UNIVERSITÉ BORDEAUX I
UE: MHT 531

Algorithmique Algébrique

Devoir Surveillé (Corrigé)

le 13 novembre 2013

Durée 1h30. Documents non autorisés

Exercice 1. Trouvez toutes les solutions du système

$$\begin{cases} 14x \equiv 4 \pmod{30}, \\ 15x \equiv 21 \pmod{81}. \end{cases}$$

Solution. Le système est équivalent au système suivant :

$$\begin{cases} 7x \equiv 2 \pmod{15}, \\ 5x \equiv 7 \pmod{27} \end{cases}$$

et donc au système

$$\begin{cases} x \equiv 2 \pmod{3}, \\ 2x \equiv 2 \pmod{5}, \\ 5x \equiv 7 \pmod{27}. \end{cases}$$

Comme $PGCD(2,5) = 1$, la deuxième congruence est équivalente à $x \equiv 1 \pmod{5}$ et on a

$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 1 \pmod{5}, \\ 5x \equiv 7 \pmod{27}. \end{cases}$$

On a $5 \cdot 11 + 27 \cdot (-2) = 1$, d'où on obtient que les solutions de $5x \equiv 7 \pmod{27}$ sont données par $x \equiv -4 \pmod{27}$. Comme cette congruence implique la congruence $x \equiv 2 \pmod{3}$, notre système est équivalent au système

$$\begin{cases} x \equiv -4 \pmod{27}, \\ x \equiv 1 \pmod{5}. \end{cases}$$

On en déduit que

$$x \equiv 5 \cdot 11 \cdot (-4) + 27 \cdot (-2) \cdot 1 \equiv -4 \pmod{135}.$$

Exercice 2.

1) Donner des générateurs des groupes $(\mathbb{Z}/5\mathbb{Z})^*$ et $(\mathbb{Z}/7\mathbb{Z})^*$.
Solution. Les générateurs de $(\mathbb{Z}/5\mathbb{Z})^*$ sont $\overline{2}$ et $\overline{3}$. Les générateurs de $(\mathbb{Z}/7\mathbb{Z})^*$ sont $\overline{3}$ et $\overline{5}$.
2) Rappeler la formulation du théorème chinois.

On suppose dans le reste de cet exercice que $n = pq$ est le produit des nombres premiers distincts impairs p et q.

3) Prouver qu'il existe deux éléments $\overline{a}$ et $\overline{b}$ de $\mathbb{Z}/n\mathbb{Z}$ d'ordre $p-1$ et $q-1$ respectivement tels que tout $\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^*$ s'écrit de façon unique sous la forme $\overline{x} = \overline{a}^k\overline{b}^l$, où $0 \leqslant k \leqslant p-2$ et $0 \leqslant l \leqslant q-2$.
Solution. Par le théorème chinois on a un isomorphisme

$$\psi : (\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p\mathbb{Z})^* \oplus (\mathbb{Z}/q\mathbb{Z})^*.$$

Soient A et B des générateurs de $(\mathbb{Z}/p\mathbb{Z})^*$ et $(\mathbb{Z}/q\mathbb{Z})^*$ respectivement et soient $\overline{a}$ et $\overline{b}$ les images réciproques de $(A, \overline{1})$ et de $(\overline{1}, B)$ dans $(\mathbb{Z}/n\mathbb{Z})^*$. Soit $\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^*$. Alors $\psi(\overline{x})$ s'écrit de façon unique sous la forme $\psi(\overline{x}) = (A^k, B^l)$. Donc $\overline{x}$ s'écrit de façon unique sous la forme $\overline{x} = \overline{a}^k\overline{b}^l$.

