

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

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

<input checked="" type="checkbox"/> 0%	<input type="checkbox"/> 40%	<input type="checkbox"/> 80%
<input type="checkbox"/> 10%	<input type="checkbox"/> 50%	<input type="checkbox"/> 90%
<input type="checkbox"/> 20%	<input type="checkbox"/> 60%	<input type="checkbox"/> 100%
<input type="checkbox"/> 30%	<input type="checkbox"/> 70%	

Commentaire après réponse:

On préfère l'équation

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

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 L/K une extension 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

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

Alors, l'ensemble de points L -rationnels est défini par

$$E(L) = \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

<input type="checkbox"/> 0%	<input type="checkbox"/> 40%	<input type="checkbox"/> 80%
<input type="checkbox"/> 10%	<input type="checkbox"/> 50%	<input type="checkbox"/> 90%
<input type="checkbox"/> 20%	<input type="checkbox"/> 60%	<input checked="" type="checkbox"/> 100%
<input type="checkbox"/> 30%	<input type="checkbox"/> 70%	

Commentaire après réponse:

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 $y_1 \neq y_2$.

Alors,

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

où $m = \frac{x_2 - x_1}{y_2 - y_1}$.

<input checked="" type="checkbox"/> 0%	<input type="checkbox"/> 40%	<input type="checkbox"/> 80%
<input type="checkbox"/> 10%	<input type="checkbox"/> 50%	<input type="checkbox"/> 90%
<input type="checkbox"/> 20%	<input type="checkbox"/> 60%	<input type="checkbox"/> 100%
<input type="checkbox"/> 30%	<input type="checkbox"/> 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 \bar{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 $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E(\bar{K}) \setminus \{\infty\}$ et $P_3 = (x_3, y_3)$ tels que $P_1 + P_2 = P_3$ et $P_1 = P_2$ et $y_1 = 0$.

Alors,

$$P_1 + P_2 = \infty.$$

☐ 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 \bar{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 $P = (x, y) \in E(\bar{K}) \setminus \{\infty\}$.

Alors,

$$-P = (x, -y).$$

☐ 0%
☐ 10%
☐ 20%
☐ 30%

☐ 40%
☐ 50%
☐ 60%
☐ 70%

☐ 80%
☐ 90%
☒ 100%

Commentaire après réponse:

Voir le cours [Washington, p. 29].

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

$$(0, 0) + (1, 1) = \left(\frac{1}{2}, \frac{-1}{2}\right)$$

dans E .

☐ 0%
☐ 10%
☐ 20%
☐ 30%

☐ 40%
☐ 50%
☐ 60%
☐ 70%

☐ 80%
☐ 90%
☒ 100%

Commentaire après réponse:

On a $(0, 0) + (1, 1) = \left(\frac{1}{2}, \frac{-1}{2}\right)$.

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:

Question 8 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 fini.

☒ 0%
☐ 10%
☐ 20%
☐ 30%

☐ 40%
☐ 50%
☐ 60%
☐ 70%

☐ 80%
☐ 90%
☐ 100%

Commentaire après réponse:

Cf le théorème de Mordell-Weil.

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 corps finiment engendré.

<input checked="" type="checkbox"/>	0%	<input type="checkbox"/>	40%	<input type="checkbox"/>	80%
<input type="checkbox"/>	10%	<input type="checkbox"/>	50%	<input type="checkbox"/>	90%
<input type="checkbox"/>	20%	<input type="checkbox"/>	60%	<input type="checkbox"/>	100%
<input type="checkbox"/>	30%	<input type="checkbox"/>	70%		

Commentaire après réponse:

Cf le théorème de Mordell-Weil.

Il n'y a a priori pas de structure de corps.

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

Le polynôme

$$x^3 + 3x^2z + 2yz^2$$

est homogène.

<input type="checkbox"/>	0%	<input type="checkbox"/>	40%	<input type="checkbox"/>	80%
<input type="checkbox"/>	10%	<input type="checkbox"/>	50%	<input type="checkbox"/>	90%
<input type="checkbox"/>	20%	<input type="checkbox"/>	60%	<input checked="" type="checkbox"/>	100%
<input type="checkbox"/>	30%	<input type="checkbox"/>	70%		

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, soit $G(u, v) \in K[u, v]$ un polynôme homogène non-nul et $(u_0, v_0) \in K^2 \setminus \{0, 0\}$.

