Problemas de números de clase relativos para cuerpos de funciones

Kiran S. Kedlaya
con Santiago Arango-Piñeros, María Chara, Asimina Hamakiotes, y Gustavo Rama

Department of Mathematics, University of California San Diego (EE.UU.)
kedlaya@ucsd.edu
Estas diapositivas están disponibles de https://kskedlaya.org/slides/.

Teoría de Números en las Américas 2 (Number Theory in the Americas 2)
Casa Matemática Oaxaca, Oaxaca, México
9 de septiembre, 2024

Apoyo financiero recibido de NSF (grant DMS-2401536) y UC San Diego (Warschawski Professorship).

Reconozco que mi lugar de trabajo ocupa tierras ancestrales no cedidas de la Nación Kumeyaay.

Numeros de clase relativos

En este proyecto, un **cuerpo de funciones** F es el cuerpo de las funciones racionales de una curva "chida"[1] C sobre un cuerpo finito $\mathbb{F}_q$. Sea g_F el **genero** de F (o de C) y h_F el **numero de clase** de F; es el orden del grupo $J(C)(\mathbb{F}_q)$ donde J es la **variedad Jacobiana** de C.

Sea F'/F una extensión finita y separable de cuerpos de funciones, asociada al cubrimiento $C' \to C$. El **número de clase relativo** $h_{F'/F} := h_{F'}/h_F$ es un entero; es el orden de $A(\mathbb{F}_q)$ para una variedad abeliana A sobre $\mathbb{F}_q$ (la **variedad Prym** del cubrimiento $C' \to C$).

Un poco de contexto: para una extensión de cuerpos de **numeros** no es verdad en general, excepto cuando F es totalmente real, F'/F es cuadrática, y F' es totalmente complejo. Este incluye el caso donde $F = \mathbb{Q}$ y F' es cuadrático imaginario, como en el problema de número de clase de Gauss ($h_{F'/F} = 1$ ssi $F' = \mathbb{Q}(\sqrt{-D})$ con $D \in \{2, 3, 4, 7, 11, 19, 43, 67, 163\}$).

[1] Abreviatura propuesta por Santi para "suave, proyectiva, y geométricamente irreducible"

Numeros de clase relativos

En este proyecto, un **cuerpo de funciones** F es el cuerpo de las funciones racionales de una curva "chida"[1] C sobre un cuerpo finito $\mathbb{F}_q$. Sea g_F el **genero** de F (o de C) y h_F el **numero de clase** de F; es el orden del grupo $J(C)(\mathbb{F}_q)$ donde J es la **variedad Jacobiana** de C.

Sea F'/F una extensión finita y separable de cuerpos de funciones, asociada al cubrimiento $C' \to C$. El **número de clase relativo** $h_{F'/F} := h_{F'}/h_F$ es un entero; es el orden de $A(\mathbb{F}_q)$ para una variedad abeliana A sobre $\mathbb{F}_q$ (la **variedad Prym** del cubrimiento $C' \to C$).

Un poco de contexto: para una extensión de cuerpos de **numeros** no es verdad en general, excepto cuando F es totalmente real, F'/F es cuadrática, y F' es totalmente complejo. Este incluye el caso donde $F = \mathbb{Q}$ y F' es cuadrático imaginario, como en el problema de número de clase de Gauss ($h_{F'/F} = 1$ ssi $F' = \mathbb{Q}(\sqrt{-D})$ con $D \in \{2, 3, 4, 7, 11, 19, 43, 67, 163\}$).

[1] Abreviatura propuesta por Santi para "suave, proyectiva, y geométricamente irreducible"

Numeros de clase relativos

En este proyecto, un **cuerpo de funciones** F es el cuerpo de las funciones racionales de una curva "chida"[1] C sobre un cuerpo finito $\mathbb{F}_q$. Sea g_F el **genero** de F (o de C) y h_F el **numero de clase** de F; es el orden del grupo $J(C)(\mathbb{F}_q)$ donde J es la **variedad Jacobiana** de C.

Sea F'/F una extensión finita y separable de cuerpos de funciones, asociada al cubrimiento $C' \to C$. El **número de clase relativo** $h_{F'/F} := h_{F'}/h_F$ es un entero; es el orden de $A(\mathbb{F}_q)$ para una variedad abeliana A sobre $\mathbb{F}_q$ (la **variedad Prym** del cubrimiento $C' \to C$).

Un poco de contexto: para una extensión de cuerpos de **numeros** no es verdad en general, excepto cuando F es totalmente real, F'/F es cuadrática, y F' es totalmente complejo. Este incluye el caso donde $F = \mathbb{Q}$ y F' es cuadrático imaginario, como en el problema de número de clase de Gauss ($h_{F'/F} = 1$ ssi $F' = \mathbb{Q}(\sqrt{-D})$ con $D \in \{2, 3, 4, 7, 11, 19, 43, 67, 163\}$).

