LMath
Arithmétique
Farba Faye IREMPT/UCAD

Pré requis :

- Connaitre les différents types de démonstration.

- Dans $\mathbb{Z}$ toute partie non vide et minorée a un plus petit élément ; en particulier, dans $\mathbb{N}$ qui est minoré par 0 toute partie non vide a un plus petit élément.

Dans $\mathbb{Z}$ toute partie non vide et majorée a un plus grand élément.

Par conséquent dans $\mathbb{Z}$ toute partie non vide bornée est finie.

- *Axiome d'Archimède :* Pour tout entier a et tout entier naturel $b > 0$, il existe un entier n tel que $a < bn$.

Remarquons que l'axiome d'Archimède peut être énoncé dans l'ensemble des nombres réels :

Pour tout réel a et tout réel $b > 0$, il existe un entier n tel que $a < bn$.

Dans le cadre plus général des rationnels, cet axiome permet de définir la notion de partie entière.

L'axiome signifie simplement que la suite arithmétique bn a pour limite $+\infty$.

- *La descente infinie* est un principe introduit et utilisé par Fermat. Selon ce principe, il n'existe pas de suite strictement décroissante d'entiers positifs.

On utilise ce principe pour prouver qu'il n'existe pas de solution à certains problèmes faisant intervenir des nombres entiers : si à partir d'une solution, on sait en fabriquer une autre strictement plus petite mais toujours en nombres entiers, et qu'on peut recommencer indéfiniment, alors le problème initial n'a pas de solution.

Montrons par exemple en utilisant ce principe qu'il n'existe pas d'entiers naturels a, b strictement positifs tels que $a^2 = 2b^2$ (autrement dit $\sqrt{2}$ n'est pas rationnel).

On raisonne par l'absurde en supposant qu'il existe une solution (a, b) à ce problème.

Alors a^2 est paire. par conséquent a aussi est pair : Il existe un entier naturel a_1 tel que $a = 2a_1$. La relation $a^2 = 2b^2$ devient $2a_1^2 = b^2$.

Partant de cette relation et utilisant le même raisonnement, on en déduit que b aussi est paire : Il existe un entier naturel b_1 tel que $b = 2b_1$.

La relation $2a_1^2 = b^2$ devient $a_1^2 = 2b_1^2$; de plus a_1 et b_1 sont strictement positifs et $a_1 < a$ et $b_1 < b$..

Ainsi le couple (a_1, b_1) est une solution du problème.

On peut alors répéter le processus indéfiniment. On obtient deux suites strictement décroissantes d'entiers naturels positifs. Par le principe de la descente infinie, cela est impossible.

Remarquer que si l'on avait demandé que en plus a et b soient premiers entre eux, la première étape aurait suffit pour écrire une contradiction. En effet dans ce cas 2 serait un facteur commun de a et b.

Pré test :

Exercice 1. Quel sont les quotient et reste de la division euclidienne de 7 par -3 ? de -7 par 3 ? de -7 par -3 ?

Réponse. $7 = -3 \times (-2) + 1$ quotient -2 reste 1.
$-7 = 3 \times (-3) + 2$ quotient -3 reste 2.
$-7 = -3 \times (3) + 2$ quotient 3 reste 2.

□

Exercice 2.

1. Ndew et Debo se rencontrées au marché lundi. Ndew retourne au marché tous les deux jours. Debo retourne au marché tous les trois jours. Quel est le jour de leur prochaine rencontre ?

2. Montrer que $n^5 - n$ est un multiple de 5.

3. a. Réduire $n^5 - n$ en un produit de facteurs irréductibles.

b. En déduire que $n^5 - n$ est divisible par 2 et par 3.

4.

5. en déduire que $n^5 - n$ par 30

Exercice 3. Résoudre les équation suivantes dans l'ensemble X spécifié.

1. $x + y = 1$ et $X = \mathbb{R} \times \mathbb{R}$.

2. $x + y = 1$ et $X = \mathbb{Z} \times \mathbb{Z}$.

3. a. $x + 3y = 1$ et $X = \mathbb{R} \times \mathbb{R}$.

b. $x + 3y = 1$ et $X = \mathbb{Z} \times \mathbb{Z}$.

4. a. $223092870x + 3y = 1$ et $X = \mathbb{Z} \times \mathbb{Z}$.

b. $3 \times 9699690x + 3y = 1$ et $X = \mathbb{Z} \times \mathbb{Z}$.

Réponse.

1. $\{(x, 1 - x), x \in \mathbb{R}\}$, points $\mathbb{R}^2$ de la droite d'équation $x + y = 1$.

2. $\{(x, 1 - x), x \in \mathbb{Z}\}$, points $\mathbb{R}^2$ à coordonnées entières de la droite d'équation $x + y = 1$ (l'addition dans $\mathbb{Z}$ est une relation de composition interne,...)

3. y étant donné dans $\mathbb{Z}$, $1-3y$ est aussi un entier ; donc l'ensemble des solutions est $\{(1-3y, y), y \in \mathbb{Z}\}$.

4. a. Sous cette forme cela est difficile. Mais on peut remarque que $223092870 = 3 \times 9699690$. Le problème est donc identique à celui de la question suivante.

b. Si (x, y) est une solution, alors $1 = 3 \times 9699690x + 3y$ doit être un multiple de 3, ce qui est faux. L'équation n'a pas de solution.

□

Exercice 4. Le nombre 28 s'écrit 26 en base a. Combien vaut a ?

Réponse. $28 = 2a + 6$. Donc $a = 11$.

□

Première partie

Généralités

1 Divisibilité

1.1 Premiers concepts

Cette section, comme son nom l'indique, expose le concept de base de l'arithmétique : la divisibilité.

On introduit ensuite les nombres premiers ce qui permet d'énoncer le théorème fondamental de l'arithmétique (c'est-à-dire la décomposition en facteurs premiers) dans lequel les nombres premiers jouent le rôle de briques élémentaires pour la fabrication des nombres.

1.1.1 Divisibilité

Définition 1.

Soit a et b sont deux entiers tels que a soit non nul. On dit que a *divise* b, ou que b est *divisible* par a, s'il existe un entier q telque $b = aq$. On dit aussi que a est un *diviseur* de b, ou que b est un *multiple* de a. On le note $a|b$.

Voici quelques propriétés assez immédiates que l'on pourra démontrer à titre d'exercice.

Propriétés 1.

1. a. 0 est divisible par n'importe quel entier.

b. Pour tout entier a non nul, les entiers $a, 1, -a$ et -1 sont des diviseurs de a.

2. a. La relation "divise" est symétrique : Pour tout entier non nul a, on a $a|a$.

b. La relation "divise" est transitive : Si $a|b$, et $b|c$, alors $a|c$.

c.
- Si a divise b et $b \neq 0$, alors $|a| \leq |b|$.
- Si $a|b$ et $b|a$, alors on a seulement $|a| = |b|$. La relation "divise" n'est donc pas antisymétrique ; mais sa restriction à l'ensemble $\mathbb{N}$ des entiers naturels l'est

$$\forall a, b \in \mathbb{N}, a|b \text{ et } b|a \Rightarrow a = b.$$

Ainsi la relation "divise" est un ordre sur $\mathbb{N}$. Cet ordre est partiel car par exemple 2 ne divise pas 3 et 3 ne divise pas 2.

3. Si a divise b et c, alors a divise la somme $b + c$ et pour tout entier n, a divise bn en particulier a divise le produit bc.

Soit a un entier. L'ensemble $\{an, n \in \mathbb{Z}\}$ des multiples de a est noté $a\mathbb{Z}$.

Quant à l'ensemble des diviseurs de a on le notera $Div(a)$

Exercice 5. Soient m et n des entiers. Montrer que $a = 5m + 3n$ est un multiple de 11 si et seulement si $b = 6m + 8n$ l'est.

Indication : Calculer $a + b$.

Réponse. $c = a + b = 11(m + n)$ est un multiple de 11.

Donc si a est multiple de 11, alors $b = c - a$ est un multiple de 11 et si b est multiple de 11, alors $a = c - b$ est un multiple de 11.

□

1.1.2 pgcd et ppcm

Comme déjà vu dans les propriétés précédentes tout entier a non nul a au moins 2 diviseurs : on peut citer $-1, 1, -a, a$. De plus cet ensemble est borné car tout diviseur de a appartient à l'intervalle $[-|a|, |a|]$.

Soit a et b sont des entiers non nuls.

L'ensemble des diviseurs communs de a et b est non vide car il contient 1 ; de plus cet ensemble est majoré par $|a||b|$.

L'ensemble des multiples communs strictement positifs de a et b est non vide car il contient $|a||b|$; de plus cet ensemble est minoré par 1.

Ceci motive la définition suivante du pgcd et du ppcm concepts fondamentaux de l'arithmétique.

Définition 2.

Soient a et b deux entiers non tous deux nuls. L'ensemble des diviseurs communs de a et b est non vide et majoré, il possède donc un plus grand élément appelé plus grand commun diviseur (*pgcd*).
Le pgcd de a et b est noté $a \wedge b$. Ainsi $a \wedge b = \max(Div(a) \cap Div(b))$
Lorsque $a \wedge b = 1$, on dit que a et b sont *premiers entre eux*.
L'ensemble des multiples communs *strictement positifs* a et b est non vide et minoré, il possède donc un plus petit élément appelé plus petit commun multiple (*ppcm*).
Le ppcm de a et b est noté $a \vee b$. Ainsi $a \vee b = \min(a\mathbb{N}^* \cap b\mathbb{N}^*)$

Soit a un entier non nul si n est un diviseur de a notons $a_{/n}$ l'unique entier tel que $a = na_{/n}$. (la notation traditionnelle est $\frac{a}{n}$.

Proposition 1.

1. a. $d = a \wedge b$, alors un entier n divise a et b si et seulement si il divise d.

$$\text{Div } (a \wedge b) = \text{ Div } a \cap \text{ Div } b.$$

b. $m = a \vee b$, alors un entier n est un multiple de a et b si et seulement si il est un multiple de m.

$$(a \vee b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$$

2. Si a et b sont des entiers et $n \in \mathbb{N}^*$, alors

$$\boxed{na \wedge nb = n(a \wedge b) \text{ et } na \vee nb = n(a \vee b)}$$

En particulier, si n divise a et b, alors

$$\boxed{n(a_{/n} \wedge b_{/n}) = a \wedge b.}$$

3. a et b sont des entiers distincts et non tous nuls, alors $a \wedge b = a \wedge (b - a)$ dès que le deuxième membre a un sens.
Plus généralement, si q est un entier quelconque

$$\boxed{a \wedge b = a \wedge (b - aq).}$$

Cette égalité est à la base de l'algorithme dit d'Euclide pour déterminer le pgcd de deux entiers.

Exemple 1. Deux entiers consécutifs sont premiers entre eux. En effet si n est un entier, alors par la proposition 1 item 3,

$$n \wedge (n+1) = n \wedge (n+1-n) = n \wedge 1 = 1$$

D'après cette même propriété, a et $qa + 1$ sont premiers entre eux car

$$a \wedge (qa+1) = a \wedge (qa+1-qa) = a \wedge 1 = 1$$

1. Si d est le pgcd de deux entiers a et b, alors les entiers $a_{/d}$ et $b_{/d}$ sont premiers entre eux.

Exercice 6. Soit n un entier naturel. Le $n^{\text{ième}}$ nombre de Fermat est $F_n = 2^{2^n} + 1$.

1. a. Démontrer par récurrence que

$$\forall n \in \mathbb{N}, F_{n+1} = \prod_{k=0}^{n} F_k + 2$$

b. En déduire que si m et n sont deux entiers tels que $m > n$ alors il existe un entier q telque $F_m = qF_n + 2$.

2. Démontrer que deux nombres de Fermat distincts sont premiers entre eux.

Réponse.

1. a. Par récurrence

b. Par récurrence

2. Soit F_m et F_n deux nombres de Fermat avec $m > n$. Alors il existe un entier q tel que $F_m = qF_n + 2$. Donc

$$\begin{aligned} F_n \wedge F_m &= F_n \wedge (F_m - qF_n) \text{ d'après la proposition 1 item 3} \\ &= F_n \wedge 2 = 1 \text{ car } F_n \text{ est impair} \end{aligned}$$

□

1.2 Nombres premiers

Les nombres premiers sont les atomes (les éléments insécables) de l'univers des entiers.

1.2.1 Définition et premières propriétés

Comme nous l'avons dit dans l'introduction de cette partie, les nombres premiers sont les briques élémentaires pour fabriquer les nombres. De façon plus précise et moins imagée, on a la définition suivante :

Définition 3.

Un entier non nul est dit *premier* s'il a exactement *deux* diviseurs positifs : 1 et lui-même.
Un nombre qui n'est pas premier est appelé nombre *composé.*

Les nombres $2, 3, 5, 7, 11$ sont premiers. Les nombres $1, 4, 6, 8, 9, 10$ ne sont pas premiers.

Exercice 7. Soit p un entier premier telque $p > 3$. Montrer que $p^2 - 1$ est un multiple de 12.
Indication : Un nombre premier est nécessairement impair.
De trois nombres consécutifs un et un seul est un multiple de $3^{(?)}$.

Réponse. Puisque p est premier, il est impair. Il existe donc un entier k telque $p = 2k + 1$. Alors $p^2 - 1 = 4(k^2 + k)$ est un multiple de 4.
En suivant l'indication, un des entier $p-1, p$ et $p+1$ est multiple de 3. Ce n'est pas p car p est premier et > 3. Donc $p^2 - 1 = (p - 1)(p + 1)$ est multiple de 3.
$p^2 - 1$ multiple de 3 et de 4 entraine $p^2 - 1$ multiple de $12^{(?)}$.

