Feuille 9 : Arithmétique – PGCD, PPCM, Divisibilité, Nombres premiers
Éléments de correction – Parties A, B et C

A. Exercices standards

Exercice 1 – Vrai ou Faux

Soit $n \in \mathbb{Z}$: notons n, $n+1$, $n+2$, $n+3$ et $n+4$ les cinq entiers successifs.

1. Vrai :
   - ⋆ Si n est pair : n, $n+2$ et $n+4$ sont pairs et soit n et $n+4$ sont divisibles par 4, soit $n+2$ est divisible par 4.
   - ⋆ Si n est impair : $n+1$ et $n+3$ sont pairs et :
     - si 4 ne divise par $n+1$, alors il existe $k \in \mathbb{Z}$, $n+1 = 4k+2$ et $n+3 = 4(k+1)$ donc $n+3$ est divisible par 4.
     - si 4 ne divise par $n+3$, alors il existe $k \in \mathbb{Z}$, $n+3 = 4k+2$ et $n+1 = 4k$ donc $n+1$ est divisible par 4.
2. Vrai : cf 1.
3. Faux : contre-exemple : 4, 5, 6, 7 et 8 où 6 est le seul multiple de 3.
4. Vrai : tableau des restes de la division euclidienne de ... par 5

n	0	1	2	3	4
$n+1$	1	2	3	4	0
$n+2$	2	3	4	0	1
$n+3$	3	4	0	1	2
$n+4$	4	0	1	2	3

5. Faux : contre-exemple : 7, 8, 9, 10 et 11 : il n'y a aucune multiple de 6.
6. Faux : contre-exemple : 24, 25, 26, 27 et 28 : il n'y a aucun nombre premier.

Exercice 2 – Vrai ou Faux

1. Vrai. Si d divise a et b, d divise toute combinaison linéaire $au+bv$. On peut choisir u et v tels que $au+bv = PGCD(a,b)$ et on obtient que d divise $PGCD(a,b)$.
2. Faux. C'est le contraire, $PGCD(a,b)$ divise d. En effet, $PGCD(a,b)$ divise a et b donc il divise la combinaison linéaire $au+bv = d$. On peut trouver un contre-exemple : $a = 12$, $b = 6$, $d = 1\times 12+0\times 6 = 12$, et d ne divise pas $PGCD(a,b) = 6$.
3. Vrai. Comme $PGCD(a,b)$ divise d, il existe $k \in \mathbb{Z}$ tel que $k \times PGCD(a,b) = d$. On sait qu'on peut trouver u et v tels que $au+bv = PGCD(a,b)$. On a alors $a(ku)+b(kv) = k \times PGCD(a,b) = d$.

Exercice 3 – Calcul de PGCD entre deux entiers

1. Méthode 1 : (sans égalité de Bezout) ⋆ $48 = 2^4 \times 3$ et $210 = 2\times 3\times 5\times 7$ donc $pgcd(48,210) = 2\times 3 = 6$.
   ⋆ $81 = 3^4$ et $237 = 3\times 79$ donc $pgcd(81,237) = 3$.

   Méthode 2 : ⋆ Écrivons l'algorithme d'Euclide :
   $$\begin{aligned} 210 &= 48\times 4+18\\ 48 &= 18\times 2+12\\ 18 &= 12\times 1+6\\ 12 &= 6\times 2 \text{ donc } pgcd(210,48) = 6 \end{aligned}$$
   Remontons l'algorithme d'Euclide
   $$\begin{aligned} 6 &= 18-12\times 1\\ 6 &= 18-(48-18\times 2)\times 1\\ 6 &= 18\times 3-48\times 1\\ 6 &= (210-48\times 4)\times 3-48\times 1\\ 6 &= 210\times 3-48\times 13 \end{aligned}$$

⋆ Écrivons l'algorithme d'Euclide : $237 = 81 \times 2 + 75$
$81 = 75 \times 1 + 6$
$75 = 6 \times 12 + 3$
$6 = 3 \times 2$ donc $pgcd(237, 81) = 3$

Remontons l'algorithme d'Euclide $3 = 75 - 6 \times 12$
$3 = 75 - (87 - 75 \times 1) \times 12$
$3 = 75 \times 13 - 87 \times 12$
$3 = (237 - 81 \times 2) \times 13 - 87 \times 12$
$3 = 237 \times 13 - 81 \times 38$

2. ⋆ $18\,480 = 9\,828 \times 1 + 8\,652$
$9\,828 = 8\,652 \times 1 + 1\,176$
$8\,652 = 1\,176 \times 7 + 420$
$1\,176 = 420 \times 2 + 336$
$420 = 336 \times 1 + 84$
$336 = 84 \times 4$
Donc $pgcd(18\,480, 9\,828) = 84$

