

FICHE ENSEIGNANT

Niveau concerné

Cycle 4 : à partir de la 4^e

Durée : 2 séances

L'activité contient :

Affectation	X
Variable	X
Boucle	X
Test	X
Programmation parallèle	X

Compétences mathématiques :

Chercher	X
Raisonner	X
Modéliser	X
Représenter	
Calculer	X
Communiquer	X

Domaines du socle :

Domaine 1	Comprendre, s'exprimer en utilisant les langages mathématiques, scientifiques et informatiques
Domaine 2	Coopération et réalisation de projets
Domaine 3	
Domaine 4	Démarches scientifiques Conception, création, réalisation
Domaine 5	

Pré-Requis

Informatique :

- connaissance de l'environnement Scratch
- écrire un algorithme en langage naturel
- Notion de boucle

Mathématique :

- Notion de division euclidienne et vocabulaire associé
- Savoir poser une division à la main
- Puissance de 2 si l'on souhaite aller plus loin

Modalités et matériels

En salle informatique, travail individuel pendant deux séances de 50 minutes.

Objectifs

Les objectifs de cette activité sont d'initier les élèves à un exemple de codage et de chiffrement utilisé en informatique et de pratiquer eux-mêmes ce code en réalisant un programme sur Scratch permettant de coder un nombre en langage binaire.

Scénario

L'activité commence par une brève explication sur le chiffrement binaire et son fonctionnement.

On demande aux élèves de s'essayer au chiffrement binaire d'abord à la main afin de se familiariser avec la technique. On essaye alors de leur faire comprendre l'inconvénient et les limites de cette méthode manuelle. On souhaite qu'ils s'orientent très vite sur la mise en place d'un algorithme faisant « le travail à leur place ».

Pour cela, ils doivent passer par l'écriture au préalable d'un algorithme en langage naturel qui transforme un nombre donné par l'utilisateur en base 10 en un nombre en base 2.

Ils se lancent ensuite sur le logiciel Scratch afin de mettre en application leur programme précédent. Ils découvrent alors la commande « modulo » définie comme donnant le reste de la division euclidienne.

Afin de faciliter leur composition du programme, on leur donne les différents blocs à utiliser qu'ils doivent réordonner. Le programme est découpé en deux parties afin de guider les élèves pas à pas vers dans leur programmation :

- une première où les blocs sont donnés et où les élèves doivent les réagencer
- une deuxième partie correspondant à la remise en ordre des restes de la division euclidienne par 2 afin de lire ces restes dans le bon ordre.

Enfin, on termine le TP en leur demandant de tester le programme sur trois nombres afin de vérifier que tout fonctionne correctement.

Ce TP peut s'inscrire aussi dans l'étude des puissances de nombres en faisant le lien avec les puissances de 2. Il peut également faire l'objet d'une partie d'un EPI avec la technologie.

TP initiation au chiffrement binaire

Le chiffrement binaire, c'est quoi ?

L'homme a toujours eu besoin de compter et il a inventé la numération **décimale** (celle que l'on utilise « habituellement »).

C'est ce que l'on appelle la numération en **base 10** (dix, comme le nombre total de doigts sur nos deux mains réunies).

Cependant, il existe d'autres façons de compter que la numération décimale : dans les domaines de l'électronique, de l'automatisme ou encore de l'informatique, la numération **binaire** (en base 2) est plus souvent utilisée. Cela signifie que tous les nombres s'écrivent avec deux chiffres uniquement : **0 et 1**.

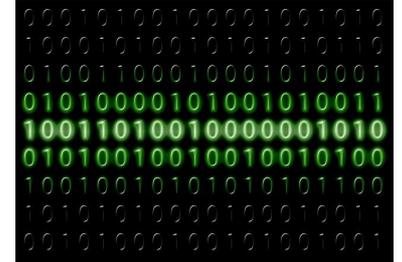
C'est Leibniz (un mathématicien allemand du XVII^{ème} siècle) qui a introduit la numération binaire telle qu'on la pratique actuellement en informatique.

Nous utilisons donc la numération binaire car les systèmes technologiques ont souvent deux états stables, par exemple : un interrupteur est **ouvert ou fermé** ; une diode est **allumée ou éteinte** ; une tension est **présente ou absente**.

Ainsi, à chaque état du système technologique, on associe un état logique binaire : l'interrupteur ouvert sera noté 1, et 0 s'il est fermé.

Le chiffre binaire qui peut prendre ces deux états est nommé « Bit » qui vient de l'anglais : *Binary digit*.

En informatique, une variable qui prend les valeurs 0 ou 1 exclusivement est dite **booléenne** (du mathématicien britannique George Boole au XIX^{ème} siècle).



Le chiffrement binaire, comment ça marche ?

Prenons un exemple : nous allons prendre un nombre dans notre numération décimale et nous allons l'écrire en numération binaire.

Choisissons le nombre 193 :

Pour transformer 193 en langage binaire, nous allons faire des divisions euclidiennes successives (c'est à dire des divisions « posées » les unes à la suite des autres) de 193 par 2 jusqu'à ce que le quotient soit égal à 0.

Rappel :

$$\begin{array}{r|l} a & b \\ r & q \end{array}$$

La division euclidienne correspond à la division « posée à la main ».

Cette image représente la division euclidienne du nombre a par le nombre b .
 q est le quotient et r le reste.

$$\begin{array}{r|l} 183 & 12 \\ 63 & 15 \\ 3 & \end{array}$$

Cette opération correspond à la division euclidienne de 183 par 12.

