TECHNIQUES & MÉTHODES S16

NB : cette fiche reprend les techniques nécessaires **minimales**; elle ne constitue donc pas un objectif, mais un prérequis !

ENTIERS RELATIFS, ARITHMÉTIQUE

Divisibilité

Comment montrer que a divise b

- en pratique, vous pouvez utiliser une décomposition primaire de a et b.
- pour les question théoriques, vous pouvez effectuer la division euclidienne de b par a et montrer que le reste est nul.
- vous pouvez utiliser le **théorème de Gauss** et montrer que a divise bc, où c est premier à a.

PGCD,PPCM

Comment calculer $\mathrm{PGCD}(a,b)$ **ou** $\mathrm{PPCM}(a,b)$

- en pratique, vous pouvez utiliser une décomposition primaire de a et b.
- vous procédez par factorisation successives à l'aide des propriétés d'homogénéité
- vous pouvez utiliser l'**algorithme d'Euclide** pour déterminer $\mathrm{PGCD}(a,b)$ puis déterminer leur PPCM en utilisant

$$\mathrm{PGCD}(a,b)\times\mathrm{PPCM}(a,b)=|ab|$$

- vous utilisez les caractérisations algébriques et arithmétiques du PGCD et du PPCM

Comment mettre en œuvre l'algorithme d'Euclide

Soit $(a,b)\in\mathbf{Z}^2$, on calcule $d=PGCD(a,b)$. Pour cela :

- on pose $a_0=\max\{|a|,|b|\}$ et $a_1=\min\{|a|,|b|\}$;
- on effectue des divisions euclidiennes successives jusqu'à l'obtention d'un reste nul :

$$\forall k\in[\![1,m]\!],\ a_{k-1}=a_k\,q_k+a_{k+1}\text{ avec }a_0\geq a_1>a_2>\cdots>a_m>a_{m+1}=0$$

- $d=a_m$ est le dernier reste non nul dans l'algorithme d'Euclide.

Comment obtenir une égalité de Bezout

Soit $(a,b)\in\mathbf{Z}^2$, on note $d=PGCD(a,b)$. Pour cela :

- l'algorithme d'Euclide fournit une suite décroissante d'entiers $a_0\geq a_1>\cdots>a_m>a_{m+1}=0$ tels que
  - $a_0=\pm a$ et $a_1=\pm b$ (ou $a_0=\pm b$ et $a_1=\pm a$), $a_m=d$
  - $\forall k\in[\![1,m]\!],\ a_{k-1}=a_k\,q_k+a_{k+1}\quad(L_k)$
- d'après (L_{m-1}) , a_m s'exprime comme combinaison linéaire de a_{m-2} et a_{m-1} :
$$a_m=CL(a_{m-2},a_{m-1})$$
- or, d'après (L_{m-2}), a_{m-1} s'exprime lui-même en fonction de a_{m-3} et a_{m-2}. En remplaçant, on obtient alors a_m comme combinaison linéaire de a_{m-3} et a_{m-2} :
$$a_m=CL(a_{m-3},a_{m-2})$$
- *par remontée*, on en déduit que a_m comme combinaison linéaire de a_0 et a_1
$$a_m=CL(a_0,a_1)=CL(a,b)$$

Exercice 28 : Déterminez le PGCD de 54 et 150 et une égalité de Bezout. *Réponse* $PGCD(150,54)=6$ et $4\times150-11\times54=6$.

Nombres premiers entre eux

Comment montrer que a et b sont premiers entre eux

- vous vérifiez que $\mathrm{PGCD}(a,b)=1$
- vous utilisez le **théorème de Bezout**
- vous montrez que a et b n'ont pas de diviseurs premiers communs.

■■■ Résolution d'équations

Comment résoudre un système PGCD,PPCM

Pour résoudre dans $\mathbf{Z}^2$ le système (S) $\left\{\begin{array}{rcl} PGCD(x,y) & = & d \\ PPCM(x,y) & = & m \end{array}\right.$

- Si d ne divise pas m, (S) n'a pas de solutions dans $\mathbf{Z}^2$. Sinon, on effectue le changement d'inconnues $x = dx'$ et $y = dy'$.
- D'après la proposition de **Factorisation par le PGCD**, x' et y' sont premiers entre eux et (S) équivaut à l'équation $x'y' = m'$.
- On achève la résolution en sélectionnant parmi les factorisations de m' celles pour lesquelles les diviseurs x' et y' sont premiers entre eux.

Cette méthode peut s'appliquer plus généralement à tout système d'équation mettant en jeu PGCD et/ou PPCM.

Comment résoudre l'équation diophantienne $ax + by = c$

Pour résoudre dans $\mathbf{Z}^2$ l'équation (E) $\quad ax + by = c$, où $(a, b, c) \in \mathbf{Z}^3$.

- On détermine $d = PGCD(a, b)$:
  - si d ne divise pas c, l'équation (E) n'a pas de solutions dans $\mathbf{Z}^2$;
  - sinon, on se ramène après simplification par d au cas où les coefficients (a', b') sont premiers entre eux :

$$(E) \iff a'x + b'y = c', \text{ où } a' \text{ et } b' \text{ sont premiers entre eux.}$$

- On détermine une solution particulière (x_0, y_0) à l'aide d'une égalité de Bezout (s'il n'y en a pas d'évidente). En remplaçant le second membre, on obtient une équation du type :

$$a'(x - x_0) = b'(y_0 - y), \text{ où } a' \text{ et } b' \text{ sont premiers entre eux.}$$

- On achève alors la résolution à l'aide du **théorème de Gauss** et d'un changement d'inconnue.

Exercice 29 : on résout dans $\mathbf{Z}^2$ l'équation (E) $\quad 9x + 15y = 18$. *Réponse :* $\mathcal{S} = \{(12 - 5k, 3k - 6);\ \ k \in \mathbf{Z}\}$.