Chapitre 9

Racines de l'unité et factorisation de polynômes dans $\mathbb{C}$

Dans cet ultime chapitre portant sur les nombres complexes, nous allons approfondir l'étude de la factorisation de polynôme à coefficients complexes.

9.1 Racines n-ièmes de l'unité

Délaissons les applications géométriques de nombres complexes pour étudier de nouveau les racines d'un polynôme et les méthodes de factorisation. En particulier, dans cette partie, nous allons nous focaliser sur un sous-ensemble du cercle unité $\mathbb{U}$.

Définition 9.1.1. *Le cercle unité $\mathbb{U} \subset \mathbb{C}$ est défini par*

$$\mathbb{U} = \{z \in \mathbb{C}\,;\, |z| = 1\}.$$

Remarque. L'ensemble $\mathbb{U}$ vérifie des propriétés de stabilité par produit et quotient. Autrement dit, si $z, z' \in \mathbb{U}$ alors

$$zz' \in \mathbb{U} \quad \text{et} \quad \frac{z}{z'} \in \mathbb{U}.$$

Nous allons nous focaliser sur une partie de $\mathbb{U}$, il s'agit des **racines n-èmes de l'unité**.

Définition 9.1.2. *Soit $n \in \mathbb{N}$, une racine de l'unité est une solution de l'équation $z^n = 1$. L'ensemble des racines n-èmes de l'unité est noté $\mathbb{U}_n$.*

Exemple 9.1.1. i est une racine quatrième de l'unité puisque $i^4 = (-1)^2 = 1$. ± 1 sont des racines secondes de l'unité.

Il est naturel de se demander s'il est possible d'obtenir une description plus précise des racines de l'unité, la proposition suivante répond à cette question.

Proposition 45. *L'ensemble $\mathbb{U}_n$ des racines n-èmes de l'unité correspond à l'ensemble suivant*

$$\mathbb{U}_n = \{e^{i\frac{2k\pi}{n}} \quad \textit{pour tout} \quad 0 \leq k < n\}.$$

De plus, si $n \geq 3$, les points $z_k = e^{i\frac{2k\pi}{n}}$ forment un polygone régulier à n côtés.

Remarque. $\mathbb{U}_n$ contient exactement n éléments. D'une certaine manière nous venons d'associer à un polynôme (ici $P(z) = z^n - 1$) un ensemble ($\mathbb{U}_n$), Galois fut le premier à observer ce genre de lien et à constater que les propriétés de l'ensemble associé avait des répercussions sur l'existence de solutions d'une équation polynomiale (ici $z^n - 1 = 0$).

Démonstration. Posons $z = re^{i\theta}$ avec $r > 0$ et $\theta \in \mathbb{R}$, par identification

$$z^n = 1 \iff r^n e^{in\theta} = 1 \iff \begin{cases} r^n = 1 \\ n\theta \equiv 0[2\pi] \end{cases} \iff \begin{cases} r = 1 \\ n\theta = 2l\pi \quad \text{avec} \quad l \in \mathbb{Z} \end{cases}$$

or, en effectuant la division euclidienne de l par n, nous avons $l = nq + k$ avec $0 \leq k < n$ et $q \in \mathbb{Z}$. Ainsi,

$$\theta = q2\pi + \frac{2k\pi}{n} \iff \theta \equiv \frac{2k\pi}{n}[2\pi].$$

Ce qui termine la démonstration. □

Exemple 9.1.2.

