UN CORRIGÉ DU DEVOIR LIBRE N°8

§ 1 DES RACINES RATIONNELLES D'UN POLYNÔME À COEFFICIENTS ENTIERS

Soient $n \in \mathbb{N}_{\geqslant 2}$, $(a_k)_{k\in[\![0,n]\!]} \in \mathbb{Z}^{n+1}$ et $P := a_n X^n + a_{n-1}X^{n-1} + \ldots + a_2 X^2 + a_1 X + a_0$ un polynôme.

Q1 — Soit $(p,q) \in \mathbb{Z}\times\mathbb{N}^*$ tel que $p \wedge q = 1$. Démontrer que si $\dfrac{p}{q}$ est racine de P, alors $p \mid a_0$ et $q \mid a_n$.

Nous savons que $0 = \displaystyle\sum_{k=0}^{n} a_k \left(\frac{p}{q}\right)^k = \sum_{k=0}^{n} a_k p^k q^{-k}$. En multipliant chaque membre par q^n il vient

$$\sum_{k=0}^{n} a_k p^k q^{n-k} = 0\,. \tag{1}$$

De (1) nous déduisons

$$a_0 q^n = -\sum_{k=1}^{n} a_k p^k q^{n-k} = p\left(-\sum_{k=1}^{n} a_k p^{k-1} q^{n-k}\right).$$

Comme, pour tout $k \in [\![1,n]\!]$, $k-1 \geqslant 0$ et $n-k \geqslant 0$, l'entier p divise $a_0 q^n$. Comme p et q sont premiers entre eux, p et q^n le sont aussi. D'après le lemme de Gauß p divise a_0.
L'identité (1) livre également

$$a_n p^n = -\sum_{k=0}^{n-1} a_k p^k q^{n-k} = q\left(-\sum_{k=0}^{n-1} a_k p^k q^{n-k-1}\right).$$

Comme, pour tout $k \in [\![0,n-1]\!]$, $k \geqslant 0$ et $n-k-1 \geqslant 0$, l'entier q divise $a_n p^n$. Comme q et p sont premiers entre eux, q et p^n le sont aussi. D'après le lemme de Gauß q divise a_n.

Q2 — Déduire de **Q1** que le polynôme $X^n - X + 1$ ne possède aucune racine rationnelle.

Raisonnons par l'absurde et supposons que le polynôme $P = X^n - X + 1$ ait une racine rationnelle. Écrivons une telle sous forme irréductible $\dfrac{p}{q}$ où $(p,q) \in \mathbb{Z}\times\mathbb{N}^*$ vérifie $p \wedge q = 1$. D'après **Q1**, p divise 1 (donc $p = 1$ ou $p = -1$) et q divise 1 (donc $q = 1$).
Ainsi $\dfrac{p}{q} = 1$ ou $\dfrac{p}{q} = -1$. Comme

$$P(1) = 1 \neq 0 \qquad \text{et} \qquad P(-1) = \begin{cases} 1 \neq 0 & \text{si } n \text{ est pair} \\ -1 \neq 0 & \text{si } n \text{ est impair} \end{cases}$$

nous obtenons une contradiction.

Q3 — Déduire de **Q1** l'ensemble des racines complexes de $3X^3 + 8X^2 + 12X - 5$.

Commençons par déterminer si $P = 3X^3 + 8X^2 + 12X - 5$ possède une racine rationnelle.
Si $\dfrac{p}{q}$, où $(p,q) \in \mathbb{Z}\times\mathbb{N}^*$ vérifie $p \wedge q = 1$, est une racine rationnelle de P alors d'après **Q1** p divise -5 (donc $p \in \{-5,-1,1,5\}$) et q divise 3 donc $q \in \{1,3\}$. Ainsi les éventuelles racines rationnelles de P sont $-5, -1, 1, 5, -\dfrac{5}{3}, -\dfrac{1}{3}, \dfrac{5}{3}, \dfrac{1}{3}$. Comme

$$P(-5) = -240\,,\ P(-1) = -12\,,\ P(1) = 18\,,\ P(5) = 630\,,\ P\left(-\frac{5}{3}\right) = -\frac{50}{3}\,,\ P\left(-\frac{1}{3}\right) = -\frac{74}{9}\,,\ P\left(\frac{5}{3}\right) = \frac{460}{9}\,,\ P\left(\frac{1}{3}\right) = 0$$

le nombre $\dfrac{1}{3}$ est la seule racine rationnelle de P. D'après le cours, il existe un unique triplet (a,b,c) de réels tel que

$$3X^3 + 8X^2 + 12X - 5 = \left(X - \frac{1}{3}\right)\left(aX^2 + bX + c\right).$$

En analysant les coefficients dominants et constants, il vient $a = 3$ et $c = 15$ d'où

$$3X^3 + 8X^2 + 12X - 5 = \left(X - \frac{1}{3}\right)\left(3X^2 + bX + 15\right).$$

En étudiant le coefficient de degré 1 dans chacun des membres, nous obtenons $12 = 15 - \frac{b}{3}$ puis $b = 9$. Ainsi :

$$3X^3 + 8X^2 + 12X - 5 = \left(X - \frac{1}{3}\right)\left(3X^2 + 9X + 15\right) = 3\left(X - \frac{1}{3}\right)\left(X^2 + 3X + 5\right).$$

En calculant la forme canonique du trinôme du second degré $X^2 + 3X + 5$ nous obtenons finalement

$$3X^3 + 8X^2 + 12X - 5 = 3\left(X - \frac{1}{3}\right)\left(X + \frac{3 + i\sqrt{11}}{2}\right)\left(X + \frac{3 - i\sqrt{11}}{2}\right).$$

Ainsi $\mathrm{Spec}_{\mathbb{C}}(3X^3 + 8X^2 + 12X - 5) = \left\{\frac{1}{3}, -\frac{3 + i\sqrt{11}}{2}, \frac{-3 + i\sqrt{11}}{2}\right\}$.

