Mathématiques pour l'informatique

Gwendal Le Bouffant

ENSSAT

L'anneau $(\mathbb{Z}, +, \times)$

Théorème 1

L'ensemble $\mathbb{Z}$ des entiers relatifs est un anneau commutatif unitaire intègre totalement ordonné.

- anneau : $\mathbb{Z}$ est un groupe commmutatif pour $+$. $\times$ est interne, associative et la multiplication est distributive par rapport à l'addition.
- Cet anneau est commutatif car $\times$ l'est.
- Cet anneau est unitaire car 1 est neutre pour $\times$.
- Cet anneau est intègre : si $ab = 0$ et $a \neq 0$ alors $b = 0$.
  conséquence : on peut faire des simplications : $ab = ac$ et $a \neq 0 \Rightarrow b = c$
- $\mathbb{Z}$ est totalement ordonné : $\leq$ munit $\mathbb{Z}$ d'une relation d'ordre et cet ordre est compatible avec $+$ et $\times$.

L'anneau $(\mathbb{Z}, +, \times)$

Théorème 2

Cet anneau est euclidien, c'est à dire muni d'une division euclidienne :
Si $a, b \in \mathbb{Z}$, $b \geq 0$ alors il existe q et $r \in \mathbb{Z}$, uniques, tels que : $a = bq + r$ et $0 \leq r < b$.

remarques : q est le quotient et r le reste.
Dans le cas où $r = 0$ on dit que b divise a et on note $b|a$.

Exemple

Déterminer q et r pour $a = 17$, $b = 9$.

Idéaux de $\mathbb{Z}$

Definition 1

On appelle idéal d'un anneau A tout sous-groupe additif qui est stable pour la multiplication par les éléments de A.

Exemple

Soit $n \in \mathbb{Z}$. L'ensemble $n\mathbb{Z}$ des multiples de n est un idéal de $\mathbb{Z}$.
Cet idéal est engendré par le seul élément n : on dit qu'il est principal.

Proposition 1

Soit $a_1, \ldots, a_k$ des éléments d'un anneau A. L'ensemble des $\{u_1 a_1 + \cdots y_k a_k | u_1 \in A, \ldots, u_k \in A\}$ est un idéal de A engendré par $a_1, \ldots, a_k$ et noté $(a_1, \cdots, a_k)$.

Ainsi $n\mathbb{Z}$ est noté (n).

Idéaux de $\mathbb{Z}$

Exercice

Montrer que si $b|a$ alors $(a) \subset (b)$.

Remarque : Dans $\mathbb{Z}$, $(2, 4, 6)$ est principal car $(2, 4, 6) = (2)$.
Plus généralement :

Proposition 2

Tous les idéaux de $\mathbb{Z}$ sont du type $n\mathbb{Z}$.

Definition 2

Tous les idéaux de $\mathbb{Z}$ étant principaux, on dit que $\mathbb{Z}$ est un anneau principal.

Remarque : On démontre de la même façon que plus généralement tout anneau unitaire est principal.

pgcd, ppcm

Definition 3

Soient deux entier n et m.

- leur pgcd, noté (n, m) est le générateur positif de l'idéal $(n, m) = n\mathbb{Z} + m\mathbb{Z}$.
- leur ppcm est le générateur positif de $n\mathbb{Z} \cap m\mathbb{Z}$.

Remarque : Deux entiers sont dit premiers entre-eux si leur pgcd vaut 1.

Propriété 1

- *On a commutativité du pgcd :* $(a, b) = (b, a)$.
- *Et l'associativité :* $(a, b, c) = (a, (b, c))$.
- $pgcd(m, n)$ *est le plus grand élément de l'ensemble des diviseurs communs à* n *et* m.

Algorithme d'Euclide

Proposition 3

Soient a et b deux entiers naturels non nuls tels que $b < a$. On note r le reste dans la division euclidienne de a par b, alors l'ensemble des diviseurs communs à a et b et le même que l'ensemble des diviseurs communs à b et r.

Conséquences :

- Lorsque b ne divise pas a, on peut appliquer la propriété jusqu'à l'obtention d'un reste nul. On obtient alors le $pgcd$ de a et b comme étant le dernier reste non nul. Ce procédé est appelé l'Algorithme d'Euclide : détermination du $pgcd(7260, 3025)$, puis $pgcd(390, 525)$.
- En supposant qu'il existe une fonction mod qui calcule le quotient et le reste de la division euclidienne de deux nombres. Écrire l'algorithme d'Euclide donnant le $pgcd$ de a et b.

théorème de Bézout

Théorème 3

Soient n et m deux entiers.

