L'arithmétique au fil de l'histoire

Solutions aux exercices

Christian Aebi

Chapitre 1

Avertissement

Ce document contient à la fois
- la quasi totalité des réponses aux exercices,
- parfois même la méthode de résolution,
- et dans trois cas des prolongements (cf. ex. 55, 69, 78)

Toute erreur peut être communiquée directement à l'auteur christian.aebi@edu.ge.ch

Chapitre 2

Préambule

2.2 La relation de divisibilité et les propriétés des opérations

Ex. 1. a)

1) $36 \nmid 12$ 2) $7 \mid 119$ 3) $13 \mid (89^2 - 63^2)$
4) $(3^2 + 4^2) \mid 675$ 5) $3 \cdot 5 \cdot 7 \nmid 1875$ 6) $(1 + 2 + 3) \mid (1^3 + 2^3 + 3^3)$

b) $D_{120} = \{1; 120; 2; 60; 3; 40; 4; 30; 5; 24; 6; 20; 8; 15; 10; 12\}$ et $D_{75} = \{1; 75; 3; 25; 5; 15\}$, $D_{120} \cap D_{75} = \{1; 3; 5; 15\} = D_{15}$.

c) $\{1001; 1008; 1015; 1022; 1029\}$

Ex. 2. a) Comme $b = a \cdot m$ et $c = b \cdot n$ alors $c = a(mn)$ par l'associativité de $\cdot$

b) Si $b = a \cdot m$ et $c = a \cdot n$ alors $b + c = a(m + n)$ par la distributivité de $+$ sur $\cdot$

Ex. 3. $(a+b)^3 = (a+b)(a^2+2ab+b^2) = a^3+2a^2b+ab^2+ba^2+2ab^2+b^3 = a^3+3a^2b+3ab^2+b^3$

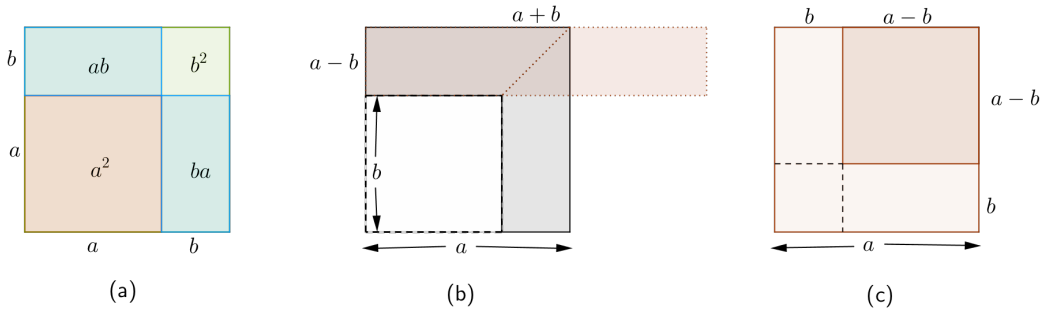

FIGURE 2.1 – Illustrations de trois identités remarquables

Ex. 4.

a) par comm. et assoc. de $+$ b) décomp. puis comm. et assoc. de $\cdot$ c) par distr.
d) identité (b) ex 3 e) identité (a) ex 3 f) $35 \cdot 33 + 55 \cdot 21 = 5 \cdot 7 \cdot 11 \cdot 3 \cdot 2 = 21 \cdot 11 \cdot 10 = 2310$

Ex. 5. $2^{100} \equiv 6 \pmod{10}$; $7^{100} \equiv 1 \pmod{10}$; $17 \cdot 2^{25} \equiv 4 \pmod{10}$; $(17 \cdot 13)^{35} \equiv 1 \pmod{10}$

Ex. 6. par commutativité et associatvité de $\cdot$

Ex. 7. $2007 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^4 + +2^2 + 2^1 + 1$

Ex. 8. a) $(2^4 + 1) \cdot 2^{25} = 2^{29} + 2^{25}$ b) $60 \cdot 60^{499} + 12 \cdot 3 = 12 \cdot (5 \cdot 600^{499} + 3)$
c) $20^{120} + 120^{20} = 20^3 \cdot 20^{117} + 120^2 \cdot 120^{18} = 64 \cdot (125 \cdot 20^{117} + 225 \cdot 120^{18})$
d) $400 - 12^{20^2} = (20 + 12^{200})(20 - 12^{200}) = (20^1 + 12^{200})(20^1 - 12^{200})$

Ex. 9. a) Dans les deux cas on obtient la décomposition : $2^{156} \cdot 3^{84}$, d'où $A = B$
b) $A = 324^{432} = 2^{864} \cdot 3^{1728}$ et $B = 432^{324} = 2^{1296} \cdot 3^{972}$, donc $A \neq B$
L'unicité de la décomposition en facteurs premiers d'un entier naturel est la clé.

Ex. 10. a) $1201206^2 = (1201205+1)^2 = 1442893452025+2\cdot 1201205+1 = 1442895854436$.

b) $(9876543211 - 987654309)^2 = 2^2 = 4$.

c) En effet, $11111^2 = (11110 + 1)^2 = 123432100 + 22220 + 1 = 123454321$.

d) $123456789^2 + 2 \cdot 123456789 \cdot 987654321 + 987654321^2 = (123456789 + 987654321)^2 = 1111111110^2 = 1234567898765432100$.

Ex. 11. a) Faux, le plus petit contre-exemple est $16 = 2^4$ et 17.

b) Faux, le plus petit contre-exemple est 2^{12}.

c) Faux. Si les deux premières égalités sont vraies en revanche, en comparant le chiffre des unités des deux membres $3^4 + 4^4 + 5^4 + 6^4 = 7^4$ on obtient $8 \neq 1$.

A propos des schémas démonstratifs

Ex. 12. a) Si $n \in \mathbb{N}^*$ alors $n^3 + 2n$ est divisible par 3.
Pour $n = 1$ on a bien $3|(1^3+2\cdot 1)$. Hyp. de réc. (HdR) : $3|\,((n-1)^3 + 2(n-1))$. D'où pour n on a $n^3+2n = ((n-1)+1)^3+2((n-1)+1) = 3(n-1)^3+2(n-1)+3(n+1)^2+3(n+1)+3$. Par HdR les deux premiers termes sont divisibles par 3. De plus, les trois derniers termes sont des multiples de 3. Dans la suite nous n'indiquerons que l'étape de récurrence.
b) $((n-1)+1)^3 + 5((n-1)+1) = [(n-1)^3 + 5(n-1)] + 3n(n-1) + 6$
c) $[1 + 2 + 2^2 + \ldots + 2^{n-1}] + 2^n = [2^n - 1] + 2^n = 2 \cdot 2^n - 1 = 2^{n+1} - 1$

$*$ **Ex. 13.** Là encore, nous ne montrons que le pas de récurrence

a) $(1+a)^{n+1} = (1+a)(1+a)^n \geq (1+a)(1+an) = 1+a^2n+an+a \geq 1+an+a = 1+a(n+1)$

b) $3^{2(n+1)} + 5 = 9 \cdot 3^{2n} + 9 - 4 = 9(3^{2n} + 1) + 4$

c) $15^4+4^{4(n+1)} = 15^4+4^4\cdot 4^{4n} = 4^4\cdot 4^{4n}+4^4\cdot 15^4+15^4-4^4\cdot 15^4 = 4^4(5^4+4^{4n})+15^4(1-4^2)(1+4^2)$

d) $(11^{n+3} + 12^{2n+3}) = 11 \cdot 11^{n+2} + 144 \cdot 12^{2n+1} = 11(11^{n+2} + 12^{2n+1}) + 133 \cdot 12^{2n+1}$

$*$ **Ex. 14.** Vrai. Pour $n = 1$ on a $11|(3^2 + 2)$. Supposons $11|(3^{2n} + 2^{6n-5})$. On a alors $3^{2n+2} + 2^{6n+1} = 9 \cdot 3^{2n} + 64 \cdot 2^{6n-5} = 9(3^{2n} + 2^{6n-5}) + 55 \cdot 2^{6n-5}$ divisible par 11 par HdR.

$*$ **Ex. 15.** a) $n(n-1) \div 2$

b) 0 ; 2 ; 5 ; $n(n-3) \div 2$

c) $n(n-1)(n-2) \div 6$

∗ **Ex. 16.** Pour n droites $\frac{n(n-1)}{2}$. En effet, supposons la formule vraie pour k droites (donc il y a $\frac{k(k-1)}{2}$ points d'intersection). Ajouter une droite qui intersecte chacune des k précédentes à des points d'intersection différents des précédents. D'où,

$$k + \frac{k(k-1)}{2} = \frac{k(k+1)}{2}.$$

∗ **Ex. 17.** Pour $u_n = \frac{1}{(3n-2)(3n+1)}$ on a $u_1 = \frac{1}{4}$, $u_2 = \frac{1}{28}$, $u_3 = \frac{1}{70}$ et $u_4 = \frac{1}{130}$. Le pas de récurrence est $\sum_{i=1}^{n+1} u_n = \frac{n}{3n+1} + \frac{1}{(3n+1)(3n+4)} = \frac{3n^2+4n+1}{(3n+1)(3n+4)} = \frac{(3n+1)(n+1)}{(3n+1)(3n+4)} = \frac{n+1}{3(n+1)+1}$

∗ **Ex. 18.** Montrons que le pas de récurrence de n à $n+1$.

a) $1 + 3 + 3^2 + \ldots + 3^n + 3^{n+1} = \frac{3^{n+1}-1}{2} + 3^{n+1} = \frac{3^{n+1}-1}{2} + \frac{3^{n+1}2}{2} = \frac{3^{n+2}-1}{2}$.

b) $1 + a + a^2 + \ldots + a^{n+1} = \frac{a^{n+1}-1}{a-1} + a^{n+1} = \frac{a^{n+1}-1}{a-1} + \frac{a^{n+1}(a-1)}{a-1} = \frac{a^{n+2}-1}{a-1}$

∗∗ **Ex. 19.** Prouvons que $(n+1)n(n-1)$ est divisible par 6 (qui n'est autre que $1 \cdot 2 \cdot 3$) sachant que 6 divise $n(n-1)(n-2)$. En effet, récrivons le produit sous la forme :

$$(n+1)n(n-1) = [(n-2)+3]n(n-1) = n(n-1)(n-2) + 3n(n-1)$$

Par HdR le premier terme est divisible par 6 et par l'exemple 3 de la brochure $n(n-1)$ est divisible par 2, d'où la conclusion.
Dans le cas général, on a à l'étape 1 que $n! := 1 \cdot 2 \cdot 3 \ldots n$ divise $1 \cdot 2 \cdot 3 \ldots n$ évidemment. L'hypothèse de récurrence complète HDRC consiste à supposer que le résultat est vrai non seulement pour un certain n pour lequel on a $n! \mid m(m+1)(m+2)\ldots(m+n-1)$, mais de surcroît $\forall k \leq n-1$ on a que $k! \mid j(j+1)(j+2)\ldots(j+k-1)$ et $\forall j \in \mathbb{N}^*$. Prouvons alors que $n! \mid (m+1)(m+2)\ldots(m+n)$, en utilisant d'abord la commutativité (passer le dernier facteur tout à gauche, puis en appliquant la distributivité) :

$$(m+1)(m+2)\ldots(m+n-1)(m+n) = [m+n](m+1)(m+2)\ldots(m+n-1) = \\ m(m+1)(m+2)\ldots(m+n-1) + n(m+1)(m+2)\ldots(m+n-1)$$

L'avant dernier terme est divisible par $n!$ par HdR et le dernier terme, sans le facteur n en rouge est divisible par $(n-1)!$ par HDRC et donc le tout est bien divisible par $n!$.

∗∗ **Ex. 20.** *Quelques indications et remarques pour faire avancer la recherche :*

a) A force de faire des essais sur des petits nombres l'on est amené à la conjecture : *tous ceux qui admettent un diviseur impair* > 1 *(c.-à-d. tout sauf les puissances de 2).* Il reste à la prouver !

b) Le premier contre-exemple devrait être recherché dans une 'zone' pauvre en nombres premiers, par exemple entre 113 et 127

c) Petite recherche qui pourrait servir d'exercice d'introduction au chapitre suivant.

d) La conjecture 2^n semble évidente...mais il faut se méfier des premières intuitions. Consulter par exemple *Le livre des nombres* de John Conway et Richard Guy.

e) Focaliser son attention sur la plus grande puissance de 2 (du dénominateur).

f) Les identités remarquables fournissent la première réponse. Quant à la deuxième, un raisonnement par l'absurde, en considérant un a minimal, ainsi qu'un b minimal, suivi d'une division euclidienne de b par a permet d'établir la deuxième.

g) Pour une preuve générale consulter :
`http://www.vsmp.ch/crm/articles_bulletin/B137_CA.pdf`

h) Étant donné qu'il y a un nombre pair de termes il est tentant de regrouper ces derniers par couple. Il reste à trouver comment. Garder à l'esprit que la somme de deux termes doit faire apparaître le premier p au numérateur. Éventuellement travailler sur un exemple concret en prenant $p = 7$, puis généraliser.

i) Utiliser le principe multiplicatif : si $n + 1 = i + j$ avec $0 < i, j < n + 1$ et que la première parenthèse gauche se referme en contenant i paires de parenthèses (y compris elle-même) alors à la droite de cette expression, il y aura j paires de parenthèses avec $i + j = n + 1$.
$C_4 = 14$, $C_5 = 42$ et $C_6 = 132$, de plus la suite obtenue s'appelle les *nombres de Catalan*. Une présentation détaillée figure à l'URL :
`https://en.wikipedia.org/wiki/Catalan_number`

Chapitre 3

Quelques situations historiques et leurs prolongements

3.1 La séparation du pair et de l'impair et les multiples d'un nombre

Ex. 21. a) $2a_1 + 2a_2 + \ldots + 2a_n = 2(a_1 + a_2 + \ldots + a_n)$, si les $a_i \in \mathbb{N}$

b) $(2m + 1) + (2n + 1) = 2(m + n + 1)$

c) $(2m) \cdot (2n + 1) = 2(m(2n + 1))$

d) $(2m_1 + 1) \cdot (2m_2 + 1) = (2m_1 + 1)2m_2 + (2m_1 + 1)$, puis par récurrence

e) Supposons $n^3 = 2m$. Par l'absurde, si n était impair alors par l'exercice précédent n^3 serait aussi impair. Contradiction.

Ex. 22. a) Si $x \neq 3n$ alors $x = 3n + 1$ ou $x = 3n + 2$ qui élevés au carré $\notin M_3$.

b) $(3n + 2)^2 - (3n + 1)^2 = 3(2n + 1) \in M_3$

c) $(5n + 1)^2 + (5n + 2)^2 + (5n + 3)^2 + (5n + 4)^2 = 5 \cdot N + (1^2 + 2^2 + 3^2 + 4^2) = 5 \cdot N + 30$ pour un certain $N \in \mathbb{N}$.

d) $(7n)^2 + (7n + 1)^2 + (7n + 2)^2 + (7n + 3)^2 + (7m - 3)^2 + (7m - 2)^2 + (7m - 1)^2 = 7 \cdot N + (1^2 + 2^2 + 3^2) \cdot 2 = 7 \cdot N + 14 \cdot 2$. Donc, oui.
$(9n)^2 + (9n + 1)^2 + (9n + 2)^2 + (9n + 3)^2 + (9n + 4)^2 + (9n - 4)^2 + (9m - 3)^2 + (9m - 2)^2 + (9m - 1)^2 = 9 \cdot N + (1^2 + 2^2 + 3^2 + 4^2) \cdot 2 = 9 \cdot N + 30 \cdot 2$. Donc, non.

e) $(n - 1)^3 + n^3 + (n + 1)^3 = 3(n^3 + 2n)$. Donc, oui.

f) A prouver (par récurrence) $1^2 + 2^2 + \ldots + (n - 1)^2 = (n - 1)n(2n + 1)/6$.
Comme $(n - 1, n) = 1$ et $(2n + 1, n) = 1$ alors la condition nécessaire et suffisante est que n soit impair et non divisible par 3.

3.2 Les nombres figurés

Ex. 23. a) $T_5 = 15$, $T_6 = 21$ et $T_7 = 28$.

b) $T_1 + T_2 = 4$, $T_2 + T_3 = 9$, $T_3 + T_4 = 16$, $\ldots$, $T_6 + T_7 = 49$, $T_{n-1} + T_n = n^2$,

c) Voir Figure (3.1) qui illustre $T_3 + T_2 = 3^2$

d) $T_7 + T_8 = (T_6 + 7) + (T_7 + 8) = (T_6 + T_7) + (7 + 7 + 1) = 7^2 + 2 \cdot 7 + 1 = 8^2$.

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

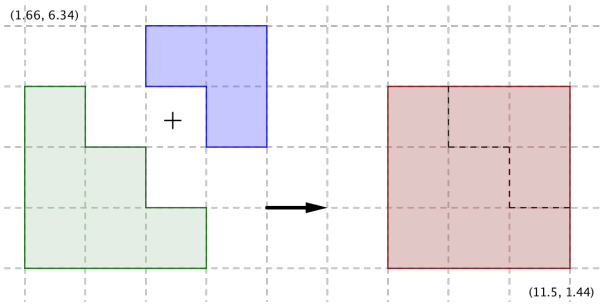

FIGURE 3.1 – La somme de T_3 et T_2

Ex. 24. a) $3^2 + 4^2 = 25 = 5^2$. Supposons que $(n-1)^2 + n^2 = (n+1)^2$. D'où $n^2 - 4n = 0$ et donc $n_1 = 0$ et $n_2 = 4$ sont les deux seules solutions.

b) $324 = 4 \cdot 81 = 18^2$, $2601 = 2700 - 99 = 9 \cdot 289 = (3 \cdot 17)^2 = 51^2$. 8007 se termine par un 7 et le chiffre des unités d'un carré ne peut être que 0 ; 1 ; 4 ; 5 ; 6 ou 9.

c)

d) Voir Figure (3.2).

e) Le pas de récurrence est : $(1 + 3 + 5 + (2n - 1)) + (2n + 1) = n^2 + 2n + 1 = (n + 1)^2$

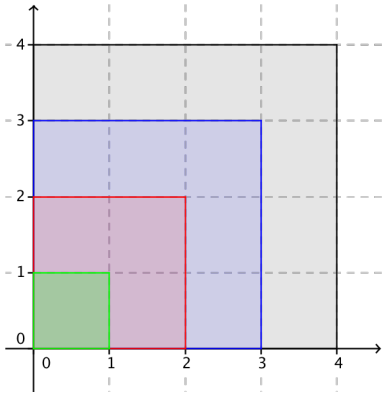

FIGURE 3.2 – La somme des quatre premiers nombres impairs $1 + 3 + 5 + 7$

Ex. 25. $T_n = C_m \Leftrightarrow \frac{n(n+1)}{2} = m^2 \Leftrightarrow 4n^2 + 4n = 2 \cdot (2m)^2 \Leftrightarrow (2n+1)^2 - 1 = 2 \cdot (2m)^2$.

