Équation diophantienne $ax + by = c$

Ce qui est affirmé sans preuve peut être nié sans preuve. *Euclide d'Alexandrie*

Théorème :

L'équation (E) :$ax + by = c$ admet au moins une solution
si et seulement si
c est un multiple du PGCD de a et de b.
(ou le PGCD de a et b divise c.)

Preuve :

Si (E) admet au moins une solution alors il existe u et v entiers relatifs tels que : $au + bv = c$

Soit ***d = pgcd (a,b)***

d divise a et b donc d divise toute combinaison linéaire à coefficients entiers de a et de b.

Par conséquent d divise $au + bv$ et comme $au + bv = c$

on a : d divise c.

Une condition nécessaire à l'existence d'au moins une solution est donc :
que le PGCD de a et de b divise c.

Cette condition est-elle suffisante ?

Supposons que d divise c.

Il existe alors k entier relatif tel que $c = kd$

d = pgcd (a,b) donc il existe a' et b' premiers entre eux tels que : $a = da'$ et $b = db'$.

Et d'après la propriété de Bézout, alors il existe u et v tels que : $a'u' + b'v' = 1$
d'où : $kda'u' + kdb'v' = kd$ Soit : $aku' + bkv' = c$

En posant : $u = ku'$ et $v = kv'$ qui sont tous deux des relatifs,
nous obtenons que l'équation admet alors au moins une solution.

La condition est donc suffisante.

Le théorème est donc démontré.

Par exemple : $15x + 21y = 20$ n'a aucune solution.

PGCD(15 ; 21) = 3 et 3 ne divise pas 20

$15x + 21y = 36$ a au moins une solution.

en factorisant 3, il vient : $3(5x + 7y) = 3\times 12$

soit : $5x + 7y = 12$ avec 5 et 7 sont des entiers premiers entre eux.

Équation diophantienne $ax + by = c$

Ce qui est affirmé sans preuve peut être nié sans preuve. *Euclide d'Alexandrie*

Méthode :	**Exemple : $5x + 7y = 12$**
Première étape : où on a besoin de Bézout	
On cherche une solution particulière $(x_0 ; y_0)$. Puisque a et b sont premiers entre eux, il existe un couple $(u ; v)$ de $\mathbb{Z}\times\mathbb{Z}$ tel que $au + bv = 1$ En multipliant par c, le couple $(x_0 ; y_0) = (cu, cv)$ est solution de (E).	La recherche de u et v n'est pas toujours immédiate. En ce cas, on utilise l'algorithme d'Euclide. Un exemple à la fin de la fiche. $5\times3 + 7\times(-2) = 1$ Le couple : $(3\times12 ; -2\times12) = (36 ; -24)$ est une solution particulière de (E)
Deuxième étape : où on remplace l'équation par une autre équation …	
On a donc l'égalité : $ax_0 + by_0 = c$ (1) Soit $(x ; y)$ une autre solution de (E), $ax + by = c$ (2) Par comparaison de (1) et (2), on a : $ax + by = ax_0 + by_0$ (3) qu'on réorganise en : $a(x - x_0) = b(y_0 - y)$ (4)	$5\times36 + 7\times(-24) = 12$ (1) $5x + 7y = 12$ (2) d'où : $5(x - 36) = 7(-24 - y)$ (4)
Troisième étape : … pour utiliser le théorème de Gauss	
L'équation (4) est de la forme $aq = bq'$ a et b sont premiers entre eux, a divise bq' donc a divise q'. Il existe un entier k tel que $q' = ak$. $y_0 - y = ak$, $k \in \mathbb{Z}$. On peut recommencer avec b divise aq ou remplacer dans (4), $y_0 - y$ par ak. On obtient : $x - x_0 = bk$.	$5(x - 36) = 7(-24 - y)$ (4) est premier avec 7 et 5 divise le produit $7(-24 - y)$, donc, 5 divise $-24 - y$. Il existe un entier k tel que : $-24 - y = 5k$. $y = -24 - 5k$, $k \in \mathbb{Z}$. En remplaçant $-24 - y$ par $5k$, il vient : $5(x - 36) = 7\times5k$, puis en réduisant par 5, $x - 36 = 7k$. $x = 36 + 7k$, $k \in \mathbb{Z}$.
Dernière étape : vérification (réciproque)	
On a montré : si $(x ; y)$ est un couple solution de (E) alors $x = x_0 + bk$ et $y = y_0 - ak$ où k est un entier. On doit se poser la question : tous les couples $(x_0 + bk ; y_0 - ak)$, $k \in \mathbb{Z}$ sont-ils solutions de (E). Il suffit de vérifier : $a(x_0 + bk) + b(y_0 - ak) = ax_0 + by_0 = c$	Réciproquement, soit $x = 36 + 7k$ et $y = -24 - 5k$ avec $k \in \mathbb{Z}$. On a : $5(36 + 7k) + 7(-24k - 5k) = 5\times36 + 7\times(-24) = 12$. Par conséquent : quelque soit $k \in \mathbb{Z}$, $(36 + 7k ; -24k - 5k)$ est un couple solution de (E).
Conclusion :	
L'ensemble des solutions de (E) est : $\{(x_0 + bk ; y_0 - ak) , k \in \mathbb{Z} \}$	L'ensemble des solutions de (E) : $5x+ 7y = 12$ est l'ensemble des couples $\{ (36 + 7k ; -24k - 5k) , k \in \mathbb{Z} \}$

Équation diophantienne $ax + by = c$

Ce qui est affirmé sans preuve peut être nié sans preuve. *Euclide d'Alexandrie*

Recherche de u et v par l'algorithme d'Euclide

732 et 381

$732 = 381\times1 + 351$ (1)

$381 = 351\times1 + 30$ (2)

$351 = 30\times11 + 21$ (3)

$30 = 21\times1 + 9$ (4)

$21 = 9\times2 + 3$ (5)

$9 = 3\times3 + 0$ (6)

Le dernier reste non nul est 3.

PGCD(732 ; 381) = 3

Il existe *u* et *v* entiers tels que $732u + 381v = 3$

On reprend l'avant-dernière égalité (5) donnant le PGCD :

$3 = 21 - 9\times2$ (6)

de (4) et (6) $9 = 30 - 21\times1$ puis : $3 = 21 - (30 - 21\times1)\times2$

Factoriser 21 $3 = -30\times2 + 21\times3$ (7)

de (3) et (7) $21 = 351 - 30\times11$ puis : $3 = -30\times2 + (351 - 30\times11)\times3$

Factoriser 30 $3 = 351\times3 - 30\times35$ (8)

de (2) et (8) $30 = 381 - 351\times1$ puis : $3 = 351\times3 - (381 - 351\times1)\times35$

Factoriser 351 $3 = -381\times35 + 351\times38$ (9)

de (1) et (9) $351 = 732 - 381\times1$ puis : $3 = -381\times35 + (732 - 381\times1)\times38$

Factoriser 381 $3 = 732\times38 - 381\times73$ (10)

On a donc : $u = 38$ et $v = -73$

Ne pas oublier de vérifier

"La différence entre le mot juste et un mot presque juste est la même qu'entre l'éclair et la luciole." ***Mark Twain***