le cnam

Algèbre de Boole, probabilités et arithmétique

Cours 6 Division euclidienne

- Entiers relatifs

Nous ne présentons pas ici la construction de l'ensemble $\mathbb{Z}$ des entiers, ou entiers relatifs. On augmente simplement l'ensemble $\mathbb{N}$ des entiers naturels de leurs opposés et
$\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N}) = \{ \ ... \ -3, -2, -1, 0, 1, 2, 3, \ ... \ \}$.
Surtout, tout entier relatif a un opposé : $\forall a \in \mathbb{Z}, \ \exists ! \, b \in \mathbb{Z}, \ a+b=0$. L'opposé b du nombre a défini par la relation $a+b=0$ est noté "$-a$", comme nous l'avons vu plus haut avec les entiers 1, 2 ou 3.
On peut étendre la multiplication des entiers naturels aux entiers relatifs. On voit alors émerger la règle des signes : $(-a)(-b) = ab$.
L'inégalité $(a \leq b)$ entre deux entiers est définie de la façon suivante : on a $(a \leq b)$ si et seulement si $((b-a) \in \mathbb{N})$. On utilisera librement les autres inégalités comme
$a \geq b$ $[(a \geq b) \Leftrightarrow (b \leq a)]$, $a < b$ $[(a < b) \Leftrightarrow (a \leq b) \, \text{et} \, (a \neq b)]$ ou
$a > b$ $[(a > b) \Leftrightarrow (a \geq b) \, \text{et} \, (a \neq b)]$ ainsi que les règles de calcul sur les inégalités : ajout d'un même nombre de part et d'autre, multiplication par un même nombre positif, multiplication par un même nombre négatif en changeant le signe de l'inégalité.
La valeur absolue $|a|$ d'un entier $a \in \mathbb{Z}$ est un entier positif défini par $|a| = a$ si a est positif, c'est à dire $a \in \mathbb{N}$, et $|a| = -a$ si a est négatif. On a par exemple $|-2| = 2 = -(-2)$. La valeur absolue d'un produit est égale au produit des valeurs absolues : $|ab| = |a| \, |b|$ pour tous les entiers a et b. L'inégalité triangulaire exprime que la valeur absolue d'une somme est inférieure ou égale à la somme des valeurs absolues : $|a+b| \leq |a| + |b|$ pour tous les entiers a et b. On en déduit facilement [exercice !] qu'on a une propriété analogue avec la différence : $|a-b| \leq |a| + |b|$. Enfin, si la valeur absolue est nulle, alors son argument est nul : $(|a| = 0) \Rightarrow (a = 0)$.
Le nombre 1 est un élément neutre pour la multiplication des entiers :
$\forall a \in \mathbb{Z}, \ a \times 1 = 1 \times a = a$. On dit que l'entier x est inversible s'il existe un autre entier y de sorte que $xy = 1$. Le nombre y est appelé "inverse" de l'entier x. On démontre que les seuls entiers inversibles sont les nombres 1 et (-1).

- Une propriété importante des entiers naturels

L'ensemble des entiers est "discret". Ceci entraîne une propriété en apparence très simple qui est mise en défaut si on s'intéresse aux nombres rationnels (les fractions) ou aux nombres réels (nombres avec une infinité de décimales).
Dans l'ensemble $\mathbb{N}$ des entiers naturels, toute partie non vide majorée a un plus grand élément. Soit $A \subset \mathbb{N}$, $A \neq \varnothing$. On dit que A est majorée si et seulement si $\exists b \in \mathbb{N}, \ \forall x \in A, \ x \leq b$.

