Chapitre 12 : Arithmétique

MPSI B Lycée Camille Jullian

22 janvier 2024

Les nombres sont le plus haut degré de la connaissance.
Le nombre est la connaissance même.

Platon.

L'arithmétique, c'est être capable de compter jusqu'à 20 *sans enlever ses chaussures.*

Walt Disney.

Ce court chapitre sera consacré aux bases d'un domaine pourtant important des mathématiques, celui de l'étude des nombres entiers. On se contentera ici d'étudier les entiers sous l'angle de l'arithmétique (en gros les propriétés liées à la divisibilité), mais il existe en fait un autre pan de cette étude (ce qu'on appelle aujourd'hui théorie des nombres) qui fait intervenir des outils beaucoup plus analytiques. Ce chapitre est pratiquement indépendant de tout ce qu'on a fait jusqu'ici cette année, mais sera d'une importance capitale pour comprendre une bonne partie du chapitre ultérieur que nous consacrerons aux polynômes, sur lesquels on retrouve une arithmétique très proche de celle des nombres entiers.

Objectifs du chapitre :

- comprendre les notions de pgcd et ppcm et les propriétés qui leur sont reliées.
- savoir exploiter les congruences et la décomposition en facteurs premiers pour résoudre des problèmes d'arithmétique.

1 Nombres premiers.

Définition 1. Soient n et p deux entiers relatifs, n est **divisible par** p (ou p divise n) s'il existe un troisième entier k tel que $n = kp$. On le note $p \mid n$. On dit également que n est un **multiple** de p.

Remarque 1. La relation de divisibilité est une relation d'ordre sur $\mathbb{N}$ mais pas sur $\mathbb{Z}$, où elle n'est pas antisymétrique. En effet, deux entiers relatifs qui se divisent l'un l'autre sont soit égaux soit opposés.

Définition 2. Deux entiers p et n tels que p divise n et n divise p sont appelés entiers **associés**.

Proposition 1. Si d est un diviseur commun des entiers n et p, alors d divise toute combinaison linéaire de n et p : $d \mid un + vp$, quels que soient $(u, v) \in \mathbb{Z}^2$.

Si p divise n, alors, $\forall k \in \mathbb{N}$, p^k divise n^k. Plus généralement, si $a \mid n$ et $b \mid p$, alors $ab \mid np$.

Démonstration. Tout est essentiellement trivial. Si d est un diviseur commun de n et p, alors $p = dk$ et $n = dl$, avec k et l deux entiers. On en déduit immédiatement que $un+vp = udl+vdk = d(un+vk)$ est un multiple de d. De même, si $n = qp$, alors $n^k = q^k p^k$ est un multiple de p^k. La dernière propriété se montre de même en multpliant les deux relations de divisibilité. □

Théorème 1. Division euclidienne.
Soit $n \in \mathbb{Z}$ et $p \in \mathbb{N}^*$, alors il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $n = pq + r$, avec $0 \leqslant r < p$. L'entier q est appelé **quotient** de la division euclidienne de n par p, et l'entier r **reste** de cette même division.

Démonstration. Commençons par prouver l'existence du couple (q, r), en supposant $n > 0$ (sinon, ce n'est pas beaucoup plus compliqué). Il existe certainement un entier a à partir duquel $ap > n$ (cette propriété présentée ici comme une évidence s'exprime de la façon suivante en langage mathématique pédant : « $\mathbb{R}$ est archimédien »). Notons alors $q = \max\{a \in \mathbb{N} \mid ap \leqslant n\}$, et $r = n - pq$. Par définition, $pq \leqslant n$, donc $r \geqslant 0$. De plus, par maximalité de q, on doit avoir $(q+1)p > n$, soit $pq + p - n > 0$, ou encore $p > n - pq = r$. Enfin, par définition de r, $n = pq + r$, l'existence du couple est donc prouvée.

