Université d'Évry Val d'Essonne 2011-2012

M54 algèbre et arithmétique 2

Corrigé de l'examen de janvier 2012

Exercice 1. On applique les méthodes II.2.4 et II.3.3.

Pour S_1, on remarque que la première équation n'a pas de solutions : en effet $\text{pgcd}(10, 42) = 2$ ne divise pas 7. Le système n'a donc pas de solutions.

Pour S_2, on simplifie puis on résout chaque équation indépendamment :

$$(S_2) \Leftrightarrow \begin{cases} 2x = 1 & \text{mod } 3 \\ -1x = -1 & \text{mod } 5 \\ 1x = -1 & \text{mod } 6 \end{cases} \Leftrightarrow \begin{cases} x = -1 & \text{mod } 3 \\ x = 1 & \text{mod } 5 \\ x = -1 & \text{mod } 6 \end{cases}$$

On résout ensuite le système formé des deux premières équations : 3 et 5 étant premiers entre eux, il admet une solution unique modulo 15. Une relation de Bézout entre 3 et 5 est $1 = 2 \cdot 3 - 5$, donc une solution est $x_1 = 2 \cdot 3 \cdot 1 - 5 \cdot (-1) = 11$, d'où

$$(S_2) \Leftrightarrow \begin{cases} x = -4 & \text{mod } 15 \\ x = -1 & \text{mod } 6 \end{cases}$$

On remarque que $\text{pgcd}(15, 6) = 3$ et que $-4 = -1 \mod 3$: ce système a donc une solution, unique modulo $\text{ppcm}(15, 6) = 30$. Une relation de Bézout entre $15/3$ et $6/3$ est $1 = 5 - 2 \cdot 2$, donc une solution particulière du système est $x_2 = 5 \cdot (-1) - 2 \cdot 2 \cdot (-4) = 11$ et au final

$$(S_2) \Leftrightarrow x = 11 \mod 30$$

Exercice 2.

1. On sait que K est un corps si et seulement si P est irréductible ; ce dernier étant de degré 3, il est irréductible si et seulement si il n'a pas de racines. Calculons donc

   $$P(0) = -1, \quad P(1) = 2, \quad P(2) = -2, \quad P(-2) = -2, \quad P(-1) = -2 \ .$$

   Ainsi, P n'a pas de racine, donc est irréductible, et K est un corps. Comme c'est une extension de $\mathbf{F}_5$ sa caratéristique est 5 ; son cardinal est $5^3 = 125$ un base sur $\mathbf{F}_5$ est $1, \alpha, \alpha^2$ d'après II.3.2.

2. Par définition de K, on a

   $$\alpha^3 = -\alpha^2 - \alpha + 1 \quad \text{et} \quad \alpha^4 = -\alpha^3 - \alpha^2 + \alpha = 2\alpha - 1$$

   On en déduit

   $$x^2 = \alpha^4 - 4\alpha^3 + 6\alpha^2 - 4\alpha + 1 = 2\alpha - 1 - \alpha^2 - \alpha + 1 + \alpha^2 + \alpha + 1 = 2\alpha + 1$$

Pour calculer x^{-1}, il s'agit de trouver une relation de Bézout entre $X-1$ et P dans $\mathbf{F}_5[X]$; on utilise l'algorithme d'Euclide.

$$
\begin{array}{rrrr|l}
X^3 + & X^2 + & X & -1 & X-1 \\
\cline{5-5}
-(X^3 - & X^2) & & & X^2+2X+3 \\
\cline{1-2}
& 2X^2 + & X & & \\
& -(2X^2 & -2X) & & \\
\cline{2-3}
& & 3X & -1 & \\
& & -(3X & -3) & \\
\cline{3-4}
& & & 2 &
\end{array}
$$

On obtient directement une relation de Bézout en remarquant que dans $\mathbf{F}_5$, l'inverse de 2 est -2 :

$$
\begin{aligned}
2 &= P - (X-1)(X^2+2X-2) \\
1 &= -2P + (X-1)(2X^2 - X + 1)
\end{aligned}
$$

donc dans K on a $(\alpha-1)^{-1} = 2\alpha^2 - \alpha + 1$.

