TD d'arithmétique groupe C : ordre modulaire et petit théorème de Fermat

Aline Cahuzac

samedi 6 janvier 2024

Exercice 1 Soit $n \in \mathbb{N}$. Montrer que $(n-1)! \equiv -1[n]$ si et seulement si n est premier.

Solution de l'exercice 1 *On distingue quatre cas possible pour la décomposition de n en facteurs premiers.*

$n = pq$, **avec** *$p < q < n$ Dans ce cas*

$$(n-1)! = 1 \cdot 2 \dots p \dots q \dots (n-1)$$

est un multiple de n, donc pas congru à -1 modulo n.

$n = p^2$, $p \geqslant 3$ Dans ce cas,

$$(n-1)! = 1 \cdot 2 \dots p \dots 2p \dots (n-1)$$

est un multiple de $2n$ donc en particulier de n, donc n'est pas congru à -1 modulo n.

$n = 4$ On calcule directement

$$(n-1)! = 3! = 6 \not\equiv -1[n = 4]$$

n **premier** *Dans ce cas on regroupe les éléments de $\mathbb{Z}/n\mathbb{Z}$, notés $\{1, \dots, n-1\}$, par paires de la forme $\{a, a^{-1}\}$. Le seul élement qui est son propre inverse st $n - 1 \equiv -1$ (en exercice pour le lecteur : vérifier ce point), donc on a bien*

$$(n-1)! \equiv 1 \cdot 1 \dots 1 \cdot (n-1) \equiv -1[n]$$

Exercice 2 A quelle condition un entier $n \in \mathbb{N}$ possède-t-il un multiple qui ne s'écrit qu'avec des 1 ?

Solution de l'exercice 2

analyse *supposons que n vérifie la propriété de l'énoncé et écrivons donc*

$$m \cdot n = 11 \dots 11 = \frac{10^k - 1}{9}$$

pour des entiers k, m. On voit immédiatement que n ne peut pas être un multiple de 2 ou de 5, donc n est premier avec 10.

synthèse *soit donc n premier avec 10. 10 est inversible modulo $9n$, donc avec*

$$k = \omega_{9n}(10)$$

on obtient $9n \mid 10^k - 1$, de sorte que $\frac{10^k-1}{9}$ soit un multiple de n qui ne s'écrit qu'avec des 1.

Exercice 3 Soit p un nombre premier et d un diviseur de $p-1$. Calculer, modulo p, le produit des éléments de $\mathbb{Z}/p\mathbb{Z}$ dont l'ordre est exactement égal à d.

Solution de l'exercice 3 *Remarquons que $\omega_p(a) = \omega_p(a^{-1})$: autrement dit, un élement et son inverse ont toujours le même ordre. Alors on distingue deux cas :*

$d \neq 2$ Dans ce cas, tous les élements vérifiant $\omega_p(a) = d$ vérifient aussi $a \neq a^{-1}$. Les éléments vont par paire élément-inverse dans le produit :

$$\prod_{\omega_p(a)=d} = 1 \cdot 1 \dots 1 = 1$$

$d = 2$ Dans ce cas, les éléments vont tous par paire, sauf -1 et le produit devient :

$$\prod_{\omega_p(a)=d} = 1 \cdot 1 \cdots -1 = -1$$

Exercice 4 Trouver les entiers $(n, m) \in \mathbb{N}$ tels que

$$m^{20} + 11^n$$

soit un carré parfait.

Solution de l'exercice 4 *On suppose l'énoncé vérifié et on écrit $m^{20} + 11^n = a^2$, soit $11^n = (a + m^{10})(a - m^{10})$ pour $a \in \mathbb{N}$. En faisant la différence des deux termes, on obtient qu'il existe des entiers $\alpha < \beta$ tels que $\alpha + \beta = n$ et*

$$2m^{10} = 11^\alpha - 11^\beta = 11^\beta(11^{\alpha-\beta} - 1)$$

On distingue alors deux cas :

$\beta = 0$ Dans ce cas $2m^{10} = 11^\alpha - 1$. Mais d'après le petit théorème de Fermat, m^{10} est congru à 0 ou 1 modulo 11. Le seul cas possible est $\alpha = 0$, ce qui donne $n = 0$. Il n'y a alors pas de solution (impossible de trouver deux carrés consécutifs non nuls).

$\beta > 0$ Dans ce cas, on écrit $m = 11^u \cdot \ell$ pour $u, \ell \in \mathbb{N}$ avec $\ell \wedge 11 = 1$ (on met à part la puissance de 11 dans la décomposition de m en facteurs premiers). Nécéssairement, $\beta = 10u$ et $2\ell^1 0 = 11^{\alpha-\beta} - 1$, mais toute puissance de ℓ est congrue à 1 modulo 11 donc il n'y a pas de solution de cette forme hormis $\ell = 0$ et $\alpha = \beta$.

En conclusion, les solutions sont les couples $(2n, 0)$ avec $n \in \mathbb{N}$ quelconque.

Exercice 5
Soit p premier. Montrer qu'on peut trouver un diviseur premier ℓ de $p^p - 1$ tel que $l \equiv 1[p]$.

Solution de l'exercice 5
On remarque que $p^p \equiv 1[\ell] \Rightarrow \omega_\ell(p)|p$. On distingue deux cas :

$\omega_\ell(p) = p$ Dans ce cas $p|\varphi(\ell) = \ell - 1$ et $\ell \equiv 1[p]$ comme on veut.

$\omega_\ell(p) = 1$ Dans ce cas $\ell|p - 1$. Or

$$p^p - 1 = (p-1)(p^{p-1} + \cdots + 1) = (p-1)K$$

pour un entier $K \in \mathbb{N}$. Il reste à montrer que K a des diviseurs premiers qui ne divisent pas $p - 1$.

On écrit donc

$$\begin{aligned} K = \sum_{k=0}^{p-1} p^k &= 1 + \sum_{k=1}^{p-1}(p^k - 1) + (p-1) \\ &= p + \sum_{k=1}^{p-1}(p-1)\sum_{j=0}^{k-1} p^j \\ &\equiv p \equiv 1[p-1] \end{aligned}$$

En particulier, $K \wedge (p-1) = 1$, donc on a même le résultat plus fort que tous les diviseurs premiers de K ne divisent pas $p - 1$, et il suffit de prendre ℓ diviseur premier de K.

Exercice 6
Soit $n_1, \ldots, n_k \in \mathbb{N}^*$ tels que $n_{i+1}|2^{n_i} - 1$ pour $1 \leqslant i \leqslant k$ (avec $n_0 = n_k$). Montrer que $n_1 = \cdots = n_k = 1$.

Solution de l'exercice 6 *:*
Si un des n_i vaut 1, tous les autres aussi.

Sinon, on note p_i le plus petit diviseur premier de n_i. On a $p_i|2^{n_{i-1}} - 1$, donc $\omega_{p_i}(2)|(p_i - 1) \wedge n_{n-1}$. Si l'ordre n'est pas 1 (cas impossible), alors il y a un facteur premier de n_{i-1} qui divise aussi $p_i - 1$. En particulier :

$$p_1 < p_2 < \cdots < p_k < p_1$$

C'est absurde.