Divisibilité et congruences (f)

Exercice f.1 (1) On a $x^3+1 = x^3-(-1)^3 = (x+1)(x^2-x+1)$ donc $x+1$ divise x^3+1.

(2) *Après avoir cherché un peu on se rend compte que pour démontrer l'hérédité, i.e. pour montrer que $P(k) \Rightarrow P(k+1)$, il faut utiliser la question (1) avec $x = x_k := 2^{3^k}$. On se rend compte ensuite que ça ne suffit pas tout à fait et qu'il faut écrire $(x_k)^3+1 = (x_k+1)((x_k)^2-x_k+1)$ et montrer que le $2^{\text{ème}}$ facteur $(x_k)^2-x_k+1$ est lui aussi multiple de 3.*

Autres remarques :

(a) *La factorisation $a^n-b^n = (a-b)(a^{n-1}+a^{n-2}b+\cdots+b^{n-1})$ est à connaître !*

(b) *Dans cet exercice il faut se méfier : on ne peut pas vraiment raisonner avec des congruences car la « base » de la congruence est variable : on devrait raisonner modulo 3^k or k varie...*

Soit pour $k \geq 1$ la propriété $P(k)$: $3^k \mid 2^{3^k}+1$.

Comme 3 divise $2^3+1 = 9$, la propriété $P(1)$ est vraie.

Soit $k \geq 1$ un entier et montrons que $P(k) \Rightarrow P(k+1)$. Écrivons la factorisation de la question (1) avec $x = x_k := 2^{3^k}$:

$$(x_k)^3+1 = (x_k+1)((x_k)^2-x_k+1)$$

D'une part, par hypothèse de récurrence on a $P(k)$: $3^k \mid 2^{3^k}+1 = x_k+1$ c'est-à-dire qu'il existe $q_k \in \mathbb{N}$ tel que $x_k+1 = 3^k q_k$.

D'autre part, de $3^k \mid x_k+1$ on déduit que $x_k+1 \equiv 0\ (3)$ donc $x_k \equiv -1 \equiv 2\ (3)$. Alors

$$(x_k)^2-x_k+1 \equiv 2^2-2+1 \equiv 0\ (3)$$

donc il existe $r_k \in \mathbb{N}$ tel que $(x_k)^2-x_k+1 = 3r_k$. En multipliant il vient

$$(x_k)^3+1 = (x_k+1)((x_k)^2-x_k+1) = 3^{k+1}q_k r_k$$

Donc 3^{k+1} divise $(x_k)^3+1 = 2^{3^{k+1}}+1$, i.e. $P(k+1)$ est vraie. Par le principe de récurrence, $P(k)$ est vraie pour tout $k \geq 1$.

Exercice f.2 Le reste de la DE de n par 5 vaut 0, 1, 2, 3 ou 4. C'est-à-dire, n est congru modulo 5 à l'un de ces 5 nombres.

$$\begin{array}{ll}
\text{Si } n \equiv 0, & n^5-n \equiv 0.\\
\text{Si } n \equiv 1, & n^5-n \equiv 1^5-1 \equiv 0.\\
\text{Si } n \equiv 2, & n^5-n \equiv 2^5-2 \equiv 32-2 \equiv 30 \equiv 0.\\
\text{Si } n \equiv 3, & n^5-n \equiv 3^5-3 \equiv 243-3 \equiv 0.\\
\text{Si } n \equiv 4, & n^5-n \equiv 4^5-4 \equiv 1024-4 \equiv 0.
\end{array}$$

Dans tous les cas, $n^5-n \equiv 0\ (5)$ i.e. il est divisible par 5.

On a déjà vu que $n^2 - n$ est toujours divisible par 2, $n^3 - n$ est toujours divisible par 3, $n^5 - n$ est toujours divisible par 5,... Les deux exercices suivants montrent que $n^p - n$ est toujours divisible par p si p est un nombre premier. Lorsque p n'est pas premier c'est faux : voir d.4(3).

Exercice f.3 On se rappelle un des premiers exercices du cours où on a montré que $i\mathrm{C}_p^i = p\mathrm{C}_{p-1}^{i-1}$ pour $0 < i < p$. Ainsi p divise $i\mathrm{C}_p^i$, or comme p est premier avec i, par le lemme de Gauß p divise C_p^i.