⋆ Remontons l'algorithme d'Euclide :
$84 = 420 - 336 \times 1$
$= 420 - (1\,176 - 420 \times 2)$
$= 420 \times 3 - 1\,176$
$= (8\,652 - 1\,176 \times 7) \times 3 - 1\,176$
$= 8\,652 \times 3 - 1\,176 \times 22$
$= 8\,652 \times 3 - (9\,828 - 8\,652) \times 22$
$= 8\,652 \times 25 - 9\,828 \times 22$
$= (18\,480 - 9\,825) \times 25 - 9\,828 \times 22$
$= 25 \times 18\,480 - 47 \times 9\,828$

Exercice 4 – Utilisation du PGCD et du PPCM

1. 6 a quatre diviseurs dans $\mathbb{N}$: 1, 2, 3 et 6. Il y a quatre couples dont le produit fait 6 : 1×6, 2×3, 3×2 et 6×1. Ils sont tous premiers entre eux, donc on a quatre couples : $(1, 6)$, $(2, 3)$, $(3, 2)$ et $(6, 1)$.
2. Comme leur PGCD est 35, les couples peuvent s'écrire $(35a, 35b)$ avec a et b premiers entre eux. Ensuite comme $210 = PPCM(35a, 35b) = 35 \times PPCM(a, b)$, on en déduit $PPCM(a, b) = 6$. Comme a et b sont premiers entre eux, leur PPCM est leur produit et donc ça revient à la question 1, il y a quatre couples (a, b). On en déduit les couples solution de la question : $(35, 210)$, $(70, 105)$, $(105, 70)$ et $(210, 35)$.
3. Cette fois-ci, les couples peuvent s'écrire $(18a, 18b)$ avec a et b premiers entre eux. Leur produit donne $6480 = 18a \times 18b = 324ab$. Donc $ab = 20$. On fait la liste des couples qui ont pour produit 20 : 1×20, 2×10, 4×5, 5×4, 10×2 et 20×1. On enlève 2×10 et 10×2 qui ne sont pas premiers entre eux. Il reste 4 couples, ce qui donne 4 solutions : $(18, 360)$, $(72, 90)$, $(90, 72)$ et $(360, 18)$.

Exercice 5 – Divisibilité et nombre premier

1. On remarque que $2^{ab} - 1 = (2^a)^b - 1^b$. On peut alors utiliser l'identité $x^n - y^n$ et on a $2^{ab} - 1 = (2^a - 1)(\sum_{k=0}^{b-1} 2^{ak})$. Donc $2^a - 1 \geq 1$ divise $2^{ab} - 1$.
2. On le montre par contraposée, supposons que p n'est pas premier, on a $p = ab$ pour deux entiers $a, b > 1$. D'après la question 1, $2^a - 1 > 1$ est un diviseur de $2^p - 1$. Donc $2^p - 1$ n'est pas premier. On a démontré la contraposée de l'affirmation, donc l'affirmation est vraie.

B. Exercices supplémentaires (plus difficiles)

Exercice 6 – Division euclidienne

⋆ Le reste de la division euclidienne de m par 4 peut être 0, 1, 2 ou 3.
⋆ Soit $(a, b) \in \mathbb{N}^2$ tels que $n = a^2 + b^2$. Alors :

a ou $b \equiv ...$ (4)	0	1	2	3
a^2 ou $b^2 \equiv ...$ (4)	0	1	0	1

$\Rightarrow$

$a^2 \equiv ...$ (4)	0	0	1	1
$b^2 \equiv ...$ (4)	0	1	0	1
$n \equiv ...$ (4)	0	1	0	2

Le reste de la division euclidienne de n par 4 n'est jamais égal à 3.

Exercice 7 – Divisibilité

Soit n l'entier naturel recherché. D'après l'énoncé, $(n+1)$ est un multiple de 8, 15, 18 et 24. On cherche donc le plus petit commun multiple de 8, 15, 18 et 24 :

⋆ $ppcm(8, 15) = \dfrac{8 \times 15}{pgcd(8, 15)} = 120$ car $pgcd(8, 15) = 1$.

$\star$ $ppcm(120,18) = \dfrac{18\times 120}{pgcd(18,120)} = \dfrac{2^3\times 3\times 5\times 2\times 3^2}{2\times 3} = 360$

$\star$ $ppcm(360,24) = \dfrac{360\times 24}{pgcd(360,24)} = \dfrac{2^3\times 3^2\times 5\times 2^3\times 3}{2^3\times 3} = 360$

Donc $n+1 = 360$ et $n = 359$.

Exercice 8 – PGCD

1. $\star$ $5a - 2b = 5(2n+3) - 2(5n-2) = 19$

$\star$ $pgcd(a,b) = pgcd(a, 5a-2b) = pgcd(2n+3, 19)$. Or, 19 étant premier :

soit $2n+3$ et 19 sont premiers entre-eux et $pgcd(a,b) = 1$

soit $19|(2n+3) \Leftrightarrow 2n+3 \equiv 0\ (19) \Leftrightarrow 2n \equiv -3\ (19) \Leftrightarrow 20n \equiv -30\ (19) \Leftrightarrow n \equiv 8\ (19)$.

