Feuille d'exercices 1

Avertissement : tous les exercices ne seront pas traités durant les séances ; pour en suivre l'avancement veuillez consulter mon site personnel dans la rubrique *Forum.*

1. PGCD et relations de Bezout

Exercice 1.1. — *1. Calculer le pgcd d de* 17640 *et* 525*. Déterminer deux entiers u et v tels que l'on ait* $d = 17640u + 525v$.

2. Soient a et b deux entiers naturels, non tous les deux nuls, et d leur pgcd. Montrer que le pgcd de $2^a - 1$ et $2^b - 1$ est $2^d - 1$.

3. Déterminer les couples $(x, y) \in \mathbb{Z}^2$ tels que $47x + 111y = 1$.

Exercice 1.2. — *Donnez en fonction de n, le pgcd $(n^3 + n^2 + 1, n^2 + 2n - 1)$.*

Exercice 1.3. — ** Variations sur le théorème de Bezout :*

(a) En utilisant l'algorithme d'Euclide, trouver les relations de Bezout entre 650 *et* 66.

(b) On suppose que l'on ne dispose que de pieces de valeurs a et b entières avec $(a, b) = 1$.

(i) Quelles sommes peut-on payer si on nous rend la monnaie ?

(ii) Même question si on ne peut pas nous rendre la monnaie ? (Indication : montrer que si $m+n = ab-a-b$ alors exactement une somme parmi m et n est payable).

(c) Étudiez le cas de 3 *pièces de valeur* 15, 20 *et* 48 *en montrant que* 217 *est la plus grande somme que l'on ne peut pas payer.*

(d) Généralisez (c) en montrant que pour $a, b, c > 0$ premiers entre eux deux à deux, $2abc - ab - bc - ac$ est le plus grand entier qui ne peut pas s'écrire sous la forme $xbc + yca + zab$ avec $x, y, z \geq 0$.

(e) Montrez par récurrence sur n que si $a_1, \cdots, a_n$ sont n entiers strictement positifs premiers entre eux deux à deux alors

$$a_1 \cdots a_n \Big(n - 1 - \sum_{i=1}^{n} \frac{1}{a_i} \Big)$$

est le plus grand entier qui ne peut pas s'écrire sous la forme $\sum_{i=1}^n x_i \prod_{j \neq i} a_j$ avec $x_i \geq 0$ pour tout $i = 1, \cdots, n$.

Exercice 1.4. — *Montrez que le nombre de solutions entières positives de l'équation diophantienne*

$$x + 2y + 3z = n$$

est égal à l'entier le plus proche de $\frac{(n+3)^2}{12}$.

Exercice 1.5. — *Montrez que le nombre de solutions entières positives des équations diophantiennes suivantes*

$$x + 2y = n, \quad 2x + 3y = n - 1, \quad 3x + 4y = n - 2, \cdots, nx + (n+1)y = 1, \quad (n+1)x + (n+2)y = 0$$

est égal à $n + 1$.

Exercice 1.6. — *Soient $a_1, \cdots, a_l$ des entiers positifs premiers entre eux dans leur ensemble. Soit A_n le nombre de solutions entières positives de*

$$a_1x_1 + a_2x_2 + \cdots + a_lx_l = n$$

(1) Montrez que

$$\lim_{n\to\infty} \frac{A_n}{n^{l-1}} = \frac{1}{a_1 \cdots a_l(l-1)!}.$$

(2) Supposons en outre que les a_i sont premiers entre eux deux à deux. Montrez alors que

$$A_n = P(n) + Q_n$$

où $P(x)$ est un polynôme à coefficients rationnels de degré $l - 1$ et où la suite Q_n est périodique de période $a_1 \cdots a_l$.

(3) Dans le cas $l = 2$ où $a_1 = a$ et $a_2 = b$ sont premiers entre eux, montrez que

$$A_n \leq 1 \text{ quand } n < ab,$$
$$A_n \geq 1 \text{ quand } n > ab - a - b,$$

et qu'en outre on a :
- $A_{ab} = 2$,
- $A_{ab-a-b} = 0$,
- $A_{n+ab} = A_n + 1$,
- A_n *est égal à* $\lfloor \frac{n}{ab} \rfloor$ *ou* $\lfloor \frac{n}{ab} \rfloor + 1$.

2. Congruences

Exercice 2.7. — *1. Donner la congruence modulo 17 de* $(1035125)^{5642}$.

2. *Déterminer l'ensemble des entiers relatifs congrus à 2 modulo 37 et à 9 modulo 19.*

3. *Montrer que 429 est inversible multiplicativement dans $\mathbb{Z}/700\mathbb{Z}$ et donner son inverse.*

4. *Montrer que si n est un entier naturel impair, 7 divise $2^{2^n} + 3$. Montrer que si n est congru à 2 modulo 6, alors 19 divise $2^{2^n} + 3$.*

Exercice 2.8. — *(i) Donnez le cardinal de l'ensemble des éléments d'ordre divisant d dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.*
(ii) Pour $d = pq$ avec p et q premiers divisant n, donnez le nombre d'éléments d'ordre d dans $(\mathbb{Z}/n\mathbb{Z})^2$.

Exercice 2.9. — *Montrer qu'il n'existe pas d'entiers $n \geq 2$ tels que n divise $2^n - 1$.*
Indication : on suppose qu'il existe un tel entier n et l'on considère le plus petit diviseur premier p de n. Trouver une contradiction en examinant l'ordre de 2 dans $\big(\mathbb{Z}/p\mathbb{Z}\big)^*$.

Exercice 2.10. — *Montrer que le seul entier impair n qui divise $3^n + 1$ est $n = 1$.*
Indication : comme ci-dessus, on suppose qu'il existe un entier impair $n \geq 3$ divisant $3^n + 1$. Si p est le plus petit diviseur premier de n, on obtient une contradiction en examinant l'ordre de 3 dans $\big(\mathbb{Z}/p\mathbb{Z}\big)^*$.

Exercice 2.11. — *Soit n un entier naturel impair. Montrer que n divise $2^{n!} - 1$.*

Exercice 2.12. — ** Existe-t-il des couples $(a, b) \in \mathbb{N}^2$ tels que :*
- *$ab(a + b)$ n'est pas divisible par 7 ;*
- *$(a + b)^7 - a^7 - b^7$ est divisible par 7^7 ?*

Exercice 2.13. — **** Soit $n \geq 2$; montrez que si $k^2 + k + n$ est premier pour tout entier $0 \leq k \leq \sqrt{n/3}$ alors c'est encore vrai pour tout entier $0 \leq k \leq n - 2$.*
Remarque : on peut montrer que les seules valeurs n telles que la condition de l'énoncé est vérifiée sont $2, 3, 5, 16$ et 41 ; on peut montrer que cette condition est équivalent à demander que $\mathbb{Z}[\sqrt{1 - 4n}]$ est factoriel, résultat prouvé par Heegner en 1952 alors qu'il était professeur de lycée à Berlin. Par ailleurs le lecteur notera que si on numérote les entiers en spirale autour de n, les nombres $k^2 + k + n$ sont sur la diagonale $y = x$: spirales d'Ulam.

Exercice 2.14. — *** On considère l'ensemble suivant $\mathcal{E} \subset \mathbb{N}$ constitué des nombres dont l'écriture n en base 3 est de la forme $\sum_{i=0}^{10} a_i 3^i$ avec $a_i = 0, 1$. Montrez que trois éléments quelconques de $\mathcal{E}$ ne sont pas les termes consécutifs d'une progression arithmétique.*
Remarque : que pensez-vous de l'avenir de l'exercice suivant : existe-il 2008 entiers > 0 inférieurs ou égaux à 10^5 et tels que trois quelconques d'entre eux ne soient pas les termes consécutifs d'une progression arithmétique ?

Exercice 2.15. — *Montrez que $y^2 = x^3 + 7$ n'a pas de solutions entières.*

3. Nombres premiers

Exercice 3.16. — *1. Déterminer les nombres premiers p tels que $p+2$ et $p+4$ soient premiers.*

2. Déterminer les nombres premiers p tels que p divise 2^p+1.

3. Soit p un nombre premier impair. Montrer qu'il existe une infinité d'entiers n tels que p divise $n2^n+1$.

Exercice 3.17. — *Montrez qu'il ne peut pas exister de polynômes de $\mathbb{Z}[X]$ non constant ne prenant sur $\mathbb{N}$ que des valeurs premières.*

Exercice 3.18. — *Montrez en utilisant le théorème de Wilson, que la fonction*

$$f(n) = 2 + 2(n!) \mod n+1$$

produit tous les nombres premiers exclusivement mais plusieurs fois.

Exercice 3.19. — *En 1947 W. Mills établit l'existence d'une constante A telle que pour tout $n>1$,*

$$\lfloor A^{3n} \rfloor \in \mathcal{P}, \qquad A \simeq 1,306377883863...$$

cependant le calcul de cette constante nécessite la connaissance de $\mathcal{P}$ ce qui convenons le n'est pas très honnête. L'escroquerie est du même genre que la suivante : posons

$$L = 0,2,0030000500000070000000011...$$

le n-ème nombre premier étant placé en position n^2. On vérifie alors aisément que

$$\lfloor L \times 10^{n^2} \rfloor - \lfloor L \times 10^{(n-1)^2} \rfloor 10^{2n-1}$$

est égal au n-ème nombre premier p_n.

