Table des matières

1. Systèmes linéaires. 3

2. Polynômes. 5
I Équations polynomiales de degré deux. . . . 5
II Degré d'un polynôme. . . . 5
III Factorisation et racine. . . . 5
IV Méthodes pratiques de factorisation. . . . 6
1 Identification polynomiale. . . . 6
2 Règle de Ruffini. . . . 6
3 Division euclidienne polynomiale. . . . 8
V Théorème d'Alembert-Gauss. . . . 8
VI Exercices. . . . 8

3. Nombres complexes. 9
I Point de vue algébrique. . . . 9
1 Ensemble, addition, multiplication. . . . 9
2 Inverse et conjugué. . . . 10
3 Formule du binôme. . . . 13
4 Résoudre des équations linéaires (y compris avec conjugaison). 13
5 Racines dans $\mathbb{C}$ des polynômes de degré deux à coefficients réels. 14
II Point de vue géométrique. . . . 14
1 De $\mathbb{C}$ vers le plan d'Argand-Cauchy et réciproquement. . . . 14
III "Racine carrée" dans $\mathbb{C}$. . . . 15

4. Arithmétique. 17
I Diviseurs. . . . 17
II Division euclidienne et congruence. . . . 19
III Résoudre une congruence : $ax \equiv b\ [n]$. . . . 21
IV PGCD . . . 22
V Couples d'entiers premiers entre eux. . . . 23
VI Théorème de Bézout. . . . 23
VII Théorème de Gauss. . . . 25
VIII Nombres premiers. . . . 25
IX Théorème fondamental de l'arithmétique. . . . 26
X Petit théorème de Fermat. . . . 26

XI Déterminer les diviseurs d'un entier. 26
XII Déterminer le PGCD de deux entiers. 26
XIII Déterminer un inverse de a $[n]$ lorsque a et n sont premiers entre eux. 27
XIV Établir et utiliser des tests de divisibilité. 27
XV Étudier la primalité de certains nombres. 27
XVI Étudier des problèmes de chiffrements. 27
XVIIIRecherche de nombres premiers particuliers (Mersenne, Fermat). . . . 27

5. Théorie de graphes. **29**

1. Systèmes linéaires.

Résoudre des systèmes de deux ou trois équations avec autant d'inconnues. Méthode du pivot de Gauss avec système échelonné puis substitution.

Exercice 1. Exprimez a et b en fonction de x et y sachant que $\left\{ \begin{array}{rcrcl} 3x & - & 2y & = & a \\ -5x & + & 3y & = & b \end{array} \right.$

2. Polynômes.

I Équations polynomiales de degré deux.

II Degré d'un polynôme.

Définition 1. On appelle degré d'un monôme aX^n avec $(a,n) \in \mathbb{R}^* \times N$ l'entier n.

On appelle degré d'un polynôme non nul le plus haut degré de ses monômes non nuls dans sa forme développée, réduite et ordonnée.

Remarques.

1. Le degré du polynôme nul est, par convention $-\infty$.

Proposition 1.

contenu...

III Factorisation et racine.

Proposition 2. Soient $(z,a) \in \mathbb{C}^2$ et $n \in \mathbb{N}^*$. $z^n - a^n = (z-a)\sum_{k=0}^{n-1} z^{n-1-k}a^a$.

Démonstration. On part du membre de droit on développe, on remarque un télescopage et on conclue.

On peut également reconnaître la somme des termes d'une suite géométrique. C'est le résultat classique de première sur la somme des termes d'une suite géométrique vu en première qui se démontre grâce à un télescopage. Procédons par disjonction des cas : si $z = 0$ le résultat est trivial. Supposons $z \neq 0$ alors : $z^n - a^n = z^n\left(1 - \left(\frac{a}{z}\right)^n\right) = z^n\left(1 - \frac{a}{z}\right)\left(\sum_{k=0}^{n-1}\left(\frac{a}{z}\right)^k\right)$

Exemples.

1. $X^3 - 8 = X^3 - 2^3 = (X-2)(X^2+2X+4)$.

Remarques.

1. On a aussi ce résultat dans $\mathbb{R}$.
2. Ce résultat est une généralisation d'une identité remarquable : $a^2 - b^2$.

Proposition 3. Soit $P \in \mathbb{C}[X]$ et $a \in \mathbb{C}$. $P(a) = 0$ si et seulement si $Q \in \mathbb{C}[X]$ tel que $P(X) = (x-a)Q(x)$.

Exemples.

1. Démarche de preuve sur un cas particulier.

Démonstration.

* Démontrons la réciproque. Si $P(X) = (X-\alpha)Q(X)$ alors $P(\alpha) = (\alpha-\alpha)Q(\alpha) = 0$ donc α est racine de P.

* Démontrons l'implication directe. Supposons que $P(\alpha) = 0$. On peu supposer que P est de degré supérieur ou égale à 2 car sinon le résultat est trivial.

Soit $n \in \mathbb{N} \setminus \{0;1\}$ le degré de P. Il existe $a_n, \dots, a_1, a_0 \in \mathbb{C}$ tels que $P(X) = a_n X^n + \cdots + a_1 X + a_0$.

α étant racine de P :

$P(X) = P(X) - P(\alpha) = a_n X^n + \cdots + a_1 X + a_0 - (a_n \alpha^n + \cdots + a_1 \alpha + a_0) = a_n(X^n - \alpha^n) + \cdots + a_1(X - \alpha) = a_n(X - \alpha)(X^{n-1} + X^{n-2}\alpha + \cdots + X\alpha^{n-2} + \alpha^{n-1}) + \cdots + a_1(X - \alpha) = (X - \alpha)\left[a_n(X^{n-1} + X^{n-2}\alpha + \cdots + X\alpha^{n-2} + \alpha^{n-1}) + \cdots + a_1\right]$.

Remarques.

1. On a aussi ce résultat dans $\mathbb{R}$.
2. Ce résultat fait un lien directe entre factorisation polynomiale et racine.

IV Méthodes pratiques de factorisation.

1 Identification polynomiale.

Proposition 4. Un polynôme P est nul si et seulement si tous les coefficients de sa forme développée, réduite et ordonnée sont nuls.

Remarques.

1. Autrement dit deux polynômes sont égaux si et si ils ont, dans leur forme développée, réduite et ordonnée, des coefficients deux à deux égaux.
2. Ce résultat absolument fondamental sera ici utilisé pour factoriser des polynômes.

Exemples.

1. Si $x^3 + 3x^2 - x - 3 = (x + 1)(ax^2 + bx + c)$ alors, en développant on peu identifier les coefficients, $1 = a$, $3 = a + b$, $-1 = b + c$ et $-3 = c$.

Exercice 2. On considère l'équation $(E) : z^3 - (2 + i)z^2 + 2(1 + i)z - 2i = 0$.

1. Montrez que (E) admet une unique solution imaginaire pure et déterminez-la.
2. Montrez que, pour tout $z \in \mathbb{C}$, $z^3 - (2 + i)z^2 + 2(1 + i)z - 2i = (z - i)(z^2 - 2z + 2)$.
3. Déduisez-en les solutions dans $\mathbb{C}$ de l'équation (E).

2 Règle de Ruffini.

La méthode de Horner est une présentation de la formule de calcul polynomiale de façon à rendre le calcul d'image plus simple.

$P(X) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a2x^2 + a_1 x + a_0 = ((((xa_n + a_{n-1})x + a_{n-2})x + a_{n-3})\dots)$.

Pour calculer l'image de α par P on fait donc :

a_n	a_{n-1}	a_{n-2}	
$r_n = a_n$	$r_{n-1} = \alpha a_{n-1} + r_n$	$r_{n-2} = \alpha a_{n-1} + r_n$	

Ce procédé permet de limiter le nombre de multiplication.

Exemples.

1. Soit $P(x) = 5x^4 - 3X^2 + 6X - 15$. Calculons l'image de 4 par P :

5	-3	6	-15
5	$4 \times 5 - 3 = 17$	$4 \times 17 = 68$	$4 \times 68 - 15 = 257$

2. $P(x) = 4x^3 + 3x^2 - 2x + 5 = x(4x^2 + 3x - 2) + 5 = x(x(4x + 3) - 2) + 5$.

   Ainsi le calcul de l'image de 2 par P se fait en respectant les priorité opératoires : $P(2) = 2(2(4 \times 2 + 3) - 2) + 5 = 2(2(8 + 3) - 2) + 5 = 2(2(11) - 2) + 5 = 2(22 - 2) + 5 = 2(20) + 5 = 40 + 5 = 45$. Nous avons pu faire le calcul sans avoir à faire des calculs de puissances.

   On présente ce calcul de la façon suivante :

Coefficients de P	4	3	-2	5
Facteur 2	4	$2 \times 4 + 3 = 11$	$2 \times 11 - 2 = 20$	$2 \times 20 + 5 = 45$

   Remarquons : $(4X^2 + 11X + 20)(X - 2) + 45 = P(x)$. Autrement dit cet algorithme fournit aussi la division de P par $X - 2$.

Exercice 3. Si l'on calcule une image par la fonction polynomiale $f(x) = 4x^3 + 3x^2 - 5x + 7$, combien d'opérations faut-il effectuer ? Par exemple, le calcul $f(11) = 4 \times 11 \times 11 \times 11 + 3 \times 11 \times 11 - 5 \times 11 + 7$ nécessite 6 multiplications et 3 additions (ou soustractions) et donc un total de 9 opérations.

Soit $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ une fonction polynomiale de degré n.

