Concepts de base en arithmétique

Jean-Louis Tu

Objectifs de ce document

Ce document s'adresse à tout élève de fin de collège ou début de lycée souhaitant s'initier aux exercices d'arithmétique de type olympique. Il rassemble les connaissances nécessaires et suffisantes pour pouvoir résoudre des exercices de compétition pour les juniors. Sa lecture est indispensable à tout élève débutant en arithmétique et souhaitant participer aux activités de l'OFM (envois d'exercices par correspondance, stages).

Les exercices de ce document sont pour l'essentiel des exercices d'apprentissage, et permettent d'acquérir certains réflexes, mais sont rarement des exercices de compétition. Par conséquent, pour être *performant* en situation de concours, l'élève devra les compléter par d'autres, par exemple le poly d'arithmétique plus volumineux disponible à l'adresse :

http://www.animath.fr/IMG/pdf/cours-arith1.pdf

Table des matières

1 Préliminaires

1.1 Notations

On note $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ l'ensemble des entiers naturels, $\mathbb{N}^*$ l'ensemble des entiers naturels non nuls ;

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ l'ensemble des entiers relatifs ;

$\mathbb{Q}$ l'ensemble des nombres rationnels, c'est-à-dire qui peuvent s'écrire sous la forme $\frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$;

$\mathbb{R}$ l'ensemble des nombres réels.

$\mathbb{Q}^*$ désigne l'ensemble des rationnels non nuls, $\mathbb{Q}_+^*$ l'ensemble des rationnels strictement positifs et $\mathbb{Q}_-^*$ l'ensemble des rationnels strictement négatifs. On introduit de même les notations $\mathbb{Z}_-$, $\mathbb{Z}^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$, $\mathbb{R}_-^*$.

Si a et b sont deux nombres, alors ab désigne le produit $a \times b$.

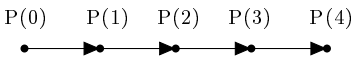
1.2 Principe de récurrence

Dans ce document, nous utiliserons fréquemment le principe de récurrence suivant.

Soit $P(n)$ une propriété d'un entier n. On suppose que

(i) (initialisation) $P(0)$ est vraie

(ii) (hérédité) pour tout entier naturel n, si $P(n)$ est vraie alors $P(n+1)$ est vraie.



Alors $P(n)$ est vraie pour tout n.

Vocabulaire : lorsque l'on essaye de démontrer l'implication $P(n) \implies P(n+1)$, la propriété $P(n)$ que l'on suppose vraie s'appelle *l'hypothèse de récurrence*.

Une variante de ce principe est la récurrence forte : supposons que

(i) (initialisation) $P(0)$ est vraie

(ii) (hérédité) pour tout entier naturel n, si $P(k)$ est vraie pour tout $k \leqslant n$ alors $P(n+1)$ est vraie.

Alors $P(n)$ est vraie pour tout n.

1.3 Mode d'emploi des exercices

Trois niveaux de difficultés (sans doute subjectifs) sont indiqués pour les exercices.

Les exercices non marqués sont des tests de compréhension immédiate, ou bien demandent simplement d'appliquer une méthode indiquée quelques lignes plus haut.

Les exercices marqués avec le symbole ¶ peuvent demander une petite idée non évidente, ou un peu de calcul.

Les exercices marqués avec ¶¶ nécessitent un temps de réflexion un peu plus long.

2 Divisibilité

Définition 2.1.

Soient a, b deux entiers relatifs. On dit que a divise b (ou que b est divisible par a, ou que b est un multiple de a) s'il existe un entier c tel que $b = ac$. On note $a \mid b$.

Par exemple, $2 \mid 6$, $2 \nmid 7$, $1 \mid n$, $n \mid n$, $n \mid 0$ pour tout entier n.

Proposition 2.2.

Soient a, b, b', c, λ des entiers.
(i) (Transitivité) Si $a \mid b$ et $b \mid c$ alors $a \mid c$.
(ii) Si $a \mid b$ alors $a \mid bc$.
(iii) Si $a \mid b$ et $a \mid b'$ alors $a \mid b + b'$.
(iv) Si $a \mid b$ et $a \mid b'$ alors $a \mid b + \lambda b'$.
(v) Si $\lambda \neq 0$ alors $a \mid b$ si et seulement si $\lambda a \mid \lambda b$.
(vi) Si $a \mid b$ et $b \neq 0$ alors $|a| \leqslant |b|$.
(vii) Si $a \mid b$ et $b \mid a$ alors $b = a$ ou $b = -a$.

Démonstration. (i) Par définition, il existe u et v tels que $b = au$ et $c = bv$. On a alors $c = (au)v = a(uv)$ donc $a \mid c$.

(ii) Il est clair que $b \mid bc$. D'après (i), on en déduit que $a \mid bc$.

(iii) Il existe u et v tels que $b = au$ et $b' = av$. On a alors $b + b' = au + av = a(u + v)$ donc $a \mid b + b'$.

(iv) D'après (ii), on a $a \mid \lambda b'$, et d'après (iii) on en déduit que $a \mid b + (\lambda b')$.

(v) Si $a \mid b$, alors il existe u tel que $b = au$. Ceci entraîne $\lambda b = (\lambda a)u$ donc $\lambda a \mid \lambda b$.
Réciproquement, si $\lambda a \mid \lambda b$, alors il existe v tel que $\lambda b = \lambda a u$. Comme $\lambda \neq 0$, on peut diviser par λ, ce qui donne $b = au$, autrement dit $a \mid b$.

(vi) Soit u tel que $b = au$. Comme $b \neq 0$, on a $u \neq 0$, donc $1 \leqslant |u|$. En multipliant membre à membre par $|a|$, on obtient $|a| \leqslant |au| = |b|$.

(vii) On suppose que $a \mid b$ et $b \mid a$.
Si $a = 0$, alors le fait que $a \mid b$ entraîne $b = 0$ donc on a bien $b = a$ ou $b = -a$. De même, si $b = 0$ alors $b = a$ ou $b = -a$.
Si $a \neq 0$ et $b \neq 0$, alors d'après (vi) on a $|a| \leqslant |b|$ et $|b| \leqslant |a|$, donc $|a| = |b|$, ce qui donne bien $b = a$ ou $b = -a$. □

Exercice 2.1.

Montrer que si $a \mid b$ et $c \mid d$ alors $ac \mid bd$.

Exercice 2.2.

Quels sont les entiers $n \in \mathbb{N}$ tels que $n \mid n+7$?

Exercice 2.3.

Quels sont les entiers $n \in \mathbb{N}$ tels que $n^2+1 \mid n$?

Exercice 2.4.

Montrer que pour tout entier n, l'entier $n(n+1)$ est pair.

Exercice 2.5.

Montrer que pour tout entier n, l'entier $n(n+1)(n+2)$ est divisible par 6.

Exercice 2.6.

Soient a, b, c des entiers. Montrer que si n est un entier vérifiant $an^2+bn+c=0$ alors $n \mid c$.

Exercice 2.7.

¶Déterminer les entiers n tels que $n^5-2n^4-7n^2-7n+3=0$.

Exercice 2.8.

¶Soient $a \geqslant 1$ et n des entiers tels que $a \mid n+2$ et $a \mid n^2+n+5$. Montrer que $a=1$ ou $a=7$.

La division Euclidienne permet de tester si un entier est divisible par un autre.

Théorème 2.3.

Soient a et b deux entiers tels que $b \geqslant 1$. Alors il existe un et un seul couple (q,r) d'entiers tel que

- $a = bq + r$;
- $0 \leqslant r \leqslant b-1$.

Les entiers q et r s'appellent respectivement le quotient et le reste de la division Euclidienne de a par b.

Démonstration. Montrons d'abord l'unicité. Si $a = bq + r = bq' + r'$ avec $0 \leqslant r \leqslant b-1$ et $0 \leqslant r' \leqslant b-1$, alors $bq - bq' = r' - r$, donc $b|q - q'| = |r' - r| < b$. En divisant par b, on en déduit $|q - q'| < 1$, donc $q = q'$. Il vient $r' - r = bq - bq' = 0$, puis $r = r'$.

Montrons l'existence. Traitons d'abord le cas $a \geqslant 0$. Remarquons d'abord que

- il existe des entiers x tels que $bx \leqslant a$ (par exemple $x = 0$) ;
- si $x > a$ alors $bx > a$ (puisque $bx > ba$).

Il existe donc un plus grand entier q tel que $bq \leqslant a$. Par définition de q, on a $b(q+1) > a$, c'est-à-dire $bq + b > a$. Posons $r = a - bq$, on a alors $0 \leqslant r < b$, ce qui prouve l'existence dans le cas $a \geqslant 0$.

