Catalogue

Niels Feld*

12 octobre 2024

Question 1 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient K un corps de caractéristique $p \notin \{2,3\}$ et $\overline{K}$ une clôture algébrique de K.
Soient $A, B \in K$ tels que $4A^3 + 27B^2 \neq 0$.
On peut définir une courbe elliptique E sur K comme l'ensemble

$$\{(x,y) \in \overline{K} \,|\, y^2 = x^3 + Ax + B\}.$$

☐ 0%	☐ 40%	☐ 80%
☐ 10%	☐ 50%	☐ 90%
☐ 20%	☐ 60%	■ 100%
☐ 30%	☐ 70%	

Commentaire après réponse:
C'est la définition choisie dans ce cours même si ce n'est pas la définition idéale.

Question 2 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient K un corps de caractéristique $p \notin \{2,3\}$ et $\overline{K}$ une clôture algébrique de K.
Soient $A, B \in K$ tels que $4A^3 + 27B^2 \neq 0$.
Soit une courbe elliptique E sur K définie par l'équation

$$y^2 = x^3 + Ax + B.$$

Soient $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_3 = (x_3, y_3) \in E(\overline{K}) \setminus \{\infty\}$ tels que $P_1 + P_2 = P_3$ et $x_1 \neq x_2$.
Alors,

$$x_3 = m^2 - x_1 - x_2, y_3 = m(x_1 - x_3) - y_1$$

où $m = \frac{y_2 - y_1}{x_2 - x_1}$.

☐ 0%	☐ 40%	☐ 80%
☐ 10%	☐ 50%	☐ 90%
☐ 20%	☐ 60%	■ 100%
☐ 30%	☐ 70%	

Commentaire après réponse:
Voir le cours [Washington, p. 28].

Question 3 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient K un corps de caractéristique $p \notin \{2,3\}$ et $\overline{K}$ une clôture algébrique de K.
Soient $A, B \in K$ tels que $4A^3 + 27B^2 \neq 0$.
Soit une courbe elliptique E sur K définie par l'équation

$$y^2 = x^3 + Ax + B.$$

Soient $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E(\overline{K}) \setminus \{\infty\}$ et $P_3 = (x_3, y_3)$ tels que $P_1 + P_2 = P_3$ et $x_1 \neq x_2$ et $y_1 \neq y_2$.
Alors,

$$P_1 + P_2 = \infty.$$

■ 0%	☐ 40%	☐ 80%
☐ 10%	☐ 50%	☐ 90%
☐ 20%	☐ 60%	☐ 100%
☐ 30%	☐ 70%	

Commentaire après réponse:
Voir le cours [Washington, p. 28].

*Merci à Damien Mégy

Question 4 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient K un corps de caractéristique $p \notin \{2,3\}$ et $\overline{K}$ une clôture algébrique de K.
Soient $A, B \in K$ tels que $4A^3 + 27B^2 \neq 0$.
Soit une courbe elliptique E sur K définie par l'équation

$$y^2 = x^3 + Ax + B.$$

Soient $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E(\overline{K}) \setminus \{\infty\}$ et $P_3 = (x_3, y_3)$ tels que $P_1 + P_2 = P_3$ et $P_1 = P_2$ et $y_1 \neq 0$.
Alors,

$$x_3 = m^2 - 2x_1, y_3 = m(x_1 - x_3) - y_1,$$

où $m = \frac{3x_1^2 + A}{2y_1}$.

- ☐ 0%
- ☐ 10%
- ☐ 20%
- ☐ 30%
- ☐ 40%
- ☐ 50%
- ☐ 60%
- ☐ 70%
- ☐ 80%
- ☐ 90%
- ■ 100%

Commentaire après réponse:
Voir le cours [Washington, p. 28].

Question 5 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient K un corps de caractéristique $p \notin \{2,3\}$ et $\overline{K}$ une clôture algébrique de K.
Soient $A, B \in K$ tels que $4A^3 + 27B^2 \neq 0$.
Soit une courbe elliptique E sur K définie par l'équation

$$y^2 = x^3 + Ax + B.$$

Soit $P \in E(\overline{K})$.
Alors,

$$P + P = \infty.$$

- ■ 0%
- ☐ 10%
- ☐ 20%
- ☐ 30%
- ☐ 40%
- ☐ 50%
- ☐ 60%
- ☐ 70%
- ☐ 80%
- ☐ 90%
- ☐ 100%

Commentaire après réponse:
Voir le cours [Washington, p. 28].