Alors, il existe un entier $k \geq 0$ et un polynôme $H(u, v) \in K[u, v]$ tels que $H(u_0, v_0) \neq 0$ et

$$G(u, v) = (v_0u - u_0v)H(u, v).$$

<input type="checkbox"/>	0%	<input type="checkbox"/>	40%	<input type="checkbox"/>	80%
<input type="checkbox"/>	10%	<input type="checkbox"/>	50%	<input type="checkbox"/>	90%
<input type="checkbox"/>	20%	<input type="checkbox"/>	60%	<input checked="" type="checkbox"/>	100%
<input type="checkbox"/>	30%	<input type="checkbox"/>	70%		

Commentaire après réponse:

Voir le cours [Washington, p. 36]

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

$$A_2 = \mu^4 A_1$$

$$B_2 = \mu^6 B_1.$$

<input type="checkbox"/>	0%	<input type="checkbox"/>	40%	<input type="checkbox"/>	80%
<input type="checkbox"/>	10%	<input type="checkbox"/>	50%	<input type="checkbox"/>	90%
<input type="checkbox"/>	20%	<input type="checkbox"/>	60%	<input checked="" type="checkbox"/>	100%
<input type="checkbox"/>	30%	<input type="checkbox"/>	70%		

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. Alors,

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

<input checked="" type="checkbox"/>	0%	<input type="checkbox"/>	40%	<input type="checkbox"/>	80%
<input type="checkbox"/>	10%	<input type="checkbox"/>	50%	<input type="checkbox"/>	90%
<input type="checkbox"/>	20%	<input type="checkbox"/>	60%	<input type="checkbox"/>	100%
<input type="checkbox"/>	30%	<input type="checkbox"/>	70%		

Commentaire après réponse:

On aimerait que p, q soient des polynômes premiers entre eux. 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 $p' \neq 0$.

<input checked="" type="checkbox"/> 0%	<input type="checkbox"/> 40%	<input type="checkbox"/> 80%
<input type="checkbox"/> 10%	<input type="checkbox"/> 50%	<input type="checkbox"/> 90%
<input type="checkbox"/> 20%	<input type="checkbox"/> 60%	<input type="checkbox"/> 100%
<input type="checkbox"/> 30%	<input type="checkbox"/> 70%	

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

Question 15 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

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

Pour tout point (x, y) de E , on note

$$\Phi(x, y) = (x^p, y^p).$$

Alors, Φ est un endomorphisme de E .

<input checked="" type="checkbox"/> 0%	<input type="checkbox"/> 40%	<input type="checkbox"/> 80%
<input type="checkbox"/> 10%	<input type="checkbox"/> 50%	<input type="checkbox"/> 90%
<input type="checkbox"/> 20%	<input type="checkbox"/> 60%	<input type="checkbox"/> 100%
<input type="checkbox"/> 30%	<input type="checkbox"/> 70%	

Commentaire après réponse:

A priori, on n'a pas $A^p = A$ mais seulement $A^q = A$.

Question 16 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,

$$\deg(\alpha) > \text{Card ker}(\alpha)$$

<input type="checkbox"/> 0%	<input type="checkbox"/> 40%	<input type="checkbox"/> 80%
<input type="checkbox"/> 10%	<input type="checkbox"/> 50%	<input type="checkbox"/> 90%
<input type="checkbox"/> 20%	<input type="checkbox"/> 60%	<input checked="" type="checkbox"/> 100%
<input type="checkbox"/> 30%	<input type="checkbox"/> 70%	

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

Question 17 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2, 3\}$, \bar{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 α un endomorphisme non-trivial séparable de E . On considère r_1, r_2 des fractions rationnelles et p, q des polynômes premiers entre eux tels que, pour tout point (x, y) de E , on a $\alpha(x, y) = (r_1(x), r_2(x)y)$ et $r_1 = p/q$.

