Chapitre XXI : Arithmétique et dénombrement

I Arithmétique

I.1 Division euclidienne

Définition I.1

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ deux entiers. On dit que a **divise** b ou que a est un **diviseur** de b ou que b est un **multiple** de a si et seulement si

$$\exists k \in \mathbb{Z}, \quad b = ak.$$

On note alors $a|b$.

Remarque 1 :

- L'entier 0 est divisible par tout entier mais ne divise que 0.
- Les entiers pairs sont les entiers divisibles par 2.

Théorème I.2 de la division euclidienne

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors il existe un unique couple d'entiers $(q, r) \in \mathbb{Z}^2$ tel que

$$\begin{cases} a = bq + r \\ 0 \leqslant r < b. \end{cases}$$

L'entier b est le diviseur, q est le quotient et r est le reste.

Démonstration. *Existence.*

- On commence par supposer que $a \geqslant 0$. On pose $\aleph = \{ k \in \mathbb{Z} \mid a - bk \geqslant 0 \}$. L'ensemble $\aleph$ est non vide car $0 \in \aleph$ et est majorée par $a+1$. En effet $b \geqslant 1$ donc pour tout $k \geqslant a+1 \geqslant 1$. Donc $bk \geqslant k \geqslant a+1 > a$ donc $a - bk < 0$. Donc $\aleph$ est une partie non vide et majorée de $\mathbb{Z}$ donc admet un maximum. Notons-le $q = \max(\aleph)$. Posons également $r = a - bq$. Puisque q est un maximum, c'est un élément de $\aleph$. Donc $r = a - bq \geqslant 0$. De plus $q+1 > q$ donc $q+1 \notin \aleph$. Ainsi $a - b(q+1) = r - b < 0$ i.e. $r < b$. Au bilan on a bien l'existence d'un entier $q \in \mathbb{Z}$ et d'un entier $r \in \mathbb{N}$ tels que $a = bq + r$ et $0 \leqslant r < b$.
- Si $a \leqslant 0$ alors $-a \geqslant 0$ donc il existe $(q_1, r_1) \in \mathbb{Z}^2$ tel que $-a = bq_1 + r_1$ et $0 \leqslant r_1 < b$.
  Si $r_1 = 0$, alors on pose $q = -q_1$ et $r = -r_1 = 0$ et on a $a = -bq_1 - r_1 = bq + r$ avec $0 \leqslant r = 0 < b$.
  Si $r_1 > 0$, alors $a = b(-q_1 - 1) + b - r_1$ et donc en posant $q = -q_1 - 1$ et $r = b - r_1$, on a bien $a = bq + r$ et comme $0 < r_1 < b$, $0 < r = r_1 - b < b$.

Ce qui démontre l'existence dans tous les cas.
Unicité. Soient $(q_1, r_1) \in \mathbb{Z}^2$ et $(q_2, r_2) \in \mathbb{Z}^2$ tels que

$$\begin{array}{lll} a = bq_1 + r_1 & \text{avec} & 0 \leqslant r_1 < b \\ a = bq_2 + r_2 & \text{avec} & 0 \leqslant r_2 < b. \end{array}$$

Par différence, $0 = b(q_1 - q_2) + r_1 - r_2 \quad \Leftrightarrow \quad b(q_1 - q_2) = r_2 - r_1$. Donc $-b < b(q_1 - q_2) < b$. Or $b > 0$ donc $-1 < q_1 - q_2 < 1$. Donc $q_1 - q_2$ est un entier strictement entre -1 et 1 donc $q_1 - q_2 = 0$ et ainsi $r_2 - r_1 = b \times 0 = 0$ i.e. $r_1 = r_2$. Ce qui démontre bien l'unicité.

□

Remarque 2 : Si $a \in \mathbb{N}^*$, $a|b$ si et seulement si le reste de la division euclidienne de b par a est nul.

I.2 Congruences

Définition I.3

Soit $n \in \mathbb{N}^*$. On dit que deux entiers a et b sont **congrus entre eux modulo** n si et seulement si n divise $a-b$. On note alors $a \equiv b\ [n]$.

Proposition I.4

Soit $n \in \mathbb{N}^*$. Soient $a, b, c, d \in \mathbb{Z}$. Soit $p \in \mathbb{N}^*$.

1. $a \equiv a\ [n]$.
2. $a \equiv b\ [n] \Leftrightarrow b \equiv a\ [n]$.
3. $a \equiv b\ [n] \Leftrightarrow \exists k \in \mathbb{Z},\ a = b + kn$.
4. si $a \equiv b\ [n]$ et $b \equiv c\ [n]$ alors $a \equiv c\ [n]$.
5. $a \equiv b\ [n]$ et $c \equiv d\ [n] \Rightarrow a + c \equiv b + d\ [n]$
6. $a \equiv b\ [n]$ et $c \equiv d\ [n] \Rightarrow ac \equiv bd\ [n]$
7. $a \equiv b\ [n] \Rightarrow a^p \equiv b^p\ [n]$.
8. $a \equiv 0\ [n] \Leftrightarrow n|a$
9. Si r est le reste de la division de a par n alors $a \equiv r\ [n]$ (réciproque fausse).
10. $a \equiv b\ [n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n.

Remarque 3 : La congruence est une relation d'équivalence.

Exemple 4 : Puisque $65 \equiv 2\ [7]$ et $13 \equiv 6\ [7]$, on a

$$78 = 65 + 13 \equiv 2 + 8 \equiv 1\ [7] \qquad \text{et} \qquad 845 = 65 \times 13 \equiv 2 \times 6 \equiv 12 \equiv 5\ [7].$$

I.3 *PGCD* et *PPCM*

Soient a et b deux entiers naturels non tous les deux nuls. L'ensemble des diviseurs commun à a et b est un sous-ensemble non vide (contient 1) et majoré (par le maximum entre a et b et même le minimum) de $\mathbb{N}$. Il admet donc un plus grand élément. De même l'ensemble des multiples strictement positifs communs à a et b est un sous-ensemble non vide (contient ab) de $\mathbb{N}$ et contient donc un plus petit élément.

Définition I.5

Soit $(a, b) \in \mathbb{N}^2$ avec $a \neq 0$ ou $b \neq 0$.

- On appelle **Plus Grand Commun Diviseur** de a et b, noté $PGCD(a, b)$ ou $a \wedge b$ le plus grand entier naturel qui divise à la fois a et à la fois b.
- On appelle **Plus Petit Commun Multiple** de a et b, noté $PPCM(a, b)$ ou $a \vee b$ le plus petit entier naturel divisible à la fois par a et à la fois par b.