§ 2 Critère de divisibilité par 3, 11 et 33

Soit $N \in \mathbb{N}^*$ d'écriture en base 10 notée $N = \sum_{k=0}^{p} a_k 10^k$, où $p \in \mathbb{N}$ et $(a_0, \dots, a_p) \in [\![0,9]\!]^{p+1}$ avec $a_p \neq 0$.

Q4 — Démontrer que 3 divise N si et seulement si 3 divise $\sum_{k=0}^{p} a_k$.

Il suffit de démontrer que N et $\sum_{k=0}^{p} a_k$ ont même reste modulo 3. Comme 10 est congru à 1 modulo 3 et comme les opérations $+$ et $\times$ sont compatibles aux congruences

$$\sum_{k=0}^{p} a_k 10^k \equiv \sum_{k=0}^{p} a_k 1^k \quad [3].$$

Comme $N = \sum_{k=0}^{p} a_k 10^k$ et $\sum_{k=0}^{p} a_k 1^k = \sum_{k=0}^{p} a_k$, la congruence annoncée au début est établie.

Q5 — Démontrer que 11 divise N si et seulement si 11 divise $\sum_{k=0}^{p} (-1)^k \cdot a_k$.

Analogue à **Q4**, en remarquant que 10 est congru à -1 modulo 11.

Q6 — Démontrer que N est divisible par 33 si et seulement si 3 divise $\sum_{k=0}^{p} a_k$ et 11 divise $\sum_{k=0}^{p} (-1)^k \cdot a_k$.

Nous raisonnons par double implication.
Supposons que N est divisible par 33. Alors N est divisible à la fois par 3 et par 11. D'après **Q4** et **Q5**, nous savons que 3 divise $\sum_{k=0}^{p} a_k$ et 11 divise $\sum_{k=0}^{p} (-1)^k \cdot a_k$.
Supposons que 3 divise $\sum_{k=0}^{p} a_k$ et 11 divise $\sum_{k=0}^{p} (-1)^k \cdot a_k$. D'après **Q4** nous savons qu'il existe $k_1 \in \mathbb{Z}$ tel que

$$N = 3k_1. \tag{2}$$

D'après **Q5**, 11 divise $N = 3k_1$. Comme $3 \wedge 11 = 1$, le lemme de Gauß livre 11 divise k_1. Il existe donc un entier k_2 tel que

$$k_1 = 11k_2. \tag{3}$$

D'après (2) et (3), $N = 33k_2$.

Q7 — Justifier que 12 435 687 est divisible par 33.

La somme des chiffres de 12 435 687 vaut 36 qui est divisible par 3.
La somme alternée des chiffres de 12 435 687 vaut 0 qui est divisible par 11.
D'après **Q6**, 12 435 687 est divisible par 33.

§ 3 Divisibilité par 7 d'une somme de carrés

Q8 — Soient $(a,b) \in \mathbb{Z}^2$. On suppose que 7 divise a^2+b^2. Démontrer qu'alors 7 divise a et b.

Nous allons nous appuyer sur les congruences modulo 7 et démontrer $a^2+b^2 \equiv 0\ [7]$ entraine que a et b sont congrus à 0 modulo 7.
Calculons tout d'abord les carrés modulo 7

$$0^2 \equiv 0\ [7] \quad ; \quad 1^2 \equiv 1\ [7] \qquad 2^2 \equiv 4\ [7] \qquad 3^2 \equiv 2\ [7] \qquad 4^2 \equiv 2\ [7] \qquad 5^2 \equiv 4\ [7] \qquad 6^2 \equiv 1\ [7]\,. \tag{4}$$

D'après la liste (4) et

$$\begin{array}{llll} 0+0 \equiv 0\ [7] & 0+1 \not\equiv 0\ [7] & 0+2 \not\equiv 0\ [7] & 0+4 \not\equiv 0\ [7] \\ 1+1 \not\equiv 0\ [7] & 1+2 \not\equiv 0\ [7] & 1+4 \not\equiv 0\ [7] & \\ 2+2 \not\equiv 0\ [7] & 2+4 \not\equiv 0\ [7] & & \\ 4+4 \not\equiv 0\ [7] & & & \end{array}$$

si a^2+b^2 est congru à 0 modulo 7 alors nécessairement a^2 et b^2 sont congrus à 0 modulo 7. Toujours d'après (4) si $n \in \mathbb{Z}$ vérifie $n^2 \equiv 0\ [7]$ alors $n \equiv 0\ [7]$. Ainsi a et b sont congrus à 0 modulo 7.

§ 4 Divisibilité par 13 d'un « grand nombre »

Q9 — Démontrer que 13 divise $2^{70}+3^{70}$.