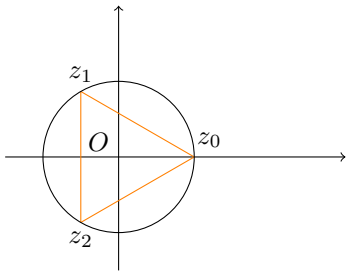
1. Traitons le cas $n = 2$. $z^2 = 1 \iff z^2 - 1 = 0 \iff (z+1)(z-1) = 0$. Les deux racines de l'unité sont $z_0 = 1$ et $z_1 = -1$.
2. Si $n = 3$, il n'est pas difficile de voir que $z_0 = 1$ est de nouveau solution. Par suite, le polynôme $P(z) = z^3 - 1$ se factorise par $z - 1$. Autrement dit, il existe $a, b, c \in \mathbb{C}$ tels que

$$z^3 - 1 = (z - 1)(az^2 + bz + c)$$

En développant et en identifiant les coefficients, nous trouvons que $a = b = c = 1$. Il ne reste plus qu'à déterminer les racines de $z \mapsto z^2 + z + 1$. Pour cela, il est possible d'utiliser Δ afin d'obtenir l'expression algébrique de z_1 et z_2. Nous pouvons également utiliser la proposition précédente pour déterminer leur expression sous forme exponentielle :

$$z_1 = e^{\frac{2i\pi}{3}} \quad \text{et} \quad z_2 = e^{\frac{4i\pi}{3}} = e^{-\frac{2i\pi}{3}}.$$

Nous obtenons alors le polygone régulier suivant :



Remarque. Souvent $e^{\frac{2i\pi}{3}}$ est noté j et $e^{\frac{4i\pi}{3}}$, j^2 ou $\bar{j}$.

Exercices à traiter : 45 page 67 ; 126 page 75 à faire à la maison ; 124,128 page 75 ; 146 page 79 en DM.

9.2 Factorisation dans $\mathbb{C}$

Lors de l'étude des racines troisième de l'unité, nous avons procédé à une **factorisation**. Ce genre d'opération est, bien entendu, valable pour des polynômes de degrés plus élevé. Voyons comment généraliser la notion de polynôme vue en classe de 1ère.

Définition 9.2.1. *1. Dans $\mathbb{C}$, un polynôme non nul, à **coefficients réels**, P de degré n est de la forme*

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$$

avec $a_i \in \mathbb{R}$ pour tout $i = 1, \ldots, n$ et $a_n \neq 0$.

2. Soit P un polynôme de degré n. Nous dirons que $a \in \mathbb{C}$ est une racine de P si $P(a) = 0$.

Remarque. 1. Bien entendu, il est possible de généraliser ceci en supposant que les coefficients a_i soient complexes.

2. Pour généraliser la notion de racine à des espaces plus abstraits (l'anneau euclidien $\mathbb{K}[X]$ des polynômes d'indéterminée X à coefficients dans un corps commutatif $\mathbb{K}$ par exemple). Nous dirons que $a \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$ si

$$X - a \quad \text{divise} \quad P.$$

Autrement dit, il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$P(X) = (X - a)Q(X) \quad \text{et} \quad 0 \leq \deg(Q) = \deg(P) - 1.$$

Ceci sous-entendant que le reste R de la division euclidienne de P par $X - a$ est nul. Bien entendu, ceci nous entraîne beaucoup plus loin que ce qui est inscrit dans le programme de terminale. Ces notions sont généralement étudiées durant les premières années d'études post-bac. Il s'agit de généraliser la notion de divisibilité euclidienne (étudiée dans $\mathbb{Z}$) aux espaces de polynômes.

Voyons un exemple.

Exemple 9.2.1. $P(z) = 5z^3 - 4z^2 + \frac{1}{2}z$ est un polynôme de degré 3.

Nous allons à présent constater qu'**étant donné une racine** a d'un polynôme, il est possible de le **factoriser par** $z - a$. De plus nous allons obtenir des informations sur le nombre de racines possédées par un polynôme de degré n.

Proposition 46. *Soit P un polynôme de degré n et $a \in \mathbb{C}$ l'une de ses racines. Alors P se factorise par $(z - a)$, c'est-à-dire qu'il existe un polynôme Q de degré **strictement inférieur à** n tel que*

$$P(z) = (z - a)Q(z).$$

En particulier, pour tout $z \in \mathbb{C}$, nous avons

$$z^n - a^n = (z - a)(z^{n-1} + az^{n-2} + \ldots + a^{n-2}z + an - 1).$$

Remarque.

