Chapitre 3

Théorie des nombres

Introduction

Définition : La *théorie des nombres* consiste en l'étude des nombres entiers.

Application dans ce cours : Cryptographie.

Recrutement Google en 2004

Google a diffusé le message crypté suivant en 2004 :
{FIRST 10 DIGIT PRIME IN CONSECUTIVE DIGITS OF E}.COM

$$
\begin{aligned}
e \quad = \quad & 2.71828182845904523536028747135266249775724709369995957496696762772407663035354759457138217852516642\mathbf{7427466391}9320030 \\
& 5992181741359662904357290033429526059563073813232862794 34\ldots
\end{aligned}
$$

7427466391.com pointait vers la page de recrutement de Google.

(Lehman, Leighton, Meyer, 2011)

Rappels

Définitions :

- $a \in \mathbb{Z}$ *divise* $b \in \mathbb{Z}$ s'il existe $k \in \mathbb{Z}$ tel que $ak = b$.
- Lorsque a divise b, on écrit $a \mid b$.
- Si a *divise* b, alors on dit de façon équivalente :
  - a est un *diviseur* de b
  - a est un *facteur* de b
  - b est *divisible* par a
  - b est un *multiple* de a.
- $\forall a \neq 0$, on a $a \mid 0$, $a \mid a$, $1 \mid a$.

- $p \in \mathbb{Z}$ est *premier* si $p > 1$ et si p n'admet aucun autre diviseur entier positif que 1 et lui-même.

Problèmes difficiles célèbres

- Conjecture de Goldbach : Tout entier pair strictement plus grand que 2 est égal à la somme de deux nombres premiers
- Test de primalité : Il existe un algorithme efficace pour déterminer si un entier est premier. Meilleur algorithme à ce jour : $O((\log n)^{12})$.
- Factorisation : Etant donné le produit de deux nombres premiers $n = pq$, il n'existe pas d'algorithme efficace pour retrouver p et q.
- Dernier théorème de Fermat : Il n'existe pas d'entiers positifs x, y, z tel que

$$x^n + y^n = z^n$$

pour un entier $n > 2$. Posé par Fermat en 1630. Résolu par Willes en 1994.

Propriétés de divisibilité

Propriété : Soient $a, b \in \mathbb{Z}$. Si $a \mid b$, alors $a \mid bc$ pour tout $c \in \mathbb{Z}$.

Démonstration :

- Comme $a \mid b$, il existe $k_1 \in \mathbb{Z}$ tel que $ak_1 = b$.
- En multipliant par c, on obtient $ack_1 = bc$.
- Donc, $a \mid bc$. □

Propriété : Soient $a, b, c \in \mathbb{Z}$. Si $a \mid b$ et $b \mid c$, alors $a \mid c$.

Démonstration :

- Comme $\begin{cases} a \mid b \\ b \mid c \end{cases}$, il existe $\begin{cases} k_1 \\ k_2 \end{cases} \in \mathbb{Z}$ tels que $\begin{cases} ak_1 = b \\ bk_2 = c \end{cases}$.
- En substituant b par ak_1 dans la seconde égalité, on obtient $ak_1k_2 = c$.
- Donc, $a \mid c$. □

Propriété : Soient $a, b, c \in \mathbb{Z}$. Si $a \mid b$ et $a \mid c$, alors $a \mid (sb + tc)$ pour tous $s, t \in \mathbb{Z}$.

Démonstration :

- Comme $\begin{cases} a \mid b \\ a \mid c \end{cases}$, on a, grâce à la première propriété, $\begin{cases} a \mid sb \\ a \mid tc \end{cases}$.
- Donc, il existe $\begin{cases} k_1 \\ k_2 \end{cases} \in \mathbb{Z}$ tels que $\begin{cases} ak_1 = sb \\ ak_2 = tc \end{cases}$.
- On obtient $a(k_1 + k_2) = sb + tc$.
- Donc, $a \mid (sb + tc)$. □

Combinaison linéaire

Définition : Un entier n est une *combinaison linéaire* des nombres $b_0, \ldots, b_k$ si et seulement si

$$n = s_0 b_0 + s_1 b_1 + \ldots + s_k b_k$$

pour des entiers $s_0, \ldots, s_k$.

Propriété : Soient $a, b \in \mathbb{Z}$. Pour tout $c \in \mathbb{Z}_0$, on a $(a \mid b) \Leftrightarrow (ca \mid cb)$.