Ex. 26. a) Voir Figure (3.3).

b) Chaque côté de P_{n+1} contient $n+1$ points et ses extrémités appartiennent à deux côtés distincts. Ainsi, si $P_n = 1 + 4 + 7 + \ldots + (3(n-1)+1)$ alors en additionnant les sommets de trois côtés on obtient : $P_{n+1} = 1 + 4 + 7 + \ldots + (3(n-1)+1) + 3(n+1) - 2 = 1 + 4 + \ldots + 3n + 1$.

c) Le pas de récurrence est $P_{n+1} = P_n + 3n + 1 = \frac{1}{2}(3(n-1)^2 + 5(n-1) + 2) + 3n + 1 = \frac{1}{2}(3n^2 + 5n + 2)$.

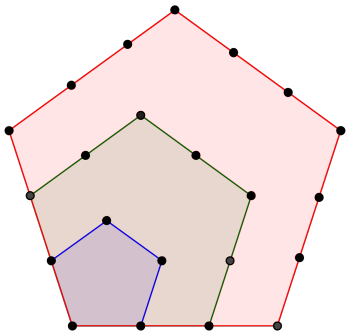

FIGURE 3.3 – Les quatre premiers nombres pentagonaux

Ex. 27. a) Voir Figure (3.4)

b) Le pas de récurrence est : $H_n = H_{n-1} + T_n = \frac{1}{6}(n-1)n(n+1) + \frac{3}{6}n(n+1) = \frac{1}{6}(n^3+3n^2+2n) = \frac{1}{6}n(n+1)(n+2)$

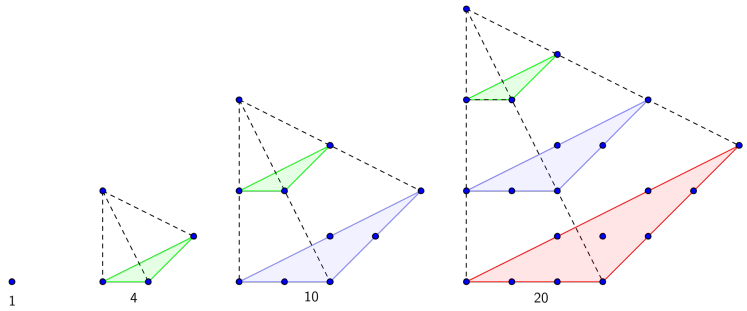

FIGURE 3.4 – Les quatre premiers nombres tétraédriques

Ex. 28. a) 1, 8, 27, 64, 125, 216, 343, 512, 729, 1000

b) *Conjecture* : $1^3 + 2^3 + \ldots + n^3 = T_n^2$
Preuve : (hérédité)

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

∗ **Ex. 29.** a) On peut soit développer $(a-b)^3$ puis réduire, soit factoriser $a^3 - b^3$.

b) Dans le membre de gauche, à l'exception des extrémités, un terme sur deux s'annule. Dans celui de droite, la distributivité permet de justifier la formule.

c) Il suffit d'isoler S_2, puis de factoriser.

d) $S_3(n) = \frac{1}{4}n^2(n+1)^2$

e) $S_4(n) = \frac{1}{30}n(n+1)(2n+1)(3n^2+3n-1)$
La forme $\frac{S_4(n)}{S_2(n)} = \frac{6 \cdot T_n - 1}{5}$ est prouvée par un simple développement, puis réduction.

3.3 Les nombres premiers ou linéaires

Ex. 30. Si n est composé alors $n = p \cdot q$ avec $p > 1$ et $q > 1$. L'un des deux facteurs doit être plus petit ou égal à $\sqrt{n}$. Sinon, on aurait $n = p \cdot q > \sqrt{n} \cdot \sqrt{n} = n$ une contradiction. Réciproquement, si $1 < p < \sqrt{n}$ et $p \mid n$ alors évidemment n est composé.

Ex. 31. Les critères élémentaires de divisibilité et une identité donnent :
a) $3 \mid 123'456'789$ b) $5 \mid 89 \cdot 95 \cdot 101$ c) $7 \mid (630 + 49)$ d) $11 \mid 1331$ e) $2 \mid (97^{98} + 1)$

Ex. 32. Si n est composé alors $2^n - 1$ est composé, car si $n = 2m$ alors $2^{2m} - 1 = (2^m - 1)(2^m + 1)$ et chacun des facteurs est > 1. Si $n = k \cdot m$ où chacun des facteurs est impair alors $2^{km} - 1^{km} = (2^k)^m - 1^m = (2^k - 1)(2^{km-k} + 2^{km-k-1} + \ldots + 2 + 1)$.
Attention, si $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$ sont premiers, en revanche $2^{11} - 1 = 2047 = 23 \cdot 89$ est donc composé.

Ex. 33. $201 = 3 \cdot 67$, $202 = 2 \cdot 101$, $203 = 7 \cdot 29$, $205 = 5 \cdot 41$ et 211 est premier.

∗ **Ex. 34.** a) si $a = 4m + 1 \in \mathfrak{H}$ et $b = 4n + 1 \in \mathfrak{H}$ alors $a \cdot b = (4m + 1)(4n + 1) = 4(4mn + m + n) + 1 \in \mathfrak{H}$.

b) L'ensemble des atomes $\{5; 9; 13; 17; 21; 29; 33; 37; 41; 49; \ldots\}$ et l'ensemble des molécules est $M = \{5^2; 5 \cdot 9; 5 \cdot 13; 9 \cdot 9; 5 \cdot 17; 5 \cdot 21; 9 \cdot 13; 5^3; 5 \cdot 29; 9 \cdot 17; 5 \cdot 33; 5 \cdot 37; 5 \cdot 41; 13 \cdot 17; \ldots\}$

c) $21 \cdot 33 = (3 \cdot 7) \cdot (3 \cdot 11) = 693 = (3 \cdot 3) \cdot (7 \cdot 11) = 9 \cdot 77$ et les nombres 21, 33, 9 et 77 sont des atomes (dans $\mathfrak{H}$).

Un exercice de ce type avait été inventé par David Hilbert (1862-1943, célèbre mathématicien allemand) pour ses élèves, d'où la lettre $\mathfrak{H}$.

3.4 Le triangle de Pascal et les coefficients binomiaux

Ex. 35. La (double) distributivité de $(a + b)$ sur $(a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4)$ impose au coefficient de a^2b^3 d'être la somme de 6 et 4.

Ex. 36. a) 12

b) $\binom{11}{8} = \frac{11 \cdot 10 \cdot 9}{1 \cdot 2 \cdot 3} = 165$.

c) 10, car à l'exception des extrémités, tous les coefficients binomiaux sont divisibles par le nombre premier 11. Cette observation est la clef de la preuve d'Euler du petit théorème de Fermat qui figure au chapitre suivant.

Ex. 37. a) $-\binom{8}{3} \cdot 3^5 \cdot 5^3 = -1701000$.

b) 4 car contrairement à l'exercice précédent, l'exposant est un nombre composé.

∗ **Ex. 38.** Un terme général aura la forme $a^i b^j c^k$, où $0 \leq i \leq 11$.
Si $i = 11$ alors il n'y a qu'un terme, $0 \cdot 7 + 1$.
Si $i = 10$ alors il y a $8 = 1 \cdot 7 + 1$ termes possibles.
Si $i = 9$ alors il y a $15 = 2 \cdot 7 + 1$ termes possibles. Et ainsi de suite.
Et si $i = 0$ alors il y a $78 = 11 \cdot 7 + 1$ termes possibles.
En tout, il y a alors $7 \cdot (1 + 2 + \ldots + 11) + 12 = 474$ termes.

∗ **Ex. 39.** a) Par la formule du binôme on obtient $7 \cdot M + 1^{123}$, où $M \in \mathbb{N}$ et donc le reste vaut 1.

b) Effectuons d'abord la division euclidienne de 1234567890 par 7. On obtient

$$1234567890 = 176366841 \cdot 7 + 3.$$

En appliquant le formule binomiale sur $(176366841 \cdot 7 + 3)^{1729}$, on voit que la division avec reste est identique à celle de 3^{1729} par 7. Si l'on observe les restes des divisions par 7 des puissances successives de 3 on obtient : 3 ; 2 ; 6 ; 4 ; 5 ; 1. Ainsi $3^6 = 7 \cdot 104 + 1$. D'où, pour obtenir le reste de 3^{1729} il suffit de l'écrire sous la forme $3^{6 \cdot 104+1} = (3^6)^{104} \cdot 3^1$. Donc le reste est 3.

c) Une fois de plus, commençons par écrire $47 = 7 \cdot 6 + 5$. D'où, par le même raisonnement qu'au point b) on aura même reste que $5^{38^{91}}$. Or, les restes des divisions par 7 des puissances successives de 5 sont 5 ; 4 ; 6 ; 2 ; 3 ; 1 et ainsi de suite (la période est aussi d'ordre 6). Ecrivons $38 = 6 \cdot 6 + 2$. D'où :

$$5^{38^{91}} = 5^{(6 \cdot 6+2)^{91}} = (5^6)^N \cdot 5^{2^{91}} \text{ pour un certain } n \in \mathbb{N}$$

Le reste de la division par 7 de $(5^6)^N$ est 1. Il demeure l'étude du reste de la division par 6 de 2^{91}. Or, les puissances successives de 2 sont 2 , 4 et ainsi de suite (donc d'ordre 2). Le reste de la division par 6 de 2^{91} est donc 2, et enfin le reste de la division par 7 de 5^2 est 4.

Remarque 1. Le calcul ci-dessus sera simplifié énormément grâce à l'invention (ou à la découverte) par Gauss du calcul modulo un nombre entier, méthode figurant au tout début son célèbre ouvrage, *Recherches Arithmétiques* de 1801.

∗ **Ex. 40.** $\binom{n}{k} = \frac{n(n-1)(n-2)...(n-k+1)(n-k)(n-k-1)...2 \cdot 1}{(n-k)(n-k-1)...2 \cdot 1 \cdot 1 \cdot 2 \cdot 3...k} = \frac{n!}{(n-k)! \cdot k!}$

∗ **Ex. 41.** a) Par la formule du binôme : $2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k}$

b) $0 = (1-1)^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k}$

∗ **Ex. 42.** a) Si D est fixé en première position alors par le résultat précédent il y a 6 possibilités. D pouvant avoir 3 autres positions on a alors $6+6+6+6 = 4 \cdot 6 = 4! = 24$.

b) Même raisonnement pour obtenir $5! = 120$.

c) Et par récurrence on obtient $n!$ dans le cas général.

∗ **Ex. 43.** a) Dénombrons le nombre de sous-ensembles n'ayant pas c comme élément. Il y en a 4. Si à chacun de ces sous-ensembles on introduit le c alors on aura toute la collection des sous-ensembles de E_3 possibles, et donc il y en a $4 + 4 = 8$. Un raisonnement analogue permet de montrer que $|\mathcal{P}(E_4)| = 16$, c'est-à-dire, le cardinal de l'ensemble des parties de E_4 vaut 16.

b) Ainsi à chaque étape le nombre de sous-ensembles va doubler.
D'où la formule 2^n dans le cas général.

∗ **Ex. 44.** Effectuons une preuve par récurrence sur n, le nombre d'éléments de l'ensemble E et où $0 \leq k \leq n$. Si $n = 1$ alors on a bien $\binom{1}{0} = \binom{1}{1} = 1$ qui sont les réponses attendues. Attention, $\emptyset$ est un sous-ensemble à 0 élément. Supposons l'affirmation pour un ensemble à n éléments et tout $0 \leq k \leq n$. Considérons un ensemble E à $n+1$ éléments dont l'un sera dénoté par $\boxed{\star}$. Par HdR le nombre de sous-ensembles de k éléments ne contenant pas $\boxed{\star}$ est $\binom{n}{k}$. Par ailleurs, le nombre de sous-ensembles de E à k éléments contenant

$\boxed{\star}$ s'obtient en ajoutant à tous les sous-ensembles de $k-1$ éléments ne contenant pas $\boxed{\star}$, justement l'élément $\boxed{\star}$. Il y en a donc $\binom{n}{k-1}$. La fin de la preuve prend appui sur la propriété fondamentale des coefficients binomiaux :

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

Chapitre 4

Le théorème fondamental de l'arithmétique et ses conséquences

4.1 Division euclidienne et théorème fondamental

Ex. 45. a) $4 = -9\cdot 156 + 11\cdot 128$ b) $29 = 1\cdot 899 - 1\cdot 870$ c) $1 = -43\cdot 125 + 42\cdot 128$
d) $91 = 1\cdot 91 + 0\cdot 1001$ e) $19 = 9\cdot 323 - 8\cdot 361$ f) $1 = 2^{100}\cdot(2^{101}-1) - (2^{100}-1)(2^{101}+1)$

Ex. 46. Le pas de récurrence : comme $p|(a_1a_2\dots a_{n-1})a_n$ alors si $p|a_n$ c'est fini. Sinon par le cas $n = 2$ on a $p|a_1a_2\dots a_{n-1}$, d'où par HdR on a p divise l'un des $n-1$ facteurs.

Ex. 47. $10 = 3\cdot 3 + 1$ qui multiplié par 10 donne $10^2 = 10\cdot(3\cdot 3) + (3\cdot 3 + 1) = 33\cdot 3 + 1$. Procédure que l'on peut reproduire. Sinon, par récurrence.

Ex. 48. a) Tout entier n peut s'écrire sous la forme $n = d\cdot 10 + u$ où d est le nombre de dizaines de n et u est le chiffre des unités de n. Comme $10 = 2\cdot 5$ alors la divisibilité de n par 2 (ou par 5) ne dépend que de celle de u par 2 (ou par 5).
b) Par extension, tout n peut s'écrire sous la forme $n = q\cdot 2^k 5^k + r$ où q et r sont respectivement le quotient et le reste de la division euclidienne de n par 10^k.

Ex. 49. Par division euclidienne : $10^n = q\cdot 11 + (-1)^{n+1}$. D'où, le critère de divisibilité *un entier est divisible par 11, si la somme alternée* $(+/-)$ *de ses chiffres* $\in M_{11}$.

Ex. 50. Justification du critère : $100 = 14\cdot 7 + 2$ et tout entier peut s'écrire sous la forme $n = m\cdot 10^2 + c$, où m est le nombre (entier) de centaines de n et c est le reste de la division euclidienne de n par 100.
Autre critère : cacher le chiffre des unités, soustraire le double du nombre caché au nombre visible, puis recommencer afin d'identifier si la différence $\in M_7$.
Justification : introduisons la fonction $f : \mathbb{Z} \to \{0; 1\}$ qui envoie un multiple de 7 sur 0, et un non multiple de 7 sur 1. Posons $n = 10\cdot d + u$, où u est le chiffre des unités et d le nombre de dizaines de n. On a alors $f(n) = f(10\cdot d + u) = f((7+3)\cdot d + u) = f(3\cdot d + u) = f((-2)\cdot(3\cdot d + u)) = f(-6\cdot d - 2u) = f(7d - 6d - 2u) = f(d - 2u)$.

Ex. 51. *'abcabc'* $= 1001\cdot$ *'abc'* $= 7\cdot 11\cdot 13\cdot$ *'abc'* $= 7\cdot 11\cdot 13\cdot(a\cdot 10^2 + b\cdot 10 + c\cdot 1)$

Ex. 52. $350 = 2\cdot 5^2\cdot 7$, $50193 = 3^3\cdot 11\cdot 13^2$, $111111 = 3\cdot 7\cdot 7\cdot 11\cdot 13\cdot 37$ et $101101 = 7\cdot 11\cdot 13\cdot 101$.

Ex. 53. Tous les nombres premiers plus petits que la racine carrée du nombre figurent soit dans le terme de droite, soit dans celui de gauche. Conclure par l'ex. 30 et 2.

Ex. 54. *Exemple* : $2 \cdot 3 + 5 \cdot 7 = 43$. Comme le plus grand nombre qui peut être atteint est $107 = 3 \cdot 5 \cdot 7 + 2$ et que ce dernier est $< 11^2$ alors par l'ex. 30 ils sont tous premiers.

Ex. 55. Non ! Si l'on a bien $13 = 5 \cdot 11 - 2 \cdot 3 \cdot 7$ et $17 = 2 \cdot 7 \cdot 13 - 3 \cdot 5 \cdot 11$, en revanche pour 19, le système d'équations $a - b = 19$ et $a \cdot b = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$ n'admet pas de solutions entières.

Remarque 2. Un autre exercice du même type qui m'amuse est le suivant :
$3 - 2 = 1$ c'est-à-dire qu'avec les deux plus petits premier j'obtiens l'unité en effectuant une différence de deux termes.
$2 \cdot 3 - 5 = 1$, avec les trois plus petits nombres premiers j'obtiens de nouveau l'unité.
$3 \cdot 5 - 2 \cdot 7 = 1$, pareil donc pour les quatre plus petits premiers.
Montrer que 1 peut s'écrire comme une différence de deux termes, constitués par les facteurs 2 ; 3 ; 5 ; 7 ; 11 ; 13 et 17, mais qu'en revanche avec les premiers jusqu'à 11 et les premiers jusqu'à 13, il n'y a pas de solution, ni pour l'un ni pour l'autre.

Remarque 3. Une question naturelle qui se pose suite aux deux exercices précédents est : "Si $P = 2; 3; 5; 7; 11; \ldots p_n$ où p_n est le n^e nombre premier est-il vrai que la méthode précédente (de la différence de deux termes contenant comme facteurs tous les éléments de P) ne produit que des nombres premiers, voire l'unité ?
Pour une réponse détaillée (en anglais) consulter :
`https://www.parabola.unsw.edu.au/files/articles/2000-2009/volume-45-2009/issue-1/vol45_no1_1_0.pdf`

Ex. 56. $\lfloor 100 \div 3 \rfloor + \lfloor 100 \div 3^2 \rfloor + \lfloor 100 \div 3^3 \rfloor + \lfloor 100 \div 3^4 \rfloor = 48$, où $\lfloor x \rfloor$ signifie la valeur entière $\leq x$.