1. Combien d'opérations sont nécessaires pour calculer une image par P en admettant que tous les coefficients a_i sont non nuls ?
2. On admet que l'écriture $P(x) = (((a_n x + a_{n-1})x + a_{n-2})\dots)x + a_0$ représente bien la fonction P. Cette présentation est celle de la méthode de Horner. Combien faut-il d'opérations pour calculer une image ?

Exercice 1.

1. Pour chaque monôme $a_k x^k$ il faut effectuer k produits. Pour additionner tous les monômes il faut faire n additions. On en déduit le nombre total d'opérations : $n + \sum_{k=0}^{n} k = n + \frac{n(n+1)}{2} = \frac{n(n+3)}{2}$.
2. On observe la succession, n fois, d'un produit puis une somme. Il faut donc $2n$ opérations.

Identification polynomiale entre $P(x) = a_n x^n + \cdots + a_0$ et $(x - \alpha)Q(X)$ avec $Q(X) = q_{n-1}x^{n-1} + q_0$.

$$\begin{aligned}(x - \alpha)Q(X) &= q_{n-1}x^n + \cdots + q_0 x - \alpha q_{n-1}x^{n-1} - \cdots - \alpha q_0 \\ &= q_{n-1}x^n + (q_{n-2} - \alpha q_{n-1})x^{n-1} + \cdots + (q_1 - \alpha q_2)x^2 + (q_0 - \alpha q_1)x - \alpha q_0\end{aligned}$$

Et par identification : $a_n = q_{n-1}$, $a_{n-1} = q_{n-2} - \alpha q_{n-1}$, $a_{n-2} = q_{n-3} - \alpha q_{n-2}$, ..., $a_2 = q_1 - \alpha q_1$ et $a_1 = q_0 - \alpha q_1$ et $a_0 = -\alpha q_0$. Ainsi, hormis pour le premier et le dernier : $a_k = q_{k-1} - \alpha q_k$. Autrement dit : $q_{k-1} = \alpha q_k + a_k$ et $q_{n-1} = a_{n-1}$.

Calcul progressif des termes de la suite sous forme d'un tableau :

a_n	a_{n-1}	a_{n-2}	$\dots$
$q_{n-1} = a_n$	$q_{n-2} = \alpha a_{n-1} + q_{n-1}$	$q_{n-3} = \alpha a_{n-2} + q_{n-1}$	$\dots$

Exemples.

1. Soit $P(X) = X^3 + 3X^2 + 3X + 2$. Démontrons que -2 est racine de P puis factorisons P par $X + 2$.

   On utilise la règle de Ruffini :

Coefficients	1	3	3	2
facteur -2	1	1	1	0

   Ainsi $P(-2) = 0$ donc -2 est racine de P et il est possible de factoriser P par $X + 2$. De plus d'après la règle de Ruffini nous voyons que la factorisation de P est $P(X) = (X + 2)(X^2 + X + 1)$.
2. $P(X) = 2X^3 - 9X^2 - 9X + 20$ et testez 5 comme racine.

Exercice 4. On considère l'équation $(E) : x^3 + 5x^2 + 11x + 15 = 0$.

1. Justifiez que, pour tout $x \in \mathbb{R}$, $x^3 + 5x^2 + 11x + 15 = (x+3)Q(x)$ où $Q \in \mathbb{R}[X]$ puis déterminez Q par la méthode de Ruffini.
2. Déduisez-en les solutions de (E) dans $\mathbb{C}$.

3 Division euclidienne polynomiale.

V Théorème d'Alembert-Gauss.

VI Exercices.

Exercice 5. Forme canonique d'une homographie.

Exercice 6. Décomposition en éléments simples d'une fraction rationnelle.

Exercice 7. Interpolation polynomiale : l'objectif est de trouver (le plus simple possible) dont la courbe représentative passe par des points placés dans un repère.

1. Polynôme de degré 1 dont la courbe passe par deux points.
2. Polynôme de degré deux dont la courbe passe par trois points.
3. Polynôme de degré deux dont la courbe passe par deux points.
4.

3. Nombres complexes.

I Point de vue algébrique.

1 Ensemble, addition, multiplication.

Lorsque nous écrivons $1 + 3x$ nous avons pris l'habitude de séparer 1 et $3x$. Nous savons que nous ne pouvons pas les additionner. De même $3 + \frac{5}{7}\sqrt{2}$ est formé d'une partie rationnelle 3 et d'une partie irrationnelle $\frac{5}{7}\sqrt{2}$. Nous allons construire des objets similaires appelés nombres complexes. L'objet qui tiendra lieu de x ou $\sqrt{2}$ est un nouveau nombre appelé nombre imaginaire et noté i. Ce nombre qui est apparu comme un outil dans la résolution d'équation s'est révélé très intéressant. i se définirait comme un nombre pour lequel $i^2 = -1$ ou encore comme une solution de l'équation $x^2 + 1 = 0$.

En ajoutant ce nombre à l'ensemble des nombres réels on voit qu'on peut construire des nombres de la forme $x + iy$.

Exercice 8. Construction de l'ensemble des nombres complexes par les couples. $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ est l'ensemble des couples de nombres réels. On muni cet ensemble de deux lois internes (opérations). L'addition : $(x,y) + (a,b) = (x + a, y + b)$. La multiplication : $(x,y) \times (a,b) = (xa - yb, ab + ya)$. On note $1_{\mathbb{C}}$ ou simplement 1 le couple $(1;0)$ et i le couple $(0;1)$. Il y a maintenant de nombreuses propriétés à montrer qui prolongent celles dont nous avons l'habitude dans $\mathbb{R}$:

1. $(a,b) = a1_{\mathbb{C}} + bi = a + ib$.
2. Commutativité des somme et produit.
3. Associativité de la somme et du produit.
4. Distributivité du produit sur la somme.
5. Existence d'un élément neutre pour les addition et multiplication.
6. Tous les couples admettent un symétrique pour l'addition. Tous les couples non nuls admettent un symétrique pour la multiplication (confer infra le conjugué).

Exercice 2.

Définition 2. On note $\mathbb{C}$ et on appelle *ensemble des nombres complexes* l'ensemble des nombres de la forme $x + iy$ où x et y sont des nombres réels muni des opération de multiplication et d'addition prolongeant celles de $\mathbb{R}$.

Exemples.

1) $3 + 5i$ est un nombre complexe. Cette présentation du nombre est appelé son *écriture algébrique* (nous en verrons d'autres). 3 est appelé sa *partie réelle* et 5 sa *partie imaginaire*.

2) $4 = 4 + 0i$ est un nombre réel et un nombre complexe. Tous les nombres réels sont des nombres complexes : $\mathbb{R} \subset \mathbb{C}$.

3) $7i = 0 + 7i$ est un nombre dont on dit qu'il est imaginaire pur.

4) Si $(a-b)+3bi = 4-5i$ avec a et b des réels alors $a-b=4$ et $3b=-5$. Autrement dit l'écriture algébrique d'un nombre complexe est unique.

5) Pour $-5+2i$ on notera souvent $z=-5+2i$ (x et y étant plutôt réservés pour les réels). Alors on note $\mathrm{Re}(z)=-5$ sa partie réelle et $\mathrm{Im}(z)=2$ sa partie réelle.

6) $(3+5i)+(2-7i)=5-2i$. $(3+5i)(2-7i)=3\times 2+3\times(-7i)+5i\times 2+5i\times(-7i)=6-21i+10i-35i^2=6-11i+35=41-11i$.

Remarques.

1. Pour une construction axiomatique plus rigoureuse considérez l'exercice 1.
2. $\mathbb{R}$ peut être vu comme une partie de $\mathbb{C}$: $\mathbb{R}\subset\mathbb{C}$ dont les opérations sont les mêmes. On dit que $\mathbb{C}$ est un surcorps de $\mathbb{R}$.
3. Si l'usage est d'utiliser les lettres x et y pour désigner des nombres réels, très souvent nous utiliserons z pour désigner un nombre complexe (mais sans préciser quelles sont ses parties réelle et imaginaire).

Exercice 9. Écrivez les nombres complexes donnés sous la forme algébrique $a+ib$.

a) -6.
b) $1-(i-1)$.
c) $-i-(-2-i)$.
d) $-2(4+3i)+i(6i-1)$.
e) $-i-(2i+1)(-2-i)$.
f) $-(-2+5i)(-i-1)$.
g) $3+i-2(5-2i)$.
h) $(1+2i)(3-2i)$.
i) $(2-5i)(2+5i)$.
j) $(1-2i)^2$.
k) $(i-1)^2$.
l) $(1+i)^2$.
m) $(1+i\sqrt{3})^2$.
n) $(\sqrt{3}-i)^2$.
o) $(2-i)^3$.
p) $(1+3i)^3$.

Exercice 3.

a) $-6=-6+0i$.
b) $1-(i-1)=2-i$.
c) $-i-(-2-i)=2$.
d) $-2(4+3i)+i(6i-1)=-14-7i$.
e) $-i-(2i+1)(-2-i)=-4+4i$.
f) $-(-2+5i)(-i-1)=-8+3i$.
g) $3+i-2(5-2i)=7+5i$.
h) $(1+2i)(3-2i)=7+4i$.
i) $(2-5i)(2+5i)=29$.
j) $(1-2i)^2=-3-4i$.
k) $(i-1)^2=-2i$.
l) $(1+i)^2=2i$.
m) $(1+i\sqrt{3})^2=-2+2i\sqrt{3}$.
n) $(\sqrt{3}-i)^2=2-2i\sqrt{3}$.
o) $(2-i)^3=(3-4i)(2-i)=2-11i$.
p) $(1+3i)^3=(-8+6i)(1+3i)=-26-18i$.

