Quelques propriétés de $\mathbb{Z}/n\mathbb{Z}^*$

Ordre modulaire et petit théorème de Fermat

Aline

Samedi 6 janvier 2024

Rappels d'arithmétique modulaire

Définition

Soit $n \in \mathbb{Z}^*$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des **classes d'équivalences modulo** n, autrement dit l'ensemble des restes possibles de division euclidienne modulo n. On note aussi $\overline{a}$ la classe de l'entier a (lorsqu'il n'y a pas d'ambigüité).

Rappels d'arithmétique modulaire

Définition

Soit $n \in \mathbb{Z}^*$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des **classes d'équivalences modulo** n, autrement dit l'ensemble des restes possibles de division euclidienne modulo n. On note aussi $\overline{a}$ la classe de l'entier a (lorsqu'il n'y a pas d'ambigüité).

Restes possibles : $0, 1, \ldots n-1 \Rightarrow |\mathbb{Z}/n\mathbb{Z}| = n$.

Rappels d'arithmétique modulaire

Définition

Soit $n \in \mathbb{Z}^*$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des **classes d'équivalences modulo** n, autrement dit l'ensemble des restes possibles de division euclidienne modulo n. On note aussi $\overline{a}$ la classe de l'entier a (lorsqu'il n'y a pas d'ambigüité).

Restes possibles : $0, 1, \ldots n-1 \Rightarrow |\mathbb{Z}/n\mathbb{Z}| = n$.
Compatibles avec les opérations $+, -, \times$: $\overline{a} \times \overline{b} = \overline{ab}, \overline{a} + \overline{b} = \overline{a+b}$
Pas de division en général !
Exemple modulo 6 *:* $\overline{3} \cdot \overline{3} = \overline{9} = \overline{3}$ *mais si on simplifie on a "*$\overline{3} = \overline{1}$*", ce qui est faux...*

Inversibles modulo n

Définition

On dit que a est **inversible modulo** n lorsqu'il existe $k \in \mathbb{Z}$, $ak \equiv 1[n]$, autrement dit $\overline{a} \cdot \overline{k} = \overline{1}[n]$. On note $\overline{k} = \overline{a}^{-1}$ et $\mathbb{Z}/n\mathbb{Z}^*$ l'ensemble des classes inversibles modulo n.

Inversibles modulo n

Définition

On dit que a est **inversible modulo** n lorsqu'il existe $k \in \mathbb{Z}$, $ak \equiv 1[n]$, autrement dit $\overline{a} \cdot \overline{k} = \overline{1}[n]$. On note $\overline{k} = \overline{a}^{-1}$ et $\mathbb{Z}/n\mathbb{Z}^*$ l'ensemble des classes inversibles modulo n.

Théorème de Bézout

Soit $a, b \in \mathbb{Z}$. Il existe $u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b = \mathrm{pgcd}(a, b)$. Réciproquement, tous les nombres de la forme $au + bv$ sont des multiples de $a \wedge b$.

Inversibles modulo n

Définition

On dit que a est **inversible modulo** n lorsqu'il existe $k \in \mathbb{Z}$, $ak \equiv 1[n]$, autrement dit $\overline{a} \cdot \overline{k} = \overline{1}[n]$. On note $\overline{k} = \overline{a}^{-1}$ et $\mathbb{Z}/n\mathbb{Z}^*$ l'ensemble des classes inversibles modulo n.

Théorème de Bézout

Soit $a, b \in \mathbb{Z}$. Il existe $u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b = \mathrm{pgcd}(a, b)$. Réciproquement, tous les nombres de la forme $au + bv$ sont des multiples de $a \wedge b$.

Corollaire

a inversible modulo $n \Leftrightarrow a \wedge b = 1$

Inversibles modulo n

Définition

On dit que a est **inversible modulo** n lorsqu'il existe $k \in \mathbb{Z}$, $ak \equiv 1[n]$, autrement dit $\overline{a} \cdot \overline{k} = \overline{1}[n]$. On note $\overline{k} = \overline{a}^{-1}$ et $\mathbb{Z}/n\mathbb{Z}^*$ l'ensemble des classes inversibles modulo n.

Théorème de Bézout

Soit $a, b \in \mathbb{Z}$. Il existe $u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b = \mathrm{pgcd}(a, b)$. Réciproquement, tous les nombres de la forme $au + bv$ sont des multiples de $a \wedge b$.

Corollaire

a inversible modulo $n \Leftrightarrow a \wedge b = 1$

Preuve : si $au + bn = 1$, $au \equiv 1[n]$. Réciproquement si a inversible, alors $\exists k, m$ tel que $ak + mn = 1$ et $a \wedge n | 1$.

Exercice 1

Théorème de Wilson

$$(n-1)! \equiv -1[n] \Leftrightarrow n \text{ est premier}$$

Exercice 1

Théorème de Wilson

$$(n-1)! \equiv -1[n] \Leftrightarrow n \text{ est premier}$$

Solution :

$n = pq,\ p < q < n$ $(n-1)! = 1 \cdot 2 \ldots p \ldots q \ldots (n-1)$ multiple de n.

$n = p^2,\ p \geqslant 3$ $(n-1)! = 1 \cdot 2 \ldots p \ldots 2p \ldots (n-1)$ multiple de $2n$ donc de n.

