<15 min si on fait pas tout. Faire des choix selon la leçon sur les lemmes.

THÉORÈME DES DEUX CARRÉS.

Perrin Cours d'Algèbre p56 → 58
corollaire = Gourdon Algèbre p 49

Prérequis : . euclidien ⇒ principal ⇒ factoriel. , irréductible, premier, dans les anneaux factoriels {irréd} = {premiers}. , I premier ⇔ A/I intègre.
a premier ⇔ (a) premier. , lemme de Gauss.

Théorème : On note $\Sigma = \{a^2+b^2, a, b \in \mathbb{N}\}$. Soit p un nombre premier.

$$p \in \Sigma \iff p = 2 \text{ ou } p \equiv 1 [4].$$

Pour démontrer ce théorème l'idée est de penser que si $n \in \Sigma$, $n = a^2+b^2 = (a+ib)(a-ib)$ dans $\mathbb{C}$. On va donc introduire l'anneau des entiers de Gauss $\mathbb{Z}[i]$.

Déf : On définit l'anneau $\mathbb{Z}[i]$ comme le plus petit sous anneau de $\mathbb{C}$ contenant $\mathbb{Z}$ et i. Comme $i^2 = -1$, $\mathbb{Z}[i] = \{a+ib, a, b \in \mathbb{Z}\}$.

Cet anneau est intègre car inclus dans $\mathbb{C}$. De plus, on a un automorphisme de $\mathbb{Z}[i]$ donné par la conjugaison : $a+ib \mapsto a-ib$. . Ce qui permet de définir une "norme" $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$, $a+ib \mapsto a^2+b^2 = z\bar{z}$ qui est multiplicative.

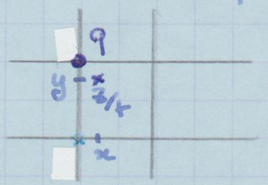
A partir de cela, on peut calculer les inversibles :

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

Dém : $\supset$ ok
$\subset$: Si $\overset{=a+ib}{z} \in \mathbb{Z}[i]^\times$, $\exists z' \in \mathbb{Z}[i]^\times$ tq $zz' = 1$ d'où $N(z)N(z') = 1$
d'où $N(z) = 1$. Ainsi $a^2+b^2 = 1$ et donc $(a = 0, b = \pm 1)$ ou $(a = \pm 1, b = 0)$.

Lemme 2 : L'anneau $\mathbb{Z}[i]$ est euclidien pour le stathme N (donc principal).

Dém : Soient $z, t \in \mathbb{Z}[i] \setminus \{0\}$, $\frac{z}{t} = x+iy \in \mathbb{C}$.



On approche z/t par un entier de Gauss $q = a+ib$.
où a et b proches de x et y :
$|x-a| \leq 1/2$, $|y-b| \leq 1/2$ d'où $|\frac{z}{t} - q| \leq \frac{\sqrt{2}}{2} < 1$

On pose $r = z - qt$. $\in \mathbb{Z}[i]$ (car anneau) et $r = t\left(\frac{z}{t} - q\right)$ d'où

$|r| = |t| \left|\frac{z}{t} - q\right| < |t|$ d'où en élevant au carré $N(r) < N(t)$.
Donc $z = qt + r$ avec $N(r) < N(t)$.

Lemme 3 : Σ est stable par multiplication.

Dém : $n \in \Sigma \iff \exists z \in \mathbb{Z}[i]$ $n = N(z) = z\bar{z}$

Prop. $p \in \Sigma \iff p$ n'est pas irréductible dans $\mathbb{Z}[i]$

Dém : • Si $p = a^2+b^2$, $p = (a+ib)(a-ib)$ or p premier donc a et b sont non nuls.
donc $a+ib$ et $a-ib$ ne sont pas inversibles donc p n'est pas irréductible
• Si $p = zz'$ avec z, z' non inversibles donc $N(z) \neq 1 \neq N(z')$, or a $N(p) = N(z)N(z') = p^2$, or p est premier dans $\mathbb{Z}$. d'où $p = N(z)$ d'où $p \in \Sigma$.

