

20 Juillet 2010, ANTS 2010, Nancy



Courbes de genre 3 de groupe d'automorphismes S_3

JEAN-FRANÇOIS MESTRE,
UNIVERSITÉ PARIS 7-DENIS DIDEROT

Soit \mathbf{F}_q un corps fini de cardinal q , et m_q la partie entière de $2\sqrt{q}$.

Courbes optimales

Soit \mathbf{F}_q un corps fini de cardinal q , et m_q la partie entière de $2\sqrt{q}$.
Si C est une courbe de genre g définie sur \mathbf{F}_q , soit

$$m(C) := q + 1 - \text{Card } C(\mathbf{F}_q).$$

Soit \mathbf{F}_q un corps fini de cardinal q , et m_q la partie entière de $2\sqrt{q}$.
Si C est une courbe de genre g définie sur \mathbf{F}_q , soit

$$m(C) := q + 1 - \text{Card } C(\mathbf{F}_q).$$

On a alors (Weil, raffiné par Serre):

$$|m(C)| \leq gm_q.$$

Soit \mathbf{F}_q un corps fini de cardinal q , et m_q la partie entière de $2\sqrt{q}$.
Si C est une courbe de genre g définie sur \mathbf{F}_q , soit

$$m(C) := q + 1 - \text{Card } C(\mathbf{F}_q).$$

On a alors (Weil, raffiné par Serre):

$$|m(C)| \leq gm_q.$$

Soit $N_q(g)$ le maximum du nombre de points de $C(\mathbf{F}_q)$, lorsque C parcourt l'ensemble des courbes de genre g définies sur \mathbf{F}_q .

Soit \mathbf{F}_q un corps fini de cardinal q , et m_q la partie entière de $2\sqrt{q}$.
Si C est une courbe de genre g définie sur \mathbf{F}_q , soit

$$m(C) := q + 1 - \text{Card } C(\mathbf{F}_q).$$

On a alors (Weil, raffiné par Serre):

$$|m(C)| \leq gm_q.$$

Soit $N_q(g)$ le maximum du nombre de points de $C(\mathbf{F}_q)$, lorsque C parcourt l'ensemble des courbes de genre g définies sur \mathbf{F}_q .

On a donc

$$N_q(g) \leq q + 1 + gm_q.$$

Une courbe C définie sur \mathbf{F}_q dont le nombre de points sur \mathbf{F}_q est égal à $q + 1 + gm_q$ est dite *optimale*, et le *défaut d'optimalité* est la quantité $D_q(g) = q + 1 + gm_q - N_q(g)$.

Une courbe C définie sur \mathbf{F}_q dont le nombre de points sur \mathbf{F}_q est égal à $q + 1 + gm_q$ est dite *optimale*, et le *défaut d'optimalité* est la quantité $D_q(g) = q + 1 + gm_q - N_q(g)$.

De plus, si C est optimale, sa jacobienne est isogène au produit de g courbes elliptiques optimales.

Une courbe C définie sur \mathbf{F}_q dont le nombre de points sur \mathbf{F}_q est égal à $q + 1 + gm_q$ est dite *optimale*, et le *défaut d'optimalité* est la quantité $D_q(g) = q + 1 + gm_q - N_q(g)$.

De plus, si C est optimale, sa jacobienne est isogène au produit de g courbes elliptiques optimales.

Une courbe dont le nombre de points est égal à $q + 1 - gm_q$ est parfois appelée "optimale minimale" (?)

Une courbe C définie sur \mathbf{F}_q dont le nombre de points sur \mathbf{F}_q est égal à $q + 1 + gm_q$ est dite *optimale*, et le *défaut d'optimalité* est la quantité $D_q(g) = q + 1 + gm_q - N_q(g)$.

De plus, si C est optimale, sa jacobienne est isogène au produit de g courbes elliptiques optimales.

Une courbe dont le nombre de points est égal à $q + 1 - gm_q$ est parfois appelée "optimale minimale" (?)

La jacobienne d'une telle courbe est isogène au produit de g courbes elliptiques "optimales minimales".

Comme on va le voir, pour q et g donnés, il peut ne pas exister de courbe optimale, y compris dans le cas du genre 1. À ce propos, Serre a posé la question suivante:

Comme on va le voir, pour q et g donnés, il peut ne pas exister de courbe optimale, y compris dans le cas du genre 1. À ce propos, Serre a posé la question suivante:

Pour g fixé, existe-t-il une constante $c(g)$ telle que, pour tout q , $D_q(g) \leq c(g)$?

Motivation initiale : codes de Goppa

La motivation initiale de la recherche de courbes sur \mathbf{F}_q ayant beaucoup de points est la construction, par Goppa (1977), de codes correcteurs d'erreurs construits sur des courbes algébriques sur des corps finis, ayant des paramètres d'autant meilleurs que les courbes possèdent beaucoup de points.

Serre s'est alors intéressé au problème, et a fait une série de cours le concernant. En particulier, il y a consacré son cours à Harvard de 1983, rédigé, à la main, par Gouvéa. Ce cours est important: il contient à peu près toutes les idées qui ont depuis été utilisées pour faire progresser le sujet.

Le cas du genre 1

Soit $q = p^a$, p premier.

Dans le cas du genre 1, on dispose du théorème suivant, dû à Waterhouse:

Le cas du genre 1

Soit $q = p^a$, p premier.

Dans le cas du genre 1, on dispose du théorème suivant, dû à Waterhouse:

Soit m un entier tel que $|m| \leq m_q$. Il existe une courbe elliptique définie sur \mathbf{F}_q dont le nombre de points est $q + 1 - m$ si et seulement si on est dans l'un des cas suivants:

Le cas du genre 1

Soit $q = p^a$, p premier.

Dans le cas du genre 1, on dispose du théorème suivant, dû à Waterhouse:

Soit m un entier tel que $|m| \leq m_q$. Il existe une courbe elliptique définie sur \mathbf{F}_q dont le nombre de points est $q + 1 - m$ si et seulement si on est dans l'un des cas suivants:

- m est premier à q .

Le cas du genre 1

Soit $q = p^a$, p premier.

Dans le cas du genre 1, on dispose du théorème suivant, dû à Waterhouse:

Soit m un entier tel que $|m| \leq m_q$. Il existe une courbe elliptique définie sur \mathbf{F}_q dont le nombre de points est $q + 1 - m$ si et seulement si on est dans l'un des cas suivants:

- m est premier à q .
- Si a est pair, $m = \pm m_q$.

Le cas du genre 1

Soit $q = p^a$, p premier.

Dans le cas du genre 1, on dispose du théorème suivant, dû à Waterhouse:

Soit m un entier tel que $|m| \leq m_q$. Il existe une courbe elliptique définie sur \mathbf{F}_q dont le nombre de points est $q + 1 - m$ si et seulement si on est dans l'un des cas suivants:

- m est premier à q .
- Si a est pair, $m = \pm m_q$.
- Si a est pair, $p \not\equiv 1 \pmod{3}$, et $m = \pm\sqrt{q}$.

Le cas du genre 1

Soit $q = p^a$, p premier.

Dans le cas du genre 1, on dispose du théorème suivant, dû à Waterhouse:

Soit m un entier tel que $|m| \leq m_q$. Il existe une courbe elliptique définie sur \mathbf{F}_q dont le nombre de points est $q + 1 - m$ si et seulement si on est dans l'un des cas suivants:

- m est premier à q .
- Si a est pair, $m = \pm m_q$.
- Si a est pair, $p \not\equiv 1 \pmod{3}$, et $m = \pm \sqrt{q}$.
- Si a est impair, $p = 2$ ou 3 , et $m = \pm p^{(a+1)/2}$.

Le cas du genre 1

Soit $q = p^a$, p premier.

Dans le cas du genre 1, on dispose du théorème suivant, dû à Waterhouse:

Soit m un entier tel que $|m| \leq m_q$. Il existe une courbe elliptique définie sur \mathbf{F}_q dont le nombre de points est $q + 1 - m$ si et seulement si on est dans l'un des cas suivants:

- m est premier à q .
- Si a est pair, $m = \pm m_q$.
- Si a est pair, $p \not\equiv 1 \pmod{3}$, et $m = \pm\sqrt{q}$.
- Si a est impair, $p = 2$ ou 3 , et $m = \pm p^{(a+1)/2}$.
- Si a est impair ou (a est pair et $p \not\equiv 1 \pmod{4}$), et $m = 0$.

Le cas du genre 1

Soit $q = p^a$, p premier.

Dans le cas du genre 1, on dispose du théorème suivant, dû à Waterhouse:

Soit m un entier tel que $|m| \leq m_q$. Il existe une courbe elliptique définie sur \mathbf{F}_q dont le nombre de points est $q + 1 - m$ si et seulement si on est dans l'un des cas suivants:

- m est premier à q .
- Si a est pair, $m = \pm m_q$.
- Si a est pair, $p \not\equiv 1 \pmod{3}$, et $m = \pm \sqrt{q}$.
- Si a est impair, $p = 2$ ou 3 , et $m = \pm p^{(a+1)/2}$.
- Si a est impair ou (a est pair et $p \not\equiv 1 \pmod{4}$), et $m = 0$.

Le cas du genre 1

Soit $q = p^a$, p premier.

Dans le cas du genre 1, on dispose du théorème suivant, dû à Waterhouse:

Soit m un entier tel que $|m| \leq m_q$. Il existe une courbe elliptique définie sur \mathbf{F}_q dont le nombre de points est $q + 1 - m$ si et seulement si on est dans l'un des cas suivants:

- m est premier à q .
- Si a est pair, $m = \pm m_q$.
- Si a est pair, $p \not\equiv 1 \pmod{3}$, et $m = \pm \sqrt{q}$.
- Si a est impair, $p = 2$ ou 3 , et $m = \pm p^{(a+1)/2}$.
- Si a est impair ou (a est pair et $p \not\equiv 1 \pmod{4}$), et $m = 0$.

On voit donc que, dès que m_q est divisible par p , que a est impair ≥ 3 , il n'existe pas de courbe elliptique optimale.

Le cas du genre 1

Remarquons que, pour p donné, pour a impair, $m_q \equiv 0 \pmod p$ si et seulement si le développement p -adique de $2\sqrt{p}$ au rang $(a-1)/2$ est nul.

Le cas du genre 1

Remarquons que, pour p donné, pour a impair, $m_q \equiv 0 \pmod p$ si et seulement si le développement p -adique de $2\sqrt{p}$ au rang $(a-1)/2$ est nul.

Expérimentalement, il y en a environ $\frac{1}{p}$.

Le cas du genre 1

Remarquons que, pour p donné, pour a impair, $m_q \equiv 0 \pmod p$ si et seulement si le développement p -adique de $2\sqrt{p}$ au rang $(a-1)/2$ est nul.

Expérimentalement, il y en a environ $\frac{1}{p}$.

Par exemple, si $p = 3$, $2\sqrt{3} = 1.1101120222201212202001\dots$, et $m_q \equiv 0 \pmod 3$ ssi $a = 7, 15, 25, 37, 41, 43\dots$

Le cas du genre 1

Remarquons que, pour p donné, pour a impair, $m_q \equiv 0 \pmod p$ si et seulement si le développement p -adique de $2\sqrt{p}$ au rang $(a-1)/2$ est nul.

Expérimentalement, il y en a environ $\frac{1}{p}$.

Par exemple, si $p = 3$, $2\sqrt{3} = 1.1101120222201212202001\dots$, et $m_q \equiv 0 \pmod 3$ ssi $a = 7, 15, 25, 37, 41, 43\dots$

En particulier, il existe une infinité de a impairs tels que m_q n'est pas divisible par p (sinon $2\sqrt{p}$ serait un entier.) Pour p fixé, il existe donc une infinité de courbes elliptiques optimales sur \mathbf{F}_{p^a} , quand a varie.

