Chapitre 8&9 PGCD, Théorèmes de Bézout et de Gauss, nombres premiers

I - PGCD de deux entiers relatifs

Exemple : les diviseurs dans $\mathbb{Z}$ de l'entier 6, est l'ensemble, noté $\mathcal{D}(6)$, avec : $\mathcal{D}(6)$ =

Les diviseurs dans $\mathbb{Z}$ de l'entier 15 est l'ensemble noté $\mathcal{D}(15)$, avec $\mathcal{D}(15)$ =

Quels sont les diviseurs communs à 6 et 15 ?

Quel est le plus grand des diviseurs communs à 6 et 15 ?

Propriété et définition

Soit a et b deux entiers relatifs non tous les deux nuls (*i.e.* $(a\ ;\ b) \neq (0\ ;0)$).

L'ensemble des diviseurs communs à a et b admet un plus grand élément qu'on appelle le Plus Grand Commun Diviseur de a et b, et que l'on note $\boldsymbol{PGCD(a\ ;\ b)}$ ou encore $\boldsymbol{a \wedge b}$: $\boldsymbol{PGCD(a\ ;\ b)} \in \mathbb{N}$

Preuve : Soit $\mathcal{D}^+(a)$ l'ensemble formé par les entiers naturels qui divisent l'entier a, et $\mathcal{D}^+(b)$ l'ensemble formé par les entiers naturels qui divisent b.

$\mathcal{D}^+(a)$ est un ensemble non vide (car il contient l'élément 1), $\mathcal{D}^+(a)$ est un ensemble inclus dans $\mathbb{N}$, et $\mathcal{D}^+(a)$ est un ensemble fini vu qu'un entier non nul admet un nombre fini de diviseurs. De même pour $\mathcal{D}^+(b)$.

Enfin l'ensemble $\mathcal{D}^+(a) \cap \mathcal{D}^+(b)$ est non vide (contient 1), inclus dans $\mathbb{N}$ et est lui aussi fini car contenu dans deux ensembles finis. En se souvenant que toute partie non vide et finie de $\mathbb{N}$ admet un plus grand élément, il existe donc un unique élément d appartenant à $\mathcal{D}^+(a) \cap \mathcal{D}^+(b)$: d est donc le diviseur commun à a et b le plus grand possible : c'est le plus grand commun diviseur de a et b.

✂----------

Exemples

PGCD(30 ; 42) = ; PGCD(25 ; 12) =

Remarque : $\boldsymbol{PGCD\ (a\ ;\ b) = PGCD(b\ ;\ a) = PGCD\ (|a|\ ;\ |b|)}$.

On peut donc toujours se ramener au cas où a et b sont des entiers naturels.

$\boldsymbol{PGCD\ (1\ ;\ a)}$ = ….. et si $a \neq 0$, $\boldsymbol{PGCD\ (0\ ;\ a)}$ = …….

La calculatrice permet de calculer "*bestialement*" le *PGCD* de deux entiers non nuls : par exemple, pour déterminer PGCD(1544 ; 266) on tape sur *TI* : touche *math* puis flèche à droite une fois : *NBRE* puis 9 : *pgcd*(1544 ; 266).

Définition

Deux entiers relatifs a et b sont dits ♥***PREMIERS ENTRE-EUX*** si et seulement si $\boldsymbol{PGCD\ (a\ ;\ b) = 1}$. ♥

Exemple : On a vu plus haut que $PGCD(25\ ;\ 12) = 1$, donc les entiers 25 et 12 sont premiers entre eux.

***Propriété des diviseurs communs à deux entiers relatifs*.**

Soient a et b deux entiers relatifs, on note $\mathcal{D}(a\ ;\ b)$ l'ensemble des diviseurs communs à a et b.

On a : $(i)\ \forall k \in \mathbb{Z}$, $\mathcal{D}(a\ ;\ b) = \mathcal{D}(a - kb\ ;\ b)$.

En particulier, $\mathcal{D}(a\ ;\ b) = \mathcal{D}(a - b\ ;\ b)$.

La notation $\mathcal{D}(a\ ;\ b)$ *n'est autre qu'une simplification de l'écriture* $\mathcal{D}(a) \cap \mathcal{D}(b)$.

Preuve : Procéder par double inclusion et similaire à déjà vu au chapitre 1 d'arithmétique.

✂----------

Exemple : Déterminer $\mathcal{D}(2025\ ;\ 2028)$

Propriétés du PGCD de deux entiers

Soient a et b deux entiers relatifs non tous les deux nuls,

$(i)\ \forall k \in \mathbb{Z}$, $PGCD(a\ ;\ b) = PGCD(a - kb\ ;\ b)$ *; en particulier,* $PGCD(a\ ;\ b) = PGCD(a - b\ ;\ b)$.

