Déf 1 : Une équation diophantienne est une équation de la forme $P(x_1, \dots, x_n) = 0$ où $P \in \mathbb{Z}[X_1, \dots, X_n]$ dont on cherche des solutions entières.

Ex 2 : Si $P(X,Y,Z) = X^n + Y^n - Z^n$, on obtient l'équation de Fermat $x^n + y^n = z^n$

I - Equations diophantiennes linéaires

A - Relations de Bezout [CON]

Ex 3 : L'équation $ax = b$ a une solution ssi $a \mid b$.

Thm 4 [BEZOUT] Soient $a, b \in \mathbb{Z}$, soit $d = \text{pgcd}(a,b)$
alors $\exists u, v \in \mathbb{Z}$, $au + bv = d$

Réciproquement, si $au + bv = c$
alors $a \wedge b \mid c$

Cor 5 : L'équation $ax + by = c$ admet une solution si et seulement si $a \wedge b \mid c$.

Rq 6 : On peut trouver explicitement des solutions grâce à l'algorithme d'Euclide.

Ex 7 :
- $42x + 66y = 10$ n'admet aucune solution
- $112x + 70y = 14$ admet des solutions par exemple $(2, -3)$.

B - Cas général d'un système linéaire [COA]

Soient $A \in \mathcal{M}_{m,n}(\mathbb{Z})$, $B \in \mathbb{Z}^m$.
On veut résoudre $AX = B$ avec $X \in \mathbb{Z}^n$.

Prop 8 : Si $A = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right)$ $d_1, \dots, d_r \in \mathbb{Z}^*$:

$$AX = B \iff \begin{cases} \forall i \in [\![1, r]\!], & d_i x_i = b_i \\ \forall i \in [\![r+1, m]\!], & b_i = 0 \end{cases}$$

Il y a une solution si et seulement si :

$$\begin{cases} \forall i \in [\![1, r]\!], & d_i \mid b_i \\ \forall i \in [\![r+1, m]\!], & b_i = 0 \end{cases}$$

Thm 9 : Soit $A \in \mathcal{M}_{m,n}(\mathbb{Z})$, il existe une unique famille d'entiers strictement positifs $d_1, \dots, d_r$ tels que :
- $d_1 \mid d_2 \mid \dots \mid d_r$
- $\exists U \in GL_m(\mathbb{Z}), \exists V \in GL_n(\mathbb{Z})$,

$$UAV = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right)$$

Rq 10 : On peut calculer explicitement les facteurs invariants $d_1, \dots, d_r$ d'une matrice en utilisant la division euclidienne dans $\mathbb{Z}$.

Ex 11 : $\begin{pmatrix} 2 & 4 \\ 3 & 8 \end{pmatrix} = P \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} Q$ où $P = \begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix} \in GL_2(\mathbb{Z})$
$Q = \begin{pmatrix} 1 & 4 \\ 0 & -1 \end{pmatrix} \in GL_2(\mathbb{Z})$

Prop 12 : Si $A = PDQ$ avec $D = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right)$, $P \in GL_m(\mathbb{Z})$, $Q \in GL_n(\mathbb{Z})$

$$AX = B \iff D(QX) = P^{-1}B$$
$$\iff X = Q^{-1}\tilde{X} \text{ et } D\tilde{X} = P^{-1}B$$

Ex 13 : $\begin{cases} 2x + 4y = -2 \\ 3x + 8y = 1 \end{cases}$ a pour unique solution $(x, y) = (-5, 2)$

II - Méthode géométrique [CON]

A - Equation $x^2 + y^2 = z^2$

Prop 14 : Soit $\mathcal{C}$ le cercle d'équation $X^2 + Y^2 = 1$
Alors $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ est une paramétrisation rationnelle de $\mathcal{C}$, c'est-à-dire :

$$\mathcal{C} = \left\{\left(\tfrac{1-t^2}{1+t^2}, \tfrac{2t}{1+t^2}\right) \mid t \in \mathbb{R}\right\} \text{ et } \left(t \in \mathbb{Q} \iff \left(\tfrac{1-t^2}{1+t^2}, \tfrac{2t}{1+t^2}\right) \in \mathbb{Q}^2\right)$$

Thm 15 : Les solutions primitives de $x^2+y^2=z^2$ sont exactement les triplets $(u^2-v^2, 2uv, u^2+v^2)$ où $u \wedge v = 1$.