Démontrons désormais l'unicité par l'absurde (c'est très classique pour démontrer des résultats d'unicité) en supposant qu'il y a deux couples convenables (q, r) et (q', r'). On a alors $pq+r = pq'+r' = n$, donc $p(q - q') = r' - r$. En particulier $r' - r$ divise p, alors que $-p < r' - r < p$. Ce n'est possible que si $r' - r = 0$, soit $r' = r$, ce qui implique $p(q' - q) = 0$, donc $q = q'$. Les deux couples sont alors identiques. □

Définition 3. Un entier naturel n est **premier** s'il n'est divisible que par 1 et par lui-même.

Remarque 2. Par convention, le nombre 1 n'est pas considéré comme un nombre premier.

Remarque 3. Il n'existe pas de méthode extrêmement simple pour savoir si un entier donné est premier ou non (à part tester sa divisibilité par tous les entiers ne dépassant pas sa racine carrée, ce qui est en pratique trop long pour des entiers très grands). Pour faire la liste des nombres premiers inférieurs à un entier donné, le plus simple est encore d'utiliser le **crible d'Eratosthène** : on place dans un tableau tous les entiers inférieurs à n (à partir de 2), et à chaque étape on entoure le plus petit entier disponible (qui sera nécessairement premier), et on raye tous ses multiples.

	(2)	(3)	~~4~~	(5)	~~6~~	(7)	~~8~~	~~9~~	~~10~~
(11)	~~12~~	(13)	~~14~~	~~15~~	~~16~~	(17)	~~18~~	(19)	~~20~~
~~21~~	~~22~~	(23)	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	(29)	~~30~~
(31)	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	(37)	~~38~~	~~39~~	~~40~~
(41)	~~42~~	(43)	~~44~~	~~45~~	~~46~~	(47)	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	(53)	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	(59)	~~60~~
(61)	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	(67)	~~68~~	~~69~~	~~70~~
(71)	~~72~~	(73)	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	(79)	~~80~~
~~81~~	~~82~~	(83)	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	(89)	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	(97)	~~98~~	~~99~~	~~100~~

Les nombres restants : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 et 97 sont tous premiers. Il y a donc 25 nombres premiers inférieurs ou égaux à 100. On peut démontrer plus généralement (mais c'est très compliqué) que le nombre de nombres premiers inférieurs à n devient proche de $\frac{n}{\ln(n)}$, plus précisément qu'il est équivalent à cette expression (c'est-à-dire que le quotient des deux tend vers 1, résultat connu sous le nom de théorème des nombres premiers), lorsque n tend vers $+\infty$ (ou, de façon équivalente, que le n-ème nombre premier vaut « à peu près » $n\ln(n)$).

Théorème 2. Il existe une infinité de nombres premiers.

Démonstration. Faisons un raisonnement par l'absurde : il existerait donc une liste finie p_1, p_2, …, p_k de nombres premiers. Notons alors $p = \prod_{i=1}^{k} p_i + 1$. Cet entier n'est sûrement pas divisible par p_1 (puisque l'entier qui le précède l'est et que $p_1 \geqslant 2$), ni par aucun des p_i. Soit il est lui-même premier (mais distinct des autres, ce qui est absurde), soit son plus petit diviseur non trivial (différent de 1) est un entier premier (sinon on pourrait trouver un diviseur encore plus petit), qui n'est lui-même aucun des p_i. Dans tous les cas, on aboutit à une contradiction. □

Définition 4. Deux entiers a et b sont **congrus modulo** n s'il existe un entier $k \in \mathbb{Z}$ tel que $b = a + kn$. On le note $b \equiv a[n]$.

Remarque 4. On a déjà croisé ces notations et définitions dans le chapitre de trigonométrie. Rappelons (les démonstrations sont évidentes) que la congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$, et que les congruences sont compatibles avec la somme (si $a \equiv b[n]$ et $c \equiv d[n]$, alors $a+c \equiv b+d[n]$) et avec le produit (si $a \equiv b[n]$ et $c \equiv d[n]$, alors $ac \equiv bd[n]$, en particulier on aura également $a^k \equiv b^k[n]$ pour tout entier naturel k). De plus, on peut « multiplier une congruence par un entier » : si $a \equiv b[n]$, alors $pa \equiv pb[pn]$.

