

Table des matières

Introduction	2
1 Logique	5
1.1 Logique assertionnelle ou propositionnelle	5
1.1.1 Généralités	5
1.1.2 But du calcul propositionnel	5
1.1.3 Syntaxe et évaluation des propositions	6
1.1.4 Propriétés	9
2 ARITHMÉTIQUE.	10
2.1 Divisibilité dans les entiers	10
2.2 Plus grand commun diviseur, Plus petit commun multiple	13
2.2.1 Définitions et propriétés	13
2.2.2 Résolution d'équations diophantiennes linéaires	14
2.3 Entiers relativement premiers	15
2.3.1 Définitions et propriétés	15
2.4 Les nombres premiers	16
2.4.1 Définitions	16
2.4.2 Propriétés	17
2.5 Quelques familles de nombres premiers	20
2.5.1 Les grands nombres premiers	20
2.5.2 Les premiers de Sophie Germain	21
2.5.3 Les factoriels et primoriels premiers	22
2.6 Production des nombres premiers	22
2.6.1 A partir les nombres de Fermat et/ou de Mersennes	23
2.6.2 Formules de nombres premiers	23
2.6.3 Nombres premiers dans une progressions Arithmetique	24
2.7 THÉORIE DES CONGRUENCES	24
2.7.1 La congruence modulo	24
2.7.2 Classes résidues et conséquences	26
2.8 LOI DE RÉCIPROCITÉ QUADRATIQUE	30
2.8.1 Généralité	30
2.8.2 Utilisation des symboles de Jacobi	31
2.8.3 Symbol de Legendre	31
2.8.4 Symbol de Jacobi	32
2.9 Numération	33
2.9.1 Bases de numération	33

2.9.2	Quelques systèmes de numération les plus usuels	34
2.9.3	Congruences particulières-Critères de divisibilité par 3, 4, 5, 9, 11 et 25	35

Introduction

La logique mathématique se fonde sur les premières tentatives de traitement formel des mathématiques, dues à Leibniz et Lambert (fin 16^{ème} siècle - début 17^{ème} siècle). Leibniz a en particulier introduit une grande partie de la notation mathématique moderne (usage des quantificateurs, symbole d'intégration, etc.). Toutefois on ne peut parler de logique mathématique qu'à partir du milieu du 19^{ème} siècle, avec les travaux de George Boole (et dans une moindre mesure ceux d'Auguste De Morgan) qui introduit un calcul de vérité où les combinaisons logiques comme la conjonction, la disjonction et l'implication, sont des opérations analogues à l'addition ou la multiplication des entiers, mais portant sur les valeurs de vérité faux et vrai (ou 0 et 1); ces opérations booléennes se définissent au moyen de tables de vérité. Le calcul de Boole véhiculait l'idée apparemment paradoxale, mais qui devait s'avérer spectaculaire fructueuse, que le langage logique pouvait se définir mathématiquement et devenir un objet d'étude pour les mathématiciens. Toutefois il ne permettait pas encore de résoudre les problèmes de fondements. Dès lors, nombre de mathématiciens ont cherché à l'étendre au cadre général du raisonnement mathématique et on a vu apparaître les systèmes logiques formalisés; l'un des premiers est dû à Frege au tournant du 20^{ème} siècle. En 1900 au cours d'une très célèbre conférence au congrès international des mathématiciens à Paris, David Hilbert a proposé une liste des 23 problèmes non résolus les plus importants des mathématiques d'alors. Le deuxième était celui de la cohérence de l'arithmétique, c'est-à-dire de démontrer par des moyens finitistes la non-contradiction des axiomes de l'arithmétique.

Le programme de Hilbert a suscité de nombreux travaux en logique dans le premier quart du siècle, notamment le développement de systèmes d'axiomes pour les mathématiques : les axiomes de Peano pour l'arithmétique, ceux de Zermelo complétés par Skolem et Fraenkel pour la théorie des ensembles et le développement par Whitehead et Russell d'un programme de formalisation des mathématiques. C'est également la période où apparaissent les principes fondateurs de la théorie des modèles : notion de modèle d'une théorie et théorème de Löwenheim-Skolem. En 1929 Kurt Gödel montre dans sa thèse de doctorat son théorème de complétude qui énonce le succès de l'entreprise de formalisation des mathématiques : tout raisonnement mathématique peut en principe être formalisé dans le calcul des prédicats. Ce théorème a été accueilli comme une avancée notable vers la résolution du programme de Hilbert, mais un an plus tard, Gödel démontrait le théorème d'incomplétude (publié en 1931) qui montrait irréfutablement l'impossibilité de réaliser ce programme. Ce résultat négatif n'a toutefois pas arrêté l'essor de la logique mathématique. Les années 1930 ont vu arriver une nouvelle génération de logiciens anglais et américains, notamment Alonzo Church, Alan Turing, Stephen Kleene, Haskell Curry et Emil Post, qui ont grandement contribué à la définition de la notion d'algorithme et au développement de la théorie de la complexité algorithmique (théorie de la calculabi-

lité, théorie de la complexité des algorithmes). La théorie de la démonstration de Hilbert a également continué à se développer avec les travaux de Gerhard Gentzen qui a produit la première démonstration de cohérence relative et a initié ainsi un programme de classification des théories axiomatiques. Le résultat le plus spectaculaire de l'après-guerre est dû à Paul Cohen qui démontre en utilisant la méthode du forcing, l'indépendance de l'hypothèse du continu en théorie des ensembles, résolvant ainsi le 1er problème de Hilbert. Mais la logique mathématique subit également une révolution due à l'apparition de l'informatique ; la découverte de la correspondance de Curry-Howard, qui relie les preuves formelles au lambda-calcul de Church et donne un contenu calculatoire aux démonstrations, va déclencher un vaste programme de recherche. La logique classique est la première formalisation du langage et du raisonnement mathématique développée à partir de la fin du 19^{ème} siècle en logique mathématique. Appelée simplement logique à ses débuts, c'est l'apparition d'autres systèmes logiques formels, notamment pour la logique intuitionniste, qui a suscité l'adjonction de l'adjectif classique au terme logique.

Il est important d'avoir un langage rigoureux. La langue française est souvent ambiguë. Prenons l'exemple de la conjonction «ou» ; au restaurant «fromage ou dessert» signifie l'un ou l'autre mais pas les deux. Par contre si dans un jeu de carte on cherche «les as ou les coeurs» alors il ne faut pas exclure l'as de coeur. Autre exemple : que répondre à la question «As-tu 15 000 francs en poche ?» si l'on dispose de 20 000 francs ?

✓ Il y a des notions difficiles à expliquer avec des mots : par exemple la continuité d'une fonction est souvent expliquée par «on trace le graphe sans lever le crayon». Il est clair que c'est une définition peu satisfaisante. Voici la définition mathématique de la continuité d'une fonction $f : I \longrightarrow \mathbb{R}$ en un point x_0 se traduit par :

$$\forall \varepsilon > 0, \exists \delta > 0, \forall x \in I, |x - x_0| < \delta \implies |f(x) - f(x_0)| < \varepsilon.$$

✓ Enfin les mathématiques tentent de distinguer le vrai du faux. Par exemple «Est-ce qu'une augmentation de vingt pour cent, puis de trente pour cent est plus intéressante qu'une augmentation de cinquante pour cent ?». Vous pouvez penser «oui» ou «non», mais pour en être sûr il faut suivre une démarche logique qui mène à la conclusion. Cette démarche doit être convaincante pour vous mais aussi pour les autres. On parle de raisonnement.

La logique classique est caractérisée par des postulats qui la fondent et la différencient de la logique intuitionniste, exprimés dans le formalisme du calcul des propositions ou du calcul des prédicats . La logique est utilisée en informatique pour modéliser de manière formelle des "objets" rencontrés par les informaticiens ; par exemple : Bases de données, Bases de connaissances, Pré-post conditions d'une procédure, . . . etc. l'informaticien doit être capable de se servir du modèle et raisonner sur celui-ci, comme la validation d'un modèle de données, prise de décision à partir des faits et d'une base de connaissances, preuve de correction d'une procédure/d'un programme. La logique est à la base de l'étude des raisonnements, c'est-à-dire des déductions que l'on peut faire sur les modèles formels. Le but de ce cours est d'étudier la base de logique mathématique (calcul propositionnel et calcul des prédicats) ainsi que les systèmes fondamentaux de numération afin de donner aux étudiants une base de notions qui le serviront en Informatique.

Chapitre 1

Logique

1.1 Logique assertionnelle ou propositionnelle

1.1.1 Généralités

Une assertion dans une théorie mathématique est une phrase à laquelle on peut attribuer une et une seule valeur de vérité, à savoir vrai (V ou 1 en abrégé) ou faux (F ou 0 en abrégé). En d'autres termes, une assertion est un énoncé (mathématique pour ce qui nous concerne dans ce cours) auquel on peut attribuer la valeur de vérité Vrai (V) ou Faux (F) mais jamais les deux à la fois (Principe du tiers exclu). Une assertion P vraie est appelée proposition. Selon l'importance que l'on donne à la proposition au sein de la théorie, celle-ci pourra aussi porter le nom de théorème, corollaire, lemme,... Un théorème est une proposition jugée importante dans le développement de la théorie. Un corollaire est une proposition qui est conséquence immédiate d'une proposition déjà démontrée. Un lemme est une proposition intermédiaire utilisée au cours de la démonstration d'une ou d'autres propositions. Les axiomes sont les phrases de la théorie que l'on admet au départ comme étant vraies. En fonction de leur importance, ils sont parfois considérés donc comme des théorèmes, avec la particularité qu'ils ne sont pas à être démontrés. En mathématiques et logique moderne, ils sont parfois confondus avec les postulats.

Ici, nous appellerons «Proposition» une assertion, donc un énoncé pouvant être vrai ou faux.

Exemple 1 1. «7 est un entier naturel premier» est une proposition.

2. «13» n'est pas une proposition.

3. « $\sqrt{2} \in \mathbb{Q}$ » est une proposition fausse.

4. «13 est un entier naturel premier» est une proposition vraie.

1.1.2 But du calcul propositionnel

Toute théorie mathématique \mathcal{T} débute par le choix de ses axiomes ou ses postulats. Ces propositions de base et leurs négations permettent de construire les autres assertions de \mathcal{T} . Notons \mathcal{P} la classe des propositions de la théorie \mathcal{T} . Cette dernière évolue au fur et à mesure de la découverte et de l'étude d'éléments de \mathcal{P} , et de l'obtention de leurs valeurs de vérité. En opérant sur les éléments de \mathcal{P} on obtient encore des éléments de \mathcal{P} , dont on

étudie les valeurs de vérité grâce à la définition des opérateurs de base et grâce à quelques règles de base dites règles logiques : c'est là la démarche du calcul propositionnel dont le but est d'étudier et de mettre en place ces règles logiques. Ce calcul étudie comment la fausseté ou la vérité d'une assertion complexe est fonction de la fausseté ou de la vérité des assertions élémentaires qui la composent. C'est donc un calcul bivalent n'admettant classiquement que deux valeurs de vérité possibles desquels il se préoccupe uniquement, sans s'intéresser du sens des propositions ou de leur contenu. Il est alors important de connaître la syntaxe à la base de ces propositions et comment ces dernières sont évaluées.