L'invariant de Hasse d'une courbe elliptique

Soit p un nombre premier. Il existe un polynôme $H_p(X_1, X_2, X_3, X_4, X_6)$ à coefficients dans \mathbf{F}_p tel que, si $q = p^n$ et si $N : \mathbf{F}_q \rightarrow \mathbf{F}_p$ est la norme, pour toute courbe elliptique d'équation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ définie sur F_q , on a

L'invariant de Hasse d'une courbe elliptique

Soit p un nombre premier. Il existe un polynôme $H_p(X_1, X_2, X_3, X_4, X_6)$ à coefficients dans \mathbf{F}_p tel que, si $q = p^n$ et si $N : \mathbf{F}_q \rightarrow \mathbf{F}_p$ est la norme, pour toute courbe elliptique d'équation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ définie sur F_q , on a

$$m(E) := q + 1 - |E(F_q)| \equiv N(H_p(a_1, a_2, a_3, a_4, a_6)) \pmod{p}.$$

L'invariant de Hasse d'une courbe elliptique

Soit p un nombre premier. Il existe un polynôme $H_p(X_1, X_2, X_3, X_4, X_6)$ à coefficients dans \mathbf{F}_p tel que, si $q = p^n$ et si $N : \mathbf{F}_q \rightarrow \mathbf{F}_p$ est la norme, pour toute courbe elliptique d'équation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ définie sur F_q , on a

$$m(E) := q + 1 - |E(F_q)| \equiv N(H_p(a_1, a_2, a_3, a_4, a_6)) \pmod{p}.$$

Par exemple,

- $H_2(X_1, \dots, X_6) = X_1$

L'invariant de Hasse d'une courbe elliptique

Soit p un nombre premier. Il existe un polynôme $H_p(X_1, X_2, X_3, X_4, X_6)$ à coefficients dans \mathbf{F}_p tel que, si $q = p^n$ et si $N : \mathbf{F}_q \rightarrow \mathbf{F}_p$ est la norme, pour toute courbe elliptique d'équation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ définie sur F_q , on a

$$m(E) := q + 1 - |E(F_q)| \equiv N(H_p(a_1, a_2, a_3, a_4, a_6)) \pmod{p}.$$

Par exemple,

- $H_2(X_1, \dots, X_6) = X_1$
- $H_3(0, X_2, 0, X_4, X_6) = X_2$

L'invariant de Hasse d'une courbe elliptique

Soit p un nombre premier. Il existe un polynôme $H_p(X_1, X_2, X_3, X_4, X_6)$ à coefficients dans \mathbf{F}_p tel que, si $q = p^n$ et si $N : \mathbf{F}_q \rightarrow \mathbf{F}_p$ est la norme, pour toute courbe elliptique d'équation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ définie sur F_q , on a

$$m(E) := q + 1 - |E(F_q)| \equiv N(H_p(a_1, a_2, a_3, a_4, a_6)) \pmod{p}.$$

Par exemple,

- $H_2(X_1, \dots, X_6) = X_1$
- $H_3(0, X_2, 0, X_4, X_6) = X_2$
- $H_5(0, 0, 0, X_4, X_6) = 2X_4$

L'invariant de Hasse d'une courbe elliptique

Soit p un nombre premier. Il existe un polynôme $H_p(X_1, X_2, X_3, X_4, X_6)$ à coefficients dans \mathbf{F}_p tel que, si $q = p^n$ et si $N : \mathbf{F}_q \rightarrow \mathbf{F}_p$ est la norme, pour toute courbe elliptique d'équation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ définie sur F_q , on a

$$m(E) := q + 1 - |E(F_q)| \equiv N(H_p(a_1, a_2, a_3, a_4, a_6)) \pmod{p}.$$

Par exemple,

- $H_2(X_1, \dots, X_6) = X_1$
- $H_3(0, X_2, 0, X_4, X_6) = X_2$
- $H_5(0, 0, 0, X_4, X_6) = 2X_4$
- $H_7(0, 0, 0, X_4, X_6) = 3X_6$

L'invariant de Hasse d'une courbe elliptique

Soit p un nombre premier. Il existe un polynôme $H_p(X_1, X_2, X_3, X_4, X_6)$ à coefficients dans \mathbf{F}_p tel que, si $q = p^n$ et si $N : \mathbf{F}_q \rightarrow \mathbf{F}_p$ est la norme, pour toute courbe elliptique d'équation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ définie sur F_q , on a

$$m(E) := q + 1 - |E(F_q)| \equiv N(H_p(a_1, a_2, a_3, a_4, a_6)) \pmod{p}.$$

Par exemple,

- $H_2(X_1, \dots, X_6) = X_1$
- $H_3(0, X_2, 0, X_4, X_6) = X_2$
- $H_5(0, 0, 0, X_4, X_6) = 2X_4$
- $H_7(0, 0, 0, X_4, X_6) = 3X_6$
- $H_{11}(0, 0, 0, X_4, X_6) = 9X_4X_6$

On a le théorème suivant (Torelli, précisé à la Serre):

On a le théorème suivant (Torelli, précisé à la Serre):

Soit A une variété abélienne sur k , principalement polarisée, et isomorphe sur \bar{k} à la jacobienne d'une courbe C définie sur \bar{k} .

- Si C est hyperelliptique, il existe une courbe C_0 définie sur k telle que A est k -isomorphe à la jacobienne de C_0 .

On a le théorème suivant (Torelli, précisé à la Serre):

Soit A une variété abélienne sur k , principalement polarisée, et isomorphe sur \bar{k} à la jacobienne d'une courbe C définie sur \bar{k} .

- Si C est hyperelliptique, il existe une courbe C_0 définie sur k telle que A est k -isomorphe à la jacobienne de C_0 .
- Sinon, il existe une courbe C_0 sur k qui est \bar{k} -isomorphe à C , et un caractère χ de G_k d'ordre 1 ou 2 tel que la tordue de A par χ est k -isomorphe à la jacobienne de C_0 ; χ est trivial si et seulement si A est la jacobienne d'une courbe définie sur k .

Lorsque $k = \mathbf{F}_q$, on est donc dans la situation suivante :
supposons que A soit isogène à un produit de courbes elliptiques optimales, et qu'elle soit jacobienne d'une courbe sur \bar{k} ; soit c 'est la jacobienne d'une courbe définie sur k , qui est alors optimale,

Lorsque $k = \mathbf{F}_q$, on est donc dans la situation suivante :
supposons que A soit isogène à un produit de courbes elliptiques optimales, et qu'elle soit jacobienne d'une courbe sur \bar{k} ; soit c 'est la jacobienne d'une courbe définie sur k , qui est alors optimale, soit c 'est la tordue quadratique de la jacobienne d'une courbe définie sur k , qui est alors “optimale minimale” !

Souvent, en fait, comme on verra plus loin, on sait construire, à partir d'une courbe elliptique E définie sur \mathbf{F}_q , une courbe, par exemple de genre 3,

Souvent, en fait, comme on verra plus loin, on sait construire, à partir d'une courbe elliptique E définie sur \mathbf{F}_q , une courbe, par exemple de genre 3, dont la jacobienne est \mathbf{F}_q -isogène au cube d'une courbe elliptique E' ayant le même invariant j que E .

Souvent, en fait, comme on verra plus loin, on sait construire, à partir d'une courbe elliptique E définie sur \mathbf{F}_q , une courbe, par exemple de genre 3, dont la jacobienne est \mathbf{F}_q -isogène au cube d'une courbe elliptique E' ayant le même invariant j que E .
On connaît même explicitement une équation de E' . Mais comment prouver que $E = E'$?

Souvent, en fait, comme on verra plus loin, on sait construire, à partir d'une courbe elliptique E définie sur \mathbf{F}_q , une courbe, par exemple de genre 3, dont la jacobienne est \mathbf{F}_q -isogène au cube d'une courbe elliptique E' ayant le même invariant j que E .

On connaît même explicitement une équation de E' . Mais comment prouver que $E = E'$?

Car en général, tout ce que l'on sait de E , c'est l'entier $m(E)$ (par exemple égal à $-m_q$). Mais cela ne renseigne en général en rien sur une équation explicite de E .

Souvent, en fait, comme on verra plus loin, on sait construire, à partir d'une courbe elliptique E définie sur \mathbf{F}_q , une courbe, par exemple de genre 3, dont la jacobienne est \mathbf{F}_q -isogène au cube d'une courbe elliptique E' ayant le même invariant j que E . On connaît même explicitement une équation de E' . Mais comment prouver que $E = E'$?

Car en général, tout ce que l'on sait de E , c'est l'entier $m(E)$ (par exemple égal à $-m_q$). Mais cela ne renseigne en général en rien sur une équation explicite de E .

Donc on est devant une situation paradoxale: on connaît mieux E' que E , en ce sens qu'on en connaît une équation - mais pas son nombre de points sur \mathbf{F}_q , qui est la seule chose que l'on connaisse de E !

Le cas du genre 2

Dans le cas du genre 2, une variété abélienne principalement polarisée qui n'est pas produit de deux courbes elliptiques est la jacobienne d'une courbe de genre 2.

Le cas du genre 2

Dans le cas du genre 2, une variété abélienne principalement polarisée qui n'est pas produit de deux courbes elliptiques est la jacobienne d'une courbe de genre 2.

Supposons donc qu'il existe une courbe elliptique E sur \mathbf{F}_q dont le nombre de points est $q + 1 - m_q$.

Le cas du genre 2

Dans le cas du genre 2, une variété abélienne principalement polarisée qui n'est pas produit de deux courbes elliptiques est la jacobienne d'une courbe de genre 2.

Supposons donc qu'il existe une courbe elliptique E sur \mathbf{F}_q dont le nombre de points est $q + 1 - m_q$.

D'après Hoffmann, si $d_q = m_q^2 - 4q$ n'est pas égal à $-3, -4$ ou -7 , il existe un module indécomposable de rang 2 sur $\mathbf{Q}(\pi)$, avec $\pi^2 - m_q\pi + q = 0$.

Le cas du genre 2

Dans le cas du genre 2, une variété abélienne principalement polarisée qui n'est pas produit de deux courbes elliptiques est la jacobienne d'une courbe de genre 2.

Supposons donc qu'il existe une courbe elliptique E sur \mathbf{F}_q dont le nombre de points est $q + 1 - m_q$.

D'après Hoffmann, si $d_q = m_q^2 - 4q$ n'est pas égal à $-3, -4$ ou -7 , il existe un module indécomposable de rang 2 sur $\mathbf{Q}(\pi)$, avec $\pi^2 - m_q\pi + q = 0$.

d'où une variété abélienne \mathbf{F}_q -isogène à E^3 , qui est jacobienne d'une courbe sur $\overline{\mathbf{F}}_q$.

Le cas du genre 2

Dans le cas du genre 2, une variété abélienne principalement polarisée qui n'est pas produit de deux courbes elliptiques est la jacobienne d'une courbe de genre 2.

Supposons donc qu'il existe une courbe elliptique E sur \mathbf{F}_q dont le nombre de points est $q + 1 - m_q$.

D'après Hoffmann, si $d_q = m_q^2 - 4q$ n'est pas égal à -3 , -4 ou -7 , il existe un module indécomposable de rang 2 sur $\mathbf{Q}(\pi)$, avec $\pi^2 - m_q\pi + q = 0$.

d'où une variété abélienne \mathbf{F}_q -isogène à E^3 , qui est jacobienne d'une courbe sur $\overline{\mathbf{F}}_q$.

Comme toute courbe de genre 2 est hyperelliptique, on a donc une courbe de genre 2 sur \mathbf{F}_q optimale (dont la tordue quadratique est "optimale minimale".)

Le cas du genre 3

Ici, commencent les difficultés, car en général une courbe de genre 3 n'est pas hyperelliptique.

Le cas du genre 3

Ici, commencent les difficultés, car en général une courbe de genre 3 n'est pas hyperelliptique.

Notons néanmoins que la dimension $\frac{g(g+1)}{2}$ des variétés abéliennes principalement polarisées est ici égale à la dimension $3g - 3$ des courbes de genre g .

Le cas du genre 3

Ici, commencent les difficultés, car en général une courbe de genre 3 n'est pas hyperelliptique.

Notons néanmoins que la dimension $\frac{g(g+1)}{2}$ des variétés abéliennes principalement polarisées est ici égale à la dimension $3g - 3$ des courbes de genre g .

Donc, pour trouver des courbes optimales, on va employer la stratégie suivante:

si m_q est premier à p , soit E une courbe elliptique optimale.

D'après Hoffmann, si $d_q = m_q^2 - 4q$ n'est pas égal à $-3, -4, -8$ ou -11 , il existe un module indécomposable de rang 3 sur $\mathbf{Q}(\pi)$, d'où une variété abélienne \mathbf{F}_q -isogène à E^3 , qui est jacobienne d'une courbe sur $\overline{\mathbf{F}}_q$.

