Cours Arithmétique Groupe C

10 janvier 2021

1 Rappel $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \cdots, n-1\}$. Sur $\mathbb{Z}/n\mathbb{Z}$ on a deux opération $+$ et $\times$. Par exemple $5 + 7 = 3[9]$

En algèbre pour avoir ce qu'on appelle un "groupe", il y a deux choses importante

-*élément neutre* : pour le $+$ c'est 0 car $x + 0 = x[n]$, pour $\times$ c'est 1 car $1 \times x = x[n]$ pour tout x.

-*inverse*. Pour le $+$ l'inverse de $x[n]$ est $-x[n]$, pour $\times$ c'est plus compliquer. Par exemple 2[4] n'a pas d'inverse. En effet $a \times 2 = 0$ ou 2[4] et jamais 1.

Lemme 1. *Les éléments dans $\mathbb{Z}/n\mathbb{Z}$ qui admettent un inverse sont ceux qui sont premiers avec n.*

Démonstration. Soit x premier avec n. Par le théorème de Bézout il existe k et k' tel que

$$kx - k'n = 1$$

Donc $kx = 1[n]$. (c'est à dire k est l'inverse de x et on le note $k = x^{-1}$).

D'un autre côté, si x n'est pas premier avec n alors il n'admet pas d'inverse. En effet par l'absurde si il existe k et k' tel que $kx = 1 + k'n$ alors $pgcd(x, n)|1$ absurde. □

Exemple :2 est l'inverse de 4 modulo 7.

Remarque : Si p est premier alors tous les éléments non nul de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles.

Notation : l'ensemble des inversibles est noté $(\mathbb{Z}/n\mathbb{Z})^\times$

Proposition 2. *Le nombre d'éléments $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$ où $\phi(n)$ est l'indicatrice d'Euler.*

Si on note $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ alors

$$\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1)...p_k^{\alpha_k - 1}(p_k - 1) = n(1 - \frac{1}{p_1})...(1 - \frac{1}{p_k})$$

Par exemple : Pour $n = 20$, $\phi(n) = 8$. En effet les nombres premiers avec 20 sont $1, 3, 7, 9, 11, 13, , 17, 19$. Remarquer qu'en éliminant tous les nombres paires on passe de $20 \to 10$, puis tous les divisibles par 5 de $10 \to 8$. Plus généralement pour chaque diviseur premier p de n, on retire « $\frac{1}{p}$ des nombres ».

Démonstration. Avec le théorème des restes chinois : On écrit

$$\mathbb{Z}/n\mathbb{Z} \approx (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times ... \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$$

Dans l'exemple avec $n = 20$ on a $\mathbb{Z}/20\mathbb{Z} \approx (\mathbb{Z}/2^2\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$

Le nombre de nombres premiers avec $p_1^{\alpha_1}$ dans $(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})$ c'est égale $p_1^{\alpha_1} - p_1^{\alpha_1 - 1}$. En effet ce sont les nombres plus petit que $p_1^{\alpha_1}$ et qui ne sont pas divisibles par p_1. Puisqu'il y a exactement $p_1^{\alpha_1 - 1}$ nombres qui sont divisibles par p_1, on a alors $p_1^{\alpha_1} - p_1^{\alpha_1 - 1}$ nombres restant. Dans l'exemple il y a $4 - 2 = 2$ nombres premiers avec 4 dans $\mathbb{Z}/2^2\mathbb{Z}$.

Maintenant être premier avec n c'est la même chose qu'être premier à la fois avec tous les $p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_k^{\alpha_k}$. et on obtient alors $(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \times ... \times (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$. Dans notre exemple il y 2 nombres premiers avec 4 dans $\mathbb{Z}/2^2\mathbb{Z}$ et 4 nombres premiers avec 5 dans $\mathbb{Z}/5\mathbb{Z}$. Ce qui donne donc $4 \times 2 = 8$ nombres premiers avec $\mathbb{Z}/20\mathbb{Z}$. On écrit aussi $\phi(20) = 8$ □

Autre exemple. Puisque $72 = 2^3 \times 3^2$ $\phi(72) = (2^3 - 2^2) \times (3^2 - 3) = 24$.