L'ensemble des solutions de $x^2+y^2=z^2$ est donc $\{(d(u^2-v^2), 2duv, d(u^2+v^2)) \mid u,v,d \in \mathbb{Z}, u \wedge v = 1\}$

[OVT1]

Ex 16 : En prenant $u=2, v=1$, on obtient le triplet $(3,4,5)$

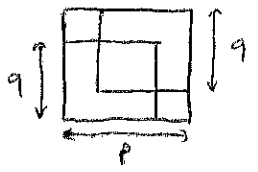
Avec $u=7, v=2$ par exemple, on a $(45, 28, 53)$

Cor 17 : Il n'existe pas de solution non triviale à l'équation $x^4+y^4=z^4$

Rq 18 : On utilise pour cela une méthode de descente : partant d'une solution positive, on construit une solution positive strictement plus petite en un certain sens.

Ex 19 : Si $p^2 = 2q^2$ avec $p, q > 0$ alors $(2q-p)^2 = 2(p-q)^2$ et :

$$\begin{cases} 0 < 2q-p < p \\ 0 < p-q < q \end{cases}$$



B- Equation $x^3+y^3 = xyz$

Prop 20 : Soit $\mathcal{F}$ le folium de Descartes d'équation $X^3+Y^3 = XY$

Alors $\left(\frac{t}{1+t^3}, \frac{t^2}{1+t^3}\right)$ est une paramétrisation rationnelle de $\mathcal{F}$.

Thm 21 : Les triplets (uv^2, u^2v, u^3+v^3) où $u \wedge v = 1$ sont des solutions primitives de $x^3+y^3 = xyz$.

Ex 22 : . $u=1, v=1 \Rightarrow (1,1,2)$ est solution

. $u=3, v=5 \Rightarrow (75, 45, 152)$ est solution

III- Méthodes algébriques

A- Anneau des entiers d'un corps quadratique [OUV]

Déf 23 : Un corps quadratique sur $\mathbb{Q}$ est une extension de $\mathbb{Q}$ dans $\mathbb{C}$ de degré 2.

Prop 24 : Tout corps quadratique sur $\mathbb{Q}$ est de la forme $\mathbb{Q}[\sqrt{d}]$ avec $d \in \mathbb{Z}$ sans facteurs carrés.

Déf 25 : Le conjugué de $x = a+b\sqrt{d}$ dans $\mathbb{Q}[\sqrt{d}]$ est $x^* = a-b\sqrt{d}$

La norme de x est $N(x) = xx^* = a^2-db^2$

Prop 26 : . $(x+y)^* = x^*+y^*$ et $(xy)^* = x^*y^*$

. $N(xy) = N(x)N(y)$.

Déf 27 : Un élément x de $\mathbb{Q}[\sqrt{d}]$ est dit entier s'il est annulé par un polynôme unitaire à coefficients dans $\mathbb{Z}$.

On note $\mathbb{A}_d$ l'ensemble des entiers de $\mathbb{Q}[\sqrt{d}]$.

Prop 28 : $\mathbb{A}_d$ est un sous-anneau de $\mathbb{Q}[\sqrt{d}]$

Thm 29 : . Si $d \equiv 2$ ou $3 \bmod 4$, $\mathbb{A}_d = \mathbb{Z}[\sqrt{d}]$

. Si $d \equiv 1 \bmod 4$, $\mathbb{A}_d = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

Déf 30 : $\varepsilon \in \mathbb{A}_d$ est appelé unité si $\varepsilon \in \mathbb{A}_d^\times$

Prop 31 : Soit $z \in A_d$. $z \in A_d^* \Leftrightarrow |N(z)| = 1$

Thm 32 : Soit $d < 0$ sans facteurs carrés.
- Si $d = -1$, $A_d^* = \{\pm 1, \pm i\}$
- Si $d = -3$, $A_d^* = \{\pm 1, \pm j, \pm \bar{j}\}$
- Sinon, $A_d^* = \{\pm 1\}$

Thm 33 : A_d est euclidien pour le stathme N dès que $d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 13\}$

B- Applications aux équations diophantiennes

* $\mathbb{Z}[i]$ est euclidien [DUV] [PER]

Thm 34 [2 carrés] : [DVT $\sqrt{2}$]
- Soit p premier. Il existe une solution à $x^2+y^2=p$ si et seulement si $p=2$ ou $p \equiv 1 [4]$
- Soit $n \in \mathbb{N}$, $n > 1$. Il existe une solution à $x^2+y^2=n$ si et seulement si pour tout premier $p \equiv 3 [4]$, $v_p(n)$ est pair.

