Chapitre 4

PGCD et applications

Les nombres sont le plus haut degré de la connaissance. Le nombre est la connaissance même.

Platon (428 av JC - 348 av JC).

I PGCD

4.1.1 Définition

Définition 1 — Si a et b sont deux entiers, on note $\mathcal{D}(a)$ l'ensemble des diviseurs positifs de a et $\mathcal{D}(a,b)$ l'ensemble des diviseurs positifs communs à a et b. Autrement dit :

- $\mathcal{D}(a) = \{n \in \mathbf{N}, n|a\}$;
- $\mathcal{D}(a,b) = \{n \in \mathbf{N}, n|a \text{ et } n|b\}$.

☞ **Exemple 1** $\mathcal{D}(12) = \{1,2,3,4,6,12\}$, $\mathcal{D}(15) = \{1,3,5,15\}$ et $\mathcal{D}(12,15) = \{1,3\}$.

Proposition 4.1 — *Soit a et b deux entiers. Alors :*

1) $\mathcal{D}(a,b) = \mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b,a)$,
2) $1 \in \mathcal{D}(a,b)$ *et donc* $\mathcal{D}(a,b) \neq \emptyset$,
3) *si a ou b est non nul, $\mathcal{D}(a,b)$ est un ensemble fini,*
4) *si a divise b alors $\mathcal{D}(a,b) = \mathcal{D}(a)$. En particulier, $\mathcal{D}(a,0) = \mathcal{D}(a)$,*
5) $\mathcal{D}(a,b) = \mathcal{D}(|a|,|b|)$.

Théorème 4.2 (Existence du PGCD) — *Si a et b sont deux entiers relatifs non tous nuls, alors l'ensemble des diviseurs communs à a et b admet un plus grand élément dans $\mathbf{Z}$. Cet élément est un entier naturel strictement positif.*

On commence avec un lemme bien utile :

Lemme 4.2-1 — *Toute partie non vide et majorée de $\mathbf{N}$ admet un plus grand élément.*

Définition 2 (PGCD) — On appelle cet élément le **Plus Grand Commun Diviseur** à a et b : on le note $\text{PGCD}(a,b)$ ou $a \wedge b$.

☞ **Exemple 2** $\text{PGCD}(12,15) = 3$.

Proposition 4.3 — *Soient a et b deux entiers relatifs non tous nuls. Alors :*

1) $\text{PGCD}(a,b) = \text{PGCD}(b,a)$,
2) $\text{PGCD}(a,b) = \text{PGCD}(|a|,|b|)$,
3) $\text{PGCD}(a,b) \geqslant 1$, $\text{PGCD}(0,a) = |a|$, $\text{PGCD}(1,a) = 1$
4) $a|b$ *si et seulement si* $\text{PGCD}(a,b) = a$,
5) $\text{PGCD}(a,b) = \text{PGCD}(a-b,b)$.

4.1.2 Algorithme d'Euclide

Comme on l'a vu précédemment, on peut considérer a et b entiers **naturels** non nuls, tels que $a > b$. Voyons maintenant une façon algorithmique de calculer le pgcd de deux nombres :

Proposition 4.4 (Euclide) — *Si r est le reste de la division euclidienne de a par b, alors* $\text{PGCD}(a,b) = \text{PGCD}(b,r)$

Ceci nous permet d'appliquer l'algorithme d'Euclide afin de déterminer le PGCD de deux entiers :

Méthode 4.1 : L'algorithme d'Euclide.

Posons $r_0 = b$ et r_1 le reste dans la division de a par $r_0 = b$. Alors, d'après la propriété d'Euclide, $\text{PGCD}(a,b) = \text{PGCD}(a,r_0) = \text{PGCD}(r_0,r_1)$. *Deux cas sont possibles :*

- *si $r_1 = 0$ alors $d = \text{PGCD}(r_0,r_1) = \text{PGCD}(r_0,0) = r_0$ et on s'arrête.*
- *sinon, $r_1 > 0$ et on peut effectuer la division euclidienne de r_0 par r_1, qui nous donne un reste r_2, de plus :* $\text{PGCD}(a,b) = \text{PGCD}(r_1,r_2)$.