Voyons comment procéder sur un exemple.

Exemple 9.2.2. Soit $P(z) = z^3 - 6z^2 + 13z - 10$. Il n'est pas difficile de vérifier que 2 est une racine de P, il existe donc $Q(z) = az^2 + bz + c$ un polynôme de degré (au plus) 2 tel que

$$P(z) = (z-2)(az^2 + bz + c).$$

Pour déterminer les nombres complexes a, b et c, il suffit de developper le membre de droite pour ensuite procéder à une identification des coefficients. Ici, nous avons

$$(z-2)(az^2 + bz + c) = az^3 + (b-2a)z^2 + (c-2b)z - 2c.$$

Nous devons alors résoudre le système

$$\begin{cases} a = 1 \\ b - 2a = -6 \\ c - 2b = 12 \\ -2c = -10 \end{cases} \iff \begin{cases} a = 1 \\ b = -4 \\ c = 5. \end{cases}$$

En résumé, $P(z) = (z-2)(z^2 - 4z + 5)$.

Le théorème fondamental suivant concerne le nombre de racines d'un polynôme de degré n.

Théorème 47 (D'Alembert-Gauss)**.** *Soit P un polynôme de degré n à coefficients complexes. Alors P admet exactement n racines.*

Remarque.
1. Ce résultat est souvent désigné sous le nom *théorème fondamental de l'algèbre*, il en existe de nombreuses démonstrations. Avec les outils du lycée, il n'est pas possible de le démontrer. Cependant il est possible de démontrer par récurrence sur n qu'un polynôme de degré n admet *au plus* n racines.
2. La terminologie savante (à propos du théorème de D'Alembert-Gauss) s'énonce comme suit :

   $\mathbb{C}$ **est algébriquement clos**.

   Autrement dit, tout polynômes P à coefficients complexes peut se factoriser en produit de polynômes de degré 1 (nous dirons que P est *scindé* sur $\mathbb{C}$) :

   $$P(z) = a_n(z - z_1)\dots(z - z_n).$$

   avec a_n le coefficient dominant de P et $z_1, \dots, z_n$ les n racines de P (celles-ci ne sont pas forcément toutes distinctes). Observons en passant que $\mathbb{R}$ n'est pas algébriquement clos puisque le polynôme $P(x) = x^2 + 1$ n'admet aucune racine de $\mathbb{R}$ (ses racines $z_1 = i$ et $z_2 = -i$ sont des nombres imaginaires purs).

Comme cela a été abordé en classe de 1ère, il est possible d'obtenir un lien entre les coefficients d'un polynôme et ses racines.

Proposition 48 (Formules de Viète)**.** *Soit $n \in \mathbb{N}_*$ et $P(z) = \sum_{k=0}^{n} a_k z^k$ un polynôme de degré n à coefficients réels (i.e. $a_k \in \mathbb{R}$ pour tout $k \in \{0; \dots; n\}$ et $a_n \neq 0$). Alors :*

- *la somme de toutes ses racines vaut $-\frac{a_{n-1}}{a_n}$.*
- *le produit de toutes ses racines vaut $(-1)^n \frac{a_0}{a_n}$.*

Remarque. Il se trouve que les formules de Viète sont plus nombreuses que cela. Celles exposées ci-dessus sont les plus utilisées.

Voyons ce que cela donne sur un exemple.

Exemple 9.2.3. Soient $z_1 = 1 + 2i$ et $z_2 = 1 - 2i$ les racines d'un polynôme unitaire P de degré 2. Puisque

$$z_1 + z_2 = 2 \quad ; \quad z_1 z_2 = z_1 \bar{z_1} = 1^2 + 2^2 = 5$$

alors z_1 et z_2 sont les racines du polynôme

$$P(z) = z^2 - 2z + 5.$$

Exercices à traiter : 45, 46 page 35 ; 47 et 49 page 35 à la maison ; 51 page 35 ; 114 page 41 ; 125 page 42 (facultatif) ; 149 page 46 en DM.