1.1.3 Syntaxe et évaluation des propositions

Syntaxe

Les propositions (parfois appelée expressions booléennes) sont construites avec :

- des *constantes booléennes* que sont Vrai et Faux,
 - de *variables booléennes* (qui peuvent prendre les valeurs Vrai ou Faux seulement),
- et
- des *opérateurs booléens* plus souvent appelés *connecteurs logiques*. Ils permettent de créer de nouvelles propositions à partir de la donnée d'une ou de plusieurs propositions.

Définition des opérateurs booléens

On distingue deux catégories d'opérateurs booléens à savoir les *opérateurs booléens unaires* et les *opérateurs booléens binaires*.

Définition 1.1.1 (*Opérateurs booléens unaires*) Ce sont les opérateurs booléens prenant un seul argument. Ils sont au nombre de quatre (04).

		<i>Id</i>	\neg	
<i>V</i>	<i>V</i>	<i>V</i>	<i>F</i>	<i>F</i>
<i>F</i>	<i>V</i>	<i>F</i>	<i>V</i>	<i>F</i>

La plus connue est la négation notée. Etant donnée une proposition p , on appelle négation de p notée $\neg p$ ou \bar{p} , la proposition qui est vraie lorsque p est fausse et fausse lorsque p est vraie.

Définition 1.1.2 (*Opérateurs booléens binaires*) Ce sont les opérateurs booléens prenant deux arguments. Ils sont au nombre de seize (16).

			\vee	\Leftarrow		\Rightarrow		\Leftrightarrow	\wedge	\bigwedge						∇	
<i>V</i>	<i>V</i>	<i>V</i>	<i>V</i>	<i>V</i>	<i>V</i>	<i>V</i>	<i>V</i>	<i>V</i>	<i>V</i>	<i>F</i>	<i>F</i>	<i>F</i>	<i>F</i>	<i>F</i>	<i>F</i>	<i>F</i>	<i>F</i>
<i>V</i>	<i>F</i>	<i>V</i>	<i>V</i>	<i>V</i>	<i>V</i>	<i>F</i>	<i>F</i>	<i>F</i>	<i>F</i>	<i>V</i>	<i>V</i>	<i>V</i>	<i>V</i>	<i>F</i>	<i>F</i>	<i>F</i>	<i>F</i>
<i>F</i>	<i>V</i>	<i>V</i>	<i>V</i>	<i>F</i>	<i>F</i>	<i>V</i>	<i>V</i>	<i>F</i>	<i>F</i>	<i>V</i>	<i>V</i>	<i>F</i>	<i>F</i>	<i>V</i>	<i>V</i>	<i>F</i>	<i>F</i>
<i>F</i>	<i>F</i>	<i>V</i>	<i>F</i>	<i>V</i>	<i>F</i>	<i>V</i>	<i>F</i>	<i>V</i>	<i>F</i>	<i>V</i>	<i>F</i>	<i>V</i>	<i>F</i>	<i>V</i>	<i>F</i>	<i>V</i>	<i>F</i>

Parmi les opérateurs booléens binaires les plus utilisés, on peut citer :

- $\checkmark \equiv, \Leftrightarrow =$: équivalence, égalité,
- $\checkmark \neq, \nabla =$: inéquivalence, inégalité,
- $\checkmark \neg$: négation, non,

-
- ✓ \vee : *dijonction, ou,*
 - ✓ \wedge : *conjonction, et,*
 - ✓ \Rightarrow : *implication, si... alors,*
 - ✓ \Leftarrow : *conséquence.*

Ordre de priorité

En tant qu'opérateurs, le tableau ci-après rend compte des règles de préséance entre ces connecteurs logiques : l'ordre étant décroissant de gauche à droite, ceux situés dans la même case ont la même priorité, de même qu'un opérateur et sa négation.

\neg	\wedge, \vee	\Rightarrow, \Leftarrow	\Leftrightarrow, \equiv
--------	----------------	---------------------------	---------------------------

(a) Équivalence-Équivalence logique

L'opérateur \equiv est à distinguer du connecteur logique \Leftrightarrow . Soient p et q deux propositions. Si

- p est vrai lorsque q est vrai, et p est faux lorsque q est faux, alors on dit que p et q sont logiquement équivalentes, et on note $p \equiv q$. Dans le cas contraire, on note $p \not\equiv q$. Par contre p et q étant des propositions, la notation $p \Leftrightarrow q$ désigne une proposition. La proposition $p \Leftrightarrow q$ (lire p équivalent à q) est : vraie lorsque p et q sont simultanément vraies ou simultanément fausses, et fausse dans tous les autres cas.

Table de vérité

p	q	$p \Leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Soient x et y deux réels. Les propositions suivantes sont vraies.

- $(x^2 \leq 9) \Leftrightarrow (x \in [-3; 3])$.
- $(x^2 = y^2) \Leftrightarrow (x = y \text{ ou } x = -y)$.
- $(x \leq y) \Leftrightarrow (x = y \text{ ou } x < y)$.
- $(x \leq 0) \Leftrightarrow (|x| = -x)$.
- $(x \geq 0) \Leftrightarrow (|x| = x)$.

(b) La disjonction \vee .

Étant données deux propositions p et q , la proposition « p ou q » notée $p \vee q$ est la proposition qui est vraie lorsque l'une au moins des propositions p et q est vraie et fausse lorsque les deux propositions sont simultanément fausses.

Table de vérité

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

(c) **Le ou exclusif \nleftrightarrow .**

Le ou exclusif (rendu par soit... soit... ; ou bien...) s'exprime par l'utilisation de l'inéquivalence \nleftrightarrow . Étant données deux propositions p et q , cet opérateur ne rend la valeur vrai que lorsqu'exactlyement l'une des deux propositions est vraie, et, elle est fausse dans les deux autres cas.

Table de vérité

p	q	$p \nleftrightarrow q$
V	V	F
V	F	V
F	V	V
F	F	F

(d) **La conjonction \wedge .**

Étant données deux propositions p et q , la proposition « p et q » notée $p \wedge q$ est la proposition qui n'est vraie que lorsque les propositions p et q sont simultanément vraies. Elle est donc fausse si et seulement l'une au moins des propositions p et q est fausse.

Table de vérité

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

(e) **L'implication \implies .**





Étant données deux propositions p et q , la proposition « p implique q » notée $p \implies q$ est la proposition qui n'est fausse que lorsque la proposition p est vraie et q ne l'est pas.

Table de vérité

p	q	$p \implies q$
V	V	V
V	F	F
F	V	V
F	F	V

Satisfiabilité et validité

Définition 1.1.3 Soit E une expression booléenne donnée. On dit que

-  E est satisfaite dans un état si elle a la valeur vrai dans cet état.
-  E est satisfiable s'il y a un état dans lequel elle est satisfaite.
-  E est valide si elle est satisfaite dans tous les états.
-  E est une tautologie lorsqu'elle est une expression booléenne valide.

Exemple 2 1. L'expression $2x - 5 > 0$ est satisfaite dans l'état $(x, 3)$. C'est donc une expression satisfiable. Mais elle n'est pas valide, car n'étant pas satisfaite dans l'état $(x, 0)$.

-
2. Considérons deux propositions p et q . L'expression $p \iff p$ est une tautologie.
Par contre les expressions $p \vee q$ et $p \wedge q$ sont satisfiables, mais non valides.

1.1.4 Propriétés

AXIOMES 1.1.1 $\models (p \iff p) \equiv \text{Vrai}$ (Réflexivité).

$\models (p \iff q) \equiv (q \iff p)$ (Symétrie).

$\models (p \iff (q \iff r)) \equiv ((p \iff q) \iff r)$ (Associativité). On écrit alors simplement $p \iff q \iff r$.

PROPRIÉTÉS 1.1.1

Chapitre 2

ARITHMÉTIQUE.

La théorie des nombres est l'étude (des propriétés) des nombres en occurrence les entiers.

Rappel

— L'ensemble des entiers est noté $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$;

— L'ensemble des entiers naturels est noté $\mathbb{N} = \{0, 1, 2, 3, \dots\}$

NB : \mathbb{Z} est aussi appelé "ensemble des entiers relatifs" et alors \mathbb{N} est "l'ensemble des entiers relatifs positifs".

2.1 Divisibilité dans les entiers

DÉFINITION 2.1.1

Soient a et $b \neq 0$ deux entiers.

On dit que a est un multiple de b ou que b est un diviseur (ou un facteur) de a s'il existe un entier k tel que $a = b \cdot k$.

— On note $b|a$ pour signifier que " $b \neq 0$ divise a ";

— L'ensemble des multiples d'un entier a est l'ensemble noté $|a|\mathbb{Z} = \{\dots, -3a, -2a, -a, 0, a, 2a, 3a, \dots\}$.

PROPRIÉTÉS 2.1.1

1. Tout entier non nul divise 0 (zéro).
2. 1 divise tout entier.
3. Tout entier non nul est divisible par lui-même.

Preuve.

1. Il suffit d'écrire $0 = a \times 0 \quad \forall a \in \mathbb{Z}^*$
2. Ici il suffit d'écrire $a = a \times 1 \quad \forall a \in \mathbb{Z}$
3. Il se déduit de 2.

■

PROPRIÉTÉS 2.1.2

Soient a, b, c et d des éléments de \mathbb{Z}^* (entiers non nuls).

1. Si $a|b$ et $b|c$ alors $a|c$ (transitivité).
2. Si $a|b$ alors $|a| \leq |b|$.
3. Si $a|b$ et $b|a$ alors $a = \pm b$ (antisymétrie).
4. Si $a|b$, $a|c$ alors $a|mb + nc$ pour tout $(m, n) \in \mathbb{Z}^2$.
5. Si $a|b$ et $c|d$ alors $ac|bd$

Preuve.

1. Supposons $a|b$ et $b|c$.
Alors il existe $(t, t') \in \mathbb{Z}^* \times \mathbb{Z}^*$ tels que $b = at$ et $c = bt'$. Ainsi, $c = (at)t' = a(tt')$.
D'où le résultat.
2. $a|b$ implique qu'il existe $t \in \mathbb{Z}^*$ tels que $b = at$ et $|b| = |a| \cdot |t|$. D'où le résultat.
3. D'après la transitivité, on a : $a = a(tt')$ pour un certain $(t, t') \in \mathbb{Z}^* \times \mathbb{Z}^*$. Donc $tt' = 1$ c'est-à-dire $t' = t^{-1} \in \{\pm 1\}$. D'où le résultat.
4. $a|b$ et $c|d$ alors il existe $(t, t') \in \mathbb{Z}^* \times \mathbb{Z}^*$ tels que $b = at$ et $d = ct'$. Donc $bd = (at)(ct') = ac(tt')$.