Exemple 5 :

1. $PGCD(a, b) = PGCD(b, a)$.
2. $PGCD(a, 0) = a = PGCD(a, a)$.
3. $PGCD(a, 1) = 1$.
4. Si $a|b$, $PGCD(a, b) = a$.
5. $PGCD(ka, kb) = kPGCD(a, b)$.
6. $PGCD(2, 3) = 1$.
7. $PGCD(12, 16) = 4$.

1. $PPCM(a, b) = PPCM(b, a)$.
2. $PPCM(a, 0) = a = PPCM(a, a)$.
3. $PPCM(a, 1) = a$.
4. Si $a|b$, $PPCM(a, b) = b$.
5. $PPCM(ka, kb) = kPPCM(a, b)$.
6. $PPCM(2, 3) = 6$.
7. $PPCM(12, 16) = 48$.

Définition I.6

Soient a et b deux entiers naturels non tous les deux nuls. On dit que a et b sont **premiers entre eux** si et seulement si $PGCD(a, b) = 1$.

Remarque 6 : Puisque $PGCD(a, b)$ divise a et b, $a' = \frac{a}{PGCD(a,b)} \in \mathbb{N}$ et $b' = \frac{b}{PGCD(a,b)} \in \mathbb{N}$. De plus,

$$PGCD(a, b)PGCD(a', b') = PGCD\left(PGCD(a, b)a', PGCD(a, b)b'\right) = PGCD(a, b).$$

Donc $PGCD(a', b') = 1$ et a' et b' sont premiers entre eux.

Les deux propositions qui suivent sont hors programme mais fondamentales en arithmétique.

Théorème I.7 (Théorème de Bezout)

Soit $(a,b) \in \mathbb{N}^2$ avec $a \neq 0$ ou $b \neq 0$. Alors

$$\exists\,(u,v) \in \mathbb{Z}^2, \quad au + bv = d \qquad \Leftrightarrow \qquad PGCD(a,b)|d.$$

En particulier, a et b sont premiers entre eux si et seulement si

$$\exists\,(u,v) \in \mathbb{Z}^2, \quad au + bv = 1.$$

Exemple 7 : Algorithme d'Euclide étendu
Calculons le $PGCD$ de 255 et 142 ainsi que les coefficients de Bezout associés. Dans la division euclidienne de a par b, $a = bq + r$ avec $0 \leqslant r < b$, on observe que $PGCD(a,b) = PGCD(b,r)$. Donc en itérant,

$$\begin{aligned} 255 &= 142 + 13 \\ 142 &= 13 \times 10 + 12 \\ 13 &= 12 + 1. \end{aligned}$$

On en déduit que $PGCD(255,142) = PGCD(12,1) = 1$. Puis on « remonte » l'algorithme de la façon suivante :

$$\begin{aligned} 1 &= 13 - 12 \\ &= 13 - (142 - 13 \times 10) \\ &= 13 \times 11 - 142 \\ &= (255 - 142) \times 11 - 142 \\ &= 255 - 142 \times 12. \end{aligned}$$

Ainsi on a bien trouvé les coefficients de Bezout $u = 1$ et $v = -12$ tel que $255u + 142v = 1$.

Proposition I.8 (Lemme de Gauss)

Soient a, b et c trois entiers naturels. Si $a|bc$ et si a et b sont premiers entre eux alors $a|c$.

Démonstration. Par le théorème de Bezout, il existe $(u,v) \in \mathbb{Z}^2$ tel que $1 = au + bv$. En multipliant par c, on obtient $c = acu + bcv$. Or si $a|bc$, alors $bc \equiv 0\ [a]$. De plus $a \equiv 0\ [a]$ et donc $c = acu + bcv \equiv 0\ [a]$ i.e. $a|c$. □

I.4 Nombres premiers

Définition I.9

Soit $p \in \mathbb{N}$, $p \geqslant 2$. On dit que p est **un nombre premier** si et seulement si 1 et p sont les seuls diviseurs de p.

Remarque 8 : $p = 2$ est le seul nombre premier pair.

Proposition I.10 (Lemme d'Euclide)

Soit a et b deux entiers naturels et p un nombre premier. Si $p|ab$ alors $p|a$ ou $p|b$.

Démonstration. Premier cas, $p|a$ alors OK.
Second cas p ne divise par a alors nécessairement p et a sont premiers entre eux. Donc d'après le Lemme de Gauss, $p|b$.

□

Théorème I.11 (Théorème fondamental de l'arithmétique)

Pour tout $n \in \mathbb{N}$, $n \geqslant 2$, il existe un entier $d \in \mathbb{N}^*$, $p_1, \dots, p_d$, d nombres premiers distincts et $\alpha_1, \dots, \alpha_d$, d entiers naturels non nuls tels que

$$n = \prod_{i=1}^{d} p_i^{\alpha_i}.$$

Autrement dit tout entier se décompose en un produit de nombres premiers. De plus cette décomposition est unique.

Démonstration. Hors programme. En voici juste une esquisse.
Existence. On procède par récurrence sur n. On pose pour tout $n \in \mathbb{N}$, $n \geqslant 2$, $\mathscr{P}(n)$ « l'entier n admet une décomposition en produit de facteurs premiers ».
Si $n = 2$, alors la décomposition est directe puisque n est premier.
Soit $n \in \mathbb{N}$, $n \geqslant 2$. Procédons par une récurrence forte et supposons que pour tout $2 \leqslant k \leqslant n$, k admet une décomposition en produit de facteurs premiers. Premier cas, $n+1$ est un nombre premier et admet donc une décomposition élémentaire. Second cas, n n'est pas premier, il existe alors deux entiers naturels $a > 1$ et $b > 1$ tels que $n+1 = ab$. Or $2 \leqslant a \leqslant n$ et $2 \leqslant b \leqslant n$. Donc par l'hypothèse de récurrence a admet une décomposition et b admet également une décomposition. Par produit de ces deux décompositions, on en déduit que $n+1$ admet aussi une décomposition en produit de facteurs premiers.
Unicité. Supposons $n = \prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{i=1}^{s} q_i^{\beta_i}$ avec $p_1 < \cdots < p_r$ des nombres premiers et $q_1 < \cdots < q_s$ des nombres premiers. Supposons $q_1 < p_1$. Alors q_1 est premier avec tous les p_i donc avec tous les $p_i^{\alpha_i}$. Or $q_1 | n = \prod_{i=1}^{r} p_i^{\alpha_i}$ ce qui est contradictoire. Donc $q_1 \geqslant p_1$. De même on montre que $p_1 \geqslant q_1$ et donc $p_1 = q_1$. Si $\alpha_1 < \beta_1$, en simplifiant $\prod_{i=2}^{r} p_i^{\alpha_i} = q_1^{\beta_1 - \alpha_1} \prod_{i=2}^{s} q_i^{\beta_i}$. Or $q_1 = p_1 < p_2 < \cdots < p_r$ et $q_1 | \prod_{i=2}^{r} p_i^{\alpha_i}$ ce qui comme précédemment est absurde. Donc $\alpha_1 \geqslant \beta_1$ et de même on montre que $\beta_1 \geqslant \alpha_1$ et donc $\alpha_1 = \beta_1$. Alors $\prod_{i=2}^{r} p_i^{\alpha_i} = \prod_{i=2}^{s} q_i^{\beta_i}$. En itérant le raisonnement, on montre alors que $p_2 = q_2$, $\alpha_2 = \beta_2$ etc et notamment que $s = r$. Ce qui assure l'unicité. □

