

Mardi : Entiers modulaires

Cours de remise à niveau MPRI 2005–2006

David A. Madore

david.madore@ens.fr

20 septembre 2005

Programme du cours

- ▶ Lundi : Entiers (\mathbb{Z})
- ▶ Mardi : Entiers modulaires ($\mathbb{Z}/n\mathbb{Z}$)
- ▶ Mercredi : Polynômes ($k[t]$)
- ▶ Jeudi : Corps finis (\mathbb{F}_q)
- ▶ Vendredi : Extensions de corps (K/k)

9h30 à 12h00 ; salle 0D1 du 19 au 22, 1C1 le 23

Mardi : Entiers
modulaires

David Madore

Programme du
cours

Table des matières

L'anneau $\mathbb{Z}/n\mathbb{Z}$

La fonction
indicatrice d'Euler

Définition

Théorème chinois

Théorème d'Euler

Structure du groupe des
unités

Nombres p -adiques

Table des matières

Mardi : Entiers
modulaires

David Madore

L'anneau $\mathbb{Z}/n\mathbb{Z}$

Programme du
cours

Table des matières

L'anneau $\mathbb{Z}/n\mathbb{Z}$

La fonction indicatrice d'Euler

La fonction
indicatrice d'Euler

Définition

Définition

Théorème chinois

Théorème chinois

Théorème d'Euler

Théorème d'Euler

Structure du groupe des unités

Structure du groupe des
unités

Nombres p -adiques

Nombres p -adiques

Quotient d'un anneau par un idéal

Mardi : Entiers
modulaires

David Madore

Rappel : Un **idéal** d'un anneau (commutatif) A est un sous-groupe additif I de A tel que $AI \subseteq I$ (i.e., $ax \in I$ dès que $x \in I$, pour tout $a \in A$).

Notamment, l'ensemble $(a) = aA$ des multiples d'un $a \in A$ est un idéal de A .

La relation d'équivalence $a \sim a'$ définie comme $a - a' \in I$ permet de mettre sur l'ensemble quotient $A/I = A/\sim$ une structure d'anneau (car $a \sim a'$ et $b \sim b'$ implique $ab \sim a'b'$, etc.). On parle de l'**anneau quotient** de A par l'idéal I .

Surjection canonique : morphisme $A \rightarrow A/I$ dont le noyau est I , envoie a sur sa classe modulo \sim .

« Réciproquement », le noyau d'un morphisme d'anneaux est toujours un idéal, et tout morphisme surjectif $\varphi: A \rightarrow A'$ peut s'identifier à la surjection canonique vers le quotient de A par le noyau $\ker \varphi$.

Programme du
cours

Table des matières

L'anneau $\mathbb{Z}/n\mathbb{Z}$

La fonction
indicatrice d'Euler

Définition

Théorème chinois

Théorème d'Euler

Structure du groupe des
unités

Nombres p -adiques

Rappel : Les idéaux de (l'anneau intègre) \mathbb{Z} sont les $n\mathbb{Z}$ (multiples de n), où n parcourt les entiers naturels. (On dit que \mathbb{Z} est un anneau principal.)

La relation d'équivalence $a \sim a'$ définie comme $a - a' \in n\mathbb{Z}$ s'appelle **congruence modulo n** et se note $a \equiv a' \pmod{n}$.

L'anneau quotient est noté $\mathbb{Z}/n\mathbb{Z}$ (parfois \mathbb{Z}/n ; éviter \mathbb{Z}_n) : c'est donc l'ensemble des classes de congruence modulo n .

On note \bar{a} (ou souvent juste a) l'image d'un $a \in \mathbb{Z}$ par la surjection canonique.

Cas dégénérés :

- ▶ Si $n = 1$ alors $\mathbb{Z}/1\mathbb{Z}$ est l'anneau nul (un seul élément, $\bar{0} = \bar{1}$).
- ▶ Si $n = 0$ alors $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ (on exclut souvent implicitement ce cas).

