Arithmétique des entiers

Alix Deleporte

6 septembre 2015

Les notions de divisibilité et de division euclidienne entre nombres entiers permettent de nombreuses constructions très classiques : pgcd, congruence, nombre premier... L'étude de ces notions est non seulement utile en tant que telle, mais permet d'illustrer les techniques de base des démonstrations mathématiques

1 La divisibilité

1.1 Division euclidienne

On commence par définir une relation entre deux entiers relatifs :

Définition 1. Soient a et b deux entiers relatifs. On dit que a divise b, et on écrit $a|b$, lorsqu'il existe $c \in \mathbb{Z}$ tel que $b = ac$.

Proposition 2. Soient a, b, c des entiers.

1. Si $a|b$ et $b \neq 0$, alors $|a| \leq |b|$.
2. Si $a|b$ et $b|c$ alors $a|c$.
3. Pour tous a, b et m, $a|b$ est équivalent à $ma|mb$.
4. Si $a|b$ et $a|c$, alors $a|ub + vc$ pour tous entiers u et v.

Démonstration. Exercice. □

Cette notion est reliée à la division euclidienne :

Proposition 3. Soient a et b deux entiers relatifs, avec $b \neq 0$. Alors il existe un unique couple (q, r) d'entiers relatifs, avec $0 \leq r < |b|$, tels que $a = bq + r$. L'entier r est appelé *reste* de la division euclidienne de a par b.

Démonstration. Démontrons d'abord la partie la plus facile, l'unicité. Si (q,r) et (q',r') conviennent, alors $0 = a - a = (q-q')b + r - r'$. Or $b|0$ et $b|b(q-q')$, donc $b|r-r'$ d'après l'item 4 de la proposition précédente. Or $-|b| < r - r' < |b|$, donc par la réciproque de l'item 1 de la proposition précédente, $r - r' = 0$, donc $r = r'$ et nécessairement $q = q'$.

Passons à l'existence. On considère l'ensemble A des nombres de la forme $a + nb$ pour $n \in \mathbb{Z}$. Si $b > 0$, alors $a + nb \to +\infty$ quand $n \to +\infty$. Si $b < 0$, alors $a + nb \to +\infty$ quand $n \to +\infty$. Dans tous les cas, $A \cap \mathbb{N} \neq \emptyset$. Soit r le plus petit des éléments de $A \cap \mathbb{N}$, et q un entier vérifiant $a - bq = r$. Alors $r \geq 0$ puisque $r \in \mathbb{N}$. Supposons par l'absurde que $r \geq |b|$. Alors $r - |b| \geq 0$, d'une part, et d'autre part $r - |b| = a - b(q + sgn(b))$, donc $r - |b| \in A \cap \mathbb{N}$, et est strictement plus petit que r, ce qui est absurde. On peut donc conclure que $r < |b|$. □

Remarque 4. Dans cette preuve, on a utilisé un outil élémentaire très puissant, la recherche d'un minimum, dans un ensemble fini ou, comme ici, dans un ensemble d'entiers naturels. On peut souvent raisonner de cette façon pour étudier ou construire des solutions.

Exercice 1. Quel est l'ensemble des restes modulo 4 des carrés des entiers ?

Solution de l'exercice 1. Soit n un entier relatif. On a $n = 4q + r$ pour un certain couple (q,r) avec $r \in \{0,1,2,3\}$. Par une identité remarquable, $n^2 = 16q^2 + 8qr + r^2 = 4(4q^2 + 2r) + r^2$. Le reste de n^2 modulo 4 est donc identique au reste de r^2 modulo 4. Or $r^2 \in \{0,1,4,9\}$, donc le reste de r^2 modulo 4 vaut nécessairement 0 ou 1.

Réciproquement, 0 et 1 sont atteints comme les restes modulo 4 de 0^2 et 1^2, respectivement. Finalement, la réponse est $\{0,1\}$. □

1.2 pgcd et ppcm

Soient a et b deux entiers relatifs, on suppose qu'au moins l'un des deux est non nul, disons a. Alors l'ensemble des nombres $c > 0$ tels que $c|a$, est fini, parce qu'il est inclus dans $\{n \in \mathbb{N}, n \leq a\}$. Cet ensemble est par ailleurs non vide, car il contient au moins 1. Quid de l'ensemble des nombres $c > 0$ tel que $c|a$ et $c|b$? Il est fini, car inclus dans l'ensemble des diviseurs de a ; et non vide, car il contient 1. Il contient donc un unique plus grand élément.