L'entier b est un majorant de l'ensemble A. Par exemple, l'ensemble des nombres impairs inférieurs ou égaux à 100 est une partie majorée de $\mathbb{N}$; le nombre $b = 100$ est un majorant de cet ensemble. La propriété énonce qu'un tel sous-ensemble non vide majoré des nombres entiers admet un plus grand élément : $\exists M \in A,\ \forall x \in A,\ x \leq M$. On ne dit rien de l'ensemble où vit le majorant b; par contre le plus grand élément M de l'ensemble A appartient à l'ensemble A. Pour l'exemple considéré plus haut, le plus grand élément M vaut $M = 99$.
On a une propriété analogue avec le plus petit élément. Dans l'ensemble $\mathbb{N}$ des entiers naturels, toute partie non vide a un plus petit élément. Il n'y a pas de condition supplémentaire car l'ensemble $\mathbb{N}$ est minoré : $\forall x \in \mathbb{N},\ x \geq 0$. Si on a $A \subset \mathbb{N}$, $A \neq \varnothing$, alors
$\exists m \in A,\ \forall x \in A,\ x \geq m$. Par exemple l'ensemble des nombres impairs a un plus petit élément ; on a $m = 1$ dans ce cas.

- Division euclidienne

La division euclidienne est une division entre nombres entiers "qui ne tombe pas toujours juste". On se donne un entier $a \in \mathbb{Z}$ et un entier naturel $b \geq 1$. Alors il existe un couple unique $(q, r) \in \mathbb{Z} \times \mathbb{N}$ de sorte que $a = bq + r$ et $0 \leq r \leq b - 1$. Le nombre a est appelé "dividende". Le nombre b est le "diviseur" ; il est toujours supérieur ou égal à 1. Le nombre q est le "quotient" ; il n'est soumis à aucune condition particulière *a priori*. Enfin, le "reste" r est un entier naturel strictement inférieur au diviseur b. Rappelons que le livre d'Euclide, *Les Éléments*, date du troisième siècle avant l'ère chrétienne.
Par exemple $10 = 3 \times 3 + 1$. On a $0 \leq 1 \leq 2 = 3 - 1$. Donc le quotient de la division euclidienne de 10 par 3 vaut 3 et le reste vaut 1.
Si le reste est nul, la division tombe juste. On dit surtout que "a est un multiple de b" ou que "b divise a", qui se note $b|a$.
La preuve de ce théorème commence par l'existence du quotient si $a \in \mathbb{N}$. L'ensemble
$A = \{a - b\ell, \ell \in \mathbb{N}\} \cap \mathbb{N}$ est une partie non vide de l'ensemble des entiers naturels (prendre $\ell = 0$) et admet donc un plus petit élément q: on a donc $a - b(q+1) < 0 \leq a - bq$. On en déduit $a - bq - b \leq -1$ et si on pose $r = a - bq$, on a la double inégalité $0 \leq r \leq b - 1$. L'unicité résulte de la condition $0 \leq r \leq b - 1$. Il n'y a qu'un seul multiple k de b qui satisfait à la double condition $-(b-1) \leq k \leq (b-1)$: c'est le nombre $k = 0$. Enfin, si $a \leq -1$, on se ramène au cas précédent : il existe q' et r' de sorte que $-a = bq' + r'$. On pose $q = -q'$ et $r = r'$ si $r' = 0$. Si $r' \geq 1$, $q = -q' - 1$ et $r = b - r'$ satisfont aux deux conditions $a = bq + r$ et $0 \leq r \leq b - 1$.

- Ensemble des diviseurs d'un entier naturel

On se donne un entier naturel $n \in \mathbb{N}$. L'ensemble $D(n)$ de ses diviseurs est par définition l'ensemble des entiers naturels qui divisent l'entier n: $D(n) = \{d \in \mathbb{N}, \exists \ell \in \mathbb{N}, n = d\ell\}$.
On a $D(0) = \mathbb{N}$ car pour tout entier d, on a $d \times 0 = 0$. Remarquons que $D(1) = \{1\}$ est un singleton. Pour les deux nombres suivants, on trouve une paire : $D(2) = \{1, 2\}$ et
$D(3) = \{1, 3\}$. On a $D(4) = \{1, 2, 4\}$, puis on retrouve une paire pour $D(5) = \{1, 5\}$ et $D(7) = \{1, 7\}$. Enfin $D(6) = \{1, 2, 3, 6\}$ et $D(8) = \{1, 2, 4, 8\}$.
Un nombre $p \in \mathbb{N}$ est dit "premier" lorsque l'ensemble de ses diviseurs est une paire. On observe que 1 n'est pas premier puisque $D(1)$ est un singleton. Par contre, le nombre 1 est

inversible dans $\mathbb{Z}$, ce qui n'est pas le cas des nombres premiers. On retiendra le début de la liste des nombres premiers : $2, 3, 5, 7, 11, 13,$ *etc*.