∗ **Ex. 57.** Si ce n'était pas le cas alors par l'ex. 2, p diviserait 1. Donc on peut associer à un $n \in \mathbb{N}$ le plus petit diviseur premier p de $n! + 1$ qui sera forcément $> n$. Si l'on recommence la procédure, en ayant préalablement définit que le nouveau n est p alors on obtient une suite infinie de nombres premiers.
Prolongement. Le théorème de Wilson, qui sera démontré par la suite, garantit que tous les nombres premiers vont apparaître dans la suite ci-dessus.

Ex. 58. En décomposant en facteurs premiers on obtient :
a) $324 = 18^2$ b) $784 = 28^2$ c) $7056 = 2^4 3^2 7^2$ d) $9801 = 3^4 11^2$ f) $12321 = 3^2 37^2$

Ex. 59.

a) $399 = 20^2 - 1^2 = \ldots$	b) $221 = 15^2 - 2^2 = \ldots$	c) $391 = 20^2 - 3^2 = \ldots$
d) $117 = 11^2 - 2^2 = \ldots$	e) $9991 = 100^2 - 3^2 = \ldots$	f) $323 = 18^2 - 1^2 = \ldots$
g) $135 = 12^2 - 3^2 = \ldots$	h) $231 = 16^2 - 5^2 = \ldots$	i) $119 = 12^2 - 5^2 = \ldots$
j) $171 = 14^2 - 5^2 = \ldots$	k) $299 = 18^2 - 5^2 = \ldots$	l) $9919 = 100^2 - 9^2 = \ldots$
m) $713 = 27^2 - 4^2 = \ldots$	n) $1073 = 33^2 - 4^2 = \ldots$	o) $1763 = 42^2 - 1^2 = \ldots$

∗ **Ex. 60.**
a) $15^4 - 4 = (15^2 - 2)(15^2 + 2) = 223 \cdot 227$ b) $15^3 + 4^3 = (15+4)(15^2 - 15 \cdot 4 + 4^2) = 19 \cdot 181$
c) $15^4 + 4 = (15^4 + 2 \cdot 15^2 \cdot 2 + 2^2) - (2 \cdot 15)^2 = (15^2 + 2)^2 - 30^2 = 257 \cdot 197$
d) $15^4 + 4^3 = 15^4 + 2 \cdot 15^2 \cdot 2^3 + (2^3)^2 - (2^2 \cdot 15)^2 = (15^2 + 2^3)^2 - (2^2 \cdot 15)^2 = 173 \cdot 293$
e) $15^6 + 4^3 = (15^2)^3 + 4^3 = (15^2 + 4)((15^2)^2 - 15^2 \cdot 4 + 4^2) = 229 \cdot 49741$

f) $(15^2)^5 + (4^2)^5 = (15^2 + 4^2)(15^8 - 15^6 4^2 + 15^4 4^4 - 15^2 4^6 + 4^8) = 241 \cdot 2392744561$
Chose amusante, toutes les décompositions ci-dessus sont en fait des produits de facteurs premiers !

∗ **Ex. 61.** En effet :

$$\begin{aligned} 2^{32} + 1 &= (2^4 + 5^4)2^{28} - 2^{28} \cdot 5^4 + 1 = 641 \cdot 2^{28} + (1^4 - (2^7 \cdot 5)^4) \\ &= 641 \cdot 2^{28} + (1 + (2^7 \cdot 5)^2)(1 + 2^7 \cdot 5)(1 - 2^7 \cdot 5) \\ &= 641 \cdot 2^{28} + 641(1 + (2^7 \cdot 5)^2)(1 - 2^7 \cdot 5) \in M_{641} \end{aligned}$$

Ex. 62. Les deux résultats sont une conséquence du *théorème fondamental de l'arithmétique* et de la définition du *pgcd* et du *ppcm*. De même en ce qui concerne la formule $a \cdot b = pgcd(a, b) \cdot ppcm(a, b) = (a, b) \cdot [a, b]$.

Ex. 63. Calculer, à l'aide de la technique de votre choix, les *ppcm* et *pgcd* de :
a) $(374, 2499) = 17$; $[374, 2499] = 54978$ b) $(10647, 3003) = 3$; $[10647, 3003] = 117117$
c) $(4567, 4576) = 1$; $[4567, 4576] = 20898592$ d) $(3721, 3599) = 61$; $[3721, 3599] = 219539$

Ex. 64. 10 ; 4 ; 8 ; 24 ; 16 ; 169 ; 30 ; 96

Ex. 65. $\sigma_0(2^{26}3^{14}5^7 7^4 11^2 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29) = 27 \cdot 15 \cdot 8 \cdot 5 \cdot 3 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2332800$.

Ex. 66. Essayons d'obtenir 32 diviseurs. Or, $32 = 4 \cdot 2 \cdot 2 \cdot 2$, d'où le nombre $2^3 \cdot 3 \cdot 5 \cdot 7 = 840$.

Ex. 67. a) $\{2; 3; 5; 7; 11; 13; 17; 19; 23; 29; 31; 37; 41; 43; 47; 53; 59; 61; 67; 71; 73; 79; 83; 89; 97\}$
b) Par hypothèse de récurrence à l'étape p, les $p - 1$ nombres entourés correspondent au $p - 1$ plus petits nombres premiers de $\mathbb{N}$ et tous les multiples de ces derniers ont été barrés. Il s'ensuit que le nombre suivant dans la liste et non barré ne peut être que le p-ième nombre premier.

Ex. 68. On obtient 977 ; 983 ; 991 et 997 qui sont tous premiers.

Ex. 69. a) $E := \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$ est de cardinal égale à 10.
b) $F := E \cup \{31, 37, 41, 43, 47, 53, 59, 61, 67\}$ et donc $^{\#}F = 19$. La formule donne aussi : $\frac{1 \cdot 2 \cdot 4 \cdot 6}{2 \cdot 3 \cdot 5 \cdot 7} \cdot 70 + 4 - 1 = 19$
c) $\pi(154) = 36$ de même que $\frac{1 \cdot 2 \cdot 4 \cdot 6 \cdot 10}{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11} \cdot 154 + 5 - 1 = 36$
∗ d) $^{\#}E_2 = 77$, $^{\#}E_3 = 51$, $^{\#}E_6 = 25$, d'où $\frac{51}{308} = P(E_2) \cdot P(E_3) \neq P(E_6) = \frac{25}{154}$

Concernant la formule célèbre, l'idée de la preuve consiste à appliquer la série géométrique à chaque facteur premier, p_i qui parcourt tous les nombres premiers.

$$\prod_{p_i} \frac{1}{1 - p_i^{-s}} = (1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \ldots)(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \ldots) \ldots (1 + \frac{1}{p_k^s} + \frac{1}{p_k^{2s}} + \ldots) \ldots$$

puis le théorème fondamental de l'arithmétique, puisque chaque $n > 1$ s'écrit de manière unique sous la forme d'un produit de facteurs premiers :

$$(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \ldots)(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \ldots) \ldots (1 + \frac{1}{p_k^s} + \frac{1}{p_k^{2s}} + \ldots) \ldots = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots$$

Faire tendre s vers 1. À droite on obtient la série harmonique qui tend vers $+\infty$. Donc le membre de gauche contient une infinité de facteurs premiers distincts. D'où, une autre

preuve de "l'infinité des nombres premiers". Poussons un peu plus loin l'analyse, en effectuant un développement limité de $\ln(\prod_{p_i} \frac{1}{1-p_i^{-s}})$:

$$\ln(\prod_{p_i} \frac{1}{1-p_i^{-s}}) = -\sum_{p_i} \ln(1-\frac{1}{p_i^s}) \cong \sum_{p_i} \frac{1}{p_i^s}.$$

Une fois de plus, si l'on fait tendre s vers 1 alors, comme l'expression de gauche tend vers $+\infty$, on en déduit que la somme des inverses des nombres premiers en fait de même !

Ex. 70. Par exemple $\{41;43\}$, $\{59;61\}$ et $\{71;73\}$.

Ex. 71. Non, car l'un des termes serait divisible par 3.

Ex. 72. a) Tous, car si $\{p;p+2\}$ sont des premiers jumeaux alors

$$p(p+2)+1 = p^2+2p+1 = (p+1)^2.$$

b) Supposons que $(p+1)^2 = n^4$. Alors $p+1 = n^2 \Leftrightarrow p = (n-1)(n+1)$. Comme p est premier alors $n-1=1$. Autrement dit $p=3$, et on a bien $3\cdot 5+1 = 2^4$

Ex. 73. Dans la liste des 6 entiers consécutifs
$[6n-3;6n-2;6n-1;6n;6n+1;6n+2;6n+3]$ on a $3|6n\pm 3$, $2|6n\pm 2$
et donc pour $n>1$ les seuls candidats pouvant être premiers sont $6n\pm 1$.

Ex. 74. En effet, par l'exercice précédent on a bien $(6n+1)^2-(6n-1)^2 = 24n \in M_{24}$.

Ex. 75. a) Pour $\{3;5\}$ on a : $3;5;9=3^2$
Pour $\{5;7\}$ on a : $5;7;11;17;25=5^2$
Pour $\{11;13\} \to 11;13;17;23;31;41;53;67;83;101;121=11^2$
Pour $\{17;19\} \to 17;19;23;29;37;47;59;73;89;107;127;149;173;199;227;257;289=17^2$
Pour $\{41;43\} \to 41;43;47;53;61;71;83;97;113;131;151;173;197;223;251;281;313;347;383;421;461;503;547;593;641;691;743;797;853;911;971;1033;1097;1163;1231;1301;1373;1447;1523;1601;1681=41^2$
Tous ces nombres sont premiers, sauf le dernier de la liste qui n'est autre que le carré du nombre initial. On a : $f_3(x)=x^2+x+3$, $f_5(x)=x^2+x+5$, $f_{11}(x)=x^2+x+11$, $f_{17}(x)=x^2+x+17$ et $f_{41}(x)=x^2+x+41$.

* **Ex. 76.** a) Posons $g_1(x)=x^2+x+p$ et $g_2(x)=x^2-x+p$. On a que $g_2(-x)=g_1(x)$. Or, $g_1(x)=\left(x+\frac{1}{2}\right)^2-\frac{1}{4}+p$ et $g_2(x)=\left(x-\frac{1}{2}\right)^2-\frac{1}{4}+p$ admettent $x=\mp\frac{1}{2}$ comme axes de symétrie et donc $g_1\left(x-\frac{1}{2}\right)=g_2\left(\frac{1}{2}-x\right)=g_2\left(\frac{1}{2}+x\right)$ et aura donc même ensemble image que g_1.
b) Par le point précédent, $g_1(x)=x^2+x+p$ ne prend que des valeurs 'premières' pour $1-p\le x\le p-2$. D'où, par changement de variable, si $x=y-p+1$ alors

$$g_3(y)=g_1(y-p+1)=(y-p+1)^2+y-p+1+p=y^2-(2p-3)y+(p-1)^2+1$$

fait de même pour $0\le y\le 2p-3$.

** **Ex. 77.** Soit un polynôme $p\in\mathbb{Z}[x]$ de degré n. Alors p ne peut prendre une valeur y plus de n fois (car, si x_0 annule p alors $p(x)=(x-x_0)q(x)$ où $q(x)\in\mathbb{R}[x]$). Pour $a\in\mathbb{Z}$ supposons $p(a)=b$ et $b\notin\{0;\pm 1\}$ (qui par la remarque précédente doit exister). Alors $b|p(a+kb)$ pour tout $k\in\mathbb{Z}$. Une infinité de ces valeurs sont donc composées et distinctes.

4.2 La somme des diviseurs

Ex. 78.

Conjecture 1. Comme 6 est parfait, puis 12 est abondant, 18 aussi, il semble donc que tout multiple strict (ou propre ?) de 6 soit abondant. Plus généralement, l'on aurait : "tout multiple d'un abondant est abondant". Réponse donnée plus loin dans ce chapitre.

Conjecture 2. Il semblerait qu'à l'inverse, il est possible de trouver des suites de nombres consécutifs abondants aussi longues que l'on veut .

L'idée de la preuve me semble relativement directe : montrons qu'il existe 3 nombres abondants consécutifs. Commençons par décomposer l'ensemble des premiers en 3 classes distinctes pour obtenir trois sommes > 1. Comme la somme des inverses des premiers diverge alors c'est réalisable :

$$a = \frac{1}{2} + \frac{1}{7} + \frac{1}{17} + \frac{1}{29} + \frac{1}{41} + \ldots + \frac{1}{p_1}$$

$$b = \frac{1}{3} + \frac{1}{11} + \frac{1}{19} + \frac{1}{31} + \frac{1}{43} + \ldots + \frac{1}{p_2}$$

$$c = \frac{1}{5} + \frac{1}{13} + \frac{1}{23} + \frac{1}{37} + \frac{1}{47} + \ldots + \frac{1}{p_3}$$

Posons $A :=$ le dénominateur de a, $B :=$ le dénominateur de b et $C :=$ le dénominateur de c. Ces trois nombres sont abondants et n'admettent aucun diviseur commun. On peut montrer (officiellement, grâce au lemme chinois) que parmi les A multiples consécutifs de B il en existe exactement deux couples qui sont des voisins directs d'un multiple de A, puisque $(A, B) = 1$. En additionnant AB un nombre suffisamment de fois à l'un de ces couples précédents l'on peut à nouveau déduire qu'un multiple de C est voisin du couple choisi. Comme un multiple d'un abondant est un abondant alors on a obtenu nos trois abondants consécutifs.

Conjecture 3. La somme des inverses

1. des abondants diverge (provient du fait que la série harmonique diverge)
2. des déficients diverge (provient du fait que la série des inverses des premiers diverge. Existe-t-il une autre preuve sans utiliser le résultat précédent (dû à Euler) ?

Conjecture 4. Il existe une infinité de suites de 5 déficients consécutifs.

La réponse figure dans le journal, *American Mathematical Monthly*, mars, 1983, page 215. On y trouve aussi une autre preuve à la conjecture 2.

Conjecture 5. La somme des inverses des nombres parfaits converge

Démonstration. Par la caractérisation d'Euler des nombres parfaits pairs (NPP)on a :

$$\sum_{n \in NPP} \frac{1}{n} < \sum_{n \in \mathbb{N}^*} \frac{1}{2^{n-1}(2^n - 1)} < \sum_{n \in \mathbb{N}} \frac{1}{2^n} = 2$$

Par ailleurs, concernant les nombres parfaits impairs (NPI), démontrons d'abord qu'ils s'écrivent sous la forme $n = p^a Q^2$ avec $(p, Q) = 1$, p premier (impair) et Q et a sont

impairs aussi. En effet, si $n = p_1^a p_2^b \dots$ (produit fini de premiers impairs distincts) est parfait alors

$$2n = \sigma(n) = (p_1^a + p_1^{a-1} + \dots)(p_2^a + p_2^{a-1} + \dots)\dots$$

le nombre de termes dans chaque facteur ci-dessus est impair à l'exception d'un seul, donc tous les exposants sont pairs sauf un seul, et on a bien $n = p^a Q^2$ A présent, montrons que pour chaque Q il existe un unique p. Sinon, il existerait deux parfaits impairs $n_1 = p_1^a Q^2$ et $n_2 = p_2^b Q^2$ tels que $2n_1 = \sigma(n_1) = \frac{p_1^{a+1}-1}{p_1-1}\sigma(Q^2)$ et $2n_2 = \sigma(n_2) = \frac{p_2^{b+1}-1}{p_2-1}\sigma(Q^2)$. De ces deux équations on tire :

$$\frac{\sigma(n_1)}{\sigma(n_2)} = \frac{p_1^a}{p_2^b} = \frac{p_1^a + p_1^{a-1} \dots + 1}{p_2^b + p_2^{b-1} \dots + 1}$$

ce qui est absurde, puisque les numérateur et dénominateur précédents sont ni l'un ni l'autre divisible par p_1 et respectivement par p_2. Pour conclure, l'on peut majorer la somme des inverses par .

$$\sum_{n \in NPI} \frac{1}{n} < \sum_{Q \in \mathbb{N}^* \setminus \{1\}} \frac{1}{3 \cdot Q^2} < \frac{1}{3} \sum_{n \in \mathbb{N}^*} \frac{1}{Q(Q+1)} = \frac{1}{3}$$

□

Ex. 79. $496 = 2^4 \cdot 31 = 2^4 \cdot (2^5 - 1)$.
Donc $D_{496} = \{1, 2, 2^2, 2^3, 2^4,$ "puis ces derniers multipliés par 31" $, 31, 31 \cdot 2, 31 \cdot 2^2, 31 \cdot 2^3, 31 \cdot 2^4\}$. D'où leur somme est :
$\sigma(496) = 1+2+2^2+2^3+2^4+31 \cdot (1+2+2^2+2^3+2^4) = (2^5-1)(31+1) = 2^5(2^5-1) = 2 \cdot 496$
Observons que $6 = 2 \cdot 3 = 2^1 \cdot (2^2 - 1)$ et que $28 = 2^2 \cdot 7 = 2^2 \cdot (2^3 - 1)$. Il semble donc que le nombre parfait suivant soit de la forme $2^{p-1} \cdot (2^p - 1)$. Le calcul pour 496 ci-dessus révèle l'importance du fait que $2^p - 1$ soit premier. Le corrigé de l'exercice 32 indique alors que p doit être premier. Un candidat serait donc $8128 = 2^6(2^7 - 1)$ et un petit calcul le prouve.

Ex. 80.

$$\begin{aligned}\sigma(6) \cdot \sigma(25) &= (1+2+3+6)(1+5+5^2) \\ &= 1+2+3+6+1 \cdot 5+2 \cdot 5+3 \cdot 5+6 \cdot 5+1 \cdot 5^2+2 \cdot 5^2+3 \cdot 5^2+6 \cdot 5^2 \\ &= \sigma(6 \cdot 25)\end{aligned}$$

Ex. 81. Le pas de récurrence est

$$\sigma(p^{n+1}) = (1+p+p^2+\dots+p^n)+p^{n+1} = \frac{p^{n+1}-1}{p-1}+p^{n+1} = \frac{p^{n+1}-1}{p-1}+\frac{p^{n+1}(p-1)}{p-1} = \frac{p^{n+2}-1}{p-1}.$$

Ex. 82. $\sigma(1000) = \sigma(2^3 5^3) = \sigma(2^3)\sigma(5^3) = 2340$
$\sigma(1024) = \sigma(2^{10}) = 2047$, $\sigma(1025) = \sigma(5^2 41) = \sigma(5^2)\sigma(41) = 1302$
$\sigma(783000) = \sigma(2^3)\sigma(3^3)\sigma(5^3)\sigma(29) = 2808000$.

