MATHEMATICAL.
OLYMPIAD.CH
MATHEMATIK-OLYMPIADE
OLYMPIADES DE MATHÉMATIQUES
OLIMPIADI DELLA MATEMATICA

Théorie des nombres I

Thomas Huber

Actualisé: 1er août 2021
vers. 1.1.0

Table des matières

1 Divisibilité

Dans ce qui suit, a et b sont des entiers. S'il existe un $k \in \mathbb{Z}$ avec $a = kb$, on dit que a est *divisible* par b ou que b est un *diviseur* de a. En symboles: $b \mid a$. Tout entier n est divisible par ± 1 et $\pm n$ et tout entier est un diviseur de 0. Lorsqu'on considère les *diviseurs* d'un nombre positif $a > 0$, d'habitude on n'entend par là que l'ensemble de ses diviseurs positifs.
Un nombre $p \in N$ est appelé *premier* ou un *nombre premier* si $p > 1$ et p et 1 sont les seuls diviseurs de p.

Quelques propriétés simples mais importantes:

- $a \mid b$ et $b \mid c \quad \Longrightarrow \quad a \mid c$
- $a \mid b_1, \ldots, a \mid b_n$, alors pour des entiers arbitraires $c_1, \ldots, c_n$
$$a \mid \sum_{i=1}^{n} b_i c_i.$$
- $a \mid b$ et $c \mid \mathrm{d} \quad \Longrightarrow \quad ac \mid bd$
- p premier et $p \mid ab \quad \Longrightarrow \quad p \mid a$ ou $p \mid b$
- $a \in \mathbb{N}$, $b \in \mathbb{Z}$ et $a \mid b \quad \Longrightarrow \quad b = 0$ ou $a \leq |b|$

Exemple 1 *Trouver tous les nombres naturels x, y avec*
$$x^2 - y! = 2001.$$

Solution. 2001 est divisible par 3 mais pas par 9. Si $y \geq 3$, alors $y!$ est divisible par 3, donc x aussi. Alors x^2 est divisible par 9. Pour $y \geq 6$ $y!$ est aussi divisible par 9, donc 2001 devrait avoir la même propriété, ce qui n'est pas le cas. Il reste les possibilités $y = 1, 2, 3, 4, 5$. En testant tous les cas, on trouve que la seule solution est $(x, y) = (45, 4)$. □

Si on a deux entiers, on peut toujours faire une division avec reste. Plus précisément:

Proposition 1.1 (Division avec reste) *Soient a, b des entiers avec $b > 0$. Alors il existe deux entiers q et r uniquement déterminés avec $0 \leq r < b$, tels que*
$$a = qb + r,$$
r s'appelle le reste *de la division et on a $r = 0$ si et seulement si $b \mid a$.*

Un des points les plus importants de toute la théorie des nombres est le fait que tout nombre naturel peut s'écrire de manière unique comme produit de nombres premiers :

Théorème 1.2 (Décomposition en facteurs premiers) *Soit a un nombre naturel. Alors il existe des nombres premiers distincts $p_1, p_2, \ldots, p_r$ et des nombres naturels $n_1, n_2, \ldots, n_r$ avec*

$$a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}.$$

Les p_i et les n_i sont uniquement déterminé par a.

On peut démontrer ce théorème par induction à l'aide de la division avec reste mais on n'entrera pas dans les détails ici. Le cas $a = 1$ correspond au produit vide au côté droit de l'équation, c'est-à-dire qu'il n'y a aucun facteur premier et on a $r = 0$. Ce théorème a beaucoup de conséquences importantes dont nous allons mentionner deux.