Chapitre 10

Nombres premiers

Après avoir étudier l'ensemble des entiers relatifs à l'aide de la division euclidienne, nous allons approfondir nos connaissances de cet ensemble grâce à la notion de nombres premiers.

10.1 L'ensemble des nombres premiers

Nous avons vu plutôt le fait que deux nombres relatifs pouvaient être premier entre eux. Nous avons notamment vu (via le théorème de Bézout ou de Gauss) que cela avait des conséquences intéressantes. Plus généralement, cela nous mène à étudier la notion suivante.

Définition 10.1.1. *Un entier naturel est un* ***nombre premier*** *s'il admet exactement deux diviseurs positifs :* 1 *et lui-même.*

Remarque. Ainsi, d'après la définition, 1 n'est pas premier (puisqu'il admet un seul diviseur positif) et 0 n'est pas premier également.

Savoir si un nombre est premier est quelque chose de très complexe. Pourtant, en imitant Eratosthène nous pouvons établir la liste des nombres premiers compris entre 0 et 100.

Pour cela, dans la liste ci-dessous, nous allons pouvoir supprimer les multiples de 2, de 3, de 5,... à l'aide des tables de multiplications pour déterminer la liste voulue (donnée ci-dessous).

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

FIGURE 10.1 – Crible d'Eratosthène

Bien qu'il existe des critères beaucoup plus complexes, voici une condition permettant de savoir si un nombre est premier ou non. Bien entendu, cette méthode n'est intéressante que lorsque le nombre n en question n'est pas trop grand.

Proposition 49 (critère de primalité)**.** *Soit $n \geq 4$ un entier. Si n n'est divisible par aucun nombre premier p tel que $2 \leq p \leq \sqrt{n}$ alors n est premier.*

Démonstration. Pour démontrer ceci nous allons procéder par contraposée. Rappelons à ce propos qu'un énoncé

$$A \Rightarrow B$$

s'écrit de manière équivalente (il s'agit de **la contraposée** de l'énoncé) sous la forme

$$\text{non}\, B \Rightarrow \text{non}\, A.$$

Ce procédé est souvent utile pour démontrer plus simplement certaines affirmations. Ici

$\boldsymbol{A}$: n n'est divisible par aucun nombre premier p tel que $2 \leq p \leq \sqrt{n}$ et $\boldsymbol{B}$: n est premier.

Nous devons donc montrer que si « *n n'est pas premier* » (non B) alors « *n admet au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$* » (non A).

Soit $n \geq 4$ un entier non premier et notons p **le plus petit de ses diviseurs** supérieurs à 2 et différent de n (ce nombre existe : puisque n n'est pas premier, il admet au moins un diviseur

différent de 1 et de lui-même). Procédons par l'absurde et supposons que ce diviseur p **n'est pas premier.** Il admet alors un diviseur d tel que

$$2 \leq d < p.$$

Dans ce cas nous avons, par construction, $d|p$ et $p|n$. D'où $d|n$. Ceci est absurde car cela **contredit le caractère minimal de** p. En conclusion, p est bien un nombre premier.

Montrons à présent que $2 \leq p \leq \sqrt{n}$: puisque $p|n$, il existe $k \in \mathbb{N}$ tel que

$$n = pk \quad \text{avec} \quad 2 \leq p \leq k.$$

En particulier, $p^2 \leq pk = n$. Par suite, $p \leq \sqrt{n}$. □

Voyons une application de ce résultat.

Exemple 10.1.1.
1. 133 est-il un nombre premier ? Les nombres premiers inférieurs à $\sqrt{133}$ sont $2, 3, 5, 7, 11$. De plus, 133 n'est pas divisible par $2, 3$ et 5 mais $133 = 7 \times 19$. Alors, par définition, 133 n'est pas premier.
2. Même question pour 547, nous devons regarder si 547 est divisible par $2, 3, 5, 7, 11, 13, 17, 19$ et 23. Ce n'est pas le cas donc, d'après la proposition précédente, 547 est premier.

