NOTES DEL SEMINARI DE

teoria adeno mbres
ub·uab·upc

20è ANY

Criptografía: mini-curso.
Galois representations and Diophantine problems.
Successions de Sloane

20 ANYS
teoria adeno mbres
ub·uab·upc

Barcelona 2006

15

Notes del Seminari de Teoria de Nombres
(UB-UAB-UPC)

Criptografía: mini-curso.
Galois representations and Diophantine problems.
Successions de Sloane

Especial 20è aniversari

Edició a cura de

J. C. Lario D. Remón

Amb contribucions de

P. Bayer T. Crespo G. Frey J. González-Rovira

N. Koblitz A. Rio X. Xarles

J. C. Lario
Facultat de Matemàtiques
i Estadística
Universitat Politècnica de Catalunya
Pau Gargallo, 5
08028 Barcelona

D. Remón
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de
les Corts Catalanes, 585
08007 Barcelona

Barcelona, 2006
Amb suport parcial de MTM2006-15038-C02-01, BFM2003-01898 i
MTM2006-04895

ISBN: 84-934244-4-7

Índex

Introducció

Aquesta vegada el Seminari de Teoria de Nombres (UB-UAB-UPC) tenia raons per estar de Festa Major. Es tractava de la 20a edició del Seminari i la nostra col·lega Pilar Bayer feia anys rodons. Per aquest motiu el programa va ser un xic especial, diferent del d'altres edicions.

Vam comptar amb la presència de Neal Koblitz, que va impartir un minicurs sobre aspectes matemàtics de la Criptografia en relació amb les corbes el·líptiques.

La tarda de dimecres vam fer una sessió especial dedicada a l'aniversari de Pilar Bayer. Vam comptar amb una xerrada de la historiadora Ann Koblitz sobre el quefer de les dones matemàtiques i una altra xerrada de Gerhard Frey sobre problemes diofàntics i l'aritmètica de les representacions del grup de Galois absolut. Al final d'aquestes notes trobareu algunes fotos de la festa i de l'original pastís commemoratiu.

Amb les intervencions de Neal Koblitz i Gerhard Frey, hem tingut l'oportunitat de reviure algunes de les aportacions que més han marcat el nostre seminari al llarg d'aquests anys.

D'altra banda, i com de costum, les sessions matinals van incloure cinc xerrades per part de membres del STNB (UB-UAB-UPC). En aquesta ocasió, sota el títol "Successions de Sloane" s'amagaven algunes sorpreses per contribuir a l'esperit festiu.

Si bé per raons de la mare natura no vam podar comptar amb la presència d'alguns i alguna col·lega (que tant haurien volgut participar en aquesta edició), cal destacar que la presència de nous joves que s'incorporaven al STNB per primera vegada fa preveure que tindrem moltes més ocasions per celebrar la teoria i els nombres.

J. C. Lario
Barcelona, 8 de gener de 2007

30 de enero de 2006

Seminario de Teoría de Números

Celebración del 20 Aniverario del Seminario y del 60 Aniversario de Pilar Bayer

Barcelona

LA RELACIÓN ENTRE LA CRIPTOGRAFÍA Y LAS MATEMÁTICAS PURAS:

I. ALGUNOS TEMAS EN LA CRIPTOGRAFÍA DE CURVAS ELÍPTICAS

II. LA "SEGURIDAD DEMOSTRABLE"

Neal Koblitz

Universidad del Estado de Washington

Seattle, EEUU

koblitz@math.washington.edu

LA CRIPTOGRAFÍA DE CLAVE PÚBLICA

1976 — el concepto de clave pública fue inventado por Whit Diffie y Martin Hellman

1977 — el primer sistema práctico fue propuesto por Ron Rivest, Adi Shamir, y Leonard Adleman

(La criptografía de clave pública y el sistema de RSA fueron descubiertos un poco más temprano en secreto en Inglaterra, pero los servicios de inteligencia británicos no entendían su importancia o la posibilidad de tales aplicaciones como las firmas digitales.)

La idea central:

La función de enciframiento está accesible a cualquier persona, usando la clave pública. Sin embargo, la función inversa (de desciframiento) puede ser calculada solamente por la persona que posee otra clave — la secreta.

Además del enciframiento de los mensajes secretos, la criptografía de clave pública tiene muchas otras aplicaciones, tales como

(a) las firmas digitales;

(b) el control de acceso a datos;

(c) los protocolos para tirar un volado electrónicamente;

(d) el intercambio de claves para un criptosistema tradicional (de clave privada).

Durante los primeros años de la criptografía de clave pública, el único sistema que prometió ser competidor del de RSA fue el de Merkle–Hellman.

El sistema de Merkle–Hellman fue basado en el "problema de mochila," es decir, el problema, dado un número N y un conjunto de números enteros, de encontrar un subconjunto cuya suma sea igual a N.

Pero dentro de 3 ó 4 años, Brickell, Odlyzko y otros lograron romper los criptosistemas de mochila.

Tal vez pareciera que el RSA no iba a tener competidor.

En diciembre de 1984, Hendrik Lenstra distribuyó un esbozo de un algoritmo nuevo para la factorización de los números enteros.

El aspecto muy novedoso del método de Lenstra fue el uso de las curvas elípticas. Esto fue la primera vez que las curvas elípticas fueron usadas en la criptografía.

En enero de 1985 fui a Moscú para medio año como participante en un intercambio científico organizado por las Academias de Ciencia de la Unión Soviética y los Estados Unidos.

En este entonces yo estaba pensando mucho sobre las aplicaciones de la teoría de números en la criptografía. (De hecho, en febrero de 1985 presenté un discurso sobre este tema en la reunión de la Sociedad Matemática de Moscú.)

Me gustó mucho el método de factorización de Lenstra, y me ocurrió considerar otro uso de las curvas elípticas: para reemplacer el grupo multiplicativo de un cuerpo finito en los sistemas del tipo Diffie–Hellman.

Escribí una carta a Andrew Odlyzko sobre mi propuesta de un criptosistema basado en el problema del logaritmo discreto en una curva elíptica.

Tuve que esperar casi un mes para recibir su respuesta muy alentadora. Dijo que le pareció una idea interesante, y que otro matemático, el Dr. Victor Miller de la compañía IBM, le había escrito con la misma propuesta independientemente y simultáneamente.

En 1985 nadie habría creído que en el futuro cercano la criptografía de curvas elípticas (CCE) iba a jugar un papel importante en la criptografía práctica — e iba a llegar a ser el competidor principal de los sistemas de RSA.

Ni Victor ni yo patentamos la CCE.

En mi caso, esto no tenía significado, porque no soy partidario del sistema de patentes, y siempre he tenido un punto de vista anti-capitalista.

Pero Victor trabajaba para una compañía muy capitalista, la cual siempre ha insistido en que sus empleados intentaran conseguir el máximo número posible de patentes.

Por esta razón es un poco sorprendiente que Victor tampoco patentó la CCE.

VENTAJAS DE LAS CURVAS ELÍPTICAS

• No se conoce ningún algoritmo de tiempo subexponencial para romper la clave (cuando se usa una curva escogida cuidadosamente).

• Como resultado podemos usar claves más pequeñas que las de RSA.

• Existe un gran número de posibilidades en la selección de la curva.

Comparación: RSA — CCE:

El record para la factorización:
N **de 174 dígitos decimales.**

El record para romper la CCE:
N **de 33 dígitos decimales.**

A pesar de la larga historia de investigaciones de las curvas elípticas, muchos criptógrafos tienen una actitud sospechosa hacia ellas y prefieren un sistema basado en las matemáticas más sencillas. En los años 1990 la compañía RSA intentó fomentar esta actitud de temor de las curvas elípticas.

"Sin embargo, la seguridad de los criptosistemas basados en las curvas elípticas no es bien entendida, debido en gran parte a la naturaleza abstracta de las curvas elípticas. Son pocos los criptógrafos quienes entienden las curvas elípticas, por lo cual ... el intentar evaluar la seguridad de un criptosistema de curvas elípticas es un poco parecido al intentar evaluar un fragmento recién descubierto de la poesia caldeana."

> **— Ron Rivest en el sitio de web de RSA en 1996-1998**

LAS CURVAS ELÍPTICAS

Una curva elíptica E definida sobre un cuerpo F es una ecuación

$$Y^2 = X^3 + aX + b, \qquad a, b \in F.$$

(Tiene que ser suave, es decir, el polinomio cúbico no puede tener ceros múltiples; y la ecuación es un poco diferente en el caso de característica 2 ó 3.)

Los puntos $x, y \in F$ que satisfacen esta ecuación, conjuntamente con el "punto al infinito" O, forman un grupo abeliano cuya identidad es O.

Si $F = \mathbb{F}_q$ es el cuerpo de q elementos, entonces E es un grupo finito. Según el Teorema de Hasse, el número de puntos en E satisface la desigualdad

$$|\#E - (q+1)| \leq 2\sqrt{q}.$$

Es decir, $\#E$ es de la misma magnitud que q.

Por ejemplo, para la curva $Y^2 = X^3 - X$ definida sobre $\mathbb{F}_p$ tenemos dos casos:

(1) Caso "supersingular":

$$p \equiv 3 \pmod 4.$$

Es fácil demostrar que

$$\#E(\mathbb{F}_p) = p + 1.$$

(2) Caso "no-supersingular":

$$p \equiv 1 \pmod 4.$$

El mismo Gauss investigó este caso y encontró una fórmula para $\#E(\mathbb{F}_p)$.

En primer lugar se escribe $p = A^2 + B^2$, donde A es impar y $A + B \equiv 1 \pmod 4$. Entonces

$$\#E(\mathbb{F}_p) = p + 1 - 2A.$$

LOS CRIPTOSISTEMAS ELÍPTICOS

En la criptografía trabajamos en el grupo G generado por un punto fijo $P \in E$, y es deseable que este subgrupo tenga orden primo N, donde N es casi de la misma magnitud que q.

En otras palabras, tenemos que escoger un cuerpo $\mathbb{F}_q$ y una curva E de tal modo que $\#E(\mathbb{F}_q)$ tenga un factor primo N muy grande.

También supongamos que hemos codificado las unidades de mensaje como puntos de E, y queremos enviar un mensaje $M \in E$.

Información pública:

$\mathbb{F}_q$, E, punto fijo $P \in E$.

Clave secreta de Alicia:

un número entero x
(escogido aleatoriamente).

Clave pública de Alicia:

el punto xP.

Beatriz quiere enviarle a Alicia el mensaje $M \in E$.

Ella escoge aleatoriamente un número entero ℓ, y calcula los dos puntos ℓP y $\ell(xP)$. Ella le envía a Alicia los dos puntos

$$(\ell P,\ \ell xP + M).$$

Es decir, el mensaje está "disfrazado" por el punto ℓxP; pero este punto también es igual a $x(\ell P)$, y Alicia puede "quitar la máscara," multiplicando el primer punto por su clave secreta y sustrayendo el resultado del segundo punto:

$$\ell xP + M - x(\ell P) = M.$$

¿Qué tendría que poder hacer una persona no autorizada para encontrar el mensaje M? Sería suficiente resolver el problema del logaritmo discreto en el grupo E (el "ECDLP").

Este es el problema, dado $Q \in G \subset E$, de encontrar un número entero x tal que $Q = xP$.

El "ECDLP" en español es el PLDCE — el problema del logaritmo discreto en una curva elíptica.

En general, la dificultad del PLDCE depende de la magnitud del factor primo más grande del orden del grupo $G \subset E$.

Por esta razón es mejor usar curvas E cuyos grupos tienen orden primo o "casi primo."

En 1988 en *Pacific Math J.* (vol. 131, pág. 157-165) hice varias conjeturas sobre la probabilidad de que la reducción módulo p de una curva elíptica E definida sobre el cuerpo de números racionales tenga orden primo (aquí la curva E está fijada — por ejemplo, $Y^2 = X^3 - X$ — y el primo p varía).

Existe evidencia tanto computacional como heurística de que esta probabilidad es aproximadamente igual a $C/\log p$, donde la constante C depende de la curva (más precisamente, de las imágenes de las representaciones módulo ℓ del grupo de Galois de los puntos de orden ℓ).

Pero los resultados que pueden ser demostrados son mucho más débiles que estas conjeturas.

**A mi conocimiento el teorema más fuerte de este tipo (de S. Ali Miri y V. Kumar Murty) dice que, con probabilidad $\geq 1/\log p$,
el orden de $E(\mathbb{F}_p)$ tenga ≤ 16 factores primos.**

El resultado de Miri–Murty es hermoso, pero es inútil en la práctica.

El trabajo de Miri–Murty es un ejemplo de la influencia de la criptografía sobre las matemáticas puras.

De vez en cuando la criptografía provee una fuente de nuevos problemas.

Bajo la influencia de la CCE, los matemáticos teóricos han investigado aspectos de las curvas elípticas que anteriormente no habían recibido su atención.

(Nota: Un trabajo más reciente con un resultado más fuerte que el de Miri y Murty fue publicado por A. C. Cojocaru en *Acta Arithmetica*, 119.3 (2005).)

Es de notar que en 2000 S. Galbraith y J. McKee (J. London Math. Soc., vol. 62, pág. 671-684) investigaron la misma cuestión, pero con el primo p fijado y la curva variable.

Es decir, cuando p está fijado y se varían los coeficientes de la ecuación de E, se estudió la probabilidad de que el orden de $E(\mathbb{F}_p)$ sea primo.

Otro problema que asumió una gran importancia en la CCE y atrajo la atención de muchos matemáticos:

> **Determinar el orden $N = \#E(\mathbb{F}_q)$**
> **para cualquier curva elíptica E.**

El algoritmo de Schoof en 1985 fue el primer algoritmo de tiempo polinomial (pero no fue muy eficiente).

Schoof determinó el valor de N módulo ℓ para varios primos pequeños ℓ a través de los polinomios de ℓ-división (cuyas raíces son las coordenadas-x de los puntos de orden ℓ).

Atkins y Elkies modificaron el método de Schoof, usando los polinomios modulares que son más finos que los de división.

En el caso de curvas definidas sobre cuerpos finitos de pequeña característica p, en 1999 Satoh encontró un algoritmo p-adico muy eficaz.

Algunas versiones del algoritmo p-adico pueden determinar $\#E(\mathbb{F}_{2^{163}})$ en unas pocas segundas por computadora.

Resulta que en la CCE es muy práctico usar curvas sobre $\mathbb{F}_{2^{163}}$ con coeficientes aleatorios.

ATAQUES CONTRA CRIPTOSISTEMAS

Contra el de RSA:

la criba de cuerpos numéricos

Tiempo$\approx 2^{n^{1/3+\epsilon}}$

Contra las curvas elípticas:

el método de Pollard-ρ

Tiempo$\approx 2^{(1/2+\epsilon)n}$

(En ambos casos $n = \log_2 N$**.)**

El número record

para la factorización: $N > 2^{575}$

para la CCE: $N \approx 2^{108}$

La ventaja principal de la criptografía de curvas elípticas:

Todos los ataques generales (es decir, además de casos especiales) requieren tiempo exponencial, por lo cual se puede conseguir un nivel adecuado de seguridad con claves de tamaño relativamente pequeño.

Firmas digitales usando curvas elípticas:

(1) El ECDSA/AFDCE = algoritmo para firmas digitales con curvas elípticas

> **está basado en el DSA (introducido en 1991 por el instituto nacional de estandares del gobierno de EEUU)**

la versión con curvas elípticas es más eficaz y ha reemplazado el DSA

(2) "Firmas digitales cortas usando el mapa bilineal de Weil,"

> **("Short signatures from the Weil pairing," Boneh, Lynn & Shacham, *J. Cryptology*, vol. 17 (2004), pág. 297-319), también disponible en el sitio de web de Dan Boneh: http://www.cs.stanford.edu/~dabo**

Este sistema de firmas digitales depende de las propiedades específicas de las curvas elípticas.

En contraste al ECDSA/AFDCE, el sistema de Boneh-Lynn-Shacham no está parecido a ningún sistema que use grupos más sencillos.

A continuación presento una versión sencilla de la construcción de Boneh–Lynn–Shacham.

En cualquier sistema de firmas digitales se usa un "mapa de picadillo" (*hash* en inglés)

$$\mathcal{M} \mapsto H$$

H es más o menos una huella dactilar del mensaje $\mathcal{M}$.

El mapa de picadillo no es secreto.

Otra vez vamos a usar la curva con ecuación

$$E: \quad Y^2 = X^3 - X,$$

definida sobre $\mathbb{F}_p$, $p \equiv 3 \pmod 4$. Este es el caso supersingular, donde

$$\#E = p + 1.$$

Supongamos que el primo

$$N \mid p + 1,$$

$$N \approx p,$$

y $P \in E$ es un punto de orden N.

$G \subset E$ es el grupo generado por P.

Vamos a trabajar también en la extensión cuadrática del cuerpo $\mathbb{F}_p$:

$$\mathbb{F}_{p^2} = \mathbb{F}_p[X]/(X^2+1) = \mathbb{F}_p(i).$$

Sobre este cuerpo la curva tiene $(p+1)^2$ puntos, y tiene N^2 puntos de orden N.

Trabajando con los puntos de E con coordenadas en $\mathbb{F}_{p^2}$, tenemos un mapa

$$Q = (u, v) \mapsto \widetilde{Q} = (-u, iv)$$

bajo el cual

$$G = \{\text{múlt. de } P\} \longrightarrow \widetilde{G} = \{\text{múlt. de } \widetilde{P}\}.$$

(Es de notar que si (u, v) satisface la ecuación $Y^2 = X^3 - X$, entonces $(-u, iv)$ la satisface también.)

El "emparejamiento [mapa bilineal] de Weil" está definido para pares de puntos en el conjunto de los N^2 $\mathbb{F}_{p^2}$-puntos de orden N en la curva. Sus valores son potencias de la raíz de unidad

$$\zeta \in F_{p^2}, \quad \zeta^N = 1.$$

El emparejamiento $\langle\ ,\ \rangle$ tiene las propiedades

$$\langle P, \widetilde{P} \rangle = \zeta$$

y

$$\langle iP, j\widetilde{P} \rangle = \zeta^{ij}$$

(la última resulta de la propiedad bilineal).

Supongamos que Alicia quiere firmar un mensaje que tiene valor de "picadillo" H, el cual podemos suponer es un punto de la curva, $H \in G$.

De igual manera que en otros criptosistemas de curvas elípticas, la clave secreta de Alicia es un número x generado aleatoriamente, y su clave pública es el punto xP.

La firma de Alicia es simplemente el punto

$$S = xH.$$

Para verificar la firma, la recipiente del mensaje, Beatriz, calcula $\widetilde{Q}$ (es decir, el imagen de Q bajo el mapa $(u, v) \mapsto (-u, iv)$) y los dos valores del emparejamiento

$$\langle H, \widetilde{Q} \rangle$$

y

$$\langle S, \widetilde{P} \rangle;$$

Beatriz acepta la firma si estos son iguales.

Si Alicia ha creado la firma correctamente, entonces ambos valores son iguales a

$$\langle H, \widetilde{P} \rangle^x.$$

Beatriz acepta la firma porque se confía en que solamente Alicia habría podido hallar el punto que tiene el logaritmo discreto con base H igual al logaritmo discreto de Q con base P.

$$S = xH \qquad \text{y} \qquad Q = xP.$$

Para usar este sistema de firmas es necesario poder calcular en el cuerpo $\mathbb{F}_{p^2}$.

El único modo que se conoce para falsificar una firma es solucionar el PLDCE, es decir, encontrar la clave secreta x de Alicia.

Para la máxima seguridad se recomienda

$$p > 2^{500}.$$

(A pesar de esta recomendación, la firma de Boneh-Lynn-Shacham es relativamente corta y eficaz.)

En otros criptosistemas de curvas elípticas es necesario tener solamente $p \approx 2^{163}$.

¿Porqué p debe ser mayor en el sistema de Boneh-Lynn-Shacham?

La razón es que el emparejamiento de Weil puede ser usado para traducir el PLDCE al problema del logaritmo discreto en el grupo más sencillo $\mathbb{F}_{p^2}^{\times}$.

Es de notar que si $Q = xP$, entonces

$$\langle Q, \widetilde{P} \rangle = \langle P, \widetilde{P} \rangle^x = \zeta^x.$$

En otras palabras, el logaritmo discreto de Q con base P en el grupo E es igual al logaritmo discreto de $\langle Q, \widetilde{P} \rangle$ con base ζ en el grupo $\mathbb{F}_{p^2}^{\times}$.

El PLD en este último grupo tiene complejidad menor que el del PLDCE en el caso general.

Más bien, este PLD es un problema solamente un poco más difícil que la factorización de un entero N de la misma magnitude que p^2, es decir, de 1000 bits si $p > 2^{500}$.

En otros criptosistemas de curvas elípticas se usan solamente las curvas no-supersingulares.

En el caso no-supersingular de la curva $Y^2 = X^3 - X$**, donde** $p \equiv 1 \pmod 4$**, tenemos**

$$\#E(\mathbb{F}_p) = p + 1 - 2A,$$

donde $p = A^2 + B^2$**.**

En este caso también existe el emparejamiento de Weil, pero tiene valores en el cuerpo $\mathbb{F}_{p^k}$ **donde**

$$(p + 1 - 2A) | (p^k - 1).$$

En el caso supersingular tuvimos

$$(p + 1) | (p^2 - 1).$$

Pero en el caso no-supersingular casi nunca tenemos $(p + 1 - 2A) | (p^k - 1)$ **para** $k \ll p$**.**

Si $k \approx p$, no es factible trabajar en el cuerpo $\mathbb{F}_{p^k}$. No tiene sentido traducir el PLDCE al PLD en el grupo $\mathbb{F}_{p^k}^{\times}$.

Resulta que el nivel de dificultad del PLDCE es mucho mayor para (casi todas) las curvas no-supersingulares que para las supersingulares.

Por esta razón la mayoría de los criptosistemas de curvas elípticas usan curvas no-supersingulares.

Es decir, el sistema de firmas de Boneh-Lynn-Shacham se diferencia de los otros sistemas de curvas elípticas porque

> **(1) usa las curvas supersingulares (o curvas no-supersingulares con valores muy pequeños de k), y**
>
> **(2) está basado en el mapa de Weil, el cual no existe para grupos más sencillos**

El uso del emparejamiento bilineal para construir protocolos criptográficos es un tema de muchos estudios.

El investigador pionero fue Dan Boneh (http://www.cs.stanford.edu/~dabo).

Otras fuentes de información:

(1) S. Galbraith, "Pairings," capítulo IX de *Advances in Elliptic Curve Cryptography*, Cambridge Univ. Press, 2005;

(2) Koblitz y Menezes, "Pairing-based cryptography at high security levels," http://eprint.iacr.org/2005/076.pdf

Una de las aplicaciones importantes del emparejamiento es para solucionar el problema del "enciframiento basado en identidad" (*identity-based encryption* en inglés).

En un sistema de este tipo la clave pública es simplement el nombre (u otra identificación) del usuario.

Véase, por ejemplo, el artículo de Boneh y Franklin en *SIAM J. Computing*, vol. 32 (2003), pág. 586-615 (también disponible en el sitio de web de Dan Boneh).

EL ATAQUE DE JOSEPH SILVERMAN

(en una forma simplificada)

E es una curva elíptica definida sobre $\mathbb{F}_p$, y P, Q son dos de sus puntos.

Queremos hallar un entero x tal que $Q = xP$.

Seleccionemos dos puntos $\widetilde{P}$, $\widetilde{Q}$ con coordenadas en $\mathbb{Z}$ (=los números enteros) cuyos residuos módulo p son nuestros puntos P, Q.

También seleccionemos una curva elíptica $E(\mathbb{Q})$ con coeficientes racionales que contiene $\widetilde{P}$ y $\widetilde{Q}$ y que módulo p se reduce a la curva $E(\mathbb{F}_p)$.

Supongamos que $\widetilde{P}$ y $\widetilde{Q}$ son dependientes en $E(\mathbb{Q})$, es decir, que

$$n_1\widetilde{P} + n_2\widetilde{Q} = O.$$

En este caso, trabajando módulo p tenemos

$$O = n_1P + n_2Q = n_1P + n_2xP = (n_1 + n_2x)P,$$

por lo cual

$$n_1 + n_2x \equiv 0 \pmod{N},$$

donde N es el orden del punto P, y fácilmente encontraremos x.

Sin embargo, en general la probabilidad de que $\widetilde{P}$ y $\widetilde{Q}$ sean dependientes es muy, muy pequeña. La idea de Silverman fue el aumentar esta probabilidad, imponiendo condiciones del siguiente tipo:

$$\#E(\mathbb{F}_l) \approx l + 1 - 2\sqrt{l} \qquad (**)$$

para todos los primos l entre 5 y L (donde $L \approx 100$). Aquí $E(\mathbb{F}_l)$ denota la reducción de $E(\mathbb{Q})$ módulo el primo l.

Según el Teorema de Hasse, siempre tenemos

$$l + 1 - 2\sqrt{l} \leq \#E(\mathbb{F}_l) \leq l + 1 + 2\sqrt{l},$$

por lo cual la condición (**) dice que hay relativamente pocos puntos módulo l.

Si r denota el número máximo de puntos independientes en la curva $E(\mathbb{Q})$, entonces Silverman quiere aumentar la probabilidad de que r sea pequeño.

Silverman justifica la imposición de las condiciones (**), basándose en

(1) la Conjetura de Birch y Swinnerton-Dyer, que dice, entre otras cosas, que r es igual al orden del cero en $s = 1$ de la L-función de $E(\mathbb{Q})$ (esta "L-función de Hasse–Weil" está formada usando la secuencia de números $\#E(\mathbb{F}_l)$ para los primos l);

(2) una fórmula analítica de J.-P. Mestre para el valor de r. La demostración de esta fórmula requiere la Conjetura de Taniyama, que dice que cualquier curva $E(\mathbb{Q})$ es "modular," y por lo tanto puede ser estudiada a través de la teoría de formas modulares. (Ahora la Conjetura de Taniyama es muy famosa como resultado de la demostración del Último Teorema de Fermat por Andrew Wiles; pero, curiosamente, el trabajo de Wiles no parece tener aplicación práctica alguna.)

En septiembre de 1998, cuando nos informó Silverman sobre su algoritmo, reaccionamos con un poco de temor, ya que a primera vista las ideas muy sútiles que se aplicaron en el algoritmo parecieron dificultar el análisis de éste.

Pero después de varias semanas de trabajo en la Universidad de Waterloo, logramos demostrar que el ataque de Silverman no es práctico. Nuestro análisis de su algoritmo está basado en

- **las propiedades de la así-llamada "altura logarítmica canónica" de un punto (la cual es más o menos proporcional al número de símbolos requeridos para escribir las coordenadas del punto);**

- **la geometría de números (y de puntos en un reticulado);**

- **la Conjetura de Lang, que da una cota para la menor posible altura de un punto.**

RESUMEN DE LAS IDEAS DE LA GEOMETRÍA ALGEBRÁICA ARITMÉTICA USADAS EN EL ALGORITMO DE SILVERMAN Y/O NUESTRO ANÁLISIS DE ÉSTE

• la L-función de Hasse–Weil, la cual proviene de la secuencia $\#E(\mathbb{F}_l)$ para primos l;

• la Conjetura de Birch y Swinnerton-Dyer;

• la fórmula analítica de Mestre para el valor de r;

• la Conjetura de Taniyama (ahora un teorema de Andrew Wiles y otros);

• la altura logarítmica canónica de Néron–Tate;

• la Conjetura de Lang.

Ningunos de estos matemáticos muy destacados del siglo XX — Hasse, Weil, Birch, Swinnerton-Dyer, Mestre, Taniyama, Néron, Tate, o Lang — se habrían imaginado que sus trabajos iban a tener aplicaciones en el mundo práctico.

El nivel de sofisticación de las ideas matemáticas usadas en la criptografía ha crecido mucho durante los últimos 30 años.

Muchos temas de las matemáticas muy teóricas (en la teoría de cuerpos numéricos y la geometría algebráica y aritmética) — que anteriormente fueron considerados como muy lejanos de cualesquiera aplicaciones — ahora juegan un papel clave en el desarrollo y el análisis de los criptosistemas más importantes.

Barcelona, febrero de 2006

¿ES POSIBLE "DEMOSTRAR" LA SEGURIDAD DE UN CRIPTOSISTEMA?

Esta charla está basada en trabajo conjunto con Alfred Menezes; véase
http://eprint.iacr.org/2004/152.pdf

También se recomienda leer:
http://eprint.iacr.org/2005/205.pdf
("Another look at HMQV" por Menezes)

El santo grial de la criptografía teórica:

Una demostración matemática de la seguridad de un protocolo criptográfico.

¿Quien está perseguiendo este grial?

