

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

<b>Cours</b>	<b>2</b>
1	Congruences . . . . . 2
1.1	Définition . . . . . 2
1.2	Compatibilité avec les lois . . . . . 2
1.3	Le petit théorème de Fermat . . . . . 2
2	L'anneau $\mathbb{Z}/n\mathbb{Z}$ . . . . . 2
2.1	Complément : ensemble quotient . . . . . 2
2.2	L'ensemble $\mathbb{Z}/n\mathbb{Z}$ . . . . . 2
2.3	Structure d'anneau . . . . . 3
2.4	Calcul dans $\mathbb{Z}/n\mathbb{Z}$ . . . . . 3
3	Inversibles de $\mathbb{Z}/n\mathbb{Z}$ . . . . . 4
4	Le théorème chinois . . . . . 5
4.1	Présentation du problème chinois . . . . . 5
4.2	Structure d'anneau produit . . . . . 5
4.3	À propos de la notation . . . . . 5
4.4	Le théorème chinois . . . . . 6
5	Indicatrice d'Euler . . . . . 6
6	Annexes . . . . . 7
6.1	Démonstrations du petit théorème de Fermat . . . . . 7
<b>Exercices</b>	<b>8</b>
	Exercices du CCINP . . . . . 8
	Exercices de calcul . . . . . 8
	Exercices . . . . . 8
	Petits problèmes d'entraînement . . . . . 9

## 1 Congruences

### 1.1 Définition

**Définition.** Soit  $n \in \mathbb{N}^*$ . Pour  $a, b \in \mathbb{Z}$ , on dit que  $a$  est congru à  $b$  modulo  $n$  si et seulement si  $n \mid b - a$ .  
On note  $a \equiv b [n]$  ou parfois  $a \equiv b \pmod{n}$ .

**Proposition.** La relation de congruence modulo  $n$  est un relation d'équivalence sur  $\mathbb{Z}$ .

### 1.2 Compatibilité avec les lois

**Proposition.** Soit  $n \in \mathbb{N}^*$ ,  $a, b, c, d \in \mathbb{Z}$ . On a alors :

$$\left. \begin{array}{l} a \equiv b [n] \\ c \equiv d [n] \end{array} \right\} \implies a + c \equiv b + d [n]$$

$$\left. \begin{array}{l} a \equiv b [n] \\ c \equiv d [n] \end{array} \right\} \implies ac \equiv bd [n]$$

**Corollaire.** Si  $a \equiv b [n]$ , alors pour tout  $k \in \mathbb{N}$ ,  $a^k \equiv b^k [n]$ .

**Exemple.** Justifier le critère de divisibilité par 3 : la somme des chiffres dans l'écriture en base 10 est divisible par 3.

### 1.3 Le petit théorème de Fermat

**Petit théorème de Fermat.**

Soit  $p$  un nombre premier,  $a$  un entier non multiple de  $p$ . Alors :

$$a^{p-1} \equiv 1 [p]$$

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

### 2.1 Complément : ensemble quotient

**Définition.** Soit  $X$  un ensemble et  $\mathcal{R}$  une relation d'équivalence sur  $X$ . Pour  $x \in X$ , on appelle **classe d'équivalence de  $x$  pour la relation  $\mathcal{R}$** , et on note  $\bar{x}$ , l'ensemble des éléments  $y \in X$  tels que  $y\mathcal{R}x$  :

$$y \in \bar{x} \iff y\mathcal{R}x$$

**Proposition.** Si  $y \in \bar{x}$ , alors  $\bar{y} = \bar{x}$ . On dit que  $y$  est un **représentant de la classe d'équivalence  $\bar{x}$** .

**Proposition.** Les classes d'équivalences pour  $\mathcal{R}$  forment une partition de  $X$  : elles sont non vides, deux à deux disjointes et leur réunion est  $X$ .

### 2.2 L'ensemble $\mathbb{Z}/n\mathbb{Z}$

**Définition.** Soit  $n \geq 2$ . On note  $\mathbb{Z}/n\mathbb{Z}$  l'ensemble quotient de  $\mathbb{Z}$  par la relation de congruence modulo  $n$ .