□

Ce n'est pas toujours facile de voir si un nombre est premier ou non.
Les nombres de Fermat F_0, F_1, F_2, F_3 et F_4 sont premiers.
Fermat pensait que tous les nombres de Fermat étaient premiers. En 1732, Euler prouva que F_5 était divisible par 641.
Soit a un entier naturel distinct de 1. L'ensemble des diviseurs de a strictement supérieurs à 1 est non vide car il contient a. Cet ensemble contient donc un plus petit élément.
La proposition suivante est utile dans les tests de primalité, dont l'un des plus célèbre est le crible d'Eratosthène.

Proposition 2.

1. Soit a un un entier naturel non nul. Son plus petit diviseur $d > 1$ est un nombre premier.

2. Si a est premier, alors $d = a$.
Si de plus a est composé, alors $d^2 \leq a$.

Démonstration.

1. Démontrons cela par l'absurde. Si d n'est pas premier, il a un diviseur positif d', distinct de 1 et de d.

Dans ce cas d' est aussi un diviseur de d et comme il est $< d$, cela contredit la minimalité de d.

2. Si a est premier, il a deux diviseurs positifs : 1 et a. Le plus petit qui est strictement supérieur à 1 est bien a. Il existe un entier q telque $a = dq$. Si de plus a est composé, alors $d<a = dd'$; donc $q > 1$. Du coup $q \geq d$ (car d est le plus petit diviseur de a qui est strictement supérieur à 1). On conclut en multipliant par d que $a \geq d^2$. □

Remarque 1.

On déduit de la propriété précédente que pour tester si un entier $a > 1$ est premier, il suffit de regarder s'il est divisible ou non par un des entiers compris entre 2 et $\sqrt{a}$. Par exemple, pour vérifier que 31 est premier, il suffit de voir qu'il n'est divisible ni par 2, ni par 3, ni par 4, ni par 5.
Comme aucun de ces entiers n'est divisible par 31, et que l'entier suivant 6 a un carré supérieur à 31, on peut conclure que 31 est premier.
On aurait pu évidemment s'épargner le test de la divisibilité par 4 si on savait par avance que 4 est composé.

Remarque 2.

La proposition nous amène à la méthode, appelée *crible d'Eratosthène* pour lister tous les nombres premiers entre 1 et a : on écrit à la suite les uns des autres tous les entiers compris entre 1 et a.
2 est premier. On le choisit et on barre tous ses multiples.
Le suivant non barré est 3. Il est premier car sinon son plus petit diviseur ne pourrait être que 2. Mais on a barré tous les multiples de 2 ! !
Le suivant non barré est 5. Il est premier car sinon son plus petit diviseur ne pourrait être que 2 ou 3. Mais on a barré tous les multiples de 2 et de 3 ! !
Par ce procédé quand on aura atteint le dernier nombre dont le carré est inférieur à $\sqrt{a}$, on aura terminé : tous les autres nombres non barrés seront premiers.

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

1.2.2 L'ensemble des nombres premiers est infini

Proposition 3 (Euclide)**.**

Il existe une infinité de nombres premiers.

Démonstration. Pour tout nombre de Fermat F_n, notons d_n le plus petit diviseur premier de F_n. Alors si m et n sont des entiers distincts, F_n et F_m étant premiers entre eux, d_n et d_m sont distincts.

On crée ainsi une application injective $d : n \to d_n$ de $\mathbb{N}$ dans l'ensemble $\mathbb{P}$ des nombres premiers. L'ensemble $\mathbb{P}$ est donc infini. □

Démonstration d'Euclide, par l'absurde. Si l'ensemble $\mathbb{P}$ des nombres premiers était fini, l'ensemble de nombres premiers positifs serait aussi fini. Notons $p_1, p_2, \ldots, p_n$ ces nombres et posons $p = p_1 p_2 p_n + 1$. Alors, p strictement plus grand que chacun des p_i, n'est pas premier. p a un plus petit diviseur positif premier ; ce plus petit diviseur positif est l'un de p_i, notons-le p_j. Notons q le produit de tous les autres. Il existe un entier d telque $p = p_j d$. Alors, $p = p_1 p_2 p_n + 1 = p_j q + 1 = p_j d$; donc $p_j(d - q) = 1$. C'est impossible car p_j n'est pas inversible dans $\mathbb{Z}$. □

Exercice 8. Un nombre premier est premier avec tout entier qu'il ne divise pas.

Réponse. Soit p un nombre premier, a un entier non multiple de p et notons d leur pgcd. Alors d divise p. Comme n n'est pas multiple de p, l'entier d est différent de p donc est supérieur strictement à p. Puisque p est premier, $d = 1$.(N'oublions pas que p n'a que deux diviseurs positifs : 1 et p.)

□

Exercice 9. Bien que l'ensemble des nombres premiers soit infini, leur répartition dans $\mathbb{N}$ est assez rare. Plus précisément :

Prouver que pour tout entier naturel $n \geq 1$ (aussi grand que l'on veut) l'intervalle $[(n+1)! + 2, (n+1)! + n + 1,]$, dont la longueur est n, ne contient aucun nombre premier.

Réponse. En effet, un entier appartenant à cet intervalle est de la forme $(n+1)! + k$, k étant un entier compris entre 2 et $n + 1$.

Or le produit $(n+1)!$ contient le facteur k : il existe q tel que $(n+1)! = kq$. Donc $(n+1)! + k = k(q+1)$.

□

2 Division euclidienne et conséquences

2.1 Division euclidienne

Théorème 1 (Division euclidienne)**.**

Soit b un entier non nul. Tout entier a s'écrit de manière unique sous la forme $a = bq + r$, avec q et r entiers et $0 \leq r < |b|$.
Les entiers q et r sont appelés respectivement quotient et reste de la division euclidienne de a par b.

On remarque immédiatement que a est divisible par b si et seulement si $r = 0$. Comme pour les parties entières, on prendra garde à ce qui se produit lorsque l'un des nombres a et b est négatif.

Démonstration.

1. *Existence.* Si $a = 0$ on peut prendre $q = r = 0$. Supposons donc a non nul.
Supposons d'abord $b > 0$ et posons $B = \{n \in \mathbb{Z} : bn \leq a\}$
Si $a > 0$ alors B contient tous les entiers négatifs. De plus, d'après l'axiome d'Archimède, il existe un entier n_0 telque $a < bn_0$. Alors, pour tout élément $n \in B$, on a $bn \leq a < bn_0$. Par conséquent $n < n_0$ et B est majoré.
Si $a < 0$ alors d'après l'axiome d'Archimède, il existe un entier n_1 tel que $-a < bn_1$ c'est à dire $b(-n_1) < a$; B est donc non vide. De plus, pour tout entier positif m et tout élément n de B on a $bn \leq a < 0 \leq bm$. Par conséquent $n < m$ et B est majoré.
On voit ainsi que dans tous les cas, B est non vide et majoré. Il a donc un plus grand élément q. Alors $q + 1$ n'appartient pas à B, autrement dit, $a < b(q + 1)$.
En résumé, $bq \leq a < b(q + 1)$. (On vient en fait de définir q comme la partie entière de $\frac{a}{b}$.) Il suffit alors de poser $r = a - bq$.
Si $b < 0$, on se ramène au cas précédent avec $-b$.

2. *Unicité.* si a s'écrit $a = bq + r = bq' + r'$, alors $b(q - q') = r' - r$.
La non nullité de $|q' - q|$ aurait entrainé $|b| > |r' - r| = |b||q - q'| \geq |b|$, une contradiction ! !
Donc $q = q'$ puis $r = r'$. □

Exercice 10. Soit p un entier naturel premier tel que $8p^2 + 1$ soit premier. Montrer que $8p^2 -$ est aussi premier. *Indication :* Discuter suivant les valeurs du reste de la division euclidienne de p par 3.

2.2 Conséquences principales

2.2.1 Théorème de Bézout

Théorème 2 (Bezout).

1. Soient a et b des entiers non tous nuls. Notons d le pgcd de a et b : $d = a \wedge b$. Alors il existe des entiers u et v tels que :

$$au + bv = d$$

2. En particulier, a et b sont premiers entre eux si, et seulement s'il existe des entiers u et v tels que $au + bv = 1$.

Démonstration.

1. Posons $B = \{am + bn \text{ où } m \text{ et } n \text{ sont entiers non tous nuls}\} \cap \mathbb{N}^*$. En prenant dans $\mathbb{R}^2$ le vecteur $A = (a, b)$, B est en fait l'ensemble des produits scalaires positifs AX, X étant le vecteur (m, n).
B est non vide car il contient $|a| + |b|$ (faire $m = signe(a)$ et $n = signe(b)$).
Comme B un sous ensemble de $\mathbb{N}^*$, il est minoré par 1.
B a donc un plus petit élément $\delta = au + bv$.
Maintenant montrons que $\delta = a \wedge b$.
Posons $d = a \wedge b$. Comme d divise a et b, il divise aussi au et bv donc $au + bv = \delta$; alors $d \leq \delta$.
Soit q et r le quotient et le reste de la division euclidienne de a par δ :

$$a = \delta q + r, 0 \leq r < \delta.$$

Alors $r = a - \delta q = a(1 - uq) + vqr$. La non nullité de r entraine alors son appartenance à B ; ce qui est impossible puisque $r < d$ et d est le plus petit élément de B. Donc $r = 0$ et $a = \delta q$ est divisible par δ.
Par un raisonnement analogue, b est un divisible par δ.
Ainsi δ est un diviseur commun de a et b. Donc $\delta \leq d$.
Finalement $\delta = d$.

2. Si a et b sont premiers entre eux, leur pgcd vaut 1, alors, d'après la première partie, il existe des u et v tels que $au + bv = 1$.
Réciproquement, supposons cette propriété réalisée et notons d le pgcd de a et b.
Comme d divise a et b, il divise aussi au et bv donc $au + bv$ qui vaut 1. on conclut que $d = 1$. □

Remarque 3.

Attention ! ! Soit c un entier. La relation $au + bv = c$ n'entraine pas que c est le pgcd de a et b.
En revanche, on en déduit en notant d le pgcd de a et b : il existe un entier m telque $a = dm$ et il existe un entier n telque $b = dn$.
La relation devient alors $dmu + dnv = c$. c est donc un multiple de d.
Ainsi, l'équation $au + bv = c$, d'inconnue le couple (u, v) n'a de solution que si c est un multiple de $a \wedge b$.
Dans ce cadre, puisque la division euclidienne de b par a s'écrit aussi $a(-q) + b.1 = r$, le reste r est nécessairement un multiple du pgcd $a \wedge b$.

Corollaire 1.

Si un entier est premier avec deux autres, alors il est premier avec leur produit.

$$\left\{ \begin{array}{lcl} a \wedge b_1 & = & 1 \\ a \wedge b_2 & = & 1 \end{array} \right. \Rightarrow a \wedge b_1 b_2 = 1$$

Démonstration. Si a est premier avec b_1 et b_2, par Bezout, il existe des entiers u_1, v_1, u_2, v_2 tels que

$$\begin{cases} au_1 + b_1v_1 &= 1 \\ au_1 + b_2v_2 &= 1 \end{cases}$$

En faisant le produit membre à membre on obtient $au_3 + bv_3 = 1$ avec $u_3 = au_1u_2 + b_2u_1v_2 + b_1v_1u_2$ et $v_3 = v_1v_2$. On conclut alors par Bezout. □

Exercice 11. Montrer que si a et b sont premiers entre eux, toute puissance de a est premier avec toute puissance de b en particulier pour tout entier n, a^n et b^n sont premiers entre eux.

$$a \wedge b = 1 \Rightarrow \forall m, n \in \mathbb{N}^*, a^m \wedge b^n = 1$$

Indication : Utiliser Bezout pour montrer d'abord que $a^m \wedge b = 1$.

Réponse. Si a et b sont premiers entre eux, par Bezout, il existe des entiers u et v tels que $au + bv = 1$ c'est à dire $au = 1 - bv$. On élève à la puissance m et on utilise la formule du binôme au second membre. $a^mu^m = (1 - bv)^m$.

Une fois développé, ce second membre est la somme de 1 et de termes contenant tous le facteur b : il existe un entier w tel que $(1 - bv)^m = 1 - bw$. La relation précédente devient $a^mu^m = 1 - bw$; autrement dit $a^mu^m + bw = 1$. On conclut encore une fois par Bezout que a^m et b sont premiers entre eux.

On vient de démontrer que : *Si deux entiers sont premiers entre eux chacun des deux est premier avec toute puissance de l'autre.*

Appliquons cela aux deux nombres premiers entre eux a^m et b avec l'entier n : a^m est premier avec b^n.

□

2.2.2 Lemme de Gauss

Enoncé du lemme

Théorème 3 (Gauss)**.**

Soit a, b et c trois entiers non nuls. Si a divise le produit bc et est premiers avec b alors a divise c.

$$\begin{cases} a|bc \\ a \wedge b = 1 \end{cases} \Rightarrow a|c$$

Démonstration. Puisque a divise bc, il existe un entier q tel que $bc = aq$.

Par Bezout il existe des entiers u et v tels que $au + bv = 1$.

Alors en multipliant par c on a $acu + bcv = c$. Ensuite, on remplace bc par aq pour avoir

$$c = acu + bcv = acu + aqv = a(cu + qv)$$

On conclut que a divise c. □

Corollaire 2.

Si un entier *premier* divise un produit $a_1a_2 \dots a_n$ alors p divise au moins l'un des a_i.

Remarque 4.

Attention ! ! Il est essentiel de supposer l'entier premier. Par exemple, 8 divise 4×6 (en trois parties) mais il ne divise aucun des facteurs.