Remarque *Soit $a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ la décomposition en facteurs premiers du nombre naturel a. Alors on a :*

- *a possède exactement $(n_1 + 1)(n_2 + 1) \cdots (n_r + 1)$ diviseurs positifs distincts.*
- *a est la m-ème puissance d'un nombre naturel si et seulement si tous les exposants n_k sont divisibles par m.*

L'application suivante du théorème est un résultat classique d'Euclide:

Proposition 1.3 *Il existe une infinité de nombres premiers.*

Preuve. Supposons qu'il existe un nombre fini de premiers $p_1, p_2, \ldots, p_n$ et considérons le nombre $N = p_1 p_2 \cdots p_n + 1$. Comme $N > 1$, par le théorème 1.2 il existe un diviseur premier q de N. Or aucun des premiers p_k ne divise N, car sinon on aurait $p_k \mid 1$, ce qui est absurde. Donc q est différent de $p_1, p_2, \ldots, p_n$. Contradiction. □

2 PGCD et PPCM

Pour deux entiers naturels a, b, le $\mathrm{pgcd}(a, b)$ est le *plus grand diviseur commun* de a et b, en d'autres termes le plus grand entier positif qui est un diviseur de a et un diviseur de b. Le $\mathrm{ppcm}(a, b)$ est le *plus petit multiple commun*, donc le plus petit nombre positif qui admet a et b comme diviseurs. On définit de façon analogue le pgcd et le ppcm de plus que deux nombres. On utilise les abréviations $(a_1, a_2, \ldots, a_n)$ et $[a_1, a_2, \ldots, a_n]$ pour le pgcd, respectivement le ppcm. On peut caractériser le pgcd par les équivalences suivantes:

(a) $c = \mathrm{pgcd}(a, b)$

(b) $c > 0$ est un diviseur de a et de b et pour tout nombre positif x on a

$$x \mid a, x \mid b \quad \Longrightarrow \quad x \mid c.$$

On a une équivalence analogue pour le ppcm. Si $\mathrm{pgcd}(a, b) = 1$, alors a et b sont dits *premiers entre eux*. On a les propriétés suivantes:

- $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, a)$
- $\mathrm{pgcd}(a, b, c) = \mathrm{pgcd}(\mathrm{pgcd}(a, b), c)$
- $c \mid ab$ et $\mathrm{pgcd}(a, c) = 1 \quad \Longrightarrow \quad c \mid b$
- $a \mid c$, $b \mid c$ et $\mathrm{pgcd}(a, b) = 1 \quad \Longrightarrow \quad ab \mid c$
- Si $d = \mathrm{pgcd}(a, b)$, alors il existe deux entiers x et y premiers entre eux tels que $a = xd$ et $b = yd$. De plus on a alors $\mathrm{ppcm}(a, b) = xyd$ (cf. théorème 2.1).
- Si a, b sont des nombres naturels premiers entre eux, tels que ab est une m-ème puissance, alors a et b sont les deux des puissances m-èmes.

En utilisant la décomposition en facteurs premiers, on peut calculer le pgcd et le ppcm explicitement:

Proposition 2.1 *Soient $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ et $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ décomposition en facteurs premiers de a et b avec des p_k distincts et des exposants $\alpha_k, \beta_k \geq 0$, alors on a*

$$\begin{aligned} \mathrm{pgcd}(a, b) &= p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_r^{\min\{\alpha_r, \beta_r\}} \\ \mathrm{ppcm}(a, b) &= p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \cdots p_r^{\max\{\alpha_r, \beta_r\}} \end{aligned}$$

De plus, en connaissant la formule $\min\{x, y\} + \max\{x, y\} = x + y$ on peut immédiatement conclure que

$$\mathrm{pgcd}(a, b) \cdot \mathrm{ppcm}(a, b) = ab.$$

Exemple 2 *(Russie 95) Soient m et n deux nombres naturels avec*

$$\mathrm{pgcd}(m, n) + \mathrm{ppcm}(m, n) = m + n.$$

Montrer qu'un des nombres divise l'autre.

