Les Mathématiques pour Commencer

BOOK · JANUARY 2007

DOI: 10.13140/RG.2.1.1496.1367

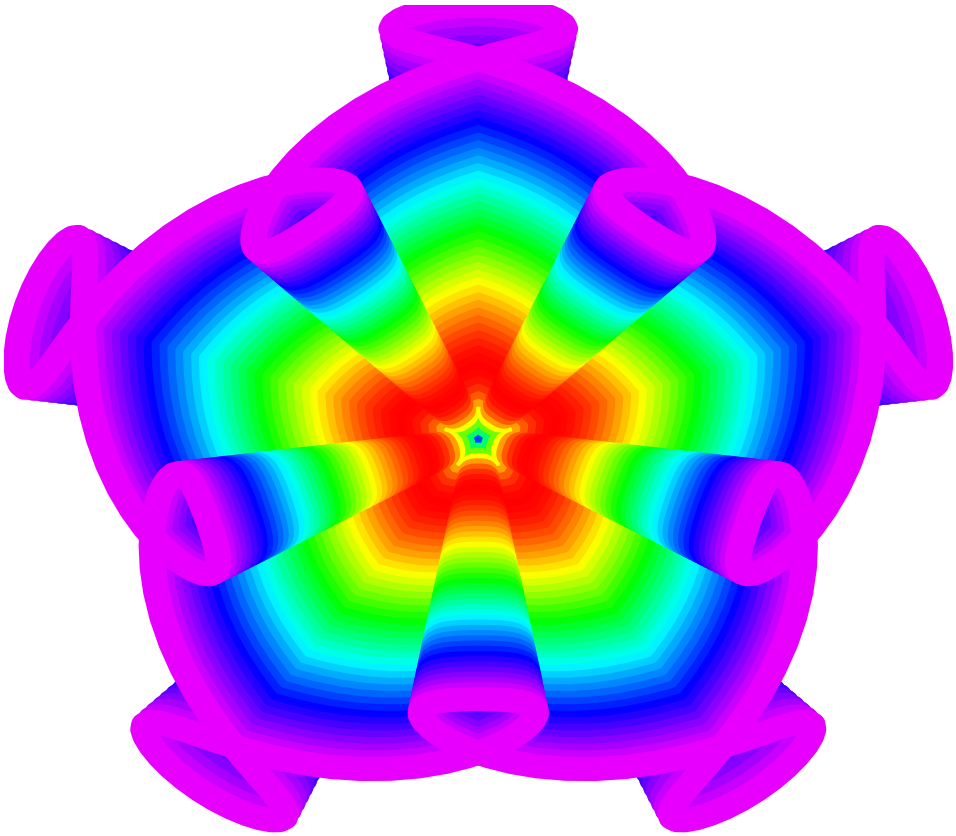
1 AUTHOR:

Omran Kouba

72 PUBLICATIONS **82** CITATIONS

SEE PROFILE

Les Mathématiques Pour Commencer



Omran Kouba

le 10 Février 2007

Introduction

La définition des mathématiques par leur méthodes est très stable et n'a pas varié des Grecs à nos jours: les mathématiques développent à partir de notions de base, des théories ne faisant appel qu'au raisonnement logique. Le degré de lucidité de cette démarche a pu varier au cours des temps ou selon les individus, mais elle n'a pas changé de nature. L'objet sur lequel porte le raisonnement mathématique est en lui-même arbitraire. Il suffit qu'un sujet donne prise au raisonnement et intéresse un mathématicien ou ceux au profit desquels il travaille, pour que naisse un nouveau chapitre des mathématiques. Un mathématicien est par conséquent un homme qui, par goût ou profession, développe des théories à partir de notions de base posées a priori en s'appuyant uniquement sur le raisonnement.

Le point exprimé précédemment explique aussi l'introduction et l'utilisation accrue des mathématiques dans les autres sciences à cause de la soif de ces dernières à l'exactitude, à la rigueur, et à la construction de théories bien fondées. De nos jours, on imagine très difficilement les théories de la mécanique quantique, ou la théorie des champs loin de leurs bains mathématiques naturels.

On a aussi vécu, dans le $XX^{\text{ième}}$ siècle, la mathématisation de beaucoup de sciences comme la chimie, la biologie, l'économie, et les sciences sociales. La valeur des sciences mathématiques n'est plus discutable.

Dans ce livre, nous nous proposons d'introduire l'étudiant aux mathématiques comme modes de raisonnement en choisissant des sujets simples sans difficultés théoriques et tenant compte du fait que l'enseignement se déroule en langue française.

Décrivons le contenu de ce livre. Le premier chapitre présente des exercices permettant de développer l'aptitude au raisonnement logique. Le deuxième chapitre décrit deux problèmes récurrents qui constituent des modèles de raisonnement mathématique. Le troisième chapitre introduit les techniques simples de manipulation de sommes. Le quatrième chapitre étudie la fonction partie entière et les propriétés simples dont elle jouit. Le cinquième chapitre est plus riche en connaissances, on y trouve beaucoup de problèmes de dénombrement. Le sixième chapitre étudie la divisibilité dans l'ensemble des entiers relatifs. Enfin dans le septième chapitre on présente les congruences dans l'ensemble des entiers relatifs.

Je voudrais à la fin de cette introduction exprimer ma gratitude à H. HACHEM et K. HALAWÉH pour les remarques qu'ils ont formulées sur le contenu de ce livre, et pour les exercices qu'ils ont apportés. Je voudrais aussi remercier ma femme Y. ATASSI pour sa patience, ses encouragements et aussi pour avoir lu et corrigé beaucoup de fautes de frappe.

OMRAN KOUBA

Table Des Matières

La théorie élémentaire des nombres est la discipline la mieux adaptée à un enseignement primaire des mathématiques. Elle ne demande que très peu de connaissances antérieures, et le sujet de son étude est concret et familier ; les méthodes de raisonnement employées sont simples, générales et peu nombreuses ; et elle est unique parmi les diverses branches des mathématiques pour la curiosité humaine qu'elle requiert.

Godfrey Harold HARDY

Chapitre Premier

Logique et raisonnement

Comme toute autre science, les mathématiques sont exprimées, décrites et formulées avec des mots du langage courant. Il est donc indispensable et impératif d'utiliser les mots dans leur sens qui leur correspond en mathématiques, et qui peut être différent de leur sens dans la langue d'usage.

D'autre part, l'organisation d'un texte mathématiques n'est pas celle d'un discours ordinaire ; les appréciation vagues, qualitatives, suggestives, en sont exclues. Dans la langue mathématique, tout usage un peu abusif, toute phrase floue ou approximative, conduisent immédiatement à des erreurs énormes, bien au-delà de la faute de logique.

Tout ce qui ressemble à la vérité, mais n'est pas vérifié dans ses moindres détails, est faux.

L'étudiant qui souhaite aborder les études scientifiques dans de bonnes conditions, doit se préparer à un changement radical dans ses méthodes de pensé et de reflexion.

L'essentiel du travail mathématique porte sur la manipulation de propositions. Par proposition on entend une affirmation – portant sur des objets mathématiques: points, nombres,*etc.*– à laquelle on peut attribuer clairement la valeur *vraie* ou bien la valeur *fausse*, par exemple "7 est un nombre premier" est une proposition vraie. Souvent les propositions contiennent des variables: nombre x, entier naturel n, ... Nous noterons alors une telle proposition $P(x)$, $P(n)$, ... pour marquer la dépendance de sa valeur de vérité vis-à-vis de la variable. Par exemple "n est un multiple de 7" peut être vraie ou fausse suivant la valeur de n.

Si P et Q sont deux propositions, alors on peut construire de nouvelles propositions à partir de ces deux là, en utilisant des opérations logiques:

- "P ET Q" est la proposition qui est vraie si, seulement si, les deux propositions P et Q sont vraies.
- "P OU Q" est la proposition qui est vraie si, seulement si, une des deux propositions P ou Q est vraie.
- "NON P" est la proposition qui est vraie si, seulement si, P est fausse. Cette proposition s'appelle la négation de P.
- "$P \implies Q$" c'est la proposition d'implication, elle coïncide avec la proposition " (NON P) OU Q", donc "$P \implies Q$" est vraie si et seulement si, P est fausse ou Q est vraie.
- "$P \iff Q$" c'est la proposition d'équivalence, elle est vraie si, seulement si, la proposition "$P \implies Q$ ET $Q \implies P$" est vraie.

Démontrer la vérité d'une proposition P consiste à effectuer une suite d'opérations logiques portant sur des propositions vraies ou des faits connus pour arriver à prouver la vérité de P. Cette démarche s'appelle raisonnement.

Nous allons, en traitant des exemples, apprendre à répondre à faire des raisonnements.

1. L'île de la sagesse !

Les habitants de cette île sont soit sages, soit fous. Sachant qu'il y a cent habitants sur l'île et que:

– Il y a au moins un sage parmi eux.

– Il y a au moins un fou parmi chaque couple d'habitants.

Combien de sages et de fous y a -t- il sur l'île ?

Discussion:

S'il y a au moins deux sages dans l'île, alors on y trouve un couple ne contenant pas de fous, ce qui contredit la deuxième assertion. En utilisant la première assertion on déduit alors qu'il y a un sage et quatre-vingt-dixneuf fous sur l'île. Ils doivent s'amuser bien.

2. Moi, je n'aime pas les chapeaux

Messieurs Dupont,Durand et Dubois sont réputés pour leur intelligence. Le Maire de la ville, Monsieur Charpentier, décide alors, de les mettre à l'épreuve:

1°. Il envoie son assistant chercher cinq chapeaux, trois rouges et deux bleus, puis il met un châpeau sur la tête de chacun des trois messieurs et cache les chapeaux restant. Chacun des trois messieurs pouvait voir les chapeaux des autres mais pas le sien.

Le Maire leur pose la question: "*Est-ce que quelqu'un parmi vous connaît la couleur de son chapeau ?* ". Une minute de silence est passée avant que Monsieur Dubois (le plus intelligent) trouve la couleur de son chapeau.

Quelle est la couleur du chapeau de Monsieur Dubois ?

2°. Le Maire décide, alors, de les soumettre à une deuxième épreuve, mais cette fois avec sept chapeaux ; deux rouges, deux jaunes et trois bleus. Il procède comme avant, et il leur pose la question suivante: "*Est-ce que l'un de vous peut indiquer de façon certaine une couleur (parmi les trois: rouge, jaune ou bleu), qui ne soit pas celle de son chapeau ?*". Monsieur Dupont répond "*Non*". Tout de suite après, Monsieur Durand répond "*Moi, non plus*".

De quelle couleur est le chapeau de Monsieur Dubois ?

Discussion:

1°. Le fait qu'il y ait eu un certain temps d'attente montre qu'il n'y avait pas deux chapeaux bleus sur les têtes des amis. S'il y avait seulement un chapeau bleu alors les deux amis qui le voyaient auraient donc découvert la couleur rouge de leurs chapeaux. Monsieur Dubois, ayant fait ce raisonnement assez vite, a découvert par conséquent que les trois chapeaux étaient rouges.

2°. Si le chapeau de Dubois était rouge ou jaune, alors Durand aurait dû savoir que le sien n'a pas la même couleur de celui de Dubois (Sinon Dupont aurait répondu "*Oui*"). Par conséquent le chapeau de Dubois était bleu.

3. Au village de Karo

Il était une fois un village qui s'appelait *Karo*. *Karo* n'était habité que par deux familles ; les Durand et les Dupont. Les Durand disaient toujours la vérité, les Dupont mentaient toujours.

1°. Un jour, deux habitants de *Karo*, A et B, se sont rencontrés. A a dit "*Au moins l'un de nous est Dupont* ". De quelles familles étaient A et B ?

2°. Le jour d'aprés, deux autres villageois, C et D discutaient en sortant d'un Bistro, et on a entendu C dire "*Soit je suis un Dupont, soit D est Durand* ". De quelles familles étaient C et D ?

3°. Trois habitants E, F et G de *Karo*, se sont rencontrés, et E et F ont affirmé:

E: "*Nous sommes tous des Dupont* ".

F: "*Il y a exactement un parmi nous qui soit Durand* ".

De quelles familles étaient E, F et G ?

4°. Un jour de printemps, un voyageur a rencontré quatre villageois et il a demandé au premier "*Êtes vous des Durand ou des Dupont ?* ". "*Nous sommes tous des Dupont*" affirma le villageois. Le second déclara aussitôt: "*Non, un seul d'entre nous est Dupont* ". Le troisième a dit alors "*Ne les croyez pas, il y a exactement deux Dupont parmi nous* ". Quant au quatrième, il affirma "*Je suis un Durand* ". A-t-il dit la vérité ?

5°. Deux pas plus loin le même voyageur rencontra K, L et M. K lui a dit "*L et M sont de la même famille*", alors le voyageur posa à M la question: "*Est-ce que K et L sont de la même famille ?*". Quelle réponse a-t-il obtenu ?

Discussion:

1°. Si A était Dupont alors il aurait menti et par conséquent aucun des deux ne serait Dupont ce qui est absurde. Donc A est Durand et comme il ne ment pas B est Dupont.

2°. Si C était Dupont alors il aurait menti et par conséquent il ne serait pas Dupont et D ne serait pas Durand ce qui est absurde. Donc C est Durand et comme il ne ment pas D est aussi Durand.

3°. Comme les Durand ne disent que la vérité, E ne peut être un Durand, il est, alors, Dupont. Par conséquent il y a au moins un Durand parmi F et G. Si F était Dupont, il y aurait exactement un Durand parmi les trois et F n'aurait pas menti ce qui est absurde. F est alors un Durand et comme il ne ment pas G doit être Dupont.

4°. Le premier villageois est forcément un Dupont, donc il y a au moins un Durand parmi les trois autres. Les paroles du deuxième et du troisième villageois sont contradictoires donc il y a un autre Dupont parmi ces deux villageois ce qui met en défaut la parole du deuxième il est donc un Dupont. On distingue alors deux cas:- Soit le troisième est un Durand, alors les deux Dupont dont il a parlé sont les deux premiers et le quatrième a dit la vérité.- Soit le troisième est un Dupont, et alors le quatrième est le seul Durand parmi les quatre villageois et il a dit la vérité.

5°. Distinguons deux cas:

1. K est Durand, alors il aurait dit la vérité et on peut envisager deux cas:
   1.1 L et M sont Durand, M aurait dit la vérité et répondu "*Oui* ".
   1.2 L et M sont Dupont, M aurait menti et répondu "*Oui* ".
2. K est Dupont, alors il aurait menti, donc il y a deux cas:
   2.1 L est Dupont et M est Durand, M aurait dit la vérité et répondu "*Oui*".
   2.2 L est Durand et M est Dupont, M aurait menti et répondu "*Oui* ".

Dans tous les cas M aurait répondu "*Oui*".

4. À la station de Transylvanie

A la station de transylvanie il y a quatre types de travailleurs:

- Les humains sains d'esprit.
- Les humains fous.
- Les vampires sains d'esprit.
- Les vampires fous.

Tout ce qu'un humain sain d'esprit dit est vrai. Tout ce qu'un humain fou dit est faux. Tout ce qu'un vampire sain d'esprit dit est faux. Tout ce qu'un vampire fou dit est vrai.

1°. Une fois j'ai rencontré un transylvanien. Il a dit "*Je suis un humain ou je suis sain d'esprit*". De quel type il était ?.

2°. Un autre travailleur a dit "*Je ne suis pas un humain sain d'esprit* ". De quel type il était ?.

3°. Un autre travailleur a dit "*Je suis un humain fou* ". Est-ce qu'il est du même type que le précédent ?.

Discussion:

1°. Si ce travailleur a menti, il doit être un vampire fou or ceux-là ne disent que la vérité ce qui est absurde. Donc, le travailleur a dit la vérité, par conséquent il ne peut pas être un vampire fou, alors il est un humain sain d'esprit.

2°. Si ce travailleur a menti, il doit être un humain sain d'esprit or ceux-là ne disent que la vérité ce qui est absurde. Donc, le travailleur a dit la vérité, comme il ne peut pas être un humain sain d'esprit, alors il est un vampire fou.

3°. Si ce travailleur a dit la vérité, il doit être un humain fou or ceux-là mentent toujours ce qui est absurde. Donc, le travailleur a menti, il n'est pas un humain fou, alors il est un vampire sain d'esprit, et il n'est pas du même type que le précédent.

5. Une princesse ou un tigre ?

Un roi a eu l'idée de donner à ses prisonniers une chance de retrouver la liberté. Un prisonier doit choisir entre deux cellules dont chacune peut cacher une princesse ou un tigre. S'il en choisit une cachant une princesse, il doit l'épouser, mais s'il tombe sur une cachant un tigre, il est dévoré (ou il dévorera le tigre !). Toutes les combinaisons étaient possibles ; Il pouvait y avoir deux tigres, deux princesses, ou un tigre et une princesse.

1°. Le roi entraîna le premier prisonnier et lui montra les affiches qu'il avait lui-même collées sur les portes des cellules:

$$\left\{\begin{array}{c} -1- \\ \textit{Il y a une princesse dans} \\ \textit{cette cellule et} \\ \textit{un tigre dans l'autre} \end{array}\right\} \qquad \left\{\begin{array}{c} -2- \\ \textit{Il y a une princesse dans} \\ \textit{une cellule et il y a} \\ \textit{un tigre dans une cellule} \end{array}\right\}$$

Le roi promit au prisonnier: "*Une des affiches dit la vérité et l'autre ment*". Quelle cellule devrait choisir le prisonnier ?

2°. Le deuxième prisonnier s'était trouvé en face des deux affiches suivantes, collées sur les portes des cellules:

−1−	−2−
Il y a un tigre dans cette cellule ou il y a une princesse dans l'autre	*Il y a une princesse dans l'autre cellule*

Le roi affirma: "*Les deux affiches sont, soit toutes les deux sincères, soit toutes les deux fausses*".

Que contenait la première cellule ? Et la seconde ?

3°. Le roi décida de changer les règles de jeu comme l'expliqua lui même aux prisonniers: "*L'affiche que je collerai sur la cellule* 1 *dira la vérité quand il y aura une princesse dans cette cellule et mentira quand ce sera un tigre. Pour la cellule* 2 *ce sera exactement le contraire ; quand il y aura une princesse l'affiche mentira et quand ce sera un tigre elle dira la vérité. Une fois encore chaque cellule pourra cacher indifféremment un tigre ou une princesse*".

Le roi emmena le troisième prisonnier voir les affiches:

−1−	−2−
Choisis n'importe quelle cellule, ça n'a pas d'importance !	*Il y a une princesse dans l'autre cellule*

Que devait faire le prisonnier ?

4°. Avec les mêmes règles du jeu qu'au 3° on montra au quatrième prisonnier les affiches suivantes:

−1−	−2−
Choisis bien ta cellule, ça a de l'importance !	*Tu ferais mieux de choisir l'autre cellule !*

Que devait faire le prisonnier ?

5°. Enfin, (avec les mêmes règles qu'au 3°.) on donna au prisonnier les deux affiches suivantes:

$$\left\{\begin{array}{c}-?-\\ \textit{Les deux cellules contiennent}\\ \textit{des tigres}\end{array}\right\} \qquad \left\{\begin{array}{c}-?-\\ \textit{Cette cellule contient}\\ \textit{un tigre}\end{array}\right\}$$

mais on ne lui dit pas laquelle des deux affiches appartient à la première cellule, et laquelle appartient à la seconde.

Que feriez-vous si vous étiez à la place du prisonnier ?

Discussion:

1°. Si l'affiche de la première cellule dit la vérité, alors l'affiche de la deuxième cellule sera aussi vrai, ce qui contredit la parole du roi. On en déduit que l'affiche 1 ment et la princesse est dans la deuxième cellule.

Le prisonnier devrait choisir celle-là.

2°. Si les deux affiches étaient fausses alors, de l'affiche 2, on déduit qu'il y avait un tigre dans la première cellule et l'affiche 1 serait vraie: une contradiction. Par conséquent, les deux affiches étaient sincères, et les deux cellules cachaient des princesses.

Le prisonnier pouvait choisir n'importe quelle cellule.

3°. Supposons qu'il y avait une princesse dans la première cellule, alors l'affiche 1 serait sincère, et la deuxième cellule cacherait aussi une princesse, donc son affiche ne devrait pas dire la vérité ce qui est absurde. Par conséquent la première cellule cachait un tigre. L'affiche 2 mentait donc il y avait une princesse dans la deuxième cellule.

Le prisonnier devrait choisir la deuxième cellule.

4°. Supposons que la première cellule cachait un tigre, alors son affiche est fausse ce qui veut dire que la deuxième cellule cachait aussi un tigre, et son affiche disait la vérité ce qui est absurde. Par conséquent la première cellule cachait une princesse, et la sincérité de son affiche montre que la deuxième cellule contenait un tigre.

Le prisonier devrait choisir la première cellule.

5°. Supposons que l'affiche sur laquelle est écrit {*Cette cellule contient un tigre*} appartenait à la première cellule. Dans ce cas, soit la première cellule cachait un tigre, et l'affiche dit la vérité ce qui est contre la règle du jeu, soit elle cachait une princesse, et l'affiche

mentait ce qui est aussi contre la règle du jeu. Par conséquent cette affiche appartient à la deuxième cellule.

L'affiche de la première cellule: {*Les deux cellules contiennent des tigres*}, devrait donc être fausse, (car si elle était vrai, il y aurait une princesse et un tigre dans la première cellule, ce qui est absurde). Par conséquent il y avait un tigre dans la première cellule, et une princesse dans la seconde.

Le prisonnier devrait choisir la deuxième cellule.

6. Y a-t-il un crime parfait ?

Rapport du Commissariat de Police concernant le meurtre de *Jacques D.*

Lieu: Allée du Roi, Paris.

Date: Le 17 Mars à trois heures trente du matin.

Circonstances: Un homme inconnu attaque M. *Jacques D.* et le tue.

Une semaine plus tard, la Police interpelle cinq hommes *Jean*, *Philippe*, *Yves*, *Gilles* et *Patrick* au sujet du meurtre. Chacun a donné quatre affirmations dont trois étaient vraies et une était fausse:

Jean : (J_1) J'étais à Lyon au moment du meurtre. (J_2) Je n'ai jamais tué quelqu'un. (J_3) *Patrick* est le meurtrier. (J_4) *Gilles* et moi sommes amis.

Philippe : (Ph_1) Je n'ai pas tué *Jacques*. (Ph_2) Je n'ai jamais eu de revolver. (Ph_3) *Patrick* me connaît. (Ph_4) J'était à Toulouse la nuit du 17 Mars.

Yves : (Y_1) *Philippe* a menti lorsqu'il a dit qu'il n'avait jamais eu de revolver. (Y_2) Le crime a été commis le 17 Mars. (Y_3) *Jean* était à Lyon au moment du meurtre. (Y_4) L'un de nous est le meurtrier.

Gilles : (G_1) Je n'ai pas tué *Jacques*. (G_2) *Patrick* n'était jamais à Paris. (G_3) Je n'ai jamais rencontré *Jean* avant. (G_4) *Philippe* et moi étions à Toulouse la nuit du 17 Mars.

Patrick : (P_1) Je n'ai pas tué *Jacques*. (P_2) Je n'étais jamais à Paris. (P_3) Je n'ai pas rencontré *Philippe* avant. (P_4) *Jean* a menti en disant que j'ai tué *Jacques*.

Est-ce que l'un de ces hommes a tué *Jacques* ? Si oui, lequel ?

Discussion:

– Comme (P_1) ou (P_4) est vraie, alors

$$(J_1, J_2, J_3, J_4) = (\text{Vraie, Vraie, Fausse, Vraie})$$

– Comme (J_4) est vraie, alors

$$(G_1, G_2, G_3, G_4) = (\text{Vraie, Vraie, Fausse, Vraie})$$

– Comme (G_2) est vraie, et (J_3) est fausse, alors

$$(P_1, P_2, P_3, P_4) = (\text{Vraie, Vraie, Fausse, Vraie})$$

– On a aussi (Ph_3), (Ph_4), (Y_2) et (Y_3) sont vraies.

– Comme (Ph_4) est vraie, alors (Ph_1) est aussi vraie, et donc

$$(Ph_1, Ph_2, Ph_3, Ph_4) = (\text{Vraie, Fausse, Vraie, Vraie}).$$

– Par conséquent, (Y_1), (Y_2), (Y_3) sont vraies, et (Y_4) est fausse.

Conclusion: Prenez garde ! le tueur est toujours en libérté.

7. L'histoire des douze boules

On dispose douze boules identiques en apparence. Onze de ces boules ont le même poids P et la douzième a un poids différent $\widetilde{P}$, qui peut être plus grand ou plus petit que P. On dispose aussi d'une balance qui permet de faire des comparaisons.

On demande d'identifier la boule différente et de préciser si elle est plus lourde ou plus légère, en utilisant la balance n fois seulement. Expliquer comment procéder lorsque $n = 4$. Pouvez vous le faire lorsque $n = 3$?

Discussion:

Nous allons traiter le cas $n = 3$ qui demande un raisonnement logique assez complexe.

Commençons par grouper les boules en trois sous-ensembles, chacun formé de quatre boules: G_1, G_2 et G_3.

Comparons les poids des deux sous-ensembles G_1 et G_2. Deux cas sont possibles:

Cas 1. Les deux sous-ensembles G_1 et G_2 sont de même poids:

$$\underbrace{G_1 \quad = \quad G_2}$$

Cas 2. Les deux sous-ensembles G_1 et G_2 sont de poids différents. On peut supposer que le poids de G_1 est inférieur à celui de G_2:

$$\underbrace{G_1 \quad < \quad G_2}$$

Étudions le premier cas :

1. Dans ce cas la boule différente se trouve parmi les quatre boules restantes que nous allons les noter : $G_3 = \{\otimes_1, \otimes_2, \otimes_3, \otimes_4\}$. Les boules de $G_1 \cup G_2$ sont toutes normales de poids P.

Choisissons trois boules normales $\{\odot_1, \odot_2, \odot_3\}$, et *comparons* ces trois boules avec $\{\otimes_1, \otimes_2, \otimes_3\}$. Trois cas sont possibles:

1.1.

$$\underbrace{\underbrace{\{\otimes_1, \otimes_2, \otimes_3\}} \quad = \quad \underbrace{\{\odot_1, \odot_2, \odot_3\}}}$$

C'est alors la boule $\otimes_4$ qui est différente, on la *compare* avec une boule normale pour décider si elle est plus lourde ou plus légère qu'une boule normale.

1.2.

$$\underbrace{\underbrace{\{\otimes_1, \otimes_2, \otimes_3\}} \quad > \quad \underbrace{\{\odot_1, \odot_2, \odot_3\}}}$$

La boule différente est parmi $\{\otimes_1, \otimes_2, \otimes_3\}$, et elle est plus lourde que les boules normales: $\widetilde{P} > P$. Il suffit alors de *comparer* deux de ces boules. Si elles sont égales c'est la troisième qui est la boule différente, et si elles ne le sont pas alors la plus lourde est la boule différente.

1.3.

$$\underbrace{\underbrace{\{\otimes_1, \otimes_2, \otimes_3\}} \quad < \quad \underbrace{\{\odot_1, \odot_2, \odot_3\}}}$$

La boule différente est parmi $\{\otimes_1, \otimes_2, \otimes_3\}$, et elle est plus légère que les boules normales: $\widetilde{P} < P$. Il suffit alors de *comparer* deux de ces boules. Si elles sont égales c'est la troisième qui est la boule différente, et si elles ne le sont pas alors la plus légère est la boule différente. Ceci achève l'étude du **Cas 1.**

Venons au deuxième cas:

2. Ce cas est plus délicat à traiter. Notons $G_1 = \{\otimes_1, \otimes_2, \otimes_3, \otimes_4\}$ et $G_2 = \{\oplus_1, \oplus_2, \oplus_3, \oplus_4\}$. La boule différente est parmi $G_1 \cup G_2$. Soit $\odot$ une boule normale prise dans G_3.

On *compare* $\{\otimes_1, \otimes_2, \oplus_2\}$ avec $\{\oplus_1, \otimes_3, \odot\}$, là aussi il y a trois cas possibles:

2.1.

$$\underbrace{\{\otimes_1, \otimes_2, \oplus_2\}}_{} \quad < \quad \underbrace{\{\oplus_1, \otimes_3, \odot\}}_{}$$

Dans ce cas, on *compare* $\otimes_1$ et $\otimes_2$. S'il y a égalité alors $\oplus_1$ est la boule différente et elle est plus lourde qu'une boule normale: $\widetilde{P} > P$, et s'il n'y a pas d'égalité alors la plus légère des boules $\otimes_1$ et $\otimes_2$ est la boule différente (et elle est, donc, plus légère qu'une boule normale: $\widetilde{P} < P$).

2.2.

$$\underbrace{\{\otimes_1, \otimes_2, \oplus_2\}}_{} \quad = \quad \underbrace{\{\oplus_1, \otimes_3, \odot\}}_{}$$

Dans ce cas, on *compare* $\oplus_3$ et $\oplus_4$. S'il y a égalité alors $\otimes_4$ est la boule différente et elle est plus légère qu'une boule normale: $\widetilde{P} < P$, et s'il n'y a pas d'égalité alors la plus lourde des boules $\oplus_3$ et $\oplus_4$ est la boule différente (et elle est, donc, plus lourde qu'une boule normale: $\widetilde{P} > P$).

2.3.

$$\underbrace{\{\otimes_1, \otimes_2, \oplus_2\}}_{} \quad > \quad \underbrace{\{\oplus_1, \otimes_3, \odot\}}_{}$$

Dans ce cas, on *compare* $\otimes_3$ et $\odot$. Si $\otimes_3$ est plus légère alors elle est la boule différente (et elle est plus légère qu'une boule normale: $\widetilde{P} < P$), et s'il y a égalité alors $\oplus_2$ est la boule différente (et elle est plus lourde qu'une boule normale: $\widetilde{P} > P$).

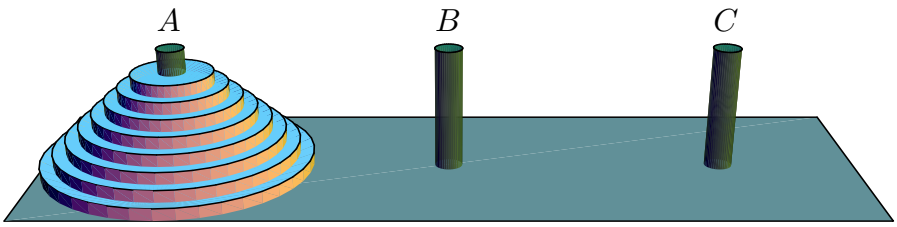
On a, donc, réussi à déterminer la boule différente et à déterminer si elle est plus lourde qu'une boule normale ou plus légère, et cela en utilisant la balance trois fois seulement.

Problémes récurrents

Nous allons dans ce chapitre traiter deux problèmes qui ont en commun la particularité que leurs solutions utilisent l'idée de *récurrence*, c'est à dire que la solution de chaque problème dépend des solutions d'exemples plus petits du même problème.

1. La tour de Hanoï

C'est un jeu inventé par le mathématicien français Edouard Lucas en 1883. On se donne trois chevilles et une tour de huit disques, initialement empilés dans l'ordre décroissant de la taille, sur l'une des chevilles.



L'objectif est de déplacer la tour en entier à l'une des autres chevilles, en déplaçant seulement un disque à chaque fois, et en ne mettant jamais un disque grand sur un autre plus petit.

Il n'est pas tout à fait évident qu'il y a une solution à ce problème, mais avec un peu de réflexion, nous arrivons à nous en convaincre. La question qui surgit tout de suite est: "*Quel est le mieux qu'on peut faire ?*", c'est à dire "*Quel est le nombre de déplacements*

nécessaires et suffisants pour effectuer la tâche ?".

La meilleure façon d'attaquer une question comme celle-là est de la généraliser un peu. La tour de Hanoï contenait 8 disques, voyons ce qui se passe si l'on suppose que la tour contient n disques.

Un avantage de cette généralisation est qu'elle nous permet de considérer le problème dans une petite échelle, c'est à dire de regarder les cas correspondant à un ou deux disques. Une petite expérimentation nous montre aussi comment transférer une tour de trois disques.

Il est toujours avantageux de considérer les cas particuliers simples.

L'étape suivante dans la résolution du problème réside dans l'introduction d'une notation appropriée. Notons T_n le plus petit nombre de déplacements pour transférer une tour de n disques d'une cheville à une autre en respectant les règles de Lucas. Il est alors clair que T_1 vaut 1 et $T_2 = 3$.

Il est toujours important d'introduire des notations convenables.

On peut aussi voir que $T_0 = 0$, car pour transférer une tour ne contenant pas de disques ! 0 déplacement suffit ! !.

Changeons de point de vu, et considérons le cas général ; comment peut-on transférer une grande tour ? L'expérience avec trois disques montre que l'idée gagnante est de transférer d'abord les deux disques du haut, à la cheville du milieu B, de déplacer, ensuite, le plus grand disque à la troisième cheville C, et enfin, de transférer les deux autres au dessus. Ceci nous donne une idée pour le cas général: D'abord, on transfère les $n-1$ disques du haut, à la cheville du milieu B (ce qui demande T_{n-1} déplacements), ensuite, on déplace le plus grand disque à la troisième cheville (ce qui demande 1 déplacement), et enfin, on transfère les $n-1$ disques au dessus de ce dérnier (ce qui demande aussi T_{n-1} déplacements). Par conséquent, on peut transférer une tour de n disques en au plus $1 + 2T_{n-1}$ déplacements:

$$T_n \leq 2T_{n-1} + 1, \qquad \text{pour tout } n > 0.$$

La formule précédente contient "$\leq$" au lieu de "=" car notre construction montre que $2T_{n-1} + 1$ déplacements suffisent, mais nous n'avons pas démontré que $2T_{n-1} + 1$

déplacements sont nécessaires. Est-ce qu'on peut faire mieux ? En fait on ne peut pas. À un certain moment on doit déplacer le plus grand disque, les autres $n-1$ disques doivent se trouver sur une même cheville et ils ont nécessité au moins T_{n-1} déplacements pour y être transférés. On peut déplacer le plus grand disque plusieurs fois, mais après l'avoir fait pour la dernière fois, on doit transférer les autres $n-1$ disques (qui se trouvent forcement sur une seule cheville) au dessus du plus grand (encore au moins T_{n-1} déplacements). Alors

$$T_n \geq 2T_{n-1} + 1, \qquad \text{pour tout } n > 0.$$

Ces deux inégalités, avec le cas trivial pour $n = 0$, impliquent

$$\begin{aligned} T_0 &= 0; \\ T_n &= 2T_{n-1} + 1, \qquad \text{pour } n > 0 \end{aligned} \tag{1}$$

Remarquons que ces formules sont en accord avec les valeurs connues $T_1 = 1$ et $T_2 = 3$.

Calculons successivement: $T_3 = 2 \cdot 3 + 1 = 7$, $T_4 = 2 \cdot 7 + 1 = 15$, $T_5 = 2 \cdot 15 + 1 = 31$, $T_6 = 2 \cdot 31 + 1 = 63$. Cela ressemble à

$$T_n = 2^n - 1, \qquad \text{pour } n > 0 \tag{2}$$

c'est au moins vrai si $n \leq 6$.

La relation (2) peut être démontrée à partir de (1) par *récurrence*. Supposons que, pour un certain $n > 0$, on a $T_{n-1} = 2^{n-1} - 1$ alors, en utilisant (1), on a

$$T_n = 2T_{n-1} + 1 = 2(2^{n-1} - 1) + 1 = 2^n - 1.$$

La formule (2) est donc vraie, et on arrive à la conclusion suivante:

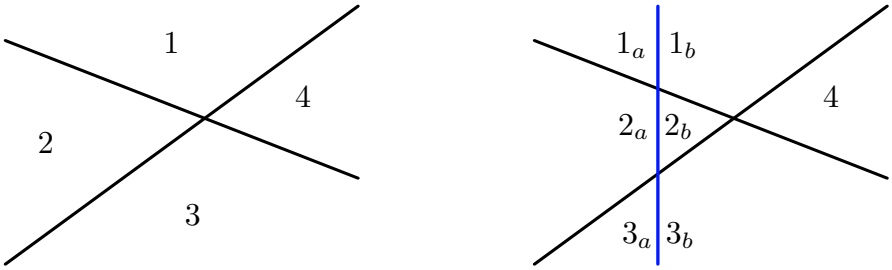
Le plus petit nombre de déplacements nécessaires pour transférer une tour de n disques d'une cheville à une autre en respectant les règles de Lucas est $T_n = 2^n - 1$.

2. Droites dans le plan

Notre deuxième exemple est un peu géométrique: "*Combien de morceaux de pizza peut-on obtenir en effectuant n coupes droites de la pizza par un couteau ?* ". D'une façon plus académique: "*quel est le plus grand nombre L_n de régions définies par n droites dans le plan ?*" Ce problème a été résolu pour la première fois par le mathématicien suisse Jacob Steiner en 1826.

Encore une fois nous allons commencer par traiter les cas simples correspondant aux petites valeurs de n. Le plan sans aucune droite est formé d'une seule région ($L_0 = 1$), avec une seule droite le plan contient deux régions ($L_1 = 2$), et avec deux droites (non parallèles) il contient quatre régions ($L_2 = 4$).

Bien sûr, on peut penser que $L_n = 2^n$; ajouter une droite dédouble le nombre de régions. Malheureusement c'est faux. Ce serait vrai si la $n^{\text{ième}}$ droite coupe toutes les anciennes régions en deux. Mais si l'on rajoute une troisième droite, on se rend compte rapidement qu'elle ne peut couper qu'au plus trois des quatre régions déterminées par deux droites.



Donc $L_3 = 4 + 3 = 7$ est ce qu'on peut faire de mieux.

Avec un peu de réflexion on arrive à la généralisation appropriée. La $n^{\text{ième}}$ droite ($n > 0$) augmente le nombre de régions par k si, et seulement si, elle rencontre k des anciennes régions ou, d'une façon équivalente, si elle rencontre $k - 1$ des anciennes droites en $k - 1$ points différents. Mais la $n^{\text{ième}}$ droite rencontre au plus les $n - 1$ anciennes droites en $n - 1$ points différents donc elle augmente le nombre de régions d'au plus n. Nous avons alors

prouvé que:

$$L_n \leq L_{n-1} + n, \qquad \text{pour } n > 0.$$

D'autre part, il est facile de voir, par récurrence, que l'on a égalité dans cette formule. Si l'on a une disposition de $n-1$ droites dans le plan, découpant ce plan en L_{n-1} régions, alors il suffit de positionner la $n^{\text{ième}}$ droite de telle manière qu'elle ne soit parallèle à aucune des anciennes droites, et qu'elle ne passe par aucun point d'intersection déjà existant.

La relation de récurrence qui détermine L_n est alors,

$$\begin{aligned} L_0 &= 1; \\ L_n &= L_{n-1} + n, \qquad \text{pour tout } n > 0 \end{aligned} \tag{3}$$

Les valeurs de L_n pour $n \in \{1, 2, 3\}$ vérifient cette relation.

Cherchons à résoudre cette récurrence. Pour cela nous utilisons l'idée suivante:

$$\begin{aligned} L_n - L_0 &= (L_n - L_{n-1}) + (L_{n-1} - L_{n-2}) + \cdots + (L_2 - L_1) + (L_1 - L_0) \\ &= n + (n-1) + \cdots + 2 + 1 \\ &= S_n \end{aligned}$$

Pour calculer la somme S_n, on peut utiliser une astuce, (qu'on rapporte qu'elle est due à Gauss en 1786 lorsqu'il avait neuf ans):

$$\begin{array}{rcccccccccccc} S_n & = & 1 & + & 2 & + & 3 & + & \cdots & + & (n-1) & + & n \\ +S_n & = & n & + & (n-1) & + & (n-2) & + & \cdots & + & 2 & + & 1 \\ \hline 2S_n & = & (n+1) & + & (n+1) & + & (n+1) & + & \cdots & + & (n+1) & + & (n+1) \end{array}$$

D'où en simplifiant: $S_n = \dfrac{n(n+1)}{2}$ pour tout $n \geq 0$, et la solution de notre problème est

$$L_n = \frac{n(n+1)}{2} + 1, \qquad \text{pour tout } n \geq 0.$$

Manipulation de sommes

Nous allons commencer par introduire quelques notations.

Dans le chapitre précédent, nous avons rencontré la somme des n premiers entiers naturels non nuls, et nous avons écrit $1 + 2 + \cdots + (n-1) + n$. Les '$\cdots$' dans la formule précédente nous disent de compléter cette somme par les *termes* manquant que nous devons connaître en regardant les termes apparaissant dans la formule. Cette notation est un peu ambigue, si, par exemple, l'on écrit

$$1 + 2 + \cdots + 2^{n-1}$$

alors cela peut désigner, soit la somme des entiers naturels non nuls entre 1 et 2^{n-1} qui comporte 2^{n-1} termes, soit, en notant que $2^0 = 1$, la somme des puissances de 2 qui sont inférieures ou égales à 2^{n-1} qui comporte n termes seulement.

C'est pour cela qu'on a recours à d'autres notations ; par exemple, la *notation* '$\sum$' ; on écrit, alors

$$\sum_{k=1}^{n} a_k \tag{1}$$

pour désigner la somme des termes de la suite finie $(a_k)_{1\leq k\leq n}$. C'est Joseph Fourier qui a introduit cette notation en 1820 et elle a, tout de suite, eu un succès très grand dans le monde des Mathématiques.

La variable k dans (1), (appelée aussi *indice*), est dite *muette*, car on peut la remplacer par n'importe quelle autre variable sans changer la valeur de la somme.

On peut aussi utiliser la *notation* '$\sum$' *généralisée* qui consiste à écrire sous le signe '$\sum$' une ou plusieurs conditions pour préciser l'ensemble des indices sur lesquels s'étend la somme. La somme (1) s'écrit, alors

$$\sum_{1\leq k\leq n} a_k \tag{2}$$

dans cet exemple il n'y a pas de grande différence entre la nouvelle forme et (1), mais la nouvelle forme nous permet de prendre des sommes sur des ensembles d'indices qui ne sont

pas des entiers naturels consécutifs. Par exemple, on peut exprimer la somme des carrés d'entiers naturels impairs et inférieurs à 50, en écrivant: $\sum_{\substack{1\leq k<50\\ k \text{ impair}}} k^2$,

ceci est équivalent à l'écriture plus compliquée suivante: $\sum_{k=0}^{24}(2k+1)^2$.

Un autre exemple est la somme des inverses de tous les nombres premiers entre 1 et N:

$$\sum_{\substack{p\leq N\\ p \text{ premier}}} \frac{1}{p},$$

si l'on veut écrire cette somme en utilisant la notation '$\sum$', on doit écrire:

$$\sum_{k=1}^{\pi(N)} \frac{1}{p_k},$$

où p_k désigne le $k^{\text{ième}}$ nombre premier et $\pi(N)$ est le nombre des nombres premiers $\leq N$.

Nous savons maintenant exprimer une somme, mais comment peut-on trouver la valeur d'une somme ? Nous allons présenter différentes téchniques sur quelques exemples.

1. La famille $\sum_{k=1}^{n} k^\alpha$, pour $\alpha \in \mathbb{N}$.

Notons $S_n^{(\alpha)} = \sum_{k=1}^{n} k^\alpha$. Il est immédiat que $S_n^{(0)} = n$ pour tout $n \geq 1$, et on a trouvé au chapitre précédent que $S_n^{(1)} = \frac{n(n+1)}{2}$. Considérons alors le cas $\alpha = 2$, Nous allons présenter trois méthodes pour calculer $S_n^{(2)} = \sum_{k=1}^{n} k^2$.

– **Première Méthode :** l'idée clé de cette méthode réside dans l'observation: $k = S_k^{(1)} - S_{k-1}^{(1)}$. Si l'on suppose, par convention, que $S_0^{(1)} = 0$ alors pour tout $k \geq 1$ on a $k^2 = k(S_k^{(1)} - S_{k-1}^{(1)})$. D'où

$$\begin{aligned}
S_n^{(2)} =& \sum_{k=1}^{n} k(S_k^{(1)} - S_{k-1}^{(1)}) \\
=& \sum_{k=1}^{n} kS_k^{(1)} - \sum_{k=1}^{n} kS_{k-1}^{(1)} \\
=& \sum_{k=1}^{n} kS_k^{(1)} - \sum_{k=1}^{n-1} (k+1)S_k^{(1)} \\
=& \sum_{k=1}^{n} kS_k^{(1)} - \sum_{k=1}^{n} (k+1)S_k^{(1)} + (n+1)S_n^{(1)} \\
=& \sum_{k=1}^{n} [k-(k+1)]S_k^{(1)} + (n+1)S_n^{(1)} \\
=& (n+1)S_n^{(1)} - \sum_{k=1}^{n} S_k^{(1)} \\
=& (n+1)S_n^{(1)} - \frac{1}{2}\sum_{k=1}^{n} k^2 + k \\
=& (n+1)S_n^{(1)} - \frac{1}{2}(S_n^{(2)} + S_n^{(1)}) \\
=& (n+\frac{1}{2})S_n^{(1)} - \frac{1}{2}S_n^{(2)}
\end{aligned}$$

Par conséquent, $S_n^{(2)} = \frac{2}{3}(n+\frac{1}{2})S_n^{(1)}$, d'où

$$S_n^{(2)} = \frac{n(n+1/2)(n+1)}{3}. \tag{3}$$

Cette méthode est à rapprocher de l'intégration par parties.

– **Deuxième Méthode :** Cette méthode suppose que l'on connaisse le résultat (2) et alors on démontre la validité de (2) par récurrence sur n. On vérifie que (2) est valable pour $n = 1$, et si (2) est valable pour $n-1$, alors

$$\begin{aligned}
S_n^{(2)} =& S_{n-1}^{(2)} + n^2 \\
=& \frac{1}{6}(n-1)n(2n-1) + n^2 \\
=& \frac{n}{6}\left(2n^2 - 3n + 1 + 6n\right) \\
=& \frac{n(n+1)(2n+1)}{6}.
\end{aligned}$$

Donc (2) est aussi valable pour n.

– **Troisième Méthode :** Cette méthode est basée sur la remarque suivante:

$$\frac{1}{3}\left((k+1)^3-k^3\right)=k^2+k+\frac{1}{3},\quad \text{pour } k\geq 1.$$

Alors, en prenant la somme de ces égalités pour k entre 1 et n, on trouve:

$$\begin{aligned}\frac{1}{3}\left((n+1)^3-1\right)=&\frac{1}{3}\sum_{k=1}^{n}\left((k+1)^3-k^3\right)\\ =&\sum_{k=1}^{n}k^2+k+\frac{1}{3}\\ =&S_n^{(2)}+S_n^{(1)}+\frac{1}{3}S_n^{(0)}\end{aligned}$$

Par conséquent,

$$\begin{aligned}S_n^{(2)}=&\frac{n^3+3n^2+3n}{3}-\frac{n^2+n}{2}-\frac{n}{3}\\ =&\frac{n(n+1)(2n+1)}{6}\end{aligned}$$

Passons au cas $\alpha=3$. Les trois méthodes présentées donnent le résultat voulu, nous laissons au lecteur le soin de faire les calculs nécessaires. Mais voici une approche différente qui nous permet de manipuler des "sommes doubles":

Notons

$$S=\sum_{\substack{1\leq i\leq n\\ 1\leq j\leq n}} ij.$$

D'une part, on peut écrire

$$\begin{aligned}S=\sum_{i=1}^{n}\sum_{j=1}^{n}ij=&\sum_{i=1}^{n}i\left(\sum_{j=1}^{n}j\right)\\ =&\sum_{i=1}^{n}iS_n^{(1)}\\ =&(S_n^{(1)})^2.\end{aligned}$$

D'autre part, en notant que les ensembles: $\{(i,i):1\leq i\leq n\}$, $\{(i,j):1\leq i<j\leq n\}$, et $\{(i,j):1\leq j<i\leq n\}$ forment une partition de l'ensemble des indices, on peut écrire

$$\begin{aligned}
S &= \sum_{i=1}^{n} i^2 + \sum_{1\le i<j\le n} ij + \sum_{1\le j<i\le n} ij \\
&= \sum_{i=1}^{n} i^2 + 2\sum_{1\le i<j\le n} ij \\
&= \sum_{i=1}^{n} i^2 + 2\sum_{j=2}^{n} j\left(\sum_{i=1}^{j-1} i\right) \\
&= \sum_{i=1}^{n} i^2 + 2\sum_{j=2}^{n} j\left(\frac{j(j-1)}{2}\right) \\
&= \sum_{i=1}^{n} i^2 + \sum_{j=1}^{n}(j^3 - j^2) \\
&= \sum_{j=1}^{n} j^3 = S_n^{(3)}.
\end{aligned}$$

On conclut que $S_n^{(3)} = (S_n^{(1)})^2$, soit

$$S_n^{(3)} = \frac{n^2(n+1)^2}{4}.$$

Quelles observations peut-on faire ? Pour $\alpha \in \{0,1,2,3\}$, la quantité $(\alpha+1)S_n^{(\alpha)}$ est égale à $P_{\alpha+1}(n)$ où $P_{\alpha+1}(X)$ est une fonction polynômiale de degré $\alpha+1$, qui s'annule en 0, dont le terme du plus haut degré est $X^{\alpha+1}$, et qui vérifie, pour tout $n \ge 1$, $P_{\alpha+1}(n) - P_{\alpha+1}(n-1) = (\alpha+1)n^\alpha$.