Si $n > 0$, les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont $\bar{0}, \bar{1}, \dots, \overline{n-1}$.

Idéaux de $\mathbb{Z}/n\mathbb{Z}$

Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ proviennent des idéaux de \mathbb{Z} : ce sont les $\bar{m}(\mathbb{Z}/n\mathbb{Z})$ avec m diviseur de n .

Quotient : $(\mathbb{Z}/n\mathbb{Z})/\bar{m}(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/m\mathbb{Z}$ (pour tout diviseur m de n). D'où une surjection canonique $\mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$ dès que $m|n$.

Attention : On ne peut réduire un $a \in \mathbb{Z}/n\mathbb{Z}$ modulo m que lorsque $m|n$.

Cas particulier : $\mathbb{Z}/n\mathbb{Z}$ n'a que deux idéaux ((0) et $\mathbb{Z}/n\mathbb{Z}$ tout entier) exactement lorsque $n = p$ est premier : c'est alors un **corps**, noté \mathbb{F}_p .

(Par convention, l'anneau nul $\mathbb{Z}/1\mathbb{Z}$ n'est pas un corps, et 1 n'est pas premier.)

Calculs dans $\mathbb{Z}/n\mathbb{Z}$

$n > 0$ ici comme souvent ailleurs.

On représente les éléments de $\mathbb{Z}/n\mathbb{Z}$ par les entiers $0, \dots, n - 1$. Tout calcul se fait sur ces entiers et est suivi d'une opération de division euclidienne par n dont on ne garde que le *reste*.

On peut parfois simplifier : par exemple, pour une addition, on a juste à soustraire n si le résultat dépasse $n \dots$

Si $n = 2^r$ est une puissance de 2 l'implémentation sur ordinateur est immédiate.

Si $n = 2^r - 1$, réduire modulo n (après multiplication, par exemple) se fait en ajoutant les ($\leq r$) bits de poids fort aux r bits de poids faible.

Il est souvent important de calculer a^t modulo n avec a, t, n grands (calculer a^t dans \mathbb{Z} n'est pas envisageable).

Méthode : Écrire t en binaire : $t = \sum_i t_i 2^i$ (où $t_i \in \{0, 1\}$).

Les a^{2^i} se calculent facilement par élévation au carré successive modulo n , et a^t est le produit (modulo n) des a^{2^i} pour lesquels $t_i = 1$.

Groupe cyclique : groupe engendré par un seul élément,
 $G = \langle \sigma \rangle$.

Deux cas possibles :

- ▶ σ (ou G) est d'ordre infini : alors $G \cong \mathbb{Z}$ (où σ correspond à 1),
- ▶ σ (ou G) est d'ordre n : alors $G \cong \mathbb{Z}/n\mathbb{Z}$ (où σ correspond à $\bar{1}$).

Dans tous les cas, G est *abélien*.

Attention : Un groupe cyclique a en général plus d'un générateur : l'isomorphisme $G \cong \mathbb{Z}/n\mathbb{Z}$ existe mais n'est en général pas *unique* (souvent pas « canonique »).

Unités de $\mathbb{Z}/n\mathbb{Z}$

Notation : Si A est un anneau (commutatif), on note A^\times l'ensemble de ses éléments inversibles, ou **unités**.

Soit $n > 0$: pour $m \in \mathbb{Z}$, il y a *équivalence* entre :

- ▶ \bar{m} est inversible dans $\mathbb{Z}/n\mathbb{Z}$ (soit $\bar{m} \in (\mathbb{Z}/n\mathbb{Z})^\times$),
- ▶ \bar{m} est un générateur du groupe cyclique (additif) $\mathbb{Z}/n\mathbb{Z}$,
- ▶ m est premier à n (soit $\text{pgcd}(m, n) = 1$),
- ▶ il existe une relation de Bézout $um + vn = 1$ entre m et n .

On note $\varphi(n)$ le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$: on appelle φ la **fonction (indicatrice) d'Euler**.

