COURS
LA FIN DE L'ARITHMÉTIQUE

Un grand merci à Yvan Monka pour ses vidéos illustrant très bien ce cours en cette période de télétravail!

Table des matières

I. PGCD

Soient a et b deux entiers non tous les deux nuls.
On notera $\mathscr{D}(a,b)$ l'ensemble de leurs diviseurs communs. Il contient au moins le nombre 1 (même pour des nombres négatifs) et son élément le plus grand est toujours inférieur à $\min(|a|,|b|)$.
Par conséquent :

I.1. Généralité

Définition 1. (et Propriété)

$\mathscr{D}(a,b)$ est un ensemble non vide fini : il admet donc un plus grand élément, appelé **Plus Grand Diviseur Commun** de a et b ou encore $\text{PGCD}(a,b)$. On le note parfois $a \wedge b$.

Exemples :

$\text{PGCD}(4,6) = 2$ $\text{PGCD}(12,13) = 1$ $\text{PGCD}(21,-35) = +7$

Quel est le PGCD de -72 et de 165 ? Quel est le PGCD de -72 et de 1 ?

Quel est le PGCD de -72 et de 0 ? Quel est le PGCD de -72 et de 288 ?

Donner deux couples de nombres dont le PGCD est 20.

Définition 2.

On dit que a et b sont **premiers entre eux** si et seulement si $\text{PGCD}(a,b) = 1$

Exemples :

$\text{PGCD}(3,2) = 1$ $\text{PGCD}(10,21) = 1$ $\text{PGCD}(51,113) = 1$

Les nombres 72 et 145 sont-il premiers entre eux? Donner deux nombres premiers entre eux.

Propriété 1. (Immédiates)

1. $0 < 1 \leq \text{PGCD}(a,b) = \text{PGCD}(b,a) = \text{PGCD}(|a|,|b|) \leq min(|a|,|b|)$
   (c'est ce qui a été dit dans l'intro en gros)
2. $\text{PGCD}(a,0) = |a|$
3. $\text{PGCD}(a,1) = 1$
4. Si $b|a$ alors $\text{PGCD}(a,b) = |b|$

Remarque : Dans tout le chapitre, sauf indication contraire, on considérera désormais les diviseurs positifs communs à deux entiers naturels a et b non tous les deux nuls.

Propriété 2. (Caractéristique)

Soit $d \in \mathbb{N}$. $\quad d = pgcd(a,b) \iff \begin{cases} a = da' \text{ et } b = db' \\ pgcd(a',b') = 1 \end{cases}$

Preuve

$\Longrightarrow$: Si $d = pgcd(a,b)$ alors $d|a$ et $d|b$ il existe a', b' tels que $a = da'$ et $b = db'$.
De plus, si $pgcd(a',b') = k$ et $k \neq 1$, alors il existe a'' et b'' tels que $a' = ka''$ et $b = kb''$ donc $a = dka''$ et $b = dkb''$.
Ainsi $kd|a$ et $kd|b$ donc kd est un diviseur commun de a et b.
Mais $kd > d$ ce qui contredit le fait que d soit le plus grand diviseur commun de a et b.
Donc nécessairement $k = 1$.
$\Longleftarrow$: Si $a = da'$ et $b = db'$ avec $pgcd(a',b') = 1$.
Comme a et b ne sont pas tous les deux nuls, on a $d \neq 0$ et donc $pgcd(a,b) = pgcd(da',db') = d \times pgcd(a',b') = d$.

Remarque : Toute fraction peut alors s'écrire sous forme irréductible.

Pour voir une application de cette propriété, on peut regarder cette vidéo

Il existe plusieurs méthodes pour trouver le pgcd de deux nombres, telles que :

1. Lister les diviseurs comme présenté sur un exemple dans cette vidéo
2. Décomposer les nombres en produits de facteurs premiers
3. Une méthode de réduction
4. L'algorithme d'Euclide dont nous parlerons plus tard

I.2. Détermination du PGCD

I.2.a. A base de produit avec la décomposition en facteurs premiers

Commençons, pour ceux qui se sentent fragile, par un exemple en vidéo rappelant comment on trouve la décomposition en produit de facteurs premiers d'un nombre.

Voyons ensuite un nouvel exemple complet, pour déterminer un PGCD en utilisant la décomposition en produit de facteurs premiers en vidéo jusqu'à 8 min 28 (le PPCM dont Yavan Monka parle n'est plus au programme).

