DOMAINE : Arithmétique
NIVEAU : Débutants
CONTENU : Cours et exercices

AUTEUR : Maxime ZAVIDOVIQUE
STAGE : Montpellier 2012

Divisibilité

L'arithmétique est l'étude des nombres entiers $0, 1, 2 \ldots$. On note $\mathbb{N}$ l'ensemble des nombres entiers et on utilisera aussi la notation $n \in \mathbb{N}$, qui se lit « n appartient à $\mathbb{N}$ » pour dire que n est un nombre entier.

- Identités remarquables -

On commence par rappeler quelques identités remarquables :

$$(a+b)^2 = a^2 + 2ab + b^2, \quad (a-b)^2 = a^2 - 2ab + b^2, \quad a^2 - b^2 = (a+b)(a-b).$$

$$1 + a + \cdots + a^{k-1} + a^k = \sum_{i=0}^{k} a^i = \frac{1-a^{k+1}}{1-a}, \text{ si } a \neq 1.$$

Exercice 1

1. Montrer que si n est somme des carrés de deux entiers consécutifs alors $2n-1$ est le carré d'un entier.
2. Montrer que si $2n-1$ est le carré d'un entier alors n est somme des carrés de deux entiers consécutifs.

Solution de l'exercice 1

1. Par hypothèse, il existe un entier a tel que $n = a^2 + (a+1)^2$. On développe ce qui donne :
$$n = 2a^2 + 2a + 1.$$
Un calcul donne maintenant que
$$2n - 1 = 4a^2 + 4a + 1 = (2a)^2 + 2 \times (2a) \times 1 + 1^2.$$

On reconnaît une identité remarquable :

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

ce qui prouve bien que $2n - 1$ est le carré d'un entier.

2. Par hypothèse, il existe un entier b tel que $2n - 1 = b^2$. De plus, comme $2n - 1$ est impair, on remarque que b est aussi forcément impair (le carré d'un entier pair est pair et le carré d'un entier impair est impair). Ainsi, il existe un entier a tel que $b = 2a + 1$. On a donc

$$2n - 1 = (2a + 1)^2 = 4a^2 + 4a + 1.$$

Ainsi un calcul donne que

$$n = 2a^2 + 2a + 1 = a^2 + (a^2 + 2a + 1) = a^2 + (a + 1)^2.$$

Comme a est entier, on a bien montré que n est somme de deux entiers consécutifs.

- Divisibilité -

On dit qu'un entier $n \in \mathbb{N}$ divise un entier $m \in \mathbb{N}$ s'il existe un troisième entier $k \in \mathbb{N}$ tel que $m = kn$. On dit aussi que m est un multiple de n. On note alors $n \mid m$.

Exemple 1.
- $4 \mid 12$, 4 divise 12 car $12 = 4 \times 3$;
- 5 ne divise pas 12 (on le note $5 \nmid 12$) ;
- 0 est un multiple de tout nombre car si $n \in \mathbb{N}$, alors $0 = 0 \times n$;
- 1 divise tout nombre car si $n \in \mathbb{N}$, alors $n = 1 \times n$.

Nombres premiers : on dit qu'un nombre $p \in \mathbb{N}$ est premier s'il possède exactement deux diviseurs : 1 et p. Attention, 1 n'est pas premier d'après cette définition, en effet il n'a qu'un diviseur.

Exercice 2 Déterminer les nombres premiers inférieurs à 100. Critère d'Eratosthène.

Solution de l'exercice 2 $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73,$
$79, 83,$
$89, 97.$

Exercice 3 Montrer qu'il existe une infinité d'entiers $a \in \mathbb{N}$ tels que $n^4 + a$ n'est premier pour aucun entier $n \in \mathbb{N}$.

Solution de l'exercice 3 Il faut bien choisir la forme de a. Pour $a = 4k^4$, on peut utiliser les identités remarquables comme suit :

$$n^4 + 4k^4 = (n^2 + 2k^2)^2 - 4n^2k^2 = (n^2 + 2k^2 - 2nk)(n^2 + 2k^2 + 2nk).$$

De plus $n^2 + 2k^2 - 2nk = (n-k)^2 + k^2$, donc $n^4 + 4k^4$ n'est pas premier (sauf si $k = 1$ et $n = 1$).

Une propriété importante des nombres premiers est qu'il sont en nombre infini. Voici la preuve qu'en donne Euclide (à peu près 300 ans avant J.C.).