Démonstration. Par l'absurde, supposons que p ne divise aucun des a_i. Alors p est premier avec chacun d'eux.

p est premier avec a_1 et divise $a_1(a_2 \dots a_n)$; par Gauss p divise $a_2 \dots a_n$.

p est premier avec a_2 et divise $a_2(a_3 \dots a_n)$; par Gauss p divise $a_3 \dots a_n$.

En itérant on arrive à p divise $a_{n-1}a_n$ et comme il est premier avec a_{n-1}, il devra diviser a_n ; une contradiction. □

Résolution de l'équation Diophantienne linéaire $au + bv = c$

a. Résolution de l'équation homogène $au + bv = 0$ Quitte à simplifier par d, le pgcd de a et b on peut supposer a et b premiers entre eux.

L'équation est équivalente à $au = -bv$.

Alors a divise bv et comme il est premier avec b il doit diviser v, d'après Gauss. Il existe donc un entier k telque $v = ak$. L'équation devient $au = -bak$ c'est dire $u = -bk$.

L'ensemble des solutions de l'équation homogène $au + bv = 0$ dans $\mathbb{Z}^2$ est

$$\{k(-b, a), k \in \mathbb{Z}\}$$

Remarque 5.

On pouvait s'attendre à ce résultat. En effet, l'ensemble des solutions de l'équation homogène $au+bv = 0$ dans $\mathbb{R}^2$ est bien la droite vectorielle engendrée par le vecteur $(-b, a)$. Les solutions dans $\mathbb{Z}^2$ sont donc les points de cette droite ayant de coordonnées entières.

b. Résolution de l'équation avec second membre $au + bv = c$

Soit (u_0, v_0) une solution de l'équation $au + bv = c$. Pour toute autre solution (u,v) de cette équation, on a :

$$\begin{cases} au_0 + bv_0 &= c \\ au + bv &= c \end{cases}$$

et en faisant la différence membre à membre, $a(u - u_0) + b(v - v_0) = 0$. Ainsi, le couple $(u - u_0, v - v_0)$ est solution de l'équation homogène. Il existe donc $k \in Z$ telque $u = u_0 - kb$ et $v = v_0 + ka$

(u_0, v_0) étant une solution particulière de l'équation avec second membre $au + bv = c$ dans $\mathbb{Z}^2$, l'ensemble des solutions de cette équation est

$$\{(u_0 - kb, v_0 + ka), k \in \mathbb{Z}\}$$

Par conséquent, pour résoudre cette équation, il suffit d'en connaitre une solution particulière. Une solution particulière peut être fournie par l'algorithme dit d'Euclide.

Corollaire 3.

Soient a et b des entiers non tous nuls.

$$(a \vee b) \,.\, (a \wedge b) = |a| \, |b|$$

Démonstration. Supposons d'abord que a et b soient premiers entre eux c'est à dire $a \wedge b = 1$.

Soit μ un multiple commun de a et de b. Il existe deux entiers m et n tels que $\mu = am = bn$

Le couple (m, n) est donc solution de l'équation homogène $au - bv = 0$. Par conséquent, il existe un entier k tel que $m = bk$ et $n = ak$; donc $\mu = abk$ est un multiple de ab.

Puisque tout multiple commun de a et b est un multiple de ab donc de $|a| \, |b|$, on a $a \vee b = |a| \, |b|$.

Dans le cas général, en notant d le pgcd de a et de b, les entiers $a_{/d}$ et $b_{/d}$ sont premiers entre eux ; on a donc par ce qui précède $a_{/d} \vee b_{/d} = |a_{/d}| \, |b_{/d}|$ soit, en multipliant par d^2 : $d^2(|a_{/d} \vee b_{/d}) = |a| \, |b|$.

Finalement $|a| \, |b| = d[d(a_{/d} \vee b_{/d})] = d(da_{/d} \vee db_{/d}) = d(a \vee b)$ □

Exercice 12. Déterminer tous les entiers naturels n tels que $5^{n-1} + 3^{n-1}$ divise $5^n + 3^n$.

Réponse. $5^{n-1}+3^{n-1}$ divise 5^n+3^n si et seulement s'il existe un entier q tel que $5^n+3^n = q(5^{n-1}+3^{n-1})$ c'est à dire $5^{n-1}(5-q) - 3^{n-1}(q-3) = 0$.

Le couple $(5-q, q-3)$ est donc solution de l'équation diophantienne $5^{n-1}u - 3^{n-1}v = 0$.

comme 3 et 5 sont premiers entre eux, 3^{n-1} et 5^{n-1} sont aussi premiers entre eux,

On en déduit qu'il existe un entier k tel que $5-q = 3^{n-1}k$ et $q-3 = 5^{n-1}k$. Soit en faisant la différence membre à membre $(5^{n-1}+3^{n-1})k = -2$. Ainsi, $5^{n-1}+3^{n-1}$ est un diviseur de 2 qui est ≥ 2. Donc $5^{n-1}+3^{n-1} = 2$ la seule valeur possible est $n = 1$. L'hypothèse de départ devient 2 divise 8.

□

Exercice 13. Montrer que pour tout entier n, $n^3 - n$ est un multiple de 6.

Réponse. $n^3 - n = (n-1)n(n+1)$ est un multiple de 2 car il contient deux facteurs entiers consécutifs c'est aussi un multiple de 3 car il contient trois facteurs entiers consécutifs. Il existe donc deux entiers p et q tels que $n^3 - n = 2p = 3q$; donc $2p - 3q = 0$.

Le couple (p, q) est donc solution de l'équation diophantienne $2u - 3v = 0$.

comme 2 et 3 sont premiers entre eux, on en déduit qu'il existe un entier k tel que $p = 3k$ et $q = 2k$. Alors $n^3 - n = 2p = 6k$ est bien un multiple de 6.

□

Exercice 14. Montrer que pour tout entier n, $14n+3$ et $21n+4$ sont premiers entre eux.

Réponse. Il suffit de trouver deux entiers u et v tels que $(14n+3)u + (21n+4)v = 1$ c'est à dire $(14u+21v)n + (3u+4v) = 1$.

Pour cela il *suffit* que $\left\{ \begin{array}{rcl} 2u+3v & = & 0 \\ 3u+4v & = & 1 \end{array} \right.$. La seule solution de ce système linéaire à deux inconnues est $u == 3$ et $v = -2$. Une fois ce résultat trouvé, il devient évident que $3(14n+3) - 2(21n+4)v = 1$.

□

2.2.3 Algorithmes

Algorithme de calcul du pgcd

Comme déjà dit, l'algorithme d'Euclide de calcul du pgcd repose sur la relation suivante :

$a \wedge (aq+r) = a \wedge r$ valable pour a et r entiers non tous nuls.

Soit a et b deux entiers strictement positifs. Pour avoir une formule générale posons $b = r_0$ et $a = r_1$. Par division euclidienne de b par a, il existe des entiers r_2 et q_2 tels que $b = aq_2 + r_2$ et $0 \leq r_2 < a$

La relation devient $r_0 = r_1q_2 + r_2$ et $0 \leq r_2 < r_1$ et alors $a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2$.

On en déduit, si r_2 est non nul et par division euclidienne de r_1 par r_2 qu'il existe deux entiers q_3 et r_3 tels $r_1 = r_2q_3 + r_3, 0 \leq r_3 < r_2$ et alors $r_1 \wedge r_2 = r_2 \wedge r_3$.

Si r_3 est non nul, on peut reprendre le processus.

On poursuit... Si aucun reste n'est nul, on obtient une suite strictement décroissante de restes $r_i > 0$ tels que $a \wedge b = r_0 \wedge r_1 = \cdots = r_i \wedge r_{i+1} \ldots$. Par le principe de la descente infinie, cela est impossible.

On aboutit donc nécessairement au bout d'un nombre fini d'étapes à un reste r_n nul.

Alors
$$a \wedge b = r_0 \wedge r_1 = \cdots = r_i \wedge r_{i+1} = \cdots = r_{n-2} \wedge r_{n-1} = r_{n-1} \wedge 0 = r_{n-1}.$$
Avec $r_0 = b, r_1 = a$ et $r_i = r_{i+1}q_{i+2} + r_{i+2}, \quad 0 \leq r_{i+2} < r_{i+1}$

Soit par exemple à déterminer le pgcd de 6525 et de 2353.

6525	=	$2353 \times 2 + 1819$	$6525 \wedge 2353 = 2353 \wedge 1819$
2353	=	$1819 \times 1 + 534$	$2353 \wedge 1819 = 1819 \wedge 534$
1819	=	$534 \times 3 + 217$	$1819 \wedge 534 = 534 \wedge 217$
534	=	$217 \times 2 + 100$	$534 \wedge 217 = 217 \wedge 100$
100	=	$17 \times 5 + 15$	$217 \wedge 100 = 100 \wedge 15$
17	=	$15 \times 1 + 2$	$100 \wedge 15 = 15 \wedge 2$
15	=	$2 \times 7 + 1$	$15 \wedge 2 = 2 \wedge 1$
2	=	$1 \times 2 + 0$	$2 \wedge 1 = 1 \wedge 0 = 1$

Algorithme étendu (de détermination d'une solution de l'équation diophantienne)

Voir le fichier index.html

2.3 Décompositions

2.3.1 Décomposition d'un nombre premier

Théorème 4.

Tout entier > 1 se décompose d'une manière unique (à l'ordre des facteurs près) en un produit de nombres premiers.
Autrement dit, pour tout $n \in \mathbb{N}$ et $a > 1$, il existe des entiers premiers et deux à deux distincts $p_1, p_2 \ldots, p_k$ et des entiers strictement positifs $\alpha_1, \alpha_2 \ldots, \alpha_k$ tels que $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots . p_k^{\alpha_k}$

Démonstration.

1. *Existence :* Par récurrence forte, démontrons la propriété $\forall \in \mathbb{N}, n \geq 2 \Rightarrow \mathcal{P}_n$: n se décompose en un produit de nombres premiers.

$\mathcal{P}_2$ est vrai car 2 est premier.

Soit $n \geq 3$ un entier. Supposons $\mathcal{P}_k$ vraie pour tout entier strictement inférieur à n et montrons que $\mathcal{P}_n$ est vraie.

Distinguons deux cas.

- Si n est premier, il s'écrit bien comme un produit de nombres premiers.

- Si n n'est pas premier, il a deux facteurs propres a et b, c'est à dire des entiers distincts de 1 et de n tels que $n = ab$. Chacun des entiers a et b est $\leq n - 1$; $\mathcal{P}_a$ et $\mathcal{P}_b$ sont donc vraies : Chacun de ces entiers est un produit fini d'entiers premiers deux à deux distincts. Donc leur produit n est bien un produit fini d'entiers premiers deux à deux distincts.

Unicité : Remarquons d'abord que deux entiers naturels distincts et premiers sont premiers entre eux. Rappelons ensuite, corollaire 2, que si un entier premier divise un produit, il divise l'un des facteurs .

Supposons que a s'écrit $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots . p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \ldots . q_l^{\beta_l}$.

Alors p_1 est premier et divise le produit $q_1^{\beta_1} q_2^{\beta_2} \ldots . q_l^{\beta_l}$. p_1 doit alors diviser l'un des facteurs $q_1, q_2, \ldots, q_l$. p_1 est donc égal à l'un de ces facteurs. Par le même raisonnement, chaque p_i est égal à l'un des q_j.

Par le même raisonnement, chaque q_i est égal à l'un des p_j.

Donc les p_i et le q_j sont égaux et $k = l$.

Ainsi on a $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots . p_k^{\alpha_k} = p_1^{\beta_1} p_2^{\beta_2} \ldots . p_k^{\beta_k}$.

Je dis que $\alpha_1 = \beta_1$.

En effet, si par exemple $\alpha_1 > \beta_1$, on pourra écrire $p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2} \ldots . p_k^{\alpha_k} = p_2^{\beta_2} \ldots . p_k^{\beta_k}$. Alors p_1 qui est premier divise le produit $p_2^{\beta_2} \ldots . p_k^{\beta_k}$ sans diviser aucun des facteurs $p_2, \ldots, p_k$. Cela contredit le corollaire 2.

Par un raisonnement analogue $\alpha_i = \beta_i$ pour tout i. □

Voici une conséquence immédiate de ce théorème, donnant tous les diviseurs d'un entiers, connaissant sa décomposition en produits de facteurs premiers.

Proposition 4.

Si la décomposition en facteurs premiers d'un entier $a \geq 2$ est $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots . p_k^{\alpha_k}$, alors les diviseurs positifs de a sont les entiers de la forme $p_1^{\gamma_1} p_2^{\gamma_2} \ldots . p_k^{\gamma_k}$ avec pour chaque i, γ_i est un entier vérifiant $0 \leq \gamma_i \leq \alpha_i$.
Le nombre total de diviseurs positifs de a est donc $(\alpha_1 + 1)(\alpha_2 + 1) \ldots . (\alpha_k + 1)$

Corollaire 4.

Si la décomposition en facteurs premiers de deux entiers a et $b \geq 2$ est

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots . p_k^{\alpha_k} \text{ et } b = p_1^{\alpha_1} p_2^{\alpha_2} \ldots . p_k^{\alpha_k}$$

alors

$$\begin{array}{rcl} a \wedge b & = & p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \ldots . p_k^{\min(\alpha_k,\beta_k)} \\ a \vee b & = & p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \ldots . p_k^{\max(\alpha_k,\beta_k)} \end{array}$$

En général a et b *n'ont pas les mêmes facteurs premiers dans leur décomposition.* Si c'est le cas on reporte dans a les facteurs premiers de b absent dans la décomposition de a en leur affectant la puissance 0 et on reporte dans b les facteurs premiers de a absents dans la décomposition de b en leur affectant la puissance 0.