Donc $pgcd(a,b) = \begin{cases} 1 & \text{si } n \equiv 8\ (19) \\ 19 & \text{sinon} \end{cases}$

2. $2(9n+4) - 9(2n-1) = 17$ donc $pgcd(2n-1, 9n+4) = pgcd(2n-1, 17)$. Or, 17 étant premier :

soit $2n+1$ et 17 sont premiers entre-eux et $pgcd(2n-1, 9n+4) = 1$

soit $17|(2n-1) \Leftrightarrow 2n-1 \equiv 0\ (17) \Leftrightarrow 2n \equiv 1\ (17) \Leftrightarrow 18n \equiv 9\ (17) \Leftrightarrow n \equiv 9\ (17)$.

Donc $pgcd(a,b) = \begin{cases} 17 & \text{si } n \equiv 9\ (17) \\ 1 & \text{sinon} \end{cases}$

C. Exercices d'entraînement (à faire en autonomie)

Exercice 9 – Entiers premiers entre eux

On suppose que a et b sont premier entre eux. Soit $d = \text{PGCD}(ab, a+b)$. On suppose que $d \neq 1$. Il existe donc un entier premier p qui divise d.
Comme $d|ab$ alors $p|ab$, et comme a et b sont premiers entre eux, on a soit $p|a$, soit $p|b$, mais p ne peut pas diviser a et b simultanément.
Si $p|a$, alors, comme $p|a+b$, p divise aussi $a+b-a = b$, contradiction.
Si $p|b$ alors de même p divise $a+b-b = a$, contradiction.
Ainsi, un tel entier premier p n'existe pas, donc $d = 1$.

Exercice 10 –PGCD

On cherche a et b entiers tels que $\text{PGCD}(a,b) = 18$ et $a+b = 360$. Soient a et b de tels entiers et a' et b' premiers entre eux tels que $a = 18a'$ et $b = 18b'$. On a alors

$$a+b = 18(a'+b') = 360,$$

donc $a'+b' = 20$. Cherchons de tels entiers premiers entre eux. On trouve

$$(a',b') \in \{(1,19),(19,1),(3,17),(17,3),(7,13),(13,7),(9,11),(11,9)\}.$$

Ainsi, en remultipliant par 18, les solutions sont donc

$$\{(18,342),(342,18),(54,306),(306,54),(126,234),(234,126),(162,198),(198,162)\}.$$

Exercice 11 – PGCD et division euclidienne

Soit $a \in \mathbb{N}$, $b \in \mathbb{N}$ deux entiers tels que $0 < a < b$.

1. On suppose que $a|b$. Alors il existe $k \in \mathbb{N}$ tel que $b = ka$ et donc, d'après la formule de factorisation de $n^\alpha - p^\alpha$, on obtient
$$n^b - 1 = (n^a)^k - 1^k = (n^a - 1)m, \quad m \in \mathbb{N},$$
donc $n^a - 1 | n^b - 1$.

2. Soit $n \in \mathbb{N}^*$ et $b = aq + r$ la division euclidienne de b par a, alors, par le même raisonnement,

$$n^b - 1 = n^{aq+r} - 1 = n^r(n^{aq} - 1) + n^r - 1 = n^r m(n^a - 1) + n^r - 1.$$

Comme $0 \leq n^r - 1 < n^a - 1$, on a bien obtenu la division euclidienne de $n^b - 1$ par $n^a - 1$ et donc $n^r - 1$ est bien le reste recherché.

3. Soit d le PGCD de a et b. On voit d'après la question précédente que les divisions euclidiennes de (a, b) et $(n^b - 1, n^a - 1)$ sont similaires. Ainsi, l'algorithme d'euclide appliqué à (b, a) donnera d comme dernier reste non-nul et ainsi le même algorithme appliqué à $(n^b - 1, n^a - 1)$ donnera $n^d - 1$ qui sera le PGCD de ces deux entiers.

Exercice 12 – Divisibilité et nombres premiers

Soit $n \geq 2$ un entier.

1. Si n n'est pas premier, alors il admet un plus petit diviseur premier $p \geq 2$. Si $p > \sqrt{n}$, alors on obtient $q = \dfrac{n}{p} < \sqrt{n}$.
Si q est premier, alors q divise n et comme $q < \sqrt{n} < p$, cela contredit la minimalité de p.
Si q n'est pas premier, il admet un plus petit diviseur premier $p' < p$, qui divise aussi n, ce qui contredit encore une fois la minimalité de p.
Finalement, $p \leq \sqrt{n}$ et le résultat est démontrée par contraposée.

2. Pour tout $k \in \{2, ..., n\}$, $k|n!$ et donc $n! + k$ est divisible par k. Ainsi, ces entiers ne sont pas premiers.

3. Les $n - 1$ entiers de la question précédente étant consécutif, on a bien montré que, pour tout $n \geq 2$, existe $n - 1$ entiers non premiers, d'où le résultat.
On remarquera que les n entiers $(n + 1)! + k$ avec $k \in \{2, ..., n + 1\}$ sont consécutifs et non premiers.