Quelques résultats sur les polynômes à coefficients entiers

Les notations suivantes sont valables dans tout le devoir :

- Étant donné deux entiers $m \in \mathbb{N}^*$ et $k \in \mathbb{Z}$, on notera $[k]_m$ la classe de k dans $\mathbb{Z}/m\mathbb{Z}$.
- Étant donné un nombre premier p, on notera $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.
- Étant donné un anneau commutatif A (en pratique $A = \mathbb{Z}$ ou $A = \mathbb{Z}/m\mathbb{Z}$), on utilisera la notation A[X] pour les polynômes à coefficients dans A.
  On pourra utiliser sans démonstration que A[X] est un anneau commutatif et que la réduction modulo m, coefficient par coefficient, fournit un morphisme d'anneaux $\mathbb{Z}[X] \to (\mathbb{Z}/m\mathbb{Z})[X]$.

A. Généralités sur les polynômes cyclotomiques

Soit $n \in \mathbb{N}^*$.
On notera $\zeta_n = \exp\left(i\frac{2\pi}{n}\right)$, de telle sorte que $\mathbb{U}_n = \{\zeta_n^k \,|\, k \in \mathbb{Z}\}$.

1. Soit $\omega \in \mathbb{U}_n$. Montrer que les assertions suivantes sont équivalentes :
   (i) Pour tout $d \in [\![1, n-1]\!]$, $\omega \notin \mathbb{U}_d$.
   (ii) Pour tout $d \in [\![1, n-1]\!]$ divisant n, $\omega \notin \mathbb{U}_d$.
   (iii) Il existe $k \in [\![0, n-1]\!]$ premier avec n tel que $\omega = \zeta_n^k$.

   On notera $\zeta = \zeta_n$ pour simplifier.
   - *L'implication (i) $\Rightarrow$ (ii) est tautologique.*
   - *Supposons (ii). On sait pouvoir trouver $k \in [\![0, n-1]\!]$ tel que $\omega = \zeta_n^k$. Posons $m = k \wedge n$ et supposons par l'absurde $m > 1$.*
     On a alors (en faisant attention à n'écrire que des exposants entiers) $\omega^{n/m} = \zeta^{kn/m} = (\zeta^n)^{k/m} = 1$, donc $\omega \in \mathbb{U}_{n/m}$, ce qui contredit (ii). Ainsi, k est premier avec n, ce qui montre (iii).
   - *Supposons (iii) et fixons k premier avec n tel que $\omega = \zeta^k$.*
     Soit $d \in \mathbb{N}^*$ tel que $\omega \in \mathbb{U}_d$. En passant aux arguments, l'égalité $\omega^d = 1$ entraîne $n \mid kd$. Comme k est premier avec n, on en déduit $n \mid d$. En particulier, $d \notin [\![1, n-1]\!]$.

   Quand ces assertions sont vraies, on dit que ω est une *racine primitive n-ième de l'unité*. L'ensemble des racines primitives n-ièmes de l'unité sera noté $\widehat{\mathbb{U}}_n$.

On définit maintenant le *n-ième polynôme cyclotomique* $\Phi_n = \prod_{\omega \in \widehat{\mathbb{U}}_n} (X - \omega)$.

2. Déterminer Φ_p, pour tout nombre premier p, les polynômes Φ_n pour $n \in [\![1, 8]\!]$ et Φ_{12}.

   - *Pour p premier, la définition des racines primitives de l'unité montre que $\widehat{\mathbb{U}}_p = \mathbb{U}_p \setminus \{1\}$, si bien qu'en passant par $\mathbb{C}(X)$ pour plus de commodité d'écriture :*

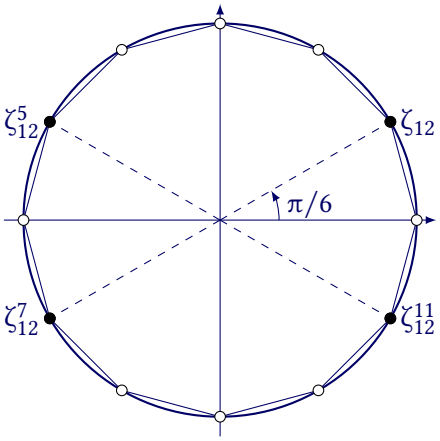
$$\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

- *On obtient explicitement les polynômes suivants :*

$$\begin{aligned}
\Phi_1 &= X - 1\\
\Phi_2 &= X + 1\\
\Phi_3 &= (X - j)(X - \bar{j})\\
&= X^2 + X + 1\\
\Phi_4 &= (X - i)(X + i)\\
&= X^2 + 1\\
\Phi_5 &= X^4 + X^3 + X^2 + X + 1\\
\Phi_6 &= (X - \zeta_6)(X - \zeta_6^5)\\
&= X^2 - X + 1\\
\Phi_7 &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1\\
\Phi_8 &= \underbrace{(X - \zeta_8)(X - \zeta_8^7)}_{=X^2-\sqrt{2}X+1}\underbrace{(X - \zeta_8^3)(X - \zeta_8^5)}_{=X^2+\sqrt{2}X+1}\\
&= X^4 + 1.
\end{aligned}$$

  (Contrairement à ce que ces exemples pourraient suggérer, les polynômes cyclotomiques peuvent avoir des coefficients autres que 0 et ± 1, mais le premier exemple est Φ_{105}. En revanche, on verra dans la suite du devoir qu'ils sont toujours à coefficients entiers.)
- *Enfin, en détaillant un peu plus les calculs :*

$$\begin{aligned}
\Phi_{12} &= \underbrace{(X - \zeta_{12})(X - \zeta_{12}^{11})}_{\text{racines conjuguées}}\underbrace{(X - \zeta_{12}^5)(X - \zeta_{12}^7)}_{\text{racines conjuguées}}\\
&= (X^2 - \sqrt{3}X + 1)(X^2 + \sqrt{3}X + 1) \qquad \text{car } \cos\frac{2\pi}{12} = \frac{\sqrt{3}}{2}\\
&= (X^2 + 1)^2 - (\sqrt{3}X)^2\\
&= X^4 - X^2 + 1.
\end{aligned}$$



$\mathbb{U}_{12}$ *et* $\widehat{\mathbb{U}}_{12}$

3. Montrer $X^n - 1 = \prod_{d|n} \Phi_d$, où le produit porte sur les diviseurs positifs de n.

   Les deux polynômes sont unitaires et complexes, donc ils sont égaux si et seulement s'ils ont les mêmes racines, avec les mêmes multiplicités. Autrement dit, il s'agit de montrer $\mathbb{U}_n = \bigsqcup_{d|n} \widehat{\mathbb{U}}_d$.

   - *Soit $\omega \in \mathbb{U}_n$. Soit $d \in [\![1, n]\!]$ le plus petit diviseur de n tel que $\omega \in \mathbb{U}_d$. On a alors $\omega \in \widehat{\mathbb{U}}_d$: en effet, si ce n'était pas le cas, la définition (ii) forcerait l'existence d'un diviseur strict δ de d tel que $\omega \in \mathbb{U}_\delta$. Mais dans ce cas, δ serait aussi un diviseur de n, ce qui contredit la minimalité de d.*

Cela montre $\mathbb{U}_n \subseteq \bigcup_{d|n} \widehat{\mathbb{U}}_d$.

- *Soit* d_1 *et* d_2 *deux diviseurs différents de* n*, et montrons* $\widehat{\mathbb{U}}_{d_1} \cap \widehat{\mathbb{U}}_{d_2} = \emptyset$*. Quitte à les échanger, on suppose* $d_1 < d_2$*. Tout élément de* $\widehat{\mathbb{U}}_{d_1}$ *est alors élément de* $\mathbb{U}_{d_1}$*. D'après la définition (i), il ne saurait être élément de* $\widehat{\mathbb{U}}_{d_2}$*.*
- *Enfin, pour tout* $d \mid n$*, les inclusions* $\widehat{\mathbb{U}}_d \subseteq \mathbb{U}_d \subseteq \mathbb{U}_n$ *sont essentiellement évidentes, et elles montrent l'inclusion réciproque.*

4. Soit p un nombre premier et $k \in \mathbb{N}^*$. Montrer $\Phi_{p^k} = \Phi_p(X^{p^{k-1}})$.

Les diviseurs de p^k *forment une chaîne* $1 \mid p \mid p^2 \mid \cdots \mid p^{k-1} \mid p^k$*.*
D'après la définition (ii), on en déduit que $\widehat{\mathbb{U}}_{p^k} = \mathbb{U}_{p^k} \setminus \mathbb{U}_{p^{k-1}}$*. En passant là encore dans* $\mathbb{C}(X)$*, on en déduit*

$$\Phi_{p^k} = \frac{X^{p^k}-1}{X^{p^{k-1}}-1} = 1 + X^{p^{k-1}} + \cdots + X^{(p-1)p^{k-1}} = \Phi_p(X^{p^{k-1}}).$$

