
CORRECTION TD1

† *Principe de récurrence*

Exercice 1.

1. Initialisation : On montre la propriété P_1 :

$$P_1 : \sum_{i=1}^1 i = 1 = \frac{1(1+1)}{2}$$

Hérédité : On montre l'implication $P_n \Rightarrow P_{n+1}$. Supposant P_n pour un certain entier n , on a

$$\begin{aligned} \sum_{i=1}^{n+1} i &= \sum_{i=1}^n i + n + 1 \\ &= \frac{n(n+1)}{2} + n + 1 \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+2)(n+1)}{2} \end{aligned}$$

Qui est bien la propriété P_{n+1} . Par le principe de récurrence, on a montré que P_n est vraie pour tout $n \geq 1$.

2. Initialisation : On montre la propriété P_1 :

$$P_1 : \sum_{i=1}^1 i^2 = 1 = \frac{1(1+1)(2+1)}{6}$$

Hérédité : On montre l'implication $P_n \Rightarrow P_{n+1}$. Supposant P_n pour un certain entier n , on a

$$\begin{aligned} \sum_{i=1}^{n+1} i^2 &= \sum_{i=1}^n i^2 + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\ &= \frac{(n+1)(n(2n+1) + 6(n+1))}{6} \\ &= \frac{(n+1)(2n^2 + n + 6n + 6)}{6} \\ &= \frac{(n+1)(2n^2 + 7n + 6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \\ &= \frac{(n+1)(n+2)(2(n+1)+1)}{6} \end{aligned}$$

Qui est bien la propriété P_{n+1} . Par le principe de récurrence, on a montré que P_n est vraie pour tout $n \geq 1$.

3. Initialisation : On montre la propriété P_1 :

$$P_1 : \left(\sum_{i=1}^1 i \right)^2 = 1 = \sum_{i=1}^1 i^3$$

Hérédité : On montre l'implication $P_n \Rightarrow P_{n+1}$. On note S_n la somme $\sum_{i=1}^n i = \frac{n(n+1)}{2}$. Supposant P_n pour un certain entier n , on a

$$\begin{aligned} \left(\sum_{i=1}^{n+1} i \right)^2 &= (S_n + (n+1))^2 \\ &= S_n^2 + 2S_n(n+1) + (n+1)^2 \\ &= \sum_{i=1}^n i^3 + 2 \frac{n(n+1)}{2} (n+1) + (n+1)^2 \\ &= \sum_{i=1}^n i^3 + (n+1)^2 n + (n+1)^2 \\ &= \sum_{i=1}^n i^3 + (n+1)^2 (n+1) \\ &= \sum_{i=1}^{n+1} i^3 \end{aligned}$$

Qui est bien la propriété P_{n+1} . Par le principe de récurrence, on a montré que P_n est vraie pour tout $n \geq 1$.

Exercice 2.

1. a) P_0 est donnée par $0 + 0 = 0$, qui est vrai.
- b) Non, il faudrait faire l'hérédité de la récurrence, qui est fausse.
- c) Si P_n est vraie, alors $n + n = n$, en soustrayant n de chaque côté, on obtient $n = 0$, donc P_n n'est vraie que pour $n = 0$.
2. a) Supposons que P_n est vraie pour un entier n , on a $9^{n+1} - 9^n$ est un multiple de 10. En multipliant par 9, on obtient que $9^{n+2} - 9^{n+1} = 9(9^{n+1} - 9^n)$ est également un multiple de 10. Donc P_{n+1} est vraie.
- b) Non ! Il faudrait faire l'initialisation de la récurrence, qui est fausse !
- c) La propriété P_0 est fausse car $9^1 - 9^0 = 9 - 1 = 8$ n'est pas un multiple de 10.

Exercice 3.

