Cours – Arithmétique

L'arithmétique désigne la branche mathématique qui traite des opérations et des propriétés des nombres entiers. Les premières découvertes en arithmétique, qui forgent toujours la base de ce que nous connaissons aujourd'hui, proviennent des écrits du grec Euclide. Il s'intéressait notamment aux divisibilités des entiers naturels, et aux nombres premiers. L'étude des nombres premiers est encore maintenant un domaine très riche et très actif dans la recherche mathématique, puisqu'elle possède plusieurs liens merveilleux avec d'autres domaines.

Sections

1. **pgcd**

   Thèmes : Divisibilité et calcul de pgcd via l'algorithme d'Euclide.

   Objectifs : Connaître les conditions qui définissent la division euclidienne. Connaître le lien entre pgcd et ppcm. Savoir poser une division d'entiers afin de calculer le quotient et le reste. Savoir calculer un pgcd à l'aide de l'algorithme d'Euclide.

2. **Théorème de Bézout**

   Thèmes : Le théorème de Bézout et les nombres premiers entre eux.

   Objectifs : Connaître le théorème de Bézout. Comprendre ce que sont les nombres premiers entre eux. Connaître le lemme de Gauss. Savoir calculer les coefficients de Bézout par remontée de l'algorithme d'Euclide.

3. **Nombres premiers**

   Thèmes : Les nombres premiers et la décomposition en facteurs premiers.

   Objectifs : Connaître la définition de nombre premier. Savoir qu'il en existe une infinité. Connaître le lemme d'Euclide. Savoir calculer une décomposition en facteurs premiers. Savoir en déduire des pgcd et ppcm.

4. **Congruences**

   Thèmes : Les calculs modulo un entier naturel n.

   Objectifs : Comprendre la définition de la congruence. Connaître le petit théorème de Fermat. Savoir faire des calculs modulo n.

Auteur : Barnabé Croizat de l'université de Lille.
Adaptation : Arnaud Bodin et Christine Sacré. Relecture de Guillemette Chapuisat.

Ce travail a été effectué en 2021-2022 dans le cadre d'un projet Hilisit porté par Unisciel.

Arithmétique – Partie 1 : pgcd

Savoir.

- ☐ Connaître les conditions qui définissent la division euclidienne.
- ☐ Connaître le lien entre pgcd et ppcm.

Savoir-faire.

- ☐ Savoir poser une division d'entiers afin de calculer le quotient et le reste.
- ☐ Savoir calculer un pgcd à l'aide de l'algorithme d'Euclide.

Division euclidienne

Dans tout ce chapitre, les lettres utilisées désigneront par défaut des nombres entiers. Des spécifications seront apportées dans les énoncés si besoin.

— **Définition de la division euclidienne.** Soit a un entier positif et b un entier strictement positif. Alors il existe des entiers q et r uniques tels que :

$$\boxed{a = bq + r \qquad \text{avec } 0 \leqslant r \leqslant b-1.}$$

— *Exemple.* $45 = 7 \times 6 + 3$ ou encore $117 = 13 \times 9 + 0$.

— On dit que b **divise** a s'il existe un entier k tel que $a = kb$. On note alors $b|a$. Cela revient à dire que le reste dans la division euclidienne de a par b est nul.

Il revient au même de dire que b *divise* a et que a *est un multiple de* b.

— Sur les exemples précédents $13 \mid 117$, mais 7 ne divise pas 45.

— **Proposition.** Si $a|b$ et $a|c$, alors pour tous les entiers m et n, $a|mb+nc$. En particulier a divise $b+c$ et $b-c$.

Preuve. Il s'agit d'une simple factorisation. On écrit $b = ka$ et $c = la$. Alors $mb + nc = mka + nla = (mk + nl)a$ qui est bien un multiple de a.

Critères de divisibilité

— Un entier est divisible par 2 (autrement dit c'est un entier pair) si et seulement si son chiffre des unités est 0, 2, 4, 6 ou 8.