> **¿Los matemáticos? No.**
>
> **Los que provienen de la ciencia de computación.**

Los matemáticos tenemos un punto de vista más escéptico y pragmático.

Supongamos que alguien está usando la criptografía de clave pública para

- **proteger los números de tarjeta de crédito durante el comercio electrónico;**

- **mantener la confidencialidad de los archivos médicos;**

- **crear firmas digitales.**

¿Como puede ella confiar en la seguridad del sistema que está usando?

¿Es posible "demostrar" la seguridad del sistema?

En 1994 Bellare y Rogaway "demostraron la seguridad" de cierto sistema, basado en la RSA, que llamaron el "Relleno Optimo para el Enciframiento Asimétrico" — en inglés *Optimal Asymmetric Encryption Padding* **(OAEP).**

Las compañías MasterCard y Visa incluyeron la OAEP en sus estandares para el pago electrónico.

En 2001, Victor Shoup examinó cuidadosamente la "demostración de seguridad" de Bellare-Rogaway, y encontró una falla.

Este tipo de cosa tiende a causar un problema de credibilidad.

¿Qué sentido podrían tener las palabras "demostrar la seguridad"?

Vamos a partir de la palabra "seguridad" (en el enciframiento).

Nuestra primera respuesta:

Cualquier sistema de clave pública está basado en una función o construcción de dirección única.

Ejemplo:

En el sistema RSA, esta función es la multiplicación de dos primos grandes p y q para obtener el "módulo" N:

$$N = pq.$$

El proceso inverso es la factorización del número entero N, la cual supuestamente no es factible.

Por lo cual nuestra primera definición provisional de "seguridad" es:

estar seguro de que la función de dirección única no puede ser invertida.

Sin embargo, desde el comienzo del estudio de la criptografía de clave pública (en la década de los 1970) entendieron que en principio es posible que la función de enciframiento de RSA

$$y = x^e \pmod{N}$$

(donde e es una exponente fija, x es el texto sencillo, y y es el texto encifrado) podría ser invertida sin poder factorizar el módulo N.

(Nadie tiene idea alguna como hacerlo.)

Entonces, una segunda respuesta a la pregunta sobre el sentido de la palabra "seguridad" es:

estar seguro de que no es factible invertir la función de enciframiento.

La mayoría de los libros de criptografía escritos por matemáticos no van más allá que estas dos respuestas a la pregunta sobre "seguridad."

Por ejemplo, mis dos libros sobre la criptografía tienen este defecto.

Este punto de vista muy limitado no puede anticipar la mayoría de los ataques contra los criptosistemas con los cuales nos enfrentamos en la práctica.

Ejemplo (Bleichenbacher 1998):

Supongamos que Alicia está recibiendo mensajes a través de un sistema del tipo RSA.

Antes del enciframiento los mensajes deben tener cierta forma. Si un mensaje descifrado no tiene esta forma, entonces el ordinador de Alicia transmite la notificación de un error.

Parece bastante inocuo.

Sin embargo, Bleichenbacher puede (a veces) usar estas notificaciones de error para descifrar el texto encifrado SIN haber factorizado N.

Esbozo del ataque de Bleichenbacher:

y es el texto encifrado.

El adversario envia a Alicia ciertos textos "perturbados" y' (escogidos cuidadosamente a partir de y) y estudia cuales de los y' están rechazados por no tener la forma correcta.

Con toda esta información puede descifrar y.

El ataque de Bleichenbacher es ejemplo de un ataque de "texto encifrado escogido" (en inglés: *chosen-ciphertext attack*).

Un pleno ataque de texto encifrado escogido quiere decir que el adversario puede obtener de Alicia el desciframiento de cualquier mensaje que escoge excepto el texto encifrado y que es blanco del ataque.

El ataque de Bleichenbacher es un ataque parcial de este tipo, en el sentido de que obtiene de Alicia alguna información sobre el texto descifrado (es decir, si tiene la forma correcta o no).

Durante la década de los 1980 — mucho más temprano que el ataque de Bleichenbacher — Goldwasser, Micali, Rivest y otros especialistas entendieron que un concepto fuerte de "seguridad" debe incluir la capacidad de resistir a un ataque de texto encifrado escogido.

Este es un concepto de seguridad mucho más fuerte, porque se supone que el adversario es poderoso en el sentido de que puede obtener de Alicia mucha información.

Ahora, ¿qué quiere decir la palabra"demostración" (de seguridad)?

La respuesta ampliamente aceptada:

Es un argumento de "reducción."

La idea de "reducir un problem al otro" es común tanto en las matemáticas como en la ciencia de computación.

Ejemplo en las matemáticas:

Teorema de Ribet (1986). El Ultimo Teorema de Fermat se reduce a la Conjetura de Taniyama.

Es decir, la dificultad de la Conjetura de Taniyama es igual o mayor que la del Ultimo Teorema de Fermat.

Al pensar un poco sobre este ejemplo famoso, podemos notar una de las sutilezas de las demostraciones de reducción:

a veces ellas tienen dos posibles interpretaciones mutuamente contradictorias.

En este caso:

Interpretación A: Tal vez el Ultimo Teorema ahora es accesible a través de la teoría de formas modulares, por lo cual vale la pena atacar la Conjetura de Taniyama.

(Esta fue la interpretación de Wiles.)

Interpretación B: Si la Conjetura de Taniyama es aún más difícil que el Ultimo Teorema, entonces no vale la pena intentar de trabajar en esta area.

(Esta fue la interpretación de casi todos los demás matemáticos.)

Ejemplo en la ciencia de computación:

La teoría de NP-completitud

Para demostrar que un problema $\mathcal{P}$ es NP-completo, es suficiente mostrar que el problema 3SAT se reduce a $\mathcal{P}$ — en otras palabras, que cualquier algoritmo para $\mathcal{P}$ puede ser usado también (con cierto esfuerzo mínimo adicional) para solucionar 3SAT.

En este caso la dificultad de $\mathcal{P}$ es igual o mayor que la de 3SAT — en otras palabras, es un problema NP-completo.

En la criptografía en vez del problema 3SAT usamos un problema matemático en cuya dificultad todos confiamos — por ejemplo, la factorización de números enteros muy grandes; y $\mathcal{P}$ es el problema de romper nuestro criptosistema en un sentido dado.

Los resultados del tipo "demostración de seguridad" tienen la siguiente forma condicional:

Si el problema X es difícil, entonces el criptosystema Y es seguro contra ataques del tipo Z.

Es de notar que

• la dificultad del problema matemático básico es la suposición y no la conclusión de la demostración; y

• no se dice nada sobre las consecuencias de un ataque del tipo Z', donde $Z' \neq Z$.

El primer ejemplo de una demostración de reducción para la seguridad de un criptosistema:

El sistema de enciframiento de Rabin.

Recordamos que la función de enciframiento de RSA es

$$y = x^e \pmod{N},$$

donde e es una exponente fija que es relativamente prima con $\varphi(N) = (p-1)(q-1)$ (aquí el módulo N es el producto de dos primos muy grandes p y q).

Alicia, quien recibe el mensaje, conoce los factores de N y por lo tanto puede hallar una exponente d de desciframiento tal que

$$x = y^d \pmod{N}.$$

Sin embargo, es teóricamente posible que alguien encontre el x sin haber hallado los factores de N.

El método de Rabin (quien lo inventó prontamente después de RSA) es una versión de RSA donde $e = 2$.

Pero Rabin necesita de algunas modificaciones, ya que el mapa $x \mapsto x^2 \mod N$ es 4-a-1.

En el desciframiento Alicia halla una de las raíces cuadradas de y módulo N y la ajusta si no es la raíz deseada.

Alicia puede ajustarla multiplicando por $-1 \pmod N$ o por $\pm\varepsilon \pmod N$, donde ε es la solución de las relaciones

$$\varepsilon \equiv 1 \pmod p,$$

$$\varepsilon \equiv -1 \pmod q.$$

Para Alicia, quien conoce los factores de N, es fácil calcular todos los x tales que $y \equiv x^2 \pmod N$.

En contraste con el enciframiento de RSA, el de Rabin tiene la propiedad inversa:

Solamente una persona que conozca los factores de N habría podido descifrar textos de Rabin.

En contraste con el enciframiento de RSA, el de Rabin tiene la propiedad de que se puede *demostrar* que romperlo es equivalente a la factorización del módulo en el sentido a continuación:

TEOREMA. La factorización de N se reduce al problema de encontrar el texto descifrado a partir del texto encifrado en el sistema de Rabin.

CONSECUENCIA. Si la factorización es difícil, entonces el criptosistema de Rabin es seguro en cuanto a la inversión de la función de enciframiento.

No se conoce ninguna reducción de este tipo para el RSA.

De hecho, en 1998 Boneh y Venkatesan demostraron que hay poca posibilidad que exista una reducción del problema de factorización al problema de inversión de la función de enciframiento de RSA.

Específicamente, ellos demostraron que para e pequeño, si existe una reducción "algebráica" del problema de factorización al problema de RSA, entonces el problema mismo de factorización debe ser fácil.

Por lo tanto podemos decir que el enciframiento de Rabin tiene una propiedad básica de "seguridad demostrable" de que el sistema de RSA carece.

Entonces, ¿han demostrado la seguridad del enciframiento de Rabin?

Pués no.

El mismo argumento usado para demostrar el teorema sobre la equivalencia de la inversión de Rabin y la factorización también muestra que el enciframiento de Rabin es completamente vulnerable al ataque de texto encifrado escogido.

Si el adversario puede lograr que Alicia descifre $y = x^2 \pmod{N}$ para k diferentes valores de x, escogidos aleatoriamente por el adversario, entonces con la probabilidad $1 - 2^{-k}$ el podrá factorizar N.

En otras palabras, todo depende de la definición de "seguridad."

El mismo argumento puede "demostrar" o la seguridad del sistema de Rabin... o su inseguridad.

NOTA: En 2001, Boneh mostró una modificación del sistema de Rabin — con cierta "relleno" y una "ronda de Feistel" — que parece ser eficiente y aparentemente seguro.

Ahora pasemos del tema de enciframiento al de firmas digitales.

Ingrediente crucial: una función de picadillo $H(m)$ (en inglés: *hash function*).

En general, una función de picadillo es una función desde secuencias largas de bits m (en la criptografía, m es el mensaje) a secuencias mucho más cortas $H(m)$ que sirven de "huellas dactilares" de los mensajes.

H es una función pública que cualquier persona fácilmente puede calcular.

La función de picadillo debe tener ciertas propiedades. La suposición más comun es que "resiste choques."

La propiedad de resistencia a choques quiere decir que no es posible en tiempo razonable encontrar un par de mensajes m, m' con el mismo picadillo $H(m') = H(m)$.

En las demostraciones de reducción muchas veces es necesario suponer una propiedad más fuerte — que H tiene el mismo comportamiento que una función aleatoria.

En otras palabras, en vez de suponer que tenemos un algoritmo determinístico público para calcular H, se supone que en cualquier ocasión cuando alguien quiere saber un valor $H(m)$, un "oráculo" le dará un valor aleatorio. La única condición es que, si alguien pregunta otra vez sobre el mismo mensaje m, entonces el oráculo responderá con el mismo valor $H(m)$.

Si usamos esta suposición, decimos que estamos trabajando

> **"en el modelo del oráculo aleatorio."**

La firma digital básica de RSA:

Supongamos que los valores de la función de picadillo H (los cuales en la práctica tienen un comportamiento aleatorio) están distribuídos en todo el intervalo $0 < H(m) < N$, donde N es el módulo de Alicia.

Alicia quiere firmar un mensaje m que envió a Beatriz.

Ella calcula $H(m)$ y su potencia mod N con su exponente secreta d; es decir, su firma es

$$s = H(m)^d \pmod{N}.$$

Cuando Beatriz recibe el mensaje m y la firma s, ella también calcula $H(m)$, y usa la exponente publica e para verificar que

$$H(m) = s^e \pmod{N}.$$

Si $H(m)$ es igual a s^e (mod N), entonces Beatriz puede estar seguro de que

• Alicia fue la persona que le envió el mensaje (porque supuestamente solamente ella conoce la exponente d que es inversa a la exponente e); y

• el mensaje no ha sido alterado (porque nadie habría podido encontrar otro mensaje m' con el mismo $H(m') = H(m)$).

En las investigaciones de las firmas digitales el concepto que corresponde a

> **"seguro contra ataques de texto encifrado escogido"**

es

> **"seguro contra ataques de mensajes escogidos por un falsificador existencial."**

Quiere decir que el adversario puede obtener de Alicia firmas válidas s_i para cualesquiera mensajes m_i que escoge.

Lo consideraremos un falsificador exitoso si produce una firma válida para un mensaje m que es diferente de todos los m_i.

TEOREMA. Si el problema de inversión de la función $x \mapsto x^e \pmod N$ es difícil (es decir, el imagen inversa no puede ser calculada en tiempo razonable), entonces esta firma de RSA es segura (en el modelo del oráculo aleatorio) contra ataques de mensajes escogidos por un falsificador existencial.

DEMOSTRACION. Queremos dar un argumento de reducción — una reducción del problema de la inversión del mapa de RSA al problema de producir una firma falsificada.

En otras palabras, supongamos que tenemos un programa de ordinador cuya entrada es la clave pública (N, e) de Alicia. Se le permite hacer nada más que q preguntas sobre los valores $H(m_i)$ y más adelante (si quiere) sobre las firmas correspondientes s_i para cualesquiera mensajes m_i.

Este programa de ordinador es un falsificador existencial de mensajes escogidos (en ingles: *chosen-message existential forger*) si producirá finalmente una firma válida para uno de los mensajes para que recibió solamente el valor de picadillo $H(m)$ y no la firma.

Tenemos que mostrar un método para usar este programa de ordinador para solucionar el problema: Dado y, halle x tal que $y \equiv x^e \pmod{N}$.

Versión informal (pero completa)

Visto que H es una función aleatoria, los mensajes m_i no tienen relevancia alguna.

Lo que el falsificador tiene disponible:
una secuencia aleatoria h_i
conjuntamente con los x_i correspondientes
(las $e^{\mathbf{mas}}$ raíces mod N)

Para tener éxito, el falsificador debe producir la $e^{\mathbf{ma}}$ raíz mod N de cierto valor aleatorio h, donde $h \notin \{h_i\}$.

El teorema consta que esta tarea no es más fácil que la de producir la $e^{\mathbf{ma}}$ raíz mod N de un valor dado aleatorio sin tener la secuencia de pares (h_i, x_i).

La demostración en esencia se reduce a la siguiente observación trivial:

Ambas secuencias h_i y x_i son distribuídas aleatoriamente en el intervalo $\{0, 1, \ldots, N-1\}$, por lo cual uno puede obtener una secuencia de pares (h_i, x_i) equivalente a partir de los x_i usando la exponente pública e, es decir, $h_i = x_i^e \pmod N$.

En otras palabras, no se puede diferenciar una secuencia aleatoria

$$(h_i, h_i^d \bmod N)$$

de una secuencia aleatoria

$$(x_i^e \bmod N, x_i);$$

es igual mirar a la secuencia de pares desde la izquierda o desde la derecha.

Esta "demostración" en realidad no es nada más que la tautología a continuación:

El problema de solucionar una ecuación es equivalente al problema de solucionarla con algunos datos adicionales (h_i, x_i) que no tienen ninguna relevancia y que cualquier persona puede generar a partir de información pública.

Sin embargo, tenemos que mencionar una sutileza.

En la demostración de reducción formal el programa de falsificador debe ser corrido $O(q)$ veces para estar casi seguro de haber encontrado la $e^{\mathbf{ma}}$ raíz deseada.

¿Cuales son las consecuencias prácticas (en el sentido del término de Bellare–Rogaway "seguridad demostrable orientada hacia la práctica," o en inglés *practice-oriented provable security*)**?**

Supongamos que estamos usando un valor de N tan grande que confiamos en que las $e^{\mathbf{mas}}$ raíces mod N no pueden ser calculadas en menos de 2^{80} operaciones.

Supongamos que podemos esperar ataques de mensajes escogidos en que el adversario puede hacer un millón ($= 2^{20}$) preguntas al oráculo de firmas.

La reducción formal implica que podemos estar seguros solamente de que el falsificador necesitará por lo menos

$$2^{80}/2^{20} = 2^{60}$$

operaciones.

Por otro lado, la versión informal dice que el falsificador necesitará el mismo tiempo — 2^{80} operaciones — que cualquier otra persona que quiere producir una e^{ma} raíz mod N.

¿Qué tiene razón,

(1) la demostración de reducción?

(2) el sentido común?

Pregunta equivalente: ¿los dos problemas a continuación son equivalentes el uno al otro, o no?

El RSA-problema:

Dados N, e, y,
halle la e^{ma} raíz de y mod N.

El RSA1(q)-problema:

Dados N, e y un conjunto finito de y_i
aleatorios, se permite seleccionar
$\leq q$ de los y_i, para cada uno de los cuales
se da su e^{ma} raíz mod N;
se requiere producir la e^{ma} raíz mod N
de uno de los demas y_i.

Argumento informal:

RSA1(q) no es más fácil que RSA.

Reducción formal:

RSA puede ser solucionado con $O(q)$ repeticiones de un algoritmo para RSA1(q),

por lo cual un límite inferior para el tiempo para el problema RSA debe ser dividido entre $O(q)$ para obtener un límite inferior para el problema RSA1(q).

Algunos criptógrafos han desarrollado modificaciones de este sistema de firmas de RSA para tener reducciones "apretadas."

Es decir, pueden demostrar que un algoritmo que rompe su sistema podría ser usado para solucionar el RSA-problema en casi el mismo tiempo.

¿Vale la pena hacer eso?

¿Es prudente reemplacer un sistema sencillo por un sistema más complicado para poder dar una reducción apretada?

Mi opinión: ¡Tal vez no!

(1) Con una estructura más complicada hay más posibilidades de una falla. Por ejemplo, si require un generador de números aleatorios, alguien podría comprometer este generador.

(2) En la criptografía todo el mundo está implícitamente suponiendo de que el RSA-problema no es más fácil que el problema de factorización. Sin embargo, según Boneh y Venkatesan, es poco probable que exista una reducción del problema de factorización al RSA-problema. Es decir, la supuesta equivalencia de estos dos problemas es basada en "sentido común" y la experiencia de los especialistas.

Es un poco contradictorio negarse usar "sentido común" en el caso de RSA vs RSA1(q).

En la secuencia de supuesta equivalencia

$$\textbf{Factorizacion} \Longleftrightarrow \textbf{RSA} \Longleftrightarrow \textbf{RSA1}(q),$$

la primera $\Longleftrightarrow$ es seguramente el punto débil.

En otras palabras:

Argumentos formales con reducciones apretadas son cosas buenas.

Pero a veces en la criptografía queremos suponer que $\mathcal{P}_1$ es equivalente a $\mathcal{P}_2$ hasta si no podemos construir una reducción apretada de $\mathcal{P}_2$ a $\mathcal{P}_1$.

Resumen:

I. Una "demostración de seguridad" establece la seguridad del sistema solamente contra cierto tipo de ataques — y solamente con la suposición de que cierto problema matemático es difícil.

En la discusión sobre el sistema de Rabin notamos que la misma propiedad que permite demostrar la seguridad en cierto sentido podría causar la vulnerabilidad total a otro tipo de ataques.

Estamos tan preocupados por el mejoramiento de la cerradura de la puerta de la calle que nos escapa la atención que la puerta de atrás está completamente abierta.

II. Una "demostración de la seguridad" de un criptosistema no siempre está de acuerdo con el sentido común.

Por falta de reducción apretata algunos criptógrafos deciden a rechazar un sistema sencillo y pasar a un sistema más complicado, lo cual puede ser una mala idea.

III. El campo de "seguridad demostrable" perdió un poco de credibilidad cuando Shoup encontró una falla en la "demostración" de Bellare y Rogaway para su OAEP.

En la criptografía existe una tradición lamentable de tratar de publicar artículos con la mayor posible rapidez.

Y no existe tradición alguna de leer cuidadosamente los trabajos de otros investigadores.

Durante 7 años después de su publicación, nadie examinó cuidadosamente el artículo de Bellare–Rogaway, a pesar de que éste fue un trabajo importante con gran influencia en el mundo de comercio.

En contraste, en las matemáticas

1993 — el examen del trabajo de Wiles

2002 — 'Primes is in P' de Agrawal et al ('El problema "Primalidad" pertenece a P')

IV. La mayoría de los "demostraciones de seguridad" son casi imposible de leer, debido a la jerga, el formalismo excesivo, y los errores.

V. El uso del paradigma "teorema/demostración" causa malentendidos y confusión.

Prefiero las palabras

> **"afirmación"**

y

> **"argumento"**

(más precisamente:

> **"afirmación sobre la seguridad reduccionista"**

y

> **"argumento de reducción en apoyo a la afirmación").**

La palabra "demostración" tiene dos connotaciones:

(1) 100% certidumbre;

(2) una secuencia intrincada de argumentos muy técnicos que nadie fuera de un círculo estrecho de especialistas habría podido entender o cuestionar.

Una "demostración de un teorema" es algo intimidante.

Un "argumento en apoyo de una afirmación" tiene un sonido más humilde — sugiere algo que cualquier persona inteligente podría entender y tal vez poner en duda.

En la criptografía las connotaciones de los términos juegan un papel mucho más importante que en otros campos de las matemáticas.

En el álgebra usamos el término "anillo" sin preocuparnos por la posibilidad de malentendidos por no-matemáticos.

Es poco probable que un joven pensaría que puede usar como regalo para su novia.

En contraste, el público fácilmente puede interpretar las palabras "demostración de seguridad" de una manera muy exagerada — como lo hicieron las compañías Visa y MasterCard con respecto al OAEP.

Conclusión:

En los Estados Unidos tenemos una tradición larga de exagerar la capacidad de la tecnología para garantizar la seguridad.

Durante las primeras décadas de la época nuclear:

> **construcción de refugios contra la lluvia radioactiva**

Más recientemente:

> **políticos tontos gastan $> 10^{10}$ dólares para construir un "escudo anti-misil"**

Tanto en la criptografía como en la vida en general no nos debemos engañar con una sensación ilusoria de seguridad.

¿Es posible demostrar la seguridad de un criptosystema?

Mi respuesta: No.

La búsqueda de un criptosistema seguro es más arte que ciencia.

Nunca podemos estar 100% seguros de que lo hemos logrado.

Es poco probable que alcancemos este santo grial.

Galois Representations and Diophantine Problems

Gerhard Frey
IEM
University of Duisburg-Essen

Lecture
for a very special occasion and a **very special colleague**
at the
Number Theory Seminar
Barcelona, February 1, 2006

Prelude

About 20 years ago I had the great pleasure to be a visitor at CRM in Bellaterra!
I made the observation: The group S_3 is equal to $Gl(2, \mathbb{Z}/2)$.
So we can get it as image of the Galois group $G_{\mathbb{Q}}$ acting on points of order 2 of an (in fact many) elliptic curve E, and we feel at home.
S_4 is an extension of S_3 by $\mathbb{Z}/2 \times \mathbb{Z}/2$, and so we solve an embedding problem if we realize S_4 as Galois group over $\mathbb{Q}$.
Geometry gives us the group $H^1(G_{\mathbb{Q}}, E[2])$, and hence we can solve these embedding problems by using 2−coverings of the chosen elliptic curve which are easy to be handled, especially if we restrict ramification and use Selmer groups.
I discussed this with Pilar Bayer, and we decided to use Geometry to compute Witt invariants of trace forms; and we did it in a very rapid way!
Why where we interested?
Because T. Crespo had made explicit Serre's criterion for the solvability of the embedding problem

$$1 \to \mathbb{Z}/2\mathbb{Z} \to \tilde{S}_4 \to S_4 \to 1$$

(and for other 2-covers of alternating and symmetric groups).
In fact, as result we got a machinery to produce (thanks to the theory provided by Langlands and Tunnell and the computational help of J. Quer and J.C. Lario) cusp forms of weight 1 and given level quite easily, and ready was a paper, and I was well integrated in the team...
Surprisingly our machine is used rather constantly till today.

0.1 ...there is more behind...

In fact, at that time we knew already that Galois representations on torsion points may be important for diophantine questions.
I had the pleasure to give a series on lectures in the number theory seminar on Ribet' theorem proving Serre's conjecture conditionally, and this reduced **FLT** to the problem to show that every semi stable elliptic curve is modular.
What we did not know is that Wiles looked at $\tilde{S}_4$ as group isomorphic to $Gl(2, \mathbb{F}_3)$ and got, as first tiny step, that the Galois representation attached to points of order 3 of elliptic curves is modular, and then dared to go on!

In the following I shall try to sketch the big frame of Galois representations which proved to be immensely fruitful for arithmetic geometry, discuss some results and conjectures which came up during the history of the Seminar **teoria de nombres**. Nearly all of the were discussed in the seminar, and many contributions were achieved by members of the seminar.
This leads me to

0.2 Acknowledgments

Thanks to the whole TEAM
of
teoria de nombres!

and, of course, special thanks to Pilar Bayer!

PART I Galois Representations

1 The Deepest Mystery

All we want to understand is

$$\mathbb{N},$$

the ordered set of natural numbers with semi-group structures induced by addition and multiplication.

We believe that we would get "all" information if we would know

$$G_{\mathbb{Q}}$$

the group of automorphisms of the algebraic numbers $\bar{\mathbb{Q}}$. This is a huge group but it is compact with respect to the profinite topology.
Two questions arise in a natural way:

1. Which are the finite(ely generated) factors of $G_{\mathbb{Q}}$ and what can we say about the corresponding fields, the **number fields**? For example is the

   Conjecture 1.1 *(Inverse Galois Problem)*
   Every finite group is a quotient of $G_{\mathbb{Q}}$

   true?

2. What can be said about finitely generated subgroups and their fixed fields, the **large fields**?
   Here "special subgroups" like subgroups of order 2 generated by complex conjugations are interesting but in many cases one gets results for "almost all" subgroups with given number of generators.

2 Galois Representations

Let G_K be the absolute Galois group of a global (in most cases number) field K with separable closure K_s.
Let R be a ring with a topology (often discrete).
A Galois representation is a continuous homomorphism

$$\rho : G_K \to Gl(k, R).$$

ρ is (un-)ramified at p if p is (un-)ramified in $K_\rho := {K_s}^{ker(\rho)}/K$.
The *conductor* N'_ρ of ρ measures the ramification of ρ.
Examples for R are

- $\mathbb{C}$ with discrete topology,
- $\mathbb{Z}/n$ or $\mathbb{F}_q$,
- $\mathbb{Z}_l$ with l-adic topology.

Since G_K is compact the image of ρ is finite if the topology of R is discrete.

2.1 Semisimple representations

Let ρ be as above.
Let σ be an element of G_K.
By

$$\chi_{\rho(\sigma)}(T)$$

we denote the characteristic polynomial of $\rho(\sigma)$.
Example:
For $k = 2$

$$\chi_{\rho(\sigma)}(T) = T^2 - Tr(\rho(\sigma))T + det(\rho(\sigma)).$$

Definition 2.1 *ρ is semisimple if it is the direct sum of simple representations. In particular, ρ is determined (up to equivalence) by $\{(\sigma, \chi_{\rho(\sigma)}(T)); \sigma \in G_K\}$.*

For example Galois representations over $\mathbb{C}$ are always semisimple.

2.2 Čebotarev's Density Theorem

Assume that a place $v \in \Sigma_K$ is unramified in K_ρ, i.e. v does not divide N'_ρ.
Take an extension $\tilde{v}$ of v to K_s and let π_v be a Frobenius automorphism with respect to $\tilde{v}$.
Then

$$\chi_{\rho(\pi_v)}(T)$$

is well-defined and independent of the choice of $\tilde{v}$.

Theorem 2.2 ***(Čeboratev)***
Assume that ρ is ramified only in finitely many places and semisimple.
Then ρ is determined by

$$\{(v, \chi_{\rho(\pi_v)}(T)); v \in \Sigma_K \text{ and not dividing } N'_\rho\}.$$

In fact there is an effectively computable bound $M = M(K, N'_\rho)$ such that ρ is determined by

$$\{(v, \chi_{\rho(\pi_v)}(T)); v \in \Sigma_K \text{ with } norm(v) \leq M\}.$$

3 Sources for Representations

3.1 Representations attached to Group Schemes

Let $\mathcal{G}$ be a geometrically connected commutative group scheme defined over K.
Let $\mathcal{G}[n]$ denote the kernel of the scalar multiplication by n.
The operation of G_K on $\mathcal{G}[n]$ induces a Galois representation $\rho_{\mathcal{G},n}$ over $\mathbb{Z}/n$.
Taking $n = \ell^k$ (ℓ a prime) and passing to the projective limit the action of G_K induces the ℓ-adic representation $\tilde{\rho}_{\mathcal{G},l}$ which is a lift of $\rho_{\mathcal{G},l}$.