Proposition I.12

L'ensemble des nombres premiers est infini.

Démonstration. Soit $\mathscr{P}$ l'ensemble des nombres premiers. Supposons que $\mathscr{P}$ soit fini. On pose alors n son nombre d'éléments et on note $p_1, p_2, \dots, p_n$ ses éléments : $\mathscr{P} = \{p_1, \dots, p_n\}$. Posons enfin

$$p = \prod_{i=1}^{n} p_i + 1.$$

Soit k un diviseur premier de p (existence à l'aide du théorème précédent). Il existe $i \in [\![1; n]\!]$ tel que $k = p_i$. Donc k divise $\prod_{i=1}^{n} p_i$ et comme k divise p, on en déduit que k divise $p - \prod_{i=1}^{n} p_i = 1$. Donc $k = 1$. Or k est supposé premier, ce qui est absurde. Donc l'ensemble $\mathscr{P}$ est infini. □

Exemple 9 : On lit directement le $PGCD$ et le $PPCM$ dans la décomposition en produit de facteurs premiers. Si $a = 51450$ et $b = 30800$, alors

$$a = 5145 \times 10 = 5 \times 1029 \times 5 \times 2 = 2 \times 5^2 \times 3 \times 343 = 2 \times 3 \times 5^2 \times 7 \times 49 = 2 \times 3 \times 5^2 \times 7^3.$$

De plus

$$b = 308 \times 100 = 154 \times 2 \times 5^2 \times 2^2 = 2^3 \times 5^2 \times 2 \times 77 = 2^4 \times 5^2 \times 7 \times 11.$$

Alors le $PGCD$ est calculé à partir des facteurs communs avec la plus petite multiplicité

$$PGCD\,(51450, 30800) = 2 \times 5^2 \times 7 = 350.$$

Le $PPCM$ est calculé à partir de tous les facteurs présents avec la plus grande multiplicité :

$$PPCM\,(51450, 30800) = 2^4 \times 3 \times 5^2 \times 7^3 \times 11 = 4 \times 3 \times 100 \times 343 \times 11 = 100 \times 4 \times 3 \times 3773 = 100 \times 4 \times 11319 = 4527600.$$

On remarque en particulier que

$$PGCD\,(51450, 30800)\, PPCM\,(51450, 30800) = 2^5 \times 3 \times 5^4 \times 7^4 \times 11 = ab,$$

qui est un résultat général.
Crible d'Eratosthène.

1. On écrit tous les nombres entre 2 et n.
2. On barre tous les multiples de 2 sauf 2.
3. On prend le premier entier non barré après 2, ici 3 et on barre tous les multiples de 3 sauf 3.
4. On recommence le procédé jusqu'à dépasser $\sqrt{n}$. On s'arrête alors et tous les nombres non barrés sont les entiers premiers entre 2 et n.

Exemple 10 : Appliquer le crible pour $n = 100$.

II Dénombrement

II.1 Cardinal

Définition II.1

Soit E un ensemble non vide.

- On dit que E est **un ensemble fini** s'il existe $n \in \mathbb{N}^*$ ainsi qu'une bijection entre E et $[\![1;n]\!]$.
- L'entier n est alors appelé **le cardinal** de E et est noté $\text{Card}(E)$ ou $|E|$ ou encore $\#E$.

Remarque 11 :

- La définition sous-entend l'unicité de l'entier n ou encore de l'ensemble $[\![1;n]\!]$ avec lequel E est en bijection. Nous admettons ce résultat.
- Par convention $\text{Card}(\emptyset) = 0$.
- Si E est de cardinal n, on peut numéroter ses éléments et écrire $E = \{e_1, e_2, \dots, e_n\}$. Dénombrer E i.e. déterminer son cardinal revient à expliciter que l'on peut obtenir cette numérotation (sans forcément exhiber la bijection).

Exemple 12 : Pour tout $(p,q) \in \mathbb{Z}^2$, on a $\text{Card}([\![q;p]\!]) = p - q + 1$. En effet,

$$\begin{aligned} \varphi : \quad [\![q;p]\!] &\to [\![1;p-q+1]\!] \\ k &\mapsto k - q + 1, \end{aligned}$$

est bijective.

Proposition II.2

Deux ensembles finis E et F ont le même cardinal si et seulement s'il existe une bijection entre E et F.

Démonstration. Si $\text{Card}(E) = \text{Card}(F) = n$ alors par définition il existe $f : E \to [\![1;n]\!]$ et $g : F \to [\![1;n]\!]$ deux applications bijectives. Puisque g est bijective, g^{-1} existe et $g^{-1} : [\![1;n]\!] \to F$. On pose alors $h = g^{-1} \circ f : E \to F$ et h est bien une bijection entre E et F.
Réciproquement, s'il existe $f : E \to F$ une bijection. Notons $p = \text{Card}(F)$ alors par définition, il existe une bijection $g : F \to [\![1;p]\!]$. Par composition, $g \circ f : E \to [\![1;p]\!]$ est une bijection et donc $\text{Card}(E) = p = \text{Card}(F)$. □

Proposition II.3

Soit E un ensemble fini et A une partie de E. Alors

- A est un ensemble fini et $\text{Card}(A) \leqslant \text{Card}(E)$.
- De plus $\text{Card}(A) = \text{Card}(E)$ si et seulement si $A = E$.