— Un entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

— Un entier est divisible par 5 si et seulement si son chiffre des unités est 0 ou 5.

— Un entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

Exemple. $n = 35\,418$. Le chiffre des unités est 8 donc n est divisible par 2 mais pas par 5. La somme des chiffres est $3+5+4+1+8 = 21$. Comme 21 est divisible par 3 alors n est divisible par 3. En plus, comme 21 n'est divisible par 9 alors n n'est pas divisible par 9.

pgcd

— **Définition du pgcd.** Soient a et b deux entiers positifs. Le plus grand nombre entier qui divise à la fois a et b est appelé le **plus grand diviseur commun** de a et b. On le note $\text{pgcd}(a,b)$.

— *Exemple.* Les diviseurs communs de 24 et 36 sont les entiers : $1, 2, 3, 4, 6, 8, 12$. Ainsi le pgcd de 24 et 36 est 12.

— Le pgcd possède les propriétés suivantes :

$$\text{pgcd}(na, nb) = n\,\text{pgcd}(a,b) \qquad \text{pgcd}(a,0) = a \qquad \text{pgcd}(a,1) = 1$$

Algorithme d'Euclide

Une méthode pour calculer un pgcd est l'algorithme d'Euclide. Cette méthode est basée sur le résultat suivant :

Proposition. Soient deux entiers $a \geqslant 0$ et $b > 0$, et $a = bq + r$ le résultat de la division euclidienne de a par b. Alors $\boxed{\text{pgcd}(a,b) = \text{pgcd}(b,r)}$.

Preuve. Soit d un diviseur de a et de b. Alors d divise $a - bq$ donc d divise r. Réciproquement, si d divise b et r, il divise $bq + r$ donc il divise a. Ainsi les diviseurs communs de a et de b sont les mêmes que ceux de b et de r, donc en particulier le plus grand (le pgcd) est identique.

L'algorithme d'Euclide repose sur la proposition précédente : pour trouver le pgcd de deux entiers positifs a et b, on effectue la division euclidienne de a par b (ou le contraire si $b > a$) : $a = bq_0 + r_0$. Si le reste r_0 est nul, b est un diviseur de a, et par conséquent $\text{pgcd}(a,b) = b$. Sinon, on recommence en effectuant la division euclidienne de b par r_0 : $b = q_1 r_0 + r_1$. Si r_1 est nul, $\text{pgcd}(a,b) = \text{pgcd}(b,r_0) = r_0$. Sinon, on poursuit avec la division euclidienne de r_0 par r_1, et ainsi de suite.
Le processus se termine, car les restes forme une suite d'entiers positifs strictement décroissants. Enfin :

$$\boxed{\text{Le pgcd de } a \text{ et } b \text{ sera le dernier reste non nul.}}$$

Exemple. Recherchons $\text{pgcd}(1\,188, 120)$:

$$\begin{aligned} 1\,188 = 120 \times 9 + 108 \quad &\to \quad \text{pgcd}(1\,188, 120) = \text{pgcd}(120, 108) \\ 120 = 108 \times 1 + \boxed{12} \quad &\to \quad \text{pgcd}(120, 108) = \text{pgcd}(108, 12) \\ 108 = 12 \times 9 + 0 \quad &\to \quad \text{pgcd}(108, 12) = \text{pgcd}(12, 0) = 12 \end{aligned}$$

Ainsi on a $\text{pgcd}(1\,188, 120) = 12$.

Exemple. Cherchons maintenant à déterminer $\text{pgcd}(144, 48)$:

$$144 = 48 \times 3 + 0 \quad \to \quad \text{pgcd}(144, 48) = 48$$

48 est un diviseur de 144, donc $\text{pgcd}(144, 48) = 48$.

Exercice. Déterminer $\text{pgcd}(585, 247)$ et $\text{pgcd}(121, 73)$.

ppcm

— **Définition du ppcm.** Soient deux entiers positifs a et b, le **plus petit multiple commun** de a et b, noté $\text{ppcm}(a,b)$, est le plus petit entier positif qui est à la fois un multiple de a et un multiple de b.