1.1 Ordre d'un élément.

Proposition 3. *Si $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ alors existe k tel que $x^k = 1[n]$.*

Démonstration. $\mathbb{Z}/n\mathbb{Z}$ a n éléments. Donc $x^k[n]$ prend au plus n valeurs différentes lorsque k varie sur l'ensemble des entiers. Parce qu'il y a une infinité d'entiers on peut utiliser le principe des tiroirs : il existe $k < k'$ tel que $x^k = x^{k'}[n]$. On multiplie alors par $(x^{-1})^k$ (existe car x est premier avec n) et on a

$$(x^{-1})^k x^k = (x^{-1})^k x^{k'}[n]$$

$$1 = x^{k'-k}[n]$$

□

Exemple : Avec $x = 2$ et $n = 7$. On calcule $2^2 = 4[7]$, $2^3 = 8 = 1[7]$.

On a alors $2^{-1} = 4[7]$, car $2 \times 4 = 8 = 1[7]$

Il est possible de prendre des puissances négatives $2^{-3} = 1[7]$. Attention ce ne sont pas des fractions des entiers modulo 7.

Lemme 4. *Si $x^k = 1[n]$ et $x^{k'} = 1[n]$ alors $x^{pgcd(k,k')} = 1[n]$.*

Démonstration. Avec le Théorème Bézout : il existe a et b tel que $k \times a + k' \times b = pgcd(k, k')$.

$$\begin{aligned} x^{pgcd(k,k')} &= x^{k\times a+k'\times b}[n] \\ &= x^{k\times a}x^{k'\times b}[n] \\ &= (x^k)^a \times (x^{k'})^b[n] \\ &= 1^a \times 1^b[n] \\ &= 1[n] \end{aligned}$$

□

.

Définition 5. L'ordre $o(x)$ d'un élément x dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est plus petit entier $k > 0$ tel que $x^k = 1[n]$.

Par exemple $o(2) = 3$ dans $(\mathbb{Z}/7\mathbb{Z})^\times$ parce que $2^3 = 1[7]$ (et $2^2 = 4 \neq 1[7]$).

Autre exemple $o(3) = 6$ dans $(\mathbb{Z}/7\mathbb{Z})^\times$. Car $3^2 = 2[7]$, $3^3 = 6[7]$, $3^4 = 4[7]$, $3^5 = 5[7]$, et $3^6 = 1[7]$.

Proposition 6. *Si $x^k = 1[n]$ alors $o(x)$ divise k.*

Démonstration. On a que $x^{pgcd(o(x),k)} = 1[n]$. De plus $pgcd(o(x), k)|o(x)$ par la définition du PGCD. Donc $pgcd(o(x), k) \leq o(x)$. Or par la définition de l'ordre $o(x)$ est le plus petit entier possible donc $o(x) \leq pgcd(o(x), k)$ et conlusion $o(x) = pgcd(o(x), k)$.

Pour finir puisque par définition du PGCD on a aussi $pgcd(o(x), k)|k$, on a donc $o(x)|k$. □

Théorème 7. *Le petit théorème de Fermat. Soit p un nombre premier alors pour tout x premier avec p*

$$x^{p-1} = 1[p]$$

On a aussi

$$x^p = x[p]$$

On peut aussi exprimer le petit théorème de Fermat ainsi «l'ordre x divise $p - 1$».

Exemple :

$$3^6 = 1[7], \quad 2^6 = (2^3)^2 = 1[7]$$

Théorème 8. *Le théorème de Euler-Fermat. Soit n un entier alors pour tout x premier avec n*

$$x^{\phi(n)} = 1[n]$$

où $\phi(n)$ est la fonction indicatrice d'Euler.

Rappel : attention ne fonctionne que pour x premier avec n. Par exemple puisque 2 n'est pas inversible pour $\mathbb{Z}/4\mathbb{Z}$, on n'a pas de $2^{\phi(4)} = 1[4]$

Démonstration. Soit x un nombre premier avec n. Remarque : si x et y sont premiers avec n alors xy et aussi premier avec n. Autrement dit tant qu'on multiplie des éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ on reste dans $(\mathbb{Z}/n\mathbb{Z})^\times$. (c'est également important pour la notion de « groupe »). Et on a l'inverse $(xy)^{-1} = x^{-1}y^{-1}$.

On énumère tous les éléments : $(\mathbb{Z}/n\mathbb{Z})^\times = \{y_1, ..., y_{\phi(n)}\}$.