La remarque précédente ne serait-elle pas vraie pour tout $\alpha \in \mathbb{N}$? Si, et nous allons voir cela par récurrence sur α.

Nous allons utiliser la troisième méthode, d'après le développement du binôme de Newton, on a:

$$(k+1)^{\alpha+1} - k^{\alpha+1} = \sum_{\beta=0}^{\alpha} C_{\alpha+1}^{\beta} k^\beta.$$

D'où, en prenant la somme de ces égalités pour k variant entre 1 et n, on trouve

$$(n+1)^{\alpha+1} - 1 = \sum_{\beta=0}^{\alpha} C_{\alpha+1}^{\beta} S_n^{(\beta)}.$$

ou bien

$$(n+1)^{\alpha+1} - 1 = \sum_{\beta=0}^{\alpha-1} \frac{1}{1+\beta} C_{\alpha+1}^{\beta} P_{\beta+1}(n) + (\alpha+1)S_n^{(\alpha)}.$$

Cette égalité nous permet de calculer $(\alpha+1)S_n^{(\alpha)}$ à partir de $P_1(n)$,...,$P_\alpha(n)$:

$$\begin{aligned}(\alpha+1)S_n^{(\alpha)} =&(n+1)^{\alpha+1}-1-\sum_{\beta=0}^{\alpha-1}\frac{1}{1+\beta}C_{\alpha+1}^{\beta}P_{\beta+1}(n)\\ =&(n+1)^{\alpha+1}-1-\frac{1}{\alpha+2}\sum_{\beta=0}^{\alpha-1}C_{\alpha+2}^{\beta+1}P_{\beta+1}(n)\\ =&(n+1)^{\alpha+1}-1-\frac{1}{\alpha+2}\sum_{\beta=1}^{\alpha}C_{\alpha+2}^{\beta}P_{\beta}(n).\end{aligned}$$

où pour l'avant dernière égalité on a utilisé le fait simple suivant $\frac{1}{k+1}C_n^k=\frac{1}{n+1}C_{n+1}^{k+1}$.

Si l'on définit la fonction polynômiale $P_{\alpha+1}(X)$ à partir des fonctions $P_1(X)$,...,et $P_\alpha(X)$ par

$$P_{\alpha+1}(X)=(X+1)^{\alpha+1}-1-\frac{1}{\alpha+2}\sum_{\beta=1}^{\alpha}C_{\alpha+2}^{\beta}P_{\beta}(X).$$

Alors $P_{\alpha+1}$ est bien une fonction polynômiale de degré $\alpha+1$, de terme du plus haut degré égal à $X^{\alpha+1}$, s'annulant en 0, et $P_{\alpha+1}(n)=(\alpha+1)S_n^{(\alpha)}$.

Récapitulons, si l'on définit par récurrence la suite de fonctions polynômiales $(P_\alpha)_{\alpha\geq 1}$ par

$$\begin{cases}P_1(X)=&X;\\ P_\alpha(X)=&(X+1)^{\alpha}-1-\frac{1}{\alpha+1}\sum_{\beta=1}^{\alpha-1}C_{\alpha+1}^{\beta}P_{\beta}(X).\end{cases}\tag{4}$$

Alors, pour tout $n\geq 1$ et tout $\alpha\geq 0$ on a $P_{\alpha+1}(n)=(\alpha+1)S_n^{(\alpha)}$. De plus pour chaque α, la fonction polynômiale P_α est de degré α, de terme de plus haut degré égal à X^α et s'annule en 0.

Etudions les fonctions polynômiales $(P_\alpha)_{\alpha\geq 1}$.

Si l'on pose, pour $\alpha\geq 1$, $Q_\alpha(x)=P_\alpha(x)-P_\alpha(x-1)-\alpha x^{\alpha-1}$ alors c'est une fonction polynômiale qui vérifie

$$Q_\alpha(n)=\alpha(S_n^{(\alpha-1)}-S_{n-1}^{(\alpha-1)}-n^{\alpha-1})=0,\quad \text{pour } n\geq 1.$$

Donc c'est une fonction polynômiale qui admet une infinité de zéros, elle est, par conséquent, très malhonnête pour ne pas être identiquement nulle. d'où

$$\begin{cases}\forall\, x\in\mathbb{R}, & P_\alpha(x)-P_\alpha(x-1)=\alpha x^{\alpha-1};\\ & P_\alpha(0)=0.\end{cases}\tag{5}$$

Les conditions précédentes déterminent uniquement la fonction polynômiale P_α. En effet, si Q est une fonction polynômiale vérifiant les conditions de (5) alors

$$\forall\, x \in \mathbb{R}, \quad Q(x) - Q(x-1) = P_\alpha(x) - P_\alpha(x-1).$$

On en déduit que

$$\forall\, n \in \mathbb{N}^*, \quad Q(n) - P_\alpha(n) = Q(n-1) - P_\alpha(n-1) = \cdots = Q(0) - P_\alpha(0) = 0.$$

Par conséquent, la fonction polynômiale $Q - P_\alpha$ admet une infinité de zéros, elle est donc identiquement nulle et $Q = P_\alpha$.

L'idée gagnante à ce stade est de dériver les deux membres de la première égalité de (5) : $P_{\alpha+1}(x) - P_{\alpha+1}(x-1) = (\alpha+1)x^\alpha$ lorsque $\alpha \geq 1$. On obtient

$$\forall\, x \in \mathbb{R}, \quad \frac{1}{\alpha+1}\left(P'_{\alpha+1}(x) - P'_{\alpha+1}(x-1)\right) = \alpha x^{\alpha-1}$$

Par conséquent si $Q_\alpha(x) = \dfrac{1}{\alpha+1}\left(P'_{\alpha+1}(x) - P'_{\alpha+1}(0)\right)$, alors

$$\begin{cases} \forall\, x \in \mathbb{R}, & Q_\alpha(x) - Q_\alpha(x-1) = \alpha x^{\alpha-1}; \\ & Q_\alpha(0) = 0. \end{cases}$$

L'unicité de la fonction polynômiale P_α vérifiant (5) montre que $Q_\alpha = P_\alpha$, Alors

$$P_\alpha(x) = \frac{1}{\alpha+1}\left(P'_{\alpha+1}(x) - P'_{\alpha+1}(0)\right)$$

En intégrant les deux membres de cette formule entre 0 et x, on trouve

$$(1+\alpha)\int_0^x P_\alpha(t)\,dt = P_{\alpha+1}(x) - P_{\alpha+1}(0) - xP'_{\alpha+1}(0).$$

En remplaçant $x = -1$, et en remarquant d'après (5) que $P_{\alpha+1}(0) - P_{\alpha+1}(-1) = 0$, on trouve

$$(1+\alpha)\int_0^{-1} P_\alpha(t)\,dt = P'_{\alpha+1}(0).$$

ce qui donne la nouvelle formule suivante

$$\forall\, x \in \mathbb{R}, \quad P_{\alpha+1}(x) = (1+\alpha)\left(x\int_0^{-1} P_\alpha(t)\,dt + \int_0^x P_\alpha(t)\,dt\right). \tag{5}$$

Inversement, si P_α vérifie (5), et si $P_{\alpha+1}$ est définie par la relation (5) alors $P_{\alpha+1}$ vérifie aussi (5). En effet, clairement $P_{\alpha+1}(0) = 0$, et

$$\begin{aligned}
P_{\alpha+1}(x) - P_{\alpha+1}(x-1) =& (\alpha+1)\left(\int_0^{-1} P_\alpha(t)\,dt + \int_{x-1}^{x} P_\alpha(t)\,dt\right)\\
=& (\alpha+1)\left(\int_0^{-1} P_\alpha(t)\,dt + \int_0^{x} P_\alpha(t)\,dt - \int_0^{x-1} P_\alpha(t)\,dt\right)\\
=& (\alpha+1)\left(\int_0^{x} P_\alpha(t)\,dt - \int_{-1}^{x-1} P_\alpha(t)\,dt\right)\\
=& (\alpha+1)\left(\int_0^{x} P_\alpha(t)\,dt - \int_0^{x} P_\alpha(t-1)\,dt\right)\\
=& (\alpha+1)\int_0^{x} \left(P_\alpha(t) - P_\alpha(t-1)\right)\,dt\\
=& (\alpha+1)\int_0^{x} \alpha t^{\alpha-1}\,dt = (\alpha+1)x^\alpha.
\end{aligned}$$

En guise de conclusion, si l'on définit la suite de fonctions polynômiales $(P_\alpha)_{\alpha\geq 1}$ par

$$\begin{cases}
\forall\, x \in \mathbb{R}, \quad P_1(x) = x;\\
\qquad\qquad P_{\alpha+1}(x) = (1+\alpha)\left(x\displaystyle\int_0^{-1} P_\alpha(t)\,dt + \int_0^{x} P_\alpha(t)\,dt\right), \quad (\alpha \geq 1)
\end{cases}$$

Alors, pour tout $\alpha \geq 0$ et tout $n \geq 1$ on a

$$\sum_{k=1}^{n} k^\alpha = \frac{P_{\alpha+1}(n)}{\alpha+1}.$$

De plus P_α est une fonction polynômiale de degré α, de terme de plus haut degré égal à X^α, et telle que $x(x+1)$ divise P_α pour tout $\alpha \geq 2$. (C'est parce que $P_\alpha(0) = P_\alpha(-1) = 0$).

Il est à ce stade important de retrouver nos résultats en déterminant les P_α pour les premières valeurs de α. Une tâche que nous laissons au lecteur.

2. Les nombres harmoniques

Il s'agit des nombres, que nous allons noter H_n, définis par

$$H_n = \sum_{k=1}^{n} \frac{1}{k}.$$

Cette fois nous n'avons pas la possibilité d'exprimer plus facilement H_n comme fonction de n, et ce n'est pas notre but. Nous nous proposons d'abord de simplifier des sommes faisant intervenir les nombres harmoniques, et ensuite d'étudier ces nombres pour les grandes valeurs de n. Par commodité nous posons par convention $H_0 = 0$.

1°. $\sum_{k=1}^{n} H_k$.

Pour simplifier cette somme nous allons utiliser une méthode qui ressemble à la première méthode exposée dans l'étude précédente. On remarque que $1 = k - (k-1)$, d'où:

$$\begin{aligned}\sum_{k=1}^{n} H_k &= \sum_{k=1}^{n} (k-(k-1))H_k \\ &= \sum_{k=1}^{n} kH_k - \sum_{k=1}^{n} (k-1)H_k \\ &= \sum_{k=1}^{n} kH_k - \sum_{k=1}^{n-1} kH_{k+1} \\ &= \sum_{k=1}^{n} kH_k - \sum_{k=1}^{n} kH_{k+1} + nH_{n+1}\end{aligned}$$

et en combinant de nouveau les deux sommes:

$$\begin{aligned}\sum_{k=1}^{n} H_k =& nH_{n+1} - \sum_{k=1}^{n} k(H_{k+1} - H_k) \\ =& nH_{n+1} - \sum_{k=1}^{n} \frac{k}{k+1} \\ =& nH_{n+1} - \sum_{k=1}^{n} 1 + \sum_{k=1}^{n} \frac{1}{k+1} \\ =& nH_{n+1} - n + H_{n+1} - 1 \\ =& (n+1)(H_{n+1} - 1) \\ =& (n+1)H_n - n\end{aligned}$$

Alors,

$$\sum_{k=1}^{n} H_k = (n+1)(H_{n+1} - 1) = (n+1)H_n - n. \tag{6}$$

2°. $\sum_{k=1}^{n} (2k+1)H_k$.

Nous allons utiliser la même méthode. On remarque que $(2k+1) = (k+1)^2 - k^2$, d'où:

$$\begin{aligned}
\sum_{k=1}^{n}(2k+1)H_k =& \sum_{k=1}^{n}((k+1)^2-k^2)H_k \\
=& \sum_{k=1}^{n}(k+1)^2H_k - \sum_{k=1}^{n}k^2H_k \\
=& \sum_{k=2}^{n+1}k^2H_{k-1} - \sum_{k=1}^{n}k^2H_k \\
=&(n+1)^2H_n - 1 + \sum_{k=2}^{n}k^2H_{k-1} - \sum_{k=2}^{n}k^2H_k \\
=&(n+1)^2H_n - 1 - \sum_{k=2}^{n}k^2(H_k - H_{k-1}) \\
=&(n+1)^2H_n - \sum_{k=1}^{n}k \\
=&(n+1)^2H_n - \frac{n(n+1)}{2}
\end{aligned}$$

Alors,

$$\sum_{k=1}^{n}(2k+1)H_k = (n+1)^2H_n - \frac{n(n+1)}{2}. \tag{7}$$

Les deux calculs précédents nous permettent de trouver

$$\sum_{k=1}^{n}kH_k = \frac{n(n+1)}{2}\left(H_{n+1} - \frac{1}{2}\right) = \frac{n(n+1)}{2}H_n - \frac{n(n-1)}{4}. \tag{8}$$

On remarque que dans les deux cas nous avons utilisé presque les mêmes transformations, ce qu'on peut formuler de la manière suivante: Si $(A_k)_{k\geq 1}$ est une suite de réels alors

$$\begin{aligned}
\sum_{k=1}^{n}(A_{k+1}-A_k)H_k =& \sum_{k=1}^{n}A_{k+1}H_k - \sum_{k=1}^{n}A_kH_k \\
=& \sum_{k=2}^{n+1}A_kH_{k-1} - \sum_{k=1}^{n}A_kH_k \\
=&A_{n+1}H_n - A_1 + \sum_{k=2}^{n}A_kH_{k-1} - \sum_{k=2}^{n}A_kH_k \\
=&A_{n+1}H_n - A_1 - \sum_{k=2}^{n}A_k(H_k - H_{k-1}) \\
=&A_{n+1}H_n - \sum_{k=1}^{n}\frac{A_k}{k}
\end{aligned}$$

Soit, en récapitulant,

$$\sum_{k=1}^{n}(A_{k+1}-A_k)H_k = A_{n+1}H_n - \sum_{k=1}^{n}\frac{A_k}{k}. \tag{9}$$

Cette transformation qui ressemble à l'intégration par parties pour les intégrales s'appelle *Transformation d'Abel*.

3°. $\displaystyle\sum_{k=1}^{n} H_k^2$.

Nous allons utiliser la transformation d'Abel, En prenant pour A_k la somme $\displaystyle\sum_{j=1}^{k-1} H_j$ qui est égale d'après (6) à $k(H_k-1)$. On trouve

$$\begin{aligned}\sum_{k=1}^{n} H_k^2 =& A_{n+1}H_n - \sum_{k=1}^{n}(H_k-1)\\ =&(n+1)H_n^2 - nH_n - ((n+1)H_n - n) + n\\ =&(n+1)H_n^2 - (2n+1)H_n + 2n.\end{aligned}$$

D'où

$$\sum_{k=1}^{n} H_k^2 = (n+1)H_n^2 - (2n+1)H_n + 2n. \tag{10}$$

4°. $\displaystyle\sum_{k=1}^{n}\frac{H_k}{(k+1)(k+2)}$.

Cet exemple n'est pas plus difficile que le précédent, il suffit de trouver le bon $(A_k)_{k\geq 1}$, Or il est facile de voir que $\dfrac{1}{k+1}-\dfrac{1}{k+2} = \dfrac{1}{(k+1)(k+2)}$. Alors si l'on pose $A_k = 1/(k+1)$ dans la formule (9) on trouve

$$\begin{aligned}\sum_{k=1}^{n} -\frac{H_k}{(k+1)(k+2)} =& \frac{H_n}{n+2} - \sum_{k=1}^{n}\frac{1}{k(k+1)}\\ =&\frac{H_n}{n+2} - \sum_{k=1}^{n}\left(\frac{1}{k}-\frac{1}{k+1}\right)\\ =&\frac{H_n}{n+2} - 1 + \frac{1}{n+1}.\end{aligned}$$

D'où

$$\sum_{k=1}^{n}\frac{H_k}{(k+1)(k+2)} = 1 - \frac{H_n}{n+2} - \frac{1}{n+1}. \tag{11}$$

5°. $\displaystyle\sum_{1\leq i,j\leq n}\frac{1}{i+j}$.

Nous allons traiter cette somme de deux manières. Premièrement, on peut écrire:

$$\begin{aligned}\sum_{1\leq i,j\leq n}\frac{1}{i+j} &= \sum_{i=1}^{n}\left(\sum_{j=1}^{n}\frac{1}{i+j}\right)\\ &= \sum_{i=1}^{n}\left(\sum_{k=i+1}^{n+i}\frac{1}{k}\right)\\ &= \sum_{i=1}^{n}(H_{n+i}-H_i)\\ &= \sum_{i=1}^{n}H_{n+i}-\sum_{k=1}^{n}H_k\\ &= \sum_{k=n+1}^{2n}H_k-\sum_{k=1}^{n}H_k\\ &= \sum_{k=1}^{2n}H_k-2\sum_{k=1}^{n}H_k\end{aligned}$$

$$\begin{aligned}\sum_{1\leq i,j\leq n}\frac{1}{i+j} &= (2n+1)H_{2n}-2n-2((n+1)H_n-n)\\ &= (2n+1)H_{2n}-2(n+1)H_n.\end{aligned}$$

D'où

$$\sum_{1\leq i,j\leq n}\frac{1}{i+j}=(2n+1)H_{2n}-2(n+1)H_n. \tag{12}$$

Deuxièmement, notons d'abord que $i+j$ parcourt l'ensemble $\{2,3,\ldots,2n\}$ lorsque (i,j) parcourt l'ensemble $\mathcal{A}=\{1,\ldots,n\}\times\{1,\ldots,n\}$. D'autre part, pour chaque $k\in\{2,3,\ldots,2n\}$ l'ensemble $\mathcal{A}_k$ des couples $(i,j)\in\mathcal{A}$ qui vérifient $i+j=k$ contient $k-1$ éléments si $k\leq n+1$, et $2n-k+1$ éléments si $n+1<k\leq 2n$, ce qu'on peut résumer en écrivant

$$\text{Card }(A_k)=\begin{cases}k-1 & \text{si} \quad k\leq n+1\\ 2n+1-k & \text{si} \quad n+1<k\leq 2n\end{cases}$$

Les ensembles $(\mathcal{A}_k)_{2\leq k\leq 2n}$ forment une partition de $\mathcal{A}$. Alors

$$\begin{aligned}\sum_{1\leq i,j\leq n}\frac{1}{i+j}=&\sum_{k=2}^{2n}\frac{1}{k}\ \text{Card}\ (A_k)\\ =&\sum_{k=2}^{n+1}\frac{k-1}{k}+\sum_{k=n+2}^{2n}\frac{2n+1-k}{k}\\ =&n-\sum_{k=2}^{n+1}\frac{1}{k}-(n-1)+(2n+1)\sum_{k=n+2}^{2n}\frac{1}{k}\\ =&1-(H_{n+1}-1)+(2n+1)(H_{2n}-H_{n+1})\\ =&(2n+1)H_{2n}-2(n+1)H_{n+1}+2\\ =&(2n+1)H_{2n}-2(n+1)H_n.\end{aligned}$$

Et on retrouve le résultat.

Voici une variante du calcul précédent.

6°. $\displaystyle\sum_{1\leq i,j\leq n}\frac{1}{i+j-1}$. Nous allons ramener ce calcul au cas précédent.

$$\begin{aligned}\sum_{1\leq i,j\leq n}\frac{1}{i+j-1}=&\sum_{\substack{2\leq i\leq n\\1\leq j\leq n}}\frac{1}{i+j-1}+\sum_{j=1}^{n}\frac{1}{j}\\ =&\sum_{\substack{1\leq i\leq n-1\\1\leq j\leq n}}\frac{1}{i+j}+\sum_{j=1}^{n}\frac{1}{j}\\ =&\sum_{\substack{1\leq i\leq n-1\\1\leq j\leq n-1}}\frac{1}{i+j}+\sum_{j=1}^{n}\frac{1}{j}+\sum_{i=1}^{n-1}\frac{1}{i+n}\\ =&\sum_{1\leq i,j\leq n-1}\frac{1}{i+j}+\sum_{k=1}^{2n-1}\frac{1}{k}\\ =&(2n-1)H_{2n-2}-2nH_{n-1}+H_{2n-1}\\ =&2n(H_{2n}-H_n).\end{aligned}$$

D'où

$$\sum_{1\leq i,j\leq n}\frac{1}{i+j-1}=2n(H_{2n}-H_n). \tag{13}$$

7°. **Les nombres harmoniques pour les grandes valeurs de n.**

Nous allons maintenant étudier le comportement de H_n lorsque n est au voisinage de l'infini. Ceci va nous permettre d'introduire une nouvelle technique ; l'utilisation des intégrales.

Notons que pour tout $x \in [k, k+1]$ on a $\dfrac{1}{k+1} \leq \dfrac{1}{x} \leq \dfrac{1}{k}$, donc en intégrant cette inégalité sur l'intervalle $[k, k+1]$ on trouve

$$\frac{1}{k+1} = \int_k^{k+1} \frac{dx}{k+1} \leq \int_k^{k+1} \frac{dx}{x} \leq \int_k^{k+1} \frac{dx}{k} = \frac{1}{k}.$$

Comme cette inégalité est valable pour tout $k \in \mathbb{N}^*$ alors en prenant la somme de ces inégalités pour k entre 1 et n on trouve

$$\sum_{k=2}^{n+1} \frac{1}{k} \leq \int_1^{n+1} \frac{dx}{x} \leq \sum_{k=1}^{n} \frac{1}{k}.$$

ce qui s'ecrit

$$H_{n+1} - 1 \leq \operatorname{Log}(n+1) \leq H_n.$$

ou bien

$$\forall\, n \in \mathbb{N}^*, \quad \operatorname{Log}(n+1) \leq H_n \leq 1 + \operatorname{Log} n. \tag{14}$$

Le résultat précédent nous dit que H_n diverge vers l'infini lorsque n croit indéfiniment, et nous donne une idée de l'ordre de grandeur de H_n, Par exemple, $H_{1000000} \in [13.81, 14.82]$. Peut-on faire mieux ? Les formules de (14) nous suggèrent d'étudier les différences $A_n = H_n - \operatorname{Log} n$ et $B_n = H_n - \operatorname{Log}(n+1)$. Clairement, pour tout $n \geq 1$, on a $0 \leq B_n \leq A_n$.

Voyons si les suites $(A_n)_n$ et $(B_n)_n$ sont monotones.

$$\begin{aligned} B_n - B_{n-1} &= \frac{1}{n} - \operatorname{Log}\left(1 + \frac{1}{n}\right). \\ A_n - A_{n-1} &= \frac{1}{n} + \operatorname{Log}\left(1 - \frac{1}{n}\right). \end{aligned} \tag{15}$$

Il est maintenant clair que la fonction $f(x) = x - \operatorname{Log}(1+x)$ joue un rôle dans l'histoire, alors ouvrons une paranthèse et étudions cette fonction:

{

f est définie sur $]-1, +\infty[$. La dérivée de f est donnée par $f'(x) = \dfrac{x}{1+x}$, ce qui donne le tableau de variation suivant:

x	-1		0		$+\infty$
$f'(x)$		$-$	0	$+$	
$f(x)$	$+\infty$	$\searrow$	0	$\nearrow$	$+\infty$

On en déduit que

$$\begin{aligned} \forall\, x \in]0,1[, \quad & x + \operatorname{Log}(1-x) < 0; \\ & x - \operatorname{Log}(1+x) > 0. \end{aligned} \tag{16}$$

}

L'étude précédente montre, avec (15) que

$$\forall\, n > 1, \quad B_{n-1} < B_n < A_n < A_{n-1} \tag{17}$$

D'autre part, il est clair que $A_n - B_n = \mathrm{Log}\,(1 + 1/n)$ tend vers 0 lorsque n tend vers l'infini. Les deux suites $(A_n)_n$ et $(B_n)_n$ sont alors dites *adjacentes*, et elles sont convergentes vers une limite commune que nous allons noter γ. γ s'appelle la *constante d'Euler*.

$$\forall\, n \in \mathbb{N}^*, \quad B_n < \gamma < A_n. \tag{18}$$

En particulier si l'on met $n = 3$ on obtient l'encadrement $\gamma \in [0.45, 0.74]$.

On peut écrire (18) sous la forme

$$0 < H_n - \mathrm{Log}\, n - \gamma < \mathrm{Log}\,(1 + \frac{1}{n}) < \frac{1}{n}. \tag{19}$$

Voici une valeur approchée, à 10^{-40} près, de γ:

$$\gamma = 0.57721\ 56649\ 01532\ 86060\ 65120\ 90082\ 40243\ 10422\ldots!$$

On ne sait pas si ce nombre mystérieux est rationnel ou irrationnel.

En utilisant la valeur approchée de γ et la formule (19), on peut trouver $H_{1000000}$ à 10^{-6} près: $H_{1000000} = 14.392726$.

EXERCICES

EXERCICE .1 Pour $n \in \mathbb{N}^*$, calculer $\displaystyle\sum_{k=0}^{n}(n-k)^2(-1)^k$.

EXERCICE .2 Pour $n \in \mathbb{N}^*$, calculer $\displaystyle\sum_{k=0}^{n}(2k+1)$.

EXERCICE .3 Pour $n \in \mathbb{N}^*$, calculer $S = \sum_{\substack{1\leq i\leq n\\ 1\leq j\leq n}} \min(i,j)$.

EXERCICE .4 Pour $n \in \mathbb{N}^*$, calculer $S = \sum_{\substack{1\leq i\leq n\\ 1\leq j\leq n}} i^2+ij+j^2$.

EXERCICE .5 En étudiant, $S = \displaystyle\sum_{\substack{1\leq i\leq n\\ 1\leq j\leq n}} ij^2$, et $\widetilde{S} = \displaystyle\sum_{\substack{1\leq i\leq n\\ 1\leq j\leq n}} i^2j^2$. Montrer les relations:

$$S_n^{(4)} = \frac{1}{5}S_n^{(2)}(6S_n^{(1)}-1), \quad S_n^{(5)} = \frac{1}{2}\left(3(S_n^{(2)})^2 - S_n^{(3)}\right).$$

EXERCICE .6 Exprimer $U_n = \displaystyle\sum_{k=1}^{2n}\frac{(-1)^k}{k}$ en utilisant les nombres harmoniques. En déduire la limite de $(U_n)_n$ lorsque n tend vers l'infini.

EXERCICE .7 Étudier la suite récurrente:

$$T_0 = 5, \quad \text{et} \quad 2T_n = nT_{n-1} + 3\,n!, \qquad \text{pour } n > 0.$$

EXERCICE .8 Étudier la suite récurrente:

$$V_0 = 0, \quad \text{et} \quad V_n = n+1+\frac{2}{n}\sum_{k=0}^{n-1}V_k, \qquad \text{pour } n > 0.$$

EXERCICE .9 Pour tout entier $n \in \mathbb{N}^*$, appelons E_n l'ensemble des points $M(x,y)$ du plan, de coordonnées $(x,y) \in \mathbb{N}_n \times \mathbb{N}_n$. Quel est le nombre de segments MM' qui sont parallèles à la droite d'équation $y = x$ et qui joignent deux points M et M' de E_n ?

EXERCICE .10 Quel est le nombre maximum de régions dans l'espace que l'on peut obtenir en effectuant n coupes planes ?

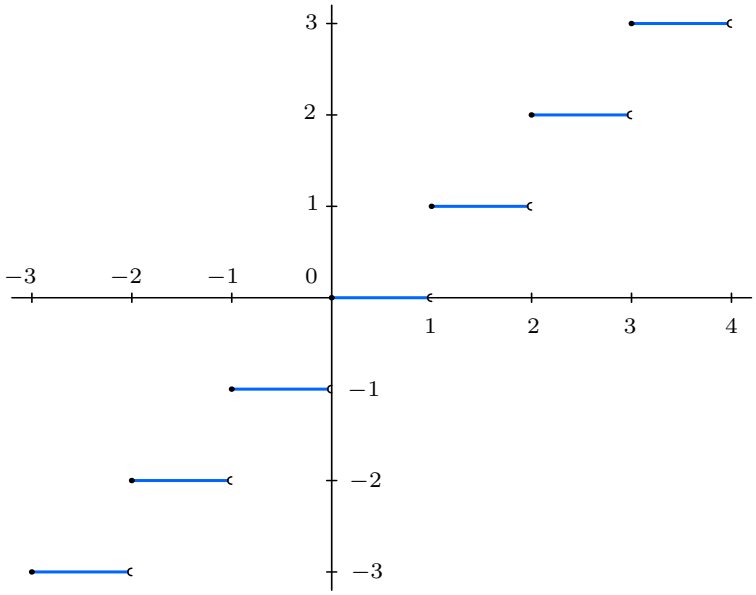
EXERCICE .11 Quel est le nombre maximum de régions dans le plan que l'on peut obtenir en y dessinant n cercles ?

Partie entière

Soit x un nombre réel. On définit la partie entière de x comme le plus grand entier relatif $E(x)$ inférieur ou égal à x.

$$E(x) = \max\{k \in \mathbb{Z} : \ k \leq x\}. \tag{1}$$

Par exemple $E(1.25) = 1$, $E(\pi) = 3$, et $E(-\sqrt{2}) = -2$. Il y a d'autres notations utilisées pour noter la partie entière de x, ce sont $[x]$ et $\lfloor x \rfloor$. Voici le graphe de la fonction $E : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto E(x)$.



Pour un réel x, on utilise la notation $\{x\}$ pour désigner $x - E(x)$, qu'on appelle la partie fractionnaire de x.

Nous allons nous familiariser avec la fonction partie entière en traitant des exemples variés. Notons d'abord quelques propriétés simples:

a. Pour tout $x \in \mathbb{R}$, $-E(-x) = \min\{k \in \mathbb{Z} : \ x \leq k\}$. Dans certains livres on note $\lceil x \rceil = -E(-x)$. On a $E(x) = \lceil x \rceil$ si, et seulement si, x est un entier relatif.

b. Pour tout $x \in \mathbb{R}$ et tout $m \in \mathbb{Z}$, on a $E(m+x) = m + E(x)$.

c. Pour tout $(x, y) \in \mathbb{R}^2$, on a $E(x+y) - E(x) - E(y) \in \{0, 1\}$.

En effet,

$$E(x) \leq x < E(x) + 1,$$
$$E(y) \leq y < E(y) + 1.$$

donc

$$E(x) + E(y) \leq x + y < E(x) + E(y) + 2.$$

alors

$$E(x) + E(y) \leq E(x+y) \leq E(x) + E(y) + 1.$$

d'où le résultat.

Exemples:

1°. Soient $x \in \mathbb{R}$ et $n \in \mathbb{N}^*$. On se propose de simplifier la somme

$$S_n(x) = \sum_{k=0}^{n-1} E\left(x + \frac{k}{n}\right).$$

Reprenons nos vieilles habitudes, et regardons d'abord les cas correspondants à des petites valeurs de n. Si $n = 1$ on a clairement $S_1(x) = E(x)$. Passons au cas $n = 2$.

$$S_2(x) = E(x) + E(x + \frac{1}{2}).$$

On voit que si $\{x\} < 1/2$ alors $E(x + \frac{1}{2}) = E(x)$ et $S_2(x) = 2E(x) = E(2x)$. D'autre part si $\{x\} \geq 1/2$ alors $E(x + \frac{1}{2}) = 1 + E(x)$ et $S_2(x) = 2E(x) + 1 = E(2x)$. Dans tous les cas $S_2(x) = E(2x)$.

Voyons si l'on peut généraliser l'approche précédente pour montrer que $S_n(x) = E(nx)$. Soit $x \in \mathbb{R}$, $\{x\}$ est un élément de $[0, 1[$ donc appartient à un, et un seul, intervalle parmi $\left[\frac{k}{n}, \frac{k+1}{n}\right[$, $(0 \leq k < n)$. Disons $\{x\} \in \left[\frac{q}{n}, \frac{q+1}{n}\right[$, alors

$$E\left(x + \frac{k}{n}\right) = \begin{cases} E(x) & \text{si} \quad 0 \leq k < n - q \\ \\ E(x) + 1 & \text{si} \quad n - q \leq k < n \end{cases}$$

Et $S_n(x) = nE(x) + q$. D'autre part, $\frac{q}{n} \leq x - E(x) < \frac{q+1}{n}$, ce qui donne $E(nx) = nE(x) + q$. Par conséquent $S_n(x) = E(nx)$.

2°. Étudions les sommes

$$S_n = \sum_{k\geq 1} E\left(\frac{n}{2^k}+\frac{1}{2}\right), \qquad T_n = \sum_{k\geq 1} 2^k \left(E\left(\frac{n}{2^k}+\frac{1}{2}\right)\right)^2.$$

Remarquons que les sommes s'étendent sur un nombre fini de termes ; à partir d'un certain $k_0(n)$ la fraction $n/2^k$ est strictement inférieure à $1/2$ et les termes dans les sommes deviennent nuls.

Donnons les premières valeurs de S_n et de T_n.

n	1	2	3	4	5
S_n	1	2	3	4	5
T_n	2	6	12	20	30

Ce tableau suggère les réponses suivantes: $S_n = n$ et $T_n = n(n+1)$. Essayons de les prouver, pour cela nous allons, pour n fixé, étudier $S_n - S_{n-1}$ et $T_n - T_{n-1}$, ces deux différences font intervenir le terme

$$A_k = E\left(\frac{n}{2^k}+\frac{1}{2}\right) - E\left(\frac{n-1}{2^k}+\frac{1}{2}\right).$$

A_k est de la forme $E(x)-E(y)$ avec $0 < x-y < 1$. Alors A_k vaut 0 ou 1. Cherchons les valeurs de k pour lesquelles $A_k = 1$. Notons $p = E\left(\frac{n}{2^k}+\frac{1}{2}\right)$. L'égalité $A_k = 1$ équivaut à

$$\left(\frac{n}{2^k}+\frac{1}{2}\right) \geq p > \left(\frac{n-1}{2^k}+\frac{1}{2}\right).$$

ou bien

$$n + 2^{k-1} \geq p2^k > n + 2^{k-1} - 1.$$

qui est équivalent à $n + 2^{k-1} = 2^k p$, ou bien $n = 2^{k-1}(2p-1)$. Conclusion: $A_k = 1$ si, et seulement si, $k-1$ est la plus grande puissance de 2 qui divise n.

Tout entier naturel n s'écrit d'une manière unique $n = 2^{r-1}(2m-1)$ avec $(r,m) \in \mathbb{N}^* \times \mathbb{N}^*$. La discussion précédente montre que $A_k = 0$ si $k \neq r$ et $A_k = 1$ si $k = r$. Par conséquent

$$S_n - S_{n-1} = \sum_{k\geq 1} A_k = A_r = 1,$$

et

$$\begin{aligned} T_n - T_{n-1} &= \sum_{k\geq 1} 2^k A_k \left(E\left(\frac{n}{2^k}+\frac{1}{2}\right) + E\left(\frac{n-1}{2^k}+\frac{1}{2}\right)\right) \\ &= 2^r \left(E\left(\frac{2m-1}{2}+\frac{1}{2}\right) + E\left(\frac{2m-2}{2}+\frac{1}{2}\right)\right) \\ &= 2^r(2m-1) = 2n. \end{aligned}$$

On a donc prouvé que, pour tout $n \geq 1$,

$$S_n - S_{n-1} = 1, \qquad T_n - T_{n-1} = 2n.$$

ce qui permet aussitôt de voir que $S_n = n$ et $T_n = n(n+1)$.

3°. Etudions cette fois la somme

$$U_m = \sum_{1 \leq k \leq m(m+1)/2} E(\sqrt{2k} + \frac{1}{2}).$$

Pour traiter cette somme nous utiliserons ce qu'on peut appeler "sommation par tranches".

Soit $p \in \mathbb{N}$, on pose $\mathcal{B}_p$ l'ensemble des entiers k tels que $p = E(\sqrt{2k} + 1/2)$. On note $b_p = \text{ Card }(\mathcal{B}_p)$ le nombre des éléments de $\mathcal{B}_p$.

$$\begin{aligned} p = E(\sqrt{2k} + 1/2) \quad &\Longleftrightarrow \quad \sqrt{2k} - \frac{1}{2} < p \leq \sqrt{2k} + \frac{1}{2} \\ &\Longleftrightarrow \quad \left(p - \frac{1}{2}\right)^2 \leq 2k < \left(p + \frac{1}{2}\right)^2 \\ &\Longleftrightarrow \quad \frac{p(p-1)}{2} + \frac{1}{8} \leq k < \frac{p(p+1)}{2} + \frac{1}{8} \\ &\Longleftrightarrow \quad \frac{p(p-1)}{2} < k \leq \frac{p(p+1)}{2}. \end{aligned}$$

La dernière équivalence vient du fait que $p(p-1)/2$ et $p(p+1)/2$ sont des entiers. Par conséquent

$$\mathcal{B}_p = \left]\frac{p(p-1)}{2}, \frac{p(p+1)}{2}\right] \bigcap \mathbb{N}, \quad \text{et} \quad b_p = p.$$

Si f est une fonction de $\mathbb{N}$ dans $\mathbb{R}$ on a

$$\sum_{1 \leq k \leq m(m+1)/2} f(E(\sqrt{2k} + 1/2)) = \sum_{p=1}^{m} f(p) \text{ Card }(\mathcal{B}_p).$$

ou bien

$$\sum_{1 \leq k \leq m(m+1)/2} f(E(\sqrt{2k} + 1/2)) = \sum_{p=1}^{m} p f(p).$$

Dans le cas particulier $f(k) = k$ pour tout $k \in \mathbb{N}$ on trouve

$$U_m = \sum_{p=1}^{m} p^2 = \frac{m(m+1)(2m+1)}{6}.$$

4°. Voici un autre exemple où l'on utilise la même technique. On se propose de calculer

$$V_n = \sum_{k=1}^{n} E(\lg k).$$

où lg désign le logarithm en base 2.

Notons que

$$\begin{aligned} \ell = E(\lg k) &\iff \ell \le \lg k < \ell + 1 \\ &\iff 2^\ell \le k < 2^{\ell+1} \\ &\iff k \in [2^\ell, 2^{\ell+1}[\cap \mathbb{N}. \end{aligned}$$

Alors, si l'on note pour simplifier $m = E(\lg n)$

$$\begin{aligned} V_n = \sum_{k=1}^{n} E(\lg k) &= \sum_{0 \le \ell \le m} \ell \,\mathrm{Card}\,(\{k \le n :\ \ell = E(\lg k)\ \}) \\ &= \sum_{0 \le \ell \le m-1} \ell\,(2^{\ell+1} - 2^\ell) + (n - 2^m + 1)m \\ &= \sum_{0 \le \ell \le m-1} \ell\, 2^{\ell+1} - \sum_{0 \le \ell \le m-1} \ell\, 2^\ell + (n - 2^m + 1)m \\ &= \sum_{1 \le \ell \le m} (\ell - 1)2^\ell - \sum_{1 \le \ell \le m-1} \ell\, 2^\ell + (n - 2^m + 1)m \\ &= m2^m - \sum_{1 \le \ell \le m} 2^\ell + (n - 2^m + 1)m \\ &= (n+1)\, m - 2^{m+1} + 2. \end{aligned}$$

Alors

$$\sum_{k=1}^{n} E(\lg k) = (n+1)\, E(\lg n) - 2^{1+E(\lg n)} + 2.$$

5°. **Le spectre d'un nombre réel.**

Soit α un nombre réel donné, on définit le spectre de α, comme étant la suite $(E(\alpha n))_{n \ge 1}$; on note cette suite $\mathrm{Spec}\,(\alpha)$.

Il est facile de voir que si $\alpha \ne \beta$ alors $\mathrm{Spec}\,(\alpha) \ne \mathrm{Spec}\,(\beta)$. En effet, sans perdre la généralité on peut supposer que $\alpha < \beta$, alors il exite un entier positif m tel que $m(\beta - \alpha) \ge 1$. Alors, $m\beta \ge 1 + m\alpha$ ce qui implique que $E(m\beta) > E(m\alpha)$ d'où le résultat.

Les spectres ont quelques belles propriétés. Par exemple, considérons les deux spectres:

$$\begin{aligned} \mathrm{Spec}\,(\sqrt{2}) &= (1, 2, 4, 5, 7, 8, 9, 11, 12, 14, 15, 16, 18, 19, 21, 22, 24, \ldots), \\ \mathrm{Spec}\,(2 + \sqrt{2}) &= (3, 6, 10, 13, 17, 20, 23, 27, 30, 34, 37, 40, 44, 47, 51, \ldots). \end{aligned}$$

Le calcul de $\text{Spec}\,(\sqrt{2})$ est facile en utilisant une calculatrice de poche (mais pour n n'est pas très grand), et le $\text{Spec}\,(2+\sqrt{2})$ s'en déduit en remarquant que $E((2+\sqrt{2})\,n) = 2n + E(\sqrt{2}\,n)$. Mais un regard plus approfondi sur les deux spectres nous montre que ces deux spectres sont liés d'une façon surprenante: Il semble que tout nombre manquant dans l'un des deux spectres apparaît dans l'autre, mais aucun nombre n'apparaît dans les deux ! En effet, si l'on pose $\mathcal{S}\,(\alpha) = \{E(k\alpha) :\ k \in \mathbb{N}^*\}$, c'est à dire l'ensemble des valeurs prises par le spectre de α, alors les deux ensembles $\mathcal{S}\,(\sqrt{2})$ et $\mathcal{S}\,(2+\sqrt{2})$ forment une partition de $\mathbb{N}^*$.

Pour montrer cette propriété, nous allons compter combien d'éléments de $\mathcal{S}\,(\sqrt{2})$ sont dans $[1,n]$ et combien d'éléments de $\mathcal{S}\,(2+\sqrt{2})$ sont dans $[1,n]$. Si, pour tout n, le total vaut n, alors les deux ensembles partitionnent effectivement les entiers strictement positifs.

Soit $\alpha \in]1,+\infty[$. Notons $N(\alpha,n)$ le nombre d'eléments de $\mathcal{S}\,(\alpha) \cap [1,n]$.

$$\begin{aligned}\mathcal{S}\,(\alpha)\cap[1,n] =& \{E(k\alpha) : 1 \le k,\ \text{et}\ E(k\alpha) \le n\}\\ =& \{E(k\alpha) : 1 \le k,\ \text{et}\ E(k\alpha) < n+1\}\\ =& \{E(k\alpha) : 1 \le k,\ \text{et}\ k\alpha < n+1\}\\ =& \{E(k\alpha) : 0 < k < (n+1)/\alpha\}.\end{aligned}$$

comme $\alpha > 1$ le spectre est une suite strictement croissante et par conséquent,

$$N(\alpha,n) = \ \text{Card}\ \ (]0,(n+1)/\alpha[\cap\mathbb{N}^*).$$

Alors,

$$N(\alpha,n) = \begin{cases} E\left(\dfrac{n+1}{\alpha}\right) & \text{si} \quad \dfrac{n+1}{\alpha} \notin \mathbb{N};\\ E\left(\dfrac{n+1}{\alpha}\right) - 1 & \text{si} \quad \dfrac{n+1}{\alpha} \in \mathbb{N}\end{cases}$$

(Remarquons que nous aurions pu écrire $N(\alpha,n) = \left\lceil \dfrac{n+1}{\alpha} \right\rceil - 1$.)

Maintenant, que nous avons $N(\alpha,n)$ nous pouvons écrire (tenant compte du fait que $\sqrt{2}$ et $2+\sqrt{2}$ sont irrationnels),

$$\begin{aligned}N(\sqrt{2},n) + N(2+\sqrt{2},n) =& E\left(\frac{n+1}{\sqrt{2}}\right) + E\left(\frac{n+1}{2+\sqrt{2}}\right)\\ =& \frac{n+1}{\sqrt{2}} - \left\{\frac{n+1}{\sqrt{2}}\right\} + \frac{n+1}{2+\sqrt{2}} - \left\{\frac{n+1}{2+\sqrt{2}}\right\}\\ =& n+1 - \left\{\frac{n+1}{\sqrt{2}}\right\} - \left\{\frac{n+1}{2+\sqrt{2}}\right\}.\end{aligned}$$

Tout se simplifie parce que $\dfrac{1}{\sqrt{2}} + \dfrac{1}{2+\sqrt{2}} = 1$.

La fin de l'histoire vient du fait suivant:

Si $x \in \mathbb{R} \setminus \mathbb{Z}$ et si $y \in \mathbb{R}$ tels que $x + y \in \mathbb{Z}$ alors $\{x\} + \{y\} = 1$.

En effet, on a $E(x) < x < E(x) + 1$ et $E(y) \leq y < E(y) + 1$ d'où

$$E(x) + E(y) < x + y < E(x) + E(y) + 2$$

mais $x+y$ est un entier relatif donc $x+y = E(x)+E(y)+1$ ou bien $x-E(x)+y-E(y) = 1$.

On arrive, alors, à la conclusion suivante:

$$N(\sqrt{2}, n) + N(2 + \sqrt{2}, n) = n. \quad \text{pour tout } n \geq 1.$$

Ceci démontre que $\mathcal{S}(\sqrt{2})$ et $\mathcal{S}(2 + \sqrt{2})$ forment une partition de $\mathbb{N}^*$.

La démarche suivie dans cet exemple est assez générale et permet de démontrer la proposition suivante,

Soient $\alpha > 1$ et $\beta > 1$ deux nombres irrationnels liés par la relation $\dfrac{1}{\alpha} + \dfrac{1}{\beta} = 1$. Alors $\mathcal{S}(\alpha)$ et $\mathcal{S}(\beta)$ forment une partition de $\mathbb{N}^*$.

6°. **La représentation p-adique des nombres entiers naturels.**

Lorsqu'on écrit 1994 alors cela représente l'entier naturel $n = 4+9\times10+9\times10^2+1\times10^3$, on dit que 1994 ou $(1994)_{10}$ est la représentation décimale de l'entier n. Plus généralement tout entier naturel n admet une écriture $b_k b_{k-1} \dots b_0$ où les $(b_j)_{0\leq j\leq k}$ sont des symboles pris dans $0, 1, 2, \dots, 9$, et tels que $n = \sum_{j=0}^{k} b_j\, 10^j$. Les $(b_j)_{0\leq j\leq k}$ s'appellent des *chiffres*, et 10 s'appelle la base. Depuis plusieurs millénaires les Babiloniens ont utilisé un système de représentation des entiers à base de 60 que nous continuons à utiliser pour la mesure des angles. Par contre, l'utilisation des composants électroniques ayant deux états 0 et 1 pour construire des machines, permettant d'effectuer des calculs numériques, a favorisé la représentation des entiers dans la base 2 (on dit *représentation binaire*). Notre but ici est d'étudier la représentation des entiers naturels dans une base p,($p > 1$ et $p \in \mathbb{N}$).

Dans la suite $p > 1$ est un entier fixé. si n est un nombre naturel, on définit la suite $(x_j^{(n)})_{0\leq j}$ par

$$x_0^{(n)} = n, \quad x_j^{(n)} = E\left(\frac{x_{j-1}^{(n)}}{p}\right), \quad \text{pour } j \geq 1.$$

Remarquons que $E\left(\dfrac{E(x)}{p}\right) = E\left(\dfrac{x}{p}\right)$. Car $x = pE(x/p) + r$ avec $r \in [0, p[$, d'où $E(x) = pE(x/p) + E(r)$ avec $E(r) \in \{0, 1, \dots, p-1\}$ et par conséquent $E(E(x)/p) = E(x/p) + E(E(r)/p) = E(x/p)$.