Par exemple si $a = 2^3.3^4.5$ et $b = 3^1.5^2.7^2$, on écrira

$$a = 2^3.3^4.5^1.7^0 \text{ et } b = 2^0.3^1.5^2.7^2$$

et donc

$$a \wedge b = 2^0.3^1.5^1.7^0 \text{ et } a \vee b = 2^3.3^4.5^2.7^2$$

Avec le corollaire précédent, on retrouve un résultat déjà démontré : $ab = (a \wedge b).(a \vee b)$. Il suffit de se rappeler que si α et β sont des nombres quelconques, alors $\alpha + \beta = \min(\alpha, \beta) + \max(\alpha, \beta)$

Exercice 15 (proposé par El Hadji Dame Seye)**.** Soit a et b des entiers. Démontrer que prour tout entier naturel non nul m, a^m divise b^m si et seulement si a divise b.

Réponse. Si a divise b ; im existe un entier q tel que $b = aq$. Alors $b^m = a^m q^m$. donc a^m divise b^m (en q^m parties).

Réciproquement, supposons que a^m divise b^m. On peut supposer a et b positifs.

Il existe des entiers naturels premiers $p_1, \ldots, p_n$ et des entiers naturels $\alpha_1, \ldots, \alpha_n$ et $\beta_1, \ldots, \beta_n$ (certains d'entre eux pouvant être nuls) tels que $a = p_1^{\alpha_1} + \cdots + p_n^{\alpha_n}$ et $b = p_1^{\beta_1} + \cdots + p_n^{\beta_n}$.

Donc $a^m = p_1^{m\alpha_1} + \cdots + p_n^{m\alpha_n}$ et $b^m = p_1^{m\beta_1} + \cdots + p_n^{m\beta_n}$. Puisque a^m divise b^m, pour chaque indice $i, m\alpha_i \leq m\beta_i$ c'est à dire $\alpha_i \leq \beta_i$. Donc a divise b.

□

2.3.2 Décomposition d'un entier dans une base

Le entiers que nous avons l'habitude de manipuler sont en fait écrit en base 10.

Ainsi $123 = 1.10^2 + 2.10^1 + 3.10^0$ et $1002 = 1.10^3 + 0.10^2 + 0.10^1 + 210^0$.

Dans cette section, on souhaite montrer qu'un entier naturel donné peut être décomposé dans n'importe quelle base $b \geq 2$.

Théorème 5.

Soit b un entier ≥ 2. Tout entier strictement positif a s'écrit de façon unique sous la forme :

$$a = a_k b^k + \cdots + a_2 b^2 + a_1 b + a_0$$

où k est un entier, les a_i sont des entiers compris entre 0 et $b-1$ et où $a_k \neq 0$.

On note parfois $a = \overline{a_k a_{k-1} \ldots a_0}^b$. Cette notation est l'écriture de a en base b.

Si $b = 10$, les a_i correspondent aux chiffres usuels de a.

Si $a = 16$ les chiffres sont $0, 1, \ldots, 9, A, B, C, D, E, F$.

Démonstration. *Existence :* Elle consiste à effectuer des divisions euclidiennes successives par b.

a s'écrit $\boxed{a = bq_0 + a_0, 0 \leq a_0 \leq b-1.}$ Alors $0 \leq q_0 < a$. Si $q_0 = 0$, alors $a = a_0$ et c'est fini.

Si $q_0 \neq 0, q_0$ s'écrit $q_0 = bq_1 + a_1, 0 \leq a_1 \leq b-1$. Alors $0 \leq q_1 < q_0$. $a = b^2q_1 + ba_1 + a_0$. Si $q_1 = 0$ alors $a = ba_1 + a_0$ et c'est fini.

Si $q_1 \neq 0$, on continue, construisant q_2, a_2, q_3, a_3.

Supposons avoir construit les $q_0 > \cdots > q_i$ et les $0 \leq a_0, a_1, \ldots, a_i \leq b-1$ tels que $a = q_ib^i + a_ib^i + \cdots + a_1b + a_0$.

Si $q_i = 0, a = a_ib^i + \cdots + a_1b + a_0$ c'est fini.

Si $q_i \neq 0, q_i$ s'écrit $\boxed{q_i = bq_{i+1} + a_{i+1}, 0 \leq a_{i+1} \leq b-1.}$

Le processus va s'arrêter en un rang donné k, car la suite (q_i) est positive et *strictement décroissante* et alors on obtient la décomposition attendue.

Unicité : Si a s'écrit $a = a_kb^k + \cdots + a_2b^2 + a_1b + a_0 = a'_lb^l + \cdots + a'_2b^2 + a'_1b + a'_0$. Alors $|a_0 - a'_0|$ qui est $< b$ est un multiple de b. Ce qui nécessite $a_0 = a'_0$.

Alors $a_kb^k + \cdots + a_2b^2 + a_1b = a'_lb^l + \cdots + a'_2b^2 + a'_1b$.

On simplifie par b et on reprend le même raisonnement pour montrer que $a_1 = a'_1$. On continue le processus. □

Exemple 2. Comment s'écrit 48 en base 5?

48	5		
3	9	5	
	4	1	5
		1	0

L'écriture de 48 en base 5 est $\overline{143}^5$.

2.4 Exercices

Exercice 16. Le nombre 29 dans le système décimal s'écrit 27 en base a. Combien vaut a ?

Réponse. $29 = 2a^1 + 7a^0$ Donc $a = 11$.

□

Exercice 17. **Réponse.** Calculer $\overline{34124}^5 + \overline{2222}^5$

□

Deuxième partie

Arithmétique modulaire

L'arithmétique modulaire ou des congruences est un outil très puissant pour traiter de manière simple des problème d'arithmétique assez complexes.

3 Congruence modulo n

3.1 Congruence modulo n

Définition 4.

Soit n un entier naturel non nul.
Un entier a est congru modulo n à un entier b si et seulement si $a-b$ est un multiple de n. on écrit $a \equiv b[n]$.

$$\begin{array}{lll} a \equiv b[n] & \Leftrightarrow & a-b \in n\mathbb{Z} \\ & \Leftrightarrow & \exists q \in \mathbb{Z} \ : a-b=nq \end{array}$$

La relation "congru modulo n" vérifie les propriété suivantes :

Proposition 5 (Propriétés immédiates).

1. a. Tout entier est congru modulo n à lui-même : $\forall a \in \mathbb{Z}, a \equiv a[n].$
On dit que la "congru modulo n" est *réflexive.*

b. Si a est congru modulo n à b, alors b est congru modulo n à a : $\forall a, b \in \mathbb{Z}, a \equiv b[n] \Rightarrow b \equiv a[n].$
On dit que la "congru modulo n" est *symétrique.*

c. Si a est congru modulo n à b et b est congru modulo n à c alors a est congru modulo n à c : $\forall a, b, c \in \mathbb{Z}, \left\{ \begin{array}{l} a \equiv b[n] \\ b \equiv c[n] \end{array} \right. \Rightarrow a \equiv c[n].$
On dit que la "congru modulo n" est *transitive.*
On résume ces trois propriétés en disant que la relation "congru modulo n" est une *relation d'équivalence*

2. Si $\left\{ \begin{array}{l} a \equiv b[n] \\ a' \equiv b'[n] \end{array} \right.$ alors $\left\{ \begin{array}{l} a+a' \equiv b+b'[n] \\ aa' \equiv bb'[n] \end{array} \right.$ On résume cette propriété en disant que la relation "congru modulo n" *respecte (ou est compatible avec) l'addition et la multiplication.*

Soit a un entier. Un entier b est congru modulo n à a si et seulement s'il existe un entier q tel que $b-a=nq$ c'est à dire $b=nq+a$.

L'ensemble des entiers congrus modulo n à a est donc $\{a+qn, q \in \mathbb{Z}\}$; il est souvent noté $\dot{a}$ ou $a+n\mathbb{Z}$ et appelé *classe de a modulo n* et l'ensemble des classes modulo n est noté $\mathbb{Z}/n\mathbb{Z}$

La classe de 0 modulo n est $\{qn, q \in \mathbb{Z}\}$; c'est l'ensemble des multiples de n.

L'item 2 de compatibilité de la relation de congruence avec lois + et . dans $\mathbb{Z}$ permet de définir une addition (notée encore +)et un multiplication (notée encore .) par : $\forall a, b \in \mathbb{Z}, \dot{\overline{a+b}} = \dot{a} + \dot{b}$ et $\dot{\overline{a.b}} = \dot{a}.\dot{b}$.

Ces deux lois sont commutatives, associatives. $\dot{0}$ est l'élément neutre de l'addition, $\dot{1}$ est l'élément neutre de la multiplication.

Enfin, la multiplication est distributive par rapport à l'addition : $\dot{a}.(\dot{b} + \dot{c}) = \dot{a}.\dot{b} + \dot{a}.\dot{c}$.

Exercice 18. Soit n_1 et n_2 des entiers naturels non nuls. Démontrer que

$$\text{Si } \begin{cases} a \equiv b[n_1] \\ a \equiv b[n_2] \end{cases} \quad \text{alors } a \equiv b[n_1 \vee n_2]$$

Réponse. L'hypothèse se traduit par $a-b$ est un multiple commun de n_1 et de n_2. Donc c'est un multiple de leur ppcm.

□

3.2 Système complet de résidus modulo n

.

Soit n entier naturel non nul.

Pour tout tout entier a, il existe par division euclidienne, un couple d'entiers (q, r) tel que $a = nq + r$ et $0 \leq r < n$. Comme $r = a - nq$, l'entier r appartient à la classe de a.

Si r' est un représentant de la classe de a vérifiant la condition $0 \leq r' < n$ alors il existe un entier q' tel que $r' = a + nq'$. Par conséquent $|r' - r| = n|q + q'|$ est un multiple de n ; comme il est plus petit que n, il est nécessairement nul. Donc $r = r'$.

Ainsi r, reste de la division euclidienne de a par n est l'unique élément de la classe de a vérifiant la condition $0 \leq r < n$.

Définition 5.

Soit n un entier naturel non nul. L'ensemble $\{0, 1, \ldots, n-1\}$ est appelé *un système complet de résidus modulo n.* Un élément de cet ensemble est appelé un résidu modulo n.
Plus généralement un système complet de résidus modulo n est une partie R de $\mathbb{Z}$ tel que deux éléments de R qui sont distincts sont non congrus et tout entier contient un et un seul élément de R dans sa classe.

Toute partie de $\mathbb{Z}$ constitué de n entiers consécutifs est un système complet de résidus modulo n. Souvent, lorsqu'on à résoudre une équation faisant intervenir des congruences dont le modulo est un entier n connu, il suffit d'étudier cette équation dans un système de résidus modulo n.

Exercice 19. Déterminer tous les entiers a tels que $a^2 + a + 1$ est multiple de 3.

Réponse. L'hypothèse se traduit par $a^2 + a + 1 \equiv 0[3]$

Soit a un solution. Pour tout entier b dans la classe de a (c'est à dire $b \equiv a[3]$), on a d'après la proposition 5 item 2 $b^2 + b + 1 \equiv a^2 + a + 1[3]$. b est alors une solution. On peut donc chercher les solutions appartenant au système complet de résidus $\{0, 1, 2\}$.

Si $a = 0, a^2 + a + 1 = 1 \not\equiv 0[3]$. 0 n'est pas solution.

Si $a = 1, a^2 + a + 1 = 3 \equiv 0[3]$. 1 est solution.

Si $a = 2, a^2 + a + 1 = 7 \not\equiv 0[3]$. 2 n'est pas solution.

L'ensemble des solution est 1 et tous les entiers qui lui sont congrus $= \{1 + 3q, q \in \mathbb{Z}\}$.

Si on vouait utiliser la notion de classe, on dirait simplement que l'hypothèse signifie : $\dot{a}^2 + \dot{a} + 1 = 0$. La seule classe qu convient est $\dot{1} = \{1 + 3q, q \in \mathbb{Z}\}$.

□

3.3 Bezout et Gauss modulaires

. Le théorème suivant est la version modulaire du théorème de Bezout.

Théorème 6.

Soit a un entier naturel > 1. Un entier b est premier avec a si et seulement si il existe un entier u tel que $au \equiv 1[b]$. L'entier u est appelé *un* inverse de a modulo n.

Démonstration.

$$\begin{array}{rcl} b \text{ premier avec a} & \Leftrightarrow & a \wedge b = 1 \\ & \Leftrightarrow & \exists u, v \in \mathbb{Z} \ : au + bv = 1 \text{ d'après Bezout} \\ & \Leftrightarrow & \exists u \in \mathbb{Z} \ : au \equiv 1[b] \end{array}$$

□

Exercice 20.

1. Déterminer tous les inverses de 2 modulo 8.
2. Déterminer tous les inverses de 3 modulo 8.

Réponse.

1. u est un inverse de 2 modulo 8 signifie $2u \equiv 1[8] \Leftrightarrow \exists v \in \mathbb{Z} \ : 2u + 8v = 1$ ce qui est impossible puisque $2u + 8v$ est pair. On pouvait s'attendre à ce résultat puisque 2 et 8 ne sont pas premiers entre eux.

2. u est un inverse de 3 modulo 8 signifie $3u \equiv 1[8] \Leftrightarrow \exists v \in \mathbb{Z} \ : 3u + 8v = 1$. C'est une équation diophantienne linéaire. Le couple $(3, -1)$ est une solution de cette équation.

L'ensemble des solutions est donc $\{(8k + 3, -3k - 1), k \in \mathbb{Z}\}$.