Question 6 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soit E la courbe elliptique sur $\mathbb{Q}$ définie par l'équation

$$y^2 = \frac{x(x+1)(2x+1)}{6}$$

Alors, on a

$$(0,0) + (1,1) = (1,1)$$

dans E.

- ■ 0%
- ☐ 10%
- ☐ 20%
- ☐ 30%
- ☐ 40%
- ☐ 50%
- ☐ 60%
- ☐ 70%
- ☐ 80%
- ☐ 90%
- ☐ 100%

Commentaire après réponse:
On a $(0,0) + (1,1) = (\frac{1}{2}, \frac{-1}{2})$.

Question 7 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soit E la courbe elliptique sur $\mathbb{Q}$ définie par l'équation

$$y^2 = x^3 - 25x.$$

Alors, on a

$$(0,0) + (-5,0) = (-5,0)$$

dans E.

- ■ 0%
- ☐ 10%
- ☐ 20%
- ☐ 30%
- ☐ 40%
- ☐ 50%
- ☐ 60%
- ☐ 70%
- ☐ 80%
- ☐ 90%
- ☐ 100%

Commentaire après réponse:
On a

$$(0,0) + (-5,0) = (5,0)$$

Question 8 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soit K un corps fini de caractéristique $p \notin \{2,3\}$.
Soit E une courbe elliptique sur K.
Alors, l'ensemble $E(K)$ est un groupe fini.

- ☐ 0%
- ☐ 10%
- ☐ 20%
- ☐ 30%
- ☐ 40%
- ☐ 50%
- ☐ 60%
- ☐ 70%
- ☐ 80%
- ☐ 90%
- ■ 100%

Commentaire après réponse:

Question 9 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soit E une courbe elliptique sur $\mathbb{Q}$.
Alors, l'ensemble $E(\mathbb{Q})$ est un groupe abélien de type fini.

- [ ] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [x] 100%

Commentaire après réponse:
Cf le théorème de Mordell-Weil.

Question 10 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Le polynôme

$$x^3 + 6xyz + 9yz^2$$

est homogène.

- [ ] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [x] 100%

Commentaire après réponse:
Voir le cours [Washington, p. 32-33]

Question 11 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient K un corps de caractéristique $p \notin \{2,3\}$ et E la courbe elliptique sur K définie par l'équation

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

où $e_1, e_2, e_3 \in K$. On note

$$x_1 = (e_2 - e_1)^{-1}(x - e_1)$$

$$y_1 = (e_2 - e_1)^{-3/2} y$$

$$\lambda = \frac{e_3 - e_1}{e_2 - e_1}.$$

Alors, $\lambda \notin \{0, 1\}$ et

$$y_1^2 = x_1(x_1 - 1)(x_1 - \lambda).$$

- [ ] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [x] 100%

Commentaire après réponse:
Voir aussi le cours [Washington, p. 49]

Question 12 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient K un corps de caractéristique $p \notin \{2,3\}$, $\overline{K}$ une clôture algébrique de K, $A_1, A_2, B_1, B_2 \in K$ et, pour $i \in \{1,2\}$, E_i la courbe elliptique sur K, de j-invariant notée j_i, définie par l'équation

$$y_i^2 = x_i^3 + A_i x_i + B_i.$$

Alors, $j_1 = j_2$ si, et seulement si, il existe $\mu \in \overline{K}$ tel que

$$A_2 = \mu^6 A_1$$

$$B_2 = \mu^4 B_1.$$

- [x] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [ ] 100%

Commentaire après réponse:
Cf [Washington, p.60].

Question 13 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient K un corps de caractéristique $p \notin \{2,3\}$, E une courbe elliptique sur K et α un endomorphisme non-trivial de E. On écrit

$$\alpha(x,y) = (r_1(x), r_2(x)y)$$

où r_1, r_2 sont des fractions rationnelles. On écrit $r_1(x) = p(x)/q(x)$ où p, q sont des polynômes premiers entre eux.
Alors,

$$\deg(\alpha) = \max(\deg(p), \deg(q)).$$

- [ ] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [x] 100%

Commentaire après réponse:
Cf [Washington, p.65].