Corollaire II.4 (Principe des tiroirs)

Si $f : [\![1;p]\!] \to [\![1;n]\!]$ est injective alors $p \leqslant n$.

Remarque 13 :

- En prenant la contraposée, on obtient que si $p > n$ alors toute application de $[\![1;p]\!] \to [\![1;n]\!]$ n'est pas injective. Notamment si l'on range p paires de chaussettes dans n tiroirs avec $p > n$ alors le rangement n'est pas injectif. Donc deux antécédents, ici deux paires de chaussettes, vont avoir la même image, être rangées dans le même tiroir.

- En anglais on parle de pigeonhole principle.

Proposition II.5

Soient E et F deux ensembles finis et $\varphi : E \to F$. On suppose que $\text{Card}(E) = \text{Card}(F)$. Alors les trois assertions suivantes sont équivalentes :

1. φ est injective.
2. φ est surjective.
3. φ est bijective.

Démonstration.

- 3) $\Rightarrow$ 1) et 3) $\Rightarrow$ 2) de façon immédiate.
- 1) $\Rightarrow$ 3). On suppose φ injective. En restreignant l'ensemble d'arrivée on construit une application

$$\begin{aligned} \psi : \quad & E \to \varphi(E) \\ & x \mapsto \varphi(x). \end{aligned}$$

L'application ψ est bien définie, est injective comme φ et puisque l'on a restreint son arrivée à l'ensemble des images de φ, ψ est bien surjective. Donc ψ définie une bijection entre E et $\varphi(E)$. Donc par la proposition II.2, on en déduit que $\text{Card}(\varphi(E)) = \text{Card}(E)$ et par hypothèse, $\text{Card}(E) = \text{Card}(F)$. Donc $\text{Card}(\varphi(E)) = \text{Card}(F)$. Or $\varphi(E)$ est une partie de F, donc d'après la proposition II.3, $\varphi(E) = F$ i.e. φ est surjective et donc φ est bijective.

- 2) $\Rightarrow$ 3). On suppose maintenant que φ est surjective. Par définition, pour tout $a \in F$, il existe $x_a \in E$ tel que $\varphi(x_a) = a$. Ainsi pour chaque élément $a \in F$, on choisit et on fixe UN de ces antécédents x_a et l'on définit ainsi une application

$$\begin{aligned} \psi : \quad & F \to E \\ & a \mapsto x_a. \end{aligned}$$

L'application ψ est en quelque sorte une réciproque partielle de φ. Comme φ est surjective, l'application ψ est bien définie . Elle est de plus injective : soient $(a, b) \in F^2$ tels que $\psi(a) = x_a = x_b = \psi(b)$. Notons $x = x_a = x_b$. Par définition, x est un antécédent de a donc $\varphi(x) = a$ mais c'est aussi un antécédent de b donc $\varphi(x) = b$. Donc $a = b$ et ψ est bien injective. On a construit une application injective entre F et E deux ensembles de même cardinal donc d'après le point précédent de notre démonstration, on en déduit que ψ est bijective. Or pour tout $a \in F$, $\varphi \circ \psi(a) = \varphi(x_a) = a$. Donc $\varphi \circ \psi = \text{Id}_E$. Donc en composant à droite par ψ^{-1} (existe car ψ surjective) on en déduit que $\varphi = \psi^{-1}$ et donc φ est bijective.

□

II.2 Opérations sur les cardinaux

Définition II.6

Soient A et B deux parties d'un ensemble E. On dit que A et B sont **disjoints** si et seulement $A \cap B = \emptyset$.

Remarque 14 : Lorsque deux parties sont disjointes, leur union $A \cup B$ est parfois notée $A \sqcup B$.

Proposition II.7

Soient A et B deux parties d'un ensemble fini E. On suppose que A et B sont disjoints. Alors

$$\text{Card}(A \sqcup B) = \text{Card}(A) + \text{Card}(B).$$

Démonstration. On note $p = \text{Card}(A)$ et $q = \text{Card}(B)$. Par définition, il existe $f : A \to [\![1; p]\!]$ et $g : B \to [\![1; q]\!]$ deux bijections. On pose

$$\begin{aligned} \varphi : \quad & A \sqcup B \to [\![1; p+q]\!] \\ & x \mapsto \begin{cases} f(x) & \text{si } x \in A \\ g(x) + p & \text{si } x \in B. \end{cases} \end{aligned}$$

L'application φ est bien définie car tout élément admet bien une image et une seule image : les ensembles étant disjoints aucun élément de $A \sqcup B$ n'est à la fois dans A et à la fois dans B. De plus pour tout $x \in B$, $1 \leqslant g(x) \leqslant q$ et donc $1 + p \leqslant g(x) + p \leqslant p + q$ et pour tout $x \in A$, $1 \leqslant f(x) \leqslant p$. Donc l'ensemble d'arrivée est bien posé.
L'application φ est injective : soient $(x, y) \in A \sqcup B$ tel que $\varphi(x) = \varphi(y)$.

- Premier cas, les deux éléments sont dans A. Alors $f(x) = \varphi(x) = \varphi(y) = f(y)$. Comme f est bijective, f est injective et donc $x = y$.
- Deuxième cas, les deux éléments sont dans B. Alors de même $g(x) = \varphi(x) - p = \varphi(y) - p = g(y)$ et donc par l'injectivité de g, $x = y$.
- Troisième cas, l'un des éléments est dans A et l'autre est dans B. Mettons $x \in A$ et $y \in B$ (le cas $y \in A$ et $x \in B$ se traite de la même façon). Alors $\varphi(x) = f(x) \leqslant p < p+1 \leqslant p + g(y) = \varphi(y)$ ce qui contredit que $\varphi(x) = \varphi(y)$ et donc ce cas est impossible.

Conclusion, on en déduit que $x = y$ et donc que φ est injective.
L'application φ est surjective. Soit $k \in [\![1; p+q]\!]$.

- Premier cas, $k \in [\![1; p]\!]$ alors par surjectivité de f, il existe $x \in A$ tel que $f(x) = k$ et donc $k = \varphi(x)$ car $x \in A$.
- Second cas, $k \in [\![p+1; p+q]\!]$ alors en posant $k' = k - p$, on a $k' \in [\![1; q]\!]$ et $k = p + k'$. Par la surjectivité de g, il existe $x \in B$ tel que $g(x) = k'$ et donc $k = g(x) + p = \varphi(x)$ car $x \in B$.

Dans tous les cas, on a trouvé un antécédent de k dans $A \sqcup B$. Donc φ est surjective.
Conclusion, φ est bijective.

