Leonid Monin
Léo Navarro Chafloque

Solutions – Semaine 7

Exercice 1.
Entiers de Gauss.

1. Montrer que l'anneau $\mathbb{Z}[i]$ est euclidien avec $N(a+ib) = a^2+b^2$. Pour $a, b \in \mathbb{Z}[i], a \neq 0$ on appelle une égalité de la forme $b = aq + r$, avec $q, r \in \mathbb{Z}[i]$ et $N(r) < N(a)$ une division avec reste.

   Indication: Montrer que pour diviser b par a il suffit de trouver $q \in \mathbb{Z}[i]$ avec $|\frac{b}{a} - q| < 1$ Où $|-|$ est la norme complexe.

2. Effectuer une division avec reste de $5+5i$ par $4+2i$ et montrer que les quotients et restes de la division dans $\mathbb{Z}[i]$ ne sont pas uniques.

3. Les entiers de Gauss $2, 3$ et 5 sont-ils irréductibles dans $\mathbb{Z}[i]$? Et $2i$ et $2-3i$?

4. Montrer que le quotient $\mathbb{Z}[i]/(3)$ est un corps de cardinalité 9.

Solution.

1. On voit d'abord qu'il faut et il suffit de trouver q tel que $N(b-aq) < N(a)$. Ensuite en divisant par a on voit que c'est équivalent à trouver un tel $q \in \mathbb{Z}[i]$ avec

$$|\frac{b}{a} - q| < 1.$$

   Maintenant cela est toujours possible: soit $q \in \mathbb{Z}[i]$ tel que $|Re(q-b/a)| \leq \frac{1}{2}$ et $|Im(q-b/a)| \leq 1/2$. On voit maintenant que $|q - b/a \leq \sqrt{2}/2 < 1$.

2. We first do this division in $\mathbb{C}$. There, we obtain that

$$\frac{(5+5i)}{(4+2i)} = \frac{(5+5i)(-4+2i)}{(4+2i)(-4+2i)} = \frac{3}{2} + \frac{1}{2}i.$$

   By either rounding up or down both the real and imaginary part, we find the closest elements in $\mathbb{Z}[i]$ to be the quotients $1, 2, 1+i, 2+i$. The division by these with rest are

   - $(5+5i) = 1 \cdot (4+2i) + (1+3i)$
   - $(5+5i) = 2 \cdot (4+2i) + (-3+i)$
   - $(5+5i) = (1+i) \cdot (4+2i) + (3-i)$
   - $(5+5i) = (2+i) \cdot (4+2i) + (-1-3i)$

   Remark that we need to take the closest elements in $\mathbb{Z}[i]$ to $\frac{3}{2} + \frac{1}{2}i \in \mathbb{C}$ as otherwise the norm of the rest would exceed the norm of $4+2i$, which is a contradiction. In all of the above cases, this is satisfied. This also shows that the quotent and rest of the euclidean division are not unique.

3. We have

   - $2 = (1+i)(1-i)$ and since $1+i, 1-i \notin (\mathbb{Z}[i])^\times$ it follows that 2 is not irreducible. On note que *en tant qu'idéaux* $(2) = (1+i)^2$.

- Assume that $3 = x \cdot y$, with $x, y \in \mathbb{Z}[i]$. Then $9 = N(xy) = N(x)N(y)$, so both $N(x)$ and $N(y)$ divide 9. This is possible if $N(x), N(y) \in \{1, 3, 9\}$. If $N(x) = 1$, then x is a unit. If $N(x) = 9$, then $N(y) = 1$ and y is a unit. If $N(x) = 3$, with $x = a + ib$ for $a, b \in \mathbb{Z}$, then $N(x) = a^2 + b^2$, but for natural numbers a and b this is impossible. So $N(x) \neq 3$, and the only way to write 3 as a product of two elements x, y in $\mathbb{Z}[i]$ is if either of them is a unit, which means that 3 is irreducible.
- $5 = (2 + i)(2 - i)$ is not irreducible, as both factors are not units.
- $2i = (1 + i)^2$ is not irreducible, as $1 + i$ is not a unit.
- Since $N(2 - 3i) = 13$ is irreducible in $\mathbb{Z}$, it follows that $2 - 3i$ is irreducible in $\mathbb{Z}[i]$.