On note S l'ensemble des $x \in \bar{K}$ tel que

$$(pq' - p'q)(x)q(x) = 0.$$

Alors, il existe $(a, b) \in E(\bar{K})$ tel que toutes les conditions suivantes sont satisfaites :

1. $a \neq 0$,
2. $b \neq 0$,
3. $(a, b) \neq \infty$,
4. $\deg(p(x) - aq(x)) = \deg(\alpha)$,
5. $a \notin r_1(S)$,
6. $(a, b) \in \alpha(E(\bar{K}))$.

<input type="checkbox"/> 0%	<input type="checkbox"/> 40%	<input type="checkbox"/> 80%
<input type="checkbox"/> 10%	<input type="checkbox"/> 50%	<input type="checkbox"/> 90%
<input type="checkbox"/> 20%	<input type="checkbox"/> 60%	<input checked="" type="checkbox"/> 100%
<input type="checkbox"/> 30%	<input type="checkbox"/> 70%	

Commentaire après réponse:
Voir [Washington, p.68].

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

Alors,

$$\alpha : E(\bar{K}) \rightarrow E(\bar{K})$$

est surjectif.

<input type="checkbox"/> 0%	<input type="checkbox"/> 40%	<input type="checkbox"/> 80%
<input type="checkbox"/> 10%	<input type="checkbox"/> 50%	<input type="checkbox"/> 90%
<input type="checkbox"/> 20%	<input type="checkbox"/> 60%	<input checked="" type="checkbox"/> 100%
<input type="checkbox"/> 30%	<input type="checkbox"/> 70%	

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

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 , et $n \in \mathbb{N}^*$. On note $[n]$ l'endomorphisme de E défini par la multiplication par n . Alors, $[n]$ est séparable.

<input checked="" type="checkbox"/> 0%	<input type="checkbox"/> 40%	<input type="checkbox"/> 80%
<input type="checkbox"/> 10%	<input type="checkbox"/> 50%	<input type="checkbox"/> 90%
<input type="checkbox"/> 20%	<input type="checkbox"/> 60%	<input type="checkbox"/> 100%
<input type="checkbox"/> 30%	<input type="checkbox"/> 70%	

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

Question 20 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 inséparable si, et seulement si, p ne divise pas s .

<input checked="" type="checkbox"/> 0%	<input type="checkbox"/> 40%	<input type="checkbox"/> 80%
<input type="checkbox"/> 10%	<input type="checkbox"/> 50%	<input type="checkbox"/> 90%
<input type="checkbox"/> 20%	<input type="checkbox"/> 60%	<input type="checkbox"/> 100%
<input type="checkbox"/> 30%	<input type="checkbox"/> 70%	

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

Question 21 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 $y = 0$, alors, $3x^2 + A \neq 0$.

<input type="checkbox"/> 0%	<input type="checkbox"/> 40%	<input type="checkbox"/> 80%
<input type="checkbox"/> 10%	<input type="checkbox"/> 50%	<input type="checkbox"/> 90%
<input type="checkbox"/> 20%	<input type="checkbox"/> 60%	<input checked="" type="checkbox"/> 100%
<input type="checkbox"/> 30%	<input type="checkbox"/> 70%	

Commentaire après réponse:
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 22 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient $\mathbb{P}_{\mathbb{R}}^2$ le plan projectif réel et $\mathbb{S}^2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$. On note $\psi : \mathbb{S}^2 \rightarrow \mathbb{P}_{\mathbb{R}}^2$ définie, pour tout $(x, y, z) \in \mathbb{S}^2$ par

$$\psi(x, y, z) = [x : y : z].$$

Alors, ψ est une bijection.

<input checked="" type="checkbox"/> 0%	<input type="checkbox"/> 40%	<input type="checkbox"/> 80%
<input type="checkbox"/> 10%	<input type="checkbox"/> 50%	<input type="checkbox"/> 90%
<input type="checkbox"/> 20%	<input type="checkbox"/> 60%	<input type="checkbox"/> 100%
<input type="checkbox"/> 30%	<input type="checkbox"/> 70%	

Commentaire après réponse:
L'image réciproque d'un élément $[x : y : z]$ par contient deux éléments.

