Aujourd'hui nous allons discuter :

- Représentation décimal, binaire, hexadécimal
- Divisibilité par 9 ou 7, et cetera.
- Théorème de Fermat (sans preuve)
- Changement de sujet : appliquer ensembles/fonctions
- Un principe de tiroir de Dirichlet
- et un autre principe de tiroir de Dirichlet

Représentations des nombres naturels

Maintenant nous représentons les entiers en forme décimale. Ce n'était pas toujours le cas.

Les romains : ex. *MMXIX* (=2019).

Par exemple, 12054 veut dire

$$12054 = 1 \cdot 10^4 + 2 \cdot 10^3 + 0 \cdot 10^2 + 5 \cdot 10^1 + 4 \cdot 10^0.$$

On peut aussi utiliser une base autre que 10. Par exemple les bases 2 et 16 sont utilisées en informatique. Sur base 2 (forme binaire) :

$$\begin{aligned} [100101]_2 &= 2^5 + 2^2 + 2^0 \\ &= [32]_{10} + [4]_{10} + [1]_{10} \\ &= [37]_{10}. \end{aligned}$$

Soit $b > 1$, un nombre naturel, la base choisie. Alors on peut écrire $n \in \mathbb{N}$ sur la forme

$$n = [c_s, c_{s-1}, \ldots, c_1, c_0]_b = c_s b^s + c_{s-1} b^{s-1} + \ldots + c_1 b^1 + c_0 b^0,$$

ou chaque "chiffre" $c_i \in \mathbb{N}$ est plus petit que b.

Possiblement il faut inventer des notations pour les chiffres !

Par exemple, pour base 16 on utilise les 16 chiffres

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$$

$A =$dix, $B =$onze, $C =$ douze, D treize, $E =$ quatorze, $F =$ quinze.

Par exemple

$$N = [2AE0B]_{16}$$

signifie dans notre notation décimale usuelle le nombre

$$N = 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = 175627.$$

Alternativement, on écrit

$$[2, 10, 14, 0, 11]_{16}$$

Comment écrire un nombre N sur la base $b > 1$?
Réponse : Avec division-avec-reste par b répété !

• Par division avec reste il y a q_0 et c_0 tel que $N = q_0 b + c_0$, et $0 \leq c_0 < b$.

• Puis il y a q_1 et c_1 tel que $q_0 = q_1 b + c_1$, et $0 \leq c_1 < b$.

• Puis il y a q_2 et c_2 tel que $q_1 = q_2 b + c_2$, et $0 \leq c_2 < b$.
Et cetera.

• On arrête dès que q_i devient 0.

Alors

$$N = [c_s, c_{s-1}, \ldots, c_1, c_0]_b.$$

Exemple, si $b = 16$ et $N = 357899$.

$$\begin{aligned} 357899 &= 22368 \cdot 16 + 11 \\ 22368 &= 1398 \cdot 16 + 0 \\ 1398 &= 87 \cdot 16 + 6 \\ 87 &= 5 \cdot 16 + 7 \\ 5 &= 0 \cdot 16 + 5 \end{aligned}$$

Donc (rappel : $A = 10, B = 11, C = 12, D = 13, E = 14, F = 15$).

$$357911 = [5760B]_{16} = [5, 7, 6, 0, 11]_{16}.$$

Supposons on a écrit le nombre naturel N sur la base 7 :

$$N = [6, 5, 6, 3, 0, 2, 3, 5, 0, 0]_7$$

Alors $7|N$ et même $7^2|N$.

Pourquoi ?

Problème :

Soit $n = (13^{27} + 199 \cdot 23 - 311) \cdot (2345 + 11^5)$.

Quel est le dernier chiffre de n dans la représentation hexadécimale ?

Réponse : On a $n > 0$ donc nous cherchons le nombre $0 \leq r < 16$ tel que $n \equiv r \mod 16$. Calculons modulo 16.

$$\begin{aligned}
n &\equiv_{16} ((-3)^{27} + 7 \cdot 7 - 7) \cdot (9 + (-5)^5) \\
&\equiv_{16} ((9)^{13} \cdot (-3) + 42) \cdot (9 + (25)^2 \cdot (-5)) \\
&\equiv_{16} ((81)^6 \cdot 9 \cdot (-3) + 10) \cdot (9 + (9)^2 \cdot (-5)) \\
&\equiv_{16} ((1)^6 \cdot (-27) + 10) \cdot (9 + (81) \cdot (-5)) \\
&\equiv_{16} (-17) \cdot (9 + (1) \cdot (-5)) \\
&\equiv_{16} (-1) \cdot (4) \\
&\equiv_{16} -4 \\
&\equiv_{16} 12
\end{aligned}$$

Donc le dernier chiffre est C(douze).

Divisibilité par 9.

Soit N est le nombre naturel qu'on écrit sur la base 10 comme

$$N = 3576043.$$

Est-ce que N est divisible par 9 ?

