TD11

Entiers naturels et dénombrement

Exercice 4 (Numérotation en base $b \geq 2$)

1. Démontrer que tout entier $a \in \mathbb{N}^*$ s'écrit sous la forme
$$a = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0,$$
où $n \in \mathbb{N}$ et $0 \leq a_i \leq b-1$, $a_n \neq 0$.

2. Démontrer que la décomposition précédente est unique. On l'appelle **l'écriture de l'entier** a **dans la base** b.

3. (a) Écrire 17 en base $10, 9, 8, 7, 6, 5, 4, 3, 2$ respectivement.
   (b) Trouver la base b dans laquelle on a $14 \times 41 = 1224$.

4. En notant que $7 \times 11 \times 13 = 1001$, déterminer un critère de divisibilité d'un entier $n = \overline{a_n \cdots a_2 a_1 a_0}$ par $7, 11$ ou 13 faisant intervenir la somme $\overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \cdots$.

5. Écrire un algorithme de numérotation en base b.

Solution.

3. (b) On cherche la base b dans laquelle $14 \times 41 = 1224$. Tout d'abord on a $b \geq 5$ puisque le chiffre 4 est utilisée dans l'écriture de ces nombres. On traduit l'égalité de l'énoncé par :
$$(b+4) \times (4b+1) = b^3 + 2b^2 + 2b + 4$$
soit encore
$$4b^2 + 17b + 4 = b^3 + 2b^2 + 2b + 4 \quad \Leftrightarrow \quad (b^2 - 2b - 15)b = 0.$$
Puisque $b \neq 0$, on a $b^2 - 2b - 15 = 0$, et donc $b = -3$ ou $b = 5$. Finalement $b = 5$.

4. Prenons $n = \overline{a_p \cdots a_2 a_1 a_0}$. On a, quitte à rajouter des zéros dans l'écriture décimale de n :
$$n = (a_0 + 10a_1 + 10^2 a_2) + 1000(a_3 + 10a_4 + 10^2 a_5) + \cdots + 1000^k (a_{3k} + 10a_{3k+1} + 10^2 a_{3k+2}).$$
Maintenant on a
$$1000^k = (1001-1)^k = \sum_{i=0}^{k} \binom{n}{k} 1001^i (-1)^{k-i}$$
qui est de la forme $(-1)^k + 1001 N_k$ avec $N \in \mathbb{N}$. Ainsi on obtient en remplaçant :
$$\begin{aligned} n &= (a_0 + 10a_1 + 10^2 a_2) + (-1 + 1001N_1)(a_3 + 10a_4 + 10^2 a_5) \\ &\quad + \cdots + ((-1)^k + 1001N_k)(a_{3k} + 10a_{3k+1} + 10^2 a_{3k+2}) \\ &= (a_0 + 10a_1 + 10^2 a_2) - (a_3 + 10a_4 + 10^2 a_5) + \cdots + (-1)^k (a_{3k} + 10a_{3k+1} + 10^2 a_{3k+2}) + 1001N \end{aligned}$$
avec $N \in \mathbb{N}$. Donc 1001 divise n si et seulement si il divise la somme $\overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \cdots$.
Finalement un entier n est divisible par $7, 11$ ou 13 si et seulement si 1001 divise la $\overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \cdots$.

5. On procède comme à la question 1. en faisant les divisions successives.

Entrer n.
$q \leftarrow n$
Tant que $q > 0$, faire :
  $r \leftarrow$ reste de la division euclidienne de q par b
  $q \leftarrow$ quotient de la division euclidienne de q par b
  Sortir r.

Exercice 5

Calculer le pgcd de $a = 9100$ et $b = 1848$, puis de $a = n^3 + 2n$ et $b = n^4 + 3n^2 + 1$ pour tout $n \in \mathbb{N}^*$.

Solution.