Ex. 83. a) $\sigma(3^n) = (3^{n+1} - 1) \div 2 < 2 \cdot 3^n$ car $3 \cdot 3^n - 1 < 4 \cdot 3^n$.

b) $(p-1)\sigma(p^n) = p^{n+1} - 1 < 2(p-1)p^n$, car $2p^n < p \cdot p^n + 1$.

c) $8 \cdot \sigma(3^a \cdot 5^b) = (3^{a+1} - 1)(5^{b+1} - 1) = 15 \cdot 3^a \cdot 5^b - 3^{a+1} - 5^{b+1} + 1 < 16 \cdot 3^a \cdot 5^b$

Ex. 84. $\sigma(2^a \cdot 127) = (2^{a+1}-1)2^7 = 2^{a+8}-2^7 > 2^{a+1}127 \quad \Leftrightarrow \quad 2^{a+8}-128 > 2^{a+1}127 \quad \Leftrightarrow$ $a > 6$.

Ex. 85. $\sigma(3^a \cdot 5 \cdot 7) = (3^{a+1}-1) \cdot 24 > 70 \cdot 3^a \Leftrightarrow 72 \cdot 3^a - 24 > 70 \cdot 3^a$. D'où, pour $a \geq 3$.

** **Ex. 86.** A résoudre $\sigma(n)-n = 3n \Leftrightarrow \sigma(n) = 4n$ pour $n = 2^a 3^b \cdot 35$. Dans ce cas on obtient : $(2^{a+1}-1)(3^{b+1}-1) \cdot 48 = 2^{a+3}3^b \cdot 35 \Leftrightarrow (4 \cdot 2^{a-1}-1)(9 \cdot 3^{b-1}-1) = 2^{a-1}3^{b-1} \cdot 35$ que l'on développe, pour réduire en : $2^{a-1}3^{b-1}+1 = 4 \cdot 2^{a-1}+9 \cdot 3^{b-1}$. Posons $x = 2^{a-1}$ et $y = 3^{b-1}$ et résolvons l'équation diophantienne $xy + 1 = 4x + 9y$ en 'complétant le rectangle' : $0 = xy - 4x - 9y + 1 = (x-9)(y-4) - 35$ D'où $35 = 1 \cdot 35 = 7 \cdot 5 = (x-9)(y-4)$ qui admet un nombre fini de solutions entières, dont l'une est $x = 16 = 2^{5-1}$ et $y = 9 = 3^{3-1}$, des puissances de 2 et de 3. Ainsi $a = 5$ et $b = 3$.

** **Ex. 87.** D'une manière analogue à l'exercice précédent : $\sigma(n) - n = 2n \Leftrightarrow \sigma(n) = 3n$. D'où : $\sigma(3p \cdot 2^{n-1}) = 3^2 \cdot p \cdot 2^{n-1} \Leftrightarrow (p+1)(2^n-1) = 3^2 p 2^{n-3}$. Posons $2^{n-3} = q$. D'où l'équation $= pq + p - 8q + 1 = (q+1)(p-8) + 9$ qui ne peut admettre qu'un nombre fini de solutions entières. En particulier, on trouve $p_1 = 7$, d'où $q_1 = 8 = 2^{6-3}$ et donc $n_1 - 1 = 5$. Autre solution, $p_2 = 5$, d'où $q_2 = 2 = 2^{4-3}$ et donc $n_2 - 1 = 3$.

Ex. 88. Voir `http://www.vsmp.ch/crm/telechargements/`

Ex. 89. $\sigma(m) = \sigma(2 \cdot 3 \cdot k) = 3 \cdot 4 \cdot \sigma(k) \geq 12(1+k) > 12k = 2(2 \cdot 3 \cdot k) = 2m$

* **Ex. 90.** Par l'exercice précédent il suffit de montrer que $2^a \cdot 3^b$ est abondant pour $a > 1$ ou $b > 1$ et $a, b \in \mathbb{N}^*$. Supposons l'affirmation démontrée pour $n = 2^a \cdot 3^b$ et prouvons-la pour $2^a \cdot 3^{b+1}$. Alors $\sigma(2^a \cdot 3^{b+1}) = \sigma(2^a \cdot 3^b) + 3^{b+1}\sigma(2^a) > 2^{a+1}3^b + 3^{b+1}\sigma(2^a) > 2^{a+1}3^b + 3^{b+1}(2^{a+1}-1) = 2 \cdot (2^a 3^b) + 6(2^a 3^b) - 3 \cdot 3^b = 8 \cdot (2^a 3^b) - 3 \cdot 3^b > 6 \cdot (2^a 3^b)$ La dernière inéquation est vraie car $2 \cdot (2^a 3^b) > 3 \cdot 3^b$, puisque que l'on suppose $a \geq 1$. Un raisonnement tout à fait analogue peut être effectué par rapport à l'exposant de 2 augmenté d'une unité et celui du 3 restant fixe.

Ex. 91. $6 = 2^1(2^2-1) \qquad 28 = 2^2(2^3-1) \qquad 496 = 2^4(2^5-1) \quad 8128 = 2^6(2^7-1)$
$33550336 = 2^{12}(2^{13}-1)$

Ex. 92. En se basant sur les propriétés de σ, si $p = 2^n - 1$ est premier, on a :

$$\sigma(2^{n-1}p) = \sigma(2^{n-1})\sigma(p) = (2^n-1)(p+1) = (2^n-1)(2^n-1+1) = p \cdot (2^n-1+1) = 2p2^{n-1}$$

On peut aussi le montrer comme suite :
$p = 1 + 2 + 2^2 + \ldots + 2^{n-1} = 2^n - 1$ est premier alors

$$\begin{aligned}\sigma(2^{n-1}p) &= 1 + 2 + 2^2 + \ldots + 2^{n-1} + (1 + 2 + 2^2 + \ldots + 2^{n-1})p \\ &= (2^n-1)(1+p) = p(1+2^n-1) = 2(2^{n-1}p).\end{aligned}$$

Ex. 93. Si $n = 2m$ est pair alors $2^n - 1 = 2^{2m} - 1^2 = (2^m-1)(2^m+1)$.
Sinon, n étant supposé composé on a $n = pq$, où p et q sont impairs > 1 alors
$2^n - 1 = 2^{pq} - 1^{pq} = (2^p)^q - (1^p)^q = (2^p-1)(2^{pq-p} + 2^{pq-2p} + \ldots + 2 + 1)$.
Comme tout premier $p > 2$ est impair, $p = 2k+1$ et que le chiffre des unités des puissances de 2 forme une suite cyclique d'ordre 4 de la forme $\{2; 4; 8; 6; \ldots\}$ alors $2^{p-1}(2^p-1) = 4^k(2^{2k+1}-1)$ ne peut prendre que 6 ou 8 comme chiffre des unités.

Remarque. Contrairement à ce qu'affirmait Nicomaque de Gérase, [1], à savoir l'alternance systématique des chiffres $6, 8, 6, 8, \ldots$ dans la suite des nombres parfaits P_i, l'on a que P_5 et P_6 se terminent tous les deux par 6.

Ex. 94. a) Sur `http://www.mersenne.org/` on indiquait en mars 2019 que le 21 décembre 2018, le 51^e nombre de Mersenne avait été identifié. Il s'agit de

$$M(82589933) = 2^{82589933} - 1.$$

Son écriture décimale est constituée de 24'862'048 de chiffres.
b) On ne sait toujours en 2019 s'il existe des nombres parfaits impairs.

** **Ex. 95.**

$$2^{12} \cdot (2^{13}–1) = 1^3 + 3^3 + 5^3 + 7^3 + 9^3 + 11^3 + 13^3 + 15^3 + 17^3 + 19^3 + \ldots + 125^3 + 127^3.$$

On observe que le nombre de termes impairs à droite est la racine carrée du premier facteur de gauche.

Conjecture : Si $2^p - 1$ est premier alors $2^{p-1} \cdot (2^p - 1) = \sum_{k=1}^{2^{\frac{p-1}{2}}} (2k-1)^3$
Pour la preuve, commencer par prouver (par récurrence) que pour $n \in \mathbb{N}$ quelconque, on a $\sum_{k=1}^{n}(2k-1)^3 = n^2(2n^2-1)$. Terminer en posant $n = 2^{(p-1)/2}$. Sinon, consulter l'article de Steven Kahn, *Perfectly Odd Cubes*, Mathematics Magazine, April 1998.

Ex. 96. À prouver $\sigma(2^n pq) - 2^n pq = 2^n r$ et $\sigma(2^n r) - 2^n r = 2^n pq$ dans le cas où $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$ et $r = 3^2 \cdot 2^{2n-1} - 1$ sont des premiers distincts.

$$\begin{aligned}
\sigma(2^n pq) - 2^n pq &= (2^{n+1} - 1)(p+1)(q+1) - 2^n pq \\
&= (2^{n+1} - 1) \cdot 3 \cdot 2^{n-1} 3 \cdot 2^n - 2^n (3 \cdot 2^{n-1} - 1)(3 \cdot 2^n - 1) \\
&= 3^2 \cdot 2^{2n-1}(2^{n+1} - 1) - 2^n (3 \cdot 2^{n-1} - 1)(3 \cdot 2^n - 1) \\
&= 2^n \left[3^2 \cdot 2^{n-1}(2^{n+1} - 1) - 3^2 \cdot 2^{2n-1} + 3 \cdot 2^{n-1} + 3 \cdot 2^n - 1\right] \\
&= 2^n \left[3^2 \cdot 2^{2n} - 3^2 \cdot 2^{n-1} - 3^2 \cdot 2^{2n-1} + 3 \cdot 2^{n-1} + 3 \cdot 2^n - 1\right] \\
&= 2^n \left[3^2 \cdot 2^{2n-1} - 3^2 \cdot 2^{n-1} + 3^2 \cdot 2^{n-1} - 1\right] \\
&= 2^n \cdot r.
\end{aligned}$$

Un calcul analogue permet de vérifier $\sigma(2^n r) - 2^n r = 2^n pq$.

Ex. 97. À résoudre

$$\begin{cases} 4qr = & (1+2+4)(1+p) - 4p \\ 4p = & (1+2+4)(1+q)(1+r) - 4qr \end{cases}$$

qui est équivalent à

$$\begin{cases} 4qr = & 7 + 3p \\ 4p = & 3qr + 7q + 7r + 7 \end{cases}$$

Par élimination de p, réduction, puis complétion du rectangle, on a alors

$$16qr - 28 = 9qr + 21q + 21r + 21 \Leftrightarrow 0 = qr - 7 - 3q - 3r = (q-3)(r-3) - 16$$

D'où $(q-3)(r-3) = 16$ qui n'admet qu'un nombre fini de solutions entières que l'on teste toutes. On obtient finalement $q = 11$, $r = 5$ et $p = 71$, et donc les nombres 220 et 284.

1. Mathématicien et philosophe néo-pythagoricien $\sim$ 60-120 apr. J.-C.

4.3 Les triplets pythagoriciens

Ex. 98. a) $169^2 - 119^2 = 2^6 3^2 5^2$; $18541^2 - 12709^2 = 2^4 3^6 5^6$; $106^2 - 56^2 = 2^2 3^4 5^2$

b) Le théorème de Pythagore et sa réciproque.

c) Par l'algorithme d'Euclide :
$(12709, 18541) = (5832, 12709) = (1045, 5832) = (607, 1045) = (180, 169) = 1$

Ex. 99. a) $5^2 - 4^2 = 3^2$ $143^2 - 102^2 \neq 101^2$ $17^2 - 15^2 = 8^2$ $101^2 - 99^2 = 20^2$

b) Si $a^2 + b^2 = c^2$ alors $(ak)^2 + (bk)^2 = (a^2 + b^2)k^2 = (ck)^2$

c) Utiliser Thalès et agrandir le triangle (3 ;4 ;5) par un facteur 5, ou le triangle (5 ;12 ;13) par un facteur 13, etc.

d) Soit p et $p+2$ des nombres premiers (et donc impairs tous les deux). Étudions d'abord $p^2 + (p+2)^2 = c^2 \Leftrightarrow 2p^2 + 4p + 4 = (2n)^2 \Leftrightarrow p^2 = 2(n^2 - p - 1)$ qui est absurde, puisque p est impair. L'autre cas à étudier est $a^2 + p^2 = (p+2)^2 \Leftrightarrow (2m)^2 + p^2 = (p+2)^2 \Leftrightarrow (m-1)(m+1) = p$. D'où $m = 2$ et l'on obtient le triplet (3 ;4 ;5).

e) De $a + b + \sqrt{a^2 + b^2} = ab/2$ on obtient (en isolant la racine, en élevant au carré, puis en réduisant) $0 = ab - 4a - 4b + 8$. Compléter le rectangle donne $(a-4)(b-4) = 8$ dont les solutions entières sont en nombre fini : $a_1 = 6$, $b_1 = 8$, $c_1 = 10$ et $a_2 = 5$, $b_2 = 12$, $c_2 = 13$.

Ex. 100. $(1 + 3 + 5 + \ldots + 23) + 5^2 = ((23+1)/2)^2 \Leftrightarrow 12^2 + 5^2 = 13^2$
D'une manière générale, on obtient :

$$\begin{aligned}\big[1 + 3 + 5 \ldots + ((2n-1)^2 - 2)\big] + (2n-1)^2 &= \big[1 + 3 + 5 \ldots + 2(2n^2 - 2n) - 1\big] + (2n-1)^2 \\ &= (2n^2 - 2n)^2 + (2n-1)^2 = (2n^2 - 2n + 1)^2\end{aligned}$$

Le fait que deux des termes dans le triplet soient consécutifs implique qu'il est primitif.

Ex. 101. $10^2 + 24^2 = 26^2$ car $26^2 - 24^2 = 2 \cdot 50 = 10^2$.
Formule générale : $(2a)^2 + x^2 = (x+2)^2 \Leftrightarrow a^2 - 1 = x$. D'où : $(2a)^2 + (a^2-1)^2 = (a^2+1)^2$.

Ex. 102. a) $a^2 + b^2 = (b+3)^2 \Leftrightarrow a^2 = 6b + 9$. Cette dernière égalité ne peut être vraie pour des entiers premiers entre eux, puisque le membre de droite est divisible par 3, mais pas par 9.

b) $a^2 + (a+k)^2 = (a+2k)^2 \Leftrightarrow 0 = a^2 - 2ak - 3k^2 = (a-k)^2 - (2k)^2 = (a-3k)(a+k)$
Donc $a = 3k$ (ou $a = -k$) et le triplet n'est pas primitif.

Ex. 103. Oui, car $(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$.

Ex. 104. *Lemme.* Si $(a, b) = 1$ et $a \cdot b = c^2$ alors $a = m^2$ et $b = n^2$, a, b, c, m et $n \in \mathbb{N}$.
Par le théorème fondamental de l'arithmétique, chaque facteur premier p de a, ne peut diviser b et doit apparaître un nombre pair de fois, puisqu'il apparaît un nombre pair de fois dans c^2. De même concernant les facteurs premiers de b.

Théorème 7. *Tout triplet primitif admet la forme* $(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$ *où* m *et* n *sont de parités différentes et* $m > n$.

Ex. 105. Soit le triplet pythagoricien $a^2 + b^2 = c^2$ avec $(a, b) = 1$.

a) Sinon on aurait $a = 2k+1$, $b = 2l+1$ et $c = 2m$. D'où, $a^2+b^2 = 4(k^2+k+l^2+l)+2 = 4m^2$ Absurde, 2 de plus qu'un multiple de 4 n'est pas égal à un multiple de 4.

b) Si $p|(c-b)$ et $p|(c+b)$ alors p divise leur différence et leur somme qui sont respectivement $2b$ et $2c$. Or, $(b, c) = 1$ et sont impairs. D'où $((c-b), (c+b)) = 2$.

c) Comme $a^2 = (c-b)(c+b)$ alors par le lemme précédent, chaque facteur de droite est le double d'un carré : $c-b = 2m^2$ et $c+b = 2m^2$. Ainsi, $c = n^2+m^2$, $b = n^2-m^2$ et $a = 2mn$ avec $(m, n) = 1$. Par ailleurs, n et m ne peuvent être impairs tous les deux puisque $c = m^2+n^2$ est impair.

Ex. 106. Ce sont les premiers p de la forme $p = 4k-1$, car sinon, par le théorème 7, on aurait $n^2+m^2 = p$, où n et m sont de parités différentes, $n = 2s$, $m = 2t+1$ et donc $n^2+m^2 = 4(s^2+t^2+t)+1 = p = 4k-1$. Absurde.

Ex. 107. Par le théorème 7, on a soit $b^2 = m^2-n^2$, soit $b^2 = 2mn$. Dans le premier cas on peut prendre par exemple : $b = 3$, $m = 5$ et $n = 4$, d'où $40^2+3^4 = 41^2$. Autre exemple : $312^2+5^4 = 313^2$.

4.4 Les théorèmes de Fermat et de Wilson

Ex. 108. a) Voir l'exercice 19 (par récurrence) ou factoriser directement : $n^3-n = (n-1)n(n+1)$ et constater qu'on obtient le produit de trois entiers consécutifs (dont au moins un est divisible par 2 et exactement un par 3).

b) $n^5-n = (n-1)n(n+1)(n^2+1)$. L'un des facteurs est pair. De plus, si les trois premiers facteurs ne sont pas divisibles par 5 alors $n = 5m \pm 2$, qui élevé au carré auquel on ajoute 1 est un multiple de 5.

c) Prouvons l'affirmation par récurrence : si $n = 0$ alors il est clair que $7|(n^7-n)$. Supposons l'affirmation pour $n = k$ et prouvons-la pour $n = k+1$: on a $(k+1)^7-(k+1) = (k+1)^7-k^7-1+(k^7-k)$. Par hypothèse de récurrence le dernier terme entre parenthèses est divisible par 7. Par ailleurs en développant par la formule du binôme l'expression de gauche, les termes k^7 et les constantes s'annulent. Il ne reste qu'une somme de termes de la forme $\binom{7}{i} = \frac{7!}{(7-i)!i!}$, où le dénominateur ne contient que des facteurs < 7 et le numérateur est un multiple de 7.

d) Fausse, car en prenant par exemple $n = 2$, on a $2^9-2 = 510 = 2 \cdot 3 \cdot 5 \cdot 17 \notin M_9$

e) *Conjecture.* Si p est premier alors $2p \mid k^p-k \quad \forall k \in \mathbb{N}$

Ex. 109. Les diviseurs de $2^{11}-1$ sont $23 = 2 \cdot 11+1$ et $89 = 8 \cdot 11+1$.
De $2^{23}-1$ on a $47 = 2 \cdot 23+1$ et $178481 = 7760 \cdot 23+1$.
De $2^{29}-1$ on a $233 = 8 \cdot 29+1$, $1103 = 38 \cdot 29+1$ et $2089 = 72 \cdot 29+1$.
Plusieurs de ces résultats figurent dans *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus* (E26), de L. Euler, 1729.

