1. (Ear01) Soit $P \in \mathbb{C}[X]$.
   a. Montrer que le nombre de racines distinctes de P est $\deg(P) - \deg(P \wedge P')$.
   b. Montrer que $P \wedge P'$ et $(P-1) \wedge P'$ sont premiers entre eux. En déduire
   $$\deg(P \wedge P') + \deg((P-1) \wedge P') \leq \deg(P) - 1.$$
   c. Montrer que le nombre de racines *distinctes* de $P(P-1)$ est supérieur ou égal à $\deg(P) + 1$.
   d. Soit P et Q dans $\mathbb{C}[X]$ tels que
   – P et Q ont les mêmes racines,
   – $P-1$ et $Q-1$ ont les mêmes racines.
   Montrer que $P = Q$.
2. (Ear02) Soit $V \in \mathbf{K}[X]$ de degré $v \geq 1$. Montrer que pour tout $P \in \mathbf{K}[X]$, il existe $p \in \mathbb{N}$ et $A_0, \cdots, A_p \in \mathbf{K}[X]$, tous de degré strictement plus petit que v tels que
   $$P = \sum_{i=0}^{p} A_i V^i.$$
   Exemple avec
   $$P = X^7 + 3X^5 + 6X^4 + 7X^3 + 7X^2 + 4X + 2,$$
   $$V = X^2 + X + 1.$$
3. (Ear03) Quels sont les polynômes $A \in \mathbb{C}[X]$ tels que
   $$X^2 + 1 \text{ divise } A \text{ et } X^3 + 1 \text{ divise } A - 1?$$
4. (Ear04) Soit $P \in \mathbb{C}[X]$. Exprimer $\deg(P \wedge P')$ avec le nombre des racines distinctes de P. Si $\deg(P \wedge P') = 2$, quels sont les deux cas possibles ?
5. (Ear05) Soit $A, B, P, Q, R, S \in \mathbf{K}[X]$ tels que
   $$\deg(PS - QR) = 0.$$
   Montrer que
   $$A \wedge B = 1 \Leftrightarrow (PA + QB) \wedge (RA + SB) = 1.$$
6. (Ear08) Montrer que $A = X^4 + X^3 - 2X + 1$ et $B = X^2 + X + 1$ sont premiers entre eux. Déterminer les polynômes U et V tels que $UA + VB = 1$.
7. (Ear09) Soit $S = P \wedge P'$ avec $P = QS$ et α une racine de S de multiplicité m, montrer que α est une racine de Q. Soit $P = X^5 - 13X^4 + 67X^3 - 171X^2 + 216X - 108$. Calculer $P \wedge P'$, en déduire une factorisation de P.
8. (Ear10) Soit A, B, C des polynômes de $\mathbb{C}[X]$ deux à deux premiers entre eux et tels que $A^2 + B^2 = C^2$. Montrer que $C + B$ et $C - B$ sont premiers entre eux et qu'ils sont des carrés de polynômes. En déduire les expressions de A, B, C.
9. (Ear11) Montrer qu'il existe un unique $P \in \mathbb{R}[X]$ de degré 7 tel que $(X-1)^4$ divise $P+1$ et $(X+1)^4$ divise $P-1$. (considérer la dérivée)
10. (Ear12) Soit p et q deux naturels plus grands que 1, montrer que si r est le reste de la division de p par q dans $\mathbb{Z}$ alors $X^r - 1$ est le reste de la division euclidienne de $X^p - 1$ par $X^q - 1$ dans $\mathbb{Q}[X]$. En déduire que
    $$(X^p - 1) \wedge (X^q - 1) = X^{p \wedge q} - 1$$
11. (Ear13) Montrer qu'il existe un unique polynôme P (à déterminer) unitaire de degré inférieur ou égal à 3, divisible par $X-1$ et tel que les restes des divisions de P par $X-2$, $X-3$, $X-4$ soient égaux. On pourra considérer $\widehat{P}(X+1) - P$.
12. (Ear14) Montrer que le polynôme
    $$4X^3 - 3X - \frac{1}{2}$$
    est irréductible dans $\mathbb{Q}[X]$.
13. (Ear17) Transformation de Tschirnhaus.
    Soit $P \in \mathbb{C}[X]$ et y une lettre qui désigne un nombre complexe. On exécute formellement l'algorithme d'Euclide en utilisant P et $X^2 - y$ comme entrées. L'algorithme renvoie un nombre complexe (0 ou un polynôme de degré 0) qui est une expression de y. On la désigne par $A(y)$. Montrer que $A(y) = 0$ si et seulement si y est le carré d'une racine de P.
    Soit $P = X^3 + 2X^2 - X + 3$. Former un polynôme Q dont les racines sont les carrés de celles de P.
14. (Ear18) Discriminant d'un polynôme.
    On considère un polynôme à coefficients complexes
    $$P = X^3 + pX + q$$
    avec $p \neq 0$. On appelle *discriminant* de ce polynôme, le nombre complexe
    $$\Delta = 4p^3 + 27q^2$$
    a. En utilisant l'algorithme d'Euclide pour P et P', montrer que P admet une racine multiple si et seulement si $\Delta = 0$.
    b. On suppose ici
    $$P = (X - z_1)(X - z_2)(X - z_3)$$
    Montrer que
    $$\Delta = \widetilde{P'}(z_1)\widetilde{P'}(z_2)\widetilde{P'}(z_3) = \prod_{(i,j) \in \{1,2,3\}^2, i \neq j} (z_i - z_j)$$
    c. On suppose p et q réels.
       i. Déduire de la question précédente que P admet trois racines réelles distinctes si et seulement si son discriminant est strictement négatif.
       ii. Retrouver le résultat précédent (sans utiliser aucune question de cet exercice) en étudiant la fonction
       $$x \to x^3 + px + q$$
       On formera en particulier le produit des valeurs de la fonction aux extrémas locaux (lorsqu'ils existent).