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 $q(x_0) \neq 0$.
Alors, $t(x_0) \neq 0$.

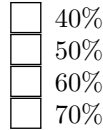
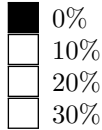
<input type="checkbox"/> 0%	<input type="checkbox"/> 40%	<input type="checkbox"/> 80%
<input type="checkbox"/> 10%	<input type="checkbox"/> 50%	<input type="checkbox"/> 90%
<input type="checkbox"/> 20%	<input type="checkbox"/> 60%	<input checked="" type="checkbox"/> 100%
<input type="checkbox"/> 30%	<input type="checkbox"/> 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 les polynômes p et q sont constants.



Commentaire après réponse:

En fait, on a que la dérivée de la fraction rationnelle

$$\frac{p}{q}$$

est identiquement nulle si, et seulement si $p' = q' = 0$.

En effet, on suppose $\frac{p}{q}$ possède une dérivée nulle.

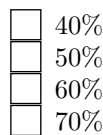
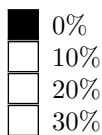
Alors, $p'q = q'p$ donc q divise q' (car q est premier à p) donc $q' = 0$; de même pour p . La réciproque est triviale.

Il se peut que $p' = 0$ sans pour autant que p soit constant (e.g. $p = X^p$ où $p > 0$ est la caractéristique de K).

Question 25 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :

Soient K un corps de caractéristique $p \notin \{2, 3\}$, \bar{K} une clôture algébrique de K , et E une courbe elliptique sur K .

Alors, le groupe $E[2]$ est isomorphe au groupe $\mathbb{Z}/(2)$.



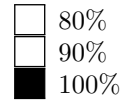
Commentaire après réponse:

Voir [Washington, p. 91].

Question 26 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :

Soient K un corps de caractéristique $p \notin \{2, 3\}$, \bar{K} une clôture algébrique de K , et E une courbe elliptique sur K .

Alors, le groupe $E[3]$ est isomorphe au groupe $\mathbb{Z}/(3) \oplus \mathbb{Z}/(3)$.



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 divise n , alors le groupe $E[n]$ est isomorphe au groupe $\mathbb{Z}/(n) \oplus \mathbb{Z}/(n)$.



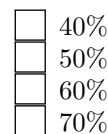
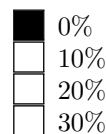
Commentaire après réponse:

Voir [Washington, p. 93].

Question 28 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :

Soient K un corps de caractéristique $p \notin \{2, 3\}$, E une courbe elliptique sur K et $n \in \mathbb{N}^*$.

Si $p > 0$ et p divise n , alors on écrit $n = p^r n'$ où $p \nmid n'$ et $r \in \mathbb{N}^*$ de sorte que le groupe $E[n]$ est isomorphe au groupe $\mathbb{Z}/(n) \oplus \mathbb{Z}/(n)$ ou bien au groupe $\mathbb{Z}/(n) \oplus \mathbb{Z}/(n')$.



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 $p > 3$, E une courbe elliptique sur K . On dit que E est *ordinaire* si

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

☒ 0%
☐ 10%
☐ 20%
☐ 30%

☐ 40%
☐ 50%
☐ 60%
☐ 70%

☐ 80%
☐ 90%
☐ 100%

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

Question 30 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient x, y, A, B des indéterminées. On définit les polynômes de division $\psi_m \in \mathbb{Z}[x, y, A, B]$ par

$$\psi_0 = 0$$

$$\psi_1 = 1$$

$$\psi_2 = 2y$$

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$$

$$\psi_4 =$$

$$4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{pour } m \geq 2$$

$$\psi_{2m} = (2y)^{-1} (\psi_m) (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$$

pour $m \geq 3$.

Si $n > 5$ est pair, alors ψ_n est un polynôme dans $2y\mathbb{Z}[x, y^2, A, B]$.

☐ 0%
☐ 10%
☐ 20%
☐ 30%

☐ 40%
☐ 50%
☐ 60%
☐ 70%

☐ 80%
☐ 90%
☒ 100%

Commentaire après réponse:
Voir [Washington, p. 95].

