Index

Équation diophantienne :

Une équation diophantienne, en mathématiques, est une équation dont les coefficients sont des nombres entiers et dont les solutions recherchées sont également entières.
Carl Friedrich Gauss (xixe siècle), disait des problèmes de cette nature : « Leur charme particulier vient de la simplicité des énoncés jointe à la difficulté des preuves. »
Ce type d'équation doit son nom au mathématicien grec Diophante d'Alexandrie, un mathématicien vivant à une date incertaine, probablement autour du iiie siècle. Il est l'auteur d'un traité, Arithmétiques, étudiant des questions de cette nature

Extrait de Wikipedia : http://fr.wikipedia.org/wiki/Équation_diophantienne

En particulier : Résolution de ax + by = c

a, b, c sont des entiers et on cherche tous les couples d'entiers (x, y) solutions de cette équation.

Les théorèmes utiles :

Identité de Bézout

lorsque c est un multiple du PGCD de a et b, on sait (**Identité de Bézout**) qu'il existe des entiers u et v tels que $au + bv = c$.

Lorsque a et b sont premiers entre eux, PGCD$(a, b) = 1$.

théorème de Gauss

Le théorème de Gauss : Si a et b sont premiers entre eux et si a divise le produit bc alors a divise c.

La méthode :

Soit (E) : $ax + by = c$.
1/ On réduit l'équation de façon à avoir a et b premiers entre eux (sinon le théorème de Gauss ne s'applique pas).
2/ On cherche un couple solution (u_0 , v_0). (Algorithme d'Euclide)
On a alors une **égalité** : $au_0 + bv_0 = c$ (autrement dit : on peut remplacer c par $au_0 + bv_0$ puisque ces deux nombres sont égaux)
3/ Par comparaison, l'équation (E) devient : $ax + by = au_0 + bv_0$
et, on réorganise : $a(x - u_0) = b(v_0 - y)$ (E_1) (comprendre : $aq = bq'$)
Autrement dit : Si le couple (x, y) est solution de (E) alors a divise le produit $b(v_0 - y)$ *(ou b divise le produit $a(x - u_0)$.*
4/ Comme a et b sont premiers entre eux, notre cher ami Gauss nous permet de dire :
a divise $v_0 - y$.
Ou encore, il existe un entier k tel que $ak = v_0 - y$. $(y = v_0 - ak)$

(ou bien : b divise $x - u_0$, et, il existe un entier k' tel que $bk' = x - u_0$)
5/ Dans (E_1), on remplace $v_0 - y$ par ak.
Donc (E_1) devient : (E_2) $a(x - u_0) = bak$ qui après réduction par a, nous donne :
$x - u_0 = bk$. $(x = u_0 + bk)$

Conclusion à cette étape :
On a montré : Si un couple $(x\ ;\ y)$ est solution de (E)
alors (nécessairement) ces couples sont de la forme $(u_0 + bk\ ;\ v_0 - ak)$ $k \in \mathbb{Z}$.
Autrement dit : on sait comment s'écrivent ces couples, mais, on n'est pas certain que tous les couples qui s'écrivent ainsi conviennent, d'où,
6/ Il reste à vérifier que TOUS les couples conviennent.
On calcule $a(u_0 + bk) + b(v_0 - ak) = au_0 + abk + bv_0 - bak = au_0 + bv_0 = c$.
Conclusion : L'ensemble des couples solutions de (E) est : $\{(u_0 + bk\ ;\ v_0 - ak) / k \in \mathbb{Z}\}$.

Savoir : $ax + by = 1 \Leftrightarrow ax \equiv 1 \pmod{b}$ ce qui permet de trouver l'inverse de a dans la table de multiplication des congruences modulo b (dans $\mathbb{Z}/b\mathbb{Z}$)
Sion a des conditions sur x et/ou y, (appartenance à un intervalle $[\alpha\ ;\ \beta]$), il reste à résoudre dans $\mathbb{Z}$: $\alpha \leqslant u_0 + bk \leqslant \beta$ et/ou $\alpha \leqslant v_0 - ak \leqslant \beta$ (c'est k l'inconnue)

Voir les exercices et exemples traités dans le livre et en classe et en DM et …

Remarque :
La méthode s'applique dans d'autres cas ….
Un exemple avec le second degré : (même s'il y a plus rapide)
On veut résoudre $ax^2 + bx = c$ et on sait qu'un nombre α est solution. $a \neq 0$
Autrement dit : on peut remplacer c par $a\alpha^2 + b\alpha$ et on a la nouvelle équation :
$ax^2 + bx = a\alpha^2 + b\alpha$ qui se réorganise en $a(x^2 - \alpha^2) = b(\alpha - x)$
En factorisant $x^2 - \alpha^2 = (x - \alpha)(x + \alpha)$, il vient : $a(x - \alpha)(x + \alpha) = b(\alpha - x)$.
Attention !!! si $x \neq \alpha$, on peut réduire …. par $x - \alpha$ $(\alpha - x = -(x - \alpha))$
et, on a : $a(x + \alpha) = -b$.
Si les conditions sont toutes vérifiées, l'autre solution est : $x = -\dfrac{b}{a} - \alpha$.

Illustration :
$x^2 - 2x = 3$ a une solution évidente (-1), d'où, $x^2 - 2x = (-1)^2 - 2\times(-1)$, soit : $(x - 1)(x + 1) = -2(-1 - x)$
L'autre solution est : $x - 1 = 2$, soit : $x = 3$.