5. Calculer $\Phi_n(1)$.

Pour tout $n \geq 1$*, on note* $\mathrm{P}(n)$ *l'assertion*

$$\Phi_n(1) = \begin{cases} 0 & \text{si } n = 1 \\ p & \text{s'il existe } k \geq 1 \text{ et } p \text{ premier tels que } n = p^k \\ 1 & \text{sinon.} \end{cases}$$

Montrons $\forall n \geq 1, \mathrm{P}(n)$ *par récurrence forte.*

Initialisation. *On constate que* $\Phi_1(1) = 0$*, ce qui montre* $\mathrm{P}(1)$*.*

Hérédité. *Soit* $n \geq 2$ *tel que* $\forall m \in [\![1, n-1]\!], \mathrm{P}(m)$*. Montrons* $\mathrm{P}(n)$*. On distingue plusieurs cas :*

- *S'il existe* p *premier et* $k \geq 1$ *tels que* $n = p^k$*, on a* $\Phi_n = \Phi_p(X^{p^{k-1}})$*, donc* $\Phi_n(1) = \Phi_p(1) = 1^0 + 1^1 + 1^2 + \cdots + 1^{p-1} = p$*.*
- *Sinon, on peut trouver* $r \geq 2$*,* $p_1, \ldots, p_r$ *premiers distincts et* $\alpha_1, \ldots, \alpha_r \in \mathbb{N}^*$ *tels que* $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$*. En simplifiant de part et d'autre par* $X - 1$ *(ce qui est possible car* $\mathbb{C}[X]$ *est intègre) la relation* $X^n - 1 = \prod_{d|n} \Phi_d$ *puis en évaluant en* 1*, on obtient*

$$\sum_{k=0}^{n-1} X^k = \prod_{\substack{d|n \\ d>1}} \Phi_d \qquad \text{donc} \qquad n = \prod_{\substack{d|n \\ d>1}} \Phi_d(1) = \Phi_n(1) \times \prod_{\substack{d|n \\ 1<d<n}} \Phi_d(1).$$

Mais, d'après l'hypothèse de récurrence, ce dernier produit s'effondre puisque seuls y contribuent les diviseurs stricts de n *qui sont des puissances de nombres premiers. Ainsi,*

$$\prod_{\substack{d|n \\ 1<d<n}} \Phi_d(1) = \prod_{j=1}^{r} \prod_{k=1}^{\alpha_j} \underbrace{\Phi_{p_j^k}(1)}_{=p_j} = \prod_{j=1}^{r} p_j^{\alpha_j} = n.$$

La relation précédente s'écrit donc $n = \Phi_n(1) \times n$*, d'où* $\Phi_n(1) = 1$*.*

Tous les cas ayant été traités, on a montré $\mathrm{P}(n)$*, ce qui clôt la récurrence.*

B. Contenu et lemme de Gauss (1801)

Un polynôme non nul à coefficients entiers sera dit *primitif* si ses coefficients sont premiers entre eux dans leur ensemble. On note $\mathbb{Z}[X]_{\text{prim}}$ l'ensemble des polynômes primitifs.

6. Soit K un corps. Montrer que l'anneau K[X] est intègre.

   Par contraposée, il s'agit de montrer que si $P, Q \in K[X]$ *sont non nuls, alors* $PQ \neq 0$. *Soit donc* $P, Q \in K[X]$ *et notons* $n = \deg P$, $m = \deg Q$. *On refait pour ainsi dire la démonstration de* $\deg(PQ) = \deg P + \deg Q$ *:*

   $$\operatorname{coeff}_{n+m}(PQ) = \sum_{k=0}^{n} \operatorname{coeff}_k(P) \operatorname{coeff}_{n+m-k}(Q) = \operatorname{coeff}_n(P) \operatorname{coeff}_m(Q) \neq 0,$$

   car la somme s'effondre : les indices $k < n$ *ne contribuent pas car* $n+m-k > m$. *On remarque d'ailleurs que la même démonstration donne que si* A *est un anneau intègre, alors* A[X] *est intègre. (Par récurrence, on en déduit que l'anneau* $K[X_1, \dots, X_n]$ *des polynômes en n variables est intègre, ce qui peut servir à l'occasion.)*

7. Soit $P \in \mathbb{Q}[X]$ non nul. Montrer qu'il existe un unique couple $(c, \tilde{P}) \in \mathbb{Q}_+^* \times \mathbb{Z}[X]_{\text{prim}}$ tel que $P = c\tilde{P}$.

   On va utiliser intensément le fait[1] *que pour* $n+1$ *entiers* $x_0, x_1, \dots, x_n$ *non tous nuls et un facteur* $k \in \mathbb{N}^*$, *on a* $\operatorname{pgcd}(kx_0, \dots, kx_n) = k \operatorname{pgcd}(x_0, \dots, x_n)$.

   Existence. *En réduisant au même dénominateur les coefficients de* P, *on trouve d'abord un entier* $N \in \mathbb{N}^*$ *tel que* $NP \in \mathbb{Z}[X]$. *Notons* $(a_i)_{i=0}^n$ *la famille de ses coefficients, si bien que* $NP = \sum_{k=0}^{n} a_k X^k$. *Posons* $d = \operatorname{pgcd}(a_0, a_1, \dots, a_n)$, *qui est bien défini car les coefficients de* P *ne sont pas tous nuls (sinon,* $NP = 0$, *ce qui contredit la non-nullité de* P*). On a donc obtenu la décomposition* $P = \underbrace{\frac{d}{N}}_{\in \widetilde{\mathbb{Q}}_+^*} \underbrace{\sum_{k=0}^{n} \frac{a_k}{d} X^k}_{=:\tilde{P} \in \mathbb{Z}[X]}$.

   Reste à montrer $\tilde{P} \in \mathbb{Z}[X]_{\text{prim}}$. *D'après la propriété rappelée, on a l'égalité*

   $$d = \operatorname{pgcd}(a_0, \dots, a_n) = d \operatorname{pgcd}\left(\frac{a_0}{d}, \dots, \frac{a_n}{d}\right),$$

   si bien que $\operatorname{pgcd}\left(\frac{a_0}{d}, \dots, \frac{a_n}{d}\right) = 1$ *: le polynôme* $\tilde{P}$ *est primitif.*

   Unicité. *Soit* $c_1, c_2 \in \mathbb{Q}_+^*$ *et* $\tilde{P}_1, \tilde{P}_2 \in \mathbb{Z}[X]_{\text{prim}}$ *tels que* $P = c_1\tilde{P}_1 = c_2\tilde{P}_2$. *On écrit* $c_1 = \frac{a_1}{b_1}$ *et* $c_2 = \frac{a_2}{b_2}$, *avec* $a_1, b_1, a_2, b_2 \in \mathbb{N}^*$ *(il n'est même pas nécessaire que ces écritures soient irréductibles).*
   On en déduit l'égalité $a_1b_2\tilde{P}_1 = a_2b_1\tilde{P}_2$ *entre polynômes de* $\mathbb{Z}[X]$. *En utilisant la primitivité de* $\tilde{P}_1$ *et la formule rappelée au début de la question, le PGCD des coefficients de ce polynôme est*

   $$a_1b_2 \operatorname{pgcd}(\operatorname{coeff}_0(\tilde{P}_1), \dots, \operatorname{coeff}_n(\tilde{P}_1)) = a_1b_2$$

   mais aussi, de manière symétrique, a_2b_1. *Ainsi,* $a_1b_2 = a_2b_1$, *si bien que* $c_1 = \frac{a_1}{b_1} = \frac{a_2}{b_2} = c_2$.

   On en déduit que $\tilde{P}_1 = \frac{1}{c_1}P = \frac{1}{c_2}P = \tilde{P}_2$.

   Bonne question. *Voyez-vous où l'on a utilisé la positivité de* c_1 *et* c_2 *dans cette démonstration ?*

Ce nombre $c \in \mathbb{Q}_+^*$ sera noté $c(P)$ et appelé le *contenu* du polynôme P.

8. Soit $P \in \mathbb{Q}[X]$ non nul. Montrer que $P \in \mathbb{Z}[X]$ si et seulement si $c(P) \in \mathbb{N}^*$.

   - *Si* $P \in \mathbb{Z}[X]$, *on peut noter* $d \in \mathbb{N}^*$ *le PGCD des coefficients de* P, *si bien que le polynôme* $\tilde{P} = \frac{1}{d}P$ *est primitif. La décomposition de la question précédente est alors* $P = d\tilde{P}$, *si bien que* $c(P) = d \in \mathbb{N}^*$.

1. (Presque) du cours. En tout cas, la version pour $n = 1$ est au programme de MPSI. Savez-vous le démontrer ?