    On peut définir le discriminant pour un polynôme de degré quelconque par le produit des valeurs du dérivé aux racines et vérifier que c'est encore le produit de toutes les différences des racines (pour des indices distincts). La nullité du discriminant caractérise toujours l'existence de racines multiples.

15. (Ear19) (avec un logiciel de calcul formel) Pour quelle valeur de a les polynômes $X^4 - X + a$ et $X^2 - aX + 1$ ont ils une racine en commun ?

16. (Ear20) Le polynôme

$$X^4 - 3X^3 - 12X^2 + 48X - 64$$

admet deux racines opposées. Trouvez les.

17. (Ear21) Soit p un nombre premier, on note $v(x)$ la valuation p-adique d'un entier x. Soit $m \in \mathbb{N}^*$ et $q = p^m$. On définit[1] le polynôme P par :

$$P = \frac{1}{(q-2)!}(X-2)(X-3)\cdots(X-q+1)$$

a. Soit a et b dans $\mathbb{Z}$. Montrer que

$$\left.\begin{array}{ll} a \equiv b & \mod q \\ a \not\equiv 0 & \mod q \end{array}\right\} \Rightarrow v(a) = v(b)$$

b. Montrer que $v(x)v(x-1) = 0$ pour $x \in \mathbb{Z}$.

c. Quel est le degré de P ? Montrer que $P(z) \in \mathbb{Z}$ pour tout $z \in \mathbb{Z}$.

d. Montrer que, pour tout $z \in \mathbb{Z} \setminus \{2, 3, \cdots, q-1\}$,

$$P(z) \equiv 0 \mod p \Leftrightarrow \left\{\begin{array}{ll} z \not\equiv 0 & \mod q \\ z \not\equiv 1 & \mod q \end{array}\right.$$

18. (Ear22) Racines primitives. Polynômes cyclotomiques. Soit $n \in \mathbb{N}^*$ et $w_n = e^{\frac{2i\pi}{n}}$. On appelle *racine primitive* n-ième de l'unité tout élément du groupe multiplicatif $\mathbb{U}_n$ qui engendre $\mathbb{U}_n$. On note $\mathcal{D}(n)$ l'ensemble des diviseurs naturels de n.

a. Montrer que les racines primitives dans $\mathbb{U}_n$ sont les ω^k pour $k \in [\![1, n]\!]$ et $k \wedge n = 1$. Combien existe-t-il de racines primitives ? Voir l'exercice sur l'indicatrice d'Euler.