**Exemple.** Pour  $n = 2$ , on a :

$$\mathbb{Z}/2\mathbb{Z} = \{I, P\} = \{\bar{0}, \bar{1}\}$$

**Proposition.** Soit  $n \geq 2$ . L'ensemble  $\mathbb{Z}/n\mathbb{Z}$  est un ensemble à  $n$  éléments, que l'on peut décrire ainsi :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

**Remarque.** La description donnée ci-dessus n'est pas la seule possible. Ainsi :

$$\begin{aligned} \mathbb{Z}/7\mathbb{Z} &= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\} \\ &= \{\overline{-3}, \overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}, \overline{3}\} \end{aligned}$$

## 2.3 Structure d'anneau

**Rappel.** Pour  $n \geq 2$ , il existe une unique loi de groupe sur  $\mathbb{Z}/n\mathbb{Z}$ , encore notée  $+$ , pour laquelle l'application  $k \mapsto \overline{k}$  soit un morphisme de groupes, i.e. :

$$\forall a, b \in \mathbb{Z}, \overline{a+b} = \overline{a} + \overline{b}$$

**Remarque.** Si l'on considère  $x, y \in \mathbb{Z}/n\mathbb{Z}$  et que l'on veut parler de  $x + y$ , on envisage donc  $a, b \in \mathbb{Z}$  qui sont des représentants des classes d'équivalence  $x$  et  $y$  :  $\overline{a} = x$  et  $\overline{b} = y$ . Alors :

$$x + y = \overline{a+b}$$

**Proposition.** Pour  $n \geq 2$ , il existe une unique loi interne sur  $\mathbb{Z}/n\mathbb{Z}$ , notée  $\times$ , pour laquelle l'application :

$$\begin{aligned} \mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \text{ vérifie :} \\ k &\mapsto \overline{k} \end{aligned}$$

$$\forall a, b \in \mathbb{Z}, \overline{a \times b} = \overline{a} \times \overline{b}$$

Alors  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un anneau commutatif, dont l'unité est  $\overline{1}$ .

**Exemple.** Dresser la table d'addition de  $\mathbb{Z}/5\mathbb{Z}$ .

Dresser la table de multiplication de  $\mathbb{Z}/5\mathbb{Z}$ , de  $\mathbb{Z}/6\mathbb{Z}$ .

**Remarque.** Notons bien que :

$$\begin{aligned} \mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ k &\mapsto \overline{k} \end{aligned}$$

est un morphisme surjectif de l'anneau  $(\mathbb{Z}, +, \times)$  sur l'anneau  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ .

## 2.4 Calcul dans $\mathbb{Z}/n\mathbb{Z}$

**Remarque.** On travaille dans  $\mathbb{Z}/n\mathbb{Z}$ , où  $n \geq 2$ .

Pour  $k, a \in \mathbb{Z}$ , que représentent :

$$k\overline{a}, \overline{ka} \text{ et } \overline{k}\overline{a}$$

**Exemple.** Est-ce que l'écriture suivante, dans  $\mathbb{Z}/17\mathbb{Z}$ , a du sens ?

$$\overline{15} \times (\overline{3})^{-1} = \overline{5}$$

**Remarque.** On évite de dire : « soit  $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$  », mais plutôt : « soit  $x \in \mathbb{Z}/n\mathbb{Z}$  et  $a$  un représentant de  $x$ , c'est-à-dire tel que  $x = \overline{a}$  ».

En particulier, si on définit :

$$f : \mathbb{Z}/n\mathbb{Z} \rightarrow \dots$$

on peut vouloir écrire  $\overline{a} \mapsto f(a)$ , c'est-à-dire définir  $f(x)$  en utilisant un représentant de  $x$ . Mais il faut bien justifier qu'alors, la définition est indépendante du choix du représentant :

