-1}{2}\right)! \cdot \left(\frac{n-1}{2}\right)! \equiv \left(\frac{n-1}{2}\right)! \cdot 1 \cdot 2 \cdots \frac{n-1}{2} \\ &\equiv \left(\frac{n-1}{2}\right)! \cdot (-(n-1)) \cdot (-(n-2)) \cdots \left(-\left(n - \frac{n-1}{2}\right)\right) \\ &\equiv (-1)^{\frac{n-1}{2}} \left(\frac{n-1}{2}\right)! \cdot (n-1) \cdot (n-2) \cdots \left(\frac{n-1}{2} + 1\right) \\ &\equiv (-1)^{\frac{n-1}{2}} (n-1)!. \end{aligned} \pmod{n}$$

4. D'après l'identité admise dans cette question appliquée à $p = 17$ (qui est bien premier) :
$$16! \equiv -1. \pmod{17}$$
L'identité de la question 3 appliquée à $n = 17$ donne alors :
$$8!^2 \equiv (-1)^8 16! = 16! \equiv -1. \pmod{17}$$

5. Les éléments de $(\mathbf{Z}/p\mathbf{Z})^*$ qui sont leur propre inverse sont ceux qui vérifient $x^2 = \overline{1}$ i.e. sont les racines du polynôme $x^2 - \overline{1}$. Celui-ci est de degré 2, donc a au plus 2 racines puisque $(\mathbf{Z}/p\mathbf{Z})^*$ est un corps (p premier), par conséquent ses seules racines sont $\overline{1}$ et $\overline{-1}$.
Cela signifie que chaque élément de $(\mathbf{Z}/p\mathbf{Z})^*$ autre que $\overline{1}$ et $\overline{-1} = \overline{p-1}$ a un inverse autre que lui-même. Dans le produit
$$(p-1)! \equiv 1 \times 2 \times \cdots \times (p-2) \times (p-1) \pmod{p}$$
on peut donc regrouper par paires les éléments inverse l'un de l'autre, qui se simplifient, et il ne reste que $\overline{1}$ et $\overline{-1} = \overline{p-1}$ qui ne se simplifient pas : $(p-1)! \equiv 1 \times (-1) \equiv -1 \pmod{p}$.

Exercice 2.

1. Comme 19 et 11 sont des nombres premiers distincts, ils sont premiers entre eux. Le théorème chinois assure alors que l'ensemble des solutions du système est
$$\{x_0 + 19 \cdot 11 \cdot k \mid k \in \mathbf{Z}\}$$
où x_0 est n'importe quelle solution particulière du système. Vu que $19 \times 11 = 209$ et que $x_0 = 2004$ est solution évidente, l'ensemble des solutions du système est donc
$$\{2004 + 209k \mid k \in \mathbf{Z}\}.$$
On cherche la plus petite solution <u>positive</u> : celle-ci est obtenue pour $k = -9$ et vaut $2004 - 9 \times 209 = 123$.

2. (a) Les années x où on peut observer les deux comètes simultanément sont précisément les solutions du système de la question précédente, et on vient de voir que ce sont toutes les années de la forme $2004 + 209k$. La prochaine telle année est $2004 + 209 = 2213$.

(b) Les années x où on peut observer les trois comètes simultanément sont précisément les solutions du système suivant (où la première congruence a été obtenue dans la question 1) :

$$\begin{cases} x & \equiv & 2004 & [209] \\ x & \equiv & 2011 & [20] \end{cases}$$

Comme 209 et 20 n'ont aucun facteur premier en commun (209 n'est divisible ni par 2 ni par 5), ils sont premiers entre eux. Le théorème chinois assure alors que l'ensemble des solutions du système ci-dessus est

$$\{x_1 + 209 \cdot 20 \cdot k \mid k \in \mathbf{Z}\}$$

où x_1 est n'importe quelle solution particulière du système. L'écart entre deux solutions consécutives est donc égal à $209 \times 20 = 4180$ ans.
(Remarque : on ne demandait pas de résoudre ce système !)

Exercice 3.

1. Par le petit théorème de Fermat (c'est-à-dire le théorème de Lagrange dans le cas d'un modulo premier), comme 2 et 1023 sont premiers entre eux, **si** 1023 **était premier** alors on aurait

$$2^{1022} \equiv 1 \pmod{1023}$$

ce qui n'est manifestement pas le cas d'après l'énoncé. Donc 1023 n'est pas premier.
(Note : c'est le *test de Fermat*. Ici, 2 est un *témoin de Fermat* de la non-primalité de 1023.)

2. Il se trouve que $1022 = 1024 - 2$ et $1024 = 2^{10}$, donc :

$$1022_{10} = 10000000000_2 - 10_2 = 1111111110_2.$$

3. Par mises au carré successives, on calcule :

$$\begin{aligned}
2^2 &= 4 && \pmod{11} \\
2^4 &\equiv 4^2 = 16 \equiv 5 && \pmod{11} \\
2^8 &\equiv 5^2 = 25 \equiv 3 && \pmod{11} \\
2^{16} &\equiv 3^2 = 9 \equiv -2 && \pmod{11} \\
2^{32} &\equiv (-2)^2 = 4 && \pmod{11} \\
2^{64} &\equiv 5 && \pmod{11} \\
2^{128} &\equiv 3 && \pmod{11} \\
2^{256} &\equiv -2 && \pmod{11} \\
2^{512} &\equiv 4 && \pmod{11}
\end{aligned}$$