Solution. Soit d le plus grand diviseur commun de m et n et écrivons $m = ad, n = bd$. Alors on a $\mathrm{ppcm}(m, n) = abd$ par le théorème 2.1 et l'équation se transforme en $d + abd = ad + bd$ ou encore $d(ab - a - b + 1) = 0$. On factorise le côté gauche et on trouve $d(a-1)(b-1) = 0$, ce qui entraîne $a = 1$ ou $b = 1$. Dans le premier cas il s'ensuit que $m = d$, donc $m \mid n$. Dans le deuxième cas on trouve de façon analogue $n \mid m$. $\square$

En principe on peut toujours calculer le pgcd à l'aide des formules du théorème 2.1. Malheureusement il n'est pas toujours facile de factoriser des nombres très grands. Par chance, il existe un algorithme très simple et efficace pour calculer le pgcd, *l'algorithme d'*EUCLIDE. Il est basé sur la proposition suivante:

Proposition 2.2 *Pour tous nombres entiers a, b et n on a:*

$$(a, b) = (a, b + na). \tag{1}$$

Preuve. Il suffit de montrer ceci pour le cas $n = \pm 1$, le cas général s'ensuit alors en itérant. Si c est un diviseur commun de a et b, alors c divise aussi $b \pm a$, donc $(a, b) \mid (a, b \pm a)$. Inversement, soit c un diviseur commun de a et $b+a$, respectivement $b-a$. Alors c divise aussi $(b+a)-a = b$, respectivement $(b-a)+a = b$. Par conséquent on a $(a, b\pm a) \mid (a, b)$. □

Pour donner un exemple, on va calculer $(2541, 1092)$ en appliquant l'équation (1) jusqu'à ce que lésultat soit clair:

$$\begin{aligned}(2541, 1092) &= (2541 - 2 \cdot 1092, 1092) = (357, 1092)\\ &= (1092 - 3 \cdot 357, 357) = (21, 357)\\ &= (357 - 17 \cdot 21, 21) = (0, 21) = 21.\end{aligned}$$

Manifestement l'idée est de continuer les calculs avec le reste de la division du plus grand nombre par le plus petit. Tout ceci est formalisé dans l'algorithme d'Euclide:

Algorithme 2.3 (EUCLIDE) *Calcul de (a, b) pour $a, b \geq 0$.*

1. *Soient $a_1 = \max\{a, b\}$ et $a_2 = \min\{a, b\}$ ainsi que $n = 2$.*
2. *Soient $a_{n-1} = q_n a_n + a_{n+1}$ avec $0 \leq a_{n+1} < a_n$ (division avec reste).*
3. *Si $a_{n+1} = 0$, alors on obtient $(a, b) = a_n$, sinon on augmente n de 1 et on retourne au pas 2.*

La validité de cet algorithme découle directement de la formule (1). Pour notre exemple, on a les calculs suivants à faire:

$$\begin{aligned}2541 &= 2 \cdot 1092 + 357\\ 1092 &= 3 \cdot 357 + 21\\ 357 &= 17 \cdot 21 + 0.\end{aligned}$$

Puisque le reste dans la dernière ligne vaut 0, on a $(2541, 1092) = 21$.

Proposition 2.4 (BÉZOUT) *Si a, b sont premiers entre eux, alors il existe des entiers x, y avec*

$$xa + yb = 1.$$

Plus généralement: si $d = \mathrm{pgcd}(a, b)$, alors il existe des entiers x, y avec

$$xa + yb = d.$$

Preuve. Ceci découle directement de l'algorithme d'Euclide, car dans l'avant-dernière ligne on trouve $\mathrm{pgcd}(a, b) = a_n$. En substituant l'expression pour a_n dans la formule de la $(n-1)$-ème ligne et en itérant ce procédé pour les a_k de plus en plus petits, on trouve une équation de la forme: $\mathrm{pgcd}(a, b) = xa + yb$. □

Dans notre exemple, on obtient successivement:

$$\begin{aligned} 21 &= 1 \cdot 1092 - 3 \cdot 357 \\ &= 1 \cdot 1092 - 3(2541 - 2 \cdot 1092) \\ &= (-3) \cdot 2541 + 7 \cdot 1092. \end{aligned}$$

En guise d'application on considère l'équation linéaire de Diophante en deux variables.

