Chapitre 8

Identité de Bezout

Cryptographie à clé publique (Rivest et al, 1978)

Il s'agit d'un système permettant à tous les membres d'un réseau de coder leurs messages. Seul le chef du réseau qui a fourni la clé du codage possède la clé du décodage de tous les messages.

Le principe est le suivant :

- le chef du réseau choisit deux grands nombres premiers p et q ;
- il calcule $n=pq$ et $\phi(n)=(p-1)(q-1)$;
- il choisit un entier naturel d inférieur à $\phi(n)$ et premier à $\phi(n)$;
- il détermine un entier naturel e tel que $d.e \equiv 1 \pmod{n}$;
- il diffuse aux membres du réseau les nombres n et e, tout en gardant secrets les nombres p, q, $\phi(n)$ et d.

Le codage s'effectue de la manière suivante :

- le message est traduit en nombres N inférieurs à n ;
- chacun de ces nombres N est remplacé par un nombre C défini par $C \equiv N^e \pmod{n}$, c'est ce nombre codé qui est transmis.

Pour procéder au décodage, c'est à dire obtenir N à partir de C, il suffit de calculer C^d.

En effet, d'après le petit théorème de Fermat $C^d \equiv N^{ed} \equiv N^{1+\phi(n)} \equiv N \pmod{n}$.

Ce décodage nécessite la connaissance de d donc de $\phi(n)$.

Si l'on connaît $\phi(n)$, on procède à la recherche du PGCD de $\phi(n)$ et e en utilisant l'algorithme d'Euclide et on écrit les restes successifs en utilisant $\phi(n)$ et e. On aboutit alors à une Identité de Bezout de la forme $d.e + k\phi(n) = 1$, k un entier.

(J-L Chabert et al, Histoire d'algorithmes, 1993).

Chapitre 8

Identité de Bezout

Dans ce chapitre on désigne par $\mathbb{N}$ l'ensemble des entiers naturels et par $\mathbb{Z}$ l'ensemble des entiers.

I. PGCD de deux entiers

Activité 1

Déterminer $a \wedge b$ dans chacun des cas suivants

1. $a = 465$; $b = 225$,
2. $a = 196$; $b = 116$,
3. $a = 144$; $b = 388$.

On rappelle que si a et b sont deux entiers naturels non nuls alors leur plus grand commun diviseur est l'entier naturel $a \wedge b$, tel que $a \wedge b$ divise a et b et tout diviseur commun à a et b divise $a \wedge b$.

Activité 2

Dans cette activité nous nous proposons d'utiliser l'algorithme d'Euclide pour déterminer le plus grand diviseur commun de deux entiers naturels a et b

Le plus grand diviseur commun de deux entiers naturels a et b est le dernier reste non nul dans la succession des divisions euclidiennes de l'algorithme d'Euclide de a et b.

1. Recherche de $4851 \wedge 616$.

En écrivant les divisions successives de l'algorithme d'Euclide pour les entiers 4851 et 616, on obtient $4851 = 616 \times 7 + 539$; $616 = 539 \times 1 + 77$; $539 = 77 \times 7 + 0$.

Le dernier reste non nul étant 77, on en déduit que $4851 \wedge 616 = 77$.

2. Utiliser l'algorithme d'Euclide pour déterminer $a \wedge b$ dans chacun des cas ci-dessous.

1. $19625 \wedge 1155$. 2. $17680 \wedge 4960$. 3. $30870 \wedge 15750$.

Activité 3

On se propose de déterminer le plus grand commun diviseur de deux entiers en utilisant la calculatrice.

1. Recherche de $2003 \wedge 365$

En tapant 2003 $\boxed{ab/c}$ $365 =$, la calculatrice affiche $5 \lrcorner 178 \lrcorner 365$.

Le résultat affiché signifie que $\frac{2003}{365} = 5 + \frac{178}{365}$ et que la fraction $\frac{178}{365}$ est irréductible, ou encore que $365 \wedge 178 = 1$.

La division euclidienne $2003 = 365 \times 5 + 178$ nous permet d'affirmer que $2003 \wedge 365 = 365 \wedge 178 = 1$.

2. Recherche de $4010 \wedge 365$.

En tapant ' 4010 $\boxed{ab/c}$ 365 = ' , la calculatrice affiche $10 \lrcorner 72 \lrcorner 73$.

Ce qui signifie que $\frac{4010}{365} = 10 + \frac{72}{73}$ et que la fraction $\frac{72}{73}$ est irréductible, ou encore que $72 \wedge 73 = 1$

La division euclidienne $4010 = 365 \times 10 + 360$ et les propriétés du plus grand commun diviseur nous permettent d'affirmer que $4010 \wedge 365 = 365 \wedge 360 = 5(73 \wedge 72) = 5$.

3. Utiliser la calculatrice pour déterminer $a \wedge b$ dans chacun des cas ci-dessous.

$a = 8623$ et $b = 1155$; $a = 19662$ et $b = 865$; $a = 4830$ et $b = 3122$.

Activité 4

Soit a et b deux entiers naturels non nuls et d un entier non nul, diviseur commun de $7a + 9b$ et $3a + 4b$.

1. Montrer que d est un diviseur commun de $21a + 27b$ et $21a + 28b$.
   En déduire que d divise b.
2. Montrer que d divise a.
3. Montrer que $(7a + 9b) \wedge (3a + 4b) = a \wedge b$.

Activité 5

Soit a et b deux entiers non nuls et d un entier.

Montrer que d divise a et b, si et seulement si, d divise $|a|$ et $|b|$.

Théorème et définition

Si a et b sont deux entiers non nuls, alors il existe un unique entier naturel d qui vérifie les deux conditions suivantes:

1. d divise a et d divise b,
2. Si un entier k divise a et b alors il divise d.

L'entier d défini plus haut est noté $a \wedge b$ et appelé le plus grand commun diviseur de a et b.

Conséquences

Pour tous entiers a et b non nuls, $a \wedge b > 0$.

Pour tous entiers a et b non nuls, $a \wedge b = |a| \wedge |b|$.

