Racines $p^{\text{èmes}}$ de l'identité

Partie 1 : Théorème de Bezout

Soient a et b deux entiers naturels non nuls.

Les entiers a et b sont dits premiers entre eux si $\text{pgcd}\left((\,;a\right),b) = 1$. Le but de cette partir est d'établir le théorème de Bezout :

Théorème 1 :
Les entiers a et b sont premiers entre eux si et seulement si il existe des entiers u et v tels que $au + bv = 1$.

1. Montrer que s'il existe des entiers relatifs u et v tels que $au + bv = 1$ alors a et b sont premiers entre eux.
2. On prouve la réciproque de cette propriété.

   On suppose donc que a et b sont premiers entre eux et on considère l'ensemble $\mathcal{E}$ des entiers relatifs de la forme $au + bv$ où u et v sont des entiers relatifs,

   $$i.e.\ \ \mathcal{E} = \left\{au + bv,\ (u, v) \in \mathbb{Z}^2\right\}.$$

   (a) Montrer que l'ensemble $\mathcal{E} \cap \mathbb{N}^*$ admet un plus petit élément que l'on notera n_0.
   (b) On note r (respectivement r') le reste de la division euclidienne de a (respectivement b) par n_0. Montrer que r et r' appartiennent à $\mathcal{E}$.
   (c) En déduire que $r = r' = 0$.
   (d) Conclure.

Partie 2 : Racines de l'identité

Soient $n \in \mathbb{N}^*$ et p un entier supérieur ou égal à 2. On note

$$\mathcal{R}_n(p) = \{\mathrm{A} \in \mathcal{M}_n(\mathbb{C}),\ \mathrm{A}^p = \mathrm{I}_n\}.$$

1. Soit $\mathrm{P} \in \mathcal{M}_n(\mathbb{C})$ inversible.

   Montrer que si $\mathrm{A} \in \mathcal{R}_n(p)$ alors $\mathrm{P}^{-1}\mathrm{AP} \in \mathcal{R}_n(p)$.
2. Soit $\mathrm{A} \in \mathcal{R}_n(p)$.

   Montrer que A est inversible et exprimer A^{-1} en fonction de A. En déduire que $\mathrm{A}^{-1} \in \mathcal{R}_n(p)$.
3. Montrer que l'ensemble des matrices diagonales de $\mathcal{R}_n(p)$ forme un ensemble fini dont on déterminera le cardinal.
4. On considère q un entier naturel supérieur ou égal 2 et on note $d = \text{pgcd}\,(p\,;q)$.

   (a) Montrer que $\mathcal{R}_n(d) \subset \mathcal{R}_n(p) \cap \mathcal{R}_n(q)$.
   (b) Justifier qu'il existe deux entiers u et v tels que $pu + qv = d$.
   (c) En déduire que $\mathcal{R}_n(d) = \mathcal{R}_n(p) \cap \mathcal{R}_n(q)$.