■

EXERCICE 1 Soient n et d deux entiers tels que d divise $5n + 4$ et $8n - 5$.

1. Justifier que d divise 53.
2. En déduire les valeurs possibles de d .

EXERCICE 2

On considère le nombre $A_n = n(n+1)(n+2)$, $n \in \mathbb{Z}$.

1. Justifier que $2|A_n$, pour tout $n \in \mathbb{Z}$.
2. Pour n pair, A_n est-il divisible par 8 ?

Théorème 2.1.1 (Algorithme de division)

Soient a et b deux entiers avec $b > 0$.

Il existe un unique couple d'entiers (q, r) tel que $a = b \cdot q + r$ avec $0 \leq r < b$

NB : On dit qu'on a effectué la division euclidienne de a par b .

- a est le dividende ;
- b le diviseur ;
- q le quotient ;
- r le reste

Preuve. Nous allons procéder en deux étapes.

1^{ère} étape : Supposons que $a \geq 0$.

$0 = 0 \cdot b + 0$. On peut alors considérer $a > 0$.

L'ensemble $b\mathbb{N}$ n'est pas majoré alors il existe $n \in \mathbb{N}$ tel que $a < bn$. $a > 0$ et \mathbb{N} est minoré alors $\mathcal{A} = \{n \in \mathbb{N}, bn > a\}$ n'est pas vide et possède un plus petit élément $k > 0$. On a $k-1 \in \mathbb{N}$ et $k-1 \notin \mathcal{A}$ ainsi $b(k-1) \leq a < bk$. On prend $q = k-1$ et $r = a - bq$.

Unicité :

Si $a = bq + r = bq' + r'$ avec $0 \leq r < b$ et $0 \leq r' < b$ alors $-b < r - r' < b$ et $r - r' = b(q' - q)$. Donc $r = r'$ car $r - r'$ est un multiple de b strictement contenu dans $] -b, b[$. Et puisque $b \neq 0$ on obtient $q = q'$.

2^{ème} étape : Supposons que $a < 0$.

On a $-a > 0$ et d'après ce qui précède, il existe un unique $(q, r) \in \mathbb{N}^2$ tel que $-a = bq + r$ avec $0 \leq r < b$. Ce qui implique que $a = b(-q) - r = b(-q - 1) + b - r$. On a $0 \leq b - r < b$ alors on prend le couple $(-q - 1, b - r)$ dont l'unicité vient de celui de (q, r) . ■

COROLLAIRE 2.1.1 (ALGORITHME DE DIVISION)

Soient a et b deux entiers avec $b \neq 0$.

Il existe un unique couple d'entiers (q, r) tel que $a = b \cdot q + r$ avec $0 \leq r < |b|$

EXERCICE 3

Compléter le tableau suivant.

Dividende	Diviseur	Quotient	Reste
25	7		
32	-3		
-48	9		
-38	-5		
15	21		
-8	10		

EXERCICE 4

Soit a un entier.

1. Quels sont les restes possibles dans la division euclidienne de a par 4.
2. Prouver que si a est impair alors 8 divise $a^2 - 1$.

DÉFINITION 2.1.2 (NOMBRES AMIABLES)

On dit que deux entiers sont amis (ou amiables) si la somme des diviseurs positifs autres que lui-même de chacun de ces deux nombres est égale à l'autre nombre.

EXEMPLE 2.1.1

Les nombres 220 et 284 sont amiables.

EXERCICE 5 Prouver que

- (a) 1 184 et 1 210 sont amiables.
- (b) 2 620 et 2 924 sont amiables.

DÉFINITION 2.1.3 (NOMBRES PARFAITS)

Un nombre parfait, est un entier naturel qui est égal à la somme de ses diviseurs stricts.

EXEMPLE 2.1.2

Les nombres 6 et 28 sont parfaits.

DÉFINITION 2.1.4 (NOMBRES TRIANGULAIRES)

Un nombre triangulaire, est un entier naturel de la forme $T_n = \frac{n(n+1)}{2}$ où $n > 0$ est un entier.

DÉFINITION 2.1.5 (NOMBRES DE THABIT)

Un nombre de Thabit, est un entier naturel de la forme $K_n = 3 \times 2^n - 1$ où $n > 0$ est un entier.

Remarque 2.1.1

Un nombre de Thabit en binaire se présente sous la forme : $10\underbrace{1 \cdots 1}_{n \text{ fois}}$.

Par exemple, $K_3 = 23_{10} = 10111_2$.

EXERCICE 6

1. Citer 4 nombres triangulaires plus grands que 6.
2. Justifier que les nombres 496 et 8128 sont parfaits.
3. Démontrer qu'un entier naturel pair est parfait si et seulement s'il est de la forme $2^{n-1}(2^n - 1)$, avec $n \in \mathbb{N}$, $2^n - 1$ premier.
4. Justifier que sont amiables.

2.2 Plus grand commun diviseur, Plus petit commun multiple

2.2.1 Définitions et propriétés

Théorème 2.2.1

Soient a et b deux entiers.

Il existe un unique entier positif μ vérifiant : $\forall n \in \mathbb{Z}, \quad a|n \text{ et } b|n \Leftrightarrow \mu|n$

Preuve. Soient a et b deux entiers. $a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal de \mathbb{Z} , donc principal. Ainsi il existe $\mu\mathbb{Z}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$. On prend $\mu \in \mathbb{N}$ car $\mu\mathbb{Z} = (-\mu)\mathbb{Z}$.

S'il existe $\mu' \in \mathbb{N}$ tel que $\mu'\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$ alors on a $\mu|\mu'$ et $\mu'|\mu$; donc $\mu = \pm\mu'$ d'après la proposition 2.1.2. On obtient donc $\mu = \mu'$ car ils sont tous positifs.

Soit $n \in \mathbb{Z}$.

$a|n \text{ et } b|n \Leftrightarrow n \in a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$. D'où $\mu|n$ ■

DÉFINITION 2.2.1

L'entier μ est le plus petit commun multiple positif de a et b . On le note $\text{ppcm}(a, b)$.

Théorème 2.2.2

Soient a et b deux entiers.

Il existe un unique entier positif δ qui satisfait à : $\forall d \in \mathbb{Z}, \quad d|a \text{ et } d|b \Leftrightarrow d|\delta$

Preuve. Soient a et b deux entiers. $a\mathbb{Z} + b\mathbb{Z}$ est un idéal de \mathbb{Z} alors il existe $\delta\mathbb{Z}$ tel que $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$. L'unicité de δ se montre de la même manière que celle de μ précédente.

Soit $d\mathbb{Z}^*$.

$$\begin{aligned} d|a \text{ et } d|b &\Leftrightarrow d|(au + bv), \forall (u, v) \in \mathbb{Z}^2 \quad (\text{d'après 2.1.2}). \\ &\Leftrightarrow a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z} \subset d\mathbb{Z} \\ &\Leftrightarrow d|\delta \end{aligned}$$

■

DÉFINITION 2.2.2

L'entier δ est le plus grand commun diviseur de a et b . On le note $\text{pgcd}(a, b)$ ou $a \wedge b$.

EXEMPLE 2.2.1

Soient $a \in \mathbb{Z}^*$.

$$\text{pgcd}(a, 0) = |a|, \text{pgcd}(a, 1) = 1, \text{ppcm}(a, 0) = 0, \text{ppcm}(a, 1) = |a|, \text{ppcm}(-3, 4) = 12$$

PROPRIÉTÉS 2.2.1

Soient a, b , et c des entiers.

1. $\text{ppcm}(ac, bc) = |c| \cdot \text{ppcm}(a, b)$.
2. $\text{pgcd}(ac, bc) = |c| \cdot \text{pgcd}(a, b)$.
3. $\text{ppcm}(a, b) \cdot \text{pgcd}(a, b) = |ab|$.

Proposition 2.2.1 (Algorithme d'Euclide)

Soient a et b deux entiers tels que $|a| > |b|$.

- Si $b = 0$ alors $\text{pgcd}(a, b) = \text{pgcd}(a, 0) = |a|$.
- Si $b \neq 0$ alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$, où r est le reste de la division euclidienne de a par b .

L'algorithme d'Euclide consiste à réitérer la deuxième formule jusqu'à ce que l'on tombe sur un reste nul puis on applique la première formule.

Remarque 2.2.1 (Principe)

Soient a et b deux entiers ($|b| < |a|$).

Si a n'est pas un multiple de b alors il existe un entier positif k et les entiers $q_1, \dots, q_k, r_1, \dots, r_k$ pour que :

$$\begin{array}{ll} a = q_1 \cdot b + r_1, & 0 < r_1 < |b| \\ b = q_2 \cdot r_1 + r_2, & 0 < r_2 < r_1 \\ r_1 = q_3 \cdot r_2 + r_3, & 0 < r_3 < r_2 \\ \vdots & \vdots \\ r_{k-3} = q_{k-1} \cdot r_{k-2} + r_{k-3}, & 0 < r_{k-3} < r_{k-2} \\ r_{k-2} = q_k \cdot r_{k-1}, & r_k = 0 \end{array}$$

EXERCICE 7

1. Détermine $\text{ppcm}(6, -15, 33)$, $\text{pgcd}(-6, -15)$ et $\text{pgcd}(6, -15, 35)$.
2. Applique l'Algorithme d'Euclide pour trouver le pgcd de 2772 et 390.

2.2.2 Résolution d'équations diophantiennes linéaires**DÉFINITION 2.2.3**

Une équation diophantienne linéaire est une équation polynomiale de degré 1 à coefficients entiers et dont les solutions sont entières. Elle est de la forme $a_1x_1 + a_2x_2 + \dots + a_nx_n = k$ avec $k \in \mathbb{Z}^*$ et les $a_i (1 \leq i \leq n)$ des entiers donnés.

EXEMPLE 2.2.2

$$3x + 2y = 3, 64x + 108y = 2$$

Théorème 2.2.3

Soient a, b des entiers non nuls.

-
1. Il existe d'entiers (x, y) solution de l'équation diophantienne $ax + by = \text{pgcd}(a, b)$.
 2. Soit $k \in \mathbb{Z}$. L'équation $ax + by = k$ est résoluble en entiers si et seulement si $\text{pgcd}(a, b)$ divise k .

Preuve.