Activité 6

En utilisant la calculatrice, déterminer $a \wedge b$ dans chacun des cas ci-dessous.

1. $a = 462$; $b = -1155$.
2. $a = -196625$; $b = 654$.

L'égalité $a \wedge b = |a| \wedge |b|$ nous permet de généraliser les propriétés du plus grand commun diviseur de deux entiers naturels non nuls à celles du plus grand commun diviseur de deux entiers non nuls.

Propriétés

Soit a et b deux entiers non nuls.

- Si b divise a alors $a \wedge b = |b|$.
- Si b ne divise pas a et si r est le reste modulo b de a alors $a \wedge b = b \wedge r$.
- $a \wedge b = b \wedge a$.
- Pour tout entier non nul k, $ka \wedge kb = |k|(a \wedge b)$.
- $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

Activité 7

1. A l'aide de la calculatrice, déterminer le quotient et le reste de -2921 par 18.
2. Existe-t-il deux entiers a et b tels que $a - b = -2921$ et $a \wedge b = 18$?

II. Entiers premiers entre eux

Définition

Deux entiers non nuls a et b sont dits premiers entre eux, si $a \wedge b = 1$.

Activité 1

Soit n un entier et d un entier naturel non nul.

1. Montrer que si d est un diviseur commun de $n+1$ et $n+9$, alors d divise 8.
2. En déduire que si n est pair alors $(n+1)$ et $(n+9)$ sont premiers entre eux.

Théorème

Soit a et b deux entiers non nuls. Alors il existe un unique couple d'entiers (a', b') tel que $a = (a \wedge b)a'$, $b = (a \wedge b)b'$ et $a' \wedge b' = 1$.

Démonstration

Soit a et b deux entiers non nuls. Posons $d = a \wedge b$.

L'entier d étant un diviseur commun à a et b, il existe deux entiers non nuls a' et b' tels

Que $a = da'$ et $b = db'$. On en déduit que $d = a \wedge b = da' \wedge db' = d(a' \wedge b')$.

Ce qui prouve que $a' \wedge b' = 1$.

L'unicité est évidente.

Activité 2

Déterminer dans chaque cas les entiers premiers entre eux a' et b' tels que

$a = (a \wedge b).a'$ et $b = (a \wedge b).b'$.

1. $a = -60$ et $b = 84$ 2. $a = 77$ et $b = -150$ 3. $a = -240$ et $b = -150$.

Exercice résolu 1

Pour tout entier n, on pose $a = 2n + 5$ et $b = n - 3$.

1. Montrer que tout diviseur commun de a et b est un diviseur de 11.
2. En déduire, suivant les valeurs de n, la valeur de $a \wedge b$.
3. Application

Déterminer $a \wedge b$ lorsque $a = 2 \times 12^{3120} + 5$ et $b = 12^{3120} - 3$.

Solution

1. Si un entier non nul d divise a et b, alors il divise $a - 2b = 11$.
2. D'après la question précédente, tout diviseur commun de a et b est un élément de l'ensemble $\{-11\ ,\ -1\ ,\ 1\ ,\ 11\}$. Il en résulte que $a \wedge b = 11$ ou $a \wedge b = 1$.

Par ailleurs, $n - 3 \equiv 0 \pmod{11}$, si et seulement si, $n \equiv 3 \pmod{11}$ et dans ce cas $2n + 5 \equiv 0 \pmod{11}$.

Il en résulte que $a \wedge b = 11$, si et seulement si, $n \equiv 3 \pmod{11}$.

Par suite, $a \wedge b = 1$, si et seulement si, n n'est pas congru à 3 modulo 11.

3. Les entiers $a = 2 \times 12^{3120} + 5$ et $b = 12^{3120} - 3$ sont de la forme $2n + 5$ et $n - 3$, avec $n = 12^{3120}$.

Les relations $12 \equiv 1 \pmod{11}$ et $12^{3120} \equiv 1 \pmod{11}$ impliquent que $\left(2 \times 12^{3120} + 5\right) \wedge \left(12^{3120} - 3\right) = 1$.

Activité 3

Pour tout entier n, on pose $a = n - 2$ et $b = 3n + 1$. Déterminer $a \wedge b$, suivant les valeurs de n.

Activité 4

Soit a et b deux entiers non nuls tels que $a \wedge b = 1$ et soit c un entier non nul.

1. Justifier que $ac \wedge bc = |c|$.
2. Montrer que si a divise bc alors a divise c.

L'activité précédente permet d'énoncer le théorème ci-dessous.

Lemme de Gauss

Soit a, b et c trois entiers non nuls. Si $a \wedge b = 1$ et a divise bc alors a divise c.

Activité 5

On se propose de résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $(E) : 43x + 71y = 0$.

1. Montrer que si (a, b) est solution de (E) alors 43 divise b et 71 divise a.
2. En déduire l'ensemble des solutions de (E).

Activité 6

Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ les équations ci-dessous.

a. $13x+9y=0$. b. $20x=17y$. c. $21x+35y=0$.

Exercice résolu 2

Soit a et b deux entiers naturels non nuls tels que $a\wedge b=1$.

1. Montrer que $a+b$ et ab sont premiers entre eux.
2. Montrer que $a+b$ et a^2-ab+b^2 sont soit premiers entre eux, soit divisibles par 3.

Solution

1. Soit p un diviseur premier de ab.

   L'égalité $a\wedge b=1$ implique l'une des deux possibilités suivantes:

   ou bien p divise a et ne divise pas b et dans ce cas p ne divise pas $a+b$,

   ou bien p divise b et ne divise pas a et dans ce cas p ne divise pas $a+b$.

   Il en résulte que $a+b$ et ab n'ont aucun diviseur premier commun et alors $(a+b)\wedge ab=1$.

2. On peut écrire $(a+b)^2-\left(a^2-ab+b^2\right)=3ab$. Il en résulte que tout diviseur d commun à $a+b$ et a^2-ab+b^2 divise nécessairement 3ab.