Question 31 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2, 3\}$, \bar{K} une clôture algébrique de K , $n \in \mathbb{N}^*$, et $\mu_n = \{x \in \bar{K} \mid x^n = 1\}$. Alors, $\text{Card}(\mu_n) = n$.

☒ 0%
☐ 10%
☐ 20%
☐ 30%

☐ 40%
☐ 50%
☐ 60%
☐ 70%

☐ 80%
☐ 90%
☐ 100%

Commentaire après réponse:

On veut que $n \in \mathbb{N}^*$ soit premier avec p (sinon, on peut avoir des racines multiples).

Question 32 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2, 3\}$, \bar{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 $E[n]$. Si $S \in E[n]$ vérifie $e_n(S, T_1) = e_n(S, T_2) = 1$, alors $S = \infty$.

☐ 0%
☐ 10%
☐ 20%
☐ 30%

☐ 40%
☐ 50%
☐ 60%
☐ 70%

☐ 80%
☐ 90%
☒ 100%

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

Question 33 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient K un corps de caractéristique $p \notin \{2, 3\}$, \bar{K} une clôture algébrique de K , $n \in \mathbb{N}^*$ premier à p , $\mu_n = \{x \in \bar{K} \mid x^n = 1\}$, et E une courbe elliptique sur K . Alors $E[n] \subset E(K)$ et $\mu_n \not\subset K$.

☒ 0%
☐ 10%
☐ 20%
☐ 30%

☐ 40%
☐ 50%
☐ 60%
☐ 70%

☐ 80%
☐ 90%
☐ 100%

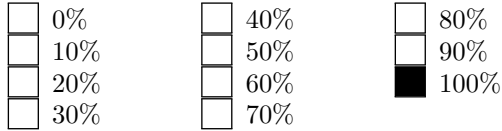
Commentaire après réponse:
Voir [Washington, p. 102].

Question 34 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :

Soient K un corps de caractéristique $p \notin \{2, 3\}$, \bar{K} une clôture algébrique de K , $n \in \mathbb{N}^*$ premier à p , E une courbe elliptique sur K , α un endomorphisme de E , α_n l'endomorphisme $\mathbb{Z}/(n)$ -linéaire de $E[n]$ induit par α .

Alors,

$$\det(\alpha_n) \equiv \deg(\alpha) \pmod{n}.$$

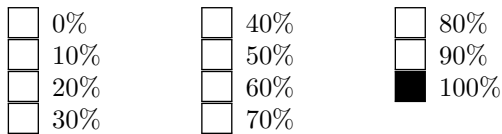


Commentaire après réponse:
Voir [Washington, p. 103].

Question 35 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :

Soient K un corps de caractéristique $p \notin \{2, 3\}$, $n \in \mathbb{N}^*$ premier à p , E une courbe elliptique sur K , e_n l'accouplement de Weil associé à E , P un point d'ordre n et $Q \in E[n]$.

Il existe $k \in \mathbb{N}$, $Q = kP$ si, et seulement si, $e_n(P, Q) = 1$.



Commentaire après réponse:

Supposons $e_n(P, Q) = 1$. On sait que $E[n] = \mathbb{Z}/(n) \oplus \mathbb{Z}/(n)$ donc $Q = kP + k'P'$ où $k, k' \in \{0, \dots, n-1\}$ et P' est tel que (P, P') forme une base de $E[n]$. On a alors $e_n(P, P')^k = e_n(P, k'P') = e_n(P, Q - kP) = 1$. Or $e_n(P, P')$ est une racine n -ème primitive donc n divise k' donc $k' = 0$.

La réciproque est claire.

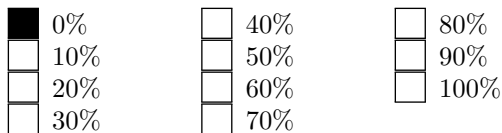
Question 36 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :

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

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



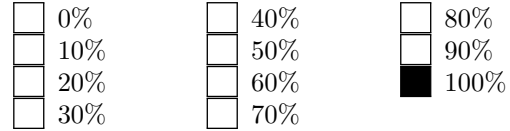
Commentaire après réponse:
Voir [Washington, p.110].