(ii) *Si* $0 < b \leq a$, *alors* ♥ $PGCD(a\ ;\ b) = PGCD(b\ ;\ r)$ ♥, *où r est le reste dans la division euclidienne de a par b.*

(iii) *Si b est un diviseur positif de a, alors* $PGCD(a\ ;\ b) =$ …….

Preuve : Là encore, cela repose sur la propriété précédente.

✂----------

Exercice 1

1) Montrer que deux entiers consécutifs sont premiers entre eux.

2) Démontrer que si un entier naturel n est congru à 1 modulo 7, alors $PGCD(3n + 4\ ;\ 4n+3) = 7$.

✂----------

II –L'algorithme d'Euclide

***Propriété* : L'algorithme d'Euclide** (*pratique pour calculer rapidement le PGCD de deux entiers*)

Soient a et b deux entiers naturels non nuls tels que : $a \geq b$.

- ***Si b divise a, alors PGCD(a ; b) = b.***
- ***Si b ne divise pas a*** :

  On effectue la division euclidienne de a par b : il existe des entiers q_1 *et* r_1 *tels que :* $a = bq_1 + r_1$ *avec :* $0 \leq r_1 < b$.

  Si $r_1 = 0$, *alors* $PGCD(a\ ;\ b) =$ ….. *car* ……

  Si $r_1 \neq 0$, *alors* $PGCD(a\ ;\ b) = PGCD(b\ ;\ r_1)$, *et on effectue la division euclidienne de b par* r_1.

  Il existe des entiers q_2 *et* r_2 *tels que :* $b = r_1q_2 + r_2$ *avec :* $0 \leq r_2 < r_1$.

  Si $r_2 = 0$, *alors* $PGCD(a\ ;\ b) = PGCD(b\ ;\ r_1) =$ ….. *car* ……

  Si $r_2 \neq 0$, *alors* $PGCD(b\ ;\ r_1) = PGCD(r_1\ ;\ r_2)$, *et on effectue la division euclidienne de* r_1 *par* r_2.

  Il existe des entiers q_3 *et* r_3 *tels que :* $r_1 = r_2q_3 + r_3$ *avec :* $0 \leq r_3 < r_2$.

Cette succession de divisions euclidiennes permet ainsi de déterminer une suite de restes $r_1, r_2, \ldots\ldots r_n$ *avec :* $0<r_n<\ldots\ldots<r_2<r_1$. *Cette suite de restes est une suite d'entiers naturels strictement décroissante : à ce titre il va exister un reste qui sera nul.*

Notons r_n ***le dernier reste non nul.*** *On :* $PGCD(a\,;b) = PGCD(b\,;r_1)=PGCD(r_1\,;r_2) = \ldots\ldots=PGCD(r_n\,;0) = r_n$.

Ainsi, on retiendra que :

♥♥***Lorsque b divise a, PGCD(a ; b)=…..*** ♥♥

♥♥***Lorsque b ne divise pas a****, PGCD(a ; b) est le*……

……♥♥

Exemple

Déterminer *PGCD*(135 ; 72) à l'aide de l'algorithme *d'Euclide*.

Propriétés

Soient *a* et *b* deux entiers non nuls.

1) Tout diviseur commun à *a* et *b* divise *PGCD* (*a* ; *b*).

2) Pour tout entier naturel ***k non nul, PGCD(ka ; kb) = k×PGCD(a; b).*** Cette propriété est appelée ***l'homogénéité*** du *PGCD*.

Preuve : A lire.

1) *Avec les notations de la démonstration de l'algorithme d'Euclide, on a, en notant D(k) l'ensemble des diviseurs de l'entier k :*

$D(a)\cap D(b)=D(b)\cap D(r_1)=D(r_1)\cap D(r_2)=\ldots\ldots=D(r_n)\cap D(0)=D(r_n)$. Or $r_n = PGCD(a\,;b)$, donc si *d* est un diviseur commun à *a* et *b*, c'est-à-dire si $d\in D(a)\cap D(b)$, alors $d\in D(r_n)$, donc *d* divise *PGCD*(*a* ; *b*).

2) *Soit* $d=PGCD(a; b)$ *et* $d'=PGCD(ka; kb)$.

Vu que d divise a et b, l'entier kd divise les entiers ka et kb : [*en effet, il existe* $\lambda\in\mathbb{Z}$ *tel que* $a=\lambda d$, *donc* $ka = \lambda kd$ *donc kd divise ka car* λ *est entier, et même raisonnement pour kd divise kb*].

Par suite, kd est un diviseur commun aux entiers ka et kb, donc d'après le point 1) *de cette propriété, kd divise PGCD*(*ka ; kb*), *à savoir kd divise d'*.

Ainsi, il existe un entier ω *tel que :* $d'=\omega kd$.