Exemple : $\varphi(10) = 4$ car les classes génératrices de $\mathbb{Z}/10\mathbb{Z}$ sont $\bar{1}, \bar{3}, \bar{7}, \bar{9}$.

On ne donnera pas de sens à $\varphi(0)$.

Théorème chinois

Si $b|a$ on a toujours une surjection canonique
 $\mathbb{Z}/a\mathbb{Z} \rightarrow \mathbb{Z}/b\mathbb{Z}$.

Si m et n sont deux naturels non nuls **premiers entre eux**,
considérons le morphisme composé des deux surjections
canoniques

$$\mathbb{Z}/(mn)\mathbb{Z} \rightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

- ▶ il est injectif car un entier multiple de m et de n est multiple de mn (lemme de Gauß),
- ▶ il est surjectif car les cardinaux coïncident (mn au départ et à l'arrivée),

c'est donc un **isomorphisme**.

(Qin Jiushao, c. 1247)

Toujours m et n naturels non nuls premiers entre eux.

On a vu comment trouver une relation de Bézout
 $um + vn = 1$. On a alors l'isomorphisme réciproque

$$\begin{aligned}(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) &\rightarrow \mathbb{Z}/(mn)\mathbb{Z} \\ (x, y) &\mapsto umy + vnx\end{aligned}$$

Pourquoi est-ce bien défini, et pourquoi est-ce bien l'isomorphisme réciproque ?

Plus généralement, connaissant la classe d'un entier modulo m_1, \dots, m_ℓ , on peut retrouver sa classe modulo $\text{ppcm}(m_1, \dots, m_\ell)$. (Pourquoi ?)

Exemple : trouver l'entier entre 0 et 100 congru à 9 modulo 11 et à 3 modulo 13.

Technique : Au lieu de faire un calcul dans \mathbb{Z} ,

- ▶ faire le calcul dans $\mathbb{Z}/m_i\mathbb{Z}$ pour suffisamment de m_i , et
- ▶ obtenir une borne sur le résultat final, permettant de le reconstituer.

Utilité : Lorsque les résultats intermédiaires sont très gros (entiers gigantesques pour un résultat final de taille modeste, ou bien rationnels de gros dénominateurs pour un résultat final entier) cette technique permet d'éviter cette complexité.

Difficulté : Savoir borner le résultat final.

Calcul de l'indicatrice d'Euler

Si m et n (naturels non nuls) sont premiers entre eux, par le théorème chinois on a

$$(\mathbb{Z}/(mn)\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times, \text{ donc}$$

$$\varphi(mn) = \varphi(m) \varphi(n)$$

Si p est premier alors $\varphi(p^r) = (p-1)p^{r-1}$ (car être premier avec p^r équivaut à être premier à p , et c'est le cas de $p-1$ entiers sur p).

On en déduit :

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

où p parcourt les premiers divisant n .

Algorithmiquement : *lent* en général (demande de connaître la d.f.p.).

Théorème d'Euler

Mardi : Entiers
modulaires

David Madore

Théorème : Si n est un entier naturel non nul et a un entier premier à n alors

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Démonstration : \bar{a} , élément du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, a un ordre qui doit diviser celui de ce dernier, soit $\varphi(n)$.

Cas particulier (« *petit* » *théorème de Fermat*) : Si p est un nombre premier alors pour tout entier a on a

$$a^p \equiv a \pmod{p}$$

Remarque : Ceci fournit une condition nécessaire pour que p soit premier. Attention cependant : elle n'est pas suffisante, même si on l'affirme pour *tout* a . (Exercice : pour tout $a \in \mathbb{Z}$, on a $a^{1729} \equiv a \pmod{1729}$...) De tels nombres s'appellent *nombres de Carmichael*.)

Programme du
cours

Table des matières

L'anneau $\mathbb{Z}/n\mathbb{Z}$

La fonction
indicatrice d'Euler

Définition

Théorème chinois

Théorème d'Euler

Structure du groupe des
unités

Nombres p -adiques

Inverses dans $\mathbb{Z}/n\mathbb{Z}$

Soit n naturel non nul et m entier premier avec n : alors $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ est inversible (est une unité). Comment trouver son inverse ?

