$\boxed{\text{CCINP 66}}$

1. $\overline{0} = \{y \in \mathbb{Z},\ y \mathcal{R} 0\} = \{y \in \mathbb{Z},\ y \equiv 0 [p]\} = p\mathbb{Z}$

$\overline{p} = \{y \in \mathbb{Z},\ y \mathcal{R} p\} = \{y \in \mathbb{Z},\ y \equiv p [p]\} = p\mathbb{Z}$

2.

$$+ \begin{cases} \mathbb{Z}/p\mathbb{Z}^2 \longrightarrow \mathbb{Z}/p\mathbb{Z} \\ (\overline{a}, \overline{b}) \longmapsto \overline{a+b} \end{cases}$$

Soient $a, b, c, d \in \mathbb{Z}$. Supp $\begin{cases} \overline{a} = \overline{c} \\ \overline{b} = \overline{d} \end{cases}$

Ainsi $\begin{cases} a \equiv c\ [p] \\ b \equiv d\ [p] \end{cases}$

$\Rightarrow a+b \equiv c+d\ [p]$ (stabilité par $+$)

$\Rightarrow \overline{a+b} = \overline{c+d}$

$$\times \begin{cases} \mathbb{Z}/p\mathbb{Z}^2 \longrightarrow \mathbb{Z}/p\mathbb{Z} \\ (\overline{a}, \overline{b}) \longmapsto \overline{a \times b} \end{cases}$$

Soient $a, b, c, d \in \mathbb{Z}$

Supp $\begin{cases} \overline{a} = \overline{c} \\ \overline{b} = \overline{d} \end{cases}$

Ainsi $\begin{cases} a \equiv c [p] \\ b \equiv d [p] \end{cases}$

$\Rightarrow a \times b \equiv c \times d\ [p]$

$\Rightarrow \overline{a \times b} = \overline{c \times d}$

3. (exemples)

Avec $p=4$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

pas de $\bar{1}$ dans la ligne, $\bar{2}$ n'a pas d'inverse dans $\mathbb{Z}/4\mathbb{Z}$

$\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps

Avec $p=5$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\boxed{\bar{1}}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\boxed{\bar{1}}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\boxed{\bar{1}}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\boxed{\bar{1}}$

Tout $\bar{a} \neq \bar{0}$ a un inverse dans $\mathbb{Z}/5\mathbb{Z}$

3.

$\Rightarrow$: par contraposition. Supp $p \notin \mathbb{P}$.

p est composé (car $p \geq 2$).

$\Leftrightarrow$ il existe $k, d \in [\![2, p[\![$ tq $p = kd$.

Mtq $\bar{k}$ n'a pas d'inverse par l'absurde.

ie $\forall a \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$, $\bar{a} \times \bar{k} \neq \bar{1}$.

Supp qu'il existe $\bar{a} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$ tq $\bar{a} \times \bar{k} = \bar{1}$.

$$\text{Alors } \bar{a} \times \bar{k} = \bar{1} \Leftrightarrow \bar{a} \times \underbrace{\bar{k} \times \bar{d}} = \underline{\bar{1} \times \bar{d}}$$

$$\Leftrightarrow \bar{a} \times \bar{p} = \bar{d}$$

$$\Leftrightarrow \bar{0} = \bar{d}$$

$\Leftarrow$: Supp $p \in \mathbb{P}$. Mq pour tout $a \in [\![1, p[\![$, $\bar{a}$ a un inverse.
Soit $a \in [\![1, p[\![$.

$p \in \mathbb{P} \wedge a \notin p\mathbb{Z} \Rightarrow a \wedge p = 1$ d'ap. le lien $\mathbb{P}$-p.e.e

$\Rightarrow \exists (u,v) \in \mathbb{Z}^2, au + pv = 1$ d'ap Bézout

$\Rightarrow \exists (u,v) \in \mathbb{Z}^2, au = pv - 1 \equiv 1 [p]$

$\Rightarrow \exists u \in \mathbb{Z}, \overline{a \times u} = \bar{1}$

$\Leftrightarrow \exists u \in \mathbb{Z}, \bar{a} \times \bar{u} = \bar{1}$

$\Rightarrow \bar{a}$ a un inverse

$\boxed{\text{CCINP 86}}$

1. Supp $\begin{cases} p \wedge a = 1 \\ p \wedge b = 1 \end{cases}$.

Notons $\begin{cases} \alpha_1 \alpha_2 \cdots \alpha_r \text{ la DFP de } a \\ \beta_1 \beta_2 \cdots \beta_s \text{ la DFP de } b \end{cases}$

On a $ab = \alpha_1 \alpha_2 \cdots \alpha_r \beta_1 \beta_2 \cdots \beta_s$

p n'apparaît pas dans la DFP de a ni dans celle de b
donc pas dans celle d'ab.

On a $p \wedge ab = 1$.

Version d'El Baki en 2 lignes

Supp $\begin{cases} p \wedge a = 1 \text{ ie } v_p(a) = 0 \\ p \wedge b = 1 \text{ ie } v_p(b) = 0 \end{cases} \Rightarrow v_p(ab) = v_p(a) + v_p(b) = 0 + 0 = 0$

donc $ab \wedge 1$

2. b.

Procédons par récurrence.

Init ($n=0$):

$$n^p = 0^p = 0 = n \Rightarrow 0^p \equiv 0\ [n]$$

Her $n^p \equiv n\,[p]$ (hdr)

$$(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k 1^{p-k}$$

$$= \underbrace{\binom{p}{0}}_{1} + \underbrace{\binom{p}{1}}_{\in p\mathbb{Z}} n + \underbrace{\binom{p}{2}}_{\in p\mathbb{Z}} n^2 + \dots + \underbrace{\binom{p}{p-1}}_{\in p\mathbb{Z}} n^{p-1} + \underbrace{\binom{p}{p}}_{1} n$$

$$\equiv 1 + 0 + 0 + \dots + 0 + n^p\ [p]$$

$$\equiv n^p + 1\ [p]$$

$$\equiv n+1\ [p]$$

2. c. Supp $p \nmid n$ d'ap le $\Leftrightarrow$ $\mathbb{P}$-pee : $p \wedge n = 1$

onsq $n^p \equiv n\,[p]$

$$\Rightarrow \exists k \in \mathbb{Z},\ n^p - n = kp$$

$$\Rightarrow \begin{cases} p \mid n^p - n = n(n^{p-1} - 1) \\ p \wedge n = 1 \end{cases} \Rightarrow p \mid n^{p-1} - 1 \text{ d'après Gauss}$$

$\boxed{\text{CCINP 94}}$

2. implication directe

$$\text{Supp } \begin{cases} a \mid c. \\ b \mid c \end{cases}$$