### 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

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

0% 10%	40% 50%	80%
$\frac{10\%}{20\%}$	60%	100%
$\square$ 30%	<b>70</b> %	<u>—</u>

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  $4A^3 + 27B^2 \neq 0$ .

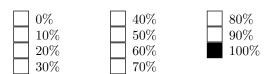
Soit une courbe elliptique E sur K définie par l'équation

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

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  $m = \frac{y_2 - y_1}{x_2 - x_1}$ .



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

$$P_1 + P_2 = \infty.$$

0% 10%	40% 50%	80% 90%
20%	$\begin{bmatrix} 50\% \\ 60\% \end{bmatrix}$	100%
30%	70%	

Commentaire après réponse:

Voir le cours [Washington, p. 28].

<sup>\*</sup>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  $m = \frac{3x_1^2 + A}{2u_1}$ .



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.

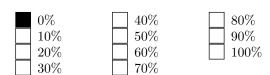
Soient  $A, B \in K$  tels que  $4A^3 + 27B^2 \neq 0$ .

Soit une courbe elliptique E sur K définie par l'équation

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

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

 $P + P = \infty$ .



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.



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%	$\square$ 40%	80%
10%	$\square$ 50%	90%
$\square$ 20%	$\square$ 60%	100%
30%	$\square$ 70%	

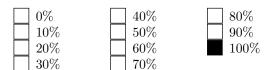
Commentaire après réponse: On a

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

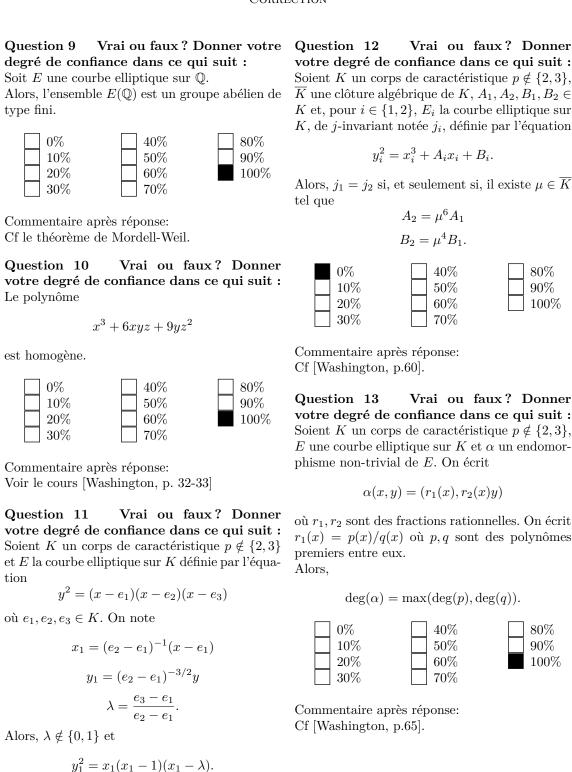
# Question 8 Vrai ou faux? Donner votre degré de confiance dans ce qui suit :

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.



Commentaire après réponse:



Commentaire après réponse:

0%

10%

20%

30%

Voir aussi le cours [Washington, p. 49]