De plus, d' divise ka et kb, donc $\omega kd(=d')$ *est un diviseur commun de ka et kb : donc* ωd *divise a et b* [*en effet, il existe* $\tau\in\mathbb{Z}$ *tel que* $ka =\tau wkd$, *donc comme* $k\neq 0$, $a=\tau wd$, *donc* ωd *divise a et même raisonnement pour b*], *donc* ωd *divise le PGCD*(*a* ; *b*) *c'est-à-dire* ωd *divise d*.

Par suite $w=1$, *et donc,* $d'=kd$ *c'est-à-dire :* $PGCD(ka\,;kb)=kPGCD(a\,;b)$.

Exemple

PGCD(1500 ; 2500) =

***Propriété caractéristique du PGCD* (*utile en pratique*)**

Soient a et b deux entiers relatifs non tous les deux nuls et d un entier naturel.

♥♥ $d = PGCD(a\,;\,b) \Leftrightarrow \exists (a'\,;\,b') \in \mathbb{Z}^2$ tels que : $PGCD(a'\,;\,b') = 1$ et $\begin{cases} a = da' \\ b = db' \end{cases}$ ♥♥ .

Preuve : *Supposons que $d = PGCD(a\,;\,b)$. Alors, $d \mid a$ et $d \mid b$, donc il existe des entiers relatifs a' et b' tels que : $a=da'$ et $b=db'$.*

De plus, $d=PGCD(a\,;\,b)=PGCD(da'\,;\,db')=d\times PGCD(a'\,;\,b')$ par propriété *d'homogénéité* du *PGCD*.

Vu que a et b sont non tous les deux nuls, $d \neq 0$, de sorte que l'égalité : $d = d\times PGCD(a'\,;\,b')$ *implique, après simplification par d, que* $PGCD(a'\,;\,b')=1$.

Réciproquement, on suppose qu'il existe des entiers relatifs a' et b' tels que : $PGCD(a'\,;\,b') = 1$ et $\begin{cases} a = da' \\ b = db' \end{cases}$.

Alors, $PGCD(a\,;\,b) = PCGD(da'\,;\,db') = d\times PGCD(a'\,;\,b')$ *par propriété d'homogénéité* du *PGCD*,

$PGCD(a\,;\,b)=d\times 1=d$ ce qui termine la démonstration.

Application :

Expliquer le résultat suivant bien connu des collégiens : pour rendre une fraction $\frac{a}{b}$ irréductible, il suffit de diviser a et b par $PGCD(a\,;\,b)$.

III- Théorèmes célèbres de l'arithmétique

A-Théorème de Bézout

***Propriété* (*appelée l'identité de Bézout*)**

Soient a et b deux entiers relatifs non tous les deux nuls, et $d = PGCD(a\,;\,b)$.

Il existe des entiers relatifs u et v tels que : $au + bv = d$: c'est l'identité de Bézout.

Cette identité de Bézout dit que le PGCD de deux entiers non tous les deux nuls est une combinaison linéaire de ces deux entiers.

Preuve : Les notations utilisées sont celles de la démonstration de l'algorithme d'Euclide.

♣ *L'idée est de fabriquer les entiers u et v, à partir des étapes de l'algorithme d'Euclide.*

De $a = bq_1 + r_1$, *on déduit que :* $r_1=a-bq_1$ *qui est bien de la forme* au_1+bv_1 *avec :* $u_1=1$ *et* $v_1=-q_1$.

(u_1 et v_1 sont bien des entiers).

De la relation : $b=r_1q_2 + r_2$, on déduit que : $r_2=b-r_1q_2=b-(au_1+bv_1)q_2$ qui est bien de la forme : au_2+bv_2 avec : $u_2=-u_1q_2$ *et* $v_2=1-v_1q_2$. (u_2 *et* v_2 *sont bien des entiers en tant que combinaisons linéaires d'entiers*).

On exprime donc, de proche en proche, chaque reste r_k comme une combinaison linéaire à coefficients entiers des entiers a et b.*

Comme l'algorithme d'Euclide se termine en un nombre fini d'étapes, et que le dernier reste non nul r_n est PGCD(a ; b), il en résulte que le PGCD(a ; b) s'écrit comme une combinaison linéaire à coefficients entiers des entiers a et b ce qui termine la démonstration.

**Dans l'absolu, il faudrait faire une récurrence (dite forte) si l'on veut être parfaitement rigoureux. Sera vu à bac +1.*

Remarques :

La réciproque de l'identité de Bézout est fausse ! *Pour contre-exemple on peut prendre : ……*

……..

Il n'y a pas unicité du couple (u ; v) dans l'identité de Bézout.

Par exemple, avec $a = 15$ et $b = 18$ on a $d = …$, et : $…\times 15 + …\times 18 = 3$, donc $(u ; v) = (… ; …)$ convient, mais on a aussi : $…\times 15 + (…)\times 18 = 3$, donc $(u ; v) = (… ; …)$ convient aussi !