Par conséquent l'ensemble des inverse de 3 modulo 8 est $\{8k + 3, k \in \mathbb{Z}\}$. Ainsi par exemple 3 est un inverse de 3 modulo 8 : $3.3 \equiv 1[8]$.

Noter bien que les inverses de 3 modulo 8 constitue une classe : la classe de 11 par exemple. On peut en fait étudier cette équation dans le système complet de congruences modulo 8 ou dans $\mathbb{Z}/8\mathbb{Z}$. Pour cela il suffit il suffit de dresser la table de multiplication de $\mathbb{Z}/8\mathbb{Z}$.

Post quantum RSA

Francois Arnault cours de DEA crypto

Voici par exemple la table de multiplication de $\mathbb{Z}/9\mathbb{Z} \setminus \{\dot{0}, \dot{1}\}$

$\times$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$
$\dot{2}$	$\dot{4}$	$\dot{6}$	$\dot{8}$	$\dot{1}$	$\dot{3}$	$\dot{5}$	$\dot{7}$
$\dot{3}$	$\dot{6}$	$\dot{0}$	$\dot{3}$	$\dot{6}$	$\dot{0}$	$\dot{3}$	$\dot{6}$
$\dot{4}$	$\dot{8}$	$\dot{3}$	$\dot{7}$	$\dot{2}$	$\dot{6}$	$\dot{1}$	$\dot{5}$
$\dot{5}$	$\dot{1}$	$\dot{6}$	$\dot{2}$	$\dot{7}$	$\dot{3}$	$\dot{8}$	$\dot{4}$
$\dot{6}$	$\dot{3}$	$\dot{0}$	$\dot{6}$	$\dot{3}$	$\dot{0}$	$\dot{6}$	$\dot{3}$
$\dot{7}$	$\dot{5}$	$\dot{3}$	$\dot{1}$	$\dot{8}$	$\dot{6}$	$\dot{4}$	$\dot{2}$
$\dot{8}$	$\dot{7}$	$\dot{6}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

On y voit nettement que 3 et 6 ne sont pas inversibles, les inverses de $\dot{2}, \dot{4}, \dot{5}, \dot{7}, \dot{8}$ sont respectivement $\dot{5}, \dot{7}, \dot{2}, \dot{4}, \dot{8}$.

Évidemment pour les "gros" nombres, il n'est pas question d'utiliser cette méthode.

□

Exercice 21. Démontrer que si p est un entier premier, tout entier non multiple de p admet des inverses modulo p.

Voici une traduction du lemme de Gauss en termes de congruences :

Théorème 7 (Simplification)**.**

Soit n un entier naturel supérieur strictement à 1 et a, b et c des entiers.

$$\text{Si } \begin{cases} ac \equiv bc[n] \\ c \wedge n = 1 \end{cases} \text{ alors } a \equiv b[n]$$

Dans $\mathbb{Z}/n\mathbb{Z}$, le lemme se traduit par $$\text{Si } \begin{cases} \dot{a}\dot{c} = \dot{b}\dot{c} \\ c \wedge n = 1 \end{cases} \text{ alors } \dot{a} = \dot{b}$$ On dit que $\dot{c}$ est un élément régulier de $\mathbb{Z}/n\mathbb{Z}$. Il existe des éléments non réguliers. Par exemple, dans $\mathbb{Z}/9\mathbb{Z}, \dot{3}.\dot{1} = \dot{3}.\dot{7}$ mais $\dot{1} \neq \dot{7}$

Démonstration. $ac \equiv bc[n] \Leftrightarrow ac - bc \equiv 0[n] \Leftrightarrow \exists q \in \mathbb{Z} \ : c(a-b) = nq$.

Puisque n divise $c(a-b)$ et est premier avec c, d'après le lemme de Gauss, il doit diviser $a - b$. Il existe donc un entier q' tel que $a - b = nq'$ autrement dit $a \equiv b[n]$ □

Exercice 22. Soit p un entier naturel non nul. Montrer que p est premier si et seulement si tout élément (classe) non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible.

Réponse. Si p est non premier, il a deux diviseurs propres $1 < a \leq b < p$. La relation $ab = p$ entraine $\dot{a}.\dot{b} = \dot{0}$. Alors $\dot{a}$ et $\dot{b}$ sont tous les deux distincts de $\dot{0}$.

Je dis que a est non inversible.

En effet si a était inversible, il existerait $c \in \mathbb{Z}$ tel que $\dot{a}.\dot{c} = \dot{1}$. On pourrait alors écrire en multipliant la relation $\dot{a}.\dot{b} = \dot{0}$ par $\dot{c}$:

$$\dot{b} = \dot{1}.\dot{b} = (\dot{a}.\dot{c})\dot{b} = \dot{c}.(\dot{a}\dot{b}) = \dot{c}.\dot{0} = \dot{0}, \text{ une contradiction}$$

Réciproquement : Supposons p premier. Soit a tel que $\dot{a} \neq \dot{0}$ c'est à dire a non multiple de p. Alors p et a sont premiers entre eux. D'après le théorème 6 (version modulaire de Bezout), a admet un inverse.

□

Corollaire 5 (Petit théorème de Fermat)**.**

Si p est un nombre premier et a est un entier quelconque, alors $$a^{p-1} \equiv 1[p]$$ autrement dit, $a^{p-1} - 1$ est divisible par p.

Démonstration. La relation est vraie si $\dot{a} = 0$ c'est à dire si a est multiple de p.

Supposons donc $\dot{a} \neq \dot{0}$. Alors *a est premier avec p* . Posons $E = \mathbb{Z}/p\mathbb{Z} \setminus \{\dot{0}\}$. C'est un ensemble fini ayant $p - 1$ éléments.

L'application $f : \begin{array}{ccc} E & \to & E \\ \dot{x} & \to & \dot{a}\dot{x} \end{array}$ est alors injective. En effet, pour tout $\dot{x}, \dot{y} \in E$,

$$\begin{array}{rcll} f(\dot{x}) = f(\dot{y}) & \Rightarrow & \dot{a}\dot{x} = \dot{a}\dot{y} & \\ & \Rightarrow & \dot{x} = \dot{y} & \text{d'après le théorème 7 de simplication} \end{array}$$

Puisque E est fini, f est bijective. Par conséquent, $\prod_{\dot{x} \in E} \dot{x} = \prod_{\dot{x} \in E} \dot{a}\dot{x} = \dot{a}^{p-1} \prod_{\dot{x} \in E} \dot{x}$. Une dernière application du théorème 7 permet de simplifier et d'obtenir $\dot{1} = \dot{a}^{p-1}$. □

Remarque 6.

1. Souvent, le théorème est décliné de la manière suivante que l'on obtient en multipliant la congruence par a :
Si p est un nombre premier et a est un entier quelconque, alors $a^p \equiv a[p]$.

2. En théorie des groupes, cela signifie que tout élément du groupe monogène $(E, .)$ est d'ordre $p-1$.
En fait on montre que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est nombre premier.

Exercice 23.

1. Soit p un nombre premier. Montrer que pour tout entier naturel $n, 5^{n+p} - 5^{n+1}$ est divisible par p.

2. a. En utilisant les congruences montrer que, pour tout entier naturel $n, 3^{6n} - 1$ est divisible par 7.

b. Retrouver ce résultat à l'aide du petit théorème de Fermat.

3. Montrer que, pour tout entier naturel a non nul, $a^{13} - a$ est divisible par 26. Indication : Décomposer 26 en produit de facteurs premiers et appliquer la remarque à chacun de ces facteurs.

4 Conséquences

4.1 Critères de divisibilité

Théorème 8.

Soit $b > 2$ un entier et d un diviseur de b. Alors un entier est divisible par d si, et seulement si le dernier chiffre de son écriture en base b est lui-même divisible par d.

Théorème 9.

Soit $b > 2$ un entier et d un diviseur de $b-1$. Alors un entier est divisible par d si, et seulement si la somme des chiffres de son écriture en base b est elle-même divisible par d.

Remarque 7.

- Un entier est divisible par 4 si, et seulement si le nombre formé par ses deux derniers chiffres (en base 10) l'est.
- Un entier est divisible par 11 si, et seulement si la somme des ses chiffres (en base 10) de rang pair diminuée de la somme de ses chiffres de rang impair est divisible par 11.

4.2 Théorème chinois

Le nombre de soldats du général Han Xin est compris entre 10 000 et 10 200. Il sait que s'il range les soldats par 3 il en reste 2. S'il les range par 5, il en reste 3 et s'il les range par 7, il en reste 2. De combien de soldats dispose le général Han Xi ?.

Théorème 10 (Théorème chinois)**.**

Soit $n_1, \ldots, n_k$ des entiers naturels non nuls deux à deux premiers entre eux et $r_1, \ldots, r_k$ des entiers quelconques. Il existe un entier unique modulo $n = n_1 \ldots n_k$ telque

$$\begin{cases} x \equiv r_1[n_1] \\ \ldots\ldots\ldots \\ x \equiv r_k[n_k] \end{cases}$$

Démonstration. avec $n = 3$ pour fixer les idées. *Unicité :* Si x et y sont des solutions du système, alors $\begin{cases} x-y \equiv 0[n_1] \\ x-y \equiv 0[n_2] \\ x-y \equiv 0[n_3] \end{cases}$ Ainsi, $x-y$ est un multiple commun de n_1, n_2 et n_3, donc un multiple de leur ppcm qui n'est rein d' autre que N (puisque les trois nombres, n_1, n_2 et n_3 sont premiers entre eux deux à deux). Donc $x \equiv y[n]$. *Existence :* Pour tout indice i posons $N_i = n_{/ni}$ (c'est le produit de tous les n_j sauf n_i.) Puisque N_i et n_i son premiers entre eux, l'entier N_i a un inverse x_i modulo n_i : $x_i N_i \equiv 1[n_i]$.

Alors on a $\begin{cases} r_1x_1N_1 & \equiv & r_1[n_1] \\ r_2x_2N_2 & \equiv & 0[n_1] \text{ car } N_2 \text{ contient le facteur } n_1 \\ r_3x_3N_3 & \equiv & 0[n_1] \text{ car } N_3 \text{ contient le facteur } n_1 \end{cases}$

En posant $x = r_1x_1N_1 + r_2x_2N_2 + r_3x_3N_3$ et en faisant la somme membre à membre, on voit que $x \equiv r_1[n_1]$. Même raisonnement pour établir les deux autres relations. □

Notons x le nombre de soldats du général. On doit avoir : $\begin{cases} x & \equiv & 2[3] \\ x & \equiv & 3[5] \\ x & \equiv & 2[7] \end{cases}$ Ici $n_1 = 3, n_2 = 5$ et $n_3 = 7$; donc $N_1 = 5 \times 7 = 35, N_2 = 3 \times 7 = 21$ et $N_3 = 3 \times 5 = 15$; Par l'algorithme étendu de Bezout, $x_1 = -1$ est un inverse de 35 modulo $3, x_2 = 1$ est un inverse de 21 modulo $5, x_3 = -1$ est un inverse de 35 modulo 3 et 1 est un inverse de 15 modulo 7. On peut donc prendre comme solution

$$x = r_1x_1N_1 + r_2x_2N_2 + r_3x_3N_3 = 2 \times (-1) \times 35 + 3 \times 1 \times 21 + 2 \times 1 \times 15 = 23$$

ou tout entier y congru à 23 modulo $n_1n_2n_3 = 105$. Un tel entier s'écrit $y = 23 + 105k, k \in \mathbb{Z}$. On doit donc avoir $10000 \leq 23 + 105k \leq 10200$. On trouve $k = 95$ et $y = 10103$.

5 Exercices Bac

Exercice 1 (Bac 2009, remplacement)**.** On rappelle la propriété connue sous le nom de petit théorème de Fermat :

"Si p est un nombre premier et a un entier naturel premier avec p, alors $a^{p-1}-1$ est divisible par p."

1. Prouver à l'aide du petit théorème de Fermat, que $4^{28}-1$ est divisible par 29.

2. Soient a et n deux entiers naturels non nuls.
Démontrer que

$$(a+1)^n \equiv 1^n \ [a].$$

En déduire que $4^n \equiv 1 \ [3]$.

3. Soient a et n deux entiers naturels non nuls.
Démontrer que

$$(a-1)^{2n} \equiv (-1)^{2n} \ [a].$$

En déduire que $4^{4n} \equiv 1 \ [17]$ et $4^{2n} \equiv 1 \ [5]$.

4. A l'aide des questions précédentes, déterminer 4 diviseurs premiers de $4^{28}-1$.

Réponse. [1]

1. En appliquant le petit théorème de Fermat avec $p = 29$ qui est premier et $a = 4$, on peut écrire : $4^{29-1} - 1$ est divisible par 29.

↬ Soient a, b, c, d, p et n des entiers naturels avec p et n non nuls. Alors on a modulo p :

$$\left.\begin{array}{rcl} a & \equiv & c \\ b & \equiv & d \end{array}\right| \Rightarrow a+b \equiv c+d \ ; \qquad \left.\begin{array}{rcl} a & \equiv & c \\ b & \equiv & d \end{array}\right| \Rightarrow ab \equiv cd \ ; \qquad a \equiv c \Rightarrow a^n \equiv c^n$$

Autrement dit, on peut additionner membre à membre des congruences, les multiplier ou les élever à une puissance donnée.

2. On peut donc écrire d'après ce préliminaire et pour tous entiers a et n non nuls :

$$\left.\begin{array}{rcl} a & \equiv & 0 \ [a] \\ 1 & \equiv & 1 \ [a] \end{array}\right| \Rightarrow a+1 \equiv 1 \ [a] \Rightarrow (a+1)^n \equiv 1^n \ [a]$$

On obtient alors la relation demandée $4^n \equiv 1 \ [3]$ en prenant $a = 3$.

