Master1, mathématiques
Algèbre 1

Devoir à la maison n° 1

à rendre la semaine du 4 novembre 2003

On note G le groupe $(\mathbb{Z}/3^\alpha\mathbb{Z})^\times$, où $\alpha \geq 2$ est fixé.

1.a) Pour tout $y \in \mathbb{N}$ et tout $j \geq 2$ établir la congruence

$$(1+3)^{3^{j-2}y} \equiv 1 + 3^{j-1}y \bmod 3^j .$$

b) Déterminer l'ordre de $\overline{4}$ dans $(\mathbb{Z}/3^\alpha\mathbb{Z})^\times$.

c) En déduire que l'élément $\overline{2}$ engendre $(\mathbb{Z}/3^\alpha\mathbb{Z})^\times$ (on pourra utiliser l'homomorphisme canonique $\mathbb{Z}/3^\alpha\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$).

2. Soit a un entier non divisible par 3. Dans la suite on cherche à résoudre la congruence $2^x \equiv a \bmod 3^\alpha$ (logarithme discret dans G).

a) Montrer que cela revient à résoudre l'équation $\overline{2}^u \cdot \overline{a} = \overline{1}$ dans le groupe G, et que cette équation admet une unique solution u dans $\{0, \cdots, 2 \cdot 3^{\alpha-1} - 1\}$.

b) Montrer qu'on peut se ramener au cas où $a \equiv 1 \bmod 3$, et qu'alors $u = 2y$ est pair.

Ceci nous ramène à résoudre l'équation (**E**) : $\overline{4}^y \cdot \overline{a} = \overline{1}$ dans G, où on a $a \equiv 1 \bmod 3$: on en cherche l'unique solution $y \in \{0, \cdots, 3^{\alpha-1} - 1\}$.

3. Soit y dans cet intervalle. On note $y = \sum_{i=0}^{\alpha-2} 3^i y_i$, $y_i \in \{0, 1, 2\}$ son écriture en base 3, et $y_{-1} = 0$. Pour $1 \leq j \leq \alpha$, on considère la congruence $\mathbf{C_j}$:

$$4^{y_0 + 3y_1 + \cdots + 3^{j-2}y_{j-2}} a \equiv 1 \bmod 3^j \qquad (\mathbf{C_j})$$

De plus on pose $a_1 = a$, a_j $(j \geq 2)$ est le reste de la division du premier membre de $\mathbf{C_j}$ par 3^α.

a) Vérifier que $\mathbf{C_1}$ est vraie.

b) On suppose que la congruence $\mathbf{C_{j-1}}$ est vraie pour l'entier $j \geq 2$. En utilisant **1**a) et a_{j-1}, montrer que $\mathbf{C_j}$ est vraie si et seulement si y_{j-2} est le reste de la division par 3 de l'entier $(1 - a_{j-1})/3^{j-1}$.

4. En déduire un algorithme de résolution de l'équation **E**. Montrer que cet algorithme est polynomial en l'ordre de G, avec un nombre d'opérations en $O(\alpha^3)$.

5. Appliquer ce qui précède pour résoudre la congruence $2^x \equiv 101 \bmod 243$. Vérifier le résultat par la méthode d'exponentiation rapide.

*****