Nous allons nous appuyer sur les congruences modulo 13 et démontrer que $2^{70}+3^{70} \equiv 0\ [13]$.
Le nombre 13 est premier. Les nombres 2 et 3 sont premiers avec 13. D'après le petit théorème de Fermat

$$2^{12} \equiv 1\ [13] \qquad \text{et} \qquad 3^{12} \equiv 1\ [13]\,.$$

Comme les opérations + et × sont compatibles aux congruences

$$2^{70}+3^{70} \equiv 2^{5\times 12+10}+3^{5\times 12+10} \equiv \left(2^{12}\right)^5 \times 2^{10} + \left(3^{12}\right)^5 \times 3^{10} \equiv 1^5 \times 2^{10} + 1^5 \times 3^{10} \equiv 2^{10}+3^{10}\ [13]\,. \tag{5}$$

En remarquant que $2^4 \equiv 3\ [13]$ et $3^3 \equiv 1\ [13]$, nous déduisons de (5) que

$$2^{70}+3^{70} \equiv 2^{10}+3^{10} \equiv 2^{4\times 2+2}+3^{3\times 3+1} \equiv \left(2^4\right)^2 \times 2^2 + \left(3^3\right)^2 \times 3^1 \equiv 3^2 \times 2^2 + 1^2 \times 3^1 \equiv 0\ [13]\,.$$

§ 5 Primalité relative d'une somme et d'un produit

Q10 — Soit $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$. Démontrer que $a+b$ et ab sont premiers entre eux si et seulement si $a+b$ et $a \cdot b$ sont premiers entre eux.

Nous raisonnons par double implication.
Supposons $a+b$ et ab premiers entre eux et considérons une relation de Bézout liant $a+b$ et ab

$$(a+b)u + abv = 1$$

où $(u,v) \in \mathbb{Z}^2$. Nous en déduisons

$$a(u+bv) + bu = 1\,.$$

Comme $u+bv$ et u sont entiers le théorème de Bézout livre $a \wedge b = 1$.
Supposons désormais $a+b$ et ab premiers entre eux. Considérons de plus d un diviseur positif commun à a et b. Il existe donc $(\alpha,\beta) \in \mathbb{Z}^2$ tel que $a = d\alpha$ et $b = d\beta$. Nous observons que

$$a+b = d(\alpha+\beta) \qquad \text{et} \qquad ab = d\alpha b$$

et en déduisons que d divise $a+b$ et ab ($\alpha+\beta$ et αb sont entiers). Or $(a+b)\wedge(ab)=1$. Ainsi $d=1$ et les nombres a et b sont premiers entre eux.

§ 6 PGCD DE DEUX NOMBRES DE FIBONACCI

On considère la suite de Fibonacci $(u_n)_{n\in\mathbb{N}}$, définie par $u_0=0$, $u_1=1$ et, pour tout $n\in\mathbb{N}$, $u_{n+2}=u_{n+1}+u_n$.

Q11 — Démontrer que, pour tout $n\in\mathbb{N}_{\geqslant 2}$, $u_n\in\mathbb{N}$ et $u_n<u_{n+1}$.

Démontrons que pour tout entier $n\geqslant 2$

$$\mathscr{P}(n)\ :\ \text{« } u_n\in\mathbb{N} \text{ et } u_n<u_{n+1}\text{ »}$$

à l'aide d'un raisonnement par récurrence à deux pas.
Initialisation à $n=2$ et $n=3$. Nous calculons $u_2=1$, $u_3=2$ et $u_4=3$. Ainsi $(u_2,u_3)\in\mathbb{N}^2$, $u_2<u_3$ et $u_3<u_4$.
Hérédité. Soit $n\in\mathbb{N}_{\geqslant 2}$ tel que $\mathscr{P}(n)$ et $\mathscr{P}(n+1)$ sont vraies.
Comme $(u_n,u_{n+1})\in\mathbb{N}^2$, $u_{n+2}=u_n+u_{n+1}\in\mathbb{N}$.
Comme $u_n<u_{n+1}$ et $u_{n+1}<u_{n+2}$

$$u_{n+2}=u_n+u_{n+1}<u_{n+1}+u_{n+2}=u_{n+3}\,.$$

Q12 — Démontrer que, pour tout $n\in\mathbb{N}^*$:

$$u_{n+1}\cdot u_{n-1}-u_n^2=(-1)^n\,.$$

Démontrons que pour tout $n\in\mathbb{N}^*$

$$\mathscr{P}(n)\ :\ \text{« } u_{n+1}\cdot u_{n-1}-u_n^2=(-1)^n\text{ »}$$

à l'aide d'un raisonnement par récurrence à deux pas.
Initialisation à $n=1$ et $n=2$. Comme

$$u_2\cdot u_0-u_1^2=1\cdot 0-1^2=-1=(-1)^1 \qquad \text{et} \qquad u_3\cdot u_1-u_2^2=2\cdot 1-1^2=1=(-1)^2$$

les assertions $\mathscr{P}(1)$ et $\mathscr{P}(2)$ sont vraies.
Hérédité. Soit $n\in\mathbb{N}^*$ tel que $\mathscr{P}(n)$ et $\mathscr{P}(n+1)$ sont vraies. Ainsi

$$u_{n+1}\cdot u_{n-1}-u_n^2=(-1)^n \qquad \text{et} \qquad u_{n+2}\cdot u_n-u_{n+1}^2=(-1)^{n+1}\,.$$

Nous calculons

$$\begin{aligned}
u_{n+3}\cdot u_{n+1}-u_{n+2}^2 &= (u_{n+2}+u_{n+1})\cdot(u_n+u_{n-1})-(u_{n+1}+u_n)^2\\
&= u_{n+2}u_n+u_{n+2}u_{n-1}+u_{n+1}u_n+u_{n+1}u_{n-1}-u_{n+1}^2-u_n^2-2u_nu_{n+1}\\
&= \left(u_{n+2}u_n-u_{n+1}^2\right)+\left(u_{n+1}u_{n-1}-u_n^2\right)+u_{n+2}u_{n-1}-u_nu_{n+1}\\
&= (-1)^{n+1}+(-1)^n+(u_{n+1}+u_n)u_{n-1}-u_n(u_n+u_{n-1})\\
&= u_{n+1}u_{n-1}-u_n^2\\
&= (-1)^n\,.
\end{aligned}$$

Nous en déduisons $u_{n+3}\cdot u_{n+1}-u_{n+2}^2=(-1)^{n+2}$ d'où $\mathscr{P}(n+2)$.