- Plus grand commun diviseur [pgcd]

Commençons par considérer l'exemple suivant : on a $D(24) = \{1, 2, 3, 4, 6, 8, 12, 24\}$ et $D(54) = \{1, 2, 3, 6, 9, 18, 27, 54\}$. L'intersection $D(24) \cap D(54)$ s'évalue sans difficulté : $D(24) \cap D(54) = \{1, 2, 3, 6\}$. C'est une partie non vide de $\mathbb{N}$ puisqu'elle contient le nombre 1. De plus, elle est majorée par 24 par exemple. Elle admet donc un plus grand élément, le nombre 6 dans l'exemple considéré. Le nombre 6 est le "plus grand commun diviseur" de 24 et 54. On écrit $\text{pgcd}\,(24, 54) = 6$.

De façon générale, on se donne deux entiers n et m supérieurs ou égaux à 1. Alors l'intersection $D(n) \cap D(m)$ de leurs diviseurs est une partie non vide de $\mathbb{N}$ puisqu'elle contient toujours le nombre 1. Elle est de plus majorée par chacun des deux nombres n et m. Elle admet donc un plus grand élément, le plus grand commun diviseur des enters n et m: $\text{pgcd}\,(n, m)$, noté aussi $n \wedge m$.

On a bien sûr $n \wedge m = m \wedge n$ et l'intersection $D(n) \cap D(m)$ de l'ensemble des diviseurs de deux entiers est aussi l'ensemble des diviseurs de leur pgcd : $D(n) \cap D(m) = D(n \wedge m)$.

- Nombres premiers entre eux

On dit par définition que deux entiers n et m supérieurs ou égaux à 1 sont "premiers entre eux" lorsque leur plus grand commun diviseur est égal à 1. On a l'équivalence
$\big((n \wedge m = 1) \Leftrightarrow (D(n) \cap D(m) = \{1\})\big)$.

On a par exemple $D(8) = \{1, 2, 4, 8\}$ et $D(15) = \{1, 3, 5, 15\}$. On constate que l'interserction $D(8) \cap D(15)$ est réduite au singleton $\{1\}$. Les nombres 8 et 15 sont premiers entre eux. On remarque que dans cet exemple, aucun des nombres 8 et 15 n'est premier. Malgré la proximité des dénominations, il ne faut pas confonde "nombre premier" et "nombres premiers entre eux".

- Algorithme d'Euclide pour le calcul du pgcd

On a vu que $24 \wedge 54 = 6$. L'algorithme d'Euclide permet de calculer ce pgcd par une suite de divisions euclidiennes. On a d'abord $54 = (24 \times 2) + 6$. Puis on divise 24 par 6 :
$24 = (6 \times 4) + 0$. Lorsque le reste est nul, le dernier diviseur, c'est à dire le reste de la précédente division euclidienne, est égal au plus grand commun diviseur des deux nombres.

Dans le cas général de deux nombres entiers a et b supérieurs ou égaux à 1, on suppose pour fixer les idées que $a \geq b$ et on fait la division euclidienne de a par b: $a = bq + r$ avec
$0 \leq r \leq b - 1$. Si $r = 0$, alors $a = bq$ et b divise a. Tout diviseur de b est donc un diviseur de a, $D(b) \subset D(a)$ et $\text{pgcd}\,(a, b) = b$.