Il serait intéressant d'en apprendre plus sur les nombres premiers. Par exemple, combien y-a-t-il de nombres premiers ?

Théorème 50. *Il existe une infinité de nombre premiers.*

Démonstration. Raisonnons par l'absurde et supposons qu'il existe un nombre fini de nombres premiers que nous numérotons $\mathcal{P} = \{p_1, p_2 \ldots, p_N\}$ pour un certain $N \in \mathbb{N}$. Considérons ensuite le nombre $a = p_1 p_2 \ldots p_N + 1$, nous allons montrer que ce nombre est premier. Cela contredira notre hypothèse de départ puisqu'il ne faisait pas parti de notre liste $\mathcal{P}$.

Puisque $a \geq 2$, nous savons qu'il admet au moins un diviseur premier $p_i \in \mathcal{P}$ (avec $i \in \{1; \ldots; N\}$). Ce nombre premier divise a mais il divise aussi le produit $p_1 \times p_2 \times \ldots \times p_N$. Par suite, en utilisant un résultat vu plus tôt dans l'année, p_i divise donc toute combinaison linéaire de a et de $p_1 \times \ldots \times p_N$ deux nombres. En particulier, p_i divise

$$a - p_1 \ldots p_N = 1$$

ce qui est absurde puisque les seules diviseurs de 1 sont 1 et -1 qui ne sont pas des nombres premiers. L'ensemble des nombres premiers $\mathcal{P}$ est donc infini.

□

Exercices à traiter : 23 page 156 ; 51 page 158 ; 52 page 159.

10.2 Décomposition d'un entier en produit de facteurs premiers

Observons le fait suivant :

$$1008 = 2^4 \times 3^2 \times 7$$

Ce nombre a été décomposé en produit (de puissances) de nombres premiers. Il est naturel de s'interroger :

- est-il toujours possible de faire cela ?
- cette écriture est-elle unique ?

Il se trouve que dans $\mathbb{Z}$ la réponse est oui (en termes savants, nous dirons que $\mathbb{Z}$ est un *anneau commutatif factoriel*) : **tout entier se décompose en un produit unique** (à permutation près) **de nombres premiers.** Nous comprenons alors pourquoi les nombres premiers jouent un rôle primordial dans $\mathbb{Z}$, il s'agit **des briques élémentaires** qui permettent de construire tous les autres nombres. C'est l'objet du théorème suivant.

Théorème 51 (Décomposition en facteurs premiers)**.** *Si $n \geq 2$, il existe des nombres premiers distincts $p_1, \ldots, p_k$ et des entiers non nuls $\alpha_1, \ldots, \alpha_k$ tels que*

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}.$$

De plus cette ***décomposition est unique à permutation des facteurs près****.*

Cette décomposition permet d'identifier facilement les diviseurs d'un entier.

Proposition 52. *Soit $n \geq 2$ dont la décomposition en facteurs premiers est $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$. Les diviseurs d de n sont alors précisément de la forme*

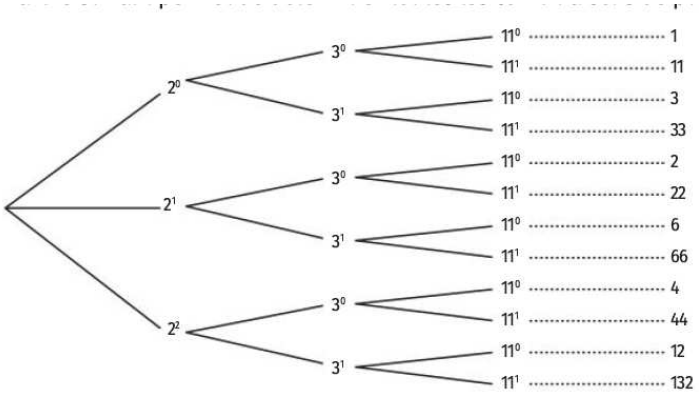
$$d = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_k^{\beta_k} \quad \textit{avec} \quad 0 \leq \beta_i \leq \alpha_i \quad \textit{pour tout} \quad i \in \{1, \ldots, k\}.$$

Voyons sur un exemple.