Puis on multiplie chacun de ces éléments par x $\{xy_1, xy_2, \cdots, xy_{\phi(n)}\}$.

Remarque 1 : Chacun de ces éléments est dans $(\mathbb{Z}/n\mathbb{Z})^\times$ (par la remarque précédente).

Remarque 2 : Tous les éléments sont différents. En effet

$$xy_i = xy_j[n] \Rightarrow x^{-1}xy_i = x^{-1}xy_j[n] \Rightarrow y_i = y_j[n].$$

Conclusion on a alors $\{y_1, ..., y_{\phi(n)}\} = \{xy_1, xy_2, \cdots, xy_{\phi(n)}\}$

Exemple : Avec $(\mathbb{Z}/7\mathbb{Z})^\times = \{1, 2, 3, 4, 5, 6\}$ et $x = 2$ on a $\{2, 4, 6, 1, 3, 5\}$ et on retrouve bien tous les éléments de $(\mathbb{Z}/7\mathbb{Z})^\times$.

Astuce : multiplions tous les éléments ensemble.

$$\Delta = y_1 \times y_2 \times ... \times y_{\phi(n)}$$

Puisque les deux ensembles sont les même alors

$$\Delta = xy_1 \times xy_2 \times \cdots \times xy_{\phi(n)} = x^{\phi(n)} \times y_1 \times y_2 \times ... \times y_{\phi(n)}[n]$$

Conclusion

$$\Delta = x^{\phi(n)} \times \Delta[n]$$

Enfin puisque Δ est aussi inversible modulo n, (c'est un produit d'éléments inversibles) alors

$$\Delta^{-1} \times \Delta = x^{\phi(n)} \times \Delta \times \Delta^{-1}[n] \Rightarrow 1 = x^{\phi(n)}[n]$$

□

2 Exercices.

On fait des exercices de la feuille de TD (dans le désordre).

Exercice. (6) Montrer que $13|5^{60} - 3^{48}$.

Solution. On utilise le petit théorème de Fermat

$$5^{12} = 1[13] \quad \text{et} \quad 3^{12} = 1[13]$$

Donc

$$5^{60} = (5^{12})^5 = 1[13] \quad \text{et} \quad 3^{48} = (3^{12})^4 = 1[13]$$

Conclusion $5^{60} - 3^{48} = 1 - 1 = 0[13]$ et donc $13|5^{60} - 3^{48}$.

Exercice. (7) Montrer que 5 divise $2^{3n+5} + 3^{n+1}$.

Solution. On a $2^3 = 8 = 3[5]$. Par Fermat on a aussi $2^5 = 2[5]$. Donc

$$2^{3n+5} + 3^{n+1} = 3^n \times 2 + 3^n \times 3 = 3^n \times (2+3) = 0[5]$$

Autre méthode : on peut écrire les table de $2^n[5]$ et $3^n[5]$ mais c'est plus laborieux.

Exercice. (8) Pour n impair, $n|2^{n!} - 1$.

Solution. Puisque n est impaire 2 est premier avec n. Par Euler-Fermat $2^{\phi(n)} = 1[n]$. On remarque que $\phi(n) \leq n$ et donc $n! = 1 \times 2 \times ... \times \phi(n) \times ... \times n$. On écrit alors

$$2^{n!} = (2^{\phi(n)})^{1\times...\times(\phi(n)-1)\times(\phi(n)+1)\times...\times n} = 1[n]$$

Conclusion $2^{n!} - 1 = 0[n]$.

Exercice. (1) : Soit p un nombre premier. Montrer que

$$(p-1)! = -1[p].$$

Solution. On regarde $\{1, 2, \cdots, p-1\}$ et on les regroupent par paire (x, x^{-1}). (Remarquer qu'on a $(x^{-1})^{-1} = x$ et que si $x^{-1} = y^{-1}$ alors $xx^{-1} = xy^{-1}$ Donc $xy^{-1} = 1$ donc $xy^{-1}y = y$ donc $x = y$.) Quels éléments restent seuls ? C'est à dire peut-on avoir $x^{-1} = x$. Oui par exemple $x = 1$ et $x = (p-1) = -1[p]$. Question : Est ce les seuls ? Il faut résoudre

$$x^2 = 1[p] \Rightarrow x^2 - 1 = 0[p] \Rightarrow (x-1)(x+1) = 0[p].$$

Et donc$p|(x-1)(x+1)$. Puisque p est un nombre premier alors $p|(x+1)$ ou $p|(x-1)$ et donc $x = 1$ ou $x = p-1$. On a alors

$$(p-1)! = 1 \times \prod_{\text{paires}} (x \times x^{-1}) \times (p-1) = p - 1 = -1[p].$$

Exercice. (2) : Soit n premier avec 10. Montrer qu'il existe un multiple de n qui s'écrit qu'avec des 1.

