Correction séance 3 (29 septembre)

† *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

$$n:=\sum_{i=0}^{\infty} n_i 10^i$$

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 $i \geqslant 1$.

$$n=\sum_{i=0}^{\infty} n_i 10^i=\sum_{i=1}^{\infty} n_i 10^i+n_0 \equiv n_0[2]$$

  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

$$n=\sum_{i=0}^{\infty} n_i 10^i \equiv \sum_{i=0}^{\infty} n_i[3]$$

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

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

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

$$n=\sum_{i=0}^{\infty} n_i 10^i=\sum_{i=1}^{\infty} n_i 10^i+n_0 \equiv n_0[5]$$

  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

$$5n=5\sum_{i=0}^{\infty} n_i 10^i \equiv 5\sum_{i=1}^{\infty} n_i 10^i+5n_0 \equiv \sum_{i=1}^{\infty} n_i 10^{i-1}+5n_0[7]$$

- 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 $0, \ldots 17$. 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 $1, \ldots 16$ 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 $17=5\cdot3+2$ et $5=2\cdot2+1$, donc

$$1=5-2\cdot2=5-2(17-5\cdot3)=-2\cdot17+7\times5$$

donc 5 et 7 sont inverses l'un de l'autre modulo 17. De même $-5\equiv12[17]$ est l'inverse de $-7\equiv10[17]$.
- 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

$$13=2\cdot6+1$$

Donc 2 est l'inverse de $-6\equiv7[13]$. De même 6 est l'inverse de $-2\equiv11[13]$.
- Pour $k=3$, on a

$$13=3\cdot4+1$$

Donc 3 est l'inverse de $-4\equiv9[13]$. De même 4 est l'inverse de $-3\equiv10[13]$.
- Le cas $k=4$ a déjà été traité.
- Pour $k=5$, on a

$$1=13\cdot2-5\cdot5$$

Donc 5 est l'inverse de $-5\equiv8[13]$.

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 $k\geqslant1$, 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 $10^1+1=1\equiv11[3]$. Appliquant ce qui précède, on obtient

$$10^2+1=9\cdot11+2=101\equiv10[13]$$

$$10^3+1=9\cdot10+2=92\equiv1[13]$$

$$10^4+1=9\cdot1+2=11\equiv11[13]$$

2. On a $5^2=25\equiv2[23]$. Donc

$$\begin{aligned}5^{10}=(5^2)^5\equiv2^5\equiv32\equiv9[23]\\5^{11}=5\cdot5^{10}\equiv5\cdot9\equiv-1[23]\\5^{22}=(5^{11})^2\equiv1[23]\end{aligned}$$

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.