Si $r \neq 0$, alors $\text{pgcd}\,(a, b) = \text{pgcd}\,(b, r)$. En effet, si l'entier d divise à la fois a et b, alors il divise le reste r et $(D(a) \cap D(b)) \subset D(r) \subset (D(b) \cap D(r))$. Réciproquement, l'entier d divise à la fois b et r, alors il divise $bq + r = a$ donc il divise a. On en déduit que
$(D(b) \cap D(r)) \subset D(a)$. Comme $(D(b) \cap D(r)) \subset D(b)$, on a $(D(b) \cap D(r)) \subset (D(a) \cap D(b))$.
Les deux inclusions $(D(a) \cap D(b)) \subset (D(b) \cap D(r))$ et $(D(b) \cap D(r)) \subset (D(a) \cap D(b))$ établies ci-dessus montrent l'égalité $(D(a) \cap D(b)) = (D(b) \cap D(r))$, c'est à dire $\text{pgcd}\,(a, b) = \text{pgcd}\,(b, r)$.
On effectue ensuite la division euclidienne de b par r.

On formalise l'algorithme. On pose $r_0 = a$, $r_1 = b$, $r_2 = r$ qui vient d'être étudié au paragraphe précédent. On a $r_0 = r_1 q_1 + r_2$ avec $0 \leq r_2 \leq r_1 - 1$. On a ensuite $r_1 = r_2 q_2 + r_3$ avec $0 \leq r_3 \leq r_2 - 1$. De proche en proche, on construit une suite de quotients q_ℓ et de restes r_ℓ de sorte que $r_{\ell-1} = r_\ell \, q_\ell + r_{\ell+1}$ avec $0 \leq r_{\ell+1} \leq r_\ell - 1$. On a comme plus haut,
$\text{pgcd}\,(r_0, r_1) = \text{pgcd}\,(r_1, r_2) = ... = \text{pgcd}\,(r_{\ell-1}, r_\ell)$. La suite d'entiers positifs $(r_\ell)_{\ell \in \mathbb{N}}$ est strictement décroissante donc finit par être nulle pour un certain rang : $0 = r_{k+1} \leq r_k - 1$. Dans ce cas $r_{k-1} = r_k \, q_k$ et $\text{pgcd}\,(r_{k-1}, r_k) = r_k$. Le pgcd des deux nombres a et b est le dernier reste non nul dans la suite des divisions des restes successifs.
On peut par exemple appliquer l'algorithme d'Euclide au couple de nombres $(114, 35)$. Avec des divisions euclidiennes successives, on a $114 = (3 \times 35) + 9$, $35 = (3 \times 9) + 8$,
$9 = (1 \times 8) + 1$ et enfin $8 = 8 \times 1$ et le dernier reste est nul. Le pgcd des deux nombres 114 et 35 est égal au dernier diviseur ou bien l'avant dernier reste, c'est à dire 1 ici.

- Identité de Bézout (Étienne Bézout, 1730-1783)

