Chapitre III

Nombres premiers entre eux Théorèmes de Bézout et Gauss

3.1 Donner quelques exemples de nombres premiers entre eux, en démontrant cette propriété par l'algorithme d'Euclide.

3.2 On dit que b est un inverse de a modulo n si $ab \equiv 1[n]$.

1. Prouver que 2 n'a pas d'inverse modulo 6.
2. Déterminer les entiers n tels que 2 ait un inverse modulo n.

3.3 Les théorèmes de Bezout et Gauss sont notamment utilisés pour la résolution des équations *diophantiennes*. Nous allons voir dans cet exercice un exemple de la méthode utilisée pour ce type d'équations.

1. (a) Utiliser l'algorithme d'Euclide pour déterminer d, le PGCD de 24 et 17.
   (b) L'équation $24x + 17y = 1$ admet-elle des solutions dans $\mathbf{Z}$?
   (c) Utiliser les différentes étapes de l'algorithme d'Euclide de la question 1.a. pour exprimer chacun des restes successifs en tant que combinaison linéaire de 24 et 17.
   (d) Déduire de la question précédente deux entiers u_0 et v_0 tels que $24u_0+17v_0 = 1$. Le couple (u_0, v_0) est appelé *solution particulière* de l'équation
   $$24x + 17y = 1.$$
2. Soit (u, v) une autre couple solution de l'équation $24x + 17y = 1$.
   (a) Prouver que $24(u_0 - u) = 17(v - v_0)$.
   (b) Utiliser le théorème de Gauss pour prouver qu'il existe un entier k tel que $v = v_0 + 24k$.
   (c) Utiliser les questions précédentes pour prouver que $u = u_0 - 17k$.
   (d) Vérifier que tous les couples $(u_0 - 17k, v_0 + 24k)$, où k est un entier, sont solutions de l'équation $24x + 17y = 1$.

3.4 On se propose de déterminer les entiers relatifs x vérifiant le système de congruence :

$$\begin{cases} x \equiv 3 \mod 11 \\ x \equiv 4 \mod 15 \end{cases}$$

1. Montrer que la résolution de ce système se ramène a résoudre dans $\mathbf{Z} \times \mathbf{Z}$ l'équation $11u + 15v = 1$.
2. Résoudre cette équation et en déduire les solutions du système.

3.5 Soit $\mathbf{N}^*$ l'ensemble des entiers naturels non nuls. On considère, lorsque n appartient à $\mathbf{N}^*$, les deux entiers a et b définis par $a = 11n + 3$ et $b = 13n - 1$.

1. Démontrer que tout diviseur commun de a et b est un diviseur de 50.
2. Résoudre, pour x appartenant à $\mathbf{N}^*$ et y appartenant à $\mathbf{N}^*$, l'équation $50x - 11y = 3$. En déduire les valeurs de n pour lesquelles les nombres a et b ont 50 pour PGCD.
3. Pour quelles valeurs de n les nombres a et b ont-ils 25 pour PGCD ?

3.6 *Amérique du Nord 4 juin 2009*

Soit A l'ensemble des entiers naturels de l'intervalle $[1\ ;\ 46]$.

1. On considère l'équation
$$(E):\quad 23x + 47y = 1$$
où x et y sont des entiers relatifs.
   (a) Donner une solution particulière $(x_0,\ y_0)$ de (E).
   (b) Déterminer l'ensemble des couples $(x,\ y)$ solutions de (E).
   (c) En déduire qu'il existe un unique entier x appartenant à A tel que $23x \equiv 1 \quad (47)$.
2. Soient a et b deux entiers relatifs.
   (a) Montrer que si $ab \equiv 0 \quad (47)$ alors $a \equiv 0 \quad (47)$) ou $b \equiv 0 \quad (47)$.
   (b) En déduire que si $a^2 \equiv 1 \quad (47)$ alors $a \equiv 1 \quad (47)$ ou a $a \equiv -1 \quad (47)$.
3. (a) Montrer que pour tout entier p de A, il existe un entier relatif q tel que $p \times q \equiv 1 \quad (47)$.
   Pour la suite, on admet que pour tout entier p de A, il existe un unique entier, noté $inv(p)$, appartenant à A tel que $p \times inv(p) \equiv 1 \quad (47)$.
   Par exemple :
   $inv(1) = 1$ car $1 \times 1 \equiv 1 \quad (47)$, $inv(2) = 24$ car $2 \times 24 \equiv 1 \quad (47)$, $inv(3) = 16$ car $3 \times 16 \equiv 1 \quad (47)$.
   (b) Quels sont les entiers p de A qui vérifient $p = inv(p)$?
   (c) Montrer que $46! \equiv -1 \quad (47)$.