[1] Abreviatura propuesta por Santi para "suave, proyectiva, y geométricamente irreducible"

Un teorema y dos problemas

Theorem (K, 2022)

En los casos donde $\dim(A) > 0$*, tenemos una clasificación finita de los casos con* $h_{F'/F} = 1$*. (Las excepciones son cuando* $g_{F'} = g_F$ *y tambien* $g_F = 0$ *o* $q' = q$*.)*

Problem

Demonstrar que para cada $m > 1$*, hay una cota* **efectiva** *(computable) para los casos con* $h_{F'/F} = m$*. (Tenemos que controlar* q, g, g'*.)*

Problem

Hacer una clasificación completa para $h_{F'/F} = 2$*.*

Es natural dividir el trabajo según si $q \geq 5$; $q = 3, 4$; o $q = 2$; y basta considerar los casos donde F'/F es **constante** ($F' = F \cdot \mathbb{F}_{q'}$) or **totalmente geométrica** ($q' = q$).

Un teorema y dos problemas

Theorem (K, 2022)

En los casos donde $\dim(A) > 0$*, tenemos una clasificación finita de los casos con* $h_{F'/F} = 1$*. (Las excepciones son cuando* $g_{F'} = g_F$ *y tambien* $g_F = 0$ *o* $q' = q$*.)*

Problem

Demonstrar que para cada $m > 1$*, hay una cota* **efectiva** *(computable) para los casos con* $h_{F'/F} = m$*. (Tenemos que controlar* q, g, g'*.)*

Problem

Hacer una clasificación completa para $h_{F'/F} = 2$*.*

Es natural dividir el trabajo según si $q \geq 5$; $q = 3, 4$; o $q = 2$; y basta considerar los casos donde F'/F es **constante** ($F' = F \cdot \mathbb{F}_{q'}$) or **totalmente geométrica** ($q' = q$).

Un teorema y dos problemas

Theorem (K, 2022)

En los casos donde $\dim(A) > 0$*, tenemos una clasificación finita de los casos con* $h_{F'/F} = 1$*. (Las excepciones son cuando* $g_{F'} = g_F$ *y tambien* $g_F = 0$ *o* $q' = q$*.)*

Problem

Demonstrar que para cada $m > 1$*, hay una cota* **efectiva** *(computable) para los casos con* $h_{F'/F} = m$*. (Tenemos que controlar* q, g, g'*.)*

Problem

Hacer una clasificación completa para $h_{F'/F} = 2$*.*

Es natural dividir el trabajo según si $q \geq 5$; $q = 3, 4$; o $q = 2$; y basta considerar los casos donde F'/F es **constante** ($F' = F \cdot \mathbb{F}_{q'}$) or **totalmente geométrica** ($q' = q$).

Esquema de la prueba

- Paso 1: Obtener una lista finita que **no depende** en q que siempre contiene el polinomio de Weil de A si $\#A(\mathbb{F}_q) = m$. (Esto incluye acotar $\dim(A)$ para cada q, y también q.)
- Paso 2a: Para cada q, obtener una lista finita de pares $(P_C, P_{C'})$ que siempre contiene los polinomio de Weil de C y C' si F'/F es constante. (Nota: $A = (\mathrm{Res}_{\mathbb{F}_{q'}/\mathbb{F}_q} J(C'))/J(C)$.)
- Paso 2b: Para cada (q, d) con $d > 1$, obtener una lista finita de pares $(P_C, P_{C'})$ que contiene los polinomio de Weil de C y C' si F'/F es geométrica de grado d.
- Paso 3: Identificar todas las curvas C cuyos polynomios de Weil aparecen en estas listas.
- Paso 4: Para cada curva C que aparece en la lista de (q, d), computar todas las extensiónes **cíclicas** de F de grado d y buscar casos con $h_{F'/F} = m$.
- Paso 5: Para cada (q, d) con $d > 2$, para cada par $(P_C, P_{C'})$ en la lista de (q, d), computar todas las extensiónes **no cíclicas** de F de grado d y buscar casos con $h_{F'/F}$ **o** usar los polinomios para demonstrar que no es posible.