Le fait que deux entiers a et b $(a \geq 1$ et $b \geq 1)$ sont premiers entre eux se caractérise par une égalité, dite "identité de Bézout". Elle fait intervenir deux entiers relatifs u et v de sorte que $a\,u + b\,v = 1$. Le théorème énonce que $(a \wedge b = 1)$ si et seulement si
$\big(\exists (u, v) \in \mathbb{Z}^2,\ a\,u + b\,v = 1\big)$. On remarque que les entiers u et v ne sont pas uniques.
Par exemple, on a vu que $8 \wedge 15 = 1$. Étudions l'algorithme d'Euclide dans ce cas particulier : $15 = (8 \times 1) + 7$, puis $8 = (7 \times 1) + 1$ et enfin $7 = (1 \times 7) + 0$; le pgcd de 8 et 15 est bien égal à 1. On déduit de ces égalités : $1 = 8 - 7 = 8 - (15 - 8) = -15 + 2 \times 8$, ce qui établit l'identité de Bézout dans ce cas particulier avec $u = -1$ et $v = 2$.
Dans le cas général, on se donne deux entiers a et b supérieurs ou égaux à 1 de sorte que $a \wedge b = 1$. On peut d'abord supposer que ce pgcd a été obtenu dès la première division euclidienne de a par b : alors $a = b\,q + 1$. L'identité de Bézout est satisfaite avec $u = 1$ et $v = -q$.
Dans le cas général, on écrit l'algorithme d'Euclide qui conduit à un dernier reste égal à zéro : $r_0 = r_1 \, q_1 + r_2$ avec $0 \leq r_2 \leq r_1 - 1$, $r_1 = r_2 \, q_2 + r_3$ avec $0 \leq r_3 \leq r_2 - 1$, ... , $r_{\ell-1} = r_\ell \, q_\ell + r_{\ell+1}$ avec $0 \leq r_{\ell+1} \leq r_\ell - 1$, ... , $r_{k-2} = r_{k-1} \, q_{k-1} + r_k$ avec $0 \leq r_k = 1 \leq r_{k-1} - 1$ et enfin $r_{k-1} = r_k \, q_k$ avec $r_{k+1} = 0$ et $a \wedge b = r_k = 1$. Alors $r_k = 1 = r_{k-2} - r_{k-1} \, q_{k-1}$. Or $r_{k-3} = r_{k-2} \, q_{k-2} + r_{k-1}$ et en remplaçant r_{k-1} par son expression en fonction de r_{k-2} et r_{k-3}, on a $1 = r_{k-2} - (r_{k-3} - r_{k-2} \, q_{k-2}) \, q_{k-1} = -r_{k-3} + (1 + q_{k-2} \, q_{k-1}) \, r_{k-2}$. On remonte comme cela la suite des restes successifs. On montre par récurrence [exercice laissé au lecteur !] qu'il existe une double suite d'entiers (u_p, v_p) pour $2 \leq p \leq k$ de sorte que $1 = u_p \, r_{k-p} + v_p \, r_{k-(p-1)}$. En prenant $p = k$, on en déduit $1 = u_p \, r_0 + v_p \, r_1$ c'est à dire le résultat avec $u = u_p$ et $v = v_p$ puisque $r_0 = a$ et $r_1 = b$.
Réciproquement, si l'identité de Bézout est satisfaite, tout diviseur d commun aux nombres a et b divise 1. le nombre entier naturel d est donc inversible dans $\mathbb{N}$ et $d = 1$ nécessairement. Le seul diviseur commun vaut 1 et $\text{pgcd}\,(a, b) = 1$.
Une conséquence de l'identité de Bézout est que deux entiers consécutifs sont premiers entre eux. En effet, pour tout entier naturel n, la relation $(n+1) - n = 1$ exprime l'identité de Bézout avec $u = 1$ et $v = -1$.
On peut trouver les entiers u et v de l'identité de Bézout en suivant l'algorithme d'Euclide

depuis la fin jusqu'au début. Dans le cas où $114 \wedge 35 = 1$, on a grâce aux calculs faits plus haut : $1 = 9-8 = 9-\big(35-(3\times 9)\big) = (4\times 9)-35 = 4\times\big(114-(3\times 35)\big)-35$
$= (4\times 114)-(13\times 35)$ et on a dans ce cas $u = 4$ et $v = -13$.

- Extensions de l'identité de Bézout

Le résultat précédent s'étend au cas d'un pgcd quelconque, mais il donne lieu à deux résultats distincts. On se donne deux entiers a et b supérieurs ou égaux à 1. Alors si $a \wedge b = \text{pgcd}\,(a,b)$, alors il existe deux entiers u et v tels que $au+bv = a\wedge b$.
Par ailleurs, si il existe deux entiers u et v tels que $au+bv = \alpha$, alors le nombre α est un multiple du pgcd de a et b : $\exists k \in \mathbb{Z},\ \alpha = k(a\wedge b)$.