On s'interdit désormais d'utiliser des nombres pouvant cacher une infinité d'informations. Le premier exemple du à Roland Yéléhada repose sur la formule suivante

$$t(n) = 2 + n \lfloor \frac{1}{1+\sum_{p=2}^{m+1} \lfloor \frac{n+2}{p} - \lfloor \frac{n+1}{p} \rfloor \rfloor} \rfloor$$

laquelle produit tous les nombre premiers. Montrez cette affirmation.

Exercice 3.20. — *Montrez que le développement décimal de $\frac{1}{p}$ est périodique, après la virgule, de période l'ordre de 10 dans $(\mathbb{Z}/p\mathbb{Z})^\times$.*

Exercice 3.21. — *Soit T la période du développement décimal de $\frac{1}{p} = 0, a_1a_2 \cdots, a_T\ a_1 \cdots$ et notons $n = \sum_{i=1}^d a_i 10^{T-i}$. Montrez que*

$$np = 10^T - 1.$$

Exercice 3.22. — *Soit $d=2e$ un multiple de l'ordre T de 10 dans $(\mathbb{Z}/p\mathbb{Z})^\times$ tel que e n'est pas un multiple de T. Pour*

$$A = \sum_{i=1}^e a_i 10^{e-i}, \qquad B = \sum_{i=1}^e a_{e+i} 10^{e-i}.$$

Montrez que $A+B = 10^e - 1$.

Exercice 3.23. — *Soit p premier tel que la période de son développement décimal soit égale à $p-1$; montrez que le nombre dn s'obtient alors à partir de n par permutation circulaire.*
Par exemple : pour $p=7$, on a

$$\begin{aligned}
2 \times 142857 &= 285714\\
3 \times 142857 &= 428571\\
4 \times 142857 &= 571428\\
5 \times 142857 &= 714285\\
6 \times 142857 &= 857142
\end{aligned}$$

Exercice 3.24. — *Soit $p>11$ premier ; montrez que $a_{(p+1)/2} = 0$ si et seulement si $(\frac{10}{p}) = 1$ et sinon elle est égale à 9.*

4. Des exemples simples d'équations diophantiennes sur $\mathbb{Z}$

4.1. Descente infinie à la Fermat. —

Exercice 4.25. — *Soient $a, b > 0$ tels que $ab + 1 | a^2 + b^2$; montrez que le quotient est un carré parfait.*

Exercice 4.26. — *Soit l'équation $x^4 + y^4 = z^2$.*

(1) Montrez que si (x, y, z) est une solution avec $x \wedge y \wedge z = 1$ alors $z > 0$ y pair et x impair

(2) On suppose $y \neq 0$ et on écrit $y^4 = (z - x^2)(z + x^2)$. Montrez que $(z - x^2) \wedge (z + x^2) = 2$ et en déduire que

$$(z - x^2, z + x^2) = (2a^4, 8b^4) \text{ ou } (8b^4, 2a^4), \quad a \equiv 1 \mod 2, \quad a \wedge b = 1, \quad a > 0.$$

(3) Montrez que le cas $(z - x^2, z + x^2) = (2a^4, 8b^4)$ est impossible.

(4) Construisez une solution (c, d, a) de l'équation telle que $0 < a < z$ et concluez.

4.2. Infinité de solutions. —

Exercice 4.27. — *Le plan $\mathcal{P}$ étant rapporté à un repère orthonormal $(O, \vec{u}, \vec{v})$, on considère l'hyperbole $\mathcal{H}$ d'équation $x^2 - 3y^2 = 1$ et on désigne par $\mathfrak{S}$ l'ensemble des points du plan dont les deux coordonnées sont des éléments de $\mathbb{Z}$. On se propose d'étudier l'ensemble $\mathcal{H} \cap \mathfrak{S}$.*

(1) A tout point M de coordonnées (x, y) dans $(O, \vec{u}, \vec{v})$, on associe son affixe $z = x + iy \in \mathbb{C}$. On définit une application $f : \mathbb{C} \to \mathbb{C}$ par $f(z) = (2 - i)z + 2i\bar{z}$. A f on associe l'application $F : \mathcal{P} \to \mathcal{P}$ qui au point d'affixe z associe $M' = F(M)$ d'affixe $z' = f(z)$.

(i) Montrez que F est une application affine et bijective qui conserve les aires des triangles. Est-ce une isométrie ?

(ii) Montrez que M appartient à $\mathcal{H}$ (resp. $\mathfrak{S}$) si et seulement si M' aussi.

(2) On construit par récurrence une suite de points $(A_n)_{n \in \mathbb{N}}$ en posant pour tout n : $A_{n+1} = F(A_n)$, A_0 étant le point de coordonnées $(1, 0)$.

(i) Calculez les coordonnées de A_1 et A_2 puis montrez que pour tout n, $A_n \in \mathcal{H} \cap \mathfrak{S}$.

(ii) Quels sont les points de $\mathfrak{S}$ situés sur l'arc $[A_0, A_1]$ de $\mathcal{H}$?

(3) On définit sur $\mathcal{H}$ une opération $*$ ainsi : M et N étant deux points de $\mathcal{H}$, on leur associe la droite $D_{M,N}$ issue de A_0 et parallèle à la droite (MN) (ou à la tangente en M à $\mathcal{H}$ si $M = N$). Dans le cas où $D_{M,N}$ est tangente à $\mathcal{H}$ en A_0, on pose $M * N = A_0$ et sinon $M * N$ est le second point de rencontre de $D_{M,N}$ avec $\mathcal{H}$, cf. la figure 1

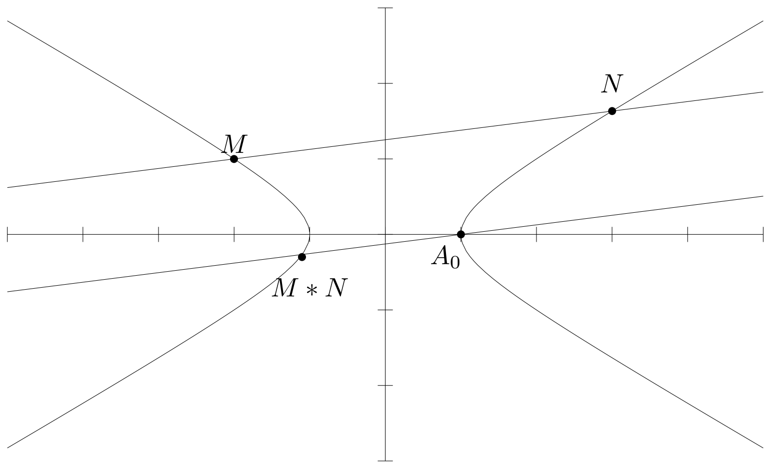

Figure 1. Loi de groupe sur une hyperbole

(i) Montrez qu'il existe un repère $\mathcal{R}$ de $\mathcal{P}$ dans lequel $\mathcal{H}$ a pour équation $XY = 1$. Exprimez alors dans ce repère l'abscisse de $M * N$ en fonction de celle de M et N. En déduire que $(\mathcal{H}, *)$ est un groupe isomorphe au groupe multiplicatif $(\mathbb{R}^*, \times)$.

(ii) *Montrez que pour tout $M \in \mathcal{H}$, $F(M) = A_1 * M$ et calculez les coordonnées (X_n, Y_n) de A_n dans $\mathcal{R}$ en fonction de X_1 et n.*
(iii) *Montrez que la tangente en A_n à $\mathcal{H}$ est parallèle à la droite $(A_{n-1}A_{n+1})$ puis calculez l'aire du triangle $A_{n-1}A_nA_{n+1}$.*
(iv) *Prouvez que M est un point de l'arc $[A_n, A_{n+1}]$ de $\mathcal{H}$ si et seulement si $M' = A_1 * M$ appartient à l'arc $[A_{n+1}, A_{n+2}]$ de $\mathcal{H}$. Décrivez alors l'ensemble $\mathcal{H} \cap \mathfrak{S}$.*
(4) *Donnez tous les couples (x, y) de nombres entiers naturels solutions de l'équation $x^2 - 3y^2 = 1$.*

Equation de Thue Il s'agit d'équations de la forme $F(X, Y) = m$ avec $F(X, Y) \in \mathbb{Z}[X, Y]$ homogène de degré au moins 3. Dès 1909, Thue a montré que ces équations ne possédaient qu'un nombre fini de solution et dans les années 60 Baker parvint à donner une majoration sur la taille des solutions en fonction des coefficients de F et de m. Cependant sa majoration était trop large pour être efficace et ce n'est qu'en 1989 que Tzanakis et de Weger ont donnés un algorithme efficace permettant de résoudre ces équations : celui-ci repose sur l'algorithme LLL. La preuve de la finitude du nombre de solutions d'une équation de Thue repose sur le résultat difficile suivant

Théorème de Thue *Soit $\alpha \in \mathbb{R}$ un nombre algébrique de degré d ; pour tout $\epsilon > 0$, il existe une constante $C_\epsilon(\alpha) > 0$ telle que pour tout p/q avec $p \wedge q = 1$,*

$$|\alpha - \frac{p}{q}| > \frac{c}{q^{d/2+1+\epsilon}}.$$

Exercice 4.28. — *Soit $F(x, y) = a_n x^n + a_{n-1}x^{n-1}y + \cdots + a_0 y^n \in \mathbb{Z}[x, y]$ un polynôme homogène irréductible de degré $n \geq 3$. Montrez alors que pour tout $m \in \mathbb{Z}$, l'équation diophantienne $F(x, y) = m$ possède un nombre fini de solutions entières.*