Thm 35 : L'équation de Mordell $y^2 = x^3 - 1$ a pour unique solution $(1, 0)$.

* $\mathbb{Z}[j]$ est euclidien

Prop 36 : $\forall x \in \mathbb{Z}[j], \exists \varepsilon \in \mathbb{Z}[j]^*, \exists y \in \mathbb{Z}[i\sqrt{3}], x = \varepsilon y$.

Thm 37 : L'équation $x^3+y^3 = z^3$ n'a pas de solution non triviale.

Rq 38 : $\mathbb{Z}[\sqrt{-3}]$ n'est pas euclidien. Il n'est en fait même pas factoriel :

$$2 \times 2 = (1+i\sqrt{3})(1-i\sqrt{3})$$

C- Equation de Pell-Fermat [HIN]

L'équation est $x^2 - dy^2 = \pm 1$ (*), $d > 0$

Prop 39 : $(x, y) \in \mathbb{Z}^2$ est solution de (*) si et seulement si $x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]^\times$

Thm Lo : Soit $d > 0$. Il existe une unité $\omega > 1$ telle que $\mathbb{Z}[\sqrt{d}]^\times = \{\pm \omega^n \mid n \in \mathbb{Z}\}$

Cor 41 : Soit $d > 0$. Il existe une solution non triviale $(x_1, y_1) \in (\mathbb{N}^*)^2$ à $(*)' : x^2 - dy^2 = 1$ telle que l'ensemble des solutions soit :

$$\{(\pm x_n, \pm y_n) \mid x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, n \in \mathbb{N}^*\}$$

On a alors : $(x_{n+1}, y_{n+1}) = (x_1 x_n + d y_1 y_n, y_1 x_n + x_1 y_n)$

Rq 42 : Il existe un algorithme pour trouver cette solution fondamentale qui utilise le développement en fraction continue de $\sqrt{d}$.

Ex 43 : Si $d = 19$, la solution fondamentale de $x^2 - 19y^2 = 1$ est $(170, 39)$

App 44 : Chercher les triangles rectangles à côtés entiers dont les petits côtés sont des entiers consécutifs revient à chercher $(x, z) \in (\mathbb{N}^*)^2$ tels que

$$(2x+1)^2 - 2z^2 = -1$$

Références :

- [COM] Combes, Algèbre et géométrie
- [OA] Beck, Malick, Peyré, Objectif Agrégation
- [OUV] Ouvrey, Théorie des nombres
- [PER] Perrin, Cours d'algèbre
- [HIN] Hindry, Arithmétique

Résolution de $x^2 + y^2 = z^2$ et $x^4 + y^4 = z^2$

Référence : Combes, *Algèbre et géométrie*

Théorème 1 *Des entiers x, y, z vérifient l'équation $x^2+y^2 = z^2$ si, et seulement si il existe $d \in \mathbb{Z}$ et $u, v \in \mathbb{Z}$ premiers entre eux tels que (x, y, z) ou (y, x, z) soit égal à $(d(u^2-v^2), 2duv, d(u^2+v^2))$.*

Démonstration :

Tout d'abord, un calcul simple montre que les triplets exhibés sont effectivement solution.

Soit (x, y, z) un triplet non trivial vérifiant $x^2 + y^2 = z^2$. Quitte à diviser x, y et z par leur pgcd, on peut supposer qu'ils sont premiers entre eux. Mais d'après l'équation, si d divise deux des nombres x, y, z, alors il divise le troisième. On peut donc même supposer x, y, z premier entre eux deux à deux.
Ainsi, seul l'un des trois peut être pair, et ça ne peut être z car sinon on aurait $x^2 \equiv y^2 \equiv 1[4]$ et donc $z^2 \equiv 2[4]$ ce qui est absurde puisqu'il est divisible par 4. On peut donc finalement supposer **x impair, y pair, et z impair, et premiers entre eux deux à deux.**

Maintenant, il apparait que $(\frac{x}{z})^2 + (\frac{y}{z})^2 = 1$, ce qui, par la paramétrisation rationnelle du cercle, implique l'existence d'un rationnel t tel que la paire $\{\frac{x}{z}, \frac{y}{z}\}$ soit égale à $\{\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\}$. Ecrivons $t = \frac{u}{v}$ avec $u \wedge v = 1$. On a alors

$$\{\frac{x}{z}, \frac{y}{z}\} = \{\frac{v^2-u^2}{u^2+v^2}, \frac{2uv}{u^2+v^2}\}$$