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

n premier on regroupe tous les éléments de $\{1, \ldots, n-1\}$ par paire $\{a, a^{-1}\}$. Le seul élément qui est son propre inverse est $n - 1 \equiv -1$:

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

Opérations dans $\mathbb{Z}/n\mathbb{Z}^*$

- En général, a et b inversibles $\not\Rightarrow$ $a+b$ inversible. **Pas d'addition**.

Opérations dans $\mathbb{Z}/n\mathbb{Z}^*$

- En général, a et b inversibles $\not\Rightarrow$ $a+b$ inversible. **Pas d'addition**.
- En revanche (Lemme de Gauss) a, b inversibles $\Rightarrow$ ab inversible : on peut faire de la **multiplication** dans $\mathbb{Z}/n\mathbb{Z}^*$.

Opérations dans $\mathbb{Z}/n\mathbb{Z}^*$

- En général, a et b inversibles $\not\Rightarrow$ $a+b$ inversible. **Pas d'addition**.
- En revanche (Lemme de Gauss) a, b inversibles $\Rightarrow$ ab inversible : on peut faire de la **multiplication** dans $\mathbb{Z}/n\mathbb{Z}^*$.
- On peut faire de la **simplification** en multipliant par l'inverse :

$$\overline{a}\overline{b} = \overline{ac} \Rightarrow \overline{a}^{-1}\overline{a}\overline{b} = \overline{a}^{-1}\overline{ac} \Rightarrow \overline{b} = \overline{c}$$

La division n'est pas une vraie opération, ce qui existe c'est la multiplication par l'inverse. Il faut juste s'assurer que l'inverse existe bien !

Cardinal de $\mathbb{Z}/n\mathbb{Z}^*$

Définition

La **fonction indicatrice d'Euler** est définie sur $\mathbb{Z}$ par

$$\varphi(n) = |\mathbb{Z}/n\mathbb{Z}^*|$$

Cardinal de $\mathbb{Z}/n\mathbb{Z}^*$

Définition

La **fonction indicatrice d'Euler** est définie sur $\mathbb{Z}$ par

$$\varphi(n) = |\mathbb{Z}/n\mathbb{Z}^*|$$

- $\varphi(p) = p - 1$ car $\mathbb{Z}/p\mathbb{Z}^* = \{1, 2, \ldots, p-1\}$
- $\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$ car $\mathbb{Z}/p^k\mathbb{Z}^* = \{1, \ldots, p^k\} \setminus \{\text{multiples de } p\}$ (et p^{k-1} multiples de p entre 1 et p^k).

Multiplicativité de φ

Lemme

Si n et m sont premiers entre eux, alors $\varphi(nm) = \varphi(n)\varphi(m)$. On dit que φ est **multiplicative**.

Multiplicativité de φ

Lemme

Si n et m sont premiers entre eux, alors $\varphi(nm) = \varphi(n)\varphi(m)$. On dit que φ est **multiplicative**.

Preuve : on regarde les nombre de la forme $an + bm[nm]$.

Multiplicativité de φ

Lemme

Si n et m sont premiers entre eux, alors $\varphi(nm) = \varphi(n)\varphi(m)$. On dit que φ est **multiplicative**.

Preuve : on regarde les nombre de la forme $an + bm[nm]$.

- Bézout : on trouve $a_0 n + b_0 m = 1$. Donc tout $k \in \mathbb{Z}/nm\mathbb{Z}^*$ peut s'écrire $ka_0 n + kb_0 m$.

Multiplicativité de φ

Lemme

Si n et m sont premiers entre eux, alors $\varphi(nm) = \varphi(n)\varphi(m)$. On dit que φ est **multiplicative**.

Preuve : on regarde les nombre de la forme $an + bm[nm]$.

- Bézout : on trouve $a_0 n + b_0 m = 1$. Donc tout $k \in \mathbb{Z}/nm\mathbb{Z}^*$ peut s'écrire $ka_0 n + kb_0 m$.
- Gauss : ka_0 premier avec m, kb_0 premier avec n.
- $\varphi(m)$ choix pour $a = ka_0$ et $\varphi(n)$ choix pour $b = kb_0$:

$$\begin{aligned} an + bm \equiv a'n + b'm[nm] &\Leftrightarrow (a - a')n \equiv (b' - b)m[nm] \\ &\Leftrightarrow nm|(a - a')n + (b - b')m \\ &\Leftrightarrow a \equiv a'[m] \text{ et } b \equiv b'[n] \end{aligned}$$

Formule explicite de φ

Proposition

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

Formule explicite de φ

Proposition

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

Preuve : on écrit $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$.

