



$$P = \{2, 3, 5, 7, 11, 13, 17, \dots\} \quad \text{I \& P}$$

Déf: $p \in \mathbb{N}_{\geq 2}$ est premier si $d|p \Rightarrow d=1$ ou $d=p$
 $6 \nmid P \quad 2|6 \quad 3|6$

Prop: $p \neq p' \in P$ premiers $\Rightarrow p \wedge p' = 1$

Pv: $d := \text{pgcd}(p, p')$ $d|p$ et $d|p'$. Mais p et p' sont premiers ($d=1$ ou $d=p$) et ($d=1$ ou $d=p'$)
 $\Rightarrow d=1 = \text{pgcd}(p, p')$

Prop: Soit $p \in P$ alors $\forall a \in \mathbb{Z}$:

$$(i) p \wedge a = 1$$

(ii) $p \nmid a$ ne divise pas

par l'absurde

Pv: $\Downarrow$ Hyp $p \wedge a = 1$ si (ii) fausse i.e si $p|a$

$$\text{on aurait } \text{pgcd}(p, a) = p \geq 2$$

$$\text{contradisant } \text{pgcd}(p, a) = 1$$

$\neg$ Hyp: $p \nmid a$ Noter: $d := \text{pgcd}(p, a)$
 But $d = 1$

$$d|p \stackrel{\text{def}}{\Rightarrow} (d=1 \text{ ou } d=p)$$

contrad

IMPOSSIBLE car
 sinon $d = p|a$

$$\text{Donc } d=1$$

□

Thm: [d'Euclide] Soit $p \in \mathcal{P}$ nombre premier.

Alors: $\forall a, b \in \mathbb{Z}$

$$p \mid ab \Rightarrow (p \mid a \text{ ou } p \mid b)$$

De plus, si a et b sont aussi premiers, alors
($p=a$ ou $p=b$).

pr: Hyp $p \mid ab$. Si $p \mid a$ rien à faire.
Donc OPS $p \nmid a$.

Prp donne $p \nmid a = 1$

Donc ($p \mid ab$ et $p \nmid a = 1$) $\xRightarrow{\text{gauss}} p \mid b$ le 2^{ème} cas! $\square$

Prp: ^{REC FACILE} Soit $p \in \mathcal{P}$ Alors $\forall a, b, c, \dots, l \in \mathbb{Z}$

$$p \mid abc \dots l \Rightarrow (p \mid a \text{ ou } p \mid b \text{ ou } p \mid c \text{ ou } \dots \text{ ou } p \mid l)$$

De plus $a, b, c, \dots, l \in \mathcal{P}$ alors ($p=a$ ou $p=b$ ou $\dots$ ou $p=l$) $\square$

Thm: Tout nombre $n \geq 2$ entier se décompose comme produit
de nombres premiers.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

avec

$$2 \leq p_1 < p_2 < p_3 < \dots < p_r$$

$$\text{avec } \alpha_1 \geq 1, \alpha_2 \geq 1, \dots, \alpha_r \geq 1$$

$$\text{Ex: } 888 = 2^3 \cdot 3 \cdot 37$$

$$1235 = 5 \cdot 13 \cdot 19$$

Thm 2: Cette décomposition est unique: n

$$n := p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r} \quad \text{seul de ce type}$$

$$= q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \dots \cdot q_s^{\beta_s}$$

$$\Rightarrow r = s \text{ et } \begin{array}{ccccccc} p_1 & p_2 & \dots & p_r & \text{et} & \alpha_1 & \alpha_2 & \alpha_3 \\ \parallel & \parallel & & \parallel & & \parallel & \parallel & \parallel \\ q_1 & q_2 & & q_3 & & \beta_1 & \beta_2 & \beta_3 \end{array}$$