Q13 — Démontrer que, pour tout $n\in\mathbb{N}$:

$$u_n\wedge u_{n+1}=1\,.$$

Soit $n\in\mathbb{N}$. Nous raisonnons par disjonction de cas, suivant la parité de n.
Supposons n pair. D'après **Q12**

$$u_n\cdot u_{n+2}+u_{n+1}\cdot(-u_{n+1})=1\,.$$

D'après le théorème de Bézout, $u_n\wedge u_{n+1}=1$.

Supposons n impair. D'après **Q12**, $u_n \cdot u_{n+2} + u_{n+1} \cdot (-u_{n+1}) = -1$ d'où

$$u_n \cdot (-u_{n+2}) + u_{n+1} \cdot u_{n+1} = 1\,.$$

D'après le théorème de Bézout, $u_n \wedge u_{n+1} = 1$.

Q14 — Démontrer que, pour tout $m \in \mathbb{N}^*$, pour tout $n \in \mathbb{N}$:

$$u_{m+n} = u_m \cdot u_{n+1} + u_{m-1} \cdot u_n\,.$$

Soit $m \in \mathbb{N}^*$. Démontrons que pour tout $n \in \mathbb{N}$

$$\mathscr{P}(n) : \text{« } u_{m+n} = u_m \cdot u_{n+1} + u_{m-1} \cdot u_n \text{ »}$$

à l'aide d'un raisonnement par récurrence à deux pas.
Initialisation à $n = 0$ et $n = 1$. Nous calculons

$$u_m \cdot u_1 + u_{m-1} \cdot u_0 = u_m = u_{m+0} \qquad \text{et} \qquad u_m \cdot u_2 + u_{m-1} \cdot u_1 = u_m + u_{m-1} = u_{m+1}$$

et donc les assertions $\mathscr{P}(0)$ et $\mathscr{P}(1)$ sont vraies.
Hérédité. Soit $n \in \mathbb{N}$ tel que $\mathscr{P}(n)$ et $\mathscr{P}(n+1)$ sont vraies. Ainsi

$$u_{m+n} = u_m \cdot u_{n+1} + u_{m-1} \cdot u_n \qquad \text{et} \qquad u_{m+n+1} = u_m \cdot u_{n+2} + u_{m-1} \cdot u_{n+1}\,.$$

Nous calculons

$$\begin{aligned} u_m \cdot u_{n+3} + u_{m-1} \cdot u_{n+2} &= u_m \cdot (u_{n+2} + u_{n+1}) + u_{m-1}(u_{n+1} + u_n) \\ &= u_m \cdot u_{n+2} + u_{m-1} \cdot u_{n+1} + u_m \cdot u_{n+1} + u_{m-1} u_n \\ &= u_{m+n+1} + u_{m+n} \\ &= u_{n+n+2}\,. \end{aligned}$$

Q15 — Déduire de **Q14** que, pour tout $(m, n) \in \mathbb{N}^* \times \mathbb{N}$:

$$u_m \wedge u_n = u_m \wedge u_{m+n}\,.$$

Soit $(m, n) \in \mathbb{N}^* \times \mathbb{N}$. Nous démontrons que $\mathrm{Div}(u_m) \cap \mathrm{Div}(u_n) = \mathrm{Div}(u_m) \cap \mathrm{Div}(u_{m+n})$ par double inclusion, ce qui livrera le résultat par passage au max.
Soit $d \in \mathrm{Div}(u_m) \cap \mathrm{Div}(u_n)$. Alors il existe des entiers k_1, k_2 tels que $u_m = k_1 \cdot d$ et $u_n = k_2 \cdot d$. D'après **Q14**

$$u_{m+n} = u_m \cdot u_{n+1} + u_{m-1} \cdot u_n = d \cdot (k_1 \cdot u_{n+1} + k_2 \cdot u_{m-1})$$

et donc $d \in \mathrm{Div}(u_{m+n})$. Ainsi $d \in \mathrm{Div}(u_m) \cap \mathrm{Div}(u_{m+n})$.
Soit $d \in \mathrm{Div}(u_m) \cap \mathrm{Div}(u_{m+n})$. Alors il existe des entiers k_1, k_2 tels que $u_m = k_1 \cdot d$ et $u_{m+n} = k_2 \cdot d$. D'après **Q14**

$$u_{m-1} \cdot u_n = u_{m+n} - u_m \cdot u_{n+1} = d \cdot (k_2 - k_1 \cdot u_{n+1})$$

et donc d divise $u_{m-1} \cdot u_n$. Comme d divise u_m et $u_m \wedge u_{m-1} = 1$ (**Q13**), d et u_{m-1} sont premiers entre eux. D'après le lemme de Gauß, d divise u_n. Ainsi $d \in \mathrm{Div}(u_m) \cap \mathrm{Div}(u_n)$.