Voici un autre exemple rédigé pour trouver le pgcd de 1800 et de 4125, en utilisant les décompositions de ces nombres en produits de facteurs premiers.

$$\left.\begin{array}{l} 1800 = 2^3 \times 3^2 \times 5^2 = 2^3 \times 3^2 \times 5^2 \times 11^0 \\ 4125 = 3 \times 5^3 \times 11 = 2^0 \times 3 \times 5^3 \times 11 \end{array}\right\} \text{ Alors il est simple de voir que } \quad \text{PGCD}(360, 4125) = 3 \times 5^2 = 75$$

Ceci se généralise ainsi :
Soient a et b deux nombres dont voici la décomposition en produit de facteurs premiers, (faisant intervenir tous les nombres premiers qui interviennent dans la décomposition de a **et** tous les nombres premiers qui interviennent dans celle de b, pour cela certains des α_i et des β_i peuvent-être nuls) :

$$\left.\begin{array}{l} a = p_1^{\alpha_1} p_2^{\alpha_2} \times \ldots\ldots p_n^{\alpha_n} \\ b = p_1^{\beta_1} p_2^{\beta_2} \times \ldots\ldots p_n^{\beta_n} \end{array}\right\} \text{ Alors } \quad \text{PGCD}(a;b) = p_1^{min(\alpha_1,\beta_1)} p_2^{min(\alpha_2,\beta_2)} \times \cdots \times p_n^{min(\alpha_n,\beta_n)}$$

Exemple :

Déterminer le pgcd de $2^6 \times 3^2 \times 11^2 \times 17$ et $3^4 \times 7^4 \times 11 \times 19^2$.

Propriété 3.

Soient a et b deux entier supérieur ou égaux à 2.

- S'ils n'ont aucun facteur commun, $pgcd(a,b) = 1$
- Sinon, $pgcd(a,b)$ est égal au produit des facteurs premiers communs aux deux nombres, chacun étant affecté du plus petit exposant avec lequel il figure dans leurs deux décompositions.

Preuve

Découle de l'homogénéité.

I.2.b. Avec la méthode des réductions (encore appelé algorithme des soustractions)

Commençons par un exemple en vidéo
Maintenant, voyons pourquoi cette méthode fonctionne et la propriété utilisée.

Propriété 4. (Réduction ou soustraction)

L'ensemble des diviseurs de a et b est égal à l'ensemble des diviseurs de b et $a-b$. En fait :

$$\mathscr{D}(a,b)=\mathscr{D}(a-b,b)=\mathscr{D}(a-kb,b) \quad \text{pour tout } k\in\mathbb{Z}$$

Preuve

Il s'agit de montrer une double inclusion. Soit $k\in\mathbb{Z}$.
$\mathscr{D}(a,b)\subset\mathscr{D}(a-kb,b)$: Si d divise a et b, il divise aussi $a-kb$.
$\mathscr{D}(a,b)\supset\mathscr{D}(a-kb,b)$: Si d divise b et $a-kb$ alors il divise $(a-kb)+kb=a$.
D'où l'égalité $\mathscr{D}(a,b)=\mathscr{D}(a-kb,b)$. En prenant $k=1$, on obtient la propriété.

Remarque : Comme l'ensemble des diviseurs de a et b est le même que celui de $a-kb$ et b, leur plus grand élément est en particulier le même.
On peut donc ainsi déterminer des PGCD en avançant certes pas à pas, mais sans aucun calculs complexes.

Exemples :

PGCD(12,8)=PGCD(12-8,8)=PGCD(4,8)=PGCD(4,8-2× 4)=PGCD(4,0)=4

PGCD(7,10)=... PGCD(264,168)=... PGCD(250,71)=...

I.2.c. Avec l'algorithme d'Euclide

Commençons par voir un exemple en vidéo
Retrouver par cette méthode le PGCD(264,168).

Maintenant voyons pourquoi cette méthode fonctionne et le corollaire utilisé.

Corollaire 1. (de la propriété précédente)

Si $0<b\leq a$, alors $\mathscr{D}(a,b)=\mathscr{D}(r,b)$ où r est le reste de la division euclidienne de a par b.

Preuve

Cas particulier de la propriété précédente puisque r est tel que $a=bq+r \Leftrightarrow a-bq=r$ avec $q\in\mathbb{N}$

Exemples :

Là encore, l'égalité des ensembles de diviseurs nous permet de déterminer des PGCD à partir de calculs successifs mais simples.