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{\alpha_1}) \dots \varphi(p_1^{\alpha_1}) \\
&= (p_1 - 1)p_1^{\alpha_1 - 1} \dots (p_k - 1)p_k^{\alpha_k - 1} \\
&= \left(1 - \frac{1}{p_1}\right) p_1^{\alpha_1} \dots \left(1 - \frac{1}{p_k}\right) p_k^{\alpha_k}
\end{aligned}$$

Un résultat utile

Proposition

$$n = \sum_{d|n} \varphi(d)$$

Un résultat utile

Proposition

$$n = \sum_{d|n} \varphi(d)$$

Preuve : Si $n = p^k$, c'est vrai :

$$\sum_{d|p^k} \varphi(d) = \sum_{j=0}^{k} \varphi(p^j) = \varphi(1) + \sum_{j=1}^{k} (p^j - p^{j-1}) = 1 + p^k - 1$$

Si c'est vrai pour n, alors si $p \not| n$:

$$\sum_{d|np^k} \varphi(d) = \sum_{d|n} \sum_{d'|p^k} \varphi(dd') = \sum_{d|n} \sum_{d'|p^k} \varphi(d)\varphi(d') \quad \text{car } d \wedge d' = 1$$

$$= \sum_{d|n} \varphi(d) \sum_{d'|p^k} \varphi(d') = np^k$$

Puissances d'un élément

Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}^*$.

Définition

Pour $k \in \mathbb{Z}$, on définit

$$\overline{a}^k = \begin{cases} \overline{a^k} & \text{si } k \geqslant 1 \\ \overline{1} & \text{si } k = 0 \\ (\overline{a}^{-1})^{-k} & \text{si } k < 0 \end{cases}$$

Puissances d'un élément

Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}^*$.

Définition

Pour $k \in \mathbb{Z}$, on définit

$$\overline{a}^k = \begin{cases} \overline{a^k} & \text{si } k \geqslant 1 \\ \overline{1} & \text{si } k = 0 \\ (\overline{a}^{-1})^{-k} & \text{si } k < 0 \end{cases}$$

- La suite $\overline{a}, \overline{a}^2, \ldots, \overline{a}^k, \ldots$ est à valeurs dans $\mathbb{Z}/n\mathbb{Z}^*$

Puissances d'un élément

Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}^*$.

Définition

Pour $k \in \mathbb{Z}$, on définit

$$\overline{a}^k = \begin{cases} \overline{a^k} & \text{si } k \geqslant 1 \\ \overline{1} & \text{si } k = 0 \\ (\overline{a}^{-1})^{-k} & \text{si } k < 0 \end{cases}$$

- La suite $\overline{a}, \overline{a}^2, \ldots, \overline{a}^k, \ldots$ est à valeurs dans $\mathbb{Z}/n\mathbb{Z}^*$

$\Rightarrow$ nombre **fini** de valeurs (au plus $\varphi(n)$)

Puissances d'un élément

Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}^*$.

Définition

Pour $k \in \mathbb{Z}$, on définit

$$\overline{a}^k = \begin{cases} \overline{a^k} & \text{si } k \geqslant 1 \\ \overline{1} & \text{si } k = 0 \\ (\overline{a}^{-1})^{-k} & \text{si } k < 0 \end{cases}$$

- La suite $\overline{a}, \overline{a}^2, \ldots, \overline{a}^k, \ldots$ est à valeurs dans $\mathbb{Z}/n\mathbb{Z}^*$

$\Rightarrow$ nombre **fini** de valeurs (au plus $\varphi(n)$)

$\Rightarrow$ $\exists k < l$, $\overline{a}^k = \overline{a}^l$ ie $\overline{a}^{l-k} = \overline{1}$

Puissances d'un élément

Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}^*$.

Définition

Pour $k \in \mathbb{Z}$, on définit

$$\overline{a}^k = \begin{cases} \overline{a^k} & \text{si } k \geqslant 1 \\ \overline{1} & \text{si } k = 0 \\ (\overline{a}^{-1})^{-k} & \text{si } k < 0 \end{cases}$$

- La suite $\overline{a}, \overline{a}^2, \ldots, \overline{a}^k, \ldots$ est à valeurs dans $\mathbb{Z}/n\mathbb{Z}^*$

$\Rightarrow$ nombre **fini** de valeurs (au plus $\varphi(n)$)

$\Rightarrow$ $\exists k < l$, $\overline{a}^k = \overline{a}^l$ ie $\overline{a}^{l-k} = \overline{1}$

$\Rightarrow$ suite **périodique** dont $(l-k)$ est *une* période

Ordre de a modulo n

Définition

On appelle **ordre de a modulo n** et on note $\omega_n(a)$ la plus petite période de $\{\overline{a}^k\}_{k\in\mathbb{Z}}$ ie le plus petit entier $k \geqslant 1$ tel que $\overline{a}^k = \overline{1}$.

Ordre de a modulo n

Définition

On appelle **ordre de a modulo n** et on note $\omega_n(a)$ la plus petite période de $\{\overline{a}^k\}_{k\in\mathbb{Z}}$ ie le plus petit entier $k \geqslant 1$ tel que $\overline{a}^k = \overline{1}$.

- $\omega_n(a)$ n'existe que si a est inversible modulo n.

Ordre de a modulo n

Définition

On appelle **ordre de a modulo n** et on note $\omega_n(a)$ la plus petite période de $\{\overline{a}^k\}_{k\in\mathbb{Z}}$ ie le plus petit entier $k \geqslant 1$ tel que $\overline{a}^k = \overline{1}$.

- $\omega_n(a)$ n'existe que si a est inversible modulo n.
- $\omega_n(a) \leqslant \varphi(n)$ puisque la suite peut prendre au plus $\varphi(n)$ valeurs avant de se répéter.

