Feuille d'exercices n^{o}17 : Arithmétique dans les entiers

Exercice 1 [Quelques divisibilités]

Par récurrence. Initialisation immédiate et pour l'hérédité :

1. $3^{2n+3}+2^{n+3}=9\cdot 3^{2n+1}+2\cdot 2^{n+2}=7\cdot 3^{2n+1}+2\cdot(3^{2n+1}+2^{n+2})$;
2. $5^{n+1}-1-4(n+1)=5\cdot 5^n-1-4n-4=5\cdot(5^n-1-4n)+16n$;
3. $(n+1)(n+2+1)(7n-5+7)=n(n+2)(7n-5)+21n^2+39n+6=n(n+2)(7n-5)+3n\cdot(7n+13)+6$ où $n(7n+13)$ est toujours pair (disjonction suivant la parité de n) ce qui donne bien un multiple de 6 à la fin.

Exercice 2 [Divisibilités . . . ou pas !]

On fait des combinaisons linéaires (à coefficients entiers) pour montrer que l'on a des divisions avec des nombres plus petits, donc on explicite tous les diviseurs.

1. si n divise n^2+1, alors n divise $1=(n^2-1)-n\cdot n$ donc $n=\pm 1$. Réciproque vraie. Donc divisions ssi $n=\pm 1$.
2. si $n+1$ divise n^2+1, alors $n+1$ divise $2n=(n+1)^2-(n^2+1)$ puis $n+1$ divise $2=2(n+1)-2n$. Donc $n+1=\pm 2$ ou ± 1. Donc $n\in\{-3,-2,0,1\}$. Réciproque vraie. Donc division ssi $n\in\{-3,-2,0,1\}$.
3. si $n-4$ divise $3n-17$, alors $n-4$ divise $5=3(n-4)-(3n-17)$ donc $n-4\in\{\pm 1,\pm 5\}$ donc $n\in\{-1,3,5,9\}$. Réciproque vraie. Donc division ssi $n\in\{-1,3,5,9\}$.
4. si $n-1$ divise $2n^2-2n+4$, alors $n-1$ divise $4=2n^2-2n+4-2n(n-1)$ donc $n-1\in\{\pm 1,\pm 2,\pm 4\}$. Donc $n\in\{-3,-1,0,2,3,5\}$. Réciproque vraie. Donc division ssi $n\in\{-3,-1,0,2,3,5\}$.

Exercice 3 [Nombres non premiers consécutifs]

Un nombre entre $n!$ et $n!+n$ est de la forme $n!+k$ pour $k\in[\![2;n]\!]$. Mais k et $n!$ sont divisibles par k, donc $n!+k$ aussi. Et $n!+k>k>1$, donc $n!+k$ admet un diviseur non trivial (compris strictement entre 1 et lui-même) : il n'est pas premier.

Exercice 4 [Calculs de pgcd]

On passe par l'algorithme d'Euclide

1. $94\wedge 267=1$;
2. $106\wedge 317=1$;
3. $82\wedge 519=1$;
4. $9348\wedge 1640=164$;
5. $25\wedge 38=1$;
6. $19\wedge 54=1$;
7. $18\wedge 29=1$;
8. $51\wedge 148=1$;
9. $293\wedge 107=1$.

Exercice 5 [Couples d'entiers premiers entre eux]

On essaie de faire une division avec un reste petit (un peu comme une division euclidienne) pour montrer que les diviseurs sont "petits" :

1. $(n+1)!+1 = (n+1)\cdot(n!+1) - n$ donc un diviseur commun divise n. Puis $n!+1 = n\cdot((n-1)!)+1$ donc un diviseur commun divise 1 : $n!$ et $(n+1)!+1$ sont premiers entre eux.

2. $3^{n+1}+2^{n+1} = 3\cdot(3^n+2^n) - 2^n$ donc un diviseur commun divise 2^n (et est donc au signe près une puissance de 2). Mais $3^{n+1}+2^{n+1}$ est impair (impair + pair = impair), donc la seule puissance de 2 qui le divise est 1. Donc $3^{n+1}+2^{n+1}$ et 3^n+2^n sont premiers entre eux.

Exercice 6 [Famille d'entiers deux-à-deux premiers entre eux]

Soient $i, j \in \{1, \dots, n+1\}$ distincts. Si d divise a_i et a_j, alors d divise $ja_i - ia_j = j - i$. Donc d divise $n!$ (car $j-i$ apparaît comme facteur dans $n!$), donc d divise $1 = a_i - in!$.

Donc a_i et a_j sont premiers entre eux.