$$\overline{a} = \overline{b} \implies f(a) = f(b)$$

**Exemple.** Résoudre, dans  $\mathbb{Z}/11\mathbb{Z}$ , l'équation :

$$x^2 - \bar{6}x + \bar{5} = \bar{0}$$

**Exemple.** Résoudre, dans  $\mathbb{Z}/31\mathbb{Z}$ , l'équation :

$$x^2 - \bar{11}x - \bar{1} = \bar{0}$$

**Exemple.** Discuter, suivant les valeurs de  $a \in \mathbb{Z}/13\mathbb{Z}$ , le nombre de solutions de l'équation :

$$x^2 + x + a = \bar{0}$$

**Proposition.** Pour  $p$  premier, calculer  $\text{Card}(A)$  où :

$$A = \{x^2, x \in (\mathbb{Z}/p\mathbb{Z})^*\}$$

### 3 Inversibles de $\mathbb{Z}/n\mathbb{Z}$

**Théorème.**

Soit  $n$  entier,  $n \geq 2$ . Les éléments inversibles de  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  sont les classes  $\bar{k}$  où  $k \in \{0, \dots, n-1\}$  est premier avec  $n$ .

**Remarque.** Ce sont les générateurs du groupe cyclique  $(\mathbb{Z}/n\mathbb{Z}, +)$ .

**Définition.** On note  $\varphi(n)$  le nombre d'inversibles de  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  :

$$\varphi(n) = \text{Card}(\{k \in \{0, \dots, n-1\}, k \wedge n = 1\})$$

$\varphi$  s'appelle l'**indicatrice d'Euler**.

**Remarque.** On convient que  $\varphi(1) = 1$ .

**Théorème d'Euler.**

Soit  $n \geq 2$ . Si  $a \wedge n = 1$ , alors  $a^{\varphi(n)} \equiv 1 [n]$ .

**Remarque.** Lorsque  $n$  est premier, on reconnaît le petit théorème de Fermat.

**Théorème.**

Les trois propriétés suivantes sont équivalentes :

- (i)  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un corps ;
- (ii)  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un anneau intègre ;
- (iii)  $n$  est premier.

**Notation.** Pour  $p$  nombre premier, on note  $\mathbb{F}_p$  le corps  $\mathbb{Z}/p\mathbb{Z}$ .

## 4 Le théorème chinois

### 4.1 Présentation du problème chinois

#### Exemple.

- Déterminer une relation de Bézout entre 14 et 25.
- Déterminer  $x_1$  et  $x_2$  dans  $\mathbb{Z}$  tels que :

$$\begin{cases} x_1 \equiv 1 [14] \\ x_2 \equiv 0 [25] \end{cases} \quad \text{et} \quad \begin{cases} x_2 \equiv 1 [14] \\ x_2 \equiv 0 [25] \end{cases}$$

- Utiliser  $x_1$  et  $x_2$  pour déterminer une solution du système :

$$\begin{cases} x_1 \equiv 2 [14] \\ x_2 \equiv 3 [25] \end{cases}$$

- Déterminer toutes les solutions du système précédent.

**Remarque.** Pourquoi le système :

$$\begin{cases} x_1 \equiv 2 [26] \\ x_2 \equiv 3 [38] \end{cases}$$

n'a pas de solution ?

### 4.2 Structure d'anneau produit

**Définition.** Soit  $(A, +, *)$  et  $(B, +, \star)$  deux anneaux. On définit l'**anneau produit** en munissant le produit cartésien  $A \times B$  des lois :

$$\begin{aligned} (a, b) + (a', b') &= (a + a', b + b') \\ (a, b) \times (a', b') &= (a * a', b \star b') \end{aligned}$$

**Proposition.** Muni de cette structure,  $A \times B$  est un anneau.

**Remarque.** On peut étendre cette définition et cette proposition au cas d'un nombre fini d'anneaux.

### 4.3 À propos de la notation

**Remarque.** Pour  $a \in \mathbb{Z}$ , on note  $\bar{a}$  l'élément de  $\mathbb{Z}/n\mathbb{Z}$  qui est la classe de  $a$ . Mais si on travaille à la fois dans  $\mathbb{Z}/n\mathbb{Z}$  et  $\mathbb{Z}/m\mathbb{Z}$ , la notation devient ambiguë.

**Notation.** Pour  $n \geq 2$  et  $a \in \mathbb{Z}$ , on note :

$$(a \bmod n) \quad \text{ou} \quad [a]_n$$

la classe de  $a$  modulo  $n$ , que l'on note aussi  $\bar{a}$  lorsqu'il n'y a pas d'ambiguïté.