3.2 Good Reduction and Semisimpleness

We give two examples of relations between arithmetic and Galois representations. The proof of the first one is relatively easy.

Theorem 3.1 ***(Criterion of Néron-Ogg-Shafarevich)***
Let K be a field with discrete valuation v which does not divide the prime ℓ.
Let $\mathcal{A}$ be an abelian variety over K.
Then $\mathcal{A}$ has good reduction modulo v iff $\tilde{\rho}_{\mathcal{A},\ell}$ is unramified at v.

The next result is much deeper. In fact, it is the key ingredient for Faltings' proof of Mordell's Conjecture.

Theorem 3.2 ***(Faltings, Tate, Zarhin, Mori ...)***
Let K be a field of finite type, $\mathcal{A}$ an abelian variety over K and ℓ prime to char(K).
Then $\tilde{\rho}_{\mathcal{A},l}$ is semisimple.

3.3 The Conjecture of Fontaine-Mazur

In the previous subsections we produced ℓ-adic representations ρ by Tate modules of group schemes.
This can be interpreted as using the first étale cohomology group. So more generally we can use de Rham, ℓ-adic or $p-$adic cohomology groups of schemes over K to get Galois representations.

Definition 3.3 *Let K be a global field.*
An ℓ-adic representation of G_K is geometric *if it is unramified outside of a finite set of places of K and if its restriction to decomposition groups is potentially semi-stable.*

Conjecture 3.1 ***(****Fontaine-Mazur****)***
Let ρ be an irreducible ℓ-adic geometric Galois representation.
Then the representation space of ρ is isomorphic to a subquotient of an étale cohomology group of an algebraic variety over K (with coefficients in a Tate twist $\mathbb{Q}_\ell(r)$).

Consequence for number fields:
Assume that the Fontaine-Mazur conjecture is true.
Let K be a number field, and let L/K be an unramified Galois extension with $G(L/K)$ a ℓ-adic Lie group. Then L/K is finite.
This is wrong for curves over function fields K of characteristic $p > 0$.

Theorem 3.4 ***(F.-Kani)***
There exist function fields K over finite fields and non-isotrivial curves C/K (explicitly given for every genus > 2 if $p \equiv 3 \mod 4$) with regular unramified Galois pro-covers in which at least one point is totally split with Galois group $PSL_3(\mathbb{Z}_p)$.

Though the theorem "contradicts" the consequences of the Fontaine-Mazur conjecture it follows its spirit. The representation is given by the Galois action on the Tate-module of a carefully constructed Jacobian variety of a cyclic cover C of the projective line such that J_C has potentially good reduction at all places and at one place the fibre has complex multiplication of a special type.

4 Two-dimensional Representations

4.1 Two-dimensional Modular Representations

Modular representations are representations induced by Cohomology groups of the Jacobians $J_1(n)$ of modular curves $X_1(n)$ which are explicitly given curves whose points have a modular interpretation.
A very special property is that the ring of endomorphisms on $J_1(n)$ contains a large commutative subring, the **Hecke algebra** $\mathbb{T}_n$ generating an order of a totally real field.
The Hecke algebra acts in a canonical way on geometric and arithmetic objects related to $X_1(n)$ and, since $\mathbb{T}_n$ is defined over $\mathbb{Z}$, it commutes with Galois actions. In particular, $\mathbb{T}_n$ acts on the space of cusp forms (closely related to holomorphic differentials on $X_1(n)$) of weight k and splits it up in spaces generated by eigenforms. The Galois action corresponding to the cover

$$X_1(n) \to X_0(n)$$

yields a further splitting of the eigenspaces of cusp forms with respect to $\Gamma_0(n)$ with nebentype ϵ where ϵ is a Dirichlet character modulo n.

The **Eichler-Shimura relation** connects Frobenius automorphisms acting on $X_1(n) \times \mathbb{Z}_p$ with the p-th Hecke operator T_p.

Theorem 4.1 ***(Deligne)***
For $k \geq 2$ and an eigenform f of level n, weight k and nebentype ϵ there exists a two-dimensional $\overline{Q}_\ell[G_\mathbb{Q}]$-representation ρ_λ which is not ramified outside of $n\ell$ with $Tr(\rho_\lambda(\pi_p)) = a_p$ (a_p the eigenvalue of T_p) and $det(\rho_\lambda(\pi_p)) = \epsilon(p)p^{k-1}$.

As special case of the Fontaine- Mazur conjecture one gets:
Geometric ℓ-adic odd irreducible two-dimensional representations are attached to modular forms!

4.1.1 mod $-\ \ell$-version: Serre's conjecture[1]

Conjecture 4.1 *Let ρ be an odd irreducible Galois representation of $G_\mathbb{Q}$ into $Gl(2,k)$ with k a finite field of characteristic p.*

[1] added in proof: This is no longer a conjecture but a theorem of Khare-Wintenberger and Kisin. We shall use this in the sequel.

- *ρ is attached to a modular form.*
- *The local behavior of ρ at p determines the minimal weight, the minimal level and the nebentype of an attached cusp form.*
- *If the group scheme attached to ρ is finite at p then the minimal weight is 2, the level is the prime-to-p-part of N_ρ and the nebentype is trivial.*

4.2 The non-geometric case: $k = 1$

The Theorem of Deligne stated above is true for $k = 1$ if we use $\mathbb{C}$ as ground field.

Theorem 4.2 ***(Deligne-Serre)***
For an eigenform f of level n, weight 1 and nebentype ϵ there exists an odd irreducible two-dimensional $\mathbb{C}$-representation ρ_f with Artin conductor n with $Tr(\rho_f(\pi_p)) = a_p$ (a_p the eigenvalue of T_p) and $det(\rho_f(\pi_p)) = \epsilon(p)$.

In combination with a result of Langlands-Weil we get

Corollary 4.3 *Artin's conjecture is true for odd two-dimensional representations iff every such representation is modular.*

Remark 4.4 *As indicated in the header of the subsection we do not have a a geometric interpretation of modular forms of weight 1 via an Eichler-Shimura isomorphism. Nevertheless one uses geometry to construct* mod $-\ell$*-representations (multiply by Eisenstein series to raise the weight), then lifts these representations to ℓ-adic representations, and finally uses analytic number theory (Rankin) to show that these representations are coming from complex representations.*

This opens a wide area for numerical experiments.
On the one hand try to compute the number of eigenforms of weight one to given level, and on the other side compute the number of odd two-dimensional representations with given Artin conductor.
Both numbers have to be the same, and in fact they are in all tested cases.
The possible images of such representations modulo the center are very restricted (dihedral, A_4, S_4, A_5), and so it is interesting to interpret them geometrically (cf. Prelude).

PART II

5 Finiteness Results

5.1 Isogeny Theorems

We have mentioned already that Faltings, Tate et al. have proved that the ℓ-adic representations attached to abelian varieties over fields of finite type are semi-simple.
Consequence: The L-series of abelian varieties determine the isogeny classes.
In fact, everything is effective, and so two abelian varieties over fields K of finite type are isogenous if "enough" (e.g. infinitely many) Galois representations on ℓ-torsion points are equivalent.
Here "enough" depends on the arithmetic of the abelian variety, e.g. their conductor, and on the field K. Does this result remain true if we replace equivalence between representations by equality of the kernels of the representations?

5.1.1 Horizontal Isogeny Theorem for Elliptic Curves

Using crucially results of Serre and investing some work in the CM case we (F.-Jarden) prove

Theorem 5.1 *Assume that K is a finitely generated field which is not finite, and let E and E' be elliptic curves over K.*
Assume that there exists an infinite set Λ of primes and a constant c such that for $\ell \in \Lambda$

$$[K(E[\ell], E'[\ell]) : K(E[\ell]) \cap K(E'[\ell])] \leq c.$$

Then E is isogenous to a twist of E'.

It is remarkable that this result is not true if K is a finite field. In this case Λ has to be a set of Dirichlet density $> 3/4$.

5.2 Shared Torsion Structures

As in the last section the statements and conjectures make sense for arbitrary fields of finite type. Here we restrict ourselves to the case that the ground field is $\mathbb{Q}$.
Let A_1 and A_2 be two abelian varieties defined over $\mathbb{Q}$ with conductor N_1 and N_2.

Assume that we find Galois invariant finite subgroups $C_i \subset A_i$ with C_1 Galois isomorphic to C_2. How large (depending on $\dim A_i$, N_i) has the order of C_1 to be in order to force A_1 and A_2 to have isogenous abelian subvarieties?
The best results known in this direction are due to Faltings and Masser-Wüstholz. Typically the bounds involve the heights of A_i. It is *conjectured* that the heights depend polynomially on the degree of the conductors.
We restrict ourselves to the case that A_1 is an elliptic curve.

Conjecture 5.1 *(Degree Conjecture) There is a polynomial function $m(t)$ such that for all elliptic curves E and all abelian varieties A of dimension g over $\mathbb{Q}$ we get:*
Assume that the degree of the conductor of $E \times A$ is bounded by M, that $m \geq m(2^M)$ and that a Galois invariant subgroup C of order m of $E(\overline{\mathbb{Q}})$ can be embedded (as $G_{\mathbb{Q}}$- module) into $A(\bar{\mathbb{Q}})$.
Then A contains a subvariety isogenous to E.

For pairs of elliptic curves much sharper conjectures should be true.

Conjecture 5.2 *(Representation Conjecture) For fixed elliptic curve E_0 there is a number m_0 such that for all $m > m_0$ and for all elliptic curves E with $\rho_{E_0,m} = \rho_{E,m}$ it follows that E_0 is isogenous to E.*

Kani and Darmon conjecture that fixing E_0 is not necessary and that it is (maybe up to finitely many exceptions (Kani)) sufficient to have $m \geq 23$.
These conjectures are motivated by standard conjectures like Lang's conjecture for surfaces of general type applied to moduli spaces of pairs of elliptic curves having common torsion structures.

5.3 The Asymptotic Fermat Conjecture

We formulate Serre's conjecture in the geometric context.

Assume that ρ is an irreducible and odd two-dimensional representation of $G_{\mathbb{Q}}$ to $\mathrm{Gl}(2, \bar{\mathbb{F}}_\ell)$ such that the group scheme A_ρ is finite at ℓ. Then A_ρ can be embedded into $J_0(N'_\rho)$ where N'_ρ is the prime-to-ℓ-part of the Artin conductor of ρ.

We apply this to representations attached to elliptic curves.
Consequence 1: Let $A, B \in \mathbb{Z}$ be relatively prime. Then the elliptic curve

$$E_{A,B} : Y^2 \;=\; X(X-A)(X-B)$$

is semi stable outside of 2 and $E_{A,B}[\ell]$ is finite as group scheme at all odd primes p with $v_p(AB(A-B)) \equiv 0 \bmod \ell$.

So $E_{A,B}[\ell]$ can be embedded into $J_0(N_{A,B})$ with

$$N_{A,B} = 2^{\delta}\Pi_{v_p(AB(A-B))\not\equiv 0\, mod\, \ell}\ p$$

with $\delta \leq 4$.

Remark 5.2 *Of course, this result proves FLT!*

Consequence 2: Let ℓ_i, $i \in \mathbb{N}$, be an infinite sequence of different prime numbers, and for each i let ρ_i be an odd irreducible representation of $G_{\mathbb{Q}}$ to $\mathrm{Gl}(2, \bar{\mathbb{F}}_{\ell_i})$ finite at ℓ_i.
If the Serre conductors N_{ρ_i} are bounded then there is an elliptic curve E_0 defined over $\mathbb{Q}$ such that for infinitely many i we get:

$$\rho_i = \rho_{E_0,\ell_i}.$$

Corollary 5.3 *Assume that there is a number N_0 such that for infinitely many prime numbers $\ell_i \geq 7$ there is an elliptic curve E_i defined over $\mathbb{Q}$ such that $\mathbb{Q}(E_i[\ell_i])$ is unramified outside of $\ell_i N_0$ and such that $E_i[\ell_i]$ is finite at ℓ_i. Then there is an elliptic curve E_0 with $E_0[\ell_i] = E_i[\ell_i]$ for infinitely many i, and the conductor of E_0 is $\leq N_0$.*

These two consequences give an equivalence between the **Asymptotic Fermat Conjecture** and Representation Conjecture 5.2 for elliptic curves.

Theorem 5.4 *Fix $a, b, c \in \mathbb{Z}$ relatively prime. Assume that for infinitely many primes $\ell \geq 5$ and $x, y, z \in \mathbb{Z}$, relatively prime, one has*

$$ax^{\ell} \ + \ by^{\ell} \ = \ cz^{\ell}.$$

Then there is an elliptic curve E_0 defined over $\mathbb{Q}$ of conductor $N_0 = 2^{\delta} \cdot \Pi_{l|abc} l$ such that for infinitely many ℓ

$$E_0[2\ell] = E_{ax^{\ell},by^{\ell}}[2\ell] \ as \ G_{\mathbb{Q}} - module.$$

*Hence the **Asymptotic Fermat Conjecture** true over $\mathbb{Q}$ if and only if the Representation Conjecture 5.2 for even m_i is true.*

5.4 The ABC-Conjecture and the Degree-Conjecture

Recall the **ABC-Conjecture** over $\mathbb{Q}$ stated in a weak form:
There are constants c and d such that for all relatively prime integers A and B we have

$$\mid A \mid \leq c(\prod_{p|AB(A-B)} p)^d.$$

Let

$$\varphi : X_0(N_E) \to E$$

be a minimal modular parametrization of the elliptic curve E.

Fact:

$$\log(deg(\varphi)) \leq 2h(E) + O(\log(N_E))$$
$$\leq \log(deg(\varphi)) + O(\log N_E) + O(1)$$

where $h(E)$ is the Faltings height of E. For semi stable E the conductor N_E is square free and hence $J_0(N_E)$ has no multiple factors. Since $deg(\varphi)^2$ is the order of the intersection of E with the kernel of φ_* the Conjecture 5.1 predicts that it is bounded by a polynomial in N_E.
We apply this to the curve

$$E : Y^2 = X(X - A)(X - B)$$

and get

Theorem 5.5 *The ABC-conjecture over $\mathbb{Q}$ is equivalent with the degree conjecture 5.1 for semi stable elliptic curves with rational points of order 2 over $\mathbb{Q}$ applied to their modular parametrization.*

PART III

6 Large Fields

6.1 Notation and Definitions

Let e be a non-negative integer.
Since $G_{\mathbb{Q}}$ is compact the cartesian product $G_{\mathbb{Q}}^e$ has a unique normalized Haar measure.
In the following $\sigma = (\sigma_1, \ldots, \sigma_e)$ is an element in $G_{\mathbb{Q}}^e$,
$\overline{\mathbb{Q}}(\sigma)$ is the fixed field in $\overline{\mathbb{Q}}$ of $\sigma_1, \ldots, \sigma_e$. We say that a property $\mathcal{E}$ holds for almost all σ iff it is true outside of a set of measure 0 in $G_{\mathbb{Q}}^e$. It turns out that this gives a lot of information about the behavior of $\mathcal{E}$ over number fields.
$e \geq 1$ is a *cut number* if a (arithmetic-geometric) property is true for almost all $\sigma \in G_{\mathbb{Q}}^{e-1}$ but not in $G_{\mathbb{Q}}^e$.
A first example for "almost all":(Fried-Jarden)
For all $e \geq 1$ and for almost for almost all σ the Galois group of $\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(\sigma)$ is profinite free and $\overline{\mathbb{Q}}(\sigma)$ is hilbertian.

6.2 Large fields are large

Example 6.1 *For all e and almost all σ and all irreducible varieties V defined over $\overline{\mathbb{Q}}(\sigma)$ we have*

$$V(\overline{\mathbb{Q}}(\sigma)) \neq \emptyset.$$

So $\overline{\mathbb{Q}}(\sigma)$ is a PAC field.

In a similar direction points the next example:

Example 6.2 *(F.-Jarden) For all e, for almost all σ and for all abelian varieties over $\overline{\mathbb{Q}}(\sigma)$ the rank of $A(\overline{\mathbb{Q}}(\sigma))$ is infinite.*

Reason: For varieties V there are infinitely many linear disjoint extensions of K of *fixed degree* over which V has "new" rational points.

6.3 Torsion points in large fields

The argument given in the last section for points on varieties does not hold for torsion points of a fixed group scheme. First take the multiplicative group G_m.
A by now classical result of Jarden is:
For almost all $\sigma \in G_{\mathbb{Q}}$ the field $\overline{\mathbb{Q}}(\sigma)$ contains infinitely many roots of unity.
For $e \geq 2$ the field $\overline{\mathbb{Q}}(\sigma)$ contains only finitely many roots of unity.
So 1 and 2 are "cut numbers".
Much deeper is the following result of **Geyer-Jarden**:
Let E be an elliptic curve defined over $\mathbb{Q}$.
Then

1. If $e = 1$ then there are infinitely many prime numbers ℓ with $E(\overline{\mathbb{Q}}(\sigma))[\ell] \neq 0$.
2. If $e \geq 2$ then there are only finitely many prime numbers ℓ with $E(\overline{\mathbb{Q}}(\sigma))[\ell] \neq 0$.
3. For all $e \geq 1$ and all ℓ the fixed elements in the Tate module, $T_\ell(E)^{G_{\overline{\mathbb{Q}}(\sigma)}}$, is equal to $\{0\}$.

The proof of these results uses our knowledge about the Galois representations on torsion points of elliptic curves.
A key ingredient is Serre's open image theorem on the Galois action on the products of the ℓ-torsion points (It is tricky in the case of complex multiplication.)

With these remarks one can hope to generalize the results.
Without problems one can replace "$\mathbb{Q}$" by "number field" resp. "field of finite type".
What about abelian varieties of higher dimension?
A conjecture of Geyer and Jarden stated already 1978 claims that analogous results should hold.
The difficulty comes from the fact that Serre has not proved strong enough results for the images of the representations in all cases!
What is known?
The result on Tate modules is true for all abelian varieties over finitely generated fields (Jacobson-Jarden).
The second part of the result above is true for all abelian varieties over finitely generated fields in characteristic 0 (Jacobson-Jarden).
The first part is true for abelian varieties A if either $\mathrm{End}(A) = \mathbb{Z}$, $\dim(A) = 2, 6$ or odd, or A has real multiplication and not potentially good reduction. (In these cases Serre's results about the Galois representations attached the A are strong enough.) In the number field case there is a new result (2004) of Geyer and Jarden which use the rudiments known about Galois representations in an ingenious way.
They prove

Theorem 6.3 *Let K be a number field and A an abelian variety defined over K. Then K has a finite Galois extension L such that for almost all $\sigma \in G_L$ there are infinitely many primes ℓ with*
$A(\overline{\mathbb{Q}}(\sigma))[\ell] \neq 0$.

6.4 Elliptic curves with CM

Some questions:
Are there cut numbers larger than 2?
What about torsion and isogenies of elliptic curves over large fields?

Using the results about roots of unity one gets immediately restrictions for elliptic curves having all points of order n in a field $\overline{\mathbb{Q}}(\sigma)$.
But the modular curves $X_1(n)$ and $X_0(n)$ have for all e and almost all σ infinitely many points in $\overline{\mathbb{Q}}(\sigma)$ (PAC-property).
We know (Merel) that over number fields the torsion of elliptic curves is uniformly bounded, and we believe that the same is true for isogenies, *as long as we avoid elliptic curves with complex multiplication.*
Can we hope for such a result over $\overline{\mathbb{Q}}(\sigma)$? Answer:

Theorem 6.4 ***(F.-Jarden 06)***
We identify twists of elliptic curves and claims hold for almost all σ.

1. *If $e \leq 2$ then there are infinitely many non-isomorphic elliptic curves E with CM over $\overline{\mathbb{Q}}(\sigma)$ and all endomorphisms defined over $\overline{\mathbb{Q}}(\sigma)$.*
2. *If $e \geq 3$ then there are only finitely many such curves.*
3. *If $e \leq 3$ there are infinitely many elliptic curves defined over $\overline{\mathbb{Q}}(\sigma)$ with CM over $\mathbb{C}$.*
4. *For $e \geq 4$ there are only finitely many elliptic curves E over $\overline{\mathbb{Q}}(\sigma)$ with CM.*

So 3 and 4 are cut numbers.

The proof of the theorem uses (of course) the knowledge about the degree of j-invariants of CM-curves and the relation to the class number $h(d)$ of imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ which is "about" $\sqrt{d}$.
But this is not precise enough. We need

Theorem 6.5 *(partly courtesy of R. Murty)*

$$\sum_{p \equiv 3 \mod 4} h(p)^{-2} = \infty.$$

A000079

Anna Rio

Departament de Matemática Aplicada II
Universitat Politécnica de Catalunya

STNB 2006

Keywords: core, easy, nice

$$a(0) = 1$$

a(1) =

- An octahedral-elliptic type equality in $Br_2(k)$
- On curves of genus 2 with Jacobian of GL_2-type
- Dyadic exercises for octahedral extensions
- Octahedral Galois representations arising from $\mathbb{Q}-$curves of degree 2
- Determining the $2-$Sylow subgroup of an elliptic curve over a finite field

$a(2)=$

Aritmètica d'àlgebres de quaternions
Corbes de Shimura, STNB 2001

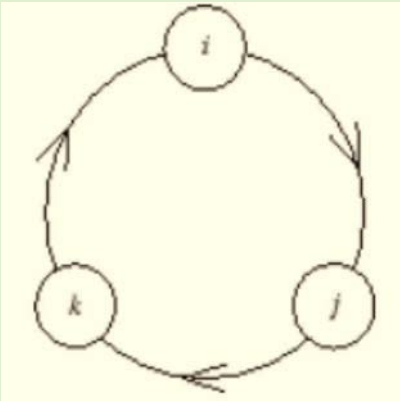
- Una K –àlgebra de quaternions és una K –àlgebra central i simple, de dimensió 4 sobre K
- Una K –àlgebra de quaternions o bé és isomorfa a $M_2(K)$ o bé és una K –àlgebra de divisió

- Sobre $\mathbb{R}$ les úniques àlgebres de quaternions són $M_2(\mathbb{R})$ i $\mathbb{H} = (-1,-1)_{\mathbb{R}}$

$\mathbb{H}$ és una $\mathbb{R}-$àlgebra de dimensió 4 amb base $1, i, j, k$

Producte

- 1 és l'element identitat
- i, j, k són arrels quadrades de -1
- $ij = k$, $ji = -k$ i totes les identitats obtingudes d'aquestes per permutacions cícliques de (i, j, k)



Complexos $\mathbb{C}$

$z =< a, b >$

Producte

$< a_1a_2 - b_1b_2, a_1b_2 + a_2b_1 >$

Norma

$$|z| = \sqrt{a^2 + b^2}$$

Geometria

$$|z| = 1$$
$$\Downarrow$$
Rotació 2D
$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

Quaternions $\mathbb{H}$

$\mathbb{H} = \mathbb{R} \oplus \mathbb{H}^+$

$q =< \alpha, v >=< q_0, [q_1, q_2, q_3] >$

Producte

$< \alpha\beta - v.u, \alpha u + \beta v + (v \times u) >$

Norma

$$|q| = \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2}$$

Geometria

$$|q| = 1$$
$$\Downarrow$$
Rotació 3D

$$\mathbf{q} = \left[\cos\frac{\theta}{2} \quad a_x \sin\frac{\theta}{2} \quad a_y \sin\frac{\theta}{2} \quad a_z \sin\frac{\theta}{2} \right]$$

$$\mathbf{q} = \left\langle \cos\frac{\theta}{2}, \mathbf{a}\sin\frac{\theta}{2} \right\rangle$$

Rotació d'angle θ al voltant de l'eix de direcció unitària **a**

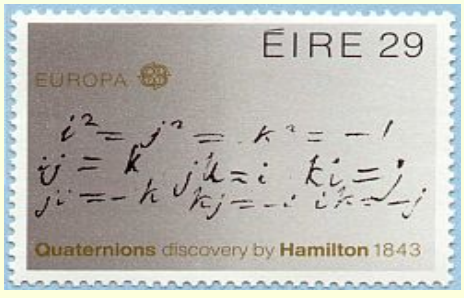
$$\begin{bmatrix} 1-2q_2^2-2q_3^2 & 2q_1q_2+2q_0q_3 & 2q_1q_3-2q_0q_2 \\ 2q_1q_2-2q_0q_3 & 1-2q_1^2-2q_3^2 & 2q_2q_3+2q_0q_1 \\ 2q_1q_3+2q_0q_2 & 2q_2q_3-2q_0q_1 & 1-2q_1^2-2q_2^2 \end{bmatrix}$$

Sir William Rowan Hamilton

Fascinat per la relació entre $\mathbb{C}$ i la geometria plana, intentava trobar una àlgebra més gran que jugués el mateix paper a la geometria de l'espai

Cercava una àlgebra de divisió normada de dimensió 3. Però tal cosa no existeix. En realitat necessitava una àlgebra de dimensió 4

La va trobar el 16 d'octubre de 1843



L'endemà, Hamilton va escriure al seu col.lega John T. Graves. El 26 de desembre aquest li va escriure parlant-li d'una nova àlgebra de dimensió 8, i demostrant que era una àlgebra de divisió normada.

Els nombres octavians

Hamilton es va oferir a fer-ne difusió, però ho va anar deixant i mentrestant, el març de 1845, Arthur Cayley, que buscava relacions entre quaternions i funcions hiperel.líptiques, va publicar l'article "*On Jacobi's Elliptic Functions (...) and on Quaternions*", on de passada descrivia la mateixa àlgebra.

Els nombres de Cayley

$$a(3)=$$

Els octonions $\mathbb{O}$

Àlgebra de divisió normada de dimensió 8

$$\mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H} \subseteq \mathbb{O}$$

Teorema Són les úniques àlgebres de divisió normades

Adolf Hurwitz

Über die Composition der quadratischen Formen von beliebig vielen Variabeln, Nachr. Ges. Wiss. Göttingen (1898) 309-316.