Exercice 7 [Divisions dans les puissances]

On suppose que m divise n. On pose $n = mk$ (pour $k \in \mathbb{N}$). Alors :

$$a^n - b^n = a^{mk} - b^{mk} = (a^m)^k - (b^m)^k = (a^m - b^m)\underbrace{\left(\sum_{i=0}^{k-1}(a^m)^i\,(b^m)^{k-1-i}\right)}_{\in\mathbb{Z}}$$

et on a bien que $a^m - b^m$ divise $a^n - b^n$.

Exercice 8 [Un critère de double divisibilité]

On prend les valeurs de x^2 et y^2 modulo 7. On a le tableau suivant :

x [7]	0	± 1	± 2	± 3
x^2 [7]	0	1	$4 = -3$	$2 = -5$

Et ainsi :

- si $7|x$ et $7|y$: alors $7|x^2$ et $7|y^2$ donc $7|x^2+y^2$;
- si $7|x^2+y^2$: alors x^2 et y^2 sont opposés modulo 7. Mais le seul nombre qui possède son opposé dans la seconde ligne du tableau est 0, qui est son propre opposé. Donc $7|x$ et $7|y$.

Exercice 9 [Critères usuels de divisibilité]

On considère un entier $n \in \mathbb{N}$, dont on note $a_0, \dots a_m$ les chiffres dans l'écriture décimale.

1. Pour $N \in \{2, 5, 10\}$ on a : $n \equiv a_0\ [N]$ donc $N|n \Leftrightarrow N|a_0$ c'est-à-dire :
   - pour $N = 2$: $a_0 \in \{0, 2, 4, 6, 8\}$;
   - pour $N = 5$: $a_0 \in \{0, 5\}$;
   - pour $N = 10$: $a_0 = 0$.

2. Pour tout $k \in \mathbb{N}$ le reste de la division euclidienne de 10^k par 3 et par 9 vaut 1. Pour $N \in \{3, 9\}$ on a donc : $n \equiv \sum_{i=0}^{m} a_i$. Donc n est divisible par N si, et seulement si, la somme des chiffres de n (en base 10) est un multiple de N (valable pour $N = 3$ ou $N = 9$).

3. Le reste de la division euclidienne de 10^{2k} par 11, et celui de 10^{3k} par 37 valent 1. On retrouve les critères de divisibilité par 11 et 37 :

- un nombre est un multiple de 11 si, et seulement si, la somme de ses chiffres groupés par 2 à partir des unités est un multiple de 11 ;
- un nombre est un multiple de 37 si, et seulement si, la somme de ses chiffres groupés par 3 à partir des unités est un multiple de 37.

Et on a même mieux : dans les deux cas, la somme obtenu a même reste dans la division euclidienne par 37 ou 11 (suivant les cas).

Exercice 10 [Amélioration du critère de divisibilité par 37]

La nullité du reste dans la division euclidienne par 37 est préservée. En multipliant par 3, on a ainsi un multiple de 37 au départ si, et seulement si, on a un multiple de $3 \times 37 = 111$ à l'arrivée : la condition nécessaire et suffisante cherchée est donc $a = b = c$.

Exercice 11 [Un autre critère de divisibilité]

1. Par récurrence : $10^n \equiv 1\ [11]$ si n est pair et -1 si n est impair.
2. Un nombre est un multiple de 11 si, et seulement si, la somme alternée de ses chiffres (c'est-à-dire la différence entre la somme de ses chiffres et rangs pairs et ceux de rangs impairs) est un multiple de 11.

Exercice 12 [Équations d'entiers]

1. $7x = 4y^3$: pour (x, y) solution, y est un multiple de 7 et x est un multiple de 4. Si on écrit $x = 4a$ et $y = 7b$, on obtient $a = 49b^3$. Et pour tout $b \in \mathbb{Z}$, le couple $(4 \cdot 49b^3, 7b)$ est solution.
2. $xy = 3x + 2y$: on a $xy = 3x + 2y \Leftrightarrow (x-2)(y-3) = 6$. En notant $a = y - 3$, on déduit que pour (x, y) solution $a \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Si on fixe un tel a, alors (x, y) (non nuls) forme une solution si, et seulement si, $x = \dfrac{6}{a} + 2$ et $y = 3 + a$. Ce qui donne comme solutions :

$$(8,4),\ (-4,2),\ (5,5),\ (-1,1),\ (4,6),\ (0,0),\ (3,9),\ (1,-3)$$

correspondant (dans l'ordre) à a valant $1, -1, 2, -2, 3, -3, 6, -6$.