  Remarque. Comme $\mathbb{Z}[i]$ est euclidien, donc principal, donc *factoriel*, un élément est irréductible si et seulement si l'idéal associé est premier. Ainsi pour $a + bi \in \mathbb{Z}[i]$ le quotient
  $$\mathbb{Z}[t]/(t^2 + 1, a + bt)$$
  est intègre si et seulement si $a + bi$ est irréductible.

4. We note that $\mathbb{Z}[i]$ is Euclidean, from which it follows that $\mathbb{Z}[i]$ is principal. The since 3 is irreducible in $\mathbb{Z}[i]$, the ideal (3) is maximal in $\mathbb{Z}[i]$. It follows that $\mathbb{Z}[i]/(3)$ is a field.

   Comme
   $$\mathbb{Z}[i]/(3) \cong \mathbb{F}_3[t](t^2 + 1)$$
   c'est un $\mathbb{F}_3$-espace vectoriel de dimension 2, donc de cardinalité 9.

Exercice 2.
Entiers d'Eisenstein. Soit $\omega = e^{\frac{2\pi i}{3}}$ et $\mathbb{Z}[\omega]$ l'anneau des entiers d'Eisenstein.

1. Montrer que $N(a+b\omega) = a^2 - ab + b^2$ coïncide avec le module au carré dans le plan complexe de $a + b\omega$.

2. Montrer que $N(a + b\omega) = a^2 - ab + b^2$ munit $\mathbb{Z}[\omega]$ d'une fonction euclidienne. On pourra par exemple montrer que le point milieu d'une maille du réseau $\mathbb{Z}[\omega]$ se trouve à une distance strictement plus petite que 1 de chacun des quatre sommets de cette maille.

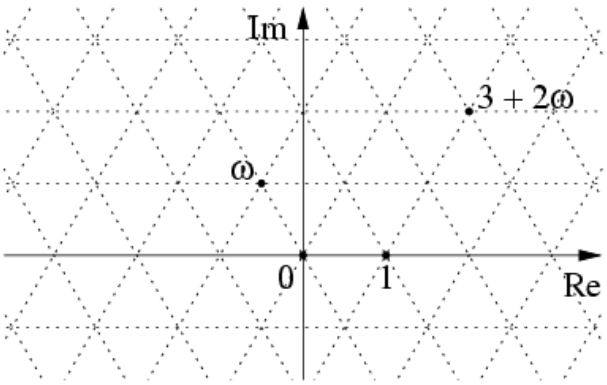
3. Trouver les éléments inversibles de $\mathbb{Z}[\omega]$ (quelle est leur norme?).

Solution.

1. On the one hand, we have $\mid a + b\omega \mid^2 = (a + b\omega)(a + b\bar{\omega}) = a^2 + ab(\omega + \bar{\omega}) + b^2\omega\bar{\omega}$. On the other hand, we see that both $\omega = e^{\frac{2\pi i}{3}}$ and its complex conjugate $\bar{\omega} = e^{-\frac{2\pi i}{3}}$ are roots of the polynomial $z^3 - 1 = 0$. Since $z^3 - 1 = (z - 1)(z^2 + z + 1)$, both ω and $\bar{\omega}$ are roots of the polynomial $(z^2 + z + 1)$ and therefore $(z^2 + z + 1) = (z - \omega)(z - \bar{\omega}) = z^2 - (\omega + \bar{\omega})z + \omega\bar{\omega}$, from which it follows by comparing coefficients that $\omega + \bar{\omega} = -1$ and $\omega\bar{\omega} = 1$. Therefore, $\mid a + b\omega \mid^2 = a^2 - ab + b^2 = N(a + b\omega)$.

2. La norme au carré étant toujours positive, la formule définissant N montre que cette norme prend des valeurs entières. Pour montrer qu'il s'agit d'une fonction euclidienne on procède

comme pour les entiers de Gauss. Voici une illustration tirée de Wikipedia de $\mathbb{Z}[\omega]$:



La maille fondamentale de ce réseau est un losange de côté 1 dont les sommets sont par exemples $0, 1, \omega$ et $1+\omega$, ce dernier étant aussi de norme $1-1+1=1$. Ainsi la petite diagonale est de longueur 1 et la grande est de longueur $\sqrt{3} = \sqrt{N(1-\omega)}$. Par conséquent le cercle dont le centre est le milieu du losange (point d'intersection des diagonales) et dont le rayon vaut $\sqrt{3}/2$ contient toute la maille. Comme $\sqrt{3} < 2$ on a $\sqrt{3}/2 < 1$ ce qui montre qu'étant donné $0 \neq x, y \in \mathbb{Z}[\omega]$ alors on trouve toujours $q \in \mathbb{Z}[\omega]$ avec $|y/x - q| < 1$. On conclut que N est une fonction Euclidienne pour $\mathbb{Z}[\omega]$

3. Let $z \in \mathbb{Z}[\omega]$ be invertible, with inverse element denoted by z^{-1}. Then by the multiplicative properties of the norm, we have that $1 = N(1) = N(z) \cdot N(z^{-1})$, and therefore, $N(z) \in \mathbb{N}$ needs to be equal to 1. This is obtained for the elements $z = \pm 1, \pm\omega, \pm(1+\omega)$. One checks that these are indeed units: ± 1 is clearly a unit, and by the first point, we have that $\omega + \bar{\omega} = -1$. From this, it follows with $\omega^2 = \bar{\omega}$ that $\omega(1+\omega) = \omega + \omega^2 = \omega + \bar{\omega} = -1$. Hence the inverse of $\pm\omega$ is $\mp(1+\omega)$.

Exercice 3.
L'anneau $\mathbb{Z}[i\sqrt{5}]$.

1. Montrer que le polynôme $3 + 2t + 2t^2$ irréductible dans $\mathbb{Z}[i\sqrt{5}][t]$, mais pas dans $\mathbb{Q}[i\sqrt{5}][t]$.

2. **Généralisation.** Soient a, b, c, d des éléments irréductibles non associés d'un anneau commutatif et intègre A tels que $ab = cd$. Calculer $(a+ct)(b+ct)$ et conclure que le polynôme $d + (a+b)t + ct^2$ est irréductible dans $A[t]$, mais pas dans $K[t]$ où K est le corps des fractions de A.

3. Montrer qu'il n'y a pas de fonction euclidienne sur $\mathbb{Z}[i\sqrt{5}]$.

Solution.

1. On sait grâce à la norme complexe que 3 et 2 sont irréductibles dans $\mathbb{Z}[i\sqrt{5}]$. Supposons que

$$3 + 2t + 2t^2 = fg$$

avec f et g des éléments de $\mathbb{Z}[i\sqrt{5}][t]$. Le degré de ces éléments doit être 0 et 2 ou 1 et 1. S'il y avait un élément de degré zéro, alors il diviserait 3 et serait donc inversible. Traitons maintenant le cas de degré 1. Notons que les termes constants divisent 3 donc sans perte de généralité (comme 3 est irréductible et que les seuls inversibles de l'anneau sont ± 1) disons on a pour $x, y \in \mathbb{Z}[i\sqrt{5}]$

$$3 + 2t + 2t^2 = (xt+3)(yt+1) = xyt^2 + (3y+x)t + 3.$$

Alors $xy = 2$ et $3y + x = 2$. Ainsi on $3y^2 + 2 = 2y$. Donc $2 = y(2 - 3y)$. Comme 2 est irréductible on a les possibilités suivantes. Si $y = 2$ alors $-4 = 2 - 3y = 1$, c'est absurde. Si $y = -2$ alors $8 = 2 - yc = -1$, encore absurde. Si $y = 1$ alors $2 = 2 - 3y = -1$, absurde. Si $y = -1$ alors $-2 = 2 - 3y = 5$, absurde.

On conclut finalement que ce polynôme est irréductible dans $\mathbb{Z}[i\sqrt{5}]$.

We calculate the complex roots of the polynomial $3 + 2t + 2t^2$. They are $\frac{-2 \pm i\sqrt{20}}{4} = \frac{-1 \pm i\sqrt{5}}{2}$. The roots are elements in $\mathbb{Q}[i\sqrt{5}]$ and we have that $3+2t+2t^2 = 2(t+\frac{1+i\sqrt{5}}{2})(t+\frac{1-i\sqrt{5}}{2})$. This means that $3 + 2t + 2t^2$ is not irreducible in $\mathbb{Q}[i\sqrt{5}]$, as we can express it as the product of $2(t + \frac{1+i\sqrt{5}}{2})$ and $(t + \frac{1-i\sqrt{5}}{2})$, both of which are not units.