■

EXEMPLE 2.2.3

Réolvons dans \mathbb{Z} , l'équation $803x + 154y = \text{pgcd}(803, 154)$

— Nous déterminons d'abord $\text{pgcd}(803, 154)$ par l'algorithme d'Euclide. On a :

$$803 = 5 \times 154 + 33$$

$$154 = 4 \times 33 + 22$$

$$33 = 1 \times 22 + 11$$

$$22 = 2 \times 11 + 0 \quad \text{donc } \text{pgcd}(803, 154) = 11$$

— L'équation devient

$$803x + 154y = 11.$$

En reprenant la technique inverse de l'algorithme d'Euclide, on a :

$$11 = 33 - 1 \times 22$$

$$= 33 - 1 \times (154 - 4 \times 33) = 5 \times 33 - 154$$

$$= -154 + 5 \times (803 - 5 \times 154) =$$

$$= 5 \times 803 - 26 \times 154$$

D'où $(x_0, y_0) = (5, -26)$ est solution. On déduit toutes les solutions à partir de cette solution.

EXERCICE 8

Réolvons les équations diophantiennes suivantes.

1. $64x + 108y = 4$

2. $64x + 108y = 1$

3. $52x + 18y = 24$

2.3 Entiers relativement premiers

2.3.1 Définitions et propriétés

DÉFINITION 2.3.1

Deux entiers a et b sont dit premiers entre eux (ou relativement premiers) si et seulement si $\text{pgcd}(a, b) = 1$

Remarque 2.3.1

$$\text{pgcd}(a, b) = 1 \quad \Leftrightarrow \quad a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$$

Théorème 2.3.1 (Bézout)

Pour tous entiers a et b , on a : $\text{pgcd}(a, b) = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2, au + bv = 1$

Preuve. On sait $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$ avec $\delta = \text{pgcd}(a, b)$

$$\begin{aligned}\text{pgcd}(a, b) = 1 &\Leftrightarrow a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z} \\ &\Leftrightarrow a\mathbb{Z} + b\mathbb{Z} = \langle 1 \rangle \\ &\Leftrightarrow \exists (u, v) \in \mathbb{Z}^2, au + bv = 1.\end{aligned}$$

■

Théorème 2.3.2 (Gauss)

$a|bc$ et $\text{pgcd}(a, b) = 1$ alors $a|c$

Preuve. $a|bc$ implique qu'il existe $t \in \mathbb{Z}$ tel que $bc = at$. Or $\text{pgcd}(a, b) = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2, au + bv = 1$.

$$\begin{aligned}au + bv = 1 &\Rightarrow tau + tbv = t \\ &\Rightarrow bcu + tbv = t \\ &\Rightarrow ab(cu + tv) = at = bc \\ &\Rightarrow a(cu + tv) = c \quad \text{car } \mathbb{Z} \text{ a la propriété de simplification}\end{aligned}$$

D'où le résultat. ■

Théorème 2.3.3

$(a|c \text{ et } b|c \text{ et } \text{pgcd}(a, b) = 1)$ alors $ab|c$

Preuve. $a|c$ et $b|c$ implique qu'ils existent t et t' tel que $c = at = bt'$ alors b divise at donc $b|t$ car $\text{pgcd}(a, b) = 1$ (d'après ce qui précède). Il existe alors $t_1 \in \mathbb{Z}$ tel que $t = bt_1$. Ainsi $c = abt_1$, d'où $ab|c$ ■

2.4 Les nombres premiers

2.4.1 Définitions

DÉFINITION 2.4.1

On dit qu'un entier $p > 1$ est premier s'il admet exactement deux diviseurs positifs distincts (1 et lui-même).

EXEMPLE 2.4.1

2, 3, 5, 7, 11, 13, 17, 19, ...

DÉFINITION 2.4.2

Un entier naturel qui n'est pas premier est dit composé.

DÉFINITION 2.4.3 (NOMBRES PREMIERS Jumeaux)

Deux nombres premiers p et q , ($p < q$), sont dits jumeaux si $q = p + 2$. On note (p, q) couple de nombres premiers jumeaux.

EXEMPLE 2.4.2

On a les premiers nombres premiers jumeaux suivants (3,5), (5,7), (11,13), (17,19), (29,31).

Remarque 2.4.1

Hormis la distance entre la paire de nombres premiers $\{2;3\}$, la distance $|p - q| = 2$ est la plus petite distance possible entre deux nombres premiers p et q .

DÉFINITION 2.4.4 (PREMIER CIRCULAIRE)

Un nombre premier circulaire est un nombre premier qui reste premier en permutant circulairement ses chiffres

EXEMPLE 2.4.3

Les nombres premiers suivants sont circulaires : 37, 131, 199.

DÉFINITION 2.4.5 (PREMIER PRESQUE CIRCULAIRE)

Un nombre premier presque circulaire est un nombre premier dont toutes les permutations sont des nombres premiers, sauf une.

EXERCICE 9

L'entier 1193 est-il un nombre premier circulaire ? un nombre premier presque circulaire ? Justifier votre réponse.

2.4.2 Propriétés

Théorème 2.4.1 (Euclide)

L'ensemble des entiers premiers est infini.

Preuve. Soit \mathcal{P} l'ensemble des nombres premiers. On a $\mathcal{P} \neq \emptyset$.

Supposons que \mathcal{P} est fini avec $\mathcal{P} = \{p_1, \dots, p_k\}$.

L'entier $a = 1 + \prod_{i=1}^k p_i$ est supérieur à 2, donc admet un diviseur premier $p_j \in \mathcal{P}$. Alors

p_j divise $1 = \left(a - \prod_{i=1}^k p_i\right)$ ce qui est impossible. D'où le résultat. ■

Théorème 2.4.2 (Euclide)

Tout entier n supérieur ou égal à 2 a au moins un diviseur premier.

Preuve. Pour tout entier $n \geq 2$ l'ensemble \mathcal{D}_n des diviseurs strictement positifs de n a au moins deux éléments, 1 et n ; donc $\mathcal{D}_n \setminus \{1\}$ est non vide dans $\mathbb{N} \setminus \{0,1\}$ et il admet un plus petit élément p qui est nécessairement premier. En effet si p n'est pas premier il admet un diviseur q tel que $2 < q < p$ avec q qui divise n , ce qui contredit le caractère minimal de p . ■

COROLLAIRE 2.4.1

Tout entier relatif $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ a au moins un diviseur premier.

Preuve. Tout diviseur premier de $|n| \geq 2$ convient. Un entier naturel non premier s'écrit donc $n = pq$ avec $p \geq 2$ premier q un entier relatif. ■

Remarque 2.4.2

Le Corollaire ci-dessus est aussi énoncé comme suit :

Tout entier composé admet au moins un facteur premier.

Un diviseur premier de $n \geq 2$, est nécessairement inférieur ou égal à n . En fait, pour n non premier, on peut toujours en trouver un qui est inférieur ou égal à \sqrt{n} , c'est $p = \min(\mathcal{D}_n \setminus \{1\})$.

PROPRIÉTÉ 2.4.1

Tout entier n supérieur ou égal à 2 qui est composé a au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$.

Preuve. En supposant n composé et en gardant les notations de la démonstration du théorème précédent, on a vu que $p = \min(\mathcal{D}_n \setminus \{1\})$ est un diviseur premier de n . On a donc $n = pq$ avec $2 \leq q \leq n$ (on a $q \neq 1$ puisque n n'est pas premier) et $q \in \mathcal{D}_n \setminus \{1\}$, ce qui implique que $p \leq q$ et $p^2 \leq pq = n$, soit $p \leq \sqrt{n}$. ■

EXERCICE 10

Prouver que le nombre \sqrt{p} est irrationnel pour tout entier premier p .

Proposition 2.4.1

Soit p un entier naturel premier. Pour tout entier naturel non nul n , on a soit p divise n , soit p premier avec n .

Preuve. Comme $\delta = \gcd(p, n)$ divise p , on a soit $\delta = p$ et p divise n , soit $\delta = 1$ et p est premier avec n . ■

Proposition 2.4.2

Deux nombres premiers distincts sont premiers entre eux.

Preuve. Facile ■

Proposition 2.4.3

Un entier $p \geq 2$ est premier si, et seulement si, il est premier avec tout entier compris entre 1 et $p - 1$.

Preuve. Si p est premier, comme il ne divise pas $k \in \{1, \dots, p - 1\}$, il est premier avec k . Réciproquement si p n'est pas premier, il s'écrit alors $p = ab$ avec $a \geq 2$, $b \geq 2$ et p n'est pas premier avec $a \in \{1, \dots, p - 1\}$. ■

Proposition 2.4.4

Tout couple de nombres premiers jumeaux, à l'exception du couple $(3, 5)$, est de la forme $(6n - 1, 6n + 1)$ pour un certain entier n .

Preuve. En effet, tout triplet d'entiers consécutifs comporte au moins un multiple de 2 (éventuellement deux) et un seul multiple de 3; l'entier qui se trouve entre les deux nombres premiers jumeaux est à la fois ce multiple de 2 et ce multiple de 3, car cela ne peut pas être l'un des nombres premiers. ■

EXERCICE 11

Trouver 7 couples de nombres premiers jumeaux.

Théorème 2.4.3 (fondamental de l'Arithmétique)

Tout entier $|a| \geq 2$ non premier peut s'écrire comme un produit de nombres premiers. Cette décomposition est unique à l'ordre des facteurs près.

C'est-à dire qu'il existe une collection unique de nombres premiers p_1, p_2, \dots, p_k et d'entiers positifs $\alpha_1, \alpha_2, \dots, \alpha_k$ tel que $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

Preuve. On démontre tout d'abord l'existence d'une telle décomposition par récurrence sur $a \geq 2$.

Pour $a = 2$, on a déjà la décomposition.

Supposons le résultat acquis pour tout entier k compris entre 2 et $a \geq 2$.

Si $a + 1$ est premier, on a déjà la décomposition, sinon on écrit $a + 1 = pq$ avec p et q compris entre 2 et a et il suffit d'utiliser l'hypothèse de récurrence pour p et q .

L'unicité d'une telle décomposition peut aussi se montrer par récurrence sur $a \geq 2$. Le résultat est évident pour $a = 2$.

Supposons le acquis pour tout entier k compris entre 2 et $a \geq 2$.

Si $a + 1$ a deux décompositions :

$$a + 1 = p_1^{\alpha_1} \times p_2^{\alpha_2} \dots p_r^{\alpha_r} = q_1^{\beta_1} \times q_2^{\beta_2} \dots q_s^{\beta_s}$$

où les p_i [resp. q_j] sont premiers deux à deux distincts et les α_i [resp. β_j] entiers naturels non nuls. L'entier p_1 est premier et divise le produit $q_1^{\beta_1} \times q_2^{\beta_2} \dots q_s^{\beta_s}$, il divise donc nécessairement l'un des q_k . L'entier q_k étant également premier la seule possibilité est $p_1 = q_k$. En simplifiant par p_1 on se ramène à la décomposition d'un entier inférieur ou égal à a et il suffit alors d'utiliser l'hypothèse de récurrence pour conclure. ■

EXERCICE 12

Montrer que si $n > 4$ est un entier composé alors n divise $(n - 1)!$.