3.7 *Asie, juin 2009*

1. On se propose, dans cette question, de déterminer tous les entiers relatifs N tels que
$$\left\{\begin{array}{lll} N & \equiv & 5 \quad (13) \\ N & \equiv & 1 \quad (17) \end{array}\right.$$
   (a) Vérifier que 239 est solution de ce système.
   (b) Soit N un entier relatif solution de ce système.
   Démontrer que N peut s'écrire sous la forme $N = 1 + 17x = 5 + 13y$ où x et y sont deux entiers relatifs vérifiant la relation $17x - 13y = 4$.
   (c) Résoudre l'équation $17x - 13y = 4$ où x et y sont des entiers relatifs.
   (d) En déduire qu'il existe un entier relatif k tel que $N = 18 + 221k$.
   (e) Démontrer l'équivalence entre $N \equiv 18 \quad (221)$ et $\left\{\begin{array}{lll} N & \equiv & 5 \quad (13) \\ N & \equiv & 1 \quad (17) \end{array}\right.$.

2. *Dans cette question, toute trace de recherche, même incomplète, ou d'initiative, même infruxtueuse, sera prise en compte dans l'évaluation.*

   (a) Existe-t-il un entier naturel k tel que $10^k \equiv 1 \quad (17)$?

   (b) Existe-t-il un entier naturel l tel que $10^l \equiv 18 \quad (221)$?

3.8 *Liban, juin 2009*

Le but de l'exercice est de montrer qu'il existe un entier naturel n dont l'écriture décimale du cube se termine par 2009, c'est-à-dire tel que $n^3 \equiv 2009 \bmod 10000$.

Partie A

1. Déterminer le reste de la division euclidienne de 2009^2 par 16.
2. En déduire que $2009^{8001} \equiv 2009 \mod 16$.

Partie B

On considère la suite (u_n) définie sur $\mathbf{N}$ par :
$u_0 = 2009^2 - 1$ et, pour tout entier naturel n, $u_{n+1} = (u_n + 1)^5 - 1$.

1. (a) Démontrer que u_0 est divisible par 5.

   (b) Démontrer, en utilisant la formule du binôme de Newton, que pour tout entier naturel n,
   $$u_{n+1} = u_n \left[{u_n}^4 + 5\left({u_n}^3 + 2{u_n}^2 + 2u_n + 1\right)\right].$$

   (c) Démontrer par récurrence que, pour tout entier naturel n, u_n est divisible par 5^{n+1}.

2. (a) Vérifier que $u_3 = 2009^{250} - 1$ puis en déduire que $2009^{250} \equiv 1 \bmod 625$.

   (b) Démontrer alors que $2009^{8001} \equiv 2009 \bmod 625$.

Partie C

1. En utilisant le théorème de Gauss et les résultats établis dans les questions précédentes, montrer que $2009^{8001} - 2009$ est divisible par 10000.
2. Conclure, c'est-à-dire déterminer un entier naturel dont l'écriture décimale du cube se termine par 2009.

3.9 *Asie, juin 2008*

Soit a et b deux entiers naturels non nuls ; on appelle *réseau* associé aux entiers a et b l'ensemble des points du plan, muni d'un repère orthogonal, dont les coordonnées $(x; y)$ sont des entiers vérifiant les conditions : $0 \leqslant x \leqslant a$ et $0 \leqslant y \leqslant b$. On note $R_{a,b}$ ce réseau.
Le but de l'exercice est de relier certaines propriétés arithmétiques des entiers x et y à des propriétés géométriques des points correspondants du réseau.

Partie A – Représentation graphique de quelques ensembles

Dans cette question, les réponses sont attendues sans explication, sous la forme d'un graphique qui sera dûment complété sur la feuille annexe 1 à rendre avec la copie.
Représenter graphiquement les points $M(x; y)$ du réseau $R_{8,8}$ vérifiant :

1. $x \equiv 2 \pmod 3$ et $y \equiv 1 \pmod 3$, sur le graphique 1 de la feuille annexe
2. $x + y \equiv 1 \pmod 3$, sur le graphique 2 de la feuille annexe ;
3. $x \equiv y \pmod 3$, sur le graphique 3 de la feuille annexe.