— *Exemple.* Les multiples (positifs) commun à 9 et 12 sont 36, 72, 108,... Le ppcm de 9 et 12 est donc 36.

— *Lien entre le pgcd et le ppcm.* Le pgcd et le ppcm sont liés par la formule

$$\boxed{ab = \text{pgcd}(a,b) \times \text{ppcm}(a,b)}$$

Ceci permet d'obtenir le ppcm une fois qu'on a calculé le pgcd : $\text{ppcm}(a,b) = \frac{ab}{\text{pgcd}(a,b)}$

— *Exemple.* Puisque $\text{pgcd}(1\,188, 120) = 12$, on a : $\text{ppcm}(1\,188, 120) = \frac{1\,188\times 120}{12} = 11\,880$.

— *Autre exemple.* $\text{pgcd}(144, 48) = 48 \implies \text{ppcm}(144, 48) = \frac{144\times 48}{48} = 144$, ce qui est normal puisque 144 est lui-même un multiple de 48.

— *Facultatif.* Voici des explications concernant la relation pgcd/ppcm : $d|a$ donc $a = kd$, et $d|b$ donc $b = ld$. Ainsi $\frac{ab}{d} = kb = la$ est bien un multiple de a et de b. Pour montrer que $\frac{ab}{\text{pgcd}(a,b)}$ est bien le plus petit des multiples communs à a et b, nous aurons besoin soit du *lemme de Gauss*, soit de la *décomposition en facteurs premiers*, ce que nous verrons dans la suite.

Arithmétique – Partie 2 : Théorème de Bézout

Savoir.

- ☐ Connaître le théorème de Bézout.
- ☐ Comprendre ce que sont les nombres premiers entre eux.
- ☐ Connaître le lemme de Gauss.

Savoir-faire.

- ☐ Savoir calculer les coefficients de Bézout par remontée de l'algorithme d'Euclide.

Le théorème de Bézout

Théorème de Bézout. Soient a et b deux entiers positifs et $d = \text{pgcd}(a,b)$. Alors il existe deux entiers u et v tels que :

$$\boxed{au + bv = d}$$

Les coefficients de Bézout

Les entiers u et v de ce théorème (souvent appelés *coefficients de Bézout*) ne sont pas uniques ! Loin s'en faut... Mais on peut tout de même parvenir à déterminer un couple (u,v) convenable grâce à l'algorithme d'Euclide. C'est d'ailleurs sur cet algorithme que repose la preuve du théorème.
Nous allons expliquer la méthode sur un exemple. On a vu dans les exemples précédents que $\text{pgcd}(1\,188, 120) = 12$. Déterminons des entiers u et v tels que $1\,188u + 120v = 12$. La méthode consiste à "remonter" l'algorithme d'Euclide en exprimant, à partir du pgcd (qui est le dernier reste non nul), chaque reste comme une différence impliquant le dividende et le quotient.

Pour les calculs suivants il faut d'abord lire la colonne de gauche de haut en bas (qui n'est rien d'autre que l'algorithme d'Euclide), puis remonter la colonne de droite de bas en haut (afin de déterminer les coefficients de Bézout u et v).

$$\begin{aligned} 1\,188 = 120 \times 9 + 108 \quad &\rightarrow \quad \boxed{12} = 120 - 108 = 120 - (1\,188 - 120 \times 9) \\ &\qquad = 1\,188 \times (-1) + 120 \times 10 \\ 120 = 108 \times 1 + \boxed{12} \quad &\rightarrow \quad \boxed{12} = 120 - 108 \times 1 = 120 - 108 \end{aligned}$$

Ainsi on a $1\,188 \times (-1) + 120 \times 10 = 12$.

Exercice.

— Déterminer des entiers u et v tels que $585u + 247v = 13$.

— Déterminer des entiers u et v tels que $121u + 73v = 5$.