PROPOSITIONS 2.4.1 (UTILITÉ DE DÉCOMPOSITION AU CALCUL DE PPCM, PGCD)

Soient a et b deux entiers composés dont les décompositions en facteurs premiers sont :

$$a = \pm \prod_{i=1}^k p_i^{\alpha_i} \text{ et } b = \pm \prod_{i=1}^k p_i^{\beta_i} \text{ où les } \alpha_i \text{ et } \beta_i \text{ sont des entiers naturels.}$$

$$\text{Alors } \text{ppcm}(a, b) = \prod_{i=1}^k p_i^{\max(\alpha_i, \beta_i)} \text{ et } \text{pgcd}(a, b) = \prod_{i=1}^k p_i^{\min(\alpha_i, \beta_i)}$$

EXEMPLE 2.4.4

1. $2016 = 2^5 \cdot 3^2 \cdot 7$, $2160 = 2^4 \cdot 3^3 \cdot 5$. On a :

$$\text{ppcm}(2160, 2016) = 2^5 \cdot 3^3 \cdot 5 \cdot 7 \text{ et } \text{pgcd}(2160, 2016) = 2^4 \cdot 3^2.$$

2. On utilise aussi la décompositions en facteurs premiers pour déterminer le nombres de diviseurs positifs d'un entier.

On peut déterminer celui de $308 = 2^2 \cdot 7 \cdot 11$ via un arbre de dénombrement.

COROLLAIRE 2.4.2

Si a est un entier composé de factorisation (ou décomposition) $a = \pm p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$ alors le nombre de ces diviseurs positifs est :

$$(s_1 + 1)(s_2 + 1) \dots (s_k + 1)$$

Théorème 2.4.4

Soit p un entier premier

1. $\forall a \in \mathbb{Z}, \text{pgcd}(a, p) = 1$ ou $\text{pgcd}(a, p) = p$.
2. $\forall (a, b) \in \mathbb{Z}^2$, si $p|ab$ alors $p|a$ ou $p|b$.
3. Soient p_1, p_2, \dots, p_k des entiers premiers.
Si $p|p_1 p_2 \dots p_k$ alors $\exists j \in \{1, 2, \dots, k\}$ tel que $p = p_j$.

EXERCICE 13

1. Déterminer le nombres de diviseurs positifs de chacun des nombres 2016, 105^6 et 1119.
2. Déterminer $\text{ppcm}(2016, 105^6)$ et $\text{pgcd}(4032, 2 \times 1119)$.

EXERCICE 14

Soit k, m et n des entiers tel que $\text{gcd}(m, n) = 1$.

On suppose qu'un nombre premier $p > 2$ divise $\text{gcd}(km^2 + 4, kn^2 - 4)$.

Justifier que p ne divise aucun des entier k, m et n .

2.5 Quelques familles de nombres premiers

2.5.1 Les grands nombres premiers

Les grands nombres premiers trouvés sont pour la plupart les nombres de Mersenne ou celui de Fermat.

DÉFINITION 2.5.1 (LES NOMBRES DE FERMAT)

Un nombre de Fermat est tout entier de la forme $F_n = 2^{2^n} + 1$ où n est un entier naturel.

EXEMPLE 2.5.1

$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537, F_7 = 2^{2^7} + 1, F_8 = 2^{2^8} + 1, \dots$

Remarque 2.5.1 (Euler)

Tous les nombres de Fermat ne sont pas premiers :

$$F_5 = 4294967297 = 641 \times 6700417,$$

$$F_6 = 18446744073709551617 = 274177 \times 67280421310721.$$

DÉFINITION 2.5.2 (LES NOMBRES DE MERSENNE)

Les nombres de Mersenne sont les entiers M_n de la forme $2^n - 1$.

EXEMPLE 2.5.2

$M_2 = 3, M_3 = 7, M_4 = 15, M_5 = 31, M_6 = 63, M_7 = 127, M_8 = 255, \dots$

Attention

Tous les nombres de Mersenne ne sont pas premiers : $M_8 = 3 \times 5 \times 17, M_{11} = 2047 = 23 \times 89, \dots$

EXEMPLE 2.5.3

Le plus grand nombre de Mersenne premier connu ce jour 07-Dec-2018 est $2^{82589933} - 1$, 24862048 chiffres. C'est le 51ème trouver jusque là. Pour plus d'information voir le site GIMPS (Great Internet Mersenne Prime Search) [5].

Les nombres de Fermat premiers record sont disponibles sur le site [6].

EXERCICE 15

1. Justifier qu'un entier x est un nombre de Fermat si et seulement si $\frac{\ln(\ln(x-1)) - \ln(\ln 2)}{\ln 2} \in \mathbb{N}$.
2. L'entier dont l'écriture hexadécimale est $\overline{8 \cdot 10^{15}}$ est-il un nombre de Fermat ?

EXERCICE 16

Soient $a \geq 2$, $m \geq 2$ deux entiers et $p = a^m - 1$.

1. Montrer que si p est premier alors $a = 2$ et m est premier.
2. La réciproque est-elle vraie ?

EXERCICE 17 (NOMBRES PARFAITS PAIRS)

Soit n un entier premier.

1. Justifier que si $2^n - 1$ est premier alors le nombre $2^{n-1}(2^n - 1)$ est un nombre parfait.
2. Donner alors cinq nombres parfaits.

2.5.2 Les premiers de Sophie Germain

DÉFINITION 2.5.3

Un nombre premier p est appelé nombre premier de Sophie Germain si $2p + 1$ est aussi un nombre premier. Dans ce cas, $2p + 1$ est appelé nombre premier sûr.

EXEMPLE 2.5.4

2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, ... sont des nombres premiers de Sophie Germain.

EXERCICE 18

Les nombres suivants : 59, 179, 491, 983, 1103, 1223, 1259, 1289, 1397. sont-ils

1. des premiers de Sophie Germain ? Justifier.
2. des premiers sûrs ? Justifier.

Remarque 2.5.2

Le premier de Sophie Germain record, en 2016, est $2618163402417 \times 2^{1290000} - 1$ [4], les deux nombres possèdent 388342

Il y a une **Conjecture** qui dit qu'il existe une infinité de nombres premiers de Sophie Germain

DÉFINITION 2.5.4 (CHAÎNE DE CUNNINGHAM)

Une suite $\{p, 2p + 1, 2(2p + 1) + 1, \dots\}$ de nombres premiers de Sophie Germain est appelée une chaîne de Cunningham de première espèce.

EXEMPLE 2.5.5

L'ensemble (ordonné) $\{2, 5, 11, 23, 47\}$ est une chaîne de Cunningham.

Remarque 2.5.3

Dans une chaîne de Cunningham, à l'exception du premier élément et du dernier élément, chaque élément est à la fois un nombre premier de Sophie Germain et un nombre premier sûr. Le premier élément dans la chaîne est un nombre premier de Sophie Germain et le dernier un nombre premier sûr.

EXERCICE 19

Donner deux chaînes de Cunningham.

2.5.3 Les factoriels et primoriels premiers

DÉFINITION 2.5.5 (FACTORIELLE PREMIÈRE)

Un nombre premier de la forme $n! + 1$ ou $n! - 1$ est appelé **factorielle première**.

EXEMPLE 2.5.6

1. L'entier $n! + 1$ est premier pour $n = 1, 2, 3, 11, 27, 37, 41, \dots$
2. L'entier $n! - 1$ est premier pour $n = 3, 4, 6, 7, 12, 14, 30, 32, \dots$

DÉFINITION 2.5.6

Soit p un nombre premier. Le **primoriel** p est l'entier défini par $p\# = 2 \times 3 \times 5 \times 7 \times \dots \times p$.

DÉFINITION 2.5.7 (PRIMORIELLE PREMIÈRE)

Une primorielle première est un nombre premier de la forme $p\# + 1$ ou $p\# - 1$.

EXEMPLE 2.5.7

1. L'entier $p\# + 1$ est premier pour $p = 2, 3, 5, 7, 11, 31, \dots$
2. L'entier $p\# - 1$ est premier pour $p = 3, 5, 11, 13, 41, \dots$

2.6 Production des nombres premiers

Une façon naïve de produire tous les nombres premiers plus petit qu'un entier N fixé à l'avance, consiste à mettre en oeuvre le crible d'Eratosthène : on écrit tous les entiers **inférieur ou égal à N puis on supprime tous les multiples de 2 qui sont supérieur à 2, puis les multiples de 3 qui sont supérieur à 3 ; et ainsi de suite**. À chaque étape, on sélectionne le premier nombre non barré strictement supérieur au nombre premier dont on vient de supprimer tous les multiples : celui-ci est un nombre premier. La liste obtenue est celle de tous les premiers inférieur ou égal à N .

Bien entendu l'algorithme proposé n'est pas efficace, on en cherche d'autres. En outre on peut aussi s'intéresser aux problématiques suivantes :

- comment produire de nombreux nombres premiers ?
- comment battre le record du monde du plus grand nombre premier ?

2.6.1 A partir les nombres de Fermat et/ou de Mersennes

PROPRIÉTÉ 2.6.1

Soit $n \in \mathbb{N}^*$. Le nombre de Fermat f_n est premier si et seulement si F_n divise $1 + 3^{\frac{F_n-1}{2}}$.

La preuve utilise des notions qui ne sont pas encore vu.

PROPRIÉTÉ 2.6.2

Soit $n \geq 2$ un entier. Si le nombre de Mersenne $M_n = 2^n - 1$ est premier alors n est un nombre premier.

Preuve. Elle repose sur l'identité $x^{pq} - 1 = (x^q - 1)(x^{q(p-1)} + \dots + x^q + 1)$ ■

La réciproque de cette proposition est fausse comme le montre $2^{11} - 1 = 23 \times 89$.

2.6.2 Formules de nombres premiers

Les formules existantes pour la génération de nombres premiers utilisent la **fonction partie entière** notée ici par $\lfloor \bullet \rfloor$. Elle est donnée par : $\forall x \in \mathbb{R}$,

$$\lfloor x \rfloor = \{n \in \mathbb{Z}; n \leq x < n+1\}.$$

Théorème 2.6.1 (Roland Yéléhada et Minac)

Pour tout $n \in \mathbb{N}$,

$$t(n) = 2 + n \left\lfloor \frac{(n+1)! + 1}{n+2} - \left\lfloor \frac{(n+1)!}{n+2} \right\rfloor \right\rfloor$$

donne toujours un nombre premier.

Plus précisément, si on enlève le nombre 2 dans la suite $(t(n))_{n \in \mathbb{N}}$, on obtient la liste des nombres premiers dans l'ordre croissant.