Dém thm: $\mathbb{Z}[i]$ est factoriel (car euclidien) donc {irréd} <=> {premier}

p n'est pas irréductible dans $\mathbb{Z}[i]$ $\iff$ p n'est pas premier dans $\mathbb{Z}[i]$
$\iff$ (p) n'est pas premier dans $\mathbb{Z}[i]$
$\iff$ $\frac{\mathbb{Z}[i]}{(p)}$ n'est pas intègre

Or on a $\mathbb{Z}[i] \simeq \frac{\mathbb{Z}[X]}{(X^2+1)}$ donc

$$\frac{\mathbb{Z}[i]}{(p)} \simeq \frac{\mathbb{Z}[X]}{(X^2+1,p)} \simeq \left(\frac{\mathbb{Z}[X]/(p)}{(X^2+1)} \right) \simeq \frac{\mathbb{F}_p[X]}{(X^2+1)}$$ ← voir plus loin.

$\mathbb{F}_p$ corps donc $\mathbb{F}_p[X]$ factoriel

Donc p n'est pas irréductible dans $\mathbb{Z}[i]$ $\iff$ X^2+1 n'est pas irréductible dans $\mathbb{F}_p[X]$
$\iff$ X^2+1 admet une racine dans $\mathbb{F}_p$.
$\deg(X^2+1)=2$ $\iff$ -1 est un carré dans $\mathbb{F}_p$.

D'après la proposition, il reste à démontrer que -1 est un carré dans $\mathbb{F}_p$ $\iff$ $p \equiv 1[4]$ ou $p=2$.

Pour cela, soit on utilise le symbole de Legendre avec le critère d'Euler soit on le démontre: Combes

Pour $p=2$ ok. Soit $p \neq 2$.

- si $x^2 \equiv -1[p]$, $x^4 \equiv 1[p]$ d'où $o(x) \mid 4$ or $x^2 \not\equiv 1[p]$ d'où $o(x) \overset{=}{=} 4$. Or d'après le thm de Lagrange, $o(x) \mid p-1 = |\mathbb{F}_p^\times|$ d'où $4 \mid p-1$.
- Récipqm^t, $\mathbb{F}_p^\times$ est cyclique et $4 \mid p-1 = |\mathbb{F}_p^\times|$ d'où il existe un unique sg d'ordre 4 dans $\mathbb{F}_p^\times$: $\{1, x, x^2, x^3\}$. $x^4 = 1$ d'où x^2 racine de $X^2-1 = (X-1)(X+1)$ or p premier d'où $x^2 = \pm 1$ or $x^2 \neq 1$ d'où $x^2=-1$ dans $\mathbb{F}_p$.

⌞

trop compliqué voir + loin.

Corollaire: Soit $n \in \mathbb{N}^*$, $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$

$n \in \Sigma \iff \forall p \in \mathcal{P}$ tq $p \equiv 3[4]$, $\nu_p(n) \equiv 0[2]$.

Dém: $\Leftarrow$:

$$n = \underbrace{\left(\prod_{p \equiv 3[4]} p^{\frac{\nu_p(n)}{2}} \right)^2}_{\in \Sigma \text{ : carré}} \left(\prod_{p \not\equiv 3[4]} p^{\nu_p(n)} \right)$$

Dans le produit de droite, chaque p est congru à 1 modulo 4 ou égal à 2 donc par thm $p \in \Sigma$. On conclut par le fait que Σ est stable par multiplication.

$\Rightarrow$. $n = a^2+b^2 = d^2(A^2+B^2)$ où $d = \mathrm{pgcd}(a,b)$ $A = a/d$ $B = b/d$ $A \wedge B = 1$.
Soit p premier diviseur impair de A^2+B^2 alors $p \mid (A+iB)(A-iB)$.

- Supposons par l'absurde que p est irréductible dans $\mathbb{Z}[i]$, alors il est premier donc $p \mid A+iB$ ou $p \mid A-iB$. mais par passage au conjugué, s'il divise l'un, il divise l'autre donc il divise les 2 et donc par somme et différence, $p \mid 2A$ et $p \mid 2B$ (dans $\mathbb{Z}[i]$). d'où en passant à N: $p^2 \mid 4A^2$ et $p^2 \mid 4B^2$ ds $\mathbb{Z}$. or $p \neq 2$ d'où par Gauss. $p \mid A$ et $p \mid B$. $\lightning$

Donc p n'est pas irréductible dans $\mathbb{Z}[i]$ donc par prop $p \in \Sigma$ donc $p \equiv 1[4]$ par thm. Donc les $p \equiv 3[4]$ sont "dans" le d^2. donc de valuation paire.