   Les entiers $a+b$ et ab étant premiers entre eux, on déduit du lemme de Gauss que d divise 3, c'est-à-dire $d=1$ ou $d=3$. Ce qui prouve le résultat.

Exercice résolu 3

On se propose de résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation (E): $2x\equiv 12y\ (\text{mod } 10)$.

1. Montrer que si $2x\equiv 12y\ (\text{mod } 10)$ alors $x-y\equiv 0\ (\text{mod } 5)$.
2. a. Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $x\equiv y\ (\text{mod } 5)$.

   b. En déduire les solutions de $2x\equiv 12y\ (\text{mod } 10)$.

Solution

1. a. Un couple (x, y) est solution de $2x\equiv 12y\ (\text{mod } 10)$, si et seulement si, $2x-12y$ est divisible par 10, ou encore, si et seulement si, $2(x-6y)$ est divisible par 10.

Il en résulte que 5 divise $x-6y$ et par suite 5 divise $x-y$ car $x-6y=x-y-5y$.

On en déduit que si $2x\equiv 12y\ (\text{mod } 10)$ alors $x\equiv y\ (\text{mod } 5)$.

2. a Les solutions de l'équation $x\equiv y\ (\text{mod } 5)$ sont tous les couples de la forme $(x, x+5k)$ tels que $x\in\mathbb{Z}$ et $k\in\mathbb{Z}$.

b. D'après ce qui précède si un couple (x, y) est solution de $2x\equiv 12y\ (\text{mod } 10)$ alors ce couple est de la forme $(x, x+5k)$ avec $x\in\mathbb{Z}$ et $k\in\mathbb{Z}$.

Montrons que tout couple de cette forme est solution de (E).
Si $(x, y) = (x, x+5k)$ avec $x \in \mathbb{Z}$ et $k \in \mathbb{Z}$ alors $12(x+5k) = 12x + 60k = 2x + 10(6k+x)$.
Ce qui prouve que $2x \equiv 12y \pmod{10}$.
En conclusion
$2x \equiv 12y \pmod{10}$, si et seulement si, $(x, y) = (x, x+5k)$ avec $x \in \mathbb{Z}$ et $k \in \mathbb{Z}$.

Activité 7

1. Donner une condition nécessaire et suffisante pour qu'un entier soit divisible par 187.
2. Un entier qui est divisible par 2 et par 28 est-il nécessairement divisible par 56 ?
3. Soit a et b deux entiers naturels non nuls et premiers entre eux.
   Montrer que si a divise n et b divise n alors ab divise n.

L'activité précédente nous permet d'énoncer le théorème ci-dessous.

Théorème

Soit a et b deux entiers naturels non nuls et n un entier.
Si $a \wedge b = 1$, $n \equiv 0 \pmod{a}$ et $n \equiv 0 \pmod{b}$ alors $n \equiv 0 \pmod{ab}$.

Activité 8

Déterminer les restes respectifs modulo 13 et modulo 17 de 129286.
En déduire le reste modulo 221 de 129286.

III. PPCM de deux entiers

Activité 1

Soit a et b deux entiers non nuls, $d = a \wedge b$ et a' et b' les entiers tels que $a' \wedge b' = 1$,
$a = da'$ et $b = db'$.
On pose $m = d|a'b'|$

1. Vérifier que m est un multiple commun à a et à b et que tout multiple commun à a et b est un multiple de m.
2. En déduire que m est le plus petit multiple commun strictement positif de a et b.

Théorème et définition

Pour tous entiers a et b non nuls il existe un unique entier m strictement positif qui vérifie les deux conditions suivantes.
- m est un multiple de a et b,
- tout multiple commun de a et b est un multiple de m.

L'entier m ainsi défini est le plus petit commun multiple de a et b et est noté $a \vee b$.

Conséquences

- Pour tous entiers a et b non nuls, $a \vee b = |a| \vee |b|$.
- Pour tous entiers a et b non nuls, $(a \vee b) \times (a \wedge b) = |ab|$.

Cette dernière conséquence nous permet d'affirmer que les propriétés du plus petit commun multiple de deux entiers non nuls sont les mêmes que celles du plus petit commun multiple de deux entiers naturels non nuls.

Propriétés

Soit a et b deux entiers non nuls.

- Si b divise a alors $a \vee b = |a|$.
- Pour tout entier non nul k, $ka \vee kb = |k|(a \vee b)$.
- $a \vee b = b \vee a$.
- $a \vee (b \vee c) = (a \vee b) \vee c$.

Activité 2

Déterminer $a \wedge b$ dans chacun des cas. En déduire $a \vee b$.

1. $a = 495$ et $b = 2541$ 2. $a = -24$ et $b = -56$ 3. $a = 123$ et $b = -82$.

Activité 3

Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ les systèmes ci-dessous.

$$S : \begin{cases} ab = -1176, \\ a \vee b = 84. \end{cases} \qquad S' : \begin{cases} ab = 168, \\ a \vee b = 24. \end{cases}$$

Activité 4

Soit a un entier non nul et $a\mathbb{Z}$ l'ensemble de tous les multiples de a.

1. Déterminer $2\mathbb{Z}$.
2. Déterminer les ensembles E, F et G définis par

$E = \{n \in 6\mathbb{Z} \text{ et } |n| < 31\}$, $F = \{n \in -5\mathbb{Z} \text{ et } |n| < 31\}$ et G l'intersection de E et F.

Activité 5

1. a. Montrer que si $a \equiv 0 \pmod 8$ et $a \equiv 0 \pmod{12}$, alors $a \equiv 0 \pmod{24}$.

   b. La réciproque est-elle vraie ?

2. Déterminer les entiers a vérifiant $\begin{cases} a \equiv 1 \pmod 8, \\ a \equiv 1 \pmod{12}, \\ |a| \leq 225. \end{cases}$

IV. Inverses modulo b

Activité 1

1. Soit u un entier.

   a. Déterminer à l'aide d'un tableau de congruence les restes possibles de 6u modulo 9.

   b. Existe-t-il un entier u tel que $6u \equiv 1 \pmod 9$?