Ordre de a modulo n

Définition

On appelle **ordre de a modulo n** et on note $\omega_n(a)$ la plus petite période de $\{\overline{a}^k\}_{k\in\mathbb{Z}}$ ie le plus petit entier $k \geqslant 1$ tel que $\overline{a}^k = \overline{1}$.

- $\omega_n(a)$ n'existe que si a est inversible modulo n.
- $\omega_n(a) \leqslant \varphi(n)$ puisque la suite peut prendre au plus $\varphi(n)$ valeurs avant de se répéter.
- *Exemple dans* $\mathbb{Z}/11\mathbb{Z}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ *:*

a	1	2	3	4	5	6	7	8	9	10
$\omega_{11}(a)$										

Ordre de a modulo n

Définition

On appelle **ordre de a modulo n** et on note $\omega_n(a)$ la plus petite période de $\{\overline{a}^k\}_{k\in\mathbb{Z}}$ ie le plus petit entier $k \geqslant 1$ tel que $\overline{a}^k = \overline{1}$.

- $\omega_n(a)$ n'existe que si a est inversible modulo n.
- $\omega_n(a) \leqslant \varphi(n)$ puisque la suite peut prendre au plus $\varphi(n)$ valeurs avant de se répéter.
- *Exemple dans* $\mathbb{Z}/11\mathbb{Z}^* = \{1,2,3,4,5,6,7,8,9,10\}$ *:*

a	1	2	3	4	5	6	7	8	9	10
$\omega_{11}(a)$	1	10	5	5	5	10	10	10	5	2

Ordre de a modulo n

Définition

On appelle **ordre de a modulo n** et on note $\omega_n(a)$ la plus petite période de $\{\overline{a}^k\}_{k\in\mathbb{Z}}$ ie le plus petit entier $k \geqslant 1$ tel que $\overline{a}^k = \overline{1}$.

- $\omega_n(a)$ n'existe que si a est inversible modulo n.
- $\omega_n(a) \leqslant \varphi(n)$ puisque la suite peut prendre au plus $\varphi(n)$ valeurs avant de se répéter.
- *Exemple dans* $\mathbb{Z}/11\mathbb{Z}^* = \{1,2,3,4,5,6,7,8,9,10\}$ *:*

a	1	2	3	4	5	6	7	8	9	10
$\omega_{11}(a)$	1	10	5	5	5	10	10	10	5	2

- *Exemple dans* $\mathbb{Z}/15\mathbb{Z}^* = \{1,2,4,7,8,11,13,14\}$ *:*

a	1	2	4	7	8	11	13	14
$\omega_{15}(a)$								

Ordre de a modulo n

Définition

On appelle **ordre de a modulo n** et on note $\omega_n(a)$ la plus petite période de $\{\overline{a}^k\}_{k\in\mathbb{Z}}$ ie le plus petit entier $k \geqslant 1$ tel que $\overline{a}^k = \overline{1}$.

- $\omega_n(a)$ n'existe que si a est inversible modulo n.
- $\omega_n(a) \leqslant \varphi(n)$ puisque la suite peut prendre au plus $\varphi(n)$ valeurs avant de se répéter.
- *Exemple dans* $\mathbb{Z}/11\mathbb{Z}^* = \{1,2,3,4,5,6,7,8,9,10\}$ *:*

a	1	2	3	4	5	6	7	8	9	10
$\omega_{11}(a)$	1	10	5	5	5	10	10	10	5	2

- *Exemple dans* $\mathbb{Z}/15\mathbb{Z}^* = \{1,2,4,7,8,11,13,14\}$ *:*

a	1	2	4	7	8	11	13	14
$\omega_{15}(a)$	1	4	2	4	4	2	4	2

Exercice 2

Exercice

À quelle condition un entier n possède un multiple qui ne s'écrit qu'avec des 1 ?

Exercice 2

Exercice

À quelle condition un entier n possède un multiple qui ne s'écrit qu'avec des 1 ?

$11\ldots1 = \frac{10^k-1}{9}$.

Exercice 2

Exercice

À quelle condition un entier n possède un multiple qui ne s'écrit qu'avec des 1 ?

$11\ldots1 = \frac{10^k-1}{9}$.

cas à exclure $2|n$ ou $5|n$.

Exercice 2

Exercice

À quelle condition un entier n possède un multiple qui ne s'écrit qu'avec des 1 ?

$11\ldots1 = \frac{10^k-1}{9}$.

cas à exclure $2|n$ ou $5|n$.

cas $n \wedge 10 = 1$ 10 inversible modulo $9n$, donc avec $k = \omega_{9n}(10)$, $9n|10^k - 1$ et $\frac{10^k-1}{9}$ est un multiple de n qui ne s'écrit qu'avec des 1.

Propriétés de ω_n

- $\omega_n(a) = 1 \Leftrightarrow \overline{a} = \overline{1}$

Propriétés de ω_n

- $\omega_n(a) = 1 \Leftrightarrow \overline{a} = \overline{1}$
- $\omega_n(-1) = 2$ pour $n \geqslant 3$

Propriétés de ω_n

- $\omega_n(a) = 1 \Leftrightarrow \overline{a} = \overline{1}$
- $\omega_n(-1) = 2$ pour $n \geqslant 3$
- $\omega_n(a^{-1}) = \omega_n(a)$

En général, pas de méthode pour trouver $\omega_n(a)$ à part regarder la suite $\overline{a}, \overline{a}^2, \ldots$.