Nombres premiers entre eux

— Deux entiers a et b sont dits **premiers entre eux** si $\text{pgcd}(a,b) = 1$. Cela signifie que a et b n'ont aucun diviseur en commun autre que 1.

— **Variante du théorème de Bézout.**

$$\boxed{a \text{ et } b \text{ sont premiers entre eux} \iff \text{il existe } (u,v) \in \mathbb{Z}^2 \text{ tels que } au + bv = 1}$$

— *Démonstration.* Il s'agit d'un emploi du théorème de Bézout. Si $\text{pgcd}(a,b)=1$, alors le théorème de Bézout assure l'existence des entiers u et v tels que $au+bv=1$.
Réciproquement si $au+bv=1$, considérons d un diviseur commun à a et à b. $d|a$ et $d|b$ donc $d|au+bv$ et donc $d|1$! Le seul diviseur commun à a et b est donc 1, ce qui signifie qu'ils sont premiers entre eux.

— *Exercice.* Sachant que $83\times 11-24\times 38=1$, détermine quatre couples d'entiers qui sont premiers entre eux.

— *Exercice.* Dans chaque cas, explique si tu peux trouver des entiers u et v tels que $au+bv=1$ et si c'est le cas trouve-les effectivement :
  — $a=1\,498$ et $b=1\,122$
  — $a=331$ et $b=82$
  — $a=17\,802$ et $b=11\,043$

— Donnons un exemple d'utilisation un peu plus théorique de cette identité de Bézout en montrant que pour tout $n\in\mathbb{Z}$:

$$\text{pgcd}(2n+3,5n+7)=1.$$

En d'autres termes, les nombres $2n+3$ et $5n+7$ sont toujours premiers entre eux, quelle que soit la valeur de l'entier n.
Le but ici est de déterminer une identité de Bézout, c'est-à-dire de trouver des nombres u et v tels que $(2n+3)u+(5n+7)v=1$. Pour cela, on cherche donc à éliminer le nombre n : prenons $v=-2$ et $u=5$, cela donne :

$$(2n+3)\times 5+(5n+7)\times(-2)=10n+15-10n-14=1$$

D'après le théorème de Bézout, on a bien $\text{pgcd}(2n+3,5n+7)=1$.

Lemme de Gauss

Voici une application importante du théorème de Bézout.
Lemme de Gauss. Soient trois entiers non nuls a,b,c.

Si $a\|bc$ et $\text{pgcd}(a,b)=1$, alors $a\|c$

Démonstration. Puisque $a|bc$, il existe $k\in\mathbb{Z}$ tel que $bc=ka$. D'autre part, d'après le théorème de Bézout on a $au+bv=1$. On multiplie l'égalité de Bézout par c : $auc+bcv=c$. Puis on remplace bc par ka : $auc+kav=c$. Ainsi $a(uc+kv)=c$ c'est-à-dire $a|c$.

Corollaire. Si a et b divisent c et $\text{pgcd}(a,b)=1$, alors $ab|c$.
Démonstration. On sait que $c=ka=lb$. Donc $a|lb$, mais $\text{pgcd}(a,b)=1$ et d'après le lemme de Gauss $a|l$ donc $l=am$. Par conséquent $c=lb=amb$ et ainsi $ab|c$.

Exemples.

— *Exemple 1.* $273=7\times 39=13\times 21$; donc $13|(7\times 39)$.
Or $\text{pgcd}(13,7)=1$, donc d'après le lemme de Gauss $13|39$.

— *Exemple 2.* Montrons que pour tout $n\in\mathbb{Z}$, $\frac{n(n+1)(n+2)}{6}$ est un entier.
  — Il s'agit de montrer $6|n(n+1)(n+2)$. Puisque n et $n+1$ sont deux entiers consécutifs, l'un des deux est un multiple de 2, donc $2|n(n+1)$ et a fortiori $2|n(n+1)(n+2)$.
  — Pour la même raison, n, $n+1$ et $n+2$ sont trois entiers consécutifs donc l'un des trois est un multiple de 3. Ainsi $3|n(n+1)(n+2)$.
  — Puisque 2 et 3 sont premiers entre eux, d'après le (corollaire du) lemme de Gauss, 2×3 divise $n(n+1)(n+2)$, donc $6|n(n+1)(n+2)$.