On raisonne par l'absurde, c'est-à-dire qu'on suppose qu'il n'existe qu'un nombre fini, N, de nombres premiers. On les note $p_1, \ldots, p_N$. On considère alors l'entier $n = 1 + p_1 \times \cdots \times p_N$. Soit maintenant p un nombre premier tel que $p \mid n$. Comme p est premier, c'est forcément l'un des p_i, pour un certain $1 \leqslant i \leqslant N$. Donc $p \mid p_1 \times \cdots \times p_N$. Mais $p \mid n$, donc p divise la différence, soit

$$p \mid n - p_1 \times \cdots \times p_N = 1.$$

C'est absurde car aucun nombre premier ne divise 1. Ainsi, il existe une infinité de nombres premiers.

Décomposition en facteurs premiers : une propriété fondamentale est que tout entier $n \neq 0$ peut s'écrire de manière unique sous la forme

$$n = (1\times)p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i},$$

où les p_i sont des nombres premiers distincts $p_1 < \cdots < p_k$ et les α_i strictement positifs. Bien sûr, k dépend de n.

Exemple 2.

$$30 = 2 \times 3 \times 5, \quad 135 = 3^3 \times 5.$$

Exercice 4 Énumérer les diviseurs de 30 et de 135, les compter.

Solution de l'exercice 4 Pour 30 : $1, 2, 3, 5, 6, 10, 15, 30$ soit $8 = 2 \times 2 \times 2$ diviseurs. Pour 135 : $1, 3, 5, 9, 15, 27, 45, 135$ soit $8 = 4 \times 2$ diviseurs.

Plus généralement, on peut deviner de l'exercice précédent que si un entier n se décompose en facteurs premiers :

$$n = (1\times)p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i},$$

alors n possède exactement $(1+\alpha_1)\times\cdots\times(1+\alpha_k)=\prod_{i=1}^{k}(1+\alpha_i)$ diviseurs. En effet, si m divise n, alors il ne possèdera dans sa décomposition en facteurs premiers que des nombres premiers qui apparaissent dans la décomposition de n, et à une puissance inférieure. Ainsi, m peut s'écrire

$$m = p_1^{\beta_1}\times\cdots\times p_k^{\beta_k} = \prod_{i=1}^{k} p_i^{\beta_i},$$

où pour chaque i, on a $0 \leqslant \beta_i \leqslant \alpha_i$. (Attention au fait que l'écriture de m ci-dessus n'est pas forcément sa décomposition en facteurs premiers ; en effet certaines puissances peuvent-être nulles.) Ainsi, choisir un diviseur de n revient à choisir les puissances $\beta_1,\ldots,\beta_k$ sui vérifient les inégalités ci-dessus, et pour β_i il y a $1+\alpha_i$ choix.

pgcd, ppcm : le **pgcd** de deux entiers n et m, noté $n\wedge m$ est le plus grand commun diviseur de m et n (noter que 1 est toujours un diviseur commun) c'est-à-dire le plus grand entier l tel que $l \mid n$ et $l \mid m$.

Exemple 3. Le pgcd de 30 et de 135 est $30\wedge 135 = 15$.

On peut déterminer le pgcd de deux nombres d'après leur décomposition en facteurs premiers. En effet, les facteurs premiers du pgcd doivent apparaître dans les 2 nombres, et à une puissance inférieure à celle des deux nombres (mais quand même maximale). On obtient donc la formule suivante : si

$$n = p_1^{\alpha_1}\times\cdots\times p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i},$$

$$m = p_1^{\beta_1}\times\cdots\times p_k^{\beta_k} = \prod_{i=1}^{k} p_i^{\beta_i},$$

alors

$$n\wedge m = p_1^{\min(\alpha_1,\beta_1)}\times\cdots\times p_k^{\min(\alpha_k,\beta_k)} = \prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)}.$$

Vérifier que ça coïncide bien avec l'exemple précédent.

On dit que deux entiers m et n sont **premiers entre eux** si $m\wedge n = 1$. Dans le cas général, si a et b sont deux entiers quelconques, et si l'on pose $d = a\wedge b$, alors on peut écrire $a = d\times a'$ et $b = d\times b'$ où a' et b' sont deux entiers tels

que $a' \wedge b' = 1$.

Le **ppcm** de deux entiers m et n, noté $m \vee n$, est le plus petit commun multiple de m et de n (noter que $m \times n$ est toujours un commun multiple de m et n) c'est-à-dire le plus petit entier l tel que $n \mid l$ et $m \mid l$.

Exemple 4. Le ppcm de 30 et de 135 est $30 \wedge 135 = 270$.