- ▶ En général : par l'algorithme d'Euclide étendu, qui donne une relation de Bézout $um + vn = 1$ entre m et n . Alors $um \equiv 1 \pmod{n}$, i.e., u est l'inverse de m modulo n .
- ▶ Si $\varphi(n)$ est connu (par exemple $n = 2^r$ ou $n = p$ premier), il peut être avantageux d'utiliser le théorème d'Euler et de calculer $m^{\varphi(n)-1}$ modulo n .

Si $x = a/b$ est un rationnel et n premier avec b (cas le plus important : $n = p$ premier et $p \nmid b$, i.e. $v_p(x) \geq 0$) alors on peut donner un sens au résidu de x modulo n (dans $\mathbb{Z}/n\mathbb{Z}$) comme \bar{a} fois l'inverse de \bar{b} . Compatible avec addition, multiplication...

Théorème de Wilson : p est premier si, et seulement si,
 $(p-1)! \equiv -1 \pmod{p}$.

Exercice : le démontrer.

Théorème de Wolstenholme : si $p \geq 5$ est premier, le
numérateur de $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$ est divisible par p^2 .

Exercice : le démontrer (on pourra regrouper $\frac{1}{k}$ et $\frac{1}{p-k}$, diviser par p , et
chercher à étudier une congruence modulo p ; on pourra faire usage du
fait que $1^2 + 2^2 + 3^2 + \cdots + (p-1)^2 = \frac{1}{6}p(p-1)(2p-1)$).

Éléments primitifs

Soit n un entier naturel non nul. On dit que $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ est (un résidu) **primitif** (modulo n) lorsqu'il engendre $(\mathbb{Z}/n\mathbb{Z})^\times$ (comme groupe abélien multiplicatif) — ce qui entraîne que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

Autrement dit, $a^{\varphi(n)} = 1$ est optimal ($\varphi(n)$ est exactement l'ordre de a).

Attention ! Ne pas confondre :

- ▶ $\mathbb{Z}/n\mathbb{Z}$ (groupe *additif*, d'élément neutre 0) est d'ordre n et est *toujours* cyclique (avec pour générateurs au moins 1 et -1 , et tous les éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$).
- ▶ $(\mathbb{Z}/n\mathbb{Z})^\times$ (groupe *multiplicatif*, d'élément neutre 1) est d'ordre $\varphi(n)$ et est *parfois* cyclique (auquel cas ses générateurs s'appellent éléments *primitifs*).

Question : S'il y a des résidus primitifs modulo n , combien y en a-t-il ?
(Rappel : un groupe cyclique est uniquement déterminé par son ordre.)

Existence d'éléments primitifs

Exemple : Les puissances de 2 modulo 9 sont : 2, 4, 8, 7, 5, 1 ; il y en a bien $\varphi(9) = 6$ donc 2 est primitif modulo 9.

Cas où $n = p^r$ est une **puissance d'un nombre premier** :

- ▶ Si p est *impair*, alors il existe des éléments primitifs : $(\mathbb{Z}/p^r\mathbb{Z})^\times \cong \mathbb{Z}/((p-1)p^{r-1})\mathbb{Z}$ (isomorphisme de groupes abéliens). Mieux : si a est primitif modulo p^2 alors il l'est modulo p^r pour tout r .
- ▶ Si $p = 2$ et $r \geq 3$ alors $(\mathbb{Z}/2^r\mathbb{Z})^\times$ est produit d'un groupe cyclique d'ordre 2 engendré par -1 et d'un groupe cyclique d'ordre 2^{r-2} engendré par 5. (Il n'y a donc pas d'élément primitif, mais 5 est ce qu'il y a de plus près.)
- ▶ Si $p = 2$ et $1 \leq r \leq 2$ alors $(\mathbb{Z}/2^r\mathbb{Z})^\times$ est trivialement cyclique.