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 $a = q + 1 - \text{Card}(\mathbb{F}_q)$.

Alors,

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



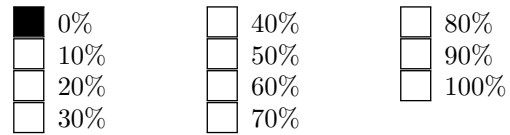
Commentaire après réponse:
Voir [Washington, p.114].

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 , α, β les deux racines du polynôme caractéristique de ϕ_q et $n \in \mathbb{N}^*$.

Alors,

$$E(\mathbb{F}_{q^n}) = q^n + 1 + (\alpha^n + \beta^n).$$



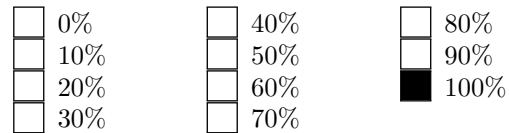
Commentaire après réponse:
Voir [Washington, p.116].

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 , $a = q + 1 - \text{Card}(E(\mathbb{F}_q))$, 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 $n > 0$,

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



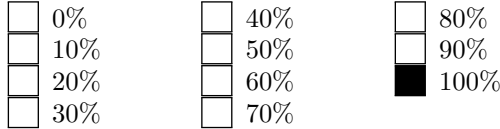
Commentaire après réponse:
Voir [Washington, p.116].

Question 40 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

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

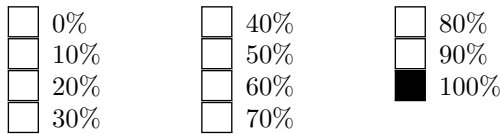
Alors,

$$\text{Card}(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q} \right).$$



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

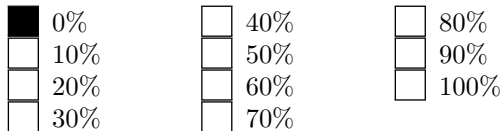
Question 41 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soit E une courbe elliptique sur \mathbb{F}_{101} admettant un point d'ordre 116. Alors, $E(\mathbb{F}_{101})$ est cyclique.



Commentaire après réponse:
Voir [Washington, p.120].

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

$$\text{Card}(E(\mathbb{F}_q)) \equiv 0 \pmod{p}.$$

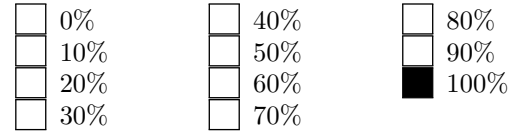


Commentaire après réponse:
Voir [Washington, p.143].

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

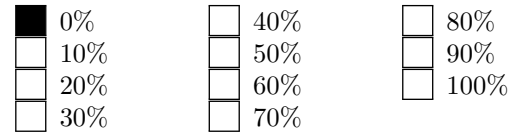
$$\text{Card}(E(\mathbb{F}_p)) = p + 1$$

alors, E est supersingulière.



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

Question 44 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient $p \notin \{2, 3\}$ un nombre premier, $n \in \mathbb{N}^*$, $q = p^n$, E une courbe elliptique sur \mathbb{F}_q . Soient P, Q deux points dans $E(\mathbb{F}_q)$ et N l'ordre de P . On suppose que N est premier avec q . Alors, il existe $k \in \mathbb{Z}$ tel $Q = kP$ si, et seulement si, $NQ = \infty$.

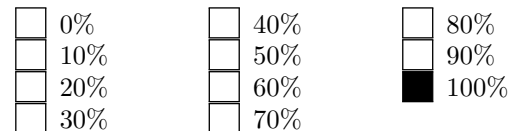


Commentaire après réponse:
Voir [Washington, p.168].

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 , et $N \in \mathbb{N}^*$.

Alors, il existe $m \in \mathbb{N}^*$ tel que

$$E[N] \subset E(\mathbb{F}_{q^m}).$$



Commentaire après réponse:
Voir [Washington, p.168].