Ceci montre que $x_j^{(n)} = E\left(\frac{n}{p^j}\right)$. On en déduit que si $j > \ell_p(n) = E(\log_p(n))$ alors $x_j^{(n)} = 0$.

On pose ensuite $b_j^{(n)} = x_j^{(n)} - px_{j+1}^{(n)}$ pour tout $j \geq 0$. $b_j^{(n)}$ est un entier appartenant à l'ensemble $\{0, 1, 2, \ldots, p-1\}$, et de plus $n = \sum_{j\geq 0} b_j^{(n)} p^j$. En effet

$$\begin{aligned}\sum_{j\geq 0} b_j^{(n)} p^j =& \sum_{j\geq 0} \left(x_j^{(n)} p^j - x_{j+1}^{(n)} p^{j+1}\right)\\ =& \sum_{j\geq 0} x_j^{(n)} p^j - \sum_{j\geq 0} x_{j+1}^{(n)} p^{j+1}\\ =& \sum_{j\geq 0} x_j^{(n)} p^j - \sum_{j\geq 1} x_j^{(n)} p^j\\ =& x_0^{(n)} = n.\end{aligned}$$

D'autre part, cette écriture est unique (nous laissons la vérification de l'unicité comme exercice au lecteur).

Habituellement, on utilise la notation $(b_\ell b_{\ell-1} \ldots b_0)_p$ pour désigner l'entier $n = \sum_{j=0}^{\ell} b_j p^j$.

Voici un exemple, $(15)_{10} = (1111)_2 = (33)_4 = (23)_6$.

Les bases les plus utilisées (autre que 10 bien entendu) sont 2, 8, et 16, et pour la dernière les chiffres sont: $1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$. Donc $(15)_{10} = (F)_{16}$.

EXERCICES

EXERCICE .1 Montrer que pour tout $(x, y) \in \mathbb{R}^2$ on a

$$E(x) + E(x+y) + E(y) \leq E(2x) + E(2y).$$

EXERCICE .2 Exprimer plus simplement la somme $\sum_{k=0}^{n} E(\sqrt{k})$.

EXERCICE .3 Un entier naturel n est dit *honnête* si l'on peut trouver $(a, b) \in \mathbb{N} \times \mathbb{N}$ tels que $n = E(a\sqrt{2} + b\sqrt{3})$. Combien d'entiers honnêtes y a-t-il entre 0 et 20 ? Généraliser.

EXERCICE .4 Est-ce qu'on peut trouver des couples de fonctions *strictement croissantes* f et g de $\mathbb{N}^*$ dans $\mathbb{N}^*$ telles que $\operatorname{Im} f$ et $\operatorname{Im} g$ forment une partition de $\mathbb{N}^*$ et $\forall\, n \in \mathbb{N}^*, \quad g(n) = 1 + f(f(n))$?

EXERCICE .5 Soit p un entier naturel plus grand ou égal à 2.

1°. Exprimer la somme

$$\Delta_m(p) = \sum_{k=1}^{pm} \frac{k - pE(k/p)}{k(k+1)}.$$

en utilisant les nombres harmoniques. Quelle est la limite de $\Delta_m(p)$ lorsque m tend vers l'infini ?

2°. Pour un entier naturel k on note $S_p(k)$ la somme des chiffres de l'écriture de k en base p.(Par exemple $S_2(15) = 4$, $S_{10}(15) = 6$...). Montrer que

$$\lim_{N\to\infty} \sum_{k=1}^{N} \frac{S_p(k)}{k(k+1)} = \frac{p}{p-1} \operatorname{Log} p.$$

EXERCICE .6 Étudier la fonction $f : \mathbb{N}^* \longrightarrow \mathbb{R}$ définie par les relations

$$f(1) = 1, \quad f(3) = 3, \quad \forall\, n \geq 1, \quad \begin{cases} f(2n) &= f(n) \\ f(4n+1) &= 2f(2n+1) - f(n) \\ f(4n+3) &= 3f(2n+1) - 2f(n) \end{cases}$$

(On comparera l'écriture binaire de n et de $f(n)$ pour quelques valeurs de n).

EXERCICE .7 Soit $f : \mathbb{N}^* \longrightarrow \mathbb{N}$ telle que, pour tout $(x, y) \in \mathbb{N}^* \times \mathbb{N}^*$, on a $f(x+y) - f(x) - f(y) \in \{0, 1\}$. Montrer qu'il existe $\alpha \in \mathbb{R}_+$ tel que

$$(\forall\, n \in \mathbb{N}^*, \quad f(n) = E(\alpha n)) \quad \text{ou} \quad (\forall\, n \in \mathbb{N}^*, \quad f(n) = \lceil \alpha n \rceil - 1).$$

Principes de dénombrement

Beaucoup de problèmes en mathématiques, et dans d'autres branches de la science, se ramènent à un calcul du nombre d'éléments d'un ensemble fini, c'est ce qu'on appelle *dénombrement*.

Nous allons, en traitant des exemples, exhiber quelques principes de dénombrement ou d'analyse combinatoire. Introduisons d'abord quelques notations.

Pour $n \in \mathbb{N}$, on notera $\mathbb{N}_n$ l'ensemble des nombres entiers naturels k qui vérifient les inégalités $1 \leq k \leq n$, en particulier $\mathbb{N}_0 = \emptyset$.

Un ensemble *non vide* A est dit *fini* si, et seulement s'il existe $n \in \mathbb{N}^*$ et une bijection $\varphi : \mathbb{N}_n \longrightarrow A$, (un tel n est nécessairement unique !), et dans ce cas on dit que le *cardinal* de A est n et on écrit $\text{Card}\,(A) = n$. Si A est vide on convient que $\text{Card}\,(A) = 0$, *i.e.* un ensemble vide contient 0 élément. Si A n'est pas fini on convient de noter $\text{Card}\,(A) = +\infty$.

Les deux propriétés suivantes sont alors immédiates:

$\mathcal{D}_1$: *Si A est un ensemble fini et si B est un ensemble en bijection avec A, alors B est aussi fini et* $\text{Card}\,(A) = \text{Card}\,(B)$.

$\mathcal{D}_2$: *Si A et B sont deux parties finies et disjointes d'un ensemble, alors $A \cup B$ est finie et* $\text{Card}\,(A \cup B) = \text{Card}\,(A) + \text{Card}\,(B)$.

1. L'ensemble des parties d'un ensemble fini

1°. L'ensemble $\mathcal{P}^{(n)}$.

Si E est un ensemble, on note $\mathcal{P}(E)$ l'ensemble des parties de E, et on note plus simplement $\mathcal{P}^{(n)}$ au lieu de $\mathcal{P}(\mathbb{N}_n)$. Combien d'éléments y a-t-il dans $\mathcal{P}^{(n)}$?

Clairement, $\mathcal{P}^{(0)} = \{\emptyset\}$, $\mathcal{P}^{(1)} = \{\{1\}, \emptyset\}$, et $\mathcal{P}^{(2)} = \{\{1,2\}, \{2\}, \{1\}, \emptyset\}$ donc

$$\text{Card}\left(\mathcal{P}^{(0)}\right) = 1, \quad \text{Card}\left(\mathcal{P}^{(1)}\right) = 2, \quad \text{et} \quad \text{Card}\left(\mathcal{P}^{(2)}\right) = 4.$$

Venons au cas général, supposons $n \geq 1$ et notons $\widetilde{\mathcal{P}}^{(n)}$ l'ensemble des parties de $\mathbb{N}_n$ ne contenant pas l'élément n et $\widehat{\mathcal{P}}^{(n)}$ l'ensemble des parties de $\mathbb{N}_n$ contenant l'élément n.

Comme toute partie de $\mathbb{N}_n$ soit elle contient n soit elle ne contient pas n alors

$$\widetilde{\mathcal{P}}^{(n)} \cap \widehat{\mathcal{P}}^{(n)} = \emptyset, \qquad \widetilde{\mathcal{P}}^{(n)} \cup \widehat{\mathcal{P}}^{(n)} = \mathcal{P}^{(n)}. \tag{1}$$

D'autre part, il est évident que les éléments de $\widetilde{\mathcal{P}}^{(n)}$ sont les parties de $\mathbb{N}_{n-1}$ d'où $\widetilde{\mathcal{P}}^{(n)} = \mathcal{P}^{(n-1)}$, et finalement, il y a une bijection simple entre $\mathcal{P}^{(n-1)}$ et $\widehat{\mathcal{P}}^{(n)}$ qui est donnée par

$$\varphi : \mathcal{P}^{(n-1)} \longrightarrow \widehat{\mathcal{P}}^{(n)} : A \mapsto A \cup \{n\}.$$

On en déduit, d'après $\mathcal{D}_1$, que si $\mathcal{P}^{(n-1)}$ est fini alors il en est de même pour $\widetilde{\mathcal{P}}^{(n)}$ et $\widehat{\mathcal{P}}^{(n)}$ et

$$\text{Card}\left(\mathcal{P}^{(n-1)}\right) = \text{Card}\left(\widetilde{\mathcal{P}}^{(n)}\right) = \text{Card}\left(\widehat{\mathcal{P}}^{(n)}\right),$$

par conséquent, d'après (1) et $\mathcal{D}_2$, $\mathcal{P}^{(n)}$ est aussi fini et

$$\text{Card}\left(\mathcal{P}^{(n)}\right) = \text{Card}\left(\widetilde{\mathcal{P}}^{(n)}\right) + \text{Card}\left(\widehat{\mathcal{P}}^{(n)}\right) = 2\text{Card}\left(\mathcal{P}^{(n-1)}\right).$$

Résumons ce que nous avons démontré:

$$\mathcal{P}^{(n-1)} \text{ est fini} \quad \Longrightarrow \quad \begin{cases} \mathcal{P}^{(n)} \text{ est fini,} \\ \text{Card}\left(\mathcal{P}^{(n)}\right) = 2\text{Card}\left(\mathcal{P}^{(n-1)}\right). \end{cases}$$

Ce qui démontre par récurrence sur n que $\text{Card}\left(\mathcal{P}^{(n)}\right) = 2^n$.

Conclusion:

$\mathcal{D}_3$: *L'ensemble des parties d'un ensemble fini A est fini et de cardinal* $2^{\text{Card}(A)}$.

2°.L'ensemble $\mathcal{P}_k^{(n)}$.

Notons, pour $k \in \mathbb{N}$, $\mathcal{P}_k^{(n)}$ l'ensemble des parties de $\mathbb{N}_n$ qui sont de cardinal k.

$$\mathcal{P}_k^{(n)} = \{\, A \subset \mathbb{N}_n : \text{ Card } (A) = k \,\}.$$

On pose par définition $C_n^k = \text{Card } \left(\mathcal{P}_k^{(n)}\right)$.

Il y a une seule partie de $\mathbb{N}_n$ qui a 0 élément, et une seule ayant n éléments, d'où

$$C_n^n = C_n^0 = 1, \quad \text{pour tout } n \geq 0.$$

Comme il n'y a pas de parties ayant strictement plus de n éléments dans $\mathbb{N}_n$, alors

$$C_n^k = 0, \quad \text{pour tout } k > n \geq 0.$$

Notons, pour $k \geq 0$ et $n \geq 0$, $A_{k+1}^{(n+1)}$ l'ensemble des parties de $\mathbb{N}_{n+1}$ qui sont de cardinal $k+1$ et qui contiennent l'élément $n+1$, et $B_{k+1}^{(n+1)}$ l'ensemble des parties de $\mathbb{N}_{n+1}$ qui sont de cardinal $k+1$ et qui ne contiennent pas l'élément $n+1$. Il est clair que

$$A_{k+1}^{(n+1)} \cap B_{k+1}^{(n+1)} = \emptyset, \quad \text{et} \quad A_{k+1}^{(n+1)} \cup B_{k+1}^{(n+1)} = \mathcal{P}_{k+1}^{(n+1)},$$

ce qui démontre que

$$C_{k+1}^{n+1} = \text{Card } \left(A_{k+1}^{(n+1)}\right) + \text{Card } \left(B_{k+1}^{(n+1)}\right). \tag{2}$$

Mais $A_{k+1}^{(n+1)}$ est en bijection avec $\mathcal{P}_k^{(n)}$, la bijection étant donnée par:

$$\varphi : \mathcal{P}_k^{(n)} \longrightarrow A_{k+1}^{(n+1)} : A \mapsto A \cup \{n+1\},$$

et $B_{k+1}^{(n+1)}$ est égal à $\mathcal{P}_{k+1}^{(n)}$, la relation (2) est, par conséquent, équivalente à

$$C_{n+1}^{k+1} = C_n^k + C_n^{k+1}, \quad \text{pour tout } (n,k) \in \mathbb{N}^2. \tag{3}$$

Cette formule permet par récurrence de calculer les valeurs non nulles des nombres C_n^k:

	$k=$	0	1	2	3	4	5
$n=0$		1					
$n=1$		1	1				
$n=2$		1	2	1			
$n=3$		1	3	3	1		
$n=4$		1	4	6	4	1	
$n=5$		1	5	10	10	5	1

$$\begin{array}{ccc} C_n^k & + & C_n^{k+1} \\ & \longrightarrow & \\ & \downarrow & || \\ & & C_{n+1}^{k+1} \end{array}$$

Nous allons utiliser une nouvelle technique pour expliciter C_n^k, qui s'appelle la technique des *fonctions génératrices*.

Posons, pour chaque $n \in \mathbb{N}$,

$$P_n(x) = \sum_{k \geq 0} C_n^k \, x^k$$

(la somme s'étend sur un nombre fini d'indices car $C_n^k = 0$ si $k > n$). Par exemple $P_0(x) = 1$ et $P_1(x) = 1 + x$.

Maintenant, en multipliant les deux membres de la relation (3) par x^{k+1} et en faisant la somme pour $k \geq 0$ on trouve

$$\sum_{k \geq 0} C_{n+1}^{k+1} \, x^{k+1} = \sum_{k \geq 0} C_n^k \, x^{k+1} + \sum_{k \geq 0} C_n^{k+1} \, x^{k+1},$$

ce qui s'écrit

$$P_{n+1}(x) - C_{n+1}^0 = xP_n(x) + P_n(x) - C_n^0$$

ou bien $P_{n+1}(x) = (1 + x)P_n(x)$. Ceci permet de déduire une nouvelle expression de $P_n(x)$, à savoir $P_n(x) = (1 + x)^n$, et démontre l'identité

$$(1 + x)^n = \sum_{k=0}^{n} C_n^k x^k, \quad \text{pour tout } n \geq 0. \tag{4}$$

Soit p un entier naturel tel que $0 < p < n$. En dérivant p fois les deux membres de l'égalité (4) et en substituant 0 à x, on trouve

$$n \times (n-1) \times \cdots \times (n-p+1) = p \times (p-1) \times \cdots \times 2 \times 1 . C_n^p$$

ou bien

$$C_n^p = \frac{n \times (n-1) \times \cdots \times (n-p+1)}{p \times (p-1) \times \cdots \times 2 \times 1}, \quad 0 < p < n,$$

cette écriture suggère d'introduire la notation suivante, pour $p \in \mathbb{N}^*$,

$$p! = 1 \times 2 \times \cdots \times (p-1) \times p \tag{5}$$

et $p!$ est lu " factoriel p ". Avec cette notation on a $C_n^p = \dfrac{n!}{p!(n-p)!}$, pour $0 < p < n$. On pose par convention $0! = 1$ pour que la formule précédente soit aussi vraie pour $p = 0$ et $p = n$.

Conclusion:

$\mathcal{D}_4$: *Soit $\mathcal{P}_k(A)$ l'ensemble des parties ayant k éléments d'un ensemble A de cardinal n, (avec $(k,n) \in \mathbb{N}^2$). Alors le cardinal C_n^k de $\mathcal{P}_k(A)$ est donné par*

$$C_n^k = \begin{cases} 0 & si \quad n < k \\ \dfrac{n!}{p!(n-p)!} & si \quad 0 \leq k \leq n \end{cases}$$

De plus les $(C_n^k)_{n,k}$ vérifient, pour $(k,n) \in \mathbb{N}^2$ les relations

$$C_{n+1}^{k+1} = C_n^k + C_n^{k+1}, \qquad C_{n+1}^{k+1} = \frac{n+1}{k+1} C_n^k, \qquad C_{n+k}^n = C_{n+k}^k. \tag{6}$$

La vérification des deux dernières égalités est laissée au lecteur.

Les nombres $(C_n^k)_{n,k}$ sont appelés les *coefficients binomiaux*. On dit aussi que C_n^k est le nombre des combinaisons de n éléments pris k à k.

3°. **Les partitions.**

Soit A un ensemble non vide, on dit que $(A_i)_{1\leq i\leq k}$ est une partition de A si, pour tout i l'ensemble A_i n'est pas vide, pour tout couple (i,j) avec $i \neq j$ l'intersection $A_i \cap A_j$ est vide, et enfin $A = A_1 \cup A_2 \cup \ldots \cup A_k$.

Si A est un ensemble non vide, on note $A^{\{k\}}$ l'enesmble des partitions de A en k parties. Si Card $(A) = n$, on note $\left\{ {n \atop k} \right\}$ le cardinal de $A^{\{k\}}$, ou bien

$$\left\{ {n \atop k} \right\} = \text{Card } \left(\mathbb{N}_n^{\{k\}} \right). \tag{7}$$

Il est immédiat que $\mathbb{N}_n$ admet une seule partition en une partie, et une seule partition en n parties, et enfin n'admet aucune partition en strictement plus de n parties. D'où

$$\left\{ {n \atop 1} \right\} = 1, \quad \left\{ {n \atop n} \right\} = 1, \quad \left\{ {n \atop k} \right\} = 0, \quad \text{pour } k > n. \tag{8}$$

Soit $(n,k) \in \mathbb{N} \times \mathbb{N}$ et considérons $\mathbb{N}_{n+1}^{\{k+1\}}$. Cet ensemble est la réunion de deux ensembles disjoints Ξ_1 et Ξ_2, où Ξ_1 est l'ensemble des partitions de $\mathbb{N}_{n+1}$ en $k+1$ parties dont une partie est $\{n+1\}$, et Ξ_2 est l'ensemble des partitions de $\mathbb{N}_{n+1}$ en $k+1$ parties dont $\{n+1\}$ n'et pas une partie.

Clairement Ξ_1 est en bijection avec $\mathbb{N}_n^{\{k\}}$. Donc Card $(\Xi_1) =$ Card $\left(\mathbb{N}_n^{\{k\}}\right)$.
D'autre part, à chaque partition $(A_i)_{1\leq i\leq k+1}$ de $\mathbb{N}_n$ qui est élément de $\mathbb{N}_n^{\{k+1\}}$ on peut associer $k+1$ partitions qui sont éléments de Ξ_2 (en mettant l'élément $n+1$ dans l'une des parties $A_1,\ldots,A_{k+1}$). Donc Card $(\Xi_2) = (k+1)$Card $\left(\mathbb{N}_n^{\{k+1\}}\right)$.
Comme Card $\left(\mathbb{N}_{n+1}^{\{k+1\}}\right) =$ Card $(\Xi_1)+$Card (Ξ_2), on déduit la relation importante suivante

$$\left\{ {n+1 \atop k+1} \right\} = (k+1)\left\{ {n \atop k+1} \right\} + \left\{ {n \atop k} \right\} \quad \text{pour } (n,k)\in\mathbb{N}^2. \tag{9}$$

Cette formule permet par récurrence de calculer les valeurs non nulles des nombres $\left\{ {n \atop k} \right\}$:

	$k=$	1	2	3	4	5
$n=1$		1				
$n=2$		1	1			
$n=3$		1	3	1		
$n=4$		1	7	6	1	
$n=5$		1	15	25	10	1

;

$$\left\{ {n \atop k} \right\} \xrightarrow{+(k+1)} \left\{ {n \atop k+1} \right\}$$
$$\downarrow \qquad\qquad ||$$
$$\left\{ {n+1 \atop k+1} \right\}$$

D'où

$\mathcal{D}_5$:

Soit $A^{\{k\}}$ l'ensemble des partitions d'un ensemble A de cardinal n en k parties, (avec $(n,k)\in\mathbb{N}^*\times\mathbb{N}^*$). Alors le cardinal de $A^{\{k\}}$ est donné par $\left\{ {n \atop k} \right\}$.
où les $\left\{ {n \atop k} \right\}$ sont définis par les relations

$$\left\{ {n \atop 1} \right\} = 1, \quad \left\{ {1 \atop k+1} \right\} = 0, \quad \left\{ {n+1 \atop k+1} \right\} = (k+1)\left\{ {n \atop k+1} \right\} + \left\{ {n \atop k} \right\}.$$

qui sont valables pour $(n,k)\in\mathbb{N}^*\times\mathbb{N}^*$.

Les nombres $\left\{ {n \atop k} \right\}$ s'appellent *les nombres de Stirling de seconde espèce*. Nous allons donner la propriété dont s'est servie le mathématicien anglais James Stirling (1692-1770) pour définir ses nombres.

Considérons, pour commencer, la suite de fonctions polynômiales définie par

$$W_0(x) = 1, \quad W_k(x) = x(x-1)\cdots(x-k+1) = \prod_{j=0}^{k-1}(x-j), \quad \text{pour } k\geq 1. \tag{10}$$

Soit, pour $n \geq 1$, la fonction $P_n(x) = \sum_{k\geq 1} \left\{ {n \atop k} \right\} W_k(x)$. C'est une fonction polynômiale de degré n car $\left\{ {n \atop k} \right\} = 0$ si $k > n$.
En utilisant (9) on a

$$\begin{aligned}
P_{n+1}(x) =& \sum_{k\geq 1} \left\{ {n+1 \atop k} \right\} W_k(x) \\
=& x + \sum_{k\geq 2} \left\{ {n+1 \atop k} \right\} x(x-1)\cdots(x-k+1) \\
=& x + \sum_{k\geq 1} \left\{ {n+1 \atop k+1} \right\} x(x-1)\cdots(x-k) \\
=& x + \sum_{k\geq 1} \left((k+1) \left\{ {n \atop k+1} \right\} + \left\{ {n \atop k} \right\} \right) W_{k+1}(x) \\
=& x + \sum_{k\geq 1} (k+1) \left\{ {n \atop k+1} \right\} W_{k+1}(x) + \sum_{k\geq 1} \left\{ {n \atop k} \right\} W_{k+1}(x) \\
=& x + \sum_{k\geq 2} k \left\{ {n \atop k} \right\} W_k(x) + \sum_{k\geq 1} \left\{ {n \atop k} \right\} W_{k+1}(x) \\
=& \sum_{k\geq 1} \left\{ {n \atop k} \right\} (kW_k(x) + W_{k+1}(x))
\end{aligned}$$

soit

$$\begin{aligned}
P_{n+1}(x) =& \sum_{k\geq 1} \left\{ {n \atop k} \right\} (k + x - k) W_k(x) \\
=& x \sum_{k\geq 1} \left\{ {n \atop k} \right\} W_k(x) = xP_n(x)
\end{aligned}$$

Comme $P_1(x) = x$, on en déduit par récurrence que, pour tout $n \in \mathbb{N}^*$, $P_n(x) = x^n$. Alors on a l'identité suivante

$$x^n = \sum_{k\geq 1} \left\{ {n \atop k} \right\} x(x-1)\cdots(x-k+1). \quad \text{pour } n \geq 1 \tag{11}$$

Voici maintenat une propriété importante des fonctions polynômiales $(W_k)_{k\geq 0}$:

$$\begin{aligned}
W_{k+1}(x+1) - W_{k+1}(x) =& (x+1)x(x-1)\cdots(x+1-k) - x(x-1)\cdots(x-k) \\
=& x(x-1)\cdots(x-k+1)\left((x+1) - (x-k)\right) \\
=& (k+1)W_k(x).
\end{aligned}$$

En utilisant cette propriété et l'identité (11) on déduit que, pour $n \geq 1$

$$x^n = \sum_{k=1}^{n} \frac{1}{k+1} \left\{ {n \atop k} \right\} W_{k+1}(x+1) - \sum_{k=1}^{n} \frac{1}{k+1} \left\{ {n \atop k} \right\} W_{k+1}(x). \tag{12}$$

Si l'on pose alors

$$Q_n(x) = \sum_{k=1}^{n} \frac{1}{k+1} \left\{ {n \atop k} \right\} W_{k+1}(x).$$

On trouve que $x^n = Q_n(x+1) - Q_n(x)$ pour tout $n \geq 1$. D'où

$$\begin{aligned} \sum_{p=1}^{m} p^n =& \sum_{p=1}^{m} Q_n(p+1) - Q_n(p) \\ =& \sum_{p=1}^{m} Q_n(p+1) - \sum_{p=1}^{m} Q_n(p) \\ =& \sum_{p=1}^{m+1} Q_n(p) - \sum_{p=1}^{m} Q_n(p) \\ =& Q_n(m+1). \end{aligned}$$

Par conséquent

$$\sum_{p=1}^{m} p^n = \sum_{k=1}^{n} \left\{ {n \atop k} \right\} \frac{(m+1)m \cdots (m+1-k)}{k+1}.$$

Ce qui s'ecrit d'une façon plus condensée:

$$\sum_{p=1}^{m} p^n = \sum_{k=1}^{n} k! \left\{ {n \atop k} \right\} C_{m+1}^{k+1}. \tag{13}$$

Nous laissons au lecteur le soin de retrouver les résultats du troisième chapitre.

2. Les applications entre deux ensembles finis

1°.L'ensemble $\mathcal{F}(\mathbb{N}_n, \mathbb{N}_p)$.

C'est l'ensemble des applications de $\mathbb{N}_n$ dans $\mathbb{N}_p$, avec $(n,p) \in \mathbb{N}^* \times \mathbb{N}^*$. Notons $F(n,p)$ le cardinal de $\mathcal{F}(\mathbb{N}_n, \mathbb{N}_p)$.

Il est immédiat que $F(n,1) = 1$ et que $F(1,p) = p$. Fixons n et p, et posons, pour $k \in \mathbb{N}_p$,

$$B_k = \{f \in \mathcal{F}(\mathbb{N}_n, \mathbb{N}_p) : \ f(n) = k\}.$$

Il est evident que si k et ℓ sont distincts alors B_k et B_ℓ sont disjoints, et que

$$\mathcal{F}(\mathbb{N}_n, \mathbb{N}_p) = B_1 \cup B_2 \cup \cdots \cup B_p.$$

D'où

$$F(n,p) = \sum_{k=1}^{p} \text{Card } (B_k)\,. \tag{14}$$

Mais B_k est en bijection avec $\mathcal{F}(\mathbb{N}_{n-1}, \mathbb{N}_p)$. (La bijection est l'application φ de B_k dans $\mathcal{F}(\mathbb{N}_{n-1}, \mathbb{N}_p)$, qui à f associe la restriction $f_{|\,\mathbb{N}_{n-1}}$ de f à $\mathbb{N}_{n-1}$). Alors Card $(B_k) = F(n-1,p)$, et par conséquent la relation (14) montre que l'on a $F(n,p) = pF(n-1,p)$. Cette relation avec le fait que $F(1,p) = p$ permettent de démontrer par récurrence sur n que $F(n,p) = p^n$.

Conclusion:

$\mathcal{D}_6$: *Soit $\mathcal{F}(A,B)$ l'ensemble des applications d'un ensemble A de cardinal n, dans un ensemble B de cardinal p, (avec $(n,p) \in \mathbb{N}^* \times \mathbb{N}^*$). Alors le cardinal de $\mathcal{F}(A,B)$ est p^n.*

2°.L'ensemble $\mathcal{F}_{\text{sc}}(\mathbb{N}_n, \mathbb{N}_p)$.

C'est l'ensemble des applications *strictement croissantes* de $\mathbb{N}_n$ dans $\mathbb{N}_p$, avec $(n,p) \in \mathbb{N}^* \times \mathbb{N}^*$. Une application strictement croissante est nécessairement injective et donc son image contient au moins autant d'éléments que son ensemble de départ, alors $\mathcal{F}_{\text{sc}}(\mathbb{N}_n, \mathbb{N}_p)$ est vide si $p < n$.

Nous supposons désormais que $p \geq n$. Considérons l'application

$$\varphi : \mathcal{F}_{\text{sc}}(\mathbb{N}_n, \mathbb{N}_p) \longrightarrow \mathcal{P}_n^{(p)} : f \mapsto \text{Im}\, f \tag{15}$$

où $\mathcal{P}_n^{(p)}$ est l'ensemble des parties ayant n éléments dans $\mathbb{N}_p$, et $\text{Im}\, f$ est l'image de f.

Nous allons voir que cette application est bijective en exhibant son inverse. Si A est une partie ayant n éléments dans $\mathbb{N}_p$, on définit l'application $f_A : \mathbb{N}_n \longrightarrow \mathbb{N}_p$ en posant

$$f_A(k) = \min\left(A \setminus f_A(\mathbb{N}_{k-1})\right), \quad \text{pour } k \in \mathbb{N}_n, \tag{16}$$

cette définition ne semble pas claire au premier regard car il y a " f_A " dans les deux membres de l'égalité, alors nous allons la détailler un peu. D'abord, pour $k = 1$, on a $f_A(\emptyset) = \emptyset$ et $f_A(1) = \min(A)$ c'est le plus petit élément de A. Maintenant, pour $k = 2$, on a $f_A(\mathbb{N}_1) = \{f_A(1)\}$ et $f_A(2) = \min\left(A \setminus \{f_A(1)\}\right)$. On voit donc comment ça tourne !, si pour un certain $k > 1$ on a déjà $f_A(1)$, $f_A(2)$, ..., et $f_A(k-1)$, alors, pour trouver $f_A(k)$, on supprime ces éléments de A et $f_A(k)$ est le plus petit élément qui reste. (On dit que f_A est définie par récurrence). Il est par construction clair que f_A est strictement croissante et que $\text{Im}\, f_A = A$.

Considérons, alors, l'application

$$\vartheta : \mathcal{P}_n^{(p)} \longrightarrow \mathcal{F}_{\text{sc}}(\mathbb{N}_n, \mathbb{N}_p) : A \mapsto f_A. \tag{17}$$

Quelques instants de réflexion permettent de nous convaincre que $\varphi \circ \vartheta$ est l'application identité de $\mathcal{P}_n^{(p)}$ sur lui-même, et que $\vartheta \circ \varphi$ est l'application identité de $\mathcal{F}_{\text{sc}}(\mathbb{N}_n, \mathbb{N}_p)$ sur lui-même. Par conséquent φ est une bijection et $\varphi^{-1} = \vartheta$.

Comme φ est bijective alors $\text{Card}\left(\mathcal{P}_n^{(p)}\right) = \text{Card}\left(\mathcal{F}_{\text{sc}}(\mathbb{N}_n, \mathbb{N}_p)\right)$. D'où

$\mathcal{D}_7$: *Soit $\mathcal{F}_{\text{sc}}(\mathbb{N}_n, \mathbb{N}_p)$ l'ensemble des applications strictement croissantes de $\mathbb{N}_n$ dans $\mathbb{N}_p$, (avec $(n,p) \in \mathbb{N}^* \times \mathbb{N}^*$). Alors*

$$\text{Card}\left(\mathcal{F}_{\text{sc}}(\mathbb{N}_n, \mathbb{N}_p)\right) = C_p^n.$$

Application:

Soit, pour $(n,p) \in \mathbb{N}^* \times \mathbb{N}^*$, l'ensemble $\mathcal{U}(n,p)$ des n-uplets $(x_1, x_2, \ldots, x_n)$ de $(\mathbb{N}^*)^n$ tels que $\sum_{k=1}^{n} x_k \leq p$.

$$\mathcal{U}(n,p) = \left\{ (x_1, x_2, \ldots, x_n) \in (\mathbb{N}^*)^n : \sum_{k=1}^{n} x_k \leq p \right\}.$$

On se propose de calculer le cardinal de cet ensemble. Pour cela nous allons démontrer que $\mathcal{U}(n,p)$ est en bijection avec $\mathcal{F}_{\text{sc}}(\mathbb{N}_n, \mathbb{N}_p)$.

Considérons pour cela les deux applications suivantes

$$\varphi : \mathcal{U}(n,p) \longrightarrow \mathcal{F}_{\text{sc}}(\mathbb{N}_n, \mathbb{N}_p) : \overline{x} = (x_1, \ldots, x_n) \mapsto \varphi(\overline{x}) = f_{\overline{x}}$$

où $f_{\overline{x}}(k) = \sum_{i=1}^{k} x_i$. Et

$$\vartheta : \mathcal{F}_{\text{sc}}(\mathbb{N}_n, \mathbb{N}_p) \longrightarrow \mathcal{U}(n,p) : f \mapsto \vartheta(f) = \overline{x}_f$$

où $\overline{x}_f = (x_1, \ldots, x_n)$ avec $x_1 = f(1)$ et $x_k = f(k) - f(k-1)$ pour k tel que $1 < k \leq n$. Nous laissons au lecteur le soin de vérifier que φ et ϑ sont bien définies, que $\varphi \circ \vartheta$ est l'identité de $\mathcal{F}_{\text{sc}}(\mathbb{N}_n, \mathbb{N}_p)$, et que $\vartheta \circ \varphi$ est l'identité de $\mathcal{U}(n,p)$.

On en déduit que

$\mathcal{D}_8$: *Pour $(n,p) \in \mathbb{N}^* \times \mathbb{N}^*$. On a*

$$\text{Card}\left(\left\{ (x_1, x_2, \ldots, x_n) \in (\mathbb{N}^*)^n : \sum_{k=1}^{n} x_k \leq p \right\} \right) = C_p^n$$

Si l'on pose d'une façon similaire

$$\widetilde{\mathcal{U}}(n,p) = \left\{ (x_1, x_2, \ldots, x_n) \in (\mathbb{N}^*)^n : \sum_{k=1}^{n} x_k = p \right\}$$

alors clairement $\mathcal{U}(n,p-1)$ et $\widetilde{\mathcal{U}}(n,p)$ forment une partition de $\mathcal{U}(n,p)$ et par conséquent

$$\text{Card}\left(\widetilde{\mathcal{U}}(n,p)\right) = \text{Card}\left(\mathcal{U}(n,p)\right) - \text{Card}\left(\mathcal{U}(n,p-1)\right) = C_p^n - C_{p-1}^n = C_{p-1}^{n-1}.$$

D'où

$\mathcal{D}_9$: *Soit $(n,p) \in \mathbb{N}^* \times \mathbb{N}^*$. Alors*

$$\text{Card}\left(\left\{ (x_1, x_2, \ldots, x_n) \in (\mathbb{N}^*)^n : \sum_{k=1}^{n} x_k = p \right\} \right) = C_{p-1}^{n-1}$$

3°.L'ensemble $\mathcal{F}_{\rm c}(\mathbb{N}_n, \mathbb{N}_p)$.

C'est l'ensemble des applications *croissantes* de $\mathbb{N}_n$ dans $\mathbb{N}_p$, avec $(n,p) \in \mathbb{N}^* \times \mathbb{N}^*$. Pour déterminer le cardinal de cet ensemble nous allons utiliser la technique, qui nous est devenue familière, et qui consiste à trouver une bijection entre cet ensemble et un autre dont on connaît le cardinal.

Soit $f \in \mathcal{F}_{\rm c}(\mathbb{N}_n, \mathbb{N}_p)$. Pour $k \in \mathbb{N}_n$ on pose $\widetilde{f}(k) = f(k) + k - 1$. On a clairement $\widetilde{f}(k+1) - \widetilde{f}(k) = 1 + f(k+1) - f(k) \geq 1$, donc $\widetilde{f}$ est strictement croissante. De plus $\widetilde{f}(1) = f(1) \geq 1$, et $\widetilde{f}(n) = f(n) + n - 1 \leq n + p - 1$. On en déduit que $\widetilde{f} \in \mathcal{F}_{\rm sc}(\mathbb{N}_n, \mathbb{N}_{n+p-1})$. Inversement, soit $g \in \mathcal{F}_{\rm sc}(\mathbb{N}_n, \mathbb{N}_{n+p-1})$. Pour $k \in \mathbb{N}_n$ on pose $\widehat{g}(k) = g(k) - k + 1$. On a clairement $\widehat{g}(k+1) - \widehat{g}(k) = g(k+1) - g(k) - 1 \geq 0$, donc $\widehat{g}$ est croissante. De plus $\widehat{g}(1) = g(1) \geq 1$, et $\widehat{g}(n) = g(n) - n + 1 \leq p$. On en déduit que $\widehat{g} \in \mathcal{F}_{\rm c}(\mathbb{N}_n, \mathbb{N}_p)$. Enfin on a immédiatement $\widetilde{\widehat{g}} = g$ pour tout élément $g \in \mathcal{F}_{\rm sc}(\mathbb{N}_n, \mathbb{N}_{n+p-1})$, et $\widehat{\widetilde{f}} = f$ pour tout élément $f \in \mathcal{F}_{\rm c}(\mathbb{N}_n, \mathbb{N}_p)$. On a donc démontré que

$$\varphi : \mathcal{F}_{\rm c}(\mathbb{N}_n, \mathbb{N}_p) \longrightarrow \mathcal{F}_{\rm sc}(\mathbb{N}_n, \mathbb{N}_{n+p-1}) : f \mapsto \widetilde{f}.$$

est une application bijective dont l'inverse est donnée par

$$\vartheta : \mathcal{F}_{\rm sc}(\mathbb{N}_n, \mathbb{N}_{n+p-1}) \longrightarrow \mathcal{F}_{\rm c}(\mathbb{N}_n, \mathbb{N}_p) : g \mapsto \widehat{g}.$$

On arrive, par conséquent, à la propriété suivante:

$\mathcal{D}_{10}$: *Soit $\mathcal{F}_{\rm c}(\mathbb{N}_n, \mathbb{N}_p)$ l'ensemble des applications croissantes de $\mathbb{N}_n$ dans $\mathbb{N}_p$, (avec $(n,p) \in \mathbb{N}^* \times \mathbb{N}^*$). Alors*

$$\text{Card}\,(\mathcal{F}_{\rm c}(\mathbb{N}_n, \mathbb{N}_p)) = C^n_{n+p-1}.$$

Application:

Soit, pour $(n,p) \in \mathbb{N}^* \times \mathbb{N}$, l'ensemble $\mathcal{T}(n,p)$ des n-uplets $(x_1, x_2, \ldots, x_n)$ de $\mathbb{N}^n$ tels que $\sum_{k=1}^{n} x_k \leq p$.

$$\mathcal{T}(n,p) = \left\{ (x_1, x_2, \ldots, x_n) \in \mathbb{N}^n : \sum_{k=1}^{n} x_k \leq p \right\}.$$

Comme avant, pour calculer le cardinal de cet ensemble. nous allons démontrer que $\mathcal{T}(n,p)$ est en bijection avec $\mathcal{F}_{\rm c}(\mathbb{N}_n,\mathbb{N}_{p+1})$.

Considérons pour cela les deux applications suivantes

$$\varphi:\mathcal{T}(n,p)\longrightarrow\mathcal{F}_{\rm c}(\mathbb{N}_n,\mathbb{N}_{p+1}):\overline{x}=(x_1,\ldots,x_n)\mapsto\varphi(\overline{x})=f_{\overline{x}}.$$

où $f_{\overline{x}}(k)=1+\sum_{i=1}^{k}x_i$. Et

$$\vartheta:\mathcal{F}_{\rm c}(\mathbb{N}_n,\mathbb{N}_{p+1})\longrightarrow\mathcal{T}(n,p):f\mapsto\vartheta(f)=\overline{x}_f.$$

où $\overline{x}_f=(x_1,\ldots,x_n)$ avec $x_1=f(1)-1$ et $x_k=f(k)-f(k-1)$ pour k tel que $1<k\leq n$. Nous laissons au lecteur le soin de vérifier que φ et ϑ sont bien définies, que $\varphi\circ\vartheta$ est l'identité de $\mathcal{F}_{\rm c}(\mathbb{N}_n,\mathbb{N}_{p+1})$, et que $\vartheta\circ\varphi$ est l'identité de $\mathcal{T}(n,p)$.

On en déduit que

$\mathcal{D}_{11}$: *Pour* $(n,p)\in\mathbb{N}^*\times\mathbb{N}$. *On a*

$$\text{Card}\left(\left\{(x_1,x_2,\ldots,x_n)\in\mathbb{N}^n:\sum_{k=1}^{n}x_k\leq p\right\}\right)=C_{p+n}^{n}$$

Si l'on pose d'une façon similaire

$$\widetilde{\mathcal{T}}(n,p)=\left\{(x_1,x_2,\ldots,x_n)\in\mathbb{N}^n:\sum_{k=1}^{n}x_k=p\right\}$$

alors clairement $\mathcal{T}(n,p-1)$ et $\widetilde{\mathcal{T}}(n,p)$ forment une partition de $\mathcal{T}(n,p)$ et par conséquent

$$\text{Card}\left(\widetilde{\mathcal{T}}(n,p)\right)=\text{Card}\left(\mathcal{T}(n,p)\right)-\text{Card}\left(\mathcal{T}(n,p-1)\right)=C_{p+n}^{n}-C_{n+p-1}^{n}=C_{n+p-1}^{n-1}.$$

D'où

$\mathcal{D}_{12}$: *Soit* $(n,p)\in\mathbb{N}^*\times\mathbb{N}$. *Alors*

$$\text{Card}\left(\left\{(x_1,x_2,\ldots,x_n)\in\mathbb{N}^n:\sum_{k=1}^{n}x_k=p\right\}\right)=C_{n+p-1}^{n-1}$$

4°.L'ensemble $\mathcal{F}_{\mathrm{i}}(\mathbb{N}_n, \mathbb{N}_p)$.

C'est l'ensemble des applications injectives de $\mathbb{N}_n$ dans $\mathbb{N}_p$. Cet ensemble est vide si $p < n$. On suppose dans la suite $p \geq n$.

Si $\widetilde{f} : \mathbb{N}_{n+1} \longrightarrow \mathbb{N}_p$ est injective alors sa restriction $f = \widetilde{f}_{|\,\mathbb{N}_n}$ à $\mathbb{N}_n$ est aussi injective, et inversement si $f : \mathbb{N}_n \longrightarrow \mathbb{N}_p$ est injective alors il y a exactement $p - n$ prolongements injectifs $\widetilde{f} : \mathbb{N}_{n+1} \longrightarrow \mathbb{N}_p$ de f, (car $f(n+1)$ est pris dans $\mathbb{N}_p \setminus \mathrm{Im}\ f$). On en déduit que

$$\forall\, f \in \mathcal{F}_{\mathrm{i}}(\mathbb{N}_n, \mathbb{N}_p), \quad \mathrm{Card}\left(\{\widetilde{f} \in \mathcal{F}_{\mathrm{i}}(\mathbb{N}_{n+1}, \mathbb{N}_p) : \widetilde{f}_{|\,\mathbb{N}_n} = f\}\right) = p - n.$$

Il en résulte que

$$\begin{aligned}\mathrm{Card}\ (\mathcal{F}_{\mathrm{i}}(\mathbb{N}_{n+1}, \mathbb{N}_p)) &= \sum_{f \in \mathcal{F}_{\mathrm{i}}(\mathbb{N}_n, \mathbb{N}_p)} \mathrm{Card}\left(\{\widetilde{f} \in \mathcal{F}_{\mathrm{i}}(\mathbb{N}_{n+1}, \mathbb{N}_p) : \widetilde{f}_{|\,\mathbb{N}_n} = f\}\right) \\ &= (p-n) \sum_{f \in \mathcal{F}_{\mathrm{i}}(\mathbb{N}_n, \mathbb{N}_p)} 1 \\ &= (p-n)\ \mathrm{Card}\ (\mathcal{F}_{\mathrm{i}}(\mathbb{N}_n, \mathbb{N}_p))\,.\end{aligned}$$

Comme l'on a clairement $\mathrm{Card}\ (\mathcal{F}_{\mathrm{i}}(1, p)) = p$ alors, par récurrence sur n, on trouve aussitôt que

$$\mathrm{Card}\ (\mathcal{F}_{\mathrm{i}}(\mathbb{N}_n, \mathbb{N}_p)) = p(p-1)\cdots(p-n+1) = \frac{p!}{(p-n)!}.$$

Conclusion

$\mathcal{D}_{13}$: *Soit $\mathcal{F}_{\mathrm{i}}(A, B)$ l'ensemble des applications injectives d'un ensemble A de cardinal n dans un ensemble B de cardinal p, (avec $(n, p) \in \mathbb{N}^* \times \mathbb{N}^*$). Alors le cardinal de $\mathcal{F}_{\mathrm{i}}(A, B)$ est donné par*

$$\mathrm{Card}\ (\mathcal{F}_{\mathrm{i}}(A, B)) = \begin{cases} 0 & \text{si} \quad n > p \\ \dfrac{p!}{(p-n)!} & \text{si} \quad n \leq p. \end{cases}$$

5°.L'ensemble $\mathcal{S}(n)$.

C'est l'ensemble des applications bijectives sur $\mathbb{N}_n$, qu'on appelle aussi *permutations*.
Il est immédiat de voir que $\mathcal{S}(n) = \mathcal{F}_{\mathrm{i}}(\mathbb{N}_n, \mathbb{N}_n)$, car, pour une application f de $\mathbb{N}_n$ dans $\mathbb{N}_n$, être bijective est équivalent à être injective, et est aussi équivalent à être surjective. D'où

$\mathcal{D}_{14}$: *Soit $\mathcal{S}(A)$ l'ensemble des applications bijectives d'un ensemble A de cardinal n, (avec $n \in \mathbb{N}^*$). Alors le cardinal de $\mathcal{S}(A)$ est donné par*

$$\mathrm{Card}\,(\mathcal{S}(A)) = n!$$

6°.L'ensemble $\mathcal{F}_{\mathrm{s}}(\mathbb{N}_n, \mathbb{N}_p)$.

C'est l'ensemble des applications surjectives de $\mathbb{N}_n$ sur $\mathbb{N}_p$. Notons $S(n,p)$ le cardinal de l'ensemble $\mathcal{F}_{\mathrm{s}}(\mathbb{N}_n, \mathbb{N}_p)$. Clairement on a $S(n,1) = 1$, et $S(n,n) = n!$ car $\mathcal{F}_{\mathrm{s}}(\mathbb{N}_n, \mathbb{N}_n) = \mathcal{S}(n)$. De plus $S(n,p) = 0$ si $n < p$.
Soit $(n,p) \in \mathbb{N}^* \times \mathbb{N}^*$. Pour $k \in \mathbb{N}_{p+1}$ on note

$$\Xi_k = \{f \in \mathcal{F}_{\mathrm{s}}(\mathbb{N}_{n+1}, \mathbb{N}_{p+1}) :\ f(n+1) = k\}.$$

Les ensembles $\Xi_1, \ldots, \Xi_{p+1}$ forment une partitions de $\mathcal{F}_{\mathrm{s}}(\mathbb{N}_{n+1}, \mathbb{N}_{p+1})$. Pour un $k \in \mathbb{N}_{p+1}$ fixé on pose

$$\Xi'_k = \{f \in \Xi_k :\ \mathrm{Card}\,\left(f^{-1}(\{k\})\right) = 1\},$$
$$\Xi''_k = \{f \in \Xi_k :\ \mathrm{Card}\,\left(f^{-1}(\{k\})\right) > 1\}.$$

Il est immédiat de voir que les applications

$$\varphi : \Xi'_k \longrightarrow \mathcal{F}_{\mathrm{s}}(\mathbb{N}_n, \mathbb{N}_{p+1} \setminus \{k\}) : f \mapsto f_{|\mathbb{N}_n}.$$

$$\vartheta : \Xi''_k \longrightarrow \mathcal{F}_{\mathrm{s}}(\mathbb{N}_n, \mathbb{N}_{p+1}) : f \mapsto f_{|\mathbb{N}_n}.$$

sont bijectives, d'où $\mathrm{Card}\,(\Xi_k) = S(n,p) + S(n,p+1)$. Il en résulte que

$$S(n+1,p+1) = \sum_{k=1}^{p+1} \mathrm{Card}\,(\Xi_k) = (p+1)\,(S(n,p) + S(n,p+1))\,. \tag{18}$$

Cette formule permet par récurrence de calculer les valeurs non nulles des nombres $S(n,p)$:

	$k=$ 1	2	3	4	5
$n=1$	1				
$n=2$	1	2			
$n=3$	1	6	6		
$n=4$	1	14	36	24	
$n=5$	1	30	150	240	120

En comparant ces valeurs avec celles donnant les nombres de Stirling de seconde espèce, on remarque un lien étroit, à savoir $S(n,k) = k!\left\{ n \atop k \right\}$, pour $1 \leq n,k \leq 5$. Montrons que ceci est vrai en général.