— *Exemple 3.* Pour finir, remarquons que $6|12$ et $4|12$, mais pourtant $6\times 4=24$ ne divise pas 12 ! Cela vient bien sûr du fait que 6 et 4 ne sont pas premiers entre eux.

— *Exercice.* Montrer que pour tout entier $n\in\mathbb{Z}$, $(n^3-4n)(n^2-1)$ est un multiple de 15 (et même en fait un multiple de 30).

Autre application du théorème de Bézout

— **Proposition.** Soient deux entiers a et b et $d = \text{pgcd}(a, b)$. Si l'on note $a = da'$ et $b = db'$, alors les entiers a' et b' sont premiers entre eux.

— *Démonstration.* Il s'agit d'une application de la propriété $\text{pgcd}(na, na) = |n|\,\text{pgcd}(a, b)$. En effet, $\text{pgcd}(a, b) = d = \text{pgcd}(da', db') = d\,\text{pgcd}(a', b')$ donc $\text{pgcd}(a', b') = \frac{d}{d} = 1$.

— *Exemple.* Puisque $\text{pgcd}(1\,188, 120) = 12$, alors 12 divise 1 188 et 120. On obtient :

$$\text{pgcd}\left(\frac{1\,188}{12}, \frac{120}{12}\right) = \text{pgcd}(99, 10) = 1$$

De même, puisque $\text{pgcd}(144, 48) = 48$, on a : $\text{pgcd}(\frac{144}{48}, \frac{48}{48}) = \text{pgcd}(3, 1) = 1$.

Arithmétique – Partie 3 : Nombres premiers

Savoir.

- ☐ Connaître la définition de nombre premier.
- ☐ Savoir qu'il en existe une infinité.
- ☐ Connaître le lemme d'Euclide.

Savoir-faire.

- ☐ Savoir calculer une décomposition en facteurs premiers.
- ☐ Savoir en déduire des pgcd et ppcm.

Les nombres premiers

— **Définition.** Un **nombre premier** est un entier naturel supérieur ou égal à 2 qui n'est divisible que par 1 et par lui-même.

— *Exemple.* $2, 3, 5$ ou encore 17 sont des nombres premiers. En revanche $9 = 3 \times 3$ ou encore $14 = 2 \times 7$ ne sont pas premiers.

— **Lemme.** Tout entier naturel $n \geqslant 2$ admet un diviseur premier.

— *Démonstration.* Si n est lui-même premier, il n'y a rien à démontrer (car n se divise lui-même).
Sinon, cela signifie que n admet un diviseur strictement compris entre 1 et n. Notons $\mathscr{D}$ l'ensemble des diviseurs de n strictement compris entre 1 et n. Cet ensemble d'entiers est non vide, donc il possède un plus petit élément, que nous noterons p.
Supposons par l'absurde que p ne soit pas premier, alors il possède lui-même un diviseur q strictement compris entre 1 et p. Mais $q|p$ et $p|n$ donc $q|n$. Ainsi q est un diviseur de n (qui n'est pas 1) et qui est plus petit que p. Ceci est une contradiction car p est le plus petit diviseur de n.
Donc p est premier, et par conséquent n est bien divisible par un nombre premier.

Théorème (Euclide).

Il existe une infinité de nombres premiers.

Démonstration. Voilà la démonstration d'Euclide, par l'absurde :
Supposons que l'ensemble des nombres premiers soit fini : on les note alors $p_1, p_2, ..., p_n$. Soit

$$N := p_1 \times p_2 \times \cdots \times p_n \ + 1 = \prod_{i=1}^{n} p_i \ + \ 1$$

N admet un diviseur premier d'après le lemme précédent. Notons p_k un tel diviseur. $p_k|N$, mais $p_k|(\prod_{i=1}^{n} p_i)$ donc $p_k|N - (\prod_{i=1}^{n} p_i) = 1$. Ainsi $p_k|1$ donc $p_k = 1$ ce qui est une contradiction avec $p_k \geqslant 2$.
Ceci démontre par l'absurde que l'ensemble des nombres premiers est infini.