Le cas du genre 3

Ici, commencent les difficultés, car en général une courbe de genre 3 n'est pas hyperelliptique.

Notons néanmoins que la dimension $\frac{g(g+1)}{2}$ des variétés abéliennes principalement polarisées est ici égale à la dimension $3g - 3$ des courbes de genre g .

Donc, pour trouver des courbes optimales, on va employer la stratégie suivante:

si m_q est premier à p , soit E une courbe elliptique optimale.

D'après Hoffmann, si $d_q = m_q^2 - 4q$ n'est pas égal à $-3, -4, -8$ ou -11 , il existe un module indécomposable de rang 3 sur $\mathbf{Q}(\pi)$, d'où une variété abélienne \mathbf{F}_q -isogène à E^3 , qui est jacobienne d'une courbe sur $\overline{\mathbf{F}}_q$.

Mais on ignore si c'est elle, ou sa tordue, qui est une jacobienne d'une courbe sur \mathbf{F}_q . Dans le premier cas, on a gagné, sinon on a perdu.

Le cas du genre 3: ce qui est connu

Dans le cas du genre 3, rappelons les résultats suivants, en relation avec ceux obtenus ici:

- Top a trouvé de nombreux cas de courbes de genre 3 optimales en faisant une recherche systématique, en particulier pour $q \leq 100$.

Le cas du genre 3: ce qui est connu

Dans le cas du genre 3, rappelons les résultats suivants, en relation avec ceux obtenus ici:

- Top a trouvé de nombreux cas de courbes de genre 3 optimales en faisant une recherche systématique, en particulier pour $q \leq 100$.
- Lauter a prouvé que, pour tout q , il existe une courbe C de genre 3 telle que $|q + 1 - \text{Card } C(\mathbf{F}_q)| \geq 3m_q - 3$.

Le cas du genre 3: ce qui est connu

Dans le cas du genre 3, rappelons les résultats suivants, en relation avec ceux obtenus ici:

- Top a trouvé de nombreux cas de courbes de genre 3 optimales en faisant une recherche systématique, en particulier pour $q \leq 100$.
- Lauter a prouvé que, pour tout q , il existe une courbe C de genre 3 telle que $|q + 1 - \text{Card } C(\mathbf{F}_q)| \geq 3m_q - 3$.
- Lorsque n est pair, et que $p \equiv 3 \pmod{4}$, il existe une courbe optimale de genre 3, qui plus est hyperelliptique. Pour $p \equiv 1 \pmod{4}$ et $n \equiv 2 \pmod{4}$, on sait aussi qu'il existe une courbe optimale.

On ignore s'il existe une infinité de nombres premiers p pour lesquels il existe une courbe de genre 3 optimale, i.e. tels que $N_p(3) = p + 1 + 3m_p$.

On ignore s'il existe une infinité de nombres premiers p pour lesquels il existe une courbe de genre 3 optimale, i.e. tels que $N_p(3) = p + 1 + 3m_p$.

Expérimentalement, cela semble vrai ...

Genre 3, caractéristique 2

Théorème.- (Nart, Ritzenthaler)

- Pour n pair ≥ 4 , et $p = 2$, il existe une courbe de genre 3 optimale.

Théorème.- (Nart, Ritzenthaler)

- Pour n pair ≥ 4 , et $p = 2$, il existe une courbe de genre 3 optimale.
- Il existe une courbe optimale sur \mathbf{F}_{2^n} pour une infinité de n impairs.

Théorème.- (Nart, Ritzenthaler)

- Pour n pair ≥ 4 , et $p = 2$, il existe une courbe de genre 3 optimale.
- Il existe une courbe optimale sur \mathbf{F}_{2^n} pour une infinité de n impairs.
- $D_{2^n}(3) \leq 9$.

Genre 3, caractéristique 3

- D'après ce qui précède, pour n pair, il existe des courbes de genre 3 (hyperelliptiques) optimales (et aussi des courbes “optimales minimales”) sur \mathbf{F}_{3^n} .

Genre 3, caractéristique 3

- D'après ce qui précède, pour n pair, il existe des courbes de genre 3 (hyperelliptiques) optimales (et aussi des courbes “optimales minimales”) sur \mathbf{F}_{3^n} .
- Auer et Top ont prouvé que, pour n impair, $D_{3^n}(3) \leq 21$.

Genre 3, caractéristique 3

- D'après ce qui précède, pour n pair, il existe des courbes de genre 3 (hyperelliptiques) optimales (et aussi des courbes “optimales minimales”) sur \mathbf{F}_{3^n} .
- Auer et Top ont prouvé que, pour n impair, $D_{3^n}(3) \leq 21$.

Genre 3, caractéristique 3

- D'après ce qui précède, pour n pair, il existe des courbes de genre 3 (hyperelliptiques) optimales (et aussi des courbes “optimales minimales”) sur \mathbf{F}_{3^n} .
- Auer et Top ont prouvé que, pour n impair, $D_{3^n}(3) \leq 21$.

Donc, en caractéristique 2 et 3, on peut répondre par l'affirmative à la question de Serre.

Pour les “petits” n impairs, on a:

- $N_3(3) = 10$ (défaut 3)

Pour les “petits” n impairs, on a:

- $N_3(3) = 10$ (défaut 3)
- $N_{27}(3) = 56$ (défaut 2)

Pour les “petits” n impairs, on a:

- $N_3(3) = 10$ (défaut 3)
- $N_{27}(3) = 56$ (défaut 2)
- Lauter (2002) : pour $q = 3^5$, défaut ≥ 3 .

Plusieurs de ces résultats ont été obtenus en considérant la famille de courbes $ax^4 + by^4 + cz^4 + ey^2z^2 + fz^2x^2 + gx^2y^2 = 0$, dites *quartiques de Ciani*, qui possèdent un groupe d'automorphismes isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$.

Plusieurs de ces résultats ont été obtenus en considérant la famille de courbes $ax^4 + by^4 + cz^4 + ey^2z^2 + fz^2x^2 + gx^2y^2 = 0$, dites *quartiques de Ciani*, qui possèdent un groupe d'automorphismes isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$.

Ces courbes ont en particulier des points d'ordre 2; en particulier, pour q et m_q impairs, comme alors $q + 1 + 3m_q$ est impair, elles ne peuvent pas fournir de courbe optimale sur \mathbf{F}_q .

Nous montrons dans cet exposé que l'étude d'une autre famille de courbes,

Nous montrons dans cet exposé que l'étude d'une autre famille de courbes, à savoir les courbes de genre 3 avec groupe d'automorphismes S_3 , permet :

Nous montrons dans cet exposé que l'étude d'une autre famille de courbes, à savoir les courbes de genre 3 avec groupe d'automorphismes S_3 , permet :

- De prouver que, pour tout $n \geq 7$, il existe une courbe optimale sur \mathbf{F}_{3^n} , dès que $m_{3^n} \not\equiv 0 \pmod{3}$

Nous montrons dans cet exposé que l'étude d'une autre famille de courbes, à savoir les courbes de genre 3 avec groupe d'automorphismes S_3 , permet :

- De prouver que, pour tout $n \geq 7$, il existe une courbe optimale sur \mathbf{F}_{3^n} , dès que $m_{3^n} \not\equiv 0 \pmod{3}$
- En caractéristique 7, de répondre par l'affirmative à la question de Serre.

Nous montrons dans cet exposé que l'étude d'une autre famille de courbes, à savoir les courbes de genre 3 avec groupe d'automorphismes S_3 , permet :

- De prouver que, pour tout $n \geq 7$, il existe une courbe optimale sur \mathbf{F}_{3^n} , dès que $m_{3^n} \not\equiv 0 \pmod{3}$
- En caractéristique 7, de répondre par l'affirmative à la question de Serre.
- D'obtenir expérimentalement de nombreuses courbes optimales

Nous montrons dans cet exposé que l'étude d'une autre famille de courbes, à savoir les courbes de genre 3 avec groupe d'automorphismes S_3 , permet :

- De prouver que, pour tout $n \geq 7$, il existe une courbe optimale sur \mathbf{F}_{3^n} , dès que $m_{3^n} \not\equiv 0 \pmod{3}$
- En caractéristique 7, de répondre par l'affirmative à la question de Serre.
- D'obtenir expérimentalement de nombreuses courbes optimales
- De construire explicitement des courbes de genre 3 sur \mathbf{Q} dont la jacobienne est isogène au cube de courbes elliptiques de type CM.

Plus précisément:

THÉORÈME.

- Soit $q = 3^n$, n impair. Si E est une courbe elliptique définie sur \mathbf{F}_q dont l'invariant modulaire n'est pas dans \mathbf{F}_3 , il existe une courbe de genre 3 dont la jacobienne est isogène sur \mathbf{F}_q à E^3 .

Plus précisément:

THÉORÈME.

- Soit $q = 3^n$, n impair. Si E est une courbe elliptique définie sur \mathbf{F}_q dont l'invariant modulaire n'est pas dans \mathbf{F}_3 , il existe une courbe de genre 3 dont la jacobienne est isogène sur \mathbf{F}_q à E^3 .
- Soit $q = 3^n$, avec n impair ≥ 7 ; si m_q n'est pas divisible par 3 (donc pour une infinité de n), il existe une courbe de genre 3 optimale (et aussi une courbe dont le nombre de points est $q + 1 - 3m_q$).

Plus précisément:

THÉORÈME.

- Soit $q = 3^n$, n impair. Si E est une courbe elliptique définie sur \mathbf{F}_q dont l'invariant modulaire n'est pas dans \mathbf{F}_3 , il existe une courbe de genre 3 dont la jacobienne est isogène sur \mathbf{F}_q à E^3 .
- Soit $q = 3^n$, avec n impair ≥ 7 ; si m_q n'est pas divisible par 3 (donc pour une infinité de n), il existe une courbe de genre 3 optimale (et aussi une courbe dont le nombre de points est $q + 1 - 3m_q$).
- Dans le cas où n est pair, il existe des courbes optimales non hyperelliptiques.

THÉORÈME.

Soit $q = 7^n$, n impair, et a un entier premier à 7, $|a| \leq m_q$; si a est divisible par 3, et est un carré mod 7, il existe une courbe de genre 3 dont le nombre de points est $q + 1 - 3a$. Si $a \equiv 1, 4, 5, 7, 8$ ou $11 \pmod{12}$, il existe une courbe de genre 3 dont le nombre de points est $q + 1 - 3a$ et une courbe de genre 3 dont le nombre de points est $q + 1 + 3a$.

COROLLAIRE.

- *Pour tout n , on a $D_{3^n}(3) \leq 3$.*

COROLLAIRE.

- *Pour tout n , on a $D_{3^n}(3) \leq 3$.*
- *Pour tout n , on a $D_{7^n}(3) \leq 9$*

Recherche systématique de courbes optimales via les quartiques de type S_3

Une recherche systématique avec les courbes en question permet expérimentalement d'obtenir de nombreuses courbes optimales.

Recherche systématique de courbes optimales via les quartiques de type S_3

Une recherche systématique avec les courbes en question permet expérimentalement d'obtenir de nombreuses courbes optimales.

Par exemple, pour p premier ≤ 10000 , on obtient, par spécialisation convenable de telles courbes, une courbe optimale sur \mathbf{F}_p dans environ 90% des cas.

La quartique de Klein $x^3y + y^3z + z^3x = 0$ a un groupe d'automorphismes égal à $L_2(7)$, d'ordre 168, qui contient un groupe isomorphe à S_3 . Sa jacobienne est isogène au cube de la courbe elliptique à multiplications complexes par $\mathbf{Z}(\frac{1+\sqrt{-7}}{2})$.

La quartique de Klein $x^3y + y^3z + z^3x = 0$ a un groupe d'automorphismes égal à $L_2(7)$, d'ordre 168, qui contient un groupe isomorphe à S_3 . Sa jacobienne est isogène au cube de la courbe elliptique à multiplications complexes par $\mathbf{Z}(\frac{1+\sqrt{-7}}{2})$.

Par la construction que nous décrivons plus loin, on obtient huit quartiques, à groupe d'automorphismes (contenant) S_3 , définies sur \mathbf{Q} dont la jacobienne est \mathbf{Q} -isogène au cube d'une courbe elliptique à multiplications complexes, les anneaux d'endomorphismes étant $-3, -7, -19, -43, -67, -163, -16, -28$.