On a $b - na = n^2 + 1$, $a - n(n^2 + 1) = n$ et $n^2 + 1 - n \times n = 1$. Ainsi, si d divise a et b, il divise successivement $n^2 + 1$, n et 1. Donc $d = 1$ et $a \wedge b = 1$.

Exercice 11

Déterminer les entiers $b \in \mathbb{N}^*$ tels que $\text{ppcm}(28, b) = 140$.

Solution.

On a $28 = 2^2 \times 7$ et $140 = 2^2 \times 5 \times 7$. Puisque b divise 140, b est de la forme $b = 2^p \times 5^q \times 7^r$ avec $0 \leq p \leq 2$, $0 \leq q \leq 1$ et $0 \leq r \leq 1$. Alors $28 \vee b = 2^2 \times 5 \times 7$ équivaut à

$$\max(2, p) = 2, \quad \max(0, q) = 1 \quad \text{et} \quad \max(1, r) = 1.$$

Ainsi b satisfait cette égalité si et seulement si $b = 2^p \times 5 \times 7^r$ avec $0 \leq p \leq 2$ et $0 \leq r \leq 1$.

Exercice 14 (Petit théorème de Fermat)

1. Soit $p \in \mathbb{P}$. Montrer que pour tout $k = 1, \cdots, p - 1$, $p | \binom{p}{k}$.
2. En déduire que pour tout $n \in \mathbb{Z}$, p divise $n^p - n$.
3. (a) Montrer que pour tout $a \in \mathbb{Z}$, 42 divise $a^7 - a$.
   (b) Montrer que pour tout $n \in \mathbb{Z}$, $\frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35} \in \mathbb{Z}$.

Solution.

3. b) Par le petit théorème de Fermat,on a 7 qui divise $n^7 - n$ et 5 qui divise $n^5 - n$ pour tout $n \in \mathbb{Z}$. Ainsi, on a :

$$\frac{n^7 - n}{7} + \frac{n^5 - n}{5} \in \mathbb{Z}.$$

Mais ce nombre est égal à $\dfrac{n^7 - n}{7} + \dfrac{n^5 - n}{5} = \frac{n^7}{7} + \frac{n^5}{5} - \frac{12}{35}n = \frac{n^7}{7} + \frac{n^5}{5} + \frac{23}{35}n - n$. Finalement, on a bien que pour tout $n \in \mathbb{Z}$,

$$\frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35} \in \mathbb{Z}.$$

Exercice 15 (Infinité de nombres premiers de la forme 4n-1)

On suppose qu'il existe un nombre fini N d'entiers premiers de la forme $4n - 1$ où $n \geq 1$. On les note $p_1, \ldots, p_N$, et on forme le nombre $4p_1 \ldots p_N - 1$. Montrer que ce nombre admet nécessairement un diviseur premier de la forme $4n - 1$, et en déduire une contradiction. Conclure.

Solution.
Le nombre $A = 4p_1 \dots p_N - 1$ est impair. Ainsi ses diviseurs premiers sont de la forme $4n-1$ ou $4n+1$. Supposons que ce nombre n'admet aucun diviseur premier de la forme $4n-1$, alors tous ces diviseurs premiers sont de la forme $4n+1$. Mais alors il serait lui même de la forme $4n+1$ (en remarquant que $(4p+1)(4q+1) = 4(4pq+p+q)+1$). Or ceci est impossible, puisqu'alors

$$4p_1 \dots p_N - 1 = 4n+1 \quad \Leftrightarrow \quad 4(p_1 \dots p_N - n) = 2$$

et 4 diviserait 2.
Donc A a au moins un diviseur premier de la forme $4n-1$, par exemple p_1. Or ceci est impossible également car sinon p_1 diviserait $4p_1 \dots p_N - A = 1$.
Ainsi l'hypothèse de départ était absurde, et on a bien démontré l'existence d'une infinité de nombres premiers de la forme $4n-1$.

On peut montrer qu'il y a également une infinité de nombres premiers de la forme $4n-1$, mais la preuve est plus difficile.