Licence Informatique L3
(Ens-Lyon, Université Lyon-I)

Calcul formel et cryptographie
Contrôle du vendredi 20 mai 2005 . Corrigé

Exercice 1

1. Pour tout x de $\mathbb{F}_3$, vu le théorèmr de Fermat, $f(x) = x^3 - 2x = x - 2x = -x$. La seule solution de $f(x) = 0$ est donc 0.
2. Si $f(x) \equiv 0 \pmod 9$ on a $f(x) \equiv 0 \pmod 3$, et donc par le 1), $x \equiv 0 \pmod 3$. x est donc de l forme $x = 3z$ et il faut résoudre $f(3z) \equiv 0 \pmod 9$ soit

$$27z^3 - 6z + 3 \equiv -6z + 3 \equiv 0 \pmod 9,$$

et, après division par 3, $-2z + 1 \equiv 0 \pmod 3$. La solution $z \equiv 2 \pmod 3$ donne $x = 3(2 + 3k)$ soit $x \equiv 6 \pmod 9$.

3. C'est la méthode de Hensel. Par récurrence sur n. Soit x_n l'unique solution modulo 3^n de $f(x) \equiv 0 \pmod{3^n}$. Si x est une solution de $f(x) \equiv 0 \pmod{3^{n+1}}$ c'est évidemment une solution de $f(x) \equiv 0 \pmod{3^n}$. Par hypothèse de récurrence x est donc de la forme $x_n + 3^n z$. Or

$$\begin{aligned} f(x) &= (x_n + 3^n z)^3 - 2(x_n + 3^n z) + 3 \\ &\equiv x_n^3 - 2x_n + 3 - 2 \times 3^n z = f(x_n) - 2 \times 3^n z \pmod{3^{n+1}}. \end{aligned}$$

Par hypothèse il existe un entier y_n tel que $f(x_n) = 3^n y_n$. L'équation $f(x) \equiv 0 \pmod{3^{n+1}}$ s'écrit donc

$$y_n - 2z \equiv 0 \pmod 3.$$

Il y a une solution unique modulo 3 pour z, ce qui donne une unique valeur de x modulo 3^{n+1}.

Exercice 2

Soit a un entier non carré.

1. – ou bien $|a|$ n'est pas un carré, et dans ce cas l'un des facteurs premiers de a a un exposant impair dans la décomposition primaire de a. Si ce nombre est 2 on est dans le cas (b). Si l'exposant de 2 est pair on est dans le cas (c).

– ou bien $|a| = b^2$. Puisque a est non carré, $a \neq b^2 = |a|$, donc $a = -|a| = -b^2$.

2. Ecrivons $b = 2^\alpha c$ avec c impair. Par le théorème des restes chinois il existe m solution de $m \equiv 3 \pmod 4$ et $m \equiv 1 \pmod c$. Ceci implique que $m = 4k+3$ est impair, et premier avec c, donc aussi premier avec $b = 2^\alpha c$. Puisque m est premier avec b le symbole de Jacobi $\left(\frac{b}{m}\right)$ est egal à ± 1, et puisque $m \equiv 3 \pmod 4$ le symbole $\left(\frac{-1}{m}\right)$ est 1. On a alors
$$\left(\frac{a}{m}\right) = \left(\frac{-b^2}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{b}{m}\right)^2 = \left(\frac{-1}{m}\right) = -1.$$

3. Si $q = 1$ $\left(\frac{a}{5}\right) = \left(\frac{\pm 2^{2k+1}}{5}\right) = \left(\frac{\pm 1}{5}\right) \times \left(\frac{2}{5}\right)^{2k+1} = 1 \times (-1)^{2k+1} = -1.$
Si $q > 1$, par le théorème des restes chinois il existe $m > 0$ solution de $m \equiv 5 \pmod 8$ et $m \equiv 1 \pmod q$. On a alors
$$\left(\frac{a}{m}\right) = \left(\frac{2}{m}\right)^{2k+1} \times \left(\frac{\pm 1}{m}\right)\left(\frac{q}{m}\right) = -1 \times 1 \times \left(\frac{q}{m}\right)$$
car m n'étant pas congru à ± 1 moduo 8, on a $\left(\frac{2}{m}\right) = -1$. Enfin, par la loi de réciprocité quadratique $\left(\frac{q}{m}\right) = \left(\frac{m}{q}\right) = \left(\frac{1}{q}\right) = 1$, car $m \equiv 1 \pmod q$.

4. Soit u tel que $\left(\frac{u}{q}\right) = -1$. Comme q est impair par le théorème des restes chinois il existe m avec $m \equiv 5 \pmod 8$ et $m \equiv u \pmod q$. On a alors
$$\left(\frac{a}{m}\right) = \left(\frac{\pm 1}{m}\right)\left(\frac{2}{m}\right)^{2k} \times \left(\frac{q}{m}\right) = 1 \times 1 \times \left(\frac{q}{m}\right) = \left(\frac{q}{m}\right).$$
Par la loi de réciprocité quadratique $\left(\frac{q}{m}\right) = \left(\frac{m}{q}\right) = \left(\frac{u}{q}\right) = -1$.