Existence d'éléments primitifs (suite)

Mardi : Entiers
modulaires

David Madore

Programme du
cours

Table des matières

L'anneau $\mathbb{Z}/n\mathbb{Z}$

La fonction
indicatrice d'Euler

Définition

Théorème chinois

Théorème d'Euler

Structure du groupe des
unités

Nombres p -adiques

Cas général : On utilise le théorème chinois : si m_1, \dots, m_ℓ sont premiers entre eux deux à deux,

$$(\mathbb{Z}/(\prod_i m_i)\mathbb{Z})^\times \cong \prod_i (\mathbb{Z}/m_i\mathbb{Z})^\times$$

ce qu'on peut appliquer avec pour m_i des puissances de nombres premiers.

Exercice : Quelle est la structure de $(\mathbb{Z}/56\mathbb{Z})^\times$? Quel est le plus grand ordre possible d'un élément de ce groupe ?

Bilan : Il y a des éléments primitifs modulo n lorsque n vaut $1, 2, 4, p^r$ ou $2p^r$ avec p premier impair et $r \geq 1$.

Découverte d'éléments primitifs

Mardi : Entiers
modulaires

David Madore

Programme du
cours

Table des matières

L'anneau $\mathbb{Z}/n\mathbb{Z}$

La fonction
indicatrice d'Euler

Définition

Théorème chinois

Théorème d'Euler

Structure du groupe des
unités

Nombres p -adiques

Si p est premier, pas de meilleure technique connue pour trouver a primitif modulo p que d'essayer successivement 2, 3, 5, 6... Il faut faire statistiquement $(p-1)/\varphi(p-1)$ essais (mais pour un nombre premier p « moyen » cela ne fait pas beaucoup).

(On *conjecture* (Artin, 1927) que chaque entier $\neq 1$ qui n'est pas un carré est primitif modulo une infinité de premiers p .)

Une fois a primitif trouvé modulo p , il est très facile de le trouver primitif modulo p^2 ($p-1$ des p relèvements conviennent) et ensuite il l'est modulo p^r pour tout r .

Si a est primitif modulo n , il définit un isomorphisme de groupes (l'exponentiation modulaire)

$$\begin{aligned}\mathbb{Z}/\varphi(n)\mathbb{Z} &\rightarrow (\mathbb{Z}/n\mathbb{Z})^\times \\ t &\mapsto a^t\end{aligned}$$

dont la réciproque s'appelle **logarithme discret** de base a modulo n .

Pour $n = p$ premier, le logarithme discret est (supposé) *très difficile* à calculer (applications en cryptographie).

(Attention : modulo p^r avec p petit, le logarithme est *facile* à calculer par des calculs p -adiques.)

L'anneau \mathbb{Z}_p des entiers p -adiques est une sorte de limite (« limite projective ») des $\mathbb{Z}/p^r\mathbb{Z}$ quand $r \rightarrow +\infty$. Précisément :

Un **entier p -adique** est une suite $(a_i)_{i \in \mathbb{N}}$ avec $a_i \in \mathbb{Z}/p^i\mathbb{Z}$ telle que si $i \leq j$ alors a_j a pour classe a_i modulo p^i . (La donnée de chaque a_i détermine donc tous les précédents.)

En particulier, l'écriture en base p de a_i comporte i chiffres qui sont les i derniers chiffres de tous les a_j ultérieurs. On peut donc voir un entier p -adique comme une écriture en base p « infinie à gauche ». Les opérations sur cette écriture se font *exactement* de la même façon que sur les entiers.

Exemple : ...1100110011001101 est un entier 2-adique, écrit en binaire. Que se passe-t-il si on le multiplie par 5 ?

Programme du
cours

Table des matières

L'anneau $\mathbb{Z}/n\mathbb{Z}$

La fonction
indicatrice d'Euler

Définition

Théorème chinois

Théorème d'Euler

Structure du groupe des
unités

Nombres p -adiques

Entiers p -adiques (suite)

Attention : On peut réduire un entier p -adique modulo p (donne a_1), p^2 (donne a_2), p^3 (donne a_3), etc., mais modulo aucun autre entier qu'une puissance de p . On ne peut pas écrire un p -adique dans une autre base que p .