Propriétés de ω_n

Proposition

1. $a^{\omega_n(a)} \equiv 1[n]$

Propriétés de ω_n

Proposition

1. $a^{\omega_n(a)} \equiv 1[n]$
2. $a^k \equiv 1[n] \Leftrightarrow \omega_n(a) | k$

Propriétés de ω_n

Proposition

1. $a^{\omega_n(a)} \equiv 1[n]$
2. $a^k \equiv 1[n] \Leftrightarrow \omega_n(a) | k$
3. $\omega_n(a^k) = \frac{\omega_n(a)}{k \wedge \omega_n(a)}$

Propriétés de ω_n

Proposition

1. $a^{\omega_n(a)} \equiv 1[n]$
2. $a^k \equiv 1[n] \Leftrightarrow \omega_n(a) | k$
3. $\omega_n(a^k) = \frac{\omega_n(a)}{k \wedge \omega_n(a)}$
4. $\omega_n(ab) | \omega_n(a)\omega_n(b)$

Propriétés de ω_n

Proposition

1. $a^{\omega_n(a)} \equiv 1[n]$
2. $a^k \equiv 1[n] \Leftrightarrow \omega_n(a)|k$
3. $\omega_n(a^k) = \frac{\omega_n(a)}{k \wedge \omega_n(a)}$
4. $\omega_n(ab)|\omega_n(a)\omega_n(b)$
5. Si $\omega_n(a) \wedge \omega_n(b) = 1$, $\omega_n(ab) = \omega_n(a)\omega_n(b)$

Propriétés de ω_n

Proposition

1. $a^{\omega_n(a)} \equiv 1[n]$
2. $a^k \equiv 1[n] \Leftrightarrow \omega_n(a)|k$
3. $\omega_n(a^k) = \frac{\omega_n(a)}{k \wedge \omega_n(a)}$
4. $\omega_n(ab)|\omega_n(a)\omega_n(b)$
5. Si $\omega_n(a) \wedge \omega_n(b) = 1$, $\omega_n(ab) = \omega_n(a)\omega_n(b)$

Propriétés de ω_n

Proposition

1. $a^{\omega_n(a)} \equiv 1[n]$
2. $a^k \equiv 1[n] \Leftrightarrow \omega_n(a)|k$
3. $\omega_n(a^k) = \frac{\omega_n(a)}{k \wedge \omega_n(a)}$
4. $\omega_n(ab)|\omega_n(a)\omega_n(b)$
5. Si $\omega_n(a) \wedge \omega_n(b) = 1$, $\omega_n(ab) = \omega_n(a)\omega_n(b)$

Preuve de (5) :
Si $(ab)^m \equiv 1[n]$, alors $a^m \equiv (b^{-1})^m[n]$ et en particulier,

$$\omega_n(a^m) = \omega_n((b^{-1})^m) = \omega_n(b^m) \quad \text{ie} \quad \frac{\omega_n(a)}{m \wedge \omega_n(a)} = \frac{\omega_n(b)}{m \wedge \omega_n(b)}$$

Mais le premier membre est diviseur de $\omega_n(a)$ et le deuxième de $\omega_n(b)$: c'est nécessairement 1, donc $\omega_n(a)\omega_n(b)|m$.

Liens entre φ et l'ordre

Petit théorème de Fermat

1. Si $a \in \mathbb{Z}/n\mathbb{Z}^*$, $\overline{a}^{\varphi(n)} = \overline{1}$
2. Si p premier, $a^p \equiv a[p]$
3. Si p premier et $a \wedge p = 1$, alors $a^{p-1} \equiv 1[p]$, autrement dit $\omega_p(a) \mid p - 1$

Liens entre φ et l'ordre

Petit théorème de Fermat

1. Si $a \in \mathbb{Z}/n\mathbb{Z}^*$, $\overline{a}^{\varphi(n)} = \overline{1}$
2. Si p premier, $a^p \equiv a[p]$
3. Si p premier et $a \wedge p = 1$, alors $a^{p-1} \equiv 1[p]$, autrement dit $\omega_p(a) \mid p-1$

Le point (1) est la formulation la plus générale. Parfois, on ne donne que la version dans laquelle n est premier et $\varphi(n) = n - 1$.

Exercice 3

Exercice

Soit p un nombre premier et $d \neq 1$ 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.

Exercice 3

Exercice

Soit p un nombre premier et $d \neq 1$ 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 : Remarquons que $\omega_p(a) = \omega_p(a^{-1})$.

$d \neq 2$ $\omega_p(a) = d \Rightarrow a \neq a^{-1}$ donc les éléments vont par paire :

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

$d = 2$ et les éléments vont tous par paire, sauf -1 :

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

Preuve du théorème

En fait, le petit théorème de Fermat est un cas particulier du

Théorème de Lagrange

Dans un groupe fini, l'ordre d'un élément divise l'ordre (le cardinal) du groupe.

Mais on va le prouver sans utiliser explicitement de théorie des groupes.

Preuve du théorème

En fait, le petit théorème de Fermat est un cas particulier du

Théorème de Lagrange

Dans un groupe fini, l'ordre d'un élément divise l'ordre (le cardinal) du groupe.