Posons $s(n,k) = \dfrac{1}{k!}S(n,k)$. En divisant les deux membres de la relation (18) par $(p+1)!$ on trouve

$$s(n+1,p+1) = (p+1)s(n,p+1) + s(n,p). \tag{19}$$

C'est la même relation récurrente (9) définissant les nombres de Stirling de seconde espèce. Notons $\mathcal{H}_n$ la propriété "$s(n,p) = \left\{ n \atop p \right\}$, pour tout $p \geq 1$". La propriété $\mathcal{H}_1$ est évidemment vraie. Supposons que la propriété $\mathcal{H}_n$ est vraie, on a $s(n+1,1) = S(n+1,1) = 1 = \left\{ n+1 \atop 1 \right\}$, et si $p \in \mathbb{N}^*$ on a

$$s(n+1,p+1) = (p+1)s(n,p+1) + s(n,p) = (p+1)\left\{ n \atop p+1 \right\} + \left\{ n \atop p \right\} = \left\{ n+1 \atop p+1 \right\},$$

alors la propriété $\mathcal{H}_{n+1}$ est vraie, ce qui démontre que

$$S(n,p) = p!\left\{ n \atop p \right\}, \qquad \text{pour } (n,p) \in \mathbb{N}^* \times \mathbb{N}^*.$$

D'où la conclusion

$\mathcal{D}_{15}$: *Soit $\mathcal{F}_s(A,B)$ l'ensemble des applications surjectives d'un ensemble A de cardinal n, sur un ensemble B de cardinal p (avec $(n,p) \in \mathbb{N}^* \times \mathbb{N}^*$). Alors le cardinal de $\mathcal{F}_s(A,B)$ est donné par*

$$\text{Card}\,(\mathcal{F}_s(A,B)) = p!\left\{ n \atop p \right\}$$

où les $\left\{ n \atop p \right\}$ sont les nombres de Stirling de seconde espèce définis par les relations

$$\left\{ n \atop 1 \right\} = 1, \quad \left\{ 1 \atop p+1 \right\} = 0, \quad \left\{ n+1 \atop p+1 \right\} = (p+1)\left\{ n \atop p+1 \right\} + \left\{ n \atop p \right\}.$$

qui sont valables pour $(n,p) \in \mathbb{N}^* \times \mathbb{N}^*$.

3. Le principe d'inclusion-exclusion

Soient A et B deux parties finies d'un ensemble. Comme A est la réunion disjointe de $A \cap B$ et de $A \setminus B$ alors

$$\text{Card}\,(A) = \text{Card}\,(A \cap B) + \text{Card}\,(A \setminus B)\,.$$

De même on a

$$\text{Card}\,(B) = \text{Card}\,(A \cap B) + \text{Card}\,(B \setminus A)\,.$$

Mais $A \cup B$ est la réunion disjointe de $A \cap B$, de $A \setminus B$ et de $B \setminus A$ alors

$$\text{Card}\,(A \cup B) = \text{Card}\,(A \cap B) + \text{Card}\,(A \setminus B) + \text{Card}\,(B \setminus A)\,.$$

On conclut que

$$\text{Card}\,(A \cup B) = \text{Card}\,(A) + \text{Card}\,(B) - \text{Card}\,(A \cap B)\,. \tag{20}$$

La relation (20) est un cas particulier du principe d'inclusion-exclusion qui s'énonce de la manière suivante:

$\mathcal{D}_{16}$: *Soit $n \in \mathbb{N}^*$, pour $k \in \mathbb{N}_n$ on note $\mathcal{P}_k^{(n)}$ l'ensemble des parties de $\mathbb{N}_n$ de cardinal k. Soient $(A_k)_{1\leq k\leq n}$ des parties finies d'un ensemble. Alors*

$$\text{Card}\left(\bigcup_{k=1}^{n} A_k\right) = \sum_{k=1}^{n} (-1)^{k-1} \left(\sum_{B\in\mathcal{P}_k^{(n)}} \text{Card}\left(\bigcap_{i\in B} A_i\right)\right)$$

Pour démontrer ce principe nous allons procéder par récurrence sur n. C'est trivialement vrai si $n = 1$, et pour $n = 2$ nous l'avons démontré ; c'est la relation (20). Supposons que $\mathcal{D}_{16}$ est vrai pour un $n \geq 2$.

Soient $(A_k)_{1\leq k\leq n+1}$ des parties finies d'un ensemble. Alors d'après (20) on a

$$\text{Card}\left(\bigcup_{k=1}^{n+1} A_k\right) = \text{Card}\,(A_{n+1}) + \underbrace{\text{Card}\left(\bigcup_{k=1}^{n} A_k\right)}_{\Delta_1} - \underbrace{\text{Card}\left(\bigcup_{k=1}^{n} (A_k \cap A_{n+1})\right)}_{\Delta_2}\,. \tag{21}$$

En utilisant l'hypothèse de récurrence Δ_2 s'écrit

$$\begin{aligned}\Delta_2 &= \sum_{k=1}^{n}(-1)^{k-1}\left(\sum_{B\in\mathcal{P}_k^{(n)}}\text{Card}\left(\bigcap_{i\in B}(A_i\cap A_{n+1})\right)\right)\\ &= \sum_{k=1}^{n}(-1)^{k-1}\left(\sum_{B\in\mathcal{P}_k^{(n)}}\text{Card}\left(\bigcap_{i\in B\cup\{n+1\}}A_i\right)\right)\\ &= \sum_{k=1}^{n}(-1)^{k-1}\left(\sum_{B\in\mathcal{P}_{k+1}^{*(n+1)}}\text{Card}\left(\bigcap_{i\in B}A_i\right)\right)\end{aligned}$$

Où $\mathcal{P}_k^{*(n+1)}$ est l'ensemble des parties de $\mathbb{N}_{n+1}$ de cardinal k et qui contiennent l'élément $n+1$. Donc en effectuant un changement d'indice $k\mapsto k+1$ on trouve

$$\Delta_2 = -\sum_{k=2}^{n+1}(-1)^{k-1}\left(\sum_{B\in\mathcal{P}_k^{*(n+1)}}\text{Card}\left(\bigcap_{i\in B}A_i\right)\right)$$

ou bien

$$\text{Card}\,(A_{n+1})-\Delta_2 = \sum_{k=1}^{n+1}(-1)^{k-1}\left(\sum_{B\in\mathcal{P}_k^{*(n+1)}}\text{Card}\left(\bigcap_{i\in B}A_i\right)\right) \tag{22}$$

D'autre part, si $\mathcal{P}_k^{**(n+1)}$ est l'ensemble des parties de $\mathbb{N}_{n+1}$ de cardinal k et qui ne contiennent pas l'élément $n+1$. Alors $\mathcal{P}_k^{**(n+1)} = \mathcal{P}_k^{(n)}$, d'où Δ_1 s'écrit, en utilisant l'hypothèse de récurrence

$$\Delta_1 = \sum_{k=1}^{n}(-1)^{k-1}\left(\sum_{B\in\mathcal{P}_k^{**(n+1)}}\text{Card}\left(\bigcap_{i\in B}A_i\right)\right) \tag{23}$$

En remarquant que $\mathcal{P}_k^{**(n+1)}\cup\mathcal{P}_k^{*(n+1)} = \mathcal{P}_k^{(n+1)}$, et en remplaçant (22) et (23) dans (21) on trouve

$$\begin{aligned}\text{Card}\left(\bigcup_{k=1}^{n+1}A_k\right) &= \sum_{k=1}^{n}(-1)^{k-1}\left(\sum_{B\in\mathcal{P}_k^{(n+1)}}\text{Card}\left(\bigcap_{i\in B}A_i\right)\right)+(-1)^n\text{Card}\left(\bigcap_{i=1}^{n+1}A_i\right)\\ &= \sum_{k=1}^{n+1}(-1)^{k-1}\left(\sum_{B\in\mathcal{P}_k^{(n+1)}}\text{Card}\left(\bigcap_{i\in B}A_i\right)\right).\end{aligned}$$

ce qui achève la démonstration de $\mathcal{D}_{16}$.

Application : Retour sur les $\left\{ \begin{matrix} n \\ p \end{matrix} \right\}$.

Rappelons que $\mathcal{F}(\mathbb{N}_n, \mathbb{N}_p)$ (resp. $\mathcal{F}_{\rm s}(\mathbb{N}_n, \mathbb{N}_p)$) désigne l'ensemble des fonctions (resp. des fonctions surjectives) de $\mathbb{N}_n$ dans $\mathbb{N}_p$. Pour $k \in \mathbb{N}_p$ on note A_k l'ensemble des fonctions $f \in \mathcal{F}(\mathbb{N}_n, \mathbb{N}_p)$ telles que $k \notin {\rm Im}f$. Alors on a la propriété suivante

$$f \in \mathcal{F}_{\rm s}(\mathbb{N}_n, \mathbb{N}_p) \quad \Longleftrightarrow \quad \mathcal{F}(\mathbb{N}_n, \mathbb{N}_p) \setminus (\bigcup_{k=1}^{p} A_k). \tag{24}$$

Donc notre stratégie consiste à utiliser $\mathcal{D}_{16}$ pour déterminer le cardinal de l'ensemble $A_1 \cup \ldots \cup A_p$.

Pour arriver à notre but nous allons introduire une notation plus générale. Si U est une partie de $\mathbb{N}_p$ on pose A_U pour désigner l'ensemble des fonctions $f \in \mathcal{F}(\mathbb{N}_n, \mathbb{N}_p)$ telles que $U \cap {\rm Im}f = \emptyset$ ou bien ${\rm Im}f \subset \mathbb{N}_p \setminus U$. De telle manière que $A_k = A_{\{k\}}$ et $\bigcap_{i \in B} A_i = A_B$.

Le principe d'inclusion-exclusion s'écrit alors

$$\text{Card } \left(\bigcup_{k=1}^{p} A_k \right) = \sum_{k=1}^{p} (-1)^{k-1} \left(\sum_{B \in \mathcal{P}_k^{(p)}} \text{Card } (A_B) \right).$$

Mais A_B est aussi l'ensemble des applications de $\mathbb{N}_n$ dans $\mathbb{N}_p \setminus B$ donc $\text{Card } (A_B) = (p - \text{Card } (B))^n$, d'où

$$\begin{aligned} \text{Card } \left(\bigcup_{k=1}^{p} A_k \right) &= \sum_{k=1}^{p} (-1)^{k-1} \left(\sum_{B \in \mathcal{P}_k^{(p)}} (p - \text{Card } (B))^n \right) \\ &= \sum_{k=1}^{p} (-1)^{k-1} C_p^k (p-k)^n \end{aligned}$$

En revenant à (24) on trouve

$$\text{Card } (\mathcal{F}_{\rm s}(\mathbb{N}_n, \mathbb{N}_p)) = p^n + \sum_{k=1}^{p} (-1)^k C_p^k (p-k)^n = \sum_{k=0}^{p} (-1)^k C_p^k (p-k)^n.$$

Mais on a vu que Card $(\mathcal{F}_{\mathrm{s}}(\mathbb{N}_n, \mathbb{N}_p)) = p!\left\{ n \atop p \right\}$, d'où

$\mathcal{D}_{17}$: *Pour $(n,p) \in \mathbb{N}^* \times \mathbb{N}^*$, les nombres de Stirling de seconde espèce sont donnés*

$$\left\{ n \atop p \right\} = \begin{cases} 0 & si \quad p > n \\ \dfrac{1}{p!} \displaystyle\sum_{k=0}^{p} (-1)^k C_p^k \, (p-k)^n & si \quad p \leq n \end{cases}$$

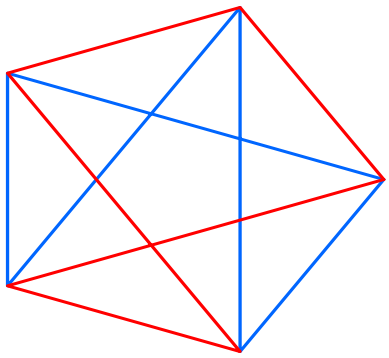
4. Exemples de problèmes faisant appel au dénombrement

1°. Je préfère le rouge.

On se donne A un ensemble de n points sur un cercle, ce qui permet de former C_n^2 segments. Chaque segment est colorié en rouge ou en bleu. *On suppose que chaque triangle formé par trois quelconques des n points a au moins un côté rouge.*

Un cas particulier d'un théorème célèbre de *Ramsey* affirme que pour chaque $m \in \mathbb{N}$ il existe un entier $R(m)$ tel que si $n \geq R(m)$, on trouve une partie B dans A de cardinal m dont tous les segments joignant ses points sont rouges. Ce théorème veut dire que si l'on veut créer du désordre dans la coloration des segments joignant un grand nombre de points, et cela en empêchant la formation de triangles de côtés bleus alors nous n'y arriveront pas car nous allons nous trouver avec des configurations grandes dont tous les segment sont rouges !.

La figure ci-contre montre que l'on doit avoir $R(3) > 5$, car avec $n = 5$ il y a un moyen de colorier les segments joignant les cinq points de telle sorte qu'il n'y ait pas de triangle dont les côtés sont de la même couleur.



Nous n'allons pas démontrer ce résultat qui est trop avancé, mais nous allons seulement voir que l'on peut prendre $R(3) = 6$ et $R(4) = 9$, c'est à dire que si $n = 6$ alors il y a forcément un triangle de côtés rouges et si $n = 9$ alors il y a forcément un quadrilatère de côtés et de diagonales rouges.

Introduisons quelques notations. D'abord, rappelons que $\mathcal{P}_2^{(n)}$ est l'ensemble des parties de $\mathbb{N}_n$ qui sont de cardinal 2. Une Coloration des segments joignant les n points est en fait une application $f : \mathcal{P}_2^{(n)} \longrightarrow \{0, 1\}$ définie par $f(\{i, j\}) = 1$ si le segment joignant le $i^{\text{ième}}$ point au $j^{\text{ième}}$ point est colorié en rouge et $f(\{i, j\}) = 0$ si ce segment est colorié en bleu. On peut prolonger l'application f à $\mathcal{P}^{(n)}$ en posant, pour $B \subset \mathbb{N}_n$, $f(B) = \sum_{S \in \mathcal{P}_2(B)} f(S)$, (bien sûr on convient que $f(B) = 0$ si Card $(B) \leq 1$), $f(B)$ est par conséquent le nombre de segments coloriés en rouge et d'extemités appartenant à B.
Avec la notation précédente, l'hypothèse peut être formulée de la manière suivante:

$$(\mathcal{H}) \qquad \forall\, B \in \mathcal{P}_3^{(n)}, \quad f(B) \geq 1.$$

a. **Cas $n = 6$.**
Considérons l'application

$$\varphi : \mathbb{N}_5 \longrightarrow \{0, 1\} : j \mapsto f(\{j, 6\}).$$

Comme on a Card $\left(\varphi^{-1}(\{0\})\right) + \text{Card}\left(\varphi^{-1}(\{1\})\right) = \text{Card}\,(\mathbb{N}_5) = 5$, alors on distingue deux cas:

I. Card $\left(\varphi^{-1}(\{0\})\right) \geq 3$.

Donc il y a une partie $A = \{\alpha_1, \alpha_2, \alpha_3\}$ de cardinal 3 dans $\mathbb{N}_5$ telle que $f(\{\alpha_1, 6\}) = 0$, $f(\{\alpha_2, 6\}) = 0$ et $f(\{\alpha_3, 6\}) = 0$. Si alors i et j sont deux éléments distincts de $\mathbb{N}_3$, on a

$$\begin{aligned} 1 \leq & f(\{\alpha_i, \alpha_j, 6\}) \\ = & f(\{\alpha_i, 6\}) + f(\{\alpha_j, 6\}) + f(\{\alpha_i, \alpha_j\}) \\ = & f(\{\alpha_i, \alpha_j\}). \end{aligned}$$

D'où $f(\{\alpha_i, \alpha_j\}) = 1$, et $f(\{\alpha_1, \alpha_2, \alpha_3\}) = 3$, c'est le résultat demandé dans ce cas.

II. Card $\left(\varphi^{-1}(\{1\})\right) \geq 3$.

Donc il y a une partie $A = \{\alpha_1, \alpha_2, \alpha_3\}$ de cardinal 3 dans $\mathbb{N}_5$ telle que $f(\{\alpha_1, 6\}) = 1$, $f(\{\alpha_2, 6\}) = 1$ et $f(\{\alpha_3, 6\}) = 1$. Mais d'après l'hypothèse $f(\{\alpha_1, \alpha_2, \alpha_3\}) \geq 1$, il existe deux indices distincts i et j de $\mathbb{N}_3$ tels que $f(\{\alpha_i, \alpha_j\}) = 1$. D'où $f(\{\alpha_i, \alpha_j, 6\}) = 3$, ce qui démontre aussi le résultat dans ce cas.

b. **Cas $n = 9$.**

Pour $k \in \mathbb{N}_9$, on définit l'application

$$\varphi_k : \mathbb{N}_9 \setminus \{k\} \longrightarrow \{0, 1\} : j \mapsto f(\{j, k\}).$$

Distinguons les trois cas suivants:

I. Il existe $k \in \mathbb{N}_9$ tel que Card $\left(\varphi_k^{-1}(\{1\})\right) \geq 6$.
Cela veut dire qu'il existe une partie $A \subset \mathbb{N}_9 \setminus \{k\}$ de cardinal 6 et telle que

$$\forall\, a \in A, \quad f(\{a, k\}) = 1$$

Mais d'après le cas $n = 6$, il existe dans A une partie $B = \{\beta_1, \beta_2, \beta_3\} \subset A$ de cardinal 3 et telle que $f(\{\beta_i, \beta_j\}) = 1$ pour tout couple (β_i, β_j) d'éléments distincts de B. Il en résulte que $f(\{\beta_1, \beta_2, \beta_3, k\}) = 6$ et c'est le résultat cherché.

II. Il existe $k \in \mathbb{N}_9$ tel que Card $\left(\varphi_k^{-1}(\{1\})\right) \leq 4$.
Alors Card $\left(\varphi_k^{-1}(\{0\})\right) \geq 4$, et par conséquent, il existe une partie $A = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ de $\mathbb{N}_9 \setminus \{k\}$ de cardinal 4, telle que

$$\forall\, a \in A, \quad f(\{a, k\}) = 0$$

Si alors i et j sont deux éléments distincts de $\mathbb{N}_4$, on a

$$\begin{aligned} 1 \leq & f(\{\alpha_i, \alpha_j, k\}) \\ = & f(\{\alpha_i, k\}) + f(\{\alpha_j, k\}) + f(\{\alpha_i, \alpha_j\}) \\ = & f(\{\alpha_i, \alpha_j\}). \end{aligned}$$

D'où $f(\{\alpha_i, \alpha_j\}) = 1$ et $f(\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}) = 6$ et c'est le résultat cherché.

III. Quel que soit $k \in \mathbb{N}_9$ on a Card $\left(\varphi_k^{-1}(\{1\})\right) = 5$.

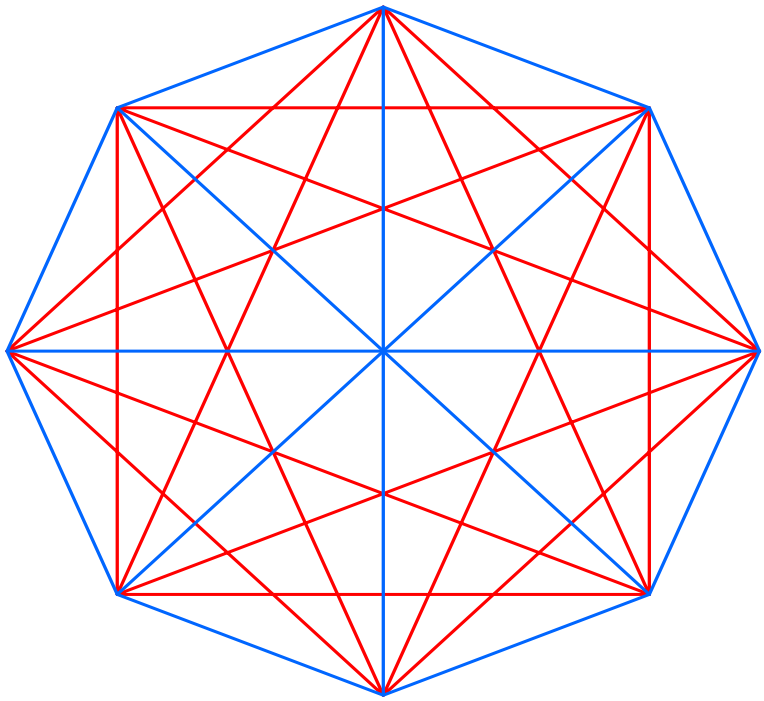
Dans ce cas

$$\begin{aligned} 2 \sum_{\{j,k\} \in \mathcal{P}_2^{(9)}} f(\{j,k\}) &= \sum_{\substack{(j,k) \in \mathbb{N}_9 \times \mathbb{N}_9 \\ j \neq k}} f(\{j,k\}) \\ &= \sum_{k=1}^{9} \left(\sum_{j \in \mathbb{N}_9 \setminus \{k\}} f(\{j,k\}) \right) \\ &= \sum_{k=1}^{9} \text{Card } \left(\varphi_k^{-1}(\{1\})\right) \\ &= 45 \end{aligned}$$

ce qui est contradictoire car 45 n'est pas un nombre pair ! et ce cas ne se produit jamais.

On a donc démontré que l'on peut prendre $R(4) = 9$.

La figure ci-contre montre que l'on doit avoir $R(4) > 8$, car avec $n = 8$ il y a un moyen de colorier les segments joignant les huit points de telle sorte que tout triangle ait au moins un côté rouge et tout quadrilatère ait au moins un côté ou un diagonal blue.



2°. Encore des couleurs.

Nous allons démontrer le résultat suivant:

Théorème.1 : *On se donne $V = \{A_1, \ldots, A_n\}$ un ensemble de n points sur un cercle, ce qui permet de former C_n^2 segments. Supposons que l'on a réussi à colorier ces segments à l'aide de p couleurs de telle manière qu'aucun triangle $A_iA_jA_k$ $(i, j, k$ distincts) n'ait trois côtés de la même couleur. Alors $n \leq E(e\,p!)$, où e est la base du logarithme népérien.*

Pour démontrer ce théorème nous allons commencer par énoncer et démontrer un lemme simple mais très important, qu'on appelle " Le principe des tiroirs de Dirichlet ".

Lemme.2 : *Soient A et B deux ensembles finis, tels que* $\text{Card}\,(A) > (m-1)\,\text{Card}\,(B)$, *$(m \in \mathbb{N}^*)$, et $f : A \longrightarrow B$ une application. Alors il existe une partie C de A telle que* $\text{Card}\,(C) = m$ *et f prend la même valeur sur C.*

Preuve: Notons pour simplifier $C_b = f^{-1}(\{b\})$, et raisonnons par l'absurde. Supposons que l'énoncé n'est pas vrai alors pour tout $b \in B$ on aura $\text{Card}\,(C_b) \leq m-1$. Mais

$$A = \bigcup_{b\in B} C_b, \quad \text{et} \quad C_{b_1} \cap C_{b_2} = \emptyset \quad \text{si } b_1 \neq b_2.$$

Par conséquent

$$\text{Card}\,(A) = \sum_{b\in B} \text{Card}\,(C_b) \leq (m-1)\text{Card}\,(B)\,.$$

ce qui contredit l'hypothèse, et achève la démonstration. □

Remarque: On peut formuler ce lemme en disant: Supposons que nous avions p tiroirs et k objets à mettre dans ces tiroirs. Si $k > (m-1)p$ alors il y a un tiroir qui contient plus que m objets, d'où le nom du lemme.

Avant de commencer la démonstration du théorème.1 nous avons aussi besoin du lemme suivant:

Lemme.3 : *Soit $\lambda : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ une application définie par les relations*

$$\lambda(1) = 2, \qquad \lambda(p+1) = (p+1)\lambda(p) + 1 \quad \textit{pour } p \in \mathbb{N}^*.$$

Alors $\lambda(p) = E(e\,p!)$.

Preuve : Remarquons que la relation définissant λ s'écrit

$$\frac{\lambda(k+1)}{(k+1)!} - \frac{\lambda(k)}{(k)!} = \frac{1}{(k+1)!}.$$

En faisant la somme pour k entre 1 et $p-1$ on trouve $\dfrac{\lambda(p)}{p!} = \displaystyle\sum_{k=0}^{p} \frac{1}{k!}$. D'où

$$\lambda(p) = p! \sum_{k=0}^{p} \frac{1}{k!}.$$

Si l'on pose alors $\mu_n = \sum_{k=0}^{n} \frac{1}{k!}$ et $\nu_n = \sum_{k=0}^{n} \frac{1}{k!} + \frac{1}{n.n!}$, alors il est facile de voir que

$$\mu_n \leq \mu_{n+1} \leq \nu_{n+1} \leq \nu_n \quad \text{pour tout } n.$$

Mais nous savons que $\lim_{n\to\infty} \mu_n = e$. D'où

$$\mu_n < e < \nu_n \quad \text{pour tout } n > 0.$$

Ce qui implique que

$$\lambda(p) < e\,p! < \lambda(p) + \frac{1}{p} \leq \lambda(p) + 1 \quad \text{pour tout } p > 0.$$

Par conséquent $\lambda(p) = E(e\,p!)$. □

Preuve du théorème.1 : Nous allons démontrer par récurrence sur p la propriété suivante:

$$\mathbb{P}_p : \left\{ \begin{array}{l} \text{Si pour un entier naturel } n > 0, \text{ on se donne un ensemble de } n \text{ points} \\ V = \{A_1, \ldots, A_n\} \text{ sur un cercle, et si l'on réussit à colorier les } C_n^2 \\ \text{droites déterminées par ces } n \text{ points à l'aide de } p \text{ couleurs de telle} \\ \text{manière qu'aucun triangle } A_iA_jA_k \ (i,j,k \text{ distincts}) \text{ n'ait trois côtés} \\ \text{de la même couleur. Alors } n \leq \ \lambda(p), \end{array} \right\}$$

Il est immédiat que la propriété $\mathbb{P}_1$ est vraie. Supposons que la propriété $\mathbb{P}_p$ est vraie, et soit $V = \{A_1, \ldots, A_n\}$ un ensemble de n points sur un cercle, avec $n > \lambda(p+1)$. Colorier les C_n^2 droites à l'aide de $p+1$ couleurs revient à donner une application

$$f : \mathcal{P}_2(V) \longrightarrow \mathbb{N}_{p+1}.$$

qui associe à la droite A_iA_j la couleur numéro $f(\{A_i, A_j\})$.

Considérons aussi l'application

$$\varphi : \{A_1, \ldots A_{n-1}\} \longrightarrow \mathbb{N}_{p+1} : A_i \mapsto f(\{A_i, A_n\}).$$

On applique alors le lemme.2 à l'application φ. On a

$$\text{Card } (\{A_1, \ldots A_{n-1}\}) = (n-1) > \lambda(p+1) - 1 = (p+1)\lambda(p) = \lambda(p)\text{Card } (\mathbb{N}_{p+1}) .$$

D'où l'on trouve une partie $\mathcal{C}$ de $\{A_1, \ldots, A_{n-1}\}$ et un entier $k \in \mathbb{N}_{p+1}$ tels que Card $(\mathcal{C}) = \lambda(p) + 1$ et $f(\{C, A_n\}) = k$ pour tout $C \in \mathcal{C}$.

Distinguons alors deux cas:

I. Les couleurs de toutes les droites déterminées par les points de $\mathcal{C}$ sont différentes de k. (*i.e.* $\forall \{C_1, C_2\} \in \mathcal{P}_2(\mathcal{C})$, $f(\{C_1, C_2\}) \neq k$).
On applique alors l'hypothèse de récurrence $\mathbb{P}_p$ à l'ensemble $\mathcal{C}$ qui a $n' = \lambda(p)+1 > \lambda(p)$ points et aux p couleurs numérotées par $\mathbb{N}_{p+1} \setminus \{k\}$, on en déduit qu'il y a un triangle de sommets dans $\mathcal{C}$ et dont les trois côtés sont de la même couleur.

II. Il y a deux points $\{C_1, C_2\} \in \mathcal{P}_2(\mathcal{C})$ tels que $f(\{C_1, C_2\}) = k$. Mais alors les côtés du triangle $C_1C_2A_n$ sont de la même couleur.

Récapitulons, On a démontré que si $n > \lambda(p+1)$, alors on trouve un triangle dont les côtés sont de la même couleur. Ceci démontre $\mathbb{P}_{p+1}$ et achève la preuve. □

EXERCICES

EXERCICE .1 On considère dans un plan, un polygône convexe de n sommets. Trouver, en se limitant au cas le plus général, le nombre des points d'intersection des segments diagonaux.

EXERCICE .2 Soit $\mathcal{P}^{(n)}$ l'ensemble des parties de $\mathbb{N}_n$. Calculer

$$\sum_{X\in\mathcal{P}^{(n)}} \text{Card}\,(X)\,; \qquad \sum_{(X,Y)\in\mathcal{P}^{(n)}\times\mathcal{P}^{(n)}} \text{Card}\,(X\cap Y)\,; \qquad \sum_{(X,Y)\in\mathcal{P}^{(n)}\times\mathcal{P}^{(n)}} \text{Card}\,(X\cup Y)\,.$$

EXERCICE .3 Sur les trois axes d'un repère affine $(O, \overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k})$, on considère les points A, B, C définis par $\overrightarrow{OA} = n\overrightarrow{i}$, $\overrightarrow{OB} = n\overrightarrow{j}$, et $\overrightarrow{OC} = n\overrightarrow{k}$, $(n \in \mathbb{N})$. Calculer le nombre des points à coordonnées entières à l'intérieur du tétraèdre $OABC$.

EXERCICE .4 Calculer le cardinal de l'ensemble

$$\left\{(x_1,\ldots,x_n)\in\{-1,0,1\}^n : \sum_{k=1}^{n} x_k = 0\right\}.$$

EXERCICE .5 Soit n un entier strictement positif. On note $P_k^{(n)}$ l'ensemble des parties de $\mathbb{N}_n$ qui sont de cardinal k.

1°. *a.* Montrer par récurrence sur n que pour tout $a_1, a_2, \ldots, a_n$ dans $\mathbb{R}$, et pour tout $x \in \mathbb{R}$, l'on a

$$\prod_{k=1}^{n}(1+xa_k) = 1+\sum_{k=1}^{n}\Big(\sum_{B\in P_k^{(n)}}\prod_{i\in B} a_i\Big)x^k.$$

b. En déduire une expression de $\displaystyle\prod_{k=1}^{n}(1-a_k)$.

2°. Soient E un ensemble fini, $\mathcal{P}(E)$ l'ensemble des parties de E. On considère aussi $\mathcal{F}$ l'ensemble des fonctions $f : E \longrightarrow \{0,1\}$. À une partie $A \subset E$ on associe l'élément Γ_A de $\mathcal{F}$ défini par $\Gamma_A(x) = \begin{cases} 1 & \text{si} \quad x \in A \\ 0 & \text{si} \quad x \notin A \end{cases}$.

a. Montrer que l'application $\Gamma : \mathcal{P}(E) \longrightarrow \mathcal{F} : A \mapsto \Gamma_A$ est une bijection.

b. Montrer que

$\Gamma_{A\cap B} = \Gamma_A.\Gamma_B$.

$\Gamma_{E\setminus A} = 1 - \Gamma_A$.

$\Gamma_{A\cup B} = \Gamma_A + \Gamma_B - \Gamma_A.\Gamma_B$.

c. Soient $A_1, A_2, \ldots, A_n$ des parties de E, On note $A = \bigcup_{k=1}^{n} A_k = A_1 \cup A_2 \cup \cdots \cup A_n$. Montrer $\Gamma_A = 1 - \prod_{k=1}^{n}(1 - \Gamma_{A_k})$. En déduire que

$$\Gamma_A = \sum_{k=1}^{n}(-1)^{k-1}\left(\sum_{B \in P_k^{(n)}} \prod_{i \in B} \Gamma_{A_i}\right)$$

.

d. Soit $A \subset E$, montrer que $\operatorname{Card} A = \sum_{x \in E} \Gamma_A(x)$.

e. Déduire de ce qui précède que, si $A_1, A_2, \ldots, A_n$ sont des parties de E, alors

$$\operatorname{Card}\left(\bigcup_{k=1}^{n} A_k\right) = \sum_{k=1}^{n}(-1)^{k-1}\left(\sum_{B \in P_k^{(n)}} \operatorname{Card}\left(\bigcap_{i \in B} A_i\right)\right).$$

3°. Soient $B \subset \mathbb{N}_n$ une partie de cardinal k, $\mathcal{S}(n)$ l'ensemble des bijections de $\mathbb{N}_n$. Montrer que $\operatorname{Card}\left(\{\sigma \in \mathcal{S}(n) \ : \ \forall\, i \in B, \quad \sigma(i) = i\}\right) = (n-k)!$.

4°. Pour $j \in \mathbb{N}_n$ on note A_j l'ensemble des $\sigma \in \mathcal{S}(n)$ qui laissent fixe l'élément j: $A_j = \{\sigma \in \mathcal{S}(n) : \sigma(j) = j\}$. Montrer que $\operatorname{Card}\left(\bigcup_{k=1}^{n} A_k\right) = n!\left(\sum_{k=1}^{n} \frac{(-1)^{k-1}}{k!}\right)$.

5°. Soit $G_n = \{\sigma \in \mathcal{S}(n) \ : \ \forall\, j \in \mathbb{N}_n, \quad \sigma(j) \neq j\}$. On note g_n le nombre d'éléments de G_n. Exprimer G_n en fonction de $\mathcal{S}(n)$ et des ensembles $\{A_k\}_{1 \leq k \leq n}$ de la question précédente. En déduire que $g_n = n!\left(\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right)$.

6°. On note $a_n = \sum_{k=0}^{n} \frac{(-1)^k}{k!}$.

a. Montrer que, pour tout $n \geq 1$, $a_{2n-1} \leq a_{2n+1} \leq a_{2n} \leq a_{2n-2}$.

b. En déduire que la suite $(a_n)_{n \geq 1}$ converge vers une limite λ.(On ne demande pas de déterminer λ)

c. Montrer que si n est *pair* alors $0 \leq g_n - \lambda(n!) \leq \frac{1}{n+1}$.

d. Montrer que si n est *impair* alors $0 \leq \lambda(n!) - g_n \leq \frac{1}{n+1}$.

e. En déduire que, pour tout $n \geq 1$,$g_n = E\left(\frac{n!}{e}\right) + \frac{1 + (-1)^n}{2}$. On admettra que $\lambda = 1/e$.

EXERCICE .6 Soient $A_1, \ldots, A_{1066}$, 1066 sous-ensembles d'un ensemble X. On suppose que pour chaque i, $(1 \leq i \leq 1066)$, le cadinal de A_i dépasse strictement la moitié du cardinal de X. Montrer que l'on peut trouver une partie B de X telle que

$$\operatorname{Card}(B) \leq 10, \quad A_i \cap B \neq \emptyset \quad \text{pour } i \in \mathbb{N}_{1066}.$$

EXERCICE .7 Soient $n \in \mathbb{N}^*$ et $r \in \mathbb{N}_n$. On note $f(r,n)$ la moyenne arithemétique du minimum de B lorsque B parcourt l'ensemble des parties de $\mathbb{N}_n$ à r éléments. Exprimer simplement $f(r,n)$ en fonction de n et de r.

EXERCICE .8 Soit $F : \mathbb{R}_+^* \longrightarrow \mathbb{R}$ une fonction de classe C^n ($n \geq 1$). On pose pour $t \in \mathbb{R}$, $g(t) = F(e^t)$. Montrer que, pour $t \in \mathbb{R}$,

$$g^{(n)}(t) = \sum_{k=1}^{n} \left\{ {n \atop k} \right\} F^{(k)}(e^t)\, e^{kt}.$$

La divisibilité dans $\mathbb{Z}$

1. Généralités

Nous allons dans ce chapitre étudier quelques poropriétés de base des nombres entiers relatifs dont l'ensemble est noté habituellement $\mathbb{Z}$.

Soient a et b deux nombres entiers. On dit que " a est un multiple de b " si, et seulement si $a = bc$ pour un certain nombre entier c. Par exemple 12 est un multiple de 3, et -15 est multiple de 5.

La relation inverse est celle de la divisibilité. Dire que " b divise a" est équivalent à dire que " a est un multiple de b ". D'où la définition:

Définition: Pour tout $(a, b) \in \mathbb{Z}^2$, on dit que b **divise** a (et on note $b \,|\, a$) si, et seulement si, il exite $c \in \mathbb{Z}$ tel que $a = bc$.

Voici deux propriétés simples :

- ◇ Si $(a, b) \in \mathbb{Z}^2$ alors $(a \,|\, b \text{ et } b \,|\, a) \implies a \in \{b, -b\}$.

  C'est immédiat et laissé en exercice au lecteur.

- ◇ Si $(a, b) \in \mathbb{Z}^2$ avec $b \neq 0$ alors il existe un couple unique $(q, r) \in \mathbb{Z} \times \mathbb{Z}$, tel que

$$a = qb + r \quad \text{avec} \quad 0 \leq r < |b| \tag{$\mathcal{E}$}$$

  où $|b|$ est la valeur absolue de b. q est appelé le *quatient de la division de a par b*, et r est appelé le *reste de la division de a par b*. Obtenir (q, r) à partir de (a, b) s'appelle *division euclidienne*.

  Démontrons d'abord l'unicité. Supposons que

$$a = qb + r = q'b + r' \quad \text{avec} \quad 0 \leq r < |b|\,,\ 0 \leq r' < |b|\,.$$

Alors $(q-q')\,b=(r'-r)\in]-|b|\,,|b|\,[$, ce qui montre, en prenant la valeur absolue et en divisant par $|b|$, que: $|\,q-q'|\in\mathbb{Z}\cap[0,1[$ c'est-à-dire $|\,q-q'|=0$ ou bien $q=q'$ et par conséquent $r=r'$.

Pour démontrer l'existence du couple (q,r), distinguons deux cas:

1°. $b>0$, dans ce cas

$$E\left(\frac{a}{b}\right)\leq\frac{a}{b}<E\left(\frac{a}{b}\right)+1,$$

d'où

$$bE\left(\frac{a}{b}\right)\leq a<bE\left(\frac{a}{b}\right)+b,$$

soit

$$0\leq a-bE\left(\frac{a}{b}\right)<b.$$

On prend alors $q=E(a/b)$ et $r=a-bE(a/b)$.

2°. $b<0$, alors $-b>0$ donc d'après ce qui précède on trouve $(\widetilde{q},r)\in\mathbb{Z}^2$ tels que $a=\widetilde{q}\,(-b)+r$ avec $0\leq r<|b|$. Si l'on pose alors $q=-\widetilde{q}$ on trouve $a=qb+r$ avec $0\leq r<|b|$. □

Remarque: Si $(a,b)\in\mathbb{Z}\times\mathbb{Z}^*$, alors $b\,|\,a$ si, et seulement si, le reste de la division de a par b est nul.

2. Le plus grand commun diviseur

Commençons par une définition importante.

Définition : Soient a et b deux entiers relatifs, *non tous les deux nuls*. On appelle le plus grand commun diviseur de a et b, (et on note PGCD (a,b)), le plus grand entier de l'ensemble $\{d:\,d\,|\,a\quad\text{et}\quad d\,|\,b\}$.

$$\text{PGCD}\,(a,b)=\max\{d:\,d\,|\,a\quad\text{et}\quad d\,|\,b\}.$$

Remarquons que l'on a toujours PGCD $(a,b)=$ PGCD (b,a) et $1\leq$ PGCD $(a,b)\leq\min(|a|\,,|b|)$, pour tout couple (a,b) d'entiers non nuls.

Par exemple PGCD $(15,9)=3$ et PGCD $(45,-30)=15$.

Soit $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$. On dit que a *et* b *sont premiers entre eux* si, et seulement si, Pgcd $(a,b) = 1$.

Nous allons maintenant démontrer que le Pgcd $(,)$ peut être exprimé d'une manière très utile pour l'étude de cette fonction.

Théorème.1 : (Théorème de Bezout).*Soit* $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$. *Alors il existe deux enties relatifs* $(x,y) \in \mathbb{Z}^2$ *tels que*

$$d = \text{Pgcd } (a,b) = xa + yb.$$

Preuve : Nous démontrons ce résultat en étudiant l'ensemble S de toutes les combinaisons linéaires de a et b à coefficients entiers:

$$S = \left\{au + bv : (u,v) \in \mathbb{Z}^2\right\}.$$

Par définition, d divise a et d divise b donc d divise tous les éléments de S c'est-à-dire

$$S \subset d\mathbb{Z} = \{dk : k \in \mathbb{Z}\}.$$

Pour démontrer le résultat il nous suffit de montrer que $d \in S$.

Comme $a^2 + b^2 \in S$, l'intersection $S \cap \mathbb{N}^*$ n'est pas vide, on pose alors

$$s = \min S \cap \mathbb{N}^*.$$

On a $s = au_0 + bv_0 \in \mathbb{N}^*$. Soit $c \in S$, alors $c = au + bv$. Effectuons la division euclidienne de c par s, on trouve q et r tels que $c = qs + r$ avec $0 \leq r < s$.

Alors

$$r = c - qs = a(u - qu_0) + b(v - qv_0) \in S.$$

On déduit que r est un élément positif de S strictement plus petit que s, mais la définition de s montre alors que l'on doit avoir $r = 0$ et par conséquent $c = sq$ ou bien que $s \mid c$. On a donc prouvé que s divise tous les éléments de S. En particulier s divise a et b. D'où $s \leq d$. D'autre part s est un élément de S donc c'est un multiple de d et $s \geq d$. On conclut que $s = d$ et par conséquent $d \in S$. □

Voici quelques corollaires de ce théorème.

Corollaire.2 : *Soient* $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ *et* $d = \text{PGCD}\ (a,b)$. *Alors*

$$\left\{xa + yb : \ (x,y) \in \mathbb{Z}^2\right\} = \{dk : \ k \in \mathbb{Z}\}.$$

Corollaire.3 : *Soient* $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ *et* $d = \text{PGCD}\ (a,b)$. *Alors tout diviseur de* a *et de* b *est un diviseur de* d.

Corollaire.4 : *Soit* $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$. *Alors* a *et* b *sont premiers entre eux si, et seulement si, il existe deux enties relatifs* $(x,y) \in \mathbb{Z}^2$ *tels que* $1 = xa + yb$.

Nous laissons la preuve de ces corollaires comme exercice au lecteur.

Corollaire.5 : (Lemme de Gauss).*Soient* a, b *deux entiers non tous les deux nuls et* c *un entier. On suppose que*

- ◇ a *et* b *sont premiers entre eux,i.e.* $\text{PGCD}\ (a,b) = 1$.
- ◇ b *divise* ac,*i.e.* $b \mid ac$.

Alors b *divise* c.

Preuve : On sait d'après le théorème de Bezout qu'il existe deux entiers x et y tels que $ax + by = 1$. Alors $acx + bcy = c$. Maintenant, par hypothèse $b \mid (ac)$, donc $b \mid (acx)$ et bien sûr $b \mid (bcy)$, et par conséquent b divise la somme de ces deux, qui vaut c. □

Corollaire.6 :*Soient* a, b_1 *et* b_2 *des entiers. On suppose que*

- ◇ a *et* b_1 *sont premiers entre eux,i.e.* $\text{PGCD}\ (a,b_1) = 1$.
- ◇ a *et* b_2 *sont premiers entre eux,i.e.* $\text{PGCD}\ (a,b_2) = 1$.

Alors a *et* b_1b_2 *sont aussi premiers entre eux.*

Preuve : L'hypothèse se traduit, d'après le corollaire.4, par l'existence de x_1, x_2, y_1 et y_2 tels que $x_1a + y_1b_1 = 1$ et $x_2a + y_2b_2 = 1$.

D'où, par multiplication membre à membre: $xa+yb_1b_2 = 1$ avec $x = x_1x_2a+x_1y_2b_2+x_2y_1b_1$ et $y = y_1y_2$, ce qui, d'après le corollaire.4, montre que a et b_1b_2 sont premiers entre eux. □

Nous laissons en exercice au lecteur, la généralisation du corollaire.6, où l'on remplace b_1, b_2 par $b_1, b_2, \ldots, b_n$, à démontrer par récurrence.

Corollaire.7 : *Soient a, b_1 et b_2 des entiers. On suppose que*

- ◇ *b_1 et b_2 divisent a,i.e. $b_1 \mid a$ et $b_2 \mid a$.*
- ◇ *b_1 et b_2 sont premiers entre eux,i.e.* $\text{PGCD}\ (b_1, b_2) = 1$.

Alors $b_1 b_2$ divise a.

Preuve : On écrit $a = b_1 c_1$; b_2 divisant $b_1 c_1$ et étant premier avec b_1, il divise c_1, (d'après le lemme de Gauss). Par conséquent $c_1 = b_2 c_2$ et $a = b_1 b_2 c_2$. □

Nous allons Maintenant présenter *l'algorithme d'Euclide* qui permet de calculer le plus grand commun diviseur de deux entiers. Cet algorithme est basé sur le lemme suivant:

Lemme.8 : *Soient $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}$. Alors pour tout $\lambda \in \mathbb{Z}$ on a*

$$\text{PGCD}\ (a, b) = \text{PGCD}\ (a, b - \lambda a)\,.$$

Preuve : Notons $\delta = \text{PGCD}\ (a, b)$ et $\Delta = \text{PGCD}\ (a, b - \lambda a)$. Comme δ divise a et b alors il divise a et $b - \lambda a$, donc $\delta \mid \Delta$. On démontre de même que $\Delta \mid \delta$. D'où $\delta = \Delta$. □

Décrivons l'algorithme d'Euclide qui permet le calcul de $d = \text{PGCD}\ (a, b)$ où $0 < b < a$, (Notons que cela suffit car $\text{PGCD}\ (a, b) = \text{PGCD}\ (|a|, |b|) = \text{PGCD}\ (|b|, |a|)$). On définit par récurrence la suite $(r_k)_{k \in \mathbb{N}}$ en posant

$$r_0 = a, \quad r_1 = b, \quad r_{k+1} = \begin{cases} \text{le reste de la division de } r_{k-1} \text{ par } r_k, & \text{si} \quad r_k > 0. \\ 0, & \text{si} \quad r_k = 0. \end{cases}$$

Si pour tout $k \in \mathbb{N}_{b+1}$ on a $r_k > 0$, alors la définition de r_{k+1} à partir de r_{k-1} et r_k montre que, pour $1 \leq k \leq b$, $r_{k+1} < r_k$. Il en résult que, pour tout $k \in \mathbb{N}_b$, $r_k - r_{k+1} \geq 1$. En faisant la somme de ces inégalités entre $k = 1$ et $k = b$ on trouve $b - r_{b+1} \geq b$ c'est-à-dire $r_{b+1} \leq 0$ ce qui est absurde. De cette contradiction on déduit qu'il existe un entier $p \in \mathbb{N}_{b+1}$ tel que $r_p = 0$. On peut alors considérer

le premier indice n tel que $r_n \neq 0$ et $r_{n+1} = 0$.