Théorème 2.6.2 (Minac et Willans en 1995)

Soit $m \geq 2$ un entier. On pose $\pi(1) = 0$

$$\pi(m) = \sum_{j=2}^m \left\lfloor \frac{(j-1)! + 1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor$$

alors le n -ème nombre premier p_n est donné par

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \left[\frac{n}{1 + \pi(m)} \right]^{1/n} \right\rfloor.$$

Il existent d'autres formules telles que celle de **Ruiz, (en 2000)** et la tentative par une suite récurrente de **Rowland, (en 2008)**. Mais comme on peut le constater avec celles données ci-dessus ces formules sont aussi lourde pour manipulation.

2.6.3 Nombres premiers dans une progressions Arithmetique

Théorème 2.6.3 (Dirichlet, 1842)

Soit k et l deux entiers strictement positifs premiers entre eux. La suite $(l + nk)_{n \geq 1}$ contient une infinité de nombres premiers

EXEMPLE 2.6.1

Considerons la suite $(u_n)_{n \geq 1}$ où $u_n = 3n + 1$.

Les nombres premiers 7, 13, 19, 31, \dots sont des éléments de cette suite.

Théorème 2.6.4 (Dirichlet en 1842)

Soit $\pi(x, k, l)$ le cardinal de l'ensemble

$$\{p, \text{premier} / p \leq x \text{ et } p \equiv l \pmod{k}\}.$$

Alors pour x assez grand on a

$$\pi(x, k, l) \sim \frac{x}{\phi(k) \log x}.$$

Recherches

1. Trouver s'ils existent d'autres types de nombres premiers (avec propriétés particulières). Par exemple **les nombres premiers de Woodall** ?
2. La suite $(n^2 + 1)_{n \geq 1}$ contient-elle une infinité de nombres premiers ?
3. Nombres économes, équidistants et prodiges.

Ecrivez des programme non coûteux en temps (consistant) pour générer ces types de nombres !!!

2.7 THÉORIE DES CONGRUENCES

Etant donné un entier $n \geq 2$, l'arithmétique modulo n consiste à faire des calculs sur les restes dans la division euclidienne des entiers par n .

2.7.1 La congruence modulo

DÉFINITION 2.7.1

Soient a, b des entiers et n un entier naturel non nul.

Si n divise $a - b$, on dit que a est congru à b modulo n et on écrit $a \equiv b \pmod{n}$.

Dans le cas contraire, on dit que a est non congru à b modulo n et on écrit $a \not\equiv b \pmod{n}$

EXEMPLE 2.7.1

$$100 \equiv 9 \pmod{13}, 2022 \equiv 2 \pmod{10}, 3341 \equiv 2 \pmod{7}.$$

EXEMPLE 2.7.2 (UNE UTILITÉ)

1. Je me couche à 22h00 et je dors pendant 07h. Quelle heure sera-t-il au réveil ?
2. Aujourd'hui on est mardi (2ème jour de la semaine). Quel jour sera-t-on dans 65 jours ?

PROPRIÉTÉS 2.7.1 (Relation d'équivalence)

Soient a, b et c des entiers et n un entier naturel non nul.

1. $a \equiv a \pmod{n}$. On dit que la relation de congruence modulo n est réflexive.
2. Si $a \equiv b \pmod{n}$, alors $b \equiv a \pmod{n}$. On dit que la relation de congruence modulo n est symétrique.
3. Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $a \equiv c \pmod{n}$. On dit que la relation de congruence modulo n est transitive.

On résume la propriété précédente en disant que la relation de congruence modulo n dans \mathbb{Z} est une relation d'équivalence. De façon générale une relation d'équivalence sur un ensemble non vide E est une relation binaire sur E qui est à la fois réflexive, symétrique et transitive :

- (a) $\forall a \in E, a\mathcal{R}a$ (réflexivité).
- (b) $\forall (a, b) \in E^2, a\mathcal{R}b \implies b\mathcal{R}a$ (symétrie).
- (c) $\forall (a, b, c) \in E^3, (a\mathcal{R}b) \wedge (b\mathcal{R}c) \implies a\mathcal{R}c$ (transitivité).

PROPRIÉTÉS 2.7.2 (Compatibilité avec l'addition et la multiplication dans \mathbb{Z})

Soient a, b, c, d des entiers et n un entier naturel non nul.

1. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors $a + c \equiv b + d \pmod{n}$. On dit que la relation de congruence modulo n est compatible avec l'addition dans \mathbb{Z} .
2. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors $ac \equiv bd \pmod{n}$. On dit que la relation de congruence modulo n est compatible avec la multiplication dans \mathbb{Z} .

Remarque 2.7.1 Pour tous entiers a et b et pour tous entiers naturels non nuls n et k , on a :

$$(a \equiv b \pmod{n}) \implies (a^k \equiv b^k \pmod{n}).$$

PROPRIÉTÉS 2.7.3

Soient a, b, c, d des entiers et n un entier naturel non nul.

1. Si $a \equiv b \pmod{n}$ et d divise n , $d > 0$, alors $a \equiv b \pmod{d}$
2. Si $a \equiv b \pmod{n}$ alors $ac \equiv bc \pmod{nc}$ pour tout entier $c > 0$.
3. Soit f est une fonction polynomiale à coefficients entiers.
Si $a \equiv b \pmod{n}$ alors $f(a) \equiv f(b) \pmod{n}$
4. Si (n_1, n_2, \dots, n_k) est une famille d'entiers naturels non nuls et $a \equiv b \pmod{n_i}$ pour tout $i \in \{1, 2, \dots, k\}$, alors $a \equiv b \pmod{\text{ppcm}(n_1, n_2, \dots, n_k)}$
5. Si $a \equiv b \pmod{n}$, alors $\text{pgcd}(a, n) = \text{pgcd}(b, n)$.

Théorème 2.7.1 (Loi d'annulation)

1. $ax \equiv ay \pmod{m} \Leftrightarrow x \equiv y \pmod{\frac{m}{\text{pgcd}(a, m)}}$
2. Si $ax \equiv ay \pmod{m}$ et $\text{pgcd}(a, m) = 1 \Rightarrow x \equiv y \pmod{m}$

EXERCICE 20

1. Déterminer le dernier chiffre (chiffre des unités) du nombre 7^{20} .

2. Montrer que $2^{20} \equiv 1 \pmod{41}$

3. D  duire que 41 divise $\sum_{k=0}^{19} 2^k$.

EXERCICE 21

Le R.I.B. (Relev   d'Identit   Bancaire) est un nombre constitu   de gauche    droite de la fa  on suivante :

$\underbrace{\hspace{2cm}}_{\text{5 chiffres}} \underbrace{\hspace{2cm}}_{\text{5 chiffres}} \underbrace{\hspace{2cm}}_{\text{11 chiffres}} \underbrace{\hspace{1cm}}_{\text{2 chiffres}}$
Code de la banque Code du guichet Num  ro de compte cl  

Pour calculer la cl   de contr  le d'un RIB, on consid  re le nombre a form   par les 21 premiers chiffres ; on calcule le reste r de la division euclidienne de $N = 100 \times a$ par 97 ; la cl   R.I.B est $97 - r$.

Soit le RIB (incomplet)

Code de la banque	Code du guichet	Num��ro de compte	cl��
12345	25896	35715942681	?

1. Soit $n \in \{2, \dots, 19\}$. Donner dans un tableau les restes des divisions euclidiennes de 10^n par 97.
2. Calculer la cl   de contr  le d'un RIB.

2.7.2 Classes r  sidues et cons  quences

D  FINITION 2.7.2

Soient $m \geq 2$, a, b des entiers.

1. Si $a \equiv b \pmod{m}$, alors b est appel   un r  sidu de $a \pmod{m}$.
2. La classe de congruence (ou classe de r  sidus) de $a \pmod{m}$ est l'ensemble $\{a + km, k \in \mathbb{Z}\}$
3. Un syst  me complet de r  sidus de $a \pmod{m}$ est un ensemble d'entiers contenant un   l  ment de chaque classe.
4. Un syst  me modulaire de r  duction \pmod{m} est un ensemble d'entiers r_i avec $\text{pgcd}(r_i, m) = 1$ o   pour tout a relativement premier avec m , il existe r_i tel que $a \equiv r_i \pmod{m}$.

D  FINITION 2.7.3 (FONCTION ARITHM  TIQUE MULTIPLICATIVE)

1. Une fonction Arithm  tique est toute application de $\mathbb{N} \setminus \{0\}$ dans \mathbb{C} .
2. Une fonction Arithm  tique g est dite multiplicative si $g(1) \neq 0$ et $g(pq) = g(p)g(q)$ pour tout entiers (strictement) positifs p et q premiers entre eux. Elle est dite compl  tement multiplicative si $g(pq) = g(p)g(q)$ pour tout entiers (strictement) positifs p et q .

EXERCICE 22

1. Soit g une fonction Arithm  tique. Justifier que si g est multiplicative alors $g(1) = 1$.
2. Soit $a \in \mathbb{R}$. Justifier que N_a donn   par $N_a(n) = n^a$ pour tout $n \in \mathbb{N} \setminus \{0\}$, est une fonction Arithm  tique multiplicative.

DÉFINITION 2.7.4 (FONCTION D'EULER)

La fonction $\varphi: \mathbb{N} \rightarrow \mathbb{N}; m \mapsto \text{card}\{a \in \mathbb{N}^*, a < m \text{ et } \text{pgcd}(a, m) = 1\}$ est appelée fonction d'Euler.

EXEMPLE 2.7.3 $\varphi(12) =$

Remarque 2.7.2

- La fonction d'Euler est multiplicative.
- Le système modulaire de réduction $(\text{mod } m)$ est un groupe multiplicatif contenant $\varphi(m)$ éléments.

PROPRIÉTÉ 2.7.1

Soient n un entier naturel non nul et p un entier premier. On a :

$$\varphi(p^n) = p^n - p^{n-1}$$

.

Preuve. Par récurrence sur n . ■

COROLLAIRE 2.7.1 Soit $m \in \mathbb{N}^*$. Si la décomposition en produit de facteurs premiers est $m = \prod_{p|m} p^\alpha$, alors $\varphi(m) = \prod_{p|m} (p^\alpha - p^{\alpha-1}) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$.

Théorème 2.7.2 (Euler)

Soient a et m des entiers avec $m > 0$.

Si $\text{pgcd}(a, m) = 1$ alors $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Preuve. $\text{pgcd}(a, m) = 1$ alors la classe \bar{a} , résidu de $a \pmod{m}$ est un élément du système modulaire de réduction $(\text{mod } m)$. Ainsi il est inversible (car le système modulaire de réduction $(\text{mod } m)$ est un groupe multiplicatif). Par ailleurs l'ordre de \bar{a} divise l'ordre du système modulaire de réduction $(\text{mod } m)$ qui est $\varphi(m)$. Donc $(\bar{a})^{\varphi(m)} = \bar{1} = \overline{a^{\varphi(m)}}$. D'où $a^{\varphi(m)} \equiv 1 \pmod{m}$. ■

On déduit le résultat suivant qu'on appelle " le petit théorème de Fermat".