Recherchons par exemple le PGCD de 10 et 7 grâce à ce corollaire.

$$\begin{aligned} 10 &= 7\times 1+3 \quad \text{Donc PGCD(10,7)=PGCD(7,3)} \\ 7 &= 3\times 2+1 \quad \text{Donc PGCD(7,3)=PGCD(3,1)=1} \end{aligned}$$

Remarque : Grâce au corollaire précédent, on peut s'arrêter dès que la réponse est triviale (même si dans cet exemple, c'est le cas de suite!).

Cependant, dans la suite du chapitre, nous aurons besoin d'appliquer l'algorithme d'Euclide en entier, c'est pourquoi je reviens dessus en détails ici.

Déjà, et ce n'est pas rien, on est sûr que cet algorithme s'arrête, et en plus on sait que le pgcd cherché est le dernier reste non nul dans la succession de divisions faites, grâce aux points suivants (rappelons que $b \leq a$) :

— Si $b|a$ alors PGCD$(a,b) = b$.

— Si b ne divise pas a, alors $\exists!\,(q,r) \in \mathbb{N}^2$ tel que $0 < r < b$ et l'on a $\mathscr{D}(a,b) = \mathscr{D}(b,r)$.

Dans le deuxième cas, comme $b < a$ et $r < b$, on s'est ramené à travailler sur des nombres plus petits.

De plus, comme $r > 0$ (b ne divise pas a), on peut réitérer le processus, autant de fois que nécessaire (c'est-à-dire tant que le reste n'est pas nul).

Il arrivera forcément un moment où le reste de la division sera nul, car la suite des restes est strictement décroissante, minorée par 0.

Grâce au corollaire, on aura alors $\mathscr{D}(a,b) = \mathscr{D}(b,r) = \mathscr{D}(r,r_1) = \mathscr{D}(r_1,r_2) = \cdots = \mathscr{D}(r_k,0)$,

d'où $pgcd(a,b) = r_k$.

Formalisation de l'Algorithme d'Euclide en vue d'une programmation

On note D = $pgcd(a,b)$. On cherche D

1. J'effectue la division euclidienne de a par b : $a = bq + r$. On a alors $\mathscr{D}(a,b) = \mathscr{D}(b,r)$
2. Si $r = 0$ alors $\mathscr{D}(a,b) = \mathscr{D}(b,0)$ et $pgcd(a,b) = pgcd(b,0) = b$.
   Sinon :
   - On pose $r_0 \longleftarrow b$, $r_1 \longleftarrow r$, $i \longleftarrow 1$
   - Tant que $r_i \neq 0$:
     — J'effectue la division euclidienne de r_{i-1} par r_i : $r_{i-1} = r_i q_{i+1} + r_{i+1}$.
     On a alors $\mathscr{D}(a,b) = \mathscr{D}(r_i, r_{i+1})$
     — i prend la valeur $i+1$
3. On a alors $\mathscr{D}(a,b) = \mathscr{D}(r_i, r_{i+1}) = \mathscr{D}(r_i,0)$ et $pgcd(a,b) = pgcd(r_i,0) = r_i$.

II. L'aboutissement de votre programme !

II.1. Equations diophantiennes

Exemples :

— Un groupe d'hommes et de femmes, du temps où l'on pouvait sortir, a dépensé 100 € dans une auberge.
Les hommes ont dépensé 8 € chacun et les femmes 5 € chacune.
Combien pouvait-il y avoir d'hommes et de femmes dans le groupe ?

— Un astronome a observé un jour J un corps céleste A qui apparaît périodiquement tous les 105 jours.
Six jours plus tard (à J + 6), il observe un corps céleste B dont la période d'apparition est de 81 jours.
Quel est le prochain jour J′ où l'astronome verra simultanément les deux objets A et B ?

Dans les deux exemples précédents, on est amené à considérer des équations à deux inconnues **entières** u et v :

— un nombre d'hommes et de femmes.
On a $8u+5v=100$

— un nombre de périodes effectuées par A et par B entre J et J′.
On a $105u = 6+81v \iff 35u-27v=2$

On appelle ce type d'équation, des équations diophantiennes. Il s'agit en fait d'équations polynomiales, à une ou plusieurs inconnues, dont on cherche les solutions **parmi les nombres entiers relatifs**.
En spécialité mathématiques, on s'intéresse aux équations diophantiennes d'inconnues $(x;y)$ du type $ax+by=c$ et ces équations ont un lien avec le pgcd(a,b), d'où tout ce qui a précédé dans votre cours d'arithmétique.