Exemple : On souhaite prouver que $80^{427} + 82^{892}$ est un nombre divisible par 3. Cela revient simplement à dire que ce nombre immonde est congru à 0 modulo 3. Or, $80 \equiv -1[3]$ et $82 \equiv 0[3]$, donc $80^{427} + 82^{892} \equiv (-1)^{427} + 1^{892}[3] \equiv -1 + 1[3] \equiv 0[3]$, ce qui prouve le résultat.

Exercice : Calculer le reste de la division de 2^{424243} par 7.

Il est bien entendu hors de question d'effectuer entièrement cette division euclidienne, il faut trouver une astuce. Le plus simple est d'exploiter les congruences de puissances : $2^3 = 8 \equiv 1[7]$, donc, pour tout entier k, $2^{3k} \equiv 1^k[7] \equiv 1[7]$. Comme 424243 est de la forme $3k+1$ (ou, si on préfère, il est congru à 1 modulo 3), on en déduit que $2^{424243} \equiv 2^1[7] \equiv 2[7]$. De façon équivalente, on peut constater que les puissances de 2 ont des congruences modulo 7 qui sont périodiques de période 3 et valent donc alternativement 2, 4 et 1. Il suffit donc de connaitre le reste modulo 3 de l'exposant n pour connaitre celui modulo 7 de 2^n. C'est d'ailleurs vrai pour n'importe quel calcul de congruence de puissance, dès qu'on trouve un entier k pour lequel $a^k \equiv 1[b]$, le calcul de $a^n[b]$ se déduit de celui de $n[k]$.

2 PGCD, PPCM.

Définition 5. Soient n et p deux entiers non nuls. Le **plus grand commun diviseur** (ou pgcd) de n et p est, comme son nom l'indique, le plus grand entier divisant simultanément n et p. On le note parfois $n \wedge p$. Le **plus petit commun multiple** (ou ppcm) de n et p est le plus petit entier naturel que divisent n et p. On le note $n \vee p$.

Algorithme d'Euclide de calcul du PGCD : l'algorithme d'Euclide est basé sur le principe très simple suivant : si $a \equiv b[n]$, alors $a \wedge n = b \wedge n$. En effet, tout diviseur commun de a et de n divise également tout entier de la forme $a + kn$, donc divise b (et réciproquement). On peut donc calculer le pgcd de deux entiers naturels (si les entiers sont relatifs, leur pgcd sera identique à celui de leurs valeurs absolues) à l'aide de l'algorithme suivant :

- on pose $r_0 = a$ et $r_1 = b$
- tant que $r_k \neq 0$, on définit par récurrence r_k comme étant le reste de la division euclidienne de r_{k-2} par r_{k-1}.
- quand $r_k = 0$ l'avant-dernier reste calculé r_{k-1} est le pgcd des entiers a et b.

L'algorithme termine nécessairement puisque la suite (r_k) est constituée d'entiers naturel et décroit strictement. Le fait que le pgcd corresponde à l'avant-dernier reste est simplement une conséquence du fait que, si $r_k = 0$, $r_{k-1} \mid r_{k-2}$, donc $r_{k-2} \wedge r_{k-1} = r_{k-1}$.

Exemple : On souhaite calculer le pgcd des entiers $a = 1\ 386$ et $b = 942$. On effectue donc les divisions euclidiennes successives suivantes :

- $1\ 386 = 1 \times 942 + 444$, donc on pose $r_2 = 444$.
- $942 = 2 \times 444 + 54$, donc on pose $r_3 = 54$.
- $444 = 8 \times 54 + 12$, donc on pose $r_4 = 12$.
- $54 = 4 \times 12 + 6$, donc on pose $r_5 = 6$.
- enfin, $12 = 2 \times 6$, on arrête là et on conclut : $1\ 386 \wedge 942 = 6$.