2. Déterminer un entier u tel que $34u \equiv 1 \pmod 7$.

Théorème

Soit a et b deux entiers naturels non nuls tels que $b \geq 2$ et $a \wedge b = 1$.
Alors il existe un unique entier non nul u appartenant à $\{0, 1, ..., b-1\}$ tel que $au \equiv 1 \pmod{b}$. On dit que u est un inverse de a modulo b.

Démonstration

Soit m et n deux entiers.

La congruence $ma \equiv na \pmod{b}$ est équivalente à $(m-n)a \equiv 0 \pmod{b}$.

Les entiers a et b étant premiers entre eux, il résulte de ce qui précède que $ma \equiv na \pmod{b}$, si et seulement si, b divise $m-n$ (*).

Soit i et j deux entiers tels que $0 \leq i < j \leq b-1$. Remarquons que b ne divise pas $j-i$ car $0 < j-i < b$. On déduit alors de (*) que ia et ja ont nécessairement des restes modulo b distincts. Par suite, à chaque élément ia de $E = \{0, a, ..., (b-1)a\}$, il correspond un unique reste appartenant à $\{0, 1, 2, ..., b-1\}$. Ce qui équivaut à dire que la relation $au \equiv 1 \pmod{b}$ possède une unique solution dans $\{0, 1, ..., b-1\}$.

Exercice résolu 4

1. Déterminer un inverse de 4 modulo 13.
2. Résoudre dans $\mathbb{Z}$ l'équation $4x \equiv 1 \pmod{13}$.
3. En déduire les solutions dans $\mathbb{Z}$ de $43x \equiv 1 \pmod{13}$.

Solution

1. Les entiers 4 et 13 étant premiers entre eux, il existe un entier u_0 appartenant à $\{0, 1, 2, ..., 12\}$ tel que $4u_0 \equiv 1 \pmod{13}$.

La division euclidienne $40 = 3 \times 13 + 1$ implique $u_0 = 10$.

2. Si x est solution de $4x \equiv 1 \pmod{13}$ alors $4x \equiv 4u_0 \pmod{13}$, ou encore, $4(x-10) \equiv 0 \pmod{13}$.

Ce qui implique nécessairement que $x \equiv 10 \pmod{13}$ car 13 ne divise pas 4.

Réciproquement, si $x \equiv 10 \pmod{13}$ alors $4x \equiv 1 \pmod{13}$.

Les solutions cherchées sont tous les entiers $x = 10 + 13k,\ k \in \mathbb{Z}$.

3. On vérifie facilement que $43 \equiv 4 \pmod{13}$ et par suite $43x \equiv 4x \pmod{13}$.

Il en résulte que $43x \equiv 1 \pmod{13}$, si et seulement si, $4x \equiv 1 \pmod{13}$.

Les solutions dans $\mathbb{Z}$ de l'équation $43x \equiv 1 \pmod{13}$ sont donc les entiers $x = 10 + 13k,\ k \in \mathbb{Z}$.

V. Identité de Bezout

Activité 1

1. a. Déterminer un inverse de 25 modulo 13.
   b. En déduire deux entiers u et v tels que $25u+13v=1$.
2. Déterminer deux entiers u et v tels que $27u+10v=1$.
3. Déterminer, dans chacun des cas suivants, deux entiers u et v tels que $au+bv=1$.
   $a=9$ et $b=14$; $a=9$ et $b=8$.

Théorème (Identité de Bezout)

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

Démonstration

Nous démontrerons d'abord le théorème dans le cas où a et b sont des entiers naturels premiers entre eux. Puis nous déduirons le cas général.

Supposons que a et b sont deux entiers naturels premiers entre eux et montrons l'existence de deux entiers u et v tels que $au+bv=1$.

Si $b=1$ alors $a\times 0+b\times 1=1$ et les entiers 0 et 1 conviennent.

Si $b>1$ alors la relation $au\equiv 1\ (\text{mod } b)$ possède une unique solution w dans $\{0,1,2,...,b-1\}$ et alors il existe un entier k tel que $aw+bk=1$.

Il suffit donc de prendre $u=w$ et $v=k$.

Réciproquement, supposons qu'il existe deux entiers u et v tels que $au+bv=1$. Alors tout diviseur d commun à a et b divise nécessairement 1, ce qui veut dire que $a\wedge b=1$.

Le théorème est ainsi démontré lorsque a et b sont deux entiers naturels non nuls.

Supposons à présent que a est un entier négatif non nul et b un entier naturel non nul.

On sait d'après ce qui précède qu'il existe deux entiers u et v tels que $(-a)u+bv=1$. On en déduit que $a(-u)+bv=1$. Ce qui démontre le théorème.

Les autres cas se traitent de la même manière.

Corollaire

Soit a et b deux entiers non nuls et $d=a\wedge b$. Alors il existe deux entiers u et v tels que $au+bv=d$.

Démonstration

On sait qu'il existe deux entiers a' et b' tels que $a=(a\wedge b)a'$, $b=(a\wedge b)b'$ et $a'\wedge b'=1$.

D'après le théorème de Bezout il existe deux entiers u et v tels que $a'u+b'v=1$ et alors $da'u+db'v=au+bv=d$.

Exercice résolu 5

1. Montrer que les entiers 22826 et 537 sont premiers entre eux.
2. Trouver deux entiers u et v tels que $22826u+537v=1$.

Solution

1. En tapant ' 22826 ab/c 537 = la calculatrice affiche 42 ⌟ 272 ⌟ 537 .

On en déduit que $22826 \wedge 537 = 272 \wedge 537 = 1$.

2. Nous donnons un procédé pour trouver deux entiers u et v tels que $22826u + 537v = 1$.

On écrit les divisions euclidiennes successives jusqu'à obtenir un reste nul.