On est sûr que cet algorithme s'arrête au bout d'un nombre fini d'étapes car la suite des restes est strictement décroissante. Ainsi, il existe $k \in \mathbf{N}$ tel que $r_k \neq 0$ et $r_{k+1} = 0$. D'après la propriété d'Euclide :

$$\mathcal{D}(a,b) = \mathcal{D}(r_0,r_1) = \mathcal{D}(r_1,r_2) = \ldots = \mathcal{D}(r_k,r_{k+1}) = \mathcal{D}(r_k,0) = \mathcal{D}(r_k).$$

Or le plus grand élément de $\mathcal{D}(r_k)$ est r_k car $r_k \neq 0$ donc on a la propriété suivante :

Proposition 4.5 — *Le* PGCD *de a et b est le dernier reste non nul dans l'algorithme d'Euclide.*

☞ **Exemple 3**

Déterminons par l'algorithme d'Euclide le PGCD des nombres 1636 et 1128.

$$1636 = 1128 \times 1 + 508$$
$$1128 = 508 \times 2 + 112$$
$$508 = 112 \times 4 + 60$$
$$112 = 60 \times 1 + 52$$
$$60 = 52 \times 1 + 8$$
$$52 = 8 \times 6 + 4$$
$$8 = 4 \times 2 + 0$$

Le PGCD des nombres 1636 et 1128 est le dernier reste non nul, c'est-à-dire 4.

4.1.3 Corollaires

Proposition 4.6 — *L'ensemble des diviseurs positifs communs à a et b est l'ensemble des diviseurs positifs de* $\text{PGCD}(a,b)$.

Proposition 4.7 — *Soient a et b deux entiers non tous nuls.*
d est un diviseur commun à a et b si et seulement si d divise le pgcd de a et b.

II Nombres premiers entre eux

4.2.1 Définition

Dans toute la suite, a et b sont deux entiers relatifs non nuls.

Définition 3 (Nombres premiers entre eux) — a et b sont dits **premiers entre eux** lorsque $\text{PGCD}(a,b) = 1$.

Par exemple, 21 et 11 sont premiers entre eux, de même que tout entier relatif et 1.

4.2.2 Théorème de Bézout

Théorème 4.8 (Théorème de Bézout) — *Si a et b sont deux entiers non tous nuls, alors a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que :*

$$au + bv = 1.$$

*L'égalité $au + bv = 1$ est appelée **identité de Bézout**.*

☞ **Exemple 4 (Justifier l'existence et déterminer deux entiers u et v tels que $257u+124v=1$.)**
Déterminons par l'algorithme d'Euclide le PGCD des nombres 257 et 124.
Le PGCD des nombres 257 et 124 est le dernier reste non nul, c'est-à-dire 1.
Donc le PGCD de 257 et 124 vaut 1, ainsi ces deux nombres sont premiers entre eux, donc d'après le théorème de Bézout il existe deux entiers u et v tels que $257u+124v=1$. Pour déterminer u et v, on remonte l'algorithme d'Euclide et on trouve :

$$114\times 124-55\times 257=1.$$

Ainsi, $u=114$ et $v=-55$ conviennent.

Remarque 1 Les entiers u et v sont aussi premiers entre eux. Ils ne sont pas uniques, par exemple $3\times 1+2\times(-1)=1$ et $3\times 3+2\times(-4)=1$.

Théorème 4.9 — *Soit a et b deux entiers non tous nuls et d un entier strictement positif. Les propositions suivantes sont équivalentes :*

1) $d=a\wedge b$,
2) *d divise a, d divise b et les entiers $a'=\dfrac{a}{d}$ et $b'=\dfrac{b}{d}$ sont premiers entre eux,*
3) *d divise a, d divise b et il existe deux entiers u et v tels que $au+bv=d$.*

Remarque 2 L'hypothèse $d|a$ et $d|b$ dans le point 3 est essentiel :

$$3\times 2+2\times(-2)=2$$

mais $3\wedge 2=1$.

Proposition 4.10 — *Soit a, b et k trois entiers naturels non nuls. Alors :*

1) $\mathrm{PGCD}(ka,kb)=k\,\mathrm{PGCD}(a,b)$.
2) *Si b et k sont premiers entre eux, alors* $\mathrm{PGCD}(ka,b)=\mathrm{PGCD}(a,b)$.

III Applications

4.3.1 Théorème de Gauss

Théorème 4.11 (Théorème de Gauss) — *Soient a, b et c trois entiers non nuls.*
Si $a|bc$ et si a et b sont premiers entre eux, alors $a|c$.