(On sait d'après ce qui précède que $n \leq b$). On a alors le fait suivant:

$$r_n = \text{PGCD}\ (a, b)\,.$$

En effet, pour $1 \leq k \leq n$, on a $r_{k-1} = q_k r_k + r_{k+1}$, ce qui s'écrit $r_{k+1} = r_{k-1} - q_k r_k$ et en utilisant le lemme.8 on trouve

$$\begin{aligned} \text{PGCD}\ (r_k, r_{k-1}) &= \text{PGCD}\ (r_k, r_{k-1} - q_k r_k) \\ &= \text{PGCD}\ (r_k, r_{k+1}) = \text{PGCD}\ (r_{k+1}, r_k)\,. \end{aligned}$$

Il en résulte que PGCD (r_k, r_{k-1}) ne dépend pas de k lorsque ce dernier varie entre 1 et n, d'où

$$\text{PGCD}\ (a,b) = \text{PGCD}\ (r_1, r_0) = \cdots = \text{PGCD}\ (r_{n+1}, r_n) = \text{PGCD}\ (0, r_n) = r_n.$$

Le tableau suivant résume cet algorithme:

k	1		2		$\cdots$	$n-1$		n
r_{k-1}	a		b		$\cdots$	r_{n-2}		r_{n-1}
		$\nearrow$		$\nearrow$			$\nearrow$	
r_k	b		r_2		$\cdots$	r_{n-1}		$r_n = d$
		$\nearrow$		$\nearrow$			$\nearrow$	
r_{k+1}	r_2		r_3		$\cdots$	r_n		0

Voici un exemple de ce calcul pour déterminer le plus grand commun diviseur de 5313 et 2047.

k	1	2	3	4	5	6
r_{k-1}	5313	2047	1219	828	391	46
r_k	2047	1219	828	391	46	$\boxed{23}$
r_{k+1}	1219	828	391	46	23	0

Supposons maintenant que l'on cherche à trouver deux entiers x et y tels que $23 = 5313x + 2047y$. On sait, d'après le théorème de Bezout, que de tels entiers existent mais comment les trouver ? Nous allons, dans ce qui suit, présenter une variante de l'algorithme d'Euclide qui permet de trouver ces entiers.

Supposons toujours que l'on se donne $(a,b) \in \mathbb{N}^2$ avec $b < a$. On définit, comme dans l'algorithme d'Euclide, la suite (r_k) dont le dernier terme non nul est $r_n = d$. Si $k \in \mathbb{N}_n$, on peut définir aussi q_k le quotient de la division euclidienne de r_{k-1} par r_k, *i.e.* $r_{k-1} = q_k r_k + r_{k+1}$.

On définit aussi deux suites d'entiers $(t_k)_{0\leq k\leq n}$ et $(s_k)_{0\leq k\leq n}$. En utilisant les relations

$$t_0 = 1, \quad t_1 = 0, \quad t_{k+1} = t_{k-1} - q_k t_k.$$

$$s_0 = 0, \quad s_1 = 1, \quad s_{k+1} = s_{k-1} - q_k s_k.$$

Avec ces suites ainsi définies, on a $d = r_n = t_n a + s_n b$. On peut donc prendre $x = t_n$ et $y = s_n$.

En effet ceci résulte du fait suivant, que nous allons démontrer par récurrence sur k.

$$\forall\, k \in \{0, 1, 2, \ldots, n\}, \quad r_k = t_k a + s_k b.$$

Si k vaut 0 ou 1 c'est immédiat. Supposons que la relation est vraie pour tout $j \leq k$,(avec $k \geq 1$), alors

$$\begin{aligned} r_{k+1} =& r_{k-1} - q_k r_k = (t_{k-1}a + s_{k-1}b) - q_k(t_k a + s_k b) \\ =& (t_{k-1} - q_k t_k)a + (s_{k-1} - q_k s_k)b = t_{k+1}a + s_{k+1}b. \end{aligned}$$

Nous allons illustrer ces calculs en cherchant x et y qui vérifient $23 = 5313x + 2047y$, et en présentant les valeurs intermédiaires des différentes suites dans un tableau.

k	r_k	q_k	t_k	s_k
0	5313		1	0
1	2047	2	0	1
2	1219	1	1	-2
3	828	1	-1	3
4	391	2	2	-5
5	46	8	-5	13
6	$\boxed{23}$		$\boxed{42}$	$\boxed{-109}$
7	0			

Alors $23 = 42 \times 5313 - 109 \times 2047$.

Remarque: Supposons que $d = \text{Pgcd}\ (a, b) = ax_0 + by_0$. Le couple (x_0, y_0) n'est pas unique. En effet, commençons par diviser les deux membres de cette égalité par d, on obtient $1 = a'x_0 + b'y_0$, (où $a = da'$ et $b = db'$). En particulier $\text{Pgcd}\ (a', b') = 1$.
Si $(x, y) \in \mathbb{Z}^2$ vérifie $d = ax + by$, alors $1 = a'x + b'y$. Ceci implique

$$(x - x_0)\, a' = (y_0 - y)\, b'. \tag{1}$$

On en déduit que $b' \mid (x - x_0)\, a'$ et a' et b' sont premiers entre eux. Donc, d'après le corollaire.5, b' divise $x - x_0$. Par conséquent, il existe $\lambda \in \mathbb{Z}$ tel que $x = x_0 + \lambda b'$, et en revenant à (1) on trouve aussi $y = y_0 - \lambda a'$. On a donc démontré que

$$\{(x, y) \in \mathbb{Z}^2 :\ ax + by = d\} \subset \{(x_0 + \lambda b', y_0 - \lambda a') \in \mathbb{Z}^2 :\ \lambda \in \mathbb{Z}\}.$$

L'inclusion inverse est plus facile à prouver et elle est laissée au lecteur. D'où :

Proposition.9 : *Soient* $(a,b) \in \mathbb{Z}^2$ *non tous les deux nuls et* $d = \text{PGCD}\,(a,b)$, *et soit* $(x_0,y_0) \in \mathbb{Z}^2$ *une solution de* $d = ax_0 + by_0$. *Alors*

$$\{(x,y) \in \mathbb{Z}^2 : ax+by=d\} = \{(x_0+\lambda b', y_0-\lambda a') \in \mathbb{Z}^2 : \lambda \in \mathbb{Z}\} \quad \text{où } a=da' \text{ et } b=db'.$$

3. Le plus petit commun multiple

C'est une notion moins importante que celle du plus grand commun diviseur, et elle est liée à cette dernière.

Définition : Soient a et b deux entiers relatifs, *non nuls*. On appelle le plus petit commun multiple de a et b, (et on note $\text{PPCM}\,(a,b)$), le plus petit entier de l'ensemble $\{m \in \mathbb{N}^* : a \,|\, m \quad \text{et} \quad b \,|\, m\}$.

$$\text{PPCM}\,(a,b) = \min\{m \in \mathbb{N}^* : a \,|\, m \quad \text{et} \quad b \,|\, m\}.$$

Remarquons que l'on a toujours $\max(|a|,|b|) \leq \text{PPCM}\,(a,b)$, et $\text{PPCM}\,(a,b) = \text{PPCM}\,(b,a)$ pour tout couple (a,b) d'entiers non nuls.

Par exemple $\text{PPCM}\,(15,9) = 45$ et $\text{PPCM}\,(45,-30) = 90$.
Le théorème suivant montre un lien important entre le PGCD et le PPCM.

Théorème.10 : *Soient* a *et* b *deux entiers strictement positifs,* $\delta = \text{PGCD}\,(a,b)$ *et* $\mu = \text{PPCM}\,(a,b)$. *Alors* $\delta\mu = ab$.

Preuve : Définissons a' et b', premiers entre eux par $a = \delta a'$ et $b = \delta b'$. Le produit $a'b'\delta$ est égal à $ab' = ba'$ donc c'est un multiple commun de a et de b ; on a donc $\mu \leq a'b'\delta$.
Inversement, en écrivant $\mu = xa$ et $\mu = yb$ on a une égalité de la forme $xa = yb$ ou $xa' = yb'$, (en simpifiant par δ). Comme $\text{PGCD}\,(a',b') = 1$, on peut écrire, d'après le lemme de Gauss $y = ka'$; d'où $\mu = ka'b$ ou $\mu = ka'b'\delta$, ce qui implique $\mu \geq a'b'\delta$. Alors $\mu = a'b'\delta$, ce qui donne $\delta\mu = ab$. □

4. Les nombres premiers

Nous allons maintenant étudier les *nombres premiers* et leurs propriétés simples.

Définition : Un **nombre premier** est un entier p strictement plus grand que 1, dont les seules diviseurs sont $\{1, -1, p, -p\}$. On note $\mathcal{P}$ l'ensemble des nombres premiers. Ainsi 2 est le plus petit élément de $\mathcal{P}$.

Les nombres premiers ont fasciné les mathématiciens depuis le temps d'Euclide (et peut-être même avant lui). Ils ont une distribution très irrégulière dans l'ensemble des entiers naturels. Un problème très célèbre, posé depuis l'antiquité et reste toujours sans solution, est de savoir s'il y a une infinité de nombres premiers jumeaux. (*i.e.* $(p, p+2) \in \mathcal{P} \times \mathcal{P}$, par exemple $(3, 5)$, $(5, 7)$ et $(11, 13)$).

Voici quelques propriétés élémentaires :

- ◇ Soient $p \in \mathcal{P}$, et $n \in \mathbb{Z}$. Alors ou bien p et n sont premiers entre eux, ou bien p divise n.

  Car Pgcd (p, n) est un diviseur de p.

- ◇ Soient a et b deux entiers relatifs, et p un nombre premier. Si $p \,|\, ab$, alors $p \,|\, a$ ou $p \,|\, b$.

  Car, d'après le point précédent, si $p \not| a$, (*i.e.* p ne divise pas a), alors p est premier avec a et le lemme de Gauss montre par conséquent que $p \,|\, b$.

- ◇ Soient $q_1, \ldots, q_r$ et p des nombres premiers, (avec $r \geq 1$). Alors $p \,|\, q_1.q_2 \cdots q_r$ si, et seulement si, il existe k tel que $p = q_k$.

  C'est immédiat d'après les deux points précédents.

Le théorème suivant montre la propriété de base qui donne aux nombres premiers leur importance.

Théorème.11 : *Tout entier naturel $n \geq 2$ est le produit de nombres premiers. Plus précisément, Si $n \geq 2$, alors il existe des nombres premiers $p_1, p_2, \ldots, p_r$, (avec $r \geq 1$), tels que*

$$n = p_1 p_2 \ldots p_r. \tag{2}$$

De plus cette décomposition est unique à l'ordre des facteurs près.

Preuve : Commençons par l'existence, et raisonnons par l'absurde. Supposons qu'il y ait un nombre entier naturel $m \geq 2$ qui ne s'écrive pas sous la forme (2). On définit alors m_0 comme le plus petit entier, plus grand que 2, et qui ne s'écrit pas sous la forme (2), alors evidemment $m_0 \notin \mathcal{P}$, ce qui se traduit par l'existence de deux entiers a et b

tels que $1 < a < m_0$, $1 < b < m_0$ et $m_0 = ab$. Mais $1 < a < m_0$ implique, avec la définition de m_0, l'existence de nombres premiers $p_1, p_2, \ldots, p_r$, tels que $a = p_1 p_2 \ldots p_r$. De même, il existe des nombres premiers $q_1, q_2, \ldots, q_s$, tels que $b = q_1 q_2 \ldots q_s$. Par conséquent $m_0 = ab = p_1 p_2 \ldots p_r q_1 q_2 \ldots q_s$, ce qui est contradictoire avec la définition de m_0. D'où l'existence.

Pour l'unicité, nous allons, comme avant, raisonner aussi par l'absurde. Supposons l'existence d'entiers plus grands que 2 et pour lesquels la factorisation n'est pas unique à l'ordre près ; et soit n_0 le plus petit entier, plus grand que 2, et admettant deux factorisations distinctes: $n_0 = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$. Comme $p_1 \,|\, (q_1 q_2 \ldots q_s)$ alors p_1 doit être égal à l'un des $q_1, q_2, \ldots, q_s$, donc quitte à permuter les indices on peut supposer que $p_1 = q_1$. Alors, si l'on pose

$$n_1 = p_2 \ldots p_r = q_2 \ldots q_s$$

on aura, ou bien $n_1 = 1$ est divisible par l'un des nombres premiers $p_2, \ldots, p_r, q_2, \ldots, q_s$ ce qui absurde, ou bien $2 \leq n_1 < n_0$ et n_1 admet deux décompositions différentes en produit de nombres premiers ce qui, à son tour, contredit la minimalité de n_0. Cette contradiction achève la démonstration et prouve le théorème. □

Ce théorème nous permet d'écrire tout entier $n \geq 2$ d'une manière unique sous la forme

$$n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r}.$$

où $r \geq 1$, les $p_1, \ldots, p_r$ sont des nombres premiers *distincts*, et $\nu_k \in \mathbb{N}^*$. Par exemple

$$24 = 2^3 \cdot 3, \quad 30 = 2^1 \cdot 3^1 \cdot 5^1, \quad 22\,408\,353 = 3^3 \cdot 11^2 \cdot 19^3.$$

Nous pouvons pousser cette idée encore plus loin, en disant que tout entier $n \in \mathbb{N}^*$ s'écrit d'une manière unique sous la forme

$$n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$$

où le produit s'étend sur tous les nombres premiers, et $\nu_p(n) = 0$ pour tout $p \not| n$, (bien sûr $p^0 = 1$). Le produit est, par conséquent, un produit fini de termes différents de 1 multiplié par un produit de 1s (qui vaut 1).

Avec cette notation commode nous pouvons énoncer la proposition suivante:

Proposition.12 : *Pour tout* $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$, *on a*

$$\text{Pgcd } (a,b) = \prod_{p\in\mathcal{P}} p^{\min(\nu_p(a),\nu_p(b))}, \quad \text{Ppcm } (a,b) = \prod_{p\in\mathcal{P}} p^{\max(\nu_p(a),\nu_p(b))}$$

Nous laissons la démonstration de cette proposition comme exercice au lecteur.

Théorème.13 : *Il y a une infinité de nombres premiers, (*Card $(\mathcal{P}) = +\infty$*).*

Preuve : En effet, s'il n'y a qu'un nombre fini n de nombres premiers ; $\mathcal{P} = \{p_1, \ldots, p_n\}$. Alors le nombre $P = 1+p_1p_2\cdots p_n$ doit être divisible par un élément p_k de $\mathcal{P}$; par conséquent $p_k \mid P$ et $p_k \mid (P-1)$, d'où $p_k \mid 1$. ce qui est une contradiction. □

5. Le théorème des nombres premiers

Avant d'entrer dans le vif du sujet nous allons étudier une question amusante et classique : "Par combien de zéros se termine l'écriture décimale de (200!) ?".

Bien sûr, on peut calculer 200! et puis compter ensuite les zéros :

200! =788 657 867 364 790 503 552 363 213 932 185 062 295 135 977
687 173 263 294 742 533 244 359 449 963 403 342 920 304 284
011 984 623 904 177 212 138 919 638 830 257 642 790 242 637
105 061 926 624 952 829 931 113 462 857 270 763 317 237 396
988 943 922 445 621 451 664 240 254 033 291 864 131 227 428
294 853 277 524 242 407 573 903 240 321 257 405 579 568 660
226 031 904 170 324 062 351 700 858 796 178 922 222 789 623
703 897 374 720 000 000 000 000 000 000 000 000 000 000 000
000 000 000 000 000

Et voilà, 200! se termine par 49 zéros dans son écriture décimale. Le lecteur a sûrement remarqué que ce n'est pas cette approche que l'on cherche ; et si l'on remplaçait 200 par 100000 ou par n ?

L'idée gagnante ici est la remarque suivante :" l'écriture décimale de m se termine par k zéros si, et seulement si, 10^k est la plus grande puissance de 10 qui divise m". Une telle

information s'obtient directement de la décomposition en nombres premiers de m:

$$m = 2^{\nu_2(m)} \cdot 5^{\nu_5(m)} \prod_{p \in \mathcal{P} \setminus \{2,5\}} p^{\nu_p(m)}.$$

qui donne immédiatement $k = \min(\nu_2(m), \nu_5(m))$.

Revenons à notre exemple, l'ensemble $\mathbb{N}_{200}$ contient 100 entiers pairs parmi lesquels 50 multiples de 4, 25 multiples de 8, 12 multiples de 16, 6 multiples de 32, 3 multiples de 64 et en fin 1 multiple de 128. Ce qui donne

$$\nu_2(200!) = 100 + 50 + 25 + 12 + 6 + 3 + 1 = 197.$$

De même, l'ensemble $\mathbb{N}_{200}$ contient 40 entiers multiples de 5 parmi lesquels 8 multiples de 25, et en fin 1 multiple de 125. Ce qui donne

$$\nu_5(200!) = 40 + 8 + 1 = 49.$$

Par conséquent 200! se termine par $k = \min(197, 49) = 49$ zéros dans son écriture décimale.

Généralisons le calcul précédent. Notons $M_n(a)$ l'ensemble des multiples de a dans $\mathbb{N}_n$. Clairement

$$M_n(a) = \left\{ ka : 1 \leq k \leq E\left(\frac{n}{a}\right) \right\}.$$

et le cardinal de cet ensemble est $E(n/a)$, qui est consistant avec le fait que $M_n(a) = \emptyset$ si $a > n$. Si p est un nombre premier alors l'ensemble $A(n,p,j) = M_n(p^j) \setminus M_n(p^{j+1})$, (avec $j \geq 1$), est l'ensemble des entiers de $\mathbb{N}_n$ qui sont divisibles par p^j et qui ne sont pas divisibles par p^{j+1}: si $m \in \mathbb{N}_n$, alors

$$\begin{aligned} m \in M_n(p^j) \setminus M_n(p^{j+1}) &\iff p^j \mid m \quad \text{et} \quad p^{j+1} \nmid m. \\ &\iff \nu_p(m) = j. \end{aligned}$$

L'ensemble $M_n(p)$ est une réunion disjointe des ensembles $(A(n,p,j))_{j \geq 1}$, et

$$\text{Card } (A(n,p,j)) = E\left(\frac{n}{p^j}\right) - E\left(\frac{n}{p^{j+1}}\right).$$

D'où,

$$\begin{aligned} \nu_p(n!) &= \sum_{k=1}^{n} \nu_p(k) = \sum_{k \in M_n(p)} \nu_p(k) \\ &= \sum_{j \geq 1} \left(\sum_{m \in A(n,p,j)} \nu_p(m) \right) \end{aligned}$$

Avec la convention $\displaystyle\sum_{k \in \emptyset} () = 0$.

D'où

$$\begin{aligned}\nu_p(n!) &= \sum_{j\geq 1} j\text{Card }(A(n,p,j)) \\ &= \sum_{j\geq 1} j\left(E\left(\frac{n}{p^j}\right) - E\left(\frac{n}{p^{j+1}}\right)\right) \\ &= \sum_{j\geq 1} jE\left(\frac{n}{p^j}\right) - \sum_{j\geq 2}(j-1)E\left(\frac{n}{p^j}\right) \\ &= \sum_{j\geq 1} E\left(\frac{n}{p^j}\right)\end{aligned}$$

On a, alors la proposition suivante:

Proposition.14 : *Pour tout entier $n \in \mathbb{N}^*$, on a $n! = \prod_{p\in\mathcal{P}} p^{\nu_p(n!)}$, avec*

$$\nu_p(n!) = \sum_{j\geq 1} E\left(\frac{n}{p^j}\right).$$

Remarque : Notons que $p \mapsto \nu_p(n!)$ est une fonction décroissante en p, et par conséquent $\nu_2(n!) \geq \nu_5(n!)$, pour tout n. L'écriture décimale de $n!$ se termine par $\sum_{j\geq 1} E(n/5^j)$ zéros. Par exemple, l'écriture décimale de 1000! se termine par 249 zéros, et l'écriture décimale de 100000! se termine par 24999 zéros.

Venons aux choses sérieuses. Si $N \in \mathbb{N}$, on définit $\pi(N)$ comme le cardinal de l'ensemble des nombres premiers qui se trouvent dans l'intervalle $[1, N]$.

$$\pi(N) = \text{Card }(\mathbb{N}_N \cap \mathcal{P}).$$

Par exemple $\pi(0) = \pi(1) = 0$ et $\pi(10) = 4$. La fonction $N \mapsto \pi(N)$ est une fonction très importante en théorie des nombres. Le théorème des nombres premiers affirme que

$$\lim_{N\to\infty} \pi(N)\frac{\text{Log } N}{N} = 1.$$

Ce résultat a été démontré pour la première fois en 1896 de façon indépendante par les mathématiciens *Hadamard* et *De la Vallée-Poussin*. Il y a maintenant beaucoup de démonstrations de ce théorème mais elles sortent toutes du cadre de ce livre. Nous allons quand même présenter une forme faible de ce théorème, dû à *Chebychev* qui l'a présenté au milieu du $XIX^{\text{ième}}$ siècle.

Théorème.15 : *Il existe deux constantes* $0 < a < A$ *telles que*

$$\forall\, N \in \mathbb{N},\ (N \geq 2), \qquad a\frac{N}{\operatorname{Log} N} < \pi(N) < A\frac{N}{\operatorname{Log} N}.$$

Preuve : La démonstration est basée sur l'étude de la suite d'entiers naturels $(b_n)_{n\geq 1}$, définie par $b_n = C_{2n}^n$. Commençons par donner un encadrement simple de la suite (b_n).

◇ Comme $2^{2n} = (1+1)^{2n} = \sum_{k=0}^{2n} C_{2n}^k \geq C_{2n}^n$, alors

$$\forall\, n \in \mathbb{N}, \qquad b_n \leq 4^n. \tag{3}$$

◇ Comme $\dfrac{b_{n+1}}{b_n} = 2\dfrac{2n+1}{n+1} \geq 2$, alors

$$\forall\, n \in \mathbb{N}, \qquad b_n \geq 2^n. \tag{4}$$

Regardons, ensuite, la décomposition en nombres premiers de b_n. En utilisant le fait que $b_n = \dfrac{(2n)!}{(n!)^2}$ et la proposition.14, on trouve $b_n = \prod_{p\in\mathcal{P}} p^{\alpha_p(n)}$, avec

$$\alpha_p(n) = \sum_{j\geq 1}\left(E\left(\frac{2n}{p^j}\right) - 2E\left(\frac{n}{p^j}\right)\right). \tag{5}$$

Notons que $E(2x) - 2E(x) \in \{0,1\}$ pour tout $x \in \mathbb{R}$, et que si $j > \dfrac{\operatorname{Log}(2n)}{\operatorname{Log} p}$ alors $E\left(\dfrac{2n}{p^j}\right) = 0$. Il en résulte que

$$\alpha_p(n) \leq E\left(\frac{\operatorname{Log}(2n)}{\operatorname{Log} p}\right).$$

ce qui implique que

$$\forall\, n \in \mathbb{N}^*, \quad \forall\, p \in \mathcal{P}\cap\mathbb{N}_{2n}, \qquad p^{\alpha_p(n)} \leq 2n. \tag{6}$$

D'autre part, si $p \in \mathcal{P}\cap]n, 2n]$ alors la relation (5) se réduit à $\alpha_p(n) = 1$ d'où

$$\forall\, n \in \mathbb{N}^*, \qquad \left(\prod_{\substack{n<p\leq 2n\\ p\in\mathcal{P}}} p\right) \mid b_n. \tag{7}$$

En utilisant (6) et (7) on obtien l' encadrement

$$n^{\pi(2n)-\pi(n)} < \prod_{\substack{n<p\leq 2n\\ p\in\mathcal{P}}} p \leq b_n \leq \prod_{\substack{1<p\leq 2n\\ p\in\mathcal{P}}} p^{\alpha_p(n)} \leq (2n)^{\pi(2n)}.$$

D'où, en utilisant (3) et (4),

$$n^{\pi(2n)-\pi(n)} < 2^{2n}, \quad \text{et} \quad 2^n \leq (2n)^{\pi(2n)}. \tag{8}$$

Remplaçons n par 2^k, $(k \geq 0)$, dans les inégalités précédentes, et prenons les logarithmes:

$$k(\pi(2^{k+1}) - \pi(2^k)) < 2^{k+1}, \qquad 2^k \leq (k+1)\pi(2^{k+1}). \tag{9}$$

Comme les nombres pairs (autres que 2) ne sont pas premiers, alors on a $\pi(2^{k+1}) \leq 2^k$, on déduit de (9) que

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < \pi(2^{k+1}) + 2^{k+1} \leq 3 \cdot 2^k. \tag{10}$$

En effectuant, la somme de ces inégalités, pour k variant entre 0 et $m-1$, on obtient

$$m\pi(2^m) < 3\sum_{k=0}^{m-1} 2^k < 3 \cdot 2^m. \tag{11}$$

Enfin, on utilise la deuxième inégalité de (9), et on trouve

$$\forall\, m \in \mathbb{N}^*, \quad \frac{2^m}{2m} \leq \pi(2^m) < \frac{3 \cdot 2^m}{m}. \tag{12}$$

Soit n un entier $n \geq 2$. On pose $m = E(\lg n)$, de telle manière que $2^m \leq n < 2^{m+1}$. Comme $N \mapsto \pi(N)$ est une fonction croissante alors

$$\pi(n) \leq \pi(2^{m+1}) < \frac{3 \cdot 2^{m+1}}{m+1} \leq \frac{6 \cdot 2^m}{m+1} \leq 6\mathrm{Log}\, 2\, \frac{n}{\mathrm{Log}\, n}.$$

et

$$\pi(n) \geq \pi(2^m) \geq \frac{2^m}{2m} \geq \frac{2^{m+1}}{4m} > \frac{\mathrm{Log}\, 2}{4}\, \frac{n}{\mathrm{Log}\, n}.$$

et finalement

$$\forall\, n \in \mathbb{N}, (n \geq 2), \qquad \frac{\mathrm{Log}\, 2}{4}\, \frac{n}{\mathrm{Log}\, n} < \pi(n) < 6\mathrm{Log}\, 2\, \frac{n}{\mathrm{Log}\, n}.$$

Ce qui achève la démonstration, avec $a = (\mathrm{Log}\, 2)/4 > 1/6$ et $A = 6\mathrm{Log}\, 2 < 5$. □

EXERCICES

EXERCICE .1 Montrer que $\forall\, n \in \mathbb{Z}$, $\text{PGCD}\left(15n^2+8n+6, 30n^2+21n+13\right) = 1$

EXERCICE .2 On définit les entiers a_n, b_n par $a_n + \sqrt{2}b_n = (1+\sqrt{2})^n$ pour tout $n \in \mathbb{N}$. Montrer que $\forall\, n$, $\text{PGCD}\,(a_n, b_n) = 1$.

EXERCICE .3 Soient $a, b, c \in \mathbb{N}^*$, on pose $d = \text{PGCD}\,(b, c)$. Montrer que

$$\text{PGCD}\left(a^b-1, a^c-1\right) = a^d - 1$$

Montrer aussi que

$$(a^c-1)(a^b-1) \,|\, (a^d-1)(a^m-1)$$

Où $m = \text{PPCM}\,((,b)\,,c)$.

EXERCICE .4 Montrer que $\forall\, n \in \mathbb{N}$ $\quad 7 \,\big|\, 2^{2^{2n}} - 2$ et $7 \,\big|\, 2^{2^{2n+1}} - 4$. En déduire que

$$\forall\, n \in \mathbb{N} \quad 7 \,\big|\, 4^{2^{2n}} + 2^{2^{2n}} + 1.$$

EXERCICE .5 Montrer que $\forall\, n \in \mathbb{N} \quad 9 \,|\, 2^{2n} + 6n - 1$.

EXERCICE .6 Montrer que pour tout $n \in \mathbb{N}$, 121 ne divise pas $n^2 + 3n + 5$.

EXERCICE .7 Soient $n, p, q \in \mathbb{Z}$, avec p un nombre premier. Montrer que

$$p^2 \mid n^2 + (p-2q)n + q^2 \Longrightarrow p \mid q.$$

(Noter que $n^2 + (p-2q)n + q^2 = (n-q)(n+p-q) + pq$).

EXERCICE .8 Montrer que $\text{PGCD}\left(n^3+n, 2n+1\right) = 1 \Longleftrightarrow 5 \not| n-2$

EXERCICE .9 Déterminer les entiers n tels que $n+1 \,|\, n^2+1$.

EXERCICE .10 Déterminer les entiers n tels que $n-3 \,|\, n^3-3$.

Exercice .11 Montrer que $\forall\ k \in \mathbb{N}, \qquad 3^{k+1} \mid 2^{3^k} + 1$

Exercice .12 Montrer que $\forall\ a, b\ \in\ \mathbb{N}^*,$ avec $a > b, \qquad \dfrac{a^2+b^2}{a^2-b^2} \notin \mathbb{N}.$

Exercice .13 On considère les deux nombres $b = 60809$ et $a = 58483$.

i. Calculer le Pgcd de a et b. On note $d = \text{Pgcd}\ (a, b)$.

ii. Trouver $s, t \in \mathbb{N}$ tels que $sb - ta = d$.

Exercice .14 Pour $n \in \mathbb{N}$, on définit $F_n = 2^{2^n} + 1$.

i. Montrer que si $m > n$ alors $2^{2^{n+1}} - 1 \mid F_m - 2$. En déduire que $F_n \mid F_m - 2$.

ii. Montrer que si $m \neq n$ alors $\text{Pgcd}\ (F_n, F_m) = 1$.

iii. Déduire de ce qui précède qu'il y a une infinité de nombres premiers.

Exercice .15 On considère la suite de nombres entiers $\{U_n\}_{n\geq 0}$ définie par

$$U_0 = 0, \quad U_1 = 1, \qquad U_{n+2} = U_{n+1} + U_n$$

i. Montrer que $\forall\ n \in \mathbb{N}, \qquad \text{Pgcd}\ (U_{n+1}, U_n) = 1.$

ii. Montrer que $\forall\ (n, p) \in \mathbb{N}^* \times \mathbb{N}^*, \qquad U_{n+p-1} = U_{n-1}U_{p-1} + U_nU_p$.(On pourra raisonner par récurrence sur p).

iii. Soient $a, b, c \in \mathbb{N}^*$. Montrer que si a et c sont premiers entre eux, alors $\text{Pgcd}\ (bc, a) = \text{Pgcd}\ (b, a)$.

iv. Déduire de ce qui précède que $\forall\ n \geq 0,\ \forall\ q > 0,\ \forall\ r \geq 0$ on a

$$\text{Pgcd}\ (U_{qn+r}, U_n) = \text{Pgcd}\ \left(U_{(q-1)n+r}, U_n\right).$$

puis que

$$\text{Pgcd}\ (U_{qn+r}, U_n) = \text{Pgcd}\ (U_n, U_r).$$

v. Soient $m, n \in \mathbb{N}^*$, et $d = \text{Pgcd}\ (m, n)$. Montrer que $\text{Pgcd}\ (U_m, U_n) = U_d$.

Exercice .16 Trouver la factorisation de 46127 en produit de nombres premiers. On pourra commencer par chercher b et a tels que $46127 = b^2 - a^2$.

Exercice .17 Déterminer le plus petit entier strictement positif n tel que $n/2$ soit un carré, $n/3$ soit un cube, et $n/5$ soit une puissance cinquième.

EXERCICE .18 Soient p un nombre premier différent de 2, a un entier plus grand que 2. Montrer que si $p \mid a+1$, alors $p^{k+1} \mid a^{p^k}+1$.

EXERCICE .19 soit n un entier naturel $n \geq 2$. On pose

$$\lambda_n = E(\lg n), \quad \text{et} \quad A_n = \prod_{0 \leq k < n/2} (2k+1).$$

Montrer que, tout entier $m \in \mathbb{N}_n \setminus \{2^{\lambda_n}\}$ divise $2^{\lambda_n - 1} A_n$. En déduire que

$$\forall\, n \geq 2, \qquad \sum_{k=1}^{n} \frac{1}{k} \notin \mathbb{N}.$$

Les congruences dans $\mathbb{Z}$

1. Généralités

En dehors du fait que la théorie des congruences est belle, elle a beaucoup d'applications, par exemple, en cryptographie, dans les codes correcteurs d'erreurs, et dans les ordinateurs. C'est aussi la base de la théorie des groupes et la théorie des nombres. Les notions et les notations de la théorie des congruences, qui en font un outil très puissant, ont été introduites par le mathématicien Allemand *Karl Friedrich Gauss* (1777-1855), dans son livre *Disquisitiones Arithmeticae*, apparu en 1801, où il mettait les fondements de la théorie moderne des nombres.
Venons à la définition.

Définition : Soient a, b, et n des entiers relatifs. On dit que "*a et b sont congrus modulo n*" si, et seulement si, $a - b$ est un multiple de n. S'il en est ainsi on écrit $a \equiv b \bmod (n)$.

Une relation du type précédent s'appelle *une congruence modulo n* ; l'entier n s'appelle *le module* de la congruence.
Il est clair que la congruence modulo n est la même chose que la congruence modulo $(-n)$, et que

$$a \equiv b \bmod (n) \iff n \,|\, (a-b) \iff (a-b) \in n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}.$$

En particulier si $n = 0$ la congruence modulo 0 n'est autre que l'égalité dans $\mathbb{Z}$.
Voici quelques propriétés élémentaires des congruences dont la démonstration est laissée au lecteur:

◇ La relation binaire $\Re_n$ définie sur $\mathbb{Z}$ par $x \,\Re_n\, y \iff x \equiv y \bmod (n)$ est une relation d'équivalence. (*i.e.* réflexive, symétrique, et transitive).

◇ Pour $(a, b, a', b') \in \mathbb{Z}^4$, on a

$$(a \equiv b \bmod (n) \quad \text{et} \quad a' \equiv b' \bmod (n)) \quad \Longrightarrow (a + a' \equiv b + b' \bmod (n)).$$

qui exprime la compatibilité de la congruence $\bmod (n)$ avec l'addition.

◇ Pour $(a, b, a', b') \in \mathbb{Z}^4$, on a

$$(a \equiv b \bmod (n) \quad \text{et} \quad a' \equiv b' \bmod (n)) \quad \Longrightarrow (aa' \equiv bb' \bmod (n)).$$

C'est la compatibilité de la congruence $\bmod (n)$ avec la multiplication.

◇ Pour $(a, b) \in \mathbb{Z}^2$, et pour tout $k \in \mathbb{N}$, on a

$$(a \equiv b \bmod (n) \quad \Longrightarrow (a^k \equiv b^k \bmod (n)).$$

◇ Pour $(a, b) \in \mathbb{Z}^2$, et pour tout $\lambda \in \mathbb{N}^*$, on a

$$(a \equiv b \bmod (n) \quad \Longrightarrow (\lambda a \equiv \lambda b \bmod (\lambda n)).$$

◇ Si $a \equiv b \bmod (n)$ alors $a \equiv b \bmod (n')$ pour tout diviseur n' de n.

◇ Si $d \neq 0$ divise a, b et n, alors

$$a \equiv b \bmod (n) \quad \Longrightarrow \quad \frac{a}{d} \equiv \frac{b}{d} \bmod (\frac{n}{d})$$

▽ Mais attention, si $d \neq 0$ divise seulement a et b, la congruence $a \equiv b \bmod (n)$ n'entraîne pas, en générale, $\dfrac{a}{d} \equiv \dfrac{b}{d} \bmod (n)$.

On suppose désormais $n \in \mathbb{N}^*$.

Si $a \in \mathbb{Z}$, alors la classe d'équivalence de a modulo la relation $\Re_n$ ou "*la classe de congruence de a modulo n*" est

$$[a]_n = \{a + \lambda n : \ \lambda \in \mathbb{Z}\} \stackrel{\text{def}}{=} a + n\mathbb{Z}.$$

D'après l'étude de la division euclidienne dans $\mathbb{Z}$ on a

◇ Pour tout $a \in \mathbb{Z}$ l'ensemble $[a]_n \cap \{0, \ldots, n-1\}$ contient un, et un seul, élément:

$$\forall\, a \in \mathbb{Z}, \qquad \text{Card}\ ([a]_n \cap \{0, \ldots, n-1\}) = 1.$$

On convient de désigner par $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes de congruence $\bmod(n)$ dans $\mathbb{Z}$. Si $\gamma \in \mathbb{Z}/n\mathbb{Z}$, l'unique élément de $\gamma \cap \{0, \ldots, n-1\}$ s'appelle son **reste mod** (n). De même si $a \in \mathbb{Z}$, l'unique $r \in \{0, \ldots, n-1\}$ tel que $a \equiv r \bmod(n)$ est appelé son reste $\bmod(n)$. On déduit immédiatement, que l'application $r \mapsto r + n\mathbb{Z}$ définit une bijection de $\{0, \ldots, n-1\}$ sur $\mathbb{Z}/n\mathbb{Z}$. En particulier, Card $(\mathbb{Z}/n\mathbb{Z}) = n$.

Voici quelques exemples:

- $641 \mid 2^{32} + 1$.

  En effet, notons d'abord que $641 = 1 + 5 \times 128 = 1 + 5 \cdot 2^7 = 5^4 + 2^4$. Donc

  $$5 \cdot 2^7 \equiv -1 \bmod(641) \quad \text{et} \quad 5^4 \equiv -2^4 \bmod(641).$$

  Il en resulte que $(5 \cdot 2^7)^4 \equiv (-1)^4 \bmod(641)$, c'est-à-dire $5^4 \cdot 2^{28} \equiv 1 \bmod(641)$, ou bien $-2^4 \cdot 2^{28} \equiv 1 \bmod(641)$. Finalement $2^{32} + 1 \equiv 0 \bmod(641)$. □

- Cherchons le reste de la division euclidienne de $(795)^{25}$ par 11.

  Comme $795 \equiv 3 \bmod(11)$, alors $(795)^{25} = 3^{25} \bmod(11)$. Nous réduisons $3^{25} \bmod(11)$ avec un peu plus d'efforts.

  $$\begin{aligned} 3^2 &= 9 \equiv -2 \bmod(11) \\ 3^4 &= (3^2)^2 \equiv (-2)^2 = 4 \bmod(11) \\ 3^8 &= (3^4)^2 \equiv 4^2 = 16 \equiv 5 \bmod(11) \\ 3^{16} &= (3^8)^2 \equiv 5^2 = 25 \equiv 3 \bmod(11) \end{aligned}$$

  Mais $25 = 16 + 8 + 1$, d'où $3^{25} = 3^{16} \cdot 3^8 \cdot 3 \equiv 3 \cdot 5 \cdot 3 = 45 \equiv 1 \bmod(11)$. Alors $(795)^{25} \equiv 1 \bmod(11)$. □

- Si $n = (b_m b_{m-1} \ldots b_1 b_0)_{10}$. (c'est l'écriture décimale de n). Alors

  $$\begin{aligned} &i\ . && n \equiv \left(\sum_{k=0}^{m} b_k \right) && \bmod(9) \\ &ii\ . && n \equiv \left(\sum_{k=0}^{m} b_k \right) && \bmod(3) \\ &iii. && n \equiv \left(\sum_{k=0}^{m} b_k (-1)^k \right) && \bmod(11) \end{aligned}$$

En effet, pour tout $k \in \mathbb{N}$, $(10)^k \equiv 1 \bmod (9)$, $(10)^k \equiv 1 \bmod (3)$ et enfin $(10)^k \equiv (-1)^k \bmod (11)$. □

On retrouve ainsi les régles de divisibilités bien connues. Par exemple le nombre 11 divise 2345678987654321 et 9 divise 12345678987654321.

La proposition suivante est une reformulation importante du théorème de Bezout.

Proposition.1 : *Soient $n \in \mathbb{N}^* \setminus \{1\}$, et $a \in \mathbb{Z}$. Si $\text{PGCD}\ (a, n) = 1$ alors il existe un unique $b \in \mathbb{Z}$ avec $1 \leq b < n$ tel que $ab \equiv 1\ mod\ (n)$.*

Preuve : D'après Bezout, il existe $(x, y) \in \mathbb{Z}^2$ tels que $xa + yn = 1$. On prend alors $b = x - nE(x/n)$, et on trouve immédiatement $ab \equiv 1 \bmod (n)$ avec $1 \leq b < n$. Si $1 \leq b' < n$ vérifie aussi $ab' \equiv 1 \bmod (n)$ alors $n \,|\, a(b - b')$ et a est premier avec n donc (d'après le lemme de Gauss) $n \,|\, (b - b')$. Mais $|b - b'| < n$ alors $b = b'$. □

Corollaire.2 : *Soient $(a, b, c) \in \mathbb{Z}^3$, et $n > 2$. Alors*

$$\left.\begin{array}{l} ab \equiv ac \bmod (n) \\ \\ \text{PGCD}\ (a, n) = 1 \end{array}\right\} \quad \Longrightarrow \quad b \equiv c \bmod (n).$$

Preuve: Comme $\text{PGCD}\ (a, n) = 1$, alors, d'après la proposition.1, on trouve $d \in \mathbb{Z}$ tel que $ad \equiv 1 \bmod (n)$, on conclut que $b \equiv bad \equiv cad \equiv c \bmod (n)$. □

2. La fonction φ d'Euler

Définition : Soit $n \in \mathbb{N}^*$. On note $\mathbb{Z}_n^* = \{k \in \mathbb{N}_n : \text{PGCD}\ (k, n) = 1\}$, et on définit $\varphi(n)$ par la relation:

$$\varphi(n) = \text{Card}\ (\mathbb{Z}_n^*)\,.$$

En particulier, $\varphi(1) = 1$.

Théorème.3 : *Soit $n \in \mathbb{N}$ tel que $n \geq 2$. Alors*

$$\varphi(n) = n \prod_{\substack{p \,|\, n \\ p \in \mathcal{P}}} \left(1 - \frac{1}{p}\right).$$

Preuve : D'après le linkthéorème.11 du sixième chapitrecor11, on sait que l'on peut écrire de façon unique $n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_m^{\nu_m}$.
Si $k \in \{1, \ldots, m\}$, on pose $A_k = \{r \in \mathbb{N}_n : p_k \,|\, r\}$. Alors

$$\mathbb{Z}_n^* = \mathbb{N}_n \setminus (A_1 \cup A_2 \cup \cdots \cup A_m)\,.$$

On utilise, alors le principe d'inclusion-exclusion, pour calculer Card $(A_1 \cup A_2 \cup \cdots \cup A_m)$.

$$\text{Card}\,(A_1 \cup A_2 \cup \cdots \cup A_m) = \sum_{k=1}^{m} (-1)^{k-1} \sum_{B \in P_k^{(m)}} \text{Card}\left(\bigcap_{j \in B} A_j\right).$$

Où $P_k^{(m)}$ désigne l'ensemble des parties de $\mathbb{N}_m$ qui sont de cardinal k. Mais

$$\bigcap_{j \in B} A_j = \{r \in \mathbb{N}_n : (\prod_{j \in B} p_j) \,|\, r\}$$

et

$$\text{Card}\left(\bigcap_{j \in B} A_j\right) = \frac{n}{\prod\limits_{j \in B} p_j} = n \prod_{j \in B} \frac{1}{p_j}.$$

Il en résulte,

$$\begin{aligned}\varphi(n) =& n - n \sum_{k=1}^{m} (-1)^{k-1} \sum_{B \in P_k^{(m)}} \prod_{j \in B} \frac{1}{p_j} \\ =& n + n \sum_{k=1}^{m} \left(\sum_{B \in P_k^{(m)}} \prod_{j \in B} \frac{-1}{p_j} \right) = n \prod_{\substack{p \,|\, n \\ p \in \mathcal{P}}} \left(1 - \frac{1}{p}\right).\end{aligned}$$

On a utilisé la propriété suivante

$$\prod_{k=1}^{n} (1 + a_k) = 1 + \sum_{k=1}^{n} \left(\sum_{B \in P_k^{(n)}} \prod_{i \in B} a_i \right).$$

qui fait l'objet de la question 1°.*a* de l'exercice.5 du cinquième chapitre. □

Par exemple, $255 = 3 \cdot 5 \cdot 17$, d'où

$$\varphi(255) = 255 \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{17}\right) = 128.$$

Et $2025 = 3^4 \cdot 5^2$, donc

$$\varphi(2025) = 2025 \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 1080.$$

Si $p \in \mathcal{P}$ est un nombre premier, et $\nu \in \mathbb{N}^*$, alors $\varphi(p^\nu) = p^{\nu-1}(p-1)$.

Corollaire.4 : *Soit* $(n,m) \in \mathbb{N}^* \times \mathbb{N}^*$. *Alors*

$$\text{PGCD } (n,m) = 1 \quad \Longrightarrow \quad \varphi(nm) = \varphi(n)\varphi(m).$$

Preuve : Si PGCD $(n,m) = 1$, alors les ensembles $\{p \in \mathcal{P} : p \,|\, n\}$ et $\{p \in \mathcal{P} : p \,|\, m\}$ forment une partition de $\{p \in \mathcal{P} : p \,|\, nm\}$. Donc

$$\begin{aligned}
\varphi(nm) &= nm \prod_{\substack{p \,|\, nm \\ p \in \mathcal{P}}} \left(1 - \frac{1}{p}\right) \\
&= nm \prod_{\substack{p \,|\, n \\ p \in \mathcal{P}}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \,|\, m \\ p \in \mathcal{P}}} \left(1 - \frac{1}{p}\right) \\
&= \varphi(n)\varphi(m).
\end{aligned}$$

□

Le théorème suivant montre l'interêt de la fonction d'Euler.

Théorème.5 : (Théorème d'Euler) *Soient* n *un entier* $n \geq 2$, *et* $a \in \mathbb{Z}$. *Alors*

$$\text{PGCD } (a,n) = 1 \quad \Longrightarrow \quad a^{\varphi(n)} \equiv 1 \ mod\ (n).$$

Preuve: Clairement, on peut supposer que $a \in \{0, 1, \ldots, n-1\}$. Soit $k \in \mathbb{Z}_n^*$. On pose $\delta(k) = ak - nE(ak/n)$.

Comme PGCD $(a,n) =$ PGCD $(k,n) = 1$ alors Le corollaire.6 du chapitre précédent montre que PGCD $(ak,n) = 1$ et par conséquent PGCD $(\delta(k),n) = 1$. Il en résulte clairement que $\delta(k) \in \mathbb{Z}_n^*$, et que δ définit une application de $\mathbb{Z}_n^*$ dans lui-même.

Montrons que δ est injective. En effet, si $\delta(k) = \delta(k')$, (pour k et k' dans $\mathbb{Z}_n^*$), alors $ak \equiv ak' \bmod (n)$, et d'après le corollaire.2, on déduit que $k \equiv k' \bmod (n)$, ou bien $k = k'$, car k et k' appartiennent à $\mathbb{Z}_n^*$.

Il résulte que $\delta : \mathbb{Z}_n^* \longrightarrow \mathbb{Z}_n^*$ est une bijection. D'où

$$\begin{aligned}
\Delta = \prod_{k \in \mathbb{Z}_n^*} k &= \prod_{k \in \mathbb{Z}_n^*} \delta(k) \\
&\equiv \prod_{k \in \mathbb{Z}_n^*} (ka) \quad \bmod (n) \\
&\equiv a^{\varphi(n)} \prod_{k \in \mathbb{Z}_n^*} k \quad \bmod (n) \\
&\equiv a^{\varphi(n)} \Delta \quad \bmod (n).
\end{aligned}$$

Mais d'après le corollaire.6 du chapitre précédent on sait que PGCD $(\Delta, n) = 1$, et par le corollaire.2 on déduit que $a^{\varphi(n)} \equiv 1 \bmod (n)$. □

Le théorème précédent permet de poser la définition suivante:

Définition : Soit n un entier supérieur ou égal à 2. Pour tout $a \in \mathbb{Z}$ telle que PGCD $(a, n) = 1$, on appelle **l'ordre de** a **modulo** n le plus petit entier e de $\mathbb{N}^*$ telle que $a^e \equiv 1 \mod (n)$. Cet entier e sera noté $\mathrm{Ord}_n(a)$.

$$\mathrm{Ord}_n(a) = \min \{k \in \mathbb{N}^* : a^k \equiv 1 \mod (n)\}$$

Voici un corollaire de cette définition:

Corollaire.6 : *Soit n un entier supérieur ou égal à 2. Pour tout $a \in \mathbb{Z}$ telle que* PGCD $(a, n) = 1$, $\mathrm{Ord}_n(a)$ *divise $\varphi(n)$. Plus généralement, si $a^k \equiv 1 \mod (n)$, alors* $\mathrm{Ord}_n(a)$ *divise k.*

Preuve : En effet, effectuons la division euclidienne de k par $e = \mathrm{Ord}_n(a)$: $k = eq + r$ avec $0 \leq r < e$. alors

$$1 \equiv a^k \equiv (a^e)^q \cdot a^r \equiv a^r \mod (n).$$

Par conséquent $a^r \equiv 1 \mod (n)$. Le fait $r \neq 0$ contredit la définition de $e = \mathrm{Ord}_n(a)$. Alors $r = 0$ et $k = eq$. □

Corollaire.7 : (Le petit théorème de Fermat) *Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$ on a*

$$p \not| a \quad \Longrightarrow \quad a^{p-1} \equiv 1 \ mod \ (p).$$

Preuve : C'est immédiat après le théorème.5, car $\varphi(p) = p - 1$. □

Remarque : Il résulte de ce qui précède que, si p est un nombre premier alors $a^p \equiv a \mod (p)$, pour tout entier a.

