Culte du corps (fini)

Emmanuel Hallouin

L3 MIASHS, parcours Informatique, UT2J

Année 2021-2022

Congruences

Définition

On dit que x et y sont congrus modulo n et on écrit $x \equiv y \pmod{n}$, si et seulement s'ils vérifient l'une des assertions équivalentes suivantes :

- l'entier n divise $(x - y)$,
- la différence $(x - y)$ est multiple de n,
- on a $y = x +$ un multiple de n,
- il existe $q \in \mathbb{Z}$ tel que $y = x + qn$.

Relation d'équivalence

Proposition

La relation de congruence est ce que l'on appelle une relation d'équivalence, c'est-à-dire qu'elle est :

- **réflexive** : $x \equiv x \pmod{n}$,
- **symétrique** : $x \equiv y \pmod{n} \Leftrightarrow y \equiv x \pmod{n}$,
- et **transitive** : $x \equiv y \pmod{n}$ et $y \equiv z \pmod{n} \Rightarrow x \equiv z \pmod{n}$.

Maniement des congruences

Proposition

Un entier est toujours congru modulo n à son reste par la division par n ; autrement dit, pour tout $x \in \mathbb{Z}$, on a $x \equiv r \pmod{n}$, où r est le reste de la division de x par n.

Proposition

La relation congruence modulo n se manipule comme une égalité, c'est-à-dire que l'on peut ajouter ou multiplier deux congruences modulo n. La seule opération usuelle qui n'est pas toujours autorisée est la simplification.

Remarque : je parle bien d'ajouter ou de multiplier des congruences modulo **le même** n.
Une simplification illicite : on a $2 \times 3 \equiv 2 \times 1 \pmod{4}$ mais $3 \not\equiv 1 \pmod{4}$ (simplification par 2 impossible).

Classes modulo n

Définition

Soit $n \geqslant 2$. Pour chaque $x \in \mathbb{Z}$, on introduit la **classe** de x, notée $\overline{x}$, et définie par :

$$\overline{x} = \{x + nq, q \in \mathbb{Z}\} = \{x + \text{ un multiple de } n\}$$

Tout entier appartenant à cette classe s'appelle un **représentant** de la classe $\overline{x}$.

Proposition

- Deux entiers x et y ont la même classe, c-a-d $\overline{x} = \overline{y}$, si et seulement si $x \equiv y \pmod{n}$.
- Les classes $\overline{0}, \dots, \overline{n-1}$ forment une partition de $\mathbb{Z}$.

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

Proposition

L'ensemble des classes modulo n peut être muni de deux lois, une addition, un produit, via :

$$\overline{x} + \overline{y} = \overline{x+y} \qquad\qquad \overline{x} \times \overline{y} = \overline{x \times y}$$

(les opérations rouges sont des opérations entre classes, les opérations noires sont de banales opérations entre entiers.

Définition

L'ensemble des classes modulo n est noté $\mathbb{Z}/n\mathbb{Z}$. Muni de ces deux lois, on dit que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un **anneau**.

On a $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \ldots, \overline{n-1}\right\}$ donc il compte n éléments.

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

Définition

Une classe $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est dite **inversible** si et seulement s'il existe $\overline{y} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{x} \times \overline{y} = \overline{1}$.

Caractérisation

Pour que $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ soit **inversible** il faut et il suffit que $\text{pgcd}(x, n) = 1$, i.e. que x et n soient premiers entre eux.
Les inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les classes des entiers premiers à n.

Calcul de l'inverse

C'est pour calculer l'inverse que l'on a recourt à l'algorithme d'Euclide étendu. En effet, si x est premier à n, alors d'après le théorème de Bezout, on sait qu'il existe $u, v \in \mathbb{Z}$ tels que $ux + nv = 1$. Si on considère cette égalité modulo n, il vient :

$$\overline{ux} + \overline{nv} = \overline{u} \times \overline{x} + \overline{0} \times \overline{v} = \overline{u} \times \overline{x} = \overline{1}$$

Du coup l'inverse de $\overline{x}$ dans $\mathbb{Z}/n\mathbb{Z}$ n'est ni plus ni moins que le coefficient de Bezout entre x et n devant x.
Conséquence : calculer un inverse modulo n revient à effectuer un Euclide étendu.

