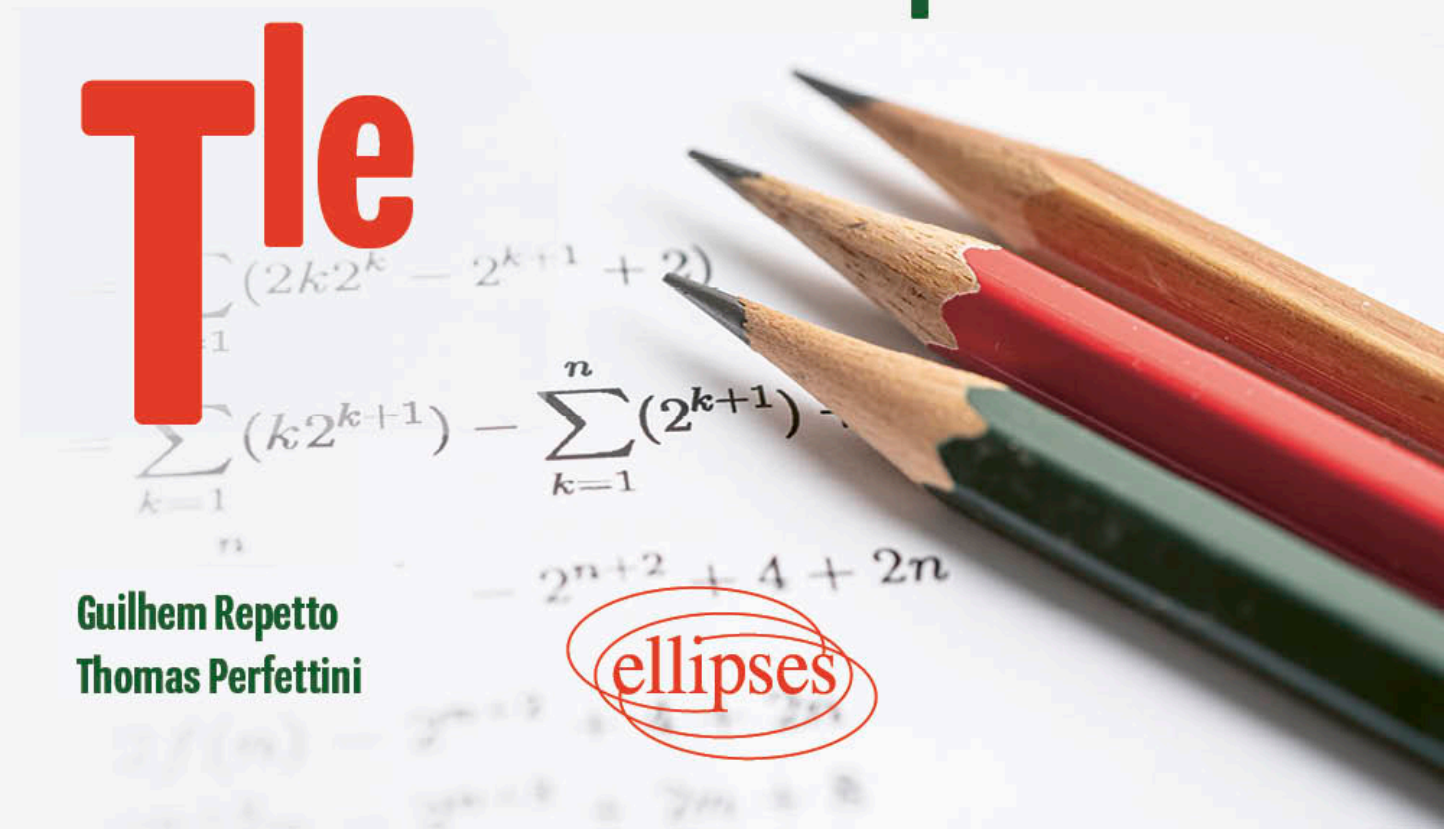
PROBLÈMES ORIGINAUX

pour l'éveil d'une curiosité mathématique

Tle



Guilhem Repetto
Thomas Perfettini

ellipses

Problème 1
Tous les critères de divisibilité

Le terme *arithmétique* provient du mot *arithmòs* qui, en grec ancien, signifie *nombre*. L'arithmétique désigne en conséquence l'étude des nombres, entiers, rationnels, voire réels, leurs relations et leurs propriétés, n'en déplaise à Walt Disney (1901-1966) qui disait : "*l'arithmétique, c'est être capable de compter jusqu'à 20 sans enlever ses chaussures*". Le "*prince des mathématiques*" Carl Friedrich Gauss (1777-1855), pour qui "*la mathématique est la reine des sciences et l'arithmétique est la reine des mathématiques*", en fut l'un des grands artisans. Si le théorème d'arithmétique qui porte son nom figurait déjà dans les *Éléments* d'Euclide (III^{e} siècle avant notre ère environ), c'est bien dans son ouvrage *Recherches arithmétiques* paru en 1801 qu'apparaît avec un formalisme inédit le principe fondamental des congruences, une notion qui aura de grandes conséquences dans le domaine de la théorie des nombres. Les contributions de Gauss ne se limitent pas à l'arithmétique. Ses travaux sont à l'origine de très riches développements algébriques et suscitent la formulation de structures explicites communes visant à répondre à une unité profonde des mathématiques. Gauss effectue également quelques avancées majeures en mécanique céleste ou en électromagnétisme. Célèbre dans toute l'Europe pour ces résultats, Gauss est aujourd'hui souvent considéré comme l'un des plus grands mathématiciens de tous les temps. La première expédition allemande en Antarctique au début du XX^{e} siècle, baptisée *expédition Gauss* et à l'origine de la découverte du *mont Gauss*, volcan éteint de l'est du continent, témoigne de la grande renommée du scientifique.

Notions utilisées : Congruences. Divisibilité. Nombres premiers.

L'objectif est d'établir et de démontrer en base dix des critères de divisibilité. On établit une méthode permettant de trouver un critère de divisibilité par tout nombre premier.

1 Critères classiques