La quartique de Klein $x^3y + y^3z + z^3x = 0$ a un groupe d'automorphismes égal à $L_2(7)$, d'ordre 168, qui contient un groupe isomorphe à S_3 . Sa jacobienne est isogène au cube de la courbe elliptique à multiplications complexes par $\mathbf{Z}(\frac{1+\sqrt{-7}}{2})$.

Par la construction que nous décrivons plus loin, on obtient huit quartiques, à groupe d'automorphismes (contenant) S_3 , définies sur \mathbf{Q} dont la jacobienne est \mathbf{Q} -isogène au cube d'une courbe elliptique à multiplications complexes, les anneaux d'endomorphismes étant $-3, -7, -19, -43, -67, -163, -16, -28$. On retrouve pour $d = -7$ la courbe de Klein, et chacune de ces courbes se réduit modulo $3, 7, 19, 43, 67, 163, 2, 7$ en une courbe hyperelliptique, ce qui généralise le résultat bien connu pour la courbe de Klein.

Construction de courbes de genre 3 de groupe d'automorphismes S_3

Soit k un corps, $a_1, a_2, a_3, a_4, X, Y, Z$ des indéterminées, $T_1 = X + Y + Z$, $T_2 = XY + YZ + ZX$, $T_3 = XYZ$; la courbe projective plane C_{a_1, a_2, a_3, a_4} à coefficients dans $k(a_1, a_2, a_3, a_4)$ d'équation

$$a_1 T_1^4 + a_2 T_1^2 T_2 + a_3 T_1 T_3 + a_4 T_2^2 = 0$$

a comme groupe d'automorphismes le groupe symétrique S_3 agissant de la façon naturelle sur $\{X, Y, Z\}$.

La jacobienne de ces courbes est isogène à $E_1^2 \times E_2$, où E_1 (resp. E_2) est la courbe quotient de C par l'un quelconque des sous-groupes d'ordre 2 (resp. par le sous-groupe d'ordre 3) de S_3 .

Le cas de caractéristique 3, $a_3 \neq 2$

On considère comme précédemment la famille de courbes d'équation

$$a_1 T_1^4 + a_2 T_1^2 T_2 + a_3 T_1 T_3 + T_2^2.$$

Le cas de caractéristique 3, $a_3 \neq 2$

On considère comme précédemment la famille de courbes d'équation

$$a_1 T_1^4 + a_2 T_1^2 T_2 + a_3 T_1 T_3 + T_2^2.$$

Supposons $a_3 \neq 2$. Par une transformation linéaire de la forme

$$X' = X + aT_1, Y' = Y + aT_1, Z' = Z + aT_1,$$

qui est de déterminant 1 et commute aux permutations, on se ramène à $a_2 = 0$ en prenant $a = -\frac{a_2}{1+a_3}$.

Le cas de caractéristique 3, $a_3 \neq 2$

On considère comme précédemment la famille de courbes d'équation

$$a_1 T_1^4 + a_2 T_1^2 T_2 + a_3 T_1 T_3 + T_2^2.$$

Supposons $a_3 \neq 2$. Par une transformation linéaire de la forme

$$X' = X + aT_1, Y' = Y + aT_1, Z' = Z + aT_1,$$

qui est de déterminant 1 et commute aux permutations, on se ramène à $a_2 = 0$ en prenant $a = -\frac{a_2}{1+a_3}$.

On note désormais, dans ce qui suit, C_{a_1, a_3} la courbe d'équation

$$a_1 T_1^4 + a_3 T_1 T_3 + T_2^2.$$

Le cas de caractéristique 3, $a_3 \neq 2$

On considère comme précédemment la famille de courbes d'équation

$$a_1 T_1^4 + a_2 T_1^2 T_2 + a_3 T_1 T_3 + T_2^2.$$

Supposons $a_3 \neq 2$. Par une transformation linéaire de la forme

$$X' = X + aT_1, Y' = Y + aT_1, Z' = Z + aT_1,$$

qui est de déterminant 1 et commute aux permutations, on se ramène à $a_2 = 0$ en prenant $a = -\frac{a_2}{1+a_3}$.

On note désormais, dans ce qui suit, C_{a_1, a_3} la courbe d'équation

$$a_1 T_1^4 + a_3 T_1 T_3 + T_2^2.$$

Son discriminant est $2(a_3 + 1)^9 a_1^3 a_3^{12}$.

La courbe E_1 quotient de C par l'une quelconque des involutions naturelles de C a comme équation

$$v^2 = u^3 + a_3(a_3 + 1)u^2 + 2a_3^2a_1,$$

La courbe E_1 quotient de C par l'une quelconque des involutions naturelles de C a comme équation

$$v^2 = u^3 + a_3(a_3 + 1)u^2 + 2a_3^2a_1,$$

son invariant modulaire étant

$$J_1 = \frac{a_3(a_3 + 1)^3}{a_1},$$

La courbe E_1 quotient de C par l'une quelconque des involutions naturelles de C a comme équation

$$v^2 = u^3 + a_3(a_3 + 1)u^2 + 2a_3^2a_1,$$

son invariant modulaire étant

$$J_1 = \frac{a_3(a_3 + 1)^3}{a_1},$$

Un morphisme du modèle affine de C (obtenu en posant $Z = 1$) vers E_1 est donné par

$$u = \frac{-a_3}{T_1}, \quad v = \frac{T_2 - a_3 T_1}{T_1^2}.$$

La courbe E_2 quotient de C par le groupe d'ordre 3 engendré par $(x, y, z) \mapsto (y, z, x)$ a comme équation

$$v^2 = u^3 + a_3(a_3 + 1)u^2 + a_1a_3^5,$$

La courbe E_2 quotient de C par le groupe d'ordre 3 engendré par $(x, y, z) \mapsto (y, z, x)$ a comme équation

$$v^2 = u^3 + a_3(a_3 + 1)u^2 + a_1a_3^5,$$

Un morphisme de C vers E_2 étant donné par

$$\begin{cases} u = 2a_3^2 \frac{a_1 UV + a_3}{(U+V)(2+a_1(U+V))} \\ v = (U-V) \frac{a_1 a_3^4 + u^2}{a_3^2} \end{cases}$$

avec $U = \frac{x^2y+y^2+x}{xy}$ et $V = \frac{y^2x+x^2+y}{xy}$.

La courbe E_2 quotient de C par le groupe d'ordre 3 engendré par $(x, y, z) \mapsto (y, z, x)$ a comme équation

$$v^2 = u^3 + a_3(a_3 + 1)u^2 + a_1a_3^5,$$

Un morphisme de C vers E_2 étant donné par

$$\begin{cases} u = 2a_3^2 \frac{a_1UV + a_3}{(U+V)(2+a_1(U+V))} \\ v = (U-V) \frac{a_1a_3^4 + u^2}{a_3^2} \end{cases}$$

avec $U = \frac{x^2y + y^2 + x}{xy}$ et $V = \frac{y^2x + x^2 + y}{xy}$.

L'invariant de E_2 est

$$J_2 = \frac{2(a_3 + 1)^3}{a_1a_3^2}$$

et donc

$$\frac{J_1}{J_2} = -a_3^3.$$

Par ailleurs, les coefficients de u^2 dans les équations de E_1 et E_2 sont les mêmes, et sont non nuls.

Par ailleurs, les coefficients de u^2 dans les équations de E_1 et E_2 sont les mêmes, et sont non nuls.

Par suite,

$$\text{Card } E_1(\mathbf{F}_q) \equiv \text{Card } E_2(\mathbf{F}_q) \pmod{3}.$$

Soit donc $k = \mathbf{F}_{3^n}$, et J_1 et J_2 deux éléments distincts et non nuls de k .

Soit donc $k = \mathbf{F}_{3^n}$, et J_1 et J_2 deux éléments distincts et non nuls de k .

Il existe une courbe de genre 3 définie sur k dont la jacobienne est isogène à $E_1^2 \times E_2$, où E_1 (resp. E_2) a comme invariant J_1 (resp. J_2).

Soit donc $k = \mathbf{F}_{3^n}$, et J_1 et J_2 deux éléments distincts et non nuls de k .

Il existe une courbe de genre 3 définie sur k dont la jacobienne est isogène à $E_1^2 \times E_2$, où E_1 (resp. E_2) a comme invariant J_1 (resp. J_2).

Le coefficient a_3 est déterminé par $J_1/J_2 = -a_3^3$, d'où

$$a_1 = \frac{a_3(a_3+1)^3}{J_1}.$$

Supposons désormais n impair ≥ 3 , et $q = 3^n$.

Supposons désormais n impair ≥ 3 , et $q = 3^n$.

Pour tout $j \in k - \mathbf{F}_3$, on obtient ainsi une courbe C associée au couple $(J_1 = j, J_2 = j^3)$, le coefficient a_3 correspondant vérifiant $a_3^3 = -J_1/J_2 = -1/J_1^2$,

Supposons désormais n impair ≥ 3 , et $q = 3^n$.

Pour tout $j \in k - \mathbf{F}_3$, on obtient ainsi une courbe C associée au couple $(J_1 = j, J_2 = j^3)$, le coefficient a_3 correspondant vérifiant $a_3^3 = -J_1/J_2 = -1/J_1^2$,

et une courbe C' associée au couple (J_2, J_1) , le coefficient a'_3 correspondant étant égal à $1/a_3$.

Supposons désormais n impair ≥ 3 , et $q = 3^n$.

Pour tout $j \in k - \mathbf{F}_3$, on obtient ainsi une courbe C associée au couple $(J_1 = j, J_2 = j^3)$, le coefficient a_3 correspondant vérifiant $a_3^3 = -J_1/J_2 = -1/J_1^2$,

et une courbe C' associée au couple (J_2, J_1) , le coefficient a'_3 correspondant étant égal à $1/a_3$.

Le coefficient en x^2 de la courbe E_1 est $a_3(a_3 + 1)$, alors que celui de la courbe E'_1 est $a'_3(1 + a'_3)$. Le quotient de ces deux termes vaut $a_3^3 = -1/J_1^2$, et n'est donc pas un carré. Par suite, les courbes E_1 et E'_1 sont tordues quadratiques l'une de l'autre, et la jacobienne de C' est la tordue quadratique de celle de C .

Par suite:

Soit $q = 3^n$, n impair. Si E est une courbe elliptique sur \mathbf{F}_q dont l'invariant $j(E)$ n'appartient pas à \mathbf{F}_3 , il existe une courbe C dont la jacobienne est isogène à E^3 , et une courbe C' dont la jacobienne est isogène à E'^3 , E' tordue quadratique de E .

Par suite:

Soit $q = 3^n$, n impair. Si E est une courbe elliptique sur \mathbf{F}_q dont l'invariant $j(E)$ n'appartient pas à \mathbf{F}_3 , il existe une courbe C dont la jacobienne est isogène à E^3 , et une courbe C' dont la jacobienne est isogène à E'^3 , E' tordue quadratique de E .

Corollaire.-

Soit $q = 3^n$, n impair. Si E est une courbe elliptique sur \mathbf{F}_q dont l'invariant $j(E)$ n'appartient pas à \mathbf{F}_3 , il existe une courbe C sur \mathbf{F}_q dont le nombre de points est $q + 1 + 3m(E)$ et une courbe C' dont le nombre de points est $q + 1 - 3m(E)$.

Pour $j = 1$ (resp. -1), la trace du Frobenius sur \mathbf{F}_3 vaut $m = \pm 1$ (resp. ± 2), d'où un discriminant $m^2 - 12 = -11$ (resp. -8).

Pour $j = 1$ (resp. -1), la trace du Frobenius sur \mathbf{F}_3 vaut $m = \pm 1$ (resp. ± 2), d'où un discriminant $m^2 - 12 = -11$ (resp. -8).
Or il existe m tel que $m^2 - 4 \times 3^n = -8$ (resp. -11) si et seulement si $n = 1$ ou $n = 3$ (resp. $n = 1$ ou 5).

Pour $j = 1$ (resp. -1), la trace du Frobenius sur \mathbf{F}_3 vaut $m = \pm 1$ (resp. ± 2), d'où un discriminant $m^2 - 12 = -11$ (resp. -8).