40%

50%

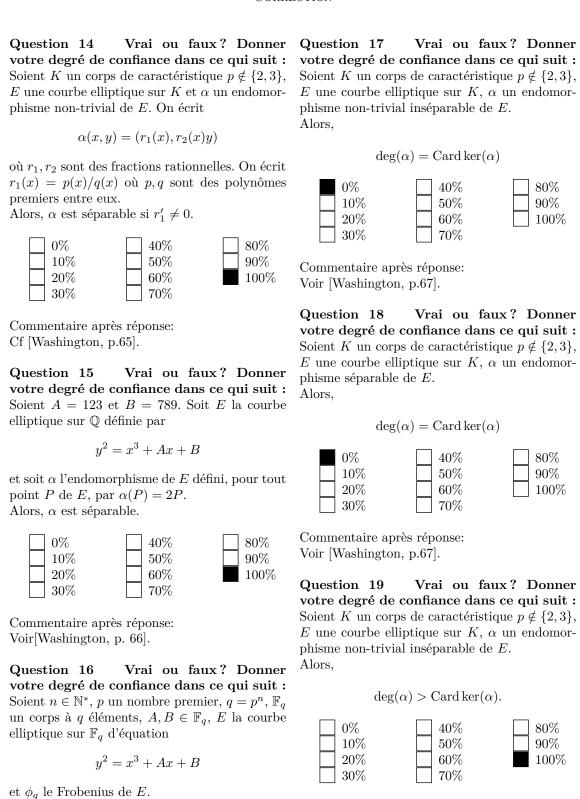
60%

70%

80%

90%

100%



Commentaire après réponse:

Voir [Washington, p.67].

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

40%

50%

60%

70%

80%

90%

100%

Alors,  $\phi_q$  est séparable.

0%

10%

20%

30%

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,  $\alpha$  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,  $(r,s) \in \mathbb{Z}^2 \setminus \{0,0\}$ ,  $\phi_q$  l'endomorphisme de Frobenius de E.

Alors,  $r \cdot \phi_q + s$  est séparable si, et seulement si, p ne divise pas r.

0%	<b>40</b> %	80%
10%	$\Box$ 50%	90%
$\square$ 20%	$\square$ 60%	<b>100</b> %
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  $\alpha$  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%
<b>10</b> %	$\square$ 50%	90%
$\square$ 20%	$\square$ 60%	100%
30%	<b>70</b> %	

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.

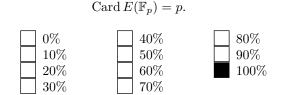
Question 25 Vrai ou faux? Donner votre degré de confiance dans ce qui suit : Soient $K$ un corps de caractéristique $p \notin \{2,3\}$ , $\overline{K}$ une clôture algébrique de $K$ , $E$ une courbe elliptique sur $K$ et $n \in \mathbb{N}^*$ . Alors,	Question 28 Vrai ou faux? Donner votre degré de confiance 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
$E[n] = \{ P \in E(K)     nP = \infty \}.$	$E[p] \simeq \{0\}.$
$\begin{array}{c cccc} & 0\% & & & & & & & & & & & & & & & & & $	$\begin{array}{ c c c c c c c c c c c c c c c c c c c$
Commentaire après réponse: Voir [Washington, p. 91].	Commentaire après réponse: Voir [Washington, p. 93].
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 $\mathbb{Z}/(3)$ .	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 $p^j$ .
$\begin{array}{c cccc} & 0\% & & & & 40\% & & 80\% \\ \hline 10\% & & 50\% & & 90\% \\ \hline 20\% & & 60\% & & 100\% \\ \hline 30\% & & 70\% & & \end{array}$	$\begin{array}{ c c c c c c c c c c c c c c c c c c c$
Commentaire après réponse: Voir [Washington, p. 92].	Commentaire après réponse: Voir [Washington, p. 100].
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 $\mathbb{Z}/(n^2)$ . $\begin{array}{c ccccccccccccccccccccccccccccccccccc$	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. $\begin{array}{c ccccccccccccccccccccccccccccccccccc$