Mais on va le prouver sans utiliser explicitement de théorie des groupes.

On prend a dans $\mathbb{Z}/n\mathbb{Z}^*$.

- $k \in \mathbb{Z}/n\mathbb{Z}^* \mapsto ak \in \mathbb{Z}/n\mathbb{Z}^*$ est une **bijection**.

Preuve du théorème

En fait, le petit théorème de Fermat est un cas particulier du

Théorème de Lagrange

Dans un groupe fini, l'ordre d'un élément divise l'ordre (le cardinal) du groupe.

Mais on va le prouver sans utiliser explicitement de théorie des groupes.

On prend a dans $\mathbb{Z}/n\mathbb{Z}^*$.

- $k \in \mathbb{Z}/n\mathbb{Z}^* \mapsto ak \in \mathbb{Z}/n\mathbb{Z}^*$ est une **bijection**.
- On peut donc écrire

$$\prod_{k\in\mathbb{Z}/n\mathbb{Z}^*} k \equiv \prod_{k\in\mathbb{Z}/n\mathbb{Z}^*} (ak) \equiv a^{|\mathbb{Z}/n\mathbb{Z}^*|} \prod_{k\in\mathbb{Z}/n\mathbb{Z}^*} k[n]$$

Preuve du théorème

En fait, le petit théorème de Fermat est un cas particulier du

Théorème de Lagrange

Dans un groupe fini, l'ordre d'un élément divise l'ordre (le cardinal) du groupe.

Mais on va le prouver sans utiliser explicitement de théorie des groupes.

On prend a dans $\mathbb{Z}/n\mathbb{Z}^*$.

- $k \in \mathbb{Z}/n\mathbb{Z}^* \mapsto ak \in \mathbb{Z}/n\mathbb{Z}^*$ est une **bijection**.
- On peut donc écrire

$$\prod_{k\in\mathbb{Z}/n\mathbb{Z}^*} k \equiv \prod_{k\in\mathbb{Z}/n\mathbb{Z}^*} (ak) \equiv a^{|\mathbb{Z}/n\mathbb{Z}^*|} \prod_{k\in\mathbb{Z}/n\mathbb{Z}^*} k[n]$$

- Comme le produit est encore un élément inversible modulo n (produit d'inversibles), on peut simplifier : $1 \equiv a^{|\mathbb{Z}/n\mathbb{Z}^*|}[n]$

Exercice 4

Exercice

Trouver les entiers $(n, m) \in \mathbb{N}$ tels que $m^{20} + 11^n$ soit un carré parfait.

Exercice 4

Exercice

Trouver les entiers $(n, m) \in \mathbb{N}$ tels que $m^{20} + 11^n$ soit un carré parfait.

Solution : On écrit $m^{20} + 11^n = a^2$, soit
$11^n = (a + m^{10})(a - m^{10})$ Différence des deux termes :

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

On distingue alors deux cas :

- $\beta = 0$ Dans ce cas $2m^{10} = 11^{\alpha} - 1$. Mais d'après le petit théorème de Fermat, $m^{10} \equiv 0$ ou $1[11]$. Seul cas possible : $\alpha = 0$, puis $n = 0$, puis pas de solution.
- $\beta > 0$ Dans ce cas, $m = 11^u \cdot \ell$ avec $\ell \wedge 11 = 1$. Nécéssairement, $\beta = 10u$ et $2\ell^{10} = 11^{\alpha-\beta} - 1$, mais $\ell^{10} \equiv 1[11]$ donc pas de solution sauf $\ell = \alpha - \beta = 0$.

Conclusion : sont solutions les $(2n, 0)$ avec $n \in \mathbb{N}$ quelconque.

Générateurs

Définition

On appelle **générateur** de $\mathbb{Z}/n\mathbb{Z}^*$ un élément d'ordre maximal $\varphi(n)$, ie tel que la suite $\overline{a}, \overline{a}^2, \ldots$ parcourt tout $\mathbb{Z}/n\mathbb{Z}^*$. Si un tel élément existe, on dit que $\mathbb{Z}/n\mathbb{Z}^*$ est **cyclique**.

Générateurs

Définition

On appelle **générateur** de $\mathbb{Z}/n\mathbb{Z}^*$ un élément d'ordre maximal $\varphi(n)$, ie tel que la suite $\overline{a}, \overline{a}^2, \ldots$ parcourt tout $\mathbb{Z}/n\mathbb{Z}^*$. Si un tel élément existe, on dit que $\mathbb{Z}/n\mathbb{Z}^*$ est **cyclique**.

- $\mathbb{Z}/3\mathbb{Z}^* = 1, 2$ est cyclique de générateur $\overline{2}$.

Générateurs

Définition

On appelle **générateur** de $\mathbb{Z}/n\mathbb{Z}^*$ un élément d'ordre maximal $\varphi(n)$, ie tel que la suite $\overline{a}, \overline{a}^2, \ldots$ parcourt tout $\mathbb{Z}/n\mathbb{Z}^*$. Si un tel élément existe, on dit que $\mathbb{Z}/n\mathbb{Z}^*$ est **cyclique**.

- $\mathbb{Z}/3\mathbb{Z}^* = 1, 2$ est cyclique de générateur $\overline{2}$.
- $\mathbb{Z}/8\mathbb{Z}^* = 1, 3, 5, 7$ n'est pas cyclique puisque tous les éléments sont d'ordre $\leqslant 2$.