4.3. Extension de corps. —

Exercice 4.29. — *Soit $A = \mathbb{Z}[i\sqrt{2}] = \{a+ib\sqrt{2} \ / \ (a, b) \in \mathbb{Z}^2\}$. On définit pour $z = a+ib\sqrt{2} \in A$, $N(z) = a^2+2b^2$.*
(a) *Montrez que B est euclidien et donc factoriel.*
(b) *Soient $(x, y) \in \mathbb{Z}^2$, vérifiant l'équation $y^2 + 2 = x^3$. Montrez que x est impair puis que dans B, $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux. En déduire qu'il existe $(a, b) \in \mathbb{Z}^2$ tels que $x = a^2+2b^2$ et $y+i\sqrt{2} = (a+ib\sqrt{2})^3$, puis décrire les solutions de l'équation précédente.*
(c) *Étudiez comme dans l'exercice précédent l'ensemble $S = \{n \in \mathbb{N} \ / \ \exists (x, y) \in \mathbb{Z}^2, \ n = x^2 + 2y^2\}$.*
Indication : on utilisera que -2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1, 3 \mod 8$.
(d) *Étudiez de même l'ensemble $\{n \in \mathbb{Z} \ / \ \exists (x, y) \in \mathbb{Z}^2, \ n = x^2 - 2y^2\}$.*

Exercice 4.30. — *Soit $d > 1$ sans facteurs carrés avec $d \equiv 1, 2 \mod 4$, on suppose que le nombre de classes de $\mathbb{Q}(i\sqrt{d})$ n'est pas divisible par 3. Montrez alors $y^2 = x^3 - d$ a une solution entière si et seulement si d est de la forme $3t^2 \pm 1$ auquel ses solutions sont $(t^2 + d, \pm t(t^2 - 3d))$.*

Remarque : d'autres équations :
- *courbes elliptiques* : il s'agit de trouver les points entiers et rationnels de la courbe régulière $E : y^2+a_1xy+a_3y = x^3 + a_2x^2 + a_4x + a_6$. Le fait remarquable est que ces courbes peuvent être munis d'une loi de groupe qui géométriquement se définit à la manière de celle sur l'hyperbole. Le théorème de Mordell-Weil dit que pour tout corps K, $E(K)$ est un groupe abélien de type fini dont le rang est conjecturalement égal à l'ordre du zéro en $s = 1$ de la fonction L attachée à E ; c'est la version faible de la conjecture de Birch-Swinnerton-Dyer ;
- *travaux de Siegel* : en 1929 Sigel a donné des CNS sur le polynôme $f \in \mathbb{Z}[X, Y]$ pour qu'il possède une infinité de solutions.
- *théorème de Faltings* : soit C une courbe algébrique non singulière de genre g alors :
  - si $g = 0$, il y a soit aucun point rationnel soit une infinité (cf. l'exercice 4.29 ;
  - si $g = 1$, i.e. C est une courbe elliptique, il y a soit un nombre fini de points formant un groupe abélien soit l'ensemble des points rationnels est un groupe abélien de type fini (théorème de Mordell) ;
  - si $g > 1$ il n'y a qu'un nombre fini de points rationnels.

- **Principe de Hasse** : une équation diophantienne vérifie le principe de Hasse si l'existence de solutions rationnelles « globales », i.e. sur $\mathbb{Q}$, découle de l'existence de solutions dans $\mathbb{Q}_p$ pour tout p premier ainsi que dans $\mathbb{R}$. L'exemple standard du à Selmer d'une équation diophantienne ne vérifiant pas le principe de Hasse est $3x^3 + 4y^3 + 5z^3 = 0$. Au contraire les formes quadratiques non dégénérées vérifient le principe de Hasse, c'est le fameux théorème de Hasse-Minkowski, cf. [**2**] p.73 : dans le cas particulier des formes ternaires le résultat est du à Legendre, cf. loc. cit. ou [**1**] chapitre 17 §3.

Références

[1] K. Ireland and M. Rosen. *A classical introduction to modern number theory.* Springer-Verlag, 1982.

[2] J.-P. Serre. *Cours d'arithmétique.* Puf, 1970.

5. Solutions

1.1 1) On utilise l'algorithme d'Euclide. Conformément à cet algorithme, on obtient le tableau suivant

	33	1	1	2	
17640	525	315	210	105	0
1	0	1	-1	2	
0	1	-33	34	-67	

Il en résulte que 105 est le pgcd de 17640 et 525. On en déduit par ailleurs la relation de Bezout $2\times 17640-67\times 525=105$. Notons que pour déterminer le pgcd de ces deux entiers, on peut aussi expliciter leurs factorisations en produit de nombres premiers. On trouve $17640=2^3.3^2.5.7^2$ et $525=3.5^2.7$, d'où $d=3.5.7=105$.

2) Puisque d divise a et b, l'entier 2^d-1 divise 2^a-1 et 2^b-1. Considérons alors un diviseur commun c à 2^a-1 et 2^b-1. Il s'agit de vérifier que c divise 2^d-1. On remarque pour cela qu'il existe deux entiers u et v tels que l'on ait $d=au+bv$ (théorème de Bézout). Dans le groupe $\left(\mathbb{Z}/c\mathbb{Z}\right)^*$, on a les égalités $\overline{2}^{au}=\overline{1}$ et $\overline{2}^{bv}=\overline{1}$, d'où $\overline{2}^{d}=\overline{2}^{au+bv}=\overline{1}$, ce qui établit l'assertion. Cet exercice se généralise en remplaçant 2 par n'importe quel entier $n\geq 2$.

On peut aussi utiliser l'algorithme d'Euclide. En effet, il existe q et r dans $\mathbb{N}$ tels que l'on ait $a=bq+r$ avec $0\leq r<b$. On a les égalités

$$2^a-1=(2^b)^q2^r-1=\big((2^b)^q-1\big)2^r+(2^r-1).$$

Par ailleurs, 2^b-1 divise $(2^b)^q-1$. Il existe donc $t\in\mathbb{N}$ tel que l'on ait

$$2^a-1=(2^b-1)t+2^r-1.$$

On a $0\leq 2^r-1<2^b-1$ donc 2^r-1 est le reste de la division euclidienne de 2^a-1 par 2^b-1. L'entier d étant le dernier reste non nul dans l'algorithme d'Euclide de division de a par b, il en résulte que 2^d-1 est le dernier reste non nul dans l'algorithme d'Euclide de division de 2^a-1 par 2^b-1, d'où l'assertion.

3) On détermine une solution particulière en utilisant l'algorithme d'Euclide. On obtient le tableau suivant :

	2	2	1	3	
111	47	17	13	4	1
1	0	1	-2	3	-11
0	1	-2	5	-7	26

On en déduit l'égalité $26\times 47-11\times 111=1$. L'ensemble des solutions est donc formé des couples $(26+111k,-11-47k)$ où $k\in\mathbb{Z}$.

1.2 Le but est de faire des combinaisons pour faire descendre le degré ; concrètement appelons $\delta(n)$ ce pgcd. On a $n^3+n^2+1=(n^2+2n-1)(n-1)-(n+1)$ de sorte que $\delta(n)=(n^2+2n-1,n+1)$. De même $n^2+2n-1=(n+1)^2-2$ et donc $\delta(n)=(n+1,2)$ soit $\delta(n)=2$ si $n\equiv 1 \mod 2$ et $\delta(n)=1$ si $n\equiv 0 \mod 2$.

1.3 (a) On remarque tout d'abord que $650=2.325$ et $66=2.33$. On va appliquer l'algorithme d'Euclide à 325 et 33 puis on multipliera par deux, ce qui nous permet de gagner quelques lignes de calculs (on n'est pas un ordinateur...)

$$\begin{aligned}325&=33.9+28\\33&=28+5\\28&=5.5+3\\5&=3+2\\3&=2+1\end{aligned}$$

On remonte alors les calculs :

$$\begin{aligned}
1 &= 3-2 \\
1 &= 3-(5-3) = 2.3-5 \\
1 &= 2.(28-5.5)-5 = 2.28-11.5 \\
1 &= 2.28-11.(33-28) = 13.28-11.33 \\
1 &= 13.(325-9.33)-11.33 = 13.325-128.33
\end{aligned}$$

Finalement la relation de Bezout est $2 = 13.650 - 128.66$, c'est la plus "simple" ; on rappelle que les autres sont données par

$$2 = (13 + k.66)650 - (128 - k.650)66$$

pour $k \in \mathbb{Z}$.

(b) (i) D'après la relation de Bezout, il existe $u, v \in \mathbb{Z}$ tels que $1 = ua + vb$, i.e. si on nous rend la monnaie (u ou v est forcément négatif), pouvant payer la somme 1, on peut payer n'importe quelle somme entière.

