Catalogue

Niels Feld *

27 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 $A, B \in K$.
On peut définir une courbe elliptique E sur K comme l'ensemble

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

muni d'un élément à l'infini noté ∞.

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

Commentaire après réponse:
On veut aussi que $4A^3 + 27B^2 \neq 0$

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

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

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

Commentaire après réponse:
Ne pas oublier le point à l'infini ∞.

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 $x_1 = x_2$ et $y_1 \neq y_2$.
Alors,

$$P_1 + P_2 = \infty.$$

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

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

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

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

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

$$P + \infty = P.$$

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

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

*Merci à Damien Mégy

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

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

- [x] 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

$$(1,1) + (\frac{1}{2}, \frac{-1}{2}) = (24, -70)$$

dans E.

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

Commentaire après réponse:
On a

$$(1,1) + (\frac{1}{2}, \frac{-1}{2}) = (24, -70)$$

dans E.

Question 7 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soit K un corps de caractéristique $p \notin \{2,3\}$.
Soit E une courbe elliptique sur K.
Alors, l'ensemble $E(K)$ est un groupe fini.

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

Commentaire après réponse:
C'est faux si $K = \mathbb{Q}$.

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

$$x^3 + 3x^2z + 2y^2z$$

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

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

est homogène.

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

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

Question 10 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 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

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

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

Commentaire après réponse:
Prendre $K = \mathbb{Q}$, $G(u,v) = u^2 - v$ et $(u_0, v_0) = (2,4)$.
Voir aussi le cours [Washington, p. 36]

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

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

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

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

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

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

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

Commentaire après réponse:
On a

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

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

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

Supposons que $j_1 = j_2$ et montrons qu'il existe $\mu \in \overline{K}$ tel que

$$A_2 = \mu^4 A_1$$

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

Tout d'abord, supposons que $A_1 \neq 0$. Puisque cela équivaut à $j_1 \neq 0$, nous avons également $A_2 \neq 0$. Choisissons μ tel que $A_2 = \mu^4 A_1$. Alors

$$\frac{4A_2^3}{4A_2^3+27B_2^2} = \frac{4A_1^3}{4A_1^3+27B_1^2}$$

$$= \frac{4\mu^{-12}A_2^3}{4\mu^{-12}A_2^3+27B_1^2} = \frac{4A_2^3}{4A_2^3+27\mu^{12}B_1^2},$$

ce qui implique que

$$B_2^2 = (\mu^6 B_1)^2.$$

Par conséquent, $B_2 = \pm\mu^6 B_1$. Si $B_2 = \mu^6 B_1$, nous avons terminé. Si $B_2 = -\mu^6 B_1$, alors changeons μ en $i\mu$ (où $i^2 = -1$). Cela préserve la relation $A_2 = \mu^4 A_1$ et donne également $B_2 = \mu^6 B_1$. Si $A_1 = 0$, alors $A_2 = 0$. Comme (pour $i \in \{1,2\}$) $4A_i^3 + 27B_i^2 \neq 0$, nous avons $B_1, B_2 \neq 0$. Choisissons alors μ tel que $B_2 = \mu^6 B_1$.

☐ 0%	☐ 40%	☐ 80%
☐ 10%	☐ 50%	☐ 90%
☐ 20%	☐ 60%	■ 100%
☐ 30%	☐ 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 premiers entre eux.
Alors, α est séparable si $p' \neq 0$ et $q' \neq 0$.

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

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

Question 14 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 et E une courbe elliptique sur $\mathbb{F}_q$ d'équation

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

où $A, B \in \mathbb{F}_q$.
Le Frobenius de E est l'endomorphisme ϕ_q défini par

$$\phi_q(x,y) = (x^q, y^q).$$

Lorsque $n = 1$, le théorème de Fermat implique que

$$\forall x \in \mathbb{F}_p, x^p = x$$

et donc, dans ce cas particulier, on a

$$\phi_p(x,y) = (x,y)$$

pour tout point (x,y) de E, d'où $\phi_p = \mathrm{Id}$.