☞ **Exemple 5 (Déterminer l'ensemble des entiers a et b tels que $3a=5b$.)**
$5|3a$ or $3\wedge 5=1$ donc $5|a$: ainsi il existe $k\in\mathbf{Z}$ tel que $a=5k$. Ainsi $3\times 5k=5b$ donc $b=3k$. Réciproquement... ça marche ! Donc l'ensemble des couples (a,b) solutions sont les couples $(5k,3k)$ où $k\in\mathbf{Z}$.

Un petit corollaire maintenant :

Théorème 4.12 — *Soient a, b et c trois entiers relatifs non nuls.*
Si b et c sont premiers entre eux et divisent a, alors bc divise a.

☞ **Exemple 6** Si $n\in\mathbf{N}$, alors $n(n+1)(n+2)$ est divisible par 6 car divisible par 3 et par 2.

4.3.2 L'équation diophantienne

Si a, b et c sont trois entiers et $d=a\wedge b$, alors l'équation :

$$(E)\qquad ax+by=c$$

d'inconnues $(x,y)\in\mathbf{Z}^2$, est dite équation **diophantienne**.

Proposition 4.13 — *L'équation (E) possède des solutions si et seulement si d divise c.*

☞ **Exemple 7 (Résoudre dans $\mathbf{Z}^2$ l'équation (E) : $24x+18y=36$.)**
► **Existence des solutions :** $\mathrm{PGCD}(24,18)=6$ et 36 est un multiple de 6 donc cette équation admet des solutions

dans $\mathbf{Z}^2$.

► **Détermination d'une solution :**

$$24 = 18 + 6$$
$$18 = 3 \times 6 + 0$$

On a donc immédiatement :

$$6 = 24 - 18$$
$$36 = 6 \times 24 - 6 \times 18$$

Donc $(6, -6)$ est un couple solution de (E).

► **Détermination de toutes les solutions :**

Soit (x,y) une solution de (E). Alors

$$\begin{aligned} 24x + 18y &= 36 && (L_1) \\ 24(6) + 18(-6) &= 36 && (L_2) \\ 24(x-6) + 18(y+6) &= 0 && (L_1 - L_2) \\ 24(6-x) &= 18(y+6) \\ 4(6-x) &= 3(y+6) \end{aligned}$$

4 divise $3(y+6)$ or 4 est premier avec 3 donc 4 divise $y+6$: ainsi il existe $k \in \mathbf{Z}$ tel que $y+6 = 4k$ soit $y = 4k-6$. En reportant dans l'équation (E), on obtient $x = 6-3k$.

► **Réciproquement**, tout couple $(6-3k; 4k-6)$ est solution de (E) donc finalement, les solutions de (E) sont les couples $(6-3k; 4k-6)$ où $k \in \mathbf{Z}$.

4.3.3 Fractions irréductibles

Définition 4 (Nombre rationnel) — Un nombre x est dit **rationnel** s'il peut s'écrire sous forme de fraction : $x = \dfrac{a}{b}$ où $(a,b) \in \mathbf{Z} \times \mathbf{N}^*$.

Définition 5 (Fraction irréductible) — Une fraction $\dfrac{a}{b}$ est dite **irréductible** si $a \wedge b = 1$.

Proposition 4.14 (Unicité de la forme irréductible) — *Toute faction $\dfrac{a}{b}$ est égale à une unique fraction irréductible $\dfrac{a'}{b'}$.*

IV Exercices

Introduction

♦ **PGCD.1** (**Des bonbons et des chocolats**) Lucas et Chloé sont de grand amateurs de bonbons. Leurs préférés sont un bonbon rose à 25 centimes et une barre au chocolat à 45 centimes. Ils disposent, ce jour là, d'une somme maximale de 4,80 euros.
On s'intéresse aux différents achats qu'ils peuvent faire, et on note x et y le nombre de bonbons et de barres au chocolat achetés par les deux enfants.

1) a) Lucas est prêt à dépenser les 4,80 euros qu'ils possèdent et Chloé voudrait avoir 10 confiseries. Est-ce possible ?

b) Chloé veut avoir trois fois plus de barres que de bonbons et Lucas veut encore dépenser le plus possible. Combien auront-ils de confiseries ?

2) a) Justifier que x et y vérifient :

$$x \geqslant 0, \quad y \geqslant 0, \quad y \leqslant -\frac{5}{9}x + \frac{32}{3}.$$

b) Représenter, dans un repère d'unité graphique 1cm, la zone du plan définie par les inéquations ci-dessus.

c) Préciser, dans la zone en question, les points représentants les achats possibles de Lucas et Chloé. Combien y en a-t-il ?

d) Lucas et Chloé peuvent-ils dépenser tout leur argent ?