- *Il existe u, $v \in \mathbb{Z}$ tels que $un + vm = (n, m)$.*
- *n et m sont premier entre-eux si, et seulement s'il existe u et v tels que $un + vm = 1$.*

Exemple

Déterminer u et v pour $a = 17$, $b = 9$.

Attention

Il n'y a pas unicité de u et v.

Applications

Pour calculer des identités de Bezout on peut utiliser les différentes équations obtenues dans l'algorithme d'Euclide :

Exemple

Déterminer les coefficients de Bezout pour $a = 48$ et $b = 27$.

Corollaire 1 (Lemme de Gauss)

Si un entier a divise un produit bc de deux entiers et si a est premier avec b alors a divise c.

Équations Diophantiennes

Definition 4

Soient a, b et c trois entiers relatifs fixés avec $(a, b) \neq (0, 0)$.
On appelle équation diophantienne l'équation à deux inconnues :

$$ax + by = c,\ (x, y) \in \mathbb{Z}^2$$

Proposition 4

L'équation $ax + by = c$ admet des solutions dans $\mathbb{Z}$ si,$pgcd(a, b)$ divise c.

Exemples caractéristiques :

Résoudre dans $\mathbb{Z}^2$ les équations suivantes :

1. $15x - 6y = 9$.
2. $5x - 18y = 4$.
3. $6x + 15y = 28$.

Nombres premiers

Definition 5

- On dit que $p \in \mathbb{N}^*$ est un nombre premier si et seulement s'il admet exactement deux diviseurs dans $\mathbb{N}$: 1 et lui-même.
- Un nombre qui n'est pas premier est dit **composé**.

Proposition 5

Soit $n \geq 2$ un entier. Si n n'est pas premier, il existe un nombre premier $p \leq \sqrt{n}$ qui divise n.

Proposition 6

Soit $n \geq 2$ un entier. Alors n est premier ou n peut s'écrire comme produit de nombres premiers.

Théorème de décomposition en facteurs premiers

On a vu que tout entier admet un diviseur premier. Nous allons voir qu'il y a, à l'ordre près, une unique façon d'écrire tout nombre entier comme produit de nombres premiers.

Théorème 4 (Théorème de décomposition en facteurs premiers)

Tout entier $n \geq 2$ s'écrit de façon unique sous la forme :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

où $p_1,\ p_2 \dots,\ p_r$ sont des nombres premiers tels que $p_1 \leq p_2 \leq \dots \leq p_r$ et $\alpha_1,\ \alpha_2,\ \dots,\ \alpha_r$.
Cette écriture est la **décomposition de n en produit de facteurs premiers**.

Pour démontrer l'unicité on utilise le lemme d'Euclide :

Théorème 5 (Lemme d'Euclide)

Soit p un nombre premier, si $p|ab$ et p ne divise pas a alors $p|b$.

Applications

Exercices

Déterminer la décomposition en facteurs premiers puis la liste des diviseurs de 2014, 2904 et 4116.

Cette écriture nous fournit ainsi une méthode simple de déterminer le $pgcd$ et le $ppcm$ de deux nombres :

Exemple

- $pgcd(48, 27)$.
- $ppcm(48, 27)$.

Détermination des nombres premiers

La méthode la plus simple pour déterminer les entiers jusqu'à une certaine borne qui sont des nombres premiers, reste celle du *crible d'Ératosthène*.

Exemple

Détermination de tous les nombres premiers inférieurs à 30.

Cependant ce procédé n'est pas très efficace, on faudra donc chercher d'autres caractérisations des nombres premiers, pour tester la primalité d'un nombre.

Combien y a-t-il de nombres premiers ?

Théorème 6

L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Exercice

Soit X l'ensemble des nombres premiers de la forme $4k+3$ avec $k \in \mathbb{N}$.

1. Montrer que X est non vide.
2. Montrer que le produit de nombres de la forme $4k+1$ est encore de cette forme.
3. On suppose que X est fini et on l'écrit alors $X = \{p_1, \ldots, p_n\}$. Soit $a = 4p_1p_2 \ldots p_n - 1$. Montrer par l'absurde que a admet un diviseur premier de la forme $4k+3$.
4. Montrer que ceci est impossible et donc que X est infini.

Congruences

Definition 6

Soit n un entier naturel non nul, a et b deux entiers relatifs quelconques.
On dit que a est congru à b modulo n et on note

$$a \equiv b \mod n$$

si a et b ont même reste dans la division euclidienne par n.
On dit aussi que a et b sont congrus modulo n.