Proposition 2.5 *Soient a, b, c des entiers. L'équation*

$$ax + by = c$$

possède une solution (x, y) avec $x, y \in \mathbb{Z}$ si et seulement si $d = \mathrm{pgcd}(a, b) \,|\, c$. Si c'est le cas et si (x_0, y_0) est une solution, alors l'ensemble des solutions est donné par

$$(x, y) = \left(x_0 + k \cdot \frac{b}{d}, \, y_0 - k \cdot \frac{a}{d} \right), \qquad k \in \mathbb{Z}.$$

Preuve. Supposons que (x, y) est une solution. Alors d divise le terme de gauche, et ainsi il divise c. Si par contre $d \,|\, c$, l'existence d'une solution (x_0, y_0) découle directement du théorème de Bézout. Soit (x, y) une autre solution. Alors on a $a(x - x_0) + b(y - y_0) = c - c = 0$, donc

$$\frac{a}{d} \cdot (x - x_0) = -\frac{b}{d} \cdot (y - y_0).$$

Or $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux, donc $(x - x_0)$ est divisible par $\frac{b}{d}$ et $(y - y_0)$ par $\frac{a}{d}$. Il s'ensuit que toutes les solutions sont de la forme donnée. En introduisant ces valeurs dans l'équation, on montre que ce sont effectivement des solutions. □

3 Estimations

Une méthode très importante pour résoudre des problèmes de théorie des nombres est l'estimation de certaines grandeurs. Souvent on peut tout réduire à quelques cas particuliers qui sont faciles à résoudre, ou ce pas est nécessaire tout simplement pour rendre le problème plus abordable. Lors d'une estimation, il s'agit de comparer la croissance de certaines grandeurs dans une équation. Nous allons présenter ici quelques situations où cette méthode s'applique.

Le premier cas d'application concerne les relations de divisibilité:

Exemple 3 *Trouver tous les nombres naturels n avec $n^2 + 11 \mid n^3 + 13$.*

Solution. n^2+11 divise n^3+13, donc n^2+11 divise aussi $n(n^2+11)-(n^3+13) = 11n-13$. Il est clair que $n = 1$ n'est pas une solution. Pour $n \geq 2$ on a $11n - 13 > 0$ et puisque ce nombre doit être divisible par $n^2 + 11$, on a

$$n^2 + 11 \leq 11n - 13.$$

Voilà donc notre estimation. Comme le membre de gauche est quadratique en n et le membre de droite est linéaire, cette inéquation ne peut être satisfaite que pour de petites valeurs de n. Elle est équivalente à $n^2 - 11n + 24 = n(n-11) + 24 \leq 0$. Mais pour $n \geq 12$, on a toujours $n(n - 11) + 24 \geq 12 \cdot 1 + 24 > 0$, donc on doit avoir $n \leq 11$. On teste tous ces cas et on trouve les solutions $n = 3$ et $n = 8$. □

Le point central de cet exemple était d'observer simplement que $a \mid b$ et $b > 0$ entraîne $|a| \leq |b|$ Ce principe est souvent applicable, même quant il s'agit d'exercices d'OIM. Retenez-le!

Le deuxième cas d'application utilise le fait qu'entre deux carrés *consécutifs* (n-ème puissances, puissances de deux, etc.), il n'y en a pas d'autre. Ceci peut être utile si on a affaire à une grandeur qui est proche d'un carré et dont on sait qu'elle en est un également. Bien que la formulation de ce principe semble triviale a priori, elle s'avère étonamment utile en pratique.

