Correction séance 4 (6 octobre)

† *Équations et congruences*

Exercice 6.
1. Soit x une solution du système proposé. Par hypothèse $x-1$ est congru à 0 modulo $3, 5, 7$, autrement dit $x-1$ est divisible par le ppcm de $3, 5, 7$, soit 105. Le plus petit tel entier est 105 (on pourrait prendre 0, mais ça donnerai $x = 1$ et on veut $x > 2$), qui donne $x = 106$.

2. Même raisonnement, $x + 1$ doit être divisible par $7, 11, 13$, donc par leur ppcm 1001. L'entier $x = 1000$ est la plus petite solution convenable.

Exercice 7.
1. On se doute que 261 et 305 sont premiers entre eux, on voudrait une relation de Bézout entre les deux :

$$\begin{aligned}305 &= 261 \cdot 1 + 44\\ 261 &= 44 \cdot 5 + 41\\ 44 &= 41 \cdot 1 + 3\\ 41 &= 3 \cdot 13 + 2\\ 3 &= 2 \cdot 1 + 1\end{aligned}$$

En remontant, on trouve $305 \cdot 89 - 261 \cdot 104 = 1$. Donc l'inverse de 261 modulo 305 est $-104 = 201[305]$. L'équation demandée est équivalente à

$$261x \equiv -2[305] \Leftrightarrow x \equiv 201 \cdot (-2) \equiv -402 \equiv -97[305]$$

Les solutions recherchées sont donc les entiers x congrus à -97 modulo 305, soit les entiers de la forme $305k - 97$ pour $k \in \mathbb{Z}$.

2. On voit que 12 et 19 sont premiers entre eux. Par le théorème des restes chinois, les solutions x du système étudié existent quels que soient a et b, et ces solutions sont uniques modulo $12 \cdot 19 = 228$. Il suffit donc de trouver une solution particulière au système.
On considère les systèmes auxiliaires

$$(S_1) : \begin{cases}\varepsilon \equiv 1[12]\\ \varepsilon \equiv 0[19]\end{cases} \qquad (S_2) : \begin{cases}\eta \equiv 0[12]\\ \eta \equiv 1[19]\end{cases}$$

Si on trouve ε et η des solutions de ces systèmes, $x = a\varepsilon + b\eta$ sera une solution du système de départ et on aura terminé.
Pour trouver des solutions particulières à (S_1) et à (S_2), on cherche d'abord une relation de Bézout entre 12 et 19 (cela revient à chercher l'inverse de 12 modulo 19)

$$\begin{aligned}19 &= 12 \cdot 1 + 7\\ 12 &= 7 \cdot 1 + 5\\ 7 &= 5 \cdot 1 + 2\\ 5 &= 2 \cdot 2 + 1\end{aligned}$$

En remontant, on trouve $12 \cdot 8 - 19 \cdot 5 = 1$.
Si ε est une solution de (S_1), on a $\varepsilon = 12p + 1 = 19q$, donc $-12p + 19q = 1$, la relation de Bézout nous donne une solution $(p, q) = (-8, -5)$, donc $\varepsilon = 12 \cdot -8 + 1 = -95$.
Si η est une solution de (S_2), on a $\eta = 12t = 19s + 1$, donc $12t - 19s = 1$, la relation de Bézout nous donne une solution $(s, t) = (8, 5)$, donc $\eta = 12 \cdot 8 = 96$.
Une solution du premier système est alors donnée par $x = -95a + 96b$. Les solutions générales du système sont alors données par

$$x = -95a + 96b + 228k, \quad k \in \mathbb{Z}$$

Exercice 8.
1. Comme $2, 3, 5$ sont premiers entre eux, les solutions du premier système existent et sont uniques modulo $2 \cdot 3 \cdot 5 = 30$ (théorème des restes chinois). Il suffit donc de trouver une solution particulière.
Comme $x \equiv 3[5]$, $x - 3$ doit être divisible par 5, donc son dernier chiffre doit être 0 ou 5. Donc le dernier chiffre de x est 3 ou 8.
Comme $x \equiv 5 \equiv 1[2]$, x est impair et son dernier chiffre est impair : le dernier chiffre de x est 3.
Comme $x \equiv 2[3]$, la somme des chiffre de x doit être congrue à 2 modulo 3 : 23 convient.
Les solutions générales du système sont de la forme

$$x = 23 + 30k, k \in \mathbb{Z}$$

2. Comme $4, 3, 7$ sont premiers entre eux, les solutions du deuxième système existent et sont uniques modulo $4 \cdot 3 \cdot 7 = 84$ (théorème des restes chinois. Il suffit donc de trouver une solution particulière. Premièrement x doit être divisible par 3 et par 7, donc par leur ppcm : 21.
Tiens ! 21 est également congru à 1 modulo 4 : c'est une solution particulière du système.
Les solutions générales sont de la forme

$$x = 21 + 84k, \ k \in \mathbb{Z}$$

Exercice 9.
1. Décortiquons un peu l'équation $ax \equiv b[n]$: elle est équivalente à l'existence d'un $k \in \mathbb{Z}$ tel que $ax = b + kn$, i.e $ax - nk = b$. C'est une équation de Bézout, dont les solutions (x, k) existent si et seulement si le pgcd de a et n divise b : c'est le résultat voulu.

2. Si a et n sont premiers entre eux, a est inversible modulo n, on peut réécrire l'équation par $x \equiv a^{-1}b[n]$: la solution est bien unique.
Réciproquement si $a \wedge n = d > 1$, on doit montrer qu'il n'existe pas une unique solution : autrement dit soit il n'y a pas de solution, soit il y en a plusieurs :
Si d ne divise pas b, il n'y a pas de solutions.
Si d divise b, on peut diviser par d dans l'équation pour obtenir $a'x = b'[n']$, où $a' = \frac{a}{d}, b' = \frac{b}{d}, n' = \frac{n}{d}$. Comme a' et b' sont premiers entre eux, il existe une unique solution modulo n'. Mais comme $n' < n$ (car $d > 1$), deux solutions x et $x + n'$ ne sont pas égales modulo n : il existe plusieurs solutions.

Exercice 10. C'est le seul cas de la feuille où les modulis ne sont pas premiers entre eux. On a $21 \wedge 24 = 3$. Si x est une solution, on a $x = a + 21s = b + 24t$ et $21s - 24t = b - a$. Des solutions à cette équation de Bézout existent si et seulement si 3 divise $b - a$.

Trouvons les solutions si $b - a = 3k$. L'équation est alors équivalente à $7s - 8t = k$. Une solution particulière est donnée par $s = -k$, $t = -k$. Pour les solutions globales, on a

$$7(-k) - 8(-k) = 7s - 8t \Leftrightarrow 8(k + t) = 7(s + k)$$

On obtient $7p = k + t$ et $8p = s + k$, les solutions générales sont de la forme $(s, t) = (8p - k, 7p - k)$. On trouve donc

$$x = a + 21s = a + 21(8p - k) = a + 168p - 7 \cdot 3k = a + 168p - 7(b - a) = 8a - 7b + 168p, \quad p \in \mathbb{Z}$$