Si maintenant $a < 0$, on remarque que $a - ba = (b-1)(-a) \geqslant 0$. On applique la division Euclidienne de $a - ba$ par b : il existe q' et r tels que $a - ba = bq' + r$ et $0 \leqslant r < b$. On a alors $a = b(a + q') + r = bq + r$ avec $q = a + q'$. □

Exemple : pour $a = 25$ et $b = 7$, le quotient est 3 et le reste est 4. Pour déterminer ces valeurs, on a en fait procédé exactement comme dans la preuve du théorème. On essaye $7 \times 1 = 7$, $7 \times 2 = 14$, $7 \times 3 = 21$, $7 \times 4 = 28$ dépasse la valeur a. Donc le quotient q est égal à 3. Pour calculer le reste, on effectue la soustraction $25 - (7 \times 3)$.

Remarque 2.4.

Si b est un entier *relatif* non nul quelconque, il existe encore un et un seul couple (q, r) d'entiers tel que $a = bq + r$ et $0 \leqslant r \leqslant |b| - 1$. Le cas $b \geqslant 1$ ayant déjà été traité, supposons $b \leqslant -1$. L'unicité se montre de la même façon. Pour l'existence, on effectue la division Euclidienne de a par $-b$, ce qui permet d'écrire $a = (-b)q' + r$. On pose alors $q = -q'$ et on a $a = bq + r$.

Par exemple, la division Euclidienne de -17 par -5 s'écrit $-17 = (-5) \times 4 + 3$.

Proposition 2.5.

Soient a, b, d, q, r des entiers. On suppose que $a = bq + r$. Alors d divise a et b si et seulement si d divise b et r.

Démonstration. Si d divise a et b alors d divise $a - bq$ d'après la Proposition 2(iv), donc d divise b et r. De même, si d divise b et r alors d divise $bq + r = a$. □

Soient maintenant $a \geqslant b > 0$. L'algorithme d'Euclide consiste à effectuer des divisions Euclidiennes successives : on pose $a_0 = a$ et $a_1 = b$, puis pour tout $k \geqslant 0$ on effectue la division Euclidienne de a_k par a_{k+1} et on appelle a_{k+2} le reste.

$$\begin{aligned} a_0 &= a_1q_1 + a_2 \\ a_1 &= a_2q_2 + a_3 \\ a_2 &= a_3q_3 + a_4 \\ &\cdots \\ a_{n-2} &= a_{n-1}q_{n-1} + a_n \\ a_{n-1} &= a_nq_n + a_{n+1} \end{aligned}$$

jusqu'à tomber sur un reste nul $a_{n+1} = 0$. Le processus s'arrête bien car les restes sont de plus en plus petits : $a_1 > a_2 > a_3 > \cdots$. On note n l'indice tel que a_n est le dernier reste non nul.

Définition 2.6.

Soient a et b deux entiers. Un entier $d \geqslant 0$ est appelé PGCD (plus grand commun diviseur) de a et b s'il vérifie la propriété suivante :
pour tout d' entier, d' divise a et b si et seulement si d' divise d.

(Par exemple, pour $a = 15$ et $b = 21$, l'entier $d = 3$ est le PGCD de a et b. En effet, les diviseurs positifs communs de 15 et 21 sont 1 et 3, et un entier naturel divise 3 si et seulement s'il est égal à 1 ou à 3.)

Remarquons que le PGCD divise a et b (il suffit de prendre $d' = d$ dans la caractérisation du PGCD : puisque d divise d, il divise a et b). De plus, le PGCD est unique car si d_1 et d_2 vérifient la propriété du PGCD alors $d_1 \mid d_2$ et $d_2 \mid d_1$, ce qui entraîne $d_1 = d_2$. Le théorème suivant montre l'existence du PGCD :

Théorème 2.7.

Si a et b sont non nuls, alors dans l'algorithme d'Euclide, a_n est le PGCD de a et b.
Si $b = 0$ alors a est le PGCD de a et b.

Démonstration. Premier cas : a et b sont non nuls. D'après la proposition précédente, on a

$$\begin{aligned} d' \mid a \text{ et } d' \mid b &\iff d' \mid a_0 \text{ et } d' \mid a_1 \\ &\iff d' \mid a_1 \text{ et } d' \mid a_2 \\ &\cdots \\ &\iff d' \mid a_n \text{ et } d' \mid a_{n+1} \\ &\iff d' \mid a_n \end{aligned}$$

(cette dernière équivalence découle du fait que $a_{n+1} = 0$ et que $d' \mid 0$ est vrai pour tout d').

Deuxième cas : $b = 0$. Alors $d' \mid a$ et $d' \mid b$ si et seulement si $d' \mid a$, donc a est le PGCD de a et b. □

Calculons par exemple le PGCD de 183 et 117 par ce procédé.

$$\begin{aligned}
\boxed{183} &= \boxed{117} \times 1 + \boxed{66} \\
\boxed{117} &= \boxed{66} \times 1 + \boxed{51} \\
\boxed{66} &= \boxed{51} \times 1 + \boxed{15} \\
\boxed{51} &= \boxed{15} \times 3 + \boxed{6} \\
\boxed{15} &= \boxed{6} \times 2 + \boxed{3} \\
\boxed{6} &= \boxed{3} \times 2 + \boxed{0}
\end{aligned}$$

(On a encadré les termes $a_0, a_1, \ldots, a_{n+1}$ pour les mettre en évidence.) Le dernier reste non nul est 3, donc le PGCD de 183 et 117 est égal à 3.

Exercice 2.9.

Vérifier par l'algorithme d'Euclide que le PGCD de 364 et de 154 est égal à 14.

Exercice 2.10.

¶Combien 10^{100} et $10^{121} + 10^{813} + 10$ ont-ils de diviseurs communs ?

On peut généraliser la notion de $PGCD$ à plusieurs entiers. On a par exemple $PGCD(a, b, c) = PGCD(PGCD(a, b), c) = PGCD(a, PGCD(b, c))$. En effet,

$$\begin{aligned}
(d \mid a \text{ et } d \mid b) \text{ et } d \mid c &\iff d \mid PGCD(a, b) \text{ et } d \mid c \\
&\iff d \mid PGCD(PGCD(a, b), c)
\end{aligned}$$

et de même $d \mid a$ et $(d \mid b$ et $d \mid c) \iff d \mid PGCD(a, PGCD(b, c))$.

On définit également le PGCD de deux (ou plusieurs) entiers relatifs par $PGCD(a, b) = PGCD(|a|, |b|)$.

Proposition 2.8.

Si $a = bq + r$ alors $PGCD(a, b) = PGCD(b, r)$.

Démonstration. Evident d'après la Proposition 5. □

Exercice 2.11.

Déterminer le $PGCD$ de 1000000000 et 1000000005.

L'une des notions les plus importantes en arithmétique est celle de nombre premier :

Définition 2.9.

Un entier p est dit *premier* si $p \geqslant 2$ et si les seuls diviseurs positifs de p sont 1 et p.

La liste des nombres premiers commence par

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

A noter que 1 n'est pas premier. La raison de cette convention est que l'on veut que tout entier $\geqslant 2$ admette une décomposition *unique* en facteurs premiers (voir plus loin).

Exercice 2.12.

131 est-il premier ? 221 est-il premier ?

Remarque 2.10.

Si p est premier, alors pour tous entiers naturels a et b, l'égalité $p = ab$ entraîne $(a = 1$ et $b = p)$ ou $(a = p$ et $b = 1)$.

Démonstration. $p = ab$ entraîne que a est un diviseur de p, donc $a = 1$ ou $a = p$. Si $a = 1$ alors $p = ab = 1 \times b = b$ et si $a = p$ alors $p = pb$ donc $b = 1$. □

Proposition 2.11.

Soit $n \geqslant 2$ un entier. Le plus petit diviseur $\geqslant 2$ de n est un nombre premier.

Exemple : pour $n = 75$, les diviseurs $\geqslant 2$ de n sont $3, 5, 15, 25, 75$. Le plus petit de ces nombres est égal à 3, qui est bien premier.

Démonstration. Notons p le plus petit entier tel que
(i) $p \mid n$;
(ii) $p \geqslant 2$.
Notons que p est bien défini puisqu'il existe des entiers (par exemple n) vérifiant les deux conditions (i) et (ii).

Soit d est un diviseur $\geqslant 2$ de p. Comme $d \mid p$ et $p \mid n$, on a $d \mid n$. De plus, p étant le plus petit diviseur $\geqslant 2$ de n, on a $p \leqslant d$. Or, $d \leqslant p$ puisque d divise p, donc $d = p$. Ceci prouve que l'unique diviseur $\geqslant 2$ de p est p lui-même, donc p est premier. □

Remarque 2.12.

