DOMAINE : Arithmétique
NIVEAU : Débutants
CONTENU : Cours et exercices

AUTEUR : Irène MARCOVICI
STAGE : Cachan 2011 (junior)

Arithmétique de base

Ces notes présentent quelques résultats fondamentaux d'arithmétique, agrémentés de petits exercices d'application. Un cours d'arithmétique contenant les démonstrations détaillées de tous ces résultats ainsi que de nombreux exercices complémentaires est disponible sur la page internet d'Animath. [1]

- Division euclidienne et congruences -

Définition 1. Si a et b sont deux entiers, on dit que a *divise* b, ou que b est *divisible* par a, s'il existe un entier q tel que $b = aq$. On dit encore que a est un *diviseur* de b, ou que b est un *multiple* de a. On le note $a|b$.

Quelques remarques :
- tout entier $a \in \mathbb{Z}$ divise 0 et est divisible par 1 et a,
- si $a|b$ et $b|c$ alors $a|c$,
- soit m un entier non nul, $a|b$ est équivalent à $ma|mb$,
- si $a|b$ et $a|c$, alors $a|bx + cy$ pour tous entiers x, y. En particulier, $a|b - c$ et $a|b + c$.

Exercice 1 Soient x, y des entiers. Montrer que $3x + 2y$ est divisible par 7 si et seulement si $4x + 5y$ l'est.

Solution. Si 7 divise $3x + 2y$, alors 7 divise $7(x + y) - (3x + 2y) = 4x + 5y$. Réciproquement, si 7 divise $4x+5y$, alors 7 divise $7(x+y)-(4x+5y) = 3x+2y$. □

Définition 2 (Nombres premiers)**.** Un entier naturel $p > 1$ est dit *premier* s'il possède exactement deux diviseurs naturels, à savoir 1 et p.

1. http://www.animath.fr/spip.php?article255

Exemple : $2, 3, 5, 7, 11, 13, 17, \ldots$ sont des nombres premiers.

Exercice 2 Parmi les nombres suivants : $67, 77, 87, 97$, lesquels sont-ils premiers ?

Solution. Le nombre 67 est premier car il n'est divisible par aucun des entiers $2, 3, 5, 7$ et comme $11^2 > 67$, si 67 avait un facteur premier plus grand que 11, il aurait aussi un facteur premier plus petit. Le nombre 77 n'est pas premier car il est divisible par 7. Le nombre 87 n'est pas premier car il est divisible par 3. Le nombre 97 est premier car il n'est pas divisible par $2, 3, 5, 7$. □

Théorème 3 (Division euclidienne)**.** Soit b un entier strictement positif. Tout entier a s'écrit, de manière unique, sous la forme $a = bq + r$, où q et r sont des entiers, avec $0 \leqslant r < b$. On appelle q le *quotient* et r le *reste* de la division euclidienne de a par b.

Définition 4 (Congruences)**.** On dit que a et b sont *congrus* modulo n et on note $a \equiv b \mod n$ si n divise $a - b$. Ainsi, si r est le reste de la division euclidienne de a par n, on a $a \equiv r \mod n$.

Exercice 3 Soit n un entier quelconque. Montrer qu'on a $n^2 \equiv 0 \mod 4$ ou $n^2 \equiv 1 \mod n$.

Solution. Si n est pair, alors il existe un entier k tel que $n = 2k$. D'où $n^2 = 4k^2$, et $n \equiv 0 \mod 4$. Si n est impair, alors $n = 2k + 1$ et $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, donc $n \equiv 0 \mod 4$. □

La relation de congruence vérifie les propriétés suivantes (*pourquoi ?*) :
– si $a \equiv b \mod n$ et $c \equiv d \mod n$, alors $a + c \equiv b + d \mod n$,
– si $a \equiv b \mod n$ et $c \equiv d \mod n$, alors $ac \equiv bd \mod n$.

Exercice 4 Soit n un nombre et $s(n)$ la somme des chiffres de n. Montrer que $n \equiv s(n) \mod 9$.

Solution. Si on écrit $n = 10^k a_k + 10^{k-1} a_{k-1} + \ldots + 10a_1 + a_0$, comme $10^i \equiv 1^i \equiv 1 \mod 9$, on obtient $n \equiv a_k + a_{k-1} + \ldots + a_1 + a_0 \mod 9$. D'où $n \equiv s(n) \mod 9$. □

- Plus grand commun diviseur et plus petit commun multiple -

Définition 5 (Plus grand commun diviseur)**.** Un entier divisant à la fois l'entier a et l'entier b (non tous les deux nuls), est appelé *diviseur commun* de a et b. Le plus grand nombre strictement positif parmi ces diviseurs communs est appelé *plus grand commun diviseur* de a et b, on le note $\mathrm{pgcd}(a, b)$. On dit que a et b sont *premiers entre eux* si $\mathrm{pgcd}(a, b) = 1$.