Lemme d'Euclide

Lemme d'Euclide. Soit p un nombre premier et a et b deux entiers.

Si $p|ab$, alors $p|a$ ou $p|b$.

Démonstration. Supposons que p ne divise pas a. Ceci signifie que $\text{pgcd}(p, a) = 1$ puisque les seuls diviseurs de p sont p et 1. On applique le lemme de Gauss : $p|ab$ et $\text{pgcd}(p, a) = 1 \implies p|b$.

Exercice. Soit p un nombre premier, montrer que $\sqrt{p}$ n'est pas un rationnel en utilisant le lemme de Gauss.

Décomposition en produit de facteurs premiers

Décomposition en produit de facteurs premiers. Soit un entier $n \geqslant 2$. Il existe une unique suite de nombres premiers $p_1 < p_2 < \cdots < p_k$ et une unique suite d'exposants entiers positifs non nuls $\alpha_1, \alpha_2, ..., \alpha_k$ tel que :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$$

Remarques.

— Les démonstrations de l'existence et de l'unicité de cette décomposition peuvent s'effectuer par récurrence.

— L'entier n admet au moins un facteur premier p_i tel que $p_i \leqslant \sqrt{n}$; si ce n'est pas le cas, cela signifie que n est premier ! Ceci est pratique pour démontrer qu'un nombre fixé est premier ou non.

Exemples.

— Le nombre 271 est un nombre premier. En effet, il n'est pas divisible par $2, 3, 5, 7, 11$ ou 13. Et cela suffit à assurer qu'il est premier puisque $\sqrt{271} \simeq 16,5 < 17$

— Recherchons la décomposition en facteurs premiers de 1 188 :

$$1\,188 = 2 \times 594 = 2^2 \times 297 = 2^2 \times 3 \times 99 = 2^2 \times 3^2 \times 33 = 2^2 \times 3^3 \times 11$$

Et cette dernière égalité est bien la décomposition en facteurs premiers.

pgcd

Proposition. Soient deux entiers $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $m = \prod_{i=1}^{k} p_i^{\beta_i}$ (avec α_i et β_i éventuellement nuls). On a alors :

$$\begin{cases} \text{pgcd}(n,m) & = \prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)} \\ \text{ppcm}(n,m) & = \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)} \end{cases}$$

En d'autres termes, on compare les exposants des nombres entiers p présents dans les décompositions de m et de n. Le plus petit exposant (c'est éventuellement 0) sera celui de $\text{pgcd}(n,m)$, et le plus grand exposant est celui de $\text{ppcm}(n,m)$.

Exemple. Reprenons l'exemple de 1 188 et de 120.

— On a déjà obtenu la décomposition en facteurs premiers de $1\,188 = 2^2 \times 3^3 \times 11$.

— Recherchons celle de 120 : $120 = 2 \times 60 = 2^2 \times 30 = 2^3 \times 15 = 2^3 \times 3 \times 5$.

— Réécrivons les décompositions en faisant apparaître tous les facteurs premiers présents dans au moins l'une des décompositions :

$$\begin{cases} 1\,188 & = 2^2 \times 3^3 \times 5^0 \times 11^1 \\ 120 & = 2^3 \times 3^1 \times 5^1 \times 11^0 \end{cases}$$

On obtient alors leur pgcd et leur ppcm en choisissant respectivement le plus petit et le plus grand des exposants pour chaque facteur premier :

$$\begin{cases} \text{pgcd}(1\,188, 120) & = 2^2 \times 3^1 \times 5^0 \times 11^0 = 4 \times 3 = 12 \\ \text{ppcm}(1\,188, 120) & = 2^3 \times 3^3 \times 5^1 \times 11^1 = 8 \times 27 \times 5 \times 11 = 11\,880 \end{cases}$$

Exercice. Déterminer les décompositions en produit de facteurs premiers de 585 et de 247, puis en déduire leur pgcd et leur ppcm.