• Supposons d'abord que $\begin{cases} \frac{x}{z} = \frac{v^2-u^2}{u^2+v^2} \\ \frac{y}{z} = \frac{2uv}{u^2+v^2} \end{cases}$

Montrons que v^2-u^2, u^2+v^2 et $2uv$ sont premiers entre eux deux à deux. Puisqu'ils vérifient l'équation initiale, il suffit pour cela de montrer qu'ils sont premier entre eux dans leur ensemble. Soit donc p un nombre premier divisant v^2-u^2, u^2+v^2 et $2uv$.

Par somme et différence de v^2-u^2 et u^2+v^2, on voit que p divise $2u^2$ et $2v^2$. Si $p \neq 2$, alors p divise u^2 et v^2, donc u et v, ce qui est exclus. Donc $p = 2$

Puisque u^2+v^2 est pair, u et v ont même parité. Mais comme u et v sont premiers entre eux, ils sont tous deux impairs. Notons $u = 2k+1$ et $v = 2l+1$. Alors on a

$$\frac{x}{z} = \frac{4(l^2+l-k^2-k)}{2(2k^2+2k+2l^2+2l+1)} = \frac{2m}{2n+1}$$

où $m = l^2+l-k^2-k$ et $n = l^2+l+k^2+k$, ce qui contredit l'imparité de x.
Finalement, v^2-u^2, u^2+v^2 et $2uv$ sont bien premiers entre eux deux à deux et on peut donc identifier : $\begin{cases} x = v^2-u^2 \\ y = 2uv \end{cases}$

• Supposons[1] maintenant que $\begin{cases} \frac{y}{z} = \frac{v^2-u^2}{u^2+v^2} \\ \frac{x}{z} = \frac{2uv}{u^2+v^2} \end{cases}$

L'étude précédente montre de la même manière que seul 2 peut diviser à la fois v^2-u^2, u^2+v^2 et $2uv$. Si tel est le cas, on a toujours u et v impairs, et alors $(v^2-u^2)/2$ et $(u^2+v^2)/2$ sont premiers entre eux (car ce dernier est impair), ce qui montre que : $\begin{cases} x = uv \\ y = (v^2-u^2)/2 \end{cases}$.

On pose[2] alors $s = \frac{u+v}{2}$ et $t = \frac{v-u}{2}$. s et t sont clairement premiers entre eux, et il apparait que $\begin{cases} x = s^2-t^2 \\ y = 2st \end{cases}$ □

Théorème 2 *Il n'existe pas de triplet d'entiers non nuls (x,y,z) tels que $x^4+y^4=z^2$*

Démonstration :

Supposons par l'absurde que cette équation a des solutions non triviales. Soit (x,y,z) un triplets d'entiers positifs solution tel que z soit minimal. Par minimalité, x, y et z sont premiers entre eux.

Par le théorème précédent, il existe donc u, v premiers entre eux tels que : $\begin{cases} x^2 = v^2-u^2 \\ y^2 = 2uv \end{cases}$ (quitte à échanger x et y) on a en particulier $x^2+u^2=v^2$.

Comme x est impair, et que x, u et v sont bien premiers entre eux dans leur ensemble (puisque $u \wedge v = 1$), par le théorème précédent, il existe r et s premiers entre eux tels que : $\begin{cases} x = r^2-s^2 \\ u = 2rs \\ v = r^2+s^2 \end{cases}$

Mais alors $y^2 = 4rs(r^2+s^2)$. Or r, s sont premier entre eux, donc chacun est premier avec (r^2+s^2). Donc r, s et (r^2+s^2) sont des carrés, et en notant $r=\alpha^2$, $s=\beta^2$ et $(r^2+s^2)=\gamma^2$, on a $\alpha^4+\beta^4=\gamma^2$ et

$$\gamma^2 = r^2+s^2 < 4rs(r^2+s^2) = y^2 \leq y^4 < x^4+y^4 = z^2$$

Donc $0 < \gamma < z$, ce qui est contredit la minimalité de z. □

1. Ce cas est oublié dans toutes les preuves que j'ai pu lire. Pourtant, ce cas est tout à fait possible : si $u=3$ et $v=5$, alors le premier cas aboutit à une contradiction puisque v^2-u^2, $2uv$ et u^2+v^2 sont tous pairs. En fait, on montre ici que ces derniers sont premiers entre eux si et seulement si u et v sont premiers entre eux **et de parité différente**.