Théorème 2.7.3 (Fermat)

Soient p un entier premier et a entier. On a : $a^p \equiv a \pmod{p}$

De plus Si p ne divise pas a (c-à-d $\text{pgcd}(a, p) = 1$), alors $a^{p-1} \equiv 1 \pmod{p}$.

Preuve. p étant premier et ne divise pas a alors $\text{pgcd}(a, p) = 1$ et $\varphi(p) = p - 1$. Le Théorème d'Euler implique donc $a^{p-1} \equiv 1 \pmod{p}$

En multipliant cette congruence par a , on obtient $a^p \equiv a \pmod{p}$. ■

Proposition 2.7.1

Soient a et b des entiers et p un entier premier. On a : $a^2 \equiv b^2 \pmod{p} \Rightarrow a \equiv \pm b \pmod{p}$

Preuve. $a^2 \equiv b^2 \pmod{p} \Rightarrow a^2 - b^2 = (a - b)(a + b) \equiv 0 \pmod{p}$ ■

Un retour sur la Production des nombres premiers

Théorème 2.7.4 (Wilson)

Un entier $p \geq 2$ est premier si et seulement si $(p-1)! \equiv -1 \pmod{p}$

PROPOSITIONS 2.7.1 (AUTRES)

1. $x^2 \equiv 1 \pmod{p} \Leftrightarrow x \equiv \pm 1 \pmod{p}$
2. $x^2 \equiv -1 \pmod{p}$ admet de solutions si et seulement si $p = 2$ ou $p \equiv 1 \pmod{4}$

EXERCICE 23 1. Déterminer les systèmes modulaires de réduction $\pmod{11}$ et $\pmod{14}$.

2. Calculer $\varphi(27)$, $\varphi(31)$, $\varphi(483)$, $\varphi(5096)$.

Résultat. 23

□

Théorème 2.7.5 (des restes chinois)

Soient m, n des entiers naturels et a, b entiers. Le système de congruences

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

est résoluble si et seulement si $a \equiv b \pmod{\text{pgcd}(m, n)}$. Dans le cas où une solution x_0 existe, x est aussi solution si et seulement si $x \equiv x_0 \pmod{\text{ppcm}(m, n)}$.

Preuve. Supposons que le système admet de solutions. Alors il existent t, t' entiers tel que $x = a + tm = b + t'n$. Donc $a - b = t'n - tm \equiv 0 \pmod{\text{pgcd}(m, n)}$.

Réciproquement si $a \equiv b \pmod{\text{pgcd}(m, n)}$, alors $a - b \equiv 0 \pmod{\text{pgcd}(m, n)}$ et d'après Bézout, il existent t, t' entiers tel que $a - b = tm + t'n$ ce qui implique que $a + (-t)m = b + t'n$. D'où le système admet de solutions.

Soit x_0 une autre solution, on :

$$\begin{cases} x_0 \equiv a \equiv x \pmod{m} \\ x_0 \equiv b \equiv x \pmod{n} \end{cases} \Rightarrow \begin{cases} x_0 - x \equiv 0 \pmod{m} \\ x_0 - x \equiv 0 \pmod{n} \end{cases}$$

Donc $x_0 - x \equiv 0 \pmod{\text{ppcm}(m, n)}$

Réciproquement, $x_0 - x \equiv 0 \pmod{\text{ppcm}(m, n)}$ implique que $x_0 - x \equiv 0 \pmod{m}$ et $x_0 - x \equiv 0 \pmod{n}$. D'où le résultat. ■

Théorème 2.7.6 (généralisé)

Soit m_1, \dots, m_k une suite d'entiers positifs premiers entre eux deux à deux. Alors le système de congruences :

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

a une solution unique $x \pmod{M = m_1 \cdot m_2 \cdot \dots \cdot m_k}$

$$x = a_1 M_1 y_1 + \dots + a_k M_k y_k$$

avec $M_i = M/m_i$ et $y_i M_i \equiv 1 \pmod{m_i}$

EXEMPLE 2.7.4

Réolvons

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

Posons $M = 3 \times 5 \times 7 = 105$, $M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$, $M_3 = \frac{105}{7} = 15$

$$\begin{cases} y_1 \times 35 \equiv 1 \pmod{3} \\ y_2 \times 21 \equiv 1 \pmod{5} \\ y_3 \times 15 \equiv 1 \pmod{7} \end{cases} \quad \text{on prend} \quad \begin{cases} y_1 = 2 \\ y_2 = 1 \\ y_3 = 1 \end{cases}$$

$$x = (1 \times 35 \times 2) + (2 \times 21 \times 1) + (3 \times 15 \times 1) = 157 \equiv 52 \pmod{105}$$

EXEMPLE 2.7.5

Lorsque les m_i ne sont pas premiers entres eux deux à deux.

$$\begin{cases} x \equiv 1 \pmod{6} \\ x \equiv 4 \pmod{15} \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \end{cases}$$

$$x \equiv 4 \pmod{15} \Leftrightarrow \begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \end{cases}$$

EXERCICE 24

Dans l'armée de Han Xing il y a entre 1000 et 1100 soldats. Combien cette armée comporte-t-elle de soldats si, rangés par 3 colonnes, il reste 2 soldats, rangés par 5 colonnes, il reste 3 soldats et, rangés par 7 colonnes, il reste 2 soldats ?

Théorème 2.7.7

Soient a, b des entiers et m un entier naturel.

L'équation $ax \equiv b \pmod{m}$ admet de solution si et seulement si $\text{pgcd}(a, m)$ divise b . Si $\text{pgcd}(a, m)$ divise b l'équation admet exactement d solutions.

Preuve. Posons $\text{pgcd}(a, m) = d$

$ax \equiv b \pmod{m}$ équivaut à qu'il existe $t \in \mathbb{Z}$ tel que $b = ax - tm$. Ce qui admet de solution si et seulement si $\text{pgcd}(a, m)$ divise b .

Soient x_1, x solutions de $ax \equiv b \pmod{m}$. Alors il existe $t \in \mathbb{Z}$ tel que $a(x - x_1) = mt$. Donc $\frac{a}{d}(x - x_1) = \frac{m}{d}t$ et comme $\text{pgcd}(\frac{a}{d}, \frac{m}{d}) = 1$ alors $\frac{m}{d}$ divise $x - x_1$. D'où $x_1 = x + k\frac{m}{d}$ pour un certain $k \in \mathbb{Z}$.

Maintenant il faut remarquer que les d entiers de la forme $x_i = x + i\frac{m}{d}$, $0 \leq i \leq d - 1$ sont tous solutions et deux à deux incongrus modulo m . D'où le résultat. ■

COROLLAIRE 2.7.2

Soient a, b des entiers et m un entier naturel.

Si $\text{pgcd}(a, m) = 1$ alors l'équation $ax \equiv b \pmod{m}$ admet une seule solution \pmod{m} .

Remarque 2.7.3

Soient a, b, c des entiers et m un entier naturel.

L'équation $ax + by \equiv c \pmod{m}$ admet de solution si et seulement si $\text{pgcd}(a, b, m)$ divise c .

Théorème 2.7.8

Soient a, b, c, d, r, s des entiers et m un entier naturel. Le système

$$\begin{cases} ax + by \equiv r \pmod{m} \\ cx + dy \equiv s \pmod{m} \end{cases}$$

admet une unique solution \pmod{m} lorsque $\text{pgcd}(ad - bc, m) = 1$

EXERCICE 25

1. Déterminer le reste dans la division euclidienne de 5^{2022} par 11.
2. Justifie que le produit de trois entiers consécutifs est divisible par 3.
3. Soit $n \geq 2$ un entier. Montrer que $n^5 - n$ est divisible par 30.

EXERCICE 26

1. Résoudre $20x \equiv 4 \pmod{30}$.
2. Montrer que si $\text{pgcd}(a, 42) = 1$ alors 168 divise $a^6 - 1$.
3. Prouver que $a^7 \equiv a \pmod{42}$, $\forall a \in \mathbb{Z}$ (utiliser le petit Théorème de Fermat).
4. Prouver $\Phi(3n) = 3\Phi(n)$ si et seulement si 3 divise n .

2.8 LOI DE RÉCIPROCITÉ QUADRATIQUE

2.8.1 Généralité

Soit p un nombre premier impair.

La question qui prévaut ici est comment résoudre l'équation

$$ax^2 + bx + c \equiv 0 \pmod{p} \tag{2.1}$$

où p est un entier premier impair et $a \not\equiv 0 \pmod{p}$ (c'est-à-dire $a \wedge p = 1$).

Définition 2.8.1 Soit p un entier naturel premier impair et soit a un entier tel que p ne divise pas a .

On dit que a est un résidu quadratique modulo p ou un carré modulo p lorsque l'équation $x^2 \equiv a \pmod{p}$ admet de solutions dans \mathbb{Z} .

Dans le cas contraire, on dira que a est non-résidu quadratique modulo p .

EXEMPLE 2.8.1 $13 \nmid 3$ et on a $3 \equiv 4^2 \pmod{13}$. Donc 3 est un résidu quadratique modulo 13.

Remarque 2.8.1

Si $a \equiv b \pmod{p}$, alors a est résidu quadratique de p si et seulement si b est résidu quadratique de p .

Théorème 2.8.1 (Critère d'Euler)

Un entier a tel que $\text{pgcd}(a, p) = 1$ est résidu quadratique de p si et seulement si $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

COROLLAIRE 2.8.1

Un entier a tel que $\text{pgcd}(a, p) = 1$ est résidu non quadratique de p si $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Théorème 2.8.2 (Loi de réciprocité quadratique)

Soient p et q deux entiers naturels premiers impairs distincts. Alors, on a : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Exemple 3 On a $\left(\frac{15508}{47}\right) = \left(\frac{45}{47}\right)$ car $15508 \equiv 45 \pmod{47}$. Donc

$$\left(\frac{15508}{47}\right) = \left(\frac{3^2 \times 5}{47}\right) = \left(\frac{3}{47}\right)^2 \left(\frac{5}{47}\right)$$

$\left(\frac{3}{47}\right)^2 = 1$ et d'après la loi de réciprocité quadratique, on a :

$$\left(\frac{5}{47}\right) = (-1)^{\frac{5-1}{2}\frac{47-1}{2}} \left(\frac{47}{5}\right) = \left(\frac{47}{5}\right).$$

$$\left(\frac{47}{5}\right) = \left(\frac{2}{5}\right) \text{ car } 47 \equiv 2 \pmod{5}$$

5 ne divise pas 2 et c'est un non résidu quadratique modulo 5, donc $\left(\frac{2}{5}\right) = -1$. Ainsi $\left(\frac{15508}{47}\right) = -1$

Corollaire 2.8.1 Soient p et q deux entiers naturels premiers impairs distincts.