On peut déterminer le ppcm de deux nombres d'après leur décomposition en facteur premier. En effet, les facteurs premiers du ppcm doivent apparaître dans au moins l'un des 2 nombres, et à une puissance supérieure à celle des deux nombres (mais quand même minimale). On obtient donc la formule suivante : si

$$n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i},$$

$$m = p_1^{\beta_1} \times \cdots \times p_k^{\beta_k} = \prod_{i=1}^{k} p_i^{\beta_i},$$

alors

$$n \wedge m = p_1^{\max(\alpha_1,\beta_1)} \times \cdots \times p_k^{\max(\alpha_k,\beta_k)} = \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)}.$$

Vérifier que ça coïncide bien avec l'exemple précédent.

Des formules précédentes, on déduit immédiatement que

$$m \times n = \prod_{i=1}^{k} p_i^{\alpha_i+\beta_i} = \prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)+\max(\alpha_i,\beta_i)} = (m \wedge n) \times (m \vee n).$$

Exercice 5 Combien existent-ils de couples n, m tels que $n \wedge m = 50$ et $n \vee m = 75$?

Et tels que $n \wedge m = 50$ et $n \vee m = 600$?

Solution de l'exercice 5 Pour le premier, la réponse est 0 ! En effet, un peu de réflexion montre qu'on doit toujours avoir $n \wedge m \mid n \vee m$, or $50 \nmid 75$.

Pour le second, on commence par décomposer en facteurs premiers : $50 = 2 \times 5^2$ et $600 = 2^3 \times 3 \times 5^2$. On sait aussi que si n, m sont solutions, on a $nm = 50 \times 600 = 2^4 \times 3 \times 5^4$. Enfin $50 \mid n$ et $50 \mid m$.

En conclusion, les solutions seront exactement de la forme $m = 50 \times 2^a \times 3^b$ et $n = 50 \times 2^{2-a} \times 3^{1-b}$, avec $0 \leqslant a \leqslant 2$ et $0 \leqslant b \leqslant 1$. En conclusion, on a 3 choix pour a et 2 pour b soit en tout 6 couples de solutions.

On conclut cette section par un résultat fondamental dû à Gauss, d'où son nom.

Lemme de Gauss : soit trois entiers a, b et c tels que $a \mid b \times c$. Si $a \wedge b = 1$ alors $a \mid c$.

Avec ce que l'on a vu précédemment, ce résultat est assez intuitif. L'hypothèse $a \mid b \times c$ peut se traduire par le fait que l'on retrouve tous les éléments de la décomposition en facteurs premiers de a dans le produit $b \times c$. Mais comme $a \wedge b = 1$, aucun de ces éléments ne figure dans la décomposition de b. Ils doivent donc tous venir de c, d'où la conclusion.

Exercice 6 Déterminer tous les triplets d'entiers a, b et c tels que $a^2 + b^2 = c^2$.

Solution de l'exercice 6 C'est un grand classique, on appelle de tels triplets, des triplets pythagoriciens. On raisonne par analyse-synthèse. On commence par considérer un tel triplet, a, b, c. Soit $d = a \wedge b$. Alors on a aussi $d \mid c$. Soit $a = da'$, $b = db'$ et $c = dc'$. De plus, on a alors $a' \wedge b' = 1$.

On s'intéresse ensuite à la parité. On a deux possibilités, ou bien a et b sont de parité différente, soit ils sont tous les deux impairs (ils ne peuvent pas être pairs tous les deux car ils sont premiers entre eux). S'ils sont tous les deux impairs, alors on peut écrire $a = 2k + 1$, et $b = 2l + 1$ et alors

$$c^2 = a^2 + b^2 = 4(k^2 + k + l^2 + l) + 2.$$

Donc c^2 est pair, mais n'est pas divisible par 4. Or si c^2 est pair, alors c aussi et on peut écrire $c = 2k'$ et $c^2 = 4c'^2$ qui est donc divisible par 4, c'est absurde.

Ainsi, on a nécessairement que a' et b' sont de parité différente, quitte à les échanger, supposons que $a' = 2A$ et $b' = 2B + 1$. Alors $c = 2C + 1$ est impair. Maintenant on réécrit l'équation initiale comme suit

$$4A^2 = c'^2 - b'^2 = (c' - b')(c' + b').$$

D'abord, montrons que $a' \wedge c' = 1$. Par l'absurde, soit p un nombre premier qui divise b' et c', alors il divise aussi $a'^2 = c'^2 - b'^2$ donc il divise a'. C'est absurde car $a' \wedge b' = 1$. Enfin, on montre que $c' - b' \wedge c' + b' = 2$. En effet, si k divise $c' - b'$ et $c' + b'$ alors il divise leur somme et leur différence, soit $2c'$ et $2b'$. Donc k vaut 1 ou 2. De plus 2 divise bien $c' - b'$ et $c' + b'$.