Ce rÃ©sultat permet par rÃ©currence de montrer que tout entier $n \geq 2$ est un produit de nombres premiers. En effet, 2 admet une dÃ©composition. Si de plus tout entier $k \leq n$ admet une dÃ©composition, alors $n+1$ admet un diviseur premier p : on Ã©crit $n + 1 = pk$. Si $k = 1$, alors $n + 1$ est premier et la dÃ©composition est immÃ©diate. Sinon, $k \leq n$ est un produit de nombres premiers donc $n+1$ aussi.

Théorème 2.13 (Euclide).

Il existe une infinité de nombres premiers.

Démonstration. Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers $p_1 < p_2 < \cdots < p_r$ avec $p_1 = 2$, $p_2 = 3$, etc. Soit $n = p_1 p_2 \cdots p_r + 1$. On a $n \geqslant p_1 = 2$. Soit p le plus petit diviseur supÃ©rieur ou Ã©gal Ã 2 de n. D'après la proposition précédente, p est un nombre premier, donc p figure dans la liste $\{p_1, \ldots, p_r\}$. Par conséquent, $p \mid p_1 p_2 \cdots p_r = n - 1$. Comme $p \mid n$, on en déduit que $p \mid n - (n-1) = 1$ donc $p \leqslant 1$. Impossible. □

Exercice 2.13.

1) Montrer que tout nombre premier $\geqslant 3$ peut s'écrire, soit sous la forme $4k+1$, soit sous la forme $4k-1$.
2) ¶Montrer qu'il existe une infinité de nombres premiers de la forme $4k-1$.
[On pourra former un nombre de la forme $4(p_1 \cdots p_r) - 1$.]

Remarque 2.14.

Il y a des résultats bien plus précis sur la répartition des nombres premiers. Par exemple, le postulat de Bertrand dit que pour tout $n \geqslant 2$, il existe au moins un nombre premier p tel que $n < p < 2n$. La démonstration de ce théorème est trop longue pour être exposée ici.

Définition 2.15.

Deux entiers a et b sont dits *premiers entre eux* si l'unique diviseur commun strictement positif est 1. Autrement dit, $PGCD(a, b) = 1$.

Par exemple, 6 et 35 sont premiers entre eux, mais 14 et 35 ne le sont pas.

Exercice 2.14.

1) Quels sont les entiers n tels que n et $n+2$ sont premiers entre eux ?
2) ¶Quels sont les entiers n tels que $n^2 - 1$ et $n^2 - 2n + 1$ sont premiers entre eux ?

Plus généralement,

Définition 2.16.

Des entiers $a_1, a_2, \ldots, a_n$ sont dits *premiers entre eux dans leur ensemble* si l'unique entier strictement positif les divisant tous est 1. Autrement dit, $PGCD(a_1, a_2, \ldots, a_n) = 1$.

Par exemple, $6, 10, 15$ sont premiers entre eux dans leur ensemble mais ne sont pas premiers entre eux deux à deux.

Proposition 2.17.

Soient a et b deux entiers non nuls, et d leur $PGCD$. Alors on peut écrire $a = da'$ et $b = db'$ avec a' et b' premiers entre eux.

(Par exemple, pour $a = 15$ et $b = 21$, on écrit $15 = 3 \times 5$ et $21 = 3 \times 7$; les entiers 5 et 7 sont bien premiers entre eux.)

Démonstration. Comme d divise a et b, les nombres $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$ sont entiers. Si un entier naturel c divise a' et b', alors cd divise $da' = a$ et $db' = b$, donc cd divise d, ce qui entraîne $c \mid 1$, puis $c = 1$. Par conséquent, a' et b' n'ont pas d'autre diviseur commun que 1, autrement dit a' et b' sont premiers entre eux. □

2.1 Le théorème de Bézout

Théorème 2.18 (Bézout).

(i) Soient a et b deux entiers. Notons $d = a \wedge b$. Alors il existe des entiers relatifs u et v tels que $d = au + bv$.

(ii) Plus précisément, pour tout entier m il existe u' et v' tels que $au' + bv' = m$ si et seulement si m est un multiple de d.

(iii) En particulier, a et b sont premiers entre eux si et seulement s'il existe u et v tels que $au + bv = 1$.

Avant de démontrer ce théorème, commençons par un exemple : reprenons le calcul de $PGCD(183, 117)$:

$$\begin{aligned}
\boxed{183} &= \boxed{117} \times 1 + \boxed{66} \\
\boxed{117} &= \boxed{66} \times 1 + \boxed{51} \\
\boxed{66} &= \boxed{51} \times 1 + \boxed{15} \\
\boxed{51} &= \boxed{15} \times 3 + \boxed{6} \\
\boxed{15} &= \boxed{6} \times 2 + \boxed{3} \\
\boxed{6} &= \boxed{3} \times 2 + \boxed{0}
\end{aligned}$$

On va écrire les restes successifs en fonction de 183 et 117.

$\boxed{66} = \boxed{183} - \boxed{117}$

$\boxed{51} = \boxed{117} - \boxed{66} = \boxed{117} - (\boxed{183} - \boxed{117}) = \boxed{117} \times 2 - \boxed{183}$

$\boxed{15} = \boxed{66} - \boxed{51} = (\boxed{183} - \boxed{117}) - (\boxed{117} \times 2 - \boxed{183}) = \boxed{183} \times 2 - \boxed{117} \times 3$

$\boxed{6} = \boxed{51} - \boxed{15} \times 3 = \boxed{117} \times 2 - \boxed{183} - (\boxed{183} \times 2 - \boxed{117} \times 3) \times 3$
$= -\boxed{183} \times 7 + \boxed{117} \times 11$

$3 = \boxed{15} - \boxed{6} \times 2 = \boxed{183} \times 2 - \boxed{117} \times 3 - (-\boxed{183} \times 7 + \boxed{117} \times 11) \times 2$
$= \boxed{183} \times 16 - \boxed{117} \times 25.$
On a ainsi trouvé que $3 = 183u + 117v$ avec $u = 16$ et $v = -25$.

Exercice 2.15.

Trouver des entiers relatifs u et v tels que $364u + 154v = 14$.

Démonstration du théorème. Montrons (i). Il suffit d'expliquer formellement l'algorithme utilisé plus haut. Si $a = 0$ ou $b = 0$ l'assertion est évidente. Supposons donc $a > 0$ et $b > 0$. Quitte à échanger a et b, on peut supposer que $a \geqslant b$. On applique l'algorithme d'Euclide : on pose $a_0 = a$ et $a_1 = b$.

On observe que

$$\begin{aligned} a_0 &= au_0 + bv_0 \\ a_1 &= au_1 + bv_1 \end{aligned}$$

avec $u_0 = 1$, $v_0 = 0$, $u_1 = 0$, $v_1 = 1$.

L'idée est de chercher à écrire a_k sous la forme $a_k = au_k + bv_k$ pour tout k.

On a ensuite $a_2 = a_0 - a_1q_1 = au_0 + bv_0 - q_1(au_1 + bv_1) = (u_0 - q_1u_1)a + (v_0 - q_1v_1)$, donc

$$a_2 = au_2 + bv_2$$

avec $u_2 = u_0 - q_1u_1$ et $v_2 = v_0 - q_1v_1$.

On continue ainsi de proche en proche jusqu'à a_n : comme $a_n = a_{n-2} - q_{n-1}a_{n-1}$, et comme a_{n-2} et a_{n-1} s'expriment en fonction de a et b, on peut exprimer a_n en fonction de a et b. Plus précisément, on a $a_n = au_n + bv_n$ avec $u_n = u_{n-2} - q_{n-1}u_{n-1}$ et $v_n = v_{n-2} - q_{n-1}v_{n-1}$. On obtient ainsi $d = au + bv$ avec $d = a_n$, $u = u_n$ et $v = v_n$.

(Cet algorithme s'appelle l'algorithme d'Euclide étendu.)

Montrons (ii). Si m est un multiple de d, alors il existe λ tel que $m = \lambda d$. On a alors $m = (\lambda u)a + (\lambda v)b$.

Réciproquement, si $m = au' + bv'$, alors comme d divise a et b, il divise $au' + bv'$ donc d divise m.

Montrons (iii). Si $au + bv = 1$ alors $PGCD(a, b)$ divise 1, donc est égal à 1. La réciproque a déjà été prouvée en première partie. □

Remarque 2.19.

Plus généralement, pour tous $a_1, \ldots, a_n$, il existe $u_1, \ldots, u_n$ tels que

$$a_1u_1 + a_2u_2 + \cdots + a_nu_n = PGCD(a_1, \ldots, a_n).$$

La démonstration n'est pas difficile mais nous l'omettons pour que ce document garde une longueur raisonnable.

Voici un corollaire important du théorème de Bézout :

Théorème 2.20 (Lemme de Gauss).

Soient a et b des entiers. Soit m un nombre qui est premier avec a, tel que $m \mid ab$. Alors $m \mid b$.