Exercice 10. Calculez i^2, i^3, i^4, i^{2013}. Déduisez-en une règle pour calculer i^n suivant les valeurs de n.

Exercice 4. $i^2=-1$, $i^3=i^2\times i=-1\times i=-i$., $i^4=i^3\times i=-i\times i=1$. Division euclidienne $2013=503\times 4+1$ donc $i^{2013}=(i^4)^{503}\times i=i$.

Exercice 11. On note $j:=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$.

1. Calculez j^2 et j^3 puis $1+j+j^2$.
2. Montrez que pour tout entier naturel n : $(1+j)^{2n+1}=-j^{n+2}$.
3. Donnez la forme algébrique de j^{2012}.

Exercice 5.

1. $j^2=-\frac{1}{2}-i\frac{\sqrt{3}}{2}$ et $j^3=1$ puis $1+j+j^2=0$.
2. Soit $n\in\mathbb{N}$. $(1+j)^{2n+1}=(-j^2)^{2n+1}=-j^{2(2n+1)}=-j^{4n+2}=-j^{3n}j^{n+2}=-j^{n+2}$.
3. $j^{2012}=j^{67\times 3+2}=j^2$.

2 Inverse et conjugué.

Définition 3. Soit $(x,y)\in\mathbb{R}^2$. Si $z=x+iy$ on appelle conjugué de z et on note $\overline{z}$ le nombre $\overline{z}=x-iy$.

Exemples.

1. $\overline{3+4i} = 3-4i$.

Nous devons parfois parler des parties réelle et imaginaire d'un nombre complexe z. Plutôt que de nommé ces parties on utilise des notations standards : $\mathrm{Re}(z)$ désigne la partie réelle de z et $\mathrm{Im}(z)$ la partie imaginaire de z. Ceci permet d'énoncé plus simplement certains résultats généraux.

Proposition 5. Soit $(z,z') \in \mathbb{C}^2$. $\overline{z+z'} = \overline{z} + \overline{z'}$. $\overline{z \times z'} = \overline{z} \times \overline{z'}$. $\overline{z^n} = \overline{z}^n$, $\overline{\overline{z}} = z$. $z\overline{z} = \mathrm{Re}(z)^2 + \mathrm{Im}(z)^2 \in \mathbb{R}$. $z + \overline{z} = 2\mathrm{Re}(z)$ et $z - \overline{z} = 2i\mathrm{Im}(z)$.

Démonstration. Démonstration au programme.

Remarques.

1. La conjugaison est très sympathique vis-à-vis des autres opérations. On dit que c'est un homomorphisme de $\mathbb{R}$-algèbre involutif.

Exercice 12. Déterminez le conjugué des nombres suivants (sans nécessairement déterminer la forme algébrique).

a) $-i$. b) $i-1$. c) $i(3+i)$. d) $-2i-2$. e) $(5+2i)^3$.

Exercice 6.

a) i. b) $-i-1$. c) $-i(3-i)$. d) $2i-2$. e) $(5-2i)^3$.

Exercice 13. Soient a, b et c des nombres réels. On pose $P(z) = az^2 + bz + c$. Démontrez que pour tout $z \in \mathbb{C}$, $\overline{P(z)} = P(b\overline{z})$.

Exercice 7. $\overline{az^2+bz+c} = \overline{az^2} + \overline{bz} + \overline{c} = \overline{a} \times \overline{z^2} + \overline{b} \times \overline{z} + c = a\overline{z}^2 + b\overline{z} + c = P(\overline{z})$.

Exercice 14. Si $z \in \mathbb{C}$, pour quels nombres peut-on être sûr qu'il est réel ou imaginaire pur parmi : $z^2 - 2$, $z\overline{z}$, $z - \overline{z}$, $z + \overline{z}$, $(z+iz)(z-iz)$ et $\frac{z+iz}{z-iz}$?

Exercice 8. $z\overline{z}$ et $z + \overline{z}$ sont des réels. $z - \overline{z}$ est un imaginaire pur. Pour les autres on peut trouver des contre-exemples.

Exercice 15. On note $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

1. Montrez que $\overline{j} = j^2 = \frac{1}{j}$.
2. Montrez que $1 + \overline{j} + \overline{j}^2 = 0$.
3. Montrez que pour tout $z \in \mathbb{C}$, $z^2 + z + 1 = (z-j)(z-\overline{j})$.

Exercice 9.

1. $\overline{j} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$. $j^2 = \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)^2 = \frac{1}{4} - \frac{\sqrt{3}}{2}i - \frac{3}{4} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i = \overline{j}$. $\frac{1}{j} = \frac{\overline{j}}{j\overline{j}} = \frac{\overline{j}}{\frac{1}{4}+\frac{3}{4}} = \overline{j}$.
2. $1 + \overline{j} + \overline{j}^2 = 1 + \overline{j} + \overline{j^2} = 1 + \overline{j} + \overline{\overline{j}} = 1 + \overline{j} + j = 1 + 2\mathrm{Re}(j) = 0$.
3. $(z-j)(z-\overline{j}) = z^2 - (j+\overline{j})z + j\overline{j} = z^2 + z + j\frac{1}{j}$.

Une petite observation dont nous aurons besoin : $a + ib = 0$ si et seulement si $a = b = 0$. Autrement dit pour qu'un complexe soit nul il faut que ces parties réelle et imaginaire soient nulles.

Proposition 6. Tout nombre complexe non nul z admet un inverse qui est unique et qui est noté $\frac{1}{z}$.

Démonstration.

* On sait que z est non nul donc $z\overline{z} = \mathrm{Re}(z)^2 + \mathrm{Im}(z)^2$ est non nul.
  $z\overline{z}$ est un réel non nul donc on peut considérer son inverse (en tant que nombre réel) : $\frac{1}{z\overline{z}}$.
* Notons $z' := \frac{1}{z\overline{z}}\overline{z}$ et démontrons que z' est l'inverse de z (autrement dit $zz' = 1$).
  $zz' = z\frac{1}{z\overline{z}}\overline{z} = \frac{1}{z\overline{z}}z\overline{z} = \frac{1}{\mathrm{Re}(z)^2+\mathrm{Im}(z)^2}(\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2) = 1$.
* Si $zz_1 = zz_2 = 1$ alors $z(z_1 - z_2) = 0$ et donc $z_1 = z_2 = 0$.

Remarques.

1. Si le résultat de la proposition est intéressant on attend surtout des élèves qu'ils soient capables de déterminer des inverses à partir des la forme algébrique dans des cas particuliers en utilisant la méthode de la quantité conjuguée. Maintenant que nous avons des inverses nous pouvons utiliser la notation fractionnaire pour signifier une division. Pour déterminer l'expression algébrique d'une telle expression fractionnaire nous utiliserons à nouveau l'astuce de la quantité conjuguée.

Exemples.

1. L'inverse de $1+2i$ est donc noté $\frac{1}{1+2i}$ et c'est un nombre complexe donc il admet une écriture algébrique le but est souvent de retrouver cette écriture. On utilise l'astuce de la quantité conjuguée de $1+2i$ à savoir $1-2i$: $\frac{1}{1+2i} = \frac{1\times(1-2i)}{(1+2i)(1-2i)} = \frac{1-2i}{1^2+2^2} = \frac{1}{5} - \frac{2}{5}i$.
2.

Exercice 16. Écrivez les nombres complexes donnés sous la forme algébrique $a+ib$.

a) $\frac{1}{i}$. b) $-\frac{2}{3i}$. c) $\frac{2-i}{2+i}$. d) $\frac{1}{1-i}$. e) $\frac{3-5i}{i}$.
f) $\frac{i}{2+i}$. g) $\frac{2+7i}{4-2i}$. h) $\frac{-1-2i}{4-i}$. i) $\frac{1}{i-\sqrt{3}}$. j) $\frac{1+\sqrt{3}}{1+i}$.
k) $\frac{3-5i}{1+i}$. l) $\frac{\sqrt{2}-i}{\sqrt{2}+2i}$. m) $\frac{6+2i}{-1+3i}$.