On comme conséquences de la définition, les propriétés suivantes :

Proposition 7

1. $a \equiv b \mod n \Leftrightarrow (a-b)$ *est divisible par* n.
2. $a \equiv 0 \mod n \Leftrightarrow a$ *est divisible par* n.
3. $a \equiv b \mod n$ *et* $b \equiv c \mod n$ *alors* $a \equiv c \mod n$.

Congruences

Exemples

1. $31 \equiv 10 \mod 7$ car $31 - 10 = 21$ est divisible par 7.
2. $8 \equiv -7 \mod 3$ car $8 + 7 = 15$ est divisible par 3.

Remarque

Si le reste de la division euclidienne de a par n est égal à 1, alors $a \equiv r \mod n$.
La réciproque est fausse : $31 \equiv 10 \mod 7$ mais 10 n'est pas le reste de la division euclidienne de 31 par 7.

Calcul modulo n

Proposition 8

Soient quatre entiers $a, b, c, d \in \mathbb{Z}$ *et* $n \in \mathbb{N}$.
Si $a \equiv b \mod n$ *et* $c \equiv d \mod n$ *alors*
$a + c \equiv b + d \mod n$ *et* $ac \equiv bd \mod n$.

Ce qui a pour conséquence :

Proposition 9

1. $\forall k \in \mathbb{Z}$, *si* $a \equiv b \mod n$ *alors* $a + k \equiv b + k \mod n$.
2. $\forall k \in \mathbb{Z}$, *si* $a \equiv b \mod n$ *alors* $ka \equiv kb \mod n$.
3. $\forall p \in \mathbb{N}$, *si* $a \equiv b \mod n$ *alors* $a^p \equiv b^p \mod n$.

Attention

Les réciproques sont fausses :
$6 \times 5 \equiv 6 \times 2 \mod 2$ mais 5 et 2 ne sont pas congrus modulo 2.
$5^2 \equiv 2^2 \mod 7$ mais 5 et 2 ne sont pas congrus modulo 7.

Applications

Exercices

1.
   1. Quel est le reste de la division euclidienne de 1000 par 37 ?
   2. En déduire que pour tout entier naturel n, le reste de la division euclidienne de 10^{3n} par 37 est égal à 1.
   3. Quel est le reste de la division euclidienne du nombre $N = 10^{10} + 10^{20} + 10^{30}$ par 37 ?
2. Soient a et b deux entiers tels que $a \equiv 3 \mod 7$ et $b \equiv 1 \mod 7$. Démontrer que $2a + b^2$ est un multiple de 7.
3. Soient a et b deux entiers tels que $a \equiv 2 \mod 5$ et $b \equiv 3 \mod 5$. Déterminer le reste de la division euclidienne de $a^2 + 2b^2$ par 5.

Petit théorème de Fermat

Dans le cas de grandes puissances, la recherche de congruences égales à 1 simplifie grandement les calculs. À l'aide du résultat suivant on peut démontrer le petit théorème de Fermat utile pour trouver ces congruences.
Si k est un entier tel que $1 \leq k \leq p-1$,

$$C_k^k = \frac{p!}{k!(p-k)!}$$

est un entier.

Théorème 7 (Petit théorème de Fermat)

Pour tout entier $n \in \mathbb{Z}$, on a $n^p \equiv n \mod p$.
Si de plus n n'est pas un multiple de p, on a $n^{p-1} \equiv 1 \mod p$.

Application

À l'aide du théorème, démontrer que $153^{100} \equiv 23[29]$.

Équations aux congruences

Résoudre une équation aux congruences de la forme $ax \equiv b[n]$ consiste à trouver tous les $x \in \mathbb{Z}$ tels que la congruence soit vraie.

Exemple

Résoudre $x \equiv 7[8]$.

Si maintenant on cherche à résoudre l'équation : $7x \equiv 11[31]$, la difficulté vient de ce qu'on n'a a priori pas la droit de faire des divisions (on est dans $\mathbb{Z}$). En effet on a $6 \equiv 4[2]$ mais $3 \not\equiv 2[2]$.

Équations aux congruences

Proposition 10

Soit n un entier ≥ 2, pour tout entier a, il existe b tel que $ab \equiv 1[n]$, si et seulement si a et n sont premiers entre eux.s

Exemples

Résoudre les congruences suivantes :

1. $5x \equiv 14[17]$.
2. $3x \equiv 2[13]$.
3. $12x \equiv 8[6]$.
4. $9x \equiv 6[12]$.