Soit n un nombre entier quelconque. Pour $n \geq 10$, on note ce nombre $\overline{a_{r-1}a_{r-2}\dots a_1a_0}$. Les a_i, pour $i \in [\![0, r-1]\!]$, sont les chiffres de n en base 10, donc $\forall i \in [\![0, r-1]\!], a_i \in [\![0, 9]\!]$. La barre permet d'éviter la confusion avec la notation du produit.
Montrer les propriétés suivantes :

$2 \mid n \iff$ le chiffre des unités de n est pair
$3 \mid n \iff$ la somme des chiffres de n est multiple de 3
$4 \mid n \iff$ le nombre formé par les deux derniers chiffres de n est multiple de 4
$5 \mid n \iff$ le chiffre des unités de n est 0 ou 5
$6 \mid n \iff 2 \mid n$ et $3 \mid n$
$8 \mid n \iff$ le nombre formé par les trois derniers chiffres de n est multiple de 8
$9 \mid n \iff$ la somme des chiffres de n est multiple de 9
$10 \mid n \iff$ le chiffre des unités de n est 0

2 Critère de divisibilité par 7

1 Justifier l'existence d'un entier b tel que $10b \equiv 1[7]$ et trouver un entier vérifiant cette propriété.

2 Montrer que

$$\overline{a_{r-1}\dots a_1a_0} \equiv 0[7] \iff \overline{a_{r-1}\dots a_1} + b \times a_0 \equiv 0[7]$$

3 Conclure sur un critère de divisibilité par 7.

4 Le nombre 5321897 est-il multiple de 7 ?

3 Généralisation à un nombre premier quelconque

Soit p un nombre premier différent de 2 et 5.

1 Justifier l'existence de $b \in \mathbb{Z}$ tel que

$$10b \equiv 1[p] \tag{1}$$

2 Soit a un entier non divisible par p. Montrer que quels que soient k et k' dans $\mathbb{Z}$, si $ka \equiv k'a[p]$, alors $k \equiv k'[p]$.

L'objectif est de décrire l'ensemble des b qui conviennent dans l'équation (1) en fonction du nombre premier p. Pour cela, on démontre dans la question suivante le "petit" théorème de Fermat :

Théorème : soit p un nombre premier et a non divisible par p. Alors,

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

3 (a) Montrer que quel que soit k non-multiple de p, on a $p \nmid ka$.
On pose $N = a \times 2a \times \cdots \times (p-1)a$.

(b) Montrer que $N = a^{p-1}(p-1)!$.

(c) Pour tout $k \in [\![1, p-1]\!]$, on pose r_k le reste de la division euclidienne de ka par p.
Montrer alors que pour tout $k \in [\![1, p-1]\!]$, $0 < r_k \leq p-1$ et que les r_k sont tous deux à deux distincts.

(d) En déduire que $N \equiv r_1 \times r_2 \times \cdots \times r_{p-1}[p]$, puis $r_1 \times r_2 \times \cdots \times r_{p-1} = (p-1)!$.