Question 14 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2, 3\}$, E une courbe elliptique sur K et α un endomorphisme non-trivial de E. On écrit

$$\alpha(x, y) = (r_1(x), r_2(x)y)$$

où r_1, r_2 sont des fractions rationnelles. On écrit $r_1(x) = p(x)/q(x)$ où p, q sont des polynômes premiers entre eux.
Alors, α est séparable si $r_1' \neq 0$.

- [ ] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [x] 100%

Commentaire après réponse:
Cf [Washington, p.65].

Question 15 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient $A = 123$ et $B = 789$. Soit E la courbe elliptique sur $\mathbb{Q}$ définie par

$$y^2 = x^3 + Ax + B$$

et soit α l'endomorphisme de E défini, pour tout point P de E, par $\alpha(P) = 2P$.
Alors, α est séparable.

- [ ] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [x] 100%

Commentaire après réponse:
Voir[Washington, p. 66].

Question 16 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient $n \in \mathbb{N}^*$, p un nombre premier, $q = p^n$, $\mathbb{F}_q$ un corps à q éléments, $A, B \in \mathbb{F}_q$, E la courbe elliptique sur $\mathbb{F}_q$ d'équation

$$y^2 = x^3 + Ax + B$$

et ϕ_q le Frobenius de E.
Alors, ϕ_q est séparable.

- [x] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [ ] 100%

Commentaire après réponse:
Cf [Washington, p.66].

Question 17 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2, 3\}$, E une courbe elliptique sur K, α un endomorphisme non-trivial inséparable de E.
Alors,

$$\deg(\alpha) = \operatorname{Card} \ker(\alpha)$$

- [x] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [ ] 100%

Commentaire après réponse:
Voir [Washington, p.67].

Question 18 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2, 3\}$, E une courbe elliptique sur K, α un endomorphisme séparable de E.
Alors,

$$\deg(\alpha) = \operatorname{Card} \ker(\alpha)$$

- [x] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [ ] 100%

Commentaire après réponse:
Voir [Washington, p.67].

Question 19 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2, 3\}$, E une courbe elliptique sur K, α un endomorphisme non-trivial inséparable de E.
Alors,

$$\deg(\alpha) > \operatorname{Card} \ker(\alpha).$$

- [ ] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [x] 100%

Commentaire après réponse:
Voir [Washington, p.67].

Question 20 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2,3\}$, $\overline{K}$ une clôture algébrique de K, E une courbe elliptique sur K, α un endomorphisme de E. Alors,

$$\alpha : E(\overline{K}) \to E(\overline{K})$$

est surjectif.

■ 0%	☐ 40%	☐ 80%
☐ 10%	☐ 50%	☐ 90%
☐ 20%	☐ 60%	☐ 100%
☐ 30%	☐ 70%	

Commentaire après réponse:
Voir [Washington, p.69].

Question 21 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient $n \in \mathbb{N}$, $p \notin \{2,3\}$ un nombre premier, $q = p^n$, $\mathbb{F}_q$ un corps à q élément, $(r,s) \in \mathbb{Z}^2 \setminus \{0,0\}$, ϕ_q l'endomorphisme de Frobenius de E.
Alors, $r \cdot \phi_q + s$ est séparable si, et seulement si, p ne divise pas r.

■ 0%	☐ 40%	☐ 80%
☐ 10%	☐ 50%	☐ 90%
☐ 20%	☐ 60%	☐ 100%
☐ 30%	☐ 70%	

Commentaire après réponse:
Voir [Washington, p.72].

Question 22 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2,3\}$, $\overline{K}$ une clôture algébrique de K, $A, B \in K$, E la courbe elliptique sur K définie par l'équation

$$y^2 = x^3 + Ax + B$$

et $(x,y) \neq \infty$ un point de E.
Si $3x^2 + A = 0$, alors $y \neq 0$.