Question 46 **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 , et $m \in \mathbb{N}^*$. Soit l un nombre premier tel que l divise $\text{Card}(E(\mathbb{F}_q))$, $E[l] \not\subset E(\mathbb{F}_q)$, et l ne divise pas $q(q-1)$.

Si $E[l] \subset E(\mathbb{F}_{q^m})$, alors

$$q^m \equiv 1 \pmod{l}.$$

☐ 0%
☐ 10%
☐ 20%
☐ 30%

☐ 40%
☐ 50%
☐ 60%
☐ 70%

☐ 80%
☐ 90%
☒ 100%

Commentaire après réponse:

Voir [Washington, p.171].

Question 47 **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 , et $m \in \mathbb{N}^*$.

Alors,

$$\text{Card}(E(\mathbb{F}_q)[m]) = \text{Card}(E(\mathbb{F}_q)/mE(\mathbb{F}_q)).$$

☐ 0%
☐ 10%
☐ 20%
☐ 30%

☐ 40%
☐ 50%
☐ 60%
☐ 70%

☐ 80%
☐ 90%
☒ 100%

Commentaire après réponse:

D'après le premier théorème d'isomorphisme et le théorème de Lagrange, si f est un endomorphisme d'un groupe fini G , alors l'indice de $f(G)$ dans G est égal au cardinal du noyau de f . En particulier, c'est vrai si $G = E(\mathbb{F}_q)$ et f est la multiplication par m .

Question 48 **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

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

alors

$$\text{Card } E(\mathbb{F}_{q^2}) \neq q^2,$$

☐ 0%
☐ 10%
☐ 20%
☐ 30%

☐ 40%
☐ 50%
☐ 60%
☐ 70%

☐ 80%
☐ 90%
☒ 100%

Commentaire après réponse:

Cf [Washington, p. 180].

Question 49 **Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :**

Soient $p \notin \{2, 3\}$ un nombre premier tel que $p \equiv 1 \pmod{3}$, $b \in \mathbb{F}_p^\times$, E la courbe elliptique sur \mathbb{F}_p définie par l'équation

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

Alors, le groupe $E(\mathbb{F}_p)$ est cyclique.

☒ 0%
☐ 10%
☐ 20%
☐ 30%

☐ 40%
☐ 50%
☐ 60%
☐ 70%

☐ 80%
☐ 90%
☐ 100%

Commentaire après réponse:

Cf [Washington, p. 201].

Question 50 **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 et β deux endomorphismes non-nuls de E .

Si α est inséparable et β est inséparable, alors $\alpha + \beta$ est inséparable.

☐ 0%
☐ 10%
☐ 20%
☐ 30%

☐ 40%
☐ 50%
☐ 60%
☐ 70%

☐ 80%
☐ 90%
☒ 100%

Commentaire après réponse:

Question 51 **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 et β deux endomorphismes non-nuls de E .

Si α est inséparable et β est inséparable, alors $\alpha + \beta$ est séparable.

☒ 0%
☐ 10%
☐ 20%
☐ 30%

☐ 40%
☐ 50%
☐ 60%
☐ 70%

☐ 80%
☐ 90%
☐ 100%

Commentaire après réponse:

Si α est inséparable et β est inséparable, alors $\alpha + \beta$ est inséparable.

Question 52

On admet qu'il existe un unique couple $(a, b) \in \mathbb{N}^2$ tel que $a > 1$ et

$$b^2 = \sum_{i=1}^a i^2.$$

Calculer b .

<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Commentaire après réponse: On vérifie que $a = 24, y = 70$ conviennent. Voir aussi [Washington, pages 15-17].

Question 53

On considère l'équation

$$v^2 = u^4 + 1$$

et on pose

$$x = \frac{2(v+1)}{u^2}$$

$$y = \frac{4(v+1)}{u^3}.$$

Il existe $\lambda \in \mathbb{N}$ tel que

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

Calculer λ .

<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Commentaire après réponse:
Voir aussi [Washington, p. 52].

Question 54

On note j le j -invariant de la courbe elliptique définie sur \mathbb{Q} par

$$y^2 = x^3 + \frac{3 \times 728}{1000}x + \frac{2 \times 728}{1000}.$$

Calculer j .