Esquema de la prueba

- Paso 1: Obtener una lista finita que **no depende** en q que siempre contiene el polinomio de Weil de A si $\#A(\mathbb{F}_q) = m$. (Esto incluye acotar $\dim(A)$ para cada q, y también q.)
- Paso 2a: Para cada q, obtener una lista finita de pares $(P_C, P_{C'})$ que siempre contiene los polinomio de Weil de C y C' si F'/F es constante. (Nota: $A = (\mathrm{Res}_{\mathbb{F}_{q'}/\mathbb{F}_q} J(C'))/J(C)$.)
- Paso 2b: Para cada (q, d) con $d > 1$, obtener una lista finita de pares $(P_C, P_{C'})$ que contiene los polinomio de Weil de C y C' si F'/F es geométrica de grado d.
- Paso 3: Identificar todas las curvas C cuyos polynomios de Weil aparecen en estas listas.
- Paso 4: Para cada curva C que aparece en la lista de (q, d), computar todas las extensiónes **cíclicas** de F de grado d y buscar casos con $h_{F'/F} = m$.
- Paso 5: Para cada (q, d) con $d > 2$, para cada par $(P_C, P_{C'})$ en la lista de (q, d), computar todas las extensiónes **no cíclicas** de F de grado d y buscar casos con $h_{F'/F}$ **o** usar los polinomios para demonstrar que no es posible.

Esquema de la prueba

- Paso 1: Obtener una lista finita que **no depende** en q que siempre contiene el polinomio de Weil de A si $\#A(\mathbb{F}_q) = m$. (Esto incluye acotar $\dim(A)$ para cada q, y también q.)
- Paso 2a: Para cada q, obtener una lista finita de pares $(P_C, P_{C'})$ que siempre contiene los polinomio de Weil de C y C' si F'/F es constante. (Nota: $A = (\mathrm{Res}_{\mathbb{F}_{q'}/\mathbb{F}_q} J(C'))/J(C)$.)
- Paso 2b: Para cada (q, d) con $d > 1$, obtener una lista finita de pares $(P_C, P_{C'})$ que contiene los polinomio de Weil de C y C' si F'/F es geométrica de grado d.
- Paso 3: Identificar todas las curvas C cuyos polynomios de Weil aparecen en estas listas.
- Paso 4: Para cada curva C que aparece en la lista de (q, d), computar todas las extensiónes **cíclicas** de F de grado d y buscar casos con $h_{F'/F} = m$.
- Paso 5: Para cada (q, d) con $d > 2$, para cada par $(P_C, P_{C'})$ en la lista de (q, d), computar todas las extensiónes **no cíclicas** de F de grado d y buscar casos con $h_{F'/F}$ **o** usar los polinomios para demonstrar que no es posible.

Esquema de la prueba

- Paso 1: Obtener una lista finita que **no depende** en q que siempre contiene el polinomio de Weil de A si $\#A(\mathbb{F}_q) = m$. (Esto incluye acotar $\dim(A)$ para cada q, y también q.)
- Paso 2a: Para cada q, obtener una lista finita de pares $(P_C, P_{C'})$ que siempre contiene los polinomio de Weil de C y C' si F'/F es constante. (Nota: $A = (\mathrm{Res}_{\mathbb{F}_{q'}/\mathbb{F}_q} J(C'))/J(C)$.)
- Paso 2b: Para cada (q, d) con $d > 1$, obtener una lista finita de pares $(P_C, P_{C'})$ que contiene los polinomio de Weil de C y C' si F'/F es geométrica de grado d.
- Paso 3: Identificar todas las curvas C cuyos polynomios de Weil aparecen en estas listas.
- Paso 4: Para cada curva C que aparece en la lista de (q, d), computar todas las extensiónes **cíclicas** de F de grado d y buscar casos con $h_{F'/F} = m$.
- Paso 5: Para cada (q, d) con $d > 2$, para cada par $(P_C, P_{C'})$ en la lista de (q, d), computar todas las extensiónes **no cíclicas** de F de grado d y buscar casos con $h_{F'/F}$ **o** usar los polinomios para demonstrar que no es posible.

Esquema de la prueba

- Paso 1: Obtener una lista finita que **no depende** en q que siempre contiene el polinomio de Weil de A si $\#A(\mathbb{F}_q) = m$. (Esto incluye acotar $\dim(A)$ para cada q, y también q.)
- Paso 2a: Para cada q, obtener una lista finita de pares $(P_C, P_{C'})$ que siempre contiene los polinomio de Weil de C y C' si F'/F es constante. (Nota: $A = (\mathrm{Res}_{\mathbb{F}_{q'}/\mathbb{F}_q} J(C'))/J(C)$.)
- Paso 2b: Para cada (q, d) con $d > 1$, obtener una lista finita de pares $(P_C, P_{C'})$ que contiene los polinomio de Weil de C y C' si F'/F es geométrica de grado d.
- Paso 3: Identificar todas las curvas C cuyos polynomios de Weil aparecen en estas listas.
- Paso 4: Para cada curva C que aparece en la lista de (q, d), computar todas las extensiónes **cíclicas** de F de grado d y buscar casos con $h_{F'/F} = m$.
- Paso 5: Para cada (q, d) con $d > 2$, para cada par $(P_C, P_{C'})$ en la lista de (q, d), computar todas las extensiónes **no cíclicas** de F de grado d y buscar casos con $h_{F'/F}$ **o** usar los polinomios para demonstrar que no es posible.