1. Parmi deux entiers consécutifs, exactement un est un multiple de 2. Le produit $n(n+1)$ contient donc un terme pair et est pair.
2. Parmi trois entiers consécutifs, exactement un est un multiple de 3. Le produit $n(n+1)(n+2)$ contient donc un terme divisible par 3 et est divisible par 3.
3. Soit d un diviseur commun à $3n+2$ et $2n+1$. L'ensemble des multiples de d est stable par somme, multiplication par un entier quelconque, soustraction (c'est un **idéal** de \mathbb{Z}). On a donc que $2(3n+2) = 6n+4$ et $3(2n+1) = 6n+3$ sont des multiples de d , de même que

$$6n+4 - (6n+3) = 1$$

donc 1 est un multiple de d : $d = 1$ et nos entiers sont premiers entre eux.

Exercice 4.

1. Pour $n \in \mathbb{N}$, on a

$$\begin{aligned} f(n+1) - f(n) &= 10^{n+1} + 3 \times 4^{n+3} + 5 - 10^n - 3 \times 4^{n+2} - 5 \\ &= 10^n(10 - 1) + 4^{n+2}(12 - 3) \\ &= 9(10^n + 4^{n+2}) \end{aligned}$$

Donc $f(n+1) - f(n)$ est un multiple de 9.

2. On procède par récurrence.

Initialisation : On montre que $f(0)$ est divisible par 9 :

$$f(0) = 10^0 + 3 \times 4^2 + 5 = 1 + 48 + 5 = 54 = 9 \times 6$$

Hérédité : Supposons que $f(n)$ est divisible par 9 pour un certain entier n . Sachant que les multiples de 9 sont stables par sommes, on a que

$$f(n+1) = f(n+1) - f(n) + f(n)$$

est un multiple de 9, ce qui termine notre raisonnement par récurrence.

† *Divisibilité.*

Exercice 5. (Crible d'Ératosthène)

Si n n'est pas premier, on a une décomposition $n = ab$ avec $a, b \geq 2$. Si $a \leq \sqrt{n}$, on a terminé. Si $a > \sqrt{n}$, alors $ab = n > b\sqrt{n}$ et on obtient $\sqrt{n} > b$, donc n admet un diviseur inférieur ou égal à \sqrt{n} .

2. A chaque étape, le plus petit entier de la liste est premier : si il n'a pas été retiré dans les étapes précédentes, il n'est multiple d'aucun entier qui lui est inférieur. Si un nombre est premier, il est forcément le plus petit nombre qui n'a pas été retiré de la liste à une certaine étape (puisqu'on a retiré que des nombres composites).

Notons que, quand on a trouvé les nombres premiers inférieurs à \sqrt{N} , tous les nombres restant de la liste sont premiers : les nombres composites inférieurs à N ont un diviseur premier inférieur à \sqrt{N} , ils ont donc déjà été retirés de la liste.

3.

Algorithm 1 Crible d'Ératosthène

```

 $L := [2, 3, \dots, N]$ 
 $P := []$ 
while  $L \neq \emptyset$  et  $L[1] < \sqrt{N}$  do
     $P := [P, L[1]]$ 
     $L := L \setminus ((L[1] * L) \cap L)$ 
end while
return  $P$ 

```

4. On applique l'algorithme précédent à notre liste.

(a) - 2 est premier, on retire ses multiples. Il reste

3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
33	35	37	39	41	43	45	47	49	51	53	55	57	59	61
63	65	67	69	71	73	75	77	79	81	83	85	87	89	91
93	95	97	99	101	103	105	107	109	111	113	115	117	119	

(b) - 3 est premier, on retire ses multiples. Il reste

5	7	11	13	17	19	23	25	29	31	35	37	41	43	47
49	53	55	59	61	65	67	71	73	77	79	83	85	89	91
95	97	101	103	107	109	113	115	119						

(c) - 5 est premier, on retire ses multiples. Il reste

7	11	13	17	19	23	29	31	37	41	43	47	49	53	59
61	67	71	73	77	79	83	89	91	97	101	103	107	109	113
119														

(d) - 7 est premier, on retire ses multiples. Il reste

11	13	17	19	23	29	31	37	41	43	47	53	59
61	67	71	73	79	83	89	97	101	103	107	109	113

(e) - Le prochain nombre sur la liste est $11 > \sqrt{120}$, par la question 2, tous les nombres de la liste sont premiers. D'où la liste des nombres premiers inférieurs à 120 :

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
53	59	61	67	71	73	79	83	89	97	101	103	107	109	113

5.