3. D'après III.5.8, on a

$$x^{25} = \left((\alpha-1)^5\right)^5 = (\alpha^5 - 1^5)^5 = \alpha^{25} - 1$$

4. On a $\operatorname{Card} K^\times = 124$ car K est un corps de cardinal 125. L'ordre de tout élément divise donc 124, or l'ensemble des diviseurs de 124 est $\{1, 2, 4, 31, 62, 124\}$.
5. Comme K est un corps, le polynôme $X^4 - 1$, qui est de degré 4, a au plus 4 racines dans K. D'après le théorème de Lagrange, pour tout $t \in \mathbf{F}_5^\times$ on a $t^4 - 1$. Ainsi, les 4 élements de $\mathbf{F}_5^\times$ sont des solutions : ce sont donc forcément les seules.
6. D'après la question précédente, les éléments dont l'ordre divise 4, c'est-à-dire ceux satisfaisant $t^4 = 1$, sont exactement ceux de $\mathbf{F}_5$. D'après la question d'avant, les ordres possibles pour des éléments de $K^\times \setminus \mathbf{F}_5^\times$ sont donc 31, 62 et 124.
7. On a vu que $\alpha^4 = 2\alpha - 1$, donc $\alpha^4 \notin \mathbf{F}_5$ et la question précédente montre que son ordre est au moins 31.

   Par ailleurs, le théorème de Lagrange dit que $\alpha^{124} = 1$, donc $(\alpha^4)^{31} = 1$ et α^4 est d'ordre au plus 31. Au final, l'ordre de α^4 est exactement 31.

   Par ailleurs, on remarque que 2 est d'ordre 4. Ainsi, $2^{31} = 2^3 = -2$ car $31 = 3 \mod 4$ et $2^{62} = 2^2 = -1$ car $62 = 2 \mod 4$. On en déduit que $(2\alpha^{31} = -2\alpha \neq 1$ et que $(2\alpha^{62} = -\alpha \neq 1$, donc 2α n'est ni d'ordre 31 ni d'ordre 62 : il est donc d'ordre 124, c'est-à-dire que c'est un générateur de $K^\times$.

Exercice 3. 1. Par définition, $I(\emptyset)$ est l'ensemble des polynômes P qui satisfont $P(x) = 0$ pour tout $x \in \emptyset$, c'est-à-dire qu'il n'y a aucune condition à satisfaire, donc $I(\emptyset) = A$.

Par ailleurs, $I(\{0\})$ est l'ensemble des polynômes P tels que $P(0) = 0$. C'est donc l'ensemble des polynômes dont le terme constant est nul.

Enfin, $I(\mathbf{C})$ est l'ensemble des polynômes qui s'annullent partout, c'est-à-dire qui sont nuls (on est sur $\mathbf{C}$. Ainsi, $I(\mathbf{C}) = \{0\}$.

2. On sait qu'un polynômes non nul de degré d a au plus d racines, en particulier il n'a qu'un nombre fini de racines. Or, si E est infini, pour appartenir à $I(E)$ un polynôme doit avoit une infinité de racines (tous les éléments de E), ce qui n'est possible que si le polynôme est nul.

   Ainsi, $I(E) = \{0\}$ si E est infini.

3. On a $ev_x(PQ + R) = (PQ + R)(x) = P(x)Q(x) + R(x) = ev_x(P)ev_x(Q) + ev_x(R)$ et $ev_x(1) = 1(x) = 1$, donc ev_x est un morphisme d'anneaux.

   De plus, pour tout $y \in \mathbf{C}$, si on note P_y le polynômes constant égal à y, on a $ev_x(P_y) = P_y(x) = y$, donc y est dans l'image de ev_x. Ainsi, ev_x est surjectif.