Programmation en Python : pour la première fois de l'année, un peu d'informatique fait irruption dans notre cours de maths. Je vais même donner deux versions de l'algorithme d'Euclide en Python, la première classique et la deuxième récursive.

```
def euclide(a,b) :
    r,s=a,b
    while s>0 :
        r,s=s,r%s
    return r

def euclideRec(a,b) :
    if b==0 :
        return a
    return euclideRec(b,a%b)
```

Définition 6. Deux entiers n et p sont **premiers entre eux** si leur pgcd est égal à 1.

Théorème 3. Théorème de Bézout.
Deux entiers n et p sont premiers entre eux si et seulement s'il existe un couple d'entiers $(a, b) \in \mathbb{Z}^2$ tels que $an + bp = 1$. Plus généralement, il existe toujours un couple d'entiers relatifs tels que $an + bp = n \wedge p$.

Démonstration. On peut en fait prouver l'existence du couple (a, b), et même en donner un algorithme de calcul explicite, en adaptant un peu l'algorithme d'Euclide. En plus des variables r_k définies plus haut, on ajoute deux autres suites (u_k) et (v_k) initialisées de la façon suivante : $u_0 = 1$, $u_1 = 0$, $v_0 = 0$ et $v_1 = 1$. De plus, ces deux suites vérifient la même relation de récurrence que la suite (r_k) : $u_k = u_{k-2} - q_{k-1}u_{k-1}$ et $v_k = v_{k-2} - q_{k-1}kv_{k-1}$, où q_{k-1} est le quotient de la division euclidienne de r_{k-2} par r_{k-1}. Prouvons par récurrence double qu'on aura toujours $r_k = nu_k + pv_k$. Au rang 0, c'est bien le cas : $n \times 1 + p \times 0 = n = r_0$. De même, $n \times 0 + p \times 1 = p = u_1$. Si la relation est vérifiée aux rang $k-2$ et $k-1$, alors $r_k = r_{k-2} - q_k r_{k-1} = (nu_{k-2} + pv_{k-2}) - q_k(nu_{k-1} + pv_{k-1}) = n(u_{k-2} - q_k u_{k-1}) + p(v_{k-2} - q_k v_{k-1}) = nu_k + pv_k$, ce qui prouve l'hérédité. □

Exemple : Reprenons l'exemple détaillé plus haut du calcul de pgcd de 1 386 et de 942, et effectuons le calcul des termes des deux suites (u_k) et (v_k) :

- $q_1 = 1$ (cf divisions euclidiennes plus haut), donc $u_2 = u_0 - u_1 = 1$ et $v_2 = v_0 - v_1 = -1$, on a bien $1\,386 - 942 = 444 = r_2$.
- $q_2 = 2$, donc $u_3 = u_1 - 2u_2 = -2$ et $v_3 = v_1 - 2v_2 = 3$, on a bien $-2 \times 1\,386 + 3 \times 942 = 54 = r_3$.
- $q_3 = 8$, donc $u_4 = u_2 - 8u_3 = 17$ et $v_4 = v_2 - 8v_3 = -25$, on a bien $17 \times 1\,386 - 25 \times 942 = 12 = r_4$.
- $q_4 = 4$, donc $u_5 = u_3 - 4u_4 = -70$ et $v_5 = v_3 - 4v_4 = 103$, on a bien $-70 \times 1\,386 + 103 \times 942 = 6 = r_5$.

Remarque 5. On peut ajouter les propriétés classiques suivantes concernant le pgcd : tout diviseur commun à n et p divise nécessairement leur pgcd. De plus, si $k \in \mathbb{Z}$, $(ka) \wedge (kb) = |k| \times (a \wedge b)$. Cette dernière propriété est vérifiée également par le ppcm, et tout multiple commun de n et de p est un multiple de leur ppcm.

Théorème 4. Théorème de Gauss.
Si n et p sont deux entiers premiers entre eux, et $n \mid pk$, alors $n \mid k$.