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 $p$ , $\mu_n = \{x \in \overline{K} \mid x^n = 1\}$ , et $E$ une courbe elliptique sur $K$ Si $E[n] \subset E(K)$ , alors $\mu_n \subset K$ .	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 $\mathbb{F}_q$ , $\phi_q$ le Frobenius de $E$ , et $P$ un point de $E$ . Alors, $P \in E(\mathbb{F}_q)$ si, et seulement si $\phi_q(P) = P$ .
	$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$
Commentaire après réponse: Voir [Washington, p. 102].	Commentaire après réponse: Voir [Washington, p.112].
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	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 $\mathbb{F}_q$ , $\phi_q$ le Frobenius de $E$ , et $n \in \mathbb{N}^*$ ,
$E(\mathbb{F}_a) \simeq \mathbb{Z}/(n)$	$\ker(\phi_q^n - 1) = \{0\}.$
ou il existe $n_1, n_2 \in \mathbb{N}^*$ tels que $n_1 n_2$ et $E(\mathbb{F}_q) \simeq \mathbb{Z}/(n_1) \oplus \mathbb{Z}/(n_2).$	$ \begin{array}{c cccc} \hline & 0\% & & \hline & 40\% & & \hline & 80\% \\ \hline & 10\% & & \hline & 50\% & & \hline & 90\% \\ \hline & 20\% & & \hline & 60\% & & \hline & 100\% \\ \hline & 30\% & & \hline & 70\% & & \hline \end{array} $
$\begin{array}{c cccc} & 0\% & & & & 40\% & & 80\% \\ & 10\% & & 50\% & & 90\% \\ & 20\% & & 60\% & & 100\% \\ \hline \end{array}$	Commentaire après réponse: Voir [Washington, p.112].
30% 70%  Commentaire après réponse:  Voir [Washington, p.110].  Question 33 Vrai ou faux? Donner	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 $\mathbb{F}_q$ , $\phi_q$ le Frobenius de $E$ , et $n \in \mathbb{N}^*$ . Alors, $\phi_q^n - 1$ est séparable.
votre degré de confiance dans ce qui suit : Soit $E$ une courbe elliptique sur un corps fini $\mathbb{F}_q$ . Alors, $ q+1-\operatorname{Card}(E(\mathbb{F}_q))  \geq 2\sqrt{q}.$	$\begin{array}{c cccc} & 0\% & & & & & & & & & & & & & & & & & $
$ \begin{array}{c cccc}  & 0\% &  &  &  &  &  &  &  &  &  &  &  &  & $	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 $\mathbb{F}_q$ , $\phi_q$ le Frobenius de $E$ , et $n \in \mathbb{N}^*$ . Alors, $\mathrm{Card}(E(\mathbb{F}_{q^n})) = \deg(\phi_q^n).$
	$ \begin{array}{c cccc} & & & & & & & & & & & & & & & & & $

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 $\mathbb{F}_q$ , $\phi_q$ le Frobenius de $E$ , et $a=q+1-\operatorname{Card}(\mathbb{F}_q)$ .	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, $\phi_q^2 + a\phi_q + q = 0.$	y = x + 11x + B. Alors,
$ \begin{array}{c cccc} \hline & 0\% & & & & & & & & & & & & \\ \hline & 10\% & & & & & & & & & \\ \hline & 20\% & & & & & & & & \\ \hline & 30\% & & & & & & & \\ \hline \end{array} $	$\operatorname{Card}(\mathbb{F}_q) = q + 1 - \sum_{x \in \mathbb{F}_q} \left( \frac{x^3 + Ax + B}{\mathbb{F}_q} \right).$
Commentaire après réponse: Voir [Washington, p.114].	$ \begin{array}{c cccc} & & & & & & & & & & & & & & & & & $
Question 39 Vrai ou faux? Donner votre degré de confiance dans ce qui suit :	Commentaire après réponse:
Soient $\mathbb{F}_q$ un corps fini, $E$ une courbe elliptique	Voir [Washington, p.118].
sur $\mathbb{F}_q$ , $\phi_q$ le Frobenius de $E$ , $m$ un entier premier avec $q$ , $(\phi_q)_m$ la restriction du Frobenius à $E[m]$ et $a=q+1-\operatorname{Card}(\mathbb{F}_q)$ . Alors, $a\equiv\operatorname{Tr}((\phi_q)_m)\pmod{m}.$	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
$\begin{array}{ c c c c c c c c c c c c c c c c c c c$	$\operatorname{Card}(E(\mathbb{F}_q)) \equiv 1 \pmod{p}.$
20% 60% 100%  Commentaire après réponse:	$\begin{array}{c cccc} & 0\% & & & & 40\% & & & 80\% \\ & 10\% & & & 50\% & & 90\% \\ & 20\% & & & 60\% & & 100\% \\ \end{array}$
Voir [Washington, p.115].	30% 70%
Question 40 Vrai ou faux? Donner votre degré de confiance dans ce qui suit :	Commentaire après réponse: Voir [Washington, p.143].
Soient $\mathbb{F}_q$ un corps fini, $E$ une courbe elliptique sur $\mathbb{F}_q$ , $a=q+1-\operatorname{Card}(E(\mathbb{F}_q))$ , $\phi_q$ le Frobenius de $E$ , $\alpha,\beta$ les deux racines du polynôme caractéristique de $\phi_q$ et $n\in\mathbb{N}$ . On note $s_n=\alpha^n+\beta^n$ . Alors, si $n>0$ ,	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
$s_{n+1} = as_n + qs_{n-1}.$	$\operatorname{Card}(E(\mathbb{F}_p)) = p$
	alors, $E$ est supersingulière.