∗ **Ex. 110.** À déterminer un nombre parfait, $2^{p-1} \cdot (2^p-1)$, compris entre 10^{20} et 10^{22}. Vu l'ordre de grandeur des deux facteurs, l'on recherche les premiers p qui vérifient $10^{20} < 2^{2p-1} < 10^{22}$. Prenant le log en base 2 on obtient $64 < 2p-1 < 73$ et donc $33 \leq p \leq 37$. Le seul premier concerné est alors $p = 37$. Montrons, comme l'a fait Fermat que $2^{37}-1$ n'est pas premier. En effet, $2^{37}-1 = 137438953471$ et n'admet que des diviseurs premiers de la forme $p = 2k \cdot 37+1$. Or pour $k = 3$ on obtient 223 qui divise (par chance) 137438953471. Il n'existe donc pas de nombre parfait pair compris entre 10^{20} et 10^{22}

Ex. 111. a) $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$.

b) Pour tout m impair. D'où l'exposant sous forme d'une puissance de 2 des F_n.

∗ c) Pour $m > n$ l'affirmation est triviale. Sinon, pour $m < n$, si $p \mid 2^{2^m} \pm 1$ alors $p \mid (2^{2^m} \pm 1)(2^{2^m} \mp 1) = 2^{2^{m+1}} - 1$ et ainsi de suite, on pourrait ajouter 1 à l'exposant de la puissance de 2 jusqu'à ce que $p \mid 2^{2^n} - 1$ ce qui est absurde puisque $p \mid 2^{2^n} + 1$ et donc p diviserait leur différence qui vaut 2.

∗∗ d) Soit p un diviseur premier de F_n ; si $p \mid 2^{2^n}+1$ alors $p \mid (2^{2^n}+1)(2^{2^n}-1) = 2^{2^{n+1}}-1$ Or, par le petit Fermat on sait que $p \mid 2^{p-1} - 1$. Le résultat va découler du fait $2^{n+1} \mid p-1$ (c'est-à-dire $p-1 = k \cdot 2^{n+1}$). Commençons par énoncer et démontrer le lemme suivant : Si a est le plus petit exposant tel que $p \mid 2^a - 1$ et que $p \mid 2^b - 1$ alors $a \mid b$. En effet, par division euclidienne $b = qa + r$, où $0 \leq r < a$. Par ailleurs, après développement, on voit que p divise aussi bien les extrémités gauche et droite ci-dessous :

$$2^b - 1 = 2^{qa+r} - 1 = (2^a)^q \cdot 2^r - 1 = ((2^a - 1) + 1)^q \cdot 2^r - 1 = p \cdot Q + 2^r - 1$$

Ce qui implique que $p \mid 2^r - 1$. Or, a avait été choisi minimal et donc $r = 0$ comme affirmé. Par ce lemme et pour ce a minimal, on a alors : $a \mid 2^{n+1}$ et donc $a = 2^m$ pour $0 < m \leq n + 1$. Mais par l'exercice précédent, il ne peut exister un tel $a \leq 2^n$ et donc $a = 2^{n+1}$. On conclut en utilisant le lemme ci-dessus : d'où $2^{n+1} \mid p - 1$.

e) D'après le critère les diviseurs premiers ont la forme : $32 \cdot k + 1$ avec $k \in \mathbb{N}$. De surcroît il suffit d'identifier ceux qui sont inférieurs à la racine carrée de F_4. Ainsi on obtient pour F_4, en barrant les composés, l'ensemble { ~~33~~ , ~~65~~ , 97 , ~~129~~ , ~~161~~ , 193 , ~~225~~ } et il n'y a que deux nombres premiers à tester.

∗ **Ex. 112.** En appliquant le critère pour F_5 on voit que les diviseurs premiers peuvent être { ~~65~~, ~~129~~, 193, 257, ~~321~~, ~~385~~, 449, ~~513~~, 577, 641 } et au cinquième essai on obtient que $F_5 = 641 \cdot 6700417$.

Ex. 113. a) Il suffit de 'combiner' les 3, 5, 17 : On obtient les 6 solutions suivantes $\{3; 5; 15; 17; 51; 85\}$

b) Est équivalent à dénombrer tous les sous-ensembles non-vides de $\{3; 5; 17; 257; 65537\}$ qui vaut donc $2^5 - 1 = 32 - 1$.

Ex. 114.

Utilisons la notation $a \leftrightarrow b$ pour signaler que a et b sont *correspondants* pour $p = 13$. On a alors $2 \leftrightarrow 7$, $3 \leftrightarrow 9$, $4 \leftrightarrow 10$, $5 \leftrightarrow 8$, $6 \leftrightarrow 11$. Ainsi que les points 'fixes' $1 \leftrightarrow 1$ et $12 \leftrightarrow 12$.

Le théorème de Girard, Fermat et Euler

Ex. 115. a) $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, $29 = 2^2 + 5^2$, $37 = 1^2 + 6^2$, $41 = 4^2 + 5^2$, $53 = 2^2 + 7^2$, $61 = 5^2 + 6^2$, $73 = 3^2 + 8^2$, $89 = 5^2 + 8^2$, $97 = 4^2 + 9^2$ et $101 = 1^2 + 10^2$.

b) Sinon, pour de raisons de parité on aurait $n = 4k + 3 = (2m + 1)^2 + (2n)^2 = 4(m^2 + m + n^2) + 1$ ce qui est absurde.

c) $(a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 = (ac \mp bd)^2 + (ad \pm bc)^2$

d) $1517 = 37 \cdot 41 = (1^2 + 6^2)(4^2 + 5^2) = 26^2 + 29^2 = 34^2 + 19^2$

Ex. 116. a) Par le théorème qui précède $u^2+v^2 \mid m$, où $\frac{u}{v} = \frac{1000-972}{235-3} = \frac{28}{232} = \frac{7}{58}$ et donc $u^2+v^2 = 7^2+58^2 = 3413$ divise m

b) Même méthode : $u^2+v^2 \mid m$, où $\frac{u}{v} = \frac{2^{2^4}-62264}{20449-1} = \frac{409}{2556}$ et donc $u^2+v^2 = 409^2+2556^2 = 6700417$ divise F_5

c) $(16^2+1^2)(a^2+b^2) = (16a-b)^2+(a+16b)^2 = (2060^2)^2+1^2$ D'où

$$\begin{cases} 16a-b &= 2060^2 \\ a+16b &= 1 \end{cases}$$

Qui admet comme solutions : $a = 264193$ et $b = -16512$ D'où $(1^2+16^2)(16512^2+264193^2) = (16512-16\cdot 264193)^2+(264193+16\cdot 16512)^2 = 4210576^2+528385^2$

Ex. 117.

$$901 = \mathbf{30^2+1^2} = 29^2+60 = 28^2+117 = 27^2+172 = 26^2+225 = \mathbf{26^2+15^2}$$

Par le théorème précédent, 901 est divisible par $4^2+1^2 = 17$.

$$437 = 20^2+37 = 19^2+76 = 18^2+113 = 17^2+148 = 16^2+181 = 15^2+212$$

à l'étape suivante le 2e terme est supérieur au premier. Conclusion, 437 ne peut s'écrire sous la forme d'une somme de deux carrés. Or, $437 \equiv 1 \pmod 4$ et donc doit être composé. Du reste, après un peu de réflexion, on voit que $437 = 441-4 = 21^2-2^2 = (21-2)(21+2) = 19\cdot 23$ (à condition de connaître les carrés < 1000 (par exemple)).

Chapitre 5

A propos des rationnels

5.1 Le corps des nombres rationnels

Ex. 118. a) $\frac{a}{b} \div \frac{c}{d} = \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{bc}$

b) $\frac{1}{\frac{a}{b}} + (-\frac{c}{d}) = \frac{b}{a} - \frac{c}{d} = \frac{bd-ac}{ad}$

c) $(\frac{a}{b})^2 - (\frac{c}{d})^2 = \frac{a^2d^2-b^2c^2}{(bd)^2}$

Ex. 119.

$$\frac{1}{n} - \frac{1}{n+1} = \frac{1(n+1)}{n(n+1)} - \frac{n}{n(n+1)} = \frac{1}{n(n+1)}$$

Par l'égalité précédente $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\ldots\frac{1}{99\cdot 100} = \left(\frac{1}{1}-\frac{1}{2}\right)+\left(\frac{1}{2}-\frac{1}{3}\right)+\left(\frac{1}{3}-\frac{1}{4}\right)+\ldots\left(\frac{1}{99}-\frac{1}{100}\right) =$ somme télescopique dont tous les termes s'annulent sauf les extrémités $= 1 - \frac{1}{100} = \frac{99}{100}$.

Ex. 120. a) $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$

b) Oui, $\frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \frac{1}{12} = 1$. Oui, $\frac{1}{2} + \frac{1}{6} + \frac{1}{9} + \frac{1}{18} = 1$.

c) $1 = \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \ldots + \frac{1}{2^{n-2}} + \frac{1}{3\cdot 2^{n-3}} + \frac{1}{6\cdot 2^{n-3}}$ avec $n \in \mathbb{N}$.

Ex. 121. $\frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{9} + \frac{1}{11} + \frac{1}{13} + \frac{1}{15} > 1$ Posons $N = ppmc(3, 5, 7, ...2n + 1)$ alors le développement de la somme précédente est composée que de diviseurs (distincts) de N au numérateur et de N au dénominateur. D'où l'affirmation, après multiplication des deux membres par N.

Ex. 122. $\frac{\sigma(3\cdot 5\cdot 7\cdot 11\cdot 13)}{3\cdot 5\cdot 7\cdot 11\cdot 13} = \frac{(1+3)(1+5)(1+7)(1+11)(1+13)}{3\cdot 5\cdot 7\cdot 11\cdot 13} > 2.$

∗ **Ex. 123.** Nous n'expliciterons que l'étape de récurrence, ou recourrons à des minorations, ou majorations si nécessaire.

a) Le pas de récurrence est : $1 + \frac{1}{2}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \ldots + \frac{1}{2^n}\right) < 1 + \frac{1}{2} \cdot 2 = 2$

b) En minorant $k!$ par $(k-1)! \cdot 2$ on obtient par récurrence :
$\sum_{i=0}^{n+1} \frac{1}{i!} \leq 1 + \frac{1}{1!} + \frac{1}{2} \cdot \left(\frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!}\right) < 1 + \frac{1}{1!} + \frac{1}{2} \cdot 2 = 3.$

c) Majorant chaque terme compris entre $\frac{1}{2^k+1}$ et $\frac{1}{2^{k+1}}$ par $\frac{1}{2^k}$ et sachant que le nombre d'entiers compris entre $2^k + 1$ et 2^{k+1} (extrémités comprises) est 2^k on obtient :
$\sum_{i=1}^{2^n} \frac{1}{i} > 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \ldots + \frac{1}{2^n} = 1 + \frac{n}{2}.$

d) $\sum_{i=1}^{n} \frac{1}{i^2} < 1 + \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \ldots + \frac{1}{(n-1)\cdot n} = 2 - \frac{1}{n}$ par l'exercice 119

e) Le pas de récurrence est $\left(1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\frac{1}{5}-\frac{1}{6}+\ldots+\frac{1}{2n-1}-\frac{1}{2n}\right)+\left(\frac{1}{2n+1}-\frac{1}{2n+2}\right)<\frac{n}{n+1}+\frac{1}{2n+1}-\frac{1}{2n+2}<\frac{n+1}{n+2}$. Cette dernière inéquation s'étudie par la méthode classique.

En fait, toutes les séries ci-dessus sont célèbres dans l'histoire des mathématiques. La première est une série géométrique que l'on retrouve dans les paradoxes de Zénon. La deuxième converge lorsque n tend vers l'infini vers le nombre $e \cong 2,71828\ldots$, définie et étudiée par L. Euler. Ce nombre est transcendant, résultat démontré par C. Hermite en 1873. La troisième tend vers l'infini lorsque n tend vers l'infini et permet de justifier que la fonction $ln(x)$ est non bornée. La quatrième, dénommé le *problème de Bâle*, restera un grand mystère pour de nombreux mathématiciens du XVIII^e, jusqu'au jour où L. Euler montra que la série converge vers $\pi^2/6$. Enfin, on peut prouver la convergence vers $ln(2)$ de la dernière à l'aide d'un critère découvert et démontré par N. Abel vers 1825.

5.2 Formes d'écriture d'un nombre rationnel

Ex. 124. a) $\frac{1}{2}=0,5$; $\frac{3}{4}=0,75$; $\frac{7}{8}=0,875$; $\frac{15}{16}=0,9375$; $\frac{31}{32}=0,96875$

b) $\frac{1}{3}=0,\overline{3}$; $\frac{1}{7}=0,\overline{142857}$; $\frac{1}{11}=0,\overline{09}$; $\frac{1}{13}=0,\overline{076923}$; $\frac{1}{17}=0,\overline{0588235294117647}$

c) $\frac{1}{11}=0,\overline{09}$; $\frac{1}{111}=0,\overline{009}$; $\frac{1}{1111}=0,\overline{0009}$; $\frac{1}{11111}=0,\overline{00009}$; $\frac{1}{111111}=0,\overline{000009}$

Ex. 125. a) $0,375=\frac{3}{8}$ b) $1,\overline{2}=\frac{11}{9}$ c) $0,\overline{65}=\frac{65}{99}$ d) $0,24\overline{9}=\frac{1}{4}$ e) $0,\overline{027}=\frac{27}{999}$

f) $0,\overline{9}=1$ g) $10,0\overline{13}=\frac{9913}{990}$

Ex. 126. Si a, b, c et d sont des entiers alors il existe une fraction irréductible $\frac{m}{n}$ et des entiers p et q tels que $\frac{a}{b}=\frac{pm}{pn}$ et $\frac{c}{d}=\frac{qm}{qn}$ avec $a=pm$, $b=pn$, $c=qm$ et $d=qn$. En substituant dans l'expression on obtient :

$$\frac{a}{b}+\frac{c}{d}=\frac{pm}{pn}+\frac{qm}{qn}=2\cdot\frac{m}{n}=2\cdot\frac{(p+q)m}{(p+q)n}=2\cdot\frac{a+c}{b+d}$$

Sinon, en multipliant par $bd(b+d)$ de part et d'autre on obtient $ad(b+d)+cb(b+d)=2bd(a+c)\Leftrightarrow ad^2+cb^2=abd+bdc$, qui se vérifient aisément sachant que par hypothèse $ad=bc$.

Ex. 127. On peut supposer a, b, c et d positifs. En multipliant l'inégalité par $bd(b+d)$ de part et d'autre, on obtient $ad(b+d)<bd(a+c)<bc(b+d)$, qui se vérifient aisément sachant que par hypothèse $ad<bc$.

Ex. 128. Par l'exercice précédent : $\frac{97}{103}<\frac{200}{212}=\frac{50}{53}<\frac{103}{109}$

Ex. 129. A) Si a et b sont deux entiers naturels, $b\neq 0$ alors l'algorithme de division classique de a par b admet à chaque étape un reste compris entre 0 et $b-1$. Si le reste est 0 à un moment donné alors l'écriture décimale de $\frac{a}{b}$ est finie et le nombre est donc décimal. Sinon, les restes ne peuvent prendre que $b-1$ valeurs comprises entre 1 et $b-1$. Dès la première répétition d'un reste, la suite des restes sera identique, d'où l'écriture périodique de $\frac{a}{b}$. D'une manière plus précise on peut démontrer :

1) Si $x = \frac{a}{b}$ est une fraction irréductible avec $b = 2^r 5^s$ (appelée communément *fraction décimale*), où r et $s \in \mathbb{N}^*$ alors l'amplification de celle-ci par $2^s 5^r$ donne une fraction équivalente dont le dénominateur est 10^{r+s}. D'où x est un *nombre décimal*.

2) Supposons que le dénominateur de x est co-premier à 10. Prenons par exemple $x = \frac{1024}{49}$. La *partie entière* de x, notée $\lfloor x \rfloor$ est le plus grand entier inférieur ou égal à x. D'où $\lfloor x \rfloor = \lfloor 20 + \frac{44}{49} \rfloor = 20$. Intéressons-nous à la *partie décimale* de x, c'est-à-dire $\frac{44}{49}$. À partir des divisions euclidiennes, définissons les valeurs q_i et r_i par $44 \cdot 10^i = q_i \cdot 49 + r_i$ pour $i \geq 0$. Par construction $1 \leq r_i \leq 48$. L'on peut démontrer que $(r_i, 49) = 1$, $\forall i$. Par ailleurs non seulement le reste $r_0 = 44$ réapparaîtra, mais de surcroît le nombre d'étapes nécessaires à sa réapparition est forcément un diviseur de $\phi(49) :=$ le nombre d'entiers compris entre 1 et 48, co-premiers à 49. D'où la périodicité des chiffres de la partie décimale et la qualification de *périodique pure* du nombre en question.

   Exemple. L'exemple ci-dessus admet une période de longueur 42 :

$$\frac{2^{10}}{49} = 20.\overline{897959183673469387755102040816326530612244}$$

3) Une *écriture décimale pré-périodique* s'obtient si une fraction irréductible p/q admet au dénominateur des diviseurs premiers de deux 'espèces' (certains premiers à 10 et d'autres non premiers à 10).

   Exemple.

$$x = \frac{13}{225} = \frac{13}{7 \cdot 5^2} = \frac{13 \cdot 2^2}{7 \cdot 10^2} = \frac{52}{7 \cdot 10^2} = (7 + \frac{3}{7}) \cdot \frac{1}{100}.$$

   Or, par le point b) la fraction 3/7 admet une écriture périodique pure et donc par 0,01 rend l'écriture décimale de 13 /225 *pré-périodique*.