(ii) On écrit $m = ax + by$ et $n = au + bv$ de la façon la plus simple possible, i.e. $0 \leq x, u \leq b-1$, de sorte que l'écriture est unique ; en effet on rappelle que $m = a(x - bt) + b(y + at)$, de sorte qu'il existe un unique t tel que $0 \leq x - bt < b$. L'égalité $m + n = ab - a - b$ donne alors $ab = a(x+u+1) + b(v+y+1)$: a et b étant premier entre eux, "le" théorème de Gauss nous dit que b divise $x + u + 1$. Or on a $1 \leq x + u + 1 \leq 2b - 1$, le seul multiple de b dans cet intervalle est b lui-même, soit $x + u + 1 = b$ et donc $v + y + 1 = 0$. Les nombres y et v étant des entiers, exactement un parmi eux deux est positif ou nul, l'autre étant strictement négatif. En language clair exactement une somme parmi m et n est payable sans rendu de monnaie. En remarquant que 0 est payable, alors $ab - a - b$ n'est pas payable. De même une somme négative n'est pas payable de sorte que si $m > ab - a - b$, la somme m est payable.

(c) On écrit $48x + 20y + 15z = 3(16x + 5z) + 20y$. D'après ce qui précède tout nombre de la forme $60 + t$ avec $t \geq 0$ peut s'écrire sous la forme $16x + 5Z$. De même tout nombre de la forme $38 + s$ avec $s \geq 0$, peut s'écrire sous la forme $3t + 20y$. Finalement toute somme supérieure ou égale à 218 est payable. Étudions le cas de 217 : $217 = 20y + 3u$, $217 \equiv -3 \mod 20$, on en déduit que $-3(u + 1)$ doit être divisible par 20, soit $u = 20k - 1$ et $220 = 20(y + 3k)$ soit $11 = y + 3k$ ce qui donne $u = 19, 39, 59$ et on vérifie aisément qu'aucune de ses possibilités ne s'écrit sous la forme $16x + 5z$ avec x, y positifs.

(d) Soit $n > 2abc - bc - ac - ab$. D'après le théorème de Bezout, il existe $0 \leq x < a$ avec $n \equiv x \mod xbc \mod a$; soit $y' \in \mathbb{Z}$ tel que $n = xbc + y'a$ de sorte que

$$y'a = n - xbc > 2abc - bc - ac - ab - (a-1)bc = (bc - b - c)a$$

et donc $y' > bc - b - c$. D'après (b), il existe $y, z \geq 0$ tel que $y' = zb + yc$ et donc $n = xbc + yac + zab$.

Supposons par l'absurde que $2abc - bc - ac - ab = xbc + yac + zab$ avec $x, y, z \geq 0$; on aurait alors $a|(x+1)bc$ et donc $a|x + 1$ d'après le lemme de Gauss, soit $x \geq a - 1$. De même on aurait $y \geq b - 1$ et $z \geq c - 1$ si bien que

$$xbc + yac + zbc \geq 3abc - bc - ac - ab > 2abc - bc - ac - ab$$

ce qui n'est pas.

(e) D'après ce qui précède la propriété est vraie pour $n = 2, 3$; on la suppose vraie jusqu'au rang $n - 1$ et prouvons la au rang n. Soit $k > M = a_1 \cdots a_n \Big(n - 1 - \sum_{i=1}^n \frac{1}{a_i}\Big)$; comme a_n est premier avec $a_1 \cdots a_{n-1}$, d'après le théorème de Bezout, il existe $0 \leq x_n < a_n$ tel que $k \equiv x_n a_1 \cdots a_{n-1} \mod a_n$; notons $q_n = (k - x_n a_1 \cdots a_{n-1})/a_n$ de sorte que

$$N > \frac{a_1 \cdots a_n \Big(n - 1 - \sum_{i=1}^n \frac{1}{a_i}\Big) - (a_n - 1)a_1 \cdots a_{n-1}}{a_n} = a_1 \cdots a_{n-1}\Big(n - 2 - \sum_{i=1}^{n-1} \frac{1}{a_i}\Big).$$

D'après l'hypothèse de récurrence $N = \sum_{i=1}^{n-1} \prod_{j \neq i} a_j$ avec $x_i \geq 0$ pour tout $i = 1, \cdots, n-1$ et donc $k = \sum_{i=1}^n x_i \prod_{j \neq i} a_j$.

Supposons désormais que $M=\sum_{i=1}^n x_i\prod_{j\neq i}a_j$ avec $x_i\geq 0$ pour tout $i=1,\cdots,n$. Alors comme dans (d), le lemme de Gauss donne que $a_i|(x_i+1)$ et donc $x_i\geq a_i-1$ et finalement que

$$M\geq \sum_{i=1}^n(a_i-1)\prod_{j\neq i}a_j > a_1\cdots a_n\Big(n-1\sum_{i=1}^n\frac{1}{a_i}\Big)=M$$

d'où la contradiction.

1.4 Le nombre cherché est le coefficient de z^n dans le développement en séries entières de la fraction rationnelle

$$\frac{1}{(1-z)(1-z^2)(1-z^3)}=\Big(\sum_{k=0}^\infty z^k\Big)\Big(\sum_{k=0}^\infty z^{2k}\Big)\Big(\sum_{k=0}^\infty z^{3k}\Big)=\sum_{n=0}^\infty a_nz^n.$$

On décompose alors cette fraction rationnelle en éléments simples ce qui donne :

$$\frac{1}{6(1-z)^3}+\frac{1}{4(1-z)^2}+\frac{17}{72(1-z)}+\frac{1}{8(1+z)}+\frac{1}{9(1-jz)}+\frac{1}{9(1-j^2z)}$$
$$=\sum_{n=0}^\infty\Big(\frac{(n+3)^2}{12}-\frac{7}{72}+\frac{(-1)^n}{8}+\frac{2}{9}\cos\frac{2n\pi}{3}\Big)z^n$$

où on a posé $j=e^{2i\pi/3}$. Le résultat découle alors de la majoration évidente suivante :

$$\Big|-\frac{7}{72}+\frac{(-1)^n}{8}+\frac{2}{9}\cos\frac{2n\pi}{3}\Big|\leq\frac{32}{72}<\frac{1}{2}.$$

1.5 Le nombre de solutions est égal au coefficient de z^n dans le développement en séries entières de la fraction rationnelle

$$\frac{1}{(1-z)(1-z^2)}+\frac{z}{(1-z^2)(1-z^3)}+\frac{z^2}{(1-z^3)(1-z^4)}+\cdots+\frac{z^k}{(1-z^{k+1})(1-z^{k+2})}+\cdots=$$
$$\frac{1}{z(1-z)}\sum_{k=0}^\infty\Big(\frac{1}{1-z^{k+1}}-\frac{1}{1-z^{k+2}}=\frac{1}{z(1-z)}\Big(\frac{1}{1-z}-1\Big)=\sum_{n=0}^\infty(n+1)z^n.$$

1.6 (1) De l'égalité

$$\sum_{n=0}^\infty A_nz^n=\frac{1}{(1-z^{a_1})\cdots(1-z^{a_l})}=\frac{1}{a_1\cdots a_l}\frac{1}{(1-z)^l}+F(z)$$

où $F(z)$ se décompose comme une somme de termes de la forme $\lambda\frac{1}{(1-\omega z)^k}$ où $\lambda\in\mathbb{Q}$, ω est une racine $a_1\cdots a_l$-ème de l'unité distincte de 1 et, comme $a_1,\cdots,a_l$ n'ont pas de facteurs communs, $k\leq l-1$. Le résultat découle alors de l'écriture

$$\frac{(k-1)!}{(1-\omega z)^k}=\sum_{n=0}^\infty(n+k-1)\cdots(n+1)z^n.$$

(2) Comme les a_i sont premiers entre eux deux à deux, on peut écrire $\prod_{i=1}^l(1-z^{a_i})$ sous la forme $(1-z)^lQ(z)$ où $Q(z)$ divise $1-z^{a_1\cdots a_l}$. En décomposant en éléments simples le pôle 1, on obtient une égalité du genre

$$\frac{1}{(1-z^{a_1})\cdots(1-z^{a_l})}=R\Big(\frac{1}{1-z}\Big)+\frac{S(z)}{1-z^{a_1\cdots a_l}}$$

où $R(z)$ et $S(z)$ sont des polynômes de degré respectivement égal à l et plus petit que $a_1\cdots a_l$. Le résultat découle alors de l'écriture

$$R\Big(\frac{1}{1-z}\Big)=\sum_{n=0}^\infty P(n)z^n,\qquad \frac{S(z)}{1-z^{a_1\cdots a_l}}=\sum_{n=0}^\infty Q_nz^n.$$

(3) Soient pour $n<ab$, $ax'+by'=n$ et $ax"+by"=n$; on a donc $0\leq x',x"<b$ et comme l'égalité $a(x'-x")=-b(y'-y")$ avec $a\wedge b=1$, $-b<x'-x"<b$ est divisible par b et donc nul. En résumé on a $A_n<2$. Pour $n=ab$, le même raisonnement donne $A_{ab}\leq 2$ et comme $ab+b.0=ab=a.0+ba$ on a bien $A_{ab}=2$.