1. Si l'un au moins des nombres premiers p et q est congru à 1 modulo 4, alors p est un résidu quadratique modulo q si et seulement si q en est un modulo p .
2. Si p et q sont tous deux congrus à 3 modulo 4, alors p est un résidu quadratique modulo q si et seulement si q est non résidu quadratique modulo p .

2.8.2 Utilisation des symboles de Jacobi**2.8.3 Symbol de Legendre****DÉFINITION 2.8.1 (SYMBOL DE LEGENDRE)**

Soient a un entier et $p \neq 2$ premier. Le symbol de Legendre est défini par :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est résidu quadratique de } p \\ 0 & \text{si } p \text{ divise } a \\ -1 & \text{si } a \text{ est résidu non quadratique de } p \end{cases}$$

PROPRIÉTÉS 2.8.1

Soient $p \neq 2$ premier et a, b des entiers relativement premiers avec p .

1. Si $a \equiv b \pmod{p}$, alors $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $\left(\frac{a^2}{p}\right) = 1$
3. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

5. $\left(\frac{1}{p}\right) = 1$ et $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. On déduit que

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{4} \\ -1 & \text{si } p \equiv 3 \pmod{4} \end{cases}$$

$$6. \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{8} \text{ ou } p \equiv 7 \pmod{8} \\ -1 & \text{si } p \equiv 3 \pmod{8} \text{ ou } p \equiv 5 \pmod{8} \end{cases}.$$

On déduit que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Théorème 2.8.3 (Loi de reciprocité quadratique)

Soient p et q deux entiers premiers impairs.

$$\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{(q-1)(p-1)}{4}}$$

COROLLAIRE 2.8.2

Si p et q sont des entiers premiers impairs alors

$$\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{4} \text{ ou } q \equiv 1 \pmod{4} \\ -1 & \text{si } p \equiv q \equiv 3 \pmod{4} \end{cases}$$

EXERCICE 27

Soient p et q deux entiers premiers impairs. Vérifier que

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{si } p \equiv 1 \pmod{4} \text{ ou } q \equiv 1 \pmod{4} \\ -\left(\frac{p}{q}\right) & \text{si } p \equiv q \equiv 3 \pmod{4} \end{cases}$$

PROPRIÉTÉS 2.8.2

Soient p un entier premier impair et a un entier relativement premier avec p .

1. Si la factorisation est $a = \pm 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ alors

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \left(\frac{2}{p}\right)^{k_0} \left(\frac{p_1}{p}\right)^{k_1} \cdots \left(\frac{p_r}{p}\right)^{k_r}$$

2.

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod{12} \\ -1 & \text{si } p \equiv \pm 5 \pmod{12} \end{cases}$$

2.8.4 Symbol de Jacobi

DÉFINITION 2.8.2 (SYMBOL DE JACOBI)

Soient a et $b > 1$ deux entiers relativement premiers. Si $b = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ est la décomposition en facteurs premiers de b alors on définit le symbol de Jacobi par

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{k_1} \left(\frac{a}{p_2}\right)^{k_2} \cdots \left(\frac{a}{p_r}\right)^{k_r}.$$

EXEMPLE 2.8.2

$$\left(\frac{3}{20}\right) = \left(\frac{3}{2}\right)^2 \left(\frac{3}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

EXERCICE 28

Soient a, b et c des entiers positifs que $\gcd(b, c) = 1$.

1. Justifier que pour tous $a > 0$ et tous $b \geq 2$ on a : $a^2b^2 + 4a < (ab + 1)^2$.
2. En deduire que si $(a, b) \neq (0, 0), (1, 0)$ alors l'entier $(a^2b^2 + 4a)$ n'est pas un carré parfait.
3. Calculer le symbole $\left(\frac{a^2b^2 + 4a}{3}\right)$ selon les valeurs des entiers a et b .
4. Prouver aussi que pour tous $a > 0$ et tous $c \geq 2$, $(a^2c^2 - 4a)$ n'est pas un carré parfait.
5. Soit $p \equiv 3 \pmod{4}$ un nombre premier qui divise a . On pose $X = (ab^2 + 4)(ac^2 - 4)$.
 - (a) Vérifier que pour $(a, b, c) = (4, 7, 3), (4, 7, 17)$, X est un carré parfait.
 - (b) Calculer le symbole $\left(\frac{X}{p}\right)$ puis conclure.

EXERCICE 29

1. Résoudre
 - (a) $3x^2 + 9x + 7 \equiv 0 \pmod{13}$;
 - (b) $x^2 - x \equiv 7 \pmod{3}$.
2. Montrer que 3 est résidu quadratique modulo 23.
3. Trouver la valeur de : $\left(\frac{-72}{131}\right)$; $\left(\frac{11}{23}\right)$; $\left(\frac{215}{253}\right)$.

2.9 Numération

2.9.1 Bases de numération

Toutes les civilisations anciennes de Chine, Mésopotamie, Égypte, Amérique du Sud,... ont inventé un système de numération. Mais ces différents systèmes de numération ne permettaient pas d'effectuer facilement les opérations.

Le système décimal (base dix) a l'avantage de rendre simples toutes les opérations.

Le système binaire (base deux) est adapté à l'Informatique qui utilise également le système hexadécimal (base seize) pour réduire la taille de l'écriture des nombres (code ASCII).

Nous admettons la proposition suivante :

Proposition 2.9.1 Soit $b \geq 2$ un entier naturel.

Tout entier naturel non nul x s'écrit de façon unique $\sum_{k=0}^p a_k b^k$, où les a_k sont des entiers naturels tels que $0 \leq a_k < b$ et $a_p \neq 0$.

On écrit $x = \overline{a_p a_{p-1} \dots a_0}^b$ écriture est appelée l'écriture de x en base b .

Par convention, les écritures "sans barres" sont en base 10.

Remarque 2.9.1 Soit $x = \overline{a_p a_{p-1} \dots a_2 a_1 a_0}^b = \sum_{k=0}^p a_k b^k = a_p b^p + a_{p-1} b^{p-1} + \dots + a_2 b^2 + a_1 b + a_0$.

• On a $x = b(a_p b^{p-1} + a_{p-1} b^{p-2} + \dots + a_2 b + a_1) + a_0$, avec $0 \leq a_0 < b$.

Donc $q_0 = \overline{a_p a_{p-1} \dots a_2 a_1}^b$ et a_0 sont respectivement le quotient et le reste de la division euclidienne de x par b .

• On a $q_0 = b(a_p b^{p-2} + a_{p-1} b^{p-3} + \dots + a_3 b + a_2) + a_1$, avec $0 \leq a_1 < b$.

Donc $q_1 = \overline{a_p a_{p-1} \dots a_2}^b$ et a_1 sont respectivement le quotient et le reste de la division euclidienne de q_0 par b .

On peut ainsi déterminer de proche en proche l'écriture de x en base b .

EXEMPLE 2.9.1

Pour écrire un entier naturel en base b , les chiffres utilisés sont $0; 1; \dots, b-1$.

2.9.2 Quelques systèmes de numération les plus usuels

Les systèmes de numération les plus usuels sont : le système décimal (base dix), le système binaire (base deux), le système octal (base huit), le système hexadécimal (base seize).

Système binaire

Pour écrire un entier naturel en base deux, les chiffres utilisés sont 0 et 1.

EXEMPLE 2.9.2 1. Écrivons en base 2 le nombre 367.

2. Écrivons en système décimal le nombre $\overline{110100111}^2$.

Système octal

C'est le système de numération de base huit. Pour écrire un entier naturel dans une telle base, les chiffres utilisés sont $0; 1; \dots, 6$ et 7 .

EXEMPLE 2.9.3 1. Écrivons en système octal le nombre 2022.

2. Écrivons en système décimal les nombres $\overline{12340567}^8$, $\overline{76504321}^8$ et $\overline{272}^8$.

Système hexadécimal

C'est le système de numération de base seize. Pour écrire un entier naturel dans une telle base, les chiffres utilisés sont $0; 1; \dots, 9$ A, B, C, D, E et F, où A, B, C, D, E et F représentent respectivement 10; 11; 12; 13; 14 et 15.

EXEMPLE 2.9.4 1. Écrivons en système décimal les nombres \overline{FAC}^{16} et $\overline{F0A5}^{16}$.

2. Écrivons en système hexadécimal les nombres 2022, 765043219 et 2988.

2.9.3 Congruences particulières-Critères de divisibilité par 3, 4, 5, 9, 11 et 25

Dans chacun des exercices suivants, x désigne un entier naturel non nul décriteure décimale $\overline{a_p a_{p-1} \dots a_2 a_1 a_0}$.

EXERCICE 30 (*Congruence modulo 5-Critère de divisibilité par 5*)

1. Démontrer $x \equiv a_0 \pmod{5}$.
2. En déduire le critère de divisibilité par 5.
3. Déterminer les restes des divisions euclidiennes par 5 de 2022, 76528639, 2340 et 79783.

EXERCICE 31 (*Congruence modulo 4 et 25-Critères de divisibilité par 4 et 25*)

1. Démontrer $x \equiv \overline{a_1 a_0} \pmod{4}$ et $x \equiv \overline{a_1 a_0} \pmod{25}$.
2. En déduire les critères de divisibilité par 4 et par 25.
3. Déterminer les restes des divisions euclidiennes par 4 et par 25 de 2022, 76528639, 2340 et 79783.

EXERCICE 32 (*Congruence modulo 3 et 9-Critères de divisibilité par 3 et 9*)

1. Démontrer $x \equiv \sum_{k=0}^p a_k \pmod{3}$ et $x \equiv \sum_{k=0}^p a_k \pmod{9}$.
2. En déduire les critères de divisibilité par 3 et par 9.
3. Déterminer les restes des divisions euclidiennes par 3 et par 9 de 2022, 76528639, 2340 et 79783.

EXERCICE 33 (*Congruence modulo 11-Critère de divisibilité par 11*)

1. Démontrer $x \equiv \sum_{k=0}^p (-1)^k a_k \pmod{11}$.
2. En déduire le critère de divisibilité par 11.
3. Déterminer les restes des divisions euclidiennes par 11 de 2022, 76528639, 2340 et 79783.

Bibliographie

- [1] <http://mathworld.wolfram.com/NumberTheory.html>
- [2] Alain Togbé, *Elementary arithmetic and cryptography*, Course CIMPA at IMSP, July 7-19, 2014
- [3] Michel Waldschmidt, *An elementary introduction to Cryptography*, Course CASPAM at BZU Multan, Nov. 23, 2015
- [4] <http://primes.utm.edu/largest.html>
- [5] <https://www.mersenne.org/primes/>
- [6] <http://primes.utm.edu/top20/page.php?id=12>