Q16 — Soit n et m deux entiers naturels tels que $1 \leqslant m \leqslant n$. Considérons la division euclidienne de n par m :

$$n = q \cdot m + r$$

où $(q, r) \in \mathbb{N} \times [\![0, m-1]\!]$. Démontrer que :

$$u_m \wedge u_r = u_m \wedge u_n\,.$$

D'après **Q15**

$$u_m \wedge u_r = u_m \wedge u_{m+r} = u_m \wedge u_{2m+r} = u_m \wedge u_{3m+r} = \ldots = u_m \wedge u_{qm+r} = u_m \wedge u_n \,.$$

Q17 — Déduire de **Q16** que, pour tout $(m,n) \in \mathbb{N}^* \times \mathbb{N}^*$:

$$u_m \wedge u_n = u_{m\wedge n} \,.$$

Nous raisonnons par récurrence sur le nombre $N \in \mathbb{N}^*$ d'étapes dans l'algorithme d'Euclide calculant $m \wedge n$.
Initialisation à $N = 1$. Soient m et n des entiers tels que $1 \leqslant m \leqslant n$. On suppose que l'algorithme d'Euclide calcule $m \wedge n$ en 1 étape. Alors le reste de la division de n par m vaut 0, i.e. m divise n. Dans ce cas, $m \wedge n = m$. D'après **Q16**

$$u_m \wedge u_0 = u_m \wedge u_n \,.$$

Comme $u_0 = 0$, il vient

$$u_m \wedge u_n = u_m \wedge 0 = u_m = u_{m\wedge n} \,.$$

Hérédité. Soit $N \in \mathbb{N}^*$. On suppose que le résultat est vrai pour tous les couples d'entiers $(m',n') \in \mathbb{N}^* \times \mathbb{N}^*$ tels que l'algorithme d'Euclide calcule $m' \wedge n'$ en N étapes. Soit $(m,n) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $1 \leqslant m \leqslant n$. On suppose que l'algorithme d'Euclide calcule $m \wedge n$ en $N+1 \geqslant 2$ étapes. Ainsi, si r est le reste de la division euclidienne de n par m, alors $r \geqslant 1$ et le calcul de $m \wedge r$ par l'algorithme d'Euclide compte N étapes. D'après l'hypothèse de récurrence

$$u_m \wedge u_r = u_{m\wedge r} \,. \tag{6}$$

L'algorithme d'Euclide livre $m \wedge r = m \wedge n$. D'après **Q16**, $u_m \wedge u_n = u_m \wedge u_r$. Ainsi (**Q7**) se réécrit

$$u_m \wedge u_n = u_{m\wedge n} \,.$$

Q18 — Exprimer, pour tout $n \in \mathbb{N}$, u_n à l'aide du nombre d'or $\Phi := \dfrac{1+\sqrt{5}}{2}$.

La suite $(u_n)_{n\in\mathbb{N}}$ est une suite récurrente linéaire d'ordre 2 dont l'équation caractéristique est

$$r^2 - r - 1 = 0$$

d'inconnue $r \in \mathbb{C}$. Cette équation possède deux solutions $\Phi := \dfrac{1+\sqrt{5}}{2}$ et $\dfrac{1-\sqrt{5}}{2}$. Comme le produit des deux solutions vaut 1 (cf. relations coefficients-racines pour un trinôme du second degré) $\dfrac{1-\sqrt{5}}{2} = -\dfrac{1}{\Phi}$. D'après le cours, il existe des nombres réels λ_1 et λ_2 tels que, pour tout $n \in \mathbb{N}$

$$u_n = \lambda_1 \cdot \Phi^n + \lambda_2 \cdot \left(-\frac{1}{\Phi}\right)^n \,.$$

Comme $u_0 = 0$ et $u_1 = 1$, λ_1 et λ_2 sont solutions du système

$$\begin{cases} \lambda_1 + \lambda_2 = 0 \\ \lambda_1 \cdot \Phi - \lambda_2 \cdot \dfrac{1}{\Phi} = 1 \,. \end{cases}$$

Nous en déduisons $\lambda_1 = \dfrac{1}{\sqrt{5}}$ et $\lambda_2 = -\dfrac{1}{\sqrt{5}}$ d'où, pour tout $n \in \mathbb{N}$

$$u_n = \frac{1}{\sqrt{5}} \cdot \left(\Phi^n + (-1)^{n+1} \cdot \Phi^{-n}\right) \,.$$

Q19 — Donner un équivalent « simple » de u_n.

D'après **Q18**, pour tout $n \in \mathbb{N}$

$$u_n = \frac{\Phi^n}{\sqrt{5}}\left(1 + (-1)^{n+1} \cdot \Phi^{-2n}\right).$$

Comme $\Phi > 1$, $\Phi^{-2n} \longrightarrow 0$. Nous en déduisons que $u_n \sim \dfrac{\Phi^n}{\sqrt{5}}$.

§ 7 Équations de congruences affines

Q20 — Résoudre l'équation :

$$5 \cdot x + 4 \equiv 3\ [13]$$

d'inconnue $x \in \mathbb{Z}$.

Notons que $5 \times 5 \equiv -1\ [13]$ et donc $1 \equiv 5 \times (-5)\ [13]$. Le nombre 5 est inversible modulo 13 (le petit théorème de Fermat l'assurait) et son inverse modulo 13 est -5. Ainsi, pour tout $x \in \mathbb{Z}$

$$\begin{aligned} 5 \cdot x + 4 \equiv 3\ [13] &\iff 5 \cdot x \equiv -1\ [13] \\ &\iff x \equiv 5\ [13] \qquad \left[(-5)\times \text{ pour } \Longrightarrow \text{ et } 5\times \text{ pour } \Longleftarrow\right]. \end{aligned}$$

Nous en déduisons que l'ensemble solution de l'équation est $\{5 + 13 \cdot k\ :\ k \in \mathbb{Z}\}$.