Àlgebra és un $\mathbb{K}-$espai vectorial equipat amb una forma bilineal $m : A \times A \to A$, anomenada *multiplicació*, i un element $1 \in A$ diferent de zero, anomenat *unitat*, tals que $m(1, a) = m(a, 1) = a$

No suposem les àlgebres associatives

Àlgebra de divisió: si $ab = 0$, aleshores $a = 0$ o $b = 0$

Si l'àlgebra és associativa equival a l'existència d'inversos multiplicatius

Àlgebra de divisió normada és una $\mathbb{R}-$àlgebra amb estructura d'espai vectorial normat tal que $||ab|| = ||a||||b||$

Implica que l'àlgebra és de divisió i que $||1|| = 1$

$\mathbb{R}, \mathbb{C}, \mathbb{H}$

$(x_1^2 + x_2^2 + \cdots + x_n^2)(y_1^2 + y_2^2 + \cdots + y_n^2) = z_1^2 + z_2^2 + \cdots + z_n^2$

$n = 1,\ 2$ (Diofant), 4 (Fermat-Lagrange)

Teorema dels vuit quadrats (C.F. Degen, 1818)

Àlgebra alternativa: qualsevol subàlgebra generada per dos elements és associativa

- (Artin) A alternativa si, i només si, per a tot $a, b \in A$

$$(aa)b = a(ab) \qquad (ab)a = a(ba) \qquad (ba)a = b(aa)$$

- Associador: $A \times A \times A \to A$

$$[a, b, c] = (ab)c - a(bc)$$

és un forma trilineal. És alternada si, i només si, l'àlgebra és alternativa

Teorema $\mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H} \subseteq \mathbb{O}$ són les úniques àlgebres de divisió alternatives

Max Zorn

Theorie der alternativen Ringe

Abh. Math. Sem. Univ. Hamburg 8 (1930), 123– 147

Els octonions $\mathbb{O}$

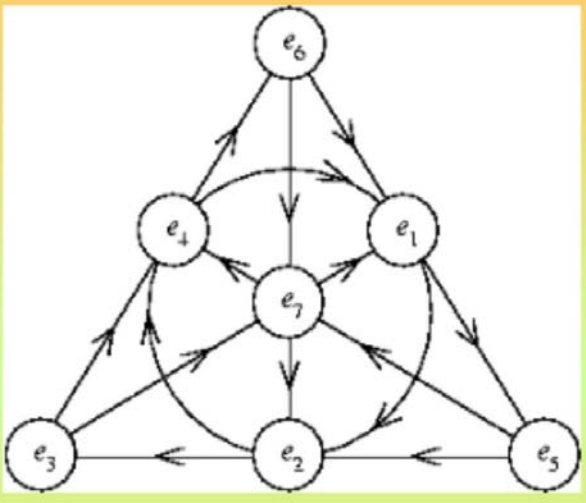
- Base: $1, e_1, e_2, e_3, e_4, e_5, e_6, e_7$
- Taula del producte

	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	-1	e_4	e_7	$-e_2$	e_6	$-e_5$	$-e_3$
e_2	$-e_4$	-1	e_5	e_1	$-e_3$	e_7	$-e_6$
e_3	$-e_7$	$-e_5$	-1	e_6	e_2	$-e_4$	e_1
e_4	e_2	$-e_1$	$-e_6$	-1	e_7	e_3	$-e_5$
e_5	$-e_6$	e_3	$-e_2$	$-e_7$	-1	e_1	e_4
e_6	e_5	$-e_7$	e_4	$-e_3$	$-e_1$	-1	e_2
e_7	e_3	e_6	$-e_1$	e_5	$-e_4$	$-e_2$	-1

- $e_1, e_2, \ldots e_7$ són arrels quadrades de -1
- anticommutativitat: $e_i e_j = -e_j e_i$ si $i \neq j$
- *index cycling* (mod 7): $e_i e_j = e_k \Rightarrow e_{i+1} e_{j+1} = e_{k+1}$
- *index doubling* (mod 7): $e_i e_j = e_k \Rightarrow e_{2i} e_{2j} = e_{2k}$

A partir d'un producte no trivial, com ara $e_1 e_2 = e_4$, aquestes propietats són suficients per recuperar tota la taula del producte

El pla de Fano



7 punts i 7 rectes. Cada parell de punts en una única recta. Cada recta té 3 punts ordenats cíclicament

$$e_i e_j = e_k \qquad e_j e_i = -e_k$$

El pla de Fano és el pla projectiu sobre $\mathbb{F}_2$

Les rectes per l'origen a l'espai $\mathbb{F}_2^3$ s'identifiquen amb els set elements diferents de zero de $\mathbb{F}_2^3$

- Els plans per l'origen donen subàlgebres de $\mathbb{O}$ isomorfes als quaternions (alternativitat)
- Les rectes per l'origen donen subàlgebres de $\mathbb{O}$ isomorfes als complexos
- L'origen dóna una subàlgebra isomorfa als reals

Els octonions com a matrius

$$\mathbb{O} = \left\{ \begin{pmatrix} \alpha & u \\ v & \beta \end{pmatrix} \mid \alpha, \beta \in \mathbb{R},\ u, v \in \mathbb{R}^3 \right\}$$

- Suma component a component
- Producte

$$\begin{pmatrix} \alpha_1 & v_1 \\ u_1 & \beta_1 \end{pmatrix} \begin{pmatrix} \alpha_2 & v_2 \\ u_2 & \beta_2 \end{pmatrix} =$$

$$\begin{pmatrix} \alpha_1\alpha_2 + v_1.u_2 & \alpha_1 v_2 + \beta_2 v_1 - (u_1 \times u_2) \\ \alpha_2 u_1 + \beta_1 u_2 + (v_1 \times v_2) & \beta_1\beta_2 + u_1.v_2 \end{pmatrix}$$

Els octonions com a parells de quaternions

Els octonions com a àlgebra de grup twistada

Podem usar qualsevol funció $\alpha : G \times G \to \{\pm 1\}$ per *twistar* el producte a l'àlgebra de grup $\mathbb{R}[G]$:

$$g \star h = \alpha(g,h)gh$$

α és $2-$cocicle $\Leftrightarrow$ associativa
α és $2-$cocicle estable $\Leftrightarrow$ commutativa

- $\mathbb{C} = \mathbb{R}[\mathbb{F}_2]$ *twistada* amb un $2-$cocicle estable
- $\mathbb{H} = \mathbb{R}[\mathbb{F}_2^2]$ *twistada* amb un $2-$cocicle
- $\mathbb{O} = \mathbb{R}[\mathbb{F}_2^3]$ *twistada* per una funció que no és $2-$cocicle

$\mathbb{O}$ és una àlgebra no associativa

$1, 2, 4, 8 \ldots$ What comes next?

A000079

La construcció de Cayley-Dickson

Successió infinita d'àlgebres, cadascuna dobla la dimensió de l'anterior i les quatre primeres són $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$

Si A és una àlgebra on hi ha definida una conjugació $a \to a^*$, aleshores definim una àlgebra A'

- elements: parells d'elements de A
- suma: component a component
- producte: $(a,b)(c,d) = (ac - db^*, a^*d + cb)$
- conjugació: $(a,b)^* = (a^*, -b)$

Equivalentment: $A' = \{ a + bi \mid a, b \in A\}$ amb $i^2 = -1$

$a(ib) = i(a^*b) \quad (ai)b = (ab^*)i \quad (ia)(bi^{-1}) = (ab)^* \quad i^* = -i$

Àlgebres normades

Una $*-$**àlgebra** és una àlgebra A amb una conjugació: $* : A \to A$ $\mathbb{R}-$lineal tal que $a^{**} = a$ i $(ab)^* = b^*a^*$

Una àlgebra commutativa es pot considerar com a $*-$àlgebra prenent $*$ =identitat. Direm que l'àlgebra és **real**

Una $*-$àlgebra A és **ben normada** (*nicely normed*) si

$$a + a^* \in \mathbb{R} \qquad \text{i} \qquad aa^* > 0 \quad \forall a \neq 0$$

Aleshores, $\mathrm{Re}(a) = \dfrac{a + a^*}{2} \in \mathbb{R}$, $\mathrm{Im}(a) = \dfrac{a - a^*}{2}$

Norma: $||a|| = \sqrt{aa^*}$

L'àlgebra té inversos multiplicatius: $a^{-1} = a^*/||a||^2$

Si A és ben normada i alternativa, és una àlgebra de divisió normada

a, b, a^*, b^* pertanyen a l'àlgebra associativa generada per Im(a), Im(b)

- $ab = 0 \Rightarrow (ab)b^{-1} = 0$
  Si $b \neq 0$, $b^{-1} = b^*/||b||$ i el producte anterior és associatiu
- $||ab||^2 = (ab)(ab)^* = ab(b^*a^*) = a(bb^*)a^* = ||a||^2||b||^2$

Efectes d'iterar la construcció de Cayley-Dickson

Proposició 1 A' mai és real

Proposició 2 A és real $\iff$ A' és commutativa

Proposició 3 A és commutativa i associativa $\iff$ A' és associativa

Proposició 4 A és associativa i ben normada $\iff$ A' és alternativa i ben normada

Proposició 5 A és ben normada $\iff$ A' és ben normada

$\mathbb{R}$ és $*-$àlgebra real, commutativa, associativa i ben normada

$\Downarrow$

$\mathbb{C}$ és $*-$àlgebra commutativa, associativa i ben normada

$\Downarrow$

$\mathbb{H}$ és $*-$àlgebra associativa i ben normada

$\Downarrow$

$\mathbb{O}$ és $*-$àlgebra alternativa i ben normada

Totes quatre són àlgebres de divisió normades

Els sedenions $\mathbb{O}'$

- Successió de $*-$àlgebres A_n de dimensió $\mathbf{2^n}$
- Ben normades, però no reals, ni commutatives, ni alternatives
- Tenen inversos multiplicatius però no són àlgebres de divisió
  $A_{16} = \mathbb{O}'$ (i, per tant, tota la resta) té divisors de zero

  $a = (e_7, e_8) \qquad b = (e_5, e_6)$

Àlgebres de Clifford

William Kingdom Clifford

Aplication's of Grassman's extensive algebra. Amer. Jour. Math. 1 (1878), 350-358

- V espai vectorial real amb un producte escalar
  $Cliff(V)$ és l'àlgebra associativa generada lliurement per V mòdul les relacions $v^2 = -||v||^2$
  Equivalentment, mòdul les relacions $vw + wv = -2\langle v, w\rangle$
- $V = \mathbb{R}^n$ amb el producte escalar usual, $Cliff(n)$.

  Àlgebra associativa lliurement generada per n arrels quadrades de -1 que anticommuten

$$Cliff(0) = \mathbb{R} \qquad Cliff(1) = \mathbb{C} \qquad Cliff(2) = \mathbb{H}$$

Àlgebres de Clifford $Cliff(n)$

n	$Cliff(n)$
0	$\mathbb{R}$
1	$\mathbb{C}$
2	$\mathbb{H}$
3	$\mathbb{H} \oplus \mathbb{H}$
4	$M_2(\mathbb{H})$
5	$M_4(\mathbb{C})$
6	$M_8(\mathbb{R})$
7	$M_8(\mathbb{R}) \oplus M_8(\mathbb{R})$

Periodicitat de Bott

$Cliff(n+8) \cong Cliff(n) \otimes M_{16}(\mathbb{R})$

Àlgebres de matrius sobre $\mathbb{R}, \mathbb{C}, \mathbb{H} \Rightarrow$ És fàcil determinar les seves representacions

Àlgebres de Clifford $Cliff(n)$: representacions

- Tota representació és suma d'irreductibles
- Única representació irreductible de $M_k(\mathbb{R}), M_k(\mathbb{C}), M_k(\mathbb{H})$
- $n \neq 3,7 \mod 8$: única rep. irreductible de $Cliff(n)$. Espai dels pinors P_n
- $n = 3,7 \mod 8$, $Cliff(n)$ és $\oplus$ de dues àlgebres de matrius reals o quaternioniques, té dues rep. irreductibles. Pinors positius P_n^+ i pinors negatius P_n^-

n	$Cliff(n)$	Representacions irreductibles
0	$\mathbb{R}$	$P_0 = \mathbb{R}$
1	$\mathbb{C}$	$P_1 = \mathbb{C}$
2	$\mathbb{H}$	$P_2 = \mathbb{H}$
3	$\mathbb{H} \oplus \mathbb{H}$	$P_3^+ = \mathbb{H}, P_3^- = \mathbb{H}$
4	$M_2(\mathbb{H})$	$P_4 = \mathbb{H}^2$
5	$M_4(\mathbb{C})$	$P_5 = \mathbb{C}^4$
6	$M_8(\mathbb{R})$	$P_6 = \mathbb{R}^8$
7	$M_8(\mathbb{R}) \oplus M_8(\mathbb{R})$	$P_7^+ = \mathbb{R}^8, P_7^- = \mathbb{R}^8$

El teorema de Hurwitz

- Suposem que $\mathbb{K}$ és una àlgebra de divisió normada

$$\begin{array}{rccc} L_a : & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & ax \end{array}$$

- Si $||a|| = 1$, l'operador L_a conserva la norma. Aplica $S(\mathbb{K})$, l'esfera unitat, sobre sí mateixa
- $\mathbb{K}$ és àlgebra de divisió $\Rightarrow$ donats dos punts qualssevol de $S(\mathbb{K})$, hi ha un operador L_a que envia un a l'altre
- Tanta simetria a $S(\mathbb{K})$ vol dir que la norma prové d'un producte escalar

$$\langle x, y \rangle = \frac{1}{2}\left(||x+y||^2 - ||x||^2 - ||y||^2 \right)$$

- $a \in \mathbb{K}$ imaginari si és ortogonal a 1. $\mathrm{Im}(\mathbb{K})$ és l'espai tangent a $S(\mathbb{K})$ en el punt 1

El teorema de Hurwitz

$$\begin{array}{rcl} a & \longrightarrow & L_a \\ S(\mathbb{K}) & \rightarrow & \text{transformacions ortogonals de } \mathbb{K} \\ \mathrm{Im}(\mathbb{K}) & \rightarrow & \text{transformacions } \textit{antiadjuntes} \end{array}$$

a imaginari de norma 1 $\Rightarrow$ L_a ortogonal i antiadjunta
Ortogonal: es pot trobar una base ortonormal en la qual la matriu és diagonal per blocs amb blocs 2×2

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \text{ i potser un bloc (1)}$$

Ortogonal i antiadjunta $\Rightarrow$ blocs 2×2 de la forma $\pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

a imaginari de norma 1 $\Rightarrow L_a^2 = -1$

$$L_a^2 = -||a||^2 \qquad \forall a \in \mathrm{Im}(\mathbb{K})$$

El teorema de Hurwitz

$$L_a^2 = -||a||^2 \qquad \forall a \in \mathrm{Im}(\mathbb{K})$$

$a \rightarrow L_a$ és una representació de $\mathit{Cliff}(\mathit{Im}(\mathbb{K}))$ en $\mathbb{K}$

Una àlgebra de divisió normada de dimensió n proporciona una representació $n-$dimensional de $\mathit{Cliff}(n-1)$

- Taula anterior: $n = 1, 2, 4, 8$
- Periodicitat de Bott: representacions irreductibles de $\mathit{Cliff}(n+8)$ s'obtenen tensorialitzant les de $\mathit{Cliff}(n)$ per $\mathbb{R}^{16}$ i, per tant, la dimensió es multiplica per 16

  Si $n > 8$, aleshores les representacions irreductibles de $\mathit{Cliff}(n-1)$ tenen dimensió més gran que n

El teorema de Hurwitz

- Les àlgebres de divisió normades només són possibles en dimensió 1,2,4,8
- $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$ són àlgebres de divisió normades d'aquestes dimensions
- Unicitat? Aprofundir en la relació amb la construcció de Cayley-Dickson

El teorema de Hurwitz. Unicitat

Suposem que $\mathbb{K}$ és una àlgebra de divisió normada

- Existeix un únic operador lineal $* : \mathbb{K} \to \mathbb{K}$ tal que $1^* = 1$ i $a^* = -a$ per a tot $a \in \mathrm{Im}(\mathbb{K})$
- Es prova que $\mathbb{K}$ és una $*-$àlgebra ben normada
- $\mathbb{K}_0$ subàlgebra de $\mathbb{K}$, és ben normada
- $\mathbb{K}_0 \neq \mathbb{K}$, element $i \in \mathbb{K}$ ortogonal a $\mathbb{K}_0$
- Podem suposar $||i|| = 1$. Ortogonal a $1 \in \mathbb{K}_0 \Rightarrow i \in \mathrm{Im}(\mathbb{K})$
- Per la definició de $*$ es té $i^* = -i$
- Com abans (ortogonal i antiadjunt), $i^2 = -1$
- Es prova
  $a(ia') = i(a^*a') \quad (ai)a' = (aa'^*)i \quad (ia)(a'i^{-1}) = (aa')^*$

Subàlgebra $\langle \mathbb{K}_0, i \rangle$ isomorfa com a $*-$àlgebra a $\mathbb{K}'_0$

El teorema de Hurwitz. Unicitat

Podem trobar un cadena de subàlgebres

$$\mathbb{K}_0 = \mathbb{R} \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_n = \mathbb{K}$$

tal que $\mathbb{K}_{i+1} = \mathbb{K}_i'$

Les úniques àlgebres de divisió normades són $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$
Àlgebres de Hurwitz

Rellevància dels octonions

Geometria: el 1925 Élie Cartan va descriure la trialitat, la simetria entre vectors i espinors a l'espai euclidià de dimensió 8

Física: On an algebraic generalization of the quantum mechanical formalism Pascual Jordan, John von Neumann, Eugene Wigner. Ann. Math. 35 (1934)

Els octonions expliquen algunes característiques curioses de la teoria de cordes.
Supersymmetry and the division algebras.
T. Kugo, P.-K. Townsend. Nucl. Phys. B 221 (1983)

Rellevància dels octonions

Els octonions connecten estructures algebraiques que sinó apareixen com a excepcions aïllades i inexplicables

Les àlgebres de Lie simples es presenten en 3 famílies infinites d'àlgebres *clàssiques*, que provenen dels grups d'isometries dels espais projectius $\mathbb{P}^n(\mathbb{R}), \mathbb{P}^n(\mathbb{C}), \mathbb{P}^n(\mathbb{H})$

A més hi ha 5 àlgebres de Lie simples *excepcionals*:

4 d'elles provenen dels grups d'isometria dels plans projectius sobre $\mathbb{O}, \mathbb{O} \otimes \mathbb{C}, \mathbb{O} \otimes \mathbb{H}, \mathbb{O} \otimes \mathbb{O}$.

La que resta és el grup d'automorfismes de $\mathbb{O}$

Rellevància dels octonions

Àlgebra de Jordan formalment real és una àlgebra commutativa i de potències associatives tal que

$$a_1^2 + \cdots + a_n^2 = 0 \Rightarrow a_1 = \cdots = a_n = 0$$

Les matrius hermítiques sobre les $\mathbb{R}, \mathbb{C}, \mathbb{H}$ tenen estructura d'àlgebra de Jordan amb el producte $x \odot y = (xy + yx)/2$

- 3 famílies infites d'àlgebres simples: $\mathfrak{h}_n(\mathbb{R}), \mathfrak{h}_n(\mathbb{C}), \mathfrak{h}_n(\mathbb{H})$
- La quarta família és $\mathbb{R}^n \oplus \mathbb{R}$ amb el producte $(v, \alpha) \odot (w, \beta) = (\alpha w + \beta v, < v, w > + \alpha\beta)$
- L'àlgebra de Jordan excepcional és l'àlgebra de matrius 3×3 octoniòniques hermítiques, també amb $x \odot y = (xy + yx)/2$

Rellevància dels octonions

Successió d'àlgebres de Jordan simples

$$\mathfrak{h}_3(\mathbb{R}) \to \mathfrak{h}_3(\mathbb{C}) \to \mathfrak{h}_3(\mathbb{H}) \to \mathfrak{h}_3(\mathbb{O})$$

de dimensions $6, 9, 15, 27$.
En mecànica quàntica els *observables* sovint es descriuen mitjançant elements de $\mathfrak{h}_3(\mathbb{C})$
Una projecció en una àlgebra de Jordan formalment real és un element p tal que $p^2 = p$. En el cas $\mathfrak{h}_3(\mathbb{C})$, corresponen a les matrius amb valors propis $0, 1$ i s'usen per descriure observables que prenen només dos valors
Les projeccions de les àlgebres de Jordan es poden tractar com a proposicions de "lògica quàntica"

$p \Rightarrow q$ si $q - p$ és una suma de quadrats

La construcció de Tits

A àlgebra de Hurwitz. J una de les 4 àlgebres de Jordan $\mathfrak{h}_3$
Siguin A_0 i J_0 els respectius conjunts d'elements de traça zero

$$a \bullet b = ab - \frac{1}{2}t(ab) \qquad X \bullet Y = XY - \frac{1}{3}t(XY)$$

Definim

$$L = Der(A) \oplus (A_0 \otimes J_0) \oplus Der(J)$$

amb la multiplicació que coincideix amb els commutadors sobre $Der(A)$ i $Der(J)$ i satisfà $[Der(A), Der(J)] = 0$

$$[a \otimes X, D] = aD \otimes X \qquad [a \otimes X, E] = a \otimes XE$$

$$[a \otimes X, b \otimes Y] = \frac{1}{12}t(XY)D_{a,b} + (a \bullet b) \otimes (X \bullet Y) + \frac{1}{2}t(ab)D_{X,Y}$$

on R, L indiquen la multiplicació per la dreta,esquerra i

$$D_{a,b} = R_{[a,b]} - L_{[a,b]} - 3[L_a, R_b] \quad D_{X,Y} = [R_X, R_Y]$$

La construcció de Tits

L'àlgebra L així construïda és una àlgebra de Lie

Si $A = \mathbb{O}$ i $J = \mathbb{R}, \mathfrak{h}_3(\mathbb{R}), \mathfrak{h}_3(\mathbb{C}), \mathfrak{h}_3(\mathbb{H}), \mathfrak{h}_3(\mathbb{O})$ s'obtenen les 5 àlgebres de Lie simples excepcionals

$$\mathbf{G}_2, \mathbf{F}_4, \mathbf{E}_6, \mathbf{E}_7, \mathbf{E}_8$$

de dimensions 14, 52, 78, 133, 248

Rellevància dels octonions

Les projeccions de $\mathfrak{h}_n(\mathbb{C})$ corresponen a subspais de $\mathbb{C}^n$

Rang d'una projecció: longitud de la cadena més llarga

$$0 = p_0 < p_1 < \cdots < p_i = p$$

Construcció de l'espai projectiu: els punts són les projeccions de rang 1, les rectes són les projeccions de rang 2, la relació d'incidència donada per l'ordre de l'àlgebra de Jordan

- Amb $\mathfrak{h}_n(\mathbb{R}), \mathfrak{h}_n(\mathbb{C}), \mathfrak{h}_n(\mathbb{H})$ i $n \geq 2$ s'obtenen els espais projectius $\mathbb{P}^n(\mathbb{R}), \mathbb{P}^n(\mathbb{C}), \mathbb{P}^n(\mathbb{H})$
- Amb $\mathbb{R}^n \otimes \mathbb{R}$ i $n \geq 2$ s'obté una sèrie d'espais projectius 1-dimensionals relacionats amb la geometria Lorentziana
- Jordan (1949): Amb $\mathfrak{h}_3(\mathbb{O})$ s'obté un pla projectiu $\mathbb{P}^2(\mathbb{O})$

Rellevància dels octonions

El pla projectiu sobre $\mathbb{O}$ no satisfà el teorema de Desargues
Ruth Moufang
Alternativ körper und der Satz vom vollständigen Vierseit
Abh. Math. Sem. Hamburg 9 (1933)

Moufang loops, isotopies, geometria 8-dimensional, SO_8, companys,...

I l'aritmètica?

Què són els quaternions $a + bi + cj + dk$ **enters**?

Enters de Lipschitz: $a, b, c, d \in \mathbb{Z}$

Enters de Hurwitz: $a, b, c, d \in \mathbb{Z}$ o $a, b, c, d \in \mathbb{Z} + \frac{1}{2}$

Divisió euclidiana $Z = Qz + R$ imitant la dels enters de Gauss:

- $q = Zz^{-1} = a + bi + cj + dk$
- A, B, C, D enters més propers
  $Q = A + Bi + Cj + Dk, \quad R = Z - Qz$

$$N(Rz^{-1}) = (a-A)^2 + (b-B)^2 + (c-C)^2 + (d-D)^2 \leq 4\left(\frac{1}{2}\right)^2 = 1$$

Enters quaterniònics

S'obté $N(R) \leq N(z)$ però no la desigualtat estricta !

Igualtat: $|a - A| = |b - B| = |c - C| = |d - D| = \frac{1}{2}$

Llavors, q enter i $Z = qz + 0$

Unitats de Hurwitz: enters de norma 1. N'hi ha 24

$$\pm 1, \pm i, \pm j, \pm k, \pm\frac{1}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}k$$

Primers: enters de norma un primer

Enters primitius: No divisibles per cap natural $n > 1$

Factorització quaterniònica

Teorema (Cas primitiu). Per a cada factorització de $N(Q) = p_0 p_1 \dots p_k$, hi ha una factorització

$$Q = P_0 P_1 \dots P_k$$

amb $N(P_i) = p_i$.

Factorització modelada

Una altra factorització modelada per la mateixa factorització de la norma serà de la forma

$$Q = P_0 U_1 \cdot U_1^{-1} P_1 U_2 \dots U_k^{-1} P_k$$

Factorització única llevat migració d'unitats

Un quaternió de norma 60 té 165888 factoritzacions

Factorització quaterniònica

Teorema (Cas no primitiu) Si Q té norma $2^{n_0}p_1^{n_1}\dots p_k^{n_k}$ i és exactament divisible per $2^{s_0}p_1^{s_1}\dots p_k^{s_k}$, el nombre de factoritzacions de Q (comptades mòdul migració d'unitats) modelades per aquesta factorització de la norma és

$$\prod_{i\geq 1} C_{n_i,s_i}(p_i)$$

on C_{n_i,s_i} són els polinomis de Catalan truncats

$$C_{n,s}(p) = C_{n-1,s}(p) + pC_{n-1,s-1}(p)$$

Què són els octonions enters?

Enter significa "pertanyent a un ordre maximal". Arrel d'un polinomi mònic a coeficients enters.
El polinomi mínim d'un octonió $a_0 + a_1e_1 + \dots a_7e_7$ és

$$x^2 - 2a_0x + (a_0^2 + a_1^2 + \dots a_7^2)$$

La traça i la norma han d'ésser enteres

L'ordre de Coxeter R

Integral Cayley numbers. Duke Math. J. 13(1946) 567-578

R és un ordre maximal en la $\mathbb{Q}-$àlgebra $\mathbb{O}_{\mathbb{Q}}$ dels octonions, únic a menys de Aut($\mathbb{O}_{\mathbb{Q}}$) amb la propietat que R/pR és una $\mathbb{F}_p-$àlgebra octoniònica per a tot primer p

L'ordre R

1-conjunts

1672	1235	0467	5034
0713	1346	2570	6245
0124	1457	3602	7356
$\emptyset$	0561	4723	Ω

Enters R: $\{i \mid a_i \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}\}$ és un 1−conjunt

Els enters de Graves M són els de coordenades enteres.
$R/M \simeq (\mathbb{Z}/2\mathbb{Z})^4$ amb base

$$\tfrac{1}{2}(1+e_1+e_2+e_4) \quad \tfrac{1}{2}(1+e_1+e_3+e_7)$$
$$\tfrac{1}{2}(1+e_1+e_5+e_6) \quad \tfrac{1}{2}(e_1+e_2+e_3+e_5)$$

Embeddings into the integral octonions

Noam Elkies, Benedict H. Gross
Pacific Journal of Mathematics, 181 (1997) 147–158

"Our interest in octonions dates from a lecture that Serre gave at Harvard on the subject, in the fall of 1990"

K cos quadràtic imaginari, A anell d'enters, D discriminant,
$\varepsilon : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$ caràcter de Dirichlet de K

Teorema El nombre d'immersions de A en R és $-252\,L(\varepsilon, -2)$

2 proves: una usa sèries theta i sèries d'Eisenstein de pes semi-enter, la segona usa la teoria de mesures de Tamagawa desenvolupada per Siegel i Weil

Embeddings into the integral octonions

K una $\mathbb{Q}-$àlgebra de quaternions definida, A un ordre maximal, S el conjunt de primers que ramifiquen en K (és a dir, $K \otimes Q_p$ és àlgebra de divisió sobre $\mathbb{Q}_p$)
Teorema El nombre d'immersions de A en R és

$$504 \prod_{p \in S} (p^2 - 1)$$

Generalitzen resultats de Hasse i Eichler sobre immersions d'anells d'enters de cossos quadràtics imaginaris en certs ordres d'àlgebres de quaternions racionals

Referències


John H. Conway, Derek A. Smith
On quaternions and octonions
AKPeters (2003)


John C. Baez
The Octonions
Bull. Amer. Math. Soc. 39 (2002) 145–205

Further Reading

- Helena Albuquerque, Shahn Majid
  Quasi algebra structure of the octonions
  J. Algebra, 220 (1999) 188-224
- Florin Panaite, Freddy Van Oystaeyen
  Quasi-Hopf algebras and representations of octonions and other quasialgebras
  Journal of Mathematical Physics, 45 (2004) 3912-3929
- Jamil Daboul, Robert Delbourgo
  Matrix representation of octonions and generalizations
  Journal of Mathematical Physics, 40 (1999) 4134-4150
- Paolo Budinich
  From the Geometry of Pure Spinors with their Division Algebras to Fermion Physics
  Foundations of Physics, 32 (2002) 1347-1398

Further Reading

- Pilar Benito, Cristina Draper, Alberto Elduque
  Models of the octonions and G_2
  Linear Algebra and its Applications, 371 (2003) 333-359

I en acabat, que cadascú es vesteixi
com bonament li plagui, i via fora!,
que tot està per fer i tot és possible.

DIVERTIMENTS ANALÍTICS-ARITMÈTICS

JOSEP GONZÁLEZ ROVIRA

Resum

Sigui $X_0^+(p)$ la corba modular $X_0(p)/\langle W_p\rangle$, on W_p és la involució d'Atkin-Lehner i p is un nombre primer. Sigui g^+ el gènere de $X_0^+(p)$. Denotem per $\mathcal{S}$ el conjunt de primers racionals

$$\{p : X_0^+(p)(\mathbb{Q})\backslash\{\infty\} \text{ conté almenys un punt sense CM}\}.$$

El conjunt $\mathcal{S}$ és la unió disjunta del conjunts finits $\mathcal{S}_i := \{p \in \mathcal{S} : g^+ = i\}$. Per a $i \leq 1$, $\mathcal{S}_i$ conté tots els primers p tal que $g^+ = i$. Així,

$$\begin{aligned}\mathcal{S}_0 = &\ \{2,3,5,7,11,13,17,19,23,29,31,41,47,59,71\},\\ \mathcal{S}_1 = &\ \{37,43,53,61,79,83,89,101,131\}.\end{aligned}$$

For $i > 1$, només cinc valors $p \in \mathcal{S}_i$ són coneguts (cf. [1], [2]): $\{73,103,191\} \subseteq \mathcal{S}_2$ i $\{137,311\} \subseteq \mathcal{S}_4$. Sabem que quan $p \neq 3$, els j-invariants d'aquestes corbes el·líptiques ($\mathbb{Q}$-corbes quadràtiques de grau p) són quasi cubs (Proposició 1.2 de [3]) i que aquesta propietat és una conseqüència de propietats de l'extensió de cossos $\mathbb{Q}(X_0(p))/\mathbb{Q}(X_0^+(p))$.