- Lemme de Gauss (Carl Friedrichs Gauss (1777-1855)

On se donne trois entiers k, a et b supérieurs ou égaux à 1 de sorte que d'une part k divise le produit ab et d'autre part k est premier relativement au nombre a. Alors k divise b.
Comme les entiers k et a sont premiers entre eux, l'identité de Bézout entraîne qu'il existe deux nombres entiers u et v de sorte que $au+kv = 1$. Alors d'une part, il est évident que k divise le produit kb et d'autre part, k divise ab par hypothèse. On en déduit que k divise la combinaison $(ab)u+(kb)v = b(au+kv) = b$.
Ainsi, si on remarque d'abord que $5\times 24 = 120$, ensuite que les entiers consécutifs 5 et 6 sont premiers entre eux et enfin que 6 divise 120, le lemme de Gauss implique que 6 divise 24.

- Nombres premiers

On rappelle qu'un nombre $p \in \mathbb{N}$ est premier si et seulement si l'ensemble de ses diviseurs est une paire. Les nombres premiers ne sont divisibles que par 1 et par eux-mêmes, qu'on suppose différents. Les nombres premiers sont supérieurs ou égaux à 2. Rappelons le début de la liste des nombres premiers : 2, 3, 5, 7, 11, 13, *etc*.
Soit $p \geq 2$ un nombre premier. Alors quel que soit l'entier ℓ compris entre 1 et $(p-1)$, les entiers ℓ et p sont premiers entre eux. En effet, les seuls diviseurs de p sont 1 et p. Donc l'intersection $D(p)\cap D(\ell)$ ne contient aucun nombre entre 2 et $p-1$ et elle est donc incluse dans le sigleton $\{1\}$.
Soit p et $q \neq p$ deux nombres premiers. Alors ils sont premiers entre eux : $p\wedge q = 1$.

- Théorème fondamental de l'arithmétique (Euclide, Gauss)

C'est le théorème de décomposition d'un nombre entier supérieur ou égal à 1 en produit de facteurs premiers : tout entier supérieur ou égal à 1 peut être écrit comme produit de nombres premiers de façon unique à l'ordre près des facteurs.
Par exemple $60 = 2^2\ 3\ 5$.
L'existence d'une telle décomposition se prouve par récurrence. On peut écrire $1 = \Pi_{j\in\varnothing}\, p_j$ qui montre que la propriété est vraie pour $n = 1$. Pour $n = 2$, le nombre entier 2 est égal au nombre premier 2 et la propriété est encore vraie dans ce cas. Si on suppose que la propriété est vraie pour tous les entiers inférieurs ou égaux à $(n-1)$, alors ou bien l'entier n est premier ou bien il n'est pas premier. La propriété est vraie dans le premier cas puisqu'on écrit simplement $n = n$. Si n n'est pas premier, soit p le plus petit entier strictement supérieur ou égal à 1 qui divise l'entier n. Alors p est premier car si d est tel que $2 \leq d \leq p$ et de plus divise p, alors d

divise n et $d = p$ car p est minimal. On peut donc écrire $n = m\,p$ pour un entier m strictement inférieur à n, pour lequel on peut appliquer l'hypothèse de récurrence.
L'unicité s'établit par l'absurde. Si $p_1 \ldots p_\ell = q_1 \ldots q_m$ avec tous les p_i premiers pour $1 \leq i \leq \ell$ et tous les q_j premiers pour $1 \leq j \leq m$, on peut supposer q_1 différent de tous les p_i sinon on divise l'égalité précédente par q_1. De même pour tous les autres q_j puis tous les p_i en échangeant les rôles des deux familles. On peut supposer pour fixer les idées p_1 inférieur à tous les autres p_i et à tous les q_j, quitte à échanger les rôles des deux familles. On a donc finalement p_1 qui divise le produit $q_1 \ldots q_m$ et qui est premier à tous les q_j car p_1 est premier inférieur ou égal aux q_j. En utilisant le lemme de Gauss successivement m fois, p_1 divise 1, ce qui établit la contradiction. La décomposition en facteurs premiers est unique, à l'ordre près des facteurs.