Exemple 10.2.1. Si $n = 132 = 2^2 \times 3 \times 11$ alors ses diviseurs sont de la forme

$$d = 2^{\beta_1} \times 3^{\beta_2} \times 11^{\beta_3} \quad \text{avec} \quad 0 \leq \beta_1 \leq 2, \quad 0 \leq \beta_2 \leq 1 \quad \text{et} \quad 0 \leq \beta_3 \leq 1.$$

Pour visualiser cela plus facilement, il est possible de faire un arbre. Voyons ce que nous obtenons dans notre exemple



Les décompositions en produits de nombres premiers permet aussi de trouver facilement le $PGCD$ ou le $PPCM$ de deux entiers.

Proposition 53. *Soient $m, n \geq 2$ tels que*

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k} \quad et \quad m = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_k^{\beta_k}$$

où $\alpha_i, \beta_i \in \mathbb{N}$ pour tout $i = 1, \ldots, k$, alors

- $PGCD(m; n) = p_1^{\min(\alpha_1;\beta_1)} \times p_2^{\min(\alpha_2;\beta_2)} \times \ldots \times p_k^{\min(\alpha_k;\beta_k)}$;
- $PPCM(m; n) = p_1^{\max(\alpha_1;\beta_1)} \times p_2^{\max(\alpha_2;\beta_2)} \times \ldots \times p_k^{\max(\alpha_k;\beta_k)}$.

Remarque. A toutes fins utiles, rappelons que le $PPCM(m; n)$ correspond au **plus petit des multiples (positifs) communs de m et n**. En général, l'algorithme d'Euclide reste le moyen le plus efficace pour déterminer le PGCD de deux nombres.

Exemple 10.2.2. $24 = 2^3 \times 3^1 \times 7^0$ et $84 = 2^2 \times 3^1 \times 7^1$. Par conséquent,

$$PGCD(24; 84) = 2^2 \times 3 \times 7^0 = 12 \quad \text{et} \quad PPCM(24; 84) = 2^3 \times 3^1 \times 7^1 = 168.$$

Exercices à traiter : 26 page 156 ; 31 page 156.

10.3 Théorème de Fermat

Nous avons déjà évoqué (rapidement) en introduction du chapitre 2, l'histoire du **grand théorème** de Fermat. En particulier, nous avons mentionné la difficulté d'établir une démonstration rigoureuse de l'affirmation de Fermat (cela a permis à A.Wiles d'obtenir une médaille Fields). A notre niveau, dans cette section, nous allons plutôt présenter le *petit* théorème de Fermat. Celui-ci donne un résultat intéressant concernant les congruences modulo un nombre premier.

Théorème 54 (Fermat)**.** *Si p est un nombre premier et si a est un entier non divisible par p alors*

$$a^{p-1} \equiv 1[p].$$

Démonstration. La démonstration s'effectue en deux temps. Tout d'abord, il faut établir le lemme suivant ; la démonstration de ce lemme fera l'objet d'un DM.

Lemme 55. *Si p est un nombre premier alors, pour tout nombre entier a, $a^p \equiv a[p]$.*

En supposant ce résultat démontré, il n'est plus difficile d'achever la démonstration du théorème de Fermat. En effet, d'après le lemme 55

$$a^p - a \equiv 0\,[p] \quad \Longleftrightarrow \quad p \quad \text{divise} \quad a^p - a.$$

En outre, $a^p - a = a(a^{p-1} - 1)$. D'après ce qui précède, nous savons donc que $p|a(a^{p-1} - 1)$. Or, puisque p est premier et ne divise pas a (par hypothèse), p est donc premier avec a. Par suite, d'après le théorème de Gauss,

$$p|a^{p-1} - 1 \quad \Longleftrightarrow \quad a^{p-1} - 1 \equiv 0[p] \quad \Longleftrightarrow \quad a^{p-1} \equiv 1[p].$$

□

Remarque. Remarquons en passant que le théorème de Fermat fournit un résultat plus fort que le précédent lemme technique 55 : si $a^{p-1} \equiv 1[p]$ alors $a^p \equiv a[p]$.