Par exemple on montrera que $264x+168y=10$ n'a pas de solution entière, tandis que $264x+168y=24$ si (attention, les deux équations ont une infinité de solutions si on se place dans les réels !).

Pour cela, réinvestissons ce que l'on vient de voir à travers l'algorithme d'Euclide.
L'algorithme d'Euclide, objet de la sous-partie précédente, est donc une méthode qui permet de trouver le pgcd de deux nombres en effectuant des divisions euclidiennes successives et bien choisies.
Le $pgcd$ des deux nombres est alors le dernier reste non nul obtenu.
. Cette méthode est certes fastidieuse, mais elle a l'avantage de donner une combinaison linéaire du type $ax+by=d$, ce qui nous intéresse ici.

Commençons par regarder un exemple en vidéo

Exemples :

Reprenons un exemple précédent "en lignes" : le pgcd de 264 et 168.

$$\begin{aligned} 264 &= 168\times 1+96\\ 168 &= 96\times 1+72\\ 96 &= 72\times 1+24\\ 72 &= 24\times 3+0 \end{aligned}$$

Le dernier reste non nul est 24 : c'est donc le pgcd de 264 et 168.

De plus, en partant de l'avant-dernière ligne et en "remontant" les égalités petit à petit, on peut remarquer que

$$\begin{aligned} 24 &= 96-72\\ &= 96-(168-96)\\ &= 2\times 96-168\\ &= 2\times(264-168)-168\\ 24 &= 2\times 264-3\times 168 \end{aligned}$$

Ceci nous a donc permis de trouver une solution à l'équation diophantienne $264x+168y=24$, à savoir le couple $(2,-3)$.

Il est alors simple de trouver des solutions aux équations diophantiennes du type $264x+168y=24k$. Donner une solution à l'équation $264x+168y=48$, puis à l'équation $264x+168y=-72$.

En suivant cette méthode, trouver une solution à l'équation $8x+5y=1$, puis proposer une réponse à la question du premier exemple de cette partie.

$$\begin{aligned} 8 &= 5\times 1+3\\ 5 &= 3\times 1+2\\ 3 &= 2\times 1+1 \end{aligned}$$

$$\begin{aligned} 1 &= 3-2\\ &= 3-(5-3)=3\times 2-5\\ &= (8-5)\times 2-5\\ 1 &= 8\times 2-5\times 3 \end{aligned}$$

Donc $8\times 200-5\times 300=100$. Donc ceci ne répond pas au pb ici, désolée.
A tâtons, on peut trouver que $8\times 5+5\times 12=100$

En suivant cette méthode, trouver une solution à l'équation $35x - 27y = 1$, puis proposer une réponse à la question du deuxième exemple de cette partie.

Bien. Voyons maintenant en détails pourquoi l'équation $264x + 168y = 10$ n'a pas de solution entière, tandis que $264x + 168y = 24$ si (à suivre ...)

II.2. Théorème de Bezout

Etienne Bezout (1730-1783) fut un génie assez précoce puisqu'à 19 ans, il était déjà adjoint de l'Académie des Sciences. Sa plus grande oeuvre, *Théorie générale des équations algébriques*, un traité clair et détaillé, témoigne de sa pédagogie et de sa volonté de rendre parfaitement accessibles ses découvertes. Bézout fit aussi une brillante carrière dans la marine royale et de chargé de l'enseignement des élèves du corps d'artillerie.

Propriété 5.

Soient a et b deux entiers relatifs non tous les deux nuls et $d = pgcd(a,b)$. Alors :

1. Il existe u et v entiers relatifs tels que $au+bv = d$
2. L'ensemble des entiers $au+bv$ (avec u et v entiers relatifs) est l'ensemble des multiples de d.

Preuve

1. C'est ce que l'on a fait la semaine dernière, en "remontant" l'algorithme d'Euclide petit à petit (on peut aussi le "descendre", ce qui est plus facile à rédiger pour les indices, d'où cette démonstration)

   On utilise l'algorithme d'Euclide. On a :
   $a = bq_0 + r_0 \iff r_0 = a - bq_0 = au_0 + bv_0$ avec $u_0 = 1$ et $v_0 = -q_0$ deux entiers relatifs.
   $b = r_0q_1 + r_1 \iff r_1 = b - r_0q_1 = b - (au_0 + bv_0)q_1 = au_1 + bv_1$ avec $u_1 = -u_0q_1$ et $v_1 = 1 - v_0q_1$ deux entiers.
   Pas à pas, on exprime chaque reste comme combinaison linéaire entière de a et b jusqu'à r_k, ie le $pgcd(a,b)$.