Les résultats sont consignés dans le tableau suivant.

r	22826	537	272	265	7	6	1	0
q		42	1	1	37	1	6	

On complète alors le tableau ci-dessous en respectant la loi

		q
α	β	$q\beta + \alpha$
γ	δ	$q\delta + \gamma$

q		42	1	1	37	1	6
0	1	$42\times1+0=42$	$1\times42+1=43$	$1\times43+42=85$	$37\times85+43=3188$	$1\times3188+85=3273$	$6\times3273+3188=22826$
1	0	$42\times0+1=1$	$1\times1+0=1$	$1\times1+1=2$	$37\times2+1=75$	$1\times75+2=77$	$6\times77+75=537$

Les deux dernières colonnes donnent $22826\times77 - 3273\times537 = 1$.

Activité 2

1. Vérifier que 11413 et 191 sont premiers entre eux.
2. Utiliser le procédé de l'exercice précédent pour déterminer deux entiers u et v tels que $11413u + 191v = 1$.

VI. Exemples d'équations de la forme $ax+by=c$; a , b et c entiers

Activité 1

Soit a, b et c trois entiers et $d = a \wedge b$. On considère dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $(E): ax + by = c$.

1. Montrer que si d ne divise pas c alors (E) n'admet pas de solution dans $\mathbb{Z}\times\mathbb{Z}$.

2. Montrer que si d divise c alors (E) admet des solutions dans $\mathbb{Z}\times\mathbb{Z}$.

Théorème

Soit a, b et c trois entiers et $d = a \wedge b$. L'équation $ax + by = c$ admet des solutions dans $\mathbb{Z}\times\mathbb{Z}$, si et seulement si, d divise c.

Activité 2

On se propose de résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $(E): 2x + 3y = 1$.

1. Déterminer une solution particulière (x_0, y_0) de (E).

2. a. Vérifier que (x, y) est solution de (E), si et seulement si, $2(x - x_0) + 3(y - y_0) = 0$.

   b. En déduire les solutions de (E).

3. Soit l'équation $(E_1): 2x+3y=5$.

Montrer que $(5x_0, 5y_0)$ est une solution particulière de (E_1).

Donner alors les solutions de (E_1).

Activité 3

1. Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $7x+11y=1$.
2. En déduire l'ensemble des solutions de chacune des équations suivantes.
   a. $7x+11y=2$.
   b. $7x+11y=-5$.
   c. $7x-11y=-5$.

Activité 4

Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $35x-14y=7$.

Activité 5

On considère dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $(E): 46x+115y=a$ où a est un entier non nul.

1. a. Déterminer $46\wedge 115$.
   b. Déterminer une condition nécessaire et suffisante sur a pour que l'équation (E) admette au moins une solution.
2. Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation (E), dans chacun des cas ci-dessous.
   • $a=23$. • $a=230$. • $a=15$.

Activité 6

1. Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ les équations $5x+3y=1$ et $5x-3y=1$.
2. En déduire les solutions entières de l'équation $25x^2-9y^2=7$.

Problème résolu

Dans le plan muni d'un repère orthonormé $(O,\vec{i},\vec{j})$, on considère les points $A(7,12)$, $B(7,0)$ et $C(0,12)$.

1. a. Déterminer les points de coordonnées entières qui appartiennent à la droite (OA).
   b. En déduire les points de coordonnées entières qui appartiennent au segment $[OA]$.
2. a. Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ les équations $12x-7y=1$ et $12x-7y=-1$.
   b. Montrer qu'à l'intérieur du rectangle ABOC. il existe deux points I et J de coordonnées entières et tels que la distance de chacun d'entre eux à la droite soit minimale.
3. Vérifier que le quadrilatère OIAJ est un parallélogramme et calculer son aire.

Solution

1. On vérifie facilement que la droite (OA) est d'équation $12x-7y=0$.

Déterminer les points M de coordonnées entières appartenant à (OA), revient à résoudre dans $\mathbb{Z}\times\mathbb{Z}$, l'équation $12x-7y=0$.

Les entiers 12 et 7 étant premiers entre eux, il en résulte que (x,y) est une solution de de $12x = 7y$ si et seulement si, 7 divise x, 12 divise y et $y = \frac{12}{7}x$.

On en déduit que les solutions entières de $12y - 7x = 0$ sont les couples $(7k, 12k)$, $k \in \mathbb{Z}$.

b. Un point $M(x,y)$ de (OA) appartient à $[OA]$, si et seulement si, $0 \le x \le 7$ et $0 \le y \le 12$.

Les seuls couples $(7k, 12k)$, $k \in \mathbb{Z}$ qui vérifient les conditions précédentes sont $(0,0)$ et $(7,12)$, donc les seuls points de $[OA]$ de coordonnées entières sont les points O et A.

2. a. L'égalité $12 \times 3 - 7 \times 5 = 1$ implique que $(3,5)$ est une solution particulière de $12x - 7y = 1$.

On en déduit que $12x - 7y = 1$, si et seulement si, $12(x-3) = 7(y-5)$.

Par suite, les solutions entières de $12x - 7y = 1$ sont les couples $(7k+3, 12k+5)$, $k \in \mathbb{Z}$.

L'équation $12x - 7y = -1$ est équivalente à l'équation $12(-x) - 7(-y) = 1$.

Par suite, les solutions entières de $12x - 7y = -1$ sont les couples $(7k'-3, 12k'-5)$, $k' \in \mathbb{Z}$.

b. Soit $M(x,y)$ un point à coordonnées entières intérieur au triangle ABOC.

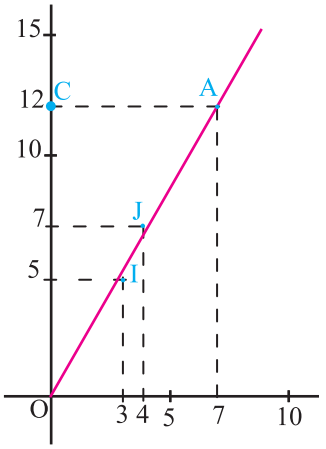
Remarquons que x est un entier strictement compris entre 0 et 7 et y est un entier strictement compris entre 0 et 12.