3. $\dfrac{1}{x} + \dfrac{1}{y} = \dfrac{1}{5} : \dfrac{1}{x} + \dfrac{1}{y} = \dfrac{1}{5} \Leftrightarrow (x-5)(y-5) = 25$. Même méthode en posant $a = y - 5 \in \{\pm 1, \pm 5, \pm 25\}$ qui donne comme solutions :

$$(30,6),\ (-20,4),\ (10,10),\ (6,30),\ (4,-20)$$

(on a retiré $a = 5$ qui donne $x = y = 0$ qui est exclu de l'ensemble des solutions).

4. $17x + 11y = a$ $(a \in \mathbb{Z})$; on utilise $17 \times 2 - 11 \times 3 = 1$ donc $(2a, -3a)$ est une solution. Et pour $(x, y) \in \mathbb{Z}^2$:

$$17x + 11y = a \Leftrightarrow 17x + 11y = 17 \times 2a + 11 \times (-3a) \Leftrightarrow 17(2a - x) = 11(y + 3a)$$

et alors $y - 3a$ est un multiple de 17 donc de la forme $y + 3a = 17n$ (pour $n \in \mathbb{Z}$) ce qui donne $2a - x = 11n$ (pour le même n). Et finalement les solutions sont les couples de la forme :

$$(x, y) = (2a - 11n, -3a + 17n),\ n \in \mathbb{Z}.$$

5. $\begin{cases} x \wedge y &= 3 \\ x \vee y &= 135 \end{cases}$: pour (x, y) solution, on écrit $x = 3x'$ et $y = 3y'$ avec x', y' premiers entre eux. On veut alors $x'y' = 45$ donc (x', y') ou $(y', x') \in \{(\pm 1, \pm 45), (\pm 5, \pm 9)\}$ donc comme solutions :

$$(\pm 3, \pm 135),\ (\pm 135, \pm 3), (\pm 15, \pm 27), (\pm 27, \pm 15).$$

6. $\begin{cases} x + y &= 100 \\ x \wedge y &= 10 \end{cases}$: pour (x, y) solution, on écrit $x = 10x'$ et $y = 10y'$ avec x', y' premiers entre eux. On veut alors $x' + y' = 10$ ce qui donne $(x', y') \in \{(1, 9), (3, 7), (7, 3), (9, 1)\}$ et donc comme solutions :

$$(10, 90), (30, 70), (70, 30), (90, 10).$$

Exercice 13 [Nombre et de diviseurs]

Chaque diviseur de n est de la forme $\prod_{i=1}^{r} p_i^{b_i}$ avec $0 \leqslant b_i \leqslant a_i$ pour tout i. Ce qui laisse $a_i + 1$ choix pour la valeur de b_i. Et donc : $\prod_{i=1}^{r}(a_i + 1)$ diviseurs en tout.

Pour la somme, on a :

$$\sum_{b_1=0}^{a_1}\sum_{b_2=0}^{a_2}\cdots\sum_{b_r=0}^{a_r} p_1^{b_1}p_2^{b_2}\cdots p_r^{b_r} = \left(\sum_{b_1=0}^{a_1} p_1^{b_1}\right)\left(\sum_{b_2=0}^{a_2} p_2^{b_2}\right)\cdots\left(\sum_{b_r=0}^{a_r} p_r^{b_r}\right)$$

$$= \frac{p_1^{a_1+1}-1}{p_1-1}\frac{p_2^{a_2+1}-1}{p_2-1}\cdots\frac{p_r^{a_r+1}-1}{p_r-1} = \prod_{i=1}^{r}\frac{p_i^{a_i+1}-1}{p_i-1}$$

Exercice 14 [Produit des diviseurs]

Un tel entier n'est pas premier (sinon il n'a pas de diviseur non trivial).

Le plus petit nombre premier p qui divise n est un diviseur non trivial de n. Donc :

- si $q = n/p = p$: alors $n = p^2$, mais son seul diviseur non trivial est p, ce qui est impossible ;
- sinon : alors $q = n/p$ vérifie $qp = n$, donc n n'a pas d'autre diviseur non triviaux que p et q. Donc ou bien q est premier (et c'est bon) ; ou bien il ne l'est pas, mais il ne peut avoir d'autre diviseur premier que p (sinon ce serait aussi un diviseur non trivial de n), donc $q = p^2$.

Et finalement $n = pq$ (pour p, q premiers distincts) ou $n = p^3$ (pour p premier).

Exercice 15 [Sommes des diviseurs et nombres de Mersenne]

1. Par contraposée : si n n'est pas premier, on pose $n = pq$ $(p, q > 1)$ et alors $2^n - 1$ se factorise par $2^p - 1$ et $2^q - 2$ (factorisation de $a^n - b^n$) donc n'est pas premier.