Exercice f.4 (1) Il faut utiliser l'exercice précédent. On développe $(a+b)^p$ par la formule du binôme de Newton :

$$(a+b)^p = \sum_{k=0}^{p} \mathrm{C}_p^k a^k b^{p-k} = a^p + \mathrm{C}_p^1 ab^{p-1} + \cdots + \mathrm{C}_p^{p-1} a^{p-1} b + b^p$$

D'après l'exercice f.3, modulo p tous les coefficients binômiaux sont congrus à zéro (sauf pour les deux termes extrêmes), et donc $(a+b)^p \equiv a^p + b^p\ (p)$.

(2) Raisonnons modulo p ; on note $a \equiv b$ au lieu de $a \equiv b\ (p)$. On montre la propriété $P(n)$: $n^p - n \equiv 0$. Pour $n = 0$ c'est clair. Soit $n \geq 0$ tel que $P(n)$ soit vraie. Alors en utilisant la question précédente on a $(n+1)^p - (n+1) \equiv n^p + 1^p - (n+1) \equiv n^p - n \equiv 0$ d'après l'hypothèse de récurrence. Donc $P(n+1)$ est vraie. Par le principe de récurrence, $P(n)$ est vraie pour tout $n \geq 0$.

(3) *Si p n'est pas premier ? Comme d'habitude, on expérimente pour se faire une idée. Le plus petit nombre non premier est 4. Le plus petit nombre n pour lequel $n^4 - n$ a une chance d'être non divisible par 4 est $n = 2$. On calcule : $n^4 - n = 2^4 - 2 = 14$ qui n'est pas divisible par 4 ! On a trouvé un contre-exemple. On répond ainsi :*

Il n'est pas vrai que la propriété ait lieu pour tout entier p, car pour $p = 4$ et $n = 2$ on a $n^4 - n = 2^4 - 2 = 14$ qui n'est pas divisible par 4. C'est donc une propriété « magique » des nombres premiers.

Exercice f.5 Soit E l'équation $x^y = y^x$ dans $\mathbb{N}$. Écartons d'abord un cas particulier : 0^0 est indéfini donc $x = y = 0$ n'est pas une solution, et si x ou y seulement est nul, E s'écrit $0 = 1$, impossible. Donc si (x, y) est une solution, ni x ni y n'est nul.

Cherchons alors les solutions avec $x > 0$ et $y > 0$. D'abord il y a bien sûr tous les couples (x, y) tels que $x = y$ (sauf $x = y = 0$). Supposons maintenant que $x < y$ (par exemple). Alors, suivant l'indication, on montre que $x|y$: en effet $x \leq y$ entraîne que x^x divise x^y, i.e. $x^x | x^y$, et comme $x^y = y^x$ on a $x^x | y^x$. Donc $x|y$ d'après un exercice qu'on a déjà fait (*c'était : $a|b$ ssi $a^n|b^n$*). Cela veut dire qu'il existe $k \in \mathbb{N}$, $k > 1$, tel que $y = kx$. Reportons cela dans E : on a $x^{kx} = (kx)^x = k^x x^x$. Il en découle $x^{(k-1)x} = k^x$ donc $x^{k-1} = k$ (*comme on travaille avec des nombres entiers, $a^x = b^x \Rightarrow a = b$*).

Résolvons à part cette équation, sachant que $k > 1$. Si $k = 2$ on obtient $x = k = 2$ donc $y = kx = 4$, c'est en effet une solution de E. Si $k \geq 3$, comme $x = 1$ n'est jamais solution, on a $x \geq 2$, donc $x^{k-1} \geq 2^{k-1}$. Or on montre par une récurrence facile que $2^{k-1} > k$ pour tout $k \geq 3$, donc $x^{k-1} > k$, donc dans ce cas il n'y a pas de solution. En conclusion les solutions avec x et y positifs sont tous les couples (x, x) avec $x > 0$, et $(2, 4)$, et $(4, 2)$.

Exercice f.6 (1) *« Résoudre » veut dire « trouver toutes les solutions de ». Vous avez tous vu rapidement qu'on trouve des solutions de l'équation lorsque x est congru à 2 modulo 5, i.e.*

$x = 2 + 5n$ avec n entier. Le problème était ensuite de rédiger correctement la réponse : est-ce que j'ai là toutes les solutions ? Comment le montrer ? Que faut-il montrer ?