Démonstration : Pour $c \neq 0$, on a successivement

$$\begin{aligned} & a \mid b \\ \Leftrightarrow \quad & (\exists k)\ ak = b \\ \Leftrightarrow \quad & (\exists k)\ cak = cb \\ \Leftrightarrow \quad & ca \mid cb. \end{aligned}$$

□

Division euclidienne

Théorème (division euclidienne) : Soient $n \in \mathbb{Z}$ et $d \in \mathbb{N}_0$. Il existe une unique paire $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ telle que

$$n = qd + r \text{ et } 0 \leq r < d.$$

(q est le *quotient* de la division, r est le *reste* de la division)

Exemple : $\underbrace{2716}_{n} = \underbrace{271}_{q} \cdot \underbrace{10}_{d} + \underbrace{6}_{r}$

Notation : Soient $n \in \mathbb{Z}$ et $d \in \mathbb{N}_0$. Le reste r de la division euclidienne de n par d est noté $n \bmod d$.
(n rem d dans le bouquin de référence)

Exemples :

- $32 \bmod 5 = 2$ car $32 = 6 \cdot 5 + 2$.
- $-11 \bmod 7 = 3$ car $-11 = (-2) \cdot 7 + 3$.

L'énigme des cruches

Données :

- une fontaine ;
- deux cruches non graduées et initialement vides, de contenances respectives de 3 et 6 litres.

Est-il possible de remplir l'une des cruches avec exactement 4 litres ?

Problème général

Théorème : Soient deux cruches non graduées et initialement vides, de contenances respectives $a, b \in \mathbb{N}$ litres. Après une suite quelconque d'opérations parmi

1. remplissage d'une cruche via la fontaine,
2. vidage d'une cruche dans la fontaine,
3. transvasement d'une cruche vers l'autre jusqu'à ce que l'une soit remplie ou que l'autre soit vide,

la quantité d'eau dans chaque cruche est toujours une combinaison linéaire de a et b, et au moins l'une des cruches est soit vide soit pleine.

Démonstration :

- La démonstration fonctionne par induction.
- Soit $P(n) =$ “Après n étapes la quantité d'eau dans chaque cruche est une combinaison linéaire de a et b, et au moins l'une des cruches est soit vide, soit pleine”.
- *Cas de base :* $P(0)$ est vrai car initialement les cruches sont tous les deux vides, et $0a + 0b = 0$.

- *Cas inductif :* Supposons que $P(n)$ soit vrai, et considérons la $(n+1)$ème étape.
  - Opération 1 ou 2 : une des deux cruches devient vide ou pleine, et les quantités restent des combinaisons linéaires de a et b.
  - Opération 3 :
    - Avant la $(n+1)$ème étape : soient $j_1 = s_1 a + t_1 b$ et $j_2 = s_2 a + t_2 b$ les quantités dans les cruches.
    - Après cette étape : l'une des cruches est soit vide (0), soit pleine (a ou b), et l'autre contient soit $j_1 + j_2$, soit $j_1 + j_2 - a$, soit $j_1 + j_2 - b$ litres.
  - Dans les trois cas, $P(n+1)$ est vrai.
- Par induction, $P(n)$ est vrai pour tout $n \in \mathbb{N}$. □

Corollaire : Il est impossible de mesurer 4 litres avec des cruches de 3 et 6 litres, car à tout moment les quantités d'eau ont la forme $3s + 6t$. Or, 4 n'est pas un multiple de 3.

Le plus grand commun diviseur

Le *plus grand commun diviseur (pgcd)* de $a, b \in \mathbb{Z}_0$ est le plus grand entier c tel que $c \mid a$ et $c \mid b$.

Pour $n \in \mathbb{Z}$, on définit $\text{pgcd}(0, n) = \text{pgcd}(n, 0) = n$.

Propriété : Si $b > 0$, alors $\text{pgcd}(a, b) = \text{pgcd}(a \bmod b, b)$.

Démonstration :

- Par le théorème de la division euclidienne, on a $a = qb + r$ avec $r = a \bmod b$.
- a est donc une combinaison linéaire de b et r, ce qui implique que tout diviseur de b et r est un diviseur de a (par la propriété du transparent 64).
- $r = a - qb$ est aussi une combinaison linéaire de a et b et donc tout diviseur de a et de b est aussi un diviseur de r.
- a et b ont donc les mêmes diviseurs que b et r et donc également le même plus grand commun diviseur. □

Algorithme d'Euclide

Cette propriété permet de calculer rapidement le pgcd de deux nombres.

Exemple :

$$
\begin{aligned}
\mathrm{pgcd}(1001, 777) &= \mathrm{pgcd}(\underbrace{1001 \bmod 777}_{=224}, 777) \\
&= \mathrm{pgcd}(\underbrace{777 \bmod 224}_{=105}, 224) \\
&= \mathrm{pgcd}(\underbrace{224 \bmod 105}_{=14}, 105) \\
&= \mathrm{pgcd}(\underbrace{105 \bmod 14}_{=7}, 14) \\
&= \mathrm{pgcd}(\underbrace{14 \bmod 7}_{=0}, 7) \\
&= 7.
\end{aligned}
$$

Propriétés

Théorème : Soient $a, b \in \mathbb{Z}_0$. On a $\text{pgcd}(a, b) =$ la plus petite combinaison linéaire strictement positive de a et b.