3. On a aussi, toujours d'après ce préliminaire et pour tous entiers a et n non nuls :

$$\left.\begin{array}{rcl} a & \equiv & 0 \ [a] \\ -1 & \equiv & -1 \ [a] \end{array}\right| \Rightarrow a-1 \equiv -1 \ [a] \Rightarrow (a-1)^{2n} \equiv (-1)^{2n} \ [a]$$

On en déduit en prenant $a = 17$ que $16^{2n} \equiv 1 \ [17]$ c'est à dire $4^{4n} \equiv 1 \ [17]$

Et en prenant $a = 5$ que $4^{2n} \equiv 1 \ [5]$.

1. Si p est premier, $\left(\mathbb{Z}/p\mathbb{Z} \setminus \{\dot{0}\}; \ .\right)$ est un groupe d'ordre $p-1$ et d'élément neutre $\dot{1}$. Alors $\forall a \in \mathbb{Z}$ et premier avec p (donc non multiple de p ou $\dot{a} \neq \dot{0}$), $\dot{a}^{p-1} = \dot{1}$ c'est à dire $a^{p-1} \equiv 1 \ [p]$

4. On déduit de $4^n \equiv 1\ [3]$ en prenant $n = 28$ que $4^{28} \equiv 1\ [3]$ c'est à dire $4^{28} - 1$ est divisible 3.
On déduit de $4^{4n} \equiv 1\ [17]$ en prenant $n = 7$ que $4^{28} \equiv 1\ [17]$ c'est à dire $4^{28} - 1$ est divisible 17.
On déduit de $4^{2n} \equiv 1\ [5]$ en prenant $n = 14$ que $4^{28} \equiv 1\ [5]$ c'est à dire $4^{28} - 1$ est divisible 5.
En résumé $4^{28} - 1$ est divisible par chacun des quatre nombres premiers $3, 5, 17$ et 29.

□

Exercice 2 (Bac 2010)**.**

On rappelle la propriété connue sous le nom de petit théorème de Fermat : "Si p est un nombre premier et a un entier naturel premier avec p, alors $a^{p-1} \equiv 1[p]$."

1. a. Démontrer que 193 est un nombre premier. 0,75 pt

b. Soit a un entier naturel inférieur à 192. Montrer que $a^{192} \equiv 1[193]$. 0,5 pt

2. On considère l'équation

$$(E) : \quad 83x - 192y = 1 \quad \text{où } x \text{ et } y \text{ sont des entiers relatifs.}$$

a. Vérifier que le couple $(155,\ 67)$ est solution de (E). 0,5 pt

b. Résoudre l'équation (E). 0,75 pt

3. On note A l'ensemble des 193 entiers naturels inférieurs ou égaux à 192 et on considère les deux fonctions f et g définies de la manière suivante :
à tout entier a de A, f associe le reste de la division euclidienne de a^{83} par 193;
à tout entier a de A, g associe le reste de la division euclidienne de a^{155} par 193.

a. Démontrer $g(f(a)) \equiv a^{83\times 155}[193]$. En déduire que pour tout $a \in A$ on a : $g\big(f(a)\big) = a$.
0,5 pt +0,5 pt

b. Déterminer $f \circ g$. 0,5 pt

Réponse.

1. a. Pour que 193 soit premier, il faut et il suffit qu'il soit non divisible par tout nombre premier dont le carré est inférieur à 193. Ces nombres sont 2, 3, 5, 7, 11, 13 et aucun d'eux ne divise 193.

b. 193 étant premier, est premier avec tout entier naturel strictement plus petit, en particulier, il est premier avec 192.
Il suffit d'appliquer le *petit théorème de Fermat* avec $a = 193$ et $p = 192$.

2. a. Le couple $(x_0, y_0) = (155, 67)$ est solution de (E) parce que $83.155 - 192.67 = 1$.

b. Si (x, y) est une solution de (E) on peut écrire :

$$\begin{cases} 83.x_0 - 192.y_0 &= 1 \\ 83.x - 192.y &= 1 \end{cases}$$

Puis en faisant la différence

$$83.(x - x_0) - 192.(y - y_0) = 0$$

c'est à dire

$$83.(x - x_0) = 192.(y - y_0)$$

Or 83 est premier avec 192 parce que l'équation (E) a une solution (*théorème de Bezout*).

La relation précédente montre que 83 divise le produit $192.(y-y_0)$ (en $x-x_0$ parties) ; comme il est premier avec 192, il divise $y-y_0$ *(théorème de Gauss)*.

Donc il existe un entier k tel que $y-y_0=83k$ soit $y=y_0+83k$.

La relation $83.x-192.y=1$ devient alors $83.x=192.(y_0+83k)+1=83.(x_0+192k)$ c'est à dire $x=x_0+192k$.

Ensuite on vérifie que n'importe quel couple du genre (x_0+192k, y_0+83k) est bien une solution de (E).

L'ensemble des solutions de (E) est $\{(155+192k, 67+83k),\ k\in\mathbb{Z}\}$

3. On utilisera la propriété suivante : Si a, b et n sont des entiers tels que

$$a\equiv b[n],$$

alors pour tout entier naturel k on a :

$$a^k\equiv b^k[n]$$

Posons $\mathcal{A}=\{0,\ldots 192\}$. Pour tout $a\in\mathcal{A}$, $f(a)$ et $g(a)$ sont les seuls éléments de $\mathcal{A}$ tels que :

$$f(a)\equiv a^{83}\ [193]\quad (1)$$
$$\text{et } g(a)\equiv a^{155}\ [193]\quad (2)$$

Puisque $g(a)$ appartient à $\mathcal{A}$, dans (2), on peut remplacer a par $f(a)$:

$$g(f(a))\equiv f(a)^{155}\ [193]$$

Dans (1) utilisons la propriété citée avec $k=155$:

$$f(a)^{155}\equiv\left(a^{83}\right)^{155}\ [193]$$

On obtient alors par transitivité de $\equiv$:

$$g(f(a))\equiv a^{83.155}\ [193]\quad (3)$$

a. Reprenons la relation

$$83.x_0+192.y_0=1$$

qui s'écrit aussi :

$$83.x_0=1+192.y_0$$

Cette relation permet d'avoir :

$$a^{83.x_0}=a^{1+192.y_0}=a\ (a^{192})^{.67}$$

Comme nous le savons déjà $a^{192}\equiv 1[193]$. Donc $a^{83.155}=a^{83.x_0}=a^{1+192.y_0}\equiv a.\ 1^{67}[193]$.

Finalement

$$a^{83.155}\equiv a[193]\quad (4).$$

(3) et (4) entraînent par transitivité :

$$g(f(a))\equiv a[193]$$

$g(f(a))$ et a sont des éléments de $\mathcal{A}$ équivalents modulo 193.

Nous allons monter qu'ils sont égaux.

$g(f(a))$ et a sont des éléments de $\mathcal{A}$ entraîne $|g(f(a))-a|\leq 192$

$g(f(a))\equiv a[193]$ signifie il existe un entier k tel que $g(f(a))-a=193k$.

On déduit de ces deux propriétés que $193|k|\leq 192$ c'est à dire $k=0$ ou $g(f(a))=a$.

Le même raisonnement montre que pour tout $a\in\mathcal{A}$, on a : $f(g(a))=a$.

Nous venons de démontrer que $f\circ g=g\circ f=I_{\mathcal{A}}$

□

Exercice 3 (4 points)**.**

1. a. Déterminer les restes respectifs des divisions euclidiennes de 3^1, 3^2, 3^3 par 13.

1 pt

b. En déduire les restes de la division euclidienne par 13 des différentes puissances de 3 à exposants entiers naturels.

1 pt

2. Déterminer les entiers naturels n tels que $A_n = 3^n + 3^{2n} + 3^{3n}$ soit divisible par 13.

1pt

3. Quels sont parmi les nombres 1010100 et 1001001000 écrits dans le système de numération de base 3 ceux qui sont divisibles par 13 ?

1 pt

Réponse.

1. a. Les restes de la division euclidienne de 3^1, 3^2, 3^3 par 13 sont 3, 9, 1

b. Soit $a = 3^n$ une puissance de 3 avec $n \in \mathbb{N}^*$. Si r est le reste de la division euclidienne de n par 3, il existe un entier q tel que $n = 3q + r$.

Ce qui entraîne :

$$\begin{array}{lll} 3^3 & \equiv & 1[13] \\ \Rightarrow \quad (3^3)^q & \equiv & 1^q[13] \\ \Rightarrow \quad 3^{3q} \times 3^r & \equiv & 3^r[13] \\ \Leftrightarrow \quad 3^n & \equiv & 3^r[13] \end{array} .$$

Puisque $0 \leq r \leq 2, 3^r$ vaut $3^0 = 1, 3^1 = 3$ ou $3^2 = 9$.

Les restes de la division euclidienne par 13 des différentes puissances de 3 à exposants entiers naturels sont donc $1, 3$ ou 9.

2. D'après la question précédente, si r est le reste de la division euclidienne de n par 3, alors $3^n \equiv 3^r[13]$

On en déduit que $A_n \equiv 3^r + 3^{2r} + 3^{3r}[13]$.

Si $r = 0$, alors $A_n \equiv 1 + 1 + 1 = 3[13]$ et A_n n'est pas un multiple de 13.

Si $r = 1$, alors $A_n \equiv 3^1 + 3^2 + 3^3 = 39 \equiv 0[13]$ et A_n est un multiple de 13.

Si $r = 2$, alors $A_n \equiv 3^2 + 3^4 + 3^6 \equiv 3^2 + 3^1 + 3^0 = 13 \equiv 0[13]$ et A_n est un multiple de 13.

En résumé pour que $A_n = 3^n + 3^{2n} + 3^{3n}$ soit divisible par 13 il faut et il suffit que n ne soit pas un multiple de 3.

3. Le nombre 1010100 en base 3 s'écrit : $\begin{array}{ll} & 1 \times 3^6 + 0 \times 3^5 + 1 \times 3^4 + 0 \times 3^3 + 1 \times 3^2 + 0 \times 3^1 + 0 \times 3^0 \\ = & 3^6 + 3^4 + 3^2 \\ = & 3^{3n} + 3^{2n} + 3^n \text{ avec } n = 2 \end{array}$

Comme 2 n'est pas multiple de 3, le nombre 1010100 en base 3 est multiple de 13. *Vérification :* l'écriture décimale de 1010100 est 819 et on a bien $819/13 = 63$ Le nombre 1001001000 en base 3 s'écrit :

$\begin{array}{ll} & 1 \times 3^9 + 1 \times 3^6 + 1 \times 3^3 \\ = & 3^{3n} + 3^{2n} + 3^n \text{ avec } n = 3 \end{array}$ Comme 3 est multiple de 3, le nombre 1001001000 en base 3 n'est pas multiple de 13.

Vérification : l'écriture décimale de 1001001000 est 20439 et on a bien $20439/13 = 1572,230769$

□

Exercice 4 (4 pts). On considère la suite (u_n) d'entiers naturels définie par :

$$\begin{array}{ll} u_0 & = 27 \\ \forall n \in \mathbb{N},\ u_{n+1} & = 3u_n - 4 \end{array}$$

1. Calculer u_1, u_2, u_3 et u_4.Quelle conjecture peut-on émettre concernant les deux derniers chiffres de u_n? 2 × 0,25 pts

2. Montrer que pour tout entier naturel n, $u_{n+2} \equiv u_n$ [8].
En déduire que pour tout entier naturel n, $u_{2n} \equiv 3$ [8] et $u_{2n+1} \equiv 5$ [8].

0,25+0,5+0,5 pts

3. Pour tout entier naturel n on pose : $v_n = u_n - 2$.
Montrer que la suite (v_n) est une suite géométrique dont on déterminera le premier terme et la raison.
En déduire que pour tout entier naturel n, $2u_n = 50 \times 3^n + 4$.

$2 \times 0{,}25$ pt

4. Montrer que pour tout entier naturel n, $2u_n \equiv 54\,[100]$.
Déterminer les deux derniers chiffres de l'écriture décimale de u_n suivant les valeurs de n.

0,25 + 0,75 pt

5. Montrer que deux termes consécutifs de la suite (u_n) sont premiers entre eux.

0,75 pt

Réponse.

