Correction TD2

† *Congruences et divisibilité*

Exercice 1. Par définition de la congruence modulo n, il existe des entiers p et q tels que $a-b=pn$ et $c-d=qn$. En ajoutant ces deux égalités, on a

$$(a+c)-(b+d)=(p+q)n$$

donc $a+c\equiv b+d[n]$. Ensuite, on a $(a-b)c=ac-bc=pnc$ et $b(c-d)=bc-bd=bqn$, on a

$$ac-bd=ac-bc+bc-bd=n(pc+bq)$$

donc $ac\equiv bd[n]$.

Exercice 2. Un peu de notations sur la base 10 : Un entier n s'écrit de manière unique sous la forme

$$n:=\sum_{i=0}^{\infty}n_i10^i$$

avec $n_i\in[\![0,9]\!]$. Ainsi, n_0 est le chiffre des unités, n_1 celui des dizaines...

1.

- Pour 2, on a $10\equiv 0[2]$, donc $10^i\equiv 0[2]$ pour $i\geqslant 1$.

$$n=\sum_{i=0}^{\infty}n_i10^i=\sum_{i=1}^{\infty}n_i10^i+n_0\equiv n_0[2]$$

  Donc n est divisible par 2 si et seulement si n_0 est divisible par 2.

- Pour 3, on a $10\equiv 1[3]$ donc $10^i=1[3]$ pour tout i. On a donc

$$n=\sum_{i=0}^{\infty}n_i10^i\equiv\sum_{i=0}^{\infty}n_i[3]$$

- Pour 4, on a $100\equiv 0[4]$, donc $10^i\equiv 0[4]$ pour $i\geqslant 2$.

$$n=\sum_{i=0}^{\infty}n_i10^i=\sum_{i=2}^{\infty}n_i10^i+10n_1+n_0\equiv 10n_1+n_0[4]$$

- Pour 5, on a $10\equiv 0[5]$, donc $10^i\equiv 0[5]$ pour $i\geqslant 1$.

$$n=\sum_{i=0}^{\infty}n_i10^i=\sum_{i=1}^{\infty}n_i10^i+n_0\equiv n_0[5]$$

  Et un entier entre 0 et 9 est divisible par 5 si et seulement si il est égal à 0 ou à 5.

- L'entier 6 est le ppcm de 2 et de 3. Donc un entier est multiple de 6 si et seulement si il est multiple à la fois de 2 et de 3. Le critère pour 6 est la conjonction des critères pour 2 et pour 3.

- Pour 7, on a $10\equiv 3[7]$, donc $5\cdot 10\equiv 15\equiv 1[7]$ et $5\cdot 10^i\equiv 10^{i-1}[7]$. Comme 7 et 5 sont premiers entre eux, n est divisible par 7 et seulement si $5n$ l'est. On a alors

$$5n=5\sum_{i=0}^{\infty}n_i10^i\equiv 5\sum_{i=1}^{\infty}n_i10^i+5n_0\equiv\sum_{i=1}^{\infty}n_i10^{i-1}+5n_0[7]$$

- Pour 8, on a $1000 \equiv 0[8]$, donc $10^i \equiv 0[8]$ pour $i \geqslant 3$.

$$n = \sum_{i=0}^{\infty} n_i 10^i = \sum_{i=3}^{\infty} n_i 10^i + 100n_2 + 10n_1 + n_0 \equiv 100n_2 + 10n_1 + n_0[8]$$

- Pour 9, on a $10 \equiv 1[9]$ donc $10^i = 1[9]$ pour tout i. On a donc

$$n = \sum_{i=0}^{\infty} n_i 10^i \equiv \sum_{i=0}^{\infty} n_i[9]$$

- Pour 11, on a $10 \equiv -1[11]$, donc $10^i \equiv (-1)^i[11]$ pour tout i. On a donc

$$n = \sum_{i=0}^{\infty} n_i 10^i \equiv \sum_{i=0}^{\infty} n_i(-1)^i[11]$$

2. C'est le même raisonnement que pour 7. Comme $10j \equiv 1[k]$, on a que j est premier avec k. Donc n est divisible par k si et seulement si nj est divisible par k. On a

$$jn = j\sum_{i=0}^{\infty} n_i 10^i \equiv \sum_{i=1}^{\infty} n_i j 10^i + jn_0 \equiv \sum_{i=1}^{\infty} n_i 10^{i-1} + jn_0[k]$$

soit le critère voulu.