Générateurs

Définition

On appelle **générateur** de $\mathbb{Z}/n\mathbb{Z}^*$ un élément d'ordre maximal $\varphi(n)$, ie tel que la suite $\overline{a}, \overline{a}^2, \ldots$ parcourt tout $\mathbb{Z}/n\mathbb{Z}^*$. Si un tel élément existe, on dit que $\mathbb{Z}/n\mathbb{Z}^*$ est **cyclique**.

- $\mathbb{Z}/3\mathbb{Z}^* = 1, 2$ est cyclique de générateur $\overline{2}$.
- $\mathbb{Z}/8\mathbb{Z}^* = 1, 3, 5, 7$ n'est pas cyclique puisque tous les éléments sont d'ordre $\leqslant 2$.
- Si g générateur de $\mathbb{Z}/n\mathbb{Z}^*$, la suite $\{g^k\}_{k\in\mathbb{N}^*}$ parcourt tous les restes modulo n, donc aussi tous les restes modulo d diviseur de n :

  $\mathbb{Z}/n\mathbb{Z}^*$ cyclique $\quad\Rightarrow\quad$ $\mathbb{Z}/d\mathbb{Z}^*$ cyclique pour tout diviseur d de n

Structure de corps et polynômes

En général, dans $\mathbb{Z}/n\mathbb{Z}$, il y a des éléments non inversibles autres que 0. Mais si $n = p$ premier, le seul non-inversible est 0.
$\Rightarrow$ on dit que $\mathbb{Z}/p\mathbb{Z}$ a une structure de **corps** : comme dans $\mathbb{R}$, on a des opérations $+$ et $\times$, tous les élements ont un opposé pour $+$ et un inverse pour $\times$ (sauf 0 le neutre pour $+$).

Structure de corps et polynômes

En général, dans $\mathbb{Z}/n\mathbb{Z}$, il y a des éléments non inversibles autres que 0. Mais si $n = p$ premier, le seul non-inversible est 0.
$\Rightarrow$ on dit que $\mathbb{Z}/p\mathbb{Z}$ a une structure de **corps** : comme dans $\mathbb{R}$, on a des opérations $+$ et $\times$, tous les élements ont un opposé pour $+$ et un inverse pour $\times$ (sauf 0 le neutre pour $+$).

C'est le bon cadre pour définir des **polynômes** : un polynôme sur $\mathbb{Z}/p\mathbb{Z}$ est de la forme

$$\overline{a}_0 + \overline{a}_1 X + \cdots + \overline{a}_{p-2} X^{p-1}$$

puisque $X^p = X$ (Fermat).

Structure de corps et polynômes

En général, dans $\mathbb{Z}/n\mathbb{Z}$, il y a des éléments non inversibles autres que 0. Mais si $n = p$ premier, le seul non-inversible est 0.
$\Rightarrow$ on dit que $\mathbb{Z}/p\mathbb{Z}$ a une structure de **corps** : comme dans $\mathbb{R}$, on a des opérations $+$ et $\times$, tous les élements ont un opposé pour $+$ et un inverse pour $\times$ (sauf 0 le neutre pour $+$).

C'est le bon cadre pour définir des **polynômes** : un polynôme sur $\mathbb{Z}/p\mathbb{Z}$ est de la forme

$$\overline{a}_0 + \overline{a}_1 X + \cdots + \overline{a}_{p-2} X^{p-1}$$

puisque $X^p = X$ (Fermat).

Théorème

Un polynôme de degré n a au plus n racines dans $\mathbb{Z}/p\mathbb{Z}$.

Cyclicité de $\mathbb{Z}/p\mathbb{Z}^*$

Théorème

$\mathbb{Z}/p\mathbb{Z}^*$ est **cyclique**.

Cyclicité de $\mathbb{Z}/p\mathbb{Z}^*$

Théorème

$\mathbb{Z}/p\mathbb{Z}^*$ est **cyclique**.

Preuve :

On peut construire un élément d'ordre m tel que pour tout $a \in \mathbb{Z}/n\mathbb{Z}^*$, $\omega_p(a)|m$ (en utilisant $\omega_p(a) \wedge \omega_p(b) = 1 \Rightarrow \omega_p(ab) = \omega_p(a)\omega_p(b)$, et $\omega_p(a^k) = \frac{\omega_p(a)}{\omega_p(a) \wedge k}$).

Cyclicité de $\mathbb{Z}/p\mathbb{Z}^*$

Théorème

$\mathbb{Z}/p\mathbb{Z}^*$ est **cyclique**.

Preuve :
On peut construire un élément d'ordre m tel que pour tout $a \in \mathbb{Z}/n\mathbb{Z}^*$, $\omega_p(a)|m$ (en utilisant $\omega_p(a) \wedge \omega_p(b) = 1 \Rightarrow \omega_p(ab) = \omega_p(a)\omega_p(b)$, et $\omega_p(a^k) = \frac{\omega_p(a)}{\omega_p(a) \wedge k}$).
Alors $X^m - 1$ s'annule $p-1$ fois dans $\mathbb{Z}/p\mathbb{Z}$. Mais alors $p - 1 \leqslant m$.
On conclut que $m = p - 1$ et qu'il existe un élément d'ordre maximal.

