Université de Bretagne Occidentale
UFR Sciences et Techniques
L3 DE MATHEMATIQUES

ARITHMÉTIQUE ET APPLICATIONS

Contrôle continu, le 16 mars 2023, 8h00-8h30

CORRIGE

Exercice 1. La décomposition en facteurs premiers de 140 est $2^2 \times 5 \times 7$. D'après le Théorème Chinois, le morphisme d'anneaux

$$f\colon \mathbb{Z}/140\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

défini par $f(\bar{x}) = (\bar{x}, \bar{x}, \bar{x})$ est un isomorphisme. Déterminons f^{-1}.

On cherche une identité de Bézout de la forme

$$u \times 5 \times 7 + v \times 4 \times 7 + w \times 4 \times 5 = 1.$$

On a

$$1 \times 5 + (-1) \times 4 = 1.$$

Donc,

$$1 \times 5 \times 7 + (-1) \times 4 \times 7 = 7.$$

Comme

$$3 \times 7 + (-1) \times 4 \times 5 = 1,$$

on obtient

$$3 \times 5 \times 7 + (-3) \times 4 \times 7 + (-1) \times 4 \times 5 = 1.$$

On vérifie :

$$3 \times 5 \times 7 + (-3) \times 4 \times 7 + (-1) \times 4 \times 5 = 105 - 84 - 20 = 105 - 104 = 1.$$

Du coup,

$$f^{-1}(\bar{a}, \bar{b}, \bar{c}) = \overline{3 \times 5 \times 7 \times a + (-3) \times 4 \times 7 \times b + (-1) \times 4 \times 5 \times c}.$$

On vérifie qu'on a bien $f(f^{-1}(\bar{a}, \bar{b}, \bar{c})) = (\bar{a}, \bar{b}, \bar{c})$:

$$\begin{aligned}
3 \times 5 \times 7 \times a + (-3) \times 4 \times 7 \times b + (-1) \times 4 \times 5 \times c &\equiv (-1) \times 1 \times (-1) \times a \\
&\equiv a \pmod 4, \\
3 \times 5 \times 7 \times a + (-3) \times 4 \times 7 \times b + (-1) \times 4 \times 5 \times c &\equiv 2 \times (-1) \times 2 \times b \\
&\equiv b \pmod 5, \text{et} \\
3 \times 5 \times 7 \times a + (-3) \times 4 \times 7 \times b + (-1) \times 4 \times 5 \times c &\equiv (-1) \times (-3) \times (-2) \times c \\
&\equiv c \pmod 7.
\end{aligned}$$

Il suit que f^{-1} induit par restriction un isomorphisme de groupes

$$f^{-1}\colon (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times \to (\mathbb{Z}/140\mathbb{Z})^\times$$

donné par la même formule que ci-dessus.

Or, un générateur de $(\mathbb{Z}/4\mathbb{Z})^\times$ est $-\bar{1}$, un générateur de $(\mathbb{Z}/5\mathbb{Z})^\times$ est $\bar{2}$, et un générateur de $(\mathbb{Z}/7\mathbb{Z})^\times$ est $-\bar{2}$. Du coup, une famille génératrice du groupe

$$(\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times$$

est

$$(-\bar{1}, \bar{1}, \bar{1}), (\bar{1}, \bar{2}, \bar{1}), (\bar{1}, \bar{1}, -\bar{2}).$$

Les images par f^{-1} constituent donc une famille génératrice de $(\mathbb{Z}/140\mathbb{Z})^\times$. On calcule :

$$\begin{aligned}
f^{-1}(-\bar{1}, \bar{1}, \bar{1}) &= \overline{3 \times 5 \times 7 \times (-1) + (-3) \times 4 \times 7 \times 1 + (-1) \times 4 \times 5 \times 1} \\
&= \overline{-105 - 84 - 20} = \overline{35 + 36} = \overline{71} = -\overline{69}, \\
f^{-1}(\bar{1}, \bar{2}, \bar{1}) &= \overline{3 \times 5 \times 7 \times 1 + (-3) \times 4 \times 7 \times 2 + (-1) \times 4 \times 5 \times 1} \\
&= \overline{105 - 168 - 20} = \overline{105 - 48} = \overline{57}, \text{et} \\
f^{-1}(\bar{1}, \bar{1}, -\bar{2}) &= \overline{3 \times 5 \times 7 \times 1 + (-3) \times 4 \times 7 \times 1 + (-1) \times 4 \times 5 \times (-2)} \\
&= \overline{105 - 84 + 40} = \overline{5 - 84} = \overline{5 + 56} = \overline{61}
\end{aligned}$$

On peut donc prendre

$$k = -69, \ell = 57, m = 61.$$

Comme ils appartiennent à $(\mathbb{Z}/140\mathbb{Z})^\times$, ils sont automatiquement premiers avec 140.