b. Soit $d \in \mathcal{D}(n)$ alors $\frac{n}{d} \in \mathcal{D}(n)$.
Quels sont les $k \in [\![1, n]\!]$ tels que $k \wedge n = \frac{n}{d}$? Pour ces k, quel est l'ensemble des w_n^k ?

c. On note Φ_n (polynôme cyclotomique) le polynôme de $\mathbb{C}[X]$ dont les racines sont les racines primitives n-ièmes. Montrer que

$$X^n - 1 \prod_{d \in \mathcal{D}(n)} \Phi_n.$$

d. Calculer les Φ_n pour $n \in [\![1, 12]\!]$.

e. Montrer que les polynômes cyclotomiques sont à coefficients dans $\mathbb{Z}$.

19. (Ear23)

a. Soit A et B deux polynômes à coefficients réels et D leur pgcd unitaire de $\mathbb{R}[X]$. On considère ces *mêmes* polynômes comme étant à coefficients complexes et on note Δ leur pgcd unitaire de $\mathbb{C}[X]$.
Montrer que $D = \Delta$.

b. Soit A et $B \neq 0$ dans $\mathbb{R}[X]$, soit $C \in \mathbb{C}[X]$ tels que $A = BC$. Montrer que $C \in \mathbb{R}[X]$.

20. (Ear24)

a. Montrer qu'il existe un unique couple (U, V) de polynômes à coefficients réels tels que

$$(X-1)^4U + (X+1)^4V = 2^7$$
$$\deg(U) \leq 3 \qquad \deg(V) \leq 3$$

b. Montrer que $V = \widehat{U}(-X)$.

c. Obtenir une expression de U avec des puissances de $X-1$ et $X+1$ en utilisant une formule du binôme.

[1] D'après *THE BOOK* p 87

1. pas de correction pour Ear01.tex
2. pas de correction pour Ear02.tex
3. pas de correction pour Ear03.tex
4. (Car04) Soit $a_1, \cdots, a_p$ les racines distinctes de P et $\alpha_1, \cdots, \alpha_p$ leurs multiplicités. D'après la caractérisation de la multiplicté avec les dérivée, α_i est racine de P' de multiplicité $\alpha_i - 1$. On en déduit que
$$\deg(P \wedge P') = \sum_{i=1}^{p} (\alpha_i - 1) = \deg(P) - p.$$
Soit n le degré de P, si $\deg(P \wedge P') = 2$ alors P admet $n-2$ racines distinctes. Les deux cas possibles sont
   - $n-3$ racines simples et une triple a, $\deg(P \wedge P') = (X-a)^2$.
   - $n-4$ racines simples et deux doubles $a \neq b$, $\deg(P \wedge P') = (X-a)(X-b)$.