On a les propriétés suivantes :
– pour tout entier c, $\text{pgcd}(a, b) = \text{pgcd}(a, b + ac) = \text{pgcd}(a + bc, b)$,
– si $d|a$ et $d|b$ alors $\text{pgcd}(a, b) = d\,\text{pgcd}(a/d, b/d)$.

Exercice 5 Montrer que pour tout entier naturel n, la fraction $\frac{21n+4}{14n+3}$ est irréductible.

Solution. On a $\text{pgcd}(21n + 4, 14n + 3) = \text{pgcd}(7n + 1, 14n + 3) = \text{pgcd}(7n + 1, 1) = 1$, d'où le résultat. □

Théorème 6. Les entiers qui s'écrivent sous la forme $ax + by$, où x et y sont des entiers relatifs, sont exactement les multiples de $\text{pgcd}(a, b)$.

Ce théorème a deux conséquences particulièrement importantes :
– il existe des entiers relatifs u et v tels que $au + bv = \text{pgcd}(a, b)$,
– les entiers a et b sont premiers entre eux si, et seulement si, il existe des entiers relatifs u et v tels que $au + bv = 1$.

Théorème 7 (Lemme de Gauss)**.** Si $a|bc$ et $\text{pgcd}(a, b) = 1$, alors $a|c$.

Démonstration. Comme a et b sont premiers entre eux, il existe des entiers relatifs x et y tels que $ax+by = 1$. En multipliant par c, on obtient $axc+byc = c$. D'où $c = a \cdot xc + bc \cdot y$. Comme $a|bc$, on en déduit que $a|c$. □

Proposition 8. Si deux entiers premiers entre eux a et b divisent n, alors le produit ab divise également n.

Démonstration. Comme a divisie n, il existe un entier k tel que $n = ak$. L'entier b divise $n = ak$ et est premier avec a, donc d'après le lemme de Gauss, b divise k. On en déduit que ab divise n. □

Exercice 6 Montrer que pour tout entier n, l'entier $n^3 - n$ est divisible par 6.

Solution. On a $n^3 - n = n(n^2 - 1) = n(n + 1)(n - 1)$. Parmi les entiers $n - 1, n, n + 1$, l'un d'entre eux au moins est pair, et l'un est divisible par 3. Donc $2|n^3 - n$ et $3|n^3 - n$. Comme 2 et 3 sont premiers entre eux, on en déduit le résultat. □

Définition 9 (Plus petit commun multiple)**.** Un entier à la fois divisible par a et par b est appelé un *multiple commun* de a et b. Le plus petit nombre strictement positif parmi ces multiples communs est appelé le *plus petit commun multiple* de a et b et noté $\text{ppcm}(a, b)$.

Théorème 10. Tout multiple commun de a et b est un multiple de $\text{ppcm}(a, b)$.

Proposition 11. Pour tous entiers $a, b \geqslant 1$, on a $ab = \text{ppcm}(a,b)\,\text{pgcd}(a,b)$.

Démonstration. Soit $m = \text{ppcm}(a,b)$, et posons $d = ab/m$. Comme ab est un multiple commun de a et b, d est un entier. De plus, comme $a = \frac{m}{b}d$ et $b = \frac{m}{a}d$, l'entier d divise a et b. Donc $\text{pgcd}(a,b) = kd$ pour un certain entier k. Comme $\frac{m}{k} = \frac{ab}{\text{pgcd}(a,b)}$ est un entier qui est un multiple commun de a et b on en déduit que $k = 1$ (sinon, cela contredirait le fait que $m = \text{ppcm}(a,b)$). □

- Nombres premiers -

Théorème 12 (Théorème fondamental de l'arithmétique)**.** Tout entier naturel $n > 1$ se décompose de manière unique en produit de nombres premiers.

Théorème 13. L'ensemble des nombres premiers est infini.

Démonstration. Supposons par l'absurde qu'il n'y a qu'un nombre fini n de nombre premiers. Notons ces nombres preiers $p_1, \ldots, p_n$, et posons $N = p_1 p_2 \ldots p_n + 1$. L'entier N n'est divisible par aucun des p_i. Donc soit il est premier, soit il admet un diviseur premier différent de $p_1, \ldots, p_n$. Dans tous les cas, on obtient une contradiction. □

Exercice 7 Montrer que pour tout entier naturel k, il est possible de trouver un entier n tel que les nombres $n+1, \ldots, n+k$ soient tous composés.

Solution. Il suffit de prendre $n = (k+1)! + 1$. □

Exercice 8 Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

Solution. On raisonne par l'absurde en supposant qu'il n'existe qu'un nombre fini de nombres premiers de cette forme, notés $p_1, p_2, \ldots p_k$. On considère alors $N = 4p_1 p_2 \ldots p_k - 1$. Les diviseurs premiers de N sont distincts de 2 et des $p_i, 1 \leqslant i \leqslant k$, et il en existe un qui est de la forme $4n+3$, car sinon on vérifie immédiatement que N ne pourrait être congru à 3 modulo 4. □