2. $\subset$: Soit $n = au+bv$.
   Comme d divise a et b on a $d|(au+bv) \iff d|n$,
   (c'est la même idée que dans les exos de la feuille 6)
   Donc n est un multiple de d.
   $\supset$: Soit n un multiple de d.
   On sait d'après le 1) de cette propriété qu'il existe u et v tels que $d = au+bv$.
   Alors il existe k tel que $n = kd = k(au+bv) = a\mathrm{U} + b\mathrm{V}$.
   Donc n est une combinaison linéaire de a et b.

Corollaire 2.

Soient a et b deux entiers relatifs non tous les deux nuls. On note d leur PGCD.
L'équation $ax+by=c$, admet des solutions entières si et seulement si $d|c$

Exemple :

PGCD(264,168)=24.
L'équation $264x+168y=10$ n'admet donc aucune solution entière!
Tandis qu'il est logique d'en avoir trouver au moins une pour l'équation $264x+168=-72$.

Théorème 1. (de Bezout)

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

Preuve

$\Rightarrow$: Si a et b sont premiers entre eux, on applique le 1) de la propriété précédente pour $d=1$.

$\Leftarrow$: S'il existe des entiers relatifs u et v tels que $au+bv=1$ alors d'après le 2) de la propriété précédente, 1 est un multiple du $pgcd(a,b)$.
Par conséquent $d=1$.

Exemples :

— $a=4$ et $b=9$ sont premiers entre eux donc on sait qu'il existe deux entiers relatifs u et v tels que $4u+9v=1$.
Par exemple $9\times1-4\times2=1$. Donc $(u,v)=(-2;1)$ convient.

— Trouver un couple (u,v) tel que $au+bv=1$ pour

- $a=7$ et $b=17$
- $a=71$ et $b=19$

— Mais ce théorème peut nous servir à prouver des résultats bien plus généraux.
Regardez par exemple cette vidéo ou encore celle-ci.

— En essayant de suivre la méthode de la deuxième vidéo proposée, montrer que pour tout $n\in\mathbb{Z}$:

- n et $n+1$ sont premiers entre eux
- $2n+1$ et $3n+1$ sont premiers entre eux
- $2n+5$ et $3n+7$ sont premiers entre eux

— Sur le même principe, déterminer le PGCD$(2n+1;2n+3)$ pour tout entier naturel n

II.3. Théorème de Gauss

Carl Friedrich Gauss (1777-1855) fut un mathématicien, astronome et physicien allemand. Il n'existe pas un seul domaine scientifique qu'il n'ait pas abordé, et on lui doit, entre autres, des travaux sur les polygone régulier, sur les nombres complexes, le magnétisme, l'algèbre et bien sûr, l'arithmétique. Il s'impliqua de plus dans les affaires politiques de son temps.

Théorème 2.

Soient a, b, et c trois entiers relatifs non nuls.
Si $a|bc$ et $pgcd(a,b) = 1$ alors $a|c$.

Preuve

a et b sont premiers entre eux, donc d'après Bezout il existe $(u,v) \in \mathbb{Z}^2$ tels que $au + bv = 1$.
Donc $c = cau + cbv$
De plus, $a|bc$ donc il existe $k \in \mathbb{Z}$ tel que $bc = ka$.
Ainsi $c = cau + kav = a(cu + kv)$ avec $cu + kv$ entier. D'où $a|c$.

Exemples :

Commençons par regarder un exemple en vidéo de résolution d'équation diophantienne particulière grâce au théorème de Gauss, jusqu'à 4min16s.
Raisonner de la même manière pour résoudre dans $\mathbb{Z}$ les équations suivantes :

1. $3x = 5y$.
2. $273x = 637y$.

Corollaire 3.

Si deux entiers a et b divise un entier c avec $pgcd(a,b) = 1$ alors $ab|c$.

Preuve

$a|c$ donc il existe un entier k tel que $c = ak$.
$b|c$ donc $b|ak$.
Comme a et b sont premiers entre eux, d'après Gauss on a $b|k$.
Ainsi, il existe un entier l tel que $k = bl$.
On a alors $c = ak = abl$. D'où $ab|c$.