5. Dans les trois cas il existe un entier impair $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots {}_k^{\alpha_k}$ tel que $\left(\frac{a}{m}\right) = -1$. Or par définion du symbole de Jacobi, $\left(\frac{a}{m}\right)$ est le produit des $\left(\frac{a}{p_i}\right)^{\alpha_i}$. L'un au moins des $\left(\frac{a}{p_i}\right)$ est donc -1.

Exercice 3

1. Il y a évidemment la solution nulle $u = 0$. Soit g un générateur du groupe cyclique $\mathbb{F}_p^\times$. Tout élément non nul u de $\mathbb{F}_p$ s'écrit $u = g^a$, pour un unique a, $0 \leq a < p-1$, et un tel u est solution de $u^e = u$ si et seulement $u^{e-1} = 1$, ou encore $g^{a(e-1)} = 1$ c'est à dire si $a(e-1)$ est un multiple de $p-1$. Soit $d = \text{pgcd}(e-1, p-1)$, et e' , p' définis par $e-1 = e'd$ et $p-1 = p'd$. e' et p' sont premiers entre eux, et $a(e-1)$ est un multiple de $p-1$ si et seulement si ae' est un multiple de p' c'est à dire si a est un multiple de p'. Les multiples de p' strictement inférieurs à $p-1$ sont $0, p', 2p', \ldots (d-1)p'$. Il y a donc d choix possibles pour a, c'est à dire d solutions non nulles de $u^e = u$. En rajoutant la solution 0, le nombre de solutions est $1 + d = 1 + \text{pgcd}(e-1, p-1)$.

2. Par le théorème des restes chinois, l'application $x \mapsto (x \bmod p, x \bmod q)$ est une bijection de $\mathbb{Z}/N\mathbb{Z}$ sur $F_p \times \mathbb{F}_q$. L'équation $x^e \equiv 0 \pmod N$ équivaut au système

$$x^e \equiv 0 \pmod p, \quad \text{et} \quad x^e \equiv 0 \pmod q.$$

Par la question 1, la première équation admet $1+\text{pgcd}(e-1, p-1)$ solutions modulo p. De même la deuxième équation admet $1+\text{pgcd}(e-1, q-1)$ solutions modulo q. Par le théorème des restes chinois, il y a donc $(1+\text{pgcd}(e-1, p-1)) \times (1+\text{pgcd}(e-1, q-1))$ solutions de $x^e = x \pmod N$.

Problème

1) C'est une question de cours, traitée en TD.

2) En utilisant la formule du binôme, on obtient successivement, modulo N,

$$\begin{aligned} C_1 &= M_1^3 \\ C_2 &\equiv (M_1+\delta)^3 \equiv M_1^3 + 3M_1^2\delta + 3M_1\delta^2 + \delta^3 \\ C_2 - C_1 + 2\delta^3 &\equiv 3M_1^2\delta + 3M_1\delta^2 + 3\delta^3. \\ C_2 + 2C_1 - \delta^3 &\equiv 3M_1^3 + 3M_1^2\delta + 3M_1\delta^2 \end{aligned}$$

d'où l'équation de l'énoncé, $M_1(C_2 - C_1 + 2\delta^3) \equiv \delta(C_2 + 2C_1 - \delta^3) \mod N$. Si Eve connait δ, multipliant modulo N les deux termes de cette égalité par l'inverse de $C_2 - C_1 + 2\delta^3$ elle obtient la valeur de M_1. Le quotient euclidien de M_1 par 2^k donne m.

3) Par définitions de C_2, C_1 et δ, on a, modulo N

$$f(M_1, \delta) \equiv M_1^3 - C_1 \equiv 0 \equiv M_2^3 - C_2 \equiv (M_1+\delta)^3 - C_1 \equiv g(M_1, \delta).$$

Autrement dit, pour $y = \delta$, M_1 est une racine commune de $f(X, y)$ et $g(X, y)$ modulo N.

4) Eve connait C_2 et C_1, donc f et g. Eve calcule le résultant $h(Y) = \text{Res}X(f, g) \in \mathbb{Z}[Y]$. Par la question précédente, pour $y = \delta$, et $f(M_1, y) \equiv 0 \equiv g(M_1, y) \pmod N$. Il en résulte que, les deux polynômes $f(X, y)$ et $g(X, y)$ ont une racine commune M_1 si on les considère comme des polynômes de $\mathbb{F}_p[X]$. Le résultant $h(\delta)$ est donc nul modulo p. De même $h(\delta)$ est nul modulo q, et donc nul modulo $N = pq$. Autrement dit δ est une racined modulo N de $h(Y)$.

5) Le degré de $h(Y)$ est majoré par $\deg_X(f) \times \deg_X(g) = 9$. Si $2^k < \frac{1}{3}N^{1/9}$, δ est une petite racine de $h(Y)$ modulo N,

$$|\delta| < \frac{1}{3}N^{\frac{1}{\deg h}}.$$

Eve calcule δ à l'aide de l'algorithme LLL, par la méthode de Coppersmith.