Esquema de la prueba

- Paso 1: Obtener una lista finita que **no depende** en q que siempre contiene el polinomio de Weil de A si $\#A(\mathbb{F}_q) = m$. (Esto incluye acotar $\dim(A)$ para cada q, y también q.)
- Paso 2a: Para cada q, obtener una lista finita de pares $(P_C, P_{C'})$ que siempre contiene los polinomio de Weil de C y C' si F'/F es constante. (Nota: $A = (\mathrm{Res}_{\mathbb{F}_{q'}/\mathbb{F}_q} J(C'))/J(C)$.)
- Paso 2b: Para cada (q, d) con $d > 1$, obtener una lista finita de pares $(P_C, P_{C'})$ que contiene los polinomio de Weil de C y C' si F'/F es geométrica de grado d.
- Paso 3: Identificar todas las curvas C cuyos polynomios de Weil aparecen en estas listas.
- Paso 4: Para cada curva C que aparece en la lista de (q, d), computar todas las extensiónes **cíclicas** de F de grado d y buscar casos con $h_{F'/F} = m$.
- Paso 5: Para cada (q, d) con $d > 2$, para cada par $(P_C, P_{C'})$ en la lista de (q, d), computar todas las extensiónes **no cíclicas** de F de grado d y buscar casos con $h_{F'/F}$ **o** usar los polinomios para demonstrar que no es posible.

Esquema de la prueba

- Paso 1: Obtener una lista finita que **no depende** en q que siempre contiene el polinomio de Weil de A si $\#A(\mathbb{F}_q) = m$. (Esto incluye acotar $\dim(A)$ para cada q, y también q.)
- Paso 2a: Para cada q, obtener una lista finita de pares $(P_C, P_{C'})$ que siempre contiene los polinomio de Weil de C y C' si F'/F es constante. (Nota: $A = (\mathrm{Res}_{\mathbb{F}_{q'}/\mathbb{F}_q} J(C'))/J(C)$.)
- Paso 2b: Para cada (q, d) con $d > 1$, obtener una lista finita de pares $(P_C, P_{C'})$ que contiene los polinomio de Weil de C y C' si F'/F es geométrica de grado d.
- Paso 3: Identificar todas las curvas C cuyos polynomios de Weil aparecen en estas listas.
- Paso 4: Para cada curva C que aparece en la lista de (q, d), computar todas las extensiónes **cíclicas** de F de grado d y buscar casos con $h_{F'/F} = m$.
- Paso 5: Para cada (q, d) con $d > 2$, para cada par $(P_C, P_{C'})$ en la lista de (q, d), computar todas las extensiónes **no cíclicas** de F de grado d y buscar casos con $h_{F'/F}$ **o** usar los polinomios para demonstrar que no es posible.

Paso 1: el polinomio de Weil de A $(q > 2)$

En lo que sigue, $T_{*,q}$ denota la traza de Frobenius de $*$.

- Por Riemann-Hurwitz, $\dim(A) \geq g - 1$. (Si F'/F es constante, $\dim(A) \geq g$.)
- Para $q \geq 5$, el teorema de Weil implica que $\#A(\mathbb{F}_q) \geq (\sqrt{q} - 1)^{2g}$.
- Para $q = 3, 4$, combinamos algunos ingredientes:
  - A es isógena a $E^m \times B$ con E la única curva elíptica sobre $\mathbb{F}_q$ con $\#E(\mathbb{F}_q) = 1$, $m \geq 0$ un entero, y B una variedad abeliana que no tiene E como factor; tenemos $T_{A,q} = q(\dim(A) - \dim(B)) + T_{B,q}$. Un teorema de Kadets implica que $\#B(\mathbb{F}_q) \geq 1{,}259^{\dim(B)}$ si $q = 3$ y $\#B(\mathbb{F}_q) \geq 2{,}236^{\dim(B)}$ si $q = 4$.
  - Si F'/F es constante, $T_{A,q} = -T_{J(C),q} = \#C(\mathbb{F}_q) - q - 1$. Si es geométrica,
  $$0 \leq \#C'(\mathbb{F}_q) = q + 1 - T_{J(C'),q} = q + 1 - (T_{J(C),q} + T_{A,q}) = \#C(\mathbb{F}_q) - T_{A,q}.$$
  - $\#C(\mathbb{F}_q) \leq 1{,}153g + 11{,}67$ si $q = 3$ y $\#C(\mathbb{F}_q) \leq 1{,}435g + 21{,}75$ si $q = 4$.