Critère de cyclicité de $\mathbb{Z}/n\mathbb{Z}^*$

Théorème

$\mathbb{Z}/n\mathbb{Z}^*$ est **cyclique** $\Leftrightarrow$ $n = 2, 4, p^k$ ou $2p^k$ avec p premier impair.

Critère de cyclicité de $\mathbb{Z}/n\mathbb{Z}^*$

Théorème

$\mathbb{Z}/n\mathbb{Z}^*$ est **cyclique** $\Leftrightarrow$ $n = 2, 4, p^k$ ou $2p^k$ avec p premier impair.

Preuve (sens direct $\Rightarrow$) :

cas faciles $\mathbb{Z}/2\mathbb{Z}^* = \{1\}, \mathbb{Z}/4\mathbb{Z}^* = \{1, 3\}$

Critère de cyclicité de $\mathbb{Z}/n\mathbb{Z}^*$

Théorème

$\mathbb{Z}/n\mathbb{Z}^*$ est **cyclique** $\Leftrightarrow$ $n = 2, 4, p^k$ ou $2p^k$ avec p premier impair.

Preuve (sens direct $\Rightarrow$) :

cas faciles $\mathbb{Z}/2\mathbb{Z}^* = \{1\}, \mathbb{Z}/4\mathbb{Z}^* = \{1, 3\}$

cas $\mathbb{Z}/8\mathbb{Z}^*$ non cyclique $\Rightarrow$ $\mathbb{Z}/2^{k\geqslant 3}\mathbb{Z}^*$ non cyclique.

Critère de cyclicité de $\mathbb{Z}/n\mathbb{Z}^*$

Théorème

$\mathbb{Z}/n\mathbb{Z}^*$ est **cyclique** $\Leftrightarrow$ $n = 2, 4, p^k$ ou $2p^k$ avec p premier impair.

Preuve (sens direct $\Rightarrow$) :

cas faciles $\mathbb{Z}/2\mathbb{Z}^* = \{1\}, \mathbb{Z}/4\mathbb{Z}^* = \{1, 3\}$

cas $\mathbb{Z}/8\mathbb{Z}^*$ non cyclique $\Rightarrow$ $\mathbb{Z}/2^{k\geqslant 3}\mathbb{Z}^*$ non cyclique.

autres cas à éliminer Si $n = uv$ avec $u \wedge v = 1$, pour tout élément a, $a^{\varphi(u)\vee\varphi(v)} \equiv 1[u]$ et $[v]$, donc le théorème chinois conclut que $a^{\varphi(u)\vee\varphi(v)} \equiv 1[uv]$. Ainsi si $\varphi(u) \wedge \varphi(v) > 1$, l'ordre maximal est $m < \varphi(u)\varphi(v) = \varphi(n)$.

$\Rightarrow$ Comme $\varphi(p^k)$ est pair sauf pour $p = 2$ et $k = 1$, n a au plus un facteur premier impair et $v_2(n) \leqslant 1$ (sauf pour $n = 4$).

Critère de cyclicité de $\mathbb{Z}/n\mathbb{Z}^*$

Théorème

$\mathbb{Z}/n\mathbb{Z}^*$ est **cyclique** $\Leftrightarrow$ $n = 2, 4, p^k$ ou $2p^k$ avec p premier impair.

Preuve (sens réciproque $\Leftarrow$) :
On considère d'abord $n = p^k$. On cherche $\omega_n(a) = p^{k-1}(p-1)$.

élément d'ordre p^{k-1} Par récurrence sur j, on montre que $(1+p)^{p^j} = 1 + \lambda_j p^{j+1}$ avec $\lambda_j \wedge p = 1$. On a donc $(1+p)^{p^{k-1}} \equiv 1[p^k]$ mais $(1+p)^{p^{k-2}} \not\equiv 1[p^k]$.
Comme $\omega_n(p+1) | p^{k-1}$, on en déduit que c'est p^{k-1}

élément d'ordre $p-1$ On prend un générateur g de $\mathbb{Z}/p\mathbb{Z}^*$:
$g^{\omega_n(g)} \equiv 1[p^k] \Rightarrow g^{\omega_n(g)} \equiv 1[p] \Rightarrow (p-1) | \omega_n(g)$.

$\Rightarrow$ on a un élément d'ordre $\varphi(p^k)$.

$n = 2p^k$ Même chose puisque $\varphi(2p^k) = \varphi(p^k)$.

Exercice 5

Exercice

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

Exercice 5

Exercice

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

Solution :

$p^p \equiv 1[\ell] \Rightarrow \omega_\ell(p)|p$. On a deux cas :

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

Exercice 5

Exercice

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

Solution :

$p^p \equiv 1[\ell] \Rightarrow \omega_\ell(p)|p$. On a 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

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

Il reste à montrer que K a des diviseurs premiers qui ne divisent pas $p - 1$.

Exercice 5 (suite)

Exercice

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

Solution (suite) :

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

En particulier, $K \wedge (p-1) = 1$, donc il suffit de prendre ℓ diviseur premier de K.

Exercice 6

Exercice

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 $n_1 = \cdots = n_k = 1$.

Exercice 6

Exercice

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 :
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 (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.