Correction de l'examen du 16 avril 2010

Exercice 1

1.1) On a $K = \{0, 1, \alpha, 1+\alpha\}$. On a $\alpha^2 + \alpha \neq \alpha$. Puisque K est de caractéristique 2, on a $1 = -1$. Ainsi, $\alpha^2 + \alpha$ est distinct de 0 et $1 + \alpha$, d'où $\alpha^2 + \alpha = 1$.

1.2) Correction tenant compte de l'erreur d'énoncé : posons $f = X^3 + X + \alpha$. On a $\alpha^3 = \alpha^2 + \alpha = 1$, d'où les égalités

$$f(\alpha^2) = \alpha^6 + \alpha^2 + \alpha = 1 + \alpha^2 + \alpha = 0.$$

Par suite, f est réductible sur K.

1.3) Soit N le nombre cherché. Le cardinal de K est $q = 4$. Par ailleurs, le polynôme $X^{q^3} - X$ est le produit des polynômes irréductibles unitaires de $K[X]$ de degré divisant 3 (th. 3.5 du cours). On a donc $q^3 = q + 3N$. On obtient

$$N = 20.$$

2.1) L'égalité

$$n = \sum_{j=0}^{p-1} 10^j$$

implique $n \equiv p$ mod. 3. Si 3 divise n, on en déduit que $p = 3$, d'où une contradiction.

2.2) On a $10^p \equiv 1$ mod. ℓ. Soit d l'ordre multiplicatif de 10 modulo ℓ (10 est inversible modulo ℓ). On a $d \neq 1$ car ℓ est distinct de 3. On a donc $d = p$. Il en résulte que p divise $\ell - 1$. Puisque $\ell - 1$ est pair et que p est distinct de 2, l'entier $2p$ divise $\ell - 1$, d'où l'assertion.

2.3) On $11111 = \frac{10^5-1}{9}$. En utilisant la question précédente, recherchons un diviseur premier de cet entier. Il n'est pas divisible par 11. On constate ensuite qu'il ne l'est pas par 31, mais qu'il est divisible par 41 (il est inutile d'essayer 21 qui n'est pas premier). On vérifie alors que l'on a

$$11111 = 41 \times 271,$$

qui est un produit de deux nombres premiers.

3) Posons $n = 65$. On a $n - 1 = 2^6$. On a donc $8^2 \equiv -1$ mod. n, d'où l'assertion (la seconde condition de la définition 5.6 est satisfaite avec $i = 1$ et $t = 1$).

4) Posons $n = 2001$. On a $\sqrt{n} \simeq 44,7$. On vérifie que l'on a

$$45^2 - n = 24, \quad 46^2 - n = 115, \quad 47^2 - n = 208, \quad 48^2 - n = 303 \quad \text{et} \quad 49^2 - n = 400 = 20^2.$$

On en déduit que $n = 49^2 - 20^2 = 29 \times 69 = 3 \times 23 \times 29$.

5.1) On calcule les premiers termes de la suite $(x_i)_{i\in\mathbb{N}}$ définie par $x_0 = 2$ et l'égalité $x_{i+1} = f(x_i)$ mod. n. On a

$$x_0 = 2, \quad x_1 = 5, \quad x_2 = 26.$$

L'égalité $\text{pgcd}(x_2 - x_1, n) = 7$ implique alors $n = 7 \times 29$.

5.2) On a l'égalité du symbole de Legendre

$$\left(\frac{2}{29}\right) = -1.$$

Ainsi, 2 n'est pas un carré modulo 29, en particulier, 2 n'est pas un carré modulo n. L'équation proposée n'a donc pas de solutions dans $\mathbb{Z}/n\mathbb{Z}$.

5.3) Il s'agit de dénombrer les entiers a tels que $1 < a < n$ vérifiant la congruence

$$a^{n-1} \equiv 1 \text{ mod. } n. \tag{1}$$

D'après le théorème chinois, $(\mathbb{Z}/n\mathbb{Z})^*$ est isomorphe au produit de groupes cycliques $(\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/29\mathbb{Z})^*$. Le nombre de solutions de l'équation $x^{n-1} = 1$ dans $(\mathbb{Z}/7\mathbb{Z})^*$ est le pgcd de $n-1$ avec 6, qui est 2. De même, le nombre de solutions de cette équation dans $(\mathbb{Z}/29\mathbb{Z})^*$ est le pgcd de $n-1$ avec 28, qui vaut 2. Il y a donc quatre éléments x dans $\mathbb{Z}/n\mathbb{Z}$ tels que $x^{n-1} = 1$. Il y a ainsi trois entiers a tels que $1 < a < n$ vérifiant la condition (1).