Un exemple

r_i	q_i	u_i	v_i
105		1	0
16	6	0	1
9	1		-6
7	1		7
2	1		-13
1	3	?	46

Ainsi $105 \times ? + 16 \times 46 = 1$. Modulo 105 cela donne :

$$\overline{105} \times \overline{?} + \overline{16} \times \overline{46} = \overline{0} \times \overline{?} + \overline{16} \times \overline{46} = \overline{16} \times \overline{46} = \overline{1}$$

On en déduit que l'inverse de $\overline{16}$ modulo 105 est $\overline{46}$.

Exponentiation dichotomique

L'algorithme «d'exponentiation dichotomique» permet de calculer efficacement une puissance g^β dans un anneau $\mathbb{Z}/n\mathbb{Z}$ (mais en fait dans n'importe quel groupe). Il repose sur l'écriture en base 2 de l'exposant β :

$$\beta = 2^k\beta_k + \cdots + 2\beta_1 + \beta_0 \qquad \beta_i \in \{0,1\}, \beta_k = 1$$

Il comporte deux phases.

- **Phase des carrés successifs :** calcul des g^{2^i}, pour $0 \leqslant i \leqslant k$
- **Phase de recomposition :** calcul du produit de certains g^{2^i} bien choisis pour trouver g^β

Phase des carrés successifs

Il s'agit de tabuler les valeurs des carrés successifs en partant de g, c'est-à-dire les :

$$g, \qquad g^2, \qquad g^4, \qquad g^8, \qquad g^{16}, \qquad \dots, \qquad g^{2^k}$$

Il suffit pour cela d'itérer la fonction carrée k fois en partant de g :

$$g \quad \xrightarrow{\text{au carré}} \quad g^2 \quad \xrightarrow{\text{au carré}} \quad g^4 \quad \cdots \quad g^{2^{k-1}} \quad \xrightarrow{\text{au carré}} \quad g^{2^k}$$

On a utilisé l'identité :

$$\left(g^{2^i}\right)^2 = g^{2\times 2^i} = g^{2^{i+1}} \qquad \text{car } \left(g^{\alpha}\right)^{\beta} = g^{\alpha\beta}.$$

Phase de recomposition

Le calcul de g^β consiste à multiplier tous les carrés déterminés dans la phase précédente pour lesquels le bit de β correspondant vaut 1. Plus précisément :

$$\begin{aligned}
g^\beta &= g^{2^k\beta_k+\cdots+2^1\beta_1+2^0\beta_0} \\
&= g^{2^k\beta_k} \times \cdots \times g^{2^1\beta_1} \times g^{2^0\beta_0} && \text{car } g^{\alpha+\beta} = g^\alpha \times g^\beta \\
&= \left(g^{2^k}\right)^{\beta_k} \times \cdots \times \left(g^{2^1}\right)^{\beta_1} \times \left(g^{2^0}\right)^{\beta_0} && \text{car } g^{\alpha\beta} = (g^\alpha)^\beta \\
&= \prod_{\beta_i=1} g^{2^i} && \text{car } \left(g^{2^j}\right)^0 = 1
\end{aligned}$$

Conclusion sur l'exponentiation dichotomique

- La complexité du de l'algorithme d'exponentiation dichotomique pour calculer $g^\beta \in \mathbb{Z}/n\mathbb{Z}$ devient :

$$O\left(\log(\beta)\log(n)^2\right) \qquad \text{ou} \qquad O\left(\log(n)^3\right)$$

  puisque l'on peut choisir $\beta \leqslant n$. C'est donc un algorithme «cubique».
- L'algorithme et tout à fait général et permet de calculer efficacement les puissances dans n'importe quel groupe.
- Les deux phases peuvent être menées de concert pour donner lieu à un algorithme purement itératif (sans nécessité de stocker la table par exemple). A vos codes !

Un exemple $\overline{7}^{20}$ modulo 23

- Décomposer l'exposant 20 en base 2 :

$$20 = 16 + 4 = 2^4 + 2^2 = (10100)_2$$

On a

β_0	β_1	β_2	β_3	β_4
0	0	1	0	1

- Calcul des carrés successifs (modulo 23 ! ! !)