Démonstration. Soient a, b, m comme dans l'énoncé. Il existe u et v tels que $mu+av = 1$. On multiplie membre à membre par b, ce qui donne $mu + (ab)v = b$. Comme m divise mu et $(ab)v$, il divise le membre de gauche, donc $m \mid b$. □

Exercice 2.16.

Montrer que si x et y sont des entiers tels que $2x + 1$ divise $8y$ alors $2x + 1$ divise y.

Dans le cas particulier où m est un nombre premier, on obtient le résultat suivant :

Théorème 2.21.

Soit p un nombre premier et a, b des entiers. Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

Démonstration. Soit p un nombre entier et a, b des entiers tels que $p \mid ab$. Si p ne divise pas a, alors p est premier avec a, donc $p \mid b$ d'après le lemme de Gauss. □

Remarque 2.22.

L'hypothèse que p est premier est indispensable ici. Par exemple, 6 divise 10×21 mais 6 ne divise ni 10, ni 21.

Plus généralement,

Théorème 2.23.

Soit p un nombre premier. Si p divise le produit $a_1 \cdots a_r$, alors p divise l'un des nombres $a_1, a_2, \ldots, a_r$.

Démonstration. On le démontre par récurrence sur r. Si $r = 1$ c'est évident. Supposons la propriété vraie au rang $r - 1$.

Si $p \mid a_1 \cdots a_r$, alors d'après le lemme de Gauss, p divise a_1 ou p divise $a_2 \cdots a_r$. Or, par hypothèse de récurrence, $p \mid a_2 \cdots a_r$ entraîne que p divise l'un des nombres $a_2, \ldots, a_r$. Il vient que p divise l'un des nombres $a_1, \ldots, a_r$. □

Soient a et b deux entiers premiers entre eux. Revenons à l'équation $au + bv = 1$ d'inconnues u et v. L'algorithme d'Euclide étendu permet d'en trouver *un* couple de solutions. Notons (u_0, v_0) cette solution particulière : on a donc $au_0 + bv_0 = 1$. Cherchons maintenant *toutes* les solutions.

Soit (u, v) un couple d'entiers tels que $au + bv = 1$. On a

$$\begin{aligned} au + bv &= au_0 + bv_0 \\ a(u - u_0) &= b(v_0 - v). \end{aligned} \tag{1}$$

Or, a divise $a(u - u_0)$, donc a divise $b(v_0 - v)$. Comme de plus a est premier avec b, il divise $v_0 - v$ d'après le Lemme de Gauss. Soit $k \in \mathbb{Z}$ tel que $v_0 - v = ak$. On reporte dans (1) :

$$a(u - u_0) = bak,$$

ce qui donne $u - u_0 = bk$, et finalement

$$\begin{cases} u = u_0 + bk \\ v = v_0 - ak. \end{cases}$$

Réciproquement, si $u = u_0 + bk$ et $v = v_0 - ak$, on vérifie que (u, v) est une solution :

$$au + bv = a(u_0 + bk) + b(v_0 - ak) = au_0 + bv_0 + abk - abk = au_0 + bv_0 = 1.$$

Conclusion : (u, v) vérifie l'équation $au + bv = 1$ si et seulement s'il existe $k \in \mathbb{Z}$ tel que $u = u_0 + bk$ et $v = v_0 - ak$.

Exercice 2.17.

Déterminer toutes les solutions de l'équation $9u - 7v = 1$.

Exercice 2.18.

¶Soit n un entier fixé. Déterminer tous les couples d'entiers (x, y) vérifiant l'équation $16x + 26y = n$.

2.2 Le théorème fondamental de l'arithmétique

Théorème 2.24.

Tout entier $\geqslant 2$ admet une décomposition en produit de nombres premiers. Cette décomposition est unique à l'ordre près.

Par exemple, $84 = 2 \times 2 \times 3 \times 7$ est une décomposition de 84 en facteurs premiers. Les autres décompositions s'obtiennent en permutant les termes, comme $84 = 3 \times 2 \times 7 \times 2$.

Démonstration. Soit $\mathcal{P}(n)$ la propriété "n admet une et une seule décomposition en produit de nombres premiers". Nous allons montrer par récurrence que $\mathcal{P}(n)$ est vraie pour tout $n \geqslant 2$.

La propriété $\mathcal{P}(2)$ est vraie : si $n = p_1 \cdots p_r$ est produit de nombres premiers, alors $r = 1$ puisque n est premier, et par suite $p_1 = 2$.

Soit $n \geqslant 3$, et supposons $\mathcal{P}(2), \mathcal{P}(3), \ldots, \mathcal{P}(n-1)$ vraies. Montrons que $\mathcal{P}(n)$ est vraie. Il faut d'abord prouver l'existence d'une décomposition de n en produit de nombres premiers.

Soit p le plus petit diviseur de n. On sait que p est premier.

Si $n = p$, alors n est bien produit de nombres premiers.

Si $p < n$, alors comme $2 \leqslant \frac{n}{p} < n$, par hypothèse de récurrence il existe des nombres premiers $p_1, \ldots, p_r$ tels que $\frac{n}{p} = p_1 \cdots p_r$. Par conséquent, $n = pp_1 \cdots p_r$ admet bien une décomposition en facteurs premiers.

Montrons maintenant l'unicité de la décomposition. Supposons que

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

avec $p_1, \ldots, p_r$ et $q_1, \ldots, q_r$ premiers.

Si n est premier, on a nécessairement $r = s = 1$, donc $p_1 = q_1$. Supposons donc n non premier.

D'après le Lemme de Gauss, comme p_1 divise $q_1 q_2 \cdots q_s$, il divise l'un des nombres $q_1, \ldots, q_s$ dont p_1 est égal à l'un de ces nombres. Quitte à changer l'ordre des $q_1, \ldots, q_s$, on peut supposer que $p_1 = q_1$. On a alors

$$p_2 \cdots p_r = q_2 \cdots q_s$$

Or, $\mathcal{P}(p_1 \cdots p_r)$ est vraie par hypothèse de récurrence, donc $(p_2, \ldots, p_r)$ est égal à $(q_2, \ldots, q_s)$ à l'ordre près. □

Plutôt que d'écrire une décomposition sous la forme $84 = 2 \times 2 \times 3 \times 7$, on préfère une écriture du type $84 = 2^2 \times 3 \times 7$. Plus généralement, un entier n peut s'écrire sous la forme

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

avec $p_1 < p_2 < \cdots < p_r$ premiers. L'entier α_j s'appelle la valuation p_j-adique de n et se note $v_{p_j}(n)$. Pour tout nombre premier p, l'entier $v_p(n)$ est le plus grand entier m tel que p^m divise n.

Par exemple, $v_2(84) = 2$, $v_3(84) = 1$, $v_5(84) = 0$, $v_p(1) = 0$ pour tout p.

Exercice 2.19.

Combien vaut $v_3(18^{100})$?

Exercice 2.20.

Combien vaut $v_2(2^{100} + 2^{200})$?

Exercice 2.21.

¶Soit $n = 1 \times 2 \times 3 \times \cdots \times 100$.
1) Déterminer $v_7(n)$.
2) Déterminer le nombre de zéros Ã la fin de l'écriture décimale de n.

Proposition 2.25.

Soient a et b des entiers $\geqslant 1$.
(i) $v_p(ab) = v_p(a) + v_p(b)$ pour tout p premier.
(ii) $a \mid b$ si et seulement si pour tout entier premier p on a $v_p(a) \leqslant v_p(b)$.
(iii) $v_p(a \wedge b) = \min(v_p(a), v_p(b))$ pour tout p premier.

Démonstration. (i) Soient $p_1, \ldots, p_r$ les nombres premiers qui divisent a ou b. On écrit $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et $b = p_1^{\beta_1} \cdots p_r^{\beta_r}$ avec $\alpha_i \geqslant 0$ et $\beta_i \geqslant 0$ pour tout $i = 1, 2, \ldots, r$.
Alors $ab = p_1^{\alpha_1+\beta_1} \cdots p_r^{\alpha_r+\beta_r}$, d'où $v_{p_i}(ab) = \alpha + \beta_i = v_{p_i}(a) + v_{p_i}(b)$ pour tout i.

(ii) Si $a \mid b$ alors il existe c tel que $b = ac$, d'où $v_p(b) = v_p a) + v_p(c) \geqslant v_p(a)$.
Réciproquement, si $v_p(a) \leqslant v_p(b)$ pour tout entier premier p, alors on peut écrire $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et $b = p_1^{\beta_1} \cdots p_r^{\beta_r}$ avec $\alpha_i \leqslant \beta_i$. Posons $\gamma_i = \beta_i - \alpha_i$ et $c = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$. Alors on a $b = ac$, donc $a \mid b$.