1. $u_0 = 27$, $u_1 = 77$, $u_2 = 227$, $u_4 = 677$
Conjecturons que les deux derniers chiffres de u_n sont 27 ou 77

2. Puisque le premier terme u_0 est un entier, on montre facilement par récurrence que pour tout $n \in \mathbb{N}^*$, u_n est bien un entier comme l'affirme l'énoncé.
On a pour tout $n \in \mathbb{N}^*$:

$$\begin{array}{rcl} u_{n+2} & = & 3\,u_{n+1} - 4 \\ & = & 3(3\,u_n - 4) - 4 \\ & = & 9\,u_n - 16 \end{array}$$

donc

$$\begin{array}{rcl} u_{n+2} - u_n & = & 8\,u_n - 16 \\ & = & 8(\,u_n - 2) \end{array}.$$

Ainsi $u_{n+2} - u_n$ est un multiple de 8 ; ce qui se traduit par :

$$u_{n+2} \equiv u_n\ [8].$$

En prenant pour n un entier pair $2p$, $p \in \mathbb{N}$ cette relation se traduit par :

$$u_{2(p+1)} \equiv u_{2p}\ [8]$$

c'est à dire en posant pour tout $p \in \mathbb{N}^*$: $u_{2p} = a_p$:

$$a_{p+1} \equiv a_p\ [8].$$

Deux termes consécutifs de la suite (a_p) sont donc congrus modulo 8 ; donc tous les termes sont congrus au premier terme $a_0 = u_0 = 27$ qui lui-même est congru à 3. Conclusion $u_{2n} \equiv 3$ [8]
(On peut aussi utiliser la relation précédente pour faire une récurrence : Le premier terme $a_0 = u_0 = 27$ est congru à 3. Supposons que a_k soit congru à 3 pour tout k appartenant à $\{0, \ldots, n\}$ et montrons que a_{n+1} est congru à 3....).
En prenant pour n un entier impair $2p+1$, $p \in \mathbb{N}$ cette relation se traduit par :

$$u_{2(p+1)+1} \equiv u_{2p+1}\ [8]$$

c'est à dire en posant pour tout $p \in \mathbb{N}^*$: $u_{2p+1} = b_p$:

$$b_{p+1} \equiv b_p\ [8]$$

Deux termes consécutifs de la suite (b_p) sont donc congrus modulo 8 ; donc tous les termes sont congrus au premier terme $b_0 = u_1 = 77$ qui lui-même est congru à 5. Conclusion $u_{2n+1} \equiv 5$ [8].
(On peut aussi utiliser la relation précédente pour faire une récurrence : Le premier terme $b_0 = u_1 = 77$ est congru à 5. Supposons que b_k soit congru à 5 pour tout k appartenant à $\{0, \ldots, n\}$ et montrons que b_{n+1} est congru à 5....).

3. On a pour tout $n \in \mathbb{N}^*$:

$$\begin{aligned} v_{n+1} &= u_{n+1} - 2 \\ &= 3u_n - 6 \\ &= 3(u_n - 2) \\ &= 3v_n. \end{aligned}$$

La suite (v_n) est donc géométrique de raison 3 et de premier terme $v_0 = u_0 - 2 = 25$.
Par conséquent, pour tout $n \in \mathbb{N}^*$: $v_n = 3^n v_0$ c'est à dire $u_n = 2 + 25 \times 3^n$ ou $2u_n = 4 + 50 \times 3^n$

4. De cette relation on déduit $2u_n - 54 = 50(3^n - 1)$, ce qui entraîne : $2u_n - 54 \equiv [50]$
De plus $(3^n - 1)$ est pair parce que 3^n est impair ; donc $2u_n - 54$ est un multiple de $2 \times 50 = 100$ c'est à dire $2u_n - 54 \equiv [100]$.
Cette dernière relation se traduit par : il existe un entier q tel que $2u_n = 54 + 100p$ soit, $u_n = 27 + 50p$. Le nombre $50p$ se terminant par 50 ou 00, le nombre u_n se termine par $27 + 50 = 77$ ou $27 + 00 = 27$

5. Remarquons d'abord que u_n est impair parce que son écriture décimale se termine par 7 ; donc tous ses diviseurs sont impairs.
Soit d un diviseur commun positif de u_{n+1} et u_n. Il existe deux entiers p et q (dépendant de n) tels que $u_{n+1} = pd$ et $u_n = qd$.
La relation $u_{n+1} = 3u_n - 4$ qui définit la suite (u_n) devient $d(3q - p) = 4$. Ainsi d, qui est un nombre impair, divise 4 c'est à dire $d = 1$ et u_{n+1} et u_n sont bien premiers entre eux.
On peut aussi dire : Si a et b sont deux entiers tels qu'il existe deux entiers q et r avec $a = bq + r$ alors $a \wedge b = b \wedge r$ et l'écriture $u_{n+1} = 3u_n - 4$ montre que $u_{n+1} \wedge u_n = u_n \wedge 4 = 1$ la dernière égalité provenant de ce que les seuls diviseurs positifs de 4 sont $1, 2$ et 4 et u_n est impair.

□

Exercice 5 (4 **points**).
On considère la suite (u_n) définie pour tout entier naturel n non nul par :

$$u_n = 2^n + 3 \times 7^n + 14^n - 1.$$

1. a. Calculer u_3

0, 5 pt

b. Montrer que, pour tout entier naturel n non nul, u_n est pair.

0, 5 pt

c. On note $(\mathcal{E})$ l'ensemble des nombres premiers qui divisent au moins un terme de la suite (u_n).
Les entiers $2, 3, 5$ et 7 appartiennent-ils à l'ensemble $(\mathcal{E})$.

0, 5 pt

2. On rappelle le petit théorème de Fermat : « Si p est un nombre premier et q un entier naturel premier avec p, alors $q^{p-1} \equiv 1[p]$.) »
Soit p un nombre premier strictement supérieur à 7.
Soient m et n deux entiers naturels tels que $14 = mn$.

a. Quelles sont les valeurs possibles de m ? 0, 5 pt

b. Montrer que $14 \times m^{p-2} \equiv n$ (modulo p). 0, 5 pt

c. En déduire que $14u_{p-2} \equiv 0$ (modulo p). 0, 5 pt

d. L'entier p appartient-il à l'ensemble $\mathcal{E}$? 0, 5 pt

e. Déterminer $\mathcal{E}$. 0, 5 pt

Réponse.

1. a. $u_3 = 3780$.

b. 2^n et 14^n sont des nombres pairs, 3×7^n produit de nombres impairs, est impair ; donc u_n est un nombre pair.

c. $u_3 = 3780 = 2^2 \times 3^3 \times 5 \times 7$; u_3 est donc divisible par $2, 3, 5$ et 7. Oui $2, 3, 5$ et 7 appartiennent à $\mathcal{E}$.

2. a. Les valeurs possibles de m sont $1, 2, 7, 14$

b. $14 \times m^{p-2} = mn \times m^{p-2} = n \times m^{p-1}$.
p étant premier et *strictement supérieur* à 7, est premier avec m ; donc, d'après le petit théorème de Fermat $m^{p-1} \equiv 1\ [p]$. On obtient, en multipliant par n :

$$14 \times m^{p-2} = n \times m^{p-1} \equiv n\ [p]$$

En appliquant ce résultat à $m = 2,\ 7$ puis 14, on en déduit modulo p :
$14u_{p-2} = (14 \times 2^{p-2}) + 3 \times (14 \times 7^{p-2}) + (14 \times 14^{p-2}) - 14 \equiv 7 + 3 \times 2 + 1 - 14 = 0$

c. Puisque p divise $14u_{p-2}$ et qu'il est premier avec 14, il divise u_{p-2} d'après le théorème de Gauss ; donc $p \in \mathcal{E}$.

d. $2, 3, 5$ et 7 appartiennent à $\mathcal{E}$ et si p est un nombre premier strictement supérieur à 7, il appartient aussi à $\mathcal{E}$.
$\mathcal{E}$ est donc l'ensemble de tous les nombres premiers.

□

Exercice 6.

1. Déterminer l'ensemble des couples (x, y) d'entiers relatifs, solutions de l'équation

$$(E) :\ 8x - 5y = 1.$$

0,5 pt

2. Soit m un entier relatif tel qu'il existe un couple (p, q) d'entiers relatifs vérifiant

$$m = -8p + 4 \text{ et } m = -5q + 3.$$

a. Montrer que le couple (p, q) est solution de l'équation (E) et en déduire que $m \equiv -12\ [40]$.
1 pt = 2 × 0,5 pt

b. Réciproquement si $m \equiv -12\ [40]$, montrer qu'il existe un couple (p, q) d'entiers relatifs vérifiant $m = -8p + 4$ et $m = -5q + 3$.
0,5 pt

c. Déterminer le plus petit des entiers naturels m tels qu'il existe un couple (p, q) d'entiers relatifs vérifiant $m = -8p + 4$ et $m = -5q + 3$. 0,5 pt

3. Un groupe de 8 menuisiers se partage à parts égales m planches de bois, il reste 4 planches qu'ils gardent dans le magasin.
Un autre groupe de 5 menuisiers se partagent le même nombre de planches à parts égales, il reste 3 planches qu'ils gardent dans le magasin.
Quelle est la valeur minimale de m ? 0,75 pt
Les questions qui suivent sont indépendantes de ce qui précède.

4. Soit n un entier naturel.

a. Montrer que pour tout entier naturel k, on a : $2^{3k} \equiv 1\ [7]$. 0,25 pt

b. Quel est le reste de la division euclidienne de 2^{2012} par 7 ? 0,25 pt

5. Soit a et b deux entiers naturels inférieurs ou égaux à 9 avec a non nul.
On considère le nombre $N = a\ 10^3 + b$.
On se propose de déterminer parmi ces nombres N ceux qui sont divisibles par 7.

a. Vérifier que $10^3 \equiv -1\ [7]$. 0,25 pt

b. En déduire tous les entiers naturels N cherchés. 1 pt

Réponse.

1. Pour trouver une solution particulière de l'équation $8x-5y=1$ on peut utiliser l'algorithme habituel ou voir la solution "évidente" $x_0=2$ et $y_0=3$.

Si (x,y) un solution quelconque, on doit avoir $\left\{\begin{array}{rcl} 8x-5y & = & 1 \\ 8x_0-5y_0 & = & 1 \end{array}\right.$ et en faisant la différence $8(x-x_0)-5(y-y_0)=0$ soit $8(x-x_0)=5(y-y_0)$. Par conséquent, 8 divise le produit $5(y-y_0)$ et comme il est premier avec 5, il divise $y-y_0$ d'après le théorème de Gauss ; il existe donc un entier k tel que $y-y_0=8k$ i.e $y=8k+3$. La relation $8(x-x_0)=5(y-y_0)$ entraine $x=5k+2$.

L'ensemble des solutions de l'équation $8x-5y=1$ est $\{(5p+2,8p+3),\ p\in\mathbb{Z}\}$

2. a. S'il existe un couple (p,q) d'entiers relatifs vérifiant $\left\{\begin{array}{rcl} m & = & -8p+4 \\ m & = & -5q+3 \end{array}\right.$, en faisant la différence on obtient $8p-4-5q+3=0$ i.e $8p-5q=1$; le couple (p,q) est bien solution de l'équation.

D'après la question précédente, il existe un entier k tel que $p=5k+2$ et alors $m=-8(5k+2)+4=-40k-12$ i.e $m\equiv -12\ [40]$.

b. Réciproquement si $m\equiv -12\ [40]$, il existe un entier k tel $m=40k-12$.
Alors $m=8(5k-2)+4=8p+4$ avec $p=5k-2$.
Et $m=5(8k-3)+3=5q+3$ avec $q=8k-3$.

c. Pour que m soit un entier naturel, il faut et il suffit que $40k-12$ soit ≥ 0 i.e $k\geq \dfrac{12}{40}$. La plus petite valeur de k est 1 et la plus petite valeur de m est $40-12=28$.

3. Puisque les 8 menuisiers se partagent les planches *à parts égales*, il existe un entier naturel p tel que $m-4=8p$ i.e $m=8p+4$.

De même il existe un entier naturel q tel que $m=5q+3$ et la question précédente entraîne que la valeur minimale du nombre de planches est 28.

4. a. Puisque $8\equiv 1\ [7]$, $2^{3k}=8^k\equiv 1^k\ [7]$; donc on a bien $2^{3k}\equiv 1\ [7]$

b.

$$\begin{array}{rcll} 2^{2012} & = & 2^{3\times 670+2} & \\ & \equiv & 2^2\ [7] & \text{d'après le a.} \end{array}$$

Donc le reste de la division euclidienne de 2^{2012} par 7 est 4.

5. a. Puisque $10^3=1000=7\times 142+6\equiv 6\ [7]\equiv -1\ [7]$.

b. D'après le a. $N=a10^3+b\equiv -a+b\ [7]$. Donc si N est divisible par 7, alors $a\equiv b\ [7]$.
Réciproquement, si $a\equiv b\ [7]$ alors il existe un entier k tel que $a=7k+b$ et

$$N=(7k+b)10^3+b=7\times 10^3k+10^3b+b\equiv 0-b+b\ [7]\equiv 0\ [7]$$

N est donc divisible par 7.

Voici les valeurs possibles de N

a	1	1	2	2	3	4	5	6	7	7	8	8	9	9
b	8	1	9	2	3	4	5	6	0	7	1	8	2	9
N	1008	1001	2009	2002	3003	4004	5005	6006	7000	7007	8001	8008	9002	9009

□

Exercice 7 (2013)**.** On considère l'équation

$$(E) : 5x+6y=29 \text{ où } x \text{ et } y \text{ sont des entiers}$$

1. a. Déterminer un couple d'entiers relatifs (u, v) tel que $5u + 6v = 1$.
En déduire une solution particulière de (E). $2 \times 0.5\,pt$

b. Résoudre dans $\mathbb{Z}^2$ l'équation (E). $0.5\,pt$

Dans l'espace $\mathcal{E}$ muni d'un repère orthonormé $(O, \vec{i}, \vec{j}, \vec{k})$, on considère le plan $\mathcal{P}$ d'équation

$$5x + 6y + 4z = 29$$

Soit $\mathcal{D}$ la droite d'intersection du plan $\mathcal{P}$ et du plan $(O, \vec{i}, \vec{j})$.

c. Représenter graphiquement la droite $\mathcal{D}$ dans le plan $(O, \vec{i}, \vec{j})$.
Montrer que $\mathcal{D}$ a un seul point dont les coordonnées sont des entiers naturels que l'on déterminera. $0.25 + 0,75\,pt$

2. On considère un point M du plan $\mathcal{P}$ dont les coordonnées x, y et z sont des entiers naturels.

a. Montrer que l'entier x est impair. $0.75\,pt$

b. On pose $x = 2p + 1$ où p est un entier naturel.
Montrer que $p + z$ est un multiple de 3. $0.75\,pt$

Réponse.

1. a. le couple $(u, v) = (-1, 1)$ vérifie $5u + 6v = 1$.