Q21 — Résoudre l'équation :

$$5 \cdot x + 4 \equiv 3\ [35]$$

d'inconnue $x \in \mathbb{Z}$.

Nous démontrons que l'équation n'a aucune solution en raisonnant par l'absurde.
Supposons dont qu'il existe $x \in \mathbb{Z}$ tel que $5 \cdot x + 4 \equiv 3\ [35]$. Nous en déduisons, en multipliant membre-à-membre par 7 modulo 35 que

$$0 + 28 \equiv 21\ [35]$$

ce qui n'est pas.

§ 8 Équations diophantiennes d'ordre un en deux variables

Q22 — Résoudre l'équation :

$$429 \cdot x + 700 \cdot y = 1$$

d'inconnue $(x, y) \in \mathbb{Z}^2$. On pourra commencer par chercher une solution particulière, avant de les déterminer toutes au moyen d'un raisonnement par analyse et synthèse.

Calculons tout d'abord $429 \wedge 700$ à l'aide de l'algorithme d'Euclide.

$$\begin{aligned} 700 &= 429 \times 1 + 271 \\ 429 &= 271 \times 1 + 158 \\ 271 &= 158 \times 1 + 113 \\ 158 &= 113 \times 1 + 45 \\ 113 &= 45 \times 2 + 23 \\ 45 &= 23 \times 1 + 22 \\ 23 &= 22 \times 1 + 1 \\ 22 &= 1 \times 22 + 0 \end{aligned}$$

Nous en déduisons que $429 \wedge 700 = 1$. L'équation admet donc une solution.
Cherchons une solution particulière de l'équation, i.e. une relation de Bézout liant 429 et 700, en remontant l'algorithme d'Euclide ci-dessus.

$$\begin{aligned}
1 &= 23-22\\
&= 23-45+23 = 2\cdot 23-45\\
&= 2\cdot(113-2\cdot 45)-45 = 2\cdot 113-5\cdot 45\\
&= 2\cdot 113-5\cdot(158-113)\\
&= 7\cdot 113-5\cdot 158\\
&= 7\cdot(271-158)-5\cdot 158\\
&= 7\cdot 271-12\cdot 158\\
&= 7\cdot 271-12\cdot(429-271)\\
&= 19\cdot 271-12\cdot 429\\
&= 19\cdot(700-429)-12\cdot 429\\
&= 19\cdot 700-31\cdot 429
\end{aligned}$$

Ainsi $(x_0, y_0) := (-31, 19)$ est solution de l'équation.
Résolvons à présent l'équation en raisonnant par analyse et synthèse.
Analyse. Soit $(x, y) \in \mathbb{Z}^2$ une solution de l'équation. En soustrayant membre-à-membre les deux identités

$$429\cdot x+700\cdot y = 1 \qquad \text{et} \qquad 429\cdot x_0+700\cdot y_0 = 1$$

il vient $429\cdot(x-x_0)+700\cdot(y-y0) = 0$ puis

$$429\cdot(x-x_0) = 700\cdot(y_0-y)\,. \tag{7}$$

Ainsi 429 divise $700\cdot(y_0-y)$. Comme 429 et 700 sont premiers entre eux, le lemme de Gauß livre que 429 divise y_0-y. Donc il existe $k\in\mathbb{Z}$ tel que

$$y_0-y = 429\cdot k\,. \tag{8}$$

De (7) et (9) on déduit

$$429\cdot(x-x_0) = 700\cdot 429\cdot k\,.$$

Comme $\mathbb{Z}$ est intègre, il vient $x-x_0 = 700\cdot k$. De cette étude, nous déduisons $(x, y) = (x_0+700\cdot k, y_0-429\cdot k)$.
Synthèse. Soit $k\in\mathbb{Z}$ et $(x, y) := (x_0+700\cdot k, y_0-429\cdot k)$. Alors comme (x_0, y_0) est solution de l'équation

$$429\cdot x+700\cdot y = 429\cdot(x_0+700\cdot k)+700\cdot(y_0-429\cdot k) = 429\cdot x_0+700\cdot y_0 = 1$$

donc (x, y) est également solution de l'équation.
L'ensemble solution de l'équation est donc $\{(-31+700\cdot k, 19-429\cdot k)\ :\ k\in\mathbb{Z}\}$.

Q23 — Résoudre l'équation :

$$323\cdot x-391\cdot y = 365$$

d'inconnue $(x, y)\in\mathbb{Z}^2$.

Comme précédemment nous appliquons l'algorithme d'Euclide pour calculer $323\wedge 391 = 17$. En particulier, 17 divisent 323 et 391.
Nous calculons la division euclidienne de 365 par 17

$$365 = 21\cdot 17+8$$

et en déduisons que $365\equiv 8\ [17]$.
Nous démontrons que l'équation n'a aucune solution en raisonnant par l'absurde.
Supposons dont qu'il existe $x\in\mathbb{Z}$ tel que $323\cdot x-391\cdot y = 365$. En considérant les congruences modulo 17 il vient

$$0\equiv 8\ [17]$$

ce qui n'est pas.

§ 9 Une équation diophantienne d'ordre trois en deux variables

On souhaite résoudre l'équation :

$$(E)\quad m^3-n^3 = 999$$

d'inconnue $(m, n)\in\mathbb{N}^2$.