(iii) Avec les notations précédentes, posons $\delta_i = \min(\alpha_i, \beta_i)$ et $d = p_1^{\delta_1} \cdots p_r^{\delta_r}$. D'après (ii), on a $d \mid a$ et $d \mid b$. D'autre part, pour tout $d' \geqslant 1$ on a $d' \mid a$ et $d' \mid b$ si et seulement si $v_p(d') \leqslant v_p(a)$ et $v_p(d) \leqslant v_p(b)$ pour tout p premier. Ceci équivaut à $v_p(d') \leqslant v_p(d)$ pour tout p premier, ou encore à $d' \mid d$. Ceci prouve que $d = a \wedge b$. □

Exercice 2.22.

Montrer sans calcul que 87457561565 ne divise pas 10000000000000000000000007.

De la même façon que ci-dessus, on montrerait :

Proposition 2.26.

Soient $a, b \geqslant 1$ des entiers. Il existe un et un seul nombre, appelé le plus petit commun multiple de a et b, et noté $PPCM(a, b)$ ou $a \vee b$, caractérisé par la propriété suivante : Soit m un entier non nul. Alors $a \mid m$ et $b \mid m$ si et seulement si $PPCM(a, b) \mid m$.
De plus, $v_p(a \vee b) = \max(v_p(a), v_p(b))$.

Exercice 2.23.

Montrer que si $a^2 \mid b^2$ alors $a \mid b$.

Exercice 2.24.

Montrer que si p est premier et $p \mid a^2$ alors $p^2 \mid a^2$.

Exercice 2.25.

Montrer que $ab = PGCD(a,b) \times PPCM(a,b)$.

Exercice 2.26.

¶Déterminer tous les couples d'entiers naturels (x,y) vérifiant :
$PGCD(x,y) = 8$, $PPCM(x,y) = 440$, $x + y = 128$.

Exercice 2.27.

Un nombre est dit *parfait* si la somme de tous ses diviseurs positifs est égale à $2n$.
Montrer que si $2^{k+1} - 1$ est un nombre premier alors $2^k(2^{k+1} - 1)$ est parfait.
¶¶Montrer que tout nombre parfait pair est de cette forme.

2.3 Nombre de diviseurs d'un entier

Théorème 2.27.

Soit $n \geqslant 1$ un entier dont la décomposition en facteurs premiers s'écrit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.
Alors n admet $(\alpha_1 + 1) \cdots (\alpha_r + 1)$ diviseurs positifs.

Démonstration. Les diviseurs de n s'écrivent sous la forme $p_1^{\beta_1} \cdots p_r^{\beta_r}$ avec

$$\begin{aligned} 0 \leqslant \quad & \beta_1 \quad \leqslant \alpha_1, \\ & \cdots \\ 0 \leqslant \quad & \beta_r \quad \leqslant \alpha_r. \end{aligned}$$

Pour β_1 on a $\alpha_1 + 1$ choix possibles, pour β_2 on a $\alpha_2 + 1$ choix, etc. ce qui donne en tout $(\alpha_1 + 1) \cdots (\alpha_r + 1)$ choix possibles. □

Par exemple, les diviseurs (positifs) de $100 = 2^2 \times 5^2$ sont
$2^0 \times 5^0$, $2^0 \times 5^1$, $2^0 \times 5^2$,
$2^1 \times 5^0$, $2^1 \times 5^1$, $2^1 \times 5^2$,
$2^2 \times 5^0$, $2^2 \times 5^1$, $2^2 \times 5^2$.
Notons $\tau(n)$ le nombre de diviseurs (positifs) de n.

Exercice 2.28.

Combien vaut $\tau(1000000)$?

Exercice 2.29.

Quels sont les entiers $n \leqslant 1000$ tels que $\tau(n) = 7$?

Exercice 2.30.

Montrer que $\tau(n) \leqslant 2\sqrt{n}$ pour tout n.

Exercice 2.31.

Un jardinier doit planter 480 arbustes en n rangées égales contenant au moins 6 arbustes. De combien de manières peut-il le faire ?

Exercice 2.32.

¶N est divisible par 6, N n'est pas divisible par 8, et N a exactement 15 diviseurs. Que vaut N ?

Exercice 2.33.

A quelle condition un entier n admet-il un nombre impair de diviseurs ?

Exercice 2.34.

Montrer que si m et n sont premiers entre eux alors $\tau(mn) = \tau(m)\tau(n)$.
¶¶Est-il vrai que si $\tau(mn) = \tau(m)\tau(n)$ alors m et n sont premiers entre eux ?

3 Congruences

3.1 Définition et propriétés de base

Définition 3.1.

Soit n un entier non nul. On dit que a et b sont congrus modulo n si n divise $a-b$. On note $a \equiv b\,[n]$, ou encore $a = b \pmod{n}$.

Lorsque l'on effectue une division Euclidienne de a par n sous la forme $a = nq + r$, on a $a \equiv r\,[n]$, donc tout entier est congru modulo n à un et un seul entier parmi $\{0, 1, \ldots, n-1\}$. Une autre manière de définir la congruence modulo n est de dire que $a \equiv b\,[n]$ si et seulement si les restes des divisions Euclidiennes de a et de b par n sont égaux.

La congruence se comporte comme l'égalité :

Proposition 3.2.

Soient a, b, c des entiers et n un entier non nul.
(réflexivité) $a \equiv a\,[n]$.
(symétrie) si $a \equiv b\,[n]$ alors $b \equiv a\,[n]$.
(transitivité) si $a \equiv b\,[n]$ et $b \equiv c\,[n]$ alors $a \equiv c\,[n]$.

Démonstration. $a - a = 0$ est divisible par n, d'où la réflexivité.

Si n divise $a-b$, alors n divise $-(a-b) = b-a$, d'où la symétrie.

Si n divise $a-b$ et n divise $b-c$, alors n divise $(a-b)+(b-c)$, donc n divise $a-c$. Ceci prouve la transitivité. □

La congruence est compatible avec l'addition et la multiplication :

Proposition 3.3.

Soient a, b, c, d des entiers et n un entier non nul. Supposons $a \equiv b\,[n]$ et $c \equiv d\,[n]$. Alors
(i) $a + c \equiv b + d\,[n]$;
(ii) $ac \equiv bd\,[n]$.

Démonstration. Par hypothèse, n divise $a-b$ et $c-d$.

(i) n divise $(a-b)+(c-d) = (a+c)-(b+d)$ donc $a + c \equiv b + d\,[n]$.

(ii) $ac - bd = a(c-d+d) - bd = a(c-d) + ad - bd = a(c-d) + (a-b)d$ est divisible par n puisque $c-d$ et $a-b$ le sont, donc $ac \equiv bd\,[n]$. □

On raisonne couramment modulo 12 dans la vie de tous les jours. S'il est 9 heures du matin, alors dans 5 heures il sera 2 heures de l'après-midi : ceci correspond au fait que $9 + 5 \equiv 2\,[12]$.

Le fait de raisonner modulo 10 est aussi très intuitif, car il correspond à regarder le dernier chiffre d'un entier. Par exemple, 857382993 est congru à 3 modulo 10 car $857382993 - 3 = 857382990$ est un multiple de 10.

Proposition 3.4.

Si $a \equiv b\,[n]$ alors pour tout entier $k \geqslant 1$, on a $a^k \equiv b^k\,[n]$.

Démonstration. Il suffit d'appliquer k fois la Proposition 3(ii). □

Exercice 3.1.

Quels sont les entiers p tels que p et $p+1$ sont premiers ?

Exercice 3.2.

¶Quels sont les entiers p tels que $p, p+2$ et $p+4$ sont premiers ?

3.2 Critéres de divisibilité

Soit n un entier. On note $\overline{a_k \cdots a_0}$ son écriture décimale.
Par exemple, si $n = 147$ alors $k = 2$, $a_0 = 7$, $a_1 = 4$, $a_2 = 1$.
On a donc $0 \leqslant a_j \leqslant 9$ pour tout j, et

$$n = a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^k a_k.$$

Proposition 3.5.

n est congru à $a_0 + \cdots + a_k$ modulo 9 et modulo 3. Par conséquent, n est divisible par 9 (respectivement) 3 si et seulement si $a_0 + \cdots + a_k$ l'est.

Démonstration. On a $10 - 1 = 9$ donc $10 \equiv 1\,[9]$. D'après la Proposition 4, on a $10^j \equiv 1\,[9]$ pour tout j, donc $n \equiv a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^k a_k \equiv a_0 + \cdots + a_k\,[9]$.

A fortiori, n est congru à $a_0 + \cdots + a_k$ modulo 3.

Enfin, n est divisible par 9 (resp. 3) si et seulement si n est congru à 0 modulo 9 (resp. 3), si et seulement si $a_0 + \cdots + a_k$ est congru à 0 modulo 9 (resp. 3). □

Exercice 3.3.

48767621 est-il divisible par 9 ?

Proposition 3.6.

n est congru à $a_0 - a_1 + a_2 - a_3 \cdots$ modulo 11. En particulier, n est divisible par 11 si et seulement si la somme alternée de ses chiffres est divisible par 11.

