# MATHÉMATIQUES – ITS

# Programme du cours

- Arithmétique modulaire
- Systèmes de numération
- Calcul Matriciel
- Graphes

# Rappels sur les ensembles de nombres

- Nombres entiers naturels : $\mathbb{N}$
  - $\{0, 1, 2, 3, 4, \dots\}$
- Nombres entiers relatifs : $\mathbb{Z}$
  - *entiers naturels auxquels on adjoint un signe positif ou négatif*
- Nombres décimaux : $\mathbb{D}$
  - *peuvent s'écrire avec une quantité quelconque, mais finie, de chiffres à droite de la virgule (en base 10)*
    - $\frac{1}{2}$ est un nombre rationnel

# Rappels sur les ensembles de nombres

- Nombres rationnels : $\mathbb{Q}$
  - *peuvent s'exprimer comme le quotient de de deux entiers relatifs*
    - $\frac{1}{3}$ est un nombre rationnel mais pas un nombre décimal car $\frac{1}{3} = 0{,}3333333\ldots$
- Nombres réels : $\mathbb{R}$
  - *nombres rationnels + nombres ne pouvant pas d'écrire sous forme d'une fraction*
    - $\pi$ et $\sqrt{2}$ sont des nombres réels mais pas rationnels
- Nombres complexes : $\mathbb{C}$
  - *Nombres pouvant s'écrire sous la forme : $a + ib$*
    *où a et b sont des réels, et i un nombre imaginaire tel que $i^2 = -1$*
- $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

# Arithmétique modulaire

Dans ce cours : entiers relatifs

- Rappels sur la division euclidienne
- PGCD (Plus Grand Diviseur Commun)
- Nombres premiers

# Rappels sur la division euclidienne

- Division euclidienne (ou division entière)
- Initialement définie pour 2 entiers naturels non nuls, elle se généralise aux entiers relatifs
- À deux entiers $a$ (le dividende) et $b$ (le diviseur), avec $b$ non nul, la division euclidienne associe un quotient $q$ et un reste $r$, qui sont tous deux des entiers naturels, vérifiant :
  - $a = b \times q + r$
  - $0 \leq r \leq |b|$
  - *Exemple :* $17 = 3 \times 5 + 2$
- Il existe un unique couple $(q, r)$ d'entiers relatifs vérifiant ces deux propriétés

# Quotient et reste (ou modulo)

- Langages de programmation :
  - *Pour le calcul du quotient on a l'opérateur de division* $(x/y)$
    *qui pour les entiers renvoie la partie entière de la division*
  - *Pour le calcul du reste on a l'opérateur* $(x \,\%\, y)$
    *qui pour les entiers renvoie le reste de la division*

# Rappel de notation en pseudo-code pour les algorithmes

# Exercices

- Écrire un algorithme qui retrouve la valeur du diviseur d'une division ($y$) en ayant pour paramètres le dividende ($x$), le quotient ($q$) et le reste ($r$).
- Écrire un algorithme qui retrouve la valeur du reste d'une division ($r$) en ayant pour paramètres le dividende ($x$), le quotient ($q$) et le diviseur ($y$).
- Écrire un algorithme qui affiche tous les entiers de 1 à 100 qui sont divisibles par 5 mais pas divisibles par 3 en utilisant l'opérateur modulo ($\%$).

# Algorithmes de calcul de la division euclidienne

On va écrire trois algorithmes qui calculent le quotient et le reste d'une division, en supposant qu'on n'a pas les opérateurs correspondants.

- Méthode naïve
- Méthode décimale
- Méthode binaire

# Division euclidienne : exercices

- Méthode naïve

  *On suppose qu'on ne dispose pas des opérateurs de multiplication (∗), de division (/) et de modulo (%). Écrire un algorithme qui permet de calculer le quotient et le reste de la division euclidienne d'un entier x par un entier y en effectuant des soustractions successives.*

# Division euclidienne : exercices

- Méthode décimale

  *La méthode consiste à multiplier $b$ (le diviseur) par 10 plusieurs fois tant qu'il est inférieur à $a$ (le dividende) puis de faire la division (à l'identique de ce qu'on a fait pour la méthode naïve) et enfin de recommencer avec comme dividende le reste de la division de l'étape précédente.*

  *Écrire un algorithme permettant retournant le reste et le quotient de la division euclidienne d'un entier $x$ par un entier $y$.*

# Division euclidienne : exercices

- Déroulement sur un exemple
- Méthode binaire : principe
  - *Remplir un tableau contenant dans la première colonne les puissances de 2 et leur produit avec le diviseur $(y)$ dans la seconde colonne.*
  - *On s'arrête de remplir le tableau juste avant de dépasser le dividende $(x)$ dans la seconde colonne.*
  - *On essaie ensuite de constituer le plus grand multiple de $y$ inférieur à $x$ en sommant certaines cases de la seconde colonne.*
  - *En sommant les cases correspondantes de la première colonne on obtient le quotient de la division.*
- Écrire un algorithme qui effectue une division euclidienne (et qui renvoie le quotient et le reste) par cette méthode.