Comment déterminer en pratique un couple d'entiers relatifs (u ; v) tel que au + bv = PGCD(a ; b) ?

Méthode* : *En "remontant" les étapes écrites dans l'algorithme d'Euclide.

Exemples : *a)* Déterminer $PGCD(135 ; 245)$, puis trouver un couple d'entiers relatifs $(u ; v)$ tel que $135u + 245v = PGCD(135 ; 245)$.

b) Expliquer pourquoi l'équation : $201x + 1002y = 3$, d'inconnues x et y, admet au moins un couple de solutions entières, et déterminer un tel couple.

✂----------

***Théorème de Bézout* (*fondamental pour les exercices*).**

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

Preuve :

✂----------

Exemples

1) Démontrer que 95 et 51 sont premiers entre eux, puis déterminer deux entiers relatifs u et v tels que : $95u + 51v = 1$.

2) Retrouver, à l'aide du théorème de *Bézout*, un résultat déjà établi : deux entiers consécutifs sont premiers entre eux.

Propriété

Soit a, b et c des entiers donnés.

L'équation (#) : ax + by = c d'inconnues (x ; y) $\in \mathbb{Z}^2$ ***admet des solutions entières si et seulement si PGCD(a ; b) divise c.***

Pourquoi ?

✂----------

1) Résoudre dans $\mathbb{Z}^2$ l'équation : $3x + 6y = 13$.

2) Dans le plan muni d'un repère, démontrer que la droite d'équation $2x + 11y - 151 = 0$ passe par au moins un point à coordonnées entières. Déterminer les coordonnées d'un tel point.

✂----------

B- Le théorème de Gauss

♥♥***Théorème de Gauss***♥♥

Soit a, b et c des entiers relatifs non nuls.

Si a | bc, et si a et b sont premiers entre eux, alors a |c.

Preuve :

✂----------

Exemple :

Remarques : Attention, il y a deux conditions à vérifier avant de pouvoir appliquer ce théorème !

💣💣Si $a \mid bc$, il est faux de dire que $a \mid b$ ou que $a \mid c$. 💣💣

Contre-exemple : $a = 8$; $b = 4$ et $c = 18$: on a $bc = 72$, donc $8 \mid 72$, pour autant, 8 ne divise ni 4 ni 18 !

Exemples d'utilisation du théorème de Gauss **:**

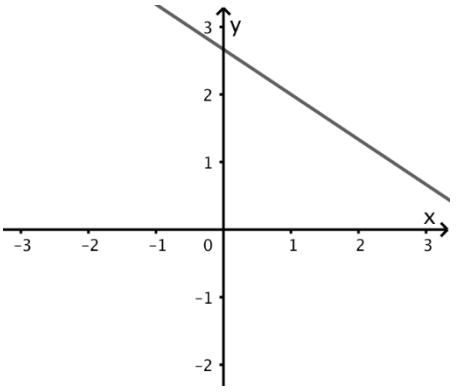
Application importante **: *Equations diophantiennes***

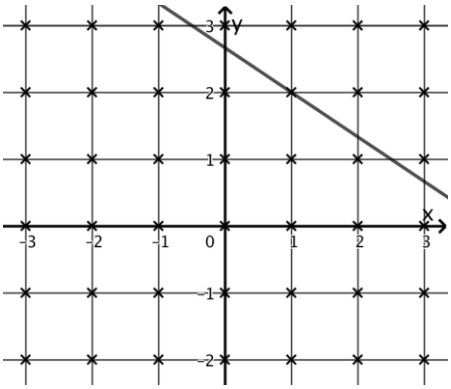
Toute équation de la forme : $ax + by = c$, où *a, b* et *c* sont trois entiers relatifs fixés et où les inconnues *x* et *y* sont aussi deux entiers relatifs est appelée équation diophantienne.

Motivation :

L'équation $ax + by = c$ peut être vue comme l'équation cartésienne d'une droite (dont un vecteur directeur est $\vec{u}\begin{pmatrix}-b\\a\end{pmatrix}$) dans un repère du plan. Tous les points de cette droite ont pour coordonnées un couple de nombres solution de cette équation, mais ici, nous ne cherchons que les couples de nombres entiers solution de cette équation.

Ci-contre est tracée la droite d'équation cartésienne : $2x + 3y = 8$.





Les couples de nombres entiers relatifs $(x\ ;\ y)$ peuvent être représentés dans un repère comme l'ensemble des points à coordonnées entières, c'est à dire les nœuds du quadrillage donné dans exemple ci-contre.

Résoudre dans $\mathbb{Z}^2$ l'équation diophantienne $2x + 3y = 8$ revient donc à déterminer les coordonnées des points situés sur cette droite et sur un nœud du quadrillage.

Rappelons la propriété vue en début de page 6 :

Soit a, b et c des entiers donnés.