**Exemple.** Préciser le diagramme de l'application :

$$\phi : a \mapsto (a \bmod 14, a \bmod 25)$$

Est-ce un morphisme d'anneaux ?  
Quel est son noyau ?

## 4.4 Le théorème chinois

### Théorème chinois.

Soit  $m, n$  entiers  $\geq 2$ , premiers entre eux. Alors l'application :

$$\begin{aligned} \mathbb{Z}/mn\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ a \bmod mn &\mapsto (a \bmod m, a \bmod n) \end{aligned}$$

est correctement définie, et est un isomorphisme d'anneaux.

**Remarque.** Si l'on dispose d'une relation de Bézout :

$$mu + nv = 1$$

l'isomorphisme réciproque est :

$$(a \bmod m, b \bmod n) \mapsto (anv + bmu \bmod mn)$$

**Corollaire.** Soit  $m, n$  entiers  $\geq 2$ , premiers entre eux. Alors le système de congruences :

$$\begin{cases} x \equiv a \pmod{m} \\ y \equiv b \pmod{n} \end{cases}$$

admet au moins une solution  $x_0 \in \mathbb{Z}$ .

L'ensemble des solutions est  $x_0 + mn\mathbb{Z}$ .

**Généralisation.** Soit  $n_1, \dots, n_k$  entiers  $\geq 2$ , deux à deux premiers entre eux, alors :

$$\begin{aligned} \mathbb{Z}/(n_1 \dots n_k)\mathbb{Z} &\rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z} \\ a \bmod n_1 \dots n_k &\mapsto (a \bmod n_1, \dots, a \bmod n_k) \end{aligned}$$

est correctement définie, et est un isomorphisme d'anneaux.

**Exemple.** Résoudre le système de congruences :

$$\begin{cases} n \equiv 4 \pmod{5} \\ n \equiv 1 \pmod{7} \end{cases}$$

## 5 Indicatrice d'Euler

**Rappel.** Pour  $n \geq 2$ ,  $\varphi(n)$  désigne le nombre d'inversibles de  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ , ou encore le nombre d'entiers premiers avec  $n$  parmi  $\{0, \dots, n-1\}$ , ou encore le nombre de générateurs du groupe cyclique  $(\mathbb{Z}/n\mathbb{Z}, +)$ .

**Théorème d'Euler.** Soit  $n$  entier,  $n \geq 2$  et  $a \in \mathbb{Z}$ . Si  $a$  est premier avec  $n$ , alors  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

**Corollaire (petit théorème de Fermat).** Soit  $p$  un nombre premier. Pour tout  $a$  non multiple de  $p$ ,  $a^{p-1} \equiv 1 \pmod{p}$ .

### Théorème.

Soit  $m, n \in \mathbb{N}^*$ . Si  $m$  et  $n$  sont premiers entre eux, alors :

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

**Proposition.** Si  $p$  est premier et  $k \in \mathbb{N}^*$ , alors :

$$\varphi(p^k) = p^k - p^{k-1}$$

**Théorème.**

Soit  $n \geq 2$  un entier. On a :

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

**Exemple.** Calculer  $\varphi(36)$ .

## 6 Annexes

### 6.1 Démonstrations du petit théorème de Fermat

**Petit théorème de Fermat.**

Soit  $p$  un nombre premier,  $a$  un entier non multiple de  $p$ . Alors :

$$a^{p-1} \equiv 1 [p]$$

*Première preuve.*

On note  $k$  l'ordre de  $\bar{a}$  dans le groupe  $(\mathbb{Z}/p\mathbb{Z})^*$  :

$$a^k \equiv 1 [p]$$

Mais l'ordre d'un élément divise le cardinal du groupe :  $k \mid p-1$ .  
Donc il existe  $q$  tel que  $kq = p-1$ . En élevant à la puissance  $q$  la relation précédente, on a donc  $(a^k)^q \equiv 1^q [p]$ , c'est-à-dire :

$$a^{p-1} \equiv 1 [p]$$

□

*Seconde preuve.*

- Tout d'abord, pour tout  $a \in \mathbb{N}$  :

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

car  $p \mid \binom{p}{k}$  pour tout  $k \in \{1, \dots, p-1\}$ .

