

La dernière fois :

Algorithme (Euclide Étendu)  
EuclideEtendu( $a, b$ )

Entrées:  $a, b \in \mathbb{Z}_{\geq 0}$ ,  $(a, b) \neq (0, 0)$

Sortie: un triplet  $(d, u, v)$  tel que  $\text{pgcd}(a, b) = d$  et  $d = au + bv$ .

1. Si  $a < b$ :

2.  $(d, u, v) \leftarrow \text{Euclide Etendu}(b, a)$

3. Renvoyer  $(d, \cancel{v}, \cancel{u})$

4. Si  $b=0$ : Renvoyer  $(a, 1, 0)$

5.  $(q, r) \leftarrow (a \text{ quo } b, a \text{ mod } b)$

6.  $(d, u', v') \leftarrow \text{Euclide Etendu}(b, r)$

7. Renvoyer  $(d, \cancel{v'}, \cancel{u' - qv'})$

Preuve de correction

On note que si on ignore les  $u$  et les  $v$  dans l'algorithme on retrouve exactement l'algorithme d'Euclide récursif.

Donc l'algorithme se termine et l'entier  $d$  est exactement le  $\text{pgcd}(a, b)$ .

Il reste à montrer que  $d = au + bv$ , où  $u$  et  $v$  sont respectivement la 2ème et la 3ème composante de la sortie.

On procède par récurrence :

Si  $b=0$ , c'est clair que  $\frac{d}{\text{pgcd}(a,0)} = a = a \cdot 1 + b \cdot 0$

Si non, on écrit  $a = bq + r$  avec  $q$  et  $r$  resp. quotient et reste de la division euclidienne de  $a$  par  $b$ .

Par hypothèse d'induction  $(d, u', v')$  satisfait

$$d = bu' + rv'$$

$\frac{r}{a-bq}$

Donc  $d = bu' + (a - bq)v' = av' + b(u' - qv')$

Remarque : Le temps d'exécution de l'algorithme d'Euclide étendu est du même ordre de l'algorithme d'Euclide.



## Nombres premiers

Rappel :  $\forall n \in \mathbb{Z}$ ,  $1|n$  et  $n|n$ .

Def : Un nombre premier est un entier naturel ( $> 0$ ) qui possède exactement deux diviseurs entiers distincts et positifs : 1 et lui-même.

Un entier  $n > 1$  qui n'est pas premier est dit composé.

Attention : 0 et 1 ne sont pas de nombres premiers (ni des nombres composés).

# Théorème fondamental de l'Arithmétique

Soit  $n \in \mathbb{Z}$ ,  $n \neq 0$ .

Alors  $n$  peut s'écrire de manière unique sous la forme

$$n = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = \pm \prod_{i=1}^k p_i^{e_i}$$

Où  $p_1 < p_2 < \dots < p_k$  sont des nombres premiers distincts et  $e_1, \dots, e_k$  sont des entiers strictement positifs ( $> 0$ ).

Remarque : Si  $n = \pm 1$ , alors  $K=0$  (note que un produit vide est égal à 1).

## Proposition (Lemme de Gauss)

Soient  $a, b, c \in \mathbb{Z}$  tels que  $a$  divise  $bc$  et  $\text{pgcd}(a, b) = 1$ . Alors  $a$  divise  $c$ .

### Dém.

Puisque  $\text{pgcd}(a, b) = 1$ ,  $\exists u, v \in \mathbb{Z}$  tels que

$$\begin{aligned} 1 &= au + bv \\ \Downarrow \\ 1 \cdot c &= (au + bv) \cdot c \\ \Downarrow \\ c &= auc + bvc \end{aligned}$$

On remarque que  $a \mid auc$ . De plus pour hypothèse on sait que  $a \nmid bc \Rightarrow a \nmid bvc \Rightarrow \Rightarrow a \nmid auc + bvc = c$ . Donc  $a \mid c$ .

Proposition : Soit  $p$  un nombre premier et soient  $a, b \in \mathbb{Z}$ . Si  $p \mid ab$  alors  $p \mid a$  ou  $p \mid b$ .

Dém : Si  $p \mid a$  l'énoncé est vrai. Si  $p \nmid a$ , alors  $\text{pgcd}(p, a) = 1$ . On sait que  $p \mid ab$ , donc par Gauss  $p \mid b$ .

## Démonstration du théorème

Sans perte de généralité on peut supposer  $n > 0$

(car si  $n < 0$ ,  $n = -\underbrace{(-n)}_{>0}$ ).

### • Existence de la factorisation :

On procède par récurrence forte.