Pour cela je donne deux solutions. Dans la première on évite le recours aux congruences, qui gêne encore beaucoup d'entre vous. On observe (écrivez la table de multiplication des restes modulo 5) que lorsque $x = 2$ on a une solution. D'autres essais donnent $x = 7$, $x = 12$... En fait tous les $x \equiv 2\ (5)$ marchent. Il reste à montrer que l'ensemble S des solutions et l'ensemble T des nombres qui sont congrus à 2 modulo 5 sont les mêmes. Pour cela une seule méthode : montrer que $S \subset T$, puis que $T \subset S$!

Dans la deuxième solution ou calcule directement avec les congruences, ça va très vite !

1ère solution. On va montrer que tout nombre x dont le reste dans la DE par 5 est 2 (càd x est congru à 2 modulo 5) est une solution. S'il y a un entier n tel que $x = 5n + 2$ alors $3x = 3(5n + 2) = 15n + 6 = 15n + 5 + 1$ qui est bien congru à 1 modulo 5. Donc c'est une solution.

Il faut maintenant montrer que ce sont là les seules solutions, c'est-à-dire qu'une solution de l'équation est congrue à 2 modulo 5. Écrivons la DE de x par 5 : $x = 5n + r$ avec $0 \leq r < 5$. On a $3x = 15n + 3r$, donc si x est une solution de l'équation on doit avoir $3x \equiv 1 \equiv 3r\ (5)$. Or $3r$ vaut 0, 3, 6, 9 ou 12 car $0 \leq r < 5$. Seul 6 est congru à 1 modulo 5, correspondant à $r = 2$. Donc $x = 5n + 2$.

On conclut que les solutions de l'équation sont les nombres congrus à 2 modulo 5, c'est-à-dire les nombres de la forme $x = 2 + 5k$ $(k \in \mathbb{Z})$.

2ème solution. On raisonne modulo 5, on note $a \equiv b$ au lieu de $a \equiv b\ (5)$.
Le reste de la DE de x par 5 est l'un des nombres 0, 1, 2, 3 ou 4. On écrit les multiples de 3 :

x	$x \equiv 0$	$x \equiv 1$	$x \equiv 2$	$x \equiv 3$	$x \equiv 4$
$3x$	$3x \equiv 0$	$3x \equiv 3$	$3x \equiv 6 \equiv 1$	$3x \equiv 9 \equiv 4$	$3x \equiv 12 \equiv 2$

Donc si $x \equiv 2$, x est une solution de l'équation proposée. De plus si $x \not\equiv 2$ (i.e. si x est congru à 0, 1, 3 ou 4) alors $3x \not\equiv 1$ comme le montrent les calculs ci-dessus, c'est-à-dire que x n'est pas solution. En conclusion, l'ensemble des solutions est l'ensemble des entiers relatifs congrus à 2 modulo 5, c'est-à-dire les nombres de la forme $x = 2 + 5k$ $(k \in \mathbb{Z})$.

(2) L'équation est maintenant $5x \equiv 2\ (7)$. On raisonne modulo 7, on note $a \equiv b$ au lieu de $a \equiv b\ (7)$. Le reste de la DE de x par 7 est l'un des nombres 0, 1, 2, 3, 4, 5, 6. On écrit les multiples de 5 modulo 7 :

x	$x \equiv 0$	$x \equiv 1$	$x \equiv 2$	$x \equiv 3$	$x \equiv 4$	$x \equiv 5$	$x \equiv 6$
$5x$	$5x \equiv 0$	$5x \equiv 5$	$5x \equiv 10 \equiv 3$	$5x \equiv 15 \equiv 1$	$5x \equiv 20 \equiv 6$	$5x \equiv 25 \equiv 4$	$5x \equiv 30 \equiv 2$

Donc si $x \equiv 6$, x est une solution de l'équation proposée. De plus si $x \not\equiv 6$ alors $5x \not\equiv 2$ comme le montre le tableau, c'est-à-dire que x n'est pas solution. En conclusion, l'ensemble des solutions est l'ensemble des entiers relatifs congrus à 6 modulo 7, c'est-à-dire les nombres de la forme $x = 6 + 7k$ $(k \in \mathbb{Z})$.

(3) *Pour raisonner par congruence on est un peu coincé : il faut choisir modulo 5 ou modulo 7, on ne peut pas faire les deux ! Après quelques essais de calculs on voit que le nombre $5 \times 7 = 35$ semble jouer un grand rôle.*

On doit trouver les $x \in \mathbb{Z}$ tels que $3x \equiv 1\ (5)$ et $5x \equiv 2\ (7)$. Soit x une solution de ces deux équations, donc par ce qui précède, $x \equiv 2\ (5)$ et $x \equiv 6\ (7)$.