L'équation (#) : ax + by = c d'inconnues (x ; y) $\in \mathbb{Z}^2$ ***admet des solutions entières si et seulement si PGCD(a ; b) divise c.***

On a donc une condition nécessaire et suffisante à ce que **(#)** ***ait un ensemble de solution non vide dans*** $\mathbb{Z}^2$. Voyons en pratique comment trouver l'ensemble de solution de cette équation.

Exercice 2 (*issu de texte de baccalauréat*).

On considère l'équation (E) : $7x - 6y = 1$ où x et y sont des entiers relatifs.

a) Trouver une solution particulière de (E).

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

✂----------

Remarque : bien avoir à l'esprit que dès lors qu'on connaît une solution d'une équation diophantienne linéaire d'ordre 2, c'est le théorème de Gauss qui permet de déterminer l'expression générale de toutes les solutions de cette dernière.

Exercice 3

1) Déterminer tous les couples d'entiers relatifs $(x\ ;\ y)$ solutions de l'équation : $7x = 3y$.

2) Déterminer tous les couples d'entiers relatifs $(a\ ;\ b)$ tels que : $15a + 19b = 7$.

En déduire tous les couples $(a\ ;\ b)$ solution de cette équation avec : $0 < a < 100$, et $-30 < b < 20$.

✂----------

♥♥***Corollaire du théorème de Gauss***

Soit a, b et c des entiers relatifs non nuls.

♥♥***Si b et c divisent a ET si b et c sont premiers entre eux, alors bc divise a.*** ♥♥

Preuve :

✂----------

💣💣Attention, là encore, nécessité absolue d'avoir b et c premiers entre eux !

Par exemple, $6 \mid 12$ et $4 \mid 12$, pour autant, $6 \times 4 = 24$ et 24 ne divise pas 12 !

Exercice 5

1) p est entier naturel non nul, n est un entier relatif non nul, et a et b sont des entiers relatifs.

Montrer que si $na \equiv nb\ [p]$ et si $n \wedge p = 1$, alors $a \equiv b\ [p]$.

2) Résoudre l'équation suivante : $2x \equiv 6\ [13]$.

✂----------

Exercice 6

Montrer que le système de congruences suivant (inconnue $x \in \mathbb{Z}$) admet des solutions, et les déterminer toutes : $\begin{cases} x \equiv 3\ (12) \\ x \equiv 4\ (5) \end{cases}$.

✂----------

Chapitre 9 *Les nombres premiers*

I – Généralités et propriétés élémentaires

Définition

Un entier naturel est un nombre premier si et seulement s'il admet, dans $\mathbb{N}$, ***exactement deux diviseurs distincts*** : …….

Exemples

2 est un nombre premier car les seuls diviseurs positifs de 2 sont : 1 et 2.

De même, 3 ; 5 ; 7 ; 11 sont quelques exemples de nombres premiers.

Le nombre 0 n'est pas premier. Pourquoi ?

Le nombre 1 est-il un nombre premier ?

Un entier pair est-il un nombre premier ?

Que peut-on dire de deux nombres premiers distincts ?

Remarques

2 est le seul nombre premier pair.

Un nombre premier supérieur ou égal à 3 est donc nécessairement impair.

On note $\mathbb{P}$ l'ensemble formé par les nombres premiers.

Un entier supérieur ou égal à 2 qui n'est pas premier est dit composé.

Mini propriété fort utile

Soit p un nombre premier et n un entier naturel.

On a l'alternative suivante : ou bien p divise n, ou bien p et n sont premiers entre eux.

Preuve :

✂----------

Théorème

1) ***Tout entier naturel $N \geq 2$ admet au moins un diviseur premier.***

2) ***Si $N \geq 2$ est NON PREMIER, alors N admet au moins un diviseur premier p tel que $p \leq \sqrt{N}$.***

Preuve : (admis, donner l'idée).

✂----------

Attention, un tel entier N peut admettre un diviseur premier strictement supérieurs à $\sqrt{N}$.

Par exemple pour $N = 22$: les diviseurs premiers de 22 sont 2 et 11.

11 est un nombre premier et $11 > \sqrt{22}$.

Test de primalité

Soit n un entier naturel supérieur ou égal à 2.

Si n n'est divisible par aucun des nombres premiers inférieurs ou égaux à $\sqrt{n}$, alors n est un nombre premier.

Pourquoi ? Ecrire la contraposée du point 2) du théorème précédent :

En fait la réciproque est aussi vraie (mais ne dit rien de transcendant : si un nombre est premier, alors il n'est divisible par aucun nombre premier inférieur ou égaux à $\sqrt{n}$).