Démonstration. D'après le théorème de Bézout, il existe un couple d'entiers (a, b) tel que $an+bp = 1$. On en déduit $k = ank+bpk$. Comme n divise de façon évidente ank et que n divise bpk par hypothèse, alors n divise k. □

Définition 7. Si n_1, n_2, …, n_k sont des entiers relatifs, leur pgcd est le plus grand entier naturel divisant simultanément tous les entiers n_i, pour i variant entre 1 et k. On définit de même le ppcm des entiers n_1, …, n_k.

Remarque 6. On vérifie très facilement que le pgcd et le ppcm sont des opérations associatives. On peut ainsi calculer des pgcd et ppcm d'ensembles quelconques d'entiers à l'aide de calculs successifs de pgcd et ppcm de deux entiers. De plus, les propriétés énoncées pour deux entiers restent valables pour une famille finie d'entiers. Ainsi, il existe toujours une famille $(a_1, a_2, \ldots, a_k)$ telle que $\sum_{i=1}^{k} a_i n_i =$ pgcd$(n_1, \ldots, n_k)$ (relation de Bézout pour une famille d'entiers).

Définition 8. Des entiers n_1, n_2, ..., n_k sont **premiers entre eux dans leur ensemble** si leur pgcd est égal à 1.

Remarque 7. Attention, cette notion ne signifie pas que ces entiers sont premiers entre eux **deux à deux** ! Par exemple, 42, 100 et 75 ne sont pas du tout premiers entre eux deux à deux : $42 \wedge 100 = 2$, $42 \wedge 75 = 3$ et $100 \wedge 75 = 25$. Pourtant, ils sont premiers entre eux dans leur ensemble puisque $(42 \wedge 100) \wedge 75 = 2 \wedge 75 = 1$.

3 Décomposition en facteurs premiers.

Définition 9. Si p est un entier premier, la **valuation p-adique** d'un entier n est définie par $v_p(n) = \max\{k \in \mathbb{N} \mid p^k \text{ divise } n\}$.

Ainsi, n a pour valuation p-adique 0 s'il n'est pas divisible par p. Plus cette valuation est élevée, plus n est divisible par des puissances élevées de p. Par exemple, $v_2(60) = 2$ (car 60 est divisible par 2 et par 4 mais pas par 8), $v_3(60) = 1$ et $v_5(60) = 1$. Toutes les autres valuations p-adiques de 60 sont égales à 0.

Proposition 2. La valuation p-adique est additive : pour tous entiers n et m, $v_p(nm) = v_p(n) + v_p(m)$.

Démonstration. En effet, si on note a et b les valuations p-adiques de n et de m, on peut par définition écrire $n = p^a \times q$, avec $q \wedge p = 1$ (puisque q n'est pas divisible par p qui est un entier premier), et de même $m = p^b \times q'$, avec $q' \wedge p = 1$. On en déduit que $nm = p^{a+b}qq'$, qui est évidemment divisible par p^{a+b} mais pas par p^{a+b+1} car qq' est premier avec p (si p divisait qq', en temps que nombre premier, il diviserait soit q soit q'). Finalement $v_p(nm) = a + b$. □

Théorème 5. Décomposition en facteurs premiers.

Tout nombre entier $n \geqslant 1$ peut se décomposer de façon unique sous la forme $n = \prod_{i=1}^{i=k} p_i^{\alpha_i} = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$, où $p_1 < p_2 < \cdots < p_k$ sont des nombres premiers distincts, et $(\alpha_1, \ldots, \alpha_k) \in (\mathbb{N}^*)^k$. De plus, $\alpha_i = v_{p_i}(n)$.