> **Définition 5.** On appelle *plus grand diviseur commun* de a et b, et on écrit des choses variées comme $a \wedge b$, (a,b) ou encore $pgcd(a,b)$, le plus grand entier naturel qui divise à la fois a et b. Les entiers a et b sont dits *premiers entre eux* lorsque leur pgcd vaut 1.

Par souci de complétion, on pose par convention $0 \wedge 0 = 0$. On dispose alors des propriétés élémentaires suivantes :

Proposition 6.

1. Pour tout entier a, on a $a \wedge 0 = a$ et $a \wedge 1 = 1$.
2. Pour tous entiers a, b, u, on a $a \wedge b = a \wedge (b + au)$.

Exercice 2. (IMO - 1959) Soit $n \in \mathbb{N}$. Démontrer que la fraction $\dfrac{21n+4}{14n+3}$ est irréductible.

Solution de l'exercice 2. Il faut démontrer que le pgcd de $21n+4$ et $14n+3$ est 1. Or ce pgcd vaut $14n+3 \wedge 7n+1 = 7n+1 \wedge 1 = 1$. □

En appliquant le principe du maximum, on peut reformuler la notion de pgcd en termes d'ensembles. Pour n un entier, on note $n\mathbb{Z}$ l'ensemble des multiples de n ; par ailleurs si A et B sont deux sous-ensembles de $\mathbb{Z}$ on pose A+B l'ensemble des sommes d'un élément de A et d'un élément de B.

Proposition 7 (Théorème de Bézout)**.** Soient a et b des entiers, on a $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$

Démonstration. Raisonnons par double inclusion, en posant $d = a \wedge b$. Tout élément de $a\mathbb{Z}$ est un multiple de a, donc de d, et de même pour b. Finalement un élément de $a\mathbb{Z} + b\mathbb{Z}$ est un multiple de d, ce qui donne l'une des inclusions.

Pour l'inclusion réciproque, observons qu'il suffit de montrer que $d \in a\mathbb{Z} + b\mathbb{Z}$. (pourquoi ? Exercice.) Observons d'abord que $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}^*$ est non vide, sauf si $a = b = 0$, auquel cas le résultat est vrai de toute façon. Sinon, soit $d' = u_0 a + v_0 b$ le plus petit des éléments de $a\mathbb{Z} + b\mathbb{Z} \cap \mathbb{N}^*$. Montrons que tout élément de $a\mathbb{Z} + b\mathbb{Z}$ est un multiple de d'. Si $c = ua + vb$, soit r le reste dans la division euclidienne de c par d'. Alors $r = ua + vb - q(u_0 a + v_0 b) \in (a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}$, et $r < d'$ par définition, donc $r = 0$ puisque d' est le plus petit élément de $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}$; autrement dit, $d'|c$. En particulier, $d'|a$ et $d'|b$, donc $d' \leq d$. Mais puisqu'on a montré $a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$, on a $d' \geq d$, et finalement $d' = d$. □

En particulier, il existe un couple u, v d'entiers tels que $d = au + bv$.

Exercice 3. Soient a, b, c trois entiers tels que $a|b$ et $a|c$. Prouver que $a|(b \wedge c)$, et que $\frac{b}{a} \wedge \frac{c}{a} = \dfrac{b \wedge c}{a}$.

Solution de l'exercice 3. On a exactement $\frac{b}{a}\mathbb{Z} + \frac{c}{a}\mathbb{Z} = \frac{1}{a}(b\mathbb{Z} + c\mathbb{Z})$. □

Exercice 4. Montrer que le pgcd est *associatif* : pour tous a, b, c, $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

Solution de l'exercice 4. On a $(a\mathbb{Z} + b\mathbb{Z}) + c\mathbb{Z} = a\mathbb{Z} + (b\mathbb{Z} + c\mathbb{Z})$. □

La propriété suivante est bien utile.

Proposition 8 (Un théorème de Gauß)**.** Si $a|bc$ et $a \wedge b = 1$, alors $a|c$.