Voici quelques exemples d'utilisation :

♣ $3^{256} \equiv 21 \bmod (100)$.

En effet, d'après le théorème d'Euler $3^{40} \equiv 1 \bmod (100)$, car $\varphi(100) = 40$. Mais $256 = 40 \times 6 + 16$, donc

$$3^{256} = (3^{40})^6 \cdot 3^{16} \equiv 3^{16} \bmod (100).$$

et

$$3^{16} = (81)^4 \equiv (-19)^4 \equiv (361)^2 \equiv (39)^2 \bmod (100)$$

enfin $(39)^2 = 1521 \equiv 21 \bmod (100)$. On conclut $3^{256} \equiv 21 \bmod (100)$.

♣ Soit n un entier impair, non divisible par 5. Alors n divise un entier dont l'écriture décimale ne contient que le chiffre 1. (Par exemple $3 \,|\, 111$, $7 \,|\, 111111$).

En effet, d'après l'hypothèse PGCD $(10, n) = 1$. D'autre part PGCD $(10, 9) = 1$ donc PGCD $(10, 9n) = 1$. D'après le théorème d'Euler $(10)^{\varphi(9n)} \equiv 1 \bmod (9n)$. Ceci démontre l'existence d'un entier k tel que $(10)^{\varphi(9n)} - 1 = 9nk$. On pose alors

$$M = \frac{(10)^{\varphi(9n)} - 1}{9} = (\underbrace{111 \cdots 111}_{\varphi(9n) \text{ chiffres}})_{10}$$

Clairement n divise M.

3. Applications

1°. Comme première application nous allons démontrer la propiété suivante connue sous le nom du théorème de Wilson.

Théorème.8 : (théorème de Wilson)*Pour tout entier $m > 0$, on a*

$$(m-1)! \equiv -1 \ mod\ (m) \iff m \quad est\ premier. \qquad (W)$$

Preuve : Supposons d'abord que p est un nombre premier avec $p \geq 5$, (les cas $p = 2$ ou $p = 3$ sont triviaux). Tout entier a tel que $1 \leq a \leq p-1$ est premier avec p alors d'après la proposition.1 il existe un unique a' tel que $1 \leq a' \leq p-1$ et $aa' = 1 \bmod (p)$.
Notons ensuite que $a = a'$ si, et seulement si, $p \,|\, (a^2 - 1)$ ou bien $p \,|\, (a-1)(a+1)$. Mais p est premier donc ce qui précède est équivalent à $p \,|\, (a-1)$ ou $p \,|\, (a+1)$ et par conséquent $a = a'$ si, et seulement si, $a = 1$ ou $a = p-1$.

Si, alors, on laisse de côté les entiers 1 et $p-1$, et on regroupe les entiers $\{2,3,\ldots,p-2\}$ en couples (a,a') avec $a \neq a'$ et $aa' \equiv 1 \bmod (p)$, on obtient $r = (p-3)/2$ couples: $(a_1,a_1'),\cdots(a_r,a_r')$. Par conséquent

$$2\cdot 3\cdots(p-2) = \prod_{k=2}^{p-2} k = \prod_{k=1}^{r} a_k a_k' \equiv 1 \bmod (p).$$

ou bien $(p-2)! \equiv 1 \bmod (p)$, et en multipliant par $(p-1) \equiv -1 \bmod (p)$ on trouve $(p-1)! = -1 \bmod (p)$.

Inversement, supposons que m n'est pas premier et que m divise $1+(m-1)!$. Soit d un diviseur de m tel que $1 < d < m$ alors $d \,|\, (m-1)!$ et $d \,|\, (1+(m-1)!)$ et par conséquent $d \,|\, 1$ ce qui est absurde. Ceci démontre le théorème de Wilson. □

Comme corollaire du théorème de Wilson on a,

Corollaire.9 : *Soit p un nombre premier impair, alors*

$$p \equiv 1 \bmod (4) \iff \exists\, n \in \mathbb{N} : \quad p \,|\, (n^2+1).$$

Preuve : Supposons que $p \,|\, (n^2+1)$. Alors $n^2 \equiv -1 \bmod (p)$. Ceci implique que $n^3 \equiv -n \bmod (p)$, par conséquent, si n ou n^3 est congru à 1 modulo p, alors n^2 sera congru à 1 modulo p ce qui est absurde car p est impair. Il en résulte que le plus petit entier $k > 0$ tel que $n^k \equiv 1 \bmod (p)$ est 4, c'est-à-dire $\mathrm{Ord}_p(n) = 4$, le corollaire.6 montre alors que $4 \,|\, \varphi(p) = p-1$.

Inversement, notons $m = (p-1)/2$, m est un entier pair, et on a

$$m! = \prod_{k=1}^{m} k \equiv (-1)^m \prod_{k=1}^{m} (p-k) \equiv \prod_{k=m+1}^{p-1} k \quad \bmod (p).$$

Alors,

$$(m!)^2 \equiv (\prod_{k=1}^{m} k)(\prod_{k=m+1}^{p-1} k) = (p-1)! \equiv -1 \quad \bmod (p).$$

Donc, $p \,|\, (n^2+1)$ où $n = (\dfrac{p-1}{2})!$. □

2°. Dans cette deuxième application, on se propose de démontrer la proposition suivante:

Proposition.10 : *Soient a un entier plus grand ou égal à 2, p et q deux nombres premiers impairs. Si $q \,|\, (a^p - 1)$ alors, $q \,|\, (a-1)$ ou $q \equiv 1 \bmod (2p)$.*

Preuve : Supposons que $q \,|\, (a^p - 1)$ et que $q \not| (a-1)$. Ceci se traduit en écrivant $a^p \equiv 1 \bmod (q)$ et $a \not\equiv 1 \bmod (q)$. La première égalité montre que $\text{PGCD}\,(q, a) = 1$, et que si $e = \text{Ord}_q(a)$ alors $1 < e$ et $e \,|\, p$, (par le corollaire.6). Il en résulte que $e = p$ car p est premier. En utilisant une deuxième fois le corollaire.6, on déduit que $p \,|\, \varphi(q) = (q-1)$. Mais $2 \,|\, (q-1)$ et les deux entiers 2 et p sont premiers entre eux, donc $(2p) \,|\, (q-1)$. □

Montrons, en utilisant ce qui précède, que $M_{17} = 2^{17} - 1$ est un nombre premier. En effet, si M_{17} n'est pas premier alors la proposition.10 montre que les diviseurs premiers q de M_{17} sont de la forme $34k + 1$, et il y en aura au moins un plus petit que $\sqrt{M_{17}} < 363$.
Or les entiers de la forme $34k + 1$ qui sont strictement plus petit que 363 sont

$$\{35, 69, 103, 137, 171, 205, 239, 273, 307, 341\}$$

et les nombres premiers dans cet ensemble sont seulement $\{103, 137, 239, 307\}$. Mais

$$2^{17} \equiv 56 \bmod (103),\ 2^{17} \equiv 100 \bmod (137),\ 2^{17} \equiv 100 \bmod (239),\ 2^{17} \equiv 290 \bmod (307).$$

Par conséquent, M_{17} n'est divisible par aucun des entiers de $\{103, 137, 239, 307\}$. On conclut que M_{17} est premier.
En utilisant ces mêmes techniques on peut facilement montrer que $M_{29} = 2^{29} - 1$ n'est pas premier. Ce que nous laissons comme exercice au lecteur.

3°. Dans cette troisième application, nous nous proposons de démontrer, pour $(n, m) \in \mathbb{N}^* \times \mathbb{N}^*$ et $x \in \mathbb{R}$, l'identité

$$\sum_{k=0}^{m-1} E\left(\frac{nk + x}{m}\right) = \sum_{k=0}^{n-1} E\left(\frac{mk + x}{n}\right). \qquad (R)$$

Nous allons pour cela utiliser un lemme simple.

Lemme : *Soient a, et b deux entiers positifs premiers entre eux, et $c \in \mathbb{Z}$. Pour k un entier vérifiant $0 \leq k \leq a-1$, on pose*

$$\psi(k) = bk + c - aE\left(\frac{bk + c}{a}\right).$$

Alors $k \mapsto \psi(k)$ définit une bijection de l'ensemble $\mathcal{T}_a = \{0, 1, \ldots, a-1\}$.

Preuve : Notons d'abord que d'après la définition de la partie entière on a

$$E\left(\frac{bk+c}{a}\right) \leq \frac{bk+c}{a} < 1 + E\left(\frac{bk+c}{a}\right).$$

Il en résulte que, $\psi(k) \in \mathcal{T}_a$, pour tout $k \in \mathcal{T}_a$.
L'application ψ est injective. En effet, si $\psi(k) = \psi(k')$ alors $bk+c \equiv bk'+c \mod (a)$, ou bien $a \,|\, b(k-k')$. Mais PGCD $(a,b) = 1$, il en résulte, (d'après le lemme de Gauss), que $a \,|\, (k-k')$. D'autre part, k et k' sont des éléments de $\mathcal{T}_a$, d'où $|\,k-k'| < a$. Les deux propriétés $a \,|\, (k-k')$ et $|\,k-k'| < a$ impliquent que $k = k'$, et $\psi : \mathcal{T}_a \longrightarrow \mathcal{T}_a$ est injective. Mais L'ensemble $\mathcal{T}_a$ est fini, donc $\psi : \mathcal{T}_a \longrightarrow \mathcal{T}_a$ est bijective. □

Du lemme précédent on déduit

$$\begin{aligned}\sum_{k=0}^{a-1} k = \sum_{k=0}^{a-1} \psi(k) &= \sum_{k=0}^{a-1} \left(bk + c - aE\left(\frac{bk+c}{a}\right)\right) \\ &= b\left(\sum_{k=0}^{a-1} k\right) + ca - a\sum_{k=0}^{a-1} E\left(\frac{bk+c}{a}\right).\end{aligned}$$

D'où

$$\sum_{k=0}^{a-1} E\left(\frac{bk+c}{a}\right) = c + \frac{(b-1)(a-1)}{2}. \qquad (*)$$

Venons au cas général. Soient $(n,m) \in \mathbb{N}^* \times \mathbb{N}^*$ et $x \in \mathbb{R}$, On pose $d =$ PGCD (n,m), et on définit a et b par $m = da$ et $n = db$, clairement PGCD $(a,b) = 1$. On pose aussi $c = E(x/d)$ et $r = x - dc \in [0,d[$.
Notons que, pour k un entier de $\{0,1,\ldots,m-1\}$,

$$bk + c - aE\left(\frac{nk+x}{m}\right) = a\left(\frac{nk+x-r}{m} - E\left(\frac{nk+x}{m}\right)\right).$$

ce qui implique $-\dfrac{r}{d} \leq bk + c - aE\left(\dfrac{nk+x}{m}\right) < a$, ou bien

$$0 \leq bk + c - aE\left(\frac{nk+x}{m}\right) < a,$$

Il en résulte

$$E\left(\frac{nk+x}{m}\right) \leq \frac{bk+c}{a} < 1 + E\left(\frac{nk+x}{m}\right),$$

et finalement

$$E\left(\frac{nk+x}{m}\right) = E\left(\frac{bk+c}{a}\right).$$

On écrit alors,

$$\begin{aligned}
\sum_{k=0}^{m-1} E\left(\frac{nk+x}{m}\right) &= \sum_{k=0}^{da-1} E\left(\frac{bk+c}{a}\right) \\
&= \sum_{r=0}^{d-1}\left(\sum_{k=ra}^{ra+a-1} E\left(\frac{bk+c}{a}\right)\right) \\
&= \sum_{r=0}^{d-1}\left(\sum_{s=0}^{a-1} E\left(\frac{b(ra+s)+c}{a}\right)\right) \\
&= \sum_{r=0}^{d-1}\left[\sum_{s=0}^{a-1}\left(br + E\left(\frac{bs+c}{a}\right)\right)\right] \\
&= ba\sum_{r=0}^{d-1} r + d\sum_{s=0}^{a-1} E\left(\frac{bs+c}{a}\right) \\
&= ba\frac{d(d-1)}{2} + d\sum_{s=0}^{a-1} E\left(\frac{bs+c}{a}\right).
\end{aligned}$$

Mais PGCD $(a,b)=1$, donc on peut utiliser $(*)$:

$$\sum_{k=0}^{m-1} E\left(\frac{nk+x}{m}\right) = ba\frac{d(d-1)}{2} + d\left(c + \frac{(b-1)(a-1)}{2}\right)$$

Ce qui donne

$$\sum_{k=0}^{m-1} E\left(\frac{nk+x}{m}\right) = \frac{(n-1)(m-1)}{2} + \frac{d-1}{2} + dE\left(\frac{x}{d}\right), \quad \text{avec PGCD } (n,m)=d. \qquad (\dagger)$$

Dans le deuxième membre de $(\dagger)$, m et n jouent un rôle symétrique et par conséquent, on a aussi

$$\sum_{k=0}^{n-1} E\left(\frac{mk+x}{n}\right) = \frac{(n-1)(m-1)}{2} + \frac{d-1}{2} + dE\left(\frac{x}{d}\right), \quad \text{avec PGCD } (n,m)=d. \qquad (\ddagger)$$

Ceci démontre (R). □

EXERCICES

EXERCICE .1 Calculer 10^3 mod (7). En déduire un critère de divisibilité par 7.

EXERCICE .2 Pour quelles valeurs de $n \in \mathbb{N}^*$ a-t-on $(16)^n - 15n - 1 \equiv 0 \mod (225)$?

EXERCICE .3 Pour quelles valeurs de $n \in \mathbb{Z}$ l'entier $n^2 + (n+1)^2 + (n+3)^2$ est-il multiple de 10 ?

EXERCICE .4 Pour quelles valeurs de $n \in \mathbb{Z}$ l'entier $4n^2 + 1$ est-il multiple de 65 ?

EXERCICE .5 Soit p un nombre premier. Calculer C_p^k mod (p), pour $0 \leq k \leq p$.

EXERCICE .6 Trouver le reste de la division euclidienne de a par b dans les cas suivants

a	$(1945)^8$	5^{10}	5^{12}	$(1945)^{12}$	$(2001)^{2001}$	7^{355}	7^{355}
b	7	11	11	11	26	10	100

EXERCICE .7 Montrer que $\displaystyle\sum_{k=1}^{10} 10^{10^k} \equiv 5 \mod (7)$.

EXERCICE .8 Montrer que si $(a, b, c) \in \mathbb{Z}^3$

$$a^3 + b^3 + c^3 \equiv 0 \mod (7) \quad \Longrightarrow \quad abc \equiv 0 \mod (7)$$

EXERCICE .9 Montrer que, si PGCD $(a, n) = 1$, alors l'équation $ax \equiv b \mod (n)$ admet comme solution $x \equiv ba^{\varphi(n)-1} \mod (n)$. En déduire toutes les solutions de $3x \equiv 5 \mod (26)$, $13x \equiv 2 \mod (40)$ et $10x \equiv 21 \mod (49)$.

EXERCICE .10 Déterminer les solutions x, s'ils existent, dans les cas suivants:

◇ $91x \equiv 84 \mod (143)$

◇ $91x \equiv 84 \mod (147)$

◇ $\begin{cases} x \equiv 2 \mod (12) \\ x \equiv 3 \mod (13) \\ x \equiv 5 \mod (7\ ) \end{cases}$

◇ $\begin{cases} 3x \equiv 2 \mod (5\ ) \\ 5x \equiv 2 \mod (12) \\ 17x \equiv 8 \mod (19) \end{cases}$

EXERCICE .11 Montrer que si PGCD $(a, n) =$ PGCD $(a-1, n) = 1$, alors

$$\sum_{k=1}^{\varphi(n)} a^{k-1} \equiv 0 \bmod (n).$$

EXERCICE .12 Soit p un nombre premier impair. Montrer

$$\sum_{k=1}^{p-1} k^{p-1} \equiv -1 \bmod (p), \qquad \sum_{k=1}^{p-1} k^{p} \equiv 0 \bmod (p).$$

EXERCICE .13 Soient $n \in \mathbb{N}^*$, et a un entier positif plus grand que 2. Montrer que $n \,|\, \varphi(a^n - 1)$.

EXERCICE .14 Soit n un entier naturel impair. Montrer que l'écriture décimale de $2^{2n}(2^{2n+1} - 1)$ se termine par 28.

EXERCICE .15 Soit p un nombre premier impair. Montrer que

$$\sum_{k=1}^{p-1} E\left(\frac{k^3}{p}\right) = \frac{(p+1)(p-1)(p-2)}{4} \qquad \clubsuit$$

$$\sum_{k=1}^{M} E\left(\sqrt[3]{kp}\right) = \frac{(3p-5)(p-1)(p-2)}{4} \qquad \spadesuit$$

où $M = (p-1)(p-2)$.

Solutions

Chapitre Troisième

Solution 3.1. Remarquons d'abord que:

$$\sum_{k=0}^{n}(-1)^k(n-k)^2 = (-1)^n\sum_{k=1}^{n}(-1)^k k^2$$

Distinguons deux cas:

1°. n est un nombre pair, $n = 2p$:

$$\begin{aligned}\sum_{k=0}^{2p}(-1)^k k^2 &= \sum_{k=1}^{p}(2k)^2 - \sum_{k=1}^{p}(2k-1)^2\\ &= \sum_{k=1}^{p}\left((2k)^2-(2k-1)^2\right)\\ &= \sum_{k=1}^{p}(4k-1) = 2p(p+1)-p = \frac{n(n+1)}{2}\end{aligned}$$

2°. n est un nombre impair, $n = 2p+1$:

$$\begin{aligned}\sum_{k=0}^{2p+1}(-1)^k k^2 &= -(2p+1)^2 + \sum_{k=0}^{2p}(-1)^k k^2\\ &= -(2p+1)^2 + p(2p+1) = -(2p+1)(p+1) = -\frac{n(n+1)}{2}\end{aligned}$$

Dans les deux cas on trouve:

$$\sum_{k=0}^{n}(-1)^k(n-k)^2 = (-1)^n\sum_{k=1}^{n}(-1)^k k^2 = \frac{n(n+1)}{2}.$$ □

Solution 3.2. Notons que $\forall\, k \in \mathbb{N}, \quad (k+1)^2 - k^2 = 2k+1$ En effectuant la somme de ces égalités entre 0 et n, on obtient:

$$\sum_{k=0}^{n}(2k+1) = \sum_{k=0}^{n}((k+1)^2-k^2) = (n+1)^2.$$ □

Solution 3.3. Posons $A_n = \sum_{(i,j)\in\mathbb{N}_n\times\mathbb{N}_n} \min(i,j)$. En Remarquant que les ensembles $\mathbb{N}_{n-1}\times\mathbb{N}_{n-1}$, $\{n\}\times\mathbb{N}_n$ et $\mathbb{N}_{n-1}\times\{n\}$ forment une partition de $\mathbb{N}_n\times\mathbb{N}_n$, on peut écrire

$$\begin{aligned} A_n =& \sum_{(i,j)\in\mathbb{N}_{n-1}\times\mathbb{N}_{n-1}} \min(i,j) + \sum_{j=1}^{n}\min(n,j) + \sum_{i=1}^{n-1}\min(i,n) \\ =& A_{n-1} + n + 2\sum_{j=1}^{n-1} j = A_{n-1} + n + n(n-1) = A_{n-1} + n^2. \end{aligned}$$

D'où

$$A_n = A_1 + \sum_{k=2}^{n}(A_k - A_{k-1}) = 1 + \sum_{k=2}^{n} k^2 = \sum_{k=1}^{n} k^2 = S_n^{(2)}.$$

Alors

$$\sum_{(i,j)\in\mathbb{N}_n\times\mathbb{N}_n} \min(i,j) = \frac{n(n+1)(2n+1)}{6}. \qquad \square$$

Solution 3.4. On a:

$$\begin{aligned} \sum_{1\le i,j\le n}(i^2+ij+j^2) =& \sum_{j=1}^{n}\left(\sum_{i=1}^{n} i^2\right) + \sum_{1\le i,j\le n} ij + \sum_{i=1}^{n}\left(\sum_{j=1}^{n} j^2\right) \\ =& 2\sum_{j=1}^{n}\left(\sum_{i=1}^{n} i^2\right) + \sum_{i=1}^{n} i\left(\sum_{j=1}^{n} j\right) \\ =& 2\sum_{j=1}^{n} S_n^{(2)} + \left(\sum_{i=1}^{n} i\right)\left(\sum_{j=1}^{n} j\right) = 2nS_n^{(2)} + \left(S_n^{(1)}\right)^2. \end{aligned}$$

D'où $\sum_{1\le i,j\le n}(i^2+ij+j^2) = \dfrac{n^2(n+1)(11n+7)}{12}$. $\square$

Solution 3.5. Notons d'abord que les ensembles $\{(i,j)\in(\mathbb{N}_n)^2 : i=j\}$, $\{(i,j)\in(\mathbb{N}_n)^2 : i<j\}$ et $\{(i,j)\in(\mathbb{N}_n)^2 : i>j\}$ forment une partition de $\mathbb{N}_n\times\mathbb{N}_n$. Alors on peut écrire:

$$S = \sum_{i=1}^{n} i^3 + \underbrace{\sum_{1\le i<j\le n} ij^2}_{S_1} + \underbrace{\sum_{1\le j<i\le n} ij^2}_{S_2} \tag{1}$$

Étudions alors S_1 et S_2.

$$\begin{aligned} S_1 = \sum_{1\le i<j\le n} ij^2 &= \sum_{j=2}^{n}\left(\sum_{i=1}^{j-1} ij^2\right) \\ &= \sum_{j=2}^{n} j^2(\sum_{i=1}^{j-1} i) = \sum_{j=2}^{n} j^2\frac{j(j-1)}{2} \\ &= \frac{1}{2}\sum_{j=1}^{n}(j^4-j^3) = \frac{1}{2}(S_n^{(4)} - S_n^{(3)}) \end{aligned}$$

Et

$$\begin{aligned} S_2 = \sum_{1\le j<i\le n} ij^2 &= \sum_{i=2}^{n}\left(\sum_{j=1}^{i-1} ij^2\right) \\ &= \sum_{i=2}^{n} i(\sum_{j=1}^{i-1} j^2) = \sum_{i=2}^{n} i\frac{i(i-1)(2i-1)}{6} \\ &= \frac{1}{6}\sum_{i=1}^{n}(2i^4-3i^3+i^2) = \frac{1}{6}(2S_n^{(4)} - 3S_n^{(3)} + S_n^{(2)}) \end{aligned}$$

En remplaçant dans (1) on trouve

$$S = \frac{5}{6}S_n^{(4)} + \frac{1}{6}S_n^{(2)}.$$

D'autre part, clairement on a

$$S = \sum_{i=1}^{n}\left(\sum_{j=1}^{n} ij^2\right) = \sum_{i=1}^{n} i\left(\sum_{j=1}^{n} j^2\right) = \sum_{i=1}^{n} iS_n^{(2)} = S_n^{(1)}S_n^{(2)}$$

D'où $S_n^{(1)}S_n^{(2)} = \frac{5}{6}S_n^{(4)} + \frac{1}{6}S_n^{(2)}$, ce qui démontre que $S_n^{(4)} = \frac{1}{5}S_n^{(2)}(6S_n^{(1)} - 1)$. □

De la même façon on a:

$$\begin{aligned}\widetilde{S} = \left(S_n^{(2)}\right)^2 =& \sum_{i=1}^{n} i^4 + 2 \sum_{1\le i<j\le n} i^2 j^2 \\ =& S_n^{(4)} + 2\sum_{j=2}^{n} j^2 \sum_{i=1}^{j-1} i^2 \\ =& S_n^{(4)} + 2\sum_{j=2}^{n} j^2 \, \frac{j(2j^2-3j+1)}{6} \\ =& S_n^{(4)} + \frac{1}{3}\sum_{j=1}^{n}(2j^5 - 3j^4 + j^3) \\ =& S_n^{(4)} + \frac{2}{3}S_n^{(5)} - S_n^{(4)} + \frac{1}{3}S_n^{(3)}.\end{aligned}$$

Finalement, on trouve: $S_n^{(5)} = \frac{3}{2}\left(S_n^{(2)}\right)^2 - \frac{1}{2}S_n^{(3)} = \frac{1}{2}\left(3\left(S_n^{(2)}\right)^2 - S_n^{(3)}\right)$. □

Solution 3.6. On remarque que:

$$\begin{aligned}\sum_{k=1}^{2n} \frac{(-1)^k}{k} =& \sum_{\substack{1\le k\le 2n \\ k \text{ pair}}} \frac{(-1)^k}{k} + \sum_{\substack{1\le k\le 2n \\ k \text{ impair}}} \frac{(-1)^k}{k} \\ =& \sum_{\substack{1\le k\le 2n \\ k \text{ pair}}} \frac{1}{k} - \sum_{\substack{1\le k\le 2n \\ k \text{ impair}}} \frac{1}{k} \\ =& 2\sum_{\substack{1\le k\le 2n \\ k \text{ pair}}} \frac{1}{k} - \sum_{k=1}^{2n} \frac{1}{k} = 2\sum_{k=1}^{n} \frac{1}{2k} - \sum_{k=1}^{2n} \frac{1}{k} = H_n - H_{2n}.\end{aligned}$$

Donc: $U_n = H_n - H_{2n}$. Pour trouver la limite de U_n, on va utiliser le fait que $(H_n - \operatorname{Log} n)_{n\ge 1}$ est une suite convergente, d'où:

$$\begin{aligned}U_n =& (H_n - \operatorname{Log}(2n)) - (H_{2n} - \operatorname{Log}(2n)) \\ =& (H_n - \operatorname{Log} n) - (H_{2n} - \operatorname{Log}(2n)) - \operatorname{Log} 2.\end{aligned}$$

Par conséquent, la limite de U_n est $-\operatorname{Log} 2$. □

Solution 3.7. Pour tout entier $n > 0$, on a $2T_n = nT_{n-1} + 3n!$. En multipliant les deux membres de cette relation par $S_n = \frac{2^n}{n!}$, $(n \ge 0)$, on trouve:

$$2S_nT_n = 2S_{n-1}T_{n-1} + 3.2^n.$$

D'où $U_n = U_{n-1} + 32^{n-1}$ avec $U_n = S_n T_n$. On détermine U_n en notant que:

$$U_n - U_0 = \sum_{k=1}^{n} U_k - U_{k-1} = 3\sum_{k=0}^{n-1} 2^k = 3(2^n - 1)$$

Et par conséquent

$$T_n = (3 + \frac{1}{2^{n-1}})n!.$$ □

La suite précédente est un cas particulier des suites récurrentes de la forme:

$$T_0 \in \mathbb{R}, \quad \text{et pour } n > 0, \quad a_n T_n = b_n T_{n-1} + c_n$$

où $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont deux suites à termes non nuls et $(c_n)_{n\in\mathbb{N}}$ est une suite quelconque. Pour trouver T_n, on va multiplier les deux membres de la relation précédente par x_n qu'on va préciser ultérieurement ; $x_n a_n T_n = x_n b_n T_{n-1} + x_n c_n$. On détermine x_n pour que la relation précédente devienne $U_n = U_{n-1} + x_n c_n$, avec $U_n = x_n a_n T_n$. Ceci impose la condition

$$x_n b_n T_{n-1} = U_{n-1} = x_{n-1} a_{n-1} T_{n-1}.$$

ce qui est vérifié si $x_n b_n = a_{n-1} x_{n-1}$, ou bien

$$x_n = x_0 \prod_{k=1}^{n} \frac{a_{k-1}}{b_k}$$

On a donc $U_n = U_0 + \sum_{k=1}^{n} c_k x_k$ et $T_n = \frac{1}{x_n a_n}(U_0 + \sum_{k=1}^{n} c_k x_k)$. □

Solution 3.8. L'idée est d'essayer de trouver une relation exprimant V_n en fonction de V_{n-1}. En effet, pour $n > 1$, on a:

$$\begin{aligned} V_n &= n+1 + \frac{2}{n} \sum_{k=0}^{n-1} V_k \\ V_{n-1} &= n + \frac{2}{n-1} \sum_{k=0}^{n-2} V_k \end{aligned}$$

D'où, en calculant, $\sum_{k=0}^{n-2} V_k$ de la deuxième équation et en remplaçant dans la première, on trouve

$$V_n = 2 + \frac{n+1}{n} V_{n-1}.$$

on a donc pour tout $k > 0$:

$$\frac{V_k}{k+1} - \frac{V_{k-1}}{k} = \frac{2}{k+1}$$

En prenant la somme pour k variant entre 1 et n on trouve:

$$\frac{V_n}{n+1} = 2\sum_{k=1}^{n} \frac{1}{k+1} = 2\sum_{k=2}^{n+1} \frac{1}{k} = 2(H_{n+1} - 1)$$

D'où: $V_n = 2(n+1)(H_{n+1} - 1)$. □

Solution 3.9. Notons D_n le nombre des segments MM', parallèls à la droite d'équation $y = x$, avec M et M' dans E_n. Notons aussi D'_n le nombre des segments MM', parallèls à la droite d'équation $y = x$, avec M dans E_{n-1} et M' dans $E_n \setminus E_{n-1}$. Clairement $D_n = D'_n + D_{n-1}$. D'autre part il y a une bijection entre l'ensemble des segments MM', parallèls à la droite d'équation $y = x$, avec M dans E_{n-1} et M' dans $E_n \setminus E_{n-1}$ et les éléments de E_{n-1}, par conséquent $D'_n = (n-1)^2$.

On conclut que, $D_n = (n-1)^2 + D_{n-1}$, pour tout $n \geq 2$, avec $D_1 = 0$. Alors $D_n = S^{(2)}_{n-1} = n(n-1)(2n-1)/6$. □

Solution 3.10. Posons L_n le nombre maximum de régions déterminées par n plans dans l'espace. On va trouver une relation entre L_n et L_{n-1}: supposons qu'on ait $n-1$ plans dans l'espace qui le partagent en L_{n-1} régions et voyons ce qui se passe lorsqu'on rajoute un $n^{\text{ième}}$ plan P. Le plan P augmente le nombre de régions de q régions si, et seulement si, les $n-1$ plans précédents déterminent sur le plan P, q régions planes. Or les $n-1$ plans précédents coupent le plan P en $n-1$ droites qui donnent au plus $1 + n(n-1)/2$ régions planes sur P, (voir le deuxième chapitre), et on a donc:

$$L_n \leq L_{n-1} + \frac{n(n-1)}{2} + 1$$

D'autre part, on peut toujours choisir P de telle manière qu'il ne soit parallèle à aucun des plans présédents, et que les droites dessinées sur lui par les autres plans donnent le nombre maximum de régions planes. Alors:

$$L_n = L_{n-1} + \frac{n(n-1)}{2} + 1.$$

Et par conséquent:

$$L_n = L_0 + \sum_{k=1}^{n} \left(\frac{k(k-1)}{2} + 1\right) = 1 + \frac{1}{2}S^{(2)}_n - \frac{1}{2}S^{(1)}_n + n = L_n = 1 + n + \frac{(n-1)n(n+1)}{6}$$ □

Solution 3.11. Posons C_n le nombre maximum de régions déterminées par n cercles dans le plan. On va trouver une relation entre C_n et C_{n-1}: supposons qu'on ait $n-1$, $(n>1)$, cercles dans le plan qui le partagent en C_{n-1} régions et voyons ce qui se passe lorsqu'on rajoute un $n^{\text{ième}}$ cercle $\mathcal{C}$. Le cercle $\mathcal{C}$ augmente le nombre de régions de q régions si, et seulement si, les $n-1$ cercles précédents déterminent sur le cercle $\mathcal{C}$, q arcs. Or les $n-1$ cercles précédents coupent le cercle $\mathcal{C}$ en au plus $2(n-1)$ points (deux cercles admettent au plus deux points en commun), qui donnent $2(n-1)$ arcs sur $\mathcal{C}$, et $2(n-1)$ régions supplémentaires dans le plan, on a donc:

$$C_n \leq C_{n-1} + 2(n-1)$$

D'autre part, cette borne supérieure est atteinte. En effet, notons, pour $k \geq 1$, $\mathcal{C}_k$ le cercle de rayon 1, et dont les coordonnées du centre sont $(2^{-k+1}, 0)$. On vérifie immédiatement et par récurrence que le nombre des points de l'ensemble $\mathcal{C}_k \bigcap (\bigcup_{1\leq j<k} \mathcal{C}_j)$ est $2(k-1)$. Si, par conséquent, T_n est le nombre de régions du plan déterminées par $(\mathcal{C}_k)_{1\leq k\leq n}$ alors d'après ce qui précède $T_n = 2(n-1) + T_{n-1}$.

Mais $C_1 = T_1 = 2$. Supposons que $C_{n-1} = T_{n-1}$, alors $C_n \geq T_n = T_{n-1} + 2(n-1) = C_{n-1} + 2(n-1) \geq C_n$, ce qui montre que $T_n = C_n$. On a donc démontré que $T_n = C_n$, pour tout $n \geq 1$, et on conclut que

$$C_1 = 2, \qquad C_n = 2(n-1) + C_{n-1} \quad \text{pour tout } n \geq 2$$

Alors $C_n = n^2 - n + 2$, pour tout $n \geq 1$. □

CHAPITRE QUATRIÈME

Solution 4.1. En utilisant le premier exemple du chapitre on a

$$\forall\, x \in \mathbb{R}, \qquad E(2x) = E(x) + E(x + \frac{1}{2}).$$

Il en résulte que pour tout $(x, y) \in \mathbb{R}^2$,

$$E(2x) + E(2y) - E(x) - E(y) = E(x + \frac{1}{2}) + E(y + \frac{1}{2}).$$

Mais nous savons aussi que pour tout $(t, z) \in \mathbb{R}^2$,

$$E(t) + E(z) - E(t + z) \in \{0, -1\}.$$

Alors en appliquant ceci à $t = x + 1/2$ et $z = y + 1/2$, on trouve, pour tout $(x, y) \in \mathbb{R}^2$,

$$E(x + \frac{1}{2}) + E(y + \frac{1}{2}) - E(x + y + 1) \in \{0, -1\}.$$

Ou bien

$$E(x + \frac{1}{2}) + E(y + \frac{1}{2}) - E(x + y) \in \{0, 1\}.$$

On conclut

$$E(2x) + E(2y) - E(x) - E(y) - E(x + y) \in \{0, 1\}. \qquad \square$$

Solution 4.2. Notons d'abord que

$$E(\sqrt{k}\,) = p \iff p \le \sqrt{k} < p + 1 \iff p^2 \le k < (p + 1)^2.$$

On déduit que

$$\begin{aligned}
\sum_{k=1}^{m^2-1} E(\sqrt{k}\,) &= \sum_{r=1}^{m-1} \left(\sum_{r^2 \le k < (r+1)^2} E(\sqrt{k}\,) \right) \\
&= \sum_{r=1}^{m-1} r((r+1)^2 - r^2) = \sum_{r=1}^{m-1} 2r^2 + r \\
&= \frac{(m-1)m(2m-1)}{3} + \frac{(m-1)m}{2} = \frac{m(m-1)(4m+1)}{6}.
\end{aligned}$$

Soit $n \in \mathbb{N}^*$, on pose $m = E(\sqrt{n})$. Alors On déduit que

$$\begin{aligned}\sum_{k=1}^{n} E(\sqrt{k}) &= \sum_{k=1}^{m^2-1} E(\sqrt{k}) + \sum_{k=m^2}^{n} E(\sqrt{k}) \\ &= \frac{m(m-1)(4m+1)}{6} + m(n-m^2+1) = mn - \frac{1}{3}m^3 - \frac{1}{2}m^2 + \frac{5}{6}m.\end{aligned}$$

Ce qui donne $\displaystyle\sum_{k=1}^{n} E(\sqrt{k}) = nE(\sqrt{n}) - \frac{1}{3}(E(\sqrt{n}))^3 - \frac{1}{2}(E(\sqrt{n}))^2 + \frac{5}{6}E(\sqrt{n}).$ □

Solution 4.3. Le lecteur vérifira que les entiers entre 0 et 20 sont tous honnêtes. En particulier

$$1 = E(\sqrt{2}), \quad 2 = E(2\sqrt{2}), \quad 3 = E(2\sqrt{3}), \quad 4 = E(3\sqrt{2}),$$

$$5 = E(4\sqrt{2}), \quad 6 = E(4\sqrt{3}), \quad 7 = E(5\sqrt{2}), \quad 8 = E(6\sqrt{2}).$$

Supposons que n est un entier plus grand ou égal à 8, alors

$$k \overset{\text{def}}{=} E(n/\sqrt{2}) \geq E(4\sqrt{2}) = 5.$$

D'autre part, la définition de k , et le fait que $n/\sqrt{2}$ n'est pas un entier, permettent d'écrire

$$k < \frac{n}{\sqrt{2}} < k+1$$

$$0 < n - k\sqrt{2} < \sqrt{2}$$

$$0 < \frac{n-k\sqrt{2}}{\sqrt{3}-\sqrt{2}} < 2+\sqrt{6}.$$

Il en résulte que

$$0 \leq t \overset{\text{def}}{=} E\left(\frac{n-k\sqrt{2}}{\sqrt{3}-\sqrt{2}}\right) \leq 4.$$

qui est équivalent à

$$t < \frac{n-k\sqrt{2}}{\sqrt{3}-\sqrt{2}} < t+1$$

$$b\sqrt{3} + a\sqrt{2} - \lambda < n < b\sqrt{3} + a\sqrt{2}$$

avec $b = t+1 \in \{1,2,3,4,5\}$, $a = k-b \in \mathbb{N}$ et $\lambda = \sqrt{3}-\sqrt{2} \in]0,1[$. Ceci démontre que $n = E(a\sqrt{2}+b\sqrt{3})$, et l'entier n est honnête. On conclut que tous les entiers naturels sont honnêtes ce qui est respectable !. □

Solution 4.4. On se propose dans cet exercice d'étudier l'existence de couples de fonctions (f, g), de $\mathbb{N}^*$ dans $\mathbb{N}^*$, qui vérifient:

C_1 : Les fonctions f et g sont strictement croissantes.

C_2 : Si $F =$ Im f et $G =$ Im g, alors $F \cup G = \mathbb{N}^*$ et $F \cap G = \emptyset$.

C_3 : Pour tout $n > 0$, $g(n) = 1 + f(f(n))$.

Commençons par supposer qu'il existe un couple de fonctions (f, g) vérifiant ces hypothèses.

♣ D'après C_1, pour tout n on a, $f(n+1) > f(n)$ qui se traduit par $f(n+1) \geq f(n)+1$.

Si, pour un certain $m \in \mathbb{N}^*$, on a $f(m+1) > f(m)+1$ alors la condition C_2 implique $f(m)+1 \in G$. D'où l'existence d'un $k \in \mathbb{N}^*$ tel que $1 + f(m) = g(k) = 1 + f(f(k))$ ce qui montre que $m = f(k) \in F$, car f est injective. On a donc montré que la condition $f(m+1) > f(m)+1$ implique $m \in F$. Inversement, si $m \in F$ alors $m = f(k)$ (pour un certain k), et alors $1+f(m) = 1+f(f(k)) = g(k) \notin F$ et par conséquent $f(m+1) > f(m)+1$. Conclusion:

$$f(n+1) > f(n)+1 \iff n \in F. \tag{1}$$

♣ Supposons qu'il y a $n \in \mathbb{N}^*$ tel que $f(n+1) > f(n)+2$. Cela se traduit par l'existence de deux entiers $p < q$ tels que $g(p) = f(n)+1$ et $g(q) = f(n)+2$. Ceci veut dire, (d'après C_3), que $f(p) = n$ et $f(f(q)) = 1+f(n)$. Mais alors $a = f(f(q)) = 1+f(n) = 1+f(f(p)) = g(p)$ et par conséquent $a \in F \cap G$ ce qui est absurde. On a, alors:

$$\forall\, n \in \mathbb{N}^*, \quad f(n+1) \in \{f(n)+1, f(n)+2\}. \tag{2}$$

Désignons par $\mathbb{1}_A$ la fontion indicatrice de l'ensemble $A \subset \mathbb{N}^*$ c'est à dire

$$\mathbb{1}_A : \mathbb{N}^* \longrightarrow \mathbb{N}^* : \mathbb{1}_A(n) = \begin{cases} 1 & \text{si} \quad n \in A \\ 0 & \text{si} \quad n \notin A \end{cases}$$

Cette notation nous aidera dans la suite. Revenons maintenant à notre étude.

En combinant (1) et (2), nous trouvons que $f(n+1) = f(n)+1$ si $n \notin F$ et $f(n+1) = f(n)+2$ si $n \in F$, ce que nous pouvons formuler sous la forme

$$\forall\, n \in \mathbb{N}^*, \quad f(n+1) = f(n)+1+\mathbb{1}_F(n). \tag{3}$$

♣ Notons que si $f(1) > 1$ alors $g(1) = 1+f(f(1)) > 1+f(1) > 2$, et par conséquent $1 \notin F \cup G$ ce qui absurde. Alors, $f(1) = 1$.

En utilisant la relation (3) et le point précédent on trouve

$$f(n) - f(1) = \sum_{k=1}^{n-1} f(k+1) - f(k) = n - 1 + \sum_{k=1}^{n-1} \mathbb{1}_F(k).$$

$$f(n) = n + \text{Card } (F \cap [1, n[)$$

On arrive alors à la propriété suivante

$$\forall\, n \in \mathbb{N}^*, \qquad f(n) = n + \text{Card } (\{k :\ f(k) < n\})\,. \tag{4}$$

C'est une relation récurrente qui détermine f uniquement.

♣ D'autre part, la croissance stricte de f permet de dire que

$$\text{Card } (\{k :\ f(k) < f(n)\}) = \text{Card } ([1, n[) = n - 1.$$

donc en utilisant (4), $f(f(n)) = f(n) + n - 1$. Ce qui permet de conclure

$$\forall\, n \in \mathbb{N}^*, \qquad g(n) = n + f(n). \tag{5}$$

Nous arrivons à la conclusion suivante:

$$\left\{ \begin{array}{l} \text{S'il existe un couple de fonctions } (f, g) \text{ de } \mathbb{N}^* \text{ dans } \mathbb{N}^*, \text{ vérifiant} \\ \text{les conditions } C_1,\, C_2 \text{ et } C_3. \text{ Alors ce couple est unique, et } f \text{ et } g \text{ sont} \\ \text{données par} \\ \qquad \forall\, n \in \mathbb{N}^*, \quad \left\{ \begin{array}{rcl} f(n) & = & n + \text{Card } (\{k :\ f(k) < n\}) \\ g(n) & = & n + f(n) \end{array} \right. \end{array} \right\} \tag{†}$$

L'étape suivante consiste à montrer l'existence des fonctions f et g. Remarquons que d'après (†) on a, pour tout $n > 0$, $n \leq f(n) \leq 2n$. Ceci nous suggère d'étudier expérimentalement le rapport $f(n)/n$. Voici quelques valeurs:

n	1	10	10^2	10^3	10^4
$f(n)$	1	16	161	1618	16180
$f(n)/n$	1	1.6	1.61	1.618	1.618

Il semble que le rapport $\dfrac{f(n)}{n}$ tend vers un réel $\alpha \in [1, 2]$ quand n tend vers l'infini. Faisons alors l'hypothèse suplémentaire suivante:

$$\lim_{n\to\infty} \frac{f(n)}{n} = \alpha \qquad (\ddagger)$$

Mais, $1 + \dfrac{f(n)}{n} = \dfrac{1}{n} + \dfrac{f(f(n))}{f(n)} \dfrac{f(n)}{n}$. Donc en faisant tendre n vers l'infini on trouve $1 + \alpha = \alpha^2$ donc $\alpha = \dfrac{1+\sqrt{5}}{2}$.

Faisons alors une deuxième expérience et étudions les premières valeurs de $\alpha n - f(n)$.

n	$f(n)$	$\alpha n - f(n)$	n	$f(n)$	$\alpha n - f(n)$
1	1	0.62	10	16	0.18
2	3	0.24	11	17	0.79
3	4	0.85	12	19	0.42
4	6	0.47	13	21	0.03
5	8	0.09	14	22	0.62
6	9	0.71	15	24	0.27
7	11	0.33	16	25	0.88
8	12	0.94	17	27	0.50
9	14	0.56	18	29	0.12

L'observation importante à ce stade est que $\alpha n - f(n) \in]0, 1[$ pour tout $n \in \{1, 2 \ldots, 18\}$, ce qui montre que $f(n) = E(\alpha n)$ pour tout $n \in \{1, 2 \ldots, 18\}$, avec $\alpha = \dfrac{1+\sqrt{5}}{2}$. Ceci démontre que pour ces mêmes valeurs de n on a aussi $g(n) = n + E(\alpha n) = E((1 + \alpha)n) = E(\alpha^2 n)$.

Cette étude expérimentale suggère de considérer les deux fonctions f et g définies par $f(n) = E(\alpha n)$ et $g(n) = E(\alpha^2 n)$, où $\alpha = \dfrac{1+\sqrt{5}}{2}$.

Montrons que ces deux fonctions conviennent. D'abord elles sont clairement strictement croissantes ($\alpha > 1$). Ensuite α est un irrationnel de $]1, +\infty[$ tel que $\frac{1}{\alpha} + \frac{1}{\alpha^2} = 1$. Donc d'après l'étude des spectres dans le cours on sait que $\mathrm{Im}f$ et $\mathrm{Im}g$ forment une partition de $\mathbb{N}^*$. Enfin, pour tout $n \in \mathbb{N}^*$, on a

$$\alpha E(\alpha n) < \alpha^2 n < \alpha E(\alpha n) + \alpha.$$

$$E(\alpha E(\alpha n)) \leq E(\alpha^2 n) \leq E(\alpha E(\alpha n) + \alpha) \leq 2 + E(\alpha E(\alpha n)).$$

$$f(f(n)) \leq g(n) \leq f(1 + f(n)) \leq 2 + f(f(n)).$$

Mais $g(n) \notin \mathrm{Im}f$ donc

$$f(f(n)) < g(n) < f(1 + f(n)) \leq 2 + f(f(n)).$$

ce qui démontre que $g(n) = 1 + f(f(n))$.