Arithmétique – Partie 4 : Congruences

Savoir.

- ☐ Comprendre la définition de la congruence.
- ☐ Connaître le petit théorème de Fermat.

Savoir-faire.

- ☐ Savoir faire des calculs modulo n.

Congruences

Définition. Soient a et b deux entiers et un entier naturel $n \geqslant 2$. On dit que ***a* est congru à *b* modulo *n*** si n divise la différence $(b-a)$. On note alors :

$$\boxed{a \equiv b\ [n]}$$

Remarques.

— $a \equiv b\ [n]$ revient à dire que les restes de a et de b dans la division euclidienne par n sont les mêmes. Cela veut aussi dire que a et b ne diffèrent que d'un multiple de n, ce qui s'écrit $b = a + kn,\ k \in \mathbb{Z}$.
C'est ainsi que $13 \equiv 8 \equiv 3 \equiv -2\ [5]$ puisque tous ces nombres ne diffèrent entre eux que de multiples de 5.

— On voit parfois dans les livres la notation $a \equiv b\ \pmod{n}$.

— $a \equiv 0\ [n]$ signifie que $n|a$.

Exemples.

— $65 \equiv 2\ [7]$. En effet 7 divise $65-2=63$ (ou encore $65 = 7 \times 9 + \mathbf{2}$).

— $13\,145 \equiv 165 \equiv 5\ [10]$. En fait un nombre entier est congru à un autre modulo 10 s'ils se terminent par le même chiffre.

— $n \equiv 0\ [2]$ signifie que n est pair, et $n \equiv 1\ [2]$ que n est impair.
Il n'y a donc que 2 possibilités modulo 2 : être congru à 0 ou à 1. De même il n'y a que trois possibilités modulo 3 : être congru à $0, 1$ ou 2 (ou encore $0, 1$ et -1 car $-1 \equiv 2\ [3]$!).
De manière générale, il y a n possibilités modulo n.

Calculs

Les congruences sont bien adaptées aux additions, soustractions et aux multiplications : autrement dit, on peut y faire de l'arithmétique.

Les règles de calcul. Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors :

$$\boxed{a + c \equiv b + d\ [n] \quad \text{(addition)}}$$

et aussi

$$a - c \equiv b - d\ [n] \quad \text{(soustraction)}$$

enfin

$$\boxed{ac \equiv bd\ [n] \quad \text{(multiplication)}}$$

*Attention.*Il n'est pas question de parler d'une éventuelle opération de division dans le monde du *modulo* ! En effet, ce monde se préoccupe exclusivement des nombres **entiers** ! On s'échapperait de ce monde merveilleux si on se hasardait à y tenter de la division... Par exemple il serait **extrêmement FAUX** de dire que :

$$2 \equiv 12\,[10] \quad \cancel{\Longrightarrow \quad \frac{2}{12} \equiv 1\,[10]}$$

Aussi on ne peut pas simplifier, par exemple ci-dessous diviser par 2 n'a pas de sens :

$$6 \equiv 2\,[4] \quad \cancel{\Longrightarrow \quad 3 \equiv 1\,[4]}$$

Démonstration des règles de calcul.

— $n|(b-a)$ et $n|(d-c)$, donc n divise l'addition $(b-a)+(d-c) = (b+d)-(a+c)$ (d'où la règle d'addition) et la soustraction $(b-a)-(d-c) = (b-d)-(a-c)$ (d'où la règle de soustraction).

— Pour la multiplication, $n|(b-a)$ donc $n|d(b-a) = db-da$ d'une part ; et $n|(d-c)$ donc $n|a(d-c) = ad-ac$ d'autre part. Par addition, $n|db-da+ad-ac = db-ac$ d'où la règle de multiplication.