Soit la DE de x par 35 : $x = 35q + r$ avec $0 \leq r < 35$. Comme $x \equiv 2\ (5)$ on doit avoir $r \in \{2, 7, 12, 17, 22, 27, 32\}$. Comme $x \equiv 6\ (7)$ on doit avoir $r \in \{6, 13, 20, 27, 34\}$. Finalement, seul $r = 27$ convient. Donc, $x \equiv 27\ (35)$.

On a montré qu'une solution est congrue à 27 modulo 35. Réciproquement, soit un entier $x = 35q + 27$, $q \in \mathbb{Z}$. Il est clair que $x \equiv 2\ (5)$ et $x \equiv 6\ (7)$, donc x est solution des deux équations simultanément.

En conclusion les solutions de (1) et (2) sont les entiers relatifs congrus à 27 modulo 35.

Exercice f.7 La DFP de 217 est $217 = 7\times 31$. Donc les diviseurs de 217 dans $\mathbb{Z}$ sont $1, 7, 31, 217$ et leurs opposés.

Résolvons maintenant l'équation proposée. Soit (x, y) un couple solution, il vérifie : $x^3+y^3 = (x + y)(x^2 - xy + y^2) = 217$. En particulier $x + y$ divise 217, donc vaut $1, 7, 31, 217$ ou l'un de leurs opposés. On va les passer en revue. On observe que $x^2 - xy + y^2 = (x + y)^2 - 3xy$, ce qui nous aidera dans la suite.

(1) Si $x+y = 1$ alors $x^2-xy+y^2 = (x+y)^2-3xy = 1-3xy$ donc l'équation s'écrit $1-3xy = 217$ càd $-xy = 72$. Comme $y = 1-x$ on trouve une équation de degré 2 : $x(x-1) = 72$ de solutions $x = 9$ ou $x = -8$.

Si $x+y = -1$ alors $x^2-xy+y^2 = 1-3xy$ est inchangé donc l'équation s'écrit $1-3xy = -217$ càd $3xy = 218$. Comme 218 n'est pas multiple de 3 il n'y a pas de solution entière.

(2) Si $x + y = 7$ alors $x^2 - xy + y^2 = 49 - 3xy$ donc l'équation s'écrit $7(49 - 3xy) = 217$ càd $xy = 6$. Comme $y = 7 - x$ on tombe sur l'équation $x(7 - x) = 6$ de solutions $x = 1$ ou $x = 6$.

Si $x + y = -7$ alors $x^2 - xy + y^2 = 49 - 3xy$ et l'équation s'écrit $3xy = 80$. Comme 80 n'est pas multiple de 3 il n'y a pas de solution entière.

(3) Si $x + y = 31$ alors $x^2 - xy + y^2 = 961 - 3xy$ donc l'équation s'écrit $31(961 - 3xy) = 217$ càd $xy = 318$. Comme $y = 31 - x$ on tombe sur l'équation $x(31 - x) = 318$. Le discriminant est <0 donc il n'y a pas de solution réelle, donc pas de solution entière.

Si $x + y = -31$ alors $x^2 - xy + y^2 = 961 - 3xy$ et l'équation s'écrit $3xy = 968$. Comme 968 n'est pas multiple de 3 il n'y a pas de solution entière.

(4) Si $x + y = 217$ alors $x^2 - xy + y^2 = 217^2 - 3xy$ donc l'équation s'écrit $217^2 - 3xy = 1$ i.e. $3xy = 217^2 - 1 = (217 - 1)(217 + 1)$ i.e. $xy = 72 \times 218$. Comme $y = 217 - x$ on tombe sur l'équation $x(217 - x) = 72 \times 218$ de discriminant <0 donc il n'y a pas de solution réelle, donc pas de solution entière.

Si $x + y = -217$ alors $x^2 - xy + y^2 = 217^2 - 3xy$ donc l'équation s'écrit $217^2 - 3xy = -1$ i.e. $3xy = 217^2 + 1$. Comme $217^2 + 1$ n'est pas multiple de 3 (vérification : $217 \equiv 1\ (3)$ donc $217^2 + 1 \equiv 1 + 1 \equiv 2\ (3)$) il n'y a pas de solution entière.

En conclusion les solutions de E sont les couples $(9, -8)$, $(8, -9)$, $(1, 6)$, $(6, 1)$. On peut vérifier que pour chacun de ces couples on a $x^3 + y^3 = 217$!