Or il existe m tel que $m^2 - 4 \times 3^n = -8$ (resp. -11) si et seulement si $n = 1$ ou $n = 3$ (resp. $n = 1$ ou 5).

Par suite, pour $n \geq 7$, pour tout entier m non divisible par 3 et tel que $|m| \leq 2\sqrt{q}$, où $q = 3^n$, il existe une courbe elliptique d'invariant dans $\mathbf{F}_q - \mathbf{F}_3$ et dont la trace du Frobenius vaut m .

Donc

Théorème.-

Soit n impair ≥ 7 ; si E est une courbe elliptique ordinaire sur $k = \mathbf{F}_{3^n}$, il existe une courbe de genre 3 sur k dont la jacobienne est k -isogène à E^3 .

D'où:

THÉORÈME.-

Soit n un entier impair ≥ 7 , et $q = 3^n$. Si m_q n'est pas divisible par 3, il existe deux courbes de genre 3 définies sur \mathbf{F}_q , l'une optimale, i.e. dont le nombre de points vaut $q + 1 + 3m_q$, l'autre "optimale minimale", i.e. dont le nombre de points vaut $q + 1 - 3m_q$.

Le plus petit n pour lequel on ne connaît pas $N_{3^n}(3)$ est $n = 5$.

Le plus petit n pour lequel on ne connaît pas $N_{3^n}(3)$ est $n = 5$.
Dans ce cas, Lauter a montré que le défaut d'optimalité en genre 3 est au moins 3, et qu'il existe une courbe C_0 pour laquelle

$$\text{Card } C_0(\mathbf{F}_q) = q + 1 + 3m_q - 3 \text{ ou}$$

$$\text{Card } C_0(\mathbf{F}_q) = q + 1 - (3m_q - 3).$$

Le plus petit n pour lequel on ne connaît pas $N_{3^n}(3)$ est $n = 5$. Dans ce cas, Lauter a montré que le défaut d'optimalité en genre 3 est au moins 3, et qu'il existe une courbe C_0 pour laquelle

$$\text{Card } C_0(\mathbf{F}_q) = q + 1 + 3m_q - 3 \text{ ou}$$

$$\text{Card } C_0(\mathbf{F}_q) = q + 1 - (3m_q - 3).$$

D'après ce qui précède, on peut en fait conclure: il existe une courbe C de genre 3 telle que $\text{Card } C(k) = 3^5 + 1 + 3m_q - 3$. En effet, l'invariant de la courbe elliptique optimale sur k , dont la trace du Frobenius vaut 31, est $J_1 = 1$; soit z une racine de $z^5 - z + 1$; z engendre k^* , et les invariants des courbes elliptiques dont la trace du Frobenius vaut $31 - 3 = 28$ sont z^{38} , z^{77} et leurs conjugués.

Prenons $J_2 = z^{38}$. Il existe une courbe C_{a_1, a_3} définie sur k , avec $a_3 = -1/J_2$, dont la jacobienne est k -isogène à $E_1^2 \times E_2$, E_1 et E_2 d'invariants respectifs J_1 et J_2 ; l'invariant de Hasse de chacune de ces deux courbes est $a_3(a_3 + 1)$, c'est-à-dire, à un carré près, $1 - J_2$; sa norme vaut 2, et est donc congrue à $-28 = -(m_q - 3) \pmod{3}$.

Prenons $J_2 = z^{38}$. Il existe une courbe C_{a_1, a_3} définie sur k , avec $a_3 = -1/J_2$, dont la jacobienne est k -isogène à $E_1^2 \times E_2$, E_1 et E_2 d'invariants respectifs J_1 et J_2 ; l'invariant de Hasse de chacune de ces deux courbes est $a_3(a_3 + 1)$, c'est-à-dire, à un carré près, $1 - J_2$; sa norme vaut 2, et est donc congrue à $-28 = -(m_q - 3) \pmod{3}$.

Par suite, la trace du Frobenius de E_1 est -31 et celle de E_2 est -28 ; donc la courbe de genre 3 associée a un nombre de points égal à $3^5 + 1 + 3m_q - 3$.

Avant de continuer ...

Une page de publicité

Une page de publicité

<http://www.manypoints.org/>

(Van der Geer, Ritzenthaler, Lauter, Howe, Top ...)

Caractéristique différente de 2 et 3. Quelques notations:

- Soit $j \neq 0, 1728$. Dans ce qui suit, on note $E(j)$ la courbe elliptique d'équation

$$y^2 = x^3 - 3\frac{j}{j-1728}x - \frac{3j}{4(j-1728)}.$$

Cette courbe est d'invariant j .

Caractéristique différente de 2 et 3. Quelques notations:

- Soit $j \neq 0, 1728$. Dans ce qui suit, on note $E(j)$ la courbe elliptique d'équation

$$y^2 = x^3 - 3\frac{j}{j-1728}x - \frac{3j}{4(j-1728)}.$$

Cette courbe est d'invariant j .

- On note $\rho \in \bar{k}$ une racine de $x^2 + x + 1$. Remarquons que $(\rho : \rho^2 : 1)$ est un point de la courbe C_{a_1, a_2, a_3, a_4} .

Caractéristique différente de 2 et 3. Quelques notations:

- Soit $j \neq 0, 1728$. Dans ce qui suit, on note $E(j)$ la courbe elliptique d'équation

$$y^2 = x^3 - 3\frac{j}{j-1728}x - \frac{3j}{4(j-1728)}.$$

Cette courbe est d'invariant j .

- On note $\rho \in \bar{k}$ une racine de $x^2 + x + 1$. Remarquons que $(\rho : \rho^2 : 1)$ est un point de la courbe C_{a_1, a_2, a_3, a_4} .
- Si E est une courbe elliptique, on note $E[3]$ le groupe de ses points d'exposant 3.

Points d'ordre 3 des courbes elliptiques et accouplement de Weil.

Soit E une courbe elliptique d'équation $y^2 = p(x)$, avec $p(x) = x^3 + ax + b$; l'équation aux abscisses de ses points d'ordre 3 est alors $f_3(x) = 2pp'' - p'^2 = 3x^4 + 6ax^2 + 12xb - a^2$. Par une homographie convenable, on peut ramener les quatre racines de f_3 à $\infty, 1, \rho, \rho^2$.

Points d'ordre 3 des courbes elliptiques et accouplement de Weil.

Soit E une courbe elliptique d'équation $y^2 = p(x)$, avec $p(x) = x^3 + ax + b$; l'équation aux abscisses de ses points d'ordre 3 est alors $f_3(x) = 2pp'' - p'^2 = 3x^4 + 6ax^2 + 12xb - a^2$. Par une homographie convenable, on peut ramener les quatre racines de f_3 à $\infty, 1, \rho, \rho^2$.

L'ensemble des birapports des 24 permutations de ces racines est égal à $\{-\rho, -\rho^2\}$, donc le groupe des homographies conservant les quatre racines de f_3 est isomorphe au groupe alterné A_4 . Si $f : E[3] \rightarrow E[3]$ est un isomorphisme préservant l'accouplement de Weil, l'équation aux abscisses de f restreinte à $E[3] - \{0\}$ est donnée par une telle homographie.

Par suite, si E' est une seconde courbe elliptique, d'équation $y^2 = x^3 + a'x + b'$, et si $g_3 = 3x^4 + 6a'x^2 + 12xb' - a'^2$, il existe douze homographies envoyant les racines de f_3 sur celles de g_3 , et elles correspondent aux isomorphismes de $E[3]$ sur $E'[3]$ commutant à l'accouplement de Weil.

Formulaire - I. De la quartique aux courbes elliptiques.

Si a_3 ou a_4 est nul, la courbe C_{a_1, a_2, a_3, a_4} n'est pas irréductible; on peut donc supposer $a_4 = 1$ et $a_3 \neq 0$.

Formulaire - I. De la quartique aux courbes elliptiques.

Si a_3 ou a_4 est nul, la courbe C_{a_1, a_2, a_3, a_4} n'est pas irréductible; on peut donc supposer $a_4 = 1$ et $a_3 \neq 0$.

De plus, comme la caractéristique de k est ici supposée différente de 2 et 3, on peut se ramener à $a_3 = 2$ par une transformation de la forme $X' = X + aT_1, Y' = Y + aT_1, Z' = Z + aT_1$, qui commute aux matrices de permutation et qui est inversible pour $3a + 1 \neq 0$, en prenant $a = \frac{2 - a_3}{3a_3}$.

Formulaire - I. De la quartique aux courbes elliptiques.

Si a_3 ou a_4 est nul, la courbe C_{a_1, a_2, a_3, a_4} n'est pas irréductible; on peut donc supposer $a_4 = 1$ et $a_3 \neq 0$.

De plus, comme la caractéristique de k est ici supposée différente de 2 et 3, on peut se ramener à $a_3 = 2$ par une transformation de la forme $X' = X + aT_1$, $Y' = Y + aT_1$, $Z' = Z + aT_1$, qui commute aux matrices de permutation et qui est inversible pour $3a + 1 \neq 0$, en prenant $a = \frac{2 - a_3}{3a_3}$.

On désigne désormais par C_{a_1, a_2} la courbe d'équation

$$a_1 T_1^4 + a_2 T_1^2 T_2 + 2T_1 T_3 + T_2^2 = 0.$$

Formulaire - I. De la quartique aux courbes elliptiques.

Si a_3 ou a_4 est nul, la courbe C_{a_1, a_2, a_3, a_4} n'est pas irréductible; on peut donc supposer $a_4 = 1$ et $a_3 \neq 0$.

De plus, comme la caractéristique de k est ici supposée différente de 2 et 3, on peut se ramener à $a_3 = 2$ par une transformation de la forme $X' = X + aT_1$, $Y' = Y + aT_1$, $Z' = Z + aT_1$, qui commute aux matrices de permutation et qui est inversible pour $3a + 1 \neq 0$, en prenant $a = \frac{2 - a_3}{3a_3}$.

On désigne désormais par C_{a_1, a_2} la courbe d'équation

$$a_1 T_1^4 + a_2 T_1^2 T_2 + 2 T_1 T_3 + T_2^2 = 0.$$

Son discriminant vaut $256 (27 a_1 + 5 + 9 a_2) d^3$, où

Formulaire - I. De la quartique aux courbes elliptiques.

Si a_3 ou a_4 est nul, la courbe C_{a_1, a_2, a_3, a_4} n'est pas irréductible; on peut donc supposer $a_4 = 1$ et $a_3 \neq 0$.

De plus, comme la caractéristique de k est ici supposée différente de 2 et 3, on peut se ramener à $a_3 = 2$ par une transformation de la forme $X' = X + aT_1$, $Y' = Y + aT_1$, $Z' = Z + aT_1$, qui commute aux matrices de permutation et qui est inversible pour $3a + 1 \neq 0$, en prenant $a = \frac{2 - a_3}{3a_3}$.

On désigne désormais par C_{a_1, a_2} la courbe d'équation

$$a_1 T_1^4 + a_2 T_1^2 T_2 + 2 T_1 T_3 + T_2^2 = 0.$$

Son discriminant vaut $256 (27 a_1 + 5 + 9 a_2) d^3$, où $d =$

$$-432 a_1 + 72 a_2^2 + 76 a_2^3 - 216 a_2^2 a_1 + 432 a_1^2 - 432 a_1 a_2 + 27 a_2^4.$$

Formulaire - I. De la quartique aux courbes elliptiques.

Si a_3 ou a_4 est nul, la courbe C_{a_1, a_2, a_3, a_4} n'est pas irréductible; on peut donc supposer $a_4 = 1$ et $a_3 \neq 0$.

De plus, comme la caractéristique de k est ici supposée différente de 2 et 3, on peut se ramener à $a_3 = 2$ par une transformation de la forme $X' = X + aT_1$, $Y' = Y + aT_1$, $Z' = Z + aT_1$, qui commute aux matrices de permutation et qui est inversible pour $3a + 1 \neq 0$, en prenant $a = \frac{2 - a_3}{3a_3}$.