♦ **PGCD.2** (**Un théorème de Bachet de Méziriac**)
Un astronome a observé un corps céleste A, il y a quelques jours, et observe un autre corps céleste B aujourd'hui. Le corps A a une période de révolution de 180 jours et le corps céleste B a une période de révolution de 186 jours.
On se demande si l'astronome pourra observer les deux corps le même jour, et si oui, dans combien de jours.

Partie A - Mise en équation

Si les deux corps sont observables le même jour, on note n le nombre de jours séparant les deux observations de A et B par l'astronome, u le nombre de périodes effectuées par A et v le nombre de périodes effectuées par B avant que l'astronome ne les observe le même jour.
Justifier que u et v sont deux entiers tels que

$$180u - 186v = n.$$

Partie B - Exploration

1) Dans un tableur, donner les valeurs prises par $180x - 186y$ pour des valeurs entières de x et y .

2) a) Quelle symétrie peut-on observer dans ce tableau ? Quel est le plus petit entier strictement positif du tableau ?

b) Quelle conjecture peut-on faire sur les entiers qui s'écrivent sous la forme $180x - 186y$?

3) Démontrer que $180x - 186y$ est toujours un multiple de 6.
Si l'astronome a vu A sept jours avant B, pourra-t-il observer les deux corps le même jour ?

4) Si l'astronome a vu A six jours avant B, sait-on s'il pourra observer les corps A et B le même jour ?

5) On considère, dans le plan muni d'un repère, la droite d d'équation $180x - 186y = 6$.

a) Quel point de la droite d connaît-on d'après le tableau ?

b) Préciser un vecteur directeur de d et en déduire d'autres points de d à coordonnées entières positives.

c) La réponse à l'astronome est-elle positive ?

Partie C - Démonstration dans le cas général

Soit a et b deux entiers naturels non nuls et l'ensemble $E = \{ax - by, \quad (x,y) \in \mathbf{Z}^2\}$, ainsi que $E^+ = E \cap \mathbf{N}^*$.

1) a) Démontrer que E^+ est non vide.

b) En déduire qu'il admet un plus petit élément noté d tel que $d = ax_0 - by_0$.

2) Démontrer que tout multiple de d est un élément de E.

3) Soit N un élément de E et r le reste de la division euclidienne de N par d.

a) Démontrer que r est un élément de E.

b) En déduire que $r = 0$ et que N est un multiple de d.

4) En déduire que E est l'ensemble des multiples de d, noté $d\mathbf{Z}$.

5) Démontrer que a et b appartiennent à E. En déduire que d divise a et divise b.

6) Démontrer que si d' est un diviseur commun positif de a et b, alors d' divise d.

☞ **Indications exercice 2 :** $d = ax_0 - by_0$.

7) Qu'en déduit-on sur d ?

PGCD et applications

♦ **PGCD.3** Soit $n \in \mathbf{N}$. On pose $a_n = 3n + 1$, $b_n = 4n + 3$ et $d_n = \text{PGCD}(a_n, b_n)$.

1) Démontrer que $d_n \in \{1; 5\}$.

2) Déterminer, en fonction du reste de n modulo 5, la valeur de d_n.

♦ **PGCD.4** (**Classique**)

1) a) En utilisant l'algorithme d'Euclide, démontrer que 43 et 47 sont premiers entre eux.

b) En déduire deux entiers naturels u et v tels que $47u-43v=1$.

2) On considère l'équation diophantienne (E) : $47x-43y=7$ d'inconnue $(x,y)\in\mathbf{Z}^2$.

a) Justifier que (E) possède des solutions (sans en donner explicitement).

b) Déterminer une solution particulière de (E).

c) Résoudre l'équation (E) dans $\mathbf{Z}^2$.

3) On veut déterminer l'ensemble des entiers n tels que :

$$\begin{cases} n\equiv 12 \mod 43 \\ n\equiv 5 \mod 47 \end{cases}$$

On pose $a=12\times 11-5\times 12\times 43$.

a) Montrer que $n\equiv a \mod 43$ et que $n\equiv a \mod 47$.

b) En déduire que $n-a$ est divisible par 43×47.

c) Conclure.

♦ **PGCD.5** Soit (u_n) la suite définie pour tout $n\in\mathbf{N}$ par $u_n=2^n-1$.

1) Montrer que, pour tout $n\in\mathbf{N}$, u_n et u_{n+1} sont premiers entre eux.