Test :

On a $3 + 5 + 7 + 6 + 0 + 4 + 3 = 28$

et $2 + 8 = 10$ et $1 + 0 = 1$.

Mais 1 n'est pas divisible par 9 donc

Non : N n'est pas divisible par 9.

Divisibilité par 7.

Soit N est le nombre naturel qu'on écrit sur la base 8 comme

$$N = [3576043]_8.$$

Est-ce que N est divisible par 7 ?

Test :

On a $3 + 5 + 7 + 6 + 0 + 4 + 3 = 28 = [34]_8$

et $3 + 4 = 7$.

On a 7 est divisible par 7 donc

Oui : N est divisible par 7.

Pourquoi ?

Soit $b > 0$ un nombre tel que $b \equiv_7 1$ (par exemple $b = 8$).
Soit le nombre naturel N représenté sur la base $b > 0$ comme $N = [c_r, c_{r-1}, \ldots, c_1, c_0]_b$.

Alors N est divisible par 7 si et seulement si la somme des chiffres est divisible pas 7. Et même : N et la somme de ses chiffres ont le même reste après division par 7 :

$$N \equiv_7 (c_0 + c_1 + c_2 + \ldots + c_r).$$

Preuve :

$$N = \sum_{i=0}^{r} c_i b^i \equiv_7 \sum_{i=0}^{r} c_i 1^i = (c_0 + c_1 + c_2 + \ldots + c_r).$$

Pour finir : théorème de Fermat.

Fermat a trouvé le théorème suivant (pas montré ici).
Soit p un nombre premier. Alors pour chaque entier a on a

$$a^p \equiv_p a.$$

(Une preuve par induction, trouvé par Euler, est faisable à la fin du cours).
Avant une preuve est donnée, vous n'avez pas encore le droit d'utiliser ce théorème.

Par example, 19 est premier. Alors le théorème prédit $5^{19} \equiv_{19} 5$. Nous allons vérifier dans ce cas :

$$\begin{array}{rcl} 5^2 & = & 25 \equiv_{19} 6 \\ 5^4 & \equiv_{19} & 36 \equiv_{19} -2 \\ 5^8 & \equiv_{19} & 4 \\ 5^{16} & \equiv_{19} & 16 \equiv_{19} -3 \\ 5^{18} & = & 5^{16} \cdot 5^2 \equiv_{19} -3 \cdot 6 \equiv_{19} 1 \\ 5^{19} & \equiv_{19} & 5 \end{array}$$

Et en effet.

Conclusion.

Nous avions discuté des propriétés des entiers, induction, factorisation première, le pgcd, l'algorithme d'Euclide-Bézout, le théorème de Bézout.

Entiers-modulo-m, et autres relations d'équivalence.

Calculer dans $\mathbb{Q}$ et $\mathbb{Z}/n\mathbb{Z}$.

Nous allons maintenant changer le sujet.

Cherchez la fonction, pardieu !

Pour résoudre beaucoup de problèmes en pratique :

La clef pour avoir du succès est de reformuler les vraies problèmes en termes de constructions avec des ensembles et des fonctions.

Cherchez l'ensemble, pardieu ! et cherchez la fonction !

(Alexandre Dumas (1854) : "Cherchez la femme, pardieu ! Cherchez la femme !")

Considérons :

Proposition

Soit $f : A \to B$ *une fonction entre deux ensembles finis. Posons* $n = |A|$ *et* $m = |B|$*.*

(i) Si $n > m$ *alors il existe un* $b \in B$ *tel que* $|f^{-1}(b)| \geq 2$*.*

(ii) Plus généralement, si pour un nombre naturel r *on a* $n > rm$ *alors il existe un* $b \in B$ *tel que* $|f^{-1}(b)| \geq r + 1$*.*

Remarque : Pour $f : A \to B$ on a en général que

$$|A| = \sum_{b \in B} |f^{-1}(b)|,$$

parce que $A = \bigcup_{b \in B} f^{-1}(b)$ est une partition :

$f^{-1}(b) \cap f^{-1}(b') = \emptyset$ (si $b \neq b'$), et $a \in f^{-1}(f(a))$.

Démonstration.

(i) est le cas spécial de (ii) où $r = 1$.

(ii) Supposons par contre que $|f^{-1}(b)| \leq r$ pour chaque $b \in B$.
Alors

$$n = |A| = \sum_{b \in B} |f^{-1}(b)| \leq |B|r = mr,$$

ce qui est en contradiction avec l'hypothèse $n > rm$. Donc en effet il existe un $b \in B$ tel que $|f^{-1}(b)| \geq r + 1$. $\square$

Une reformulation classique :

Corollaire (Principe des tiroirs de Dirichlet)

(i) Si $m + 1$ *objets ou plus sont rangés dans* m *tiroirs, alors il y aura au moins un tiroir qui contient deux objets ou plus.*

(ii) Plus généralement, supposons n *objets sont rangés dans* m *tiroirs et supposons pour un nombre naturel* r *on a* $n > rm$*. Alors il y aura au moins un tiroir que contient au moins* $r + 1$ *objets.*

Cherchez la fonction pardieu !