En effet $n \geqslant 2$, donc $n > 1$, donc par stricte croissance de la fonction racine sur $[0\ ;\ +\infty[$, $\sqrt{n} > \sqrt{1}$, donc en multipliant les deux membres de la précédente inégalité par $\sqrt{n} > 0$, on a : $n > \sqrt{n}$, et vu que n est premier, son seul diviseur autre que n est 1, et 1 n'est pas un nombre premier.

Remarque : ce test de primalité fournit un critère d'arrêt dans la recherche des diviseurs premiers d'un entier naturel donné.

Application* : *le crible* d'*Erathostène

Dresser la liste L des nombres premiers inférieurs à 100.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

$L =$

***Exercice* 1**

Le nombre 4561 est-il un nombre premier ?

Théorème

Il existe une infinité de nombres premiers.

Preuve : IMPORTANTE.

✂----------

On va s'intéresser à la répartition des nombres premiers.

A titre culturel, pour tout entier naturel $n > 1$, il existe au moins un nombre premier appartenant à l'intervalle $]n\ ;2n[$.

Ce résultat, dont la démonstration est difficile, est connu sous le nom de *Postulat de Bertrand*.

Exercice 2

a) Fabriquer un intervalle de longueur respective : 2 puis 3 puis 4 puis 5 puis 6 ne contenant aucun nombre premier.

b) Démontrer qu'on peut fabriquer un intervalle de longueur arbitraire, ne contenant aucun nombre premier.

c) Qu'en déduit-on quant à la répartition des nombres premiers ?

✂----------

Exercice 3

Soit p un nombre premier et a et b deux entiers. On suppose que p divise ab.

Démontrer que p divise a ou p divise b.

Ce résultat reste-t-il vrai si on ne suppose plus que p est un nombre premier ?

✂----------

II – Applications

Théorème fondamental de l'arithmétique

Tout entier naturel n supérieur ou égal à 2 est décomposable en un produit de nombres premiers.

Cette décomposition est unique à l'ordre des facteurs près.

On peut donc toujours écrire n sous la forme : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots\ldots p_k^{\alpha_k}$ où $p_1, p_2, \ldots\ldots\ldots p_k$ ***sont des nombres premiers deux à deux distincts et*** $\alpha_1, \alpha_2, \ldots\ldots \alpha_k$ ***sont des entiers naturels non nuls.***

Avec les notations ci-dessus : $n = \prod_{j=1}^{k} p_j^{\alpha_j}$

Preuve : A lire à titre culturel. Nous allons procéder en deux temps : d'abord l'existence, ensuite l'unicité.

Existence : Soit $n \geq 2$. Si n est premier, alors $n = n^1$ et c'est terminé.

Si n n'est pas premier, comme $n \geq 2$, alors n admet au moins un diviseur premier. Notons p_1 le plus petit diviseur premier de n : il existe donc un entier $n_1 \geq 1$ tel que $n = p_1 \times n_1$.

Observons que $n_1 < n$ car $p_1 > 1$!

Si n_1 *est premier, alors c'est terminé, n est égal au produit de deux facteurs premiers.*

Sinon, on recommence le processus, appliqué cette fois-ci à n_1.

Notons p_2 *le plus petit diviseur premier de* n_1 *: il existe donc un entier* $n_2 \geq 1$ *tel que :* $n_1 = p_2 \times n_2$.

On a : $n_2 < n_1$ *car* $p_2 > 1$.

En réitérant le procédé autant de fois que nécessaire, on fabrique donc une suite (n_k) *d'entiers naturels qui est strictement décroissante par construction et minorée par* 1.

D'après le principe de la descente infinie de Fermat, cette suite est nécessairement finie.

Il existe donc un rang m tel que $n_m = 1$ *et donc,* $n = p_1 \times p_2 \times \ldots\ldots \times p_m$ *avec les nombres premiers* p_1, p_2……, p_m *non nécessairement distincts.*

En regroupant les facteurs premiers égaux entre eux, on obtient : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots\ldots p_k^{\alpha_k}$.

Unicité : *On procède par récurrence dite forte sur l'entier n.*

L'unicité de la décomposition est claire pour $n = 2$.
On suppose que la décomposition est unique pour tout entier inférieur strictement à un n donné et on montre que la décomposition de n en produit de facteurs premiers est unique.
On suppose que n admette deux décompositions distinctes en produit de facteurs premiers :

$$n = p_1 \times p_2 \times \ldots \times p_r = q_1 \times q_2 \times \ldots \times q_s$$

Si p_1 était premier avec q_i pour tout $1 \leqslant i \leqslant s$, alors d'après un corollaire du théorème de Gauss, p_1 serait premier avec $q_1 \times q_2 \times \ldots \times q_s$; or p_1 divise $q_1 \times q_2 \times \ldots \times q_s$ d'où une contradiction.
Donc il existe i tel que p_1 et q_i ne sont pas premiers entre eux. Comme ce sont des nombres premiers, on a nécessairement $p_1 = q_i$.
Le nombre $n_1 = \dfrac{n}{p_1}$ admettrait donc deux décompositions distinctes :

$$n_1 = p_2 \times p_3 \times \ldots \times p_r = q_1 \times q_2 \times \ldots \times q_{i-1} \times q_{i+1} \times \ldots \times q_s$$

ce qui contredit l'hypothèse de récurrence car $n_1 < n$ (car $p_2 \geqslant 2$). On en déduit que n admet une décomposition unique.
On a ainsi démontré par récurrence l'unicité de la décomposition pour tout $n \geqslant 2$. ■

Exemple

Donner la décomposition en produit de facteurs premiers de : 140 ; 1001.