Algorithm 2 EstPremier

```

L :=Eratosthene( $\lfloor \sqrt{N} \rfloor$ )
for i in L do
  if i divide N then
    return false
  end if
end for
return true

```

Cet algorithme est bien gentil, mais il demande de calculer la liste des nombres premiers inférieurs à \sqrt{N} via le crible d'Ératosthène, ce qui est très coûteux !

Exercice 6.

1. Supposons par l'absurde que l'ensemble des nombres premiers est fini. Si c'est le cas, on peut considérer P le produit de tous ces nombres premiers. Par définition, P est divisible par tout nombre premier, donc $P + 1$ n'est divisible par aucun nombre premier : $P + 1$ est donc premier. Or $P + 1$ est plus grand que le produit de tous les nombres premiers, il est donc plus grand que tous les nombres premiers. C'est une contradiction.

2. a) Si p ne divise pas a , alors p et a sont premiers entre eux et $p \wedge a = 1$. En multipliant ceci par b , on trouve $b(p \wedge a) = bp \wedge ba = b$.

b) On sait que p divise ba et évidemment p divise pb , donc p divise $b = bd \wedge ba$ par définition du pgcd.

c) Si p divise a , on a gagné. Si p ne divise pas a , alors les questions b)c) donnent que p divise b .

3. On commence par prendre quelques notations : On note \mathbb{P} l'ensemble des nombres premiers. On veut montrer qu'en pour tout entier n , il existe une suite d'entiers $\{i_p\}_{p \in \mathbb{P}}$ telle que

$$n = \prod_{p \in \mathbb{P}} p^{i_p}$$

(Ce produit comporte à priori un nombre infini de termes, mais en pratique, tous les i_p sauf un nombre fini seront égaux à 0, donc ce produit comporte en fait un nombre fini de termes).

On utilise une récurrence forte :

Initialisation : L'entier 2 est un nombre premier : il est décomposable en produit de nombres premiers :

$$2 = 2^1 . 3^0 . 5^0 \dots$$

Hérédité : Soit $N \in \mathbb{N}$ et supposons que tout entier $n < N$ se décompose comme produit de nombres premiers. Si N est premier, il se décompose en produit de facteurs premiers et on a terminé. Sinon, N s'écrit comme un produit ab avec $a, b < N$. Les deux nombres a et b se décomposent en produit de facteurs premiers, de même que leur produit N .

Pour l'unicité, on procède encore par récurrence forte :

Initialisation : La décomposition des nombres premiers est évidemment unique, c'est en particulier le cas pour 2.

Hérédité : Soit $N \in \mathbb{N}$ et supposons que pour tout entier $n < N$ la décomposition comme produit de nombre premiers de n est unique. Soit deux décomposition en produit de facteurs premiers de N , et soit p un facteur du premier produit. Par hypothèse p divise le second produit, et par le Lemme d'Euclide il divise l'un des facteurs du second produit. Mais les facteurs du second produit sont premiers, donc p est égal à un de ses facteurs. On peut donc simplifier les deux produits par p et procéder par récurrence.

On a montré au final qu'il existe, pour tout entier n non nul, une unique suite $\{i_p\}_{p \in \mathbb{P}}$ d'entiers naturels tels que

$$n = \prod_{p \in \mathbb{P}} p^{i_p}$$

(Remarque : si on s'autorise $i_p \in \mathbb{Z}$, on obtiendra tous les rationnels positifs).

† PGCD, Algorithme d'Euclide

Exercice 7. Soit d un diviseur commun à $a + b$ et $a - b$. Par somme et par différence, on obtient que d divise

$$2a = a + b + a - b \text{ et } 2b = a + b - (a - b)$$

Donc d divise $2a \wedge 2b = 2(a \wedge b) = 2$.