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

Commentaire après réponse:
Un point de E désigne, par abus de langage, un élément de l'ensemble

$$E(\overline{\mathbb{F}_q}) = \{\infty\} \cup \{(x,y) \in \overline{\mathbb{F}_q}^2 \mid y^2 = x^3 + Ax + B\}.$$

Tout ce que l'on peut dire, c'est que la restriction de ϕ_q à $E(\mathbb{F}_q)$ est l'identité.

Question 15 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 séparable de E.
Alors,

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

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

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

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 séparable de E.
Alors,

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

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

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 $p \notin \{2,3\}$, E une courbe elliptique sur K, α un endomorphisme non-trivial inséparable de E.
Alors,

$$\deg(\alpha) < \mathrm{Card}\ker(\alpha)$$

■ 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 $p \notin \{2,3\}$, $\overline{K}$ 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 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 $x \in \overline{K}$ tel que

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

Alors, pour tout $(a, b) \in E(\overline{K})$, au moins l'une des conditions suivantes est satisfaite :

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

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

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

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 de E.
Alors,

$$\alpha : E(K) \to E(K)$$

est surjectif.

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

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

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 séparable si, et seulement si, p ne divise pas s.

☐ 0%	☐ 40%	☐ 80%
☐ 10%	☐ 50%	☐ 90%
☐ 20%	☐ 60%	■ 100%
☐ 30%	☐ 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 $3x^2 + A = 0$.

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

Commentaire après réponse:
En fait, on a $3x^2 + A \neq 0$.
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 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, $t(x_0) = 0$.

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

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

Question 23 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient K un corps de caractéristique $p \notin \{2,3\}$, $\overline{K}$ une clôture algébrique de K, E une courbe elliptique sur K et $n \in \mathbb{N}^*$. Alors,

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

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

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

Question 24 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 $E[2]$ est isomorphe au groupe $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.

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

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

Question 25 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 $\mathbb{Z}/(n) \oplus \mathbb{Z}/(n)$.

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

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 $p \notin \{2,3\}$, 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 $p \not| n'$ 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 $\mathbb{Z}/(n) \oplus \mathbb{Z}/(n')$.

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

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

Question 27 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

$$E[p] \simeq \mathbb{Z}/(p).$$

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

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

Question 28 **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

$$\psi_0 = 0$$

$$\psi_1 = 1$$

$$\psi_2 = 2y$$

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

$$\psi_4 =$$

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

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

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

pour $m \geq 3$.
Si $n \geq 5$ est impair, alors ψ_n est un polynôme dans $2y\mathbb{Z}[x, y^2, A, B]$.

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

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

Question 29 **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 avec p, et $\mu_n = \{x \in \overline{K} \mid x^n = 1\}$.
Alors, $\mathrm{Card}(\mu_n) = n$.

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

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

Question 30 **Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :**
Soit E une courbe elliptique sur $\mathbb{Q}$. Si n est un entier > 2, alors $E[n] \not\subset E(\mathbb{Q})$.

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

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

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, 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,

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

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

Commentaire après réponse:
Voir [Washington, p. 103, et l'exemple p.94].

Question 32 **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 $Q \in E[n]$.
Le couple (P, Q) forme une base de $E[n]$ si, et seulement si, $e_n(P, Q) = 1$.

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

Commentaire après réponse:
Voir [Washing, Ex. 3.6, p. 107].

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,

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

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

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, $P \in E(\overline{\mathbb{F}}_q)$ si, et seulement si $\phi_q(P) = P$.

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

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 $n \in \mathbb{N}^*$,

$$\ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n}).$$

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

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 inséparable.

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

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,

$$\mathrm{Card}(E(\mathbb{F}_{q^n})) = \deg(\phi_q^n - 1).$$

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

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 $k \in \mathbb{Z}$ tels que

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

Alors, $k = q + 1 - \mathrm{Card}(E(\mathbb{F}_q))$.