De plus la distance de M(x,y) à la droite (OA) est minimale, si et seulement si,

$d(M,(OA)) = \frac{|12x - 7y|}{\sqrt{144+49}} = \frac{|12x - 7y|}{\sqrt{193}}$ est minimale.

L'entier non nul $|12x - 7y|$ est minimum lorsqu'il vaut 1.

On en déduit qu'un $M(x,y)$ à coordonnées entières et intérieur au rectangle ABOC se trouve à une distance minimale de (OA), si et seulement si, $12x - 7y = 1$ ou $12x - 7y = -1$, avec les conditions $0 \le x \le 7$ et $0 \le y \le 12$.



Il résulte alors des questions précédentes que seuls les points $I(3,5)$ et $J(4,7)$ répondent à la question.

3. Le milieu S de $[OA]$ a pour coordonnées $\left(\frac{7}{2}, 6\right)$.

On vérifie facilement que S est le milieu de $[IJ]$. Par suite, le quadrilatère OIAJ est un parallélogramme.

De plus, l'aire $\mathcal{A}$ du parallélogramme OIAJ est le double de l'aire $\mathcal{A}'$ du triangle AOI.

On en déduit que $\mathcal{A} = 2\mathcal{A}' = OA \times d(I,(OA)) = \sqrt{193} \times \frac{1}{\sqrt{193}} = 1$.

QCM

Cocher la réponse exacte.

1. L'entier 5 est un inverse modulo 6 de

☐ 5. ☐ -5. ☐ 1.

2. Soit p un nombre premier.

☐ $p \wedge p^2 = 1$. ☐ $p \wedge p^2 = p$. ☐ $p \wedge p^2 = p^2$.

3. L'ensemble des solutions entières de l'équation $11x - 5y = 1$ est

☐ $\{(1+5k, 2+11k), k \in \mathbb{Z}\}$. ☐ $\{(1+11k, 2+5k), k \in \mathbb{Z}\}$. ☐ $\{(2+5k, 1+11k), k \in \mathbb{Z}\}$.

4. L'ensemble des solutions entières de l'équation $13x - 17y = 0$ est

☐ $\{(17k, 13k), k \in \mathbb{Z}\}$. ☐ $\{(13k, 17k), k \in \mathbb{Z}\}$. ☐ $\{(17+13k, 13+17k), k \in \mathbb{Z}\}$.

VRAI - FAUX

Répondre par vrai ou faux en justifiant la réponse.

1. Soit n un entier.

$n \equiv 0 \pmod{143}$, si et seulement si, $n \equiv 0 \pmod{13}$ et $n \equiv 0 \pmod{11}$.

2. Pour tous entiers a et b,

a. $-3a \wedge 3b = 3(a \wedge b)$.

b. Si $a \wedge b = a \vee b$ alors $a = b$.

3. L'équation $25x - 80y = 3$ admet des solutions entières.

4. Tout entier admet un inverse modulo 14.

5. Pour tout entier $n \geq 2$, $(n-1)$ est son propre inverse modulo n.

1 Déterminer $a \wedge b$ dans chacun des cas ci-dessous.

1. $a = 558$ et $b = -1235$.
2. $a = 924$ et $b = 990$.
3. $a = -999$ et $b = 888$.
4. $a = 1890$ et $b = -5250$.

2 Calculer $a \wedge b$ et $a \vee b$ dans chacun des cas ci-dessous.

1. $a = 588$ et $b = -1235$.
2. $a = 51$ et $b = -255$.
3. $a = 2n+1$ et $b = n$, où n est un entier non nul.

3 Trouver les valeurs possibles de l'entier a sachant que $a \wedge 180 = 36$ et $|a| < 360$.

4 Trouver tous les couples (a, b) d'entiers non nuls tels que $a \wedge b = 19$ et $ab = 2166$.

5 Montrer qu'il n'existe aucun couple (a, b) d'entiers tels que $a \wedge b = 19$ et $a^2 - b^2 = 490$.

6 1. Montrer que

$2^5 \equiv -1 \pmod{11}$ et $2^5 \equiv 1 \pmod{31}$.

2. En déduire les congruences

$2^{340} \equiv 1 \pmod{11}$ et $2^{340} \equiv 1 \pmod{31}$.

3. Montrer que 341 divise $2^{340} - 1$.

7 La décomposition de 561 en facteurs premiers est $561 = 3 \times 11 \times 17$.

Soit a un entier premier avec 561.

1. Vérifier que a est premier avec chacun des entiers 3, 11 et 17.
2. Montrer que

a. 3 divise $a^2 - 1$.

b. 11 divise $a^{10} - 1$.

c. 17 divise $a^{16} - 1$.

3. En déduire les congruences

$a^{560} \equiv 1 \pmod{3}$, $a^{560} \equiv 1 \pmod{11}$ et $a^{560} \equiv 1 \pmod{17}$.

3. Montrer que 561 divise $a^{560} - 1$.

8 Soit a, b et d trois entiers non nuls tels que $a \wedge b = d$.

1. Montrer que si un entier n divise $4a + 5b$ et $5a + 2b$ alors n divise 17a et 17b.
2. En déduire que $(4a + 5b) \wedge (5a + 2b) = d$ ou $(4a + 5b) \wedge (5a + 2b) = 17d$.

9 Soit a, b et n trois entiers non nuls.

1. Montrer que si d divise a et b alors d divise $a + bn$ et $a + b(n-1)$.
2. Montrer que si d divise $a + bn$ et $a + b(n-1)$ alors d divise a et b.
3. En déduire que $a \wedge b = (a + bn) \wedge (a + b(n-1))$.

10 1. a. Donner une solution particulière de $5x \equiv 1 \pmod{17}$.

b. En déduire les solutions dans $\mathbb{Z}$ de $5x \equiv 1 \pmod{17}$.

c. Donner les solutions dans $\mathbb{Z}$ de $345x \equiv 1 \pmod{17}$.

2. a. Résoudre dans $\mathbb{Z}$ $5x \equiv 2 \pmod{17}$.

b. Donner les solutions dans $\mathbb{Z}$ de $430x \equiv 2 \pmod{17}$.