Si a et b sont tous deux impairs, alors $a + b$ et $a - b$ sont pairs, et 2 est leur pgcd.

Si a et b sont de parité différentes, alors $a + b$ et $a - b$ sont impairs et premiers entre eux.

Exercice 8.

1. On utilise l'algorithme d'Euclide :

$$165 = 4 \cdot 35 + 25$$

$$35 = 1 \cdot 25 + 10$$

$$25 = 2 \cdot 10 + 5$$

$$10 = 2 \cdot 5 + 0$$

Le dernier reste non nul est 5, c'est le pgcd de 165 et de 35. Le ppcm de 165 et de 35 est donné par le produit, divisé par le pgcd, ici $\frac{165 \cdot 35}{5} = 33 \cdot 35 = 1155$.

2.

$$28 = 1 \cdot 16 + 12$$

$$16 = 1 \cdot 12 + 4$$

$$12 = 3 \cdot 4 + 0$$

Le dernier reste non nul est 4, c'est le pgcd de 28 et de 16.

3. La décomposition en produit de facteurs premiers de 27 est 3^3 , celle de 8 est 2^3 . Ces décompositions n'ayant aucun facteur commun, 27 et 8 sont premiers entre eux.

4. On a $24 = 8 \cdot 3$, donc 8 divise 24 et est le pgcd de 8 et 24.

Exercice 9.

1.

Algorithm 3 Division

```

 $m, n \in \mathbb{N}$ 
 $b := 1$ 
while  $m > nd$  do
   $b := b + 1$ 
end while
 $b := b - 1$ 
return  $(b, m - bn)$ 

```

2.

Algorithm 4 AlgEuclide

```

 $m, n \in \mathbb{N}$ 
 $(b, r) := \text{Division}(m, n)$ 
if  $r = 0$  then
  return  $n$ 
end if
return AlgEuclide( $n, r$ )

```

Exercice 10.

1. C'est la définition du pgcd.

2. Soit p un nombre premier, on considère p^i et p^j les deux plus grandes puissances de p divisant m et n (ce sont celles qui apparaissent dans la décomposition de m et n en produits de facteurs premiers). Par définition la plus grande puissance de p divisant $m \wedge n$ est $p^{\min(i,j)}$. Si les décompositions de m et n sont

$$\prod_{p \in \mathbb{P}} p^{j_p} \quad \text{et} \quad \prod_{p \in \mathbb{P}} p^{i_p}$$

On a

$$m \wedge n = \prod_{p \in \mathbb{P}} p^{\min(j_p, i_p)}$$

3.

Algorithm 5 Bourrin

```

 $d := 1$ 
 $N := \text{Minimum}(n, m)$ 
 $P := \text{Eratosthene}(N)$ 
for  $p$  dans  $P$  do
   $i := 0$ 
  while  $p^{i+1}$  divise  $m$  et  $n$  do
     $i := i + 1$ 
  end while
   $d := d \cdot p^i$ 
end for
return  $d$ 

```

4. Evidemment, AlgEuclide est nettement plus efficace : il ne fait appel qu'à des divisions euclidiennes, relativement faciles à obtenir, par opposition à la décomposition en produit de facteurs premiers.

Exercice 11.

1. Premièrement, notre recherche n'est pas vaine : 15 et 22 sont premiers entre eux, l'équation considérée admet donc des solutions. Commençons par trouver une telle solution via l'algorithme d'Euclide.

$$22 = 15 \cdot 1 + 7$$

$$15 = 7 \cdot 2 + 1$$

$$7 = 1 \cdot 7 + 0$$

On a donc

$$\begin{aligned} 1 &= 15 - 7 \cdot 2 \\ &= 15 - (22 - 15) \cdot 2 \\ &= 15 \cdot 3 - 22 \cdot 2 \end{aligned}$$

On a donc une solution particulière $x = 3, y = 2$.