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



Commentaire après réponse:

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

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

donc

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

donc

$$\sqrt{k} < 1.4$$

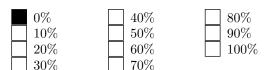
donc k < 2 donc k = 1.

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

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



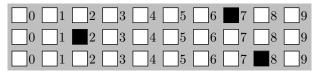
Commentaire après réponse: Cf [Washington, p. 180].

#### 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  $j(E)\frac{4A^3+27B^2}{4A^3}-1000$ .



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  $\alpha$  l'endomorphisme de E défini, pour tout point P de E, par  $\alpha(P)=2P$ . Alors  $\alpha$  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  $\lambda$ .



Commentaire après réponse: On a

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

 $_{
m et}$ 

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

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  $\alpha$  l'endomorphisme de E défini, pour tout point P de E, par  $\alpha(P)=2P$ . Alors  $\alpha$  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  $\lambda$ .



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  $\alpha$  l'endomorphisme de E défini, pour tout point P de E, par  $\alpha(P)=2P$ . Alors  $\alpha$  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  $\lambda$ .



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

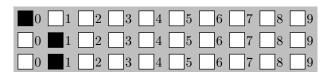


Commentaire après réponse:

Voir aussi [Washington, p. 66].

#### Question 51

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



Commentaire après réponse:

Voir [Washington, p. 66].

Question 55

Question 56

matrice de N.

Soient a = 2, b = 3.

 $\det(N) = 3.$ 

0

Question 57

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

#### Question 52

Soient a, b, c les trois racines du polynôme

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

Calculer abc.

taille $2 \times 2$ et $Com(N)^T$ la transposée de la co-
matrice de $N$ .
On suppose que $det(M + N) = 500$ , $det(M) =$
$150, \det(N) = 30.$

Soient  $M, N \in \mathbf{M}_2(\mathbb{Q})$  deux matrices carrées de taille  $2 \times 2$  et  $Com(N)^T$  la transposée de la co-

On suppose que det(M+N)=11, det(M)=5,

Soient  $M, N \in \mathbf{M}_2(\mathbb{Q})$  deux matrices carrées de



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  $\lambda \in \mathbb{Q} \setminus \{0,1\} \text{ tel que } j(\lambda) = \mathbf{j}.$ 

Calculer a.



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  $\alpha$  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  $\alpha_2$ l'endomorphisme  $\mathbb{Z}$ -linéaire de E[2] induit par

 $\mathbf{C}$ 

Soit $E$ la courbe elliptique sur $\mathbb{F}_5$ définie	par		
l'équation			
$y^2 = x^3 + x + 1.$			

3

Commentaire après réponse:

Voir [Washington, p. 106].

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

$\alpha$ .	
Calculer $Tr(\alpha_2) \in \mathbb{Z}$ .	
	Gommentaire après réponse:

Yoir [Washington, p. 108]. 3 4 5 2

Commentaire après réponse:

Cf [Washington, p. 94].