- L'ensemble des nombres premiers est infini (Euclide)

Si on suppose que la famille des nombres premiers est finie et composée de $p_1 = 2,\ p_2 = 3$ jusqu'à un certain p_m, on pose $n = 1 + p_1\,p_2 \ldots p_m$. Ce nombre est premier à tous les nombres premiers car l'égalité $n - p_1\,p_2 \ldots p_m = 1$ exprime l'identité de Bézout pour chacun des couples $(n,\, p_j)$. Donc l'entier n n'est divisible par aucun des p_j, ce qui contredit le théorème précédent de décomposition de tout nombre entier supérieur ou égal à 1 en produit de facteurs premiers.

Exercices

- Division euclidienne

Si on effectue la division euclidienne de l'entier a par 18, on trouve un reste égal à 13.

a) Ce texte est-il cohérent avec ce qui a été étudié en cours ?

b) Quel est le reste de la division euclidienne de a par 6 ? [1]

- Diviseurs

a) Décomposer le nombre 150 en produit de facteurs premiers.

b) À l'aide d'un dénombrement, en déduire le nombre d'éléments de l'ensemble $D(150)$ des diviseurs de l'entier 150. [12]

c) Expliciter l'ensemble $D(150)$.

- Diviseurs

Combien le nombre $15!$ admet-il de diviseurs ? [4032]

- Utilisation de l'identité de Bézout généralisée

On se donne un nombre entier $n \in \mathbb{Z}$.

a) Avec un calcul algébrique simple, montrer que le pgcd de $(n+1)$ et $(3n-4)$ divise le nombre 7.

b) En déduire que si un entier $n \in \mathbb{Z}$ est tel que $(n+1)$ divise $(3n-4)$, alors il divise un entier indépendant de n que l'on précisera.

c) Trouver tous les entiers $n \in \mathbb{Z}$ tels que $(n+1)$ divise $(3n-4)$. $[-8, -2, 0, 6]$

d) Reprendre l'ensemble des questions précédentes pour trouver tous les entiers $n \in \mathbb{Z}$ tels que $(n+1)$ divise (n^2+2). $[-4, -2, 0, 2]$

- Une équation linéaire

On cherche à résoudre l'équation $7x+6y=1$, avec x et y entiers relatifs.

a) Trouver une solution particulière de cette équation.

b) Montrer que la résolution de l'équation $7x+6y=1$ se ramène alors à la résolution de l'équation homogène $7\xi+6\eta=0$.

c) Expliciter la solution générale de l'équation $7x+6y=1$.

[$x=1+6k, y=-1-7k$ avec $k\in\mathbb{Z}$]

- Une équation à inconnues entières

a) Quels sont les nombres premiers inférieurs ou égaux à 21 ?

b) Démontrer que 401 est un nombre premier.

c) Trouver tous les nombres $x\in\mathbb{N}$ et $y\in\mathbb{N}$ de sorte que $x^2-y^2=401$. [$(201,200)$]

- Compter les zéros

a) Montrer qu'il existe deux entiers positifs p et q de sorte que $1000!=2^p5^qN$ avec l'entier N tel que $N\wedge 10=1$.

b) Combien de nombres inférieurs ou égaux à 1000 sont divisibles par 5 ?

c) Combien de nombres inférieurs ou égaux à 1000 sont divisibles par 5^2 ?

d) Combien de nombres inférieurs ou égaux à 1000 sont divisibles par 5^3 ?

e) Combien de nombres inférieurs ou égaux à 1000 sont divisibles par 5^4 ?

f) Quelle est la valeur de l'entier q introduit à la question a) ?

g) Montrer que $p>q$.

h) On écrit le nombre $1000!$ dans le système décimal. Par combien de zéros consécutifs ce nombre se termine-t-il ? [249]

- Divisibilité

a) Montrer que pour tout entier $n\geq 1$, le nombre $n(n+1)(n+2)(n+3)$ est divisible par 24. On pourra raisonner par récurrence.

b) Montrer que pour tout entier $n\geq 1$, le nombre $n(n+1)(n+2)(n+3)(n+4)$ est divisible par 120.

- Encore l'identité de Bézout

On se donne deux entiers naturels a et b supérieurs ou égaux à 1 et premiers entre eux. Démontrer qu'alors les entiers ab et $a+b$ sont premiers entre eux.