En effet :

$$k \binom{p}{k} = p \binom{p-1}{k-1}$$

donc  $p \mid k \binom{p}{k}$  avec  $p$  et  $k$  premiers entre eux, donc  $p \mid \binom{p}{k}$  par le lemme de Gauss.

- On raisonne alors par récurrence sur  $a \in \mathbb{N}^*$ .

- Pour  $a = 1$ , on a bien-sûr  $a^p \equiv a [p]$ .

- On suppose que  $a^p \equiv a [p]$ .

Alors

$$\begin{aligned} (a+1)^p &\equiv a^p + 1 [p] \text{ par le point précédent} \\ &\equiv a + 1 [p] \text{ par hyp. de récurrence} \end{aligned}$$

- On a montré, par récurrence que :

$$\forall a \in \mathbb{N}^*, a^p \equiv a [p]$$

- Si  $b = -a \in \mathbb{Z}_-^*$ ,

$$\begin{aligned} b^p &= (-a)^p \\ &= -a^p \\ &\equiv -a [p] \\ &\equiv b [p] \end{aligned}$$

- On a donc  $p \mid a^p - a = a(a^{p-1} - 1)$ . Or  $p$  est premier et  $a$  n'est pas multiple de  $p$ , donc  $a$  et  $p$  sont premiers entre eux. Par le lemme de Gauss, on a donc :

$$p \mid a^{p-1} - 1$$

□

## Exercices du CCINP

14.1

 86

- Soit  $(a, b, p) \in \mathbb{Z}^3$ . Prouver que : si  $p \wedge a = 1$  et  $p \wedge b = 1$ , alors  $p \wedge (ab) = 1$ .
- Soit  $p$  un nombre premier.
  - Prouver que  $\forall k \in \llbracket 1, p-1 \rrbracket$ ,  $p$  divise  $\binom{p}{k} k!$  puis en déduire que  $p$  divise  $\binom{p}{k}$ .
  - Prouver que :  $\forall n \in \mathbb{N}$ ,  $n^p \equiv n \pmod{p}$ .  
**Indication** : procéder par récurrence.
  - En déduire, pour tout entier naturel  $n$ , que :  $p$  ne divise pas  $n \implies n^{p-1} \equiv 1 \pmod{p}$ .

14.2

 94

- En raisonnant par l'absurde, montrer que le système

$$(S) : \begin{cases} x \equiv 5 & [6] \\ x \equiv 4 & [8] \end{cases}$$

n'a pas de solution  $x$  appartenant à  $\mathbb{Z}$ .

- Énoncer le théorème de Bézout dans  $\mathbb{Z}$ .
  - Soit  $a$  et  $b$  deux entiers naturels premiers entre eux. Soit  $z \in \mathbb{C}$ .  
Prouver que :  $(a \mid c \text{ et } b \mid c) \iff ab \mid c$ .
- On considère le système  $(S) : \begin{cases} x \equiv 6 & [17] \\ x \equiv 5 & [16] \\ x \equiv 4 & [15] \end{cases}$  dans lequel l'inconnue  $x$  appartient à  $\mathbb{Z}$ .
  - Déterminer une solution particulière  $x_0$  de  $(S)$  dans  $\mathbb{Z}$ .
  - Déduire des questions précédentes la résolution dans  $\mathbb{Z}$  du système  $(S)$ .  
On exprimera les solutions en fonction de la solution particulière  $x_0$ .

## Exercices de classiques

### Exercices

14.3

Résoudre dans  $\mathbb{Z}/5\mathbb{Z}$  l'équation :

$$x^2 + x + 3 = 0$$

14.4

Résoudre l'équation :

$$x^2 = \bar{1}$$

- dans  $\mathbb{Z}/7\mathbb{Z}$  ;
- dans  $\mathbb{Z}/8\mathbb{Z}$ .