☐ 0%	☐ 40%	☐ 80%
☐ 10%	☐ 50%	☐ 90%
☐ 20%	☐ 60%	■ 100%
☐ 30%	☐ 70%	

Commentaire après réponse:
On démontre la contraposée.
Par hypothèse, le polynôme $p(X) = X^3 + AX + B$ possède x comme racine et x est une racine simple, donc $p'(x) \neq 0$.

Question 23 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2,3\}$, $\overline{K}$ sa clôture algébrique, $A, B \in K$, E la courbe elliptique sur K définie par l'équation

$$y^2 = x^3 + Ax + B$$

et α un endomorphisme non-trivial de E. Il existe des polynômes $p, q, s, t \in K[x]$ tels que p et q sont premiers entre eux, r, s sont premiers entre eux, et

$$\alpha(x,y) = (p(x)/q(x), ys(x)/t(x))$$

pour tout point (x,y) de E tels que $q(x) \neq 0$ et $t(x) \neq 0$.
Soit $x_0 \in \overline{K}$ tel que $t(x_0) = 0$.
Alors, $q(x_0) = 0$.

☐ 0%	☐ 40%	☐ 80%
☐ 10%	☐ 50%	☐ 90%
☐ 20%	☐ 60%	■ 100%
☐ 30%	☐ 70%	

Commentaire après réponse:
Voir [Washington, p.89].

Question 24 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps, p et q deux polynômes à coefficients dans K sans racines communes et tel que $q \neq 0$.
Alors, la dérivée de la fraction rationnelle $\frac{p}{q}$ est identiquement nulle si, et seulement si $p' = q' = 0$.

☐ 0%	☐ 40%	☐ 80%
☐ 10%	☐ 50%	☐ 90%
☐ 20%	☐ 60%	■ 100%
☐ 30%	☐ 70%	

Commentaire après réponse:
On suppose $\frac{p}{q}$ possède une dérivée nulle. Alors, $p'q = q'p$ donc q divise q' donc $q' = 0$; de même pour p. La réciproque est triviale.

Question 25 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2,3\}$, $\overline{K}$ une clôture algébrique de K, E une courbe elliptique sur K et $n \in \mathbb{N}^*$. Alors,

$$E[n] = \{P \in E(K) \,|\, nP = \infty\}.$$

- [x] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [ ] 100%

Commentaire après réponse:
Voir [Washington, p. 91].

Question 26 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2,3\}$, $\overline{K}$ une clôture algébrique de K, et E une courbe elliptique sur K.
Alors, le groupe $E[3]$ est isomorphe au groupe $\mathbb{Z}/(3)$.

- [x] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [ ] 100%

Commentaire après réponse:
Voir [Washington, p. 92].

Question 27 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2,3\}$, E une courbe elliptique sur K et $n \in \mathbb{N}^*$.
Si p ne divise pas n, alors le groupe $E[n]$ est isomorphe au groupe $\mathbb{Z}/(n^2)$.

- [x] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [ ] 100%

Commentaire après réponse:
Voir [Washington, p. 93].

Question 28 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p > 3$, E une courbe elliptique sur K.
On dit que E est *supersingulière* si

$$E[p] \simeq \{0\}.$$

- [ ] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [x] 100%

Commentaire après réponse:
Voir [Washington, p. 93].

Question 29 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2,3\}$, E une courbe elliptique sur K, $j \in \mathbb{N}^*$, et P un point de E.
Si P est d'ordre p, alors il existe un point Q de E d'ordre p^j.

- [ ] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [x] 100%

Commentaire après réponse:
Voir [Washington, p. 100].

Question 30 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2,3\}$, $\overline{K}$ une clôture algébrique de K, E une courbe elliptique sur K, $n \in \mathbb{N}^*$ premier à p, e_n l'accouplement de Weil associé à E et $\{T_1, T_2\}$ une base du $\mathbb{Z}$-module $E[n]$.
Alors, $e_n(T_1, T_2)$ est une racine primitive n-ième.

- [ ] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [x] 100%

Commentaire après réponse:
Voir [Washington, p.101].

Question 31 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient K un corps de caractéristique $p \notin \{2,3\}$, $\overline{K}$ une clôture algébrique de K, $n \in \mathbb{N}^*$ premier à p, $\mu_n = \{x \in \overline{K} \,|\, x^n = 1\}$, et E une courbe elliptique sur K
Si $E[n] \subset E(K)$, alors $\mu_n \subset K$.