Exercice 10.

a) $\frac{1}{i} = \frac{1\times(-i)}{i\times(-i)} = -i$.
b) $-\frac{2}{3i} = -\frac{2\times(-3i)}{3i\times(-3i)} = \frac{2}{3}i$.
c) $\frac{2-i}{2+i} = \frac{(2-i)^2}{(2+i)(2-i)} = \frac{3-4i}{2^2+1^2} = \frac{3}{5} - \frac{4}{5}i$.
d) $\frac{1}{1-i} = \frac{1+i}{(1-i)(1+i)} = \frac{1+i}{1^2+1^2} = \frac{1}{2} + \frac{1}{2}i$.
e) $\frac{3-5i}{i} = \frac{(3-5i)(-i)}{i(-i)} = -5-3i$.
f) $\frac{i}{2+i} = \frac{i(2-i)}{(2+i)(2-i)} = \frac{1+2i}{2^2+1^2} = \frac{1}{5} + \frac{2}{5}i$.
g) $\frac{2+7i}{4-2i} = \frac{(2+7i)(4+2i)}{(4-2i)(4+2i)} = \frac{-6+32i}{4^2+2^2} = -\frac{3}{10} + \frac{8}{5}i$.
h) $\frac{-1-2i}{4-i} = \frac{(-1-2i)(4+i)}{(4-i)(4+i)} = \frac{-2-9i}{4^2+1^2} = -\frac{2}{17} - \frac{9}{17}i$.
i) $\frac{1}{i-\sqrt{3}} = \frac{-i-\sqrt{3}}{(i-\sqrt{3})(-i-\sqrt{3})} = \frac{-i-\sqrt{3}}{1^2+\sqrt{3}^2} = -\frac{\sqrt{3}}{4} - \frac{1}{4}i$.
j) $\frac{1+\sqrt{3}}{1+i} = \frac{(1+\sqrt{3})(1-i)}{(1+i)(1-i)} = \frac{1+\sqrt{3}-(1+\sqrt{3})i}{1^2+1^2} = \frac{1+\sqrt{3}}{2} - \frac{1+\sqrt{3}}{2}i$.
k) $\frac{3-5i}{1+i} = \frac{(3-5i)(1-i)}{(1+i)(1-i)} = \frac{-2+2i}{1^2+1^2} = -1+i$.
l) $\frac{\sqrt{2}-i}{\sqrt{2}+2i} = \frac{(\sqrt{2}-i)(\sqrt{2}-2i)}{(\sqrt{2}+2i)(\sqrt{2}-2i)} = \frac{-3\sqrt{2}i}{\sqrt{2}^2+2^2} = -\frac{3\sqrt{2}}{6}i$.
m) $\frac{6+2i}{-1+3i} = \frac{(6+2i)(-1-3i)}{(-1+3i)(-1-3i)} = \frac{-11i}{1^2+3^2} = -\frac{11}{10}i$.

Exercice 17. Déterminez le conjugué des nombres suivants (sans nécessairement déterminer la forme algébrique).

a) $\frac{i}{2}$. b) $\frac{2}{i}$. c) $\frac{1+i}{1-i}$. d) $\frac{1-i}{1+i}$. e) $\left(\frac{i}{i+1}\right)^5$.

Exercice 11.

a) $-\frac{i}{2}$. b) $-\frac{2}{i}$. c) $\frac{1-i}{1+i}$. d) $\frac{1+i}{1-i}$. e) $\left(-\frac{i}{-i+1}\right)^5$.

Exercice 18. Que dire des nombres $z_1 = \frac{2+3i}{4+i}$ et $z_2 = \frac{2-3i}{4-i}$? Déduisez-en : z_1+z_2 et z_1-z_2.

Exercice 12.

* $\overline{z_1} = \overline{\frac{2+3i}{4+i}} = \frac{\overline{2+3i}}{\overline{4+i}} = \frac{2-3i}{4-i} = z_2$.

* $z_1+z_2 = 2\mathrm{Re}(z_1)$ et $z_1-z_2 = 2i\mathrm{Im}(z_1)$. Or $\frac{2+3i}{4+i} = \frac{(2+3i)(4-i)}{(4+i)(4-i)} = \frac{11+10i}{4^2+1^2} = \frac{11}{17}+\frac{10}{17}i$ donc $z_1 = \frac{22}{17}$ et $z_2 = \frac{20}{17}i$.

Exercice 19. Écrivez les nombres complexes donnés sous la forme algébrique $a+ib$. $z_1 = \frac{1}{1-i}$. $z_2 = \frac{1}{1+z_1}$.

Exercice 13. $z_1 = \frac{1(1+i)}{(1-i)(1+i)} = \frac{1+i}{1^2+1^2} = \frac{1}{2}+i\frac{1}{2}$. $z_2 = \frac{1}{1+\frac{1}{2}+i\frac{1}{2}} = \frac{2}{3+i} = \frac{2(3-i)}{(3+i)(3-i)} = \frac{6-2i}{3^2+1^2} = \frac{3}{5}-i\frac{1}{5}$.

Exercice 20. On note $z_1 := 2-5i$ et $z_2 := 1+2i$. Donnez la forme algébrique des nombres complexes suivants.

a) z_1+z_2. b) z_1z_2. c) $\frac{z_1}{z_2}$. d) $\left(\frac{z_1}{z_2}\right)^2$. e) $z_1z_2^2$.

Exercice 14.

a) $z_1+z_2 = 3-3i$.
b) $z_1z_2 = 12-i$.
c) $\frac{z_1}{z_2} = \frac{z_1\overline{z_2}}{1^2+2^2} = \frac{-8-9i}{5} = -\frac{8}{5}-\frac{9}{5}i$.
d) $\left(\frac{z_1}{z_2}\right)^2 = \left(-\frac{8}{5}-\frac{9}{5}i\right)^2 = \left(-\frac{8}{5}\right)^2+2\left(-\frac{8}{5}\right)\left(-\frac{9}{5}i\right)+\left(-\frac{9}{5}i\right)^2 = \frac{17}{25}+\frac{144}{25}i$.
e) $z_1z_2^2 = (2-5i)(1+2i)^2 = (2-5i)(-3+4i) = 14+23i$.

Exemples.

1. Trouver la forme algébrique d'un nombre avec des conjugaisons.

Propriétés de la conjugaison.

3 Formule du binôme.

Proposition 7. Formule du binôme de Newton. $\forall (a,b)\in\mathbb{C}^2,\ (a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}$.

Démonstration. Démonstration au programme par récurrence.

Considérons

$(a+b)n = (a+b)(a+b)\dots(a+b)$.

Pour obtenir dans le développement un terme contenant exactement k facteurs b, il faut choisir les k facteurs parmi les n parenthèses dans lesquels on prend b.

Il y a donc

(nk)

façons d'obtenir un terme contenant exactement k facteurs b.

Chacune de ces contributions vaut

$a^{n-k}b^k$.

Ainsi, pour un entier k fixé, la contribution totale est

(nk)an-kbk.

Les différents cas k=0,1,...,n sont disjoints. En appliquant le principe additif, on obtient $(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$.

4 Résoudre des équations linéaires (y compris avec conjugaison).

Exercice 21. Résolvez dans $\mathbb{C}$ les équations données d'inconnue z.

a) $2z+i = 5-2i$.
b) $iz+1 = i$.
c) $1-2z = 3iz+5-i$.
d) $iz+1 = z-i$.
e) $\frac{2z+1}{z-i} = 1$.
f) $\frac{1-z}{1+z} = i$.
g) $\frac{2+iz}{2-iz} = \frac{2+i}{2-i}$.
h) $\frac{2}{iz+\sqrt{3}} = \frac{iz+\sqrt{3}}{2}$.

Exercice 22. Résolvez les équations dans $\mathbb{C}$.

a) $i\overline{z} = 1$.
b) $i\overline{z} + i = 0$.
c) $\overline{z} - 2z = 1 + 5i$.
d) $2i\overline{z} + 3z = 5 - 2i$.
e) $(1-i)\overline{z} = z$.
f) $(3+i)\overline{z} = (1-5i)z$.
g) $i\overline{z} - 2i = (2-i)z + 1$.
h) $(3-2i)\overline{z} - 2iz = 3 - 2i$.
i) $\overline{z} = \frac{1+i}{1-i}z$.
j) $(1+i\sqrt{3})\overline{z} = (1-i\sqrt{3})z$.

5 Racines dans $\mathbb{C}$ des polynômes de degré deux à coefficients réels.

Exercice 23. Résolvez les équations dans $\mathbb{C}$.

a) $z^2 = -1$.
b) $z^2 + z + 1 = 0$.
c) $z^2 + 2z + 5 = 0$.
d) $z^2 - z + 1 = 0$.
e) $z^2 - \sqrt{3}z + 31 = 0$.
f) $z^2 - 3z + 3 = 0$.
g) $z^2 - 6z + 10 = 0$.
h) $z^2 - 22z + 410 = 0$.

Exercice 24. Soit $\theta \in \mathbb{R}$ et (E) l'équation d'inconnue z : $z^2 - 2z\cos(\theta) + 1 = 0$. Déterminez les solutions complexes de l'équation d'inconnue δ, $\delta^2 = -\sin^2(\theta)$ puis déduisez-en, les solutions complexes de (E).

II Point de vue géométrique.

1 De $\mathbb{C}$ vers le plan d'Argand-Cauchy et réciproquement.

Soit $(a,b) \in \mathbb{R}^2$. Au nombre complexe $a + ib$ on associe le point M de coordonnées (a,b) d'un plan orthonormé. M est appelé l'*image* de $a + ib$. Un tel plan associé à $\mathbb{C}$ est appelé le pan d'Argand-Cauchy.

Réciproquement, un point du plan muni d'un repère orthonormé $M(a,b)$ on associe le nombre complexe $z_M = a + ib$ qui est appelé l'*affixe* de M.

Remarques.

1. On parle aussi du plan d'Argand, ou d'Argand-Gauss. Jean-Robert Argand (1768–1822) a proposé une représentation géométrique des nombres complexes, notamment dans son travail de 1806. Cauchy a ensuite joué un rôle majeur dans le développement de la théorie des fonctions d'une variable complexe. Gauss est également associé à la représentation géométrique des complexes, d'où l'appellation plan d'Argand-Gauss.
2. Chaque nombre complexes est associé à une unique image et chaque point est associé à une unique affixe. Ainsi $\mathbb{C}$ et le plan d'Argand sont en bijection.
3. Nous allons donc apprendre à traduire les questions de géométries en questions de calculs sur les nombres complexes.
4. L'affixe d'un point M sera le plus souvent notée z_M.

Exemples.

1. $-3 + 5i$ correspond au point de coordonnées $(-3;5)$.
2. L'affixe du point $M(7;8)$ est $z_M = 7 + 8i$.
3. 1 correspond au point de cordonnées $(1;0)$.
4. i correspond au point de coordonnées $(0;1)$.
5. L'ensemble des nombres réels se confond avec l'axe des abscisses du plan d'Argand. Tandis que les imaginaires pures se confondent avec l'axe des ordonnées.

