

5.5 On trouve facilement que $3 \cdot 8 \equiv 24 \equiv -1 \pmod{25}$, si bien que $\overline{3}^{-1} = \overline{-8} = \overline{17}$

En revanche, l'inverse de $\overline{11}$ est plus difficile à deviner.

On cherche un entier x tel que $11x \equiv 1 \pmod{25} \iff 11x + 25y = 1$ pour un $y \in \mathbb{Z}$. Utilisons l'algorithme d'Euclide pour résoudre cette équation diophantienne :

$$25 = 11 \cdot 2 + 3 \quad \implies \quad 3 = 25 - 11 \cdot 2$$

$$11 = 3 \cdot 3 + 2 \quad \implies \quad 2 = 11 - 3 \cdot 3$$

$$3 = 2 \cdot 1 + 1 \quad \implies \quad 1 = 3 - 2 \cdot 1$$

$$2 = 1 \cdot 2$$

$$1 = 3 - 2 \cdot 1$$

$$= 3 - (11 - 3 \cdot 3) \cdot 1 = 11 \cdot (-1) + 3 \cdot 4$$

$$= 11 \cdot (-1) + (25 - 11 \cdot 2) \cdot 4 = 25 \cdot 4 + 11 \cdot (-9)$$

Puisque $11 \cdot (-9) \equiv 1 \pmod{25}$, on obtient $\overline{11}^{-1} = \overline{-9} = \overline{16}$.

L'inverse de $\overline{23}$ est plus facile à trouver, vu que $23 \equiv -2 \pmod{25}$:

$(-2) \cdot 12 \equiv -24 \equiv 1 \pmod{25}$ entraîne $\overline{23}^{-1} = \overline{12}$.