- [ ] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [x] 100%

Commentaire après réponse:
Voir [Washington, p. 102].

Question 32 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$. Alors, il existe $n \in \mathbb{N}^*$ tel que

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/(n)$$

ou il existe $n_1, n_2 \in \mathbb{N}^*$ tels que $n_1 | n_2$ et

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/(n_1) \oplus \mathbb{Z}/(n_2).$$

- [ ] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [x] 100%

Commentaire après réponse:
Voir [Washington, p.110].

Question 33 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$. Alors,

$$|q + 1 - \mathrm{Card}(E(\mathbb{F}_q))| \geq 2\sqrt{q}.$$

- [x] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [ ] 100%

Commentaire après réponse:
Voir [Washington, p.110].

Question 34 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient $\mathbb{F}_q$ un corps fini, $\overline{\mathbb{F}}_q$ une clôture algébrique, E une courbe elliptique sur $\mathbb{F}_q$, ϕ_q le Frobenius de E, et P un point de E. Alors, $P \in E(\mathbb{F}_q)$ si, et seulement si $\phi_q(P) = P$.

- [ ] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [x] 100%

Commentaire après réponse:
Voir [Washington, p.112].

Question 35 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient $\mathbb{F}_q$ un corps fini, E une courbe elliptique sur $\mathbb{F}_q$, ϕ_q le Frobenius de E, et $n \in \mathbb{N}^*$,

$$\ker(\phi_q^n - 1) = \{0\}.$$

- [x] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [ ] 100%

Commentaire après réponse:
Voir [Washington, p.112].

Question 36 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient $\mathbb{F}_q$ un corps fini, E une courbe elliptique sur $\mathbb{F}_q$, ϕ_q le Frobenius de E, et $n \in \mathbb{N}^*$.
Alors, $\phi_q^n - 1$ est séparable.

- [ ] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [x] 100%

Commentaire après réponse:
Voir [Washington, p.113].

Question 37 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient $\mathbb{F}_q$ un corps fini, E une courbe elliptique sur $\mathbb{F}_q$, ϕ_q le Frobenius de E, et $n \in \mathbb{N}^*$.
Alors,

$$\mathrm{Card}(E(\mathbb{F}_{q^n})) = \deg(\phi_q^n).$$

- [x] 0%
- [ ] 10%
- [ ] 20%
- [ ] 30%
- [ ] 40%
- [ ] 50%
- [ ] 60%
- [ ] 70%
- [ ] 80%
- [ ] 90%
- [ ] 100%

Commentaire après réponse:
Voir [Washington, p.113].

Question 38 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient $\mathbb{F}_q$ un corps fini, E une courbe elliptique sur $\mathbb{F}_q$, ϕ_q le Frobenius de E, et $a = q + 1 - \mathrm{Card}(\mathbb{F}_q)$.
Alors,

$$\phi_q^2 + a\phi_q + q = 0.$$

■ 0% □ 10% □ 20% □ 30% □ 40% □ 50% □ 60% □ 70% □ 80% □ 90% □ 100%

Commentaire après réponse:
Voir [Washington, p.114].

Question 39 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient $\mathbb{F}_q$ un corps fini, E une courbe elliptique sur $\mathbb{F}_q$, ϕ_q le Frobenius de E, m un entier premier avec q, $(\phi_q)_m$ la restriction du Frobenius à $E[m]$ et $a = q + 1 - \mathrm{Card}(\mathbb{F}_q)$.
Alors,

$$a \equiv \mathrm{Tr}((\phi_q)_m) \pmod m.$$

□ 0% □ 10% □ 20% □ 30% □ 40% □ 50% □ 60% □ 70% □ 80% □ 90% ■ 100%

Commentaire après réponse:
Voir [Washington, p.115].

