Correction du partiel du 2 mars 2010

Exercice 1

1) On a $7 \equiv 3$ mod. 4 et $p \equiv \varepsilon$ mod. 4 avec $\varepsilon = \pm 1$. D'après la loi de réciprocité quadratique, on a donc

$$\Big(\frac{7}{p}\Big) = \varepsilon\Big(\frac{p}{7}\Big).$$

Les carrés non nuls dans $\mathbb{F}_7$ sont les classes modulo 7 des entiers 1, 2 et 4. Par suite, $7 + p\mathbb{Z}$ est un carré dans $\mathbb{F}_p$ si et seulement si on a

$$\begin{cases} p \equiv \varepsilon \text{ mod. } 4 \\ p \equiv \varepsilon \text{ mod. } 7 \end{cases} \quad \text{ou} \quad \begin{cases} p \equiv \varepsilon \text{ mod. } 4 \\ p \equiv 2\varepsilon \text{ mod. } 7 \end{cases} \quad \text{ou} \quad \begin{cases} p \equiv \varepsilon \text{ mod. } 4 \\ p \equiv 4\varepsilon \text{ mod. } 7. \end{cases}$$

Compte tenu du théorème chinois, l'ensemble cherché est donc formé des nombres premiers congrus à ± 1, ± 9 ou ± 3 modulo 28.

2) Dans l'anneau $\mathbb{Z}[X]$, on a $X^4 + 4 = (X^2 + 2)^2 - 4X^2$. On a ainsi

$$X^4 + 4 = (X^2 + 2X + 2)(X^2 - 2X + 2).$$

2.1) Le discriminant réduit des polynômes $X^2 + 2X + 2$ et $X^2 - 2X + 2$ est -1, qui d'après l'hypothèse faite n'est pas un carré dans $\mathbb{F}_p$. Ils sont donc irréductibles sur $\mathbb{F}_p$, d'où l'assertion.

2.2) Dans ce cas, -1 est un carré dans $\mathbb{F}_p$, donc F a toutes ses racines dans $\mathbb{F}_p$. Si a est une racine carrée de -1 dans $\mathbb{F}_p$, les racines de F sont

$$-1 \pm a \quad \text{et} \quad 1 \pm a.$$

2.3) On a $5^2 \equiv -1$ mod. 13. Les racines cherchées sont donc les classes modulo 13 des entiers ± 4 et ± 6.

3.1) On a $F(n) = n^4 - n^2 + 1$ qui est impair, donc on a $p \neq 2$. Par ailleurs, on a $n^4 - n^2 \equiv 0$ mod. 3, d'où $p \neq 3$. De même, on a $F(n) \equiv 1$ mod. n, donc p ne divise pas n.

3.2) Dans $\mathbb{Z}[X]$, on a $X^6 + 1 = (X^2 + 1)F$. L'égalité $X^{12} - 1 = (X^6 - 1)(X^6 + 1)$ entraîne ainsi que F divise $X^{12} - 1$.

3.3) On vérifie que l'on a

$$X^6 - 1 = (X^2 + 1)F - 2 \quad \text{et} \quad F = (X^2 + 1)(X^2 - 2) + 3. \tag{1}$$

3.4) Par hypothèse, p divise $F(n)$. D'après la première égalité de (1), p ne divise pas n^6-1, sinon p serait égal à 2. En particulier, p ne divise pas n^2-1. D'après la seconde égalité de (1), p ne divise pas n^2+1, sinon p serait égal à 3. Par suite, p ne divise pas n^4-1, d'où l'assertion.

3.5) On a vu que p ne divise pas n, autrement dit, n est non nul modulo p. Soit d l'ordre de la classe de n dans $\mathbb{F}_p^*$. Puisque F divise $X^{12}-1$ (question 3.2), on a $n^{12}\equiv 1$ mod. p, donc d divise 12. D'après la question 3.4, on a $n^6\not\equiv 1$ mod. p et $n^4\not\equiv 1$ mod. p. Il en résulte que l'on a $d=12$. D'après le théorème de Lagrange, 12 divise $p-1$.

4) Posons

$$S=\sum_{k=1}^{p-1} k\Big(\frac{k}{p}\Big).$$

Compte tenu de l'indication de l'énoncé, on a

$$S=\sum_{k=1}^{p-1}(p-k)\Big(\frac{p-k}{p}\Big).$$

On a les égalités

$$\Big(\frac{p-k}{p}\Big)=\Big(\frac{-k}{p}\Big)=\Big(\frac{-1}{p}\Big)\Big(\frac{k}{p}\Big).$$

Puisque p est congru à 1 modulo 4, on a $\big(\frac{-1}{p}\big)=1$. On obtient ainsi

$$S=\sum_{k=1}^{p-1} p\Big(\frac{k}{p}\Big)-\sum_{k=1}^{p-1} k\Big(\frac{k}{p}\Big).$$

Par ailleurs, on a (formule (4) du chapitre II, valable pour tout p premier impair)

$$\sum_{k=1}^{p-1}\Big(\frac{k}{p}\Big)=0.$$

On en déduit l'égalité $2S=0$, d'où $S=0$.