Démonstration. L'existence se prouve par une récurrence forte très simple : la décomposition existe de façon évidente pour $n = 1$ (dans ce cas très particulier, le produit est vide). Si on la suppose existante pour tout entier naturel inférieur ou égal à n, on a deux possibilités pour l'entier suivant $n+1$: soit il est premier et il n'y a rien à décomposer, soit il ne l'est pas et on peut l'écrire comme produit de deux entiers strictement inférieurs à $n+1$ auxquels on applique l'hypothèse de récurrence avant de faire leur produit. Quant à l'unicité, elle découle tout simplement de la proposition précédente : si $n = \prod_{i=1}^{i=k} p_i^{\alpha_i}$, alors on a nécessairement $v_{p_i}(n) = \alpha_i$, ce qui impose une décomposition unique. □

Proposition 3. Soient n et m deux entiers relatifs non nuls, alors $m \mid n$ si et seulement si $v_p(m) \leqslant v_p(n)$ pour tout entier premier p.

De plus, $n \wedge m = \prod_{p \text{ premier}} p^{\min(v_p(n), v_p(m))}$ et $n \vee m = \prod_{p \text{ premier}} p^{\max(v_p(n), v_p(m))}$

Démonstration. C'est assez évident : si m divise n, alors $n = km$, donc $v_p(n) = v_p(m) + v_p(k) \geqslant v_p(m)$ pour tout nombre premier p. Et la réciproque est vraiment claire : $p^{v_p(m)}$ divisera toujours $p^{v_p(n)}$, donc par produit m divisera n. Démontrons le second résultat uniquement pour le pgcd (c'est très similaire pour le ppcm). Notons donc $d = \prod_{p \text{ premier}} p^{\min(v_p(n), v_p(m))}$, d'après la première partie de la propriété, d est un diviseur commun de n et de m puisque ses valuations p-adiques sont par définition à la fois inférieures à celles de n et à celles de m. Peut-on trouver un diviseur commun plus grand ? Si c'était le cas, un tel entier aurait une décomposition en facteurs premiers avec au moins une valuation p-adique strictement supérieure à celle de d. Mais alors cet entier ne pourrait pas diviser l'entier parmi n et m qui a la même valuation p-adique que d, ce qui est absurde. □

Remarque 8. Une conséquence évidente de la deuxième partie de la proposition précédente est le résultat classique $(n \wedge m) \times (n \vee m) = n \times m$.

Exemple : La décomposition du nombre 384 est $2^7 \times 3$ (il suffit de diviser par 2 jusqu'à ce que ce ne soit plus possible, de recommencer avec 3, etc), et celle de 660 est $2^2 \times 3 \times 5 \times 11$. On calcule donc $384 \wedge 660 = 2^2 \times 3 = 12$, et $384 \vee 660 = 2^7 \times 3 \times 5 \times 11 = \dfrac{34 \times 660}{12} = 21\ 120$. Alternativement, on peut écrire $384 \vee 660 = \dfrac{384 \times 660}{12} = 384 \times 55 = 21\ 120$.

Théorème 6. Petit théorème de Fermat.

Si p est un entier premier, pour tout entier relatif n, on a $n^p \equiv n[p]$.

Si de plus $n \wedge p = 1$, alors $n^{p-1} \equiv 1[p]$.

Démonstration. Commençons par démontrer le résultat classique suivant : si $1 \leqslant k \leqslant p-1$, alors $\binom{p}{k}$ est divisible par p. En effet, la formule sans nom permet d'affirmer que $k \times \binom{p}{k} = p \times \binom{p-1}{k-1}$, donc $k \times \binom{p}{k}$ est divisible par p. Or k est premier avec p, donc $\binom{p}{k}$ est divisible par p. On constate ensuite à l'aide d'une formule du binôme assez brutale qu'on peut toujours écrire $(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k \equiv 1 + n^p[p]$. Autrement dit, les congruences modulo p des nombres n^p forment une suite arithmétique de raison 1. Comme $0^p \equiv 0[p]$, cette suite a simplement un terme général égal à n. Enfin, si n est premier avec p, on écrit simplement $n^p - n \equiv 0[p]$, donc $n^p - n$ est divisible par p. Mais $n^p - n = n(n^{p-1} - 1)$, avec n premier avec p. Le théorème de Gauss assure donc que $n^{p-1} - 1$ est divisible par p, c'est-à-dire que $n^{p-1} \equiv 1[p]$. □