□

Proposition II.8

Soit A une partie d'un ensemble fini E. Alors

$$\operatorname{Card}(C_E(A)) = \operatorname{Card}(E) - \operatorname{Card}(A).$$

Démonstration. Les ensembles A et $\overline{A} = C_E(A)$ sont disjoints dans E et $E = A \sqcup C_E(A)$. Donc par la proposition précédente,

$$\operatorname{Card}(E) = \operatorname{Card}(A) + \operatorname{Card}(C_E(A)) \quad \Leftrightarrow \quad \operatorname{Card}(C_E(A)) = \operatorname{Card}(E) - \operatorname{Card}(A).$$

□

Proposition II.9 (Formule de Poincaré)

Soient A et B deux parties d'un ensemble fini E. Alors

$$\operatorname{Card}(A \cup B) = \operatorname{Card}(A) + \operatorname{Card}(B) - \operatorname{Card}(A \cap B).$$

Remarque 15 : Tiens, revoilà Grassmann.

Démonstration. On pose $B' = B \setminus A = B \setminus (A \cap B)$ éventuellement $B' = \emptyset$ si $B \subseteq A$. Les ensembles A et B' sont disjoints donc d'après la proposition II.7,

$$\operatorname{Card}(A \sqcup B') = \operatorname{Card}(A) + \operatorname{Card}(B').$$

Or $A \sqcup B' = A \cup B$ donc

$$\operatorname{Card}(A \cup B) = \operatorname{Card}(A) + \operatorname{Card}(B').$$

De plus $B = B' \sqcup (A \cap B)$, donc toujours d'après la proposition II.7,

$$\operatorname{Card}(B) = \operatorname{Card}(B') + \operatorname{Card}(A \cap B) \quad \Leftrightarrow \quad \operatorname{Card}(B') = \operatorname{Card}(B) - \operatorname{Card}(A \cap B).$$

En conclusion,

$$\operatorname{Card}(A \cup B) = \operatorname{Card}(A) + \operatorname{Card}(B) - \operatorname{Card}(A \cap B).$$

□

Proposition II.10

Soient E et F deux ensembles finis. Alors l'ensemble

$$E \times F = \{(x, y) \mid x \in E,\ y \in F\},$$

est un ensemble fini. De plus

$$\operatorname{Card}(E \times F) = \operatorname{Card}(E) \operatorname{Card}(F).$$

Démonstration. L'ensemble E est fini. On pose $n = \text{Card}(E)$ et on numérote alors ses éléments en écrivant $E = \{x_1, \dots, x_n\}$, où les x_i sont tous distincts. Pour tout $i \in [\![1; n]\!]$, on pose

$$F_i = \{(x_i, y) \in E \times F \mid y \in F\}.$$

Montrons que $E \times F = \bigsqcup_{i \in [\![1;n]\!]} F_i$.

- Pour tout $i \in [\![1; n]\!]$, F_i est par définition un sous-ensemble de $E \times F$ et donc la réunion est aussi un sous-ensemble de $E \times F$: $\bigcup_{i \in [\![1;n]\!]} F_i \subseteq E \times F$.
- Soit $(x, y) \in E \times F$. Alors $x \in E$. Donc il existe $i \in [\![1; n]\!]$ tel que $x = x_i$. Donc $(x, y) = (x_i, y) \in F_i$. Et donc $(x, y) \in \bigcup_{i \in [\![1;n]\!]} F_i$. Ainsi, avec le point précédent, on a montré que $E \times F = \bigcup_{i \in [\![1;n]\!]} F_i$.
- Montrons maintenant que l'union est disjointe. Soit $(i, j) \in [\![1; n]\!]^2$, $i \neq j$. Montrons que $F_i \cap F_j = \emptyset$. Supposons que $F_i \cap F_j \neq \emptyset$, alors il existe $(x, y) \in F_i \cap F_j$. Puisque $(x, y) \in F_i$ alors $x = x_i$ et de même $(x, y) \in F_j$ implique $x = x_j$. Or $x_i \neq x_j$ ce qui implique une contradiction. Donc $F_i \cap F_j = \emptyset$ et l'union est disjointes.

Soit $i \in [\![1; n]\!]$. L'application

$$\begin{aligned} \phi_i : \quad & F \to F_i \\ & y \mapsto (x_i, y), \end{aligned}$$

définit une bijection entre F et F_i (vérification aisée). Donc F_i est en bijection avec F et par la proposition II.2, on en déduit que F_i est un ensemble fini et $\text{Card}(F_i) = \text{Card}(F)$. En itérant la proposition II.7, on en déduit que $\sqcup F_i$ est aussi de cardinal fini et

$$\text{Card}\left(\bigsqcup_{i \in [\![1;n]\!]} F_i\right) = \text{Card}\left(\bigsqcup_{i \in [\![1;n-1]\!]} F_i\right) + \text{Card}(F_n) = \cdots = \text{Card}(F_1) + \text{Card}(F_2) + \cdots + \text{Card}(F_n).$$

Par ce qui précède, pour tout $i \in [\![1; n]\!]$, $\text{Card}(F_i) = \text{Card}(F)$. Donc

$$\text{Card}\left(\bigsqcup_{i \in [\![1;n]\!]} F_i\right) = n\text{Card}(F).$$

Or $\bigsqcup_{i \in [\![1;n]\!]} F_i = E \times F$ et $n = \text{Card}(E)$. Finalement, on en déduit que $E \times F$ est un ensemble fini et

$$\text{Card}(E \times F) = \text{Card}(E)\,\text{Card}(F).$$

□

Remarque 16 : Par récurrence sur n, pour $E_1, \dots, E_n$ des ensembles finis,

$$\text{Card}(E_1 \times E_2 \times \cdots \times E_n) = \text{Card}(E_1)\,\text{Card}(E_2) \cdots \text{Card}(E_n).$$

En particulier, si E est un ensemble fini,

$$\text{Card}(E^n) = \text{Card}(E)^n.$$

Exemple 17 : Un restaurant propose deux entrées, quatre plats de résistance et trois desserts. Quel est le nombre de menus différents possibles ?

II.3 Les p-listes ou p-uplets

Définition II.11

Soit E un ensemble et $p \in \mathbb{N}^*$ un entier naturel non nul. Tout élément $(x_1, \dots, x_p) \in E^p$ de E^p est appelé **une p-liste** ou encore **un p-uplets** d'éléments de E.

