Université d'Évry Val d'Essonne 2011-2012

M54 algèbre et arithmétique 2

Examen — session de janvier 2012

Squelette de cours autorisé, calculatrice autorisée

Durée : 3h

Exercice 1. Résoudre les systèmes de congruences suivants.

$$(S_1)\begin{cases} 10x = 7 & \mod 42 \\ 25x = 19 & \mod 33 \\ 37x = 15 & \mod 57 \end{cases} \qquad (S_2)\begin{cases} 10x = 5 & \mod 15 \\ 24x = 19 & \mod 5 \\ 25x = 17 & \mod 6 \end{cases}$$

Exercice 2. Soit $P = X^3 + X^2 + X - 1 \in \mathbf{F}_5[X]$. On note $K = \mathbf{F}_5[X]/(P)$ et α la classe de X dans K.

1. Montrer que K est un corps, donner sa caractéristique et son cardinal, ainsi qu'une base de K en tant que $\mathbf{F}_5$-espace vectoriel.
2. On pose $x = \alpha - 1$; calculer x^4 et x^{-1}. (Questions indépendantes.)
3. Montrer que $x^{25} = \alpha^{25} - 1$.
4. Donner le cardinal de $K^\times$ et déduire du théorème de Lagrange (II.4.1) que l'ordre d'un élément de $K^\times$ appartient forcément à $\{1, 2, 4, 31, 62, 124\}$.
5. Justifier que l'équation $X^4 = 1$ a au plus 4 solutions dans K. Montrer que tous les éléments de $\mathbf{F}_5^\times$ sont solution et en déduire que ce sont les seules.
6. En déduire les ordres possibles des éléments de $K^\times \setminus \mathbf{F}_5^\times$.
7. Montrer (presque) sans calculs que α^4 est d'ordre 31 exactement. En déduire que 2α est un générateur de $K^\times$.

Exercice 3. On considère l'anneau $A = \mathbf{C}[X]$ des polynômes en une variable à coefficients complexes. Si E est un sous-ensemble de $\mathbf{C}$, on note

$$I(E) = \{P \in A \text{ tel que } (x \in E \implies P(x) = 0)\}$$

l'ensemble des polynômes qui s'annullent en tout point de E.

1. Calculer $I(\emptyset)$, $I(\{0\})$ et $I(\mathbf{C})$.
2. Plus généralement, monter que si E est infini, alors $I(E) = \{0\}$, en utilisant les propriétés des polynômes.

On suppose désormais que E est fini, de cardinal n, et que $E = \{x_1, \ldots, x_n\}$.

3. Pour chaque $x \in \mathbf{C}$, on introduit une application

$$\begin{aligned} ev_x \colon A &\to \mathbf{C} \\ P &\mapsto P(x) \end{aligned}$$

Montrer que c'est un morphisme d'anneaux, surjectif.

4. Montrer que $I(E) = \ker ev_{x_1} \cap \cdots \cap \ker ev_{x_n}$.
5. En déduire que $I(E)$ est un idéal de A.
6. Montrer que $\ker ev_x = (X - x)$.
7. En utilisant les propriétés de l'anneau A, déduire des question précédentes que :
   (a) $I(E)$ est engendré par $\prod_{i=1}^{n}(X - x_i)$;
   (b) $I(E) \cap I(F) = I(E \cup F)$;
   (c) $I(E) + I(F) = I(E \cap F)$;
   (d) $I(E) \subset I(F) \iff F \subset E$;

   où $F = \{y_1, \ldots, y_m\}$ est un autre sous-ensemble fini de $\mathbf{C}$.

Exercice 4. *Attaques élémentaires sur RSA.*

1. *Petits messages.*
   En utilisant le système RSA, Alice souhaite transmettre des messages à Bob, dont la clé publique est $(5, 1112927)$.
   (a) Alice veut transmettre le message $m_1 = 10$ à Bob. Quel message chiffré c_1 doit-elle lui envoyer ? Que remarquez-vous en calculant c_1 ?
   (b) Alice transmet un deuxième message m_2 à Bob ; vous interceptez le message chiffré $c_2 = 32768$, que vous reconnaissez immédiatement comme étant 2^{15}. Retrouvez m_2 en justifiant.
   (c) Plus généralement, expliquez pourquoi le système RSA n'est pas sûr si $m \leqslant n^{1/e}$ (avec les notations du cours).

   En pratique, on évite cette attaque en modifiant m s'il est trop petit.
2. *Attaque de Håstad (1985).*
   En utilisant le système RSA, Alice souhaite envoyer un même message m a ses trois amies Bianca, Bernard et Bob. Supposons qu'ils utilisent tous le même exposant public $e = 3$, leurs clés publiques sont donc $(n_1, 3)$, $(n_2, 3)$ et $(n_3, 3)$. Supposons de plus que $m < \min(n_1, n_2, n3)$ et que n_1, n_2, n_3 soient premiers entre eux deux à deux. On note c_1, c_2 et c_3 les messages chiffrés correspondants ; on suppose que Ève les intercepte.
   (a) Expliquer comment, à partir de c_1, c_2 et c_3, Ève peut calculer facilement un entier c' tel que $c' = m^3 \mod n_1 n_2$ puis un entier c'' tel que $c'' = m^3 \mod n_1 n_2 n_3$.
   (b) Montrer que $m^3 < n_1 n_2 n_3$ et en déduire comment Ève peut retrouver m facilement.
   (c) Supposons maintenant que l'exposant public commun de Bianca, Bernard et Bob soit $e = 5$ au lieu de 3. Cette méthode marche-t-elle encore en général ? Pourquoi ?

   En pratique, il est courant que plusieurs personnes utilisent le même exposant public, la valeur la plus courante étant 65537.
   (d) En remarquant que $65537 = 2^{16} + 1$, expliquer comment, quelle que soit la valeur de x, on peut calculer x^{65537} avec seulement 17 multiplications.