En aquesta xerrada expliquem com són els *bons* factors $R \in \mathbb{Q}(X_0(p))$ tal que $j/R \in \mathbb{Q}(X_0(p))^3$ i com poden ser calculats quan $g^+ \leq 2$.

Remarca. El contingut d'aquesta xerrada va ser preparat expressament pel STNB en ocasió del 60 aniversari de la Dra P. Bayer (febrer 2006) i dos messos després es va convertir en un article ([4]).

References

[1] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21-76. Amer. Math. Soc., Providence, RI, 1998.

[2] Steven D. Galbraith. Rational points on $X_0^+(p)$. *Experiment. Math.*, 8(4):311-318, 1999.

[3] Josep González. On the j-invariants of the quadratic **Q**-curves. *J. London Math. Soc. (2)*, 63(1):52-68, 2001.

[4] Josep González. On cubic factors of j-invariants of quadratic **Q**-curves of prime degree. *Pprint*, (03-2006).

Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú,

Av. Víctor Balaguer s/n. E-08800 Vilanova i la Geltrú
E-mail address: josepg@ma4.upc.edu

Soluciones algebraicas de ecuaciones diferenciales (o la cuarta sucesión de Sloane)

Teresa Crespo

jueves 2 de febrero de 2006

Seminari de Teoria de Nombres (UB-UAB-UPC)

Facultat de Nàutica

Consideramos el siguiente problema:

"Dada una ecuación diferencial lineal con coeficientes en $\mathbb{C}(z)$, ¿cómo reconocer si todas sus soluciones son funciones algebraicas sobre $\mathbb{C}(z)$?"

Esta cuestión fué planteada por Fuchs y Schwarz y retomada por Klein en su libro del icosaedro [K1]. En su artículo sobre las ecuaciones hipergeométricas de Gauss [S], Schwarz da una respuesta completa a esta pregunta para este tipo de ecuaciones diferenciales.

1. Función hipergeométrica de Gauss

Para $a, b, c \in \mathbb{R}$, $c \notin \mathbb{Z}_{\leq 0}$, se define la *función hipergeométrica de Gauss* por

$$F(a,b,c;z) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n n!} z^n \tag{1}$$

donde el símbolo de Pochhammer $(x)_n$ se define por

$(x)_0 = 1$

$(x)_n = x(x+1)\dots(x+n-1)$.

El radio de convergencia de (1) es 1 salvo si a o b son enteros no positivos y en este caso tenemos un polinomio. En particular

$$P_n(z) = \frac{1}{n!}\frac{d^n}{dz^n}(1-z^2)^n = 2^n F(-n, n+1, 1; \frac{1+z}{2})$$

son los polinomios de Legendre;

$$T_n(z) = (-1)^n F(-n, n, \frac{1}{2}; \frac{1+z}{2})$$

es el polinomio de Chebyshev definido por $T_n(\cos z) = \cos(nz)$.

La función hipergeométrica de Gauss (1) admite prolongación analítica mediante su representación por la integral de Euler

$$F(a,b,c;z) = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \int_0^1 t^{b-1}(1-t)^{c-b-1}(1-tz)^{-a}\, dt.$$

Las funciones hipergeométricas aparecen también en la determinación de los periodos de la red del plano complejo asociada a una curva elíptica. Concretamente

$$\omega_1(\lambda) = \int_{-\infty}^{0} \frac{dx}{\sqrt{x(x-1)(x-\lambda)}} = i\pi F(\frac{1}{2}, \frac{1}{2}, 1; 1-\lambda),$$
$$\omega_2(\lambda) = \int_{1}^{\infty} \frac{dx}{\sqrt{x(x-1)(x-\lambda)}} = \pi F(\frac{1}{2}, \frac{1}{2}, 1; \lambda),$$

son los periodos de la curva elíptica $y^2 = x(x-1)(x-\lambda)$, con λ número complejo cumpliendo $|\lambda| < 1, |\lambda - 1| < 1$ (ver [H]).

Puede comprobarse fácilmente que la función hipergeométrica de Gauss $F(a, b, c; z)$ es solución de la ecuación diferencial

$$Y'' + \frac{(a+b+1)z - c}{z(z-1)}\, Y' + \frac{ab}{z(z-1)}\, Y = 0 \tag{2}$$

Vemos ahora algunas cuestiones de ecuaciones diferenciales lineales definidas sobre el cuerpo $\mathbb{C}(z)$.

2. Ecuaciones diferenciales fuchsianas

2.1 Singularidades regulares

Para una ecuación diferencial

$$Y^{(n)} + a_1(z)\, Y^{(n-1)} + \cdots + a_{n-1}(z)\, Y' + a_n(z)\, Y = 0 \tag{3}$$

con $a_i(z) \in \mathbb{C}(z)$, un punto P de $\mathbb{P}^1(\mathbb{C})$ se llama regular si las funciones a_i no tienen polo en P. Si $P \in \mathbb{C}$ (resp. $P = \infty$) es punto singular, consideramos el límite $\lim_{z\to P}(z-P)^i a_i(z)$ (resp. $\lim_{z\to\infty} z^i a_i(z)$). Si este límite existe y es finito para $i = 1, \ldots, n$, el punto P es *singularidad regular*.

La ecuación (3) se llama *Fuchsiana* si todos los puntos de $\mathbb{P}^1(\mathbb{C})$ son regulares o singularidades regulares.

Suponemos ahora que 0 es un punto singular regular de la ecuación (3). Escribimos la ecuación en términos del operador diferencial $D = z\dfrac{d}{dz}$. A partir de la igualdad de operadores $\dfrac{d^r}{dz^r} \cdot z = r\dfrac{d^{r-1}}{dz^{r-1}} + z\dfrac{d^r}{dz^r}$, para $r \geq 1$, puede probarse por recurrencia

$$z^r \frac{d^r}{dz^r} = D(D-1)\cdots(D-r+1). \tag{4}$$

Multiplicando (3) por z^n i usando (4), la ecuación queda en la forma

$$F(D, z)(Y) := D^n Y + b_1(z) D^{n-1} Y + \cdots + b_{n-1} DY + b_n(z) Y = 0. \tag{5}$$

La condición de singularidad regular implica que las funciones $b_i(z)$ son holomorfas en el entorno de $z = 0$.

2.2 Soluciones formales en series de potencias

Teorema 1 (de Cauchy)**.** *Supongamos que* 0 *es un punto regular de (3), entonces existen n series de Taylor en z,* $f_1, \ldots, f_n$ *, soluciones de (3), linealmente independientes sobre* $\mathbb{C}$*, con radio de convergencia positivo. Además, toda serie de Taylor solución de (3) es combinación lineal de* $f_1, \ldots, f_n$ *con coeficientes en* $\mathbb{C}$*.*

Prueba. Buscamos una solución en serie de potencias $y = \sum_{k\geq 0} c_k z^k$. Multiplicando (3) por z^n i usando (4), obtenemos

$$D(D-1)\cdots(D-n+1)\,Y + \sum_{i=1}^{n} z^i a_i(z) D(D-1)\cdots(D-(n-i)+1)\,Y = 0.$$

Escribimos $z^i a_i(z) = \sum_{j=i}^{\infty} a_{ij} z^j$ y, para cada $j \geq 1$, ponemos $P_j(X) = \sum_{i=1}^{j} a_{ij} X(X-1)\cdots(X-(n-i)+1)$. Sustituyendo y en la ecuación, obtenemos la relación de recurrencia

$$k(k-1)\cdots(k-n+1)c_k + \sum_{j=1}^{k} P_j(k) c_{k-j} = 0.$$

Como $P_j(k-j) = 0$, para $1 \leq j \leq k < n$, la recurrencia es trivial para $k \leq n-1$. Por tanto podemos fijar $c_0, \cdots, c_{n-1}$ arbitrariamente y los coeficientes c_k con $k \geq n$ quedan fijados por la relación de recurrencia. Obtenemos pues n soluciones linealmente independientes de (3) que son base del espacio vectorial de soluciones.

Falta ver que cualquier solución en serie de potencias tiene radio de convergencia positivo. Para ello, elegimos $C > 1$ tal que $|P_j(k)| < C^j k^{n-1}$ para todo par j, k, $|c_j| < C^{2j+1}$ para $j = 0, \cdots n-1$ y $(k(k-1)\cdots(k-n+1))^{-1} < C/k^n$ para todo $k \geq n$. Probamos por inducción sobre k que $|c_k| < C^{2k+1}$. Para $k < n$, se cumple por la elección de C. De la relación de recurrencia, obtenemos la desigualdad

$$|c_k| \leq \frac{C}{k^n} \sum_{j=1}^{k} C^j k^{n-1} |c_{k-j}|.$$

Usando la hipótesis de inducción,

$$|c_k| \leq \frac{C}{k^n} k^{n-1} \sum_{j=1}^{k} C^j \cdot C^{2(k-j)+1} < C^{2k+1}.$$

Por tanto, los coeficientes c_k están acotados exponencialmente y la serie de potencias tiene radio de convergencia positivo. $\square$

2.3 Soluciones formales en puntos singulares regulares

Suponemos ahora que 0 es un punto singular regular de la ecuación (3). Buscamos soluciones de la forma

$$y = z^\rho \sum_{k\geq 0} c_k z^k. \tag{6}$$

Desarrollamos los coeficientes de (5) en serie de Taylor, $b_i(z) = \sum_{j=0}^{\infty} b_{ij} z^j$ y ponemos

$$\left\{ \begin{array}{lcl} F_0(D) & = & D^n + b_{10}D^{n-1} + b_{20}D^{n-2} + \cdots + b_{n0} \\ F_j(D) & = & b_{1j}D^{n-1} + b_{2j}D^{n-2} + \cdots + b_{nj} \quad \text{para} \quad j > 0. \end{array} \right.$$

La ecuación se escribe entonces

$$F(D,z)(Y) = \sum_{j=0}^{\infty} z^j F_j(D)(Y) = 0$$

y sustituyendo y, obtenemos

$$\begin{array}{rcl} F(D,z)(y) & = & \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} z^j F_j(D)(c_i z^{\rho+i}) \\ & = & \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} z^{\rho+i+j} F_j(\rho+i) c_i \\ & = & \sum_{k=0}^{\infty} z^{\rho+k} \left[\sum_{i=0}^{k} F_{k-i}(\rho+i) c_i \right] = 0. \end{array}$$

Esta expresión se anula idénticamente si los coeficientes c_i cumplen las relaciones

$$\sum_{i=0}^{k} F_{k-i}(\rho+i) c_i = 0 \quad (k \geq 0). \tag{7}$$

En particular, para obtener $c_0 \neq 0$, ρ debe ser raíz de la ecuación polinomial

$$F_0(X) = X^n + b_{10}X^{n-1} + \cdots + b_{n0} = X^n + b_1(0)X^{n-1} + \cdots + b_n(0) = 0.$$

Esta ecuación se llama *ecuación indicial*, sus raíces se llaman *exponentes locales* en el punto singular $z = 0$.

A partir de (4), se obtiene que la ecuación indicial en un punto $P \in \mathbb{C}$, regular o singularidad regular, en términos de los coeficientes de (3) es

$$X(X-1)\cdots(X-n+1)$$
$$+\sum_{k=1}^{n} lim_{z\to P}(z-P)^k a_k(z)X\cdots(X-n+k+1)$$
$$+ lim_{z\to P}(z-P)^n a_n(z)=0.$$

Si ∞ es punto regular o singularidad regular, la ecuación indicial en ∞ es

$$X(X+1)\cdots(X+n-1)$$
$$+\sum_{k=1}^{n}(-1)^k lim_{z\to\infty} z^k a_k(z)X\cdots(X+n-k-1)$$
$$+(-1)^n lim_{z\to\infty} z^n a_n(z)=0.$$

Los exponentes locales satisfacen la

Relación de Fuchs. *Si $\rho_1(P),\rho_2(P),\cdots,\rho_n(P)$ son los exponentes locales en un punto $P\in\mathbb{P}^1$, se cumple*

$$\sum_{P\in\mathbb{P}^1}(\rho_1(P)+\rho_2(P)+\cdots+\rho_n(P)-\binom{n}{2})=-2\binom{n}{2}.$$

Teniendo en cuenta que en un punto regular, los exponentes locales son $0,1,\cdots,n-1$, tenemos que la suma es de hecho finita.

Ahora, si dos soluciones independientes corresponden al mismo exponente ρ, restándolas obtenemos otra solución correspondiente a otro exponente mayor ρ' que también debe cumplir la ecuación indicial. Por tanto, cada exponente local da lugar a lo sumo a una solución en serie de potencias de la forma (6) .

Si $F_0(\rho)=0$, $F_0(\rho+k)\neq 0$ para todo entero positivo k, podemos elegir $c_0\neq 0$ y cada uno de los coeficientes c_k siguientes queda unívocamente determinado por las relaciones (7). Pero, si ρ y $\rho+k$ son ambos exponentes locales, con k entero positivo, la relación $\sum_{i=0}^{k} F_{k-i}(\rho+i)c_i=0$ puede ser incompatible.

Siempre que no tengamos un sistema completo de soluciones de la forma (6), por tener la ecuación indicial raíces múltiples o raíces que difieren en un entero, esta escasez puede suplirse con soluciones en que aparecen logaritmos.

Distribuimos los exponentes locales en conjuntos, cada uno de ellos formado por exponentes locales que difieren en un entero. Vemos ahora como calcular las soluciones correspondientes a uno de estos conjuntos, formado por h exponentes locales distintos ρ_i con multiplicidades r_i, ordenados con parte real ascendiente. Buscamos soluciones del tipo

$$y=z^\rho\sum_{k\geq 0}u_k z^k. \tag{8}$$

donde los u_k son polinomios en $t:=\log z$ de grado menor que n. Teniendo en cuenta $D(u_i)=\dfrac{du_i}{dt}$, obtenemos

$$\begin{aligned} F(D,z)(y) &= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} z^j F_j(D)(z^{\rho+i}u_i) \\ &= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} z^{\rho+i+j} F_j(D+\rho+i)u_i \\ &= \sum_{k=0}^{\infty} z^{\rho+k}\left[\sum_{i=0}^{k} F_{k-i}(D+\rho+i)u_i\right] = 0, \end{aligned}$$

que se anula idénticamente si las u_i cumplen las relaciones

$$\sum_{i=0}^{k} F_{k-i}(D+\rho+i)u_i = 0 \quad (k \geq 0).$$

Esto puede verse como un sistema de ecuaciones diferenciales lineales en la variable $t = \log z$, del cual nos interesa la solución más general en polinomios. La primera ecuación puede escribirse

$$F_0(D+\rho)(u_0) = F_0(\rho)u_0 + \frac{1}{1!}F_0'(\rho)Du_0 + \frac{1}{2!}F_0''(\rho)D^2u_0 + \cdots = 0,$$

y es la ecuación indicial generalizada. Si u_0 es un polinomio en t, no idénticamente 0, esta expresión es un polinomio del mismo grado salvo si $F_0(\rho) = 0$. Para obtener efectivamente una solución, ρ debe pues satisfacer la ecuación indicial. Para $\rho = \rho_1$, tenemos $F_0(D+\rho_1)(u_0) = G_1(D)(D^{r_1}u_0)$ con $G_1(0) \neq 0$, y por tanto, u_0 debe cumplir la ecuación $D^{r_1}u_0 = 0$.

Supongamos hallados los polinomios $u_0, u_1, \cdots, u_{k-1}$. Si $F_0(\rho_1 + k) \neq 0$, u_k queda unívocamente determinado como un polinomio cuyo grado no excede el de los anteriores por la fórmula simbólica

$$\begin{aligned} u_k &= -\frac{1}{F_0(D+\rho_1+k)}\sum_{i=0}^{k-1} F_{k-i}(D+\rho_1+i)(u_i) \\ &= -(A_0 + A_1D + A_2D^2 + \cdots)\sum_{i=0}^{k-1} F_{k-i}(D+\rho_1+i)u_i \qquad (9) \\ &= L_k(u_0, u_1, \cdots, u_{k-1}). \end{aligned}$$

Pero si $k = \rho_i - \rho_1$, tenemos $F_0(D+\rho_1+k) = F_0(D+\rho_i) = G_i(D)D^{r_i}$, con $G_i(0) \neq 0$ y por tanto, en vez de (9), tenemos la relación

$$D^{r_i}u_{\rho_i-\rho_1} = L_k(u_0, u_1, \cdots, u_{k-1}), \quad \text{con} \quad k = \rho_i - \rho_1.$$

La estructura de la solución queda completamente determinada por $u_0, \cdots, u_{\rho_h-\rho_1}$ ya que los u_k restantes quedan determinados por una relación del tipo (9). Podemos distinguir los h polinomios críticos $U_i := u_{\rho_i-\rho_1}$ y expresar los restantes explícitamente en la forma

$$u_k = \Lambda_k(U_1, U_2, \cdots, U_h)$$

donde los U_i satisfacen un sistema de ecuaciones de la forma

$$\left\{\begin{array}{rcl} D^{r_1}U_1 & = & 0 \\ f_{21}(D)U_1 + D^{r_2}U_2 & = & 0 \\ f_{31}(D)U_1 + f_{32}(D)U_2 + D^{r_3}U_3 & = & 0 \\ \cdots & & \end{array}\right. .$$

Obtenemos pues $\sum_{i=1}^{h} r_i$ soluciones linealmente independientes. Puede probarse que tienen radio de convergencia positivo (ver [P]).

Observación. Una ecuación diferencial lineal homogénea que sea ecuación de Fuchs con tres puntos singulares queda determinada por sus puntos singulares y los exponentes locales en cada punto singular.

2.4 Grupo de monodromía

Toda solución analítica de (3) en el entorno de un punto regular puede prolongarse analíticamente a lo largo de todo camino en $\mathbb{C}$ que no pase por ningún punto singular. Sea S el conjunto de singularidades de (3), $z_0 \in \mathbb{P}^1 \setminus S$. Sean $f_1, \ldots, f_n$ soluciones analíticas independientes en el entorno de z_0. Sea $\gamma \in \pi_1(\mathbb{P}^1 \setminus S, z_0)$. Por prolongación analítica a lo largo de γ, obtenemos $\widetilde{f}_1, \ldots, \widetilde{f}_n$ que son de nuevo soluciones de (3). Se tiene por tanto una matriz $M(\gamma) \in \mathrm{GL}(n, \mathbb{C})$ tal que

$$\begin{pmatrix} \widetilde{f}_1 \\ \vdots \\ \widetilde{f}_n \end{pmatrix} = M(\gamma) \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}.$$

La aplicación

$$\begin{array}{rccc} \rho: & \pi(\mathbb{P}^1 \setminus S) & \to & \mathrm{GL}(n, \mathbb{C}) \\ & \gamma & \mapsto & M(\gamma) \end{array}$$

es un morfismo de grupos. Su imagen se llama *grupo de monodromía* de (3). El *grupo de monodromía proyectivo* es el grupo de monodromía módulo escalares, es decir la imagen del grupo de monodromía por el epimorfismo $\mathrm{GL}(n, \mathbb{C}) \twoheadrightarrow \mathrm{PGL}(n, \mathbb{C})$.

Para la ecuación diferencial (3), una extensión de Picard-Vessiot es un cuerpo diferencial K con cuerpo de constantes $\mathbb{C}$, generado diferenciablemente sobre $\mathbb{C}(z)$ por un sistema fundamental de soluciones de (3). El grupo de Galois diferencial de (3) es el grupo $\mathbf{G}$ de automorfismos diferenciales de K sobre $\mathbb{C}(z)$. El grupo $\mathbf{G}$ es un grupo algebraico, subgrupo del grupo lineal $\mathrm{GL}(n, \mathbb{C})$. Para una ecuación diferencial fuchsiana, el grupo de Galois diferencial $\mathbf{G}$ es la clausura de Zariski del grupo de monodromía. Por tanto,

el tener un sistema fundamental de soluciones contenido en una extensión algebraica de $\mathbb{C}(z)$ equivale a la finitud del grupo de monodromía. Teniendo en cuenta que el subcuerpo de K generado diferenciablemente sobre $\mathbb{C}(z)$ por el determinante wronskiano de un sistema fundamental de soluciones es el cuerpo fijo por el subgrupo del grupo de Galois diferencial $\mathbf{G}$ formado por las matrices del grupo especial lineal $\mathrm{SL}(n,\mathbb{C})$, se tiene que el grupo de monodromía es finito si y sólo si lo es el grupo de monodromía proyectivo y el wronskiano es algebraico sobre $\mathbb{C}(z)$.

2.5 La ecuación hipergeométrica

La ecuación hipergeométrica (2) tiene tres puntos singulares $0, 1, \infty$ que son singularidades regulares. Escribimos los exponentes locales en el esquema de Riemann:

$$\begin{array}{ccc} 0 & 1 & \infty \\ \hline 0 & 0 & a \\ 1-c & c-a-b & b \end{array} \tag{10}$$

Sea P un punto regular de (2). Con origen en P, trazamos tres bucles en el plano complejo g_0, g_1, g_∞, alrededor de $0, 1, \infty$, respectivamente, con $g_0 g_1 g_\infty = 1$. Las correspondientes matrices de monodromía M_0, M_1, M_∞ cumplen $M_0 M_1 M_\infty = 1$ y M_0, M_∞ generan el grupo de monodromía.

A partir de los valores de los exponentes locales dados en el esquema de Riemann (10), tenemos que los valores propios de M_0 son $1, e^{2\pi i(1-c)}$, los de M_1, $1, e^{2\pi i(c-a-b)}$ y los de M_∞, $e^{2\pi i a}, e^{2\pi i b}$.

Observación: Toda ecuación fuchsiana de orden 2 con tres puntos singulares puede transformarse en una ecuación hipergeométrica mediante

-una transformación de Möbius $S(z) = \dfrac{az+b}{cz+d}, ad-bc \neq 0$ que envíe los puntos singulares a $0, 1, \infty$. Obtenemos entonces una ecuación con esquema de Riemann de la forma

$$\begin{array}{ccc} 0 & 1 & \infty \\ \hline \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \end{array}$$

donde $\alpha + \beta + \gamma + \alpha' + \beta' + \gamma' = 1$ por la relación de Fuchs.

-multiplicación de las soluciones por $z^{-\alpha}(1-z)^{-\beta}$. El esquema de Riemann obtenido corresponde a una ecuación hipergeométrica con parámetros adecuados.

3. Soluciones algebraicas

Sean f, g dos soluciones independientes de la ecuación hipergeométrica en un entorno de z_0. El cociente $D(z) = f/g$ considerado como aplicación de $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$ en $\mathbb{P}^1$ se llama aplicación de Schwarz y tenemos

Teorema 2 (de Schwarz)**.** *Sea* $\lambda = |1-c|, \mu = |c-a-b|, \nu = |a-b|$ *y supongamos* $0 \leq \lambda, \mu, \nu < 1$*. Entonces* $D(z)$ *aplica* $\mathbb{H} \cup \mathbb{R}$ *biyectivamente en un triángulo curvilíneo de vértices* $D(0), D(1), D(\infty)$ *con ángulos* $\lambda\pi, \mu\pi, \nu\pi$*.*

El grupo de monodromía proyectivo describe el comportamiento del cociente f/g de las dos soluciones de la base cuando éstas se prolongan a lo largo de un camino de $\pi(\mathbb{P}^1 \setminus S)$. Se obtiene en la forma siguiente. Sea W el grupo generado por las reflexiones respecto de una arista del triángulo curvilíneo. El grupo de monodromía proyectivo es el subgrupo de W formado por los elementos que son producto de un número par de reflexiones. A partir de las triangulaciones de la esfera, se obtienen todos los posibles valores λ, μ, ν que corresponden a ecuaciones con todas las soluciones algebraicas. Estos valores, junto con los correspondientes grupos de monodromía proyectivos, son los que aparecen en la llamada *Lista de Schwarz* [S]. Posteriormente, haciendo cociente por la relación de equivalencia proyectiva, Klein [K2] obtiene la llamada *Lista básica de Schwarz*. Decimos que dos operadores diferenciales L y L' son *proyectivamente equivalentes* si, en cualquier punto de $\mathbb{P}^1$, todo cociente de dos soluciones independientes de L es tambien cociente de soluciones independientes de L'. Reproducimos a continuación la lista básica de Schwarz.

(λ, μ, ν)	=	$(1, 1/n, 1/n)$	da grupo	cíclico	de orden	n
	=	$(1/2, 1/2, 1/n)$	da grupo	diedro	de orden	2n
	=	$(1/2, 1/3, 1/3)$	da grupo	tetraédrico	de orden	12
	=	$(1/2, 1/3, 1/4)$	da grupo	octaédrico	de orden	24
	=	$(1/2, 1/3, 1/5)$	da grupo	icosaédrico	de orden	60

En general, las ecuaciones diferenciales de orden 2 con grupo de monodromía proyectivo finito quedan caracterizadas por el siguiente teorema de Klein. Notemos que toda ecuación diferencial lineal de orden 2 es proyectivamente equivalente a una en *forma normalizada*: $Y'' + a_2(z)\, Y = 0$.

Teorema 3 (de Klein)**.** *Sea* $L(Y) = 0$ *una ecuación diferencial lineal de orden 2 en forma normalizada, con grupo de monodromía proyectivo* G *finito. Entonces existe una única ecuación hipergeométrica* $H(Y) = 0$*, con grupo de monodromía proyectivo* G *y una función racional* $f : \mathbb{P}^1 \to \mathbb{P}^1$ *tal que para todo cociente* $\tau(z)$ *de soluciones independientes de* $H(Y) = 0$*,* $\tau(f(z))$ *es cociente de soluciones independientes de* $L(Y) = 0$*. Además, la función* f *es única módulo transformaciones de Möbius que dejen* H *invariante y permuten sus puntos singulares.*

En el caso de la *ecuación de Lamé*, con parámetros $n \in \mathbb{Q}, g_2, g_3, B \in \mathbb{C}$:

$$Y'' + \frac{P'(z)}{2P(z)}\,Y' - \frac{n(n+1)z + B}{P(z)}\,Y = 0$$

donde $P(z) := 4z^3 - g_2 z - g_3$ tiene tres ceros z_1, z_2, z_3 distintos, Beukers-van der Waall [B-W] y Liţcanu [L1], completando trabajos de Baldassarri y Chiarelotto, determinan en qué casos todas las soluciones son algebraicas. En este caso, el esquema de Riemann es

z_1	z_2	z_3	∞
0	0	0	$-n/2$
$1/2$	$1/2$	$1/2$	$(n+1)/2$

Teniendo en cuenta que el determinante wronskiano W de una base del espacio de soluciones de una ecuación diferencial lineal (3) cumple $W' = -a_1 W$, obtenemos que para la ecuación de Lamé, el wronskiano siempre es una función algebraica. Beukers y van der Waall usan que el grupo de monodromía de la ecuación de Lamé es un grupo de reflexiones formado por matrices con determinante ± 1. Liţcanu usa el hecho que, para $n \notin \mathbb{Z} + \frac{1}{2}$ la función racional f en el teorema de Klein tiene a lo sumo tres puntos de ramificación y es por tanto una función de Belyi. Su método se basa en el estudio del "dessin d'enfant" asociado por la correspondencia de Grothendieck a esta función de Belyi. Las cuestiones básicas de "dessins d'enfants" pueden verse en [C-X]. Se tiene

Teorema 4. *1. Si $n \in \mathbb{Z} + \frac{1}{2}$, la ecuación de Lamé tiene soluciones algebraicas si y sólo si su grupo de monodromía proyectivo es el grupo de Klein. (Brioschi, Halphen)*

2. No hay ecuación de Lamé con grupo de monodromía proyectivo cíclico.

3. No hay ecuación de Lamé con grupo de monodromía proyectivo tetraédrico.

4. Si el grupo de monodromía proyectivo de la ecuación de Lamé es octaédrico, entonces $n \in \mathbb{Z} + \{\pm\frac{1}{4}, \pm\frac{1}{6}\}$.

5. Si el grupo de monodromía proyectivo de la ecuación de Lamé es icosaédrico, entonces $n \in \mathbb{Z} + \{\pm\frac{1}{6}, \pm\frac{1}{10}, \pm\frac{3}{10}\}$.

6. Si el grupo de monodromía proyectivo de la ecuación de Lamé es diedro, entonces $n \in \mathbb{Z}$. Si $n \in \mathbb{Z}$ y el grupo de monodromía proyectivo es finito, entonces es diedro de orden al menos 6.