4) Soit $\overline{x} = \overline{a}\overline{b}$. Prouver que $\overline{x}^{n-1} \neq \overline{1}$.
Solution. On a $\overline{x}^{n-1} = \overline{a}^{n-1}\overline{b}^{n-1}$. Comme $n-1 = (p-1)q + (q-1)$, le théorème de Fermat implique que $\overline{a}^{n-1} = \overline{a}^{q-1}$. De même, $\overline{b}^{n-1} = \overline{b}^{p-1}$. Par la question précédente, $\overline{x}^{n-1} = \overline{1}$ si et seulement si $\overline{a}^{q-1} = \overline{1}$ et $\overline{b}^{p-1} = \overline{1}$, i.e. si et seulement si $q-1 \mid p-1$ et $p-1 \mid q-1$. On en déduit que $p = q$ ce qui est impossible.

5) Trouver un entier $x \in \mathbb{Z}$ tel que $PGCD(x, 35) = 1$ et $x^{34} \not\equiv 1 \pmod{35}$.
Solution. $35 = 5 \cdot 7$. On peut prendre $A = \overline{2}$ et $B = \overline{3}$. Alors $\overline{a}$ doit vérifier les conditions $a \equiv 2 \pmod 5$ et $a \equiv 1 \pmod 7$, d'où on voit qu'on peut prendre $a = 22$. De même, $\overline{b}$ doit vérifier les conditions $b \equiv 3 \pmod 7$ et $b \equiv 1 \pmod 5$, d'où on voit qu'on peut prendre $b = 31$. Alors, par la question précédente, $x = ab = 22 \cdot 31$. convient. Comme $22 \cdot 31 \equiv (-13) \cdot (-4) \equiv 17 \pmod{35}$, on peut aussi prendre $x = 17$.

6) Comparer le résultat de la question 4) avec le théorème de Fermat.
Solution. Le théorème de Fermat affirme que $x^{n-1} \equiv 1 \pmod n$ si $PGCD(x, n) = 1$ et n est un nombre premier. On vient de prouver que cette propriété devient fausse si n est le produit de deux nombres premiers distincts.

Exercice 3. Soient m et n deux entiers strictement positifs.

1) On fait la division euclidienne de m par n:

$$m = nq + r, \qquad q, r \in \mathbb{N}, \quad 0 \leqslant r \leqslant n-1.$$

Prouver que $PGCD(X^m - 1, X^n - 1) = PGCD(X^r - 1, X^n - 1)$.
Solution. Si $m = nq + r$, alors

$$X^m - 1 = X^{qn+r} - 1 = X^r(X^{nq} - 1) + X^r - 1.$$

Comme $X^{nq} - 1 = (X^n - 1)(X^{n(q-1)} + \cdots + X^n + 1)$, on a

$$X^m - 1 = (X^n - 1)f(X) + (X^r - 1),$$

où $f(X) = X^r(X^{n(q-1)} + \cdots + X^n + 1)$. Donc

$$PGCD(X^m - 1, X^n - 1) = PGCD((X^n - 1)f(X) + X^r - 1, X^n - 1) = \\ = PGCD(X^r - 1, X^n - 1).$$

2) En déduire que $PGCD(X^m - 1, X^n - 1) = X^d - 1$, où $d = PGCD(m, n)$.
Solution. On applique la question 1) aux divisions euclidiennes qui apparaissent dans l'algorithme d'Euclide avec $r_0 = m$, $r_1 = n$, $r_2 = r$ et $q_0 = q$.

$$\begin{aligned} &r_0 = r_1 q_1 + r_1, \\ &r_1 = r_2 q_2 + r_3, \\ &\cdots\cdots \\ &r_k = r_{k+1} q_{k+1} + r_{k+2}, \\ &\cdots\cdots \\ &r_s = r_{s+1} q_{s+1}, \qquad d = r_{s+1} = PGCD(m, n). \end{aligned}$$

On en déduit que

$$PGCD(X^m - 1, X^n - 1) = \cdots = PGCD(X^{r_k} - 1, X^{r_{k+1}} - 1) = \cdots \\ = PGCD(X^{r_s} - 1, X^{r_{s+1}} - 1) = X^{r_{s+1}} - 1 = X^d - 1.$$

FIN