Démonstration :

- Soit m la plus petite combinaison linéaire strictement positive de a et b.
- $\boxed{\text{pgcd}(a, b) \leq m}$
  - On a $\text{pgcd}(a, b) \mid a$ et $\text{pgcd}(a, b) \mid b$.
  - Donc, $\text{pgcd}(a, b) \mid (sa + tb)$ pour tous $s, t \in \mathbb{Z}$.
  - En particulier, $\text{pgcd}(a, b) \mid m$, donc $\text{pgcd}(a, b) \leq m$.

- $\boxed{m \leq \text{pgcd}(a, b)}$
  - Montrons que $m \mid a$. Un raisonnement analogue permet de prouver que $m \mid b$. Ainsi, $m \leq \text{pgcd}(a, b)$.
  - Par le théorème de la division euclidienne, il existe q et r tels que $a = qm + r$, avec $0 \leq r < m$.
  - m s'écrit $m = sa + tb$ pour des entiers s et t.
  - On obtient $a = q(sa + tb) + r$, et donc $r = (1 - qs)a + (-qt)b$.
  - r est donc une combinaison linéaire positive de a et b.
  - Or, m est la plus petite combinaison linéaire strictement positive de a et b.
  - Donc, $r = 0$ et $m \mid a$. □

Deux corrolaires

Corrolaire 1 : Un entier n est une combinaison linéaire de a et b si et seulement si n est un multiple de pgcd(a, b).

Corrolaire 2 : Soient deux cruches de capacités a et b. La quantité d'eau dans chaque cruche est toujours un multiple de pgcd(a, b).

Le “pulvérisateur”

Algorithme pour calculer s et t tels que $sa + tb = \text{pgcd}(a, b)$.

Exemple : $\text{pgcd}(259, 70)$

a	b	$a \bmod b$	$=$	$a - q \cdot b$
259	70	49	$=$	$259 - 3 \cdot 70$
70	49	21	$=$	$70 - 1 \cdot 49$
			$=$	$70 - 1 \cdot (259 - 3 \cdot 70)$
			$=$	$-1 \cdot 259 + 4 \cdot 70$
49	21	7	$=$	$49 - 2 \cdot 21$
			$=$	$(259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			$=$	$\boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0		

Résolution de l'énigme des cruches

Soient deux cruches de capacités a et b avec $a < b$. Soit un entier $0 < v < b$ multiple de $\text{pgcd}(a, b)$. La procédure suivante permet d'obtenir v litres dans la cruche la plus grande :

1. Calculer s et t tels que $v = s \cdot a - t \cdot b$ avec $s, t \geq 0$
2. Répéter s fois les deux étapes suivantes :
   - 2.1 remplir la cruche la plus petite
   - 2.2 déverser le contenu de la petite cruche dans la grande. Si la grande cruche est remplie, la vider et continuer à déverser le contenu de la petite dans la grande.

Exemple : $a = 5, b = 3, v = 4 = 3 \cdot 3 - 1 \cdot 5$

$(0/3, 0/5) \xrightarrow{1} (3/3, 0/5) \xrightarrow{2} (0/3, 3/5) \xrightarrow{1} (3/3, 3/5) \xrightarrow{2}$
$(0/3, 1/5) \xrightarrow{1} (3/3, 1/5) \xrightarrow{2} (0/3, 4/5)$

Pourquoi ça marche ?

(démonstration intuitive seulement)

- L'étape 1 est toujours possible (en utilisant le pulvérisateur)
- Au terme des s itérations des étapes 1.1 et 1.2 :
  - La cruche a a été remplie s fois
  - La cruche b a été vidée t fois exactement :
    - Si elle avait été vidée $t+1$ fois ou plus, on aurait $s \cdot a - (t+1) \cdot b = v - b < 0$ litres ou moins dans la cruche b, ce qui est impossible.
    - Si elle avait été vidée $t-1$ fois ou moins, on aurait $s \cdot a - (t-1) \cdot b = v + b > b$ litres ou plus dans la cruche b, ce qui est impossible.
- Il y a donc au final exactement $v = s \cdot a - t \cdot b$ litres dans la cruche b.

Propriétés du plus grand commun diviseur

Soient $a, b, c \in \mathbb{Z}_0$.

Propriété : Tout diviseur commun de a et b divise $\text{pgcd}(a, b)$.

Démonstration :

- Soient $s, t \in \mathbb{Z}$ tels que $\text{pgcd}(a, b) = sa + tb$.
- Soit $d \in \mathbb{Z}$ tel que $d \mid a$ et $d \mid b$.
- On a $d \mid (sa + tb) = \text{pgcd}(a, b)$. □

Propriété : $\text{pgcd}(ka, kb) = k \cdot \text{pgcd}(a, b)$ pour tout $k \in \mathbb{N}_0$.