Paso 1: el polinomio de Weil de A ($q > 2$)

En lo que sigue, $T_{*,q}$ denota la traza de Frobenius de $*$.

- Por Riemann-Hurwitz, $\dim(A) \geq g - 1$. (Si F'/F es constante, $\dim(A) \geq g$.)
- Para $q \geq 5$, el teorema de Weil implica que $\#A(\mathbb{F}_q) \geq (\sqrt{q} - 1)^{2g}$.
- Para $q = 3, 4$, combinamos algunos ingredientes:
  - A es isógena a $E^m \times B$ con E la única curva elíptica sobre $\mathbb{F}_q$ con $\#E(\mathbb{F}_q) = 1$, $m \geq 0$ un entero, y B una variedad abeliana que no tiene E como factor; tenemos $T_{A,q} = q(\dim(A) - \dim(B)) + T_{B,q}$. Un teorema de Kadets implica que $\#B(\mathbb{F}_q) \geq 1{,}259^{\dim(B)}$ si $q = 3$ y $\#B(\mathbb{F}_q) \geq 2{,}236^{\dim(B)}$ si $q = 4$.
  - Si F'/F es constante, $T_{A,q} = -T_{J(C),q} = \#C(\mathbb{F}_q) - q - 1$. Si es geométrica,

$$0 \leq \#C'(\mathbb{F}_q) = q + 1 - T_{J(C'),q} = q + 1 - (T_{J(C),q} + T_{A,q}) = \#C(\mathbb{F}_q) - T_{A,q}.$$

  - $\#C(\mathbb{F}_q) \leq 1{,}153g + 11{,}67$ si $q = 3$ y $\#C(\mathbb{F}_q) \leq 1{,}435g + 21{,}75$ si $q = 4$.

Paso 1: el polinomio de Weil de A $(q > 2)$

En lo que sigue, $T_{*,q}$ denota la traza de Frobenius de $*$.

- Por Riemann-Hurwitz, $\dim(A) \geq g - 1$. (Si F'/F es constante, $\dim(A) \geq g$.)
- Para $q \geq 5$, el teorema de Weil implica que $\#A(\mathbb{F}_q) \geq (\sqrt{q} - 1)^{2g}$.
- Para $q = 3, 4$, combinamos algunos ingredientes:
  - A es isógena a $E^m \times B$ con E la única curva elíptica sobre $\mathbb{F}_q$ con $\#E(\mathbb{F}_q) = 1$, $m \geq 0$ un entero, y B una variedad abeliana que no tiene E como factor; tenemos $T_{A,q} = q(\dim(A) - \dim(B)) + T_{B,q}$. Un teorema de Kadets implica que $\#B(\mathbb{F}_q) \geq 1{,}259^{\dim(B)}$ si $q = 3$ y $\#B(\mathbb{F}_q) \geq 2{,}236^{\dim(B)}$ si $q = 4$.
  - Si F'/F es constante, $T_{A,q} = -T_{J(C),q} = \#C(\mathbb{F}_q) - q - 1$. Si es geométrica,
  $$0 \leq \#C'(\mathbb{F}_q) = q + 1 - T_{J(C'),q} = q + 1 - (T_{J(C),q} + T_{A,q}) = \#C(\mathbb{F}_q) - T_{A,q}.$$
  - $\#C(\mathbb{F}_q) \leq 1{,}153g + 11{,}67$ si $q = 3$ y $\#C(\mathbb{F}_q) \leq 1{,}435g + 21{,}75$ si $q = 4$.

Paso 1: el polinomio de Weil de A $(q > 2)$

En lo que sigue, $T_{*,q}$ denota la traza de Frobenius de $*$.