D'après la question 2, on a $1022 = 512 + 256 + 128 + 64 + 32 + 16 + 8 + 4 + 2$. On en déduit que :

$$\begin{aligned}
2^{1022} &\equiv 2^{512} \cdot 2^{256} \cdot 2^{128} \cdot 2^{64} \cdot 2^{32} \cdot 2^{16} \cdot 2^{8} \cdot 2^{4} \cdot 2^{2} && \pmod{11} \\
&\equiv 4 \cdot (-2) \cdot 3 \cdot 5 \cdot 4 \cdot (-2) \cdot 3 \cdot 5 \cdot 4 && \pmod{11} \\
&\equiv (4 \cdot 3) \cdot (4 \cdot 3) \cdot (5 \cdot (-2)) \cdot (5 \cdot (-2)) \cdot 4 && \pmod{11} \\
&\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 4 && \pmod{11} \\
&\equiv 4 && \pmod{11}
\end{aligned}$$

4. Étant donné que 31 est premier, on a $\phi(31) = 31 - 1 = 30$. Comme 2 et 31 sont premiers entre eux, le théorème de Lagrange assure donc que $2^{30} \equiv 1 \pmod{31}$. On peut ainsi simplifier le calcul en faisant la division euclidienne de l'exposant par 30. On a $1022 = 30 \times 34 + 2$, par conséquent :

$$2^{1022} \equiv (2^{30})^{34} \cdot 2^2 \equiv 1^{34} \cdot 4 = 4 \pmod{31}$$

5. Comme $2 \equiv -1 \pmod{3}$, il vient

$$2^{1022} \equiv (-1)^{1022} \equiv 1^{511} \equiv 1 \pmod{3}.$$

6. Par un heureux hasard,
$$3 \cdot 11 \cdot 31 = 341 \cdot 3 = 1023$$
et 3, 11 et 31 sont deux-à-deux premiers entre eux (puisque premiers distincts). Par le théorème des restes chinois, le morphisme de réduction
$$\begin{aligned} \mathbb{Z}/1023\mathbb{Z} &\to (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}) \times (\mathbb{Z}/31\mathbb{Z}) \\ x \pmod{1023} &\mapsto (x \pmod 3, x \pmod{11}, x \pmod{31}) \end{aligned}$$
est donc une application bijective (mieux, un isomorphisme d'anneaux). Il est clair que celle-ci envoie la classe de 4 modulo 1023 sur $(\overline{1}, \overline{4}, \overline{4})$. Mais d'après les questions précédentes, elle envoie aussi la classe de 2^{1022} modulo 1023 sur $(\overline{1}, \overline{4}, \overline{4})$. Par injectivité, on en conclut que $2^{1022} \equiv 4 \pmod{1023}$.

Exercice 4.

1. Méthode 1 : on utilise la définition $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$, et le fait que la classe de a est inversible modulo n si et seulement si a et n sont premiers entre eux. Les entiers premiers avec 8 compris entre 0 et 7 sont 1, 3, 5 et 7 donc $\phi(8) = 4$. Les entiers premiers avec 12 compris entre 0 et 11 sont 1, 5, 7, 11 donc $\phi(12) = 4$ également.
   Méthode 2 : on uilise les formules de calcul de $\phi(n)$. On a $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$, de plus 3 et $4 = 2^2$ sont premiers entre eux donc $\phi(12) = \phi(2^2)\phi(3) = (2^2 - 2^1)(3 - 1) = 4$.
2. Dans $(\mathbb{Z}/8\mathbb{Z})^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, la multiplication est donnée par la table :

$\times$	$\overline{1}$	$\overline{3}$	$\overline{-3}$	$\overline{-1}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{-3}$	$\overline{-1}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{-1}$	$\overline{-3}$
$\overline{5} = \overline{-3}$	$\overline{-3}$	$\overline{-1}$	$\overline{1}$	$\overline{3}$
$\overline{7} = \overline{-1}$	$\overline{-1}$	$\overline{-3}$	$\overline{3}$	$\overline{1}$

   On remarque qu'il n'y a que des éléments d'ordre 2.
3. Dans $(\mathbb{Z}/12\mathbb{Z})^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$, la multiplication est donnée par la table :

$\times$	$\overline{1}$	$\overline{5}$	$\overline{-5}$	$\overline{-1}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{-5}$	$\overline{-1}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{-1}$	$\overline{9}$
$\overline{7} = \overline{-5}$	$\overline{-5}$	$\overline{-1}$	$\overline{1}$	$\overline{5}$
$\overline{11} = \overline{-1}$	$\overline{-1}$	$\overline{-5}$	$\overline{5}$	$\overline{1}$

4. On peut remarquer que nécessairement 1 (mod 8) est envoyé sur 1 (mod 12), puisqu'on veut $\sigma(\overline{1}) = \sigma(\overline{1})\sigma(\overline{1})$ et $\sigma(\overline{1})$ inversible, donc on peut simplifier à gauche et à droite par $\sigma(\overline{1})$ ce qui donne $\sigma(\overline{1}) = \overline{1}$. Ensuite les tables nous invitent à envoyer $\overline{3}$ sur $\overline{5}$, $\overline{-3}$ sur $\overline{-5}$ et $\overline{-1}$ sur $\overline{-1}$. On vérifie que ça marche.

*****