Remarque 18 :

- Si $p = 2$, un 2-uplet est appelé un couple. Si $p = 3$, un 3-uplet est appelé un triplet.
- Dans une p-liste, l'ordre est important : par exemple si $n = 2$, $(I_2, 0_2)$ et $(0_2, I_2)$ sont deux couples distincts de $\mathscr{M}_2(\mathbb{R})^2$.

- Dans une p-liste, les éléments peuvent se répéter par exemple $(\cos, \sin, \cos)$ est un triplet de $\mathscr{F}(\mathbb{R}, \mathbb{R})^3$ et $(1, 0, 1, 1)$ un quadruplet de $\mathbb{N}^4$.

Remarque 19 : La construction de p-uplet s'établit par un tirage **successif** (l'ordre est important), **avec remise** (répétition possible d'un élément) de p éléments de E.

Proposition II.12

- Soit E un ensemble fini de cardinal $n \in \mathbb{N}^*$ et soit $p \in \mathbb{N}^*$. Alors le nombre de p-uplets de E est
$$\text{Card}\left(E^p\right) = n^p.$$
- Le nombre de tirages successifs avec remise de p éléments de E est n^p.

Exemple 20 : Déterminer le nombre de mots de cinq lettres que l'on peut former.

Définition II.13

Soient E et F deux ensembles. On note $\mathscr{F}(E, F)$ ou encore F^E l'ensemble des applications de E dans F.

Remarque 21 : Ici application est au sens stricte et désigne une fonction sur E bien définie sur E tout entier.

Proposition II.14

Soient E et F deux ensembles finis. Alors $\mathscr{F}(E, F)$ est un ensemble fini et
$$\text{Card}\left(F^E\right) = \text{Card}\,(F)^{\text{Card}(E)}.$$

Démonstration. On pose $n = \text{Card}\,(E)$ et $p = \text{Card}\,(F)$. On numérote E de la façon suivante : $E = \{e_1, \ldots, e_n\}$. Construire une application f de E dans F c'est choisir pour chaque élément de E une image dans F. Pour e_1, on choisit un élément de F qui sera $f(e_1)$, l'image de e_1 par f, puis pour e_2, on choisit un élément de F qui sera $f(e_2)$, l'image de $f(e_2)$ etc. Construire f revient donc à choisir un n-uplet de F. Plus précisément, l'application
$$\begin{aligned}\varphi : \mathscr{F}(E, F) &\to F^n \\ f &\mapsto (f(e_1), \ldots, f(e_n)),\end{aligned}$$
définit une bijection entre $\mathscr{F}(E, F)$ et F^n. Donc $\mathscr{F}(E, F)$ est un ensemble fini et
$$\text{Card}\left(F^E\right) = \text{Card}\left(\mathscr{F}(E, F)\right) = \text{Card}\left(F^n\right) = \text{Card}\,(F)^n = p^n = \text{Card}\,(F)^{\text{Card}(E)}.$$
□

II.4 Arrangements

Définition II.15

Soient E un ensemble fini de cardinal $n \in \mathbb{N}^*$ et $p \in [\![1; n]\!]$. On appelle **arrangement** de p éléments de E tout p-uplet d'éléments deux à deux distincts de E. Autrement dit $(x_1, \ldots, x_p)$ est un arrangement de p éléments de E si
$$\forall (i, j) \in [\![1; p]\!]^2,\ i \neq j, \qquad x_i \neq x_j.$$

Remarque 22 :

- Dans un arrangement l'ordre compte toujours et les éléments sont tous différents.
- On ne peut pas prendre plus de n objets distincts parmi un ensemble à n éléments... d'où le fait que $p \leqslant n$.

Remarque 23 : Un arrangement de p éléments de E est un tirage **successif** (l'ordre compte toujours) et **sans remise** (pas de répétition) de p éléments de E.

Définition II.16

Soient $n \in \mathbb{N}^*$ et $p \in [\![1;n]\!]$. Le nombre d'arrangements de p éléments dans un ensemble de cardinal n ou encore le nombre de tirage successif sans remise de p éléments parmi n est noté

$$A_n^p.$$

Remarque 24 : Attention dans la notation A_n^p c'est le nombre d'arrangements de p éléments parmi n avec p en haut et n en bas au contraire de la notation $\binom{n}{p}$ que l'on va revoir plus loin.

Proposition II.17

Soient $n \in \mathbb{N}^*$ et $p \in [\![1;n]\!]$. Le nombre d'arrangements de p éléments dans un ensemble de cardinal n vaut

$$A_n^p = n \times (n-1) \times \cdots \times (n-p+1) = \frac{n!}{(n-p)!}.$$

Démonstration. Pour choisir le premier élément on a n choix possibles. Il nous reste alors $n-1$ éléments encore non choisis dans E. Pour choisir le deuxième élément on a donc $n-1$ possibilités. Il nous reste alors $n-2$ éléments et donc $n-2$ choix pour le troisième élément etc. □

Remarque 25 : On peut étendre la définition de A_n^p lorsque n et/ou p est nul en posant dans ce cas $A_n^p = \frac{n!}{(n-p)!}$. On peut également étendre A_n^p lorsque $p > n$ en posant dans ce cas $A_n^p = 0$.

Exemple 26 :

1. Dans une course opposant 9 athlètes, déterminer le nombre de podiums possibles.
2. Dans une urne possédant 7 boules toutes distinctes, déterminer le nombre de tirages possibles de trois boules sans remise puis avec remise.

Proposition II.18

Soient E et F deux ensembles finis de cardinal respectivement $\text{Card}(E) = p \in \mathbb{N}^*$ et $\text{Card}(F) = n \in \mathbb{N}^*$. Le nombre d'applications injectives de E dans F est alors égal à A_n^p. Autrement dit l'ensemble des applications injectives de E dans F est fini et de cardinal A_n^p.

Démonstration. Puisque $\text{Card}(E) = p$, on peut numéroter les éléments de E par $E = \{e_1, \ldots, e_p\}$. Pour construire une application injective de E dans F, il faut donner une image dans F à chaque élément e_i mais en prenant garde de choisir des images qui soient deux à deux distinctes. Ainsi pour $f(e_1)$ on prend n'importe quel élément de F. Puis pour choisir $f(e_2)$ on prend un élément dans $F \setminus \{f(e_1)\}$. De même pour choisir $f(e_3)$ on prend un élément dans $F \setminus \{f(e_1), f(e_2)\}$ et ainsi de suite. Autrement dit $(f(e_1), \ldots, f(e_p))$ constitue un arrangement de p éléments de F. Plus rigoureusement, en notant $\mathscr{I}$ l'ensemble des injections de E dans F et $\mathscr{A}$ l'ensemble des arrangements de p éléments de F, l'application

$$\begin{aligned} \Phi : \mathscr{I} &\to \mathscr{A} \\ f &\mapsto (f(e_1), \ldots, f(e_p)) \end{aligned}$$

est bijective. Donc $\text{Card}(\mathscr{I}) = \text{Card}(\mathscr{A}) = A_n^p$. □

II.5 Permutations

Définition II.19

Soit E un ensemble fini. **Une permutation** de E une bijection de E dans E.