III "Racine carrée" dans $\mathbb{C}$.

Exercice 25.

1. Résolvez dans $\mathbb{R}$, l'équation $x^2 - 3x - 4 = 0$.
2. Déduisez-en les solutions réelles de l'équation $x^4 - 3x^2 - 4 = 0$.
3. On considère dans $\mathbb{C}$, l'équation (E) : $z^2 = 3 - 4i$.
   (a) Montrez que cette équation équivaut à (S) : $\begin{cases} z = x + iy \\ x^2 - y^2 = 3 \\ xy = -2 \end{cases}$
   (b) Démontrez que le couple de réels (x,y) est solution du système (S') : $\begin{cases} x^2 - y^2 = 3 \\ xy = -2 \end{cases}$ si et seulement si il est solution du système : $\begin{cases} x^4 - 3x^2 - 4 = 0 \\ y = -\frac{2}{x} \end{cases}$.
   (c) Déduisez-en les solutions du système (S'), puis celles du système (S).
   (d) Concluez sur les solutions de l'équation (E).

4. Arithmétique.

I Diviseurs.

Définition 4. Soient $(a,b) \in \mathbb{Z}^2$. On dit que b est *un diviseur* de a, et on note $b|a$, si et seulement si il existe $k \in \mathbb{Z}$ tel que $bk = a$.

Exemples.

1. 3 est un diviseur de 12 puisque $3 \times 4 = 12$.
2. 0 est divisible par tous les nombres.
3. 1 est un diviseur de tous les entiers.
4. Le seul nombre qui admette 0 pour diviseur est 0.
5. 1 admet deux diviseurs exactement 1 et -1.
6. Déterminons tous les diviseurs de 24. Commençons par recenser ceux positifs. $1 \times 24 = 24$, $2 \times 12 = 24$, $3 \times 8 = 24$, $4 \times 6 = 24$, $5 \times ? = 24$, $6 \times 24 = 24$ on retrouve des diviseurs déjà obtenus et donc l'ensemble des diviseurs est $\{1;2;3;4;6;8;12;24;-1;-2;-3;-4;-6;-8;-12;-24\}$.
7. Nous l'avons déjà rencontré les années précédentes (mais nous en reparlerons plus loin dans la leçon) : un nombre premier comme 3 admet exactement deux diviseurs positifs 1 et 3 lui-même.
8. 7 n'est pas divisible par 3 puisque $2 \times 3 < 7 < 3 \times 3$.

Remarques.

1. Nous nous intéresserons le plus souvent aux diviseurs positifs le cas négatif s'en déduisant par symétrie. Confer infra une proposition.
2. Dans la suite nous noterons $D(b)$ l'ensemble des diviseurs positifs de b. Nous avons déjà observé que $D(1) = \{1\}$, $D(-1) = \{1\}$, $D(24) = \{1;2;3;4;6;8;12;24\}$, $D(3) = \{1;3\}$, $D(0) = \mathbb{N}$.
3. Dire que b est un diviseur de a peut se dire de diverses façons : a est un multiple de b ou b est divisible par a.

Exercice 26. Soient $(p,q) \in \mathbb{Z}^2$. Montrez que $14p^2 - 35q$ est divisible par 7.

Exercice 15. $14p^2 - 35q = 7(2p - 5q)$ et $2p - 5q \in \mathbb{Z}$ donc $2p - 5q$ est divisible par 7.

Exercice 27. Déterminez les entiers naturels n tels que 4 divise $n + 13$.

Exercice 16. Procédons par analyse-synthèse.

Supposons qu'il existe $k \in \mathbb{Z}$ tel que $4k = n + 13$. Alors $n = 4k - 13$. De plus $n \geqslant 0$ donc $4k - 13 \geqslant 0$ et enfin $k \geqslant 4$.

On vérifie que les nombres de la forme $4k - 13$ avec $k \geqslant 4$ conviennent.

L'ensemble des nombres recherchés est $\{4k - 13 \mid k \in \mathbb{N} \text{ et } k \geqslant 4\}$.

Exercice 28. Montrez que, quel que soit $n \in \mathbb{Z}$, $2n + 5$ n'est jamais divisible par 2.

Exercice 17. Procédons à une démonstration par l'absurde.

Supposons qu'il existe $k \in \mathbb{Z}$ tel que $2k = 2n + 5$. Ainsi : $5 = 2(k - N)$ et comme $k - n \in \mathbb{Z}$ cela signifie que 5 est impair ce qui est impossible.

Proposition 8. Soient $(a,b) \in \mathbb{Z}^2$. Si $b|a$ alors $-b|a$ et $b|-a$ et $-b|-a$.

Démonstration. Soient $(a,b) \in \mathbb{Z}^2$.

Démontrons : $(b|a) \Rightarrow (-b|a)$.

Supposons donc $b|a$ et démontrons que $-b|a$.

Puisque $b|a$ il existe un entier k tel que $bk = a$. On a donc $(-b)(-k) = a$ et par conséquent $-b|a$. ■

Les autres cas se traitent de même.

Remarques.

1. On peut préciser que a et $-a$ ont les mêmes diviseurs.

Proposition 9. Soit $(a,b) \in \mathbb{N}^* \times \mathbb{Z}$. Si b est un diviseur positif de a alors $1 \leqslant b \leqslant a$.

Démonstration. Soient $a \in \mathbb{N}^*$ et $b \in \mathbb{N}$.

Démontrons : si $(b|a)$ alors $(1 \leqslant b \leqslant a)$.

* Puisque $b|a$: $\exists k \in \mathbb{Z}$, $bk = a$.
  Dans ce cas nécessairement : $k \neq 0$ car $a \neq 0$. De plus si $k < 0$ son opposé est aussi un diviseur. Soit donc $k \in \mathbb{N}^*$ tel que $bk = a$.
  $a - b = bk - b = b(k-1)$ or $b \geqslant 0$ et $k \geqslant 1$ donc $b(k-1) \geqslant 0$. Autrement dit $b \leqslant a$.
* b est positif et, comme remarqué précédemment, $k \in \mathbb{N}^*$, donc $b \geqslant 1$.

Finalement on a bien $1 \leqslant b \leqslant a$. ■.

Remarques.

1. Si $b = 0$ il y a une infinité de diviseurs c'est pourquoi ce cas est exclu de la proposition.
2. Nous en déduisons en particulier $D(b) \subset [\![1,b]\!]$, résultat que nous allons tout de suite réutilisé.

Proposition 10. Soit $a \in \mathbb{Z}$. Si $a \neq 0$ alors a possède un nombre fini de diviseurs. Si $a = 0$ alors tout entier est un diviseur de a.

Démonstration. Corollaire de la précédente proposition.

Nous allons maintenant utiliser un résultat intuitif mais qui nécessiterait un peu de réflexion : un ensemble fini de nombres a toujours un plus petit et un plus grand élément (appelés minimum et maximum). Rappelons que ce n'est pas généralisable à un ensemble infini : $[0;1[$ n'a pas de maximum *i.e.* de plus grand élément.

Proposition 11. Soit $(m,n) \in \mathbb{Z}^2$. m et n admettent un plus petit et un plus grands commun diviseur positifs.

Démonstration. Notons $b = \max(|m|,|n|)$ alors d'après la précédente proposition $D(m) \cap D(n) \subset [\![1,b]\!]$ qui est un ensemble fini donc cet ensemble admet un plus petit et un plus grand élément. ■

Remarques.

1. Nous noterons $D(m,n)$ l'ensemble des diviseurs communs à m et n. Nous avons donc établit que 1 est le minimum de $D(m,n)$ et qu'il admet un maximum.

Exercice 29. Proposez une fonction Python qui accepte pour argument un entier et renvoie la liste de ses diviseurs positifs.

Exercice 18.

```
def listediviseurs(a):
    if a<0:
        a=-a
    diviseurs=[]
    for k in range(1,a+1):
        if a%k==0:
            diviseurs.append(k)
    return diviseurs
```

Proposition 12. Soit $(a,b) \in \mathbb{Z}^2$.

(i) $(a|b) \Rightarrow (a|bc)$.

(ii) $\left\{ \begin{array}{l} (a|b) \\ (a|c) \end{array} \right. \Rightarrow (a|b+c)$.

(iii) $\left\{ \begin{array}{l} (a|b) \\ (c|d) \end{array} \right. \Rightarrow (ac|bd)$.

(iv) $\forall n \in \mathbb{N}^*$, $(a|b) \Rightarrow (a^n|b^n)$.

Démonstration.

(i) Démontrons : $(a|b) \Rightarrow (a|bc)$.
$a|b$ donc : $\exists k \in \mathbb{Z}$, $ak = b$.
Soit donc un tel k.
$bc = akc = a(kc)$ et $kc \in \mathbb{Z}$ donc $a|bc$. ■

(ii) Idem.

II Division euclidienne et congruence.

Théorème 1. Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$. Il existe un unique $(q,r) \in \mathbb{Z}^2$ tel que $\left\{ \begin{array}{l} a = bq + r \\ 0 \leqslant r < b \end{array} \right.$.
Ce dernier système est appelé *la division euclidienne* de a par b.

Démonstration.

Exemples.