Voyons deux applications de ceci.

Exemple 10.3.1. Résolvons (E) : $5x \equiv 28[31]$.

1. Puisque 31 est un nombre premier et 5 et 31 sont premiers entre eux, nous savons (d'après le théorème de Fermat) que $5^{30} \equiv 1[31]$.
2. C'est pourquoi $28 \times 5^{30} \equiv 28 \times 1[31] \quad \Longleftrightarrow \quad 5 \times (28 \times 5^{29}) = 28[31]$. Autrement dit, 28×5^{29} est une solution particulière de (E).
3. Simplifions 28×5^{29} modulo 31. Puisque $5^3 \equiv 1[31]$ et que $29 = 9 \times 3 + 2$,nous en déduisons que

   $$5^{29} \equiv (5^3)^9 \times 2^2 \equiv 5^2[31].$$

   D'où, $28 \times 5^{29} \equiv 28 \times 5^2 \equiv 700 \equiv 18[31]$. Autrement dit, 18 est une solution particulière de (E).
4. Déterminons l'ensemble des solutions de (E) à partir de ce qui précède. Observons que x est solution de (E) si et seulement si

   $$5x \equiv 28[31] \quad \Longleftrightarrow \quad 5x \equiv 5 \times 18[31] \quad \text{(d'après ce qui précède)} \quad \Longleftrightarrow \quad 5(x-18) \equiv 0[31].$$

   Ainsi, $31|5(x-18)$ or 31 et 5 sont premiers entre eux. Le théorème de Gauss nous assure alors que $31|(x-18) \quad \Longleftrightarrow \quad x - 18 = 31k$ avec $k \in \mathbb{Z}$. Les solutions de (E) sont donc de la forme

   $$x = 18 + 31k.$$

Exemple 10.3.2. Démontrons que pour tout entier naturel n,

$$n^{13} - n \quad \text{est divisible par} \quad 26.$$

L'idée est d'appliquer judicieusement le petit théorème de Fermat, pour cela il est nécessaire de trouver des nombres premiers. Observons à ce propos que $26 = 2 \times 13$ et que 2 et 13 sont des nombres premiers. A présent, nous allons chercher à montrer que $2|n^{13} - n$ et que $13|n^{13} - n$ pour ensuite utiliser une conséquence du théorème de Gauss.

1. Tout d'abord, remarquons que le théorème de Fermat implique (cf. Lemme 55) que 13 divise $n^{13} - n$.
2. A présent, travaillons modulo 2 pour montrer que $2|n^{13} - n$:

   - si $n \equiv 0[2]$ alors $n^{13} - n \equiv 0[2]$.
   - si $n \equiv 1[2]$ alors $n^{13} \equiv 1[2]$ et donc $n^{13} - n \equiv 0[2]$.

   En conclusion, par disjonction de cas, nous avons bien montré que $2|n^{13} - n$.
3. Enfin, puisque 2 et 13 sont premiers entre eux, que $2|n^{13} - n$ et $13|n^{13} - n$ alors, d'après une conséquence du théorème de Gauss, $26|n^{13} - n$.

Exercices à traiter : 71 page 161 ; 74, 76, 77 page 161 ; 78 page 162 en DM ou 80 et 82 page 162-163.

Pour conclure ce cours, quoi de mieux que la présentation d'un problème extraordinaire qui dresse un pont entre les nombres premiers et le monde des complexes via la fonction Dzéta de Riemann ?

https://www.arte.tv/fr/videos/097454-011-A/voyages-au-pays-des-maths/.