Comme $a \wedge b = 1$,

$$T(z) = \frac{(1-z^{ab})(1-z)}{(1-z^a)(1-z^b)} = \Phi_1(z) \prod_{\substack{1\neq d_1|a\\ 1\neq d_2|b}} \Phi_{d_1 d_2}(z)$$

est un polynôme de la forme $z^{ab-a-b+1} + \cdots + 1$ avec $T(1) = \frac{ab}{ab} = 1$. On en déduit alors que

$$\frac{T(z)-T(1)}{1-z} = -z^{ab-a-b} + \cdots$$

est aussi un polynôme. On a alors

$$\begin{aligned} \textstyle\sum_{n=0}^{\infty}(A_n - A_{n-ab})z^n &= (1-z^{ab}) \textstyle\sum_{n=0}^{\infty} A_n z^n \\ &= \tfrac{T(z)}{1-z} \\ &= \tfrac{T(z)-T(1)}{1-z} + \tfrac{1}{1-z} \\ &= \cdots - z^{ab-a-b} + \textstyle\sum_{n=0}^{\infty} z^n \end{aligned}$$

et donc $A_{ab-a-b} = 0$ et $A_n = A_{n-ab} + 1$ pour tout $n > ab - a - b$. Ainsi on a

$$A_n = A_{n - \lfloor \frac{n}{ab} \rfloor ab} + \lfloor \frac{n}{ab} \rfloor$$

et comme $n - \lfloor \frac{n}{ab} \rfloor ab < n - (\frac{n}{ab} - 1)ab = ab$, on en déduit que, comme $A_{n-\lfloor \frac{n}{ab} \rfloor ab} = 0$ ou 1 que A_n est égal à $\lfloor \frac{n}{ab} \rfloor$ ou $\lfloor \frac{n}{ab} \rfloor + 1$.

2.7 1) Posons $a = (1035125)^{5642}$. On a $1035125 \equiv 12 \mod 17$. D'après le petit théorème de Fermat, on a $12^{16} \equiv 1 \mod 17$. Par ailleurs, on a $5642 \equiv 10 \mod 16$. On en déduit que l'on a les congruences $a \equiv 12^{5642} \equiv 12^{10} \mod 17$. On a $12 \equiv -5 \mod 17$, $12^2 \equiv 8 \mod 17$, $12^4 \equiv -4 \mod 17$, $12^8 \equiv -1 \mod 17$, d'où $a \equiv 9 \mod 17$.

2) En utilisant l'égalité, $2 \times 19 - 37 = 1$, on constate que l'entier

$$k = 2 \times (19 \times 2) + 9 \times (-37) = -257$$

est congru à 2 modulo 37 et à 9 modulo 19. L'ensemble des solutions cherché est donc formé des entiers congrus à -257 modulo 703 (on a $703 = 19 \times 37$).

3) Il s'agit de vérifier que 429 et 700 sont premiers entre eux et de trouver deux entiers u et v tels que $429u + 700v = 1$. L'algorithme d'Euclide fournit le tableau suivant :

	1	1	1	1	2	1	1	
700	429	271	158	113	45	23	22	1
1	0	1	−1	2	−3	8	−11	19
0	1	−1	2	−3	5	−13	18	−31

On en déduit que $u = -31$ et $v = 19$ conviennent, de sorte que l'inverse multiplicatif modulo 700 de 429 est -31.

4) Soit n un entier impair. On a $2^{n-1} \equiv 1 \mod 3$, donc $2^n - 2 = 2(2^{n-1} - 1)$ est divisible par 6, i.e. il existe $k \in \mathbb{N}$ tel que $2^n = 6k + 2$. On a ainsi

$$2^{2^n} + 3 = 2^{6k+2} + 3 \equiv 0 \mod 7.$$

Pour tout entier $k \geq 0$, vérifions que 19 divise $2^{2^{6k+2}} + 3$. On remarque pour cela que l'on a $2^{6k} \equiv 1 \mod 9$, d'où $2^{6k+2} \equiv 4 \mod 9$ puis $2^{6k+2} \equiv 4 \mod 18$. D'après le petit théorème de Fermat, on a $2^{18} \equiv 1 \mod 19$. Il en résulte que l'on a $2^{2^{6k+2}} \equiv 2^4 \mod 19$, ce qui entraîne l'assertion.

2.8 Notons pour tout entier e, A_e (resp. B_e) l'ensemble des éléments de $(\mathbb{Z}/n\mathbb{Z})^2$ d'ordre e (resp. d'ordre divisant e) et soit a_e (resp. b_e) son cardinal. Un élément (x, y) appartient à A_e si et seulement si x et y sont d'ordre divisant e dans $\mathbb{Z}/n\mathbb{Z}$, de sorte que pour tout e, $b_e = (e \wedge n)^2$. Par ailleurs B_d est la réunion disjointe de $A_d \coprod A_p \coprod A_q \coprod A_1$, où A_1 est réduit à l'élément nul. De même B_p (resp. B_q) est la réunion disjointe de $A_p \coprod A_1$ (resp. $A_q \coprod A_1$). En prenant les cardinaux, on obtient alors :

– $b_d = (n \wedge d)^2 = a_d + a_p + a_q + 1$,

– $b_p = (n \wedge p)^2 = a_p + 1$ et $b_q = (n \wedge q)^2 = a_q + 1$;

soit $a_d = (n \wedge (pq))^2 - (n \wedge p)^2 - (n \wedge q)^2 + 1$.

2.9 Supposons qu'il existe un entier $n \geq 2$ tel que n divise $2^n - 1$. Soient p le plus petit diviseur premier de n et d l'ordre de 2 dans $(\mathbb{Z}/p\mathbb{Z})^*$. Par hypothèse, on a $2^n \equiv 1 \mod p$. Puisque p est impair, on a $2^{p-1} \equiv 1 \mod p$. Ainsi d divise n et $p-1$. D'après le caractère minimal de p, on déduit que $d = 1$, d'où $2 \equiv 1 \mod p$ et une contradiction.

2.10 Supposons qu'il existe un entier $n \geq 3$ impair qui divise $3^n + 1$. Soit p le plus petit diviseur premier de n. On a $p \geq 5$ (car 3 ne divise pas $3^n + 1$). On a les congruences

$$(1) \qquad 3^{p-1} \equiv 1 \mod p \quad \text{(petit th. de Fermat)} \quad \text{et} \quad 3^{2n} \equiv 1 \mod p.$$

Soit d l'ordre de la classe de 3 dans le groupe multiplicatif $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$. On déduit de (1) que d divise $p-1$ et $2n$. On est amené à distinguer deux cas. Supposons d impair. D'après le lemme de Gauss, d divise alors n. L'inégalité $d < p$ et le caractère minimal de p entraînent alors $d = 1$. Par suite, on a $3^d = 3 \equiv 1 \mod p$, d'où $p = 2$ et une contradiction. Supposons d pair et posons $d = 2k$ où $k \in \mathbb{Z}$. L'entier k divise n. Les inégalités $k < d < p$ impliquent $k = 1$, d'où $d = 2$ puis $3^2 \equiv 1 \mod p$. Cela conduit à $p = 2$ et de nouveau à une contradiction.

2.11 Puisque n est impair, on a $2^{\varphi(n)} \equiv 1 \mod n$, où $\varphi(n)$ est l'indicateur d'Euler de n. Par ailleurs, on a $\varphi(n) \leq n$, de sorte que $\varphi(n)$ divise $n!$. On en déduit que $2^{\varphi(n)} - 1$ divise $2^{n!} - 1$: si a et b sont des entiers naturels tels que a divise b, alors $2^a - 1$ divise $2^b - 1$. Cela entraîne l'assertion.

2.12 Essayons de factoriser $P(x) = (x+1)^7 - x^7 - 1$ en regardant ses racines : on remarque qu'outre 0 et 1, le nombre complexe $j = e^{2i\pi/3}$ est aussi racine car $j + 1 = -j^2$ de sorte que $P(x)$ est divisible par $x(x+1)(x^2+x+1)$ le quotient étant égal à $x^2 + x + 1$ et donc

$$(a+b)^7 - a^7 - b^7 = 7ab(a+b)(a^2 + ab + b^2)^2.$$

On est ainsi amené à résoudre $a^2 + ab + b^2 \equiv 0 \mod 7^3$ qui s'écrit encore

$$(a + \frac{b}{2})^2 \equiv -3(\frac{b}{2})^2 \mod 7^3$$

laquelle possède des solutions si et seulement si le symbole de Legendre $(\frac{-3}{7^3}) = 1$ ce que l'on vérifie aisément en utilisant la loi de réciprocité quadratique.

2.13 Raisonnons par l'absurde et supposons qu'il existe $\sqrt{n/3} \leq l \leq n-2$ tel que $l^2 + l + n$ ne soit pas premier ; on prend l minimal. Soit alors q le plus petit diviseur premier de $l^2 + l + n$; on a $q \leq 2l$ car sinon on aurait $(2l+1)^2 \leq q^2 \leq l^2 + l + n$ et donc $l \leq \sqrt{n/3}$. On écrit alors q sous la forme $l - k$ ou $l + k + 1$ avec $0 \leq k \leq l - 1$; de la factorisation

$$(l^2 + l + n) - (k^2 + k + n) = (l - k)(l + k + 1)$$

on en déduit que q divise $k^2 + k + n$ lequel par minimalité de l est premier soit $q = k^2 + k + n$. La relation $q^2 \leq l^2 + l + n$ implique

$$(k^2 + k + n)^2 \leq (n-2)^2 + (n-2) + n < n^2$$

ce qui est absurde.