Exemple :

2 et 3 divisent tous les deux 18 et le pgcd(2,3)=1 donc $2 \times 3 = 6$ divise aussi 18.
Mais ceci était déjà connu grâce à la décomposition en produit de facteurs premiers, donc ce n'est pas vraiment nouveau.

La prochaine fois, en combinant ce que nous avons appris sur Bezout et Gauss, nous verrons enfin comment résoudre de manière générale les équations diophantiennes du type $ax+by=c$, c'est-à-dire trouver **tous** les couples d'entiers solutions de ces équations.

II.4. Equations du type $ax+by=c$.

Vous pouvez commencer par regarder cette vidéo (20 min)

Exemple :

Résoudre l'équation diophantienne $6x+15y=3$.

Solution :

1. On commence toujours par **simplifier l'équation** "au maximum" :

$$6x+15y=3 \iff 2x+5y=1$$

2. On utilise alors **Bezout** pour justifier que l'équation admet ou non des solutions.

D'après le théorème de Bezout, comme 2 et 5 sont premiers entre eux, cette équation admet au moins une solution.

Cette étape n'est pas possible si vous n'avez pas simplifié l'équation correctement, d'où l'ordre important des étapes.

3. S'il y a des solutions, on cherche alors une **solution particulière** au brouillon (inutile de rédiger) :
   - **soit à tâtons** mais intelligemment :
     - en utilisant les critères de divisibilité

On veut que $y=\dfrac{1-2x}{5}$ soit entier, donc on cherche les multiples de 2 se finissant par 1 ou 6 pour que $1-2x$ se finissent par 0 ou 5 et soit donc divisible par 5.
Les multiples de 2 ne se finissent jamais pas 1, donc on en cherche un qui se finit par 6.
Par exemple $x=3$ et dans ce cas on a $y=-1$.

Cette méthode est à adapter suivant le numérateur évidemment!!
Ainsi on aurait pu chercher x tel que $x=\dfrac{1-5y}{2}$ soit entier et donc y tel que $5y$ se finisse par 1, 3, 5, 7 ou 9 (5 étant le seul non absurde) pour que $1-5y$ se finisse par 0, 2, 4, 6 ou 8 et soit ainsi divisible par 2.
Dans ce cas on aurait pu proposer $y=1$ et donc $x=-2$.
Si ce n'est pas encore clair pour vous, regardez cette vidéo de 36 secondes à 3min03

- **en utilisant les congruences**

  On cherche y tel que $5y \equiv 1\ [2]$. Avec cette méthode, on voit qu'il suffit de tester deux valeurs pour y seulement avant de trouver un solution : une valant 0 modulo 2 (absurde ici puisque dans ce cas $5y \equiv 0\ [2]$) et une valant 1 modulo 2, par exemple 1.
  Et dans ce cas, on propose aussi $x = \dfrac{1-5\times(1)}{2} = -2$.

  On peut évidemment aussi chercher x tel que $2x \equiv 1\ [5]$, mais on aurait 4 choix pour tester x au lieu de 2. Ceci dit, le premier possible que l'on proposerait serait $x = 3$ et donc $y = -1$.

— **soit en utilisant l'algorithme d'Euclide** : fastidieux mais infaillible quand les nombres sont grands

$$5 = 2\times 2+1 \iff 1 = 5-2\times 2$$

Donc on propose $x = -2$ et $y = 1$ *On peut revoir cette méthode dans cette vidéo*

4. Grâce à la solution particulière trouvée (j'ai choisis le couple $(-2,1)$) **on réécrit l'équation** :
   Si $(x;y)$ est solution de cette équation, alors

$$2x+5y = 2\times(-2)+5\times 1 \iff 2x-2\times(-2) = 5\times 1-5y \iff 2(x+2) = 5(1-y) \quad (\star)$$

5. Ce qui permet d'utiliser **Gauss** :
   Ainsi $2\,|\,5(1-y)$. Or 2 et 5 sont premiers entre eux, **donc** d'après le théorème de Gauss :

$$2\,|\,(1-y) \iff \exists k\in\mathbb{Z},\ 1-y = 2k \iff \exists k\in\mathbb{Z},\ y = 1-2k$$

6. On réinjecte cette forme pour y dans l'équation $(\star)$ pour **trouver une forme pour** x :
   D'où

$$2(x+2) = 5\times 2k \iff x+2 = 5k \iff x = 5k-2$$

   Donc les solutions de cette équation sont **des** couples de la forme $(5k-2;1-2k)$ où $k\in\mathbb{Z}$.