Solution. On écrit tous les nombres $1, 11, 111, \cdots$ par principe des tiroirs comme il y a ici une infinité d'éléments il en existe 2 qui ont le même modulo

$$1...1_{(k)} = 1...1_{(k')}[n]$$

Donc

$$1...1_{(k-k')}0...0_{k'} = 0[n]$$

Donc $n|1...1_{(k-k')}0...0_k$. On a aussi que n est premier avec 10 donc premier avec 10^k. Par le Lemme de Gauss on a alors $n|1....1_{(k-k')}$.

Deuxième preuve : On écrit

$$1....1_k = 1 + 10 + 10^2 + \cdots + 10^{k-1} = \frac{10^k - 1}{9}$$

On prend alors k tel que $10^k = 1[n]$ et donc $n|10^k - 1$. On a alors $n|1....1_k \times 9$.

L'astuce est alors d'utiliser $1...1_{9k} = 1...1_k \times (10000010000001...1)$ et $9|(10000010000001...1)$ et donc $n|1...1_{9k}$.

Exercice. (3) : Soit $p > 3$ un nombre premier. Montrer qu'il existe n tel que p divise

$$2^n + 3^n + 6^n - 1$$

Idée : On peut utiliser des « Fractions » dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Par exemple avec $2^{-1} = 4[7]$ et $4^{-1} = 2[7]$ on a $2^{-1} - 4^{-1} = 2[7]$. C'est à dire sous forme de fraction

$$\frac{1}{2} - \frac{1}{4} = \frac{1}{4}[7]$$

et c'est la même égalité que pour les « vrai » fractions dans $\mathbb{R}$. En fait ça marche avec tous les premiers p : On a que

$$4 \times (\frac{1}{2} - \frac{1}{4}) = 2 \times 2 \times \frac{1}{2} - 4 \times \frac{1}{4} = 2 - 1 = 1[p]$$

Donc par la définition de $\frac{1}{4}$ on a bien que $\frac{1}{2} - \frac{1}{4} = \frac{1}{4}$. En fait toutes les opérations sur les fractions dans $\mathbb{R}$ fonctions fonctionne de la même manière dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Autre exemple pour a, b premier avec p :

$$\frac{1}{a} + \frac{1}{b} = (a+b)\frac{1}{ab}[p]$$

On peut vérifier

$$ab(\frac{1}{a} + \frac{1}{b}) = b \times a \times \frac{1}{a} + a \times b \times \frac{1}{b} = b + a[p]$$

Solution. Ici l'astuce est de remarquer que $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 = 0$. On pose alors $n = p - 2$. Par le petit théorème de Fermat $6^{p-1} = 3^{p-1} = 2^{p-1} = 1[p]$ et donc

$$2^{p-2} + 3^{p-2} + 6^{p-2} - 1 = 2^{p-1} \times \frac{1}{2} + 3^{p-1} \times \frac{1}{3} + 6^{p-1} \times \frac{1}{6} - 1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 = 0[p].$$

Exercice. (13) : Si $p | b^{2^n} + 1$ alors $p = m2^{n+1} + 1$.

Solution. $b^{2^n} = -1[p]$ Donc $(b^{2^n})^2 = b^{2^{n+1}} = 1[p]$. Donc $o(b) | 2^{n+1}$. Puisque 2 est le seul facteur premier possible on a $o(b) = 2^l$ avec $l \leq n + 1$. Si $l < n + 1$ alors $b^{2^n} = (b^{2^l})^{\cdots} = 1 \neq -1[p]$ absurde. Donc $o(b) = 2^{n+1}$.

Par le petit théorème de Fermat $o(b) | p-1$. Donc $p-1 = m \times o(b) = m \times 2^{n+1}$. Et donc $p = m2^{n+1} + 1$.