Question 40 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient $\mathbb{F}_q$ un corps fini, E une courbe elliptique sur $\mathbb{F}_q$, $a = q+1-\mathrm{Card}(E(\mathbb{F}_q))$, ϕ_q le Frobenius de E, α, β les deux racines du polynôme caractéristique de ϕ_q et $n \in \mathbb{N}$. On note $s_n = \alpha^n + \beta^n$.
Alors, si $n > 0$,

$$s_{n+1} = as_n + qs_{n-1}.$$

■ 0% □ 10% □ 20% □ 30% □ 40% □ 50% □ 60% □ 70% □ 80% □ 90% □ 100%

Commentaire après réponse:
Voir [Washington, p.116].

Question 41 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient $\mathbb{F}_q$ un corps fini, $A, B \in \mathbb{F}_q$, E la courbe elliptique sur $\mathbb{F}_q$ définie par l'équation

$$y^2 = x^3 + Ax + B.$$

Alors,

$$\mathrm{Card}(\mathbb{F}_q) = q + 1 - \sum_{x \in \mathbb{F}_q} \Big(\frac{x^3 + Ax + B}{\mathbb{F}_q}\Big).$$

■ 0% □ 10% □ 20% □ 30% □ 40% □ 50% □ 60% □ 70% □ 80% □ 90% □ 100%

Commentaire après réponse:
Voir [Washington, p.118].

Question 42 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient $\mathbb{F}_q$ un corps fini de caractéristique $p \notin \{2, 3\}$, E une courbe elliptique sur $\mathbb{F}_q$. Si E est supersingulière, alors

$$\mathrm{Card}(E(\mathbb{F}_q)) \equiv 1 \pmod p.$$

□ 0% □ 10% □ 20% □ 30% □ 40% □ 50% □ 60% □ 70% □ 80% □ 90% ■ 100%

Commentaire après réponse:
Voir [Washington, p.143].

Question 43 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient $p \notin \{2, 3\}$ un nombre premier, E une courbe elliptique sur $\mathbb{F}_p$. Si

$$\mathrm{Card}(E(\mathbb{F}_p)) = p$$

alors, E est supersingulière.

■ 0% □ 10% □ 20% □ 30% □ 40% □ 50% □ 60% □ 70% □ 80% □ 90% □ 100%

Commentaire après réponse:
Voir [Washington, p.144].

Question 44 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient $p \notin \{2, 3, 5\}$ un nombre premier, E une courbe elliptique sur $\mathbb{F}_p$. Si $E(\mathbb{F}_p)$ contient un élément d'ordre p, alors

$$\operatorname{Card} E(\mathbb{F}_p) = p.$$

□ 0%	□ 40%	□ 80%
□ 10%	□ 50%	□ 90%
□ 20%	□ 60%	■ 100%
□ 30%	□ 70%	

Commentaire après réponse:
Cf [Washington, p. 180]. Comme p divise $\operatorname{Card} E(\mathbb{F}_p)$, il existe k un entier naturel non-nul tel que $\operatorname{Card} E(\mathbb{F}_p) = kp$. L'inégalité de Hasse peut s'écrire :

$$|\sqrt{\operatorname{Card} E(\mathbb{F}_p)} - \sqrt{p}| \leq 1$$

donc

$$|\sqrt{k} - 1| \leq 1/\sqrt{p} \leq 1/\sqrt{7} \leq 0.4$$

donc

$$\sqrt{k} \leq 1.4$$

donc $k < 2$ donc $k = 1$.

Question 45 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient $p \notin \{2, 3\}$ un nombre premier, $n \in \mathbb{N}^*$, $q = p^n$, E une courbe elliptique sur $\mathbb{F}_q$. Si

$$\operatorname{Card} E(\mathbb{F}_q) = q,$$

alors

$$\operatorname{Card} E(\mathbb{F}_{q^2}) = q^2,$$

■ 0%	□ 40%	□ 80%
□ 10%	□ 50%	□ 90%
□ 20%	□ 60%	□ 100%
□ 30%	□ 70%	

Commentaire après réponse:
Cf [Washington, p. 180].

Question 46
Soient K un corps de caractéristique $p \notin \{2, 3\}$, $A, B \in K$ et E la courbe elliptique sur K définie par

$$y^2 = x^3 + Ax + B.$$

On note $j(E)$ le j-invariant de E.
Calculer $j(E)\frac{4A^3+27B^2}{4A^3} - 1000$.