7. **Réciproque et conclusion :** Vérifions que tous les couples de cette forme sont solution.
   Soit $k\in\mathbb{Z}$, alors

$$2(5k-2)+5(1-2k) = 10k-4+5-10k = 1$$

   L'ensemble des solutions est donc l'ensemble des couples de la forme $(5k-2;1-2k)$ où $k\in\mathbb{Z}$.
   Par exemple pour $k = 10$ on obtient la solution $(48,-18)$

Méthode de Résolution

1. Simplification de l'équation.
   - On calcule $d = pgcd(a,b)$
   - On divise l'équation par d : on obtient $a'x + b'y = d'$ avec $pgcd(a',b') = 1$
2. Recherche d'une solution particulière :
   - On cherche $(x_0, y_0) \in \mathbb{Z}^2$ tels que $a'x_0 + b'y_0 = d'$ à l'aide des divisions euclidiennes
3. Recherche de toutes les solutions :
   - On désigne par x et y d'autres solutions.
     On a alors $a'(x-x_0) + b'(y-y_0) = 0 \iff a'(x-x_0) = -b'(y-y_0)$
   - D'après le théorème de Gauss, on a alors que $a' | (y-y_0)$
     ie qu'il existe $k \in \mathbb{Z}$ tel que $ka' = y - y_0 \iff y = ka' + y_0$.
   - Alors $a'(x-x_0) = -b' \times ka' \iff x = -b'k + x_0$
4. Conclusion : Les solutions sont les couples de la forme $(-b'k + x_0; a'k + y_0)$, avec $k \in \mathbb{Z}$

Exemples :

Reprendre les deux exemples concrets du II.1. pour trouver toutes les solutions aux équations

$$8u + 5v = 100 \qquad \text{et} \qquad 35u - 27v = 2$$

puis donner des solutions répondant au problème en tenant compte de leur aspect concret (solutions positives).

Solutions :

Pour $8u + 5v = 100$, on trouve qu'il a pu y avoir 0 hommes et 20 femmes, ou encore 5 hommes et 12 femmes, ou enfin 10 hommes et 4 femmes.
Pour $35u - 27v = 2$, on trouve par exemple que A et B seront visible pour la première fois la même nuit dans J + 735 jours (pour $u = 7$ et $v = 9$), mais il y a une infinité de solutions au problème.

Exercice 1 : On cherche les solutions entières de l'équation :

$$(E) : 7x + 13y = 1$$

1. Déterminer une solution $(x_0; y_0)$ de (E).
2. Montrer qu'une solution $(x; y)$ de (E) vérifie l'équation :

$$7(x - x_0) = 13(y_0 - y)$$

3. Résoudre cette équation.

Exercice 2 : Léo prend le métro pour aller au travail. A la station Bézout, il doit changer de rame, la correspondance est sur le même quai. Il sait que son premier métro (Ligne A - durée du trajet 8 minutes) passe toutes les 7 minutes et le second (ligne B) toutes les 11 minutes. Ce matin il a pris son premier métro à 6 h 52, il est arrivé à $7h$ à la station Bézout et il a du attendre 6 minutes la rame de la ligne B.
Léo voudrait savoir à qu'elle heure partir entre $6h$ et $9h$ pour ne pas attendre la rame de la ligne B à la station Bézout.
On note x le nombre de rames de la ligne A et y le nombre de rames de la ligne B **parties après** 7 h de l'endroit où Léo les prend.

1. Montrer que, pour que l'attente soit nulle à la station Bézout, x et y doivent vérifier l'équation (E_1) : $7x - 11y = -12$.
2. Déterminer une solution particulière de (E_1).
3. Déterminer l'ensemble des solutions de (E_1).
4. Déterminer à quelles heures entre 6 h et 9 h, Léo peut prendre son premier métro pour ne pas attendre à la station Bézout.

Solutions :

De l'exo 2 :

1. Cherchons le premier train de la ligne A qui part après 7h : Il y en a un à 6h52, un à 6h59 et un à 7h06.
   Donc le premier train de la ligne A part 6 min après 7h, soit 7min - 1 min après 7h.
   Ainsi le $x^{ème}$ train de la ligne A est parti $7x - 1$ minutes après 7h00. Il passera donc à la station Bézout $7x - 1 + 8$ minutes après 7h00.