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Commentaire après réponse:
Voir aussi [Washington, p. 61].

Question 55

Soient $A = 123$ 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

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

Calculer λ .

<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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 62

Soient $B \in \mathbb{F}_{11}^\times$ et E la courbe elliptique sur \mathbb{F}_{11} définie par l'équation

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

Calculus Card($E(\mathbb{F}_{11})$).

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.144].

Question 63

Soit E la courbe elliptique sur \mathbb{F}_{107} définie par l'équation

$$y^2 = x^3 + 41.$$

Calculer $\text{Card}(E(\mathbb{F}_{107}))$.

Commentaire après réponse:

Voir [Washington, p.144].

Question 64

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

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

Soit $P = (2, 1) \in E$.

Calculer l'ordre de P .

Figure 1 shows a 3x10 grid of squares. The top row contains squares labeled 0 through 9, with the square labeled 9 also labeled 'Y'. The middle row contains squares labeled 0 through 9. The bottom row contains squares labeled 0 through 9, with the square labeled 3 also labeled 'X'.

Commentaire après réponse:

Voir [Washington, p.152].

Question 65

Il existe $\lambda \in \{0, \dots, 810\}$ tel que, pour tout $x \in \mathbb{F}_{811}$,

$$\left(\frac{x}{\mathbb{F}_{811}}\right) = x^\lambda$$

(où le symbole de Legendre est utilisé dans le membre de gauche).

Calculus λ .

Commentaire après réponse:

On a pour tout q impair,

$$\left(\frac{x}{\mathbb{F}_q}\right) = x^{(q-1)/2}.$$

Question 66

Soient $q = 625$, E une courbe elliptique sur le corps fini \mathbb{F}_q telle que

$$\text{Card}(E(\mathbb{F}_q)) = q + 1 - 2\sqrt{q}.$$

On note ϕ_q le Frobenius de E . Il existe un entier A tel que ϕ_q soit égal à l'endomorphisme de multiplication par A .

Calculus A.

Three 10x10 grids are shown, each with a single black square at a different position. The first grid has a black square at (0,0). The second grid has a black square at (1,1). The third grid has a black square at (4,4). The grids are labeled 0, 1, and 2 respectively.

Commentaire après réponse:

$$A = p^m \text{ où } m = 2, p = 5.$$

Voir [Washington, p.154].

Question 67

Soient $p \notin \{2, 3\}$ un nombre premier, $A, B \in \mathbb{F}_p$, E la courbe elliptique sur le corps fini \mathbb{F}_p définie par l'équation

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

Soit $d \in \mathbb{F}_p$ ne pouvant pas s'écrire sous la forme $d = s^2$ avec $s \in \mathbb{F}_p$. On considère E' la courbe elliptique d'équation

$$y^2 = x^3 + Ad^2x + Bd^3.$$

On suppose $p = 307$ et $\text{Card}(E(\mathbb{F}_p)) = 300$.

Calculer $\text{Card}(E'(\mathbb{F}_p))$.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Commentaire après réponse:

Si $a = p + 1 - \#E(\mathbb{F}_p)$, alors $\#E'(\mathbb{F}_p) = p + 1 + a = 2 \times 307 + 2 - 300 = 316$.

change of variable $y' = d^2y$ and $x' = dx$ shows that E' is equivalent to the equation $dy'^2 = x'^3 + Ax' + B$. Since, we see that $x^3 + Ax + B$ is a square if and only if $x^3 + Ad^2x + Bd^3$ is NOT a square, so the formula with the Legendre symbols yields $\#E(\mathbb{F}_q) + \#E'(\mathbb{F}_q) = 2q + 2$.

Question 68

Soit E une courbe elliptique sur \mathbb{F}_{841} . On note α et β les racines du polynôme caractéristique du Frobenius ϕ_{841} .

Calculer $|\alpha|$ (la valeur absolue de α).

<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Commentaire après réponse: On a $841 = 29^2$.

$$|\alpha| = |\beta|$$

car ce sont les racines complexes d'un polynôme de degré de 2 donc elles sont conjuguées. Comme le produit des racines est q , on a $|\alpha| = \sqrt{q} = 29$.