   Par exemple, pour $P = X^4 + qX^2 + rX + s$,
$$\deg(p \wedge P') = 2 \Leftrightarrow \begin{cases} 8r = 4pq - p^3 \\ 64s = (4q - p^2)^2 \end{cases}$$
5. pas de correction pour Ear05.tex
6. pas de correction pour Ear08.tex
7. pas de correction pour Ear09.tex
8. pas de correction pour Ear10.tex
9. (Car11) Les conditions imposées à P entraînent que 1 est une racine de $P-1$ et que -1 est une racine de $P+1$ avec des multiplicités au moins 4. En traduisant la multiplicité sur les dérivées, on déduit que 1 et -1 sont des racines de P' de multiplicité au moins 3. Un théorème de cours assure alors que
$$(X-1)^3(X+1)^3 = (X^2-1)^3$$
divise P'. On en déduit que si P est de degré 7, il doit vérifier
$$P' = \lambda(X^2-1)^3 \text{ avec } \lambda \in \mathbb{R}$$
Il doit donc être de la forme
$$P = \mu + \lambda X + \lambda X^3 + \frac{3}{5}\lambda X^5 + \frac{1}{7}\lambda X^7$$
et vérifier de plus
$$\widetilde{P}(1) = -1 \qquad \widetilde{P}(-1) = 1$$
Le système conduit à l'unique solution
$$P = -\frac{35}{96}\left(X + X^3 + \frac{3}{5}X^5 + \frac{1}{7}X^7\right)$$
10. pas de correction pour Ear12.tex
11. (Car13) Supposons qu'un tel polynôme P existe. Il est de degré 3 et unitaire donc $P(X+1) - P$ est de degré 2 et de coefficient dominant 3. De plus il est divisible par $X-2$ et $X-3$. On en déduit
$$P(X+1) - P = 3(X-2)(X-3) = 3X^2 - 15X + 18$$
On utilise alors des coefficients indéterminés. Si
$$P = X^3 + aX^2 + bX + c$$
En identifiant les coefficients, l'expression de $P(X+1) - P$ conduit à :
$$\begin{cases} 3 + 2a = -15 \\ a + b + 1 = 18 \end{cases} \Leftrightarrow \begin{cases} a = -9 \\ a + b + 1 = 26 \end{cases}$$
Donc P est de la forme
$$P = X^3 - 9X^2 + 26X + c$$
Le c est déterminé par $P(1) = 0$. On trouve $c = -18$. Le seul polynôme possible est donc
$$P = X^3 - 9X^2 + 26X + -18$$
Il est effectivement divible par $X-1$ et prend la valeur 24 en 2, 3, 4.
12. (Car14) Si P n'est pas irréductible, comme il est de degré 3, il admet une racine rationnelle $\frac{p}{q}$ avec $p \wedge q = 1$ qui vérifient
$$8p^3 - 6pq^2 - q^3 = 0$$
Comme p divise q^3, c'est 1 ou -1. Comme q divise $8p^3$ il ne reste plus qu'un nombre fini de cas à vérifier.
13. (Car17) Comme l'algorithme d'Euclide renvoie le pgcd, $A(y)$ est non nul si et seulement si P et $X^2 - y$ sont premiers entre eux. Comme tous les polynômes à coefficients complexes sont scindés, deux polynômes de $\mathbb{C}[X]$ sont premiers entre eux si et seulement si ils n'ont pas de racine en commun. On en déduit que $A(y) = 0$ si et seulement si P et $X^2 - y$ ont une racine en commun c'est à dire si et seulement si il existe $z \in \mathbb{C}$ tel que $y = z^2$ avec $\widetilde{P}(z) = 0$.
Pour l'exemple de l'énoncé, l'algorithme d'Euclide calcule
$$X^3 + 2X^2 - X + 3, \quad X^2 - y, \quad (y-1)X + 3 + 2y, \quad \left(\frac{3+2y}{1-y}\right)^2 - y$$
On en déduit que les racines de
$$Q = (3+2X)^2 - X(1-X)^2$$
sont les carrés de celles de P.
14. pas de correction pour Ear18.tex
15. (Car19) On implémente l'algorithme d'Euclide. On obtient la suite suivante :
$$X^4 - X + a, \; X^2 - aX + 1, \; (-1 - 2a + a^3)X + a + 1 - a^2, \; \frac{a+2}{(a+1)^2}$$
Les deux polynômes ont une racine en commun si et seulement si $a = -2$.

16. (Car20) Notons A le polynôme donné par l'énoncé et B celui obtenu en substituant $-X$ à X dans A.
Le polynôme A admet deux racines opposées si et seulement si A et B ont une racine en commun. On utilise donc l'algorithme d'Euclide qui conduit aux polynômes

$$\begin{aligned} &X^4-3X^3-12X^2+48X-64,\\ &\quad X^4+3X^3-12X^2-48X-64,\\ &\qquad -6X^3+96X,\ -64+4X^2,\ 0 \end{aligned}$$

On en déduit que les racines opposées sont 4 et -4. Le polynôme se factorise en

$$(X^2-16)(X^2-3X+4)$$

17. (Car21)

a. Notons α et β les valuations p-adiques de a et b. Comme a et b ne sont pas congrus à 0 modulo $q=p^m$, on sait que α et β sont strictement plus petits que m. Écrivons la congruence entre eux. Il existe $s\in\mathbb{Z}$ tel que

$$a=b+sp^m \Rightarrow \begin{cases} p^\alpha \text{ divise } b & \Rightarrow \alpha\leq\beta \\ p^\beta \text{ divise } a & \Rightarrow \beta\leq\alpha \end{cases} \Rightarrow \alpha=\beta$$

b. Remarquons que $v(x)\neq 0$ si et seulement si p divise x. Alors, comme p est premier avec $x-1$, le théorème de Bezout entraine $v(x-1)=0$. On raisonne de même si p divise $x-1$.

