Théorèmes de Bézout et de Gauss

I) Questions de cours

1. Théorème de Bézout :

Dire que deux entiers relatifs a et b sont premiers entre eux équivaut à dire qu'il existe u et v tels que $\boxed{\text{...?}}$

Ce théorème est une équivalence, et on peut l'utiliser dans les deux sens :

– Puisqu'on sait que $2(a-3)+(7-2a)=1$, on peut en déduire que $\boxed{\text{...?}}$

– Puisque $2^3 3^2$ et $5^4 7$ sont premiers entre eux, on peut en déduire que $\boxed{\text{...?}}$

L'implication de gauche à droite n'est qu'un théorème d'existence, elle ne dit pas comment calculer u et v. C'est plutôt elle qu'on nomme le théorème de Bézout. L'implication de droite à gauche est plus facile à démontrer. Démontrez-la : $\boxed{\text{...?}}$.

2. Théorème de Gauss : Si a divise bc et si a et b sont premiers entre eux, alors $\boxed{\text{...?}}$

ROC : partir de l'identité de Bézout, multiplier par c, puis combinaison linéaire.

3. Résolution de l'équation de Bézout $ax+by=1$ (a et b donnés, trouver x et y) : trouver une solution particulière (avec des essais, ou en remontant l'algorithme d'Euclide). Par soustraction et théorème de Gauss, déterminer des formules nécessaires pour x et y , puis vérifier que ces formules sont suffisantes (réciproque)

II) Exemples

1. Démontrer que, pour tout n dans $\mathbb{Z}$, $2n+3$ et $5n+7$ sont premiers entre eux

On forme une combinaison linéaire égale à 1 : $5(2n+3)-2(5n+7)=1$. Donc d'après le théorème de Bézout, $2n+3$ et $5n+7$ sont premiers entre eux.

2. Démontrer que, si a et b sont premiers entre eux, alors a et b^2 le sont aussi

D'après le théorème de Bézout, il existe u et v tels que $au+bv=1$. On élève au carré cette identité : $a^2u^2+2aubv+b^2v^2=1$. On met en évidence a et b^2 : $a(au^2+2ubv)+b^2(v^2)=1$

D'après le théorème de Bézout (sa réciproque), a et b^2 sont premiers entre eux.

Autre méthode possible : utiliser les décompositions en facteurs premiers

3. Déterminer l'ensemble des couples (x,y) tels que $7(x-1)=6(y-1)$.
En déduire l'ensemble des couples (x,y) tels que $7x-6y=1$.

7 étant en facteur dans le premier membre, c'est un diviseur du deuxième membre $6(y-1)$. Or 7 et 6 sont premiers entre eux, donc d'après le théorème de Gauss, 7 divise $y-1$. Donc $y-1=7k$, et $y=1+7k$.

Mais ce n'est a priori qu'une condition nécessaire. Il faut étudier la réciproque.

Si $y=1+7k$, alors dire que $7(x-1)=6(y-1)$ *équivaut* à dire que $7(x-1)=42k$, c'est-à-dire $x-1=6k$, soit $x=1+6k$. *L'équivalence est essentielle ici.*

Donc l'ensemble des couples (x,y) tels que $7(x-1)=6(y-1)$. est l'ensemble des couples $(1+67k,-1+7k)$ avec $k\in\mathbb{Z}$. C'est donc aussi l'ensemble des couples solutions de $7x-6y=1$, puisque $7(x-1)=6(y-1)\Leftrightarrow 7x-7=6y-6$, soit $7x-6y=1$.

Résumé : on a un problème P à résoudre, on démontre $P\Rightarrow A$, puis (si A alors $(P\Leftrightarrow Q)$), puis (Q a pour solutions S), et donc P a pour solutions S.

On pourrait aussi montrer : $P\Rightarrow A$, donc l'ensemble des solutions de P est inclus dans S, puis : réciproquement tout élément de S est bien solution de P.

4. a et n sont deux entiers naturels non nuls, et premiers entre eux.
Démontrer que l'équation $ax\equiv 2\ [n]$ a au plus une solution x dans $[0;n-1]$.

Par l'absurde : supposons qu'il y ait deux solutions x et y. $ax\equiv 2\ [n]$ et $ay\equiv 2\ [n]$ avec x et y dans $[0;n-1]$. Alors $ax\equiv ay\ [n]$, donc $a(x-y)\equiv 0\ [n]$, donc $a(x-y)$ est divisible par n. Or a et n sont premier entre eux, donc $x-y$ est divisible par n d'après le théorème de Gauss.

Or $-(n-1)\leqslant x-y\leqslant n-1$. Donc la seule possibilité est $x-y=0$, soit $x=y$. Donc il ne peut y avoir qu'une solution au plus (*au fait, y en a-t-il une ?*).

5. Déterminer une solution particulière de l'équation $235x+67y=1$

Algorithme d'Euclide (on numérote les [étapes]) :

[1] : $235=67(3)+34$

[2] : $67=34(1)+33$

[3] : $34=33(1)+1$

Donc PGCD(235, 67) $=1$. Puis on remonte :

On tire 1 de [3] : $1=(1).34+(-1).33$

On tire 33 de [2], on remplace : $1=(-1).67+(2).34$

On tire 34 de [1], on remplace : $1=(2).235+(-7).67$

Donc une solution de $235x+67y=1$ est : $x=2, y=-7$