En sentido contrario a los enunciados del teorema anterior, se tienen los resultados siguientes, obtenidos mediante "dessins d'enfants".
-Dados $n \in \mathbb{Z}$, $N \in \mathbb{N}$, Liţcanu (para $n = 1$) y Dahmen (para n general) obtienen una fórmula explícita para el número de ecuaciones de Lamé, módulo equivalencia proyectiva, con parámetro n y grupo de monodromía proyectivo el grupo diedro de orden $2N$ (cf. [L2], [D]).
-Para cada n en $\mathbb{Z} + \{\pm\frac{1}{4}, \pm\frac{1}{6}\}$ (resp. $\mathbb{Z} + \{\pm\frac{1}{6}, \pm\frac{1}{10}, \pm\frac{3}{10}\}$), Nakanishi construye una ecuación de Lamé con parámetro n y monodromía proyectiva octaédrica (resp. icosaédrica) (cf. [N]).

En el caso de las ecuaciones de orden 2 con 4 puntos singulares, la ecuación ya no queda determinada por los puntos singulares y los exponentes locales, es decir por datos locales, como en el caso de tres puntos singulares. En el caso de cuatro puntos, hay un parámetro (B en el caso Lamé) no determinado por datos locales. Éste se llama *parámetro accesorio* de la ecuación. Se sabe poco de cómo depende el grupo de monodromía del parámetro accesorio. En el caso de la ecuación de Lamé, pueden encontrarse condiciones sobre B para que el grupo de monodromía sea un determinado grupo finito (fijando n en el conjunto adecuado) a partir de productos simétricos de la ecuación y representaciones del grupo.

Beukers-Heckmann [B-H] determinan el grupo de monodromía para la función hipergeométrica generalizada y en particular cuando ésta es algebraica sobre $\mathbb{C}(z)$. La función hipergeométrica generalizada se define por

$$ {}_nF_{n-1}(\alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_{n-1}|z) = \sum_{k=0}^{\infty} \frac{(\alpha_1)_k \ldots (\alpha_n)_k}{(\beta_1)_k \ldots (\beta_{n-1})_k k!} z^k. $$

Es solución de una ecuación diferencial lineal de orden n con singularidades regulares en $0, 1, \infty$.

4. La sucesión de Sloane A087659

A propósito de funciones hipergeométricas generalizadas, en la Enciclopedia Digital de Sucesiones Enteras de Sloane [Sl], hallamos que

$$ a(n) = {}_3F_2(-n, \frac{n+4}{2}, \frac{n+5}{2}; 3, 2| - 4) $$

es la sucesión de Sloane A087659. Sus primeros valores son

n	**a(n)**
0	1
1	6
2	57
3	701
4	10147
5	164317
6	2888282
7	54047434
8	1062530119
9	21739192762
10	459685114665
11	9993072855135
12	222421656113435
13	5052215132332492
14	116808526607319823
15	2742986603349411311
16	65306671610636210891

y está probado que es efectivamente una sucesión entera (ver [Sl]). En la página de Sloane, pueden encontrarse otras nueve sucesiones dadas por valores de funciones hipergeométricas generalizadas, aunque no para todas ellas está probado que sean efectivamente sucesiones enteras.

5. Una conjetura de Grothendieck

Consideramos ahora una ecuación diferencial

$$L(Y) = Y^{(n)} + a_1(z)\, Y^{(n-1)} + \cdots + a_{n-1}(z)\, Y' + a_n(z)\, Y = 0,$$

con $a_i \in \mathbb{Q}(z)$. Para casi todo primo p, podemos reducir las funciones racionales $a_i(z)$ módulo p. Las reducciones $a_{i,p}$ están en $\mathbb{F}_p(z)$ y podemos considerar la ecuación diferencial

$$L_p(Y) = Y^{(n)} + a_{1,p}(z)\, Y^{(n-1)} + \cdots + a_{n-1,p}(z)\, Y' + a_{n,p}(z)\, Y = 0.$$

En los años sesenta, A. Grothendieck formuló la conjetura siguiente.

Conjetura de Grothendieck. *Los dos enunciados siguientes son equivalentes.*

1. *La ecuación $L(Y) = 0$ tiene n soluciones, algebraicas sobre $\mathbb{Q}(z)$, linealmente independientes sobre $\overline{\mathbb{Q}}$.*

2. *Para casi todo p, la ecuación $L_p(Y) = 0$ tiene n soluciones en $\mathbb{F}_p(z)$, linealmente independientes sobre $\mathbb{F}_p(z^p)$.*

Prueba de $1 \Rightarrow 2$. Sea K una extensión finita de $\mathbb{Q}(z)$ que contiene una base de soluciones $y_1, y_2, \ldots, y_n$ de $L(Y) = 0$. Sea W el wronskiano de $y_1, y_2, \ldots, y_n$. Tenemos $K = \mathbb{Q}(z)[t] = \mathbb{Q}(z)[T]/(F)$, con $F(T) = T^d + b_{d-1}T^{d-1} + \cdots + b_0$ polinomio irreducible de $\mathbb{Q}(z)[T]$ y $t = T \bmod F$. La derivación de $\mathbb{Q}(z)$ se extiende en forma única a K definiendo

$$t' = -\frac{b'_{d-1}T^{d-1} + \cdots + b'_0}{F_T(t)},$$

donde F_T indica derivada de F respecto de T. Invirtiendo F_T módulo F y reduciendo módulo F, obtenemos una expresión de t' como polinomio en t de grado $< d$ con coeficientes en $\mathbb{Q}(z)$. Consideramos ahora primos p tales que

i) $b_{d-1}, \ldots, b_0 \in \mathbb{Z}[z]_p$,

ii) el discriminante de F, respecto de T, es invertible en $\mathbb{Z}[z]_p$,

iii) $y_1, \ldots, y_n \in \mathbb{Z}[z]_p[t]$,

iv) W es un elemento invertible de $\mathbb{Z}[z]_p[t]$.

Estas condiciones excluyen un número finito de primos. Como el discriminante de F es invertible en $\mathbb{Z}[z]_p$, F_T es invertible en $\mathbb{Z}[z]_p[T]$ y por tanto $t' \in \mathbb{Z}[z]_p[t]$, es decir $\mathbb{Z}[z]_p[t]$ es invariante por diferenciación. El ideal (p) es invariante por diferenciación y por tanto $\mathbb{Z}[z]_p[t]/(p)$ es anillo diferenciable, extensión de $\mathbb{F}_p(z)$. Se tiene $\mathbb{Z}[z]_p[t]/(p) = \mathbb{F}_p(z)[T]/(\overline{F})$, para $\overline{F}$ la reducción de F módulo p. Por hipótesis, el discriminante de $\overline{F}$ es invertible y por tanto $\mathbb{Z}[z]_p[t]/(p)$ es un producto $M_1 \times \cdots \times M_s$ de cuerpos M_i, extensiones separables de $\mathbb{F}_p(z)$. Por la unicidad de la extensión de la derivación, cada M_i es subcuerpo diferencial de $\mathbb{Z}[z]_p[t]/(p)$. Sean $\overline{y}_1, \ldots, \overline{y}_n, \overline{W}$ las imágenes de $y_1, \ldots, y_n, W$ en $M = M_1$. Entonces $\overline{W}$ es el wronskiano de $\overline{y}_1, \ldots, \overline{y}_n$ y, renumerando si hace falta los M_i, tenemos que $\overline{y}_1, \ldots, \overline{y}_n$ son linealmente independientes sobre el cuerpo de constantes de M. Usando que M es separable sobre $\mathbb{F}_p(z)$, se puede probar que el cuerpo de constantes de M es M^p y que $1, z, \ldots, z^{p-1}$ es también base de M sobre M^p. Tenemos pues $M = M^p \otimes_{\mathbb{F}_p(z^p)} \mathbb{F}_p(z)$. Por tanto los espacios de soluciones en $\mathbb{F}_p(z)$ y en M de la ecuación diferencial $L_p(Y) = 0$ tienen misma dimensión. En M esta dimensión es n y por tanto también lo es en $\mathbb{F}_p(z)$. $\square$

La conjetura de Grothendieck puede verse como una generalización diferencial de un corolario del teorema de densidad de Chebotarev: Un polinomio

con coeficientes en $\mathbb{Q}$ tiene todas sus raíces en $\mathbb{Q}$ si y sólo si las raíces de su reducción módulo p están en $\mathbb{F}_p$ para casi todo p.

En la conjetura de Grothendieck, el enunciado *1.* es equivalente a que el grupo de monodromía de la ecuación sea finito. Puede darse una condición equivalente al enunciado *2.* en términos de p-curvatura. Para definir la p-curvatura es más fácil trabajar con operadores diferenciales en forma matricial.

5.1. Sistemas diferenciales y p-curvatura

Recordamos que la ecuación

$$L(Y) = Y^{(n)} + a_1(z)Y^{(n-1)} + \cdots + a_{n-1}(z)Y' + a_n(z)Y = 0,$$

equivale al sistema $Y' = AY$ con matriz $n \times n$

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & & \ddots & \\ 0 & 0 & \dots & 0 & 1 \\ -a_n & -a_{n-1} & -a_{n-2} & \dots & -a_1 \end{pmatrix}.$$

El paso de sistema matricial a ecuación se hace mediante un vector cíclico del módulo diferencial asociado al sistema . Recordemos que un *módulo diferencial* (o $\mathcal{D}$-módulo) sobre un cuerpo diferencial K con derivación d es un K-espacio vectorial de dimensión finita, que es módulo por la izquierda para el anillo $\mathcal{D} = K[d]$. A un sistema diferencial $Y' = AY$ con $A = (a_{ij})_{1 \le i,j \le n}$ definido sobre el cuerpo diferencial (K, d), podemos asociarle un módulo diferencial, el K-espacio vectorial $K^n := K \times \overset{n}{\cdot} \cdots \times K$ con la estructura de $\mathcal{D}$-módulo dada por $de_i = -\sum_j a_{ji} e_j$, para $e_1, \dots, e_n$ base canónica de K^n. Un vector del módulo diferencial K^n tal que él y sus derivados forman base se llama *vector cíclico* (ver [P-S]).

Consideramos un cuerpo K de característica p tal que $[K : K^p] = p$ (donde $K^p := \{x^p | \, x \in K\}$). Entonces $K = K^p(z)$ para algún z y definimos la derivación en K por $z' = 1$. Consideramos el operador diferencial $\partial := \dfrac{d}{dz} - A$, para A matrix $n \times n$ con coeficientes en K. El operador ∂ opera sobre el espacio vectorial K^n y es K^p-lineal. Su potencia p-ésima ∂^p es por tanto también K^p-lineal. Es fácil ver que el operador ∂^p también es K-lineal. En efecto, se tiene la igualdad de operadores $\partial.z = 1 + z.\partial$ y de aquí $\partial^k.z = k\partial^{k-1} + z.\partial^k$, para $k \ge 1$, y por tanto $\partial^p.z = z.\partial^p$. El operador ∂^p se llama la *p-curvatura* de ∂.

Lema 1 (de Cartier)**.** *El operador diferencial* $\partial = \dfrac{d}{dz} - A$ *con* A *matriz* $n \times n$*,*

con coeficientes en K, tiene un espacio de soluciones en K de dimensión n sobre K^p si y sólo si su p-curvatura ∂^p es 0.

Prueba. El operador $\partial : V := K^n \to K$ es K^p-lineal. Supongamos que existen $e_1, \ldots, e_n \in V$ en el núcleo de ∂, linealmente independientes sobre K^p. Veamos que también son independientes sobre K. Sea

$$\lambda_1 e_1 + \cdots + \lambda_n e_n = 0,\ \lambda_i \in K. \tag{11}$$

Quitando denominadores, podemos suponer $\lambda_i \in K^p[z]$, ponemos $\lambda_i = b_o^i + b_1^i\, z + \cdots + b_{p-1}^i z^{p-1}$, con $b_j^i \in K^p$. Tenemos $\partial(bz^a e_i) = baz^{a-1}e_i$ para $b \in K^p$. Por tanto aplicando varias veces ∂ a (11), obtenemos una relación de dependencia sobre K^p. Entonces, ∂^p es cero en la K-base $e_1, \ldots, e_n$ de V y por tanto $\partial^p = 0$.

Recíprocamente, si $\partial^p = 0$, la aplicación K^p-lineal ∂ sobre V es nilpotente $\Rightarrow \exists e_1 \neq 0$ en V con $\partial e_1 = 0$. Como Ke_1 es invariante por ∂, ∂ opera sobre $W = V/Ke_1$. Por inducción sobre n, W tiene una base $f_2, \ldots, f_n$ sobre K con $\partial f_i = 0$ y cogiendo representantes F_i de los f_i, obtenemos una K-base $e_1, F_2, \ldots, F_n$ de V con $\partial F_i \in Ke_1$, $i = 2, \ldots, n$. Ponemos $\partial F_i = g_i e_1$, con $g_i \in K$. Ahora tenemos

$$\partial(g_i e_1) = \frac{d}{dz}(g_i e_1) - A g_i e_1 = g_i' e_1 + g_i \partial e_1 = g_i' e_1.$$

Esto vale para todo $g_i \in K$ y obtenemos $\partial^{p-1}(g_i e_1) = g_i^{p-1} e_1$ y por tanto $0 = \partial^p F_i = \partial^{p-1}(g_i e_1) = g_i^{p-1} e_1 \Rightarrow g_i^{p-1} = 0 \Rightarrow g_i = G_i'$, con $G_i \in K$. Sea $e_i = F_i - G_i e_1$, entonces $\partial e_i = \partial F_i - \partial(G_i e_1) = \partial F_i - g_i e_1 = 0 \Rightarrow$ el núcleo de ∂ en V es $K^p e_1 + \cdots + K^p e_n$. $\square$

Se tiene un algoritmo sencillo para calcular la p-curvatura: definimos la sucesión de matrices $A(k)$ por

$$A(1) := A, A(k+1) = \frac{d}{dz}(A(k)) + A.A(k)$$

entonces $A(p)$ módulo p es la matriz de la curvatura.

5.2 Casos probados

B. Dwork (hacia 1970) prueba la conjetura de Grothendieck para ecuaciones hipergeométricas, Beukers-Heckmann para las hipergeométricas generalizadas (1989), Chudnovsky-Chudnovsky en 1985 para la ecuación de Lamé. El trabajo de Honda (1974) publicado póstumamente en 1981 incluye el caso de orden 1. De hecho lo prueba como consecuencia del caso polinomial. Haraoka prueba la conjetura para las ecuaciones de Pochhammer (1994). La ecuación de Pochhammer es una ecuación diferencial de orden

n, generalización de la hipergeométrica de Gauss, en el sentido que sus soluciones tienen una representación integral del tipo de Euler. Es una ecuación libre de parámetros accesorios.

En 1972, N. Katz prueba la conjetura para conexiones de Gauss-Manin. En [Ka1] propone una reformulación muy general: Si consideramos el grupo de Galois diferencial $\mathbf{G}$ de la ecuación y el de monodromía $\mathbf{M}$, tenemos $\mathbf{M} \subset \mathbf{G} \subset \mathrm{GL}(n, \mathbb{C})$ y $\mathbf{G}$ coincide con la clausura de Zariski $\overline{\mathbf{M}}$ de $\mathbf{M}$ siempre que la ecuación es fuchsiana. Por tanto la finitud del grupo de monodromía equivale a la anulación del álgebra de Lie $\mathcal{G}$ del grupo $\mathbf{G}$. El enunciado de Katz es básicamente que el álgebra de Lie $\mathcal{G}$ de $\mathbf{G}$ sobre $\mathbb{C}(z)$ es la menor subálgebra de Lie algebraica del álgebra de matrices $M(n, \mathbb{C}(z))$ con la propiedad que su reducción módulo p contiene la p-curvatura para casi todo primo p. De hecho en [Ka1] Katz prueba que el enunciado de Grothendieck implica su enunciado, aparentemente más general.

En [Ka2], Katz prueba la conjetura para sistemas rígidos, englobando los casos probados anteriormente. Un sistema rígido queda globalmente determinado por datos locales, es decir por los puntos singulares y los exponentes locales. En 1997, Y. André la prueba más en general para sistemas diferenciales ligados a conexiones de Gauss-Manin sobre grupos de cohomología de de Rham relativa (sistemas diferenciales "que vienen de la geometría") (ver [A]). En particular, el trabajo de André incluye el caso de ecuaciones de orden uno sobre cuerpos de funciones sobre un cuerpo de números, caso del que Chudnovsky-Chudnovsky habían dado una prueba incompleta en 1985.

El primer caso en que la conjetura está totalmente abierta es el de ecuaciones diferenciales lineales sobre $\mathbb{Q}(z)$ de orden 2 con cuatro puntos singulares regulares, exponentes racionales y grupo de Galois $\mathrm{SL}(2, \mathbb{C})$. En este caso habría que probar que el enunciado *2.* de la conjetura no es cierto. La dificultad principal está en que los datos locales no determinan en este caso la ecuación diferencial.

De la misma forma en que una ecuación diferencial lineal con tres puntos singulares regulares se transforma en una ecuación hipergeométrica, toda ecuación diferencial lineal con cuatro puntos singulares regulares puede transformarse en una ecuación de Heun

$$Y'' + \frac{(a+b+1)z^2 - (a+b-d+1+(c+d)a)z + ac}{z(z-1)(z-a)}\, Y' + \frac{ab(z-q)}{z(z-1)(z-a)}\, Y = 0.$$

con puntos singularidades regulares en $0, 1, a, \infty$ (ver [E], [W-W]). El esquema de Riemann es

$$\begin{array}{cccc} 0 & 1 & a & \infty \\ \hline 0 & 0 & 0 & a \\ 1-c & 1-d & 1-e & b \end{array}$$

con $e = a + b + 1 - c - d$. La constante q es el llamado *parámetro accesorio*, cuya presencia se debe al hecho mencionado anteriormente que una ecuación fuchsiana de segundo order con cuatro (o más) puntos singulares no queda determinada por los puntos singulares y los exponentes locales.

Bibliografía.

[A] Y. André, Sur la conjecture des p-courbures de Grothendieck-Katz et un problème de Dwork, Geometric aspects of Dwork theory. Vol. I, 55–112, Walter de Gruyter GmbH & Co. KG, Berlin, 2004.

[B-H] F. Beukers, G. Heckmann, Monodromy for the hypergeometric function ${}_nF_{n-1}$, Invent. Math. 95 (1989), 325–354.

[B-W] F. Beukers, A. van der Waall, Lamé equations with algebraic solutions, J. Differential Equations 197 (2004), 1–25.

[C-X] T. Crespo, X. Xarles, Dibuixos d'infants, Notes del Seminari de Teoria de Nombres, UB-UAB-UPC, n. 12, Barcelona 2005, ISBN. 84-934244-0-4.

[D] S. Dahmen, Counting Integral Lamé Equations by Means of Dessins d'Enfants, Trans. Amer. Math. Soc., aparecerá.

[E] A. Erdélyi et alt., Higher transcendental functions, vol. III, McGraw-Hill, New York, 1955.

[F] L. Fuchs, Zur Theorie der linearen Differentialgleichungen mit veränderlichen Coefficienten, J. reine angew. Math. 66 (1866), 121-160.

[H] D. Husemöller, Elliptic Curves, Springer 1987.

[K1] F. Klein, Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade, Birkhäuser, 1993.
Versión inglesa: Lectures on the icosahedron and the solution of equations of the fifth degree, Dover, 2003.

[K2] F. Klein, Ueber lineare differentialgleichungen, Math. Ann. 12 (1878), 167-179.

[Ka1] N. Katz, A conjecture in the arithmetic theory of differential equations, Bull. Soc. Math. France 110 (1982), 203-239; corrección: Bull. Soc. Math. France 110 (1982), 347-348.

[Ka2] N. Katz, Rigid local systems, Annals of Math. Studies 139, Princeton University Press, 1996.

[L1] R. Liţcanu, Lamé operators with finite monodromy—a combinatorial approach, J. Differential Equations, 207 (2004), 93–116.

[L2] R. Liţcanu, Counting Lamé differential operators, Rend. Sem. Mat. Univ. Padova 107 (2002), 191–208.

[N] K. Nakanishi, Lamé operators with projective octahedral and icosahedral monodromies, Rend. Sem. Mat. Univ. Padova 115 (2005), 109–129.
[P] E.G.C. Poole, Introduction to the theory of linear differential equations, Oxford : The Clarendon Press, 1936.
[P-S] M. van der Put, M.F. Singer, Galois theory of linear differential equations, Springer-Verlag, 2003.
[S] H.A. Schwarz, Ueber diejenigen Fälle, in welchen die Gaussische Hypergeometrische Reihe eine algebraische Function ihres vierten Elementes darstellt, J. reine angew. Math. 75 (1873), 292-335.
[Sl] N.J.A. Sloane, The on-line encyclopedia of integer sequences, http://www.research.att.com/∼njas/sequences/
[W-W] E.T. Whittaker, G.N. Watson, A course of modern analysis, Cambridge University Press, 1940.

CONSTANTES LOCALES

Pilar Bayer & Artur Travesa

Universitat de Barcelona

•

Seminari de Teoria de Nombres (UB-UAB-UPC), 20 anys

Barcelona, 3 de febrero de 2006

Funciones automorfas y trascendencia
Vilanova i la Geltrú, julio, 2005

• Pregunta 3
Estudiar la naturaleza aritmética de las constantes locales k_P asociadas a las funciones automorfas que uniformizan X_D, $D = 6$, y sus cocientes. ¿Es cierto que son trascendentes?

• Respuesta de F. Rodríguez-Villegas
Miren Chowla-Selberg.

Contenido

1. Curvas de Shimura y puntos CM

$H(a,b) = \langle 1, \mathsf{i}, \mathsf{j}, \mathsf{k} \rangle, \quad \mathsf{i}^2 = a, \quad \mathsf{j}^2 = b, \quad \mathsf{ij} = -\mathsf{ji} = \mathsf{k}, \quad a, b \in \mathbb{Q}^*$

H indefinida, $a > 0$, $\quad \Phi : H \hookrightarrow \mathbf{M}(2, \mathbb{R})$

$$\Phi(x + y\mathsf{i} + z\mathsf{j} + t\mathsf{k}) = \begin{bmatrix} x + y\sqrt{a} & z + t\sqrt{a} \\ b(z - t\sqrt{a}) & x - y\sqrt{a} \end{bmatrix}$$

$D_H = p_1 \dots p_{2r}, \quad p_i$ primos distintos

Grupos aritméticos de unidades cuaterniónicas

$H \otimes \mathbb{R} \simeq \mathbf{M}(2,\mathbb{R})$, $\mathcal{O}(D,N)$ orden de Eichler

$\Gamma(D,N) := \Phi(\{x \in \mathcal{O} : \mathrm{Nr}(x) = 1\}) \leq \mathbf{SL}(2,\mathbb{R})$

$\overline{\Gamma(D,N)} \leq \mathbf{PSL}(2,\mathbb{R})$

$\Gamma(1,1) = \mathbf{SL}(2,\mathbb{Z})$, $\Gamma(1,N) = \Gamma_0(N)$

•

$X(1,N)/\mathbb{Q} = X_0(N)/\mathbb{Q}$ curva modular, $D = 1$

$X(D,N)/\mathbb{Q}$ curva de Shimura, $D \geq 1$

tipo **PEL** (Shimura): $\Omega = (H,\ \Phi,\ *;\mathsf{T},\ \mathcal{O};\ \mathsf{V})$

- H álgebra de cuaterniones indefinida; $\Phi : H \hookrightarrow M(2,\mathbb{R})$; $*$ anti-involución positiva de H.

- $\mathcal{O} \subseteq H$, estable por $*$; $\mathsf{T} : H \times H \to \mathbb{Q}$ forma alternada no degenerada tomando valores enteros sobre $\mathcal{O}$.

- $\mathsf{V} = (v_1, \ldots, v_s)$ estructura de nivel, $v_i \in \mathcal{O} \otimes \mathbb{Q}/\mathcal{O} = H/\mathcal{O}$.

  P = polarización, **E** = endomorfismo, **L** = nivel (*level*)

Curvas elípticas falsas: $(A, \iota, \mathcal{L}, W)/\mathbb{C}$, $\qquad \Omega = (H,\ \Phi,\ *\,;\mathsf{T},\ \mathcal{O};\ \mathsf{V})$

(i) Superficie abeliana $A/\mathbb{C}$. Un homomorfismo inyectivo $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ tal que $H_1(A, \mathbb{Z})$ es un $\mathcal{O}$-módulo isomorfo a $\mathcal{O}$.

(ii) Una polarización principal $\mathcal{L}$ de A tal que la anti-involución de Rosati asociada, $\phi_{\mathcal{L}} : \mathrm{End}^{\mathrm{o}}(A) \to \mathrm{End}^{\mathrm{o}}(A)$, restringe a la anti-involución $*$ en $\iota(\mathcal{O})$.

(iii) Una estructura de nivel $\mathsf{W} \subseteq H_1(A, \mathbb{Q})$ dada por la imagen de V por el isomorfismo $H \simeq H_1(A, \mathbb{Q})$ obtenido de (ii).

