Université de Rennes

Arithmétique

Séance 5

1 Rituel

Présentation de la décomposition en facteurs premiers.

2 Travail en séance

Exercice 1 [Dossier 2-7 (capes-math.univ-rennes1.fr/Doss0.html)]

Soit $\mathcal{E}$ l'ensemble des entiers compris entre 0 et 25 inclus. Dans cet exercice, chaque lettre de l'alphabet correspond à un élément de $\mathcal{E}$ *via* $A \leftrightarrow 0, \dots, Z \leftrightarrow 25$.

On appelle codage l'application qui associe à chaque lettre de l'alphabet l'entier correspondant, et décodage l'application qui associe à chaque entier de $\mathcal{E}$ la lettre correspondante. Soient a et b deux entiers. Soit $f\colon \mathcal{E} \to \mathcal{E}$ définie par :

pour tout x appartenant à $\mathcal{E}$, $f(x)$ est le reste de la division euclidienne de $ax+b$ par 26.

On appelle cryptage affine de clé (a, b) l'application qui associe, à chaque lettre de l'alphabet, une lettre de l'alphabet de la façon suivante : on code la lettre par un entier x de $\mathcal{E}$, on calcule $f(x)$ puis on décode $f(x)$. Pour crypter un mot, on crypte chaque lettre.

1. On suppose dans cette question a premier avec 26. Soient x et x' deux éléments de $\mathcal{E}$, montrer que si $f(x) = f(x')$ alors $x = x'$.

2. On suppose dans cette question que $\text{pgcd}(a, 26) \neq 1$. Montrer qu'il existe alors au moins deux lettres différentes ayant le même cryptage.

3. On suppose maintenant que $(a, b) = (7, 2)$.

3.a. Quel est le cryptage du mot JOUR ?

3.b. Quel est le mot dont le cryptage est QCDEY ?

Exercice 2 [Équations diophantiennes]

Réaliser une carte mentale de la résolution d'une équation diophantienne du type $ax + by = c$ d'inconnues $(x, y) \in \mathbb{Z}^2$ (les entiers a, b et c sont donc considérés comme des données du problème).

3 Travail à faire

Présentation de la notion de pgcd et ppcm (définitions et méthodes de calculs).