(e) Conclure la preuve du théorème.

4 En utilisant le petit théorème de Fermat, décrire l'ensemble des entiers b vérifiant (1).

5 Déduire un critère de divisibilité par p similaire au critère de divisibilité par 7 déterminé à la partie précédente.

6 Application : Le nombre 1358024679 est-il divisible par 11 ?

Indications

1 Critères classiques

Ne pas oublier que, pour tout entier $n \in \mathbb{N}$ et tout entier $p \in \mathbb{N}$, on a l'équivalence suivante :

$$n \text{ divisible par } p \iff n \equiv 0[p]$$

Pour les multiples de 3, remarquer que $10 \equiv 1[3]$

2 Critère de divisibilité par 7

1. Utiliser le théorème de Bézout.
2. Utiliser le fait que $\overline{a_{r-1} \dots a_0} = 10\overline{a_{r-1} \dots a_1} + a_0$.
3. Appliquer plusieurs fois le résultat démontré.
4. Application numérique immédiate de l'algorithme décrit précédemment.

3 Généralisation à un nombre premier quelconque

1. Utiliser encore le théorème de Bézout.
2. (a) Utiliser le lemme de Gauss.
   (b) Mettre tous les a ensemble et reconnaître ce qui reste.
   (c) Utiliser la définition du reste dans la division euclidienne et expliquer pourquoi p ne divise pas ka. Pour montrer que les restes sont distincts, raisonner par l'absurde.
   (d) Si les r_i sont distincts et ne peuvent valoir que $p-1$ valeurs possibles, alors le produit des r_i est le produit de ces valeurs.
   (e) Exploiter les deux expressions de l'entier N modulo p.
3. Revenir à la définition de la congruence modulo p.
4. Effectuer le produit $(p-1)!$ de deux façons différentes.
5. Utiliser à nouveau le fameux théorème en remarquant que $1, 2, \dots, (p-1)$ sont premiers avec p
6. Comprendre ce qui a été fait pour le cas particulier $p = 7$ et généraliser

Corrigé

1 Critères classiques

2. Si $n \leq 9$, alors n est divisible par 2 si et seulement si $n \in \{0, 2, 4, 6, 8\}$. Sinon, on peut écrire $n = \overline{a_{r-1} \dots a_1 a_0} = 10 \times \overline{a_{r-1} \dots a_1} + a_0$. On obtient alors :

$$\begin{aligned} & n \equiv 0[2] \\ \iff & 10 \times \overline{a_{r-1} \dots a_1} + a_0 \equiv 0[2] \\ \iff & 2 \times (5 \times \overline{a_{r-1} \dots a_1}) + a_0 \equiv 0[2] \\ \iff & a_0 \equiv 0[2] \end{aligned}$$

   Dans les deux cas, on trouve le critère souhaité.

3. On remarque que $10 = 3 \times 3 + 1 \equiv 1[3]$. On obtient les équivalences suivantes, en notant $n = \overline{a_{r-1} \dots a_1 a_0}$:

$$\begin{aligned} & \overline{a_{r-1} \dots a_1 a_0} \equiv 0[3] \\ \iff & a_{r-1} 10^{r-1} + \dots + a_1 10^1 + a_0 10^0 \equiv 0[3] \\ \iff & a_{r-1} + \dots + a_1 + a_0 \equiv 0[3] \end{aligned}$$

4. Si $n \leq 99$, rien n'est à vérifier. Sinon, on peut écrire $n = \overline{a_{r-1} \dots a_1 a_0} = 100 \times \overline{a_{r-1} \dots a_2} + \overline{a_1 a_0}$. Or, $100 = 4 \times 25$. On obtient bien $n \equiv \overline{a_1 a_0}[4]$.

5. On note u le chiffre des unités de n. On peut alors écrire $n = 10k + u$ et donc $n \equiv u[5]$. On a donc $n \equiv 0[5] \iff u \in \{0, 5\}$.

6. En remarquant que $6 = 2 \times 3$ et que $2 \wedge 3 = 1$, on conclut grâce au lemme de Gauss que n est multiple de 6 si et seulement s'il est multiple de 2 et de 3.