Exercice 3.

1. Supposons que n soit inversible modulo 18, autrement dit il existe m tel que $mn \equiv 1[18]$. Il existe alors un certain entier k tel que

$$mn - 1 = 18k \Leftrightarrow mn - 18k = 1$$

Par le théorème de Bézout, on obtient que m et 18 doivent être premiers entre eux. On a d'ailleurs la réciproque : si m est premier avec 18, on trouve par Bézout que m est inversible modulo 18.

Les éléments de $\mathbb{Z}/18\mathbb{Z}$ sont représentés par les entiers $0, \dots 17$. Ceux de ces entiers qui sont premiers à 18 sont $1, 5, 7, 11, 13, 17$. On a

$$1 \cdot 1 \equiv 1[18], \quad 13 \cdot 7 \equiv 91 \equiv 1[18], \quad 5 \cdot 11 \equiv 55 \equiv 1[18], \quad 17 \cdot 17 \equiv (-1)^2 \equiv 1[18]$$

Il y a donc 6 éléments inversibles dans l'anneau $\mathbb{Z}/18\mathbb{Z}$.

2. Comme 17 est premier, tous les nombres $1, \dots 16$ sont premiers avec 17, la question a donc un sens. Pour chaque entier k, trouver son inverse u modulo 17 revient à trouver une relation de Bézout de la forme $ku + 17v = 1$. On trouve une telle relation via l'algorithme d'Euclide. De plus, si l'on a $ab \equiv 1[17]$, on a également $(-a)(-b) \equiv 1[17]$, cela nous fera gagner du temps.

- Pour $k = 2$, on a

$$17 = 2 \cdot 8 + 1$$

  Donc 2 est l'inverse de $-8 \equiv 9[17]$. De même 8 est l'inverse de $-2 \equiv 15[17]$.

- Pour $k = 3$, on a $17 = 3 \cdot 5 + 2$ et $3 = 2 + 1$, donc

$$1 = 3 - 2 = 3 - (17 - 3 \cdot 5) = 3 \cdot 6 - 17$$

  donc 3 et 6 sont inverses l'un de l'autre modulo 17. De même $-3 \equiv 14[17]$ est l'inverse de $-6 \equiv 11[17]$.

- Pour $k = 4$, on a

$$17 = 4 \cdot 4 + 1$$

  Donc 4 est l'inverse de $-4 = 13[17]$. La même relation avec des signes $-$ ne nous apprend rien de plus.

- Pour $k=5$, on a $17 = 5\cdot 3+2$ et $5 = 2\cdot 2+1$, donc

$$1 = 5 - 2\cdot 2 = 5 - 2(17 - 5\cdot 3) = -2\cdot 17 + 7\times 5$$

donc 5 et 7 sont inverses l'un de l'autre modulo 17. De même $-5 \equiv 12[17]$ est l'inverse de $-7 \equiv 10[17]$.
- Tous les cas $k = 6,7,8,9,10,11,12,13,14,15$ sont déjà apparus plus haut.
- Pour $k=16$, on a $16 \equiv (-1)[17]$ est son propre inverse.

Au final on obtient le tableau suivant

1	2	3	4	5	8	10	11	16
1	9	6	13	7	15	12	14	16

3. C'est exactement la même question qu'au dessus, juste formulée différemment. À nouveau 13 étant premier, toutes les classes de congruences non nulles modulo 13 sont inversibles.
- Pour $k=2$, on a
$$13 = 2\cdot 6+1$$
Donc 2 est l'inverse de $-6 \equiv 7[13]$. De même 6 est l'inverse de $-2 \equiv 11[13]$.
- Pour $k=3$, on a
$$13 = 3\cdot 4+1$$
Donc 3 est l'inverse de $-4 \equiv 9[13]$. De même 4 est l'inverse de $-3 \equiv 10[13]$.
- Le cas $k=4$ a déjà été traité.
- Pour $k=5$, on a
$$1 = 13\cdot 2 - 5\cdot 5$$
Donc 5 est l'inverse de $-5 \equiv 8[13]$.