Démonstration :

- Soient $s, t \in \mathbb{Z}$ tels que $\text{pgcd}(a, b) = sa + tb$.
- Soient $s', t' \in \mathbb{Z}$ tels que $\text{pgcd}(ka, kb) = s'ka + t'kb$.
- On a d'une part

$$\begin{aligned} \text{pgcd}(ka, kb) &= s'ka + t'kb \\ &= k(s'a + t'b) \quad \geq \quad k \cdot \text{pgcd}(a, b). \end{aligned}$$

- On a d'autre part

$$\begin{aligned} k \cdot \text{pgcd}(a, b) &= k(sa + tb) \\ &= s(ka) + t(kb) \quad \geq \quad \text{pgcd}(ka, kb). \end{aligned}$$

(par le théorème du transparent 75) □

Propriété : Si $\text{pgcd}(a, b) = 1$ et $\text{pgcd}(a, c) = 1$, alors $\text{pgcd}(a, bc) = 1$.

Démonstration :

- Il existe $s, t \in \mathbb{Z}$ tels que $\text{pgcd}(a, b) = sa + tb = 1$.
- Il existe $s', t' \in \mathbb{Z}$ tels que $\text{pgcd}(a, c) = s'a + t'c = 1$.
- Dès lors, on a

$$\begin{aligned}(sa + tb)(s'a + t'c) &= 1 \\ &= (ass' + cst' + bs't)a + (tt')bc,\end{aligned}$$

  qui est une combinaison linéaire de a et bc.
- Donc, $\text{pgcd}(a, bc) = 1$. □

Propriété : Si $a \mid bc$ et $\text{pgcd}(a, b) = 1$, alors $a \mid c$.

Démonstration :

- On a $a \mid ac$ et $a \mid bc$.
- Donc, a divise toutes les combinaisons linéaires de ac et de bc.
- En particulier, on a $a \mid \text{pgcd}(ac, bc)$.
- Or, $\text{pgcd}(ac, bc) = c \cdot \text{pgcd}(a, b) = c$.
- Donc, $a \mid c$. □

Théorème fondamental de l'arithmétique

Lemme : Soit p un nombre premier, et $a, b \in \mathbb{Z}$. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Démonstration : Les seuls diviseurs de p sont 1 et p. Donc, $\text{pgcd}(a, p) = 1$ ou $\text{pgcd}(a, p) = p$.

- Si $\text{pgcd}(a, p) = p$, on a $p \mid a$.
- Si $\text{pgcd}(a, p) = 1$, on a $p \mid b$ grâce à la propriété du transparent 84. □

Corollaire : Soit p un nombre premier, et $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Si $p \mid a_1 a_2 \ldots a_n$, alors p divise un des a_i.

Théorème fondamental de l'arithmétique : Tout nombre $n \in \mathbb{N}_0$ peut être écrit de façon unique comme un produit de nombres premiers $n = p_1 p_2 \dots p_j$.

Démonstration :

Tout $n \in \mathbb{N}_0$ s'écrit comme un produit de nombres premiers.

- La démonstration fonctionne par induction forte.
- $P(n) =$ "n s'écrit comme un produit de nombres premiers".
- *Cas de base :* $P(1)$ est vrai car il s'écrit comme le produit d'un ensemble vide de nombres premiers.
- *Cas inductif :* Supposons $P(1) \wedge P(2) \wedge \dots \wedge P(n)$.
  - Si $n+1$ est premier, $P(n+1)$ est vrai.
  - Sinon, $n+1 = ab$, avec $2 \leq a, b \leq n$.
  - Par induction, a et b sont des produits de nombres premiers. Donc, $P(n+1)$ est vrai.
- Par induction, $P(n)$ est vrai pour tout $n \in \mathbb{N}_0$.

Cette écriture est unique.

- Par l'absurde, supposons qu'il existe un $n \in \mathbb{N}_0$ qui s'écrive de plusieurs façons comme produit de nombres premiers.
- Considérons le plus petit n possible.
- Soient $n = p_1 p_2 \dots p_j = q_1 q_2 \dots q_k$ deux de ces écritures.
- On a $p_1 \mid n$ et donc $p_1 \mid q_1 q_2 \dots q_k$.
- p_1 divise au moins un des nombres premiers q_i.
- Comme p_1 et q_i sont premiers, on doit avoir $p_1 = q_i$.
- En supprimant p_1 du premier produit et q_i du second, on obtient que $\frac{n}{p_1} < n$. Or, $\frac{n}{p_1} \in \mathbb{N}$ et s'écrit comme un produit de nombres premiers de plusieurs façons.
- C'est une contradiction avec le choix de n, donc l'écriture est unique. □