Proposition II.20

Soit E un ensemble fini de cardinal $n \in \mathbb{N}^*$. Le nombre de permutations de E est égal à $A_n^n = n!$.

Démonstration. Une application de E dans E est bijective si et seulement si elle est injective. Or le nombre d'injections de E dans E vaut $A_n^n = n!$.

□

Remarque 27 : Une permutation revient donc à « réordonner » les éléments de E.

Exemple 28 :

1. Sans répétition : dénombrer les anagrammes de « lapin » puis de « physique »
2. Avec répétition : dénombrer les anagrammes de « permutation » puis de « Mississipi »

II.6 Combinaisons

Définition II.21

Soit E un ensemble fini $n \in \mathbb{N}^*$ et $p \in [\![1; n]\!]$. On appelle **combinaison** de p éléments de E toute partie de E de cardinal p.

Remarque 29 : Dans un sous-ensemble, on ne compte pas les répétitions $\{x, y, x, x, y, z\} = \{x, y, z\}$ et l'ordre n'a pas d'importance $\{x, y, z\} = \{y, x, z\} = \{y, z, x\} \dots$.

Remarque 30 : Construire une combinaison ou un sous-ensemble de E c'est donc tirer simultanément (par d'ordre particulier et pas de remise) p éléments parmi n.

Définition II.22

Soient $n \in \mathbb{N}^*$ et $p \in [\![1; n]\!]$. Le nombre de combinaisons de p éléments parmi n ou encore le nombre de tirages simultanés de n éléments parmi n est noté

$$\binom{n}{p}.$$

Proposition II.23

Soient $n \in \mathbb{N}^*$ et $p \in [\![1; n]\!]$. Le nombre de combinaisons de p éléments parmi n vaut

$$\binom{n}{p} = \frac{n!}{p!\,(n-p)!}.$$

Démonstration. Pour construire un arrangement de p éléments parmi n, on choisit une partie de p éléments parmi les n de l'ensemble E puis on les ordonne i.e. on effectue une permutation sur ces p éléments. Donc

$$A_n^p = \binom{n}{p} \times p!$$

Ainsi,

$$\binom{n}{p} = \frac{A_n^p}{p!} = \frac{n!}{p!\,(n-p)!}.$$

□

Remarque 31 : On peut étendre la définition de $\binom{n}{p}$ lorsque n et/ou p est nul en posant dans ce cas $\binom{n}{p} = \frac{n!}{p!(n-p)!}$. On peut également étendre $\binom{n}{p}$ lorsque $p > n$ en posant dans ce cas $\binom{n}{p} = 0$.

Exemple 32 : Un jeu de tarot contient 78 cartes dont 3 bouts, 22 atouts et 4 rois. Dans un jeu à quatre, chaque joueur se voit distribuer 18 cartes.

1. Déterminer le nombre de mains possibles.
2. Déterminer le nombre de mains avec les trois bouts.
3. Déterminer le nombre de mains avec exactement 10 atouts (la poignée).
4. Déterminer le nombre de mains avec 2 rois et 8 atouts exactement.

Rappels

Pour tout $(n,p)\in\mathbb{N}^2$,

1. $\binom{n}{0}=\binom{n}{n}=1$
2. $\binom{n}{1}=\binom{n}{n-1}=n$
3. (Formule de Pascal) $\binom{n}{p}+\binom{n}{p+1}=\binom{n+1}{p+1}$
4. $\binom{n}{n-p}=\binom{n}{p}$

Démonstration. Avec un point de vue combinatoire de la formule de Pascal. Soit E un ensemble de cardinal $n\in\mathbb{N}^*$. Soit $p\in[\![1;n]\!]$. On fixe $a\in E$. Parmi toutes les parties de E à p éléments, il y a les parties de E à p éléments qui contiennent a et les parties de E à p éléments qui ne contiennent pas a.

- Dénombrons le nombre de parties de E à p éléments qui contiennent a. Soit A une telle partie. Pour construire a, il faut commencer par mettre a dans A. Allons-y... voilà. Vous notez qu'il n'y a qu'une façon de le faire. Maintenant pour compléter A, il nous faut prendre $p-1$ éléments (sans ordre ni répétition) parmi les $n-1$ éléments restant de E i.e. parmi les éléments de $E\setminus\{a\}$. On a donc $\binom{n-1}{p-1}$ façon de compléter A et au final de construire une partie de E à p éléments qui contient a.
- Dénombrons maintenant le nombre de parties de E à p éléments qui ne contiennent pas a. Pour construire une telle partie il faut prendre (sans ordre ni remise) p éléments parmi l'ensemble $E\setminus\{a\}$ qui contient $n-1$ éléments. On a donc $\binom{n-1}{p}$ parties de E à p éléments qui ne contiennent pas a.

Au bilan le nombre de combinaison de p parmi n i.e. de parties de E qui contiennent p éléments est la somme du nombre de parties à p éléments qui contiennent a plus le nombre de parties à p éléments qui ne contiennent pas p :

$$\binom{n}{p}=\binom{n-1}{p-1}+\binom{n-1}{p}.$$

□

Rappel (formule du binôme de Newton)

Pour tout $(a,b)\in\mathbb{C}^2$ et tout $n\in\mathbb{N}$,

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}.$$

Démonstration. Avec un point de vue combinatoire. Pour développer le produit

$$(a+b)^n=\underbrace{(a+b)\,(a+b)\,(a+b)\dots(a+b)}_{n\text{ fois}},$$

il faut choisir dans chaque facteur l'élément a ou b. On obtiendra alors une somme

$$(a+b)^n=\sum_{k=0}^{n}c_ka^kb^{n-k},$$

où les c_k sont des coefficients à déterminer. Soit $k\in[\![0;n]\!]$. Pour obtenir le terme a^kb^{n-k} il faut avoir pioché exactement k fois l'élément a (et donc automatiquement $n-k$ l'élément b). Puisque l'ordre de la pioche est sans importance et que l'on tire un seul élément dans chaque facteur, le nombre de façon d'obtenir exactement k fois l'élément a est un tirage simultané de k parmi n. Ainsi

$$c_k=\binom{n}{k}$$

et donc

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

□

Définition II.24

Soit E un ensemble, on note $\mathscr{P}(E)$ l'ensemble de toutes les parties de E.