- *Réciproquement, si* $c(P) \in \mathbb{N}^*$, *la décomposition* $P = c(P) \underbrace{\tilde{P}}_{\in \mathbb{Z}[X]_{\text{prim}}}$ *de la question précédente montre immédiatement que* $P \in \mathbb{Z}[X]$.

9. **Lemme de Gauss, première version.** Montrer que $\mathbb{Z}[X]_{\text{prim}}$ est stable par produit.

   Supposons par l'absurde pouvoir trouver $P, Q \in \mathbb{Z}[X]_{\text{prim}}$ *tels que* $PQ \notin \mathbb{Z}[X]_{\text{prim}}$.
   Comme il est clair que $PQ \in \mathbb{Z}[X]$, *cela signifie que les coefficients de* PQ *ne sont pas premiers entre eux dans leur ensemble. On peut donc trouver un nombre premier* p *qui les divise tous, c'est-à-dire qu'en notant* $\pi_p : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ *la réduction modulo* p *des polynômes, on a* $\pi_p(PQ) = 0$.
   Ainsi, $\pi_p(P)\pi_p(Q) = 0$. *Par intégrité de* $\mathbb{F}_p[X]$, *on en déduit que (quitte à les échanger),* $\pi_p(P) = 0$, *c'est-à-dire que le premier* p *divise tous les coefficients de* P. *Cela contredit la primitivité de* P, *et conclut la démonstration.*

10. **Lemme de Gauss, deuxième version.** Soit $P_1, P_2 \in \mathbb{Q}[X]$ non nuls. Montrer que $c(P_1P_2) = c(P_1)c(P_2)$.

    On peut trouver $\tilde{P}_1, \tilde{P}_2 \in \mathbb{Z}[X]_{\text{prim}}$ *tels que* $P_1 = c(P_1)\tilde{P}_1$ *et* $P_2 = c(P_2)\tilde{P}_2$.
    On en déduit $P_1P_2 = \underbrace{c(P_1)c(P_2)}_{\in \mathbb{Q}_+^*} \tilde{P}_1\tilde{P}_2$.
    D'après la première version du lemme de Gauss, on a $\tilde{P}_1\tilde{P}_2 \in \mathbb{Z}[X]_{\text{prim}}$, *et l'unicité de la décomposition montre alors* $c(P_1P_2) = c(P_1)c(P_2)$.

11. **Lemme de Gauss, version originale.** [2] Soit $P_1, P_2 \in \mathbb{Q}[X]$ unitaires. Montrer que si le produit P_1P_2 est à coefficients entiers, alors il en va de même de P_1 et P_2.

    Le point clef est que le contenu d'un polynôme unitaire est l'inverse d'un nombre entier. En effet, soit $P \in \mathbb{Q}[X]$ *unitaire, et notons* n *son degré. Le polynôme primitif* $\tilde{P} = \dfrac{1}{c(P)}P$ *est notamment à coefficients entiers, et on observe en examinant les coefficients de degré* n *que* $\operatorname{coeff}_n(\tilde{P}) = \dfrac{1}{c(P)}$, *si bien que* $c(P) = \dfrac{1}{\operatorname{coeff}_n(\tilde{P})}$ *est l'inverse d'un entier (et même d'un entier* > 0, *puisque le contenu est positif).*
    Soit maintenant $m_1, m_2 \in \mathbb{N}^*$ *tels que* $c(P_1) = \dfrac{1}{m_1}$ *et* $c(P_2) = \dfrac{1}{m_2}$. *D'après la deuxième version du lemme de Gauss et la question 8.,* $c(P_1P_2) = c(P_1)c(P_2) = \dfrac{1}{m_1m_2}$ *est un entier.*
    On en déduit $m_1m_2 = 1$, *puis* $m_1 = m_2 = 1$, *si bien que* $c(P_1) = 1 = c(P_2)$.
    En utilisant à nouveau 8., on en déduit que P_1 *et* P_2 *sont à coefficients entiers (et même qu'ils sont primitifs, mais ça n'est pas une grande nouvelle car on les savait déjà unitaires et à coefficients entiers).*

12. **Descente de la divisibilité.** Soit $A \in \mathbb{Z}[X]_{\text{prim}}$ et $B \in \mathbb{Z}[X]$. On suppose que A divise B *sur* $\mathbb{Q}$, c'est-à-dire $\exists Q \in \mathbb{Q}[X] : B = AQ$. Montrer que A divise B sur $\mathbb{Z}$, c'est-à-dire $\exists Q \in \mathbb{Z}[X] : B = AQ$.

    Soit $Q \in \mathbb{Q}[X]$ *tel que* $B = AQ$.
    - *Si* $B = 0$, *on a* $B = A \times 0$, A *divise bien* B *sur* $\mathbb{Z}$.
    - *Dans le cas contraire, on sait que* A *et* Q *ne sont pas nuls, et on peut utiliser le lemme de Gauss :* $c(B) = c(A)c(Q)$. *D'après les hypothèses,* $c(A) = 1$ *et* $c(B) \in \mathbb{N}^*$, *donc* $c(Q) \in \mathbb{N}^*$. *La question 8. montre alors que* $Q \in \mathbb{Z}[X]$, *si bien que* A *divise* B *sur* $\mathbb{Z}$.

13. Donner un exemple montrant que, dans la question précédente, on ne peut pas omettre l'hypothèse de primitivité de A.

    C'est un peu idiot : $2X$ *divise* X *sur* $\mathbb{Q}$ *(ils sont même associés) mais pas sur* $\mathbb{Z}$. *On peut faire plus discret (par exemple,* $2(X-1)$ *divise* $X^2 - 3X + 2$ *sur* $\mathbb{Q}$ *mais pas sur* $\mathbb{Z}$*) ou moins discret (*2 *divise* 1 *dans* $\mathbb{Q}[X]$ *mais pas dans* $\mathbb{Z}[X]$*), mais la mécanique est toujours la même.*

---

2. Pour être tout à fait honnête, la version originale est : *« 42. Si coefficientes* $A, B, C \dots N$; $a, b, c \dots n$ *duarum functionum formae* $x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} \dots + N$ *(P)* $x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} \dots + n$ *(Q) omnes sunt rationales, neque vero omnes integri, productumque ex (P) et (Q)* $= x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \text{etc.} + \mathfrak{Z}$ *omnes coefficientes* $\mathfrak{A}, \mathfrak{B} \dots \mathfrak{Z}$ *integri esse nequeunt. »*

14. Soit $m \in \mathbb{N}^*$. Construire un polynôme $\Pi \in \mathbb{Z}[X]$ tel que $\left\{P \in \mathbb{Z}[X] \,\middle|\, P\left(\frac{1}{m}\right) = 0\right\} = \{\Pi Q \,|\, Q \in \mathbb{Z}[X]\}$.

Soit $P \in \mathbb{Z}[X]$. On a la chaîne d'équivalences

$$\begin{aligned} P(1/m) = 0 &\Leftrightarrow \exists Q \in \mathbb{Q}[X] \,:\, P = (X - 1/m)Q && \textit{(lemme de factorisation sur } \mathbb{Q}\textit{)} \\ &\Leftrightarrow \exists Q \in \mathbb{Q}[X] \,:\, P = (mX - 1)Q \\ &\Leftrightarrow \exists Q \in \mathbb{Z}[X] \,:\, P = (mX - 1)Q && \textit{(car } mX - 1 \in \mathbb{Z}[X]_{\text{prim}}\textit{)}, \end{aligned}$$

donc le polynôme $\Pi = mX - 1$ convient.

15. **Application aux polynômes cyclotomiques.** Soit $n \geq 1$. Montrer que Φ_n est un polynôme à coefficients entiers. Quel est son coefficient dominant ?

Pour tout $n \in \mathbb{N}^*$, on note $P(n)$ l'assertion « Φ_n est un polynôme unitaire de $\mathbb{Z}[X]$ ».
Montrons $\forall n \in \mathbb{N}^*, P(n)$ par récurrence forte.[3]
Soit $n \in \mathbb{N}^*$ tel que $\forall k \in [\![1, n-1]\!], P(k)$. Montrons $P(n)$.
La question 3. montre que $X^n - 1 = \Phi_n \times \underbrace{\prod_{\substack{d|n \\ d<n}} \Phi_d}_{=:Q}$.
D'après l'hypothèse de récurrence, tous les facteurs apparaissant dans le produit définissant Q sont des polynômes unitaires à coefficients entiers. Il s'ensuit que Q lui-même est unitaire à coefficients entiers (crucialement, cette propriété reste vraie si le produit est vide).
Comme $X^n - 1$ est lui-même unitaire, l'examen des coefficients dominants montre déjà que Φ_n est unitaire. Ensuite, l'écriture $X^n - 1 = \Phi_n Q$ (que l'on peut voir comme une division euclidienne « tombant juste » dans $\mathbb{C}[X]$) montre que[4] *$\Phi_n \in \mathbb{Q}[X]$. En effet, on peut utiliser la partie « existence » du théorème sur la division euclidienne sur $\mathbb{Q}$ pour trouver $S, R \in \mathbb{Q}[X]$ tels que $X^n - 1 = SQ + R$ et $\deg R < \deg Q$. Mais la partie « unicité » du théorème sur $\mathbb{C}$ montre alors $S = \Phi_n$, donc $\Phi_n \in \mathbb{Q}[X]$ (et $R = 0$). Notons qu'à chaque fois, le théorème est applicable car Q est unitaire, donc non nul.*
Nous avons donc maintenant deux polynômes unitaires $\Phi_n, Q \in \mathbb{Q}[X]$ dont le produit $X^n - 1$ est à coefficients entiers. La version originale du lemme de Gauss entraîne que $\Phi_n \in \mathbb{Z}[X]$, ce qui conclut.

16. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ un polynôme de degré n. On note $\frac{u_1}{v_1}, \dots, \frac{u_r}{v_r}$ ses racines rationnelles, écrites sous forme irréductible et répétées selon leur multiplicité. Montrer que $v_1 \cdots v_r \mid a_n$ et $u_1 \cdots u_r \mid a_0$.

D'après le lemme de factorisation, le polynôme $\widetilde{Q} = \prod_{k=1}^{r} \left(X - \frac{u_k}{v_k}\right) \in \mathbb{Q}[X]$ divise P. Mieux, en multipliant par $v_1 \cdots v_r \in \mathbb{Q}^\times$, le polynôme $Q = \prod_{k=1}^{r} (v_k X - u_k) \in \mathbb{Z}[X]$ divise P dans $\mathbb{Q}[X]$. Mais ce polynôme est primitif : en effet, pour tout $k \in [\![1, r]\!]$, u_k et v_k sont premiers entre eux donc $v_k X - u_k \in \mathbb{Z}[X]_{\text{prim}}$. D'après la première version du lemme de Gauss, on en déduit que $Q \in \mathbb{Z}[X]_{\text{prim}}$.
Par descente de la divisibilité, Q divise donc P dans $\mathbb{Z}[X]$. On en déduit que le coefficient constant de Q divise celui de P, et idem *avec le coefficient dominant. Autrement dit, $(-1)^r u_1 \cdots u_r \mid a_0$ (mais le $(-1)^r$ est inversible dans $\mathbb{Z}$, donc il ne joue aucun rôle) et $v_1 \cdots v_r \mid a_n$.*

17. Montrer que le polynôme $X^3 - 2X + 7$ est irréductible dans $\mathbb{Q}[X]$.

Un polynôme non irréductible $P \in K[X]$ de degré 3 se factorise nécessairement sous la forme $P = P_1 P_2$, avec P_1 et $P_2 \in K[X]$ de degrés respectifs 1 et 2. Comme tout polynôme de degré 1 possède une racine, on en déduit que P possède lui aussi une racine (dans K). Par contraposée, on vient de montrer une condition

3. Pour la beauté du geste, je vais faire une récurrence forte **non initialisée**. Je vous laisse méditer pour comprendre pourquoi c'est correct, ou faire les modifications vous-mêmes.

4. Je vais refaire l'argument mais c'est un point (presque ?) de cours à retenir : si K est un sous-corps de L et que deux polynômes $A, B \in K[X]$ vérifient que B divise A dans $L[X]$, alors B divise déjà A dans $K[X]$: c'est une autre forme de **descente de la divisibilité**, plus simple car elle ne met en jeu que des corps.

suffisante d'irréductibilité très particulière[5] *: tout polynôme de degré* 3 *ne possédant pas de racine dans un corps contenant ses coefficients est irréductible sur ce corps.*
Si $P = X^3 - 2X + 7$ *avait une racine rationnelle* $\frac{u}{v}$ *(sous forme irréductible), la question précédente entraînerait que* $v \mid 1$ *et* $u \mid 7$*. Il n'y a donc que quatre possibilités, à savoir* ± 1 *et* ± 7*, et on les exclut facilement. De degré* 3 *et sans racine rationnelle,* P *est irréductible sur* $\mathbb{Q}$*.*

C. Irréductibilité de polynômes à coefficients entiers

On « rappelle » que si K est un corps, un polynôme non constant de K[X] est dit *irréductible* s'il est impossible de l'écrire comme un produit de polynômes non constants de K[X].

On fixe par ailleurs un nombre premier p, et on note $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ le morphisme d'anneaux obtenu par réduction modulo p.

18. **Condition suffisante d'irréductibilité.** Soit $P \in \mathbb{Z}[X]$ unitaire non constant tel que $\pi(P) \in \mathbb{F}_p[X]$ soit irréductible. Montrer que P est irréductible dans $\mathbb{Q}[X]$.

    Soit $Q, R \in \mathbb{Q}[X]$ *tels que* $P = QR$*. On a* $c(Q)c(R) = 1$ *donc, quitte à diviser* Q *et* R *par leurs contenus, on peut supposer* $Q, R \in \mathbb{Z}[X]_{\text{prim}}$*. Les coefficients dominants de* Q *et* R *sont deux entiers dont le produit vaut* 1*, donc tous les deux égaux à* ± 1*. En particulier,* $\deg Q = \deg \pi(Q)$ *et* $\deg R = \deg \pi(R)$*.*
    On peut maintenant appliquer le morphisme de réduction modulo p *: on a* $\pi(P) = \pi(Q)\pi(R)$*. Par irréductibilité de* $\pi(P)$ *sur* $\mathbb{F}_p$*, on en déduit que* $\pi(Q)$ *ou* $\pi(R)$ *est constant. Comme on l'a vu, la réduction modulo* p *n'a pas changé les degrés, donc* Q *ou* R *est constant.*
    Cela montre que P *est irréductible sur* $\mathbb{Q}$*.*

19. **Critère d'Eisenstein.** Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ unitaire de degré $n \geq 1$. On suppose que $v_p(a_0) = 1$ et $\forall k \in [\![1, n-1]\!], v_p(a_k) \geq 1$, où v_p désigne la valuation p-adique.
    Montrer que P est irréductible dans $\mathbb{Q}[X]$.

    Soit $Q, R \in \mathbb{Q}[X]$ *tels que* $P = QR$*. Notons* $q = \deg Q$ *et* $r = \deg R$*.*
    Quitte à multiplier Q *et* R *par des constantes non nulles, on peut les supposer unitaires, et la version originale du lemme de Gauss entraîne qu'il s'agit même de polynômes à coefficients entiers. On peut alors appliquer le morphisme d'anneaux* π *et obtenir* $\pi(P) = \pi(Q)\pi(R)$*. Notons que* $\pi(Q)$ *et* $\pi(R)$ *sont aussi unitaires, de degrés respectifs* q *et* r*.*
    Une partie des hypothèses montre que $\pi(P) = X^n$*. Les polynômes* $\pi(Q)$ *et* $\pi(R)$ *étant deux diviseurs de* X^n*, ils ne peuvent pas avoir d'autres facteurs irréductibles*[6] *que* X*. Vu qu'il s'agit de polynômes unitaires dont on connaît les degrés, on a ainsi* $\pi(Q) = X^q$ *et* $\pi(R) = X^r$*.*
    Si q *et* r *étaient tous les deux* > 0*, les deux polynômes* $\pi(Q), \pi(R) \in \mathbb{F}_p[X]$ *auraient des coefficients constants nuls, c'est-à-dire que* Q *et* R *auraient des coefficients constants multiples de p. On aurait alors la divisibilité* $p^2 \mid a_0 = Q(0)R(0)$*, ce qui contredit l'hypothèse* $v_p(a_0) = 1$*.*
    Ainsi, q *ou* r *est nul, ce qui entraîne que* Q *ou* R *est constant, et conclut.*

20. Soit $n \in \mathbb{N}^*$. Montrer qu'il existe un polynôme irréductible de degré n dans $\mathbb{Q}[X]$.

    Pour tout p *premier, le polynôme* $X^n - p$ *vérifie les hypothèses du critère d'Eisenstein, donc il est irréductible dans* $\mathbb{Q}[X]$*.*

21. Soit K un corps et $P \in K[X]$. Montrer que P est irréductible dans K[X] si et seulement si $P(X + 1)$ l'est.

    On pourrait le rédiger de beaucoup de façons différentes mais (en trichant un peu sur la chronologie), je vais

5. Elle fonctionne en degré 3 mais aussi en degré 2, avec essentiellement la même preuve, mais devient fausse juste ensuite. Par exemple, le polynôme réel $(X^2 + 1)^2$ n'est clairement pas irréductible, mais il ne possède pas de racine réelle.