Partie B – Résolution d'une équation

On considère l'équation (E) : $7x - 4y = 1$, où les inconnues x et y sont des entiers relatifs.

1. Déterminer un couple d'entiers relatifs $(x_0; y_0)$ solution de l'équation (E).
2. Déterminer l'ensemble des couples d'entiers relatifs solutions de l'équation (E).
3. Démontrer que l'équation (E) admet une unique solution $(x; y)$ pour laquelle le point $M(x; y)$ correspondant appartient au réseau $R_{4,7}$.

Partie C – Une propriété des points situés sur la diagonale du réseau.

Si a et b sont deux entiers naturels non nuls, on considère la diagonale $[OA]$ du réseau $R_{a,b}$, avec $O(0; 0)$ et $A(a; b)$.

1. Démontrer que les points du segment $[OA]$ sont caractérisés par les conditions :

$$0 \leqslant x \leqslant a \ ; \ 0 \leqslant y \leqslant b \ ; \ ay = bx.$$

2. Démonter que si a et b sont premiers entre eux, alors les points O et A sont les seuls points du segment $[OA]$ appartenant au réseau $R_{a,b}$.
3. Démontrer que si a et b ne sont pas premiers entre eux, alors le segment $[OA]$ contient au moins un autre point du réseau.
(On pourra considérer le pgcd d des nombres a et b et poser $a = da'$ et $b = db'$.)

3.10 *Antilles-Guyane, septembre 2003*
Soit l'équation (1) d'inconnue rationnelle x :

$$78x^3 + ux^2 + vx - 14 = 0.$$

où u et v sont des entiers relatifs.

1. On suppose dans cette question que $\dfrac{14}{39}$ est solution de l'équation (1).
   (a) Prouver que les entiers relatifs u et v sont liés par la relation $14x + 39y = 1129$.
   (b) Utiliser l'algorithme d'Euclide, en détaillant les diverses étapes du calcul, pour trouver un couple $(x \ ; \ y)$ d'entiers relatifs vérifiant l'équation $14x + 39y = 1$.
   (c) En déduire un couple $(u_0 \ ; \ v_0)$ solution particulière de l'équation $14u + 39v = 1129$.
   Donner la solution générale de cette équation c'est-à-dire l'ensemble des couples $(u \ ; \ v)$ d'entiers relatifs qui la vérifient.
   (d) Déterminer, parmi les couples $(u \ ; \ v)$ précédents, celui pour lequel le nombre u est l'entier naturel le plus petit possible.
2. (a) Décomposer 78 et 14 en facteurs premiers.
   En déduire, dans $\mathbf{N}$, l'ensemble des diviseurs de 78 et l'ensemble des diviseurs de 14.

(b) Soit $\frac{p}{q}$ une solution rationnelle de l'équation (1) d'inconnue x :

$$78x^3 + ux^2 + vx - 14 = 0$$

où u et v sont des entiers relatifs.
Montrer que si p et q sont des entiers relatifs premiers entre eux, alors p divise 14 et q divise 78.

(c) En déduire le nombre de rationnels, non entiers, pouvant être solutions de l'équation (1) et écrire, parmi ces rationnels, l'ensemble de ceux qui sont positifs.

3.11 *Polynésie, juin 2006*

Pour chacune des cinq propositions suivantes, indiquer si elle est vraie ou fausse et donner une démonstration de la réponse choisie. Une réponse non démontrée ne rapporte aucun point.

1. « pour tout entier naturel n, 3 divise le nombre $2^{2n} - 1$. »
2. « Si un entier relatif x est solution de l'équation $x^2 + x \equiv 0 \pmod{6}$ alors $x \equiv 0 \pmod{3}$. »
3. « l'ensemble des couples d'entiers relatifs $(x\ ;\ y)$ solutions de l'équation $12x - 5y = 3$ est l'ensemble des couples $(4 + 10k\ ;\ 9 + 24k)$ où $k \in \mathbf{Z}$. »
4. « il existe un seul couple $(a\ ;\ b)$ de nombres entiers naturels, tel que $a < b$ et $\text{PPCM}(a,\ b) - \text{PGCD}(a,\ b) = 1$. »

Deux entiers naturels M et N sont tels que M a pour écriture abc en base dix et N a pour écriture bca en base dix.

5. « Si l'entier M est divisible par 27 alors l'entier $M - N$ est aussi divisible par 27. »

3.12 *Antilles-Guyane, juin 2003*

1. (a) Calculer : $\left(1+\sqrt{6}\right)^2$, $\left(1+\sqrt{6}\right)^4$, $\left(1+\sqrt{6}\right)^6$.