$[A, \iota, \mathcal{L}, W]$ clase de isomorfía

Curvas elípticas falsas con multiplicación compleja

$\mathbb{Q}(\sqrt{d}),\ d < 0, \quad R$ orden; $\quad$ supongamos que $R \subseteq \mathcal{O} \subseteq H$

Definición. Una curva elíptica falsa $[A, \iota, \mathcal{L}, N]$ admite multiplicación compleja por un orden R si

$$\mathrm{End}[A, \iota, \mathcal{L}, N] \simeq R.$$

En este caso,

$$\mathrm{End}^{\mathrm{o}}[A, \iota, \mathcal{L}, N] \simeq \mathbb{Q}(\sqrt{d}), \quad \mathbb{Q}(\sqrt{d}) \otimes_{\mathbb{Q}} H \simeq \mathbf{M}(2, \mathbb{Q}(\sqrt{d}))$$

$$A \sim E \times E, \quad E \text{ curva elíptica con MC por } \mathbb{Q}(\sqrt{d})$$

El modelo canónico de Shimura

$\Omega: \quad \Phi : H \hookrightarrow \mathbf{M}(2,\mathbb{R}), \qquad \mu^2 = -D, \quad \alpha \to \alpha^*; \quad \mathcal{O}(D,1); \quad N$

$$(X(D,N)/\mathbb{Q}, j_{D,N})$$

$$\pi : \mathcal{H} \to \Gamma(D;N)\backslash\mathcal{H}, \quad j_{D,N} : \Gamma(D,N)\backslash\mathcal{H} \longrightarrow X(D,N)(\mathbb{C})$$

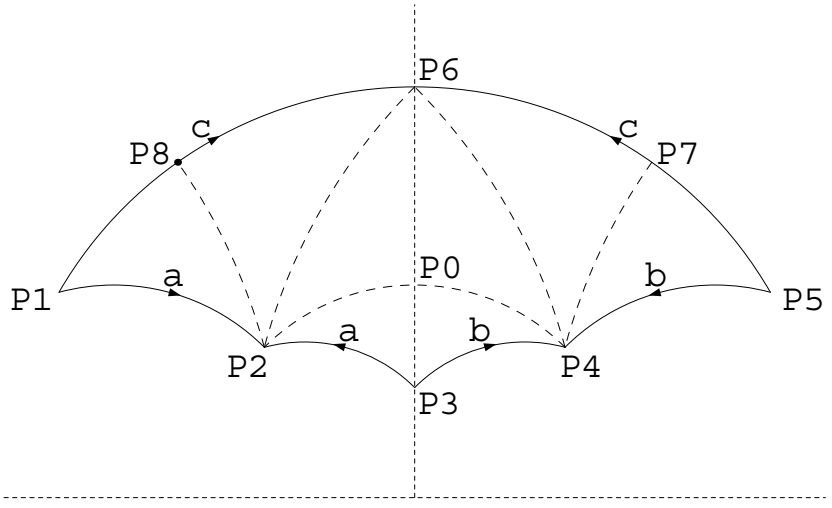
$$j_{D,N}(\pi(z)) \Longleftrightarrow [A_z, \iota_z, \mathcal{L}_z, N_z]$$

$$\tau \in \overline{\mathbb{Q}} \cap \mathcal{H} \quad \text{MC} \quad \Longleftrightarrow \quad [A_\tau, \iota_\tau, \mathcal{L}_\tau, N_\tau] \quad \text{MC}$$

• $\tau \in \overline{\mathbb{Q}} \cap \mathcal{H}$ MC $\Rightarrow$ $j_{D,N}(\tau) \in X(D,N)(\overline{\mathbb{Q}})$
Kronecker, Shimura

• $\tau \in \overline{\mathbb{Q}} \cap \mathcal{H}$, $j_{D,N}(\tau) \in X(D,N)(\overline{\mathbb{Q}})$ $\Rightarrow$ τ MC
Schneider, P. Cohen

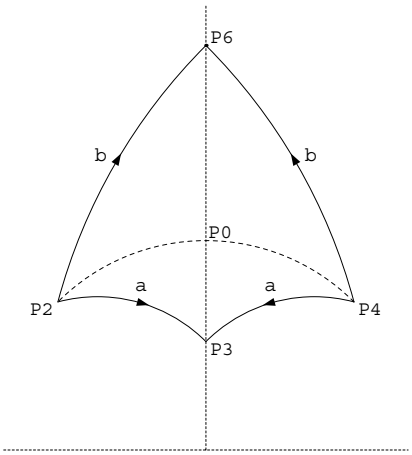
2. Uniformización en el caso $D = 6$



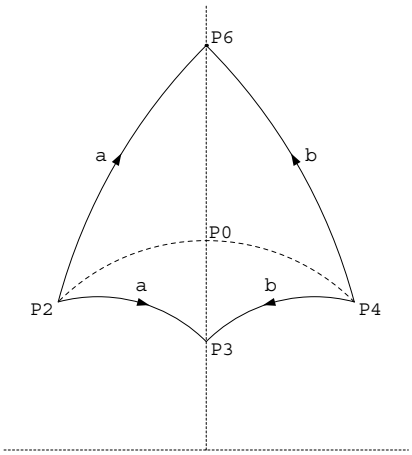
X_6 y algunas rectas hiperbólicas

	P_0	P_1	P_2	P_3	P_4	P_6
w_2	P_7	P_3	P_4	P_5	$*$	P_6
w_3	P_8	$*$	P_2	P_6	$*$	P_1
w_3'	$*$	$*$	$*$	P_6	P_4	P_5
w_6	P_0	$*$	P_4	P_6	P_2	P_3
$w_6\eta_2^{-1}$	$*$	P_6	P_4	$*$	$*$	P_5

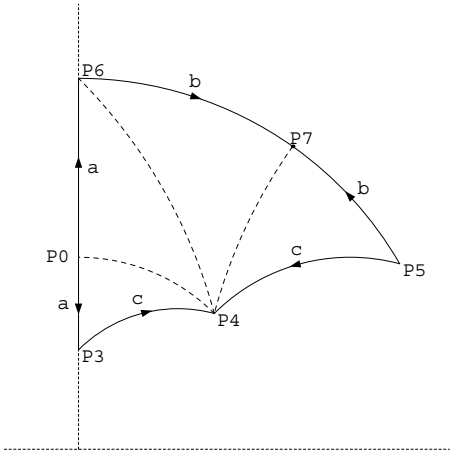
Involuciones de X_6 y sus acciones



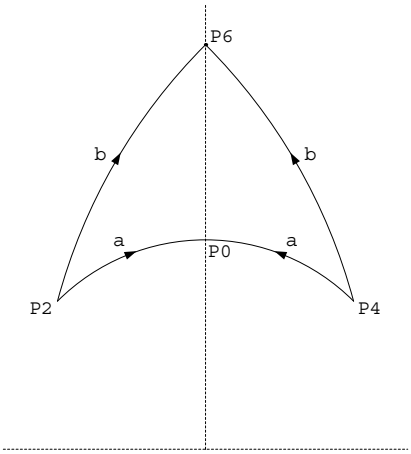
$X_6^{(2)} := X_6/\langle w_2 \rangle$



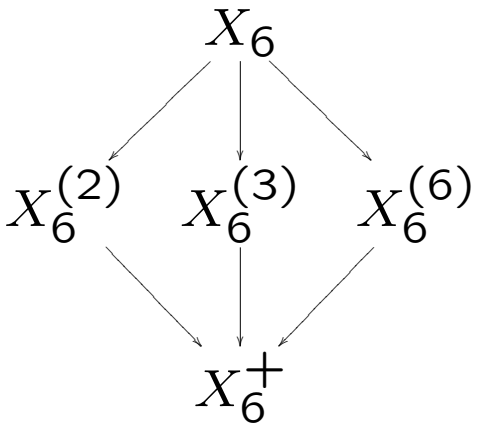
$X_6^{(3)} := X_6/\langle w_3 \rangle$



$X_6^{(6)} := X_6/\langle w_6 \rangle$



$X_6^{+} := X_6/\langle w_2, w_3 \rangle$



Funciones uniformizadoras (*Hauptmoduli*) de X_6 y de sus cocientes

$\mathbb{C}(X_6^+) = \mathbb{C}(t_6^+)$

$\mathbb{C}(X_6^{(2)}) = \mathbb{C}(t_6^{(2)}), \quad \mathbb{C}(X_6^{(3)}) = \mathbb{C}(t_6^{(3)}), \quad \mathbb{C}(X_6^{(6)}) = \mathbb{C}(t_6^{(6)})$

$\mathbb{C}(X_6) = \mathbb{C}(t_6)$

Cada función automorfa queda determinada por sus valores en tres vértices.

$t_6^{(2)}, t_6^{(3)}, t_6^+$ son funciones triangulares;

$t_6^{(6)}, t_6$ son funciones cuadrangulares.

valores iniciales	P_0	P_2	P_3	P_4	P_6	P_7	
t_6	$*$	a	0	1	∞	$*$	$a \neq 0, 1, \infty \, (\Rightarrow a = -1)$
$t_6^{(2)}$	$*$	$*$	0	1	∞	$*$	$*$
$t_6^{(3)}$	$*$	0	$*$	1	∞	$*$	$*$
$t_6^{(6)}$	0	$*$	$*$	1	∞	b	$b \neq 0, 1, \infty \, (\Rightarrow b = 2)$
t_6^+	0	$*$	$*$	1	∞	$*$	$*$

Teorema. *Se satisfacen las relaciones algebraicas siguientes:*

(a) $4t_6^+ t_6^{(2)} = (t_6^{(2)} + 1)^2$.

(b) $t_6^+ = (2t_6^{(3)} - 1)^2$.

(c) $4t_6^{(2)}(2t_6^{(3)} - 1)^2 = (t_6^{(2)} + 1)^2$.

(d) $t_6^2 = t_6^{(2)}$.

(e) $4t_6 t_6^{(3)} = (t_6 + 1)^2$.

(f) $t_6^+ + t_6^{(6)}(t_6^{(6)} - 2) = 0$.

(g) $2t_6 t_6^{(6)} = i(t_6 - i)^2$.

(h) $4t_6^2 t_6^+ = (t_6^2 + 1)^2$.

(i) $(t_6^{(2)} + 1)^2 + 4t_6^{(2)} t_6^{(6)}(t_6^{(6)} - 2) = 0$.

(j) $(2t_6^{(3)} - 1)^2 + t_6^{(6)}(t_6^{(6)} - 2) = 0$.

Derivada de Schwarz $\quad D_s(f,z) := \dfrac{2D(f,z)D^3(f,z) - 3D^2(f,z)^2}{D(f,z)^2}$

Derivada automorfa $\quad D_a(f,z) := \dfrac{D_s(f,z)}{D(f,z)^2}$

$D_a(\dfrac{az+b}{cz+d}, z) = 0$, $\quad$ para toda $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{GL}(2,\mathbb{C})$

$f^{-1}(w) = z,\ D_s(f^{-1}, w) = -D_a(f,z)$

$f(z) \in \mathcal{A}_0(\Gamma) \quad \Rightarrow \quad D_a(f,z) \in \mathcal{A}_0(\Gamma)$ $\qquad$ Schwarz, 1873

Ecuación diferencial de tercer orden:

$$D_a(t,z) + R(t(z)) = 0, \quad R(t) \in \mathbb{C}(t)$$

$$D_a(\omega,z) = 0 \Longleftrightarrow \omega(z) = \frac{az+b}{cz+d}, \quad \text{para } \omega = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{GL}(2,\mathbb{C})$$

Si $t(z)$ es una solución particular, entonces $t(\omega(z))$ es una solución para todo $\omega \in \mathbf{GL}(2,\mathbb{C})$.

Se tienen tres constantes de integración.

Buscamos únicamente soluciones Γ-automorfas. Éstas admiten desarrollos de la forma

$$t(z) = \sum_{m \geq m_0} b_m \left(k \frac{z-v}{z-\overline{v}} \right)^m, \quad v \in \mathcal{H},$$

con lo cual queda una sola constante de integración, k.

Por cuestiones de isotropía local:

$$t(z) = \sum_{n \geq n_0} a_n \left(k \frac{z-v}{z-\overline{v}} \right)^{e_v n}, \quad e_v = \sharp \overline{\Gamma}_v.$$

La constante k queda determinada por condiciones de contorno.

curva	función	ángulos	$-Da(t,z)$
X_6	t_6	$[P_2,P_3,P_4,P_6]$ $[\pi/3,\pi/2,\pi/3,\pi/2]$	$\frac{27t^4+74t^2+27}{36t^2(t^2-1)^2}$
$X_6^{(2)}$	$t_6^{(2)}$	$[P_3,P_4,P_6]$ $[\pi/4,\pi/3,\pi/4]$	$\frac{135t^2-142t+135}{144t^2(t-1)^2}$
$X_6^{(3)}$	$t_6^{(3)}$	$[P_2,P_4,P_6]$ $[\pi/6,\pi/6,\pi/2]$	$\frac{27t^2-27t+35}{36t^2(t-1)^2}$
$X_6^{(6)}$	$t_6^{(6)}$	$[P_0,P_4,P_7,P_6]$ $[\pi/2,\pi/3,\pi/2,\pi/2]$	$\frac{27t^4-108t^3+211t^2-206t+108}{36t^2(t^2-3t+2)^2}$
X_6^{+}	t_6^{+}	$[P_0,P_4,P_6]$ $[\pi/2,\pi/6,\pi/4]$	$\frac{135t^2-103t+108}{144t^2(t-1)^2}$

El caso clásico de la función j

$(X_0(1), j)$

$q(z) = e^{2\pi i z}, \qquad 2i \in \overline{\mathbb{Q}}, \quad \pi = \Gamma(1/2)^2$

$j(q) = 1728\, t(q)$

$$j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + 333202640600q^5 + 4252023300096q^6 + O(q^7)$$

1728 factor de normalización

- A000521 Coefficients of modular function j as power series in $q = e^{2\pi i z}$

Definición. Un *parámetro de uniformización local* en $v \in \mathcal{H}$ por la acción de Γ_v es cualquier función

$$q(z) := \left(k\frac{z-v}{z-\overline{v}}\right)^{e_v},$$

en donde $e_v = \sharp\overline{\Gamma}_v$ es el orden del grupo de isotropía en v y $k \in \mathbb{C}$.

Diremos que un parámetro $q(z)$ es *adaptado* a una función Γ_v-automorfa no constante

$$t(z) = \sum_{n \geq n_0} a_n q(z)^n$$

si $a_r = 1$ en el caso en que $t - a_0$ tenga un cero de orden $e_v r$ en $z = v$, o bien $a_{-r} = 1$ si t tiene un polo de orden $e_v r$ en $z = v$. La constante $k = k(v, \Gamma_v, t)$ se denomina *constante local en v adaptada a la función t*. Abreviadamente, hablaremos de *constantes locales*.

Factores de normalización en el caso $r = 1$

Caso $t(P) = 0$

$$t(z) = \sum_{n=1}^{\infty} b'_n \frac{q(z)^n}{(en)!}, \quad b'_1 = e!.$$

Substiuir q por $\nu^{-1}q$:

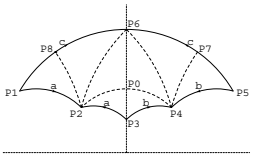
$$t(z) = \sum_{n=1}^{\infty} b''_n \frac{q(z)^n}{(en)!}, \quad b''_1 = \nu e!.$$

$\mathfrak{n}_0 := \nu e!, \quad t(P, q_P; z) := \mathfrak{n}_0^{-1} t(z)$

$$t(P, q_P; z) = \sum_{n=1}^{\infty} c_n \frac{q_P(z)^n}{(en)!}, \quad c_1 = 1, \quad q_P(z) = \frac{1}{\nu_P}\left(k_P \frac{z-P}{z-\overline{P}}\right)^{e_P}$$

Coeficientes c_n $(1 \leq n \leq 10)$ de $t_6(P_3, q_{P_3}; z)$:

$$\begin{aligned}
1 &= 1 \\
0 &= 0 \\
-48 &= -2^4 \cdot 3 \\
0 &= 0 \\
27504 &= 2^4 \cdot 3^2 \cdot 191 \\
0 &= 0 \\
-64498392 &= -2^3 \cdot 3^2 \cdot 7 \cdot 127973 \\
0 &= 0 \\
436272183216 &= 2^4 \cdot 3^4 \cdot 23 \cdot 229 \cdot 63913 \\
0 &= 0
\end{aligned}$$



The On-Line Encyclopedia of Integer Sequences:

I am sorry but the terms do not match anything in the table.

Caso $t(P) \neq 0, \infty$

$$t(z) = \sum_{n=0}^{\infty} b'_n \frac{q(z)^n}{(en)!}, \quad b'_1 = e!.$$

Substituir q por $\nu^{-1}q$,

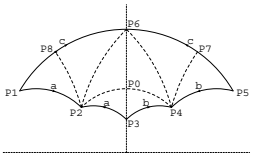
$$t(z) = \sum_{n=0}^{\infty} b''_n \frac{q(z)^n}{(en)!}, \quad b''_1 = \nu e!.$$

$\mathfrak{n}_v = \nu e!, \quad v = t(P), \quad t(P, q_P; z) := \mathfrak{n}_v^{-1} t(z)$

$$t(P, q_P; z) = \sum_{n=0}^{\infty} c_n \frac{q_P(z)^n}{(en)!}, \quad c_1 = 1, \quad q_P(z) = \frac{1}{\nu_P} \left(k_P \frac{z - P}{z - \overline{P}} \right)^{e_P}$$

Coeficientes c_n $(0 \leq n \leq 10)$ de $t_6(P_4, q_{P_4}; z)$:

$$
\begin{aligned}
1/2 &= 2^{-1} \\
1 &= 1 \\
20 &= 2^2 \cdot 5 \\
1356 &= 2^2 \cdot 3 \cdot 113 \\
227040 &= 2^5 \cdot 3 \cdot 5 \cdot 11 \cdot 43 \\
74611380 &= 2^2 \cdot 3 \cdot 5 \cdot 1243523 \\
42574294080 &= 2^6 \cdot 3^2 \cdot 5 \cdot 17 \cdot 19 \cdot 45767 \\
38683567274400 &= 2^5 \cdot 3^2 \cdot 5^2 \cdot 5372717677 \\
52554612744944640 &= 2^{10} \cdot 3^2 \cdot 5 \cdot 11 \cdot 23 \cdot 4507937111 \\
1017826040056899960000 &= 2^6 \cdot 3^4 \cdot 5^4 \cdot 139 \cdot 226002762361 \\
27062934495736204252800 0 &= 2^8 \cdot 3^4 \cdot 5^3 \cdot 29 \cdot 16126171 \cdot 223259851
\end{aligned}
$$

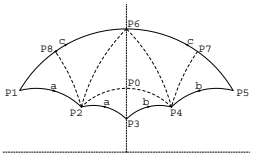


The On-Line Encyclopedia of Integer Sequences:

I am sorry but the terms do not match anything in the table.

Coeficientes c_n $(0 \leq n \leq 10)$ de $t_6(P_2, q_{P_2}; z)$:

$$
\begin{aligned}
-1/2 &= -2^{-1} \\
1 &= 1 \\
-20 &= -2^2 \cdot 5 \\
1356 &= 2^2 \cdot 3 \cdot 113 \\
-227040 &= -2^5 \cdot 3 \cdot 5 \cdot 11 \cdot 43 \\
74611380 &= 2^2 \cdot 3 \cdot 5 \cdot 1243523 \\
-42574294080 &= -2^6 \cdot 3^2 \cdot 5 \cdot 17 \cdot 19 \cdot 45767 \\
38683567274400 &= 2^5 \cdot 3^2 \cdot 5^2 \cdot 5372717677 \\
-52554612744944640 &= -2^{10} \cdot 3^2 \cdot 5 \cdot 11 \cdot 23 \cdot 4507937111 \\
1017826040056899960000 &= 2^6 \cdot 3^4 \cdot 5^4 \cdot 139 \cdot 226002762361 \\
-27062934495736204252800 0 &= -2^8 \cdot 3^4 \cdot 5^3 \cdot 29 \cdot 16126171 \cdot 223259851
\end{aligned}
$$

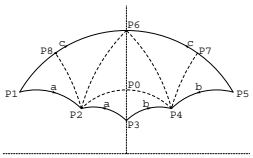


The On-Line Encyclopedia of Integer Sequences:

I am sorry but the terms do not match anything in the table.

Coeficientes c_n $(0 \le n \le 10)$ de $t_6(P_0, q_{P_0}; z)$:

$$\begin{aligned}
i/12 &= -i \cdot (1+i)^{-4} \cdot 3^{-1} \\
1 &= 1 \\
-12i &= i \cdot (1+i)^4 \cdot 3 \\
-226 &= -2 \cdot 113 \\
5664i &= (1+i)^{10} \cdot 3 \cdot 59 \\
160728 &= 2^3 \cdot 3 \cdot 37 \cdot 181 \\
-5467296i &= -(1+i)^{10} \cdot 3 \cdot 56951 \\
-211472208 &= -2^4 \cdot 3^5 \cdot 109 \cdot 499 \\
9193300992i &= -i \cdot (1+i)^{20} \cdot 3^2 \cdot 571 \cdot 1747 \\
445513958784 &= 2^7 \cdot 3^3 \cdot 128910289 \\
-23734590202368i &= -(1+i)^{18} \cdot 3^4 \cdot 15919 \cdot 35951
\end{aligned}$$



The On-Line Encyclopedia of Integer Sequences:

I am sorry but the terms do not match anything in the table.

Caso $t(P) = \infty$

$$t(z) = \sum_{n=-1}^{\infty} b'_n \frac{q(z)^n}{(2e(n+2))!}, \quad b'_{-1} = (2e)!.$$

Substituir q por $\nu^{-1}q$:

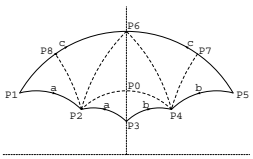
$$t(z) = \sum_{n=-1}^{\infty} b''_n \frac{q(z)^n}{(2e(n+2))!}, \quad b''_{-1} = \nu(2e)!.$$

$\mathfrak{n}_\infty = \nu(2e)!$ $\qquad t(P, q_P; z) := \mathfrak{n}_\infty^{-1} t(z)$

$$t(P, q_P; z) = \sum_{n=-1}^{\infty} c_n \frac{q_P(z)^n}{(2e(n+2))!}, \quad c_{-1} = 1, \quad q_P(z) = \frac{1}{\nu_P} \left(k_P \frac{z-P}{z-\overline{P}} \right)^{e_P}$$

Coeficientes c_n $(-1 \leq n \leq 10)$ de $t_6(P_6, q_{P_6}; z)$:

$$
\begin{aligned}
&1\\
&0\\
&18480\\
&0\\
&12803590800\\
&0\\
&-817993722627081000\\
&0\\
&-156078929845326558019950000\\
&0\\
&122859953407720110679241179380345000\\
&0
\end{aligned}
$$



The On-Line Encyclopedia of Integer Sequences:

I am sorry but the terms do not match anything in the table.

Funciones automorfas normalizadas $t(P, q_P; z) = \mathfrak{n}^{-1} t(z)$

$\mathfrak{n}_\infty$	$3870720 = 2^{12} \cdot 3^3 \cdot 5 \cdot 7$	$30965760 = 2^{15} \cdot 3^3 \cdot 5 \cdot 7$	$48 = 2^4 \cdot 3$	$96 = 2^5 \cdot 3$	$384 = 2^7 \cdot 3$
$t(P) = \infty$	$t_6^+(P_6, q_{P_6})$	$t_6^{(2)}(P_6, q_{P_6})$	$t_6^{(3)}(P_6, q_{P_6})$	$t_6^{(6)}(P_6, q_{P_6})$	$t_6(P_6, q_{P_6})$
$\mathfrak{n}_0$	$144 = 2^4 \cdot 3^2$	$\frac{27}{2} = 2^{-1} \cdot 3^3$	$10 = 2 \cdot 5$	$72 = 2^3 \cdot 3^2$	$\frac{3}{2} = 2^{-1} \cdot 3$
$t(P) = 0$	$t_6^+(P_0, q_{P_0})$	$t_6^{(2)}(P_3, q_{P_3})$	$t_6^{(3)}(P_2, q_{P_2})$	$t_6^{(6)}(P_0, q_{P_0})$	$t_6(P_3, q_{P_3})$
$\mathfrak{n}_1$	$40 = 2^3 \cdot 5$	$4 = 2^2$	$10 = 2 \cdot 5$	2	2
$t(P) = 1$	$t_6^+(P_4, q_{P_4})$	$t_6^{(2)}(P_4, q_{P_4})$	$t_6^{(3)}(P_4, q_{P_4})$	$t_6^{(6)}(P_4, q_{P_4})$	$t_6(P_4, q_{P_4})$
$\mathfrak{n}_i$	$*$	$*$	$*$	$*$	$12 = 2^2 \cdot 3$
$t(P) = i$	$*$	$*$	$*$	$*$	$t_6(P_0, q_{P_0})$

Teorema. *Sea* $F(a,b,c;w)=\sum_{n=0}^{\infty}\frac{(a)_n(b)_n}{(c)_n}\frac{w^n}{n!}$, $|w|<1$, *la serie hipergeométrica. Supongamos que* $c\neq 1$. *La función*

$$z=s(a,b,c;w):=\frac{w^{1-c}F(a-c+1,b-c+1,2-c;w)}{F(a,b,c;w)}$$

aplica el w*-semiplano* $\mathcal{H}$ *sobre el interior de un triángulo de vértices*

$$\begin{aligned} s(0) &= 0,\\ s(\infty) &= \exp(\pi i(1-c))\,\frac{\Gamma(b)\Gamma(c-a)\Gamma(2-c)}{\Gamma(c)\Gamma(b-c+1)\Gamma(1-a)},\\ s(1) &= \frac{\Gamma(2-c)\Gamma(c-a)\Gamma(c-b)}{\Gamma(c)\Gamma(1-a)\Gamma(1-b)}. \end{aligned}$$

Los ángulos internos en estos vértices son $\alpha\pi,\beta\pi,\gamma\pi$, *en donde* $\alpha=1-c\neq 0,\quad \beta=b-a,\quad \gamma=c-a-b.$

t	P	e_A	$t(A)$	ν_A	k_A
t_6^+	P_0	2	0	$2^3\cdot 3^2$	$i\frac{\sqrt{2}+\sqrt{3}}{2}\frac{\Gamma(7/24)\Gamma(11/24)}{\Gamma(19/24)\Gamma(23/24)}$
t_6^+	P_4	6	1	$\frac{1}{2\cdot 3^2}$	$\frac{2+\sqrt{3}-i}{12}\frac{\Gamma(1/6)\Gamma(7/24)\Gamma(19/24)}{\Gamma(5/6)\Gamma(11/24)\Gamma(23/24)}$
t_6^+	P_6	4	∞	$2^5\cdot 3$	$\frac{\sqrt{2}+\sqrt{3}}{4}\frac{\Gamma(1/4)\Gamma(13/24)\Gamma(17/24)}{\Gamma(3/4)\Gamma(19/24)\Gamma(23/24)}$
$t_6^{(2)}$	P_3	4	0	$\frac{3^2}{2^4}$	$\frac{(1+\sqrt{3})(1+i)}{8}\frac{\Gamma(1/4)\Gamma(5/12)}{\Gamma(3/4)\Gamma(11/12)}$
$t_6^{(2)}$	P_4	3	1	$\frac{2}{3}$	$\frac{2+\sqrt{3}-i}{6}\frac{\Gamma(1/3)^2\Gamma(7/12)}{\Gamma(2/3)^2\Gamma(11/12)}$
$t_6^{(2)}$	P_6	4	∞	$2^8\cdot 3$	$\frac{\sqrt{3}}{4}\frac{\Gamma(1/3)\Gamma(2/3)\Gamma(1/4)}{\Gamma(3/4)\Gamma(7/12)\Gamma(11/12)}$
$t_6^{(3)}$	P_2	6	0	$\frac{1}{2^3\cdot 3^2}$	$\frac{(1+\sqrt{3})(1+i)}{12}\frac{\Gamma(1/6)\Gamma(7/12)}{\Gamma(5/6)\Gamma(11/12)}$
$t_6^{(3)}$	P_4	6	1	$\frac{1}{2^3\cdot 3^2}$	$\frac{2+\sqrt{3}-i}{12}\frac{\Gamma(1/6)\Gamma(7/12)}{\Gamma(5/6)\Gamma(11/12)}$
$t_6^{(3)}$	P_6	2	2	2	$\frac{(1+\sqrt{3})(1+i)}{4}\frac{\Gamma(1/4)\Gamma(5/12)}{\Gamma(3/4)\Gamma(11/12)}$

t	P	e_P	$t(P)$	ν_P	k_P
$t_6^{(6)}$	P_0	2	0	$2^2 \cdot 3^2$	$i\frac{\sqrt{2}+\sqrt{3}}{2\sqrt{2}}\frac{\Gamma(7/24)\Gamma(11/24)}{\Gamma(19/24)\Gamma(23/24)}$
$t_6^{(6)}$	P_4	3	1	3^{-1}	$\frac{(1+\sqrt{3})(1+i)}{12}\frac{\Gamma(1/6)\Gamma(7/24)\Gamma(19/24)}{\Gamma(5/6)\Gamma(11/24)\Gamma(23/24)}$
$t_6^{(6)}$	P_7	2	2	$2^2 \cdot 3^2$	$\frac{(2\sqrt{3}+3\sqrt{2})(\sqrt{2}+i)}{12}\frac{\Gamma(7/24)\Gamma(11/24)}{\Gamma(19/24)\Gamma(23/24)}$
$t_6^{(6)}$	P_6	2	∞	2^2	$i\frac{\sqrt{2}+\sqrt{3}}{4}\frac{\Gamma(1/4)\Gamma(13/24)\Gamma(17/24)}{\Gamma(3/4)\Gamma(19/24)\Gamma(23/24)}$

t	P	e_P	$t(P)$	ν_P	k_P
t_6	P_0	1	i	$2^2 \cdot 3$	$i\frac{\sqrt{2}+\sqrt{3}}{2}\frac{\Gamma(7/24)\Gamma(11/24)}{\Gamma(19/24)\Gamma(23/24)}$
t_6	P_2	3	-1	3^{-1}	$\frac{1+(2+\sqrt{3})i}{6\sqrt[3]{2}}\frac{\Gamma(1/3)^2\Gamma(7/12)}{\Gamma(2/3)^2\Gamma(11/12)}$
t_6	P_3	2	0	$3 \cdot 2^{-2}$	$\frac{(1+\sqrt{3})(1+i)}{8}\frac{\Gamma(1/4)\Gamma(5/12)}{\Gamma(3/4)\Gamma(11/12)}$
t_6	P_4	3	1	3^{-1}	$\frac{2+\sqrt{3}-i}{6\sqrt[3]{2}}\frac{\Gamma(1/3)^2\Gamma(7/12)}{\Gamma(2/3)^2\Gamma(11/12)}$
t_6	P_6	2	∞	2^4	$\frac{\sqrt{3}(1-i)}{4\sqrt{2}}\frac{\Gamma(1/3)\Gamma(2/3)\Gamma(1/4)}{\Gamma(3/4)\Gamma(7/12)\Gamma(11/12)}$

La fórmula de Chowla-Selberg (1967)

$$\Delta(z) := e^{2\pi iz}\prod_{n=1}^{\infty}(1-e^{2\pi inz})^{24} = \sum_{n=1}^{\infty}\tau(n)q^n, \quad q = e^{2\pi iz};$$

$d<0$ discr., $\quad H(d) = \{(a_j,b_j,c_j)\}_{1\le j\le h}, \quad \tau_j = \dfrac{-b_j+i\sqrt{|d|}}{2a_j};$

$$\prod_{j=1}^{h}\Delta(\tau_j) = \frac{\prod_{j=1}^{h}a_j^6}{(2\pi|d|)^{6h}}\prod_{m=1}^{|d|}\left\{\Gamma\left(\frac{m}{|d|}\right)^{\left(\frac{d}{m}\right)}\right\}^{3w},$$

$$w = \begin{cases} 6, & \text{si } d=-3,\\ 4, & \text{si } d=-4,\\ 2, & \text{en los otros casos.}\end{cases}$$

3. Dependencia algebraica entre constantes locales

Definición. $(\mathbb{C}^*/\overline{K}^*)$ Sea K un subcuerpo de $\mathbb{C}$. Dados $a,b\in\mathbb{C}^*$, escribiremos $a\sim_K b$ para indicar que $ab^{-1}\in\overline{K}^*$; diremos que a,b tienen la misma parte trascendente sobre K. Si $K=\mathbb{Q}$, escribiremos $a\sim b$ y diremos que a,b tienen la misma parte trascendente.