- Por Riemann-Hurwitz, $\dim(A) \geq g - 1$. (Si F'/F es constante, $\dim(A) \geq g$.)
- Para $q \geq 5$, el teorema de Weil implica que $\#A(\mathbb{F}_q) \geq (\sqrt{q} - 1)^{2g}$.
- Para $q = 3, 4$, combinamos algunos ingredientes:
  - A es isógena a $E^m \times B$ con E la única curva elíptica sobre $\mathbb{F}_q$ con $\#E(\mathbb{F}_q) = 1$, $m \geq 0$ un entero, y B una variedad abeliana que no tiene E como factor; tenemos $T_{A,q} = q(\dim(A) - \dim(B)) + T_{B,q}$. Un teorema de Kadets implica que $\#B(\mathbb{F}_q) \geq 1{,}259^{\dim(B)}$ si $q = 3$ y $\#B(\mathbb{F}_q) \geq 2{,}236^{\dim(B)}$ si $q = 4$.
  - Si F'/F es constante, $T_{A,q} = -T_{J(C),q} = \#C(\mathbb{F}_q) - q - 1$. Si es geométrica,
$$0 \leq \#C'(\mathbb{F}_q) = q + 1 - T_{J(C'),q} = q + 1 - (T_{J(C),q} + T_{A,q}) = \#C(\mathbb{F}_q) - T_{A,q}.$$
  - $\#C(\mathbb{F}_q) \leq 1{,}153g + 11{,}67$ si $q = 3$ y $\#C(\mathbb{F}_q) \leq 1{,}435g + 21{,}75$ si $q = 4$.

Paso 1: el polinomio de Weil de A ($q > 2$)

En lo que sigue, $T_{*,q}$ denota la traza de Frobenius de $*$.

- Por Riemann-Hurwitz, $\dim(A) \geq g - 1$. (Si F'/F es constante, $\dim(A) \geq g$.)
- Para $q \geq 5$, el teorema de Weil implica que $\#A(\mathbb{F}_q) \geq (\sqrt{q} - 1)^{2g}$.
- Para $q = 3, 4$, combinamos algunos ingredientes:
  - A es isógena a $E^m \times B$ con E la única curva elíptica sobre $\mathbb{F}_q$ con $\#E(\mathbb{F}_q) = 1$, $m \geq 0$ un entero, y B una variedad abeliana que no tiene E como factor; tenemos $T_{A,q} = q(\dim(A) - \dim(B)) + T_{B,q}$. Un teorema de Kadets implica que $\#B(\mathbb{F}_q) \geq 1{,}259^{\dim(B)}$ si $q = 3$ y $\#B(\mathbb{F}_q) \geq 2{,}236^{\dim(B)}$ si $q = 4$.
  - Si F'/F es constante, $T_{A,q} = -T_{J(C),q} = \#C(\mathbb{F}_q) - q - 1$. Si es geométrica,
$$0 \leq \#C'(\mathbb{F}_q) = q + 1 - T_{J(C'),q} = q + 1 - (T_{J(C),q} + T_{A,q}) = \#C(\mathbb{F}_q) - T_{A,q}.$$
  - $\#C(\mathbb{F}_q) \leq 1{,}153g + 11{,}67$ si $q = 3$ y $\#C(\mathbb{F}_q) \leq 1{,}435g + 21{,}75$ si $q = 4$.

Paso 1: el polinomio de Weil de A ($q > 2$)

En lo que sigue, $T_{*,q}$ denota la traza de Frobenius de $*$.

- Por Riemann-Hurwitz, $\dim(A) \geq g - 1$. (Si F'/F es constante, $\dim(A) \geq g$.)
- Para $q \geq 5$, el teorema de Weil implica que $\#A(\mathbb{F}_q) \geq (\sqrt{q} - 1)^{2g}$.
- Para $q = 3, 4$, combinamos algunos ingredientes:
  - A es isógena a $E^m \times B$ con E la única curva elíptica sobre $\mathbb{F}_q$ con $\#E(\mathbb{F}_q) = 1$, $m \geq 0$ un entero, y B una variedad abeliana que no tiene E como factor; tenemos $T_{A,q} = q(\dim(A) - \dim(B)) + T_{B,q}$. Un teorema de Kadets implica que $\#B(\mathbb{F}_q) \geq 1{,}259^{\dim(B)}$ si $q = 3$ y $\#B(\mathbb{F}_q) \geq 2{,}236^{\dim(B)}$ si $q = 4$.
  - Si F'/F es constante, $T_{A,q} = -T_{J(C),q} = \#C(\mathbb{F}_q) - q - 1$. Si es geométrica,

$$0 \leq \#C'(\mathbb{F}_q) = q + 1 - T_{J(C'),q} = q + 1 - (T_{J(C),q} + T_{A,q}) = \#C(\mathbb{F}_q) - T_{A,q}.$$

  - $\#C(\mathbb{F}_q) \leq 1{,}153g + 11{,}67$ si $q = 3$ y $\#C(\mathbb{F}_q) \leq 1{,}435g + 21{,}75$ si $q = 4$.

Paso 1: el polinomio de Weil de A $(q > 2)$

En lo que sigue, $T_{*,q}$ denota la traza de Frobenius de $*$.