6. Si on a un peu peur de faire ainsi de l'arithmétique dans $\mathbb{F}_p[X]$, il est aussi possible de regarder les valuations de $\pi(Q)$ et $\pi(R)$, c'est-à-dire le plus petit degré d'un de leurs monômes non nuls. On voit que la somme des deux valuations doit valoir $q + r$, qui est déjà le degré de leur produit, donc la valuation de $\pi(Q)$ est nécessairement q et celle de $\pi(R)$, r, ce qui les force à être des monômes.

remarquer que la définition d'un élément irréductible dans un anneau intègre est en fait déjà invariante par isomorphisme. Soit $\varphi : A \to B$ un isomorphisme d'anneaux, que l'on suppose intègres[7]*. Soit $a \in A$ irréductible, et montrons que $\varphi(a) \in B$ l'est aussi.*

- *Déjà, comme φ est un isomorphisme, $\varphi(a)$ n'est pas inversible : s'il l'était, on aurait*
$$a\,\varphi^{-1}(\varphi(a)^{-1}) = \varphi^{-1}(\varphi(a)\,\varphi(a)^{-1}) = \varphi^{-1}(1) = 1,$$
ce qui forcerait l'inversibilité de a, exclue par irréductibilité.
- *Soit maintenant $x, y \in B$ tels que $\varphi(a) = xy$. On en déduit que $a = \varphi^{-1}(xy) = \varphi^{-1}(x)\varphi^{-1}(y)$. Par irréductibilité de a, $\varphi^{-1}(x)$ ou $\varphi^{-1}(y)$ est inversible, ce qui entraîne comme on l'a vu que x ou y est inversible, et clôt la démonstration.*

On a donc montré que pour tout $a \in A$, l'irréductibilité de a entraîne celle de $\varphi(a)$. En appliquant cela à l'isomorphisme réciproque $\varphi^{-1} : B \to A$, on obtient l'implication réciproque.
Pour conclure, il suffit donc de vérifier que $T : P \mapsto P(X+1)$ est un isomorphisme de l'anneau $K[X]$. Les propriétés de morphisme sont claires, et on constate immédiatement que $P \mapsto P(X-1)$ fournit une réciproque à T.

22. En déduire que Φ_p est irréductible dans $\mathbb{Q}[X]$.

En prenant la question précédente comme une indication peu discrète, on va montrer que $P := \Phi_p(X+1)$ est irréductible. En menant habilement les calculs dans $\mathbb{Q}(X)$ (ou $\mathbb{C}(X)$), on a :
$$P = \Phi_p(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{(X+1)^p - 1}{X} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1}.$$
On constate qu'il s'agit d'un polynôme unitaire à coefficients entiers.

- *Pour tout $k \in [\![1, \deg P - 1]\!] = [\![1, p-2]\!]$, on a $\operatorname{coeff}_k(P) = \binom{p}{k+1}$. Or, on sait que $\forall \ell \in [\![1, p-1]\!]$, $p \mid \binom{p}{\ell}$, donc $v_p(\operatorname{coeff}_k(P)) \geq 1$.*
- *Enfin, $v_p(\operatorname{coeff}_0(P)) = v_p\left(\binom{p}{1}\right) = v_p(p) = 1$.*

Le critère d'Eisenstein s'applique donc : $\Phi_p(X+1)$ est irréductible, et Φ_p aussi.
***Remarque.** Essentiellement la même démonstration fonctionne pour montrer l'irréductibilité de Φ_{p^k}. Le cas général nécessite de nouvelles idées.*

D. Cyclicité de $\mathbb{F}_p^\times$

Soit p un nombre premier. Dans cette section, pour tout $m \in \mathbb{N}^*$, on notera $\overline{\Phi}_m = \pi(\Phi_m) \in \mathbb{F}_p[X]$ la réduction modulo p du m-ième polynôme cyclotomique.

On note $\mathbb{F}_p^\times$ le groupe des inversibles de $\mathbb{F}_p$, c'est-à-dire le groupe $(\mathbb{F}_p \setminus \{0\}, \times)$.

23. Soit $x \in \mathbb{F}_p^\times$. Montrer qu'il existe $m = m(x) \in \mathbb{N}^*$ minimal tel que $x^m = 1$, puis que $m(x)$ divise $p-1$.

La « bonne réponse » serait de citer le théorème de Lagrange, que nous allons voir très bientôt, mais que vous avez peut-être déjà vu en première année. Je vais néanmoins utiliser un résultat de théorie des groupes, à savoir la classification des sous-groupes de $\mathbb{Z}$.
L'ensemble $A(x) := \{n \in \mathbb{Z} \mid x^n = 1\}$ est un sous-groupe de $\mathbb{Z}$: on peut par exemple le voir comme le noyau du morphisme de groupes $\mathbb{Z} \to \mathbb{F}_p^\times$ défini par $n \mapsto x^n$. On peut donc trouver $m \in \mathbb{N}$ tel que $A(x) = m\mathbb{Z}$.
Par ailleurs, le petit théorème de Fermat garantit que pour tout entier k premier à p, $k^{p-1} \equiv 1 \pmod p$, c'est-à-dire plus abstraitement que $\forall \kappa \in \mathbb{F}_p^\times, \kappa^{p-1} = 1$. En particulier, $p-1 \in A(x)$, ce qui force m à être un diviseur de $p-1$, et en particulier à être non nul. Ainsi, $A(x) \cap \mathbb{N}^* = \{m, 2m, 3m, \ldots\}$.

7. Évidemment, comme ils sont isomorphes, il suffirait en fait de supposer un des deux intègre...

Vu sa définition, m est bien le plus petit entier > 0 tel que $x^m = 1$.

24. Montrer que le polynôme $X^{p-1} - 1 \in \mathbb{F}_p[X]$ est scindé à racines simples et déterminer ses racines.

    À nouveau, le petit théorème de Fermat dit que $\forall \kappa \in \mathbb{F}_p^\times, \kappa^{p-1} = 1$, c'est-à-dire que les $p-1$ éléments de $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ sont racines de $X^{p-1} - 1$. Cela force le polynôme à être scindé à racines simples.

25. Montrer que le polynôme $\overline{\Phi}_{p-1} \in \mathbb{F}_p[X]$ possède (au moins) une racine $z \in \mathbb{F}_p$.

    On a $X^{p-1} - 1 = \Phi_{p-1} \underbrace{\prod_{\substack{d \mid p-1 \\ d < p-1}} \Phi_d}_{=:Q}$, où Φ_{p-1} et Q sont unitaires et éléments de $\mathbb{Z}[X]$.

    Remarquons que Φ_{p-1} possède au moins une racine complexe : la définition (iii) montre qu'au moins $\zeta_{p-1} \in \widehat{\mathbb{U}}_{p-1}$. Ainsi, $\deg \overline{\Phi}_{p-1} \geq 1$.
    En appliquant π et en notant $\overline{Q} = \pi(Q)$, on en déduit $X^{p-1} - 1 = \overline{\Phi}_{p-1}\overline{Q}$, donc $\overline{\Phi}_{p-1}$ divise $X^{p-1} - 1$. Comme Φ_{p-1} était unitaire de degré ≥ 1, il en va de même de $\overline{\Phi}_{p-1}$. Il possède donc au moins un facteur irréductible F. Comme $\overline{\Phi}_{p-1}$ divise $X^{p-1} - 1$, le polynôme irréductible est également un des facteurs irréductibles de $X^{p-1} - 1$. Comme celui-ci est scindé, le facteur F doit être de degré 1. Il possède donc une racine, et $\overline{\Phi}_{p-1}$ aussi.

26. Soit $d \in \mathbb{N}^*$ un diviseur de $p-1$ *strict*, c'est-à-dire différent de $p-1$.
    Montrer que $(X^d - 1)\Phi_{p-1}$ divise $X^{p-1} - 1$ et en déduire $z^d \neq 1$.

    La définition (i) des racines primitives de l'unité montre que $\mathbb{U}_d \cap \widehat{\mathbb{U}}_{p-1} = \emptyset$, si bien que

    $$(X^d - 1)\Phi_{p-1} = \prod_{\omega \in \mathbb{U}_d \sqcup \widehat{\mathbb{U}}_{p-1}} (X - \omega) \quad \text{divise} \quad \prod_{\omega \in \mathbb{U}_{p-1}} (X - \omega) = X^{p-1} - 1.$$

    Comme dans la question précédente, on peut trouver $R \in \mathbb{Z}[X]$ unitaire tel que $X^{p-1} - 1 = (X^d - 1)\Phi_{p-1}R$ puis, en réduisant modulo p : $X^{p-1} - 1 = (X^d - 1)\overline{\Phi}_{p-1}\overline{R}$, donc $(X^d - 1)\overline{\Phi}_{p-1}$ divise $X^{p-1} - 1$.
    Si l'on avait $z^d = 1$, l'élément $z \in \mathbb{F}_p^\times$ serait à la fois racine de $X^d - 1$ et de $\overline{\Phi}_{p-1}$, donc il serait racine multiple de $X^{p-1} - 1$, ce qui contredit le caractère scindé à racines simples de ce polynôme.