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

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 $E[n]$ et $a = q + 1 - \mathrm{Card}(E(\mathbb{F}_q))$.
Alors,

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

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

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 $\mathbb{F}_q$, ϕ_q le Frobenius de E, α, β les deux racines du polynôme caractéristique de ϕ_q et $n \in \mathbb{N}^*$.
Alors,

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

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

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,

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

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

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

Question 42 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit : Soient $m \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ tels que $|a| \leq 2m^2$.
Alors, il existe $a_0, a_1 \in \mathbb{Z}$ tels que

$$-m < a_0 \leq m,$$

$$-m \leq a_1 \leq m$$

et

$$a = a_0 + 2ma_1.$$

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

Commentaire après réponse:
Voir [Washington, p.126].

Question 43 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

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

alors, E est supersingulière.

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

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

Question 44 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 E est supersingulière, alors

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

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

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

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 $\mathbb{F}_q$. 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, $NQ = \infty$ et l'accouplement de Weil associé à E vérifie $e_n(P, Q) = 1$.

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

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 $N \in \mathbb{N}^*$. On suppose que $\mathrm{Card}(E(\mathbb{F}_q)) = q + 1$.
Si il existe un point $P \in E(\mathbb{F}_q)$ d'ordre N, alors

$$E[N] \subset E(\mathbb{F}_{q^2}).$$

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

Commentaire après réponse:
Voir [Washington, p.169].

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

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

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

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

Commentaire après réponse:
Voir [Washington, p.171].

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 $\mathbb{F}_q$, et $m \in \mathbb{N}^*$.
Si $\mathrm{Card}(E(\mathbb{F}_q)[m]) = 1$, alors,

$$\mathrm{Card}(E(\mathbb{F}_q)/mE(\mathbb{F}_q)) = 1.$$

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

Commentaire après réponse: La multiplication par m est injective si et seulement si elle est surjective car $E(\mathbb{F}_q)$ est fini.
Plus généralement :
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 G. En particulier, c'est vrai si $G = E(\mathbb{F}_q)$ et f est la multiplication par m.

Question 49 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

$$\mathrm{Card}\, E(\mathbb{F}_p) = p + 1.$$

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

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

Question 50 Vrai ou faux ? Donner votre degré de confiance dans ce qui suit :
Soient $p \notin \{2,3\}$ un nombre premier tel que $p \equiv 2 \pmod 3$, $b \in \mathbb{F}_p^\times$, 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 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 $\alpha \circ \beta$ est inséparable.

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

Commentaire après réponse:

Question 52
On suppose qu'il existe x, y, z des rationnels tels que

$$x^3 + y^3 + z^3 = 0$$

et $xyz \neq 0$. On pose

$$x_1 = -12\frac{z}{x+y}$$

$$y_1 = 36\frac{x-y}{x+y}.$$

Alors, il existe $\lambda \in \mathbb{N}$ tel

$$y_1^3 = x_1^2 - \lambda.$$

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:
Voir aussi [Washington, p. 50].

Question 53
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

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

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 54
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 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

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

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 55
Soient K un corps de caractéristique $p \notin \{2, 3\}$, E une courbe elliptique sur K, et $n \in \mathbb{N}^*$. On suppose que la multiplication par n est donnée par

$$n(x, y) = (R_n(x), S_n(x)y)$$

pour tout point (x, y) de E, où $R_n, S_n \in K(x, y)$.
On suppose $n = 16$, calculer

$$\frac{R_n'}{S_n'}.$$

■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. 72].

Question 56
Soient $A = 12$, $B = -21$, E la courbe elliptique sur $\mathbb{Q}$ définie par l'équation

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

Soit $(x, y) \in E[3] \setminus \{\infty\}$.
Calculer $3x^4 + 6Ax^2 + 12Bx$.

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

Commentaire après réponse:
On a $3x^4 + 6Ax^2 + 12Bx = A^2$. Cf [Washington, p. 92].

