(TD 18 : MD)

Exercice 4.23. Énoncer et prouver le petit théorème de Fermat.

$\forall p \in \mathcal{P}$, $\forall a \in \mathbb{Z}$, $a^p \equiv a \mod p$. (1),

On montre que : , $\forall a \in \mathbb{N}$,

$$a^p \equiv a \mod p \qquad (2)$$

$a = 0$:

$0 \equiv 0 \mod p$. ok.

Hérédité : on doit démontrer $(a+1)^p \equiv a+1 \mod p$.

$(a+1)^p = a^p + 1 \equiv a+1 \mod p$ car $a^p \equiv a \mod p$

Donc vrai.

On doit montrer $-a \in \mathbb{N}$.

On a donc $(-a)^p \equiv -a \mod p$.

Exercice 4.31. (1) Soit p un nombre premier. Montrer que, pour tout $x \in [\![1, p-1]\!]$, il existe un unique entier $x' \in [\![1, p-1]\!]$ tel que $xx' \equiv 1 \mod p$.

(2) Soit p un nombre premier. Résoudre modulo p l'équation $x^2 \equiv 1 \mod p$.

(3) En déduire le *théorème de Wilson* (John Wilson, 1741-1793) : un nombre $p \geq 2$ est premier si et seulement si $(p-1)! \equiv -1 \mod p$.

Rappelons $aX \equiv c \mod b$. Résoluble $\Leftrightarrow$ $\text{pgcd}(a;b) | c$

Donc $xx' \equiv 1 \mod p$ résoluble $\Leftrightarrow$ pgcd(x;