Théorème Chinois

On trouve dans un traité chinois (III-Ve siècle ap. J.-C.) l'énoncé suivant :
Nous avons des choses dont nous ne connaissons pas le nombre ;

- si nous les comptons par paquets de trois, le reste est 2 ;
- si nous les comptons par paquets de cinq, le reste est 3 ;
- si nous les comptons par paquets de sept, le reste est 2.

Combien y a-t-il de choses ? Réponse : 23.

Exercice

Si x est le nombre de paquets, interpréter les conditions sous forme d'équations aux congruences.

Théorème Chinois

Théorème 8

Soit m et n deux entiers premiers entre eux. Soit a et b deux entiers. Il existe un unique entier c tel que $0 \leq c < mn$ et qui vérifie $c \equiv a \mod m$ et $c \equiv b \mod n$.
Soit x un entier relatif tel que $x \equiv a \mod m$ et $x \equiv b \mod n$; alors $x \equiv c \mod mn$.

Application

Résoudre le système :

$$\begin{cases} x & \equiv & 2 & \mod 10 \\ x & \equiv & 5 & \mod 13 \end{cases}$$

Décomposition en base mixte

Pour résoudre un système de plusieurs équations congruentes, on a souvent recours à la technique dite de décomposition en base mixte.
Si l'on revient au système issu de l'exemple du début, pour déterminer la solution x, on l'écrit en base mixte, sous la forme $a + 3b + 15c + 105d$, avec $0 \leq a < 3, 0 \leq b < 5$ et $0 \leq c < 7$. Puis on traduit les conditions du système pour déterminer a, b, c et d.

Application

Quel est le plus petit entier plus grand que 10000 qui divisé par $5, 12$ et 17 ait pour reste 3 ?

la fonction d'Euler

Definition 7 (la fonction d'Euler)

on définit la fonction :

$$\begin{array}{rccc} \Phi & : & \mathbb{N}^* & \longrightarrow & \mathbb{N}^* \\ & & n & \longmapsto & \Phi(n) \end{array}$$

telle que $\Phi(1) = 1$ et
$\Phi(n) =$ le nombre d'entiers premiers avec n compris entre 1 et $n-1$.

Exemples

- $\Phi(7) = 6$ car 7 est premier
- $\Phi(10) = 4$ car 10 est premier avec $1, 3, 7, 9$
- $\Phi(12) = 4$ car 12 est premier avec $1, 5, 7, 11$

calcul de Φ

Proposition 11 (calcul de Φ)

- *si* p *est premier alors* $\Phi(p) = p - 1$
- *si* p *est premier et* $\alpha \geq 1$ *alors* $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$
- *si* $(a, b) = 1$ *alors* $\Phi(ab) = \Phi(a)\Phi(b)$.
- *si* $n = p_1^{\eta_1} p_2^{\eta_2} \dots p_k^{\eta_k}$ *alors*

$$\Phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

Exemples de calculs de Φ

- $\Phi(7) =$
- $\Phi(10) =$
- $\Phi(12) =$
- $\Phi(60) =$

Application

Théorème 9

Pour tout entier a qui est premier à n, on a la congruence $a^{\phi(n)} \equiv 1 \mod n$.

À la fin des années 1970, Rivest, Shamir et Adleman ont utilisé ce résultat pour élaborer un système de cryptographie à clef publique : système depuis appelé RSA, du nom de ses auteurs.
Il repose sur le fait qu'il existe des applications bijectives $f : A \to B$ d'un ensemble fini A dans un ensemble B pour lesquelles il est facile de calculer $f(a)$, si $a \in A$, alors que personne ne sait calculer efficacement $f^{-1}(b)$, si $b \in B$.

Description du protocole.

On suppose qu'Alice veut envoyer un message secret $m = 12$ à Bob.

1.
   1. Bob choisit deux nombres premiers, par exemple $p_1 = 7$ et $p_2 = 5$.
   2. Bob calcule $n = p_1 p_2$ et $\phi(n)$ (avec quelle formule ?).
   3. Bob choisit un nombre e premier avec $\phi(n)$.
   4. Bob calcule un nombre d tel que $ed \equiv 1 \mod \phi(n)$ (quel algorithme utilise-t-il ?).
2. Bob envoie e et n à Alice (c'est la clé publique).
3. Pour envoyer son message $m = 12$ (qui est un nombre entier modulo n) à Bob, Alice calcule le message crypté $c \equiv m^e \mod n$ et envoie c à Bob.
4. Bob reçoit c et calcule $m \equiv c^d \mod n$.