27. Montrer $m(z) = p - 1$ puis $\mathbb{F}_p^\times = \{z^0, z^1, \dots, z^{p-2}\}$.

    On sait que $m(z)$ est un diviseur de $p-1$. La question précédente montre qu'il ne peut pas s'agir d'un diviseur strict de $p-1$, donc $m(z) = p-1$.

    - *Comme $z \in \mathbb{F}_p^\times$, l'inclusion réciproque est évidente.*
    - *Montrons que les z^i (pour $0 \leq i \leq p-2$) sont distincts. Dans le cas contraire, on peut trouver $0 \leq i < j \leq p-2$ tels que $z^i = z^j$. En simplifiant par z^i, on trouve $k \in [\![1, p-2]\!]$ tel que $z^k = 1$, ce qui contredit $m(z) = p-1$.*
    - *Ainsi, $|\{z^0, z^1, \dots, z^{p-2}\}| = p-1$, ce qui montre l'égalité par inclusion et égalité des cardinaux.*

E. Lemme de Hensel et congruences modulo p^k

On fixe dans cette dernière section un nombre premier p et un polynôme $P \in \mathbb{Z}[X]$.

28. Soit $a \in \mathbb{Z}$ et $k \in \mathbb{N}^*$.
    Montrer que $[a]_p \in \mathbb{F}_p$ est inversible si et seulement si $[a]_{p^k} \in \mathbb{Z}/p^k\mathbb{Z}$ est inversible.

    On sait que, pour tout $n \geq 2$, la classe $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si a et n sont premiers entre eux. Il s'agit donc de montrer que a et p sont premiers entre eux si et seulement si a et p^k le sont.
    Or, on a $\operatorname{pgcd}(a, p) = p^{\min(1, v_p(a))}$ et $\operatorname{pgcd}(a, p^k) = p^{\min(k, v_p(a))}$, si bien que les deux conditions de coprimalité équivalent à $v_p(a) = 0$ (et sont donc équivalentes entre elles).

29. Soit $a, h \in \mathbb{Z}$ et $k \in \mathbb{N}^*$. On suppose $h \equiv 0 \pmod{p^k}$. Montrer que $\mathrm{P}(a+h) \equiv \mathrm{P}(a) + \mathrm{P}'(a)\,h \pmod{p^{2k}}$.

Posons $\tilde{\mathrm{P}} = \mathrm{P}(a + \mathrm{X})$*, qui est encore un polynôme de* $\mathbb{Z}[\mathrm{X}]$ *et que l'on note* $\sum_{k=0}^{n} b_k \mathrm{X}^k$*. On remarque que* $\tilde{\mathrm{P}} = b_0 + b_1\mathrm{X} + \mathrm{X}^2 \sum_{k=2}^{n} b_k \mathrm{X}^{k-2}$ *: on a ainsi trouvé un polynôme* $\mathrm{Q} = \sum_{k=2}^{n} b_k \mathrm{X}^{k-2} \in \mathbb{Z}[\mathrm{X}]$ *tel que* $\tilde{\mathrm{P}} = \tilde{\mathrm{P}}(0) + \tilde{\mathrm{P}}'(0)\mathrm{X} + \mathrm{X}^2\mathrm{Q}$.
Autrement dit, $\mathrm{P}(a + \mathrm{X}) = \mathrm{P}(a) + \mathrm{P}'(a)\mathrm{X} + \mathrm{X}^2\mathrm{Q}$ *pour un certain polynôme* $\mathrm{Q} \in \mathbb{Z}[\mathrm{X}]$*. Maintenant, la condition* $p^k \mid h$ *entraîne* $p^{2k} \mid h^2$*, si bien que* $p^{2k} \mid h^2\mathrm{Q}(h)$ *et que donc* $\mathrm{P}(a+h) \equiv \mathrm{P}(a) + \mathrm{P}'(a)h \pmod{p^{2k}}$.

30. **Lemme de Hensel.** Soit $a \in \mathbb{Z}$ et $k \in \mathbb{N}^*$. On suppose $\mathrm{P}(a) \equiv 0 \pmod{p^k}$ et $\mathrm{P}'(a) \not\equiv 0 \pmod{p}$.
Montrer qu'il existe $\tilde{a} \in \mathbb{Z}$ tel que $\tilde{a} \equiv a \pmod{p^k}$, $\mathrm{P}(\tilde{a}) \equiv 0 \pmod{p^{2k}}$ et $\mathrm{P}'(\tilde{a}) \not\equiv 0 \pmod{p}$.

Le point-clef des deux prochaines questions est que la résolution habituelle des équations du premier degré ($\alpha x + \beta = 0 \Leftrightarrow x = -\alpha^{-1}\beta$)*, que nous avons l'habitude de pratiquer dans un corps, est en fait valable dans n'importe quel anneau (même non commutatif), pourvu que* α *soit inversible. Une fois cela compris, on peut rédiger assez rapidement.*
Comme $\mathrm{P}'(a) \not\equiv 0 \pmod{p}$*, la question 28. entraîne l'inversibilité de* $\mathrm{P}'(a)$ *modulo* p^{2k} *: on peut trouver* $\lambda \in \mathbb{Z}$ *tel que* $\lambda\,\mathrm{P}'(a) \equiv 1 \pmod{p^{2k}}$*. Posons alors* $\tilde{a} = a - \lambda\mathrm{P}(a)$*. Vérifions les trois propriétés.*

$\tilde{a}$ **est solution modulo** p^{2k}**.** *On a*

$$\begin{aligned} \mathrm{P}\big(a - \lambda\mathrm{P}(a)\big) &\equiv \mathrm{P}(a) + (-\lambda\mathrm{P}(a))\mathrm{P}'(a) \pmod{p^{2k}} && \textit{(question 29.)} \\ &\equiv \mathrm{P}(a) - \mathrm{P}(a) \equiv 0 \pmod{p^{2k}}, \end{aligned}$$

si bien que $\mathrm{P}(\tilde{a}) \equiv 0 \pmod{p^{2k}}$.

$\tilde{a}$ **est ~~« proche de »~~** a **congru à** a **modulo** p^k**.** *Comme* $p^k \mid \mathrm{P}(a)$*,* $\tilde{a} = a - \lambda\mathrm{P}(a) \equiv a \pmod{p^k}$.

$\mathrm{P}'(\tilde{a})$ **reste non divisible par** p**.** *C'est en fait une conséquence de la propriété précédente.*

En effet, $\mathrm{P}' \in \mathbb{Z}[\mathrm{X}]$ *et les polynômes à coefficients entiers respectent les congruences*[8] *au sens où, pour tous* $b, c \in \mathbb{Z}$ *et tout* $n \geq 2$*, on a* $\forall \mathrm{Q} \in \mathbb{Z}[\mathrm{X}], b \equiv c \pmod{n} \Rightarrow \mathrm{Q}(b) \equiv \mathrm{Q}(c) \pmod{n}$.

En particulier, la congruence $\tilde{a} \equiv a \pmod{p^k}$ *entraîne* $\mathrm{P}'(\tilde{a}) \equiv \mathrm{P}'(a) \pmod{p^k}$ *et donc la congruence plus grossière* $\mathrm{P}'(\tilde{a}) \equiv \mathrm{P}'(a) \not\equiv 0 \pmod{p}$.

31. Montrer qu'avec les notations précédentes, $\tilde{a}$ est unique modulo p^{2k} : si $\hat{a}$ vérifie les mêmes propriétés, alors $\tilde{a} \equiv \hat{a} \pmod{p^{2k}}$.

Soit $\hat{a}$ *tel que* $\mathrm{P}(\hat{a}) \equiv 0 \pmod{p^{2k}}$ *et* $\hat{a} \equiv a \pmod{p^k}$ *(comme on l'a expliqué à la question précédente, la troisième propriété est une conséquence de la deuxième donc je ne la suppose pas explicitement).*
On peut alors trouver $h \in \mathbb{Z}$ *multiple de* p^k *tel que* $\hat{a} = a + h$.
On reprend la définition de l'entier λ *de la question précédente.*
La question 29. entraîne $0 \equiv \mathrm{P}(\hat{a}) \equiv \mathrm{P}(a) + \mathrm{P}'(a)h \pmod{p^{2k}}$*, donc*

$$\begin{aligned} h \equiv \lambda\,\mathrm{P}'(a)\,h &\equiv -\lambda\mathrm{P}(a) \pmod{p^{2k}} \\ \textit{donc} \qquad \hat{a} = a + h &\equiv a - \lambda\mathrm{P}(a) = \tilde{a} \pmod{p^{2k}}. \end{aligned}$$

8. C'est vraiment une propriété à connaître, presque du cours. Elle n'est d'ailleurs pas difficile à démontrer. En effet, par des combinaisons $\mathbb{Z}$-linéaires, il suffit de vérifier cette propriété pour les polynômes $\mathrm{Q} = \mathrm{X}^k$, ce que l'on peut faire au choix en utilisant de façon répétée les règles de multiplication des congruences ou d'un coup en utilisant la formule de Bernoulli (pour $k \geq 1$) : $b^k - c^k = (b-c)\sum_{j=0}^{k-1} b^j c^{k-1-j}$.