□ 0	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	■ 7	□ 8	□ 9
□ 0	□ 1	■ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9
□ 0	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	■ 8	□ 9

Commentaire après réponse:
Voir aussi [Washington, p. 60.

Question 47
Soient $A = 23$ et $B = 456$. Soit E la courbe elliptique sur $\mathbb{Q}$ définie par

$$y^2 = x^3 + Ax + B$$

et soit α l'endomorphisme de E défini, pour tout point P de E, par $\alpha(P) = 2P$. Alors α est un homomorphisme et

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)),$$

où R_1, R_2 sont des fractions rationnelles.
Il existe $\lambda \in \mathbb{N}$ tel que

$$R_1(x, y) = \left(\frac{3x^2 + A}{2y}\right)^2 - \lambda x.$$

Calculer λ.

■ 0	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9
■ 0	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9
□ 0	□ 1	■ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ 8	□ 9

Commentaire après réponse:
On a

$$R_1(x, y) = \left(\frac{3x^2 + A}{2y}\right)^2 - 2x$$

et

$$R_2(x, y) = \left(\frac{3x^2 + A}{2y}\right)\left(3x - \left(\frac{3x^2 + A}{2y}\right)^2\right) - y.$$

Voir aussi [Washington, p. 64].

Question 48
Soient $A = 456$ et $B = 789$. Soit E la courbe elliptique sur $\mathbb{Q}$ définie par

$$y^2 = x^3 + Ax + B$$

et soit α l'endomorphisme de E défini, pour tout point P de E, par $\alpha(P) = 2P$. Alors α est un homomorphisme et

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)),$$

où R_1, R_2 sont des fractions rationnelles.
Il existe $\lambda \in \mathbb{N}$ tel que

$$R_2(x, y) = \left(\frac{3x^2 + A}{2y}\right)\left(3x - \left(\frac{3x^2 + \lambda}{2y}\right)^2\right) - y.$$

Calculer λ.

☐0 ☐1 ☐2 ☐3 ■4 ☐5 ☐6 ☐7 ☐8 ☐
☐0 ☐1 ☐2 ☐3 ☐4 ■5 ☐6 ☐7 ☐8 ☐
☐0 ☐1 ☐2 ☐3 ☐4 ☐5 ■6 ☐7 ☐8 ☐

Commentaire après réponse:
On a

$$R_1(x, y) = \left(\frac{3x^2 + A}{2y}\right)^2 - 2x$$

et

$$R_2(x, y) = \left(\frac{3x^2 + A}{2y}\right)\left(3x - \left(\frac{3x^2 + A}{2y}\right)^2\right) - y.$$

Voir aussi [Washington, p. 64].

Question 49
Soient $A = 456$ et $B = 789$. Soit E la courbe elliptique sur $\mathbb{Q}$ définie par

$$y^2 = x^3 + Ax + B$$

et soit α l'endomorphisme de E défini, pour tout point P de E, par $\alpha(P) = 2P$. Alors α est un homomorphisme et on écrit

$$\alpha(x, y) = (r_1(x), r_2(x)y),$$

où r_1, r_2 sont des fractions rationnelles.
Il existe $\lambda \in \mathbb{N}$ tel que

$$r_1(x) = \frac{x^4 - 2Ax^2 - \lambda \cdot Bx + A^2}{4(x^3 + Ax + B)}.$$

Calculer λ.

■0 ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9
■0 ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9
☐0 ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ■8 ☐9

Commentaire après réponse:

$$r_1(x) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}.$$

Voir aussi [Washington, p. 66].

Question 50
Soient $A = 123$ et $B = 789$. Soit E la courbe elliptique sur $\mathbb{Q}$ définie par

$$y^2 = x^3 + Ax + B$$

et soit α l'endomorphisme de E défini, pour tout point P de E, par $\alpha(P) = 2P$.
Calculer $\deg(\alpha)$.

■0 ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9
■0 ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9
☐0 ☐1 ☐2 ☐3 ■4 ☐5 ☐6 ☐7 ☐8 ☐9

Commentaire après réponse:
Voir aussi [Washington, p. 66].

Question 51
Soient E une courbe elliptique définie sur le corps fini $\mathbb{F}_{11}$ et ϕ_{11} son Frobenius.
Calculer $\deg(\phi_{11})$.