1. $14 = 3 \times 4 + 2$ est la division euclidienne de 14 par 3 car $0 \leqslant 2 < 3$. C'est aussi la division euclidienne de 14 par 4 puisque $0 \leqslant 2 < 4$.
2. $19 = 5 \times 3 + 4$ est la division euclidienne de 19 par 5 car $0 \leqslant 4 < 5$. Ce n'est pas la division euclidienne de 19 par 3 puisque $4 \geqslant 3$.
3. $12 = 3 \times 4 + 0$ est la division euclidienne de 12 par 3 (ou par 4) car $0 \leqslant 0 < 3$ (ou 4).

Remarques.

1. Un peu de taxinomie : a est appelé le dividende, b le diviseur, a le quotient et r le reste.
2. On retrouve les différents éléments de la division euclidienne en procédant à la division posée en potence vue à l'école primaire.

Exercice 30. Sachant que le quotient et le reste dans la division euclidienne de 432 par 17 sont 25 et 7 déterminez le quotient et le reste dans la division euclidienne de -432 par 7.
Exercice 19.

Proposition 13. Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$. a est un diviseur de b si et seulement si le reste de la division euclidienne de a par b est 0.

```
def divisioneuclidienne(a,b):
    return [a,b,a//b,a%b]
```

Définition 5. Soit $(a,b,n) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}$. Nous dirons que a est congru à b modulo n si et seulement si $n|a-b$.

Exemples.

1. $24 \equiv 10\ [7]$ car $24 - 10 = 14 = 2 \times 7$.
2. $17 \equiv 29\ [3]$ car $17 = 5 \times 3 + 2$ et $29 = 9 \times 3 + 2$ (mêmes restes).
3. Deux entiers sont congrus modulo 10 si et seulement si ils ont le même chiffre des unités.

Proposition 14. Soit $(a,b,n) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}$. $a \equiv b\ [n]$ si et seulement si : $\exists k \in \mathbb{Z}$, $a = b + kn$.

Exercice 31. Déterminez $b \in \mathbb{Z}$ tel que $a \equiv b\ [7]$ et $-4 \leqslant b < 3$:

a) $a = -3$, b) $a = 15$, c) $a = 116$,
d) $a = -87$, e) $a = 28$, f) $a = 104$.

Exercice 20.

a) $b \equiv -3\ [7]$ et $-4 \leqslant b < 3 \Leftrightarrow -4 \leqslant 7k - 3 < 3 \Leftrightarrow -\frac{1}{7} \leqslant k < \frac{6}{7}$ $b \in \{0\}$.
b) $b \equiv 15\ [7] \Leftrightarrow b \equiv 1\ [7]$ et $-4 \leqslant 7k + 1 < 3 \leftrightarrow -\frac{5}{7} \leqslant k < \frac{2}{7}$ donc $k_i n\{0\}$.
c) $b \equiv 116\ [7] \equiv 4\ [7]$ et $-4 \leqslant 7k + 4 < 3 \Leftrightarrow -\frac{8}{7} \leqslant k < -\frac{1}{7}$ donc $k \in \{1\}$.
d) $a = -87$,
e) $a = 28$,
f) $a = 104$.

Proposition 15. Soit $(a,b,n) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}$.

(i) Si $a \equiv b\ [n]$ alors $b \equiv a\ [n]$.
(ii) $a \equiv a\ [n]$.
(iii) Si $a \equiv b\ [n]$ et $b \equiv c\ [n]$ alors $a \equiv c\ [n]$.

Remarques.

1. Pour le (i) nous dirons que l'équivalence modulo n est une relation symétrique (cela ressemble à la commutativité).
2. Pour le (ii) nous dirons que l'équivalence modulo n est une relation réflexive.
3. Pour le (iii) nous dirons que l'équivalence modulo n est une relation transitive.
4. Ces trois propriétés se retrouvent dans l'égalité de nombres. Elles nous permettent de manipuler les équivalences modulo$n$ comme nous le ferions avec des égalités de nombres.

Exercice 32. Montrer des congruences.

Proposition 16. Lien entre congruence et division euclidienne.

(i) $a \equiv 0\ [n]$ si et seulement si $n|a$.
(ii) r est le reste de la division euclidienne de a par ssi $a \equiv r\ [n]$ et $r \in [\![0,n-1]\!]$.

Proposition 17. Soit $(a,n) \in \mathbb{Z} \times \mathbb{N}^*$.

(i) Il existe un unique $r \in [\![0,n-1]\!]$ tel que $a \equiv k\ [n]$.
(ii) il existe $b \in \mathbb{Z}$ tel que a peut s'écrire sous la forme bn ou $bn + 1$ ou $bn + 2$ ou ... ou $bn + n - 1$.

Démonstration. C'est une conséquence de la division euclidienne de a par n et k en désigne le reste. La seconde assertion est une conséquence, une formulation différente, de la première.

Proposition 18. Soit $(a,b,c,d,) \in \mathbb{Z}^4$ et $(n,k) \in \mathbb{N}^* \times \mathbb{N}$.

(i) Si $a \equiv b\ [n]$ alors $a + c \equiv b + c\ [n]$.
(ii) Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors $a + c \equiv b + d\ [n]$.
(iii) Si $a \equiv b\ [n]$ alors $ac \equiv bc\ [n]$.
(iv) Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$ alors $ac \equiv bd\ [n]$.
(v) Si $a \equiv b\ [n]$ alors $a^k \equiv b^k\ [n]$

Remarques.

1.

Exercice 33. Montrons de trois façons différentes que le produit de trois entiers naturels consécutifs est divisible par 3.

Exercice 21. On peut le montrer par récurrence, en raisonnant sur la divisibilité directement et enfin avec la congruence.

Exercice 34. Montrer $2^{3n} - 1$ est multiple de 7.

Exercice 22. $2^{3n} - 1 \equiv 8^n - 1\ [7] \equiv 1^n - 1\ [7] \equiv 0\ [7]$.

Exercice 35. Pour quelles valeurs de l'entier naturel n, $n^2 - 3n + 6$ est-il divisible par 4 ? Pour cela vous regarderez au cas par cas selon le reste de la division euclidienne de n par 4.

Exercice 23. Si $n \equiv 0\ [4]$ alors $n^2 - 3n + 6 \equiv 6\ [4] \equiv 2\ [4]$. De même pour les autres.

Exercice 36. Déterminez le reste de la division euclidienne de 11^{2020} par 3.

Exercice 24. $11^{2020} \equiv (-1)^{2020}\ [3] \equiv 1^{1010}\ [3] \equiv 1\ [3]$.

Exercice 37. Soit n un entier naturel. Montrez que le nombre $7^n + 1$ est divisible par 8 lorsque n et pair.

Exercice 25. $7^n + 1 \equiv 7^{2k+1} + 1\ [8] \equiv 49^k \times 7 + 1\ [8] \equiv 1 \times 7 + 1\ [8] \equiv 0\ [8]$.

Exercice 38. Déterminez le reste de la division euclidienne de $2020 \times 2022 \times 2023$ par 11.

Exercice 26. $2020 = 183 \times 11 + 7$ donc $2020 \equiv 7\ [11]$ et $2022 \equiv 9\ [11]$ et $2023 \equiv 10\ [11]$. Enfin $2020 \times 2022 \times 2023 \equiv 7 \times 9 \times 10\ [11] \equiv -4 \times (-2) \times 10\ [11] \equiv 80\ [11] \equiv 3\ [11]$.

III Résoudre une congruence : $ax \equiv b\ [n]$.

Les précédents résultats sur la congruence permettent de résoudre des équations. L'idée pour résoudre une équation polynomiale avec congruence et de travailler par disjonction des cas avec les restes possibles correspondant au modulo considéré. Ainsi si l'on travail modulo 3 on considérera les cas $x \equiv 0\ [3]$, $x \equiv 1\ [3]$ et $x \equiv 2\ [3]$. Ceci permet de tester tous les entiers possibles, d'après une précédente proposition mais de plus en ne considérant que l'aspect qui nous intéresse la divisibilité par 3.

Exemples.

1. Résolvons $x^2 \equiv 1\ [4]$.
   * Si $x \equiv 0\ [4]$ alors $x^2 \equiv 0^2\ [4]$.
   * Si $x \equiv 1\ [4]$ alors $x^2 \equiv 1^2\ [4]$.
   * Si $x \equiv 2\ [4]$ alors $x^2 \equiv 2^2\ [4]$.
   * Si $x \equiv 3\ [4]$ alors $x^2 \equiv 9^2\ [4] \equiv 1\ [5]$.

   Les solutions sont les nombres de la forme $1+4k$ et ceux de la forme $2+4k$ pour $k \in \mathbb{Z}$.
2. Situation astucieuse : $3x \equiv 2\ [5] \leftrightarrow 7 \times 3x \equiv 7 \times 2\ [5] \Leftrightarrow x \equiv 4\ [5]$.

Exercice 39. Résolvez dans $\mathbb{Z}$ les équations suivantes.

a) $x + 5 \equiv 2\ [3]$. b) $3x \equiv 7\ [8]$. c) $(x-1)(x+7) \equiv 0\ [5]$.

Exercice 27.

a) Astuce : $x + 5 \equiv 2\ [3] \Leftrightarrow x \equiv -3\ [3] \Leftrightarrow x \equiv 0\ [3]$.
b) Astuce : $3x \equiv 7\ [8] \Leftrightarrow 3 \times 3x \equiv 3 \times 7\ [8] \Leftrightarrow x \equiv 5\ [8]$. Sinon on peut tester $x \equiv 0\ [8]$ ... $x \equiv 7\ [8]$.
c) Astuce comme 5 est premier $(x-1)(x+7) \equiv 0\ [5] \Leftrightarrow x - 1 \equiv 0\ [5]$ ou $x + 7 \equiv 0\ [5]$.