On arrive à la conclusion suivante:

$$\left\{ \begin{array}{l} \text{Il existe un, et un seule, couple de fonctions } (f, g) \text{ de } \mathbb{N}^* \text{ dans} \\ \mathbb{N}^*, \text{ vérifiant les conditions } C_1, C_2 \text{ et } C_3. \text{ Ce sont} \\ \qquad \forall\, n \in \mathbb{N}^*, \quad \left\{ \begin{array}{rcl} f(n) & = & E(\alpha n) \\ g(n) & = & E(\alpha^2 n) \end{array} \right. \\ \text{Où } \alpha = \dfrac{1+\sqrt{5}}{2}. \end{array} \right\}$$

□

Solution 4.5. 1°. Notons que $k - pE(k/p) = 0$ si k est un multiple de p, d'où

$$\sum_{k=1}^{pm} \frac{k - pE(k/p)}{k(k+1)} = \sum_{k=1}^{pm-1} \frac{1}{k+1} - p \sum_{k=1}^{pm-1} \frac{E(k/p)}{k(k+1)}$$

Mais $\dfrac{1}{k(k+1)} = \dfrac{1}{k} - \dfrac{1}{k+1}$. Alors

$$\begin{aligned} \sum_{k=1}^{pm} \frac{k - pE(k/p)}{k(k+1)} &= H_{pm} - 1 - p \sum_{k=1}^{pm-1} \frac{E(k/p)}{k} + p \sum_{k=1}^{pm-1} \frac{E(k/p)}{k+1} \\ &= H_{pm} - 1 - p \sum_{k=1}^{pm-1} \frac{E(k/p)}{k} + p \sum_{k=1}^{pm} \frac{E((k-1)/p)}{k} \\ &= H_{pm} - p \sum_{k=1}^{pm} \frac{E(k/p) - E((k-1)/p)}{k} = H_{pm} - H_m. \end{aligned}$$

Car $E(k/p) - E((k-1)/p) = 1$ si k est un multiple de p et $E(k/p) - E((k-1)/p) = 0$ dans le cas contraire. On déduit que

$$\Delta_m(p) = \sum_{k=1}^{pm} \frac{k - pE(k/p)}{k(k+1)} = H_{pm} - H_m. \tag{6}$$

Mais, d'après les résultats du troisième chapitre sur les nombres harmoniques nous savons que $0 < H_n - \operatorname{Log} n - \gamma < 1/n$ pour tout $n > 0$. Alors, pour tout $m > 0$,

$$-\frac{1}{m} < H_{pm} - H_m - \operatorname{Log} p < \frac{1}{pm} < \frac{1}{m}$$

$$|\Delta_m(p) - \operatorname{Log} p| < \frac{1}{m} \tag{7}$$

On conclut que $\lim_{m\to\infty} \Delta_m(p) = \operatorname{Log} p$. □

2°. Tout entier k s'écrit en base p sous la forme $(b_\ell^{(k)} b_{\ell-1}^{(k)} \dots b_1^{(k)} b_0^{(k)})_p$ avec $b_j^{(k)} = E(k/p^j) - pE(k/p^{j+1})$ pour tout $j \geq 0$ et $\ell = \ell_p(k) = E(\dfrac{\operatorname{Log} k}{\operatorname{Log} p})$. La relation (7) se traduit par

$$\left| \sum_{k=1}^{p^N} \frac{b_0^{(k)}}{k(k+1)} - \operatorname{Log} p \right| \leq \frac{p}{p^N}. \tag{8}$$

Fixons $N \in \mathbb{N}^*$. Pour chaque entier m tel que $0 < m \leq N$ on pose

$$\delta_m = \Delta_{p^{N-m}}(p^m) = \sum_{k=1}^{p^N} \frac{k - p^m E(k/p^m)}{k(k+1)}.$$

Alors, d'après (7),

$$|\delta_m - m\operatorname{Log} p| < \frac{1}{p^{N-m-1}} \tag{9}$$

D'autre part, si $m < N$,

$$\delta_{m+1} - \delta_m = p^m \sum_{k=1}^{p^N} \frac{E(k/p^m) - pE(k/p^{m+1})}{k(k+1)} = p^m \sum_{k=1}^{p^N} \frac{b_m^{(k)}}{k(k+1)}.$$

Il en résulte,

$$\left| p^m \sum_{k=1}^{p^N} \frac{b_m^{(k)}}{k(k+1)} - \operatorname{Log} p \right| < \frac{1}{p^{N-m-1}} + \frac{1}{p^{N-m}}$$

$$\left| \sum_{k=1}^{p^N} \frac{b_m^{(k)}}{k(k+1)} - \frac{\operatorname{Log} p}{p^m} \right| < \frac{p+1}{p^N}. \tag{10}$$

En combinant (8) et (10) et en remarquant que $b_m^{(p^N)} = 0$ $(0 \leq m < N)$, on trouve, pour tout $N \in \mathbb{N}^*$ et tout m tel que $0 \leq m < N$

$$\left| \sum_{k=1}^{p^N-1} \frac{b_m^{(k)}}{k(k+1)} - \frac{\mathrm{Log}\, p}{p^m} \right| < \frac{p+1}{p^N}. \tag{11}$$

Mais si $1 \leq k < p^N$ alors $\ell_p(k) < N$ et $S_p(k) = \sum_{m=0}^{N-1} b_m^{(k)}$ d'où, en faisant la somme des inégalités de (11) pour m variant entre 0 et $N-1$ on trouve

$$\left| \sum_{k=1}^{p^N-1} \frac{S_p(k)}{k(k+1)} - (1 - \frac{1}{p^N}) \frac{p\mathrm{Log}\, p}{p-1} \right| < \frac{(p+1)N}{p^N}.$$

ou bien

$$\left| \sum_{k=1}^{p^N-1} \frac{S_p(k)}{k(k+1)} - \frac{p\mathrm{Log}\, p}{p-1} \right| < \frac{(p+1)N + p}{p^N}. \tag{12}$$

car $\dfrac{\mathrm{Log}\, p}{p-1} \leq 1$.

La relation (12) montre que

$$\lim_{N\to\infty} \sum_{k=1}^{p^N-1} \frac{S_p(k)}{k(k+1)} = \frac{p\mathrm{Log}\, p}{p-1}.$$

Ceci démontre le résultat car la suite $\left(\sum_{k=1}^{N} \dfrac{S_p(k)}{k(k+1)} \right)_{N\geq 1}$ est croissante et admet une sous suite convergente. □

Solution 4.6. Commençons par suivre l'indication de l'exercice et de comparer l'écriture en base 2 de n et de $f(n)$ pour certaines valeurs de n.

n	$f(n)$	$(n)_2$	$(f(n))_2$
1	1	1	1
2	1	10	01
3	3	11	11
4	1	100	001
5	5	101	101
6	3	110	011
7	7	111	111
8	1	1000	0001
9	9	1001	1001
10	5	1010	0101
11	13	1011	1101
12	3	1100	0011
13	11	1101	1011
14	7	1110	0111
15	15	1111	1111

Ce qu'on remarque c'est la chose suivante: Si n admet $(b_\ell b_{\ell-1}\dots b_0)_2$, (avec $\ell = E(\lg n)$), comme écriture binaire alors $f(n)$ admet $(b_0 b_1 \dots b_\ell)_2$ pour écriture binaire, et ceci pour tout $n < 16$.

On peut exprimer ce qui précède en disant

$$\forall\, n > 0,\ \forall\, (b_0, \dots b_{n-1}) \in \{0,1\}^{n-1}, \quad f(2^n + \sum_{k=0}^{n-1} b_k 2^k) = 1 + \sum_{k=1}^{n} b_{n-k} 2^k. \qquad (\triangle)$$

Montrons $(\triangle)$ par récurrence. Supposons le résultat vrai pour tout $n < m$ et vérifions le pour m.

Soit $x = \sum_{k=0}^{m} b_k 2^k = b_0 + 2b_1 + 4y$ avec $y = \sum_{k=0}^{m-2} b_{k+2} 2^k$, et $b_m = 1$.

♣ Si $b_0 = 0$, alors $x = 2\sum_{k=0}^{m-1} \delta_k 2^k$, avec $\delta_k = b_{k+1}$, et par conséquent,

$$f(x) = f(\sum_{k=0}^{m-1} \delta_k 2^k) = \sum_{k=0}^{m-1} \delta_{m-1-k} 2^k = \sum_{k=0}^{m-1} b_{m-k} 2^k = \sum_{k=0}^{m} b_{m-k} 2^k.$$

♣ Si $(b_0, b_1) = (1, 0)$, alors $f(x) = f(1 + 4y) = 2f(1 + 2y) - f(y)$. Mais

$$y = \sum_{k=0}^{m-2} \alpha_k 2^k; \quad \alpha_k = b_{k+2}$$
$$1 + 2y = \sum_{k=0}^{m-1} \beta_k 2^k; \quad \beta_k = b_{k+1} \text{ si } k \geq 1 \text{ et }, \beta_0 = 1$$

Alors,

$$\begin{aligned} f(x) =& 2 \sum_{k=0}^{m-1} \beta_{m-1-k} 2^k - \sum_{k=0}^{m-2} \alpha_{m-2-k} 2^k \\ =& 2(2^{m-1} + \sum_{k=0}^{m-2} b_{m-k} 2^k) - \sum_{k=0}^{m-2} b_{m-k} 2^k \\ =& 2^m + \sum_{k=0}^{m-2} b_{m-k} 2^k = \sum_{k=0}^{m} b_{m-k} 2^k. \end{aligned}$$

♣ Si $(b_0, b_1) = (1, 1)$, alors $f(x) = f(3 + 4y) = 3f(1 + 2y) - 2f(y)$. D'où

$$\begin{aligned} f(x) =& 3(2^{m-1} + \sum_{k=0}^{m-2} b_{m-k} 2^k) - 2 \sum_{k=0}^{m-2} b_{m-k} 2^k \\ =& 2^m + 2^{m-1} + \sum_{k=0}^{m-2} b_{m-k} 2^k = \sum_{k=0}^{m} b_{m-k} 2^k. \end{aligned}$$

Nous avons ainsi démontré ($\triangle$), et donné une déscription complète de f. □

Solution 4.7. Fixons un entier $m > 0$, et posons $A_n^{(m)} = \dfrac{1}{2^n} f(2^n m)$. D'après l'hypothèse on a

$$0 \leq f(2^{n+1}m) - 2f(2^n m) \leq 1,$$

d'où en divisant par 2^{n+1}: $\quad 0 \leq A_{n+1}^{(m)} - A_n^{(m)} \leq \dfrac{1}{2^{n+1}}$. En faisant la somme de ces inégalités entre $n = p$ et $n = q - 1$, (avec $q > p$), on trouve:

$$0 \leq A_q^{(m)} - A_p^{(m)} \leq \frac{1}{2^p} - \frac{1}{2^q}.$$

Ceci démontre que la suite $(A_n^{(m)})_{n\geq 0}$ et la suite $(B_n^{(m)})_{n\geq 0}$, de terme général $B_n^{(m)} = A_n^{(m)} + 1/2^n$, sont adjacentes. (*i.e.* $(A_n^{(m)})_{n\geq 0}$ est croissante, $(B_n^{(m)})_{n\geq 0}$ est décroissante, et $\lim\limits_{n\to\infty} (B_n^{(m)} - A_n^{(m)}) = 0$). On conclut à l'existence d'une limite commune α_m à ces deux suites, qui vérifie

$$\forall\, m \in \mathbb{N}^*,\ \forall\, (n, p) \in \mathbb{N}^2, \quad \frac{1}{2^n} f(2^n m) \leq \alpha_m \leq \frac{1}{2^p} f(2^p m) + \frac{1}{2^p}. \qquad (\heartsuit)$$

En utilisant l'hypothèse une deuxième fois on a

$$\forall\,(m,n)\in(\mathbb{N}^*)^2,\qquad 0\leq A_n^{(m+1)}-A_n^{(m)}-A_n^{(1)}\leq\frac{1}{2^n}.$$

d'où en faisant tendre n vers l'infini, $\forall\, m\in\mathbb{N}^*,\qquad \alpha_{m+1}=\alpha_m+\alpha_1$. Cette relation permet de démontrer par récurrence sur m que $\alpha_m=\alpha m$. (Où l'on a noté α pour α_1).

On revient à ($\heartsuit$) et on met $n=p=0$, on trouve

$$\forall\, m\in\mathbb{N}^*,\quad f(m)\leq\alpha m\leq f(m)+1. \tag{$\diamondsuit$}$$

Il en résulte que si $\alpha m\notin\mathbb{N}$ alors $f(m)=E(\alpha m)=\lceil\alpha m\rceil-1$.

Supposons dans la suit que $\alpha=\dfrac{p}{q}$ avec p et q deux entiers premiers entre eux. (Car si $\alpha\in\mathbb{R}_+\setminus\mathbb{Q}$ l'exercice est terminé). D'après ($\diamondsuit$) on a $f(q)\in\{p-1,p\}$, distinguons alors deux cas:

1°. Dans ce cas $f(q)=p-1$. Alors Nous allons montrer par récurrence sur $k>0$ que $f(qk)=pk-1$. En effet, D'après ($\diamondsuit$) on a

$$pk-1\leq f(qk)\leq pk.$$

D'autre part $0\leq f(qk)-f(q(k-1))-f(q)\leq 1$ et donc d'après l'hypothès de récurence

$$pk-2\leq f(qk)\leq pk-1.$$

Les deux relations précédentes montrent que $f(m)=\lceil\alpha m\rceil-1$ pour tout m multiple de q. Mais si m n'est pas multiple de q alors $\alpha m\notin\mathbb{N}$ et $f(m)=E(\alpha m)=\lceil\alpha m\rceil-1$.

2°. Dans ce cas $f(q)=p$. Alors Nous allons montrer par récurrence sur $k>0$ que $f(qk)=pk$. En effet, D'après ($\diamondsuit$) on a

$$pk-1\leq f(qk)\leq pk.$$

D'autre part $0\leq f(qk)-f(q(k-1))-f(q)\leq 1$ et donc d'après l'hypothès de récurence

$$pk\leq f(qk)\leq pk+1.$$

Les deux relations précédentes montrent que $f(m)=E(\alpha m)$ pour tout m multiple de q. Mais si m n'est pas multiple de q alors $\alpha m\notin\mathbb{N}$ et $f(m)=E(\alpha m)=\lceil\alpha m\rceil-1$. □

Chapitre Cinquième

Solution 5.1. Soit S l'ensemble des n sommets du polygône. L'application qui à un point d'intersection de deux diagonales (autre qu'un sommet) fait correspondre le quadrilatère dont ils forment les diagonales est clairement une bijection entre l'ensemble des points d'intersection (autres que les sommets) des segments diagonaux et l'ensemble des parties à quatre éléments de S. On conclut que le nombre des points d'intersection des segments diagonaux vaut $C_n^4 + n$ si $n \geq 5$, vaut 1 si $n = 4$, et vaut 0 si $n \leq 3$. □

Solution 5.2. Notons $\mathcal{P}_k^{(n)}$ l'ensemble des parties à k élémentes de $\mathbb{N}_n$. Les ensembles $(\mathcal{P}_k^{(n)})_{0\leq k\leq n}$ forment une partition de $\mathcal{P}^{(n)}$.

$$\sum_{\mathcal{P}^{(n)}} \text{Card } (X) = \sum_{k=0}^{n} \left(\sum_{\mathcal{P}_k^{(n)}} \text{Card } (X) \right) = \sum_{k=0}^{n} kC_n^k.$$

Mais $(1+x)^n = \sum_{k=0}^{n} C_n^k x^k$, donc en dérivant et en substituant ensuite x par 1, on trouve $n2^{n-1} = \sum_{k=0}^{n} kC_n^k$. D'où

$$\sum_{\mathcal{P}^{(n)}} \text{Card } (X) = n2^{n-1}.$$ □

Notons $L_\emptyset$ l'ensemble des parties $(X, Y) \in \mathcal{P}^{(n)} \times \mathcal{P}^{(n)}$ telles que $X \cap Y = \emptyset$. Clairement

$$\begin{aligned}
\text{Card } \left(L_\emptyset \right) &= \sum_{X\in\mathcal{P}^{(n)}} \text{Card } (\{Y : Y \subset \mathbb{N}_n \setminus X\}) \\
&= \sum_{X\in\mathcal{P}^{(n)}} 2^{n-\text{Card}(X)} \\
&= \sum_{k=0}^{n} \left(\sum_{X\in\mathcal{P}_k^{(n)}} 2^{n-k} \right) \\
&= \sum_{k=0}^{n} 2^{n-k} C_n^k = (1+2)^n = 3^n
\end{aligned}$$

Notons de même, pour $B \in \mathcal{P}^{(n)}$, L_B l'ensemble des parties $(X, Y) \in \mathcal{P}^{(n)} \times \mathcal{P}^{(n)}$ telles que $X \cap Y = B$. Cet ensemble est en bijection avec l'ensemble des parties $(X', Y') \in \mathcal{P}(\mathbb{N}_n \setminus B) \times \mathcal{P}(\mathbb{N}_n \setminus B)$ telles que $X' \cap Y' = \emptyset$. Alors d'après le cas précédent on a

$$\text{Card } (L_B) = 3^{n-\text{Card}(B)}$$

On en déduit

$$\begin{aligned}\sum_{(X,Y)\in\mathcal{P}^{(n)}\times\mathcal{P}^{(n)}} \text{Card } (X \cap Y) &= \sum_{B\in\mathcal{P}^{(n)}} \text{Card } (B) \cdot \text{Card } (L_B) \\ &= \sum_{B\in\mathcal{P}^{(n)}} \text{Card } (B) \cdot 3^{n-\text{Card}(B)} \\ &= \sum_{k=0}^{n} \left(\sum_{B\in\mathcal{P}_k^{(n)}} k3^{n-k} \right) \\ &= \sum_{k=0}^{n} kC_n^k 3^{n-k}\end{aligned}$$

Mais $n(1+x)^{n-1} = \sum_{k=0}^{n} kC_n^k x^{k-1}$, alors

$$\sum_{(X,Y)\in\mathcal{P}^{(n)}\times\mathcal{P})(n)} \text{Card } (X \cap Y) = n4^{n-1}.$$ □

Enfin, pour la dernière somme notons que

$$\text{Card } (X \cup Y) = \text{Card } (X) + \text{Card } (Y) - \text{Card } (X \cap Y)$$

Alors, en combinant ce qui précède on trouve

$$\sum_{(X,Y)\in\mathcal{P}^{(n)}\times\mathcal{P})(n)} \text{Card } (X \cup Y) = 2^n(n2^{n-1}) + 2^n(n2^{n-1}) - n4^{n-1} = 3n4^{n-1}.$$ □

Solution 5.3. Il suffit de noter que l'ensemble considéré est

$$\mathcal{U}(3, n) = \{(x, y, z) \in \mathbb{N}^3 : x + y + z \leq n\}$$

qui est, d'après $\mathcal{D}_8$, de cardinal C_n^3. □

Solution 5.4. Notons

$$S = \left\{ (x_1, \ldots, x_n) \in \{-1, 0, 1\}^n : \sum_{k=1}^{n} x_k = 0 \right\}.$$

et

$$\widetilde{S} = \left\{ (A, B) \in \mathcal{P}^{(n)} \times \mathcal{P}^{(n)} : \text{Card}\,(A) = \text{Card}\,(B),\ A \cap B = \emptyset \right\}.$$

L'application $\varphi : S \longrightarrow \widetilde{S}$ qui à $(x_1, \ldots, x_n) \in S$ associe les deux ensembles $(A, B) \in \widetilde{S}$ définis par $A = \{i \in \mathbb{N}_n : x_i = 1\}$ et $B = \{i \in \mathbb{N}_n : x_i = -1\}$ est une bijection, donc Card (S) = Card $\left(\widetilde{S}\right)$.

D'autre part, l'ensemble $\widetilde{S}$ est une réunion disjointe des ensembles $(\widetilde{S}_k)_{0 \leq k \leq n/2}$ où

$$\widetilde{S}_k = \left\{ (A, B) \in \mathcal{P}^{(n)} \times \mathcal{P}^{(n)} : \text{Card}\,(A) = \text{Card}\,(B) = k,\ A \cap B = \emptyset \right\}.$$

et Card $\left(\widetilde{S}_k\right) = C_n^k C_{n-k}^k$. ALors

$$\text{Card}\left(\left\{ (x_1, \ldots, x_n) \in \{-1, 0, 1\}^n : \sum_{k=1}^{n} x_k = 0 \right\} \right) = \sum_{0 \leq k \leq n/2} \frac{n!}{(k!)^2 (n-2k)!}. \qquad \square$$

Solution 5.5. 1°.a L'idée est de noter que $P_k^{(n+1)} = P_k^{(n)} \cup \{B \cup \{n+1\} : B \in P_{k-1}^{(n)}\}$ et que cette réunion est disjointe. Donc, pour $1 < k \leq n+1$,

$$\sum_{B \in P_k^{(n+1)}} \prod_{i \in B} a_i = \sum_{B \in P_k^{(n)}} \prod_{i \in B} a_i + a_{n+1} \sum_{B \in P_{k-1}^{(n)}} \prod_{i \in B} a_i.$$

et

$$\sum_{B \in P_1^{(n+1)}} \prod_{i \in B} a_i = \sum_{i=1}^{n} a_i + a_{n+1}.$$

Alors,

$$\begin{aligned} 1 + \sum_{k=1}^{n+1} \left(\sum_{B \in P_k^{(n+1)}} \prod_{i \in B} a_i \right) x^k =& 1 + \sum_{k=1}^{n} \left(\sum_{B \in P_k^{(n)}} \prod_{i \in B} a_i \right) x^k + \\ & x a_{n+1} \left(1 + \sum_{k=1}^{n} \left(\sum_{B \in P_k^{(n)}} \prod_{i \in B} a_i \right) x^k \right) \\ =& (1 + x a_{n+1}) \left(1 + \sum_{k=1}^{n} \left(\sum_{B \in P_k^{(n)}} \prod_{i \in B} a_i \right) x^k \right). \end{aligned}$$

ce qui permet à la récurrence de tourner. □

1°.*b*. En prenant $x = -1$ on trouve

$$\prod_{k=1}^{n}(1-a_k) = 1 + \sum_{k=1}^{n}(-1)^k \left(\sum_{B\in P_k^{(n)}} \prod_{i\in B} a_i \right).$$

2°.*a*. L'application

$$\Theta : \mathcal{F} \longrightarrow \mathcal{P}(E) : f \mapsto f^{-1}(\{1\}).$$

vérifie que $\Theta\circ\Gamma$ est l'identité de $\mathcal{P}(E)$ et $\Gamma\circ\Theta$ est l'identité de $\mathcal{F}$. Γ est par conséquent bijective.

2°.*b*. La vérification est immédiate.

2°.*c*. On a

$$E \setminus (\bigcup_{k=1}^{n} A_k) = \bigcap_{k=1}^{n}(E \setminus A_k).$$

alors, en utilisant 2°.*b* on trouve $1 - \Gamma_A = \prod_{k=1}^{n}(1 - \Gamma_{A_k})$, puis en prenant 1°.*b*. en considération, on obtient

$$\Gamma_A = \sum_{k=1}^{n}(-1)^{k-1} \left(\sum_{B\in P_k^{(n)}} \prod_{i\in B} \Gamma_{A_i} \right).$$

2°.*d*. C'est evident.

2°.*e*. De 2°.*c*., et en utilisant 2°.*d*.,

$$\sum_{x\in E} \Gamma_A(x) = \sum_{k=1}^{n}(-1)^{k-1} \left(\sum_{B\in P_k^{(n)}} \sum_{x\in E} (\prod_{i\in B} \Gamma_{A_i}(x)) \right).$$

soit

$$\text{Card}\left(\bigcup_{k=1}^{n} A_k\right) = \sum_{k=1}^{n}(-1)^{k-1} \left(\sum_{B\in P_k^{(n)}} \text{Card}\left(\bigcap_{i\in B} A_i\right) \right).$$

3°. L'ensemble $\{\sigma \in \mathcal{S}(n) : \forall\, i \in B, \quad \sigma(i) = i\}$ est en bijection avec l'ensemble des permutations de l'ensemble $\mathbb{N}_n \setminus B$, qui est de cardinal $n - k$ alors

$$\text{Card}\,(\{\sigma \in \mathcal{S}(n) : \forall\, i \in B, \quad \sigma(i) = i\}) = (n-k)!.$$

4°. Il suffit de noter que

$$\bigcap_{i\in B} A_i = \{\sigma \in \mathcal{S}(n) : \forall\, i \in B, \quad \sigma(i) = i\}$$

et par conséquent, si $B \in P_k^{(n)}$,

$$\text{Card}\left(\bigcap_{i\in B} A_i\right) = (n-k)!.$$

Donc, en utilisant $2°.e$,

$$\begin{aligned}\text{Card}\left(\bigcup_{k=1}^{n} A_k\right) &= \sum_{k=1}^{n}(-1)^{k-1}\sum_{B\in P_k^{(n)}}(n-k)! = \sum_{k=1}^{n}(-1)^{k-1}C_n^k(n-k)!\\ &= n!\sum_{k=1}^{n}\frac{(-1)^{k-1}}{k!}\end{aligned}$$

5°. $G_n = \mathcal{S}(n) \setminus (\bigcup_{k=1}^{n} A_k)$. Alors,

$$g_n = \text{Card}\,(G_n) = n! - n!\sum_{k=1}^{n}\frac{(-1)^{k-1}}{k!} = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}.$$

$6°.a.$

$$\begin{aligned}a_{2n+1} - a_{2n-1} &= \frac{1}{(2n)!} - \frac{1}{(2n+1)!} > 0\\ a_{2n} \quad - a_{2n+1} &= \frac{1}{(2n+1)!} > 0\\ a_{2n-2} - a_{2n} \quad &= \frac{1}{(2n-1)!} - \frac{1}{(2n)!} > 0\end{aligned}$$

$6°.b.$ Les deux suites $(a_{2n})_{n\geq 0}$ et $(a_{2n+1})_{n\geq 0}$ sont adjacentes alors elles convergent vers la même limite $\lambda = 1/e$.

$6°.c.$ la relation demandée est équivalente à $a_{2n+1} < \lambda < a_{2n}$.

$6°.d.$ la relation demandée est équivalente à $a_{2n+1} < \lambda < a_{2n+2}$.

$6°.e.$ Si n est pair alors de $6°.c$ on a $g_n - 1 = E(\lambda(n!))$, et si n est impair alors de $6°.d$ on a $g_n = E(\lambda(n!))$. D'où le résultat. □

Solution 5.6. Nous allons démontrer le résultat plus général suivant:

$$\mathbb{P}: \left\{ \begin{array}{l} \text{Soit } A_1, A_2, \ldots, A_N. \ N \text{ sous ensembles d'un ensemble } X. \text{ On suppose que} \\ \qquad \forall\, i \in \mathbb{N}_N, \quad \text{Card}\,(A_i) > \dfrac{1}{2}\text{Card}\,(X)\,. \\ \text{Alors, il existe une partie } B \text{ dans } X \text{ telle que} \\ \qquad \text{Card}\,(B) \leq E(\lg(N+1)), \quad \text{et} \quad \forall\, i \in \mathbb{N}_N, \quad B \cap A_i \neq \emptyset. \end{array} \right\}$$

Fixons quelques notations, Si A est une partie de X, on note Γ_A la fonction indicatrice de A qui vaut 1 si $x \in A$ et 0 si $x \notin A$. Si x est un réel on pose $\varphi(x) = E\left(\dfrac{x+1}{2}\right) - 1$.

On remarque à propos de φ que, pour tout réel x, $\varphi^k(x) = E\left(\dfrac{x+1}{2^k}\right) - 1$, et que

$$\varphi^k(m) = 0 \iff E\left(\frac{m+1}{2^k}\right) = 1 \iff k = E(\lg(m+1)).$$

Montrons, d'abord le lemme suivant:

Lemme: Pour toute partie *non vide* $M \subset \mathbb{N}_N$, il existe $\widetilde{M} \subset M$ tel que

$$\text{Card}\left(M \setminus \widetilde{M}\right) \leq \varphi(\text{Card}\,(M)), \qquad \text{et} \qquad \bigcap_{k \in \widetilde{M}} A_k \neq \emptyset.$$

En effet, Notons, pour $x \in X$, $f(x) = \displaystyle\sum_{k \in M} \Gamma_{A_k}(x)$.

Si pour tout $x \in X$, $f(x) \leq \dfrac{1}{2}\text{Card}\,(M)$ alors

$$\frac{\text{Card}\,(M)}{2}\,\text{Card}\,(X) \geq \sum_{x \in X} f(x) \geq \sum_{k \in M} \text{Card}\,(A_k) > \text{Card}\,(M)\,\frac{\text{Card}\,(X)}{2}.$$

Ce qui est absurde.

On en déduit qu'il existe $\widetilde{x} \in X$ tel que $\displaystyle\sum_{k \in M} \Gamma_{A_k}(\widetilde{x}) > \frac{1}{2}\text{Card}\,(M)$.

On pose $\widetilde{M} = \{k \in M : \widetilde{x} \in A_k\}$. Alors clairement on a

$$\bigcap_{k \in \widetilde{M}} A_k \neq \emptyset \qquad \text{et} \qquad \text{Card}\left(\widetilde{M}\right) = \sum_{k \in M} \Gamma_{A_k}(\widetilde{x}) > \frac{1}{2}\text{Card}\,(M)\,.$$

Soit Card $\left(\widetilde{M}\right) \geq 1 + E\left(\dfrac{\text{Card }(M)}{2}\right)$, ou bien

$$\begin{aligned}\text{Card } \left(M \setminus \widetilde{M}\right) \leq & \text{Card } (M) - 1 - E\left(\frac{\text{Card } (M)}{2}\right) \\ \leq & E\left(\frac{1 + \text{Card } (M)}{2}\right) - 1 = \varphi(\text{Card } (M)).\end{aligned}$$

ce qui démontre le lemme.

On définit une suite de parties de $\mathbb{N}_N$ de la manière suivante:

a. Pour $p = 0$ on pose $T_p = \emptyset$.

b. Si $\bigcup_{k=0}^{p-1} T_k = \mathbb{N}_N$ on pose $T_p = \emptyset$.

c. Si $\bigcup_{k=0}^{p-1} T_k \neq \mathbb{N}_N$ alors d'après le lemme on trouve $T_p \subset \mathbb{N}_N \setminus (\bigcup_{k=0}^{p-1} T_k)$ telle que

$$\bigcap_{k \in T_p} A_k \neq \emptyset,$$

et
$$\text{Card } \left(\mathbb{N}_N \setminus (\bigcup_{k=0}^{p} T_k)\right) \leq \varphi\left(\text{Card } \left(\mathbb{N}_N \setminus (\bigcup_{k=0}^{p-1} T_k)\right)\right). \qquad (*)$$

Notons pour simplifier $R = E(\lg(N+1))$. Si pour tout $p \in \{0, 1, 2, \ldots, R\}$ on a $\mathbb{N}_N \neq \bigcup_{k=0}^{p} T_k$, alors d'après $(*)$

$$\begin{aligned}0 \leq \text{Card } \left(\mathbb{N}_N \setminus (\bigcup_{k=0}^{R+1} T_k)\right) \leq & \ \varphi\left(\text{Card } \left(\mathbb{N}_N \setminus (\bigcup_{k=0}^{R} T_k)\right)\right) \\ \leq & \ \varphi \circ \varphi\left(\text{Card } \left(\mathbb{N}_N \setminus (\bigcup_{k=0}^{R-1} T_k)\right)\right) \\ \leq \cdots \leq & \ \varphi^{R+1}(N) = -1\end{aligned}$$

Ce qui est contradictoire. Il en résulte qu'il existe $q \in \{1, 2, \ldots, R\}$ tel que $\mathbb{N}_N = \bigcup_{k=1}^{q} T_k$. On choisit, pour chaque $k \in \{1, \ldots, q\}$, un élément $x_k \in \bigcap_{j \in T_k} A_j$, et on pose $B = \{x_1, x_2, \ldots, x_q\}$, alors

$$\forall\, k \in \mathbb{N}_N, \quad B \cap A_k \neq \emptyset \quad \text{et} \quad \text{Card } (B) = q \leq E(\lg(N+1)). \qquad \square$$

L'exercice correspond au cas particulier $N = 1066$, où $10 = E(\lg(1067))$.

Solution 5.7. Notons que

$$f(r,n) = \frac{1}{C_n^r} \sum_{B \in \mathcal{P}_r^{(n)}} \min(B).$$

Mais si $B \in \mathcal{P}_r^{(n)}$ alors $\min(B)$ prend les valeurs $1, 2, \ldots, n-r+1$ et si $k \in \{1, 2, \ldots, n-r+1\}$ alors

$$\text{Card}\left(\{B \in \mathcal{P}_r^{(n)} : \min(B) = k\}\right) = C_{n-k}^{r-1}.$$

On conclut,

$$f(r,n) = \frac{1}{C_n^r} \sum_{k=1}^{n-r+1} k C_{n-k}^{r-1}. \qquad \spadesuit$$

$$\begin{aligned}
\sum_{k=0}^{n-r+1} k C_{n-k}^{r-1} &= \sum_{k=r-1}^{n} (n-k) C_k^{r-1} \\
&= \sum_{k=r-1}^{n} (n-k)(\, C_{k+1}^r - C_k^r \,) = \sum_{k=r-1}^{n} (n-k) C_{k+1}^r - \sum_{k=r}^{n} (n-k) C_k^r \\
&= \sum_{k=r}^{n} (n-k+1) C_k^r - \sum_{k=r}^{n} (n-k) C_k^r = \sum_{k=r}^{n} C_k^r \\
&= \sum_{k=r}^{n} (\, C_{k+1}^{r+1} - C_k^{r+1} \,) = C_{n+1}^{r+1}
\end{aligned}$$

Il en résulte, d'après $\spadesuit$, que $f(r,n) = C_{n+1}^{r+1} / C_n^r = \dfrac{n+1}{r+1}$. □

Solution 5.8. C'est une récurrence immédiate.

Chapitre Sixième

Solution 6.1. On utilise la propriété simple du cours: Pgcd $(a,b) =$ Pgcd $(a, b-\lambda a)$.

$$\begin{aligned}\text{Pgcd}\left(15n^2+8n+6, 30n^2+21n+13\right) =& \text{Pgcd}\left(15n^2+8n+6, 5n+1\right)\\ =& \text{Pgcd}\left(5n+6, 5n+1\right)\\ =& \text{Pgcd}\left(5, 5n+1\right) = \text{Pgcd}\left(5,1\right) = 1\end{aligned}$$

Ce qui démontre le résultat. □

Solution 6.2. Notons que

$$\begin{aligned}a_{n+1}+\sqrt{2}b_{n+1} =& (1+\sqrt{2}\,)^{n+1} = (1+\sqrt{2}\,)\cdot(a_n+\sqrt{2}b_n)\\ =& (a_n+2b_n)+\sqrt{2}\,(a_n+b_n).\end{aligned}$$

On en déduit les deux relations récurrentes: $a_{n+1} = a_n + 2b_n$ et $b_{n+1} = a_n + b_n$. Par conséquent

$$\text{Pgcd}\,(a_{n+1}, b_{n+1}) = \text{Pgcd}\,(b_{n+1}+b_n, b_{n+1}) = \text{Pgcd}\,(b_n, b_n+a_n) = \text{Pgcd}\,(b_n, a_n)\,.$$

Cette relation permet de démontrer par récurrence sur n que

$$\text{Pgcd}\,(a_n, b_n) = \text{Pgcd}\,(a_1, b_1) = 1.$$ □

Solution 6.3. Remarquons que si m et n sont deux entiers de $\mathbb{N}^*$, et si $m = qn + r$ avec $0 \le r < n$ alors $a^r - 1$ est le reste de la division euclidienne de $a^m - 1$ par $a^n - 1$. Car

$$\begin{aligned}a^m-1 =& a^{qn}a^r - a^r + a^r - 1 = a^r\,(a^{qn}-1) + a^r - 1\\ =& a^r\,(\sum_{k=0}^{q-1} a^{kn})\cdot(a^n-1) + a^r - 1.\end{aligned}$$

et $0 \le a^r - 1 < a^n - 1$.

Comme dans l'algorithme de calcul de PGCD, on définit par récurrence la suite $(r_k)_{k\in\mathbb{N}}$ en posant

$$r_0 = b, \quad r_1 = c, \quad r_{k+1} = \begin{cases} \text{le reste de la division de } r_{k-1} \text{ par } r_k, & \text{si} \quad r_k > 0. \\ 0, & \text{si} \quad r_k = 0. \end{cases}$$

et on note n le premier indice tel que $r_n \neq 0$ et $r_{n+1} = 0$, on sait alors que $r_n = d$.

Si l'on pose alors $R_0 = a^b - 1$, $R_1 = a^c - 1$,

$$R_{k+1} = \begin{cases} \text{le reste de la division de } R_{k-1} \text{ par } R_k, & \text{si} \quad R_k > 0. \\ 0, & \text{si} \quad R_k = 0. \end{cases}$$

On déduit de la remarque du debut et par récurrence que $R_k = a^{r_k} - 1$ pour $0 \leq k \leq n$.

On conclut que

$$\text{PGCD}\left(a^b - 1, a^c - 1\right) = \text{PGCD}\left(R_k, R_{k+1}\right) = \cdots = \text{PGCD}\left(R_n, R_{n+1}\right) = a^d - 1.$$

Comme $b \,|\, m$ et $c \,|\, m$ alors $(a^b - 1) \,|\, (a^m - 1)$ et $(a^c - 1) \,|\, (a^m - 1)$ donc

$$\text{PPCM}\left(a^b - 1, a^c - 1\right) \,|\, (a^m - 1)$$

Mais

$$\text{PPCM}\left(a^b - 1, a^c - 1\right) \cdot \text{PGCD}\left(a^b - 1, a^c - 1\right) = (a^b - 1)(a^c - 1).$$

Il en résulte,

$$(a^b - 1)(a^c - 1) \,|\, (a^m - 1)(a^d - 1). \qquad \square$$

Solution 6.4. Notons $a_n = 2^{2^{2n}} - 2$ et $b_n = 2^{2^{2n+1}} - 4$. Montrons que

$$7 \,|\, a_n \Longrightarrow (7 \,|\, b_n) \quad \text{et} \quad (7 \,|\, a_{n+1}).$$

En effet, supposons que $7 \,|\, a_n$ alors $b_n = (2^{2^{2n}})^2 - 4 = (a_n + 2)^2 - 4 = a_n(a_n + 4)$, donc $7 \,|\, b_n$. D'autre part, $a_{n+1} = (2^{2^{2n+1}})^2 - 2 = (b_n + 4)^2 - 2 = b_n(b_n + 8) + 14$, donc $7 \,|\, a_{n+1}$.

Mais $7 \,|\, a_0$, alors on a démontré par récurrence que, pour tout n, $7 \,|\, a_n$ et $7 \,|\, b_n$. Enfin $4^{2^{2n}} + 2^{2^{2n}} + 1 = a_n + b_n + 7$ donc $7 \,|\, (4^{2^{2n}} + 2^{2^{2n}} + 1)$. $\square$

Solution 6.5. Pour tout n on a,

$$2^{2n} = 4^n = (1+3)^n = 1 + 3n + 9\sum_{k=2}^{n} 3^{k-2}C_n^k = 1 + 3n + 9\lambda_n.$$

alors

$$2^{2n} + 6n - 1 = 9(n + \lambda_n).$$ □

Solution 6.6. Supposons que pour un certain n, 121 divise n^2+3n+5. On a $n^2+3n+5 = (n+7)(n-4)+33$, il en résulte que $11 \,|\, (n+7)(n-4)$. 11 étant premier alors $11 \,|\, (n+7)$ ou $11 \,|\, (n-4)$. Mais $(n+7) = (n-4)+11$ alors $11 \,|\, (n+7)$ et $11 \,|\, (n-4)$ d'où $121 \,|\, (n+7)(n-4)$. Or ceci, avec l'hypothèse $121 \,|\, (n^2+3n+5)$, implique que $121 \,|\, 33$ ce qui est contradictoire. Alors

$$\forall\, n \in \mathbb{N}, \qquad 121 \not| (n^2+3n+5).$$ □

Solution 6.7. Notons que $n^2 + (p-2q)n + q^2 = (n+p-q)(n-q) + pq$. Alors

$$p^2 \,|\, (n^2 + (p-2q)n + q^2) \quad \Longrightarrow \quad p \,|\, (n-q)(n+p-q).$$

p est un nombre premier, il en résulte que $p \,|\, (n-q)$ ou $p \,|\, (n+p-q)$. Mais ceci implique que $p \,|\, (n-q)$ et $p \,|\, (n+p-q)$, et par conséquent $p^2 \,|\, (n-q)(n+p-q)$. Or, par hypothèse $p^2 \,|\, (n+p-q)(n-q)+pq$, alors $p^2 \,|\, pq$ ce qui implique que $p \,|\, q$. □

Solution 6.8. Notons que pour tout n et m on a

$$\text{Pgcd}\,(2n+1, m) = \text{Pgcd}\,(2n+1, 2m)\,.$$

En utilisant la remarque précédente on peut écrire

$$\begin{aligned}
\text{Pgcd}\,\left(2n+1, n^3+n\right) &= \text{Pgcd}\,\left(2n+1, 2n^3+2n\right) \\
&= \text{Pgcd}\,\left(2n+1, 2n^3+2n-n^2(2n+1)\right) \\
&= \text{Pgcd}\,\left(2n+1, 2n-n^2\right) = \text{Pgcd}\,\left(2n+1, 4n-2n^2\right) \\
&= \text{Pgcd}\,\left(2n+1, 4n-2n^2+n(2n+1)\right) = \text{Pgcd}\,\left(2n+1, 5n\right) \\
&= \text{Pgcd}\,\left(2n+1, 5n-2(2n+1)\right) = \text{Pgcd}\,\left(2n+1, n-2\right) \\
&= \text{Pgcd}\,\left(2n+1-2(n-2), n-2\right)
\end{aligned}$$

Alors $\text{Pgcd}\,\left(2n+1, n^3+n\right) = \text{Pgcd}\,\left(5, n-2\right)$, ce qui donne le résultat. □

Solution 6.9. On a toujours $(n+1) \,|\, (n^2-1)$, donc $(n+1) \,|\, (n^2+1)$ implique que $(n+1)$ divise $(n^2+1)-(n^2-1) = 2$ ce qui montre que $n \in \{-3,-2,0,1\}$. D'autre part, si $n \in \{-3,-2,0,1\}$, alors $(n+1) \,|\, (n^2+1)$. Les valeurs cherchées sont donc $\{-3,-2,0,1\}$. □

Solution 6.10. Notons que

$$n^3 - 3 = (n^2+3n+9)(n-3) + 24$$

Alors $(n-3) \,|\, (n^3-3)$ si, et seulement si, $(n-3) \,|\, 24$. Alors

$$n \in \{-21,-9,-5,-3,-1,0,1,2,4,5,6,7,9,11,15,27\}.$$ □

Solution 6.11. Posons $b_k = 2^{3^k}+1$. Clairement on a $3 \,|\, b_0$. Supposons $k \geq 0$ et $3^{k+1} \,|\, b_k$. On a

$$b_{k+1} = (b_k-1)^3 + 1 = b_k^2(b_k-3) + 3b_k.$$

Or $3^{k+2} \,|\, b_k^2$ car $3^{k+1} \,|\, b_k$. Il en résulte que $3^{k+2} \,|\, b_{k+1}$. Ce qui démontre le résultat par récurrence. □

Solution 6.12. Supposons qu'il existe $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que

$$a > b, \qquad \frac{a^2+b^2}{a^2-b^2} = \lambda \in \mathbb{N}.$$

On peut, quitte à diviser a et b par $d = \text{PGCD}\,(a,b)$, supposer que $\text{PGCD}\,(a,b) = 1$. Alors $\text{PGCD}\,\left(a^2,b^2\right) = 1$.

Mais on a $(\lambda-1)\,a^2 = (\lambda+1)\,b^2$, donc a^2 divise $(\lambda+1)\,b^2$ et il est premier avec b^2, il en résulte que $a^2 \,|\, (\lambda+1)$; par exemple $\lambda+1 = a^2k$, et alors $\lambda-1 = b^2k$. De ce qui précède on trouve $k(a^2-b^2) = 2$, d'où

$$2 \geq a^2 - b^2 = (a-b)(a-b+2b) \geq 1 \cdot 3 = 3.$$

Une contradiction qui achève la démonstration de la propriété. □

Solution 6.13. Présentons les calculs dans un tableau:

k	r_k	q_k	t_k	s_k
0	60809		1	0
1	58483	1	0	1
2	2326	25	1	-1
3	333	6	-25	26
4	328	1	151	-157
5	5	65	-176	183
6	3	1	11591	-12052
7	2	1	-11767	12235
8	1		23358	-24287

Il en résulte que $\textsc{Pgcd}\,(60809, 58483) = 1$ et que $23358\,b - 24287\,a = 1$. □

Solution 6.14. *i*. Notons que pour tout $a \in \mathbb{N}^*$ et tout $k \in \mathbb{N}^*$,

$$(a-1)\,|\,(a^k-1).$$

Il en résulte que, $(2^{2^{n+1}}-1)\,|\,\left((2^{2^{n+1}})^{2^{m-n-1}}-1\right)$. Ce qui se traduit en disant que

$$\forall\, m > n, \qquad 2^{2^{n+1}}-1\,|\,F_m-2.$$

D'autre part, $2^{2^{n+1}}-1 = (2^{2^n}-1)(2^{2^n}+1)$. Alors, $\forall\, m > n, \qquad F_n\,|\,F_m-2$.

ii. On peut supposer $m > n$. Comme F_n et F_m sont des nombres impairs alors $d = \textsc{Pgcd}\,(F_n, F_m)$ est un nombre impair. D'autre part, $d\,|\,F_n$ et $F_n\,|\,(F_m-2)$, alors $d\,|\,(F_m-2)$. On sait aussi que $d\,|\,F_m$ alors $d\,|\,2$. Comme d est impair, $d = 1$.

iii. Soit, pour chaque n, p_n un nombre premier qui divise F_n. L'application

$$f : \mathbb{N} \longrightarrow \mathcal{P} : n \mapsto p_n$$

est injective d'après *ii*. Donc $\mathcal{P}$ est infini. □

Solution 6.15. *i*. On a

$$\textsc{Pgcd}\,(U_{n+2}, U_{n+1}) = \textsc{Pgcd}\,(U_{n+1}+U_n, U_{n+1}) = \textsc{Pgcd}\,(U_{n+1}, U_n)\,.$$

Comme $\textsc{Pgcd}\,(U_1, U_0) = 1$, alors une récurrence immédiate nous permet de montrer que $\textsc{Pgcd}\,(U_{n+1}, U_n) = 1$ pour tout $n \in \mathbb{N}$.

ıı. La relation demandée est vraie pour $p = 1$ et $p = 2$. Supposons qu'elle soit vraie pour $p-1$ et p (avec $p \geq 2$). ALors

$$\begin{aligned} U_{n+p} =& U_{n+p-1} + U_{n+p-2} \\ =& U_{n-1}U_{p-1} + U_nU_p + U_{n-1}U_{p-2} + U_nU_{p-1} \\ =& U_{n-1}(U_{p-1} + U_{p-2}) + U_n(U_p + U_{p-1}) \\ =& U_{n-1}U_p + U_nU_{p+1} \end{aligned}$$

d'où la relation demandée pour $p+1$.

ıı ı. Notons $\delta = \text{PGCD}\,(b, a)$ et $\Delta = \text{PGCD}\,(bc, a)$. Comme $\delta \,|\, bc$ et $\delta \,|\, a$ alors $\delta \,|\, \Delta$.

D'autre part a et c sont premiers entre eux alors Δ et c sont premiers entre eux. Mais $\Delta \,|\, bc$ alors d'après le lemme de Gauss, $\Delta \,|\, b$, or $\Delta \,|\, a$ aussi, donc $\Delta \,|\, \delta$. Par conséquent $\Delta = \delta$.

ıv. D'après *ıı*. on a

$$U_{qn+r} = U_{n-1}U_{(q-1)n+r} + U_nU_{(q-1)n+r+1}$$

Alors

$$\begin{aligned} \text{PGCD}\,(U_{qn+r}, U_n) =& \text{PGCD}\,\left(U_{qn+r} - U_nU_{(q-1)n+r+1}, U_n\right) \\ =& \text{PGCD}\,\left(U_{n-1}U_{(q-1)n+r}, U_n\right) \end{aligned}.$$

En utilisant *ıı ı*. et le fait que $\text{PGCD}\,(U_{n-1}, U_n) = 1$, on trouve

$$\text{PGCD}\,(U_{qn+r}, U_n) = \text{PGCD}\,\left(U_{(q-1)n+r}, U_n\right).$$

Cette relation permet de démontrer par récurrence sur q que

$$\text{PGCD}\,(U_{qn+r}, U_n) = \text{PGCD}\,(U_r, U_n).$$

v. Comme dans l'algorithme de calcul de PGCD, on définit par récurrence la suite $(r_k)_{k\in\mathbb{N}}$ en posant

$$r_0 = m, \quad r_1 = n, \quad r_{k+1} = \begin{cases} \text{le reste de la division de } r_{k-1} \text{ par } r_k, & \text{si} \quad r_k > 0. \\ 0, & \text{si} \quad r_k = 0. \end{cases}$$

et on note t le premier indice tel que $r_t \neq 0$ et $r_{t+1} = 0$, on sait alors que $r_t = d$.