✂----------

Nombre de diviseurs d'un entier naturel non nul

Un exemple : Déterminer la liste de tous les diviseurs entiers naturels du nombre 180.

Comment ne pas en oublier ?

✂----------

Propriété

Soit n un entier naturel supérieur ou égal à 2.

La décomposition en produit de facteurs premiers de n est : n = $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots\ldots p_k^{\alpha_k}$ ***où*** $p_1, p_2, \ldots\ldots\ldots p_k$ ***sont des nombres premiers deux à deux distincts et*** $\alpha_1, \alpha_2, \ldots\ldots \alpha_k$ ***sont des entiers naturels non nuls.***

Tout diviseur d de l'entier n a une décomposition en produit de facteurs premiers de la forme :

Le nombre de diviseur de n est égal à :

Preuve :

✂----------

***Propriété* (*admise*)**

Soit a et b deux entiers naturels supérieurs ou égaux à 2.

Ecrivons la décomposition en produit de facteurs premiers de a et b :

$a = \prod_{j=1}^{k} p_j^{a_j}$ et $b = \prod_{j=1}^{m} p_j^{\beta_j}$ avec les nombres p_j tous premiers et les exposants α_i et β_j

sont des entiers naturels non nuls.

Alors on a : ***PGCD(a ; b)*** =

Exercice 4

Pour tout entier naturel n , on note F_n le n-ième nombre de Fermat. Il est défini par

$$F_n = 2^{2^n} + 1.$$

Partie A :

Pierre de Fermat, leur inventeur, a conjecturé que :

« Tous les nombres de Fermat sont premiers »,

L'objectif est de tester cette conjecture.

1. **a.** Calculer F_0, F_1, F_2 et F_3.
   b. Peut-on en déduire que tous les nombres de Fermat sont premiers?
2. On considère l'algorithme ci-dessous :

```
F ← 2^(2^5) + 1
N ← 2
Tant que F%N ≠ 0
    N ← N + 1
Fin Tant que
Afficher N
```

$F\%N$ désigne le reste de la division euclidienne de F par N.

La valeur affichée à la fin de l'exécution est 641.
Que peut-on en déduire?

Partie B :

L'objectif est de prouver que deux nombres de Fermat distincts sont toujours premiers entre eux.

1. Démontrer que pour tout entier naturel n non nul on a $F_n = (F_{n-1} - 1)^2 + 1$.
2. Pour tout entier naturel n on note :

$$\prod_{i=0}^{n} F_i = F_0 \times F_1 \times F_2 \times \ldots \times F_{n-1} \times F_n.$$

On a donc $\prod_{i=0}^{n} F_i = \left(\prod_{i=0}^{n-1} F_i\right) \times F_n$.
Montrer par récurrence et en utilisant le résultat de la question précédente que pour tout entier naturel n non nul on a :

$$\prod_{i=0}^{n-1} F_i = F_n - 2.$$

3. Justifier que, pour tous entiers naturels n et m tels que $n > m$, il existe un entier naturel q tel que $F_n - qF_m = 2$.
4. En déduire que deux nombres de Fermat sont toujours premiers entre eux.

III-Le petit théorème de Fermat

1) *Introduction :* Pourquoi « petit » ?

Voici le grand théorème de Fermat :

« Pour tout entier naturel n, il n'existe pas de nombres entiers non nuls x, y et z tels que $x^n + y^n = z^n$ dès que n est un entier strictement supérieur à 2 ».

Pierre de Fermat (1601-1665) l'énonça dans la marge d'un livre et écrit : « j'ai trouvé une merveilleuse démonstration de cette proposition, mais la marge est trop étroite pour la contenir ». Ce théorème ne fût démontré qu'en 1995 (plus de 300 ans plus tard) par Andrew Wiles. Cette démonstration tient en plusieurs centaines de pages.

Dans le cas où n=1 l'équation diophantienne $x^n + y^n = z^n$ admet clairement une infinité de solutions.

Qu'en est-il lorsque n=2 ?

Plimpton 322 :

On appelle triplet pythagoricien un triplet (a, b, c) d'entiers strictement positifs tels que $a^2 + b^2 = c^2$ donc solution de l'équation $x^n + y^n = z^n$ pour n=2.