c. Introduisons un compteur : $2=1+1$, $q-1=1+q-2$ donc $\deg(P)=q-2$. Les valeurs de P aux entiers sont des quotients dont le numérateur est un produit de $q-2$ entiers consécutifs et $(q-2)!$ au dénominateur. C'est (au signe près) un coefficient du binôme donc un entier.

d. Pour tout z entier, $P(z)$ est entier avec

$$(q-2)!P(z)=n_z$$

où n_z est un entier qui est le produit de $q-2$ entiers consécutifs. Introduisons les valuations p-adiques. Comme p est fixé, on n'écrit pas l'indice p. Le point important est

$$\begin{aligned} &v((q-2)!)+v(P(z))=v(n_z) \text{ avec}\\ &\quad v((q-2)!)=v(2)+v(3)+\cdots+v(q-2). \end{aligned}$$

D'après la question a., on peut évaluer $v(n_z)$ en considérant les $z\geq q$ modulo q.
Si $z\equiv 0 \mod q$:

$$v(n_z)=v(q-2)+v(q-3)+\cdots+v(1)=v((q-2)!)$$

avec $v(1)=0$. On en tire

$$v(P(z))=0\Rightarrow P(z)\not\equiv 0 \mod p.$$

Si $z\equiv 1 \mod q$:

$$\begin{aligned} v(n_z)&=v(q-1)+v(q-2)+\cdots+v(2)\\ &=v((q-2)!) \end{aligned}$$

avec $v(q-1)=0$ car p ne divise pas $q-1$. On en tire $v(P(z))=0$ donc $P(z)\not\equiv 0 \mod p$.
Si $z\equiv 2 \mod q$:

$$\begin{aligned} v(n_z)&=v(q)+v(q-1)+\cdots+v(3)\\ &=m+v((q-2)!)-v(3) \end{aligned}$$

avec $v(q)=m$. On en tire $v(P(z))>0$ car $v(3)<m$ donc $P(z)\equiv 0 \mod p$.
Si $z\equiv i \mod q$ avec $1<i<q-1$:

$$\begin{aligned} &v(n_z)=v(q+i-2)+v(q+i-3)+\cdots+v(i+1)\\ &=v(i-2)+\cdots+v(1)+v(q)+v(q-1)+\cdots v(i+1)\\ &=m+v((q-2)!)-v(i)-v(i-1)>v((q-2)!) \end{aligned}$$

car un seul des $v(i)$ et $v(i-1)$ est non nul. On en tire $v(P(z))>0$ donc $P(z)\equiv 0 \mod p$.

18. pas de correction pour Ear22.tex

19. (Car23)

a. Il existe U_r et V_r dans $\mathbb{R}[X]$ tels que

$$D=U_rA+V_rB$$

On en tire que Δ divise D dans $\mathbb{C}[X]$.
De même, il existe U_c et V_c dans $\mathbb{C}[X]$ tels que

$$\Delta=U_cA+V_cB$$

On en tire que D divise Δ dans $\mathbb{C}[X]$. Les polynômes D et Δ se divisent mutuellement dans $\mathbb{C}[X]$ et sont unitaires, ils sont donc égaux.

b. Conjuguer, soustraire, simplifier.

20. (Car24)

a. Les polynômes $(X-1)^4$ et $(X+1)^4$ sont premiers entre eux. Voir dans le cours sur l'arithmétique euclidienne, la partie sur l'équation de Bézout.

b. Traduit l'unicité du couple solution après substitution de $-X$ à X.

c. On utilise développe avec la formule du binôme la relation

$$2^7=((X+1)+(X-1))^7$$

On en déduit

$$\begin{aligned} U=&(X+1)^3+7(X+1)^2(X-1)\\ &+21(X+1)(X-1)^2+35(X-1)^3 \end{aligned}$$