Démonstration. On a $10 \equiv -1\,[11]$, donc $10^k \equiv (-1)^k\,[11]$. On en déduit que

$$a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 + \cdots \equiv a_0 - a_1 + a_2 - a_3 + \cdots\,[11].$$

□

Exercice 3.4.

98473092 est-il divisible par 11 ?

Proposition 3.7.

n est divisible par 4 si et seulement si $\overline{a_1 a_0}$ est divisible par 4.

Démonstration. $a - \overline{a_1 a_0} = \overline{a_k a_{k-1} \cdots a_2 00}$ est divisible par 100, donc par 4. □

Proposition 3.8.

n est divisible par 8 si et seulement si $\overline{a_2 a_1 a_0}$ est divisible par 8.

Démonstration. Analogue. □

Exercice 3.5.

Sans effectuer la division, montrer que $\frac{3645}{45}$ est un entier.

Exercice 3.6.

Le PGCD de 193116 et de 127413 est-il pair ? Est-il divisible par 3 ? Par 9 ? Par 11 ? Par 33 ? Par 99 ?

Exercice 3.7.

¶À quelle condition sur les chiffres x et y le nombre $\overline{27x85y}$ est-il divisible par 33 ?

3.3 Inverses modulo n

Définition 3.9.

Un entier b est appelé inverse de a modulo n si et seulement si $ab \equiv 1\,[n]$. Si a possède un inverse modulo n, alors on dit que a est inversible modulo n.

Par exemple, 3 est inverse de 5 modulo 7 car $3 \times 5 = 15$ est congru à 1 modulo 7. Les nombres $\ldots, -4, 3, 10, 17, 24, 31, \ldots$ sont tous inverses de 5 modulo 7 car $(3 + 7k) \times 5 = 15 + 7(5k) \equiv 15 \equiv 1\,[7]$.

Proposition 3.10.

a est inversible modulo n si et seulement si a et n sont premiers entre eux. L'inverse de a est alors unique modulo n.

Démonstration. Si a est inversible modulo n, alors il existe u tel que $au \equiv 1\,[n]$. Par définition, cela signifie que $au-1$ est un multiple de n, donc il existe v tel que $au-1 = nv$. On obtient alors une relation de Bézout $au+n(-v) = 1$, donc a et n sont premiers entre eux.

Réciproquement, si a et n sont premiers entre eux, alors il existe une relation de Bézout $au + nv = 1$. En passant modulo n les deux membres de l'égalité, on en déduit que $au \equiv 1\,[n]$, donc a est inversible modulo n.

Montrons maintenant l'unicité. Supposons que b et b' sont deux inverses de a modulo n. Alors

$$b = b \times 1 \equiv b(ab') \equiv (ba)b' \equiv 1 \times b' = b'\,[n]$$

donc b et b' sont congrus modulo n. □

Remarquons que la démonstration ci-dessus donne un algorithme pour calculer l'inverse d'un nombre modulo n : il suffit de trouver une relation de Bézout grâce à l'algorithme d'Euclide étendu.

Proposition 3.11.

Si a est inversible modulo n, et si $ax \equiv ay\,[n]$, alors $x \equiv y\,[n]$.

Démonstration. Soit b un inverse de a modulo n. On a $x \equiv (ba)x = b(ax) \equiv b(ay) = (ba)y \equiv y\,[n]$. □

On peut donc "simplifier par a" une congruence modulo n si a est inversible modulo n.

L'hypothèse que a est inversible modulo n est nécessaire, puisque $2 \times 3 \equiv 2 \times 8\,[10]$ bien que $3 \not\equiv 8\,[10]$.

Exercice 3.8.

Vérifier que les inversibles modulo 8 sont $1, 3, 5, 7$, et qu'ils sont tous égaux à leurs inverses.

Exercice 3.9.

Trouver l'inverse de 37 modulo 53.

Proposition 3.12.

Si a et b sont inversibles modulo p alors ab est inversible modulo p.

L'idée est assez naturelle : si on peut diviser par a et par b, alors on peut diviser par ab en divisant d'abord par a puis par b.

Démonstration. Il existe a' et b' tels que $aa' \equiv 1\,[p]$ et $bb' \equiv 1\,[p]$. On en déduit $(ab)(a'b') = (aa')(bb') \equiv 1 \times 1 \equiv 1\,[p]$, donc ab est inversible modulo p et son inverse est $a'b'$. □

Proposition 3.13.

Soit p un nombre premier et a un entier non divisible par p. Alors a est égal à son inverse modulo p si et seulement si $a \equiv 1\,[p]$ ou $a \equiv -1\,[p]$.

Démonstration. a est égal à son inverse modulo p
$\iff a^2 \equiv 1\,[p]$
$\iff a^2 - 1 \equiv 0\,[p]$
$\iff (a-1)(a+1) \equiv 0\,[p]$
$\iff p \mid (a-1)(a+1)$
$\iff p \mid a-1$ ou $p \mid a+1$ (d'après le Lemme de Gauss)
$\iff a - 1 \equiv 0\,[p]$ ou $a + 1 \equiv 0\,[p]$
$\iff a \equiv 1\,[p]$ ou $a \equiv -1\,[p]$. □

Théorème 3.14 (Wilson).

Si p est premier, alors $(p-1)! \equiv -1\,[p]$.

Démonstration. Rappelons que $(p-1)! = 1 \times 2 \times 3 \times \cdots \times (p-1)$.

Si $p = 2$, on a $(p-1)! = 1 \equiv -1\,[2]$. Supposons $p \geqslant 3$.

Notons que $p - 1 \equiv -1\,[p]$.

Les nombres $2, 3, \ldots, p-2$ ne sont congrus, ni à 1, ni à -1 modulo p. Dans le produit $2 \times 3 \times \cdots \times p-2$, on regroupe chaque terme avec son inverse modulo p. On obtient ainsi

$$2 \times 3 \times \cdots \times (p-2) \equiv 1\,[p].$$

Ainsi, $2 \times 3 \times \cdots \times (p-2) \times (p-1) \equiv p - 1 \equiv -1\,[p]$, ce qui s'écrit $(p-1)! \equiv -1\,[p]$. □

3.4 Petit théorème de Fermat

Théorème 3.15.

Soit p un nombre premier. Alors pour tout entier a non divisible par p, on a

$$a^{p-1} \equiv 1\,[p].$$

Démonstration. Soit $A = \{1, 2, \ldots, p-1\}$. Soit B l'ensemble des restes modulo p de $\{a, 2a, 3a, \ldots, (p-1)a\}$.

Tous les éléments de B sont des éléments de A : en effet, si $1 \leqslant k \leqslant p-1$ alors ka n'est pas divisible par p, donc son reste modulo p est compris entre 1 et $p-1$.

De plus, les éléments $a, 2a, \ldots, (p-1)a$ sont deux à deux distincts modulo p : en effet, si $1 \leqslant k \leqslant \ell \leqslant p-1$ et $ka \equiv \ell a\,[p]$, comme a est inversible modulo p, en simplifiant par a on obtient $k \equiv \ell \pmod{p}$ donc $k = \ell$.

On en déduit que B possède $p-1$ éléments. Comme A possède le même nombre d'éléments, on a $B = A$, et donc le produit de tous les éléments de A est égal au produit de tous les éléments de B, ce qui s'écrit

$$1 \times 2 \times \cdots \times (p-1) \equiv a \times (2a) \times (3a) \times \cdots (p-1)a \pmod{p}.$$

En simplifiant par $1 \times 2 \times \cdots (p-1)$, on obtient $1 \equiv a^{p-1}\,[p]$. □

Exemple d'application : soit à calculer 2^{1000} modulo 7.
On sait que $2^6 \equiv 1\,[7]$. Comme $1000 = 6 \times 166 + 4$, on a
$2^{1000} = 2^{6\times 166} \times 2^4 = (2^6)^{166} \times 16 \equiv 1^{166} \times 2 \equiv 2\,[7]$.

Exercice 3.10.

a) Pour quelles valeurs de $n \in \mathbb{N}$, $6^{11} + 5n + 2$ est-il divisible par 7 ?
b) Quel est le reste de la division de 705432^{50} par 11 ?
c) Pour quelles valeurs de $n \in \mathbb{N}$, $5^{6n} + 5^n + 2$ est-il divisible par 7 ?
d) Pour quelles valeurs de $n \in \mathbb{N}$, $81n^5 - 45n^3 + 4n$ est-il divisible par 5 ?

Exercice 3.11.

¶Quel est le dernier chiffre de l'écriture décimale de 7^{3^9} ?

Exercice 3.12.

27^{12} est-il divisible par $3, 5, 7, 9, 11$?

3.5 Carrés modulo n

Pour illustrer la notion de carré modulo n, commençons par un exercice :

Exercice 3.13.