Si  $n=1$ , l'énoncé est vrai ( $1$  est produit de zéro nombres premiers).

Soit  $n > 1$ . On suppose que chaque entier positif  $< n$  peut s'écrire comme produit de nombres premiers.

Si  $n$  est premier, alors l'énoncé est vrai.

Sinon  $n$  est composé, c'est à dire  $\exists a, b \in \mathbb{N}^*$  tels que  $n = ab$  et  $1 < a, b < n$ .

Pour hypothèse de récurrence,  $a$  et  $b$  peuvent s'écrire comme produit de nombres premiers, donc cela vaut aussi pour  $n$ .

### • Unicité de la factorisation :

On veut montrer que si

$$n = p_1 \cdots p_s = q_1 \cdots q_t, \quad (*)$$

où  $p_i, q_j$  sont des nombres premiers pas forcément distincts, alors  $s=t$  et  $(p_1, \dots, p_s)$  est une permutation de  $(q_1, \dots, q_t)$ .

On procède par récurrence sur  $s$ .

Si  $s=0 \Rightarrow n=1 \Rightarrow t=0$  et l'énoncé est vrai.

Supposons que l'énoncé est vrai pour  $s-1$ .  
On montre qu'il est vrai pour  $s$  aussi.

Puisque  $p_1 \mid p_1 \cdots p_s$  et  $p_1 \cdots p_s = q_1 \cdots q_t$ ,  
donc  $p_1 \mid q_1 \cdots q_t$ . Pour la proposition  
précédente,  $\exists 1 \leq j \leq t$  tel que  $p_1 \mid q_{i_j} \Rightarrow$   
 $\Rightarrow p_1 = q_{i_j}$ .

En divisant (\*) à gauche par  $p_1$  et à droite  
par  $q_{i_j}$  on obtient deux égalités égales  
avec un terme de moins.

Pour hypothèse de récurrence on a  $s-1=t-1$   
et  $(p_2, \dots, p_s)$  est une permutation de  
 $(q_1, \dots, q_{i_j-1}, q_{i_j+1}, \dots, q_t)$ . Donc  $s=t$  et  
 $(p_1, \dots, p_s)$  est une permutation de  $(q_1, \dots, q_t)$   
(puisque  $p_1 = q_{i_j}$ ).

**EXERCICE 6 du TD 1**

**EXERCICES 1, 2, 3 du TD 2**

Exercice 6 du TD 1

Soient  $a, b_1, \dots, b_k \in \mathbb{Z}$ . Montrer que  
 $\text{pgcd}(a, b_1 \cdots b_k) = 1 \iff \text{pgcd}(a, b_i) = 1$   
 $\forall i=1, \dots, k$ .

Dém

$\Rightarrow)$  On suppose que  $\text{pgcd}(a, b_1 - b_k) = 1$ .  
 Alors  $\exists u, v \in \mathbb{Z}$  tels que

$$au + (b_1 - b_k) \cdot v = 1$$

On peut réécrire cette identité de la façon suivante :

$$au + b_1 \underbrace{(b_2 - b_k \cdot v)}_{\in \mathbb{Z}} = 1$$

$$\Rightarrow \text{pgcd}(a, b_1) = 1$$

De façon similaire on montre que  
 $\text{pgcd}(a, b_i) = 1 \quad \forall i = 2, \dots, k$ .

$\Leftarrow)$  Supposons que  $\text{pgcd}(a, b_i) = d \quad \forall i = 1, \dots, k$ .  
 Supposons, par l'absurde, que  
 $\text{pgcd}(a, b_1 - b_k) \neq 1 \Rightarrow \text{pgcd}(a, b_1 - b_k) = d > 1$ .

Soit  $p$  un nombre premier qui divise  $d$   
 (il existe par le théorème fondamental de l'arithmétique).

Donc  $p | a$  et  $p | b_1 - b_k$

$\Downarrow$  Proposition précédente

$\exists i = 1, \dots, k$  tel que

$p | b_i$

Donc  $p | \text{pgcd}(a, b_i) \Rightarrow \text{pgcd}(a, b_i) \neq 1$

## Exercice 1 - TD 2

Soit  $n \geq 2$  un entier. Montrer que  
 $n$  est premier  $\iff n$  n'admet aucun diviseur premier  $\leq \sqrt{n}$

$n$  est premier  $\iff \forall$  nombre premier  $p \leq \sqrt{n}$ ,  
 $p \nmid n$ .