5) Un entier pseudo-premier est un entier composé ≥ 2 tel que $2^{n-1}\equiv 1$ mod. n.

Supposons p^2 pseudo-premier. On a $2^{p^2-1}\equiv 1$ mod. p^2, d'où

$$2\equiv 2^{p^2} \text{ mod. } p^2 \quad \text{puis} \quad 2^{p-1}\equiv \big(2^{p^2}\big)^{p-1} \text{ mod. } p^2.$$

Soit φ la fonction indicatrice d'Euler. Puisque p est impair, on obtient (théorème d'Euler)

$$2^{p-1}\equiv 2^{p\varphi(p^2)}\equiv 1 \text{ mod. } p^2.$$

Inversement, si l'on a $2^{p-1} \equiv 1 \bmod. p^2$, en élevant les deux membres de cette congruence à la puissance $p+1$, on obtient $2^{p^2-1} \equiv 1 \bmod. p^2$, d'où le résultat.

Exercice 2

1) Soient P et Q des polynômes de $K[X]$ de degrés $< q$. Si $P = Q$, il est immédiat que $\widetilde{P} = \widetilde{Q}$. Inversement, supposons $\widetilde{P} = \widetilde{Q}$. Le polynôme $P - Q$ est de degré $< q$ et possède alors q racines. Il est donc nul i.e. on a $P = Q$.

2) Notons $\mathbf{P_q}$ l'ensemble des polynômes de $K[X]$ de degrés strictement plus petits que q et $F(K,K)$ l'ensemble des applications de K dans K. Considérons l'application

$$\Phi : \mathbf{P_q} \to F(K,K)$$

définie par $\Phi(P) = \widetilde{P}$. D'après la question précédente, Φ est une injection. Par ailleurs, $\mathbf{P_q}$ et $F(K,K)$ sont des ensembles de même cardinal q^q. Il en résulte que Φ est une bijection de $\mathbf{P_q}$ sur $F(K,K)$, d'où l'assertion.

3) L'application Φ induit une bijection entre le sous-ensemble de $\mathbf{P_q}$ formé des polynômes qui n'ont aucune racine dans K et le sous-ensemble de $F(K,K)$ formé des applications qui ne prennent pas la valeur 0. Il y a $(q-1)^q$ applications f de K de K telles que $f(a) \neq 0$ pour tout $a \in K$. Il y a donc $(q-1)^q$ polynômes de $\mathbf{P_q}$ qui n'ont aucune racine dans K.

4) Les polynômes unitaires de degré n de $K[X]$ qui satisfont la condition de l'énoncé sont ceux de la forme

$$(X^q - X)H + R, \tag{2}$$

où H est un polynôme unitaire de degré $n-q$. Le nombre cherché est donc le nombre de polynômes unitaires de degré $n-q$ de $K[X]$, qui est q^{n-q}.

5) Notons $\mathbf{R_n}$ l'ensemble des polynômes unitaires de degré n de $K[X]$ qui n'ont aucune racine dans K. Soit F un polynôme unitaire de degré n de $K[X]$. Pour tout $x \in K$, on a $x^q = x$. Par suite, F est dans $\mathbf{R_n}$ si et seulement si le reste de la division euclidienne de F par $X^q - X$ n'a aucune racine dans K. Les éléments de $\mathbf{R_n}$ sont donc les polynômes de la forme (2), où R est dans $\mathbf{P_q}$ sans racine dans K. Il y a $(q-1)^q$ tels polynômes R (question 3) et q^{n-q} polynômes H possibles (question 4). On a donc

$$|\mathbf{R_n}| = q^{n-q}(q-1)^q.$$

6) D'après la question précédente, il y a quatre polynômes de $\mathbb{F}_2[X]$ de degré 4 qui n'ont aucune racine dans $\mathbb{F}_2$. Ce sont

$$X^4 + X + 1, \quad X^4 + X^2 + 1, \quad X^4 + X^3 + 1 \quad \text{et} \quad X^4 + X^3 + X^2 + X + 1.$$

Exercice 3

1) D'après le critère d'Euler, on a

$$5^{11} \equiv \left(\frac{5}{23}\right) \text{ mod. } 23.$$

Par ailleurs, on a

$$\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

On obtient $5^{11} \equiv -1$ mod. 23, puis le résultat car 5^2 n'est pas congru à 1 modulo 23.

2) Modulo 23, on a

$$5^2 = 2, \quad 5^4 = 4, \quad 5^5 = -3, \quad 5^{10} = 9.$$

Il en résulte que leur clé secrète commune est $3^{10} + 23\mathbb{Z}$, autrement dit,

$$8 + 23\mathbb{Z}.$$