2. **Généralisation.** We calculate

$$(a + ct)(b + ct) = ab + (cb + ac)t + c^2t = cd + (cb + ac)t + c^2t = c(d + (a + b)t + ct^2)$$

which shows that the roots of $d + (a + b)t + ct^2$ are $-a/c$ and $-b/c$ in K. This shows that in K, we can write the polynomial $d + (a + b)t + ct^2$ as the product $c(t + \frac{a}{c})(t + \frac{b}{c})$, with both terms $c(t + \frac{a}{c})$ and $(t + \frac{b}{c})$, not units. Hence the polynomial is not irreducible in K.

On the other hand, in $A[t]$ the polynomial is irreducible. This we prove using a slightly different method thant the previous point, which could also be applied to the previous point. We assume that the polynomial decoposes into a product of two non-invertible polynomials f and g. As in the previous point we can suppose that f and g are of degree 1, otherwise one would be invertible because d is suppose irreducible.

So we now assume that the degree of f and g is 1. As c is irreducible, let's suppose that the leading coefficient of f is c and the one of g is 1. Now, note that $K[t]$ is Euclidean, so it is an UFD (=anneau factoriel). Also. the decomposition of $d + (a + b)t + ct^2$ as the product $c(t + \frac{a}{c})(t + \frac{b}{c})$ is a decomposition in irreducibles. But now we also have in $K[t]$

$$c(t + \frac{a}{c})(t + \frac{b}{c}) = fg.$$

Using the unicity in the UFD property (unicité dans la définition d'anneau factoriel) and recalling that f and g are degree one polynomials with leading coefficient being c and 1 respectively, we see that

$$g = (t + \frac{a}{c}) \quad \text{or} \quad g = (t + \frac{b}{c}).$$

But as a, c and b, c are distinct irreducibles in A, we see that a/c and b/c are not in A, a contradiction.

3. Dividing $-2 + i\sqrt{5}$ by $1 + i\sqrt{5}$ with rest and calculating the norm of the rest, we see that if $\mathbb{Z}[i\sqrt{5}]$ with the norm $N(a + i\sqrt{5}b) = a^2 + 5b^2$ was Euclidean, then the norm of the rest would need to be smaller than the norm of $1 + i\sqrt{5}$, which is 6. We perform the division over $\mathbb{C}$, and obtain $\frac{-2+i\sqrt{5}}{1+i\sqrt{5}} = \frac{1}{2} + i\frac{1}{2}\sqrt{5}$. The closest elements in $\mathbb{Z}[i\sqrt{5}]$ are $0, i\sqrt{5}, 1, 1 + i\sqrt{5}$. It holds that

- $-2 + i\sqrt{5} = (1 + i\sqrt{5}) \cdot 0 + (-2 + i\sqrt{5}) = 0 + (-2 + i\sqrt{5})$ with $N(-2 + i\sqrt{5}) = 9$
- $-2 + i\sqrt{5} = (1 + i\sqrt{5}) \cdot i\sqrt{5} + 3 = (-5 + i\sqrt{5}) + 3$ with $N(3) = 9$
- $-2 + i\sqrt{5} = (1 + i\sqrt{5}) \cdot 1 + (-3) = (1 + i\sqrt{5}) + (-3)$ with $N(-3) = 9$
- $-2+i\sqrt{5} = (1+i\sqrt{5})\cdot(1+i\sqrt{5})+(2-\sqrt{5}) = (-4+i2\sqrt{5})+(2-\sqrt{5})$ with $N(2-\sqrt{5}) = 9$

As the norm of every rest is bigger than 6, we can not find $q, r \in \mathbb{Z}[i\sqrt{5}]$ such that $-2+i\sqrt{5} = q(1+i\sqrt{5}) + r$ with $N(r) < N(1+i\sqrt{5})$, which means that $\mathbb{Z}[i\sqrt{5}]$ equipped with N is not Euclidean.

Note that we can also look at the calculations above in a geometric way. The four elements 0, $1+i\sqrt{5}$, $-5+i\sqrt{5}$ et $-4+2i\sqrt{5}$ are the edges of the rectangle of the lattice spanned by $(1+i\sqrt{5})$ that contains $-2+i\sqrt{5}$.

Exercice 4.
En s'inspirant de $\mathbb{Z}[i]$ montrer que $\mathbb{Z}[i\sqrt{2}]$ est Euclidien.