   Réciproque fausse (sinon on pourrait facilement faire des nombres premiers aussi grands que l'on veut). Exemple : $M_{11} = 2047 = 23 \cdot 89$ n'est pas premier.

2. M_p est premier impair. Les diviseurs de N sont les 2^k ou $2^k M_p$ pour $0 \leqslant k \leqslant p - 1$. Leur somme (somme géométrique) vaut : $(2^p - 1) \cdot (M_p + 1) == M_p \cdot 2^p = 2N$ donc la somme de ses diviseurs stricte vaut N (on retire N des diviseurs).

Exercice 16 [Entiers algébriques]

1. On écrit $x = \dfrac{a}{b}$ avec a, b premiers entre eux. Si x n'est pas entier, b possède un diviseur premier qui apparaît au dénominateur de $x^n = \dfrac{a^n}{b^n}$, mais pas au numérateur donc $x^n \notin \mathbb{Z}$. Et si $x \in \mathbb{Z}$, alors directement $x^n \in \mathbb{Z}$.

2. Il suffit de montrer que tout élément de $\mathbb{Z} \setminus \mathbb{Q}$ n'est pas solution de (E). Soit $x \in \mathbb{Z} \setminus \mathbb{Q}$. On écrit $x = \dfrac{a}{b}$ avec a, b premiers entre eux et on pose p diviseur premier de b (existe comme $b \notin \mathbb{Z}$). Alors (en multipliant par b^n) :

$$x \text{ solution de } (E) \Rightarrow a^n + a_{n-1}a^{n-1}b + \cdots + a_1 a b^{n-1} + a_0 b^n = 0 \Rightarrow b|a^n \Rightarrow p|a^n \Rightarrow p|a$$

ce qui est absurde. Donc x n'est pas solution de (E).

On a le cas particulier où tous les a_i sont nuls, sauf éventuellement a_0.

Exercice 17 [Nombres de Fermat]

1. Par contraposée : si n n'est pas une puissance de 2, on écrit $n = p2^k$ pour $p > 1$ impair et par factorisation de $a^n + b^n$ pour n impair il vient :

$$2^n + 1 = (2^{2^k})^p - (-1)^p = (2^{2^k} + 1) \cdot \left(\sum_{l=0}^{p-1} 2^{l2^k} (-1)^{p-1-l} \right)$$

et on a ainsi $2^{2^k} + 1$ qui est un diviseur strict de $2^n + 1$, qui n'est pas premier.

2. On procède par algorithme d'Euclide. On considère $n, m \in \mathbb{N}$ distincts. Quitte à les échanger, on peut supposer $m > n$, et on pose donc $m = n + p$ avec $p \in \mathbb{N}^*$. On a alors :

$$F_m = F_{n+p} = 2^{2^{n+p}} + 1 = 2^{2^n 2^p} + 1 = \left(2^{2^n}\right)^{2^p} + 1 = \left(2^{2^n}\right)^{2^p} - 1^{2^p} + 2$$

$$= \left(2^{2^n} - 1\right) \cdot \left(\sum_{k=0}^{2^p-1} 2^{k2^n} \right) + 2 = F_n \cdot \left(\sum_{k=0}^{2^p-1} 2^{k2^n} \right) + 2$$

qui est la division euclidienne de F_m par F_n. Et ainsi le reste est 2. Le reste suivant dans l'algorithme d'Euclide est 1 (comme F_n est impair). Et c'est le dernier reste non nul.

Donc F_m et F_n sont premiers entre eux.

Exercice 18 [Nombre de zéros] Le nombre de 0 est le nombre de fois qu'un nombre est divisible par 10 : c'est donc $\min(v_2, v_5)$.

On peut calculer ces deux nombres directement : entre 1 et 100 (tous les facteurs de 100!), il y a :

- 50 multiples de 2, parmi lesquels 25 multiples de 4, parmi lesquels 12 multiples de 8, parmi lesquels 6 multiples de 16, parmi lesquels 3 multiples de 32, parmi lesquels 1 de 64. Ce sont les seuls avec une valuation 2-adique non nulle. Par valuation d'un produit, il vient :

$$v_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97$$

- 20 multiples de 5, parmi lesquels 4 multiples de 25, et de même :

$$v_5(100!) = 20 + 4 = 24$$

et finalement il y a 24 zéros dans l'écriture de 100! (en base 10). Il y aurait 97 zéros en base 2, et seulement 2 en base 37.