Exemple 33 : Si $E = \{a, b, c\}$, déterminer $\mathscr{P}(E)$.

Proposition II.25

Soit E un ensemble fini de cardinal $n \in \mathbb{N}^*$. Alors l'ensemble $\mathscr{P}(E)$ des parties de E est un ensemble fini de cardinal

$$\mathrm{Card}\left(\mathscr{P}(E)\right) = 2^n = 2^{\mathrm{Card}(E)}.$$

Démonstration. Pour tout $k \in [\![0; n]\!]$, on note $\mathscr{P}_k$ l'ensemble de parties de E à k éléments. En particulier $\mathscr{P}_0 = \{\emptyset\}$ et $\mathscr{P}_n = \{E\}$. Soit $k \in [\![0; n]\!]$, par définition $\mathscr{P}_k$ est l'ensemble des combinaisons de k parmi n. Donc $\mathscr{P}_k$ est de cardinal fini et

$$\mathrm{Card}\left(\mathscr{P}_k\right) = \binom{n}{k}.$$

De plus les ensembles $\mathscr{P}_k$ partitionne $\mathscr{P}(E)$ i.e.

$$\mathscr{P}(E) = \bigsqcup_{k \in [\![0;n]\!]} \mathscr{P}_k.$$

Donc d'après la proposition II.7, $\mathscr{P}(E)$ est de cardinal fini et on a

$$\mathscr{P}(E) = \sum_{k=0}^{n} \mathrm{Card}\left(\mathscr{P}_k\right) = \sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n.$$

□

Pierre de FERMAT *(Beaumont-de-Lomagne (actuellement en Tarn-et-Garonne) 1601 - Castres 1665) est le fils d'un riche marchand. Il suit des études de droit à Toulouse, puis à Bordeaux avant de les terminer à Orléans en 1631. Marié et père de cinq enfants, il mène une vie paisible comme conseiller au Parlement de Toulouse. Esprit à l'aise dans plusieurs discipline, il s'intéresse en amateur aux mathématiques. Il profite de ses moments de loisirs pour lire et annoter Diophante et surtout échanger abondamment par courrier avec le cercle de Mersenne et notamment Blaise PASCAL. La santé fragile des deux hommes annulera leur projet de rencontre. Fermat attrape la peste mais en réchappe miraculeusement. Il décède à Castres à l'âge de soixante-quatre ans.*

Fermat s'est principalement intéressé à l'arithmétique à travers ses lectures de Diophante. Il est également l'un des premiers à utiliser le formalisme algébrique des coordonnées introduit par DESCARTES pour résoudre des problèmes géométriques d'études de courbes (aux prémices du calcul différentiel à venir). Enfin à travers sa correspondance avec PASCAL, il discute abondamment de problème de dénombrement ce qui constituera les prolégomènes de la théorie des probabilités.
Fermat est certainement le mathématicien le plus dense de son époque mais son caractère semble contredire tous les clichés sur les génies : il ne fut pas précoce, travaille sans passion et ne possède aucun goût pour la publication. Il se contente très souvent d'annoter des oeuvres préexistantes et énonce des résultats sans chercher à écrire leur démonstration...
En particulier il énonce les deux théorèmes suivants sans les démontrer.

Petit théorème de Fermat

Soit p un nombre premier et $a \in \mathbb{Z}$. Alors p divise $a^p - a$ i.e. $a^p \equiv a\ [p]$.

LEIBNIZ écrivit une première démonstration en 1683 sans publier sa démonstration. EULER démontra ce résultat en 1736.

Grand théorème de Fermat

Soit $n \in \mathbb{N}$, $n \geqslant 3$. L'équation $x^n + y^n = z^n$ n'admet aucune solution dans $(\mathbb{N}^*)^3$.

Andrew WILES en s'appuyant sur les travaux d'autres mathématiciens, achèvera de démontrer ce théorème... en 1994 !

Anecdote bien connue, Fermat conjecture le théorème précédent en marge d'un livre de Diophante en écrivant « J'en ai découvert une démonstration merveilleuse mais je n'ai pas la place de la mettre dans la marge ». La complexité et la modernité des arguments utilisés pour démontrer ce théorème nous incite fortement à croire que la démonstration de Fermat était erronée ou partielle.

Jean, Matéo, Axel et Célestin sont très fiers de leurs résultats cette année et la vieille de leur examen final, plutôt que de réviser (comme tout bon étudiant qui se respecte) décident d'arroser copieusement cette année qui s'achève. Naturellement le lendemain le réveil est très difficile et lorsque les quatre compères se présentent, l'examen est déjà terminé. Larmoyants, ils expliquent à leur enseignant : « Nous avons aidé un ami commun à déménager la vieille. Nous avons roulé toute la nuit pour être à l'heure ce matin cependant alors que nous nous trouvions sans réseau sur une route secondaire l'un de nos pneus a éclaté. Nous avons dû attendre des heures avant qu'une autre voiture passe et prévienne la dépanneuse. » Conciliant l'enseignant leur répond qu'il accepte pour ses quatre âmes charitables de leur faire rattraper leur examen la semaine suivante. Cette fois-ci aucun retard, nos quatre étudiants sont placés dans une grande salle, éloignés les uns des autres sous la surveillance active de l'enseignant, bref, sans possibilité de tricher. Leur sujet commence par un petit exercice facile : un DL à l'ordre 12 pour connaitre la nature d'une série dont les restes sont approchés par une intégrale à paramètre qui après trois changements de variable et quatre ipp permet de faire apparaitre une application linéaire dont la représentation matricielle est prétexte à un petit exercice sur les probabilités. Bref après 10 minutes nos étudiants (très forts cela va de soi) résolvent sans hésiter cet exercice affiché sur deux points puis tournent leur feuille pour découvrir le problème 2 sur 18 points et lisent l'énoncé suivant : « Précisez quel pneu était à plat. »

La déconvenue de nos héros vous a plu ? Alors calculez-moi le nombre total de réponses possibles et le nombre de réponses leur permettant de flouer leur (très vénéré) enseignant. Quelle est la probabilité qu'ils puissent s'en sortir ?