Q24 — Soit (m, n) une solution de (E). Démontrer que $m-n$ est un diviseur positif de 999 inférieur à 10, puis dresser la liste de toutes les valeurs possibles du couple $(m-n, mn)$.

Comme (m,n) est solution de l'équation

$$999 = m^3 - n^3 = (m-n)\cdot(m^2+mn+n^2) = (m-n)\cdot\left((m-n)^2+3mn\right). \tag{9}$$

Comme $m^3 - n^3 \geqslant 0$, $m \geqslant n$ et donc $m - n \geqslant 0$.
De (9), nous déduisons également que $m-n$ divise 999.
D'autre part, si $m-n>10$ alors

$$999 = m^3 - n^3 = (m-n)\cdot\left((m-n)^2+3mn\right) \geqslant (m-n)^3 > 1000$$

ce qui n'est pas. Ainsi $m-n \leqslant 10$.
Nous avons établi que $m-n$ est un diviseur positif de $999 = 3^3\cdot 37$ inférieur ou égal à 10. Ainsi $m-n \in \{1,3,9\}$.
En exploitant de nouveau (9), nous trouvons trois valeurs possibles pour le couple $(m-n, mn)$

$$\left(1, \frac{998}{3}\right) \quad , \quad (3,108) \quad , \quad (9,10)\,.$$

Comme mn est entier, nous en déduisons que

$$(m-n, mn) \in \{(3,108), (9,10)\}\,.$$

Q25 — À l'aide de **Q24**, déterminer l'ensemble solution de l'équation (E).

Nous raisonnons par analyse-synthèse.
Analyse. Soit (m,n) une solution de l'équation. D'après **Q24**, le couple $(m-n, mn)$ peut prendre deux valeurs.

— Cas où $(m-n, mn) = (3,108)$. D'après les relations coefficients-racines, m et $-n$ sont racines du trinôme du second degré

$$X^2 - 3X - 108\,.$$

Donc $(m,n) = (9,12)$ ou $(m,n) = (12,9)$. Comme $m > n$, $(m,n) = (12,9)$.

— Cas où $(m-n, mn) = (9,10)$. D'après les relations coefficients-racines, m et $-n$ sont racines du trinôme du second degré

$$X^2 - 9X - 10\,.$$

Donc $(m,n) = (1,10)$ ou $(m,n) = (10,1)$. Comme $m > n$, $(m,n) = (10,1)$.

Synthèse. Nous vérifions aisément que les couples $(12,9)$ et $(10,1)$ sont solutions de (E).
Conclusion. L'équation possède deux solutions : $(12,9)$ et $(10,1)$.

§ 10 Congruences simultanées et théorème des restes chinois

Soient m_1, m_2 des entiers premiers entre eux et $(a_1,a_2) \in \mathbb{Z}^2$. On considère le système d'équations de congruences :

$$(S_2) \quad \begin{cases} x \equiv a_1 \ [m_1] \\ x \equiv a_2 \ [m_2] \end{cases}$$

d'inconnue $x \in \mathbb{Z}$.

Q26 — Démontrer que le système (S_2) possède une solution.

Considérons une relation de Bézout liant m_1 et m_2 :

$$m_1 u + m_2 v = 1$$

où $(u,v) \in \mathbb{Z}^2$. Nous observons

$$\begin{cases} m_1 u \equiv 0 \ [m_1] \\ m_1 u \equiv 1 \ [m_2] \end{cases} \quad \text{et} \quad \begin{cases} m_2 v \equiv 1 \ [m_1] \\ m_2 v \equiv 0 \ [m_2] \end{cases}$$

et en déduisons

$$\begin{cases} a_2 m_1 u + a_1 m_2 v & \equiv & a_1 & [m_1] \\ a_2 m_1 u + a_1 m_2 v & \equiv & a_2 & [m_2] \end{cases}$$

Le nombre entier $a_2 m_1 u + a_1 m_2 v$ est donc solution de (S_2).

Q27 — Soit x_p une solution particulière de (S_2). Démontrer :

$$\mathrm{Sol}_{(S_2)} = \left\{ x_p + k \cdot m_1 \cdot m_2 \,:\, k \in \mathbb{Z} \right\} .$$

Notons que la solution particulière x_p existe d'après **Q26**.
Nous raisonnons par double inclusion.
Soit x une solution de S_2. Alors

$$\begin{cases} x & \equiv & a_1 & [m_1] \\ x & \equiv & a_2 & [m_2] \end{cases} \quad \text{et} \quad \begin{cases} x_p & \equiv & a_1 & [m_1] \\ x_p & \equiv & a_2 & [m_2] \end{cases}$$

d'où

$$\begin{cases} x - x_p & \equiv & 0 & [m_1] \\ x - x_p & \equiv & 0 & [m_2] \end{cases}$$

Comme m_1 divise $x - x_p$, il existe $k_1 \in \mathbb{Z}$ tel que

$$x - x_p = k_1 \cdot m_1 . \tag{10}$$

Comme m_2 divise $x - x_p = k_1 \cdot m_1$ et comme $m_1 \wedge m_2 = 1$, le lemme de Gauß livre m_2 divise k_1. Ainsi il existe $k_2 \in \mathbb{Z}$ tel que

$$k_1 = k_2 \cdot m_2 . \tag{11}$$

De (10) et (11), on déduit $x - x_p = k_2 \cdot m_1 \cdot m_2$. Ainsi $x \in \left\{ x_p + k \cdot m_1 \cdot m_2 \,:\, k \in \mathbb{Z} \right\}$.
Soit $x \in \left\{ x_p + k \cdot m_1 \cdot m_2 \,:\, k \in \mathbb{Z} \right\}$. Alors il existe $k \in \mathbb{Z}$ tel que $x = x_p + k \cdot m_1 \cdot m_2$. Comme x_p est solution de (S_2), il vient

$$x \equiv x_p \equiv a_1 \ [m_1] \qquad \text{et} \qquad x \equiv x_p \equiv a_2 \ [m_2]$$

et donc x est solution de (S_2).