11 Résoudre dans $\mathbb{Z}$

a. $17x \equiv 1 \pmod{33}$.

b. $17x \equiv -9 \pmod{33}$.

12 Déterminer l'ensemble des couples (x, y) tels que $12x \equiv 30y \pmod{15}$.

13 Déterminer l'ensemble des couples (x, y) tels que $11x \equiv 99y \pmod{77}$.

14 1. Vérifier que $2015 \wedge 2007 = 1$.
2. Déterminer deux entiers a et b tels que $2007a + 2015b = 1$.

15 1. Vérifier que $391 \wedge 323 = 17$.
2. Déterminer deux entiers a et b tels que $391a - 323b = 17$.
3. En déduire une solution de $391a - 323b = 204$.

16 1. Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $97x + 11y = 1$.
2. Soit l'équation $(E) : 97x + 77y = 7$.
a. Donner une solution particulière de (E).
b. Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation (E).

17 On pose $u = 2 + \sqrt{3}$.
1. a. Montrer par récurrence que, pour tout entier naturel $n \geq 1$, $u^n = a_n + b_n\sqrt{3}$, où a_n et b_n sont des entiers naturels.
b. Exprimer a_{n+1} et b_{n+1} à l'aide de a_n et b_n.
2. a. Montrer que $a_n^2 - 3b_n^2 = 1$ et $a_n b_{n+1} - a_{n+1} b_n = 1$.
b. En déduire que $a_n \wedge b_n = a_{n+1} \wedge a_n = b_{n+1} \wedge b_n = 1$.

18 Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ chacune des équations suivantes.
a. $7x - 14y = 5$. b. $5x - 10y = 10$. c. $29x + 58y = 3$.

19 Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ chacune des équations suivantes.
a. $(4x - 3y - 5)(4x + 3y - 1) = 0$. b. $x^2 - 9y^2 = 2$.

20 1. Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $(E) : 13x - 8y = 1$.
2. On considère les triplets (x, y, z) de $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ vérifiant le système $S : \begin{cases} 5x + y - 2z = 1, \\ 8x - 9y + 2z = 0. \end{cases}$
Montrer que si (x, y, z) est solution de S alors (x, y) est solution de (E). Résoudre S dans $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$.

21 1. Déterminer deux entiers u et v tels que $9u - 11v = 1$.
2. Soit a, b et x trois entiers. Montrer que si $x \equiv a \pmod{9}$ et $x \equiv b \pmod{11}$, alors $x \equiv 45b - 44a \pmod{99}$.
3. Résoudre dans $\mathbb{Z}$ le système $\begin{cases} x \equiv 6 \pmod{9}, \\ x \equiv 8 \pmod{11}. \end{cases}$

22 Pour tout entier n, on considère les nombres $a = 2n - 3$ et $b = 3n - 1$.
1. Quelles sont les valeurs possibles de $a \wedge b$?
2. a. Vérifier que pour tout n, le couple (a, b) est solution de l'équation $(E) : 3x - 2y = -7$.
b. Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation (E).
3. Déterminer l'ensemble des entiers n tels que $a \wedge b = 7$.

23 Soit p, q et u trois nombres premiers.
On pose n = pqu et on suppose que p–1, q–1 et u–1 divisent n–1.
Soit a un entier premier avec n.
1. Montrer que $a^{p-1} \equiv 1 \pmod{p}$, $a^{q-1} \equiv 1 \pmod{q}$ et $a^{u-1} \equiv 1 \pmod{u}$.
En déduire les congruences $a^{n-1} \equiv 1 \pmod{p}$, $a^{n-1} \equiv 1 \pmod{q}$ et $a^{n-1} \equiv 1 \pmod{u}$.
2. Montrer que $a^{n-1} \equiv 1 \pmod{n}$.
3. Décomposer 561 en produit de facteurs premiers et montrer que $224^{560} \equiv 1 \pmod{561}$.
4. Montrer que $561^{1728} \equiv 1 \pmod{1729}$.

24 1. Soit a et b des entiers naturels non nuls tels que $(a+b)\wedge ab = p$, où p est nombre premier.

a. Montrer que p est un diviseur commun de a et b.

b. Montrer que $a\wedge b = p$.

2. On désigne par a et b deux entiers naturels tels que $a \le b$.

a. Résoudre le système $\begin{cases} a\wedge b = 5 \\ a\vee b = 170 \end{cases}$.

b. En déduire les solutions du système $\begin{cases} (a+b)\wedge ab = 5 \\ a\vee b = 170 \end{cases}$.

25 On désigne par x et y deux entiers naturels non nuls tels que $x < y$.

Soit S l'ensemble des couples (x, y) tels que $x\wedge y = y - x$.

1. Calculer $363\wedge 484$.

Le couple $(363, 484)$ appartient-il à S ?

2. Soit n un entier naturel non nul.

Le couple $(n, n+1)$ appartient-il à S ?

3. a. Montrer que (x, y) appartient à S, si et seulement si, il existe un entier naturel k non nul tel que $x = k(y-x)$ et $y = (k+1)(y-x)$.

b. En déduire que pour tout couple (x, y) de S, $x\vee y = k(k+1)(y-x)$.

4. a. Déterminer l'ensemble des entiers naturels diviseurs de 228.

b. En déduire l'ensemble des couples (x, y) de S tels que $x\vee y = 228$.

26 Le plan est rapporté à un repère orthonormé direct $(O, \vec{u}, \vec{v})$. On considère l'application f qui au point M d'affixe z associe le point M' d'affixe z' tel que $z' = \frac{3+4i}{5}\overline{z} + \frac{1-2i}{5}$.

1. a. Déterminer l'ensemble des points invariants par f.

b. Quelle est la nature de f ?

2. a. Déterminer l'ensemble D des points M d'affixe z tels que z' soit réel.

b. Résoudre dans $\mathbb{Z}\times\mathbb{Z}$ l'équation $4x - 3y = 2$.

c. En déduire les points de D dont les coordonnées sont entières.