32. En déduire que si $a \in \mathbb{Z}$ vérifie $\mathrm{P}(a) \equiv 0 \pmod{p}$ et $\mathrm{P}'(a) \not\equiv 0 \pmod{p}$, alors pour tout $k \in \mathbb{N}^*$, il existe un entier $\alpha_k \in \mathbb{Z}$, unique modulo p^k, tel que $\mathrm{P}(\alpha_k) \equiv 0 \pmod{p^k}$ et $\alpha_k \equiv a \pmod{p}$.

- *Commençons par démontrer la propriété pour les exposants k qui sont des puissances de 2. Pour $j \in \mathbb{N}$, notons $\mathrm{H}(j)$ l'assertion « il existe un entier α_{2^j}, unique modulo p^{2^j}, tel que $\mathrm{P}(\alpha_{2^j}) \equiv 0 \pmod{p^{2^j}}$ et $\alpha_{2^j} \equiv a \pmod{p}$. » Montrons $\forall j \in \mathbb{N}, \mathrm{H}(j)$ par récurrence.*

  Initialisation. *L'assertion $\mathrm{H}(0)$ affirme l'existence d'un entier $\alpha_1 \in \mathbb{Z}$, unique modulo p, tel que $\mathrm{P}(\alpha_1) \equiv 0 \pmod{p}$ et $\alpha_1 \equiv a \pmod{p}$.*

  C'est automatique : $\alpha_1 = a$ convient, et il est le seul, modulo p. Cela montre $\mathrm{H}(0)$.

  Hérédité. *Soit $j \in \mathbb{N}$ tel que $\mathrm{H}(j)$. On dispose en particulier d'un entier α_{2^j} vérifiant les propriétés énoncées.*

  Existence. *On souhaite appliquer la question 30. à l'entier $k = 2^j$.*

  On a déjà l'hypothèse $\mathrm{P}(\alpha_{2^j}) \equiv 0 \pmod{p^{2^j}}$. Par ailleurs, comme on l'a expliqué en résolvant la question 30., la congruence $\alpha_{2^j} \equiv a \pmod{p}$ entraîne $\mathrm{P}'(\alpha_{2^j}) \equiv \mathrm{P}'(a) \not\equiv 0 \pmod{p}$.

  Ainsi, on trouve un nouvel entier $\alpha_{2^{j+1}} = \tilde{\alpha}_{2^j}$ vérifiant les conditions $\mathrm{P}(\alpha_{2^{j+1}}) \equiv 0 \pmod{p^{2^{j+1}}}$, $\alpha_{2^{j+1}} \equiv \alpha_{2^j} \pmod{p^{2^j}}$ et $\mathrm{P}'(\alpha_{2^{j+1}}) \not\equiv 0 \pmod{p}$. La deuxième de ces conditions entraîne notamment $\alpha_{2^{j+1}} \equiv a \pmod{p}$.

  Unicité modulo $p^{2^{j+1}}$. *Soit $\tilde{\alpha}, \hat{\alpha}$ deux entiers tels que*

  $$\mathrm{P}(\tilde{\alpha}) \equiv 0 \equiv \mathrm{P}(\hat{\alpha}) \pmod{p^{2^{j+1}}} \qquad \text{et} \qquad \tilde{\alpha} \equiv a \equiv \hat{\alpha} \pmod{p}.$$

  La première de ces congruences reste notamment vraie modulo p^{2^j}.

  D'après $\mathrm{H}(j)$, on a donc $\tilde{\alpha} \equiv \hat{\alpha} \pmod{p^{2^j}}$. La deuxième entraîne que $\mathrm{P}'(\tilde{\alpha}) \not\equiv 0 \pmod{p}$, comme on l'a déjà dit deux fois.

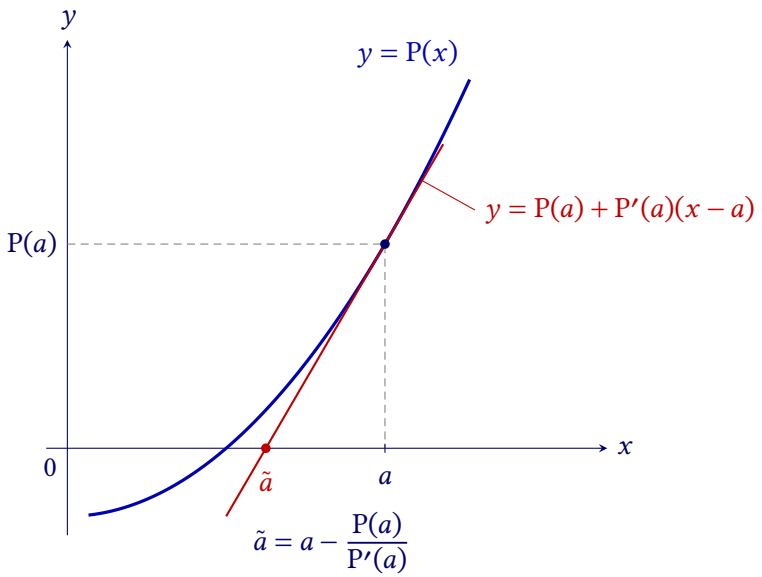
  La question précédente nous permet alors d'en déduire $\tilde{\alpha} \equiv \hat{\alpha} \pmod{p^{2^{j+1}}}$, ce qui conclut.

  Cela montre $\mathrm{H}(j+1)$ et clôt la récurrence.

- *Passons maintenant au cas des exposants généraux. Soit $k \in \mathbb{N}^*$.*
  - *On peut trouver $j \in \mathbb{N}^*$ minimal tel que $2^j \geq k$: la solution α_{2^j} trouvée au point précédent vérifie déjà $\alpha_{2^j} \equiv a \pmod{p}$ et $\mathrm{P}(\alpha_{2^j}) \equiv 0 \pmod{p^{2^j}}$, ce qui donne* a fortiori *la congruence modulo p^k demandée.*
  - *Soit $\tilde{\alpha}, \hat{\alpha} \in \mathbb{Z}$ tels que $\mathrm{P}(\tilde{\alpha}) \equiv 0 \equiv \mathrm{P}(\hat{\alpha}) \pmod{p^k}$ et $\tilde{\alpha} \equiv a \equiv \hat{\alpha} \pmod{p}$ (ce qui entraîne $\mathrm{P}'(\tilde{\alpha}) \not\equiv 0 \not\equiv \mathrm{P}'(\hat{\alpha}) \pmod{p}$).*
    D'après le lemme de Hensel, on peut trouver deux entiers $\tilde{\beta}, \hat{\beta} \in \mathbb{Z}$ tels que $\tilde{\beta} \equiv \tilde{\alpha} \pmod{p^k}$ et $\mathrm{P}(\tilde{\beta}) \equiv 0 \pmod{p^{2k}}$, et idem *pour les versions chapeautées.*
    La minimalité de j entraîne $2k > 2^j$ donc on a $\mathrm{P}(\tilde{\beta}) \equiv 0 \pmod{p^{2^j}}$ et idem *pour la version chapeautée. Vu le premier point, on en déduit $\tilde{\beta} \equiv \alpha_{2^j} \equiv \hat{\beta} \pmod{p^{2^j}}$ et donc $\tilde{\beta} \equiv \hat{\beta} \pmod{p^k}$, ce qui conclut.*

Deux remarques culturelles pour le prix d'une.

- *Le lemme de Hensel et le corollaire que l'on vient de montrer (souvent aussi appelé lemme de Hensel, il existe d'ailleurs énormément de variantes, notamment avec plusieurs variables) sont des versions arithmétiques de la* méthode de Newton.
  Autour d'une solution « approximative », on remplace l'équation par sa tangente (comme dans la question 29.), ce qui fournit une équation affine facile à résoudre, dont la solution $\hat{a}$ est (on l'espère) plus proche de la véritable solution cherchée.