Nous souhaitons étendre le résultat précédent au cas de trois équations de congruences simultanées. Soient à présent m_1, m_2, m_3 des entiers deux-à-deux premiers entre eux et $(a_1, a_2, a_3) \in \mathbb{Z}^3$. On considère le système d'équations de congruences :

$$(S_3) \quad \begin{cases} x & \equiv & a_1 & [m_1] \\ x & \equiv & a_2 & [m_2] \\ x & \equiv & a_3 & [m_3] \end{cases}$$

d'inconnue $x \in \mathbb{Z}$.

Q28 — Déduire de **Q26** et **Q27** que le système (S_3) possède une solution et que :

$$\mathrm{Sol}_{(S_3)} = \left\{ x_p + k \cdot m_1 \cdot m_2 \cdot m_3 \,:\, k \in \mathbb{Z} \right\} .$$

où x_p désigne une solution particulière de (S_3).

Soit $x \in \mathbb{Z}$.
Les entiers m_1 et m_2 sont premiers entre eux. D'après **Q26**, le système

$$(S_2) \quad \begin{cases} x & \equiv & a_1 & [m_1] \\ x & \equiv & a_2 & [m_2] \end{cases}$$

possède une solution x_p, que nous pouvons calculer à l'aide d'une relation de Bézout liant m_1 et m_2.
D'après **Q27**

$$(S_2) \quad \begin{cases} x & \equiv & a_1 & [m_1] \\ x & \equiv & a_2 & [m_2] \end{cases} \quad \Longleftrightarrow \quad x \equiv x_p \ [m_1 \cdot m_2]$$

et donc

$$(S_3) \quad \begin{cases} x & \equiv & a_1 & [m_1] \\ x & \equiv & a_2 & [m_2] \\ x & \equiv & a_3 & [m_3] \end{cases} \quad \Longleftrightarrow \quad (S_2') \quad \begin{cases} x & \equiv & x_p & [m_1 \cdot m_2] \\ x & \equiv & a_3 & [m_3] \end{cases}$$

D'après le cours, $m_1 \wedge m_3 = 1$ et $m_2 \wedge m_3$ entraîne $(m_1 \cdot m_2) \wedge m_3 = 1$. D'après **Q26**, le système (S_2') possède une solution possède une solution x_q, que nous pouvons calculer à l'aide d'une relation de Bézout liant $m_1 \cdot m_2$ et m_3.

D'après **Q27**

$$(S_2') \iff x \equiv x_q \quad [m_1 \cdot m_2 \cdot m_3]$$

De cette étude, nous déduisons que x_q est une solution de (S_3) et que

$$\text{Sol}_{(S_3)} = \{x_p + k \cdot m_1 \cdot m_2 \cdot m_3 \,:\, k \in \mathbb{Z}\} \,.$$

Q29 — Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager également, et de donner le reste au cuisinier. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Le cuisinier recevrait alors 4 pièces. Dans un naufrage ultérieur, seuls le butin, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier quand il décide d'empoisonner le reste des pirates ?

Il s'agit ici de trouver la plus petite solution strictement positive du système de congruences

$$(S_3) \quad \begin{cases} x \equiv 3 \quad [17] \\ x \equiv 4 \quad [11] \\ x \equiv 5 \quad [6] \end{cases}$$

d'inconnue $x \in \mathbb{Z}$. Nous commençons par résoudre le système (S_3) en suivant la démarche exposée dans **Q28**, après avoir remarqué que les entiers $17, 11, 6$ sont premiers entre eux.
Nous commençons par calculer une relation de Bézout liant 17 et 11.

$$2 \cdot 17 - 3 \cdot 11 = 1 \,.$$

D'après la solution proposée en (26)

$$x_p = 4 \cdot 2 \cdot 17 - 3 \cdot 3 \cdot 11 = 37$$

est solution de

$$(S_2) \quad \begin{cases} x \equiv 3 \quad [17] \\ x \equiv 4 \quad [11] \end{cases}$$

et, pour tout $x \in \mathbb{Z}$

$$(S_2) \iff x \equiv 37 \quad [17 \cdot 11]$$

Ainsi

$$(S_3) \iff (S_2') \quad \begin{cases} x \equiv 37 \quad [17 \cdot 11] \\ x \equiv 5 \quad [6] \end{cases}$$

Nous calculons une relation de Bézout liant $17 \cdot 11 = 187$ et 6

$$1 \cdot 187 - 6 \cdot 31 = 1 \,.$$

D'après la solution proposée en (26)

$$x_q = 5 \cdot 1 \cdot 187 - 37 \cdot 6 \cdot 31 = -5947$$

est solution de (S_2') donc de (S_3).
D'après **Q28**

$$\text{Sol}_{(S_3)} = \{-5947 + k \cdot 1122 \,:\, k \in \mathbb{Z}\} \,.$$

La fortune minimale que peut espérer le cuisinier est le plus petit élément strictement positif de $\text{Sol}_{(S_3)}$, donc 785.