On désigne désormais par C_{a_1, a_2} la courbe d'équation

$$a_1 T_1^4 + a_2 T_1^2 T_2 + 2 T_1 T_3 + T_2^2 = 0.$$

Son discriminant vaut $256 (27 a_1 + 5 + 9 a_2) d^3$, où $d =$

$$-432 a_1 + 72 a_2^2 + 76 a_2^3 - 216 a_2^2 a_1 + 432 a_1^2 - 432 a_1 a_2 + 27 a_2^4.$$

On note également $q_{a_1, a_3}(x, y)$ la forme non homogène de l'équation de C_{a_1, a_2} obtenue en posant $x = X/Z$, $y = Y/Z$.

Courbe quotient E_1

La courbe E_1 quotient de C_{a_1, a_2} par le groupe engendré par l'involution $(X, Y, Z) \mapsto (Y, X, Z)$ est une courbe elliptique d'équation affine

$$y^2 = x^3 - (3 + 2a_2)x - 4a_1 + 2 + 2a_2 + a_2^2$$

Courbe quotient E_1

La courbe E_1 quotient de C_{a_1, a_2} par le groupe engendré par l'involution $(X, Y, Z) \mapsto (Y, X, Z)$ est une courbe elliptique d'équation affine

$$y^2 = x^3 - (3 + 2a_2)x - 4a_1 + 2 + 2a_2 + a_2^2$$

et d'invariant modulaire

$$J_1 = 6912 \frac{(2a_2 + 3)^3}{d}.$$

Courbe quotient E_1

La courbe E_1 quotient de C_{a_1, a_2} par le groupe engendré par l'involution $(X, Y, Z) \mapsto (Y, X, Z)$ est une courbe elliptique d'équation affine

$$y^2 = x^3 - (3 + 2a_2)x - 4a_1 + 2 + 2a_2 + a_2^2$$

et d'invariant modulaire

$$J_1 = 6912 \frac{(2a_2 + 3)^3}{d}.$$

Le morphisme $\phi_1 : C_{a_1, a_2} \rightarrow E_1$ est donné par

$$\phi_1 : \begin{cases} x = \frac{X+Y-Z}{T_1}, \\ y = \frac{2(Z^2-XY)+a_2 T_1^2+4T_2}{T_1^2} \end{cases}$$

Le point à l'infini de E_1 est l'image par ϕ_1 de $(\rho : \rho^2 : 1)$ et l'on a

$$\phi_1^*\left(\frac{dx}{y}\right) = \frac{(y-x)dx}{q_y},$$

$$\text{où } q_y = \frac{\partial}{\partial y} q_{a_1, a_2}.$$

Si l'on quotiente C_{a_1, a_2} par le groupe engendré par l'involution $\tau : (X, Y, Z) \mapsto (X, Z, Y)$ (resp. $(X, Y, Z) \mapsto (X, Z, Y)$), on trouve la même courbe E_1 .

Si l'on quotiente C_{a_1, a_2} par le groupe engendré par l'involution $\tau : (X, Y, Z) \mapsto (X, Z, Y)$ (resp. $(X, Y, Z) \mapsto (X, Z, Y)$), on trouve la même courbe E_1 .

L'image réciproque de $\frac{dx}{y}$ est $\frac{(x-1)dx}{q_y}$ (resp. $\frac{(1-y)dx}{q_y}$).

Si l'on quotiente C_{a_1, a_2} par le groupe engendré par l'involution $\tau : (X, Y, Z) \mapsto (X, Z, Y)$ (resp. $(X, Y, Z) \mapsto (X, Z, Y)$), on trouve la même courbe E_1 .

L'image réciproque de $\frac{dx}{y}$ est $\frac{(x-1)dx}{q_y}$ (resp. $\frac{(1-y)dx}{q_y}$).

La somme de ces trois formes différentielles vaut 0, et elles sont deux-à-deux linéairement indépendantes.

Si l'on quotiente C_{a_1, a_2} par le groupe engendré par l'involution $\tau : (X, Y, Z) \mapsto (X, Z, Y)$ (resp. $(X, Y, Z) \mapsto (X, Z, Y)$), on trouve la même courbe E_1 .

L'image réciproque de $\frac{dx}{y}$ est $\frac{(x-1)dx}{q_y}$ (resp. $\frac{(1-y)dx}{q_y}$).

La somme de ces trois formes différentielles vaut 0, et elles sont deux-à-deux linéairement indépendantes.

La jacobienne de C_{a_1, a_2} est donc isogène à $E_1^2 \times E_2$, où E_2 est une courbe elliptique.

La seconde courbe elliptique E_2

La courbe E_2 est la jacobienne de de la courbe de genre 1 quotient de C_{a_1, a_2} par le groupe d'ordre 3 engendré par $\sigma : (X, Y, Z) \mapsto (Y, Z, X)$; une équation de E_2 est

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

La seconde courbe elliptique E_2

La courbe E_2 est la jacobienne de de la courbe de genre 1 quotient de C_{a_1, a_2} par le groupe d'ordre 3 engendré par $\sigma : (X, Y, Z) \mapsto (Y, Z, X)$; une équation de E_2 est

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

avec

$$A = -48 - 128 a_2 - 648 a_2^2 + 3456 a_1 a_2 - 648 a_2^3 + 1944 a_1 a_2^2 - 243 a_2^4 + 3168 a_1 - 3888 a_1^2$$

$$B = 512 a_2 - 2400 a_2^2 + 46080 a_1 a_2 - 7200 a_2^3 + 77760 a_1 a_2^2 - 9720 a_2^4 - 124416 a_1^2 a_2 + 54432 a_1 a_2^3 - 5832 a_2^5 - 69984 a_1^2 a_2^2 + 17496 a_1 a_2^4 - 1458 a_2^6 + 128 + 19328 a_1 - 120960 a_1^2 + 93312 a_1^3$$

Le quotient J_1/J_2 des invariants modulaires de E_1 et E_2 est un cube M_3^3

Le quotient J_1/J_2 des invariants modulaires de E_1 et E_2 est un cube M_3^3 avec

$$M_3 = \frac{A}{16(27a_1 + 5 + 9a_2)(3 + 2a_2)}.$$

Il existe un isomorphisme galoisien, commutant à l'accouplement de Weil, entre $E_1[3]$ et $E_2[3]$.

Il existe un isomorphisme galoisien, commutant à l'accouplement de Weil, entre $E_1[3]$ et $E_2[3]$.

Plus précisément, il existe une homographie définie sur k envoyant les abscisses des points d'ordre 3 de E_1 sur les abscisses des points d'ordre 3 de E_2 .

Soit J_1 un élément de $k - \{0, 1728\}$.

Soit J_1 un élément de $k - \{0, 1728\}$.

L'ensemble des courbes C_{a_1, a_2} telles que E_1 a comme invariant J_1 est une famille à un paramètre v ;

Soit J_1 un élément de $k - \{0, 1728\}$.

L'ensemble des courbes C_{a_1, a_2} telles que E_1 a comme invariant J_1 est une famille à un paramètre v ; on a

$$\begin{cases} a_1 = \frac{N}{16(J_1 - 1728)^2} \\ a_2 = \frac{3}{2} \frac{v^2 J_1 - J_1 + 1728}{J_1 - 1728} \end{cases}$$

$$\text{avec } N = 14929920 - 17280 J_1 + 5 J_1^2 + 10368 v^2 J_1 - 6 v^2 J_1^2 - 13824 v^3 J_1 + 8 v^3 J_1^2 + 9 v^4 J_1^2.$$

Soit J_1 un élément de $k - \{0, 1728\}$.

L'ensemble des courbes C_{a_1, a_2} telles que E_1 a comme invariant J_1 est une famille à un paramètre v ; on a

$$\begin{cases} a_1 = \frac{N}{16(J_1 - 1728)^2} \\ a_2 = \frac{3}{2} \frac{v^2 J_1 - J_1 + 1728}{J_1 - 1728} \end{cases}$$

$$\text{avec } N = 14929920 - 17280 J_1 + 5 J_1^2 + 10368 v^2 J_1 - 6 v^2 J_1^2 \\ - 13824 v^3 J_1 + 8 v^3 J_1^2 + 9 v^4 J_1^2.$$

La courbe E_1 est tordue de $E(J_1)$ par v .

L'invariant de E_2 est $J_2 = J_1 U^3/V^3$,

L'invariant de E_2 est $J_2 = J_1 U^3/V^3$,

avec

$$U = -2985984 + 35831808 v + J_1^2 - 3456 J_1 - 93312 v^2 J_1 + 54 v^2 J_1^2 \\ + 81 v^4 J_1^2 + 108 v^3 J_1^2 + 12 v J_1^2 - 41472 v J_1 \\ - 186624 v^3 J_1 - 559872 v^4 J_1$$

et

$$V = 243 v^4 J_1^2 + 216 v^3 J_1^2 + 54 v^2 J_1^2 - J_1^2 + 3456 J_1 \\ - 2985984 - 93312 v^2 J_1 - 373248 v^3 J_1.$$

L'invariant de E_2 est $J_2 = J_1 U^3/V^3$,

avec

$$U = -2985984 + 35831808 v + J_1^2 - 3456 J_1 - 93312 v^2 J_1 + 54 v^2 J_1^2 \\ + 81 v^4 J_1^2 + 108 v^3 J_1^2 + 12 v J_1^2 - 41472 v J_1 \\ - 186624 v^3 J_1 - 559872 v^4 J_1$$

et

$$V = 243 v^4 J_1^2 + 216 v^3 J_1^2 + 54 v^2 J_1^2 - J_1^2 + 3456 J_1 \\ - 2985984 - 93312 v^2 J_1 - 373248 v^3 J_1.$$

La courbe E_2 a comme équation $y^2 = x^3 + Cx + D$, avec

$$\begin{cases} C = -3v^2 J_1 (J_1 - 1728) J_2 V^3 \\ D = 2v^3 J_1 (J_1 - 1728) (J_2 - 1728) V^3 \end{cases}$$

Réciproquement, à tout couple d'invariants distincts J_1 et J_2 dans $k - \{0, 1728\}$ correspondent douze courbes C_{a_1, a_2} définies sur \bar{k} , dont les jacobiniennes sont isogènes à $E(J_1)^2 \times E(J_2)$.

Réciproquement, à tout couple d'invariants distincts J_1 et J_2 dans $k - \{0, 1728\}$ correspondent douze courbes C_{a_1, a_2} définies sur \bar{k} , dont les jacobiniennes sont isogènes à $E(J_1)^2 \times E(J_2)$.

Plus précisément, soit h l'une des 12 homographies envoyant les abscisses des points d'ordre 3 de $E(J_1)$ sur les abscisses des points d'ordre 3 de $E(J_2)$; le paramètre v précédent est donné par

$$\frac{1}{v} = 3h(\infty).$$

Obtention de $J(C)$ par recollement de E_1^2 et E_2

Soit $\Phi_2 = \Phi_1 \circ \tau : C_{a_1, a_2} \rightarrow E_1$, et

$\Psi : C_{a_1, a_2} \rightarrow E_2 = C_{a_1, a_2} / \langle \sigma \rangle$ un revêtement de degré 3 tel que
 $\Psi(\rho : \rho^2 : 1) = 0$.

Obtention de $J(C)$ par recollement de E_1^2 et E_2

Soit $\Phi_2 = \Phi_1 \circ \tau : C_{a_1, a_2} \rightarrow E_1$, et

$\Psi : C_{a_1, a_2} \rightarrow E_2 = C_{a_1, a_2} / \langle \sigma \rangle$ un revêtement de degré 3 tel que $\Psi(\rho : \rho^2 : 1) = 0$.

Soit $f : E_1^2 \times E_2 \rightarrow \text{Pic}^0(C_{a_1, a_2})$ définie par

$$(P, Q, R) \mapsto \Phi_1^*((P) - (0)) + \Phi_2^*((Q) - (0)) + \Psi^*((R) - (0))$$

et $g : \text{Pic}^0(C_{a_1, a_2}) \rightarrow E_1^2 \times E_2$ définie par

$$D \mapsto (\Phi_1(D), \Phi_2(D), \Psi(D));$$

L'application composée $g \circ f : E_1^2 \times E_2 \rightarrow E_1^2 \times E_2$ est donnée par la matrice $\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$.

L'application composée $g \circ f : E_1^2 \times E_2 \rightarrow E_1^2 \times E_2$ est donnée par

la matrice $\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$.

Par suite, le degré de f (resp. de g) est égal à 3.