La tablette babylonienne Plimpton 322 (du nom du collectionneur Georges Plimpton) date des années –1800 environ. C'est l'un des plus anciens textes mathématiques connus. Cette tablette donne une liste de 15 triplets pythagoriciens comme celui de la question h) de l'exercice suivant. Une recherche au hasard de tels triplets est exclue et les premiers commentateurs de la tablette pensaient que les babyloniens connaissaient déjà le résultat du a), 1300 ans avant Pythagore et 1500 ans avant Euclide. Un débat autour des méthodes employées est toujours en cours.

Découverte du petit théorème de Fermat

Soit a un entier relatif.

a) On considère l'entier p=5. Compléter le tableau ci-dessous :

a modulo 5	0	1	2	3	4
a^4 modulo 5					

b) On considère l'entier p=7. Compléter le tableau ci-dessous :

a modulo 7	0	1	2	3	4	5	6
a^6 modulo 7							

c) On considère l'entier p=11. Compléter le tableau ci-dessous :

a modulo 11	0	1	2	3	4	5	6	7	8	9	10
a^{10} modulo11											

d) Quelle condition suffisante sur p et sur a peut-on conjecturer pour que : $a^{p-1} \equiv \ldots \ldots [p]$?

Le petit théorème de Fermat

Théorème

- Soit p un nombre premier et a un entier naturel quelconque, alors $a^p \equiv a\ [p]$.

- (Corollaire crucial)

  Soit p un nombre premier et a un entier naturel non multiple de p, alors : $a^{p-1} \equiv 1\ [p]$.

Démonstration : Celle de MPSI avec coefficient binomiaux et par récurrence. (à distribuer).

Exercice 5

Montrer que pour tout $n \in \mathbb{N}$, $3^{6n} - 1$ est divisible par 7.

Exercice 6

Soit p un nombre premier différent de 3.

Démontrer que pour tout $n \in \mathbb{N}$, $3^{n+p} - 3^{n+1}$ est divisible par p.

Exercice 7

Soit $n \in \mathbb{N}$ et $a = n^5 - n$.

1) Montrer que a est divisible par 5.

2) Montrer que $a = n(n^2 - 1)(n^2 + 1)$

3) Montrer que a est divisible par 2 et par 3.

4) a est-il divisible par 30 ?

Compléments :

Exercice 4 d'arithmétique du bac Marocain 2023, excellent.

EXERCICE4 :(3 points)

Soit p **un nombre premier impair**. On considère dans $\mathbb{Z}$ l'équation $(E) : x^2 \equiv 2 \ [p]$

0.25 1- a) Montrer que : $2^{p-1} \equiv 1 \ [p]$

0.25 b) En déduire que : $2^{\frac{p-1}{2}} \equiv 1 \ [p]$ ou $2^{\frac{p-1}{2}} \equiv -1 \ [p]$

(On remarque que : $(2^{\frac{p-1}{2}} - 1)(2^{\frac{p-1}{2}} + 1) = 2^{p-1} - 1$)

2- Soit x une solution de l'équation (E)

0.5 a) Montrer que p et x sont premiers entre eux.

0.5 b) En déduire que : $2^{\frac{p-1}{2}} \equiv 1 \ [p]$ (On pourra utiliser le théorème de Fermat)

0.25 3- Montrer que pour tout $k \in \{1,2,...,p-1\}$, p divise C_p^k

(On rappelle que : $(\forall k \in \{1,2,...,p-1\})$ $C_p^k = \dfrac{p!}{k!(p-k)!}$ et que : $kC_p^k = pC_{p-1}^{k-1}$)

0.25 4-a) En utilisant la formule de Moivre, montrer que :

$$(1+i)^p = 2^{\frac{p}{2}} \cos\left(p\frac{\pi}{4}\right) + i2^{\frac{p}{2}} \sin\left(p\frac{\pi}{4}\right)$$

(i étant le nombre complexe tel que : $i^2 = -1$)

0.5 b) On admet que : $(1+i)^p = \sum_{k=0}^{k=\frac{p-1}{2}} (-1)^k C_p^{2k} + i \sum_{k=0}^{k=\frac{p-1}{2}} (-1)^k C_p^{2k+1}$

Montrer que : $2^{\frac{p}{2}} \cos\left(p\frac{\pi}{4}\right) \in \mathbb{Z}$ et $2^{\frac{p}{2}} \cos\left(p\frac{\pi}{4}\right) \equiv 1 \ [p]$ (on pourra utiliser la question3-)

0.5 5- En déduire que si $p \equiv 5 \ [8]$ alors l'équation (E) n'admet pas de solution dans $\mathbb{Z}$

Démontrer la propriété suivante :

Soit n un entier naturel, $\sqrt{n}$ est rationnel si, et seulement si n est un carré d'entier.