Enfin, on observe que si $x^2 = yz$ avec $y \wedge z = 1$ alors y et z sont tous les deux des carrés (observer la décomposition en facteurs premiers de x).

Ici, la situation est presque identique, et on trouve qu'il existe deux entiers p et q, premiers entre eux, tels que $c' - b' = 2p^2$ et $c' + b' = 2q^2$, ou encore

$$c = dc' = d(p^2 + q^2), \quad b = db' = d(q^2 - p^2), \quad a = da' = 2dpq.$$

Réciproquement, on vérifie que de tels triplets sont bien pythagoriciens.

- Division euclidienne -

Étant donnés deux nombres entiers m et n, il existe un unique couple d'entiers q et r tels que

– $n = m \times q + r$,

– $0 \leqslant r < m$.

Dans ce qui précède, on appelle n le dividende, m le diviseur, q le quotient et r le reste. L'opération qui à (n, m) associe le couple (q, r) s'appelle la division euclidienne de n par m.

Exemple 5. $135 = 30 \times 4 + 15$.

On peut constater que $m \mid n$ si et seulement si le reste de la division euclidienne de n par m est 0.

Exercice 7 Montrer que tout entier n possède un multiple qui ne s'écrit qu'avec des 1 et des 0.

Montrer que si n est impair et n'est pas divisible par 5, alors il possède un multiple qui ne s'écrit qu'avec des 1.

Solution de l'exercice 7 Soit $n \in \mathbb{N}$. On pose pour tout $k \in \mathbb{N}$, a_k le nombre qui s'écrit en base 10 par k fois le chiffre 1. Enfin, on fait la division euclidienne de a_k par n : $a_k = n \times q_k + r_k$.

Comme r_k ne peut prendre qu'un nombre fini de valeurs, par le principe des tiroirs, il existe deux entiers $k < l$ tels que $r_k = r_l$. Mais alors $a_l - a_k = n(q_l - q_k)$ est un multiple de n qui ne s'écrit qu'avec des 0 et des 1.

Pour la seconde question, on reprend le multiple trouvé précédemment qui est de la forme plus précise de un groupe de 1 à gauche puis un groupe de 0 à droite.

L'algorithme d'Euclide : prenons un autre exemple, et amusons nous à continuer les divisions euclidiennes. On va diviser $135 = 3^3 \times 5$ par $105 = 3 \times 5 \times 7$:

$$135 = 105 \times 1 + 30,$$

$$105 = 30 \times 3 + 15,$$

$$30 = 15 \times 2 + 0.$$

Comme les restes successifs des divisions euclidiennes forment une suite strictement décroissante, il y a forcément un moment où l'on ne peut plus continuer, c'est-à-dire où le reste vaut 0. L'avant dernier reste, ci-dessus 15 s'avère être le pgcd de 135 et de 105. Ce n'est pas un hasard. C'est l'algorithme d'Euclide :

étant donnés des entiers r_0 et r_1, l'algorithme d'Euclide consiste à l'étape k à effectuer la division euclidienne de r_{k-1} par r_k : $r_{k-1} = r_k \times q_k + r_{k+1}$ etc.

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, \\ r_1 &= r_2 q_2 + r_3, \\ \vdots &\qquad \vdots, \\ r_{l-2} &= r_{l-1} q_{l-1} + r_l, \\ r_{l-1} &= r_l q_l + 0. \end{aligned}$$

La suite des r_k est une suite strictement décroissante d'entiers, donc elle doit finir par s'annuler. Le dernier reste non nul (ici r_l) est alors le pgcd de r_0 et de r_1.

Démontrons ce fait. Notons $d = r_0 \wedge r_1$. Il nous faut montrer deux choses : que $d \mid r_l$ puis $r_l \mid d$, ce qui suffit pour conclure.

Pour montrer la première relation, on va montrer que pour tout $k \leqslant l$, $d \mid r_k$. On le fait par récurrence (sur deux indices). Pour commencer, on initialise la récurrence : par définition du pgcd, d divise r_0 et r_1.

Pour l'hérédité, on suppose que pour une certain k, d divise r_{k-1} et r_k. Alors $d \mid r_{k-1} - q_k r_k = r_{k+1}$. Ceci conclut la récurrence.