4. On a $\ker ev_x = \{P \in A \text{ tq } ev_x(P) = P(x) = 0\}$. Autrement dit, $\ker ev_x$ est l'ensemble des plynômes qui s'annulent en x. Par ailleurs, $I(E)$ est l'ensemble des polynômes qui s'annullent en tout point de E, c'est-à-dire qui s'annullent en x_1 et en x_2 et ... en x_n. Au final, $I(E) = \ker ev_{x_1} \cap \cdots \cap \ker ev_{x_n}$.

5. Les noyaux de morphismes sont des idéaux, donc $I(E)$ est une intersection d'idéaux : c'est donc un idéal.

6. D'après III.2.2, P s'annule en x si et seulement si il est multiple de $X - x$, c'est-à-dire si et seulement s'il appartient à $(X - x)$.

7. (a) On utilise la question 4 et II.8.2 : $I(E)$ est engendré par $\operatorname{ppcm}(X - x_1, \ldots, X - x_n)$. Or, d'après le lemme III.2.6, ces éléments sont premiers entre eux deux à deux, donc leur ppcm est leur produit.

   (b) En utilisant toujours II.8.2 et le fait que A est factoriel :

   $$I(E) \cap I(F) = (\operatorname{ppcm}(\prod_{x \in E} X - x, \prod_{y \in F}^{m} X - y)) = (\prod_{z \in E \cup F} X - z) = I(E \cup F)$$

   (c) De même,

   $$I(E) + I(F) = (\operatorname{pgcd}(\prod_{x \in E} X - x, \prod_{y \in F}^{m} X - y)) = (\prod_{z \in E \cap F} X - z) = I(E \cap F)$$

   (d) Enfin,

   $$I(E) \subset I(F) \iff \prod_{x \in E} X - x \text{ divise } \prod_{y \in F}^{m} X - y \iff F \subset E$$

Exercice 4. 1. (a) Alice doit envoyer $c_1 = 10^5 \mod 1112927 = 100000$. On remarque qu'il n'y a pas besoin de réduire modulo 1112927.

(b) On remarque que $c_2 = 8^5$. Or, c'est exactement ce que l'on obtiendrait en chiffrant 8 : comme dans la question précédente, il n'y aurait rien à réduire modulo 1112927. Comme RSA fonctionne et qu'il n'y a qu'un seul message clair possible pour chaque message chiffré, on a forcément $m_2 = 8$.

(c) À chaque fois que $m \leqslant n^{1/e}$ on aura $m^e \leqslant n$ et il n'y aura rien à réduire pendant l'étape de chiffrement. L'attaquant pourra donc simplement calculer $\sqrt[e]{c}$ (il s'agit de la racine classique, dans $\mathbf{R}$) et s'il trouve un nombre entier il saura que c'est le message.

2. (a) Il suffit à Ève de résoudre le système

$$\begin{cases} c'' = c_1 & \mod n_1 \\ c'' = c_2 & \mod n_2 \\ c'' = c_3 & \mod n_3 \end{cases}$$

comme on l'a fait à l'exercice 1. On est sûr qu'il y a une solution, unique modulo $n_1n_2n_3$, car n_1, $n2$ et n_3 sont premiers entre eux deux à deux.

(b) On a $m^3 < \min(n_1, n_2, n3)^3 < n_1n_2n_3$. On a donc $c'' = m^3$ dans $\mathbf{Z}$. Il suffit donc à Ève de calculer la racine cubique standard de c'' pour retrouver m.

(c) Cette méthode ne marche plus en général avec $e = 5$ car on n'a plus aucune garantie d'avoir $m^e < n_1n_2n_3$. En revanche, elle marche à nouveau si le nombre de destinataire est supérieur ou égal à e.

(d) On calcule x^2 avec une multiplication, puis $x^4 = (x^2)^2$ avec une deuxième multiplication, puis… $x^{2^{16}} = (x^{2^{15}})^2$ avec un seizième multiplication. Enfin, $x^{65537} = x^{2^{16}} \cdot x$ avec la dix-septième et dernière multiplication.

That's all folks !