B) Réciproquement, prenons l'exemple paradigmatique $x = 0, \overline{567}$. D'où $1000x = 567, \overline{567}$. La différence des deux membres de gauche égale celle des deux membres de droite . Ainsi, $999x = 567 \Leftrightarrow x = 21/37$.

Ex. 130. a) $100_{10} = 1 + 0 \cdot 3 + 2 \cdot 3^2 + 0 \cdot 3^3 + 1 \cdot 3^4 = 10201_3$.

b) $\frac{1}{2} = 0,5$ mais en base 3 on a : $\frac{1}{2} = \frac{3}{2 \cdot 3} = \frac{1}{3} + \frac{1}{2 \cdot 3} = \frac{1}{3} + \frac{3}{2 \cdot 3^2} = \frac{1}{3} + \frac{1}{3^2} + \frac{3}{2 \cdot 3^3} = 0, \overline{1}_3$

c) $0, \overline{3}_4 = \frac{3}{4} + \frac{3}{4^2} + \frac{3}{4^3} + \ldots$. Prenons le quadruple de chaque membre : $4_{10} \cdot 0, \overline{3}_4 = 3_{10} + 0, \overline{3}_4$. D'où $0, \overline{3}_4 = 1_{10}$.

d) $\frac{1}{5} = \frac{7}{5 \cdot 7} = \frac{1}{7} + \frac{2 \cdot 7}{5 \cdot 7^2} = \frac{1}{7} + \frac{2}{7^2} + \frac{4 \cdot 7}{5 \cdot 7^2} = \frac{1}{7} + \frac{2}{7^2} + \frac{5}{7^3} + \frac{3 \cdot 7}{5 \cdot 7^4} + \frac{5}{7^3} + \frac{4}{7^5} + \frac{1}{5 \cdot 7^5} = 0, \overline{1254}_7$.

Ex. 131. $0, \overline{349} < 0,35 = 0,34\overline{9} < 0,3\overline{5} < \frac{3}{4} < \frac{34}{45} < \frac{84}{111} < \frac{25}{33} < \frac{341}{450} < \frac{7}{9}$

Ex. 132. a) $\frac{266}{45}$ b) $\frac{49}{99}$ c) $\frac{112}{99}$ d) $\frac{5}{33}$ e) $\frac{491}{154}$ f) $\frac{27889}{8100}$ g) $\frac{1}{3}$ h) $\frac{2}{3}$ i) $\frac{5}{6}$

Ex. 133. a) $\frac{1}{7} = 0, \overline{142857}$. Comme la longueur de la période de l'écriture décimale est de 6 chiffres alors tous les restes dans le processus de division classique sont atteints (sauf le 0). Si $0 < k < 7$ alors on considère le k comme un des six restes obtenu lors de la division de 1 par 7. Ainsi il n'y qu'un 'déphasage' ou une translation de la virgule (avec annulation de la la partie entière). Si $k > 7$ on effectue d'abord la division euclidienne, $k = q_0 \cdot 7 + r_0$. Dans ce cas la partie entière est q_0 et le raisonnement précédent peut être appliqué sur $\frac{r_0}{7}$.

b) Voici la liste de tous les premiers inférieurs à 100 dont les inverses ont une écriture décimale de longueur maximale : 7, 17, 19, 23, 29, 47, 59, 61 et 97. Le mathématicien caractérise ces entiers comme étant les premiers p pour lesquels 10 est une *racine primitive modulo p*. Selon Wikipedia, "aucune formule générale simple pour calculer les racines primitives modulo n n'est connue."

c) $\frac{1}{43} = 0,\overline{0232558139534883720 93}$ et la période est donc de longueur 21.

Ex. 134. L'approche 'naturelle' consiste à utiliser ce que l'on appelle dans la littérature classique l'*algorithme glouton* qui consiste à approcher la fraction par le plus grand quantième possible + un reste positif. Ce dernier est à nouveau approché par le plus grand quantième possible + un deuxième reste positif, etc. Illustration :

$\frac{2}{5} = 0,4 = \frac{1}{3} + (\frac{2}{5} - \frac{1}{3}) = \frac{1}{3} + \frac{1}{15}$

$\frac{15}{8} = 1 + \frac{7}{8} = 1 + \frac{1}{2} + (\frac{7}{8} - \frac{1}{2}) = 1 + \frac{1}{2} + \frac{3}{8} = 1 + \frac{1}{2} + \frac{1}{3} + (\frac{3}{8} - \frac{1}{3}) = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{24}$

$\frac{25}{11} = 2 + \frac{3}{11} = 2 + \frac{1}{4} + (\frac{3}{11} - \frac{1}{4}) = 2 + \frac{1}{4} + \frac{1}{44}$

$\frac{2}{17} = \frac{1}{9} + (\frac{2}{17} - \frac{1}{9}) = \frac{1}{9} + \frac{1}{153}$

Un exercice intéressant pourrait être de rédiger un programme (en Python, voire un autre langage) qui effectue l'algorithme glouton. Dernière remarque, en fait en utilisant le fait que la série harmonique diverge, on peut aussi montrer que tout nombre rationnel admet une écriture en quantièmes distincts. En revanche, il n'est pas trop difficile de comprendre pourquoi il est impossible d'écrire 1 sous la forme d'une somme de quantièmes, dont les dénominateurs sont que des nombres premiers distincts.

Ex. 135. La première astuce consiste à comprendre que "pour fabriquer du grand, il peut être avantageux de commencer par fabriquer du minuscule strictement supérieur à zéro, car diviser par un nombre est équivalent à multiplier par son inverse, et donc pour fabriquer du minuscule, la soustraction peut aussi être très utile ! Autre considération : même si a et b sont tous deux strictement supérieur à 1 il se peut que $a + b > a \cdot b$. Sinon consulter [1] pour d'autres considérations.
Pour finir, le site de Bernard Gisin permet d'obtenir toutes les solutions maximales avec même plus de 4 rationnels :
`http://www.juggling.ch/gisin/index.php`

a) $\dfrac{d}{a(b-c)} = 1120$

b) $\dfrac{c+d}{ab} = \dfrac{205}{2}$

c) $\dfrac{c+d}{a-b} = 183$

d) $\dfrac{a}{c-b-d} = 50$

Ex. 136. a) Le "jeu" ressemble au *Compte est bon*, mais avec qu'une opération, la multiplication, et 150 rationnels (à la place de 6 entiers). Les dénominateurs sont tous de la forme $2^a \cdot 5^b$ avec a et $b \leq 2$. Les "petites" fractions qui sont données directement

sont : $\frac{1}{2}; \frac{3}{2}; \frac{1}{4}; \frac{3}{4}; \frac{5}{4}; \frac{1}{5}; \frac{2}{5}; \frac{3}{5}; \frac{4}{5}; \frac{6}{5}; \frac{7}{5}; \frac{1}{10}; \frac{3}{10}; \frac{7}{10}; \frac{11}{10}; \frac{13}{10}; \frac{32}{25}$. Cette dernière fraction joue un rôle important, car elle permet d'obtenir $2 = \frac{32}{25} \cdot \frac{5}{4} \cdot \frac{5}{4}$, qui 'combiné' avec $\frac{3}{2}$ donne 3 ; de même $2 \cdot 2 \cdot \frac{5}{4} = 5$, qui 'combiné' avec $\frac{7}{5} = 7$. Donc, oui il est bien possible de doubler, tripler, quintupler et même septupler la taille d'une image.

b) $60\% = \frac{3}{5}$, $125\% = \frac{5}{2^2}$ et $128\% = \frac{2^5}{5^2}$. Alors $\frac{5}{2^2} \cdot \frac{5}{2^2} \cdot \frac{2^5}{5^2} = 2$, qui au carré fois $\frac{5}{2^2}$ donne 5, qui multiplié par $\frac{3}{5}$ donne 3. Ainsi, l'on peut construire les nombres 2, 3 et 5, à partir desquels il est aisé de construire à présent $135\% = \frac{3^3}{2^2 \cdot 5} = (\frac{3}{5})^3 \cdot (\frac{5}{2^2})^2 \cdot 2^2$ et $24,3\% = \frac{3^5}{2^3 \cdot 5^3} = (\frac{3}{5})^5 \cdot (\frac{5}{2^2})^2 \cdot 2$. En revanche, $9\% = \frac{3^2}{2^2 5^2}$ ne peut être obtenu qu'en prenant $(\frac{3}{5})^2$ et dans ce cas il faut pouvoir générer alors $\frac{1}{2^2}$ à partir de $\frac{5}{2^2}$ et $\frac{2^5}{5^2}$. Or ceci est impossible, car en élevant la première fraction à la puissance a et la deuxième à la puissance b (des entiers positifs) on obtient en examinant les puissances respectives de 2 et de 5 dans l'équation $\frac{1}{2^2} = \frac{5^a}{2^{2a}} \cdot \frac{2^{5b}}{5^{2b}}$

$$\begin{cases} -2 & = (-2)a + 5b \\ 0 & = a - 2b \end{cases}$$

qui admet comme solution $b = -2$ et $a = -4$. En fait tout l'exercice aurait pu être fait sur ce modèle en posant et résolvant des systèmes de trois équation à trois inconnues.

∗ **Ex. 137.**

a) $r_1 = [1;1] = \frac{2}{1}$ $r_2 = [1;1,1] = \frac{3}{2}$ $r_3 = [1;1,1,1] = \frac{5}{3}$
$r_4 = [1;1,1,1,1] = \frac{8}{5}$ $r_5 = [1;1,1,1,1,1] = \frac{13}{8}$

b) Sachant que $\frac{p_{i+1}}{q_{i+1}} = 1 + \frac{q_i}{p_i} = \frac{p_i + q_i}{p_i}$ on a alors forcément que $q_{i+1} = p_i$ et que $p_{i+1} = p_i + q_i = p_i + p_{i-1}$, à condition que toutes les fractions en question soient irréductibles. Or, la preuve se fait facilement par récurrence. Par ailleurs, la même remarque est valable pour $|p_i^2 - q_i \cdot p_{i+1}| = 1$ (à faire par récurrence).

∗ **Ex. 138.** D'abord, si $a = \frac{p}{q}$ avec $(p,q) = 1$, alors le reste obtenu par la division euclidienne à la n^e étape est strictement plus petit que celui obtenu à l'étape $n-1$. Ce reste étant un entier naturel finira donc par valoir 0 au bout d'un nombre fini d'étapes.
Réciproquement, si $a = [a_0; a_1, a_2, a_3, \ldots, a_n]$ avec des $a_i \in \mathbb{N}^*$ pour $i > 0$ alors par récurrence $a = [a_0; [a_1; a_2, a_3, \ldots, a_n]] = [a_0; \frac{m}{n}] = a_0 + \frac{m}{n} \in \mathbb{Q}$.

.

∗∗ **Théorème 17.** *Soit la fraction continue infinie $[a_0; a_1, a_2, a_3, \ldots]$, où $a_i \in \mathbb{N}^*$ si $i > 0$. Posons $\frac{p_n}{q_n} = [a_0; a_1, a_2, a_3, \ldots, a_n]$ la n^e réduite. On a alors*

a) $p_n = a_n p_{n-1} + p_{n-2}$ et $q_n = a_n q_{n-1} + q_{n-2}$ pour $n \geq 2$.

b) $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$ pour $n > 0$ et $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$ pour $n \geq 2$

c) $\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}$ et $\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{a_n (-1)^n}{q_n q_{n-2}}$, c'est-à-dire que les réduites paires et impaires forment respectivement des suites strictement croissante et décroissante qui deviennent arbitrairement proche l'une de l'autre.

Démonstration. Toutes ces preuves s'obtiennent en effectuant des récurrences *la plupart d'ordre deux*. Effectuons une sorte de "prolongement par continuité" pour que les formules soient vraies pour $n \geq 0$. Pour cela ils suffit de définir $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$ et $q_{-1} = 0$.

a) Commençons la récurrence en vérifiant l'égalité pour $n = 0$ et $n = 1$:

$$\frac{p_0}{q_0} = \frac{a_0 p_{-1} + p_{-2}}{a_0 q_{-1} + q_{-2}} = \frac{a_0}{1}$$

et que

$$\frac{p_1}{q_1} = \frac{a_1 p_0 + p_{-1}}{a_1 q_0 + q_{-1}} = \frac{a_1 a_0 + 1}{a_1} = a_0 + \frac{1}{a_1}$$

De plus, on a $p_1 = a_1 p_0 + p_{-1} = a_1 a_0 + 1$ et $q_1 = a_1 q_0 + q_{-1} = a_1$
Par HdR supposons que $p_n = a_n p_{n-1} + p_{n-2}$ et que $q_n = a_n q_{n-1} + q_{n-2}$.
Pour l'étape $n + 1$ il faut se débrouiller pour faire apparaître notre HdR :

$$\begin{aligned}\frac{p_{n+1}}{q_{n+1}} &= [a_0; a_1, a_2, a_3, \ldots, a_n, a_{n+1}] = [a_0; a_1, a_2, a_3, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}] \\ &\overset{HdR}{=} \frac{(a_n + \frac{1}{a_{n+1}}) \cdot p_{n-1} + p_{n-2}}{(a_n + \frac{1}{a_{n+1}}) \cdot q_{n-1} + q_{n-2}} = \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}} \\ &\overset{HdR}{=} \frac{a_{n+1} p_n + p_{n-1}}{a_{n+1} q_n + q_{n-1}}.\end{aligned}$$

b) Par récurrence. Comme $\frac{p_0}{q_0} = \frac{a_0}{1}$ et $[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}$ sont des fractions irréductible alors $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0 a_1 + 1$ et $q_1 = a_1$. D'où :

$$p_1 q_0 - p_0 q_1 = (a_0 a_1 + 1) \cdot 1 - a_0 a_1 = 1 = (-1)^{1-1} \quad \text{ça commence bien}$$

Par HdR : $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$.
À l'étape $n + 1$ utilisons a) pour pouvoir appliquer HdR.

$$\begin{aligned}p_{n+1} q_n - p_n q_{n+1} &= (a_{n+1} p_n + p_{n-1}) q_n - p_n (a_{n+1} q_n + q_{n-1}) \\ &= p_{n-1} q_n - p_n q_{n-1} = (-1)(p_n q_{n-1} - p_{n-1} q_n) \overset{HdR}{=} (-1)^n\end{aligned}$$

c) La première égalité provient du point b) car

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} \overset{b)}{=} \frac{(-1)^{n-1}}{q_n q_{n-1}}$$

Concernant la deuxième, insérons puis retranchons un terme "arrangeant".

$$\begin{aligned}\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} &= \left(\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right) + \left(\frac{p_{n-1}}{q_{n-1}} - \frac{p_{n-2}}{q_{n-2}}\right) = \frac{(-1)^{n-1}}{q_n q_{n-1}} + \frac{(-1)^{n-2}}{q_{n-1} q_{n-2}} \\ &= (-1)^{n-2} \frac{-q_{n-2} + q_n}{q_n q_{n-1} q_{n-2}} \overset{HdR}{=} (-1)^{n-2} \cdot \frac{q_n + a_n q_{n-1} - a_n q_{n-1} - q_{n-2}}{q_n q_{n-1} q_{n-2}} \\ &\overset{a)}{=} (-1)^{n-2} \cdot \frac{a_n q_{n-1}}{q_n q_{n-1} q_{n-2}} = (-1)^{n-2} \cdot \frac{a_n}{q_n q_{n-2}}.\end{aligned}$$

□

Chapitre 6

A propos des irrationnels

6.1 Existence et propriétés de quelques irrationnels

Ex. 139. L'idée consiste à inventer des nombres qui admettent une partie décimale non périodique. Des exemples classiques sont celui de Champernowne, 0,12345678910111213... ou de Liouville $0,1100100000000000000001\ldots = \sum_{i=1}^{\infty} 10^{-i!}$ ou encore celui de Prouhet-Thue-Morse (voir Wikipedia).

Ex. 140. Deux segments sont *incommensurables* si tout segment permettant de mesurer l'un ne permet pas de mesurer l'autre.

Ex. 141. Le théorème de l'angle inscrit et de l'angle au centre permet de justifier que les triangles CDF, ACD et DFG ci-dessous sont semblables. Si un segment XY permettait de mesurer aussi bien CE que CD, alors XY mesurerait leur différence, ainsi que FG et FH=FD. Or, FH et HD sont la diagonale et le côté du petit pentagone à l'intérieur de ABCDE. En itérant le raisonnement ci-dessus sur le petit pentagone, on aurait un segment XY permettant de mesurer le côté et la diagonale d'une infinité de pentagones réguliers devenant infiniment petits, ce qui est absurde.

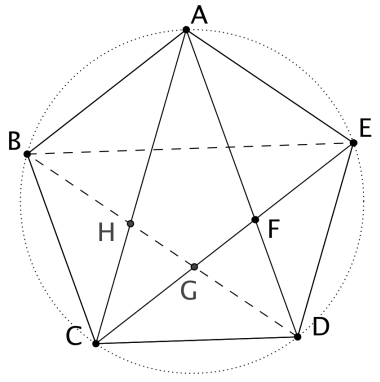

FIGURE 6.1 – Le pentagone régulier et son pentagramme

Ex. 142. Le théorème fondamental de l'arithmétique (TFAr) simplifie considérablement les preuves.

a) $\sqrt{3} = \frac{a}{b}$ pour a et $b \in \mathbb{Z}_+ \Rightarrow 3 \cdot b^2 = a^2$. Par TFAr, $3 \mid a$, de plus son exposant dans le membre de droite est pair alors qu'à gauche l'exposant du 3 est impair. D'où la contradiction.

b) Le même argument peut s'appliquer sur $\sqrt{6}$.

c) Posons $x := \sqrt{2} + \sqrt{3}$ et supposons que x est rationnel. Alors $x^2 - 5 - 2 \cdot \sqrt{6} = 0$ est rationnel. Et donc $\mathbb{Q} \ni (x^2 - 5) \div 2 = \sqrt{6} \in \mathbb{R} \backslash \mathbb{Q}$.

d) L'irrationnalité de $\sqrt[3]{2}$ peut être aussi aisément démontrée comme dans a).