Démonstration.
Soit A l'ensemble des objets et B l'ensemble des tiroirs. Si l'objet x est rangé dans le tiroir t on écrit $f(x) = t$. Ça donne une fonction $f : A \to B$.

(i) On a $|A| > m$ et $|B| = m$. Donc, par la prop. avant, il existe un $t \in B$ tel que $|f^{-1}(t)| \geq 2$.

Traduction : dans ce tiroir t on a rangé au moins 2 objets.

(ii) Similaire. $\square$

Ex :
On suppose qu'un groupe de pigeons s'envole vers un ensemble de nids pour s'y percher.
On suppose aussi qu'il y a plus de pigeons que de nids.

Alors il doit y avoir au moins un nid dans lequel se trouvent au moins deux pigeons.

Ex :

Dans un groupe avec au moins 367 personnes, il doit y avoir au moins deux personnes qui ont la même date d'anniversaire.

La fonction $f : A \to B$, ou les objets et les tiroirs sont ? ? ?

Exemple :
Dans un groupe avec au moins 241 personnes, il doit y avoir au moins vingt-et-un personnes qui ont dans le même mois leurs anniversaires.

Démonstration.
Soit A l'ensemble des personnes dans ce groupe et B l'ensemble des 12 mois. Si la personne P dans ce groupe est née dans le mois M on écrit $f(P) = M$. C'est une fonction $f : A \to B$. Ici $|A| = 241$ et $|B| = 12$ et $241 > 20 \cdot 12$. Donc il existe un mois M tel que $|f^{-1}(M)| \geq 21$.
C.-à-d., dans ce mois M au moins 21 personnes dans ce groupe a son anniversaire. $\square$

Exemple :

Soit $n > 1$ et E une collection d'au moins $n+1$ nombres entiers différents. Il existe deux nombres différents dans E, disons a et b, tels que leur différence $a - b$ est divisible par n.

Par exemple : $n = 7$ et l'ensemble de 8 entiers est

$$E = \{123-4567, -345438, 3^7-5^9, 23, 4545^3-1, 93*992, -1000, -238\}$$

La différence de deux des nombres différents dans E est divisible par 7.

(Mais quels ?)

Cherchez la fonction, pardieu !)

Démonstration.
Posons $B = \{m \in \mathbb{N} | 0 \leq m < n\}$. Soit $a \in E$. Il existe un unique $r \in B$ qui est le reste de a après division par n ; posons $f(a) = r$.

Ça donne une fonction $f : E \to B$. Ici $|E| > n$ et $|B| = n$.

Par le principe de Dirichlet : il existe un $r \in B$ tel que $|f^{-1}(r)| \geq 2$.

C.-à-d., il existe deux nombres dans E, disons a et b, qui ont le même reste r après division par n. Donc leur différence $a - b$ est divisible par n. $\square$

Un autre principe de tiroirs de Dirichlet.

Il y a un autre principe qui peut être illustré par les tiroirs de Dirichlet.

Proposition (Autre principe de tiroirs de Dirichlet)

Quelques objets sont rangés dans m tiroirs, tel que chaque tiroir contient exactement n objets. Alors on a rangé nm objets.

Évident, n'est-ce pas ? !

Proposition

Soit $f : A \to B$ une fonction entre deux ensembles finis, tels que pour chaque $b \in B$ on a $|f^{-1}(b)| = n$. Alors $|A| = |B| \cdot n$.

Démonstration.

On a en général

$$|A| = \sum_{b \in B} |f^{-1}(b)|,$$

parce que $A = \bigcup_{b \in B} f^{-1}(b)$ est une union disjointe (une partition).
Donc $|A| = |B|n$. $\square$

Démonstration de l'autre principe des tiroirs.

Soit A l'ensemble des objets et B l'ensemble des tiroirs.

Si l'objet x est rangé dans le tiroir t on écrit $f(x) = t$. Ça donne une fonction $f : A \to B$.

Dans chaque tiroir on a rangé n objets, donc $|f^{-1}(t)| = n$ pour chaque tiroir $t \in B$.

On a $m = |B|$. Par la prop. $|A| = mn$,

c.-à-d., on a rangé mn objets. $\square$

En conséquence, nous retrouvons

Corollaire

Soient E et F deux ensembles finis, et considérons le produit cartésien $E \times F$.

Alors

$$|E \times F| = |E| \times |F|.$$

Cherchez la fonction, pardieu !

Démonstration.
Posons $A = E \times F$ et $f : A \to E$ la fonction définie par $f((x, y)) = x$.

Si $x_0 \in E$, alors $f^{-1}(x_0) = \{(x_0, y) |\ y \in F\}$ est en bijection avec F.

Donc $|f^{-1}(x_0)| = |F|$.

Alors par l'autre principe des tiroirs : $|B| = |E| \cdot |F|$.
En effet. $\square$