Existe-t-il des entiers a et b tels que $a^2 + b^2 = 10^{100} + 3$?

Démonstration. La réponse est non. L'idée est de raisonner modulo 4. On a
$0^2 \equiv 0\,[4]$
$1^2 \equiv 1\,[4]$
$2^2 \equiv 0\,[4]$
$3^2 \equiv 1\,[4]$.
On en déduit que pour tous a, b, les entiers a^2 et b^2 sont congrus à 0 ou à 1 modulo 4. Par conséquent, $a^2 + b^2$ est congru à $0, 1$ ou 2 modulo 4. Or, $10^{100} + 3$ est congru à 3 modulo 4 donc ne peut pas être égal à $a^2 + b^2$. □

Ceci conduit à la

Définition 3.16.

Un entier a est un carré modulo n s'il existe b tel que $a \equiv b^2\,[n]$.

Observons par exemple les carrés modulo 13.

x	0	1	2	3	4	5	6	7	8	9	10	11	12
x^2	0	1	4	9	3	12	10	10	12	3	9	4	1

(Dans la deuxième ligne on a écrit le reste de la division Euclidienne de x^2 par 13.)
On constate une symétrie : ce n'est pas un hasard puisque $12^2 = (13-1)^2 \equiv (-1)^2 \equiv 1\,[13]$, $11^2 \equiv (13-2)^2 \equiv 2^2\,[13]$, etc.
Pour trouver la liste des carrés modulo n, il suffit juste de calculer k^2 modulo n pour $0 \leqslant k \leqslant \frac{n}{2}$.
Dans l'exemple précédent, on voit qu'il y a exactement sept carrés modulo 13, à savoir $0, 1, 3, 4, 9, 10, 13$. Plus généralement,

Proposition 3.17.

Soit p un nombre premier impair. Alors il y a exactement $\frac{p+1}{2}$ carrés modulo p.

Démonstration. D'après la discussion précédente, tout carré modulo p est congru à k^2 pour un certain entier $0 \leqslant k \leqslant \frac{p-1}{2}$. On voit déjà qu'il y a au plus $\frac{p+1}{2}$ carrés modulo p. Pour conclure, il reste à montrer que si $0 \leqslant k < \ell \leqslant \frac{p-1}{2}$ alors k^2 et ℓ^2 ne sont pas congrus modulo p.
En effet, dans le cas contraire, p diviserait $\ell^2 - k^2 = (\ell - k)(\ell + k)$. Or, $1 \leqslant \ell - k \leqslant \ell + k \leqslant p - 1$, donc p ne divise ni $\ell - k$, ni $\ell + k$, et par suite p ne divise pas $\ell^2 - k^2$, ce qui est contradictoire. □

Exercice 3.14.

Donner la liste de tous les carrés modulo 5 et de tous les carrés modulo 8.

Exercice 3.15.

Existe-t-il des entiers a, b, c tels que $a^2 + b^2 + c^2 = 10^{100} + 7$?

Exercice 3.16.

-3 est-il un carré modulo 103 ?

On s'intéresse à la question suivante : -1 est-il un carré modulo n ? Par exemple, pour $n = 5$, on a $-1 \equiv 4\,[5]$ et $4 = 2^2$, donc -1 est un carré modulo 5. Par contre, on vérifie facilement que -1 n'est pas un carré modulo 3.

Proposition 3.18.

Si p est un nombre premier impair et -1 est un carré modulo p, alors $p \equiv 1\,[4]$.

Démonstration. Comme p est impair, on peut écrire p sous la forme $p = 2m + 1$.

Soit a tel que $a^2 \equiv -1\,[p]$. Alors a n'est pas divisible par p (sinon on aurait $a^2 \equiv 0\,[p]$), donc on peut appliquer le petit théorème de Fermat à a :

$$1 \equiv a^{p-1} = a^{2m} = (a^2)^m \equiv (-1)^m\,[p].$$

Si m est impair, alors $1 \equiv -1\,[p]$ donc $p \mid 2$, ce qui est impossible.

Donc m est pair. On l'écrit sous la forme $m = 2k$. On en déduit que $p = 4k + 1$ est bien congru à 1 modulo 4. □

Remarque 3.19.

La réciproque est vraie mais un peu plus difficile à démontrer : si $p \equiv 1\,[4]$ alors -1 est un carré modulo p.

3.6 Nombres rationnels et irrationnels, développement décimal

Un nombre est dit décimal s'il a un nombre fini de chiffres après la virgule. Tout entier est un nombre décimal. Le nombre $3/8 = 0,375$ est décimal.

Un nombre est dit rationnel s'il est le quotient de deux entiers. Par exemple,

$$83/70 = 1,1857142857142857142\cdots$$

est rationnel. On constate que son développement décimal est périodique : le motif 857142 se répète. Ceci s'explique par le fait que, lorsque l'on pose la division, il n'y a qu'un

nombre fini de restes possibles. Le motif commence à se répéter lorsque l'on tombe sur un reste déjà obtenu précédemment.

Réciproquement, un nombre dont le développement décimal est périodique est rationnel. Sans le prouver formellement, expliquons-le sur un cas particulier.

Soit $x = 3,1212121212\ldots$.

On a $100x = 312,12121212\ldots$, donc $99x = 100x - x = 309$. Il vient $x = \frac{309}{99}$. Cette fraction n'est pas irréductible, elle se simplifie en $\frac{103}{33}$.

Exercice 3.17.

Ecrire le nombre $3,157157157157\ldots$ sous forme d'une fraction irréductible.

Certains nombres n'ont pas de développement décimal périodique.

Proposition 3.20.

$\sqrt{2}$ est irrationnel.

Démonstration. Supposons par l'absurde que $\sqrt{2} = \frac{a}{b}$ avec $\frac{a}{b}$ irréductible. On a $2 = \frac{a^2}{b^2}$, donc $a^2 = 2b^2$. On regarde la 2-valuation : $2v_2(a) = v_2(a^2) = v_2(2b^2) = 1 + 2v_2(b)$. Or, $2v_2(a)$ est pair et $1 + 2v_2(b)$ est impair. Contradiction. □

Plus généralement,

Exercice 3.18.

Soit $n \geqslant 2$. Montrer que si a est un entier positif qui n'est pas la puissance n-ième d'un entier, alors la racine n-ième de a (notée $\sqrt[n]{a}$) est un irrationnel.
N.B. $\sqrt[n]{a}$ est l'unique nombre réel positif tel que $(\sqrt[n]{a})^n = a$.

Exercice 3.19.

¶Montrer que $\sqrt{2} + \sqrt{3}$ est irrationnel.

On peut montrer que π est irrationnel, mais les outils nécessaires pour le démontrer dépassent largement le cadre de ce document.

4 Utilisation de factorisations

Le fait d'écrire un entier n sous la forme $n = ab$ avec $a \geqslant 2$ et $b \geqslant 2$ permet d'une part de voir que n n'est pas premier, et d'autre part d'utiliser les deux propositions suivantes :

Proposition 4.1.

Soient a et b deux entiers naturels premiers entre eux et x, m deux entiers naturels. Si $ab = x^m$, alors il existe des entiers y et z tels que $a = y^m$ et $b = z^m$.

Démonstration. Ecrivons $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.

Pour tout nombre premier p, on a $v_p(ab) = v_p(x^m) = mv_p(x)$, donc $v_p(ab)$ est un multiple de m.

Comme a et b sont premiers entre eux, $v_p(a)$ et $v_p(b)$ ne peuvent pas être tous deux non nuls.

Si $v_p(a) = 0$ alors m divise évidemment $v_p(a)$.

Si $v_p(b) = 0$ alors $v_p(ab) = v_p(a) + v_p(b) = v_p(a)$ donc m divise $v_p(a)$.

Dans tous les cas, m divise $v_p(a)$ pour tout p, donc pour tout j il existe γ_j tel que $\alpha_j = m\gamma_j$.

Soit $y = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$. On a $a = y^m$. On procède de même pour b. □

Proposition 4.2.

Soient a et b deux entiers naturels. On suppose qu'il existe un nombre premier p et un entier m tel que $ab = p^m$. Alors a et b sont des puissances de p.