Exemple 4 *(Allemagne 95) Trouver toutes les paires d'entiers non-négatifs (x, y) qui satisfont l'équation suivante:*

$$x^3 + 8x^2 - 6x + 8 = y^3.$$

Solution. Ici l'idée est la suivante: Le côté gauche doit être une 3-ème puissance (en l'occurrence y^3), mais en même temps il est assez proche de x^3. Pour quantifier cela on cherche des 3-èmes puissances aux alentours de x:

$$\begin{aligned}(x + 2)^3 &= x^3 + 6x^2 + 12x + 8,\\ (x + 3)^3 &= x^3 + 9x^2 + 27x + 27.\end{aligned}$$

Si on considère les coefficients de x^2 dans les deux équations, on voit que le premier terme semble être plus petit et le second plus grand que le côté gauche de notre équation d'origine. Calculons:

$$(x+2)^3 < x^3 + 8x^2 - 6x + 8 \Leftrightarrow 2x^2 - 18x > 0 \Leftrightarrow x > 9,$$
$$(x+3)^3 > x^3 + 8x^2 - 6x + 8 \Leftrightarrow x^2 + 33x + 15 > 0 \quad \text{vrai pour tout } x \geq 0.$$

Si $x > 9$, le terme de gauche est entre deux 3-èmes puissances et en est lui-même une, contradiction. On a par conséquent $x \leq 9$. On teste tous les cas restants et on trouve les solutions $(0,2)$ et $(9,11)$. □

Nous allons encore voir une troisième méthode d'estimation qui peut être utile pour certains problèmes de calcul de PGCD:

Proposition 3.1 *Soient a, b, c trois nombres entiers. Alors $(a, bc) \leq (a,b) \cdot (a,c)$, avec égalité lorsque b, c sont premiers entre eux. (Il existe également d'autres cas d'égalité mais il est plus simple de les traiter au cas par cas que de chercher un critère général.)*

Preuve. Soit $d = (a, bc)$. Il existe deux nombres entiers (non nécessairement uniques) d_1, d_2 tels que $d = d_1 d_2$ et $d_1 \mid b, d_2 \mid c$. De plus, nous avons également que $d_1 \mid a$ et $d_2 \mid a$ puisque $d_1 d_2 = d \mid a$. Nous obtenons ainsi

$$(a, bc) = d = d_1 d_2 \leq (a,b) \cdot (a,c).$$

Cela prouve la première partie de la proposition. Pour la seconde partie supposons que b, c soient premiers entre eux. Dans ce cas il s'en suit que $d_1 = (a,b)$ et $d_2 = (a,c)$ sont également premiers entre eux puisque si k est un diviseur commun à d_1 et d_2, alors k est également un diviseur commun à b et c et donc $k = 1$. Ainsi puisque d_1 et d_2 sont premiers entre eux et sont tous les deux des diviseurs de a, leur produit $d_1 d_2$ divise également a. Clairement $d_1 d_2$ divise bc, donc $d_1 d_2 \leq (a, bc) \leq (a,b) \cdot (a,c) = d_1 d_2$ et nous avons bien égalité. □

Concernant les cas d'égalité, nous remarquons que par exemple $(16, 2 \cdot 4) = (16, 2) \cdot (16, 4)$ bien que 2 et 4 ne soient pas premiers entre eux, mais $(4, 2 \cdot 4) = 4 < 8 = (4,2) \cdot (4,4)$.

Cette inégalité est particulièrement utile lorsqu'on veut prouver que deux termes sont premiers entre eux. Si un des deux termes est un produit on peut alors utiliser cette inégalité pour décomposer notre calcul en plusieurs calculs plus simples. Voyons tout de suite comment procéder sur un cas concret.

Exemple 5 *Soient m, n deux nombres entiers premiers entre eux. Alors mn et $m+n$ sont également premiers entre eux.*

Solution. Avec l'inégalité que nous venons de démontrer, on obtient $(mn, m+n) \leq (m, m+n) \cdot (n, m+n)$. Ainsi, si nous parvenons à prouver que $(m, m+n) = (n, m+$

$n) = 1$ nous avons fini. Nous employons maintenant l'algorithme d'Euclide pour calculer $(m, m+n) = (m, n) = 1$. On procède de même pour l'autre terme et cela conclut la solution.

$\square$