8. On procède comme pour 2 et 4 : en écrivant $n = 1000 \times \overline{a_{r-1} \dots a_3} + \overline{a_2 a_1 a_0}$, on obtient en remarquant que $1000 = 8 \times 125$ que $n \equiv \overline{a_2 a_1 a_0}[8]$

9. On procède comme pour le cas 3 : en remarquant que $10 \equiv 1[9]$, on obtient

$$\begin{aligned} & \overline{a_{r-1} \dots a_1 a_0} \equiv 0[9] \\ \iff & a_{r-1} 10^{r-1} + \dots + a_1 10^1 + a_0 10^0 \equiv 0[9] \\ \iff & a_{r-1} + \dots + a_1 + a_0 \equiv 0[9] \end{aligned}$$

10. On a $10 = 2 \times 5$ et $2 \wedge 5 = 1$, d'où $10 \mid n \iff 5 \mid n$ et $2 \mid n$. D'après les cas 2 et 5 déjà étudiés, on conclut que 0 est le seul chiffre des unités possible.

2 Critère de divisibilité par 7

1 Les nombres $10 = 2 \times 5$ et 7 sont premiers entre eux. D'après le théorème de Bézout, il existe $(b, c) \in \mathbb{Z}^2$ tel que $10b + 7c = 1$, c'est-à-dire $10b \equiv 1[7]$. Avec quelques essais, on trouve que $-2 \times 10 = -20 \equiv 1[7]$. Nous utiliserons $b = -2$ dans ce corrigé, mais on aurait pu choisir n'importe quel entier de l'ensemble $\{7k - 2, k \in \mathbb{Z}\}$.

2 On a :

$$\begin{aligned}
&\overline{a_{r-1} \dots a_1 a_0} \equiv 0[7] \\
\iff &10 \times \overline{a_{r-1} \dots a_1} + a_0 \equiv 0[7] \\
\implies &(-2) \times 10 \times \overline{a_{r-1} \dots a_1} + (-2) \times a_0 \equiv 0[7] \\
\iff &\overline{a_{r-1} \dots a_1} - 2a_0 \equiv 0[7]
\end{aligned}$$

ce qui montre le sens $\Rightarrow$ de l'équivalence recherchée. Montrons le sens $\Leftarrow$:

$$\begin{aligned}
&\overline{a_{r-1} \dots a_1} - 2a_0 \equiv 0[7] \\
\implies &10 \times \overline{a_{r-1} \dots a_1} - 10 \times 2a_0 \equiv 0[7] \\
\iff &10 \times \overline{a_{r-1} \dots a_1} + a_0 \equiv 0[7] \\
\iff &\overline{a_{r-1} \dots a_2 a_1 0} + a_0 \equiv 0[7] \\
\iff &\overline{a_{r-1} \dots a_1 a_0} \equiv 0[7]
\end{aligned}$$

Nous avons donc démontré l'équivalence demandée.

3 Pour décider si un nombre n est multiple de sept, nous avons trouvé un algorithme : il suffit de "détacher" le chiffre des unités et de le soustraire deux fois au nombre restant. On répète cette opération tant que le nombre est positif, ou jusqu'à obtenir un nombre manifestement multiple ou non de sept, qui donne alors la réponse à la question !

Pour s'assurer que cet algorithme s'arrête quel que soit le nombre à étudier, il suffit de vérifier que la suite des nombres obtenue est strictement décroissante.

Une étape quelconque transforme un nombre $10\overline{a_{r-1} \dots a_1} + a_0$ (où $a_{r-1} > 0$) en $\overline{a_{r-1} \dots a_1} - 2a_0$. On a

$$\begin{aligned}
&10\overline{a_{r-1} \dots a_1} + a_0 > \overline{a_{r-1} \dots a_1} - 2a_0 \\
\iff &9\overline{a_{r-1} \dots a_1} + 3a_0 > 0
\end{aligned}$$

Comme a_{r-1} est strictement positif, on a bien :

$$9\overline{a_{r-1} \dots a_1} + 3a_0 > \overline{a_{r-1} \dots a_1} > 0$$

Finalement, on a bien

$$10\overline{a_{r-1}\dots a_1} + a_0 > \overline{a_{r-1}\dots a_1} - 2a_0$$

ce qui montre la stricte décroissance de la suite parcourue par l'algorithme. Comme cette suite est positive, elle ne peut posséder qu'un nombre fini de termes ; l'algorithme s'arrête.

Le dernier terme de la suite possède un ou deux chiffres ; il suffit de connaître tous les multiples de sept inférieurs à cent pour déterminer si le nombre de départ est ou non multiple de sept.