   (b) Appliquer l'algorithme d'Euclide à 847 et 342. Que peut-on en déduire ?

2. Soit n un entier naturel non nul. On note a et b les entiers naturels tels que :

$$\left(1+\sqrt{6}\right)^n = a_n + b_n\sqrt{6}.$$

   Que valent a_1 et b_1 ?
   D'après les calculs de la question **1.a.**, donner d'autres valeurs de a_n et b_n.

   (a) Calculer a_{n+1} et b_{n+1} en fonction de a_n et b_n.

   (b) Démontrer que, si 5 ne divise pas $a_n + b_n$, alors 5 ne divise pas non plus $a_{n+1} + b_{n+1}$.
   En déduire que, quel que soit n entier naturel non nul, 5 ne divise pas $a_n + b_n$.

   (c) Démontrer que, si a_n et b_n sont premiers entre eux, alors a_{n+1} et b_{n+1} sont premiers entre eux.
   En déduire que, quel que soit n entier naturel non nul, a_n et b_n sont premiers entre eux.

3.13 *Liban, mai 2003*

Les suites d'entiers naturels (x_n) et (y_n) sont définies sur $\mathbf{N}$ par :

$$\begin{array}{lcl} x_0 = 3 & \text{et} & x_{n+1} = 2x_n - 1 \\ y_0 = 1 & \text{et} & y_{n+1} = 2y_n + 3. \end{array}$$

1. Démontrer par recurrence que pour tout entier naturel n, $x_n = 2^{n+1} + 1$.
2. (a) Calculer le pgcd de x_8 et x_9, puis celui de x_{2002} et x_{2003}. Que peut-on en déduire pour x_8 et x_9 d'une part, pour x_{2002} et x_{2003} d'autre part ?
   (b) x_n et x_{n+1} sont-ils premiers entre eux pour tout entier naturel n ?
3. (a) Démontrer que pour tout entier naturel n, $2x_n - y_n = 5$.
   (b) Exprimer y_n en fonction de n.
   (c) En utilisant les congruences modulo 5, étudier suivant les valeurs de l'entier naturel p le reste de la division euclidienne de 2^p par 5.
   (d) On note d_n le pgcd de x_n et y_n pour tout entier naturel n.
   Démontrer que l'on a $d_n = 1$ ou $d_n = 5$; en déduire l'ensemble des entiers naturels n tels que x_n et y_n soient premiers entre eux.

3.14 *Nouvelle Calédonie, novembre 2002*

On considère deux entiers naturels, non nuls, x et y premiers entre eux.
On pose $S = x + y$ et $P = xy$.

1. (a) Démontrer que x et S sont premiers entre eux, de même que y et S.
   (b) En déduire que $S = x + y$ et $P = xy$ sont premiers entre eux.
   (c) Démontrer que les nombres S et P sont de parités différentes (l'un pair, l'autre impair).
2. Déterminer les diviseurs positifs de 84 et les ranger par ordre croissant.
3. Trouver les nombres premiers entre eux x et y tels que : $SP = 84$.
4. Déterminer les deux entiers naturels a et b vérifiant les conditions suivantes :

$$\left\{ \begin{array}{lcl} a + b & = & 84 \\ ab & = & d^3 \end{array} \right. \quad \text{avec } d = \text{pgcd}(a; b)$$

   (On pourra poser $a = dx$ et $b = dy$ avec x et y premiers entre eux)

3.15 *Polynésie, juin 2002*

n est un entier naturel supérieur ou égal à 2.

1. Montrer que n et $2n + 1$ sont premiers entre eux.
2. On pose $\alpha = n + 3$ et $\beta = 2n + 1$ et on note δ le PGCD de α et β.
   (a) Calculer $2\alpha - \beta$ et en déduire les valeurs possibles de δ.
   (b) Démontrer que α et β sont multiples de 5 si et seulement si $(n-2)$ est multiple de 5.
3. On considère les nombres a et b définis par :

$$\begin{array}{lcl} a & = & n^3 + 2n^2 - 3n \\ b & = & 2n^2 - n - 1 \end{array}$$

   Montrer, après factorisation, que a et b sont des entiers naturels divisibles par $(n-1)$.

4. (a) On note d le PGCD de $n(n+3)$ et de $(2n+1)$. Montrer que δ divise d, puis que $\delta = d$.
   (b) En déduire le PGCD, Δ, de a et b en fonction de n.
   (c) Application :
   Déterminer Δ pour $n = 2001$;
   Déterminer Δ pour $n = 2002$.