14.5

Résoudre dans  $\mathbb{Z}$  :

- $6x + 2 \equiv 0 \pmod{11}$  ;
- $6x + 2 \equiv 0 \pmod{10}$  ;
- $6x + 2 \equiv 0 \pmod{9}$ .

14.6

Résoudre dans  $\mathbb{Z}$  le système :

$$\begin{cases} x \equiv 5 & [17] \\ x \equiv 4 & [6] \end{cases}$$

14.7

Résoudre dans  $\mathbb{Z}$  :



- (a)  $\begin{cases} x \equiv 2 [5] \\ x \equiv 3 [9] \end{cases}$
- (b)  $\begin{cases} 9x \equiv 3 [21] \\ 5x \equiv 2 [8] \end{cases}$
- (c)  $\begin{cases} x \equiv 7 [9] \\ x \equiv 6 [7] \\ x \equiv 3 [5] \end{cases}$

**14.8**

Soit  $p$  premier, et  $k \in \mathbb{N}$  tel que  $k \wedge (p-1) = 1$ . Montrer que :

$$f : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \\ x \mapsto x^k$$

est bijective.

**14.9**

Combien y a-t-il d'éléments inversibles dans  $\mathbb{Z}/69\mathbb{Z}$  ? dans  $\mathbb{Z}/99\mathbb{Z}$  ?

**Petits problèmes d'entraînement****14.10**

(a) Résoudre, dans  $\mathbb{Z} \times \mathbb{Z}$ , le système :

$$\begin{cases} x + y \equiv 4 [11] \\ xy \equiv 10 [11] \end{cases}$$

(b) Résoudre, dans  $\mathbb{Z} \times \mathbb{Z}$ , le système :

$$\begin{cases} x + y \equiv 4 [341] \\ xy \equiv 10 [341] \end{cases}$$

**14.11**

(a) Écrire, sous forme de fraction réduite :

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \text{ puis } 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6}$$

On considère  $p$  un nombre premier différent de 2.

(b) Montrer que  $x \mapsto x^{-1}$  est une bijection de  $(\mathbb{Z}/p\mathbb{Z})^*$  sur lui-même.

(c) Montrer que  $\sum_{x \in (\mathbb{Z}/p\mathbb{Z})^*} x^{-1} = \overline{0}$ .

(d) On écrit :

$$1 + \frac{1}{2} + \dots + \frac{1}{p-1} = \frac{a}{b}$$

où  $a$  et  $b$  sont entiers et premiers entre eux.

Utiliser la question précédente pour montrer que  $p \mid a$ .

On va justifier le résultat par une autre méthode.

(e) Montrer que les éléments de  $(\mathbb{Z}/p\mathbb{Z})^*$  sont les racines dans  $\mathbb{Z}/p\mathbb{Z}$  du polynôme  $X^{p-1} - \overline{1}$ .

(f) En déduire la valeur de :

$$\sum_{k=1}^{p-1} \left( \prod_{\substack{j=1 \\ j \neq k}}^{p-1} j \right)$$

puis retrouver le résultat :  $p \mid a$ .

**14.12**

Soit  $a \in \mathbb{Z}$  et  $n \geq 2$ .

(a) On suppose  $a \wedge n = 1$ . Montrer que  $a^{\varphi(n)} \equiv 1 [n]$ .

(b) On suppose  $a^{n-1} \equiv 1 [n]$  et  $a^d \not\equiv 1 [n]$  pour tout  $d \in \mathbb{N}$  diviseur strict de  $n-1$ . Montrer que  $n$  est un nombre premier.

**14.13**

Soit  $a, n$  entiers  $\geq 2$ . On pose  $N = a^n - 1$ . Montrer que :

$$n \mid \varphi(N)$$

**14.14**

Montrer que, pour tout  $n \geq 3$ ,  $\varphi(n)$  est pair.

**14.15**

Soit  $n \in \mathbb{N}^*$ .

- (a) Soit  $d \in \mathbb{N}$  un diviseur de  $n$ . Dénombrer les  $k \in \llbracket 1, n \rrbracket$  tels que  $k \wedge n = d$ .  
(b) En déduire que :

$$n = \sum_{\substack{d \mid n \\ d \geq 0}} \varphi(d)$$