4 Appliquons la méthode trouvée au nombre 5321897 :

$$\begin{aligned}
&5321897 \equiv 0[7]\\
\iff &5321897 - 2\times 7 = 532175 \equiv 0[7]\\
\iff &53217 - 2\times 5 = 53207 \equiv 0[7]\\
\iff &5320 - 2\times 7 = 5306 \equiv 0[7]\\
\iff &530 - 2\times 6 = 518 \equiv 0[7]\\
\iff &51 - 2\times 8 = 35 \equiv 0[7]
\end{aligned}$$

Comme 35 est multiple de sept, le nombre 5321897 est aussi multiple de sept.

Remarque : on peut établir un critère de divisibilité par 7 plus "proche" de ceux de divisibilité par 3 et 9 en observant les résidus modulo 7 des puissances de 10 :

k	0	1	2	3	4	5	6	7	...
$10^k \bmod 7$	1	3	2	-1	-3	-2	1	3	...

En notant $(u_n)_{n\in\mathbb{N}}$ la suite de ces résidus pris dans $[\![-3,3]\!]$, on constate que $(u_n)_{n\in\mathbb{N}}$ est périodique, et que sa plus petite période vaut 6. En notant $n = \overline{a_{r-1}\cdots a_0} = \sum_{j=0}^{r-1} a_j 10^j$, on dispose donc l'équivalence suivante :

$$n \equiv 0[7] \iff \sum_{j=0}^{r-1} a_j u_j \equiv 0[7]$$

Dans l'exemple du nombre 5321897, cela donne

$$\begin{aligned}
5648125 \equiv 0[7] &\iff 7u_0 + 9u_1 + 8u_2 + 1u_3 + 2u_4 + 3u_5 + 5u_6 \equiv 0[7]\\
&\iff 42 \equiv 0[7]
\end{aligned}$$

Corrigé

Ce nouveau critère revient à effectuer d'un coup tous les calculs plutôt que de "détacher" successivement le chiffre des unités et le soustraire deux fois au nombre restant. Dans les critères de divisibilité par 3 et 9, la suite $(u_n)_{n\in\mathbb{N}}$ était constante égale à 1. Dans le cas de la divisibilité par 7, sa plus petite période est 6, ce qui la rend plus difficile à mémoriser. La même approche pour des critères de multiplicité par un nombre premier $p > 7$ donnera toujours une suite $(u_n)_{n\in\mathbb{N}}$ de plus petite période $p - 1$.

3 Généralisation à un nombre premier quelconque

1 En particulier, p est premier avec 10, donc le théorème de Bézout assure l'existence d'entiers b, c tels que $10b + pc = 1$, donc en particulier $10b \equiv 1[p]$.

2 Soient k et k' des entiers vérifiant $ka \equiv k'a[p]$. On a alors par définition $p \mid ka - k'a$ donc $p \mid (k - k')a$. Sachant que $p \nmid a$, d'après le lemme de Gauss, on a donc $p \mid k - k'$, c'est-à-dire $k \equiv k'[p]$.

3 (a) Supposons par l'absurde qu'il existe k non-multiple de p tel que $p \mid ka$. Par le lemme de Gauss, comme $p \nmid a$, on obtient $p \mid k$, ce qui est contradictoire.

Finalement, on a bien $p \nmid ka$.

(b) On a :

$$\begin{aligned} N &= a \times 2a \times \cdots \times (p-1)a \\ &= \underbrace{a \times a \times \cdots \times a}_{p-1 \text{ fois}} \times 1 \times 2 \times \cdots \times (p-1) \\ &= a^{p-1}(p-1)! \end{aligned}$$

(c) Pour tout $k \in [\![1, p-1]\!]$, on a par définition $0 \leq r_k < p \iff 0 \leq r_k \leq p-1$; or, on sait que $p \nmid ka$ (d'après la question (a) et sachant que k n'est pas un multiple de p), donc $r_k \neq 0$ pour tout $k \in [\![1, p-1]\!]$.

Supposons désormais $r_k = r_l$ pour l et k deux entiers distincts de $[\![1, p-1]\!]$. On peut supposer par exemple $k > l$.

On sait qu'il existe deux entiers k_1 et k_2 tels que :

$$ka = k_1 p + r_k \quad \text{et} \quad la = k_2 p + r_k \iff r_k = ka - k_1 p \quad \text{et} \quad r_k = la - k_2 p$$

On obtient alors :

$$ka - k_1 p = la - k_2 p \iff a(k-l) = p(k_1 - k_2) \iff p \mid a(k-1)$$

D'après la question (a) et sachant que $k - 1$ n'est pas un multiple de p, ceci est impossible.