Démonstration. Un nombre premier divisant a doit diviser $ab = p^m$, donc doit être égal à p. Ainsi, p est le seul nombre premier divisant a. Par conséquent, a est une puissance de p. □

4.1 Identités remarquables

Voici quelques identités remarquables à mémoriser et qui sont fréquemment utiles dans des problèmes d'arithmétique :

$$\begin{aligned}
(a+b)^2 &= a^2 + 2ab + b^2 \\
(a-b)^2 &= a^2 - 2ab + b^2 \\
(a+b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3 \\
(a-b)^3 &= a^3 - 3a^2b + 3ab^2 - b^3 \\
a^2 - b^2 &= (a-b)(a+b) \\
a^3 - b^3 &= (a-b)(a^2 + ab + b^2) \\
a^3 + b^3 &= (a+b)(a^2 - ab + b^2) \\
a^n - b^n &= (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1}) \\
a^n + b^n &= (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots + b^{n-1}) \text{ si } n \text{ impair}
\end{aligned}$$

Les six premières égalités se vérifient en développant. Montrons la septième :

$$\begin{aligned}
&(a-b)(a^{n-1}+a^{n-2}b+a^{n-3}b^2+\cdots+b^{n-1})\\
&= a(a^{n-1}+a^{n-2}b+a^{n-3}b^2+\cdots+b^{n-1})-b(a^{n-1}+a^{n-2}b+a^{n-3}b^2+\cdots+b^{n-1})\\
&= (a^n+a^{n-1}b+a^{n-2}b^2+\cdots+ab^{n-1})-(a^{n-1}b+a^{n-2}b^2+a^{n-3}b^3+\cdots+ab^{n-1}+b^n)\\
&= a^n-b^n
\end{aligned}$$

(tous les termes se sont simplifiés excepté le premier et le dernier).

L'identité précédente étant vraie pour tout couple (a,b), elle est vraie pour le couple $(a,-b)$ donc

$$a^n-(-b)^n=(a-(-b))(a^{n-1}+a^{n-2}(-b)+a^{n-3}(-b)^2+\cdots+(-b)^{n-1}).$$

Si n est impair, on a $(-b)^n=-b^n$ et $(-b)^{n-1}=b^{n-1}$, d'où la dernière égalité.

Comme cas particulier de la septième égalité, on trouve pour $b=1$:

$$a^n-1=(a-1)(1+a+a^2+\cdots+a^{n-1}).$$

Ceci étant vrai pour tout entier n, l'égalité est vraie pour $n+1$ à la place de n, ce qui donne $a^{n+1}-1=(a-1)(1+a+a^2+\cdots+a^n)$. En divisant par $a-1$ (si $a\neq 1$), on obtient l'identité $\boxed{1+a+a^2+\cdots+a^n=\frac{a^{n+1}-1}{a-1}}$.

Exercice 4.1.

¶(Nombres premiers de Mersenne) Montrer que si $a\geqslant 2$ et $n\geqslant 2$ sont des entiers tels que a^n-1 est un nombre premier, alors $a=2$ et n est premier.

Remarque : on constate que $M_2=3$, $M_3=7$, $M_5=31$, $M_7=127$, $M_{11}=2047$, $M_{13}=8191$, $M_{17}=131071$ et $M_{19}=524287$ sont premiers. En revanche, $M_{23}=47\times 178481$ est composé. On ignore s'il existe une infinité de nombres premiers de Mersenne.

Exercice 4.2.

¶(Nombres premiers de Fermat) Montrer que si 2^n+1 est premier, alors n est une puissance de 2. (On montrera que n n'admet pas de diviseur impair.)

Remarque : on pose $F_k=2^{2^k}+1$. On constate que $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$ sont premiers. En revanche, $F_5=641\times 6700417$ est composé. Actuellement, on ne connaît pas d'autre nombre premier de Fermat.

4.2 L'équation $a^2 - b^2 = n$

A n fixé, on considère l'équation $a^2 - b^2 = n$ d'inconnues $a, b \in \mathbb{N}$.

Rappelons que $a^2 - b^2 = (a-b)(a+b)$. Comme $a+b = (a-b) + 2b$, les entiers $a+b$ et $a-b$ ont la même parité. S'ils sont tous deux impairs, alors n est impair, et s'ils sont tous deux pairs, alors n est divisible par 4.

Par conséquent, l'équation ne peut avoir de solution que si n est impair ou si n est divisible par 4.

Supposons que $n = (a-b)(a+b)$. Alors $a-b$ est un diviseur de n. Notons-le d. On a alors $a - b = d$ et $a + b = \frac{n}{d}$ donc $a = \frac{1}{2}\left(d + \frac{n}{d}\right)$ et $a = \frac{1}{2}\left(d - \frac{n}{d}\right)$. Il y a donc autant de solutions que d'entiers naturels d tels que d et $\frac{n}{d}$ sont des diviseurs de n de même parité.

Ecrivons $n = 2^r m$ avec m impair. Si $r = 0$ alors n'importe quel diviseur de n convient, et si $r \geqslant 2$ alors d est de la forme $2^j d'$ avec $1 \leqslant j \leqslant r-1$ et $d' \mid m$.

Par exemple, pour $n = 2016 = 2^5 \times 3^2 \times 7$, d est de la forme $2^j d'$ avec $1 \leqslant j \leqslant 4$ et $d' \in \{1, 3, 9, 7, 21, 63\}$, ce qui donne 24 solutions en tout.

4.3 L'équation $a^2 + b^2 = c^2$

Les solutions de cette équation s'appellent les triplets Pythagoriciens, car elles correspondent aux triangles rectangles dont les côtés sont entiers. Le plus connu d'entre eux est $(3, 4, 5)$ puisque $3^2 + 4^2 = 5^2$.

On remarque tout d'abord que si (a, b, c) est solution, alors pour tout entier d, (da, db, dc) est une solution. Par exemple, $(6, 8, 10)$ est encore un triplet Pythagoricien. Ceci conduit à poser la définition suivante :

Définition 4.3.

Une *solution primitive* est une solution telle que a, b, c sont premiers entre eux dans leur ensemble.

Si (a, b, c) est une solution quelconque, posons $d = PGCD(a, b, c)$. On peut écrire

$$\begin{cases} a &= da' \\ b &= db' \\ c &= dc' \end{cases}$$

pour certains entiers a', b', c'. En divisant l'équation $a^2 + b^2 = c^2$ par d^2, il vient $(a')^2 + (b')^2 = (c')^2$. De plus, a', b', c' sont premiers entre eux dans leur ensemble, donc (a', b', c') est une solution primitive.

Par conséquent, le problème revient à chercher toutes les solutions primitives de l'équation.

Remarquons également que a et b sont premiers entre eux, car s'il y avait un nombre premier p divisant a et b, alors p^2 diviserait $a^2 + b^2$, donc p^2 diviserait c^2, ce qui entraînerait que p divise c, et a, b, c ne seraient pas premiers entre eux.

De même, a et c, ainsi que b et c sont premiers entre eux. Autrement dit, a, b, c sont premiers entre eux deux à deux.

Ainsi, a et b ne peuvent pas être tous les deux pairs.

Ils ne peuvent pas non plus être tous deux impairs, sinon $a^2 + b^2 \equiv 1 + 1 = 2\,[4]$ et on a vu que 2 n'est pas un carré modulo 4.

Quitte à échanger a et b, on peut supposer que a est impair et que b est pair.

On a $(\frac{b}{2})^2 = \frac{c^2-a^2}{4} = (\frac{c-a}{2})(\frac{c+a}{2})$.

(Comme a et c sont impairs, $\frac{c-a}{2}$ et $\frac{c+a}{2}$ sont bien des entiers.)

Si un nombre p divise à la fois $\frac{c-a}{2}$ et $\frac{c+a}{2}$, il divise leur somme et leur différence, c'est-à-dire que p divise c et a. Or, a et c sont premiers entre eux, donc $p = 1$. Par conséquent, $\frac{c-a}{2}$ et $\frac{c+a}{2}$ sont premiers entre eux.

Or, leur produit est un carré, donc d'après la Proposition 1 ce sont tous deux des carrés. Ainsi, il existe u et v tels que

$$\begin{cases} \frac{c+a}{2} &= u^2 \\ \frac{c-a}{2} &= v^2 \end{cases}$$

En faisant la somme des deux égalités, on obtient $c^2 = u^2 + v^2$. En faisant la différence, on trouve $a^2 = u^2 - v^2$, et en faisant le produit, on voit que $(\frac{b}{2})^2 = u^2v^2$ donc $b = 2uv$.

Conclusion : quitte à échanger a et b, les solutions primitives sont données par les formules

$$\begin{cases} a = u^2 - v^2 \\ b = 2uv \\ c = u^2 + v^2 \end{cases}$$

pour certains entiers u et v.

On vérifie qu'on a bien

$$(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2.$$

4.4 Exercices supplémentaires

Exercice 4.3.

¶¶Résoudre dans les entiers naturels : $x^3 - y^3 = 24$.

Exercice 4.4.

¶¶Trouver tous les nombres premiers tels qu'il existe des entiers naturels x et y vérifiant $x(y^2 - p) + y(x^2 - p) = 5p$.

Exercice 4.5.

¶¶Déterminer les entiers naturels m et n tels que $2^n - 3^m = 1$. Même chose pour l'équation $3^m - 2^n = 1$.

Exercice 4.6.

¶¶Déterminer tous les entiers $a, b, c \geqslant 0$ tels $2^a 3^b + 9 = c^2$.