   Pour la ligne B, le premier train est celui de 7h06, soit 6 min après 7h, donc 11 min - 5 min après 7h.
   Ainsi le $y^{ème}$ train de la ligne B est à la station Bézout $11y - 5$ minutes après 7h00.

   On cherche donc x et y tels que $7x - 1 + 8 = 11y - 5 \iff 7x - 11y = -12$

2) $7x - 11y = -12 \iff -11y \equiv -12 \quad [7]$

$\iff -4y \equiv -5 \quad [7]$

$\iff 4y \equiv 5 \quad [7]$

y	0	1	2	3
$4y$	0	4	8	12
$4y$ [7]	0	4	1	5

Donc si $y = 3$ on a bien $4y \equiv 5 \quad [7]$.

et il suffit de choisir x tq $7x = -12 + 11y$

$= -12 + 11 \times 3$

$= -12 + 33$

$7x = 21$

$x = 3$.

Une sol. particulière de (E_1) est $(3;3)$.

3). Ainsi $7x - 11y = 7 \times 3 - 11 \times 3$

$\iff 7(x-3) = 11(y-3)$

Donc $7 \mid 11(y-3)$. Comme $PGCD(7;11) = 1$

d'après Gauss $7 \mid (y-3)$.

Ainsi $\boxed{y - 3 = 7k}$ avec $k \in \mathbb{Z}$.

D'où $7(x-3) = 11 \times 7k$

$\iff x - 3 = 11k$

$\iff \boxed{x = 11k + 3}$

Les solutions sont donc des couples de la forme $(11k+3; 7k+3)$ avec $k \in \mathbb{Z}$.

• Or $7(11k+3) - 11(7k+3) = 7 \times 3 - 11 \times 3 = -12$. $\forall k \in \mathbb{Z}$

Les sol. de (E_1) sont finalement tous les couples de la forme $(11k+3; 7k+3)$ avec $k \in \mathbb{Z}$.

4) On veut que le 1er train soit pris entre 6h et 9h
ie 7h - 60 min et 7h + 120 min.
Donc on cherche x tq $-60 \leqslant 7x - 1 \leqslant 120$ (cf 1))

$\iff -60 \leqslant 7(11k-3)-1 \leqslant 120$

$\iff \dots$

$\iff -1{,}04\dots \leqslant k \leqslant 1{,}30\dots$

D'où $k \in \{-1; 0; 1\}$ et $x = 11k+3 \in \{-8; 3; 14\}$

Il s'agit donc des trains partis $7\times -8 - 1 = -57$ min après 7h
$7\times 3 - 1 = 20$ min après 7h
$7\times 14 - 1 = 97$ min après 7h

ie des trains partis à 6h03, 7h20 et 8h37.

Vérification (facultatif)
- on peut déjà rapidement contrôler qu'il y a bien des trains de la ligne A qui partent à ces heures là.
- Ils arrivent alors à Bézout à 6h11, 7h28 et 8h45
- on peut alors vérifier que des trains de la ligne B partent bien aussi à ces heures-ci.
- Pour être sûr d'avoir toutes les sol, il faudrait lister ts les horaires, mais a priori, si on a juste avant, on a de bonnes chances de ne pas avoir oublié de solutions.

Exo 1 :

1) $7x+13y=1 \iff 13y=1 \quad [7]$.

y	0	1	2	3	4	5	6
$13y$	0	13	26	39	52	65	78
$13y\ [7]$	0	6	2	4	3	2	1

Donc si $y=6$ on a bien $13y \equiv 1 \quad [7]$.
Dans ce cas, on choisit x tq $7x = 1-13y$

$$\iff x = \frac{-77}{7} = -11.$$

Une solution de (E) est donc $(-11;6)=(x_0;y_0)$

2) (x,y) est une solution de $(E) \iff 7x+13y = 7\times(-11)+13\times 6$

$$\iff 7(x+11) = 13(6-y)$$
$$\iff 7(x-x_0) = 13(y_0-y)$$

3) Ainsi $7 \mid 13(y_0-y)$.
Or $PGCD(7;13)=1$ donc $7 \mid (y_0-y)$
Ainsi $\exists k \in \mathbb{Z}$, $y_0-y = 7k \iff 6-y=7k \iff \boxed{y=6-7k}$
Et donc $7(x+11) = 13\times 7k$

$$\iff x+11 = 13k$$
$$\iff \boxed{x = 13k-11}.$$

De plus $7(13k-11)+13\times(6-7k) = -77+78 = 1$.
Donc les solutions sont les couples $(13k-11;6-7k)$ avec k