■0 ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9
☐0 ■1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9
☐0 ■1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9

Commentaire après réponse:
Voir [Washington, p. 66].

Question 52
Soient a, b, c les trois racines du polynôme

$$x^3 + 4x^2 - 7x - 13.$$

Calculer abc.

■0	□1	□2	□3	□4	□5	□6	□7	□8	□9
□0	■1	□2	□3	□4	□5	□6	□7	□8	□9
□0	□1	□2	■3	□4	□5	□6	□7	□8	□9

Commentaire après réponse:
Formule de Viète.

Question 53
Si $\lambda \in \mathbb{Q} \setminus \{0, 1\}$, on note $j(\lambda)$ le j-invariant de la courbe elliptique d'équation

$$y^2 = x(x-1)(x-\lambda).$$

Soit $\mathbf{j} \in \mathbb{Q} \setminus \{0, 1728\}$, on note a le nombre de $\lambda \in \mathbb{Q} \setminus \{0, 1\}$ tel que $j(\lambda) = \mathbf{j}$.
Calculer a.

■0	□1	□2	□3	□4	□5	□6	□7	□8	□9
■0	□1	□2	□3	□4	□5	□6	□7	□8	□9
□0	□1	□2	□3	□4	□5	■6	□7	□8	□9

Commentaire après réponse:
Cf [Washington, p. 87].

Question 54
Soit E la courbe elliptique sur$\mathbb{R}$ définie par

$$y^2 = x^3 - 2.$$

On note α l'endomorphisme de E induit par la conjugaison complexe, i.e.

$$\alpha(x, y) = (\overline{x}, \overline{y})$$

pour tout point $(x, y) \neq \infty$ de E. On note α_2 l'endomorphisme $\mathbb{Z}$-linéaire de $E[2]$ induit par α.
Calculer $\mathrm{Tr}(\alpha_2) \in \mathbb{Z}$.

■0	□1	□2	□3	□4	□5	□6	□7	□8	□9
■0	□1	□2	□3	□4	□5	□6	□7	□8	□9
□0	□1	■2	□3	□4	□5	□6	□7	□8	□9

Commentaire après réponse:
Cf [Washington, p. 94].

Question 55
Soient $M, N \in \mathbf{M}_2(\mathbb{Q})$ deux matrices carrées de taille 2×2 et $\mathrm{Com}(N)^T$ la transposée de la comatrice de N.
On suppose que $\det(M + N) = 500$, $\det(M) = 150$, $\det(N) = 30$.
Calculer la trace de la matrice $M\,\mathrm{Com}(N)^T$.

□0	□1	□2	■3	□4	□5	□6	□7	□8	□9
□0	□1	■2	□3	□4	□5	□6	□7	□8	□9
■0	□1	□2	□3	□4	□5	□6	□7	□8	□9

Commentaire après réponse:
Voir [Washington, p. 106].

Question 56
Soient $M, N \in \mathbf{M}_2(\mathbb{Q})$ deux matrices carrées de taille 2×2 et $\mathrm{Com}(N)^T$ la transposée de la comatrice de N.
On suppose que $\det(M + N) = 11$, $\det(M) = 5$, $\det(N) = 3$.
Soient $a = 2$, $b = 3$.
Calculer $\det(aM + bN)$.
(Conseil : trouver une relation entre la trace de $M\,\mathrm{Com}(N)^T$, et $\det(M + N), \det(M), \det(N)$.

■0	□1	□2	□3	□4	□5	□6	□7	□8	□9
□0	□1	□2	□3	□4	□5	□6	■7	□8	□9
□0	□1	□2	□3	□4	■5	□6	□7	□8	□9

Commentaire après réponse:
Voir [Washington, p. 106].

Question 57
Soit E la courbe elliptique sur $\mathbb{F}_5$ définie par l'équation

$$y^2 = x^3 + x + 1.$$

Calculer $\mathrm{Card}(E(\mathbb{F}_5))$.

■0	□1	□2	□3	□4	□5	□6	□7	□8	□9
■0	□1	□2	□3	□4	□5	□6	□7	□8	□9
□0	□1	□2	□3	□4	□5	□6	□7	□8	■9

Commentaire après réponse:
Voir [Washington, p. 108].