On en déduit en mutipliant par 29, que $(x_0, y_0) = (-29, 29)$ est une solution particulière de (E).

b. Si (x, y) est une solution quelconque de (E), on a :

$$\begin{array}{rcl} 5x_0 + 6y_0 & = & 29 \\ 5x + 6y & = & 29 \end{array}$$

et en faisant la différence membre à membre : $5(x - x_0) + 6(y - y_0) = 0$ i.e $5(x - x_0) = -6(y - y_0)$. Donc 6 divise $5(x - x_0)$, et comme il est premier avec 5, il doit diviser $x - x_0$ (théorème de Gaus). Il existe un entier p tel que $x - x_0 = 6p$ et la relation $5(x - x_0) = -6(y - y_0)$ devient $y - y_0 = -5p$.

L'ensemble des solutions de (E) est donc $\{(6p - 29, -5p + 29), p \in \mathbb{Z}\}$

c. La droite $\mathcal{D}$ a pour système d'équations $\left\{ \begin{array}{rcl} 5x + 6y + 4z & = & 29 \\ z & = & 0 \end{array} \right.$.

Par conséquent dans le plan $(O, \vec{i}, \vec{j})$ elle a pour équation $5x + 6y = 29$. Voici sa représentation graphique.

Si M est un point de $\mathcal{D}$ aux coordonnées $(x, y, 0)$ entières, le couple (x, y) est solution de (E).
Si de plus ces entiers sont *positifs* , il existe un entier p tel que

$$x = 6p - 29 \geq 0 \text{ et } y = -5p + 29 \geq 0$$

i.e $29/6 \leq p \leq 29/5$ et $p = 5$.
Il existe donc un seul point de $\mathcal{D}$ ayant ses coordonnées dans $\mathbb{N}^3$.
De plus $x = 6 \times 5 - 29 = 1$ et $y = -5 \times 5 - 29 = 4$.

Les coordonnées de l'unique point de $\mathcal{D}$ dont les coordonnées sont des entiers naturels sont $(1, 4, 0)$ (voir figure).

2. a. Si M est un point de $\mathcal{P}$ aux coordonnées (x, y, z) entières, on doit avoir

$5x = 29 - 6y - 4z$ et comme le deuxième membre de cette égalité est un nombre impair, x doit être impair.

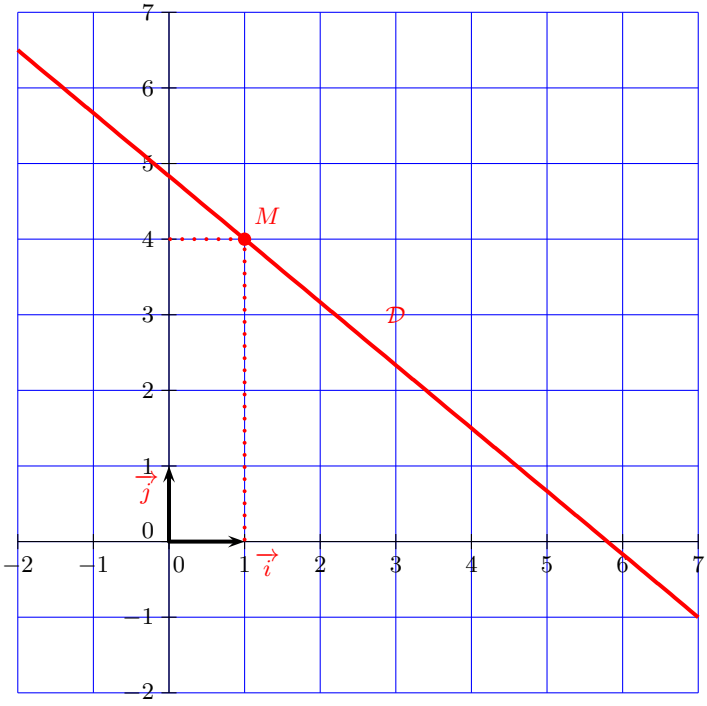

FIGURE 5.1 – La droite $\mathcal{D}$ et son unique point aux coordonnées entiers naturels

b. Si $x = 2p + 1, p \in \mathbb{Z}$, la relation précédente devient : $10p + 4z = -6y + 24$.

Mais $10 \equiv 1[3]$ et $4 \equiv 1[3]$ entraîne $p + z \equiv 10p + 4z = -6y + 24 \equiv 0[3]$

□

Exercice 8 (5 *points*)**.**

1. Soient a, b, c des entiers relatifs et n un entier naturel non nul.

a. Démontrer que a et b sont premiers entre eux si et seulement si a et b^n sont premiers entre eux. 1 *pt*

b. En déduire que si a et b sont premiers entre eux et si a divise le produit $b^n c$, alors a divise c. 0,5 *pt*

2. On se propose dans cette question de déterminer les solutions rationnelles de l'équation suivante :

$$(E) \; : \quad 7x^3 + 2x^2 + 2x - 5 = 0$$

a. Démontrer que l'équation (E) admet une solution réelle unique appartenant à l'intervalle $]0, 1[$. 1 *pt*

b. En utilisant les résultats de la question 1, démontrer que si (E) admet une solution rationnelle $\frac{p}{q}$ où p et q sont des entiers premiers entre eux, alors p divise 5 et q divise 7. 1 *pt*

c. Résoudre l'équation (E) dans $\mathbb{Q}$ ensemble des rationnels. 0,75 *pt*

3. Résoudre l'équation (E) dans $\mathbb{C}$ ensemble des nombres complexes. 0,75 *pt*

Réponse.

1. a. Si $n = 1$, la propriété est triviale. Supposons donc $n \geq 2$.

$$\begin{array}{lll} a \wedge b^n = 1 & \Leftrightarrow & \exists u, v \in \mathbb{Z} \ : au + b^n v = 1 \quad \text{d'après Bezout} \\ & \Rightarrow & au + bv' = 1 \qquad\qquad\quad \text{avec } v' = b^{n-1}v \\ & \Rightarrow & a \wedge b = 1 \end{array}$$

Réciproquement

$$\begin{array}{lll} a \wedge b = 1 & \Leftrightarrow & \exists u, v \in \mathbb{Z} \ : au + bv = 1 \quad \text{d'après Bezout} \\ & \Leftrightarrow & \exists u, v \in \mathbb{Z} \ : bv = 1 - au \\ & \Rightarrow & b^n v^n = (1 - au)^n \\ & \Leftrightarrow & b^n v^n = \displaystyle\sum_{p=0}^{n} C_n^p a^p (-u)^p \end{array}$$

Tous les termes de la somme $\displaystyle\sum_{p=0}^{n} C_n^p a^p (-u)^p$ contiennent le facteur a sauf le premier (correspondant à $p = 0$) qui vaut 1 ; donc cette somme s'écrit $1 + au'$, $u' \in \mathbb{Z}$ et

$$\begin{array}{lll} a \wedge b = 1 & \Rightarrow & b^n v' = 1 + au' \qquad \text{avec } v' = v^n \\ & \Leftrightarrow & -au' + b^n v' = 1 \\ & \Rightarrow & a \wedge b^n = 1 \qquad\quad \text{d'après Bezout} \end{array}$$

b. Si a et b sont premiers entre eux, alors a est premier avec b^n, d'après le a.
Comme a divise le produit $b^n c$, il doit diviser c, d'après Gauss.

2. a. La fonction $f \ : x \mapsto 7x^3 + 2x^2 + 2x - 5$ est définie sur $\mathbb{R}$, continue et dérivable et $\forall x \in \mathbb{R},\ f'(x) = 21x^2 + 4x + 2$.

La dérivée est un polynôme du second degré en x dont le discriminant réduit $2^2 - 42$ est strictement négatif ; la dérivé est alors strictement positive sur $\mathbb{R}$. La fonction f est donc une bijection de $\mathbb{R}$ sur $f(\mathbb{R}) = \mathbb{R}$, cette dernière égalité provenant du fait que $\lim\limits_{x \mapsto +\infty} f(x) = +\infty$ et $\lim\limits_{x \mapsto -\infty} f(x) = -\infty$. L'équation $f(x) = 0$ admet donc une solution réelle unique.

$f(0)f(1) = -30 < 0$ donc la solution réelle de l'équation appartient à $]0, 1[$, d'après le théorème des valeurs intermédiaires.

b. Si p/q est solution de l'équation, on doit avoir $7\dfrac{p^3}{q^3} + 2\dfrac{p^2}{q^2} + 2\dfrac{p}{q} - 5 = 0$ soit, en multipliant par q^3 :

$$7p^3 + 2p^2q + 2pq^2 - 5q^3 = 0$$

Cette relation s'écrit

$$p(7p^2 + 2pq + 2q^2) = 5q^3$$

donc p divise $5q^3$ et d'après la question précédente, p divise 5.

Cette relation s'écrit aussi

$$7p^3 = q(5q^2 - 2pq - 2p^2)$$

donc q divise $7p^3$ et d'après la question précédente, q divise 7.

c. Une éventuelle solution rationnelle de l'équation étant positive, on peut considérer que p et q sont positifs ; alors, les seules valeurs possibles de p sont 1 et 5 et les seules valeurs possibles de q sont 1 et 7. Comme en plus la solution appartient à l'intervalle $]0, 1[$, les seuls candidats solutions sont $1/7$ et $5/7$.

Un calcul direct montrer alors que **l'unique solution rationnelle de l'équation est $5/7$.**

3. Ce qui précède montre que $7x - 5$ est un facteur du polynôme $7x^3 + 2x^2 + 2x - 5$.
En procédant par identification ou par division euclidienne, on obtient

$$7x^3 + 2x^2 + 2x - 5 = (7x - 5)(x^2 + x + 1)$$

les autres solutions de l'équation sont donc celles de $x^2 + x + 1 = 0$.

Le discriminant de cette équation est $-3 = \left(i\sqrt{3}\right)^2$.

Les solutions complexes de l'équation sont donc $5/7$, $j = \dfrac{-1 + i\sqrt{3}}{2}$ et $\overline{j} = \dfrac{-1 - i\sqrt{3}}{2}$

□

Exercice 9 (2017).
Soit a un entier naturel non nul et $(u_n)_{n\in\mathbb{N}}$ la suite définie par : $u_n = \text{pgcd}(n, a)$.

1. a. Pour $a = 15$, calculer les 3 premiers termes de la suite (u_n). 3×0.25 *pt*

b. Pour $a = 4$, soient m et n des entiers naturels tels que $u_m = u_n = 2$.
Montrer que $u_{m+n} = 4$. 0.75 *pt*

2. a. Soit b un entier naturel.
Démontrer que pour tout entier relatif q on a : $\text{pgcd}(a, b) = \text{pgcd}(a, b - qa)$.
0.75 *pt*

b. Calculer u_0 et u_a. 2×0.25 *pt*

c. Démontrer que $u_{n+a} = u_n$.
Quelle propriété de la suite (u_n) a-t-on mise en évidence ? $0.5 + 0.25$ *pt*

3. Pour $a = 15$, calculer u_n avec $n = 15^{21} + 2$. 0.5 *pt*

Réponse. Soit a un entier naturel non nul et $(u_n)_{n\in\mathbb{N}}$ la suite définie par :
$u_n = \text{pgcd}(n, a)$.

1. a. $u_0 = \text{pgcd}\,(0, 15) = 15, u_1 = \text{pgcd}\,(1, 15) = 1, u_2 = \text{pgcd}\,(2, 15) = 1$.

b. Pour $a = 4$, $u_m = u_n = 2$ signifie $\text{pgcd}\,(m, 4) = \text{pgcd}\,(n, 4) = 2$.
m et n sont donc des *nombres paires non multiples de* 4.
Il existe donc des entiers naturels impairs $2m' + 1$ et $2n' + 1$ tels que $m = 2(2m' + 1)$ et $n = 2(2n' + 1)$.
Alors $m + n = 4(m' + n' + 1)$, puis $\text{pgcd}\,(m + n, 4) = 4$ c'est à dire $u_{m+n} = 4$.

2. a. Soit b un entier naturel.
Démontrer que pour tout entier relatif q on a : $\text{pgcd}(a, b) = \text{pgcd}(a, b - qa)$.
Soit d un entier.
Si d est un diviseur commun de a et b, il existe deux entiers m et n tels que $a = dm$ et $b = dn$. Alors $b - qa = d(n - qm)$. Donc d est un diviseur commun de a et $b - qa$.
Réciproquement, si d est un diviseur commun de a et $b - qa$, il existe deux entiers m' et n' tels que $a = dm'$ et $b - qa = dn'$. Alors $b = (b - qa) + qa = d(n' + qm')$. Donc d est un diviseur commun de a et b.
$\{a, b\}$ et $\{a, b - qa\}$ ayant les mêmes diviseurs commun ont le même pgcd.

b. $u_0 = \text{pgcd}\,(0, a) = a$ et $u_a = \text{pgcd}\,(a, a) = a$.

c.
$$\begin{array}{rcl} u_{n+a} & = & \text{pgcd}\,(a, n + a) \\ & = & \text{pgcd}\,(a, n) \text{ d'après le } \textbf{a.} \text{ avec } b = n + a \text{ et } q = -1 \\ & = & u_n \end{array}.$$
Nous venons de démontrer que la suite (u_n) est *périodique et a est une période.*

3. $n = 15^{21} + 2 = 2 + 15m$ avec $m = 15^{20}$ donc
$$\begin{array}{rcl} u_n & = & u_{2+15m} \\ & = & u_2 \text{ car 15 est une période de } (u_n) \\ & = & \text{pgcd}\,(2, 15) \\ & = & 1 \end{array}.$$

□

Table des matières