⌞

✓ **A l'oral**, 11'11 en très vite. Il faut faire une intro sur Z[i] avec inversibles et stable par multiplication. Puis corollaire, puis thm pour p premier.
✓ On peut prendre la fin du corollaire dans Duverney.
♣ Carl Gauss (1777 - 1855) est un mathématicien, astronome et physicien allemand. Il a apporté de très importantes contributions à ces trois domaines. Surnommé "le prince des mathématiciens" (Mathematicorum Principi), il est considéré comme l'un des plus grands mathématiciens de tous les temps. La qualité extraordinaire de ses travaux scientifiques était déjà reconnue par ses contemporains. Il dirigea l'Observatoire de Göttingen et ne travailla pas comme professeur de mathématiques – d'ailleurs il n'aimait guère enseigner – mais il encouragea plusieurs de ses étudiants, qui devinrent d'importants mathématiciens, notamment Eisenstein et Riemann. Il a beaucoup échangé avec Sophie Germain et était assez fan d'elle (un féministe !).

Naudin p138

$n = p$ $\quad$ $P(X) = X^2+1$ $\quad$ $\bar{a} = a \bmod n$

Montrons que $\dfrac{\mathbb{Z}[X]}{(n, P(X))} \simeq \dfrac{\mathbb{Z}/n\mathbb{Z}[X]}{(\bar{P}(X))}$

On considère $f : \mathbb{Z} \xrightarrow{\pi_1} \mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathbb{Z}/n\mathbb{Z}[X]$. On prolonge par la PU de l'anneau de polynômes en $f_{X \to X} : \mathbb{Z}[X] \to \mathbb{Z}/n\mathbb{Z}[X]$. (surjective)

Posons $g : \mathbb{Z}[X] \xrightarrow{f_{X\to X}} \mathbb{Z}/n\mathbb{Z}[X] \xrightarrow{\pi_2} \dfrac{\mathbb{Z}/n\mathbb{Z}[X]}{(\bar{P}(X))}$ morphisme.

On a $g(P(X)) = \pi_2(\overline{P(X)}) = 0$. et $g(n) = 0$.

d'où $(n, P(X))$ est annulé par g donc g se factorise par PU du quotient en

$$\bar{g} : \frac{\mathbb{Z}[X]}{(n, P(X))} \to \frac{\mathbb{Z}/n\mathbb{Z}[X]}{(\bar{P}(X))}$$

Comme g est surjective, $\bar{g}$ l'est aussi. Il reste à vérifier que $\mathrm{Ker}(g) \subset (n, P(X))$

Si $\sum_{i=1}^{d} a_i X^i \in \mathrm{Ker}(g)$ alors $\sum \bar{a}_i X^i = \overline{P(X)} \underbrace{\sum \bar{b}_i X^i}_{Q_1 \in \mathbb{Z}/n\mathbb{Z}[X]}$

On relève cette égalité dans $\mathbb{Z}[X]$:

$$\sum a_i X^i - P(X) \sum b_i X^i \equiv 0 [n]$$
$$= n Q_2 \text{ où } Q_2 \in \mathbb{Z}[X].$$

Donc $\sum a_i X^i \in (n, P(X))$ donc $\bar{g}$ est un isomorphisme.

126 = Tout sauf le lemme 2, lemme 1 s'il reste du temps.

-1 est un carré dans $\mathbb{F}_p$ ssi $p = 2$ ou $p \equiv 1 [4]$.

$p = 2$ ok

$X^{p-1} - 1 = (X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1)$ a au + p racines dans $\mathbb{F}_p$ car $\mathbb{F}_p$ corps

or $\mathbb{F}_p^*$ racines.

De plus il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p$, ils sont tous racines de $X^{\frac{p-1}{2}} - 1$

donc -1 est un carré ssi -1 racine de $X^{\frac{p-1}{2}} - 1$ ssi $(-1)^{\frac{p-1}{2}} = 1$

ssi $p \equiv 1 [4]$.

$\varphi = \mathbb{F}_p^* \to \mathbb{F}_p^*$, $x \mapsto x^{\frac{p-1}{2}}$ $\quad$ $\mathrm{Im}\,\varphi = \{\pm 1\}$ $\quad$ $\mathrm{Ker}\,\varphi = \{\text{carrés de } \mathbb{F}_p^*\}$

d'où $|\mathrm{Ker}\,\varphi| = \dfrac{|\mathbb{F}_p^*|}{|\mathrm{Im}\,\varphi|} = \dfrac{p-1}{2}$