Solution.
La technique de l'exercice 1 s'applique texto car en reprenant les notations, on trouve $q \in \mathbb{Z}[i\sqrt{3}]$ avec

$$\left|\Re e\left(\frac{b}{a} - q\right)\right| \leq \frac{1}{2} \qquad \text{et} \qquad \left|\Im m\left(\frac{b}{a} - q\right)\right| \leq \frac{1}{\sqrt{2}}$$

La clé étant que la diagonale des carrés des mailles de $\mathbb{Z}[i\sqrt{2}]$ est de longueur 2 par Pythagore. Alors la distance du point milieu au sommet est de $1/2$, ce qui explique l'affirmation ci-dessus. Ceci implique que

$$\left|\frac{b}{a} - q\right|^2 \leq \frac{1}{2^2} + \frac{1}{2} = \frac{3}{4} < 1$$

et on conclut similairement.

Exercice 5.
Considérons les polynômes $f = x^3 - 2x^2 + x - 2$ et $g = x^4 - 2x^3 + 7x - 14$ dans $\mathbb{Z}[x]$.

1. Montrez que le pgdc de f et de g dans $\mathbb{Z}[x]$ vaut $x-2$ en écrivant $f = (x-2)f_0$ et $g = (x-2)g_0$ dans $\mathbb{Z}[x]$.

2. Pour un premier p, notons $\bar{f}$ et $\bar{g}$ la réduction de f et g dans $\mathbb{F}_p[x]$. Calculez le pgdc de $\bar{f}$ et de $\bar{g}$ pour chaque p.
Indication : Remarquez que les étapes de l'algorithme d'Euclide définissables dans $\mathbb{Z}[x]$ sont des étapes de l'algorithme d'Euclide dans $\mathbb{F}_p[x]$ après réduction modulo p.

Solution.

1. On vérifie que
$$f(x) = (x-2)(x^2+1) \;\text{ et }\; g(x) = (x-2)(x^3+7),$$
et on prétend que x^2+1 et x^3+7 sont premiers entre eux. En fait, ces deux polynômes sont primitifs et ne se décomposent pas dans $\mathbb{Q}[x]$ (car -1 n'as pas de racine carrée dans $\mathbb{Q}$, et -7 n'a pas de racine cubique dans $\mathbb{Q}$), et donc ils sont irréductibles en vertu du lemme de Gauss III. Ainsi $x-2$ est un pgdc de f et de g.

2. Les décompositions $f = (x-2)(x^2+1)$ et $g = (x-2)(x^3+7)$ sont encore valables après la réduction modulo p. Après cette réduction, le pgdc n'est plus égal à $x - [2]_p$ si et seulement si $x^2 + [1]_p$ et $x^3 + [7]_p$ ne sont plus premiers entre eux dans $\mathbb{F}_p[x]$.

   Notons qu'on peut écrire (en suivant la méthode de l'algorithme d'Euclide dans $\mathbb{Q}[x]$, même si $\mathbb{Z}[x]$ n'est pas euclidien, et en se limitant aux étapes qui restent dans $\mathbb{Z}[x]$) :

$$x^3 + 7 = x(x^2+1) + (-x+7), \quad x^2 + 1 = (-x-7)(-x+7) + 50$$

   et ces égalités sont encore valables modulo p. En fait, comme $\mathbb{F}_p[x]$ est un anneau euclidien dont la fonction euclidienne est donnée par le degré, la réduction modulo p de ces deux égalités

donne les deux premiers pas de l'algorithme d'Euclide pour $x^3+[7]_p$ et $x^2+[1]_p$ (voir l'Exercice 1.1). Notons que le second reste est $[50]_p$. Si $[50]_p = 0$, alors l'algorithme est complet et

$$\text{pgdc}(x^2 + [1]_p, x^3 + [7]_p) = -x + [7]_p \quad \text{et ainsi} \quad \text{pgdc}(\bar{f}, \bar{g}) = (x - [2]_p)(-x + [7]_p).$$

Si $[50]_p \neq 0$, alors il s'agit d'une unité dans $\mathbb{F}_p[x]$, et donc la prochaine étape de l'algorithme donne un reste nul. Ainsi le pgdc de $x^2 + [1]_p$ et de $x^3 + [7]_p$ est une unité, autrement dit ces deux polynômes sont encore premiers entre eux.