2) Soit n et m deux entiers naturels non nuls. On note q et r respectivement le quotient et le reste dans la division euclidienne de n par m.

a) Justifier que $2^m\equiv 1 \mod u_m$ et en déduire que u_m divise u_{qm}.

b) Montrer que

$$u_n=u_{qm}(u_r+1)+u_r.$$

c) En déduire que $\text{PGCD}(u_n,u_m)=\text{PGCD}(u_m,u_r)$.

3) Soit n et m deux entiers naturels non nuls tels que $n\geqslant m$. On pose $d=\text{PGCD}(n,m)$. En utilisant la question précédente, montrer que

$$\text{PGCD}(u_n,u_m)=u_d.$$

4) Montrer que si n et m sont des entiers strictement positifs premiers entre eux alors u_n et u_m sont premiers entre eux.
Que penser de la réciproque ?

♦ **PGCD.6** On considère quatre entiers naturels non nuls a, b, c et d et on pose, pour tout $n\in\mathbf{N}$, $A_n=an+b$, $B_n=cn+d$ et $D_n=\text{PGCD}(A_n,B_n)$.

Partie A

Dans toute cette partie, on considère le cas où $a=5$, $b=3$, $c=4$ et $d=1$.

1) Dans cette question, on s'intéresse aux nombres $A_{100}=503$ et $B_{100}=401$.

a) En utilisant l'algorithme d'Euclide, démontrer que 503 et 401 sont premiers entre eux.

b) Déduire de l'algorithme d'Euclide deux entiers u et v tels que $503u+401v=1$.

2) Dans cette question, n est un entier naturel quelconque.

a) Montrer que $D_n\in\{1;7\}$.

b) Compléter le tableau suivant :

Reste de n modulo 7							
Reste de A_n modulo 7							
Reste de B_n modulo 7							

2) c) En déduire les valeurs de D_n selon le reste de n modulo 7.

d) Retrouver, à l'aide de la question c, le résultat de la question 1.a.

Partie B

Dans cette partie, on suppose que a, b, c et d sont des entiers naturels non nuls quelconques. On pose, de plus, $T=ad-bc$.

1) Démontrer que, pour tout $n\in\mathbf{N}$, D_n divise T.

2) On considère l'implication suivante : « si $T=1$, alors pour tout entier naturel n, A_n et B_n sont premiers entre eux » .

a) Cette implication est-elle vraie ?

b) Énoncer l'implication réciproque. Celle-ci est-elle vraie ?

3) Dans toute cette question, on suppose que $T=2$.

a) Soit $n\in\mathbf{N}$. Quelles sont les valeurs possibles pour D_n ?

b) On suppose que a et pair et que b est impair. Montrer que, pour tout $n\in\mathbf{N}$, A_n et B_n sont premiers entre eux.

c) On suppose que a, b, c et d sont tous pairs. Déterminer, pour tout $n\in\mathbf{N}$, la valeur de D_n.

d) On suppose que b et d sont tous les deux paires et qu'au moins un des deux nombres a ou c est impair. Déterminer, pour tout $n\in\mathbf{N}$, la valeur de D_n en fonction de la parité de n.

4) Dans cette question, on suppose que T est un entier naturel strictement positif quelconque. On va montrer que la suite (D_n) est T-périodique, c'est-à-dire que pour tout $n\in\mathbf{N}$, $D_{n+T}=D_n$.
On rappelle que, d'après la question 1, pour tout $n\in\mathbf{N}$, D_{n+T} divise T.

a) Montrer que pour tout $n\in\mathbf{N}$, D_n divise A_{n+T} et que D_n divise B_{n+T}.

b) Montrer de même que pour tout $n\in\mathbf{N}$, D_{n+T} divise A_n et B_n.

c) Conclure.

♦ **PGCD.7** Dans tout l'exercice, p et q désignent des entiers strictement positifs. On considère la suite (u_n) définie par $u_0 = 0$, $u_1 = 1$ et, pour tout $n \in \mathbf{N}$,

$$u_{n+2} = pu_{n+1} + qu_n.$$

On admet que, pour tout $n \in \mathbf{N}$, $u_n \in \mathbf{N}^*$. On pose, pour tout $n \in \mathbf{N}$, $d_n = \text{PGCD}(u_n, u_{n+1})$.

Partie A - Étude d'un cas particulier

Dans cette question, on suppose que $p = 7$ et $q = 1$.

1) Calculer u_2, u_3 et u_4.