Démonstration. On utilise le théorème de Bézout : il existe u et v tels que $1 = au + bv$. En multipliant par c, on trouve que $c = acu + bcv$ est somme de deux multiples de a, donc est un multiple de a. □

2 Nombres premiers et décomposition en facteurs premiers

Définition 9. Un entier $p > 1$ est dit premier lorsque les seuls diviseurs de p sont 1 et p.

Remarque 10. Par convention, 0 et 1 ne sont pas premiers.

Proposition 11. Il existe une infinité de nombres premiers.

Démonstration. Supposons l'inverse, et soit $p_1, \ldots, p_N$ la liste finie des nombres premiers. Que dire de $n = p_1 \cdots p_n + 1$? Il n'est pas dans cette liste, il est donc divisible par un nombre premier (pourquoi ? Exercice.), disons p_i. Mais p_i divise aussi $n - 1 = p_1 \ldots p_n$, donc p_i divise 1, ce qui est absurde. □

Comme on l'a vu au passage, si un nombre n'est pas premier, il est divisible par un nombre premier. Plus généralement,

Proposition 12 (Théorème fondamental de l'arithmétique)**.** Soit (p_k) la suite des nombres premiers, et $n > 1$ un entier. Alors il existe une unique suite (v_k) d'entiers positifs, tous nuls à partir d'un certain rang (qui dépend de n) tels que

$$n = \prod_{k=1}^{+\infty} p_k^{v_k}$$

L'entier v_k est appelé valuation p_k-adique de l'entier n.

Démonstration. L'existence se fait par récurrence forte sur n. Le résultat est vrai pour $n = 2$. Supposons-le vrai pour tous les entiers strictement plus petits que n. Alors ou bien n est un nombre premier, auquel cas l'affirmation est évidente ; ou bien $n = pn'$ pour un certain nombre premier p et un certain entier $n' < n$. On peut alors

décomposer n' en facteurs premiers par l'hypothèse, ce qui montre que n est de la forme demandée. □

Exercice 5. Exprimer, pour un entier n donné, la liste des diviseurs de n en fonction de sa décomposition en facteurs premiers. Comment calculer le pgcd de deux nombres ?

Solution de l'exercice 5. Par le théorème de Gauß, on voit que la relation de divisibilité de deux entiers $a|b$ est équivalente au fait que, pour tout nombre premier p, on ait $v_p(a) \leq v_p(b)$. Un argument combinatoire assez simple donne que le nombres d'entiers positifs divisant n est $\prod_p (v_p(n)+1)$ □

Proposition 13. Pour tout entier n et tout nombre premier p, on a $v_p(n!) = \sum_{k=1}^{+\infty} \lfloor \frac{n}{p^k} \rfloor$

Démonstration. Remarquons que cette somme est toujours définie, car nulle à partir d'un certain rang.

Dans un produit, les p-valuations s'additionnent. Raisonnons par récurrence. Le résultat est vrai pour $n = 1$. Supposons-le vrai pour $n-1$. Alors $n! = v_p((n-1)!) + v_p(n)$. L'entier $v_p(n)$ est le plus grand entier k tel que $p^k | n$. Par suite, pour $k \leq v_p(n)$, on a $\lfloor \frac{n}{p^k} \rfloor = \lfloor \frac{n-1}{p^k} \rfloor + 1$, et pour $k > v_p(n)$, on a $\lfloor \frac{n}{p^k} \rfloor = \lfloor \frac{n-1}{p^k} \rfloor$, ce qui permet de conclure. □

Exercice 6. Par combien de zéros l'écriture décimale de 2015! se termine-t-elle ?

Solution de l'exercice 6. Il faut calculer $v_2(2015!)$ et $v_5(2015)$. La réponse est le minimum de ces deux nombres. C'est forcément $v_5(2015!)$. Or $\lfloor \frac{2015}{5} \rfloor = 403$, par ailleurs $\lfloor \frac{2015}{25} \rfloor = 80$, ensuite $\lfloor \frac{2015}{125} \rfloor = 16$, enfin $\lfloor \frac{2015}{625} \rfloor = 3$. Donc la réponse est 502. □

Exercice 7. Soient n et k des entiers, montrer que la fraction suivante est un entier : $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$.