2. Ce changement de variable vient tout seul si on écrit $uv = s^2-t^2$ et $(v^2-u^2)/2 = 2st$

Théorème des deux carrés

Leçons : 120, 121, 122, 126

[Per], partie II.6
[Duv], partie 6.1

Théorème

Soit p un nombre premier impair, on note $\Sigma = \left\{n \in \mathbb{N} \middle| \exists a, b \in \mathbb{N}, n = a^2 + b^2\right\}$.
On a : $p \in \Sigma \Leftrightarrow p \equiv 1\,[4]$.

Démonstration :

Pour commencer, quelques mots sur $\mathbb{Z}[i]$: on définit la "norme" N : $\left|\begin{array}{ccc} \mathbb{Z}[i] & \to & \mathbb{N} \\ z = a + ib & \mapsto & z\bar{z} = a^2 + b^2 \end{array}\right.$;
alors N est multiplicative, ce qui signifie que $N(zz') = N(z)N(z')$ pour tous $z, z' \in \mathbb{Z}[i]$.

Lemme 1

On a : $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Démonstration du lemme 1 :

- $\subset$ Si $z \in \mathbb{Z}[i]^\times$, alors $N(z)N\left(z^{-1}\right) = N(1) = 1$, donc $N(z) = 1$.
  Or $z = a + ib$, avec $a, b \in \mathbb{Z}$, donc $a^2 + b^2 = 1$ et on a $(a = 0$ et $b = \pm 1)$ ou $(a = \pm 1$ et $b = 0)$.
- $\supset$ Cette vérification est immédiate...

■

Lemme 2

On a l'équivalence : $p \in \Sigma \Leftrightarrow p$ est réductible dans $\mathbb{Z}[i]$.

Démonstration du lemme 2 :

- $\Rightarrow$ Si $p = a^2 + b^2$, alors dans $\mathbb{Z}[i]$, $p = (a + ib)(a - ib)$.
  Comme $N(a + ib) = N(a - ib) = p > 1$, on sait que $a + ib$, $a - ib \notin \mathbb{Z}[i]^\times$ et donc p est réductible.
- $\Leftarrow$ Si $p = zz'$ dans $\mathbb{Z}[i]$ avec $z, z' \notin \mathbb{Z}[i]^\times$, on a : $N(p) = N(z)N(z') = p^2$.
  Mais on sait que $N(z) \neq 1 \neq N(z')$, donc $N(z) = p$.

■

Comme $\mathbb{Z}[i]$ est factoriel [1], par le lemme d'Euclide, on a :

$$p \text{ réductible dans } \mathbb{Z}[i] \Leftrightarrow (p) \text{ non-premier dans } \mathbb{Z}[i] \Leftrightarrow {}^{\mathbb{Z}[i]}/_{(p)} \text{ non-intègre}$$

Mais comme $\mathbb{Z}[i] \simeq {}^{\mathbb{Z}[X]}/_{(X^2+1)}$, on a les isomorphismes suivants :

$$\mathbb{Z}[i]/_{(p)} \underset{2}{\simeq} \mathbb{Z}[X]/_{(X^2+1,p)} \simeq \left({}^{\mathbb{Z}[X]}/_{(p)}\right)/_{\left(\overline{X^2+1}\right)} \simeq \mathbb{F}_p[X]/_{(X^2+1)}$$

En conséquence, p est réductible dans $\mathbb{Z}[i] \Leftrightarrow \mathbb{F}_p[X]/_{(X^2+1)}$ non-intègre
$\Leftrightarrow X^2 + 1$ réductible dans $\mathbb{F}_p[X]$
$\Leftrightarrow X^2 + 1$ a une racine dans $\mathbb{F}_p$
$\Leftrightarrow -1$ est un carré dans $\mathbb{F}_p$
$\Leftrightarrow (-1)^{\frac{p-1}{2}} = \left(\dfrac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1\,[4]$

■

1. Le plus simple pour montrer la factorialité, c'est de montrer que $\mathbb{Z}[i]$ est euclidien pour la norme N, puis de dire que les anneaux euclidiens sont factoriels (voir en page ??).

2. Je tape les explications pour un isomorphisme, adaptez ceci pour trouver les autres. Ce passage me semble absolument indispensable à savoir rédiger pour pouvoir présenter ce développement.