- Por Riemann-Hurwitz, $\dim(A) \geq g - 1$. (Si F'/F es constante, $\dim(A) \geq g$.)
- Para $q \geq 5$, el teorema de Weil implica que $\#A(\mathbb{F}_q) \geq (\sqrt{q} - 1)^{2g}$.
- Para $q = 3, 4$, combinamos algunos ingredientes:
  - A es isógena a $E^m \times B$ con E la única curva elíptica sobre $\mathbb{F}_q$ con $\#E(\mathbb{F}_q) = 1$, $m \geq 0$ un entero, y B una variedad abeliana que no tiene E como factor; tenemos $T_{A,q} = q(\dim(A) - \dim(B)) + T_{B,q}$. Un teorema de Kadets implica que $\#B(\mathbb{F}_q) \geq 1{,}259^{\dim(B)}$ si $q = 3$ y $\#B(\mathbb{F}_q) \geq 2{,}236^{\dim(B)}$ si $q = 4$.
  - Si F'/F es constante, $T_{A,q} = -T_{J(C),q} = \#C(\mathbb{F}_q) - q - 1$. Si es geométrica,
$$0 \leq \#C'(\mathbb{F}_q) = q + 1 - T_{J(C'),q} = q + 1 - (T_{J(C),q} + T_{A,q}) = \#C(\mathbb{F}_q) - T_{A,q}.$$
  - $\#C(\mathbb{F}_q) \leq 1{,}153g + 11{,}67$ si $q = 3$ y $\#C(\mathbb{F}_q) \leq 1{,}435g + 21{,}75$ si $q = 4$.

Paso 1: el polinomio de Weil de A ($q = 2$)

Para $q = 2$, no podemos clasificar A tan facilmente: existe una infinitud de variedades abelianas **simples** B con $\#B(\mathbb{F}_2) = 1$.

Sin embargo, cuando $\#A(\mathbb{F}_2) = m$, se puede establecer directamente una desigualdad de la forma

$$*T_{A,2} + *T_{A,4} + *T_{A,8} + *T_{A,16} \geq c_0 g + c_1.$$

Esto implica una cota de la forma

$$*\#C(\mathbb{F}_2) + *\#C(\mathbb{F}_4) + *\#C(\mathbb{F}_8) + *\#C(\mathbb{F}_{16}) \geq c_0 g + c_1.$$

Por otro lado, si a_i denota el numero de places de C de grado i, el método de "programación lineal" de Ihara–Serre–Oesterlé produce algunas desigualdades de la forma

$$*a_1 + *a_2 + *a_3 + *a_4 \leq c_0' g + c_1'.$$

Paso 1: el polinomio de Weil de A ($q = 2$)

Para $q = 2$, no podemos clasificar A tan facilmente: existe una infinitud de variedades abelianas **simples** B con $\#B(\mathbb{F}_2) = 1$.

Sin embargo, cuando $\#A(\mathbb{F}_2) = m$, se puede establecer directamente una desigualdad de la forma

$$*T_{A,2} + *T_{A,4} + *T_{A,8} + *T_{A,16} \geq c_0 g + c_1.$$

Esto implica una cota de la forma

$$*\#C(\mathbb{F}_2) + *\#C(\mathbb{F}_4) + *\#C(\mathbb{F}_8) + *\#C(\mathbb{F}_{16}) \geq c_0 g + c_1.$$

Por otro lado, si a_i denota el numero de places de C de grado i, el método de "programación lineal" de Ihara–Serre–Oesterlé produce algunas desigualdades de la forma

$$*a_1 + *a_2 + *a_3 + *a_4 \leq c_0' g + c_1'.$$

Paso 1: el polinomio de Weil de A ($q = 2$)

Para $q = 2$, no podemos clasificar A tan facilmente: existe una infinitud de variedades abelianas **simples** B con $\#B(\mathbb{F}_2) = 1$.

Sin embargo, cuando $\#A(\mathbb{F}_2) = m$, se puede establecer directamente una desigualdad de la forma

$$* T_{A,2} + * T_{A,4} + * T_{A,8} + * T_{A,16} \geq c_0 g + c_1.$$

Esto implica una cota de la forma

$$*\#C(\mathbb{F}_2) + *\#C(\mathbb{F}_4) + *\#C(\mathbb{F}_8) + *\#C(\mathbb{F}_{16}) \geq c_0 g + c_1.$$

Por otro lado, si a_i denota el numero de places de C de grado i, el método de "programación lineal" de Ihara–Serre–Oesterlé produce algunas desigualdades de la forma

$$*a_1 + *a_2 + *a_3 + *a_4 \leq c_0' g + c_1'.$$

Paso 1: el polinomio de Weil de A ($q = 2$)

Para $q = 2$, no podemos clasificar A tan facilmente: existe una infinitud de variedades abelianas **simples** B con $\#B(\mathbb{F}_2) = 1$.