15 est le quotient, 3 est le reste.

On peut écrire le calcul en ligne : $183 = 12 \times 15 + 3$.

Reprenons notre exemple :

On a arrêté les divisions car à ce stade là, l'étape suivante serait d'écrire que $1 = 2 \times 0 + 1$

Le quotient suivant serait alors 0.

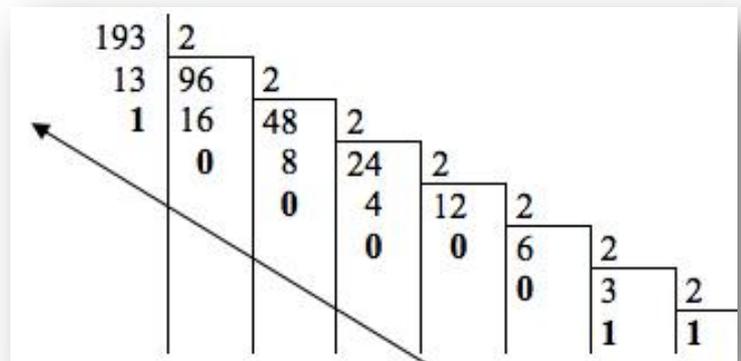
Ainsi la liste des restes obtenus par ces divisions successives est : 1 0 0 0 0 1 1

Il suffit alors de recopier cette liste à l'envers (ou bien directement de lire de bas en haut, comme sur l'image, les restes obtenus) pour dire que 193 en écriture binaire est **1 1 0 0 0 0 1**

Quel est l'inconvénient ?

C'est une méthode longue et au cours de laquelle les risques d'erreurs sont grands à cause du grand nombre de divisions.

On souhaite donc que ces calculs soient faits par un ordinateur grâce à un algorithme.



À ton tour de jouer !

1) Ecrire en langage binaire le nombre 53.



2) Ecrire avec vos propres mots un algorithme permettant de passer d'un nombre en écriture décimale à un nombre en écriture binaire.

Programmons pas à pas

Développons d'abord la partie du programme consacrée aux divisions successives par 2

- 1) Créez une variable appelée « Nombre » puis une liste appelée « restes des divisions ».

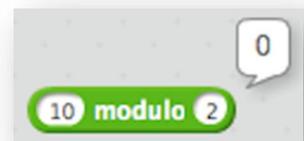
Dans la variable « Nombre » on affectera à chaque étape le nombre que l'on divise et la variable « restes des divisions » va contenir les restes des divisions successives.

- 2) Pour ajouter le reste d'une division dans la liste ainsi créée, il vous faudra utiliser la commande « modulo » dans opérateurs :



Ce nouvel opérateur donne le reste de la division euclidienne du premier nombre par le deuxième. Par exemple, si vous entrez 10 comme premier nombre et 2 comme deuxième nombre, vous obtiendrez 0 car $10 = 5 \times 2 + 0$.

De même, qu'obtenez-vous si vous mettez 53 à la place de 10 ?

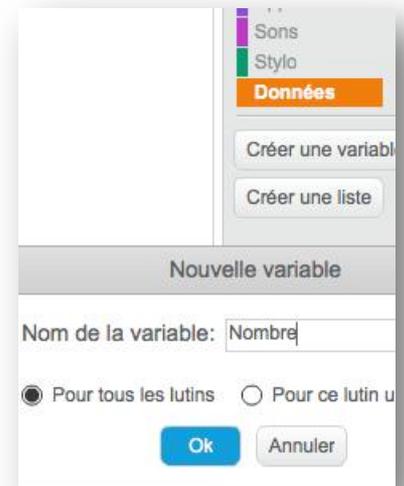


- 3) Pour obtenir le nouveau quotient des divisions successives, vous aurez besoin d'utiliser l'opérateur « plancher de » :



Par exemple,  renverra 5 comme résultat.

Familiarisez-vous avec ce nouvel opérateur : qu'obtenez-vous si vous demandez le plancher de $25/2$? Expliquez pourquoi.



- 4) Complétez la structure du programme ci-dessous afin que celui-ci demande un nombre à l'utilisateur et une fois celui-ci entré, le programme stocke les restes des divisions par 2 dans la liste appelée « restes des divisions »



Appelez le professeur pour validation avant de continuer

Développons ensuite la partie du programme consacrée à lire la liste des restes dans « l'autre sens »

- 1) Créez une variable « L » qui va lire la liste remplie précédemment des restes des divisions.
- 2) Créez une variable « Liste définitive » qui va contenir les éléments de la liste des restes des divisions lue dans le bon ordre.
- 3) Ré-assemblez les blocs suivants dans l'ordre puis rattachez-les au bloc précédent :



- 4) Faites dire au lutin de votre choix « le nombre est codé par » .
Pour cela, vous devrez utiliser l'opérateur « regroupe »

regroupe [] []

Cet opérateur vous permettra de faire des phrases qui utilisent des variables et des listes.

Tester votre programme

Testez votre programme avec votre date de naissance puis avec 2015 ; 2016.

Quels résultats obtenez-vous ?

Pour aller plus loin....

Lien entre numération binaire et puissance de 2

Déterminer l'écriture d'un nombre en binaire à partir des puissances de 2

Déterminer l'écriture d'un nombre en base 10 connaissant son écriture en base 2

Opérations avec des nombres en écritures binaires.