3. On considère les points M d'affixe $z = 1 + iy$, où $y \in \mathbb{Z}$.

Déterminer les entiers y tels que $\mathrm{Re}(z')$ et $\mathrm{Im}(z')$ soient entiers.

27 Soit a et b deux entiers.

1. Montrer que si $(a^2 + ab - b^2)^2 = 1$ alors a et b sont premiers entre eux.

On considère l'équation $(E) : (x^2 + xy - y^2)^2 = 1$.

2. Déterminer les solutions entières de (E) telles que $x = y$.

3. Soit (p, q) une solution de (E).

a . Montrer que $(q, p+q)$ est une solution de (E).

b. En déduire que $(p+q, p+2q)$ est une solution de (E).

c. Donner six solutions de (E).

28 Le but de l'exercice est déterminer l'ensemble E des triplets (x, y, z) de $\mathbb{N}^*\times\mathbb{N}^*\times\mathbb{N}^*$ tels que $x^2 + y^2 = z^2$.

1. Montrer que pour tout couple (a, b) d'entiers naturels non nuls tels que $a > b$, $(a^2 - b^2, 2ab, a^2 + b^2)$ est un élément de E.

2. Soit (x, y, z) un élément de E tel que $x\wedge y = 1$.

a. Montrer que $x\wedge z = 1$ et $y\wedge z = 1$.

b. Montrer que x et y ne sont pas tous les deux pairs.

c. Montrer que l'équation $a^2 \equiv 2 \pmod 4$ ne possède pas de solution entière.

d. Montrer que si x et y sont tous les deux impairs alors $x^2 + y^2 \equiv 2 \pmod 4$. En déduire que x et y ne peuvent pas être tous les deux impairs.

e. On suppose que x est impair et y est pair.

Montrer que z est impair et que z+x et z-x sont pairs.

En déduire qu'il existe deux entiers strictement positifs p et q, premiers entre eux, tels que $x = p - q$, $z = p + q$ et $y^2 = 4pq$ et p et q sont des carrés parfaits.

3. En déduire l'ensemble des éléments de E.

4. Donner tous les triplets de E tels que $z \le 18$.

29 On considère les dix caractères A, B, C, D, E, F, G, H, I et J auxquels on associe dans l'ordre les entiers de 1 à 10.

On note $\Omega = \{1, 2, 3, ..., 10\}$. On appelle message tout mot ayant un sens ou non formé avec ces dix caractères.

Soit a un entier compris entre 1 et 10. On désigne par f l'application qui à tout élément i de Ω associe le reste de a^i modulo 11.

1. On suppose que a = 5.

a. Coder à l'aide de f le message « BAC » en utilisant la grille de chiffrement ci-dessous

Message	B	A	C
i	2	1	3
$f(i)$	3		
Code	C		

b. Coder à l'aide de f le message « FADE ».

Peut-on déchiffrer avec certitude le message codé ?

2. On suppose que a = 2.

Donner la grille de chiffrement de f.

Peut-on déchiffrer avec certitude un message codé?

3. On se propose de déterminer les valeurs possibles de l'entier a pour que l'application f permette de chiffrer et de déchiffrer avec certitude tous les messages.

a. Soit i et i' deux entiers compris entre 1 et 9 tels que $i < i'$. Montrer que

$a^i \equiv a^{i'} \pmod{11}$ équivaut à $a^{i'-i} \equiv 1 \pmod{11}$.

b. En déduire que f permet de chiffrer et de déchiffrer avec certitude tous les messages , si et seulement si, a^i n'est pas congru à 1 modulo 11 pour tout $i \in \{1, 2, 3, ..., 9\}$.

c. On suppose que k est le plus petit entier de Ω tel que $a^k \equiv 1 \pmod{11}$. Montrer que k est un diviseur de 10.

d. Conclure.

30 On considère la suite de Fibonacci $(F_n)_{n\geq 0}$ définie par $F_0 = 0$; $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$, $n \geq 0$.

1. Calculer les termes de cette suite jusqu'à F_{10}.

2. Montrer que pour tout entier non nul n, $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.

3. En déduire que pour tout entier non nul n, $F_n \wedge F_{n+1} = 1$.

4 . Soit n un entier non nul. Montrer par récurrence sur l'entier m que $F_{n+m} = F_m F_{n-1} + F_{m+1} F_n$.

5. En déduire que $F_m \wedge F_n = F_m \wedge F_{m+n}$.

31 Pour tout entier naturel n, on note $\varphi(n)$ le nombre d'entier naturels inférieurs à n et premiers avec n.

On pose $\varphi(1) = 1$.

1. Vérifier que $\varphi(7) = 6$ et $\varphi(8) = 4$.

2. Montrer que $\varphi(n) \leq n - 1$.

Soit k un entier naturel non nul, p et q deux nombres premiers et a un entier non divisible par p et q.

3. a. Montrer que $\varphi(p) = p - 1$.

b. Montrer que $a^{\varphi(p)} \equiv 1 \pmod{p}$.

4. a. Montrer que $\varphi(pq) = \varphi(p)\varphi(q)$.

b. Montrer que $a^{\varphi(pq)} \equiv 1 \pmod{pq}$.

c. En déduire les congruences ci-dessous

$10^{1536} \equiv 1 \pmod{1649}$;

$10430^{10200} \equiv 1 \pmod{10403}$.

5. a. Montrer que $\varphi(p^k) = p^k - p^{k-1}$.

b. Déterminer $\varphi(125)$, $\varphi(256)$ et $\varphi(1331)$.

6. a. Montrer que $(1+up)^{p^{k-1}} \equiv 1 \pmod{p^k}$

(On pourra utiliser que tout entier non nul n divise C_n^j, $j \neq 0$ et $j \neq n$).

b. Montrer que $a^{\varphi(p^k)} \equiv 1 \pmod{p^k}$.

En déduire les congruences ci-dessous

$17^{100} \equiv 1 \pmod{125}$; $17^{128} \equiv 1 \pmod{256}$.