# Modulo : exercices

- Notation mathématique du reste (ou modulo) : $x \ mod \ y$

  *Exemples :* $13 \ mod \ 5 = 3$, $13 \ mod \ 6 = 1$

  *Quelle est la valeur de* $n^x mod \ n$ *?*

- On dit que deux nombres x et y sont « congrus modulo $n$ » si le reste de leur division par n est identique. En faisant appel à une des méthodes définies précédemment, écrire un algorithme (renvoyant un booléen) qui détermine si deux entiers sont congrus modulo $n$.
- Si $x \ mod \ y = 0$, on dit que « y divise x ». Écrire un algorithme qui détermine si un entier x divise un entier y.

# PGCD : définition

- Soit a et b deux entiers naturels non nuls. On appelle PGCD de $a$ et $b$ le plus grand diviseur de $a$ et $b$, et note $PGCD(a, b)$.
- Exemple
  - *Tous les diviseurs de 60 sont :*
    *1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60*
  - *Tous les diviseurs de 100 sont :*
    *1, 2, 4, 5, 10, 20, 25, 50, 100*
  - *Les diviseurs communs à 60 et 100 sont :*
    *1, 2, 4, 5, 10, 20*
  - *Le plus grand diviseur commun à 60 et 100 est 20. On le nomme le PGCD de 60 et 100.*

# PGCD : définition

- On peut étendre cette définition aux entiers relatifs.
- Dans le cas d'entiers négatifs, la recherche du PGCD se ramène au cas positif :
  - *Par exemple,* $PGCD(-60,100) = PGCD(60,100)$
- On a ainsi de façon générale : $PGCD(|a|,|b|) = PGCD(a,b)$.

# PGCD : propriétés

- Soit $a$ et $b$ deux entiers naturels non nuls
  1. $PGCD(a, 0) = a$
  2. $PGCD(a, 1) = 1$
  3. *Si $b$ divise $a$ alors $PGCD(a, b) = b$*
  - *Si $b$ divise $a$ alors tout diviseur de $b$ est un diviseur de $a$. Donc le plus grand diviseur de $b$ est un diviseur de $a$.*

# PGCD : Exercices

1. Calcul PGCD : méthode naïve
   a. *Écrire un algorithme* `diviseurs` *qui calcule tous les diviseurs d'un entier* $x$.
   b. *Algorithme calcul du PGCD de deux entiers* $x$ *et* $y$ *faisant appel à la méthode* `diviseurs`.
   c. *Combien de fois on entre dans la boucle de la méthode* `diviseurs` *?*
2. Amélioration de l'algorithme de calcul du PGCD sans utiliser la méthode `diviseurs`.

# PGCD : algorithme d'Euclide

Propriété :

- Soit $a$ et $b$ deux entiers naturels non nuls.
- Soit $r$ est le reste de la division euclidienne de $a$ par $b$.
- On a : $PGCD(a, b) = PGCD(b, r)$.

# PGCD : algorithme d'Euclide

Démonstration :

- On note respectivement $q$ et $r$ le quotient et le reste de la division euclidienne de $a$ par $b$.
- Si $D$ est un diviseur de $b$ et r alors $D$ divise $a = bq + r$ et donc $D$ est un diviseur de $a$ et $b$.
- Réciproquement, si $D$ est un diviseur de $a$ et $b$ alors $D$ divise $r = a - bq$ et donc $D$ est un diviseur de b et r.
- On en déduit que l'ensemble des diviseurs communs de $a$ et $b$ est égal à l'ensemble des diviseurs communs de $b$ et $r$ .
- Et donc en particulier, $PGCD(a, b) = PGCD(b, r)$.

# PGCD : algorithme d'Euclide

- Calcul du PGCD de deux entiers $x$ et $y$ par la méthode d'Euclide :
  - *On fait une division euclidienne de $x$ et $y$, qui donne un quotient $q$ et un reste $r$.*
  - *On recommence cette opération jusqu'à obtenir un reste nul (=0)*
  - *Le dernier reste non nul est le PGCD.*

- Déterminer (manuellement) le PGCD de 252 et 360.
- Écrire l'algorithme d'Euclide (version itérative et version récursive).

# Diviseurs communs

Propriété :

- Soit *a* et *b* deux entiers naturels non nuls.
- L'ensemble des diviseurs communs de *a* et *b* est l'ensemble des diviseurs de leur PGCD.

# Diviseurs communs

Démonstration :

- On a démontré précédemment que l'ensemble des diviseurs communs de *a* et *b* est égal à l'ensemble des diviseurs communs de *b* et *r.*
- En poursuivant par divisions euclidiennes successives, on obtient une liste strictement décroissante de restes $r, r_1, r_2, r_3, \ldots$

  En effet, on a successivement : $0 \leq r < b, 0 \leq r_1 < r, 0 \leq r_2 < r_1, 0 \leq r_3 < r_2, \ldots$
- Il n'existe qu'un nombre fini d'entiers compris entre 0 et *r*.