Notons $\pi_{X^2+1} : \mathbb{Z}[X] \to {}^{\mathbb{Z}[X]}/_{(X^2+1)}$ et $\pi_{\overline{p}} : {}^{\mathbb{Z}[X]}/_{(X^2+1)} \to \left({}^{\mathbb{Z}[X]}/_{\left(X^2+1\right)}\right)/_{(\overline{p})}$ les projections canoniques.
Alors $\operatorname{Ker} \pi_{\overline{p}} \circ \pi_{X^2+1} = \left\{f \in \mathbb{Z}[X] \middle| \exists u \in \mathbb{Z}[X], \overline{f} = \overline{pu}\right\} = \{f \in \mathbb{Z}[X] | \exists u, v \in \mathbb{Z}[X], f = pu + (X^2+1)v\} = (p, X^2+1)$.
En conséquence, ${}^{\mathbb{Z}[X]}/_{(p, X^2+1)} \simeq \left({}^{\mathbb{Z}[X]}/_{\left(X^2+1\right)}\right)/_{(\overline{p})} \simeq \mathbb{Z}[i]/_{(p)}$.

Corollaire

Soit $n \in \mathbb{N}^*$, qu'on décompose en facteurs premiers : $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ (où $\mathcal{P}$ désigne l'ensemble des nombres premiers).
On a l'équivalence : $n \in \Sigma \Leftrightarrow \left(\forall p \in \mathcal{P}, p \equiv 3\,[4] \Rightarrow v_p(n) \equiv 0\,[2]\right)$.

Démonstration :

Lemme 3

Σ est stable par multiplication.

Démonstration du lemme 3 :

En effet, on sait déjà que $n \in \Sigma \Leftrightarrow \exists z \in \mathbb{Z}[i], n = N(z)$.
En conséquence, si $n, n' \in \Sigma$, alors $nn' = N(z)N(z') = N(zz') \in \Sigma$. ■

$\Leftarrow$ On décompose n de la façon suivante :

$$n = \underbrace{\left(\prod_{\substack{p \in \mathcal{P} \\ p=3\,[4]}} p^{\frac{v_p(n)}{2}}\right)^2}_{\text{Carré parfait}} \underbrace{\left(\prod_{\substack{p \in \mathcal{P} \\ p \neq 3\,[4]}} p^{v_p(n)}\right)}_{\substack{\text{Somme de 2 carrés} \\ \text{(lemme 3)}}}$$

$\Rightarrow$ Soit $n = a^2 + b^2 \in \Sigma$, on note $\delta = a \wedge b$, $a' = \frac{a}{\delta}$ et $b' = \frac{b}{\delta}$.
Ainsi, $a' \wedge b' = 1$ et $n = \delta^2\left(a'^2 + b'^2\right)$.
Soit p un diviseur premier impair de $a'^2 + b'^2$; alors dans $\mathbb{Z}[i]$, on a : $p|(a' + ib')(a' - ib')$.
- Par l'absurde, supposons p irréductible dans $\mathbb{Z}[i]$.
  Le lemme d'Euclide nous indique que $p|(a' + ib')$ ou que $p|(a' - ib')$; mais par passage au conjugué, si p divise l'un, alors p divise l'autre.
  Donc p divise les deux, puis par somme et différence, on obtient : $p|2a'$ et $p|2ib'$ dans $\mathbb{Z}[i]$.
  En passant à la norme, on en déduit : $p^2|4a'^2$ et $p^2|4b'^2$, dans $\mathbb{Z}$.
  Mais on sait que p est impair, et donc $p|a'$ et $p|b'$.
  Contradiction !
- On peut donc écrire $p = xy$ dans $\mathbb{Z}[i]$, avec en plus $N(x) \neq 1 \neq N(y)$ (ce qui signifie, rappelons-le, que x et y peuvent être pris non-inversibles).
  En passant à la norme, on obtient : $p^2 = N(x)N(y)$; puis, p étant premier, on obtient : $p = N(x)$.
  En conséquence, $p \in \Sigma$, d'où $p \equiv 1\,[4]$.

Ainsi, on a montré que les facteurs premiers congrus à 3 modulo 4 sont "dans" le δ^2, c'est-à-dire d'exposant pair. ■

Références

[Per] D. PERRIN – *Cours d'algèbre*, Ellipses, 1996.
[Duv] D. DUVERNEY – *Théorie des nombres*, 2e éd., Dunod, 2007.