Montrons maintenant la seconde relation. Pour la première, on a descendu l'échelle des divisions euclidiennes successives, ici on va la remonter. On va montrer par récurrence que pour tout $k \leqslant l$, $r_l \mid r_{l-k}$. Encore une fois, la récurrence se fait sur deux indices, donc il faut vérifier l'initialisation pour $k = 0$ et $k = 1$. La relation est évidente pour $k = 0$, en effet on sait que $r_l \mid r_l$ est automatiquement vrai. Pour $k = 1$ on remarque que $r_l \mid r_{l-1}$ est exactement ce que nous dit la dernière ligne de l'algorithme d'Euclide.

Maintenant, on peut faire l'hérédité. On suppose pour pour un certain k, r_l divise $r_{l-(k-1)}$ et r_{l-k}. On utilise alors que r_l divise aussi $r_{l-k} q_{l-k} + r_{l-(k-1)} = r_{l-(k+1)}$ ce qui conclut la récurrence. Maintenant, pour $k = l$ et $k = l - 1$, on

trouve que r_l divise r_0 et r_1. Il divise donc leur pgcd.

Exercice 8 Déterminer $2^m - 1 \wedge 2^n - 1$.

Solution de l'exercice 8 Écrivons la division euclidienne de n par m : $n = qm + r$. Maintenant on cherche à faire celle de $2^n - 1$ par $2^m - 1$:

$$2^n - 1 = (2^{mq} - 1)2^r + 2^r - 1 = (2^m - 1)(1 + 2^m + 2^{2m} + \cdots + 2^{(q-1)m}) + 2^r - 1.$$

De plus, $2^r - 1 < 2^m - 1$. Ainsi, l'algorithme d'Euclide associé à $2^n - 1$ et $2^m - 1$ peut être fait parallèlement à celui de n et m. Si $d = n \wedge m$, on aura

$$2^m - 1 \wedge 2^n - 1 = 2^d - 1.$$

Le théorème de Bezout : le dernier jeu auquel nous allons nous prêter consiste encore une fois à remonter l'algorithme d'Euclide, à la manière de ce qu'on a fait à la fin de la démonstration précédente. On sait donc que

$$d = r_l = r_{l-2} - r_{l-1}q_{l-1} = r_{l-2}u_1 + r_{l-1}v_1.$$

On remplace alors r_{l-1} par sa valeur donnée par la ligne précédente :

$$r_l = r_{l-2} - (r_{l-3} - r_{l-2}q_{l-2})q_{l-1} = r_{l-3}(-q_{l-1}) + r_{l-2}(1 + q_{l-2}q_{l-1}) = r_{l-3}u_2 + r_{l-2}v_2.$$

Et ainsi de suite, à chaque étape, on trouve deux entiers (relatifs) u_k et v_k tels que $d = r_{l-k-1}u_k + r_{l-k}v_k$. Ainsi, à la fin, on obtient deux entiers relatifs u et v tels que $d = ur_0 + vr_1$.

On vient de montrer la moitié du célèbre **théorème de Bezout** : deux entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers relatifs u et v tels que $1 = au + bv$.

En effet, le fait que si $a \wedge b = 1$ alors il existe u et v vient de l'analyse faite ci-dessous quand $d = 1$. La réciproque doit maintenant être facile. S'il existe u et v tels que $1 = au + bv$, et si d divise a et b, alors il divise $au + bv$ donc $d = 1$.

Exercice 9 Soit a, b et c trois entiers. Trouver tous les couples d'entiers relatifs x, y (possiblement avec un signe - devant) tels que $ax + by = c$.

Solution de l'exercice 9 On raisonne encore par analyse synthèse. Soit $d = a \wedge b$. Si $ax + by = c$ alors $d \mid c$. On en déduit que si $d \nmid c$, alors il n'y a pas de solution.

Sinon, quitte à tout diviser par d, on peut supposer sans perte de généralité que $a \wedge b = 1$. On commence maintenant par chercher une solution particulière. Soient u et v, donnés par l'algorithme d'Euclide, tels que $au + bv = 1$. Alors, en posant $x_0 = cu$ et $y_0 = cv$ on a bien $ax_0 + by_0 = c$.

Soit maintenant x et y une solution quelconque. En soustrayant $ax+by = c$ et $ax_0 + by_0 = c$ on obtient

$$a(x - x_0) = b(y_0 - y).$$

Comme $a \wedge b = 1$, d'après le lemme de Gauss, $a \mid y_0 - y$, donc il existe un entier k tel que $y = y_0 - ka$. On trouve alors que nécessairement $x = x_0 + kb$.

Réciproquement, pour tout entier relatif k, les couples $x = x_0 + kb, y = y_0 - ka$ sont bien solutions.