Exemple : ...1100110011001101, qui est l'écriture binaire du 2-adique $\frac{1}{5}$, est congru à 1 modulo 2, à 1 modulo 4, à 5 modulo 8, à 13 modulo 16, etc. Ce sont les inverses de 5 modulo 2, 4, 8, 16, etc.

On peut définir la valuation p -adique d'un entier p -adique comme le nombre de 0 consécutifs à la fin (à droite) de son écriture p -adique. (Pour tout $x \in \mathbb{Z}_p$ on a $v_p(x) \geq 0$.)

Les entiers usuels peuvent être considérés comme des entiers p -adiques particuliers ($\mathbb{Z} \subseteq \mathbb{Z}_p$) : ce sont ceux qui n'ont qu'un nombre fini de chiffres non nuls ou un nombre fini de chiffres différents de $p - 1$.

Exemple : ...111111111111001 est l'écriture binaire de l'entier 2-adique -7 (opposé de 7 qui s'écrit ...00000111).

Entiers p -adiques (fin)

L'anneau \mathbb{Z}_p est **intègre** : si $ab = 0$ dans \mathbb{Z}_p alors $a = 0$ ou $b = 0$ (on utilise le fait que p est premier ici!).

Tout entier $b \in \mathbb{Z}$ qui n'est pas multiple de p (i.e., $v_p(b) = 0$) est inversible dans \mathbb{Z}_p : en effet, il est inversible modulo p, p^2, p^3 , etc., et ces inverses sont compatibles les uns avec les autres donc définissent un élément de \mathbb{Z}_p .

On peut donc définir un élément de \mathbb{Z}_p pour tout rationnel $x = a/b$ tel que $v_p(x) \geq 0$.

Exemple : $\frac{1}{5}$ définit un entier 2-adique, 3-adique ou 7-adique, mais pas un entier 5-adique !

Un **nombre p -adique** est le quotient d'un *entier* p -adique par une puissance de p . *Tout* quotient d'un entier p -adique par un entier p -adique non nul est un rationnel p -adique.

Notation : \mathbb{Q}_p le corps des nombres p -adiques : $\mathbb{Q} \subseteq \mathbb{Q}_p$.

Écriture en base p : Avec un nombre *fini* de chiffres après la virgule (et un nombre infini à gauche).

Exemple : ...0011001100110011.01 est l'écriture binaire du nombre 2-adique $\frac{1}{20}$.

Valuation p -adique : $v_p(a/b) = v_p(a) - v_p(b)$ (si négatif, compte le nombre de chiffres après la virgule en base p).

Norme p -adique : $|x|_p = p^{-v_p(x)}$. *Distance* associée : $d_p(x, y) = |x - y|_p$ (deux nombres p -adiques sont *proches* s'ils ont beaucoup de chiffres communs à l'extrémité *gauche*).

À quoi ça sert ?

Le corps \mathbb{Q}_p partage beaucoup de propriétés avec \mathbb{R} (« corps normé complet ») et peut parfois se substituer à lui.

Estimations d'erreurs / d'inégalités *beaucoup plus faciles* dans \mathbb{Q}_p que dans \mathbb{R} à cause de l'inégalité ultramétrique $|x + y|_p \leq \max(|x|_p, |y|_p)$.

Calculs dans \mathbb{Q}_2 (ou \mathbb{Z}_2) souvent *beaucoup plus simples* que dans \mathbb{R} sur ordinateur : calculer modulo 2^ℓ revient à faire un calcul approximatif dans \mathbb{Z}_2 .

Permettent de résoudre certains problèmes d'arithmétique modulaire. Exemple : comment trouver $x \in \mathbb{Z}$ tel que $x^2 \equiv 17 \pmod{2^{64}}$?