La jacobienne de C_{a_1, a_2} est obtenue par recollement de E_1^2 muni de la polarisation $\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$ et de E_2 munie de la polarisation $3 Id$, via l'isomorphisme galoisien de $E_1[3]$ sur $E_2[3]$ précédent.

Soit k un corps fini, de cardinal q , et J l'ensemble, éventuellement vide, des invariants des courbes elliptiques dont la valeur absolue de la trace du Frobenius sur \mathbf{F}_q vaut m_q ¹.

¹On exclut les cas $m_q^2 - 4q = -3, -4, -8, -11$, car il n'existe pas de courbe optimale dans ces cas.

Soit k un corps fini, de cardinal q , et J l'ensemble, éventuellement vide, des invariants des courbes elliptiques dont la valeur absolue de la trace du Frobenius sur \mathbf{F}_q vaut m_q ¹.

Pour tout couple j, j' d'éléments de J , on calcule les racines de l'équation $J_2(j, v) = j'$, puis le nombre de points de la courbe de genre 3 associée à chacune de ces racines par les formules ci-dessus.

¹On exclut les cas $m_q^2 - 4q = -3, -4, -8, -11$, car il n'existe pas de courbe optimale dans ces cas.

Pour les nombres premiers $p \leq 10723$, i.e. les 1308 premiers nombres premiers, cette méthode échoue à trouver une courbe de genre 3 dont le nombre de points est $p + 1 + 3m$ dans 97 cas.

Pour les nombres premiers $p \leq 10723$, i.e. les 1308 premiers nombres premiers, cette méthode échoue à trouver une courbe de genre 3 dont le nombre de points est $p + 1 + 3m$ dans 97 cas. Pour ces cas, le nombre de classes de $m^2 - 4p$ est en général égal à 1, sauf dans 10 cas, où on trouve
-20, -24, -35, -100, -123, -187, de nombre de classes 2, et
-59, de nombre de classes 3.

Pour les nombres premiers $p \leq 10723$, i.e. les 1308 premiers nombres premiers, cette méthode échoue à trouver une courbe de genre 3 dont le nombre de points est $p + 1 + 3m$ dans 97 cas. Pour ces cas, le nombre de classes de $m^2 - 4p$ est en général égal à 1, sauf dans 10 cas, où on trouve
-20, -24, -35, -100, -123, -187, de nombre de classes 2, et
-59, de nombre de classes 3.

Les 19 nombres premiers < 1000 pour lequel la méthode précédente ne permet pas de trouver une courbe optimale sont
53, 167, 173, 193, 293, 311, 347,
353, 359, 479, 523, 557, 569, 661, 709, 773, 787, 823, 997.

Cas où q n'est pas premier

On peut faire de même lorsque $q = p^n$ n'est pas premier, et jouer alors avec le fait que J_1 et $J_2 = J_1^p$ peuvent être distincts.

Cas où q n'est pas premier

On peut faire de même lorsque $q = p^n$ n'est pas premier, et jouer alors avec le fait que J_1 et $J_2 = J_1^p$ peuvent être distincts. Soit par exemple $q = 19^3$; en prenant $J_1 = J_2$, où J_1 est l'invariant d'une courbe elliptique optimale sur \mathbf{F}_q , on trouve une courbe de genre 3 dont le nombre de points est $q + 1 - 3m_q$. On a perdu : c'est une courbe "optimale minimale".

On peut faire de même lorsque $q = p^n$ n'est pas premier, et jouer alors avec le fait que J_1 et $J_2 = J_1^p$ peuvent être distincts.

Soit par exemple $q = 19^3$; en prenant $J_1 = J_2$, où J_1 est l'invariant d'une courbe elliptique optimale sur \mathbf{F}_q , on trouve une courbe de genre 3 dont le nombre de points est $q + 1 - 3m_q$. On a perdu : c'est une courbe "optimale minimale".

Par contre, en prenant $J_2 = J_1^{19}$, on trouve une courbe optimale !

Il s'agit d'un cas important, notamment pour étudier le cas de la caractéristique 7.

Il s'agit d'un cas important, notamment pour étudier le cas de la caractéristique 7.

Avec les notations précédentes, $J_1/J_2 = M_3^3$, donc M_3 est alors égal à 1, ρ ou ρ^2 .

$$M_3 = 1$$

L'équation $M_3 = 1$ s'écrit

$$\begin{aligned} & -288 - 720 a_2 - 936 a_2^2 + 2592 a_1 a_2 - 648 a_2^3 + 1944 a_1 a_2^2 \\ & -243 a_2^4 + 1872 a_1 - 3888 a_1^2 = 0 \end{aligned}$$

$$M_3 = 1$$

L'équation $M_3 = 1$ s'écrit

$$\begin{aligned} & -288 - 720 a_2 - 936 a_2^2 + 2592 a_1 a_2 - 648 a_2^3 + 1944 a_1 a_2^2 \\ & - 243 a_2^4 + 1872 a_1 - 3888 a_1^2 = 0 \end{aligned}$$

courbe rationnelle que l'on peut paramétrer par

$$M_3 = 1$$

L'équation $M_3 = 1$ s'écrit

$$\begin{aligned} & -288 - 720 a_2 - 936 a_2^2 + 2592 a_1 a_2 - 648 a_2^3 + 1944 a_1 a_2^2 \\ & -243 a_2^4 + 1872 a_1 - 3888 a_1^2 = 0 \end{aligned}$$

courbe rationnelle que l'on peut paramétrer par

$$\begin{cases} a_1 = \frac{1}{432} \frac{112 t^4 + 272 t^3 + 408 t^2 + 296 t + 127}{(t^2 + t + 1)^2}, \\ a_2 = -\frac{8 t^2 + 10 t + 9}{6(t^2 + t + 1)} \end{cases}$$

Dans ce qui suit, on note C_t la courbe d'équation

$$(t^2 + t + 1)^2(a_1 T_1^4 + a_2 T_1^2 T_2 + 2T_1 T_3 + T_2^2) = 0,$$

a_1 et a_2 étant les fractions rationnelles en t précédentes.

Dans ce qui suit, on note C_t la courbe d'équation

$$(t^2 + t + 1)^2(a_1 T_1^4 + a_2 T_1^2 T_2 + 2T_1 T_3 + T_2^2) = 0,$$

a_1 et a_2 étant les fractions rationnelles en t précédentes.
Le discriminant de C_t est $2^{118}3^{74}(t-1)^9(t^2+t+1)^{43}$.

Dans ce qui suit, on note C_t la courbe d'équation

$$(t^2 + t + 1)^2(a_1 T_1^4 + a_2 T_1^2 T_2 + 2T_1 T_3 + T_2^2) = 0,$$

a_1 et a_2 étant les fractions rationnelles en t précédentes.
Le discriminant de C_t est $2^{118}3^{74}(t-1)^9(t^2+t+1)^{43}$.

On a alors $J_1 = 1728t^3$.

Dans ce qui suit, on note C_t la courbe d'équation

$$(t^2 + t + 1)^2(a_1 T_1^4 + a_2 T_1^2 T_2 + 2T_1 T_3 + T_2^2) = 0,$$

a_1 et a_2 étant les fractions rationnelles en t précédentes.
Le discriminant de C_t est $2^{118}3^{74}(t-1)^9(t^2+t+1)^{43}$.

On a alors $J_1 = 1728t^3$.

Il existe donc une quartique de type S_3 sur k telle que $J_1 = J_2$ si et seulement si J_1 est un cube.

Dans ce qui suit, on note C_t la courbe d'équation

$$(t^2 + t + 1)^2(a_1 T_1^4 + a_2 T_1^2 T_2 + 2T_1 T_3 + T_2^2) = 0,$$

a_1 et a_2 étant les fractions rationnelles en t précédentes.
Le discriminant de C_t est $2^{118}3^{74}(t-1)^9(t^2+t+1)^{43}$.

On a alors $J_1 = 1728t^3$.

Il existe donc une quartique de type S_3 sur k telle que $J_1 = J_2$ si et seulement si J_1 est un cube.

La courbe E_2 a comme équation

$$y^2 = x^3 - 3t(t^3 - 1)x - 2(t^3 - 1)^2,$$

Dans ce qui suit, on note C_t la courbe d'équation

$$(t^2 + t + 1)^2(a_1 T_1^4 + a_2 T_1^2 T_2 + 2T_1 T_3 + T_2^2) = 0,$$

a_1 et a_2 étant les fractions rationnelles en t précédentes.
Le discriminant de C_t est $2^{118}3^{74}(t-1)^9(t^2+t+1)^{43}$.

On a alors $J_1 = 1728t^3$.

Il existe donc une quartique de type S_3 sur k telle que $J_1 = J_2$ si et seulement si J_1 est un cube.

La courbe E_2 a comme équation

$$y^2 = x^3 - 3t(t^3 - 1)x - 2(t^3 - 1)^2,$$

et la courbe E_1 est tordue de E_2 par $-3(t^2 + t + 1)$.

1) L'invariant modulaire d'une courbe elliptique E est un cube si et seulement si le degré de l'extension $k(E[3])/k$ est premier à 3.

2) Supposons que $k = \mathbf{F}_q$ (q impair).

2) Supposons que $k = \mathbf{F}_q$ (q impair).

a) Si $q \equiv 2 \pmod{3}$, j est toujours un cube (comme tout élément de k).

2) Supposons que $k = \mathbf{F}_q$ (q impair).

a) Si $q \equiv 2 \pmod{3}$, j est toujours un cube (comme tout élément de k).

b) Si $q \equiv 1 \pmod{3}$, une condition suffisante pour que j soit un cube est que $m(E) = q + 1 - N_q(E)$ soit divisible par 3; en effet, dans ce cas, ni E ni sa tordue quadratique n'ont de point d'ordre 3 rationnel sur \mathbf{F}_q , et le polynôme f_3 des abscisses des points d'ordre 3 de E et de sa tordue n'a donc pas de racine dans \mathbf{F}_q . Par suite, il n'a pas de facteur irréductible de degré 3.

3) La relation

$$(t^3 - 1)^2 = (t^2 + t + 1)((t\rho)^2 + t\rho + 1)((t\rho^2)^2 + t\rho^2 + 1)$$

montre que, dès que j est un cube, il existe $t \in k$ tel que $j = 1728t^3$ et $t^2 + t + 1$ est un carré dans k .

4) Lorsque $t^2 + t + 1 = 0$, i.e. $t = \rho$ ou ρ^2 , on a $J_1 = J_2 = 1728$; la quartique C_t a un discriminant nul, et sa réduction modulo $t^2 + t + 1$ est, sur une extension convenable de $k(t)$, la courbe hyperelliptique $y^2 = x(x^6 - 1)$.

4) Lorsque $t^2 + t + 1 = 0$, i.e. $t = \rho$ ou ρ^2 , on a $J_1 = J_2 = 1728$; la quartique C_t a un discriminant nul, et sa réduction modulo $t^2 + t + 1$ est, sur une extension convenable de $k(t)$, la courbe hyperelliptique $y^2 = x(x^6 - 1)$.

En effet, il suffit d'écrire l'équation de la quartique sous la forme $A^2 - \varepsilon B + O(\varepsilon^2) = 0$, $A = 0$ étant l'équation d'une conique Co non singulière; lorsque ε tend vers 0, la quartique "tend" vers la courbe hyperelliptique revêtement double de la conique Co ramifié aux points d'intersection de Co et de la courbe d'équation $B = 0$.

Pour le voir, on peut supposer que $A = y - x^2$.

Pour le voir, on peut supposer que $A = y - x^2$.

Faisons le changement de variables $(x, y) \mapsto (x, u)$, avec
 $u\sqrt{\varepsilon} = y - x^2$.

Pour le voir, on peut supposer que $A = y - x^2$.

Faisons le changement de variables $(x, y) \mapsto (x, u)$, avec $u\sqrt{\varepsilon} = y - x^2$.

La quartique devient $u^2 - B(x, x^2 + \sqrt{\varepsilon}u) + O(\varepsilon) = 0$, qui tend vers la courbe hyperelliptique $u^2 = B(x, x^2)$.

Ici, on paramètre la conique $t^2 + t + 1 = u^2$ par

$$\begin{cases} t = \rho^2 \frac{\varepsilon^2 - \rho^2}{\varepsilon^2 - 1} \\ u = -\sqrt{-3} \frac{\varepsilon}{\varepsilon^2 - 1} \end{cases} .$$

Pour $\varepsilon = 0$, on a $(t, u) = (\rho, 0)$.