Ex. 143. ll suffit de prouver l'affirmation pour un exposant de la forme $1/q$, puis d'appliquer la commutativité de la multiplication pour le cas général p/q.

$$\sqrt[q]{a \cdot b} = \sqrt[q]{\left(\sqrt[q]{a}\right)^q \cdot \left(\sqrt[q]{b}\right)^q} = \sqrt[q]{\left(\sqrt[q]{a} \cdot \sqrt[q]{b}\right)^q} = \sqrt[q]{a} \cdot \sqrt[q]{b}$$

Ex. 144. Utiliser la définition et les propriétés de la racine carrée.
a) $\sqrt{9} + \sqrt{16} = 7 \neq 5 = \sqrt{25}$ b) $\sqrt{901} + \sqrt{99} \neq 40$ car $2\sqrt{901 \cdot 99} \neq 600$
c) $\sqrt{2} + \sqrt{8} = 3\sqrt{2} = \sqrt{18}$ d) $\frac{\sqrt{63}}{\sqrt{112}} = \sqrt{\frac{63}{112}} = \sqrt{\frac{9}{16}} = \frac{3}{4} = 0,75$

Ex. 145. a) $\sqrt{18} = 3 \cdot \sqrt{2}$ b) $\sqrt{243} = 9 \cdot \sqrt{3}$ c) $\sqrt{400} = 20$ d) $\sqrt{10^7} = 10^3\sqrt{10}$
e) $\sqrt{6}\sqrt{10}\sqrt{15} = 30$ f) $\sqrt{20^7} \cdot \sqrt{24^9}\sqrt{30^{11}} = 20^3 \cdot 24^4 \cdot 30^5 \cdot 2^3 \cdot 5 \cdot 3 = 2^{26} \cdot 3^{10} \cdot 5^9$

Ex. 146. a) $9 + 3\sqrt{3}$ b) $\sqrt{2} + 2$ c) 2
d) $27 + 10\sqrt{2}$ e) $28 - 17\sqrt{6}$ f) $11 \cdot \sqrt{2} + 9 \cdot \sqrt{3}$

Ex. 147. Utiliser la définition et les propriétés de la racine carrée.

a)	$\sqrt{6} \cdot \sqrt{8} > (\sqrt{6})^2$	b)	$2\sqrt{32} + 4\sqrt{8} = 4^2\sqrt{2}$
c)	$11 + 6 \cdot \sqrt{2} = (3 + \sqrt{2})^2$	d)	$\sqrt{2} + \sqrt{3} > \sqrt{2 + 3}$
e)	$\sqrt{10} + \sqrt{8} > \sqrt{11} + \sqrt{7}$	f)	$\sqrt{2} + \sqrt{3} > \sqrt{28} - \sqrt{5}$

Ex. 148. Utiliser la définition et les propriétés de la racine carrée.

a)

$$\sqrt{1 \cdot 3 + 1} = 2 \quad ; \quad \sqrt{2 \cdot 4 + 1} = 3 \quad ; \quad \sqrt{3 \cdot 5 + 1} = 4 \quad ; \quad \sqrt{4 \cdot 6 + 1} = 5$$

D'une manière générale on a que $\sqrt{(n-1)(n+1)+1} = n$, $\forall n \in \mathbb{N}^*$.

b)

$$\frac{1}{\sqrt{2}-1} - \frac{1}{\sqrt{2}+1} = \frac{2}{1} \quad ; \quad \frac{1}{\sqrt{3}-1} - \frac{1}{\sqrt{3}+1} = \frac{2}{2} \quad ; \quad \frac{1}{\sqrt{4}-1} - \frac{1}{\sqrt{4}+1} = \frac{2}{3}$$

D'une manière générale on a que $\frac{1}{\sqrt{n}-1} - \frac{1}{\sqrt{n}+1} = \frac{2}{n-1}$, $\forall n \in \mathbb{N}^* \backslash \{1\}$.

Ex. 149. Approximations successives de $\sqrt{2}$.

$$\frac{99}{70} \qquad \frac{19601}{13860} \qquad \frac{768398401}{543339720} \qquad \frac{1180872205318713601}{835002744095575440}$$

Ex. 150. a) Soit u_n une approximation de $\sqrt{a}$ et posons $\sqrt{a} = u_n - \epsilon$, où ϵ est l'erreur que l'on suppose très proche de 0 (positive ou négative). Élevons au carré l'égalité précédente pour obtenir $a = u_n^2 - 2u_n\epsilon + \epsilon^2$. Négligeons ϵ^2 et déduisons alors $\epsilon = (u_n^2 - a)/2u_n$ qui permet de définir

$$u_{n+1} = u_n - \epsilon = u_n - \frac{u_n^2 - a}{2u_n} = \frac{u_n^2 + a}{2u_n} = \frac{1}{2}\left(u_n + \frac{a}{u_n}\right)$$

∗ b) Observons d'abord que $u_{n+1} > 0$, car a et u_1 le sont. Admettons pour commencer que u_n converge vers un certain u. En substituant dans la définition on obtient

$$u = \frac{1}{2}\left(u + \frac{a}{u}\right) \Leftrightarrow u = \frac{a}{u} \Leftrightarrow u^2 = a \Leftrightarrow u = \sqrt{a}.$$

Il reste donc à prouver que la suite des u_i converge. Evaluons

$$u_{n+1}^2 - a = \frac{1}{4}\left(u_n + \frac{a}{u_n}\right)^2 - a = \frac{1}{4}\frac{(a - u_n^2)^2}{u_n^2} > 0$$

Et donc pour $n > 1$ on a $u_{n+1} > a$ par le remarque initiale. Par ailleurs :

$$u_n - u_{n+1} = \frac{u_n^2 - a}{2u_n} > 0 \text{ par le point précédent}$$

Ainsi, la suite des u_i est positive, strictement décroissante et bornée par a et donc converge dans $\mathbb{R}$.

c) Avec une calculatrice :

pour $\sqrt{2}$ on obtient $u_2 = \frac{3}{2}$ $u_3 = \frac{17}{12}$ $u_4 = \frac{577}{408}$ à 10^{-5} près.

pour $\sqrt{11}$ on obtient $u_5 = \frac{1611045077956033}{485748365451168}$ à 10^{-7} près.

pour $\sqrt{75}$ on obtient $u_7 = \frac{12743165558034093508524347842520122910402616588120768 1}{14714529633340366829792705192316465665027191197899584}$ à 10^{-5} près.

pour $\sqrt{0,5}$ on obtient $u_4 = \frac{577}{816}$ à 10^{-5} près.

Ex. 151. Comme les nombres en question sont tous positifs alors la chaîne d'inéquations est équivalente au quadruple du carré de chaque expression :

$$4a^2 < 4ab < a^2 + 2ab + b^2 < 4b^2$$

qui se vérifie aisément. En conclusion : *la moyenne géométrique est inférieure à la moyenne arithmétique* de deux nombres réels positifs. Plus généralement on peut montrer que la *moyenne harmonique est inférieure à la moyenne géométrique, qui est inférieure à la moyenne arithmétique*, où la moyenne harmonique de a et b est $\frac{2}{\frac{1}{a}+\frac{1}{b}}$.

Ex. 152. $\sqrt{12} + \sqrt{27} = 2\sqrt{3} + 3\sqrt{3} = 5\sqrt{3} \in \mathbb{R}\backslash\mathbb{Q}$
$\sqrt{12} \cdot \sqrt{27} = 2\sqrt{3} \cdot 3\sqrt{3} = 6(\sqrt{3})^2 = 18 \in \mathbb{N}$
$\sqrt{12} \div \sqrt{27} = \frac{2}{3} \in \mathbb{Q}$

Ex. 153. Il est fréquent de devoir appliquer des raisonnements par l'absurde dans de tels contextes. Dénotons par les lettres latines $a, b, \ldots$ les rationnels et par les lettres grecques $\alpha, \beta, \ldots$ les irrationnels.

a) Si $a+\alpha = b$ alors $\alpha = b-a \in \mathbb{Q}$. De manière similaire, si $a \cdot \alpha = b$ alors $\alpha = b \div a \in \mathbb{Q}$.

b) *Preuve constructive.* Il existe $n \in \mathbb{N}^*$ tel que $b - a < \frac{1}{n}$, car $b > a$. De même, il existe $m \in \mathbb{N}^*$ tel que $\frac{\sqrt{2}}{m} < \frac{1}{2n}$. Poser $\gamma = a + \frac{\sqrt{2}}{m}$ et appliquer a).

c) Une preuve naïve consiste à considérer l'écriture décimale de chacun, que nous noterons $\alpha = a_0, a_1a_2a_3\ldots$ et $\gamma = c_0, c_1c_2c_3\ldots$ avec a_0 et c_0 les parties entières respectives. Comme $\alpha < \gamma$ il existe un indice i tel que $a_i < c_i$. Il suffit alors de considérer le nombre $b = a_0, a_1a_2\ldots a_{i-1}c_i$.
Autre preuve. Supposons $0 < \alpha < \gamma$ et que $\gamma - \alpha > \frac{1}{n}$ où $n \in \mathbb{N}$. Par définition il existe des suites de rationnels tels que $\{a_i\}_{i\in\mathbb{N}}$ converge vers α et $\{c_i\}_{i\in\mathbb{N}}$ converge vers γ. Il suffit alors de choisir un $k \in \mathbb{N}$ suffisamment grand pour que $|a_k - \alpha| < \frac{1}{2n}$ et $|c_k - \gamma| < \frac{1}{2n}$. Pour ce k, posons $b = \frac{c_k+a_k}{2}$. On affirme que $\alpha < b < \gamma$. En effet :

$$\left|\frac{\alpha+\gamma}{2} - b\right| \leq \left|\frac{\alpha - a_k}{2}\right| + \left|\frac{\gamma - c_k}{2}\right| < \frac{1}{2n}.$$

Ex. 154. a) Élevons au carré l'expression $\sqrt{a+b+c} = \sqrt{a}+\sqrt{b}$ pour obtenir $a+b+c = a+b+2\sqrt{ab} \Leftrightarrow c = 2\sqrt{ab}$. Prenons $a = 18$ et $b = 50$ d'où $c = 60$ et l'on peut vérifier que $\sqrt{18+50+60} = \sqrt{18}+\sqrt{50}$.

b) L'astuce consiste à soustraire $\sqrt{a}$ puis élever le tout au carré. On a donc

$$b = a + c^2 - 2c\sqrt{a} \Leftrightarrow \sqrt{a} = (c^2 + a - b) \div (2c) \in \mathbb{Q} \quad \text{qui est absurde !}$$

On peut prolonger l'exercice en essayant de résoudre, sous les mêmes hypothèses

$$\sqrt{a} + \sqrt{b} + \sqrt{c} = d \in \mathbb{N}.$$

Ex. 155. La motivation de base de cet exercice est de faire inventer par les élèves toutes sortes de triangles rectangles dont 1, 2 ou 3 des côtés sont des entiers, et ou des irrationnels, de même concernant l'aire et le périmètre.

a) Prendre par exemple $a = 7 - \sqrt{23}$, $b = 7 + \sqrt{23}$ et $c = 12$ alors aire $= 13$ et péri. $= 26$.

∗ b) Si une seule des cathètes est irrationnelle alors le périmètre n'est pas rationnel. Par ailleurs, si l'aire est irrationnelle alors au moins une cathète l'est aussi. Ainsi donc, les deux cathètes doivent être irrationnelles. Normalisons la situation, en effectuant une homothétie de rapport $1/c$ pour transformer notre triangle en un triangle 'unitaire'. Dénotons par α l'un des l'angles aigus, P le périmètre du triangle unitaire, et Δ son aire. D'où le système d'équations

$$\begin{cases} 2\Delta = & \sin(\alpha)\cos(\alpha) \\ 1 = & \sin^2(\alpha) + \cos^2(\alpha) \\ P = & \sin(\alpha) + \cos(\alpha) + 1 \end{cases}$$

Élevons au carré cette dernière équation puis réduisons :

$$\sin^2(\alpha) + \cos^2(\alpha) + 1 + 2(\sin(\alpha) + \cos(\alpha)) + 2\sin(\alpha)\cos(\alpha) = 2 + 2(P-1) + 4\Delta = P^2$$

Ce qui est absurde puisque l'on aurait : $\Delta = (P^2 - 2(P-1) - 2)/4 \in \mathbb{Q}$.

Ex. 156. a) Fausse, sinon π pourrait s'écrire sous la forme d'un quotient de deux entiers, ce qui est absurde.

b) Fausse, car en prenant le cube, le membre de gauche est un entier et celui de droite est de la forme $a + b\sqrt{62}$. Ainsi, de manière similaire à l'exercice précédent, on déduirait $\sqrt{62} \in \mathbb{Q}$.

c) Vraie, il suffit d'additionner $\sqrt{2}$, élever au cube, puis réduire pour obtenir l'égalité.

d) L'exercice n'est qu'une généralisation du b) de l'ex. 154 (dans un cas particulier) : additionner $\sqrt{5}$, puis élever au carré fait apparaître deux termes irrationnels, l'un en $\sqrt{5}$ et l'autre en $\sqrt{6}$. Isoler ces deux termes pour à nouveau élever au carré : d'un côté il y aura un entier et de l'autre un terme irrationnel en $\sqrt{30}$. Absurde !

Quelques problèmes classiques autour des irrationnels

∗ **Ex. 157.** Comme $(a^b)^c = a^{bc}$, de deux choses l'une : soit $\sqrt{2}^{\sqrt{2}} := \alpha$ est rationnel et on a gagné, sinon $\alpha^{\sqrt{2}} = 2 \in \mathbb{Q}$ et dans ce cas on a aussi gagné.

∗ **Ex. 158.** À réaliser : chaque $a_i = 2^{\frac{1}{2^i}} \in \mathbb{R}\backslash\mathbb{Q}$, $\forall i \in \mathbb{N}^*$. Par ailleurs leur produit (partiel) est $\prod_{i=1}^{n} 2^{\frac{1}{2^i}} = 2^{\frac{1}{2}+\frac{1}{2^2}+\ldots+\frac{1}{2^n}} = 2^{1-\frac{1}{2^{n+1}}} = 2 \div 2^{\frac{1}{2^{n+1}}}$. L'exponentiation étant une fonction continue et $1/2^{n+1}$ convergeant vers 0 lorsque n tend vers l'infini, on obtient le résultat escompté.

∗ **Ex. 159.** Dans une première approche il ne nous semble pas indispensable de trop se soucier du problème de la convergence (même si elle n'est pas difficile à prouver).On obtient par les théorèmes fondamentaux de l'analyse (à gauche) et le développement d'une série géométrique (à droite) :

$$\begin{aligned}\frac{\pi}{4} = \arctan(x)\Big|_0^1 = \int_0^1 (\arctan(x))' dx = \int_0^1 \frac{1}{1+x^2} dx \\ = \int_0^1 \left(1 - x^2 + x^4 - x^6 + \ldots \pm \frac{x^{2n+2}}{1+x^2}\right) dx\end{aligned}$$

Posons $R_n := \displaystyle\int_0^1 \frac{x^{2n+2}}{1+x^2} dx$. En analyse on démontre que R_n converge vers 0 (lentement) lorsque n tend vers l'infini, et donc il suffit d'évaluer le reste :

$$\int_0^1 \left(1 - x^2 + x^4 - x^6 + \ldots\right) dx = \left(x - \frac{1}{3}x^3 + \frac{1}{5}x^5 - \frac{1}{7}x^7 + \ldots\right)\Big|_0^1 = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots$$

6.2 ** Le corps $\mathbb{Q}(\sqrt{2})$, l'anneau $\mathbb{Z}[\sqrt{2}]$ et ses unités

Recherche 1. Les cinq plus petits 'triangulaires-carrés' sont 1 ; 36 ; 1225 ; 41616 et 1413721. Il semble que le quotient de deux candidats consécutifs converge vers une valeur estimée à $33,9706\ldots$ et donc que l'ordre de grandeur du n^e 'triangulaire-carré' soit de $33,97^n$.

Recherche 2. Les cinq plus petits triplets pythagoriciens de ce type sont (3,4,5), (20,21,29), (119,120,169), (696, 697,985) et (4059,4060,5741). Associons à chacun des triangles leur aire, puis effectuons le rapport des aires de deux triangles consécutifs de la suite. Étrangement, il semble à nouveau que le quotient converge vers cette même valeur 33.9705882....
Remarque. Amusant aussi de voir apparaître 13^2 parmi les hypoténuses. Y a-t-il d'autres carrés dans la liste (des hypoténuses) ? Encore un sujet de recherche à explorer !

Recherche 3. Si l'on suppose $x = y + 1$ et $z = x + 1$ alors les cinq plus petits x sont 24, 840, 28560, 970224 et 32959080 et le rapport de deux valeurs consécutives semble converger à nouveau vers cette valeur mystérieuse de $33.97058\ldots$. Élevons ce dernier au carré pour voir apparaître 1154 à trois dix-millièmes prés. Relevons que ce nombre 1154 peut être obtenu par une méthode géométrique permettant d'approcher $\sqrt{2}$ à sept cent-millièmes près, méthode qui figure dans des textes, dénommés *Sulbasutra* et rédigés par des érudits hindouistes datant du VI^e siècle avant J.-C. :

$$\sqrt{2} \cong 1 + \frac{1}{3} + \frac{1}{3}\cdot\frac{1}{4} - \frac{1}{3}\cdot\frac{1}{4}\cdot\frac{1}{34} - \frac{1}{3}\cdot\frac{1}{4}\cdot\frac{1}{34}\cdot\frac{1}{1154}$$

** **Ex. 160.** a) Dans le premier cas, on a $n(n+1)/2 = m^2$. Multiplions par 8 et complétons le carré $4n^2 + 4n = (2n + 1)^2 - 1 = 2(2m)^2$. Posons $x = 2n + 1$ et $y = 2m$, d'où l'équation diophantienne $x^2 - 2y^2 = 1$.

b) Ici, $a^2 + (a + 1)^2 = c^2 \Leftrightarrow 2a^2 + 2a + 1 = c^2$. Multiplions cette dernière égalité par 2 et complétons le carré : $4a^2 + 4a + 2 = (2a + 1)^2 + 1 = 2c^2$. Dans ce cas, posons : $x = 2a + 1$ et $y = c$ pour obtenir $x^2 - 2y^2 = -1$.

c) Enfin, si $x = y + 1$ et $z = y + 2$ alors

$$\begin{cases} (y+1)^2 &= a^2 + y^2 \\ (y+2)^2 &= b^2 + y^2 \end{cases}$$

En soustrayant le double de la première équation à la deuxième on obtient $b^2 - 2a^2 = 2$. Avec $b = 2c$, qui substitué dans l'équation précédente donne : $2c^2 - a^2 = 1$, autrement dit $a^2 - 2c^2 = -1$.