3.16 *Polynésie, septembre 2003*

On désigne par p un nombre entier premier supérieur ou égal à 7.
Le but de l'exercice est de démontrer que l'entier naturel $n = p^4 - 1$ est divisible par 240, puis d'appliquer ce résultat.

1. Montrer que p est congru à -1 ou à 1 modulo 3.
   En déduire que n est divisible par 3.
2. En remarquant que p est impair, prouver qu'il existe un entier naturel k tel que $p^2 - 1 = 4k(k+1)$, puis que n est divisible par 16.
3. En considérant tous les restes possibles de la division euclidienne de p par 5, démontrer que 5 divise n.
4. (a) Soient a, b et c trois entiers naturels. Démontrer que si a divise c et b divise c, avec a et b premiers entre eux, alors ab divise c.
   (b) Déduire de ce qui précède que 240 divise n.
5. Existe-t-il quinze nombres premiers p_1, p_2, ..., p_{15} supérieurs ou égaux à 7 tels que l'entier $A = p_1^4 + p_2^4 + ... + p_{15}^4$ soit un nombre premier ?

$\boxed{3.17}$ Devoir maison 3, exercice 1/2

1. Montrer que, pour tout entier naturel non nul k et pour tout entier naturel x :

$$(x-1)\left(1+x+x^2+\cdots+x^{k-1}\right)=x^k-1.$$

Dans toute la suite de l'exercice, on considère un nombre entier a supérieur ou égal à 2.

2. (a) Soit n un entier naturel non nul et d un diviseur positif de n : $n=dk$. Montrer que a^d-1 est un diviseur de a^n-1.
   (b) Déduire de la question précédente que $2^{2004}-1$ est divisible par 7, par 63 puis par 9.
3. Soient m et n deux entiers naturels non nuls et d leur pgcd.
   (a) On définit m' et n' par $m=dm'$ et $n=dn'$. En appliquant le théorème de Bezout à m' et n', montrer qu'il existe des entiers relatifs u et v tels que : $mu-nv=d$.
   (b) On suppose u et v strictement positifs.
   Montrer que : $(a^{mu}-1)-(a^{nv}-1)\,a^d=a^d-1$.
   Montrer ensuite que a^d-1 est le pgcd de $a^{mu}-1$ et de $a^{nv}-1$.
   (c) Calculer, en utilisant le résultat précédent, le pgcd de $2^{63}-1$ et de $2^{60}-1$.

$\boxed{3.18}$ Devoir maison 3, exercice 2/2

1. On considère l'équation

$$(\mathcal{E}) \quad : \quad 17x-24y=9,$$

où $(x,\ y)$ est un couple d'entiers relatifs.
   (a) Vérifier que le couple $(9;6)$ est solution de l'équation $(\mathcal{E})$.
   (b) Résoudre l'équation $(\mathcal{E})$.
2. Dans une fête foraine, Jean s'installe dans un manège circulaire représenté par le schéma donné en annexe. Il peut s'installer sur l'un des huit points indiqués sur le cercle.
   Le manège comporte un jeu qui consiste à attraper un pompon qui, se déplace sur un câble formant un carré dans lequel est inscrit le cercle. Le manège tourne dans le sens des aiguilles d'une montre, à vitesse constante. Il fait un tour en 24 secondes. Le pompon se déplace dans le même sens à vitesse constante. Il fait un tour en 17 secondes.
   Pour gagner, Jean doit attraper le pompon, et il ne peut le faire qu'aux points de contact qui sont notés A, B, C et D sur le dessin.
   A l'instant $t=0$, Jean part du point H en même temps que le pompon part du point A.

   (a) On suppose qu'à un certain instant t Jean attrape le pompon en A. Jean a déjà pu passer un certain nombre de fois en A sans y trouver le pompon. A l'instant t, on note y le nombre de tours effectués depuis son premier passage en A et x le nombre de tours effectués par le pompon. Montrer que (x,y) est solution de l'équation $(\mathcal{E})$ de la question 1.
   (b) Jean a payé pour 2 minutes ; aura-t-il le temps d'attraper le pompon ?

(c) Montrer, qu'en fait, il n'est possible d'attraper le pompon qu'au point A.

(d) Jean part maintenant du point E. Aura-t-il le temps d'attraper le pompon en A avant les deux minutes ?