D'après *ıv*. on a pour tout $1 \leq k \leq t$

$$\text{PGCD}\,\left(U_{r_{k-1}}, U_{r_k}\right) = \text{PGCD}\,\left(U_{r_k}, U_{r_{k+1}}\right)$$

ce qui permet de déduire que

$$\text{PGCD}\,(U_m, U_n) = \text{PGCD}\,\left(U_{r_t}, U_{r_{t+1}}\right) = U_d. \qquad \square$$

Solution 6.16. Notons que $a^2 = b^2 - 46127$, implique que $b > \sqrt{46127}$, ou bien $b \geq 215$. Or si $b = 215$ alors $b^2 - 46127 = 98$, et si $b = 216$ alors $b^2 - 46127 = 529 = 23^2$. Alors $46127 = b^2 - a^2$, avec $a = 23$ et $b = 216$. D'où la factorication en produit de deux nombres premiers: $46127 = (216 + 23)(216 - 23) = 239 \times 193$. □

Solution 6.17. Soit n un entier vérifiant la propriété demandée. Notons 2^α la plus grande puissance de 2 qui divise n. Alors d'après l'hypothèse $\alpha - 1$ est pair, $3 \,|\, \alpha$ et $5 \,|\, \alpha$. Par conséquent α est un multiple impair de 15:

$$\alpha = 15 + 30t, \qquad \text{pour un certain } t \in \mathbb{N}.$$

Notons 3^β la plus grande puissance de 3 qui divise n. Alors d'après l'hypothèse β est pair, $3 \,|\, (\beta - 1)$ et $5 \,|\, \beta$. Par conséquent $10 \,|\, \beta$ et $3 \,|\, (\beta - 1)$. Soit $\beta = 10u$ pour un certain entier u et tel que $3 \,|\, (10u - 1)$, mais $10u - 1 = 9u + u - 1$ donc $3 \,|\, (u - 1)$ ce qui donne $u - 1 = 3s$ pour $s \in \mathbb{N}$. D'où

$$\beta = 10 + 30s, \qquad \text{pour un certain } s \in \mathbb{N}.$$

Notons 5^γ la plus grande puissance de 5 qui divise n. Alors d'après l'hypothèse γ est pair, $3 \,|\, \gamma$ et $5 \,|\, (\gamma - 1)$. Par conséquent $6 \,|\, \gamma$ et $5 \,|\, (\gamma - 1)$. Soit $\gamma = 6v$ pour un certain entier v et tel que $5 \,|\, (6v - 1)$, mais $6v - 1 = 5v + v - 1$ donc $5 \,|\, (v - 1)$ ce qui donne $v - 1 = 5r$ pour $r \in \mathbb{N}$. D'où

$$\gamma = 6 + 30r, \qquad \text{pour un certain } r \in \mathbb{N}.$$

Enfin, si p^{α_p} est la plus grande puissance du nombre premier p, $(p \notin \{2, 3, 5\})$ qui divise n. Alors α_p doit être un multiple de 2, 3, et de 5. Alors $\alpha_p = 30\gamma_p$. On conclut que

$$n = 2^{15} \cdot 3^{10} \cdot 5^6 \cdot m^{30}$$

Où m est un entier naturel non nul. Le plus petit entier strictement positif n tel que $n/2$ soit un carré, $n/3$ sout un cube, et $n/5$ soit une puissance cinquième est

$$n = 2^{15} \cdot 3^{10} \cdot 5^6 = 30233088000000.$$ □

Solution 6.18. C'est une généralisation simple de l'exercice.11.

Solution 6.19. Notons d'abord que $2^{\lambda_n} \leq n < 2^{\lambda_n+1}$. Soit $m \in \mathbb{N}_n \setminus \{2^{\lambda_n}\}$. l'entier m s'écrit de manière unique $m = 2^r(2t+1)$. Si $r \geq \lambda_n$, alors $m = 2^{\lambda_n} v$ avec $v = 2^{r-\lambda_n}(2t+1) \geq 1$, ou bien $v = 1$ et ceci contredit le fait que $m \neq 2^{\lambda_n}$, ou bien $v \geq 2$ et alors $m \geq 2^{\lambda_n+1} > n$ ce qui est aussi contradictoire. On conclut que $m = 2^r(2t+1)$ avec $0 \leq r < \lambda_n$. D'autre part, $2t+1 \leq n$ alors $t < n/2$. on conclut que $m \,|\, (2^{\lambda_n-1} A_n)$.

Si $H_n \in \mathbb{N}$ pour un certain $n \geq 2$ alors

$$(2^{\lambda_n-1} A_n) H_n = \frac{A_n}{2} + \sum_{\substack{1 \leq k \leq n \\ m \neq 2^{\lambda_n}}} \frac{2^{\lambda_n-1} A_n}{m} \in \mathbb{N}$$

ou bien $(A_n/2) \in \mathbb{N}$ ce qui est absurde car A_n est impair. □

Chapitre Septième

Solution 7.1. On sait que $7 \,|\, 1001$, donc $10^3 \equiv -1 \bmod (7)$. Si $n = (b_\ell b_{\ell-1} \dots b_0)_{10}$ alors

$$n \equiv \sum_{k\geq 0} (-1)^k (b_{3k+2} b_{3k+1} b_{3k})_{10} \bmod (7).$$

Par exemple

$$\begin{aligned} 123\,456\,789\,987\,654\,321 &\equiv -321 + 654 - 987 + 789 - 456 + 123 \bmod (7) \\ &= -198 \equiv 5 \bmod (7). \end{aligned}$$

□

Solution 7.2. Pour tout $n \in \mathbb{N}$, on

$$(16)^n - 15n - 1 = (15+1)^n - 1 - 15n = 225 \sum_{k=2}^{n} C_n^k (15)^{k-2} \equiv 0 \bmod (225).$$ □

Solution 7.3. Notons que

$$A_n = n^2 + (n+1)^2 + (n+3)^2 = 3n^2 + 8n + 10 = 3n(n-4) + 10(n+1).$$

Mais $10 \,|\, A_n$ si, et seulement si, $2 \,|\, A_n$ et $5 \,|\, A_n$.

$$2 \,|\, A_n \iff 2 \,|\, 3n^2 \iff 2 \,|\, n.$$

et

$$5 \,|\, A_n \iff 5 \,|\, 3n(n-4) \iff \begin{cases} 5 \,|\, n \\ \text{ou} \\ 5 \,|\, (n-4) \end{cases}$$

On Conclut que

$$10 \,|\, A_n \iff \begin{cases} 2 \,|\, n \quad \text{et} \quad 5 \,|\, n \\ \text{ou} \\ 2 \,|\, n \quad \text{et} \quad 5 \,|\, (n-4) \end{cases}$$

ce qui est équivalent à

$$10 \,|\, A_n \iff \begin{cases} n \equiv 0 \bmod (10) \\ \text{ou} \\ n \equiv 4 \bmod (10) \end{cases}$$ □

Solution 7.4. Notons que

$$65 \,|\, (4n^2+1) \iff \begin{cases} 4n^2+1 \equiv 0 \bmod (5) \\ \text{et} \\ 4n^2+1 \equiv 0 \bmod (13) \end{cases}$$

Et

$$\begin{aligned} 4n^2+1 \equiv 0 \bmod (5) &\iff n^2-1 \equiv 0 \bmod (5) \\ &\iff (n-1)(n+1) \equiv 0 \bmod (5) \\ &\iff \begin{cases} 5 \,|\, (n-1) \\ \text{ou} \\ 5 \,|\, (n+1) \end{cases} \end{aligned}$$

Et

$$\begin{aligned} 4n^2+1 \equiv 0 \bmod (13) &\iff 9n^2-1 \equiv 0 \bmod (13) \\ &\iff (3n-1)(3n+1) \equiv 0 \bmod (13) \\ &\iff \begin{cases} 13 \,|\, (3n-1) \\ \text{ou} \\ 13 \,|\, (3n+1) \end{cases} \end{aligned}$$

On arrive à la conclusion suivante

$$65 \,|\, (4n^2+1) \iff \begin{cases} & (5 \,|\, (n-1) & \text{et} & 13 \,|\, (3n-1)) \\ \text{ou} & (5 \,|\, (n-1) & \text{et} & 13 \,|\, (3n+1)) \\ \text{ou} & (5 \,|\, (n+1) & \text{et} & 13 \,|\, (3n-1)) \\ \text{ou} & (5 \,|\, (n+1) & \text{et} & 13 \,|\, (3n+1)) \end{cases} \qquad \diamondsuit$$

Supposons que $5 \,|\, (n-a)$ et $13 \,|\, (3n-b)$ avec $(a,b) \in \mathbb{Z}^2$. Alors $n = a+5k$ pour un certain entier k tel que $3a-b+15k \equiv 0 \bmod (13)$ qui est équivalent à $2k \equiv b-3a \bmod (13)$. On multiplie alors les deux membres de cette égalité par 6 on trouve $-k \equiv 12k \equiv 6b-5a \bmod (13)$, ce qui donne enfin $k \equiv 5a-6b \bmod (13)$ ou bien $k = 5a-6b+13\ell$ pour un certain entier ℓ. Il en résulte que $n = a+5k = 26a-30b+65\ell$, ou d'une façon équivalente $n \equiv 26a-30b \bmod (65)$.

Inversement, si $n \equiv 26a-30b \bmod (65)$ alors $n \equiv a \bmod (5)$ et $n \equiv -4b \bmod (13)$ ou bien $3n \equiv -12b \equiv b \bmod (13)$. Conclusion,

$$5 \,|\, (n-a) \text{ et } 13 \,|\, (3n-b) \iff n \equiv 26a-30b \bmod (65).$$

En revenant à $\diamondsuit$ on trouve

$$65 \,|\, (4n^2+1) \iff \begin{cases} & n & \equiv & -4 & \bmod (65) \\ \text{ou} & n & \equiv & -9 & \bmod (65) \\ \text{ou} & n & \equiv & 9 & \bmod (65) \\ \text{ou} & n & \equiv & 4 & \bmod (65) \end{cases} \qquad \square$$

Solution 7.5. Supposons $0 < k < p$. On pose $c = k!(p-k)!$ et $b = C_p^k$. $p \not| c$ et p est un nombre premier alors PGCD $(p, c) = 1$, d'autre part, $p \,|\, bc = p!$. Alors d'après le lemme de Gauss $p \,|\, b$, ce qui se traduit par $C_p^k \equiv 0 \bmod (p)$ pout tout $k \in \{1, 2, \ldots, p-1\}$. Bien sûr $C_p^k \equiv 1 \bmod (p)$ si $k = 0$ ou $k = p$. □

Solution 7.6.

a	$(1945)^8$	5^{10}	5^{12}	$(1945)^{12}$	$(2001)^{2001}$	7^{355}	7^{355}
b	7	11	11	11	26	10	100
$a \bmod (b)$	1	1	3	4	25	3	43

Solution 7.7. D'après le théorème de Fermat, $(10)^6 \equiv 1 \bmod (7)$. Or pour tout $k \in \mathbb{N}^*$, $10^k \equiv 4 \bmod (6)$, (Par récurrence sur k). Alors, pour tout $k \geq 1$, $(10)^{10^k} \equiv (10)^4 \bmod (7)$. Par conséquent

$$\sum_{k=1}^{10} 10^{10^k} \equiv 10^5 \equiv -100 \equiv 5 \bmod (7).$$ □

Solution 7.8. Supposons que $abc \not\equiv 0 \bmod (7)$ alors les entiers a, b et c sont tous premiers avec 7. D'après le théorème de Fermat, si $7 \not| x$ alors $x^6 \equiv 1 \bmod (7)$ ou bien $7 \,|\, (x^3-1)(x^3+1)$ donc

$$7 \not| x \quad \Longrightarrow \quad x^3 \equiv 1 \bmod (7) \quad \text{ou} \quad x^3 \equiv -1 \bmod (7).$$

Il en résulte que

$$(7 \not| a,\ 7 \not| b,\ 7 \not| b) \quad \Longrightarrow \quad a^3 + b^3 + c^3 \not\equiv 0 \bmod (7).$$

Ce qui démontre le résultat. □

Solution 7.9. D'abord, la solution x, si elle existe, de $ax \equiv b \bmod (n)$ est unique modulo n. Car, comme PGCD $(a, n) = 1$, le fait $ax \equiv ay \bmod (n)$ implique $x \equiv y \bmod (n)$. Vérifions maintenant que $x = ba^{\varphi(n)-1}$ est une solution. En effet, d'après le théorème d'Euler $ax = ba^{\varphi(n)} \equiv b \bmod (n)$.

$3x \equiv 5 \bmod (26)$ alors $x = 5 \cdot 3^{11} \equiv 19 \bmod (26)$.

$13x \equiv 2 \bmod (40)$ alors $x = 2 \cdot (13)^{15} \equiv 34 \bmod (40)$.

$10x \equiv 21 \bmod (49)$ alors $x = 21 \cdot (10)^{41} \equiv 7 \bmod (49)$. □

Solution 7.10.

◇ Notons que $13 \,|\, 91$, $13 \,|\, 143$ et que $13 \not| 84$ alors l'équation $91x \equiv 84 \mod (143)$ n'admet pas de solutions.

◇ Dans ce cas $\text{PGCD}\,(91, 147) = 7$ et $7 \,|\, 84$ alors l'équation $91x \equiv 84 \mod (147)$ est équivalente à $13x \equiv 12 \mod (21)$. En multipliant les deux membres par 13 on trouve $169x \equiv 156 \mod (21)$ ou $x \equiv 9 \mod (21)$.

◇ La première équation montre que $x = 2 + 12a$ pour un certain $a \in \mathbb{Z}$. On remplace dans la deuxième équation: $2 + 12a \equiv 3 \mod (13)$ ce qui donne $a \equiv -1 \mod (13)$ ou bien $a = -1 + 13b$ pour un certain $b \in \mathbb{Z}$. Si l'on revient à x: $x = -10 + 156b$. Remplaçons alors dans la troisième équation: $-10 + 156b \equiv 5 \mod (7)$ qui est équivalente à $2b \equiv 1 \mod (7)$ ce qui montre que $b \equiv 4 \mod (7)$. *i.e.* $b = 4 + 7c$ pour un certain entier c. En revenant à x on trouve $x \equiv 614 \mod (1092)$.

◇ On trouve $x \equiv 34 \mod (1140)$. □

Solution 7.11. Notons d'abord que

$$a^{\varphi(n)} - 1 = (a-1) \sum_{k=1}^{\varphi(n)} a^{k-1}.$$

Comme $\text{PGCD}\,(a, n) = 1$ alors d'après le théorème d'Euler $n \,|\, (a^{\varphi(n)} - 1)$. Mais de plus on a $\text{PGCD}\,(a-1, n) = 1$ donc d'après le lemme de Gauss $n \,|\, \sum_{k=1}^{\varphi(n)} a^{k-1}$. □

Solution 7.12. D'après le théorème de Fermat on a, pour $1 \leq k < p$, $k^{p-1} \equiv 1 \mod (p)$ et $k^p \equiv k \mod (p)$. Alors

$$\sum_{k=1}^{p-1} k^{p-1} \equiv \sum_{k=1}^{p-1} 1 \equiv p - 1 \equiv -1 \mod (p).$$

et

$$\sum_{k=1}^{p-1} k^p \equiv \sum_{k=1}^{p-1} k \equiv p(\frac{p-1}{2}) \equiv 0 \mod (p).$$

Ce qui démontre le résultat. □

Solution 7.13. Supposons que $a^m \equiv 1 \bmod (a^n - 1)$. En effectuant une division euclidienne on a $m = qn + r$ avec $0 \leq r < n$. Mais

$$a^m - 1 = a^r(a^{nq} - 1) + a^r - 1$$

Donc $(a^n - 1) \,|\, (a^m - 1)$ et $(a^n - 1) \,|\, (a^{nq} - 1)$ d'où $(a^n - 1) \,|\, (a^r - 1)$ ce qui montre que $a^r - 1 = 0$, (car $a^r - 1 < a^n - 1$). Alors $r = 0$ et on a montré que

$$\mathrm{Ord}_{a^n-1}(a) = \min\{e \in \mathbb{N}^* : a^e \equiv 1 \bmod (a^n - 1)\} = n$$

Il en résulte d'après le corollaire.6 que $n \,|\, \varphi(a^n - 1)$. □

Solution 7.14. Notons $n = 2m + 1$ et $S_m = 2^{4m+2}(2^{4m+3} - 1) - 28$.

$$\begin{aligned} S_m =& 4\big(8 \cdot 2^{8m} - 2^{4m} - 7\big) \\ =& 4\big(8(2^{8m} - 1) - (2^{4m} - 1)\big) \\ =& 4(2^{4m} - 1)\big(8(2^{4m} + 1) - 1\big) \end{aligned}$$

Mais $2^{4m} - 1 = (16)^m - 1 \equiv 0 \bmod (5)$, et $8(2^{4m} + 1) - 1 = 8((16)^m + 1) - 1 \equiv 0 \bmod (5)$. Il en résulte que

$$100 \,|\, 4(2^{4m} - 1)\big(8(2^{4m} + 1) - 1\big).$$

D'où le résultat. □

Solution 7.15. Notons $R_p(n) = n - pE(n/p)$ pour $n \in \mathbb{N}$. Clairement $0 \leq R_p(n) < p$ et $R_p(n) = 0 \iff p \,|\, n$.

Pour $k \in \mathbb{N}_{p-1}$, on pose $f(k) = R_p(k^3) + R_p((p-k)^3)$. Comme $p \not| k^3$ et $p \not| (p-k)^3$ alors $2 \leq f(k)$. D'autre part, $f(k) < 2p$. Enfin, en développant $f(k)$ on voit immédiatement que $p \,|\, f(k)$. On conclut que $f(k) = p$ pour tout $k \in \mathbb{N}_{p-1}$.

$$\sum_{k=1}^{p-1} R_p(k^3) = \frac{1}{2}\sum_{k=1}^{p-1} f(k) = \frac{p(p-1)}{2}.$$

Mais, d'autre part,

$$\sum_{k=1}^{p-1} R_p(k^3) = \sum_{k=1}^{p-1}(k^3 - pE(\frac{k^3}{p})) = \frac{(p-1)^2p^2}{4} - p\sum_{k=1}^{p-1} E(\frac{k^3}{p})$$

En combinant ces deux résultats on trouve

$$\sum_{k=1}^{p-1} E\left(\frac{k^3}{p}\right) = \frac{(p+1)(p-1)(p-2)}{4} \qquad \clubsuit$$

Notons que si $k \in \mathbb{N}_M$ alors $1 \leq E(\sqrt[3]{kp}) < \sqrt[3]{(p-1)(p^2-2p)} < p-1$ car $p^2-2p < (p-1)^2$. Inversement, si $E(\sqrt[3]{kp}) < p-1$ alors $kp < (p-1)^3$ puis $k < p^2 - 3p + 2 + (1-1/p)$ ou bien $k \leq p^2 - 3p + 2 = M$. On a donc montré que

$$1 \leq k \leq M \iff 1 \leq E(\sqrt[3]{kp}) \leq p-2. \qquad (\dagger)$$

Soit $r \in \{1, 2, \ldots, p-2\}$, notons $B_r = \{k \in \mathbb{N}_M : r = E(\sqrt[3]{kp})\}$.

$$\begin{aligned} k \in B_r &\iff r \leq \sqrt[3]{kp} < r+1 \\ &\iff r^3 \leq kp < (r+1)^3 \\ &\iff \frac{r^3}{p} \leq k < \frac{(r+1)^3}{p} \\ &\iff E\left(\frac{r^3}{p}\right) + 1 \leq k \leq E\left(\frac{(r+1)^3}{p}\right) \end{aligned}$$

On a utilisé que $p \not| r^3$ et $p \not| (r+1)^3$. On en déduit que

$$\text{Card } (B_r) = E\left(\frac{(r+1)^3}{p}\right) - E\left(\frac{r^3}{p}\right). \qquad (\ddagger)$$

En utilisant ce qui précède

$$\begin{aligned} \sum_{k=1}^{M} E(\sqrt[3]{kp}) &= \sum_{r=1}^{p-2} r\text{Card } (B_r) \\ &= \sum_{r=1}^{p-2} r\left(E\left(\frac{(r+1)^3}{p}\right) - E\left(\frac{r^3}{p}\right)\right) \\ &= \sum_{r=1}^{p-2} rE\left(\frac{(r+1)^3}{p}\right) - \sum_{r=1}^{p-2} rE\left(\frac{r^3}{p}\right) \\ &= \sum_{r=1}^{p-1} (r-1)E\left(\frac{r^3}{p}\right) - \sum_{r=1}^{p-2} rE\left(\frac{r^3}{p}\right) \\ &= (p-1)E\left(\frac{(p-1)^3}{p}\right) - \sum_{r=1}^{p-1} E\left(\frac{r^3}{p}\right) \\ &= (p-1)^2(p-2) - \frac{(p-2)(p-1)(p+1)}{4} \end{aligned}$$

Ce qui donne

$$\sum_{k=1}^{M} E\left(\sqrt[3]{kp}\right) = \frac{(3p-5)(p-1)(p-2)}{4} \qquad \spadesuit$$

□

Exercices d'évaluation non résolus

Exercice .1 À la station de transylvanie I

À la station de transylvanie, il y a quatre types de travailleurs:

- Les hommes sains d'ésprit.
- Les hommes fous.
- Les vampires sains d'ésprit.
- Les vampires fous.

Tout ce qu'un homme sain d'ésprit dit est vrai. Tout ce qu'un homme fou dit est faux. Tout ce qu'un vampire sain d'ésprit dit est faux. Tout ce qu'un vampire fou dit est vrai. Dans les questions suivantes, on a affaire à des couples mariés, Il faut savoir qu'en transylvanie, le mariage entre un être humain et un vampire est rigoureusement interdit. Un être humain ne peut épouser qu'un être humain et un vampire se marie avec un autre vampire. On ne sait pas s'il y a des fous parmi les personnes interrogées.

1°. **Sylvain et Sylvia Nitrate.**

Comme on l'a déjà expliqué, les époux Nitrate sont deux humains ou deux vampires. Voici leurs déclarations:

Sylvia : Mon mari est un être humain.

Sylvain : Ma femme est un vampire.

Sylvia : L'un de nous deux est fous et l'autre ne l'est pas.

Monsieur et Madame Nitrate sont-ils des vampires ?

2°. Un jour je rencontre Monsieur et Madame Globule. Madame Globule m'affirma que tout ce que disait son mari était vrai. Quant à Monsieur Globule, il affirma que sa femme est folle. Que peut-on en déduire ?

3°. Un autre couple fait les déclarations suivantes:

Le mari : Nous sommes deux vampires.

L'épouse : Nous sommes dans le même état mental.

Qu'étaient-ils ?

4°. Enfin, voici les déclarations de Luigui et Manuela Byrdcliffe:

Luigui : Un de nous deux au moins est fou.

Manuela : C'est faux.

Que sont-ils ?

EXERCICE .2 **À la station de transylvanie II** (Suite de l'exercice 1.)

L'inspecteur de police **Craig** est appelé d'Angleterre pour aider à trouver les vampires. On arrête trois couples de personnes, et à chaque fois, on était sûr que l'une des deux était un vampire et l'autre un être humain.

1°. **Lucie et Minna**

Pour sa première enquête, Craig devait reconnaître le vampire, parmi deux sœurs, Lucie et Minna. Il ne savait pas si l'une d'elles était folle. Voici leur interrogatoire.

Craig à Lucie : Qu'avez vous à dire ?

Lucie : Nous sommes folles.

Craig à Minna : Est-ce vrai ?

Minna : Bien sûr que non.

L'inspecteur trouva immédiatement le vampire. Comment ?

2°. **Michael et Peter Karloff**

Pour sa deuxième enquête. L'inspecteur devait interpeler les frères Michael et Peter Karloff. Les frères déclarèrent:

Michael : Je suis un vampire.

Peter : Je suis un être humain.

Michael : Nous sommes, soit tous les deux fous, soit tous les deux sains d'esprit.

L'inspecteur trouva immédiatement le vampire. Comment ?

3°. **Karl et Martha Dracula**

Karl et Martha Dracula étaient jumeaux. On savait qu'un des deux était fou et que l'autre était sain d'esprit, mais on ne savait pas qui était le fou, et bien sûr, on ne savait pas qui était le vampire. Ils déclarèrent:

Karl : Ma sœur est un vampire.

Martha : Mon frère est fou.

Qui est le vampire ?

EXERCICE .3 Une princesse ou un tigre ?

Un roi a eu l'idée de donner à ses prisonniers une chance de retrouver la liberté. Un prisonier doit choisir entre deux cellules dont chacune peut cacher une princesse ou un tigre. S'il en choisit une cachant une princesse, il doit l'épouser, mais s'il tombe sur une cachant un tigre, il est dévoré (ou il dévorera le tigre !). Toutes les combinaisons étaient possibles ; Il pouvait y avoir deux tigres, deux princesses, ou un tigre et une princesse.

1°. Le roi emmena le premier prisonnier devant les deux cellules dont les affiches sont les suivantes:

$$\left\{\begin{array}{c}-1-\\ \textit{une au moins des deux cellules}\\ \\ \textit{contient une princesse}\end{array}\right\} \qquad \left\{\begin{array}{c}-2-\\ \textit{Il y a un tigre dans}\\ \\ \textit{l'autre cellule}\end{array}\right\}$$

Le roi affirma: "*Les deux affiches sont, soit toutes les deux sincères, soit toutes les deux fausses*". Où devait aller le prisonnier ?

2°. Le roi décida de changer les règles de jeu comme l'expliqua lui même aux prisonniers: "*L'affiche que je collerai sur la cellule* 1 *dira la vérité quand il y aura une princesse dans cette cellule et mentira quand ce sera un tigre. Pour la cellule* 2 *ce sera exactement le contraire ; quand il y aura une princesse l'affiche mentira et quand ce sera un tigre elle dira la vérité. Une fois encore chaque cellule pourra cacher indifféremment un tigre ou une princesse*". Le roi emmena le deuxième prisonnier voir affiches:

$$\left\{\begin{array}{c}-1-\\ \textit{les deux cellules}\\ \\ \textit{contiennent des princesses}\end{array}\right\} \qquad \left\{\begin{array}{c}-2-\\ \textit{les deux cellules}\\ \\ \textit{contiennent des princesses}\end{array}\right\}$$

Que devait faire le prisonnier ?

3°. Avec les mêmes règles du jeu qu'au 2° on montra au troisième prisonnier les affiches suivantes:

$$\left\{\begin{array}{c}-1-\\ \textit{Une cellule au moins}\\ \textit{contient une princesse}\end{array}\right\} \qquad \left\{\begin{array}{c}-2-\\ \textit{l'autre cellule contient}\\ \textit{une princesse}\end{array}\right\}$$

Qu'auriez vous fait à la place du prisonnier ?

4°. Le roi décida de compliquer l'épreuve, il demanda alors qu'on lui prépare une troisième cellule et expliqua au prisonnier qu'une seule cellule renfermait une princesse et qu'il avait fait mettre un tigre dans chacune des deux autres.Voici les affiches:

$\left\{\begin{array}{c}-1-\\ \textit{Il y a un tigre ici}\end{array}\right\}$ $\left\{\begin{array}{c}-2-\\ \textit{Cette cellule contient une princesse}\end{array}\right\}$ $\left\{\begin{array}{c}-3-\\ \textit{Il y a un tigre dans la cellule 2}\end{array}\right\}$

Que feriez-vous si vous étiez à la place du prisonnier ?

5°. Le roi est devenu furieux car tous les prisonniers ont eu la vie sauve. il décida de compliquer l'épreuve, emmena un autre prisonnier et lui expliqua qu'une des trois cellules contenait une princesse, une autre un tigre, et enfin la troisième était vide. l'affiche de la princesse disait la vérité, celle du tigre mentait, quant à celle de la cellule vide, il préférait ne rien dire. Voici les trois affiches:

$\left\{\begin{array}{c}1-\\ \textit{la cellule 3 est vide}\end{array}\right\}$ $\left\{\begin{array}{c}-2-\\ \textit{le tigre est dans la cellule 1}\end{array}\right\}$ $\left\{\begin{array}{c}-3-\\ \textit{cette cellule est vide}\end{array}\right\}$

Où était cachée la princesse ?

6°. **Un labyrinthe logique.**

Le roi employa les grands moyens. Au lieu de trois cellules, il en utilisa neuf, et il n'y cacha qu'une seule princesse. Toutes les autres étaient vides ou contenaient un tigre. Une fois encore le roi expliqua que l'affiche de la princesse disait vrai, et que les affiches des tigres mentaient ; pour les affiches des cellules vides il préférait ne rien dire.

voici les affiches:

$\left\{\begin{array}{c}-1-\\ \textit{La princesse est dans une cellule dont le numéro est impair}\end{array}\right\}$ $\left\{\begin{array}{c}-2-\\ \textit{cette cellule est vide}\end{array}\right\}$ $\left\{\begin{array}{c}-3-\\ \textit{l'affiche 5 est vraie ou l'affiche 7 est fausse}\end{array}\right\}$

$\left\{\begin{array}{c}-4-\\ \textit{l'affiche 1 est fausse}\end{array}\right\}$ $\left\{\begin{array}{c}-5-\\ \textit{l'affiche 2 ou l'affiche 4 est vraie}\end{array}\right\}$ $\left\{\begin{array}{c}-6-\\ \textit{l'affiche 3 est fausse}\end{array}\right\}$

$\left\{\begin{array}{c}-7-\\ \textit{la princesse n'est pas dans la cellule 1}\end{array}\right\}$ $\left\{\begin{array}{c}-8-\\ \textit{cette cellule contient un tigre et la cellule 9 est vide}\end{array}\right\}$ $\left\{\begin{array}{c}-9-\\ \textit{cette cellule contient un tigre et l'affiche 6 est fausse}\end{array}\right\}$

Le prisonnier réfléchit un long moment et finalement il s'écria: "Le problème est insoluble, vous n'êtes qu'un tricheur !", "Je sais", fit le roi en riant d'un air moqueur. "Ah, c'est drôle !" gémit le prisonnier qui ne trouvait pas ça drôle du tout. "Donnez-moi au moins un indice", supplia-t-il, "La cellule 8 est-elle vide ou non ?"

Le roi, qui avait du remords, fut assez généreux pour répondre sincèrement à cette question, mais à son grand désappointement le prisonnier découvrit aussitôt la princesse. Où était-elle ?

EXERCICE .4 Dialogue de fous

Soient a et b deux entiers compris entre 2 et 100. Pierre ne connait que leur produit P, Serge que leur somme S. S'ensuit le dialogue suivant:

Pierre: Je ne peux dire quels sont ces deux nombres.

Serge : Je le savais.

Pierre: Ah bon ? Alors je les connais.

Serge : Eh bien alors moi aussi je les connais.

Quels sont ces deux nombres ?

Indications

1°. On montrera d'abord que P n'admet pas de facteur premier strictement supérieur à 47 et on en déduira une majoration de S.

2°. On montrera ensuite que S n'est pas la somme de deux entiers premiers.

3°. Conclure.

EXERCICE .5 Pour $(n, \alpha) \in \mathbb{N}^* \times \mathbb{N}^*$, On rappelle que : $S_n^{(\alpha)} = \sum_{k=1}^{n} k^\alpha$

1°. Exprimer les sommes suivantes, en fonction de n et de $S_n^{(\alpha)}$, $S_n^{(\alpha+1)}$ et $S_n^{(\alpha+2)}$.

$$\sum_{k=1}^{n} S_k^{(\alpha)}, \qquad \sum_{k=1}^{n} k S_k^{(\alpha)}.$$

2°. Démontrer l'identité de Jacobi :

$$S_n^{(5)} + S_n^{(7)} = 2(S_n^{(3)})^2$$

EXERCICE .6

1°. On considère les quatre fonctions polynômiales:

$$B_0(x) = 1, \quad B_1(x) = x - \frac{1}{2}, \quad B_2(x) = x^2 - x + \frac{1}{6}, \quad B_3(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x.$$

a. Montrer que, pour $1 \leq k \leq 3$, on a $B_k'(x) = kB_{k-1}(x)$.

b. Étudier la fonction $x \mapsto B_3(x)$ et calculer $M = \sup_{0 \leq x \leq 1} |B_3(x)|$.

2°. Soit $\varphi : [0,1] \longrightarrow \mathbb{R}$ une fonction telle que les dérivées φ', φ'', $\varphi^{(3)}$, et $\varphi^{(4)}$ existent et sont continues. On pose

$$\psi(x) = \varphi(x) - B_1(x)\varphi'(x) + \frac{1}{2}B_2(x)\varphi''(x) - \frac{1}{6}B_3(x)\varphi^{(3)}(x).$$

En calculant la dérivée de ψ, montrer que

$$\psi(1) - \psi(0) = -\frac{1}{6}\int_0^1 B_3(x)\varphi^{(4)}(x)\,dx.$$

puis

$$\varphi(1) - \varphi(0) - \frac{1}{2}\left(\varphi'(1) + \varphi'(0)\right) + \frac{1}{12}\left(\varphi''(1) - \varphi''(0)\right) = -\frac{1}{6}\int_0^1 B_3(x)\varphi^{(4)}(x)\,dx. \quad (*)$$

3°. Soit $k \in \mathbb{N}^*$. En considérant la fonction $x \mapsto \varphi(x) = \operatorname{Log}(x+k)$, et en utilisant la relation $(*)$, montrer

$$\left|\operatorname{Log}(k+1) - \operatorname{Log} k - \frac{1}{2}\left(\frac{1}{k+1} + \frac{1}{k}\right) + \frac{1}{12}\left(\frac{1}{k^2} - \frac{1}{(k+1)^2}\right)\right| \leq M\int_0^1 \frac{dx}{(x+k)^4}. \quad (**)$$

où M est défini dans 1°.*b*.

4°. Pour $n \in \mathbb{N}^*$, on pose

$$\gamma_n = H_n - \operatorname{Log} n - \frac{1}{2n} + \frac{1}{12n^2}.$$

où $H_n = \sum_{k=1}^{n} \frac{1}{k}$ est le $n^{\text{ième}}$ nombre harmonique.

a. Montrer que la suite $(\gamma_n)_n$ converge vers γ la constante d'Euler.

b. En utilisant $(**)$, montrer que

$$|\gamma_k - \gamma_{k+1}| \leq \frac{M}{3}\left(\frac{1}{k^3} - \frac{1}{(k+1)^3}\right).$$

c. Soit $(n, m) \in \mathbb{N}^* \times \mathbb{N}^*$, avec $n < m$. En faisant la somme des inégalités précédentes pour k variant entre n et $m-1$. Montrer que

$$|\gamma_n - \gamma_m| \leq \frac{M}{3}\left(\frac{1}{n^3}\right).$$

d. En déduire que

$$\left|H_n - \operatorname{Log} n - \gamma - \frac{1}{2n} + \frac{1}{12n^2}\right| \leq \frac{1}{36\sqrt{3}\, n^3}.$$

e. En prenant $n = 3$, trouver un encadrement de γ, en précisant l'erreur commise.

EXERCICE .7 Soit p un nombre entier plus grand ou égal à 1.

1°. Calculer la valeur de $\widetilde{A}(r) = \sum_{k=rp}^{(r+1)p-1} E(\frac{k}{p})$.

2°. En déduire la valeur de $A(m) = \sum_{k=0}^{mp-1} E(\frac{k}{p})$.

3°. Trouver, enfin, la valeur de $B(n) = \sum_{k=0}^{n} E(\frac{k}{p})$ en fonction de $m = E(n/p)$ et de n.

4°. Quel est le cardinal de l'ensemble

$$\widetilde{T}(n, p) = \{(x, y) \in \mathbb{N} \times \mathbb{N} : \ x + py = n\}.$$

5°. En déduire le cardinal de l'ensemble

$$T(n, p) = \{(x, y) \in \mathbb{N} \times \mathbb{N} : \ x + py \leq n\}.$$

EXERCICE .8 Démontrer $\forall\, n \in \mathbb{N}^*, \quad E(\sqrt{n+1} + \sqrt{n}\,) = E(\sqrt{4n+2})$.

EXERCICE .9 Pour $n \in \mathbb{N}^*$, soit T_n le nombre de points à coordonnées entières dans le domaine $x > 0, y > 0, xy \leq n$. Montrer que

$$T_n = 2\left(\sum_{0<k\leq\sqrt{n}} E(n/k)\right) - (E(\sqrt{n}))^2.$$

EXERCICE .10 Ecrire la représentation binaire de $(1000)_{10}$, la représentation décimale de $(10011001)_2$.

EXERCICE .11 En base $p \geq 4$, montrer que $1 + (10)_p \times (11)_p \times (12)_p \times (13)_p = (131)_p^2$.

EXERCICE .12 Appelons x_n l'entier dont l'écriture binaire est $(\underbrace{1000\cdots001}_{n \text{ Chiffres}})_2$ où tous les chiffres sont égaux à 0 sauf ceux des bouts qui valent 1, (donc $n \geq 3$). Déterminer l'écriture binaire de x_n^2, x_n^3 et $x_n^3 - x_n^2 + x_n$.

EXERCICE .13 Résoudre les équations: $(23)_{10} = (27)_a$, $(136)_{10} = (256)_b$, et $(341)_{10} = (2331)_c$.

EXERCICE .14 Soit u_k l'entier positif dont l'écriture binaire consiste en k chiffres 1 suivis de $k+1$ chiffres 0 , suivis encore d'un seul chiffre 1. Montrer que u_k est le carré d'un certain entier v_k dont on déterminera l'écriture binaire.

EXERCICE .15 Calculer le cube en base 2 de l'entier a_k qui s'écrit dans cette base avec k chiffres 1 consécutifs.

EXERCICE .16 Soit $a = (12345679)_{10}$. Quelle est l'écriture décimale de $9a$?

EXERCICE .17 Trouver tous les entiers $n \geq 1$ dont le produit des chiffres en base 10 est égal à $n^2 - 10n - 22$.

EXERCICE .18 Trouver un entier n qui s'écrit avec trois chiffres en base 10, et tel que les écritures décimales des entiers $n, 2n, 3n$ utilisent ensemble exactement une fois les chiffres de 1 à 9.

EXERCICE .19 Calculer les deux sommes :

$$S_n = \sum_{k=1}^{n} E\left(\frac{\sqrt{k}-1}{2}\right) \quad \text{et} \quad T_n = \sum_{k=1}^{n} E(\sqrt[3]{k})$$

EXERCICE .20 On rappelle que H_n désigne le $n^{\text{ième}}$ nombre harmonique.

1°. Exprimer en fonction de n et de H_n la somme :

$$S_n = \sum_{k=1}^{n} \frac{1}{2k-1}$$

2°. Exprimer en fonction de n et des nombres harmoniques la somme :

$$T_n = \sum_{k=1}^{n} \frac{H_k}{4k^2-1}$$

3°. Exprimer en fonction de n et des nombres harmoniques les sommes :

$$A_n = \sum_{k=1}^{n} H_{2k} \quad \text{et} \quad B_n = \sum_{k=0}^{n} H_{2k+1}$$

4°. Exprimer la somme en fonction de n et de H_n la somme :

$$\sum_{k=1}^{n} k^2 H_k$$

5°. Exprimer en fonction de n et des nombres harmoniques la somme :

$$W_n = \sum_{1\leq i,j\leq n}^{n} \frac{1}{i+2j}$$

6°. Déterminer les sommes :

$$C_n = \sum_{1\leq i,j\leq n}^{n} \frac{1}{\min(i,j)} \quad \text{et} \quad C_n = \sum_{1\leq i,j\leq n}^{n} \frac{1}{\max(i,j)}$$

EXERCICE .21 Dans cet exercice p est un entier impair strictement supérieur à 1, et n est un entier naturel.

1°. Calculer Card $(\{k \in \mathbb{N}^* : 1 \leq 2kp \leq n\})$.

2°. Montrer

$$E\left(\frac{n+1}{p}\right) = \begin{cases} E\left(\frac{n}{p}\right)+1 & \text{si} \quad p \mid (n+1) \\ E\left(\frac{n}{p}\right) & \text{si} \quad p \not\mid (n+1) \end{cases}$$

3°. On considère dans le plan euclidien le triangle $\Delta_n = (OC_nD_n)$ où $C_n(n,0)$ et $D_n(n/2, n/p)$. On se propose de calculer le cardinal V_n de l'ensemble des points à coordonnées entières qui se trouvent dans le triangle Δ_n.

a. Montrer que les points O, D_n et D_{n+1} sont alignés.

b. Trouver une relation de récurrence entre V_n et V_{n+1}.

c. Déterminer V_n en fonction de n et p.

EXERCICE .22 Montrer que pour tout $n \geq 1$,

$$\sqrt{n+1} - \sqrt{n} < \frac{1}{2\sqrt{n}} < \sqrt{n} - \sqrt{n-1}.$$

1°. En déduire un encadrement similaire de $\displaystyle\sum_{k=2}^{n} \frac{1}{\sqrt{k}}$.

2°. Trouver ensuite la valeur de $E\left(\displaystyle\sum_{k=1}^{m^2} \frac{1}{\sqrt{k}}\right)$.

EXERCICE .23 Au village de $KAKO$ les gens parlent une langue simple qui s'appelle le $KOKO$. Les mots dans cette langue sont formés en utilisant seulement les deux lettres "K" et "O". Cette langue a aussi un grammaire très simple:" Un mot ne doit pas contenir deux lettres "K" consécutives". Par exemple, "$KOOK$" et "$KOKOO$" sont des mots, alors que "KKO" n'en est pas un.

On note S_n le nombre de mots formés de n lettres dans cette langue.

1°. Calculer S_1, S_2, et S_3.

2°. Trouver une relation simple entre S_{n+1}, S_n et S_{n-1}.

3°. Soit ω l'unique racine positive de $x^2 - x - 1 = 0$. On pose $v_n = S_{n+1} - \omega S_n$.

a. Montrer que $v_n = -\dfrac{1}{\omega}\, v_{n-1}$. En déduire que $v_n = \left(-\dfrac{1}{\omega}\right)^{n+2}$.

b. Calculer de deux manières la somme $\displaystyle\sum_{k=0}^{n-1} \frac{v_k}{\omega^{k+1}}$. En déduire la valeur de S_n en fonction de ω et de n.

c. Montrer que

$$S_n = E\left(\frac{\omega^{n+2}}{\sqrt{5}} + \frac{1}{2}\right).$$

EXERCICE .24 Pour $n \in \mathbb{N}^*$, on pose

$$U_n = E\left(\frac{1}{2} + \frac{1}{2} E\left(\sqrt{1 + 8E(\sqrt{n-1})}\right)\right).$$

Calculer

$$A_m = \text{Card}\left(\{n \in \mathbb{N}^* :\ U_n = m\}\right).$$

EXERCICE .25 On rappelle que H_n désigne le $n^{\text{ième}}$ nombre harmonique.

1°. En utilisant le fait que $\frac{1}{k} = \int_0^1 x^{k-1}\,dx$, pour tout $k \geq 1$, montrer que

$$\sum_{k=1}^{n}(-1)^{k-1}C_n^k\frac{1}{k} = H_n.$$

2°. Montrer aussi que

$$\sum_{k=1}^{n}(-1)^{k-1}C_n^k H_k = \frac{1}{n}.$$

EXERCICE .26 Donner suivant les valeurs de n, la valeur de PGCD $(2n+1, 9n+4)$. Même question pour PGCD $(2n-1, 9n+4)$.

EXERCICE .27 Déterminer deux entiers (s,t) tels que $143s - 67t = 1$. En déduire l'ensemble des couples $(x,y) \in \mathbb{N} \times \mathbb{N}$ tels que $143x + 67y = 20000$.

EXERCICE .28 Déterminer le reste de la division euclidienne de $(247)^{349}$ par 7.

EXERCICE .29 On se popose dans cet exercice de trouver toutes les solutions (a,b,c) dans $(\mathbb{N}^*)^3$ de l'équation:

$$a^2 + b^2 = c^2$$

1°. Soient u et v deux entiers positifs premiers entre eux tels que $uv = w^2$ pour un certain entier w. Montrer qu'il existe deux entiers positifs u_1 et v_1 tels que $u = u_1^2$ et $v = v_1^2$. (On pourrait considérer la factorisation en nombres premiers de u et de v.)

2°. Soient x, y, z trois entiers naturels strictement positifs deux à deux premiers entre eux et tels que $x^2 + y^2 = z^2$.

   a. Montrer que x ou y est pair, et que l'autre est impair. Montrer aussi que z est impair.

   On suppose dans la suite de cette question que x est impair.

   b. Montrer que PGCD $(2x, 2z)$ = PGCD $(z+x, z-x) = 2$. On pose alors $2u = z + x$ et $2v = z - x$.

   c. En déduire qu'il existe n et m tels que $u = n^2$ et $v = m^2$.

   d. Exprimer x ,y et z en fonction de n et de m.

3°. Soit $(a,b,c) \in (\mathbb{N}^*)^3$ tel que $a^2 + b^2 = c^2$.

   a. On pose $d =$ PGCD (a,b). Montrer que $d =$ PGCD $(b,c) =$ PGCD (a,c).

b. Montrer, pour $(a,b,c) \in \mathbb{N}^3$, l'équivalence entre les propriétés suivantes:

i. $a^2+b^2=c^2$.

ii. Il existe $(n,m,d) \in \mathbb{N}^3$ tel que

$$(a,b,c) = \begin{cases} (d(n^2-m^2), 2dnm, d(n^2+m^2)). \\ \text{ou} \\ (2dnm, d(n^2-m^2), d(n^2+m^2)). \end{cases}$$

EXERCICE .30 Pour tout $n \in \mathbb{N}$, on pose $\delta(n) = E(\sqrt{n+1}\,) - E(\sqrt{n}\,)$, et pour tout $p \in \mathbb{N}^*$ on pose

$$S_p = \sum_{1 \le k < p^2} \frac{E(\sqrt{k+1}\,)}{k(k+1)}.$$

1°. Montrer que, pour tout $n \in \mathbb{N}$, $\delta(n) \in \{0,1\}$.

2°. Montrer que $\delta(n)=1$ si, et seulement si, l'on peut trouver $k \in \mathbb{N}$ tel que $n = k^2-1$.

3°. Utiliser 1° et 2° pour montrer que la somme suivante

$$\widetilde{S}_p = \sum_{1 \le k < p^2} \frac{\delta(k)}{k}.$$

vaut $\dfrac{3}{4} - \dfrac{2p+1}{2p(p+1)}$.

4°. Exprimer la somme $\widetilde{S}_p$ en fonction de S_p, et de p.

5°. En déduire la valeur de la somme S_p. Quelle est la limite de S_p lorsque p tend vers l'infini ?

EXERCICE .31 Dans cet exercice nous nous proposons de démontrer

$$\forall\, n \in \mathbb{N}^*, \qquad \left| \sum_{k=0}^{n-1} (-1)^{E(\sqrt{k}\,)} \right| \le E(\sqrt{n}\,). \qquad (\spadesuit)$$

1°. Montrer que

$$\forall\, p \in \mathbb{N}, \qquad \sum_{k=p^2}^{(p+1)^2-1} (-1)^{E(\sqrt{k}\,)} = (-1)^p (2p+1).$$

2°. En déduire que

$$\forall\, m \in \mathbb{N}, \qquad \sum_{k=0}^{m^2-1} (-1)^{E(\sqrt{k}\,)} = (-1)^{m-1} m.$$

(On distinguera les cas m pair et m impair.)

3°. Soit $n \in \mathbb{N}^*$. On pose $m = E(\sqrt{n}\,)$. Montrer que

$$\sum_{k=0}^{n} (-1)^{E(\sqrt{k}\,)} = (-1)^m (n - m^2 - m + 1).$$

4°. En déduire une démonstration de (♠).

EXERCICE .32 Pour $x \in \mathbb{R}$ et $k \in \mathbb{N}^*$, on pose

$$u_k(x) = \sum_{n=1}^{m-1} \frac{1}{km+n} - \frac{x}{(k+1)m}.$$

1°. Exprimer la somme $S_{N-1}(x) = \sum_{k=0}^{N-1} u_k(x)$, en fonction des nombres harmoniques.

2°. Pour quelles valeurs de x est-ce que la limite $\lim_{N\to\infty} S_{N-1}(x)$ existe ? et quelle est la limite dans ces cas ?

Bibliographie

1°. “Concrete Mathematics”. *Graham, Knuth and Patashnik*. Addison-Wesley. 1989.

2°. “Discrete Mathematics”. *Mattsson*. John Wiley. 1993.

3°. “Le livre qui rend fou”. *Smullyan*. Dunod. 1984.

4°. “Exercices d’algèbre I”. *Monier*. Dunod université. 1991.

5°. “Combinatorics”. *Bollobás*. Cambridge. 1986.

6°. “Cours de Mathématiques spéciales I”. *Ramis, Deschamps, Odoux*. Masson. 1979.

7°. “Elementary number theory”. *Dudley* . Freeman and company. 1978.

8°. “Elementary number theory”. *Burton* . Allyn and Bacon, Inc. 1980.

9°. “A Course in number Theory”. *Rose* . Oxford Science Publications. 1988.