Détaillons l'autre méthode donnée via la notation $15x - 22y = (x, y)$ (attention il y a un moins qui s'est invité !). Avec cette notation, on a

$$\begin{aligned} 7 &= 22 - 15 = (-1, -1) \\ 1 &= 15 - 2 \cdot 7 \\ &= (1, 0) - 2(-1, -1) \\ &= (1, 0) + (2, 2) = (3, 2) \end{aligned}$$

On retrouve (bien-sûr) la même solution $(x, y) = (3, 2)$.

On cherche maintenant la totalité des solutions. Soit une autre solution x et y , on a

$$15x - 22y = 15 \cdot 3 - 22 \cdot 2 \Leftrightarrow 15(x - 3) = 22(y - 2)$$

autrement dit, un multiple commun à 15 et à 22, comme ces deux nombres sont premiers entre eux, il existe un entier k tel que

$$\begin{aligned} \frac{15 \vee 22}{15} k = x - 3 \quad \text{et} \quad \frac{15 \vee 22}{22} k = y - 2 \\ 22k + 3 = x \quad \text{et} \quad 15k + 2 = y \end{aligned}$$

Les solutions sont donc les couples de la forme $x = 22k + 3, y = 15k + 2$ pour un entier k .

2. Là c'est directement plus simple : on a $15x = 22y$, donc il existe un entier k tel que $x = 22k$ et $y = 15k$, les solutions sont les couples de la forme $(22k, 15k)$.

3. Le pgcd de 15 et 24 est 3, qui ne divise pas 5, cette équation n'a donc pas de solutions entières.

4. Calculons le pgcd de 24 et 87 par l'algorithme d'Euclide.

$$87 = 24 \cdot 3 + 15$$

$$24 = 15 \cdot 1 + 9$$

$$15 = 9 \cdot 1 + 6$$

$$9 = 6 \cdot 1 + 3$$

$$6 = 3 \cdot 2 + 0$$

On a donc $87 \wedge 24 = 3$, $87 = 3 \cdot 29$ et $24 = 3 \cdot 8$. L'équation considérée admet des solutions si et seulement si $c = 3c'$ est un multiple de 3. Dans ce cas, l'équation devient

$$8x + 29y = c' \tag{1}$$

C'est cette équation là que l'on va résoudre. Commençons par trouver une solution à l'équation

$$8u + 29v = 1$$

On peut trouver en remontant l'algorithme d'Euclide précédent que

$$8 \cdot 11 + 29 \cdot (-3) = 1$$

Autrement dit, pour tout $c' \in \mathbb{Z}$ une solution de l'équation 1 est donnée par

$$8 \cdot (11c') + 29 \cdot (-3c') = c'$$

Soit maintenant une solution quelconque de l'équation 1, on a

$$8 \cdot (11c') + 29 \cdot (-3c') = 8x + 29y \Leftrightarrow 8(11c' - x) = 29(y + 3c')$$

Toujours comme $8 \cdot 29 = 29 \cdot 8$ est le ppcm de 29 et 8, on a qu'il existe un entier k tel que

$$29k = 11c' - x \quad \text{et} \quad 8k = y + 3c'$$

Les solutions recherchées sont donc les couples de la forme $(x, y) = (11c' - 29k, 8k - 3c')$ pour k dans \mathbb{Z} .

Exercice 12. Si $(x, y) \in \mathbb{Z}$, alors il existe $u, v \in \mathbb{Z}$ tels que

$$y - 3x = 3u + 7v - 3(u + v) = 3u + 7v - 3u - 3v = 4v$$

donc $y - 3x$ est bien un multiple de 4. D'ailleurs on peut retrouver ainsi la valeurs de v , on va s'en inspirer pour la réciproque.

Si $y - 3x$ est un multiple de 4, il existe un entier v tels que $y - 3x = 4v$. On pose $u = x - v$ de sorte que $u + v = x$. On a

$$3u + 7v = 3(x - v) + 7v = 3x + 4v = 3x + y - 3x = y$$

donc $(x, y) \in E$.