  Il existe donc un rang k tel que $r_k \neq 0$ et $r_{k+1} = 0$.
- Ainsi l'ensemble des diviseurs communs de *a* et *b* est égal à l'ensemble des diviseurs communs de $r_k$ et $0$.

# Diviseurs communs : exercices

- Chercher (manuellement) les diviseurs communs de 2730 et 5610 (ce qui revient à chercher les diviseurs de leur PGCD, que l'on calculera avec la méthode d'Euclide).
- Écrire un algorithme qui utilise les méthodes définies précédemment pour afficher les diviseurs communs de deux entiers.

# Nombres premiers

- Définition : nombre qui n'est divisible que par 1 et par lui-même
- Exemples et contre-exemples :
  - *2, 3, 5, 7 sont des nombres premiers*
  - *6 n'est pas un nombre premier car divisible par 2 et 3*
  - *1 n'est pas un nombre premier car il ne possède qu'un seul diviseur positif*
- Propriété : Tout entier naturel $n$ strictement supérieur à $1$ et non premier admet un diviseur premier $p$ tel que $p \leq n$.

# Nombres premiers

- Démonstration :
  - *Soit $E$ l'ensemble des diviseurs de $n$ autre que $1$ et $n$.*
  - *Cet ensemble est non vide car $n$ n'est pas premier donc $E$ admet un plus petit élément noté $p$.*
  - *$p$ est premier car dans le cas contraire, $p$ admettrait un diviseur autre que $1$ et $p$. Ce diviseur serait plus petit que $p$ et diviserait également $n$ ce qui contredit le fait que $p$ est le plus petit élément de $E$.*
  - *On peut écrire que $n = pq$ avec $p \leq q$ car $p$ est le plus petit élément de $E$.*
  - *Donc $pp \leq pq = n$ et donc $p \leq \sqrt{n}$.*
- Remarque : Pour savoir si un nombre $n$ est premier ou non, la recherche de diviseurs peut s'arrêter au dernier entier premier inférieur à $n$.

# Crible d'Ératosthène

- Algorithme permettant de trouver tous les nombres premiers inférieurs à un entier N
- Création d'une table contenant tous les entiers de 2 à N
- On procède par élimination :
  - *pour chaque entier x (avec $2 \leq x \leq N$) contenu dans la table, on supprime tous les entiers de la table qui sont des multiples de x*
- Condition d'arrêt : le carré du plus petit entier restant est supérieur au plus grand entier restant, car dans ce cas, tous les non-premiers ont déjà été rayés précédemment (voir démonstration précédente).
- Fin du parcours : tous les entiers qui n'ont pas été supprimés sont les nombres premiers inférieurs à N

# Crible d’Ératosthène

- Exemple : déroulement pour N = 25
- Déterminer si 391 est un nombre premier ?
  Pour le vérifier, on teste la divisibilité par tous les nombres premiers inférieurs à $\sqrt{391} \approx 19{,}8$, soit : 2, 3, 5, 7, 11, 13, 17 et 19.
- Exercice : écrire un algorithme qui reproduit le crible d’Ératosthène.

# Décomposition en produit de facteurs premiers

- Appelée aussi factorisation entière en nombres premiers
- Consiste à chercher à écrire un entier naturel on nul sous forme d'un produit de nombres premiers
  - Par exemple, $45$ peut être décomposé en un produit de facteur premiers : $3 \times 3 \times 5$
- Par définition, un nombre premier ne peut pas être décomposé en produit de plusieurs nombres premiers
- La factorisation est toujours unique

# Décomposition en produit de facteurs premiers

Propriété :

- Tout entier naturel $n$ strictement supérieur à 1 se décompose en produit de facteurs premiers.
  Cette décomposition est unique.
- On note $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$

  *avec $p_1$, $p_2$, ..., $p_r$ des nombres premiers distincts*

  *et $\alpha_1$, $\alpha_2$, ..., $\alpha_r$ des entiers naturels non nuls.*

# Décomposition en produit de facteurs premiers

Démonstration (existence) :

- Si $n$ est premier, l'existence est démontrée.
- Sinon, le plus petit diviseur $p_1$ de $n$ est premier et il existe un entier naturel $n_1$ tel que : $n = p_1\ n_1$.
- Si $n_1$ est premier, l'existence est démontrée.
- Sinon, le plus petit diviseur $p_2$ de $n_1$ est premier et il existe un entier naturel $n_2$ tel que : $n_1 = p_2\ n_2$.
- On réitère le processus pour obtenir une suite décroissante et finie d'entiers naturels.
- Ainsi, *n* se décompose en un produit de facteurs premiers du type : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$.

# Décomposition en produit de facteurs premiers : exercices

- Calculer manuellement la décomposition de 600 en produit de facteurs premiers.
- Écrire un algorithme qui décompose un entier en produit de facteurs premiers, et renvoie un tableau à deux dimensions, la première ligne contenant des nombres premiers, et la seconde le nombre de fois qu'ils doivent apparaître dans le produit (la puissance).