Corollaire. Si $a \equiv b\,[n]$, alors pour tout entier l : $la \equiv lb\,[n]$ et pour tout entier k positif, on a :

$$\boxed{a^k \equiv b^k\,[n]}$$

Exemples.

— Commençons par déterminer si le nombre $4^{48}-1$ est ou non un multiple de 5.
Il s'agit de voir si $4^{48}-1 \equiv 0\,[5]$ est vraie.
Puisque $4^2 = 16 = 3\times 5+1$, on obtient $4^2 \equiv 1\,[5]$. On passe cette égalité à la puissance 24 (d'après le corollaire) puis on retranchera 1 (d'après les règles de soustraction) :

$$4^2 \equiv 1\,[5] \Longrightarrow (4^2)^{24} \equiv 1^{24}\,[5] \Longleftrightarrow 4^{48} \equiv 1\,[5] \Longleftrightarrow 4^{48}-1 \equiv 0\,[5]$$

Ainsi le nombre $4^{48}-1$ est bien un multiple de 5. Parviens-tu, en utilisant les congruences modulo 2, à déterminer s'il se termine par 0 ou par 5 ?

— Cherchons à présent quel est le chiffre des unités du nombre $3^{240}+7^{240}$. Il s'agit de déterminer la congruence de ce nombre modulo 10.
Tout d'abord, $3^2 = 9$ est congru à -1 modulo 10.
Ce sera notre point de départ :

$$3^2 \equiv -1\,[10] \Longrightarrow (3^2)^{120} \equiv (-1)^{120}\,[10] \Longleftrightarrow 3^{240} \equiv 1\,[10]$$

On rappelle que calculer $(-1)^k$ est facile : c'est $+1$ si k est pair et -1 si k est impair. Passons à la puissance de 7 : puisque $7^2 = 49$ est congru à -1 modulo 10, on obtient de même :

$$7^2 \equiv -1\,[10] \Longrightarrow (7^2)^{120} \equiv (-1)^{120}\,[10] \Longleftrightarrow 7^{240} \equiv 1\,[10]$$

Ainsi par addition, $3^{240}+7^{240} \equiv 2\,[10]$ ce qui signifie que son chiffre des unités est 2.

Exercice.

1. Montrer que pour tout entier naturel n, le nombre $4^{3n}-4^n$ est un multiple de 5.
2. Montrer que "$13|(5^{2n}+3^{3n}) \Longleftrightarrow n$ est impair".

Petit théorème de Fermat

Le calcul des congruences est particulièrement intéressant lorsque le modulo choisi est lui-même un nombre premier. C'est notamment ce qu'illustre le petit théorème de Fermat :
Petit théorème de Fermat (1 640). Si p est un nombre premier, alors pour tout entier x on a :

$$\boxed{x^p \equiv x\,[p]}$$

En particulier, **si x n'est pas un multiple de p**, alors :

$$\boxed{x^{p-1} \equiv 1\,[p]}$$

Exemple. Calculons $5^{2\,022}$ modulo 13.

— D'après le petit théorème de Fermat, 13 étant premier et 5 n'étant pas un multiple de 13, on sait que $5^{12} \equiv 1\,[13]$.

— Par ailleurs la division euclidienne de 2 022 par 12 est $= 2\,022 = 12 \times 168 + 6$. Donc en passant à la puissance 168 on obtient $5^{12\times 168} = (5^{12})^{168} \equiv 1\,[13]$.

— Or $5^2 \equiv 25 \equiv -1\,[13]$, ainsi $5^6 = (5^2)^3 \equiv (-1)^3 \equiv -1\,[13]$.
Par multiplication, on obtient : $5^{2\,022} \equiv 5^{12\times 168} \times 5^6 \equiv 1 \times (-1) \equiv -1 \equiv 12\,[13]$.

Exercice. Calculer 4^{253} modulo 11 et 25^{71} modulo 7.