0	1	2	3	4
7	7^2	7^4	7^8	7^{16}
7	3	9	12	6

- Multiplier les carrés correspondant à des bits $\neq 0$:

$$7^{20} = 7^{16} \times 7^4 = 6 \times 9 = 54 \equiv 8 \pmod{23}$$

Un autre exemple $\overline{3}^{25}$ dans $\mathbb{Z}/29\mathbb{Z}$

- Décomposer l'exposant 25 en base 2 :

$$25 = 16 + 8 + 1 = 2^4 + 2^3 + 2^0 = (11001)_2$$

On a

β_0	β_1	β_2	β_3	β_4
1	0	0	1	1

- Calcul des carrés successifs (modulo 29 ! ! !)

0	1	2	3	4
3^1	3^2	4^4	3^8	3^{16}
3	9	$81 = 23 = -6$	$36 = 7$	$49 = 20 = -9$

- Multiplier les carrés correspondant à des bits $\neq 0$:

$$3^{25} = 3^{16} \times 3^3 \times 3^1 = 20 \times 7 \times 3 \equiv \color{red}{14} \pmod{29}$$

Corps finis $\mathbb{F}_p$

Proposition

Si p est un nombre premier, alors toutes les classes non nulles de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles.

Définition

Si p est un nombre premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ s'appelle un **corps fini**. On le note $\mathbb{F}_p$.

Observations

Prenez un premier p et $\overline{x} \in \mathbb{F}_p \setminus \{\overline{0}\}$ puis calculer la suite des $\overline{x}^i$, $i \geqslant 1$; si vous choisissez plusieurs $\overline{x}$, vous devriez finir par observer que :

Observations

Pour tout $x \in \mathbb{F}_p^*$ la suite des puissances $(x^i)_{i \geqslant 0}$ boucle toujours en $\overline{1}$ et la longueur de ce cycle est un diviseur de $(p-1)$. Pour tout diviseur d de $(p-1)$, il existe toujours un cycle de longueur d ; en particulier il existe toujours un cycle de longueur maximale égale à $(p-1)$.

A vos ordres !

Définition

L'**ordre** (multiplicatif) d'un élément $x \in \mathbb{F}_p^*$ est le plus petit $\alpha \in \mathbb{N}^*$ tel que $x^\alpha = \overline{1}$.

Exemple : Dans $\mathbb{F}_7^*$, on a :

$$\begin{array}{lllll}
\overline{2}^1 = \overline{2}, & \overline{2}^2 = \overline{4}, & \overline{2}^3 = \overline{1} & \Rightarrow & \text{ordre}(\overline{2}) = 3 \\
\overline{3}^1 = \overline{3}, & \overline{3}^2 = \overline{2}, & \overline{3}^3 = \overline{6}, & \overline{3}^4 = \overline{4} & \\
 & \overline{3}^5 = \overline{5}, & \overline{3}^6 = \overline{1} & \Rightarrow & \text{ordre}(\overline{3}) = 6
\end{array}$$

Théorème de Lagrange ou Petit Fermat

Pour tout $x \in \mathbb{F}_p^*$, on a $x^{p-1} = \overline{1}$ et l'ordre x est un diviseur de $(p-1)$.

Retour aux Racines primitives

Définition

Un élément de $\mathbb{F}_p^*$ d'ordre $p-1$ s'appelle une **racine primitive de l'unité**.

Exemple : $\overline{3}$ est un racine primitive dans $\mathbb{F}_7^*$.

Théorème

Tout corps fini $\mathbb{F}_p$ contient au moins une racine primitive de l'unité.

En termes plus mathématiques, l'énoncé précédent peut être reformulé en disant que le groupe (multiplicatif) $\mathbb{F}_p^*$ est un groupe cyclique.

Quelques formules sur les ordres

- Si $x \in \mathbb{F}_p^*$ est d'ordre α, alors les puissances $x^0, x^1, x^2, \ldots, x^{\alpha-1}$ sont deux-à-deux distinctes ; en revanche $x^0 = x^\alpha$, $x^1 = x^{\alpha+1}$, etc...
- Deux puissances de x sont égales $x^\alpha = x^\beta$ si et seulement si l'ordre de x divise $\alpha - \beta$.
- Si on connaît l'ordre d'un élément, on connaît l'ordre de n'importe quelle de ses puissances car :

$$\text{ordre}\left(x^\alpha\right) = \frac{\text{ordre}(x)}{\text{pgcd}(\alpha, \text{ordre}(x))}$$