2.14 Il s'agit de vérifier que pour tout $x, y \in \mathcal{E}$, le nombre $\frac{x+y}{2}$ n'appartient pas à $\mathcal{E}$. Dans le cas contraire $x + y$ ne s'écrirait qu'avec des 0 et des 2 en base trois ce qui n'est le cas que si $x = y$, d'où le résultat.

Comme $2^11 = 2048$ et que $\sum_{i=0}^{10} 3^i = 88573$, l'exercice suggéré par la remarque aura une réponse positive jusqu'en 2048.

2.15 Si x est pair, on a $y^2 \equiv -1 \mod 8$. En écrivant y impair sous la forme $2k+1$, on obtient $y^2 = 1 + 4k(k+1) \equiv 1 \mod 8$ contradiction. On a $x^3 + 8 = (x+2)(x^2 - 2x + 4)$ avec x impair de la forme $2k+1$; $(x^2 - 2x + 4) = 4k^2 + 3$. On en déduit donc qu'il existe un p premier divisant $x^2 - 2x + 4$ avec $p \equiv 3 \mod 4$. Or si p premier divise $y^2 + 1$ alors $p \equiv 1 \mod 4$, d'où la contradiction.

3.16 1) Le seul nombre premier vérifiant la condition de l'énoncé est 3. En effet, soit p un nombre premier tel que $p+2$ et $p+4$ soient premiers. Si l'on a $p \equiv 1 \mod 3$, (resp. $p \equiv 2 \mod 3$), alors $p+2$ (resp. $p+4$) est divisible par 3. Les entiers $p+2$ et $p+4$ étant distincts de 3, on a donc $p \equiv 0 \mod 3$, puis $p = 3$. Par ailleurs, 5 et 7 sont premiers.

2) Il n'y a que $p = 3$. En effet, soit p un nombre premier divisant $2^p + 1$. D'après le petit théorème de Fermat, p divise $2^p - 2$, d'où $p = 3$.

3) Les entiers n de la forme $(p-1)(1+kp)$, où k est un entier naturel, conviennent. En effet, pour un tel entier n, on a $n \equiv -1 \mod p$. Par ailleurs, $p - 1$ divise n et l'on a $2^{p-1} \equiv 1 \mod p$, donc on a $2^n \equiv 1 \mod p$. Il en résulte que $n2^n + 1 \equiv 0 \mod p$, d'où le résultat.

3.17 Soit $P(X) = a_nX^n + \cdots + a_0$ de sorte qu'en particulier $a_0 \in \mathcal{P}$. Comme $P(n)$ tends vers l'infini quand n tends vers l'infini, il existe une valeur n_0 à partir de laquelle $P(n) > a_0$. Ainsi pour k assez grand, on a $P(ka_0) > a_0$ alors que $P(ka_0)$ est divisible par a_0.

3.18

3.19 Le principe est très élémentaire : si $n+2$ est un multiple de p alors $(n+2)/p$ est un entier q et donc $(n+1)/p = q - 1/p$ et donc $\lfloor \frac{n+2}{p} - \lfloor \frac{n+1}{p} \rfloor$ est égal à 1 alors qu'il est nul si p n'est pas un diviseur. Autrement dit la somme compte le nombre de diviseurs de $n+2$ compris entre 2 et $n+1$; ainsi si $n+2$ est premier on obtient $t(n) = n+2$ qui est premier alors que si $n+2$ n'est pas premier on a $t(n) = 2$. Ainsi la formule ne donne que des nombres premiers mais très lentement, 2 apparaissant très souvent.

Remarque : en utilisant la formule de Wilson, Minac simplifie la formule précédente :

$$t(n) = 2 + n\lfloor \frac{(n+1)!+1}{n+2} - \rfloor \frac{(n+1)!}{n+2} \rfloor \rfloor$$

laquelle contient moins de symbole et plus de somme, mais requiert de lourds calculs de factoriels.

En 1995 Minac et Willans ont imaginé une formule, avec plus de 52 symboles, donnant tous les nombres premiers dans l'ordre et sans répétition :

$$\pi(m) = \sum_{j=2}^{m} \frac{\sin^2\Big(\frac{\pi}{j}(j-1)!^2\Big)}{\sin^2(\frac{\pi}{j})} = \sum_{j=2}^{m} \lfloor \frac{(j-1)!+1}{j} - \lfloor \frac{(j-1)!}{j} \rfloor \rfloor$$

alors le n-ème nombre premier p_n est donné par

$$p_n = 1 + \sum_{m=1}^{2^n} \lfloor \lfloor \frac{n}{1+\pi(m)} \rfloor^{1/n} \rfloor.$$

En 2000, Ruiz a donné la formule suivante :

$$p_n = 1 + \sum_{k=1}^{2(\lfloor n \ln n \rfloor + 1)} \Big(1 - \lfloor \frac{\psi(k)}{n} \rfloor\Big)$$

où $\psi(k) = k - 1 + \sum_{j=2}^{k} \lfloor \frac{2}{j} \Big(1 + \sum_{s=1}^{\lfloor \sqrt{j} \rfloor} \big(\lfloor \frac{j-1}{s} \rfloor - \lfloor \frac{j}{s} \rfloor\big)\Big) \rfloor$.

Remarque : signalons aussi la suite de Perrin définie par

$$u_0 = 3, \; u_1 = 0, \; u_2 = 2 \qquad u_{n+1} = u_{n-1} + u_{n-2}.$$

Lucas a montré que pour p premier p divise u_p et on conjecture que la réciproque est vraie.

3.20 L'écriture s'obtient en effectuant la division euclidienne par p, puis en multipliant le reste par 10 et en effectuant la division euclidienne par p... Ainsi en notant r_k les restes et q_k les quotients qui sont donc les chiffres du développement décimal de $\frac{1}{p}$, on a :

$$\begin{aligned} &r_0 = 1 \\ &r_1 = 10r_0 - q_1 p \\ &\vdots \\ &r_k = 10r_{k-1} - q_k p. \end{aligned}$$

On a donc $r_k \equiv 10^k \mod p$ et si on note k_0 l'indice à partir duquel le développement est périodique de période T, on a $q_{k_0+T} = q_k$ avec $r_{k_0+T} = r_k$ et donc $10^{k_0+T} \equiv 10^{k_0} \mod p$ soit $10^T \equiv 1 \mod p$. On en déduit que $r_0 = r_T$ et donc $q_1 = q_{T+1}$, i.e. le développement est périodique dès le premier chiffre après la virgule. Notons alors $d|T$ l'ordre de 10 modulo p ; comme précédemment on a $r_{k+d} = r_k$ pour tout $k > 0$ et donc $q_{k+d} = q_k$ et donc $T|d$ d'où le résultat.

Exemples $\frac{1}{13} = 0,076923\cdots$ et 10 est d'ordre 6 dans $(\mathbb{Z}/13\mathbb{Z})^\times$.

Remarque : le même raisonnement s'applique pour les $\frac{k}{p}$ avec $1 \leq k \leq p-1$.

3.21 On a l'égalité

$$\frac{1}{p} = \sum_{i=1}^{+\infty} n10^{-iT} = \frac{10^{-T}n}{1-10^{-T}} = \frac{n}{10^T - 1}$$

et donc $np = 10^T - 1$.
Remarque : pour retrouver l'entier n associé à $p = 7$, on peut partir de l'égalité $999999 = 7n$ soit classiquement par division $999999 = 7 \times 100000 + 299999$... soit au contraire en partant de droite : $999999 = 7 \times 7 + 999950$... C'est comme cela par exemple que l'on trouve aisément le $p-1$-ème chiffre du développement décimal de $1/p$.
Remarque : comme $10^{p-1} - 1$ s'écrit avec un nombre pair de 9, l'entier pn est divisible par 99 et donc pour $p \neq 3, 11$, n est divisible par 99 ainsi donc que la somme de ses paquets de 2 chiffres ($100 \equiv 1 \mod 99$). Si $3|p-1$ alors n est divisible par 999 ainsi donc que la somme de ses paquets de 3 chiffres ($1000 \equiv 1 \mod 999$). Dans le même genre d'idée, on a le résultat suivant.

3.22 On a $n = 10^e A + B$ avec $0 \leq A, B < 10^e - 1$ car $p > 1$. Ainsi on a

$$\frac{10^{2e}}{p} = 10^e A + B + \frac{1}{p} \Rightarrow \frac{10^e + 1}{p} \times (10^e - 1) = 10^e A + B$$

. Or comme $(10^e)^2 \equiv 1 \mod p$ et que $10^e \not\equiv 1 \mod p$, on en déduit que $10^e + 1 \equiv 0 \mod p$ de sorte que $A + B \equiv 0 \mod 10^e - 1$ et le résultat découle de l'encadrement $1 \leq A + B < 2(10^e - 1)$.
Remarque : dans le cas où T est divisible par r, le raisonnement précédent donne que la somme des paquets de T/r chiffres de n est de la forme $k(10^r - 1)$ avec $1 \leq k < r$.
Exemples $\frac{1}{19} = 0,052631578947368421\cdots$ et on a

$$052 + 631 + 578 + 947 + 368 + 421 = 3 \times 999 \quad 05 + 26 + 31 + 57 + 89 + 47 + 36 + 84 + 21 = 4 \times 99.$$

3.23 On reprend les notations de la proposition 3.20 : comme $T = p - 1$ on en déduit que $\{r_1, \cdots, r_{p-1}\} = \{1, \cdots, p-1\}$. En notant $1 \leq i_0 \leq p-1$ l'indice tel que $r_{i_0} = k$, on en déduit du calcul même du développement décimal que le i-ème chiffre b_i du développement décimal de k/p est égal à $i + i_0$, d'où le résultat.
Remarque : une autre façon d'énoncer le résultat précédent est de dire que le n_k du développement décimal de k/p s'obtient par permutation circulaire de n en utilisant, avec les notations de la proposition 3.20 le premier reste $r_i = k$. Dans le cas général où la période est égale à T un diviseur quelconque de $p-1$, les restes des divisions euclidiennes des k/p pour k décrivant $\{1, \cdots, p-1\}$ se répartissent en $(p-1)/T$ sous-ensembles de sorte que les kn pour k décrivant $\{1, \ldots, p-1\}$, à permutations circulaires près, sont en nombre $(p-1)/T$.