Sin embargo, cuando $\#A(\mathbb{F}_2) = m$, se puede establecer directamente una desigualdad de la forma

$$*T_{A,2} + *T_{A,4} + *T_{A,8} + *T_{A,16} \geq c_0 g + c_1.$$

Esto implica una cota de la forma

$$*\#C(\mathbb{F}_2) + *\#C(\mathbb{F}_4) + *\#C(\mathbb{F}_8) + *\#C(\mathbb{F}_{16}) \geq c_0 g + c_1.$$

Por otro lado, si a_i denota el numero de places de C de grado i, el método de "programación lineal" de Ihara–Serre–Oesterlé produce algunas desigualdades de la forma

$$*a_1 + *a_2 + *a_3 + *a_4 \leq c_0' g + c_1'.$$

Otros pasos

SageMath puede tabular polinomios de Weil sobre $\mathbb{F}_q$ de grado especificado. Comparando a la lista de polinomios de Weil para A y usando condiciones geométricas (e.g., $\#C'(\mathbb{F}_{q'}) \geq 0$), pueden restringir los polinomios de Weil de C y C'.

Cuando g y q son pequenos, LMFDB tiene tablas completas de curvas de genero g sobre $\mathbb{F}_q$. Tal vez necesitaremos extender el alcance de las tablas...

Magma puede computar extensiones abelianas de un cuerpo de funciones F de grado especificado (usando la teoría de cuerpos de clases).

Cuando $d > 2$, generalmente se puede eliminar las extensiones no abelianas por un análisis de la clausura normal de F'/F. Cuando esto falla, se puede aplicar otras técnicas (e.g., las parametrizaciones de Bhargava por $d \leq 5$).

Otros pasos

SageMath puede tabular polinomios de Weil sobre $\mathbb{F}_q$ de grado especificado. Comparando a la lista de polinomios de Weil para A y usando condiciones geométricas (e.g., $\#C'(\mathbb{F}_{q'}) \geq 0$), pueden restringir los polinomios de Weil de C y C'.

Cuando g y q son pequenos, LMFDB tiene tablas completas de curvas de genero g sobre $\mathbb{F}_q$. Tal vez necesitaremos extender el alcance de las tablas...

Magma puede computar extensiones abelianas de un cuerpo de funciones F de grado especificado (usando la teoría de cuerpos de clases).

Cuando $d > 2$, generalmente se puede eliminar las extensiones no abelianas por un análisis de la clausura normal de F'/F. Cuando esto falla, se puede aplicar otras técnicas (e.g., las parametrizaciones de Bhargava por $d \leq 5$).

Otros pasos

SageMath puede tabular polinomios de Weil sobre $\mathbb{F}_q$ de grado especificado. Comparando a la lista de polinomios de Weil para A y usando condiciones geométricas (e.g., $\#C'(\mathbb{F}_{q'}) \geq 0$), pueden restringir los polinomios de Weil de C y C'.

Cuando g y q son pequenos, LMFDB tiene tablas completas de curvas de genero g sobre $\mathbb{F}_q$. Tal vez necesitaremos extender el alcance de las tablas...

Magma puede computar extensiones abelianas de un cuerpo de funciones F de grado especificado (usando la teoría de cuerpos de clases).

Cuando $d > 2$, generalmente se puede eliminar las extensiones no abelianas por un análisis de la clausura normal de F'/F. Cuando esto falla, se puede aplicar otras técnicas (e.g., las parametrizaciones de Bhargava por $d \leq 5$).

Otros pasos

SageMath puede tabular polinomios de Weil sobre $\mathbb{F}_q$ de grado especificado. Comparando a la lista de polinomios de Weil para A y usando condiciones geométricas (e.g., $\#C'(\mathbb{F}_{q'}) \geq 0$), pueden restringir los polinomios de Weil de C y C'.

Cuando g y q son pequenos, LMFDB tiene tablas completas de curvas de genero g sobre $\mathbb{F}_q$. Tal vez necesitaremos extender el alcance de las tablas...

Magma puede computar extensiones abelianas de un cuerpo de funciones F de grado especificado (usando la teoría de cuerpos de clases).

Cuando $d > 2$, generalmente se puede eliminar las extensiones no abelianas por un análisis de la clausura normal de F'/F. Cuando esto falla, se puede aplicar otras técnicas (e.g., las parametrizaciones de Bhargava por $d \leq 5$).