On se propose de résoudre dans Z l'équation (E) $x^2 \equiv -1$ [25]
Démontrer que (E) peut se ramener à chercher les nombres x tels que $x^2 = 49 + 25k$ ($k \in$ Z)
Résoudre alors l'équation (E)

CORRECTION

$49 = 2 \times 25 - 1$ donc $49 \equiv -1$ [25] donc $x^2 \equiv -1$ [25] $\Leftrightarrow x^2 \equiv 49$ [25]
$x^2 \equiv 49$ [25] $\Leftrightarrow x^2 - 7^2 \equiv 0$ [25] donc on a $(x-7)(x+7) \equiv 0$ [25] $(x-7)(x+7) \equiv 0$ [25] donc 25 divise $(x-7)(x+7)$
5 divise 25 et 25 divise $(x-7)(x+7)$ donc 5 divise $(x-7)(x+7)$
5 est un nombre premier donc soit 5 divise $x-7$, soit 5 divise $x+7$ (lemme d'Euclide)

Cas 1 : 5 divise $x-7$

Si 5 divise $x-7$, il existe un entier relatif k tel que $x-7 = 5k$ soit $x = 5k+7$ alors $x+7 = 5k+14$
$(x+7)(x-7) = 5k(5k+14)$,

25 divise $(x+7)(x-7)$ donc il existe un entier q tel que $(x+7)(x-7) = 25q$
$(x+7)(x-7) = 5k(5k+14) = 25q$
donc $k(5k+14) = 5q$ donc 5 divise $k(5k+14)$

$5(k+3) - (5k+14) = 1$
5 et $5k+14$ sont premiers entre eux (théorème de Bézout) donc 5 divise $k(5k+14)$ si et seulement si 5 divise k (théorème de Gauss)
25 divise $(x+7)(x-7)$ si et seulement si 5 divise k
Il existe un entier k' tel que $k = 5k'$ or $x = 5k+7$
donc $x = 25k' + 7$ ($k' \in$ Z).

On a donc une première série de solutions :
$x = 25k' + 7$ ($k' \in$ Z)

Cas 2 : 5 divise $x+7$

si 5 divise $x+7$, il existe un entier relatif k tel que $x+7 = 5k$ soit $x = 5k-7$ alors $x-7 = 5k-14$
$(x+7)(x-7) = 5k(5k-14)$,

25 divise $(x+7)(x-7)$ donc il existe un entier q tel que $(x+7)(x-7) = 25q$
$(x+7)(x-7) = 5k(5k-14) = 25q$
donc $k(5k-14) = 5q$ donc 5 divise $k(5k-14)$

$5k - 14 - 5(k-3) = 1$
5 et $5k-14$ sont premiers entre eux (théorème de Bézout) donc 5 divise $k(5k-14)$ si et seulement si 5 divise k (théorème de Gauss)
25 divise $(x+7)(x-7)$ si et seulement si 5 divise k
Il existe un entier k' tel que $k = 5k'$ or $x = 5k-7$ donc $x = 25k' - 7$ ($k' \in$ Z) soit $x = 25k' - 7$ ($k' \in$ Z).

On a donc une seconde série de solutions :
$x = 25k - 7$ ($k' \in$ Z).

On a donc deux séries de solutions : $x = 25k + 7$ et $x = 25k - 7$