3 Congruences

On a déjà vu qu'il est souvent bénéfique de raisonner en termes de restes de division euclidienne. Si n est un entier, alors il existe n restes possibles dans la division euclidienne par n. On peut donc décomposer $\mathbb{Z}$ en n sous-ensembles, deux entiers étant dans le même sous-ensemble ssi ils ont le même reste modulo n. On dit que deux entiers sont congrus modulo n lorsqu'ils sont dans le même sous-ensemble. Ces sous-ensembles sont représentés par exemple par les restes modulo n, c'est-à-dire les

entiers de 0 à $n-1$. Plus généralement, on peut les représenter par n'importe quelle famille de n nombres, non congrus deux à deux. Par exemple, $(6,13)$ représente les classes de congruence modulo 2, aussi bien que $(0,1)$. On appelle $\mathbb{Z}/n\mathbb{Z}$ l'ensemble à n éléments des classes de congruence modulo n. Peut-on réaliser des opérations sur ces classes ?

> **Proposition 14.** Soient $n \geq 2$ un entier, et encore a, b, c, d des entiers, tels que $a \equiv b \mod n$ et $c \equiv d \mod n$. Alors $a + c \equiv b + d \mod n$, et $ac \equiv bd \mod n$.
>
> Si a, b, c sont des entiers tels que $ab \equiv ac \mod n$ et $a \wedge n = 1$, alors $b \equiv c \mod n$. Plus précisément, il existe $a' \in \mathbb{N}$ tel que $aa' \equiv 1 \mod n$.

Démonstration. Exercice. □

On peut donc réaliser sans ambiguïté des additions et des multiplications entre deux éléments de $\mathbb{Z}/n\mathbb{Z}$; on peut également diviser par un nombre premier avec n. En particulier, si n est premier, tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible !

Exercice 8. Montrer que si deux entiers a et b sont tels que $7|a^2 + b^2$, alors $7|a$ et $7|b$.

Le nombre 2016 est-il la somme de deux carrés ?

4 TD

Exercice 1. Soit n un entier. Montrer que n possède un nombre impair de diviseurs, si et seulement si n est le carré d'un autre entier.

Exercice 2. Soient x et y des entiers. Montrer que $7|2x+3y$ ssi $7|5x+4y$.

Exercice 3. Pour tous entiers a et b, démontrer que $a-1|a^b-1$, et que, par ailleurs, $\frac{a^b-1}{a-1} \wedge (a-1) = b \wedge (a-1)$.

Exercice 4. Soit $p > 3$ un nombre premier. Montrer que $12|p^2-1$.

Exercice 5. Trouver tous les entiers $n \in \mathbb{N}$ tels que 2^n+3 soit un carré parfait.

Exercice 6. Soit p un nombre premier, et $k \in \mathbb{N}$. Montrer que $p|\binom{p}{k}$.

Exercice 7. Soit n un entier, on appelle F_n le n-ième nombre de Fermat : $F_n = 2^{2^n}-1$. Montrer que les F_n sont deux à deux premiers entre eux.

Exercice 8. Soit n un entier, tel que $2n$ est la somme de deux carrés d'entiers. Montrer que n est lui-même la somme de deux carrés d'entiers.

Exercice 9. (Olympiades hongroises - 1978) Soit $n > 1$. Montrer que n^4+4^n n'est pas premier.

Exercice 10. (Olympiades internationales - 1986) Soit d un entier strictement positif n'appartenant pas à $\{2,5,13\}$. Montrer qu'il existe deux nombres distincts a et b dans $\{2,5,13,d\}$ tels que $ab-1$ ne soit pas le carré d'un entier.

Exercice 11. (Olympiades chinoises - 1988) Pour tout entier $n \geq 3$, on note $a(n)$ le plus petit entier positif ne divisant pas n. Si $a(n) \geq 3$, on peut réitérer ce procédé. Au bout de combien d'étapes atteint-on 2 ?

Exercice 12. Démontrer que, pour tout entier n, le réel $\sqrt{n}$ est ou bien entier, ou bien irrationnel.

Exercice 13. Montrer que pour tout nombre premier p congru à 3 modulo 4, si a et b sont tels que $p|a^2+b^2$, alors $p|a$ et $p|b$.

Le nombre 2015 est-il la somme de deux carrés ?

Exercice 14. (Olympiades bulgares - 1993) Soit $(a_n)_{n\in\mathbb{N}^*}$ une suite strictement croissante d'entiers naturels, telle que $a_{2n} = a_n + n$ pour tout n. On suppose de plus que si a_n est premier, alors n est premier. Calculer a_{1993}.