3.24 On écrit $A = \sum_{i=1}^{(p-1)/2} a_i 10^{(p-1)/2-i}$ et $B = \sum_{i=1}^{(p-1)/2} a_{(p-1)/2+i} 10^{(p-1)/2-i}$ de sorte que d'après 3.22 soit $A = B$ soit $A + B = 9\cdots9$. Dans le premier cas comme $a_1 = 0$, on en déduit que $a_{(p+1)/2} = 0$ et dans le deuxième on obtient 9. Il faut alors décider si $(p-1)/2$ est un multiple d'une période, i.e. si $10^{(p-1)/2} \equiv 1 \mod 2$ ce qui est équivalent à $(\frac{10}{p}) = 1$ d'où le résultat.
Remarque : d'après la loi de réciprocité quadratique, le résultat ne dépend que de la congruence de p modulo 40. Dans le même ordre d'idée, on peut facilement déterminer le $(p-1)/2$-chiffres du développement décimal de $1/p$: en effet si $(p-1)/2$ est le multiple d'une période alors ce chiffre est le même que le $p-1$-ème que l'on détermine facilement comme expliqué ci-avant. Dans le cas où $(p-1)/2$ n'est pas une période comme avec les notations ci-dessus, $A + B = 9\cdots9$, on en déduit que le chiffre cherché est égal à 9 moins le $(p-1)$-ème chiffre.

Notons alors $\mathcal{P}(10)$ l'ensemble des premiers p tels que leur développement décimal est de période $p-1$: cet ensemble est-il infini et si oui quel est sa densité

$$d_{10}(x) = \frac{\sharp\{p \in \mathcal{P}(10),\ p \leq x\}}{\sharp\{p \in \mathcal{P},\ p \leq x\}}, \qquad \lim_{x \to +\infty} d_{10}(x).$$

On conjecture que cette limite est égale à

$$C_{Artin} = \prod_{p \in \mathcal{P}} \Big(1 - \frac{1}{p(p-1)}\Big) \simeq 0,3739558136\cdots$$

Le choix de la base 10 ne semble pas intervenir dans le résultat, on conjecture que le résultat doit être vrai pour tout choix d'entier a en lieu et place de 10.
Remarque : essayez de faire des simulations numériques de ces densités.

4.25 On raisonne par l'absurde; on prend (a, b) tel que $\max\{a, b\}$ soit minimal avec $\frac{a^2+b^2}{ab+1} = k$ qui n'est pas un carré parfait. Remarquons déjà que si $a = b$ alors $a = b = k = 1$ ne convient pas. Supposons donc $0 < a < b$ et écrivons l'égalité précédente sous la forme

$$b^2 - (ka)b + a^2 - k = 0$$

de sorte que b est une racine du polynôme $X^2-(ka)X+a^2-k$, lequel possède une deuxième racine b' telle que $b+b'=ka$ et donc $b'\in\mathbb{Z}$. Par ailleurs on a :

– $bb'=a^2-k$ et donc $b'=(a^2-k)/b<a$;
– $b'>0$: en effet si $b'<0$ alors $k=(a^2+(b')^2)/(ab'+1)<0$ ce qui n'est pas et si $b'=0$ alors $k=a^2$ ce qui n'est pas non plus.

En résumé le couple (a,b') avec $0<b'<a$ est plus petit que (a,b) vérifie les mêmes hypothèses ce qui contredit la minimalité de (a,b).

4.26 (1) Si $x\equiv y\equiv 0 \mod 2$ alors $z^2\equiv 2 \mod 4$ ce qui est impossible car 0 et 1 sont les seuls carré modulo 4.

(2) On a $(z-x^2)\wedge(z+x^2)=(z-x^2)\wedge 2z=(z-x^2)\wedge 2=2$. On a ainsi $z-x^2=2a^4$ et $z+x^2=2b^4$ avec $a\wedge b=1$; le résultat découle alors du fait que comme $2x^2\equiv 2 \mod 4$ exactement un parmi a et b est impair.

(3) On a $x^2=-a^4+4b^4$ ce qui n'est pas car sinon $1\equiv -1 \mod 4$.

(4) on a $z=a^4+4b^4$ et donc, comme $y=2ab\neq 0$, $0<a<z$; en éliminant z, on a aussi $4b^4=(a^2-x)(a^2+x)$ avec comme $a\wedge x=1$, $(a^2-x)\wedge(a^2+x)=2$. On en déduit comme précédemment $a^2-x=2c^4$ et $a^2+x=2d^4$ de sorte que $a^2=c^4+d^4$. En résumé à partir d'une solution (x,y,z) telle que $z>0$, on en a construit une autre (c,d,a) avec $0<a<z$ et $b=cd\neq 0$. La contradiction découle alors du fait qu'il n'est pas possible de construire une suite infinie d'entiers positifs strictement décroissante.

4.27 (1) On a $f(z)=2x+3y-i(x+2y)$ de sorte que F est affine avec $F(O)=O$ et de partie linéaire $\vec{F}=\begin{pmatrix}2&3\\1&2\end{pmatrix}$ de déterminant 1, de sorte qu'elle est inversible, conserve les volumes. Ce n'est pas une isométrie puisque ses vecteurs colonnes ne sont pas de norme 1.

Le déterminant étant égal à 1, son inverse est aussi à coefficients dans $\mathbb{Z}$ de sorte que $M\in\mathfrak{S}$ si et seulement si $F(M)\in\mathfrak{S}$. En ce qui concerne $\mathcal{H}$, on a $(2x+3y)^2-3(x+2y)^2=x^2-3y^2=1$.

(2) (i) On calcule $A_1=(2,1)$ et $A_2=(7,4)$. Par récurrence on montre que $A_n\in\mathcal{H}\cap\mathfrak{S}$ en utilisant (1 ii).

(ii) Un point $M(x,y)$ de l'arc $[A_0,A_1]$ de $\mathcal{H}$ est caractérisé par $x^2-3y^2=1$, $1\leq x\leq 2$ et $0\leq y\leq 1$. Si on veut $x,y\in\mathbb{Z}$, on a alors que deux possibilités qui donnent A_0 et A_1.

(3) (i) On se place dans le repère dont les axes sont les asymptotes de sorte que l'équation est $XY=a$. Il suffit alors d'imposer que A_0 soit de coordonnées $(1,1)$. Soient alors $M(a,b)$ et $M'(a',b')$. Supposons dans un premier temps $M\neq N$ et donc $a\neq a'$. La droite $D_{M,N}$ a alors pour équation $\frac{Y-1}{X-1}=\frac{b'-b}{a'-a}$. L'intersection avec $\mathcal{H}$ revient à prendre $Y=1/X$ avec $X\neq 0$ ce qui donne alors $X=aa'$.

Si $M=N$, la tangente en M à H a pour pente $-1/a^2$ ce qui donne $\frac{Y-1}{X-1}=-1/a^2$ et donc avec $XY=1$, $X=a^2$. Ainsi l'application $\phi:\mathcal{H}\to\mathbb{R}^\times$ qui à M associe l'abscisse de M dans le repère $\mathcal{R}$, induit un isomorphisme de $(\mathcal{H},*)$ avec $(\mathbb{R}^\times,\times)$.

Remarque : le résultat est valable pour toute hyperbole.

(ii) Si $M\neq A_1$ et $M'\neq A_0$, il s'agit de vérifier que (A_0M')et (MA_1) sont parallèles, ce qui revient à montrer que $\begin{vmatrix}2x+3y-1 & x-2\\ x+2y & y-1\end{vmatrix}=3y^2-x^2+1=0$. Si $M=A_1$, la tangente en A_1 a pour équation $2x-3y=1$ et a pour vecteur directeur $(3,2)$. Il suffit alors de vérifier que $\begin{vmatrix}7-1 & 3\\ 4 & 2\end{vmatrix}=0$. Si $M'=A_0$ alors M a pour coordonnées $(2,-1)$ et (A_1M) est parallèle à Oy donc à la tangente en A_0 à $\mathcal{H}$. Ainsi on a $A_n=A_1*\cdots*A_1$ et donc $X_n=X_1^n$.

(iii) A_n*A_n et $A_{n-1}*A_{n+1}$ sont sur $\mathcal{H}$ et ont même abscisse dans $\mathcal{R}$, ils coincident donc et la construction de $M*N$ donne le résultat. En ce qui concerne l'aire elle est égale à celle de $A_0A_1A_2$ et donc à $\frac{1}{2}\begin{vmatrix}2-1 & 7-1\\ 1 & 4\end{vmatrix}=1$.