2) Calculer d_0, d_1, d_2 et d_3 (on pourra utiliser la calculatrice).
Quelle conjecture peut-on formuler ?

3) Soit $n \in \mathbf{N}$. Montrer que d_n divise u_{n+2} et en déduire que d_n divise d_{n+1}.

4) Soit $n \in \mathbf{N}$. Montrer de même que d_{n+1} divise d_n.

5) En déduire une démonstration de la conjecture formulée précédemment.

Partie B - Cas général

On se place à présent dans le cas général où on suppose que p et q sont des entiers strictement positifs quelconques.

Pour tout $n \in \mathbf{N}$, on pose $X_n = \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix}$.

1) Déterminer la matrice A carrée d'ordre 2 telle que, pour tout $n \in \mathbf{N}$, $X_{n+1} = AX_n$.
On a donc pour tout $n \in \mathbf{N}$, $X_n = A^n X_0$ et $X_{n+1} = A^n X_1$.

2) En déduire que, pour tout $n \in \mathbf{N}$,

$$A^n = \begin{pmatrix} u_{n+1} & qu_n \\ u_n & qu_{n-1} \end{pmatrix}.$$

3) a) En utilisant les questions précédentes, montrer que, pour tout $(k,m) \in \mathbf{N} \times \mathbf{N}^*$,

$$u_{k+m} = u_m u_{k+1} + qu_{m-1}u_k.$$

b) Soit $m \in \mathbf{N}^*$. Démontrer par récurrence que, pour tout $n \in \mathbf{N}$, u_m divise u_{nm}.

4) On suppose à présent que p et q sont premiers entre eux. On considère deux entiers a et b strictement positifs. On note $\delta = \text{PGCD}(a,b)$ et $D = \text{PGCD}(u_a, u_b)$.

a) Soit u et v deux entiers premiers entre eux. Montrer que tout diviseur w de v est premier avec u.

b) Déduire de la question 3.b que u_δ divise D.

c) Montrer par récurrence que, pour tout $n \in \mathbf{N}$, u_n est premiers avec q.

d) Montrer par récurrence que, pour tout $n \in \mathbf{N}$, $d_n = 1$.

e) Justifier l'existence de deux entiers naturels r et s de signes contraires tels que $ra + sb = \delta$. Quitte à échanger a et b, on peut toujours supposer que $r \geqslant 0$ et $s \leqslant 0$. On pose alors $t = -s$ de sorte que $t \in \mathbf{N}$.

f) Justifier que $A^{ra} = A^\delta A^{tb}$ et en déduire que

$$u_{ra} = u_\delta u_{tb+1} + qu_{\delta-1}u_{tb}.$$

g) En utilisant aussi les questions 3.b et 4.d, en déduire que D divise u_δ puis conclure que $D = u_\delta$.

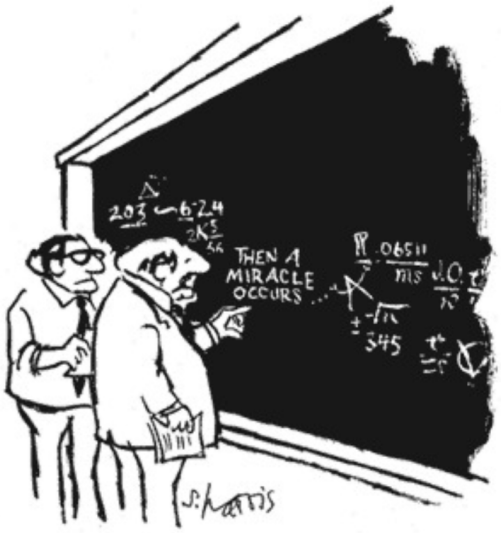
5) (*) Réciproquement, montrer que si, pour tous entiers a et b strictement positifs, $\text{PGCD}(u_a, u_b) = u_{\text{PGCD}(a,b)}$ alors p et q sont premiers entre eux.

♦ **PGCD.8** Soit un entier $n \geqslant 7$.

1) On suppose que n est impair. Démontrer qu'il existe deux entiers $a \geqslant 2$ et $b \geqslant 2$ premiers entre eux tels que $n = a + b$.

2) Montrer que le résultat précédent est également vrai si n est pair.

☞ **Indications exercice 8 :** On pourra raisonner selon le reste de n modulo 4.



"I THINK YOU SHOULD BE MORE EXPLICIT HERE IN STEP TWO."