Au final on obtient le tableau suivant

1	2	3	4	5	6	12
1	7	9	10	8	11	12

Exercice 4.
1. Pour $k \geqslant 1$, on a

$$\begin{aligned}10^k+1 &= 10^k + 10^{k-1} - 10^{k-1} + 1\\ &= 10^k + 10^{k-1} - (10^{k-1}+1) + 2\\ &= 9(10^{k-1}+1)+2\end{aligned}$$

On a évidemment $10^1 + 1 = 1 \equiv 11[3]$. Appliquant ce qui précède, on obtient

$$10^2+1 = 9\cdot 11 + 2 = 101 \equiv 10[13]$$

$$10^3+1 = 9\cdot 10 + 2 = 92 \equiv 1[13]$$

$$10^4+1 = 9\cdot 1 + 2 = 11 \equiv 11[13]$$

2. On a $5^2 = 25 \equiv 2[23]$. Donc

$$\begin{aligned}5^{10} &= (5^2)^5 \equiv 2^5 \equiv 32 \equiv 9[23]\\ 5^{11} &= 5\cdot 5^{10} \equiv 5\cdot 9 \equiv -1[23]\\ 5^{22} &= (5^{11})^2 \equiv 1[23]\end{aligned}$$

3. Tout entier est congru modulo 9 à son reste dans sa division euclidienne par 9. Ce reste est un entier compris entre 0 et 9. Par ailleurs on a $5 \equiv -4[9], 6 \equiv -3[9], 7 \equiv -2[9]$ et $8 \equiv -1[9]$, d'où le résultat. L'unicité provient du fait que la différence de deux entiers compris entre -4 et 4 est inférieure à 8, donc deux entiers compris entre -4 et 4 ne peuvent être congrus l'un à l'autre modulo 9.

4. a) Dire que $f_p(a)$ est un entier équivaut à dire que p divise $a^{p-1}-1$, autrement dit que $a^{p-1} \equiv 1[p]$: c'est le petit théorème de Fermat.
b). On a

$$\begin{aligned}
f_p(ab) &= \frac{(ab)^{p-1}-1}{p} \\
&= \frac{a^{p-1}b^{p-1}-b^{p-1}}{p} + \frac{b^{p-1}-1}{p} \\
&= f_p(a)b^{p-1} + f_p(b) \\
&\equiv f_p(a) + f_p(b)[p]
\end{aligned}$$

Car $b^{p-1} \equiv 1[p]$ d'après la question précédente.

Exercice 5.
1. Comme a est premier à p, le petit théorème de Fermat nous donne que $a^{p-1} \equiv 1 \equiv a^0[p]$. On a alors pour tout $n \in N$

$$a^{p-1+n} \equiv a^n[p]$$

autrement dit la suite $(a^n[p])$ est périodique de période $p-1$. Peut-être cette période n'est pas optimale et selon les cas, on pourra trouver une période plus courte, mais $p-1$ sera systématiquement une période.

2. Les termes successifs de la suite sont

$$1, \quad 2, \quad 4, \quad 8 \equiv 1[7], \quad 2, \quad 4, \quad 1, \quad \ldots$$

La suite est ici de période 3, qui est un diviseur de $p-1=6$.

3. Les termes successifs de la suite sont

$$1, \quad 3, \quad 9 \equiv 2[7], \quad 6, \quad 18 \equiv 4[7], \quad 12 \equiv 5[7], \quad 15 \equiv 1[7]$$

On a donc une suite périodique de période 6 cette fois-ci.

† *Équations en 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

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