Démo

$\implies$ ) Si  $n$  est premier, alors les uniques diviseurs sont 1 et  $n$  ( $> \sqrt{n}$ ).  
 $\uparrow$   
 $n \geq 2$

Donc  $n$  n'admet pas de diviseurs premiers  $\leq \sqrt{n}$ .

$$\begin{array}{l} P \Rightarrow Q \\ \Downarrow \\ \neg Q \Rightarrow \neg P \end{array}$$

$\iff$ ) Par contraposée, on montre que:

Si  $n$  est composé  $\Rightarrow \exists$  nombre premier  $p \leq \sqrt{n}$  tel que  $p \mid n$

Si  $n$  est composé,  $\exists a, b \in \mathbb{Z}$ ,  $1 < a, b < n$  tel que  $n = ab$ .

On montre, d'abord, que  $a \leq \sqrt{n}$  ou  $b \leq \sqrt{n}$ .

Si  $a > \sqrt{n}$  et  $b > \sqrt{n} \Rightarrow ab > \sqrt{n} \cdot \sqrt{n} = n \nmid n$

Donc, sans perte de généralité, on suppose  $a \leq \sqrt{n}$ . Puisque  $a > 1$ ,  $\exists p$  premier tel que  $p \mid a \Rightarrow p \mid n$  et  $p \leq \sqrt{n}$

## Entiers modulo n : $\mathbb{Z}/n\mathbb{Z}$

Dans les applications en cryptographie on travaille surtout avec des entiers limités à un certain intervalle.

### Rappels : Relations d'équivalence

Def: Soit A un ensemble. Une relation binaire  $\sim$  sur A est une relation d'équivalence si :

- $\sim$  est réflexive:  $\forall x \in A, x \sim x$
- $\sim$  est symétrique:  $\forall x, y \in A, x \sim y \Rightarrow y \sim x$
- $\sim$  est transitive:  $\forall x, y, z \in A, x \sim y \text{ et } y \sim z \Rightarrow x \sim z$ .

modulo  $\sim$

Def:  $\forall x \in A$ , la classe d'équivalence de x est le sous-ensemble de A:

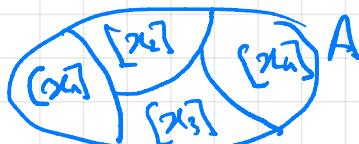
$$[x] = \{y \in A : x \sim y\}$$

Chaque élément de  $[x]$  est appelé un représentant de  $[x]$ .

L'ensemble :

$$A/\sim := \{[x] : x \in A\} \neq A$$

Proposition: Si  $\sim$  est une relation d'équivalence d'un ensemble non vide A, alors  $A/\sim$  est une partition de A



## Exercice 6, TD 2

Soit  $n \in \mathbb{Z}_{>0}$ . Soient  $a, b \in \mathbb{Z}$ :

$$a \sim b \iff n \mid (a-b)$$

1) Montrer que  $\sim$  est une relation d'équivalence

- $\sim$  est réflexive :  $\forall a \in \mathbb{Z}, n \mid a-a=0$  donc  $a \sim a$ .
- $\sim$  est symétrique :  $\forall a, b \in \mathbb{Z}$  tels que  $a \sim b$   
 $\Rightarrow n \mid (a-b) \Rightarrow n \mid -(a-b)$   
 $\Rightarrow n \mid b-a \Rightarrow b \sim a$
- $\sim$  est transitive :  $\forall a, b, c \in \mathbb{Z}$  tels que  
 $a \sim b$  et  $b \sim c \Rightarrow$   
 $\Rightarrow n \mid a-b$  et  $n \mid b-c$   
 $\Rightarrow n \mid (a-b)+(b-c)=a-c$   
 $\Rightarrow a \sim c$

2)  $[0]_n = \{a \in \mathbb{Z} : a \sim 0\} =$

$$= \{a \in \mathbb{Z} : n \mid a\} = \{nk, k \in \mathbb{Z}\}$$

$[1]_n = \{a \in \mathbb{Z} : a \sim 1\} =$

$$= \{a \in \mathbb{Z} : n \mid (a-1)\} = \{a \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ s.t. } a-1=nk\}$$

$$= \{nk+1, k \in \mathbb{Z}\}$$

$$\begin{aligned}
 [n]_n &= \{a \in \mathbb{Z} : a \sim n\} = \\
 &= \{a \in \mathbb{Z} : n \mid (a-n)\} = \\
 &= \{a \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ t.q. } a-n = nk\} = \\
 &= \{a \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ t.q. } a = n(k+1)\} = \\
 &= \{n(k+1) : k \in \mathbb{Z}\} = [0]_n.
 \end{aligned}$$