** **Ex. 161.** Soit $z_1 = a_1 + b_1\sqrt{2}$ et $z_2 = a_2 + b_2\sqrt{2}$ avec a_i et $b_i \in \mathbb{Q}$. Montrons d'abord que l'addition la multiplication sont internes. En effet on a

$$z_1 + z_2 = a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2} = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}.$$

$$z_1 \cdot z_2 = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}.$$

Par ailleurs les éléments neutres y figurent aussi : $0 = 0 + 0 \cdot \sqrt{2}$ et $1 = 1 + 0 \cdot \sqrt{2}$. La commutativité, l'associativité de $+$ et de $\cdot$ aussi bien que la distributivité sont vérifiées

d'emblée puisque $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$. L'opposé de $a+b\sqrt{2}$ est évidemment $(-a)+(-b)\sqrt{2}$. Il reste à prouver que $a+b\sqrt{2}$ admet un inverse dans $\mathbb{Q}(\sqrt{2})$ lorsque a ou b sont non nuls. Or,

$$\frac{1}{z} = \frac{1}{a+b\sqrt{2}} = \frac{1\cdot(a-b\sqrt{2})}{(a+b\sqrt{2})\cdot(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

De plus, a et b appartenant aux rationnels ne peut annuler le dénominateur, puisque $\sqrt{2}$ est irrationnel.

** **Ex. 162.** Reprendre l'exercice précédent en imaginant que a et b sont des entiers. Evidemment, inutile de s'attarder sur l'inverse : tout élément de l'anneau n'est pas forcément inversible. Cependant, l'on va découvrir dans les exercices qui suivent que l'ensemble des éléments inversibles forme un *groupe infini* et *cyclique* (c'est-à-dire admettant un seul générateur). Nous dénoterons cet ensemble par la lettre U, car il se dénomme le *groupe des unités*.

** **Ex. 163.** Si $z_1 = a_1 + b_1\sqrt{2}$ et $z_2 = a_2 + b_2\sqrt{2}$ alors

a) $\overline{z_1+z_2} = (a_1+a_2) - (b_1+b_2)\sqrt{2} = a_1 - b_1\sqrt{2} + a_2 - b_2\sqrt{2} = \overline{z_1} + \overline{z_2}$

b) $\overline{z_1\cdot z_2} = (a_1a_2+2b_1b_2) - (a_1b_2+a_2b_1)\sqrt{2} = (a_1-b_1\sqrt{2})(a_2-b_2\sqrt{2}) = \overline{z_1}\cdot\overline{z_2}$

** **Ex. 164.**

$$N(z_1\cdot z_2) = z_1\cdot z_2\cdot\overline{z_1\cdot z_2} = z_1\cdot z_2\cdot\overline{z_1}\cdot\overline{z_2} = z_1\cdot\overline{z_1}\cdot z_2\cdot\overline{z_2} = N(z_1)\cdot N(z_2)$$

D'où

$$(a_1^2-2b_1^2)(a_2^2-2b_2^2) = (a_1a_2+2b_1b_2)^2 - 2(a_1b_2+a_2b_1)^2$$

** **Ex. 165.** $1\cdot 1 = 1$ et $(-1)\cdot(-1) = 1$ et sont donc leur propre inverse. Pour les autres exercices, il suffit d'amplifier par le conjugué :

$$(1+\sqrt{2})^{-1} = \frac{1}{1+\sqrt{2}} = \frac{1-\sqrt{2}}{(1+\sqrt{2})(1-\sqrt{2})} = -1+\sqrt{2}.$$

De même,

$$(3-2\sqrt{2})^{-1} = \frac{1}{3+2\sqrt{2}} = \frac{3+2\sqrt{2}}{(3-2\sqrt{2})(3+2\sqrt{2})} = 3+2\sqrt{2}.$$

De ces exemples, on déduit que si $N(7-5\sqrt{2}) = \pm 1$ alors $7-5\sqrt{2} \in U$. Or, $N(7-5\sqrt{2}) = (7-5\sqrt{2})(7+5\sqrt{2}) = -1$. De même $N(-17-12\sqrt{2}) = (-17-12\sqrt{2})(-17+12\sqrt{2}) = 289-288 = 1$. Plus généralement, on démontre :

** **Ex. 166.** *Preuve du théorème.*
Soit u et son inverse, $u^{-1} \in U$ alors

$$1 = N(1) = N(u\cdot u^{-1}) = N(u)\cdot N(u^{-1}) \in \mathbb{Z}.$$

Comme les seuls diviseurs de 1 sont ± 1 alors chacun des deux derniers facteurs ne peut être que ± 1.
Réciproquement, si $u = a+\sqrt{2}b$ et $N(u) = \pm 1$ alors

$$\frac{1}{u} = \frac{\overline{u}}{u\cdot\overline{u}} = \frac{\overline{u}}{N(u)} = (a-\sqrt{2}b)\cdot(\pm 1)$$

En fait, si $a + \sqrt{2}b > 0$ alors son inverse est le nombre positif parmi $\pm(a - \sqrt{2}b)$. Par ailleurs, par l'exercice 164 toutes les puissances naturelles de $1 + \sqrt{2}$ sont des unités. Le but du dernier exercice est de montrer que toute unité (> 1) ne peut s'obtenir que de cette manière.

∗∗ **Ex. 167.** D'abord si $u \in U$ alors $-u$, u^{-1} et $-u^{-1}$ sont aussi des unités et l'un parmi les quatre est ≥ 1.
Ensuite, montrons qu'il ne peut exister d'unité $a + \sqrt{2}b$ comprise entre 1 et $1 + \sqrt{2}$. En effet, si $1 < a + \sqrt{2}b < 1 + \sqrt{2}$ alors a et b ne peuvent être de même signe. D'où $1 <| a - \sqrt{2}b |$. Mais alors en effectuant le produit de ces dernières inéquations on obtiendrait $1 <| a^2 - 2b^2 | = 1$, une absurdité.
Enfin, supposons l'existence d'une unité $v > 1$ ne provenant pas d'une puissance naturelle de $1 + \sqrt{2}$. Il existe alors $k \in \mathbb{N}$ tel que $(1 + \sqrt{2})^k < v < (1 + \sqrt{2})^{k+1}$. Or, la multiplication par $(1 + \sqrt{2})^{-k}$ de part et d'autre des inégalités impliquerait l'existence d'une unité comprise entre 1 et $1 + \sqrt{2}$, qui est en contradiction avec le point précédent.

Chapitre 7

À propos des nombres complexes

∗ **Ex. 168.** a) D'abord $\overline{\overline{\alpha}} = \overline{\overline{a_1 + ia_2}} = \overline{a_1 - ia_2} = a_1 + ia_2 = \alpha$.
Ensuite, soit f un automorphisme de $\mathbb{C}$ qui fixe $\mathbb{R}$. Comme $f(a_1 + ia_2) = f(a_1) + f(i)f(a_2) = a_1 + f(i)a_2$ il suffit de déterminer l'image de i. Or, $-1 = f(-1) = f(i^2) = f(i)f(i)$ et donc $f(i) = \pm i$. Il n'en existe donc que deux : l'identité et la conjugaison.

b) $\overline{\alpha + \beta} = \overline{a_1 + ia_2 + b_1 + ib_2} = \overline{a_1 + b_1 + i(a_2 + b_2)} = a_1 + b_1 - i(a_2 + b_2) = a_1 - ia_2 + b_1 - ib_2 = \overline{\alpha} + \overline{\beta}$
$\overline{\alpha \cdot \beta} = \overline{(a_1 + ia_2)(b_1 + ib_2)} = \overline{a_1b_1 - a_2b_2 + i(a_2b_1 + a_2b_2)} = a_1b_1 - a_2b_2 - i(a_2b_1 + a_1b_2) = (a_1 - ia_2)(b_1 - ib_2) = \overline{\alpha} \cdot \overline{\beta}$

∗ **Ex. 169.** Les opérations d'addition et de multiplication sont internes car, si $\alpha \in \mathbb{Z}[i]$ et $\beta \in \mathbb{Z}[i]$ alors $a_1 + ia_2 + b_1 + ib_2 = (a_1 + b_1) + i(a_2 + b_2) \in \mathbb{Z}[i]$, $(a_1 + ia_2)(b_1 + ib_2) = a_1b_1 - a_2b_2 - i(a_2b_1 + a_1b_2) \in \mathbb{Z}[i]$. De plus, $0 = 0 + i \cdot 0 \in \mathbb{Z}[i]$ et $1 = 1 + i \cdot 0 \in \mathbb{Z}[i]$ et l'opposé de α est $a_1 - ia_2 \in \mathbb{Z}[i]$. Enfin, les propriétés de commutativité, d'associativité et de distributivité sont héritée de $\mathbb{C}(+, \cdot)$.

∗ **Ex. 170.** $N(\alpha \cdot \beta) = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha) \cdot N(\beta)$, c'est-à-dire :
$(a_1^2 + a_2^2) \cdot (b_1^2 + b_2^2) = (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2$

∗ **Ex. 171.** a) Si α est réductible alors $\alpha = \beta \cdot \gamma$, dont les normes respectives de ces derniers facteurs sont > 1. Alors $N(\alpha) = N(\beta) \cdot N(\gamma)$ serait un nombre composé. D'où contradiction.
La réciproque est fausse, car $N(3) = 3^2$ et 3 est irréductible dans $\mathbb{Z}[i]$, car si α divise 3 alors $N(\alpha)$ est un diviseur propre de 9, et donc égale à 3. Or, l'équation $a^2 + b^2 = 3$ n'admet aucune solution entière.

b) $5 = 2^2+1^2 = (2+i)(2-i)$, $13 = 3^2+2^2 = (3+2i)(3-2i)$, $17 = 4^2+1^2 = (4-i)(4+i)$, $29 = 5^2+2^2 = (5-2i)(5+2i)$, $37 = 6^2+1^2 = (6-i)(6i)$, $41 = 5^2+4^2 = (5+4i)(5-4i)$, ... et plus généralement il semblerait que tout premier p qui est un de plus qu'un multiple de 4 peut s'écrire comme une somme de deux carrés et donc est réductible sur $\mathbb{Z}[i]$.

c) Le raisonnement du point a) peut être appliqué sur tout premier p de la forme $p = 4n - 1$, où $n \in \mathbb{N}$, car $N(p + 0i) = p^2$ et si α divise p alors $N(\alpha)$ est un diviseur propre de p^2, et donc devrait être égal à p. Or, l'équation $a^2 + b^2 = p$ n'admet aucune solution entière, car le membre de gauche est 1 de plus qu'un multiple de 4 et celui de droite est 1 de moins qu'un multiple de 4.

∗ **Ex. 172.** Effectuons une récurrence sur la norme des $\alpha \in \mathbb{Z}[i]$. Si $N(\alpha) = 1$ alors par ex. 171 b) α est une unité. Considérons un α et sa norme $N(\alpha) > 1$. Si α est irréductible alors OK. Sinon, $\alpha = \beta \cdot \gamma$, dont les normes respectives sont des diviseurs propres de $N(\alpha)$ de plus > 1. Par hypothèse de récurrence β et γ se décomposent en un produit de facteurs irréductibles.

∗ **Ex. 173.** Soit $\alpha = a_1 + ia_2$. Alors $2 \mid N(\alpha)$ est équivalent à a_1 et a_2 sont de même parité. Soustrayons alors $(1+i) \cdot a_1$ à α pour obtenir $i(a_2 - a_1)$. Comme $2 = (1+i)(1-i)$ et que $a_2 - a_1$ est pair alors $1 + i$ divise tous les termes en question et donc aussi α.
La réciproque est évidente car, si $(1 + i) \mid \alpha$ alors $N(1 + i) \mid N(\alpha)$ et $N(1 + i) = 2$.

∗ **Ex. 174.** Soit δ un diviseur commun de $\alpha = a + ib$ et $\overline{\alpha} = a - ib$. Alors δ divise aussi bien la somme que la différence de ces deux derniers, c'est-à-dire $\delta \mid 2a$ et $\delta \mid 2ib$. D'où, $N(\delta) \mid 4a^2$ et $N(\delta) \mid 4b^2$. Or, a et b étant de parités différentes et premiers entre eux implique que $N(\delta) = 1$.

∗ **Ex. 175.** a) Si α est un carré alors il existe $\beta = c + id \in \mathbb{Z}[i]$ t.q. $\beta^2 = (c^2 - d^2) + 2cdi = a + ib$. D'où $b = 2cd$ est donc pair. De plus, comme $i^2 = -1$ alors $-\alpha = (i\beta)^2$.

b) Comme $(-1)^3 = -1$ et $i^3 = -i$ alors -1 et $-i$ sont des cubes, ainsi que leur produit i.

$\mathbb{Z}[i]$ admet une division euclidienne pour N

∗ **Ex. 176.**

a) $\frac{3+4i}{1-2i} = \frac{(3+4i)(1+2i)}{(1-2i)(1+2i)} = -1 + 2i$

b) $\frac{3+5i}{1-i} = -1 + 4i$

c) $\frac{5+7i}{6+i} = 1 + i$

d) $\frac{15-8i}{1+4i} = -1 - 4i$

∗ **Ex. 177.** Si $\alpha = 1 - 8i$ et $\beta = 4 - 7i$ alors $N(\alpha) = 65$ et $N(\beta) = 65$ et on a bien $65 \mid 65$, mais $\frac{\alpha}{\beta} = \frac{1-8i}{4-7i} = \frac{12}{13} - \frac{5}{13}i$

∗ **Ex. 178.** De $\frac{13+15i}{1+3i} = \frac{29}{5} - \frac{12}{5}i$ on déduit $13 + 15i = (6 - 2i)(1 + 3i) + 1 - i$. De plus $1 + 3i = (-1 + 2i)(1 - i)$ et donc $1 - i = (13 + 15i, 1 + 3i)$.

∗ **Ex. 179.** Si $\alpha = 23 + 16i$ et $\beta = 5 - 12i$ alors

$$\begin{aligned} 23 + 16i &= (2i)(5 - 12i) + (-1 + 6i) \\ 5 - 12i &= (-2)(-1 + 6i) + 3 \\ -1 + 6i &= 2i \cdot 3 + (-1) \end{aligned}$$

D'où $-1 = (\alpha, \beta)$ et en 'remontant' les calculs précédents on obtient :

$$\begin{aligned} (-1) &= (-1 + 6i) + 3 \cdot 2i \\ &= (-1 + 6i) - [(5 - 12) + 2 \cdot (-1 + 6i)] \cdot (2i) \\ &= (1 - 4i)[(23 + 16i) - (2i)(5 - 12i)] - (5 - 12i) \cdot 2i \\ &= (1 - 4i)(23 + 16i) - (8 + 4i)(5 - 12i) = (1 - 4i) \cdot \alpha + (-8 - 4i) \cdot \beta \end{aligned}$$

Notons que *le* pgcd est défini à la multiplication près par une unité ± 1 ou $\pm i$.

∗ **Ex. 180.** La démonstration est identique à celle du lemme 2 (p.16), en substituant des lettres grecques aux latines : si γ ne divise pas α alors par l'algorithme d'Euclide on exprime 1 (leur pgcd) sous la forme d'une combinaison linéaire (sur $\mathbb{Z}[i]$) de α et γ. Ainsi, il existe δ et $\epsilon \in \mathbb{Z}[i]$ tels que :

$$1 = \delta\alpha + \epsilon\gamma$$

En multipliant le tout par β, on obtient

$$\beta = \delta\alpha\beta + \beta\epsilon\gamma$$

Comme $\gamma \mid \alpha\beta$ et que $\gamma \mid \gamma$ alors γ divise leur somme qui est β.

∗ **Ex. 181.** Une fois de plus, la preuve peut être recopiée presque mot pour mot en substituant les lettres grecques aux latines. La seule différence entre les deux argumentations est que sur les nombres entiers la norme n'est autre que $N(a) = \sqrt{a^2} = |a| \in \mathbb{N}$ alors que sur $\mathbb{Z}[i]$ on a $N(\alpha) = a^2 + b^2 \in \mathbb{N}$, si $\alpha = a + ib \in \mathbb{Z}[i]$.

L'exercice qui suit n'as pu être introduit dans le cahier par faute de place. Cependant j'estime qu'il mérite d'être connu !

Exercice bonus.

Soit $z \in \mathbb{Z}[i]$ tel que $\mathcal{N}(z) = p > 2$. Montrer que z est irréductible si et seulement s'il existe $n \in \mathbb{N}$ tel que $p = 4n + 1$ est premier ou si $p = q^2$ et $q = 4n + 3$ est premier.

∗∗ **Ex. 182.** Pour commencer, montrons que si $p = 4n+3$ est premier alors p est irréductible dans $\mathbb{Z}[i]$. En effet, si $(a + ib) \mid p$ alors $N(a + ib)$ divise strictement $N(p) = p^2$ et donc on aurait $a^2 + b^2 = p$. Ce qui est absurde, puisque $a^2 + b^2$ est un de plus qu'un multiple de 4. Ensuite, si $p = 4n + 1$ est premier alors $p = a^2 + b^2 = (a + ib)(a - ib)$ par le corollaire 2 (p.34) De plus, $a + ib$ doit être irréductible dans ce cas, puisque $D_p = \{1, p\}$.
Enfin, si $z = a + ib$ est irréductible et $a \cdot b \neq 0$ alors $(a, b) = 1$ et $\overline{z} = a - ib$ l'est aussi. Par ailleurs, $z\overline{z} = a^2 + b^2$ ne peut-être décomposé d'une autre manière dans $\mathbb{Z}[i]$ et admet donc exactement deux facteurs de norme identique et strictement supérieure à 1. Ainsi, $a^2 + b^2$ ne peut être qu'un nombre premier p. De plus, étant une somme de deux carrés p est un de plus qu'un multiple de 4.
Signalons enfin pour conclure que si $a \cdot b = 0$, on peut supposer que $a \neq 0$ en multipliant par une unité convenable. Dans ce cas, si $z = a$ est irréductible et que $N(a) > 1$ alors a est forcément un nombre premier p. Par le corollaire 2 (p.34), $p = 4n + 3$ pour un certain $n \in \mathbb{N}$ et $N(a) = p^2$.