Exercice 2

1) Il s'agit de montrer que n divise $q - 1$. D'après l'hypothèse faite, c'est par exemple une conséquence directe du théorème de structure du groupe $E(K)$ (th. 7.5).
On peut aussi procéder comme suit. On déduit de l'hypothèse que le groupe $E[n]$ des points de n-torsion de E est d'ordre n^2, et donc que n est premier avec la caractéristique de K (th. 7.2). Par ailleurs, $E[n]$ est contenu dans $E(K)$. Le groupe des racines n-ièmes de l'unité est donc contenu dans K (th. 7.3). C'est un sous-groupe d'ordre n de K^*, ce qui entraîne que n divise $q - 1$.

2) On a

$$q = n^2 + rn + 1. \tag{1}$$

Le groupe $E(K)$ est d'ordre n^2. D'après le théorème de Hasse, on a donc

$$|t| \leq 2\sqrt{q}.$$

En élevant les deux membres de cette inégalité au carré, on obtient

$$4 + r^2n^2 + 4rn \leq 4q = 4n^2 + 4rn + 4,$$

d'où $r^2 \leq 4$, puis $|r| \leq 2$.

3) Puisque r vaut 0, ± 1 ou ± 2, l'égalité (1) implique le résultat.

4) Pour tout entier a, on vérifie que a^2+1 est congru à $1, 2, 5$ ou 10 modulo 12, et que a^2+a+1 est congru à $1, 3, 7$ ou 9 modulo 12. Cela entraîne l'assertion.

Exercice 3

1) Le discriminant du polynôme $X^3 - X + 1 \in \mathbb{F}_5[X]$ est $-23 = 2$. Il est non nul, donc E est une courbe elliptique définie sur $\mathbb{F}_5$.

2) On vérifie que l'on a

$$E(\mathbb{F}_5) = \Big\{O, (0,1), (0,4), (1,1), (1,4), (3,0), (4,1), (4,4)\Big\},$$

où $O = [0,1,0]$.

3) Le groupe $E(\mathbb{F}_5)$ est abélien d'ordre 8. Il est donc isomorphe à l'un des groupes

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/8\mathbb{Z}.$$

Par ailleurs, un point (x, y) de E est d'ordre 2 si et seulement si $y = 0$. Le point $(3, 0)$ est donc le seul point d'ordre 2 de $E(\mathbb{F}_5)$. Ainsi $E(\mathbb{F}_5)$ contient un unique sous-groupe d'ordre 2. Il est donc isomorphe à $\mathbb{Z}/8\mathbb{Z}$.
(Remarquons que la première possibilité ne se produit jamais, vu qu'une courbe elliptique possède au plus quatre points de 2-torsion.)

4) Notons F le polynôme caractéristique du Frobenius de E. Puisque l'ordre de $E(\mathbb{F}_5)$ est 8, la trace du Frobenius de E est $6 - 8 = -2$. On a donc

$$F = X^2 + 2X + 5 \in \mathbb{Z}[X].$$

5) Soient α et β les racines de F dans $\mathbb{C}$. On a (th. 7.8)

$$\big|E(\mathbb{F}_{25})\big| = 5^2 + 1 - (\alpha^2 + \beta^2).$$

Les égalités $\alpha + \beta = -2$ et $\alpha\beta = 5$ entraînent

$$\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = -6.$$

On obtient

$$\big|E(\mathbb{F}_{25})\big| = 32.$$

6) Le point $(3,0)$ est d'ordre 2 dans $E(\mathbb{F}_5)$. Les abscisses des deux autres points d'ordre 2 de E sont donc racines d'un polynôme de degré 2 de $\mathbb{F}_5[X]$ (qui est X^2+3X+3). Elles sont ainsi dans $\mathbb{F}_{25}$, d'où l'assertion.

7) Le groupe $E(\mathbb{F}_{25})$ n'est pas cyclique car il contient un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ qui n'est pas cyclique.

8) Le groupe $E(\mathbb{F}_{25})$ est d'ordre 32. Il n'est pas cyclique et il contient au plus quatre points de 2-torsion (en fait ici exactement quatre). Il en résulte qu'il est isomorphe à l'un des groupes

$$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}.$$

Supposons $E(\mathbb{F}_{25})$ isomorphe à $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$. Il contient alors un sous-groupe isomorphe à $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Cela entraîne que le sous-groupe des points de 4-torsion de E est contenu dans $E(\mathbb{F}_{25})$. D'après l'assertion admise, on obtient ainsi une contradiction. Par suite, $E(\mathbb{F}_{25})$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$.