Puisque $50 = 2 \cdot 5^2$, on a $[50]_p = 0$ si et seulement si $p \in \{2, 5\}$. Ainsi :

(a) Si $p \notin \{2, 5\}$, alors $\text{pgdc}(\bar{f}, \bar{g}) = x - [2]_p$.

(b) Si $p = 2$, alors $\text{pgdc}(\bar{f}, \bar{g}) = x(x + [1]_2)$.

(c) Si $p = 5$, alors $\text{pgdc}(\bar{f}, \bar{g}) = (x - [2]_5)(-x + [2]_5)$.

Exercice 6. 1. Soit $d > 0$ un entier positif. Montrez que $\mathbb{Q}[i\sqrt{d}]$ est un corps de fractions de $\mathbb{Z}[i\sqrt{d}]$.

2. Montrez que $x^3 - 2i$ est irréductible dans $(\mathbb{Z}[i])[x]$.
Indication : Utilisez le lemme de Gauss, et gardez en tête qu'un élément de $\mathbb{Q}[i]$ peut s'écrire comme $\frac{a+bi}{n}$ avec $a, b, n \in \mathbb{Z}$.

Solution.

1. Montrons d'abord que $\mathbb{Q}[i\sqrt{d}]$ est un corps. Puisque $(i\sqrt{d})^2 \in \mathbb{Q}$, on voit que

$$\mathbb{Q}[i\sqrt{d}] = \{a + bi\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

Les inverses de ces éléments existent dans $\mathbb{C}$, où ils sont donnés par

$$(a + bi\sqrt{d})^{-1} = \frac{a - bi\sqrt{d}}{|a + bi\sqrt{d}|^2}, \quad \text{où } |a + bi\sqrt{d}|^2 = a^2 + b^2 d \in \mathbb{Q}.$$

Le côté droit appartient aussi à $\mathbb{Q}[i\sqrt{d}]$, on en déduit donc qu'il s'agit d'un corps.

On a l' inclusion évidente $\mathbb{Z}[i\sqrt{d}] \subset \mathbb{Q}[i\sqrt{d}]$. Pour chaque $a + bi\sqrt{d} \in \mathbb{Q}[i\sqrt{d}]$, on peut écrire

$$a + bi\sqrt{d} = \frac{a'}{n} + \frac{b'}{n} i\sqrt{d}$$

où n est le plus petit dénominateur commun de a et b, et $a', b' \in \mathbb{Z}$. Ainsi $\mathbb{Q}[i\sqrt{d}]$ est un corps de fractions pour $\mathbb{Z}[i\sqrt{d}]$.

2. Montrons que $x^3 - 2i$ est irréductible dans $\mathbb{Z}[i][x]$. Puisque le coefficient dominant est une unité, ce polynôme est primitif. En vertu du lemme de Gauss et du premier point, il est irréductible dans $\mathbb{Z}[i][x]$ si et seulement si il est irréductible dans $\mathbb{Q}[i][x]$. Si $x^3 - 2i$ se décompose dans $\mathbb{Q}[i][x]$, l'un des facteurs doit être un polynôme linéaire. Donc $x^3 - 2i$ est irréductible dans $\mathbb{Q}[i][x]$ si et seulement si il n'a pas de racines dans $\mathbb{Q}[i]$.

Supposons que $2i$ possède une racine cubique dans $\mathbb{Q}[i]$. On peut écrire cette racine $\frac{a+bi}{n}$, avec $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$. On a alors

$$n^3 2i = (a + bi)^3$$

et en prenant les modules au carré, on obtient

$$4n^6 = (a^2 + b^2)^3.$$

C'est une égalité entre deux entiers, on peut donc compter les puissances de 2 dans chaque membre et s'apercevoir qu'elles n'ont pas le même reste modulo 3. C'est une contradiction. Ainsi $2i$ n'a pas de racine cubique dans $\mathbb{Q}[i]$.

On a donc montré que $x^3 - 2i$ est irréductible dans $\mathbb{Z}[i][x]$.

Remarque : Le critère d'Eisenstein ne peut être invoqué pour résoudre l'exercice. En effet la décomposition en facteurs irréductibles de $2i$ est

$$2i = (1+i)^2,$$

où $1+i$ est irréductible, comme il est de norme 2.