1. Écrire une division euclidienne de -13 par -6.

Réponse :

$-13 = -2 \times 6 - 1$ convient.

On pouvait aussi écrire $-13 = -3 \times 6 + 5$.

Par contre je ne vois pas trop la nécessité de poser les divisions pour des nombres aussi petits...

2. Voici les tables d'addition et de multiplication dans $\mathbb{Z}/2\mathbb{Z}$:

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

et

$\cdot$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

Écrire les tables d'addition et de multiplication dans $\mathbb{Z}/4\mathbb{Z}$.

Réponse :

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

et

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

3. Résoudre dans $\mathbb{Z}$ le système de congruence $\begin{cases} x \equiv 1 \mod 3 \\ x \equiv -4 \mod 5 \end{cases}$

Réponse :

1 est une solution "évidente", et 3 et 5 étant premiers entre eux l'ensemble des solutions est alors

$$S = \{1 + 15k;\ k \in \mathbb{Z}\}.$$

Si on rate la solution évidente on peut en retrouver une à partir d'une relation de Bezout entre 3 et 5, par exemple $5 \cdot 2 - 3 \cdot 3 = 1$. En effet $x = 1 + 3k_1 = -4 + 5k_2$ donne $5k_2 - 3k_1 = 5$, donc en multipliant la relation de Bezout par 5 on trouve la solution particulière $k_1 = 15$, $k_2 = 10$, d'où $x_0 = 46$ qui est bien de la forme $1 + 15k$...

4. Trouver un PGCD de $P(X) = X^2 + 4X + 3$ et $Q(X) = X^3 + 4X^2 + 4X + 3$.

Réponse :

On utilise l'algorithme d'Euclide :

$$X^3 + 4X^2 + 4X + 3 = (X^2 + 4X + 3) \cdot X + \boxed{X + 3}$$
$$X^2 + 4X + 3 = (X + 3) \cdot (X + 1) + 0.$$

Le PGCD attendu est le dernier reste non nul, donc $\mathrm{PGCD}(P, Q) = X + 3$.

On pouvait aussi repérer les racines "évidentes" -1 et -3 de P et les reporter dans Q, mais c'est au moins aussi long et un peu trop ad-hoc (et il faut savoir faire un algorithme d'Euclide, idéalement sans poser les divisions entre polynômes !)