Codages

♦ PGCD.9 — Chiffrement affine

Partie A - Méthode classique à connaître

On considère l'équation (E) : $11x - 26y = 1$ où x et y sont des entiers.

1) Justifier que cette équation admet des solutions entières.

2) Montrer que $(-7;-3)$ est une solution particulière de (E).

3) Démontrer que (x,y) est solution de (E) si et seulement si :

$$11(x+7) = 26(y+3).$$

4) En déduire que 26 divise $x+7$.

5) En déduire toutes les solutions de l'équation.

Partie B - Le chiffrement affine

On assimile chaque lettre de l'alphabet à un nombre entier x, 0 pour A, 1 pour B, etc... et 25 pour Z. On code ce nombre entier x de la façon suivante :

- on calcule $11x+8$,
- on calcule le reste y de la division de $11x+8$ par 26, la lettre correspondant à y remplace alors la lettre correspondant à x dans le message codé.

1) Montrer que la lettre L est codée par Z.

2) Rechercher la fonction de la commande "ord()" en Python, ainsi que la commande "chr()".

3) Pour le coder, on doit d'abord transformer le mot donné en une suite de nombres représentant ce mot.

Pour cela, compléter le programme Python ci-contre, qui stocke dans une liste L la suite des nombres codant un mot :

```
def rang(mot):
    L=[]
    for lettre in .....:
        L.append(ord(lettre)-.....)
    return L
```

4) On souhaite maintenant coder une fonction "code" qui renvoie le mot codé :

Pour cela, compléter le programme Python ci-contre, qui fonctionne en deux étapes : on calcule les nouveaux nombres du mot codé, puis on le convertit en lettres :

```
def code(mot):
    L=rang(mot)
    M=[]
    N=""
    for k in range(len(mot)):
        M.append((.....)%26)
    for k in range(len(M)):
        N=N+chr(....)
    return N
```

5) Coder le message VIVELESMATHS (attention, il faut mettre le message entre guillemets pour que Python le considère comme une chaîne de caractère).

Partie C - Le décodage

1) Montrer que pour tout entier j :

$$11x \equiv j \pmod{26} \quad \Leftrightarrow \quad x \equiv 19j \pmod{26}$$

2) En déduire un procédé de décodage ; décoder la lettre W.

3) Décoder le message WIUYYAYJJNAYUJSZA.

4) Créer un message secret à faire décoder à votre voisin !

Partie D - Décodage dans le cas où on connait la clé (m,p)

Dans les parties précédentes, on a considéré le codage $11x+8$, de la forme $mx+p$. On peut se demander pour quelles valeurs de m et p le décodage est possible.

1) Justifier que $mx+p \equiv y \pmod{26}$ si et seulement si $mx \equiv y-p \pmod{26}$.

2) Si m est premier avec 26, justifier qu'il existe des entiers u et v tels que $mu+26v=1$.

3) En déduire qu'on peut décoder le message, connaissant m et p, si m est premier avec 26.

4) Si $m=7$ et $p=23$, décoder le mot $XYYMZKSMZ$.

5) Choisir une clé de codage, et transmettre un message codé à votre voisin, avec la clé de codage choisie, et laissez-le décoder votre message.

♦ PGCD.10 — Cassage d'un chiffrement affine

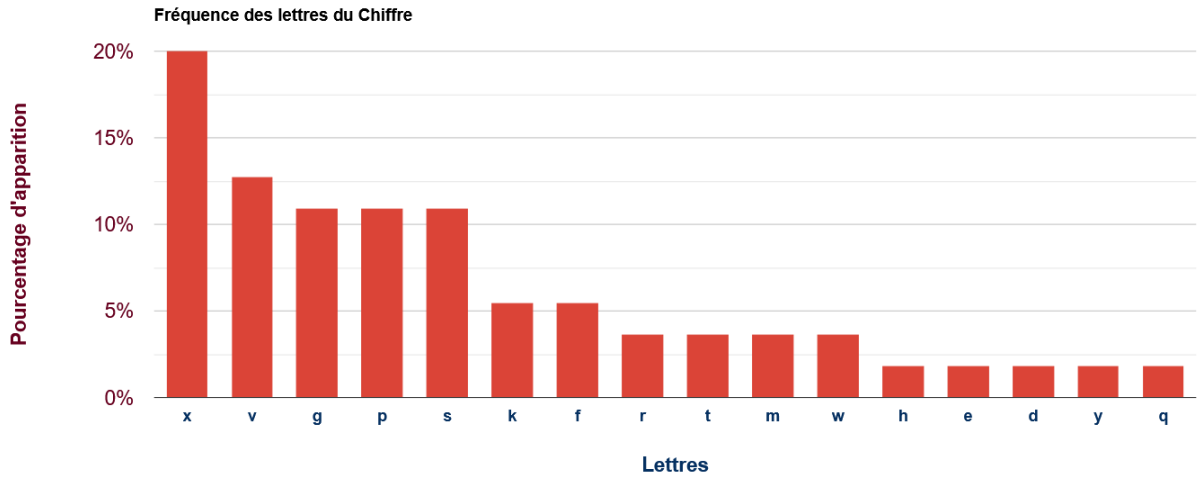
On suppose qu'on a reçu le texte codé suivant :