Question 57
Soient x, y, A, B des indéterminées, modulo la relation

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

On définit les polynômes de division $\psi_m \in \mathbb{Z}[x, y, A, B]$ par

$$\psi_0 = 0$$

$$\psi_1 = 1$$

$$\psi_2 = 2y$$

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

$$\psi_4 =$$

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

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

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

pour $m \geq 3$.
Pour $m \in \mathbb{N}^*$, on définit aussi

$$\varphi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$$

et on considère φ_n, ψ_n^2 comme des polynômes en x.
Soit $n = 9$. On note $\lambda_n = \max(\deg(\psi_n^2(x)), \deg(\varphi_n(x)))$. Calculer λ_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:
Cf [Washington, p. 97].

Question 58
Soient E une courbe elliptique sur $\mathbb{Q}$, e_2 l'accouplement de Weil associé à E, et P, Q deux points distincts de E d'ordre 2.
Calculer $e_2(P, Q) + 100$.

■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:
Soit $R = P + Q$ de sorte que $E[2] = \{\infty, P, Q, R\}$.. Par l'absurde, si $e_2(P, Q) = 1$, alors $e_2(R, P) = e_2(R, Q) = 1$ donc $R = \infty$, ce qui est absurde.

Question 59
Soit E la courbe elliptique sur $\mathbb{F}_5$ définie par l'équation

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

Il existe $a, b \in \{0, \ldots, 4\}$ tels que

$$(3, 1) + (2, 4) = (a \cdot 1_{\mathbb{F}_5}, b \cdot 1_{\mathbb{F}_5}).$$

Calculer $a + b \in \mathbb{N}$.

■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. 109]. $(3, 1) + (2, 4) = (4, 2)$.

Question 60
Soit E la courbe elliptique sur $\mathbb{F}_7$ définie par l'équation

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

On note $A = \max\{\text{ord}(P) \mid P \in E(\mathbb{F}_7)\}$ où $\text{ord}(P)$ désigne l'ordre de $P \in E(\mathbb{F}_7)$.
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:
Voir [Washington, p. 109].

Question 61
Soit E une courbe elliptique sur le corps fini $\mathbb{F}_q$. On suppose qu'il existe $n \in \mathbb{N}^*$ tel que

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

On note $a = q + 1 - \mathrm{Card}(E(\mathbb{F}_q))$. On suppose que $n > 1302$.
Calculer le reste r dans la division euclidienne de a par n.

■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:
Voir [Washington, p.121].

Question 62
Soit $u \in \mathbb{F}_{37}$. On note $\left(\frac{u}{\mathbb{F}_{37}}\right)$ le symbole de Legendre de u dans $\mathbb{F}_{37}$.
Calculer

$$\sum_{x \in \mathbb{F}_{37}} \left(\frac{x+u}{\mathbb{F}_{37}}\right).$$

■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.152].

Question 63
Soient $p \notin \{2, 3\}$, $l \in \mathbb{N}^*$, $q = p^l$, E une courbe elliptique sur le corps fini $\mathbb{F}_q$, $n, m \in \mathbb{N}^*$ tels que

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

On note r le reste dans la division euclidienne de q par n.
Calculer r.

■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.153].

Question 64
Soient $q = 625$, E une courbe elliptique sur le corps fini $\mathbb{F}_q$ telle que

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

Il existe deux entiers $k, l \in \mathbb{N}$ tels que

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

Calculer $k + l$.

■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:
$k = l = p^m - 1 = 24$ où $m = 2, p = 5$.

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

Voir [Washington, p.154].

Question 65
On considère l'ensemble $\mathcal{S}$ des réels $x \leq 999$ vérifiant la condition suivante :
Il existe un nombre premier $p \notin \{2, 3\}$, $n \in \mathbb{N}^*$, $q = p^n$, une courbe elliptique E sur le corps fini $\mathbb{F}_q$ tels que

$$x = |\sqrt{\mathrm{Card}(E(\mathbb{F}_q))} - \sqrt{q}|.$$

Calculer $\lfloor \max(\mathcal{S}) \rfloor$ (la partie entière du plus grand élément de $\mathcal{S}$).

■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.155].