Exercice 40. Résolvez dans $\mathbb{Z}$ les équations suivantes.

a) $327 \equiv x\ [11]$ et $0 \leqslant x < 11$. b) $5x \equiv 2\ [7]$ et $-3 < x < 12$.
c) $17 - x \equiv 2\ [13]$ et $-25 < x < 5$.

Exercice 28.

a) $x \equiv 327 - 242\ [11] \equiv 85\ [11] \equiv 8\ [11]$ et $0 \leqslant x < 11$ donc $x = 8$.
b) $x \equiv 6\ [7]$ et $-3 < x < 12$ donc $x \in \{-1; 6\}$.
c) $-x \equiv -15\ [13] \Leftrightarrow x \equiv 15\ [13] \Leftrightarrow x \equiv 2\ [13]$ et $-25 < x < 5 \Leftrightarrow -25 < 13k + 2 < 5 \Leftrightarrow -\frac{27}{13} < x < \frac{3}{13}$. Ainsi $x \in \{-1; 0\}$.

Exercice 41.

1. Soit $a \in \mathbb{N}$. Quels sont les restes de la division euclidienne par 4 de a^2, a^3, a^4, a^5.
2. Que pouvez-vous conjecturer grâce à la question précédente ? Démontrez cette conjecture par disjonction des cas.

Exercice 29.

1. Si $a \equiv 0\ [4]$ ou $a \equiv 2\ [4]$ alors $a^2 \equiv 0\ [4]$. Si $a \equiv 1\ [4]$ et $a \equiv 3\ [4]$ alors $a^2 \equiv 1\ [4]$.
   Si $a \equiv 0\ [4]$ ou $a \equiv 2\ [4]$ alors $a^3 \equiv 0\ [4]$. Si $a \equiv 1\ [4]$ alors $a^3 \equiv 1\ [4]$. Si $a \equiv 3\ [4]$ alors $a^3 \equiv 3\ [4]$.
   Sous forme de tableau :

$a \equiv$	0	1	2	3
a^2	0	1	0	1
a^3	0	1	0	3
a^4	0	1	0	1
a^5	0	1	0	3

2. Si a est divisible par 2 ou 4 alors le reste de la division euclidienne de a^n par 4 est 0 si $n \in \mathbb{N}^*$.
   Si a admet un reste de 1 dans la division euclidienne par 4, alors a^n admet pour reste 1 également.
   Si a admet pour reste 3 dans la division euclidienne par 4 alors a^n admet pour reste 1 ou 3 suivant que n est pair ou impair.

Exercice 42. Étudiez les congruences des puissances de 2 modulo 5. Déduisez-en le reste de la division euclidienne de 2022^{2023} par 5 ;

Exercice 30.

$a \equiv$	0	1	2	3	4

IV PGCD

On appelle plus grand commun diviseur de deux entiers a et b le plus grand entier positif m tel que $m|a$ et $m|b$. C'est aussi le plus petit élément de $D(a;b) = D(a) \cap D(b)$.

Illustration avec le découpage de la feuille en carrés : 9×24. Il faut trouver les dimensions du plus grand carré qui permette de recouvrir toute la feuille. Puis mise en œuvre : $24 = 2 \times 9 + 6$ donc la feuille peut être recouverte par deux carrés 9^2 et il reste un rectangle 6×9. $9 = 1 \times 6 + 3$ donc le rectangle 6×9 peut être recouvert par un carré 6^2 et il reste un rectangle 6×3. $6 = 2 \times 3$ donc le rectangle 6×3 peut être recouvert par deux carrés 3^2. Le plus grand carré qui permette de recouvrir toute la feuille de départ est celui de côté 3. Autrement dit 3 est le plus grand diviseur commun de 24 et de 9.

Ce que nous venons de voir c'est une illustration d'un algorithme pour obtenir le plus grand commun diviseur de deux entiers.

$$\begin{aligned} 24 &= 2 \times 9 + 6 \\ 9 &= 1 \times 6 + 3 \\ 6 &= 2 \times 3 \end{aligned}$$

Cet algorithme est appelé l'algorithme d'Euclide il repose sur le résultat suivant si on a la division euclidienne : $a = qb + r$ alors $D(a,b) = D(b;r)$ avec $b \leqslant a$ (suite décroissante d'entiers naturels donc convergente).

```
def algorithmedeuclidebis(a,b):
    if a<b:
        a,b=b,a
    c=a%b
    while c:
        a,b,c=b,c,a%b
    return b
```

```
def algorithmedeuclide(a,b):
    if a<b:
        a,b=b,a
    while b:
        c=b
        a,b=b,a%b
    return c
```

Exercice 43. Déterminer divers pgcd avec l'algorithme d'Euclide.

Exercice 44. Déterminez le pgcd de 1551 et 132 avec l'algorithme d'Euclide. Déduisez-en les diviseurs communs de 1551 et 132.

Exercice 45. Soit $n \in \mathbb{N}$. Écrivez la division euclidienne de $5n+7$ par $n+1$ puis déduisez-en que les diviseurs communs de $5n+7$ et $n+1$ sont les diviseurs communs de $n+1$ et 2. Déterminez le pgcd de $5n+7$ et $n+1$ selon les valeurs de n.

V Couples d'entiers premiers entre eux.

a et b entiers naturels sont dit premiers entre-eux si $\text{pgcd}(a,b) = 1$. Définition pour les relatifs avec 1 et -1.

Donc recherche de pgcd et si c'est 1 alors ils sont premiers entre eux.

Exercice 46. Démontrez que si a et b sont non nuls alors il existe a' et b' tels que $a = a'd$ et $b = b'd$ et $\text{pgcd}(a',b') = 1$.

Avec la décomposition en facteurs premiers. Ils sont premiers entre eux si et seulement si il ne possède aucun facteurs premier commun.

VI Théorème de Bézout.

Théorème : a et b sont premiers entre eux si et seulement si il existe des entiers u et v tels que $au + bv = 1$.

Preuve au programme.

Exercice 47. Démontrez que deux entiers consécutifs sont toujours premiers entre eux.

L'exercice précédent illustre le fait que le théorème ne donne pas les valeurs de u et v. Voici un algorithme utilisant l'algorithme d'Euclide pour déterminer des valeurs de u et v.

20 et 27. $27 = 1\times 20 + 7$, $20 = 2\times 7 + 6$, $7 = 1\times 6 + 1$. On remonte : $1 = 7 - 1\times 6 = 7 - 1\times(20 - 2\times 7) = -1\times 20 + 3\times 7 = -1\times 20 + 3\times(27 - 1\times 20) = -4\times 20 + 3\times 27$. Remarquons qu'il n'y a pas unicité du couple : si $(-4;3)$ convient $(-4+27k, 3+20k)$ convient aussi pour $k \in \mathbb{Z}$. Remarquons également que l'on peut ainsi obtenir un couple solution de l'équation $ax + by = c$.

Si on note $u_0 = a$, $u_1 = b$ et, pour tout $n \geqslant 2$, u_n le reste de la division euclidienne de u_{n-2} par u_{n-1} et q_n est le quotient euclidien de u_n par u_{n+1}. Alors, pour tout n, $u_{n+1} =$

$a_n u_n - b_n u_{n+1}$ où (a_n) et (b_n) sont des suites récurrents d'ordre deux définies par $a_0 = 1$, $a_1 = -q_1$, $a_{n+2} = a_n - q_{n+2}a_{n+1}$ et $b_0 = q_0$, $b_1 = -(1 + q_1 q_0)$ et $b_{n+2} = b_n - q_{n+2}b_{n+1}$. Les u_i sont les restes de l'algorithme d'Euclide et les a_i et b_i sont les coefficients pour l'égalité de Bézout. Cette suite permet de programmer la recherche des coefficients de Bézout.

```
def algorithmecoupledebezout(a,b):
    "il faut que a>b"
    divisionseuclidiennes=[[a,a//b,b,a%b]]
    while divisionseuclidiennes[len(divisionseuclidiennes)-1][3]:
        a,b=b,a%b
        divisionseuclidiennes.append([a,a//b,b,a%b])
    if len(divisionseuclidiennes)>1:
        coeffu=[1,-divisionseuclidiennes[1][1]]
        coeffv=[divisionseuclidiennes[0][1],-(1+
   divisionseuclidiennes[0][1]*divisionseuclidiennes[1][1])]
    if len(divisionseuclidiennes)>2:
        for i in range(2,len(divisionseuclidiennes)-1):
            coeffu.append(coeffu[i-2]-divisionseuclidiennes[i
   ][1]*coeffu[i-1])
            coeffv.append(coeffv[i-2]-divisionseuclidiennes[i
   ][1]*coeffv[i-1])
    return divisionseuclidiennes,coeffu,coeffv
```

La dernière valeur de coeffu fois a moins la dernière valeur de coeffv fois b égale 1.

On peut avoir un point de vue matriciel.

Un programme brute force :

```
def testbezout(a,b):
    for u in range(-a,a+1):
        for v in range(-b,b+1):
            if a*u+b*v==1:
                print("ok",u,v)
```

Un programme qui utilise le fait qu'il y a une infinité de couples possibles positifs ou négatifs.

```
def bezoutaffine(a,b):
    u=0
    while (1-a*u)%b:
        u=u+1
    return u,(1-a*u)/b
```

Théorème de Bachet-Bézout : pour a et b deux entiers il existe des entiers u et v tels que : $au + bv = \text{pgcd}(a,b)$.