WXVXGKXVERHFPSVSFPVVXSGWPQKXVXGXTFRYXSMPTSPGXXGXSMKDPGV

On sait qu'il est codé par un codage affine, mais on ne connait pas la clé. Comment décoder le message ?
Selon la langue, un texte comporte une répartition particulière des fréquences de lettres. Cette fréquence dépend du type de texte, d'écriture, et de nombreux autres paramètres. Dans un texte en français, la lettre la plus fréquente est en général le E, le S ou le A.

1) a) Quelle lettre semble être la plus fréquente dans le message ?

b) On obtient la répartition suivante des fréquences de lettres dans ce message :



Quelles sont les deux lettres les plus fréquentes dans ce message codé ? Quels sont leurs chiffres correspondants si on chiffre les lettres de façon usuelle (0 pour A, 25 pour Z) ?

2) Soit (m,p) la clé du codage affine. Supposons que les deux lettres correspondent à E codé 4 et S codé 18. On a alors l'un des deux systèmes suivants :

$$(S) : \begin{cases} 4m+p \equiv 23 \pmod{26} \\ 18m+p \equiv 21 \pmod{26} \end{cases} \qquad (S') : \begin{cases} 4m+p \equiv 21 \pmod{26} \\ 18m+p \equiv 23 \pmod{26} \end{cases}$$

a) Montrer que $(S) \Rightarrow 14m \equiv -2 \pmod{26}$.

b) Déterminer u et v tels que $14u-26v=-2$ et en déduire une valeur de m (inversible modulo 26 !) puis une valeur de p qui soit solution du système (S).

c) Décoder dans ce cas les 4 premières lettres du message (on pourra réutiliser le programme de l'exercice 1 avec la clé de décodage à déterminer).

d) Montrer que $(S') \Rightarrow 14m \equiv 2 \pmod{26}$. En déduire une valeur de m (inversible modulo 26 !) et p qui soit solution du système (S') et décoder les quatre premières lettres du message.

3) Quelle hypothèse retient-on ? Décoder la fin du message.

♦ PGCD.11 — Clé du RIB

Un numéro de compte bancaire est un nombre de 23 chiffres qui se décompose en plusieurs parties :

Exemple de RIB :

Code Banque	Code Guichet	N° de compte	Clé RIB
17515	90000	04243246509	87

Soit $R = \underbrace{r_1 \ldots r_5}_{B} \quad \underbrace{r_6 \ldots r_{10}}_{G} \quad \underbrace{r_{11} \ldots r_{21}}_{C} \quad \underbrace{r_{22} r_{23}}_{K}$.

La clé K du RIB est constituée de deux chiffres et est comprise entre 01 et 97. Elle est choisie de telle sorte que R soit divisible par 97. Comment la calculer sachant que ce nombre R à 23 chiffres est bien trop grand pour être entré sur une calculatrice et quelles erreurs permet-elle de détecter ?

1) a) Décomposer R à l'aide de B, G, C, K et de puissances de 10.

b) Montrer que $K \equiv 97 - 89B - 15G - 3C \pmod{97}$ et justifier l'unicité de la clé pour un compte donné.

c) Vérifier la clé de l'exemple donné ci-dessus.

2) On suppose qu'une erreur de saisie a lieu sur un des chiffres, et un seul, donnant un numéro R' différent de R. On suppose que $R' > R$.

a) Justifier que $R' - R = m \times 10^n$ où m et , sont des entiers relatifs tels que $1 \leqslant m \leqslant 9$ et $0 \leqslant n \leqslant 22$.

b) Montrer que la clé permet détecter toute erreur sur un seul chiffre.

c) La clé permet-elle de détecter certaines erreurs de saisie portant sur plus d'un chiffre ?