Il ne reste plus qu'à itérer le procédé. Dans les cas favorables, on obtient des approximations de plus en plus fines de notre solution. Pour une fonction f de classe C^2 possédant un zéro « simple » (c'est-à-dire que $f(x) = 0$ mais $f'(x) \neq 0$), on obtient en partant suffisamment près de x une convergence quadratique, *c'est-à-dire que la suite de solutions approchées $(x_n)_{n\in\mathbb{N}}$ vérifie $x_n = x + O(\rho^{2^n})$ pour un certain $\rho \in]0, 1[$.*

- *L'analogie arithmétique est qu'ici, on mesure la proximité entre deux entiers a et b non pas naïvement à l'aide de $|a - b|$, mais arithmétiquement en disant que a et b sont d'autant plus proches qu'ils sont congrus modulo une très grande puissance de p : c'est la* topologie p-adique, *une autre façon d'obtenir une information de plus en plus fine sur un entier. Grossièrement, pour $p = 10$ (on va ignorer pudiquement qu'il ne s'agit pas d'un nombre premier), le premier type d'approximation nous révèle peu à peu les chiffres les plus à gauche, alors que le second nous révèle peu à peu les chiffres les plus à droite d'un nombre donné.*
  Par exemple, modulo 5, $x = 2$ est une racine de $X^2 + 1$. Le lemme de Hensel nous trouve alors successivement des solutions modulo 5^{2^j} : les classes

$$[2]_5, [7]_{25}, [182]_{625}, [280\,182]_{390\,625}, \dots$$

sont toutes racines de $X^2 + 1$ dans leurs anneaux $\mathbb{Z}/5^{2^j}\mathbb{Z}$ respectifs, et elles sont compatibles au sens où chacune est envoyée sur la précédente par le morphisme $\pi_j : \mathbb{Z}/5^{2^j}\mathbb{Z} \to \mathbb{Z}/5^{2^{j-1}}\mathbb{Z}$.
  Ces solutions ne semblent pas « converger » vers un nombre entier, ce qui n'est guère surprenant car $X^2 + 1$ n'a pas de racine réelle. Mais elles décrivent quand même une solution dans un anneau très riche, celui des entiers 5-adiques

$$\mathbb{Z}_5 = \left\{ (x_j)_{j\in\mathbb{N}} \in \prod_{j\in\mathbb{N}} (\mathbb{Z}/5^{2^j}\mathbb{Z}) \;\middle|\; \forall j \in \mathbb{N}^*, \pi_j(x_j) = x_{j-1} \right\},$$

qui joue pour cette notion de proximité 5-adique le même rôle que $\mathbb{R}$ pour la notion de proximité usuelle.
Il est difficile d'exagérer l'importance de ce point de vue p-adique en théorie des nombres moderne.

33. Montrer que pour tout entier $n \in \mathbb{N}$, il existe $x \in \mathbb{Z}$ tel que $2^n \mid x^3 + 7$.

    C'est une application directe de la question précédente pour $P = X^3 + 7 \in \mathbb{Z}[X]$ et $p = 2$.
    On constate que $P(1) = 8 \equiv 0 \pmod 2$ et $P'(1) = 3 \not\equiv 0 \pmod 2$, donc il existe pour tout $n \in \mathbb{N}$ un entier $x \in \mathbb{Z}$ tel que $x^3 + 7 \equiv 0 \pmod{2^n}$.

Terminons par un dernier calcul, sans lien direct avec le lemme de Hensel.

34. On suppose p impair. Montrer $\forall k \in \mathbb{N}^*, (1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}$.

Pour tout $k \in \mathbb{N}^*$, on note $\mathrm{C}(k)$ l'assertion « $(1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}$ ». Montrons $\forall k \in \mathbb{N}^*, \mathrm{C}(k)$ par récurrence.

Initialisation. *On a*

$$\begin{aligned}(1+p)^p &= \sum_{j=0}^{p} \binom{p}{j} p^j \\ &\equiv 1 + \binom{p}{1} p + \binom{p}{2} p^2 \pmod{p^3} \\ &\equiv 1 + p^2 \pmod{p^3}\end{aligned}$$

la première congruence étant justifiée par le fait que, pour tout $j \geq 3$, le terme p^j sera multiple de p^3, et la seconde par le fait que $\binom{p}{2} = p\dfrac{p-1}{2}$ est multiple de p : c'est là qu'on utilise l'imparité de p.

Hérédité. *Soit $k \in \mathbb{N}^*$ tel que $\mathrm{C}(k)$. On peut donc trouver $a \in \mathbb{Z}$ tel que $(1+p)^{p^k} = 1 + p^{k+1} + ap^{k+2}$. On en déduit*

$$\begin{aligned}(1+p)^{p^{k+1}} &= \left((1+p)^{p^k}\right)^p \\ &= (1 + p^{k+1} + ap^{k+2})^p \\ &\equiv 1 + \binom{p}{1} p^{k+1} + \binom{p}{1} a\, p^{k+2} \pmod{p^{k+3}} \\ &\equiv 1 + p^{k+2} \pmod{p^{k+3}},\end{aligned}$$

la première congruence étant justifiée par le fait que tout terme obtenu en « piochant » deux facteurs différents de 1 sera multiple de p^{2k+2} et donc de p^{k+3}.

35. Avec un peu de théorie des groupes, les questions 27. et 34. permettront de montrer le résultat suivant.

Théorème. Soit p un nombre premier impair et $k \geq 1$. Alors le groupe multiplicatif $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est *cyclique*, c'est-à-dire que l'on peut trouver $z \in (\mathbb{Z}/p^k\mathbb{Z})^\times$ tel que $(\mathbb{Z}/p^k\mathbb{Z})^\times = \left\{z^n \,\middle|\, n \in \mathbb{Z}\right\}$.

Montrer que la propriété correspondante est fausse pour $(\mathbb{Z}/8\mathbb{Z})^\times$, puis pour $(\mathbb{Z}/2^k\mathbb{Z})^\times$, dès que $k \geq 3$.

- *On a $(\mathbb{Z}/8\mathbb{Z})^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ et un calcul direct montre que $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$, si bien que, pour tout $z \in (\mathbb{Z}/8\mathbb{Z})^\times$, l'ensemble $\left\{z^n \,\middle|\, n \in \mathbb{Z}\right\}$ possède au plus deux éléments.*
  Dit plus conceptuellement, le groupe multiplicatif $(\mathbb{Z}/8\mathbb{Z})^\times$ est isomorphe au groupe de Klein *$(\mathbb{Z}/2\mathbb{Z})^2$ et non pas au groupe cyclique $\mathbb{Z}/4\mathbb{Z}$.*
- *Soit $k \geq 3$. Commençons par justifier que la réduction modulo 8 fournit un morphisme de groupes surjectif $\varpi : (\mathbb{Z}/2^k\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times$.*
  - *Si $m_1, m_2 \in \mathbb{Z}$ vérifient $m_1 \equiv m_2 \pmod{2^k}$, alors $m_1 \equiv m_2 \pmod 8$, c'est-à-dire $[m_1]_8 = [m_2]_8$. Cela montre que l'application ϖ est bien définie.*
  - *Soit $x_1, x_2 \in (\mathbb{Z}/2^k\mathbb{Z})^\times$: on peut trouver $m_1, m_2 \in \mathbb{Z}$ tels que $x_1 = [m_1]_{2^k}$ et $x_2 = [m_2]_{2^k}$. On a alors*

$$\varpi(x_1x_2) = \varpi([m_1m_2]_{2^k}) = [m_1m_2]_8 = [m_1]_8[m_2]_8 = \varpi(x_1)\varpi(x_2),$$

  donc $\varpi : (\mathbb{Z}/2^k\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times$ est un morphisme de groupes.
  - *Reste à montrer que ϖ est surjectif.*[9] *Pour cela, soit $y \in (\mathbb{Z}/8\mathbb{Z})^\times$. On peut trouver $m \in \mathbb{Z}$ premier avec 8 tel que $y = [m]_8$. Mais « premier avec 8 » ou « premier avec 2^k » sont juste des manières compliquées de dire « impair », donc $x := [m]_{2^k} \in (\mathbb{Z}/2^k\mathbb{Z})^\times$ et $y = \varpi(x)$, ce qui conclut.*

9. C'est la seule partie de la démonstration qui ne soit pas complètement générale (de « l'*abstract nonsense* ») : en général, tout morphisme d'anneaux $A \to B$ induit un morphisme de groupes multiplicatifs $A^\times \to B^\times$, mais celui-ci n'a aucune raison d'être surjectif, même si le morphisme d'anneaux l'était, comme le montre par exemple le cas de la réduction $\pi_5 : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ modulo 5.

Si l'on pouvait trouver $z \in (\mathbb{Z}/2^k\mathbb{Z})^\times$ tel que $(\mathbb{Z}/2^k\mathbb{Z})^\times = \{z^n \,|\, n \in \mathbb{Z}\}$, on aurait directement en appliquant ϖ l'égalité $(\mathbb{Z}/8\mathbb{Z})^\times = \operatorname{im}\varpi = \{\varpi(z)^n \,|\, n \in \mathbb{Z}\}$, ce qui contredirait le premier point.

Remarques.

- *On peut en fait montrer que le groupe $(\mathbb{Z}/2^k\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$.*
- *Même si la démonstration est un peu plus élaborée, on peut montrer que dès que deux entiers $r, s \in \mathbb{N}^*$ vérifient $r \mid s$, la réduction modulo r $\mathbb{Z}/s\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z}$ (morphisme d'anneaux) induit un morphisme de groupes surjectif $\varpi : (\mathbb{Z}/s\mathbb{Z})^\times \to (\mathbb{Z}/r\mathbb{Z})^\times$.*