Preuve au programme.

Ou encore : a et b sont des diviseurs de d et il existe u et v tels que $au + bv = d$ équivaut à d est le pgcd de a et b.

Exercice 48. Déterminez les solutions du système : $\begin{cases} x + y = 5664 \\ \text{pgcd}(x,y) = 354 \end{cases}$.

Proposition : l'équation $ax+by = c$ admet des solutions si et seulement si c est un multiple du pgcd de a et de b.

Proposition : $\text{pgcd}(ka,kb) = k\text{pgcd}(a,b)$.

Exercice 49. Dits si chaque équation admet au moins une solution : $13x + 14y = 3$ et $39x - 42y = 2$.

Exercice 50. On souhaite résoudre (E) : $2x+5y = 4$. Déterminez une solution de $2x+5y = 1$ et déduisez-en une solution de (E). Justifiez que $(E) \Leftrightarrow 2(x-x_0) = 5(y_0-y)$ puis déduisez-en les solutions de (E).

VII Théorème de Gauss.

Théorème : si $a|bc$ et a est premier à b alors a divise c.
Preuve au programme.
Corollaire : si $a|c$, $b|c$ et a et b premiers entre eux alors $ab|c$.

Exercice 51. Soit $n \in \mathbb{N}$. Démontrez que $n(n^4 - 1)$ est divisible par 10.

VIII Nombres premiers.

Nombres premiers. Définition de nombre premier. Exemples liste des premiers et autres nombre. Algorithme du crible d'Ératosthène.

Exercice 52. Démontrer qu'un diviseur premier de n est inférieur à $\sqrt{n}$.

Crible d'Ératosthène

```
def cribleratosthene(n):
    premiers=[2]
    entiers=[x for x in range(premiers[len(premiers)-1],n+1)]
    while len(entiers)>1:
        for x in entiers:
            if not x%premiers[len(premiers)-1]:
                entiers.remove(x)
        premiers.append(entiers[0])
    return premiers
```

```
def eratosthene(n):
    listeatester=[k for k in range(2,n+1)]
    dernierpremier=2
    listepremiers=[2]
    while len(listeatester)>0:
        for i in listeatester:
            if i%dernierpremier==0:
                listeatester.remove(i)
                "print(listeatester)"
        dernierpremier=listeatester[0]
        "print(dernierpremier)"
        listeatester.remove(dernierpremier)
        "print(listeatester)"
        listepremiers.append(dernierpremier)
        "print(listepremiers)"
    return listepremiers
```

Proposition : leur ensemble est infini.
Preuve au programme.

IX Théorème fondamental de l'arithmétique.

Existence et unicité de la décomposition d'un entier en produit de facteurs premiers.

Déterminer les diviseurs, pgcd, ppcm avec la décomposition en facteurs premiers. Remarquons qu'il est plus simple d'utiliser la décomposition en facteurs premiers des deux nombres pour trouver pgcd et ppcm : il suffit de considérer le minimum et le maximum des valuations des facteurs premiers.

Exercice 53. Déterminez la décomposition en facteurs premiers de 78. Déduisez-en les diviseurs communs de 78 et 925 665.

X Petit théorème de Fermat.

Théorème : si p est un premier ne divisant pas n, alors $n^{p-1} \equiv 1\ [p]$.

Corollaire : si p est premier alors $^{p} \equiv n\ [p]$.

Le petit théorème de Fermat est un critère (test) de primalité. Il donne une condition nécessaire pour qu'un nombre soit premier. Ce critère reste peu efficace pour de grandes valeurs de p.

XI Déterminer les diviseurs d'un entier.

Méthode exhaustive.

Méthode avec la décomposition en facteurs premiers.

XII Déterminer le PGCD de deux entiers.

Algorithme d'Euclide.

Choisir parmi la liste des diviseurs (le plus grand commun).

Dans la décomposition en valeur premiers avec le minimum des valuations.

XIII Déterminer un inverse de $a\ [n]$ lorsque a et n sont premiers entre eux.

XIV Établir et utiliser des tests de divisibilité.

XV Étudier la primalité de certains nombres.

XVI Étudier des problèmes de chiffrements.

Détermination des racines rationnelles d'un polynôme à coefficients entiers. Lemme chinois et applications à des situations concrètes. Démonstrations du petit théorème de Fermat. Problèmes de codage (codes barres, code ISBN, clé du Rib, code Insee). Étude de tests de primalité : notion de témoin, nombres de Carmichaël. Problèmes de chiffrement (affine, Vigenère, Hill, RSA).

XVII Recherche de nombres premiers particuliers (Mersenne, Fermat).

Exercice 54. On appelle nombre de Mersenne tout qui peut s'écrire sous la forme $2^n - 1$ où $n \in \mathbb{N}^*$. On note M_n le n-ième nombre de Mersenne.

1. (a) Calculez M_1, M_2 et M_3.
   (b) On veut montrer la proposition : « si M_n est premier alors n est premier ».
      i. Montrez que : $\forall q \in \mathbb{N}^*$, $\forall x \in \mathbb{R}$, $x^q - 1 = (x-1)(1 + x + x^2 + \cdots + x^{q-1})$.
      ii. Donnez la contraposée de la proposition « si M_n est premier alors n est premier ».
      iii. Soit n un entier qui n'est pas premier. Il existe donc a et b tels que $n = a \times b$ avec a et b compris entre 2 et $n-1$. Montrez que M_n est divisible par M_a. Que pouvez-vous en déduire pour M_n ?
   (c) Calculer M_{11} puis déduisez-en que la réciproque de la proposition de la question 2 est fausse.
2. Un entier naturel est dit parfait si la somme de ses diviseurs est à son double.
   (a) Vérifiez que si 6 et 28 sont des nombres parfaits.
   (b) Soit $n \in \mathbb{N}$ tel que M_n soit premier. On note $P = 2^n M_n$. Dressez la liste de tous les diviseurs de P puis faire leur somme. Que constatez-vous ?
   (c) Déduisez-en un autre nombre parfait.

Exercice 31.

1. (a) $M_1 = 1$, $M_2 = 3$ et $M_3 = 7$.
   (b) i. En développant on observe un télescopage : $(x-1)(1 + x + x^2 + \cdots + x^{q-1}) = \ldots$.
      ii. Contraposée : « si n n'est pas premier alors M_n n'est pas premier ».
      iii. $M_n = (2a)^b - 1 = (2^a - 1)(1 + 2^a + 2^{2a} + \cdots + 2^{a(b-1)}) = M_a(1 + 2^a + 2^{2a} + \cdots + 2^{a(b-1)})$ est divisible par M_a. Ainsi si n n'est pas premier alors M_n n'est pas premier. Autrement dit : si M_n est premier alors n est premier.
   (c) $M_{11} = 2047 = 23 \times 89$ donc M_{11} n'est pas premier et pourtant 11 est premier donc la conjecture de Mersenne est fausse.
2. (a) $D(6) = \{1; 2; 3; 6\}$ $1 + 2 + 3 + 6 = 12 = 2 \times 6$ et $D(28) = \{1; 2; 4; 7; 14; 28\}$ et $1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \times 28$.
   (b) $D(2^n) = \{1; 2; 2^2; \ldots; 2^n\}$. $M_n \neq 2$ et M_n est premier donc $D(2^n M_n) = \{1; 2; 2^2; \ldots; 2^n; M_n; 2M_n$ $1 + 2 + 2^2 + \cdots + 2^n + M_n + 2M_n + 2^2 M_n + \cdots + 2^n M_n = 2^{n+1} - 1 + M_n(2^{n+1} - 1) = 2^{n+1} - 1 + (2^n - 1)(2^{n+1} - 1) = 2^{n+1} - 1 + 2^{2n+1} - 2^{n+1} - 2^n + 1 = 2^{2n+1} - 2^n = 2$ Dressez la liste de tous les diviseurs de P puis faire leur somme. Que constatez-vous ?
   (c) Déduisez-en un autre nombre parfait.

Exercice 55.

1. Que réalise l'algorithme ci-dessous.

   Demander N
   $D \leftarrow 1$
   Tant que $D^2 \leqslant N$ faire
      Si $\frac{N}{D} = \mathrm{E}\left(\frac{N}{D}\right)$ alors
         Afficher D et $\frac{N}{D}$
      D prend la valeur $D + 1$

2. Programmez cet algorithme en Python puis faites le tourner avec les nombres de Fermat $F_n = 2^{2^n} + 1$ pour $n \in [\![0,4]\!]$. Comment interpréter ces résultats.
3. Pierre de Fermat (1601-1665) a conjecturé que tous les nombres F_n étaient premiers. Qu'en pensez-vous ?
4. Dans cette question nous démontrerons que, si $m \neq n$ alors F_m et F_n sont premiers entre eux.
   (a) Montrez que pour tout entier naturel non nul p, $F_{n+p} - 1 = (F_n - 1)^{2p}$.
   (b) Déduisez-en que $F_{n+p} \equiv 2\ [F_n]$.
   (c) Concluez.
5. On note D_p l'ensemble des diviseurs premiers p_i de F_n et p_n son plus petit élément.
   (a) Montrez que si $m \neq n$ alors $p_m \neq p_n$.
   (b) Que pouvez en déduire quant à l'ensemble des nombres premiers ?

Exemples simples de codes correcteurs. Étude du système cryptographique RSA. Détermination des triplets pythagoriciens. Étude des sommes de deux carrés par les entiers de Gauss. Étude de l'équation de Pell-Fermat.

5. Théorie de graphes.

Exercice 56.