Ici, on paramètre la conique $t^2 + t + 1 = u^2$ par

$$\begin{cases} t = \rho^2 \frac{\varepsilon^2 - \rho^2}{\varepsilon^2 - 1} \\ u = -\sqrt{-3} \frac{\varepsilon}{\varepsilon^2 - 1} \end{cases} .$$

Pour $\varepsilon = 0$, on a $(t, u) = (\rho, 0)$.

Après le changement de variables $(X, Y, Z) \mapsto (X, Y, S)$, avec $X + Y + Z = 2Su$, la quartique C_t s'écrit $A^2 - 12\varepsilon B + O(\varepsilon^2) = 0$, où $A = S^2 - \sqrt{-3}(X^2 + XY + Y^2)$ et $B = S(X + Y)(A - \sqrt{-3}XY)$.

Ici, on paramètre la conique $t^2 + t + 1 = u^2$ par

$$\begin{cases} t = \rho^2 \frac{\varepsilon^2 - \rho^2}{\varepsilon^2 - 1} \\ u = -\sqrt{-3} \frac{\varepsilon}{\varepsilon^2 - 1} \end{cases} .$$

Pour $\varepsilon = 0$, on a $(t, u) = (\rho, 0)$.

Après le changement de variables $(X, Y, Z) \mapsto (X, Y, S)$, avec $X + Y + Z = 2Su$, la quartique C_t s'écrit $A^2 - 12\varepsilon B + O(\varepsilon^2) = 0$,

où $A = S^2 - \sqrt{-3}(X^2 + XY + Y^2)$ et

$$B = S(X + Y)(A - \sqrt{-3}XY).$$

En paramétrant la conique C_0 d'équation $A = 0$ par

$\mu = \sqrt[4]{-3}(X - \rho Y)/S$, les huit paramètres des points d'intersection de C_0 et de la quartique d'équation $B = 0$ sont $0, \infty, \pm\rho, \pm\rho^2, \pm 1$.

Ici, on paramètre la conique $t^2 + t + 1 = u^2$ par

$$\begin{cases} t = \rho^2 \frac{\varepsilon^2 - \rho^2}{\varepsilon^2 - 1} \\ u = -\sqrt{-3} \frac{\varepsilon}{\varepsilon^2 - 1} \end{cases}.$$

Pour $\varepsilon = 0$, on a $(t, u) = (\rho, 0)$.

Après le changement de variables $(X, Y, Z) \mapsto (X, Y, S)$, avec $X + Y + Z = 2Su$, la quartique C_t s'écrit $A^2 - 12\varepsilon B + O(\varepsilon^2) = 0$,

où $A = S^2 - \sqrt{-3}(X^2 + XY + Y^2)$ et

$$B = S(X + Y)(A - \sqrt{-3}XY).$$

En paramétrant la conique C_0 d'équation $A = 0$ par

$\mu = \sqrt[4]{-3}(X - \rho Y)/S$, les huit paramètres des points d'intersection de C_0 et de la quartique d'équation $B = 0$ sont $0, \infty, \pm\rho, \pm\rho^2, \pm 1$.

Par suite, sur \bar{k} , la courbe hyperelliptique "limite" de C_t quand t tend vers ρ a comme équation $y^2 = x(x^6 - 1)$.

THÉORÈME.-

Soit n un entier impair, $q = 7^n$, et E une courbe elliptique définie sur $k = \mathbf{F}_q$, dont la trace du Frobenius m est congrue à 9, 15 ou 18 mod 21. Il existe une courbe de genre 3, définie sur k , dont le nombre de points vaut $7^n + 1 - 3m$.

THÉORÈME.-

Soit n un entier impair, $q = 7^n$, et E une courbe elliptique définie sur $k = \mathbf{F}_q$, dont la trace du Frobenius m est congrue à 9, 15 ou 18 mod 21. Il existe une courbe de genre 3, définie sur k , dont le nombre de points vaut $7^n + 1 - 3m$.

En effet, les conditions sur m signifient que $m \equiv 0 \pmod{3}$ et que m est un carré modulo 7.

THÉORÈME.-

Soit n un entier impair, $q = 7^n$, et E une courbe elliptique définie sur $k = \mathbf{F}_q$, dont la trace du Frobenius m est congrue à 9, 15 ou 18 mod 21. Il existe une courbe de genre 3, définie sur k , dont le nombre de points vaut $7^n + 1 - 3m$.

En effet, les conditions sur m signifient que $m \equiv 0 \pmod{3}$ et que m est un carré modulo 7.

D'après ce qui précède, l'invariant de E est un cube $1728t^3$, et l'on peut choisir t tel que $t^2 + t + 1$ est un carré dans k .

THÉORÈME.-

Soit n un entier impair, $q = 7^n$, et E une courbe elliptique définie sur $k = \mathbf{F}_q$, dont la trace du Frobenius m est congrue à 9, 15 ou 18 mod 21. Il existe une courbe de genre 3, définie sur k , dont le nombre de points vaut $7^n + 1 - 3m$.

En effet, les conditions sur m signifient que $m \equiv 0 \pmod{3}$ et que m est un carré modulo 7.

D'après ce qui précède, l'invariant de E est un cube $1728t^3$, et l'on peut choisir t tel que $t^2 + t + 1$ est un carré dans k .

Il existe donc une courbe de genre 3 définie sur k dont la jacobienne est isogène à E_2^3 , où E_2 a comme équation $y^2 = x^3 + Ax + B$, avec $A = -3t(t^3 - 1)$, $B = -2(t^3 - 1)^2$.

Par suite, $m(E_2)$ est congru mod 7 à la norme de $3B$, qui est un carré dans \mathbf{F}_7 , comme $m(E)$.

Par suite, $m(E_2)$ est congru mod 7 à la norme de $3B$, qui est un carré dans \mathbf{F}_7 , comme $m(E)$.

Si E était tordue quadratique de E_2 , on aurait $m(E_2) = -m(E)$,

Par suite, $m(E_2)$ est congru mod 7 à la norme de $3B$, qui est un carré dans \mathbf{F}_7 , comme $m(E)$.

Si E était tordue quadratique de E_2 , on aurait $m(E_2) = -m(E)$, ce qui est exclu puisque -1 n'est pas un carré dans \mathbf{F}_7^n .

Par suite, $m(E_2)$ est congru mod 7 à la norme de $3B$, qui est un carré dans \mathbf{F}_7 , comme $m(E)$.

Si E était tordue quadratique de E_2 , on aurait $m(E_2) = -m(E)$, ce qui est exclu puisque -1 n'est pas un carré dans \mathbf{F}_7^n .

D'où le résultat.

COROLLAIRE.-

Soit $k = \mathbf{F}_q$ un corps fini de caractéristique 7; il existe une courbe de genre 3 définie sur \mathbf{F}_q dont le nombre de points est $\geq q + 1 + 3(m_q - 11)$.

Cas où $k = \mathbf{Q}$ et E_1 de type CM

Si $k = \mathbf{Q}$, E_1 et E_2 ne sont pas k -isomorphes, puisque tordues l'une de l'autre par $-3(t^2 + t + 1)$.

Cas où $k = \mathbf{Q}$ et E_1 de type CM

Si $k = \mathbf{Q}$, E_1 et E_2 ne sont pas k -isomorphes, puisque tordues l'une de l'autre par $-3(t^2 + t + 1)$.

Néanmoins, si elles sont à multiplications complexes, elles peuvent être isogènes sur \mathbf{Q} .

Cas où $k = \mathbf{Q}$ et E_1 de type CM

Si $k = \mathbf{Q}$, E_1 et E_2 ne sont pas k -isomorphes, puisque tordues l'une de l'autre par $-3(t^2 + t + 1)$.

Néanmoins, si elles sont à multiplications complexes, elles peuvent être isogènes sur \mathbf{Q} .

Dans ce cas, la jacobienne de C est isogène à E_1^3 .

Les 13 courbes elliptiques à multiplications complexes définies sur \mathbf{Q} ont comme invariant

$$2^6 3^3, 2^6 5^3, 0, -3^3 5^3, -2^{15}, -2^{15} 3^3, -2^{18} 3^3 5^3, -2^{15} 3^3 5^3 11^3, \\ -2^{18} 3^3 5^3 23^3 29^3, 2^3 3^3 11^3, 2^4 3^3 5^3, 3^3 5^3 17^3, -3 \cdot 2^{15} 5^3,$$

les anneaux d'endomorphismes associés étant ceux de discriminant

$$-4, -8, -3, -7, -11, -19, -43, -67, -163, -16, -12, -28, -27.$$

À part le onzième et le treizième, tous ces invariants sont des cubes, les valeurs de t associées étant

$$1, 5/3, 0, -5/4, -8/3, -8, -80, -440, -53360, 11/2, \frac{85}{4}.$$

La valeur $t = 1$ donne une quartique singulière; pour les dix autres valeurs, on obtient dix courbes de genre 3. À des facteurs carrés près, les quantités $-3(t^2 + t + 1)$ valent respectivement $-3, -3, -7, -3, -19, -43, -67, -163, -1, -7$, les anneaux d'endomorphismes ayant comme discriminant

$$-8, -3, -7, -11, -19, -43, -67, -163, -16, -28.$$

À part le premier et quatrième cas, les courbes E_1 et E_2 sont donc \mathbf{Q} -isogènes, et on obtient ainsi huit quartiques définies sur \mathbf{Q} dont la jacobienne est \mathbf{Q} -isogène au cube d'une courbe elliptique à multiplications complexes, les anneaux d'endomorphismes étant $-3, -7, -19, -43, -67, -163, -16, -28$.

On suppose ici que $\rho \in k$; la courbe d'équation $M_3 = \rho$ admet une paramétrisation rationnelle par un paramètre t tel que $J_1 = J_2 = \frac{(-1+24t)^3}{t^3(-1+27t)}$. On reconnaît l'invariant modulaire de la courbe E_t d'équation $y^2 + xy + ty = x^3$, i.e. la courbe elliptique universelle ayant un point d'ordre 3 (cf. 2.1). Par ailleurs, alors que, dans le cas $M_3 = 1$, E_1 et E_2 sont tordues quadratiques l'une de l'autre par $-3(t^2 + t + 1)$, ici E_1 et E_2 sont $k(t)$ -isomorphes, et tordues quadratiques par $(\rho - 1)(36t + \rho - 1)$ de la courbe E_t .

Supposons que $k = \mathbf{F}_{7^n}$, n impair, et prenons $\rho = 2$. Si E est une courbe elliptique sur k dont le nombre de points est $7^n + 1 - a$, et que $a \equiv -1 \pmod{3}$, le courbe E a un point d'ordre 3. Soit F la courbe quotient de E par le groupe engendré par ce point. D'après 2.1, il existe $t \in k$ tel que $E = E_t$ et, -3 étant un carré dans k , $F = F_{-t+1/27}$. La courbe de genre 3 associée à t (resp. $-t + 1/27$) est isogène au cube de E ou de sa tordue quadratique, selon que $t + 1$ est un carré ou non (resp. au cube de F ou de sa tordue quadratique, selon que $36(1/27 - t) + \rho - 1 = -t$ est un carré ou non). Comme, à un carré près, le discriminant de E_t est égal à $t(1 + t)$, on en déduit que, si a est impair, i.e. si E n'a pas de point d'ordre 2 sur k , ou si $a \equiv 0 \pmod{4}$, dans lequel cas, quitte à remplacer E par une courbe 2-isogène, E a trois points d'ordre 2, il existe un unique résidu quadratique dans l'ensemble $\{-t, 1 + t\}$.

Donc, si $a \not\equiv -1 \pmod{3}$ et $a \not\equiv 2 \pmod{4}$, il existe une courbe de genre 3 isogène à E^3 et une autre isogène au cube de la tordue de E . En remplaçant E par sa tordue quadratique, on a le même résultat si $a \equiv 1 \pmod{3}$ et $a \not\equiv 2 \pmod{4}$, d'où la partie 2 du théorème énoncé en introduction. Le point 2 du corollaire s'ensuit (et peut être précisé: à moins que $m_q \equiv 36, 51, 58$ ou $78 \pmod{84}$, le défaut est au plus 6).