(iv) L'arc $[A_n,A_{n+1}]$ de$\mathcal{H}$ est l'ensemble des points M de coordonnées $(X,1/X)$ avec $X_1^{n+1}\leq X\leq X_1^n$ (quitte à échanger les axes, on choisit le repère pour que $X_1<1$). L'application F se traduit par $X\mapsto X_1.X$ et induit donc la bijection de l'énoncé. En particulier d'après (2 ii), on en déduit que $\mathcal{H}\cap\mathfrak{S}$ est formé des A_n et de leurs symétriques par rapport à Ox, Oy et O.

(4) Les asymptotes de $\mathcal{H}$ ont pour vecteurs directeurs $\vec{u}'=\alpha(\sqrt{3}\vec{u}-\vec{v})$ et $\vec{v}'=\beta(\sqrt{3}\vec{u}+\vec{v})$. Pour que A_0 ait pour coordonnées (1,1 dans $\mathcal{R}$, on doit avoir $\vec{u}'+\vec{v}'=\vec{u}$ ce qui donne $\alpha=\beta=\frac{1}{2\sqrt{3}}$. On obtient alors $X_1=2-\sqrt{3}$ (et $Y_1=2+\sqrt{3}$). On en déduit alors $X_n=(2-\sqrt{3})^n$ et $Y_n=(2+\sqrt{3})^n$ et donc

$$|x|=\frac{(2+\sqrt{3})^n+(2-\sqrt{3})^n}{2}\qquad |y|=\frac{(2+\sqrt{3})^n-(2-\sqrt{3})^n}{2\sqrt{3}}.$$

4.28 On écrit l'équation diophantienne sous la forme
$$(\frac{x}{y}-\alpha_1)(\frac{x}{y}-\alpha_2)\cdots(\frac{x}{y}-\alpha_n)=\frac{m}{a_n y^n}.$$
Posons $A=\min_{1\leq i<j\leq n}|\alpha_i-\alpha_j|$. Si (x,y) avec $y\neq 0$ est une solution il existe alors au plus un α_i el que $|x/y-\alpha_i|<A/2$; α_i étant algébrique de degré n, d'après le théorème précédent on a
$$|\frac{x}{y}-\alpha_i|>\frac{C(\epsilon,\alpha_i)}{q^{n/2+1+\epsilon}}$$
et pour $j\neq i$, on a $|x/y-\alpha_j|\geq A/2$. On en déduit alors que
$$\frac{m}{|y|^n}>\frac{T}{|y|^{n/2+1+\epsilon}}$$
avec $T=C(\epsilon,\alpha_i)A^{n-1}/2^{n-1}$ et donc $m>T|y|^{n/2-1-\epsilon}$. On choisit alors ϵ tel que $n/2-1-\epsilon>0$ ce qui est possible puisque $n\geq 3$, de sorte que$|y|$ est bornée. Ainsi le nombre de y est fini, et pour un tel y fixé, il y a au plus n entiers x tels que (x,y) puissent être solutions, d'où le résultat.

4.29 (a) On raisonne comme dans l'exercice précédent ; soit $N(a+ib\sqrt{2})=a^2+2b^2$ la norme qui est une fonction multiplicative, et soit $z\in A^\times$; on a $zz'=1$ soit $N(z)N(z')=1$ et donc $N(z)=1$, soit $z=\pm 1$.
Pour montrer que A est euclidien, on remarque à nouveau que z_1/z_2 peut s'écrire sous la forme $q+e$ avec $q\in A$ et $e\in\mathbb{C}$ de norme strictement plus petite que 1. Ainsi on a $z_1=qz_2+r$, avec $r=z_1-qz_2\in A$ et $N(r)<N(z_2)$.

(b) Si x est pair, on a $y^2\equiv -2 \mod 8$, ce qui ne se peut pas, car les carrés dans $\mathbb{Z}/8\mathbb{Z}$, sont $0,1,4$. On factorise ensuite dans A : $x^3=(y+i\sqrt{2})(y-i\sqrt{2})$ et soit δ un pgcd de $y+i\sqrt{2}$ et $y-i\sqrt{2}$; on a $\delta=(y+i\sqrt{2},(i\sqrt{2})^3)$, or $i\sqrt{2}$ est irréductible car de norme 2, et la seule factorisation de 2 est 1×2, de sorte que $i\sqrt{2}=zz'$ implique que $N(z)=1$ soit z inversible (ou z'). Or $i\sqrt{2}$ ne divise pas y car sinon y^2 serait pair et donc y pair soit x pair, ce qui n'est pas ; ainsi $\delta=1$. On en déduit donc que $(y\pm i\sqrt{2})$ sont des cubes parfaits : $(y\pm i\sqrt{2})=(a\pm i\sqrt{2})^3$ et $x=a^2+2b^2$. En séparant partie réelle et imaginaire, on trouve alors $y=a^3-6ab^2$ et $1=b(3a^2-2b^2)$ soit $b=\epsilon=\pm 1=3a^2-2$, ce qui donne $b=1$ et $a=\pm 1$ soit $y=\pm 5$ et $x=3$ qui est bien une solution de l'équation.

(c) On a à nouveau $n\in S$ si et seulement si il existe $z\in A$ tel que $n=N(z)$. On étudie à nouveau les irréductibles de B ; p est irréductible si et seulement si $A/(p)$ est intègre, i.e. X^2+2 n'a pas de racine dans $\mathbb{Z}/p\mathbb{Z}$, i.e. si et seulement si -2 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$, i.e. si et seulement si $p\equiv 5,7 \mod 8$. En raisonnant comme dans l'exercice précédent, on trouve que les irréductibles de A, outre les premiers $p\equiv 5,7 \mod 8$, sont les $z\in A$ tels que $N(z)$ est premier. Toujours en suivant la même démarche, on trouve alors que $n\in S$ si et seulement si $v_p(n)$ est pair pour $p\equiv 5,7 \mod 8$.

(d) De la même façon, la détermination de S se fait via l'étude de $A=\mathbb{Z}[\sqrt{2}]$, dont la norme est a^2-2b^2, avec le morphisme de corps $c(a+b\sqrt{2})=a-\sqrt{2}b$ de sorte que N est multiplicative. Soit $z\in A^\times$, on a alors $N(z)=\pm 1$. A nouveau A est euclidien pour le stathme $|N|$. On remarque que -1 est une norme $-1=1^2-2\times 1^2=N(1+\sqrt{2})$. Si n est un diviseur de x^2-2y^2 avec x,y premiers entre eux, alors au signe près n est de la forme u^2-2v^2. En effet soit $x+\sqrt{2}y=\pi_1\cdots\pi_r$ une décomposition en produit d'irréductibles ; aucun des π_i n'appartient à $\mathbb{Z}$ car x et y sont premiers entre eux, de sorte que comme précédemment les $N(\pi_i)$ sont des premiers de $\mathbb{Z}$; on a alors $x^2-2y^2=N(\pi_1)\cdots N(\pi_r)$ et n au signe près, est un produit de certains de ces $N(\pi_i)$ et donc n est de la forme $N(z)=u^2-2v^2$.
L'égalité $-(u^2-2v^2)=N((1+\sqrt{2})(u+v\sqrt{2}))=(u+2v)^2-2(u+v)^2$ permet de négliger le signe $\pm$. Ainsi un premier impair p est de la forme x^2-2y^2 si et seulement si 2 est un carré modulo p ce qui est équivalent à $p\equiv\pm \mod 8$.

4.30 L'anneau des entiers de $K=\mathbb{Q}(i\sqrt{d})$ est $\mathcal{O}_K=\mathbb{Z}[i\sqrt{d}]$ dont les unités sont ± 1, cf. le cours. Soit alors (x,y) une solution de $y^2=x^3-d$. Comme $-d\not\equiv 1 \mod 4$, x ne peut pas être pair ; d étant sans facteurs carrés on a aussi $x\wedge d=1$. On écrit
$$x^3=(y+i\sqrt{d})(y-i\sqrt{d}).$$
S'il existait un idéal premier $\mathfrak{P}$ contenant $y\pm i\sqrt{d}$ alors $2i\sqrt{d}\in\mathfrak{P}$ avec $x\in\mathfrak{P}$ de sorte que $N(\mathfrak{P})|4d\wedge x^2=1$ ce qui n'est pas. Ainsi les idéaux $(y+i\sqrt{d})$ et $(y-i\sqrt{d})$ n'ont pas d'idéaux premiers communs dans leur décomposition en produit d'idéaux premiers de sorte qu'il existe un idéal $\mathfrak{A}$ de $\mathcal{O}_K$ tel que
$$(y+i\sqrt{d})=\mathfrak{A}^3,\quad (y-i\sqrt{d})=\bar{\mathfrak{A}}^3.$$

Or comme $3 \nmid h$, $\mathfrak{A}^3$ étant principal on en déduit que $\mathfrak{A}$ est principal de sorte qu'il existe $a, b \in \mathbb{Z}$ tels que
$$y + i\sqrt{d} = \pm(a + ib\sqrt{d})^3$$
ce qui donne $1 = \pm b(3a^2 - db^2)$ et $y = \pm a(a^2 - 3db^2)$. On en déduit alors $b = \pm 1$ et $d = 3a^2 \pm 1$ et donc le résultat.