Proposición. *Sean $\Gamma,\Gamma'\subseteq\mathbf{SL}(2,\mathbb{R})$ grupos fuchsianos conmensurables, $v\in\mathcal{H}$, t una función Γ_v-automorfa con constante local adaptada $k(v,\Gamma,t)$, t' una función Γ'_v-automorfa con constante local adaptada $k(v,\Gamma',t')$. Sea $F(X,Y)\in K[X,Y]\backslash\{0\}$ tal que $F(t,t')=0$, siendo K un subcuerpo de $\mathbb{C}$ que contenga los valores $t(v),t'(v)$. Entonces*

$$k(v,\Gamma,t)\sim_K k(v,\Gamma',t').$$

Lema. *Sea $v \in \mathcal{H}$ un punto de orden $e_v \geq 1$ por la acción de $\Gamma_v \subseteq \Gamma$, y t una función Γ-automorfa no constante. Entonces, para toda matriz $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$, las dos constantes locales adaptadas en v y $\gamma(v)$ se relacionan por*

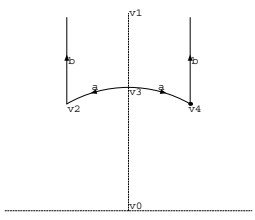
$$\left(\frac{k(\gamma(v),\Gamma,t)}{k(v,\Gamma,t)}\right)^{e_v r} = \left(\frac{cv+d}{c\overline{v}+d}\right)^{e_v r}.$$

En particular, si $v, c, d \in \overline{\mathbb{Q}}$, se tendrá que $k(\gamma(v),\Gamma,t) \sim k(v,\Gamma,t)$.

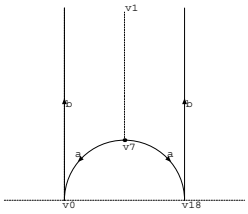
4. Trascendencia de las constantes locales en el caso $D = 1$

Teorema. (Takeuchi, 1977) *Existen exactamente nueve tipos aritméticos definidos por grupos triangulares con puntas, a saber:*

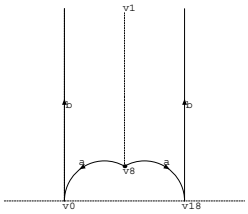
$(\infty,\infty,\infty), (\infty,\infty,3), (\infty,\infty,2),$
$(\infty,6,6), (\infty,6,2), (\infty,4,4),$
$(\infty,4,2), (\infty,3,3), (\infty,3,2).$



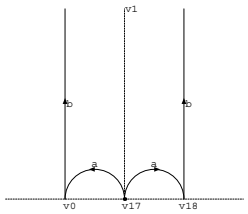
Dominio fundamental de $\Gamma_0(1)$, $(\infty,3,2)$



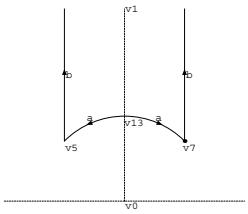
Dominio fundamental de $\Gamma_0(2)$, $(\infty, \infty, 2)$



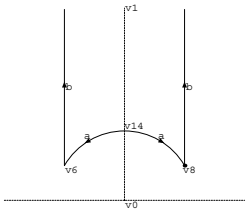
Dominio fundamental de $\Gamma_0(3)$, $(\infty, \infty, 3)$



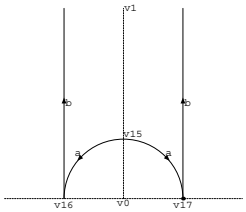
Dominio fundamental de $\Gamma_0(4)$, (∞, ∞, ∞)



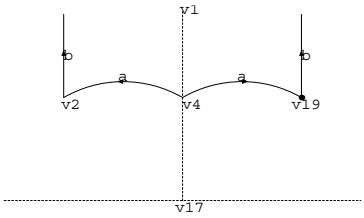
Dominio fundamental de $\Gamma_0^+(2)$, $(\infty, 4, 2)$



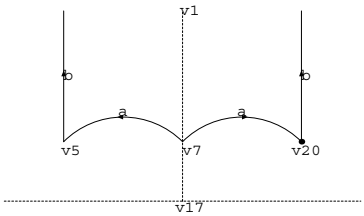
Dominio fundamental de $\Gamma_0^+(3)$, $(\infty, 6, 2)$



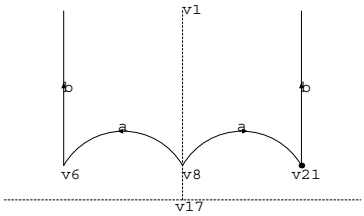
Dominio fundamental de $\Gamma_0^+(4)$, $(\infty, \infty, 2)$



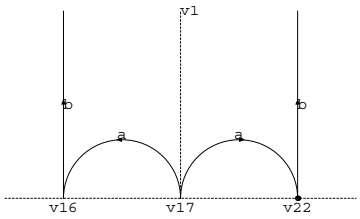
Dominio fundamental de $\Gamma_0^+(1)^*$, $(\infty, 3, 3)$



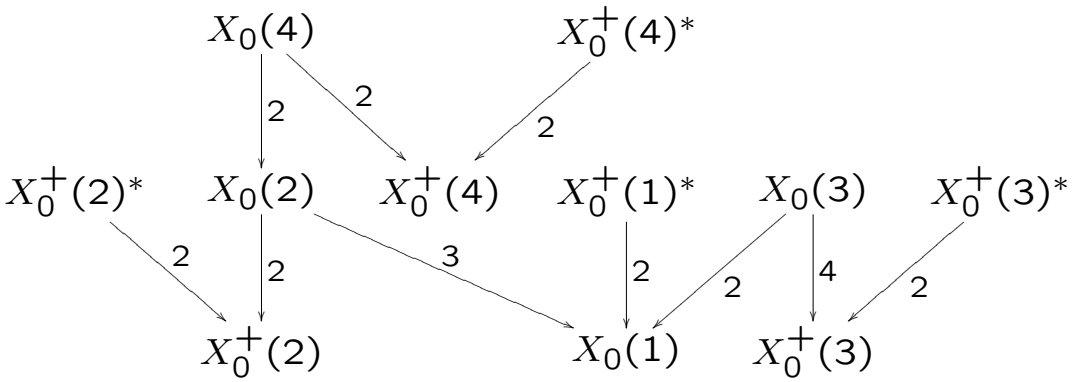
Dominio fundamental de $\Gamma_0^+(2)^*$, $(\infty, 4, 4)$



Dominio fundamental de $\Gamma_0^+(3)^*$, $(\infty, 6, 6)$



Dominio fundamental de $\Gamma_0^+(4)^*$, (∞, ∞, ∞)



Constantes locales en puntos elípticos

t	v	e_v	$t(v)$	a, c	ν_v	k_v
t_1^+	v_3	2	0	$\frac{1}{12}, \frac{1}{2}$	$2 \cdot 3^2$	$\exp(\frac{\pi i}{2})\frac{1}{2}\frac{\Gamma(\frac{1}{12})\Gamma(\frac{5}{12})}{\Gamma(\frac{11}{12})\Gamma(\frac{7}{12})}$
t_2^+	v_{13}	2	0	$\frac{1}{8}, \frac{1}{2}$	2^3	$\exp(\frac{\pi i}{2})\frac{1}{2}\frac{\Gamma(\frac{1}{8})\Gamma(\frac{3}{8})}{\Gamma(\frac{7}{8})\Gamma(\frac{5}{8})}$
t_3^+	v_{14}	2	0	$\frac{1}{6}, \frac{1}{2}$	3^2	$\exp(\frac{\pi i}{2})\frac{1}{2}\frac{\Gamma(\frac{1}{6})\Gamma(\frac{1}{3})}{\Gamma(\frac{5}{6})\Gamma(\frac{2}{3})}$
t_4^+	v_{15}	2	0	$\frac{1}{4}, \frac{1}{2}$	2	$\exp(\frac{\pi i}{2})\frac{1}{2}\frac{\Gamma(\frac{1}{4})^2}{\Gamma(\frac{3}{4})^2}$
t_1^*	v_4	3	0	$\frac{1}{6}, \frac{2}{3}$	2	$\exp(\frac{\pi i}{3})\frac{1}{3}\frac{\Gamma(\frac{1}{6})\Gamma(\frac{1}{3})}{\Gamma(\frac{5}{6})\Gamma(\frac{2}{3})}$
t_2^*	v_7	4	0	$\frac{1}{4}, \frac{3}{4}$	1	$\exp(\frac{\pi i}{4})\frac{1}{4}\frac{\Gamma(\frac{1}{4})^2}{\Gamma(\frac{3}{4})^2}$
t_3^*	v_8	6	0	$\frac{1}{3}, \frac{5}{6}$	1	$\exp(\frac{\pi i}{6})\frac{1}{6}\frac{\Gamma(\frac{1}{3})\Gamma(\frac{1}{6})}{\Gamma(\frac{2}{3})\Gamma(\frac{5}{6})}$

t	v	e_v	$t(v),$	a, c	ν_v	k_v
t_1^+	v_4	3	1	$\frac{1}{12}, \frac{2}{3}$	2^3	$\frac{1}{3}\frac{\Gamma(\frac{1}{12})\Gamma(\frac{7}{12})\Gamma(\frac{1}{3})}{\Gamma(\frac{11}{12})\Gamma(\frac{5}{12})\Gamma(\frac{2}{3})}$
t_2^+	v_7	4	1	$\frac{1}{8}, \frac{3}{4}$	1	$\frac{1}{4}\frac{\Gamma(\frac{1}{8})\Gamma(\frac{5}{8})\Gamma(\frac{1}{4})}{\Gamma(\frac{7}{8})\Gamma(\frac{3}{8})\Gamma(\frac{3}{4})}$
t_3^+	v_8	6	1	$\frac{1}{6}, \frac{5}{6}$	1	$\frac{1}{6}\frac{\Gamma(\frac{1}{6})^2\Gamma(\frac{2}{3})}{\Gamma(\frac{5}{6})^2\Gamma(\frac{1}{3})}$
t_1^*	v_{19}	3	1	$\frac{1}{6}, \frac{2}{3}$	2	$\frac{1}{3}\frac{\Gamma(\frac{1}{6})\Gamma(\frac{1}{3})}{\Gamma(\frac{5}{6})\Gamma(\frac{2}{3})}$
t_2^*	v_{20}	4	1	$\frac{1}{4}, \frac{3}{4}$	1	$\frac{1}{4}\frac{\Gamma(\frac{1}{4})^2}{\Gamma(\frac{3}{4})^2}$
t_3^*	v_{21}	6	1	$\frac{1}{3}, \frac{5}{6}$	1	$\frac{1}{6}\frac{\Gamma(\frac{1}{3})\Gamma(\frac{1}{6})}{\Gamma(\frac{2}{3})\Gamma(\frac{5}{6})}$

t	v	e_v	$t(v)$,	a, c	ν_v	k_v
t_1	v_2	3	0	$\frac{1}{12}, \frac{2}{3}$	2^3	$\exp(\frac{\pi i}{3})\frac{1}{3}\frac{\Gamma(\frac{1}{12})\Gamma(\frac{7}{12})\Gamma(\frac{1}{3})}{\Gamma(\frac{11}{12})\Gamma(\frac{5}{12})\Gamma(\frac{2}{3})}$
t_1	v_3	2	1	$\frac{1}{12}, \frac{1}{2}$	$2 \cdot 3^2$	$\frac{1}{2}\frac{\Gamma(\frac{1}{12})\Gamma(\frac{5}{12})}{\Gamma(\frac{11}{12})\Gamma(\frac{7}{12})}$
t_2	v_7	2	1	$\frac{1}{4}, \frac{1}{2}$	2	$\frac{1}{2}\frac{\Gamma(\frac{1}{4})^2}{\Gamma(\frac{3}{4})^2}$
t_3	v_8	3	1	$\frac{1}{3}, \frac{2}{3}$	2	$\frac{1}{3}\frac{\Gamma(\frac{1}{3})^3}{\Gamma(\frac{2}{3})^3}$

Órdenes de $\mathbb{Q}(i)$: dependencias algebraicas

(1) $\left(\frac{k(v(-4,P(0,1),X_0^+(1)),t_1^+))}{k(v(-4,P(0,1),X_0(1)),t_1)}\right)^2 = -1, \quad e^+ = e = 2;$

(2) $\left(\frac{k(v(-4,P(0,1),X_0(1)),t_1)}{k(v(-4,P(1/2,1/2),X_0(2)),t_2)}\right)^2 = 3, \quad e_1 = e_2 = 2;$

(3) $\left(\frac{k(v(-4,P(1/2,1/2),X_0^+(2)),t_2^+)}{k(v(-4,P(1/2,1/2),X_0(2)),t_2)}\right)^4 = \frac{1}{4}, \quad e^+ = 4,\ e = 2;$

(4) $\left(\frac{k(v(-4,P(1/2,1/2),X_0^+(2)),t_2^+)}{k(v(-4,P(1/2,1/2),X_0^+(2)^*),t_2^*)}\right)^4 = -4, \quad e^+ = e^* = 4;$

(5) $\left(\frac{k(v(-4,P(1/2,1/2),X_0^+(2)),t_2^+)}{k(v(-4,P(3/2,1/2),X_0^+(2)^*),t_2^*)}\right)^4 = 4, \quad e^+ = e^* = 4;$

(6) $\left(\frac{k(v(-16,P(0,1/2),X_0(1)),t_1)}{k(v(-16,P(0,1/2),X_0(2)),t_2)}\right)^1 = 2541, \quad e_1 = e_2 = 1;$

(7) $\left(\frac{k(v(-16,P(0,1/2),X_0(2)),t_2)}{k(v(-16,P(0,1/2),X_0(4)),t_4)}\right)^1 = \frac{3}{16}, \quad e_2 = e_4 = 1;$

(8) $\left(\frac{k(v(-4\cdot 2^2,P(0,1/2),X_0^+(4)),t_4^+)}{k(v(-4\cdot 2^2,P(0,1/2),X_0(4)),t_4)}\right)^2 = \frac{-1}{4}, \quad e^+ = 2,\ e = 1;$

(9) $\left(\frac{k(v(-4\cdot 2^2,P(0,1/2),X_0^+(4)),t_4^+)}{k(v(-4\cdot 2^2,P(0,1/2),X_0^+(4)^*),t_4^*)}\right)^2 = 4, \quad e^+ = 2,\ e^* = 1.$

Órdenes de $\mathbb{Q}(\sqrt{-3})$: dependencias algebraicas

$$(10)\quad \left(\frac{k(v(-3,P(-1/2,\sqrt{3}/2),X_0(1)),t_1)}{k(v(-3,P(1/2,\sqrt{3}/2),X_0(1)),t_1)}\right)^3 = 1, \qquad e = 3;$$

$$(11)\quad \left(\frac{k(v(-3,P(1/2,\sqrt{3}/2),X_0^+(1)),t_1^+)}{k(v(-3,P(1/2,\sqrt{3}/2),X_0(1)),t_1)}\right)^3 = -1, \qquad e^+ = e^+ = 3;$$

$$(12)\quad \left(\frac{k(v(-3,P(1/2,\sqrt{3}/2),X_0^+(1)),t_1^+)}{k(v(-3,P(1/2,\sqrt{3}/2),X_0^+(1)^*),t_1^*)}\right)^3 = -4, \qquad e^+ = e^* = 3;$$

$$(13)\quad \left(\frac{k(v(-3,P(1/2,\sqrt{3}/2),X_0^+(1)),t_1^+)}{k(v(-3,P(3/2,\sqrt{3}/2),X_0^+(1)^*),t_1^*)}\right)^3 = 4, \qquad e^+ = e^* = 3;$$

$$(14)\quad \left(\frac{k(v(-3,P(1/2,\sqrt{3}/2),X_0(1)),t_1)}{k(v(-3,P(-1/2,\sqrt{3}/6),X_0(3)),t_3)}\right)^3 = -8, \qquad e_1 = e_3 = 3;$$

$$(15)\quad \left(\frac{k(v(-3,P(-1/2,\sqrt{3}/6),X_0^+(3)),t_3^+)}{k(v(-3,P(-1/2,\sqrt{3}/6),X_0(3)),t_3)}\right)^6 = \frac{1}{4}, \qquad e^+ = 6,\ e = 3;$$

$$(16)\quad \left(\frac{k(v(-3,P(-1/2,\sqrt{3}/6),X_0^+(3)),t_3^+)}{k(v(-3,P(-1/2,\sqrt{3}/6),X_0^+(3)^*),t_3^*)}\right)^6 = -4, \qquad e^+ = e^* = 6;$$

$$(17)\quad \left(\frac{k(v(-3,P(-1/2,\sqrt{3}/6),X_0^+(3)),t_3^+)}{k(v(-3,P(3/2,\sqrt{3}/6),X_0^+(3)^*),t_3^*)}\right)^6 = 4, \qquad e^+ = e^* = 6;$$

$$(18)\quad \left(\frac{k(v(-3,P(0,1/\sqrt{3}),X_0^+(3)),t_3^+)}{k(v(-3,P(0,1/\sqrt{3}),X_0(3)),t_3)}\right)^2 = \frac{-1}{4}, \qquad e^+ = 2,\ e = 1.$$

Dependencias algebraicas deducidas por observación de la tabla

Órdenes de $\mathbb{Q}(i)$:

$$(19)\quad \left(\frac{k(v(-4\cdot 2^2,P(0,1/2),X_0^+(4)),t_4^+)}{k(v(-4,P(1/2,1/2),X_0^+(2)^*),t_2^*)}\right)^4 = -16, \qquad e_4^+ = 2,\ e_2^* = 4.$$

Órdenes de $\mathbb{Q}(\sqrt{-3})$:

$$(20)\quad \left(\frac{k(v(-3\cdot 2^2,P(0,1/\sqrt{3}),X_0^+(3)),t_3^+)}{k(v(-3,P(1/2,\sqrt{3}/2),X_0^+(3)^*),t_3^*)}\right)^6 = 729, \qquad e_3^+ = 2,\ e_3^* = 6.$$

Representantes de las clases en $\mathbb{C}^*/\overline{\mathbb{Q}}^*$

- Para $\mathbb{Q}(\sqrt{-2})$, $d=-8$:

$$k(v(-8,P(0,1/\sqrt{2}),X_0^+(2)),t_2^+)=\exp(\tfrac{\pi i}{2})\tfrac{1}{2}\frac{\Gamma(\frac{1}{8})\Gamma(\frac{3}{8})}{\Gamma(\frac{5}{8})\Gamma(\frac{7}{8})}\sim\frac{\Gamma(\frac{1}{8})\Gamma(\frac{3}{8})}{\Gamma(\frac{5}{8})\Gamma(\frac{7}{8})}$$

- Para $\mathbb{Q}(\sqrt{-1})$, $d=-4$:

$$k(v(-4,P(1/2,1/2),X_0(2)),t_2)=\tfrac{1}{2}\frac{\Gamma(\frac{1}{4})^2}{\Gamma(\frac{3}{4})^2}\sim\frac{\Gamma(\frac{1}{4})^2}{\Gamma(\frac{3}{4})^2}$$

- Para $\mathbb{Q}(\sqrt{-3})$, $d=-3$:

$$k(v(-3,P(-1/2,\sqrt{3}/6),X_0(3)),t_3)=\tfrac{1}{3}\frac{\Gamma(\frac{1}{3})^3}{\Gamma(\frac{2}{3})^3}\sim\frac{\Gamma(\frac{1}{3})^3}{\Gamma(\frac{2}{3})^3}$$

$$K=\int_0^{\frac{\pi}{2}}\frac{d\varphi}{\sqrt{1-k^2\sin^2\varphi}},\quad K'=\int_0^{\frac{\pi}{2}}\frac{d\varphi}{\sqrt{1-k'^2\sin^2\varphi}},\quad k^2+k'^2=1$$

$$iK/K'=\tau\in\mathbb{Q}(\sqrt{d}),\quad d<0,\qquad\qquad \Delta(\tau_i)\sim\Delta(\tau_j)$$

$$K\sim\sqrt{\pi}\prod_{m=1}^{|d|}\left\{\Gamma\left(\frac{m}{|d|}\right)^{\left(\frac{d}{m}\right)}\right\}^{\frac{w}{4h}}\qquad\text{Chowla-Selberg}$$

- Para $d=-8$:

$$\left(\frac{K}{\sqrt{\pi}}\right)^2\sim\frac{\Gamma(\frac{1}{8})\Gamma(\frac{3}{8})}{\Gamma(\frac{5}{8})\Gamma(\frac{7}{8})}\sim k(P(0,1/\sqrt{2}),X_0^+(2),t_2^+)$$

$$\pi_{-8}:=\frac{\Gamma(\frac{1}{8})\Gamma(\frac{3}{8})}{\Gamma(\frac{5}{8})\Gamma(\frac{7}{8})}$$

- Para $d = -4$:

$$\left(\frac{K}{\sqrt{\pi}}\right)^2 \sim \frac{\Gamma(\frac{1}{4})^2}{\Gamma(\frac{3}{4})^2} \sim k(P(1/2, 1/2), X_0(2), t_2)$$

$$\pi_{-4} := \frac{\Gamma(\frac{1}{4})^2}{\Gamma(\frac{3}{4})^2}$$

- Para $d = -3$:

$$\left(\frac{K}{\sqrt{\pi}}\right)^2 \sim \frac{\Gamma(\frac{1}{3})^3}{\Gamma(\frac{2}{3})^3} \sim k(P(-1/2, \sqrt{3}/6), X_0(3), t_3)$$

$$\pi_{-3} := \frac{\Gamma(\frac{1}{3})^3}{\Gamma(\frac{2}{3})^3}$$

Definición. Dado un discriminante $d < 0$, escribiremos

$$\pi_d := \prod_{m=1}^{|d|} \left\{ \Gamma\left(\frac{m}{|d|}\right)^{\left(\frac{d}{m}\right)} \right\}^{\frac{w}{2h}}.$$

Definición. Sea $P \in \mathcal{H}$ un punto de multiplicación compleja por un orden de discriminante $d < 0$. Sea $\Gamma \leq \mathbf{SL}(2, \mathbb{R})$ un subgrupo conmensurable con el grupo modular. Por definición, un *parámetro aritmético de uniformización local* en P por la acción de Γ_P es cualquier función

$$q_P(z) := \left(k\frac{z - P}{z - \overline{P}}\right)^{e_P},$$

en donde $e_P = \sharp\overline{\Gamma}_P$ y la constante k es tal que $k \sim \pi_d$.

Definimos $q_\infty = \exp(2\pi i z)$.

Teorema. (Chudnovsky, 1970) *Sea $E/\overline{\mathbb{Q}}$ una curva elíptica de ecuación*

$$Y^2 = 4X^3 - g_2X - g_3.$$

Si E tiene multiplicación compleja, entonces para todo período $\omega \in \Lambda$, $\omega \neq 0$, los números π, ω son algebraicamente independientes sobre $\overline{\mathbb{Q}}$.

Corolario. $\Gamma(1/4)$, $\Gamma(1/3) \notin \overline{\mathbb{Q}}$.

Demostración:

$$4\int_0^1 \frac{dt}{\sqrt{1-t^4}} = \frac{\Gamma\left(\frac{1}{4}\right)^2}{\sqrt{2\pi}}; \quad 2\int_1^\infty \frac{dt}{\sqrt{4t^3-4}} = \frac{\Gamma\left(\frac{1}{3}\right)^3}{\sqrt[3]{16}\pi}.$$

Corolario. $\Gamma(1/2)$, $\Gamma(1/3)$, $\Gamma(1/4)$, $\Gamma(2/3)$, $\Gamma(3/4)$ *son trascendentes.*

Teorema. *Para todo discriminante $d < 0$, π_d es trascendente.*

Demostración. Sea τ un punto de multiplicación compleja por un orden de discriminante d. Entonces, $j(\tau) \in \overline{\mathbb{Q}}$. Puesto que

$$j(\tau) = 2^8 \frac{(k(\tau)^4 - k(\tau)^2 + 1)^3}{k(\tau)^4(k(\tau)^2-1)^2},$$

se tendrá que $k(\tau) \in \overline{\mathbb{Q}}$. El modelo de Jacobi

$$E_k : Y^2 = (1-X^2)(1-k(\tau)X^2)$$

está definido sobre $\overline{\mathbb{Q}}$ y su red de períodos es $\langle 4K(\tau), 4K(\tau)\tau\rangle$. El modelo de Weierstrass correspondiente a esta red está definido sobre $\overline{\mathbb{Q}}$. Por el teorema de Chudnovsky, $K(\tau), \pi$ son algebraicamente independientes. Puesto que $K(\tau) \sim \sqrt{\pi} \cdot \sqrt{\pi_d}$, se deduce que π_d es trascendente.

Definición. Sean $P \in \mathcal{H}$ un punto CM y q_P un parámetro aritmético. Sea $\Gamma \leq \mathbf{SL}(2,\mathbb{R})$ un subgrupo conmensurable con el grupo modular. Una función Γ-modular f se denomina *aritmética en* P si su desarrollo en serie de potencias de q_P es de coeficientes algebraicos. Un función modular respecto de Γ se denomina *aritmética en el infinito* si su desarrollo en serie de potencias de q_∞ es de coeficientes algebraicos.

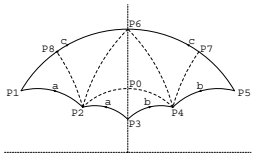
Teorema. *Las condiciones siguientes son equivalentes:*

(i) *La función f es aritmética en el infinito.*

(ii) *La función f es aritmética en un punto CM.*

(iii) *La función f es aritmética en todo los puntos CM.*

5. Trascendencia de las constantes locales en el caso $D = 6$



Órdenes de $\mathbb{Q}(i)$:

$$k(P_1, X_6, t_6) \sim k(P_3, X_6, t_6) \sim k(P_5, X_6, t_6) \sim k(P_6, X_6, t_6) \sim \frac{\Gamma(1/4)\Gamma(5/12)}{\Gamma(3/4)\Gamma(11/12)}$$

Órdenes de $\mathbb{Q}(\sqrt{-3})$: $\quad k(P_2, X_6, t_6) \sim k(P_4, X_6, t_6) \sim \frac{\Gamma(1/3)^2\Gamma(7/12)}{\Gamma(2/3)^2\Gamma(11/12)}$

Órdenes de $\mathbb{Q}(\sqrt{-6})$:

$$k(P_0, X_6, t_6) \sim k(P_7, X_6, t_6) \sim k(P_8, X_6, t_6) \sim \frac{\Gamma(7/24)\Gamma(11/24)}{\Gamma(19/24)\Gamma(23/24)}$$

Teorema. *Las constantes locales k_P asociadas a las funciones automorfas que uniformizan X_6 y sus cocientes son trascendentes. Más concretamente,*

(i) $k(P_3, X_6, t_6) \sim \frac{\Gamma(\frac{1}{4})\Gamma(\frac{5}{12})}{\Gamma(\frac{3}{4})\Gamma(\frac{11}{12})} \sim \pi_{-4}, \qquad \pi_{-4} = \frac{\Gamma(\frac{1}{4})^2}{\Gamma(\frac{3}{4})^2}.$

(ii) $k(P_4, X_6, t_6) \sim \frac{\Gamma(\frac{1}{3})^2\Gamma(\frac{7}{12})}{\Gamma(\frac{2}{3})^2\Gamma(\frac{11}{12})} \sim \pi_{-3}, \qquad \pi_{-3} = \frac{\Gamma(\frac{1}{3})^3}{\Gamma(\frac{2}{3})^3}.$

(iii) $k(P_0, X_6, t_6) \sim \frac{\Gamma(\frac{7}{24})\Gamma(\frac{11}{24})}{\Gamma(\frac{19}{24})\Gamma(\frac{23}{24})} \sim \pi_{-6}, \qquad \pi_{-6} = \left(\frac{\Gamma(\frac{1}{24})\Gamma(\frac{5}{24})\Gamma(\frac{7}{24})\Gamma(\frac{11}{24})}{\Gamma(\frac{13}{24})\Gamma(\frac{17}{24})\Gamma(\frac{19}{24})\Gamma(\frac{23}{24})}\right)^{1/2}.$

Demostración.

$\left(\frac{\pi_{-4}}{k(P_3,X_6,t_6)}\right)^4 = \frac{-256}{3}$, $\left(\frac{\pi_{-3}}{k(P_4,X_6,t_6)}\right)^{12} = \frac{-531441}{4}$, $\left(\frac{\pi_{-6}}{k(P_0,X_6,t_6)}\right)^2 = -4.$

Definición. Sea $P \in \mathcal{H}$ un punto de multiplicación compleja respecto de $\Phi : H(3,-1) \hookrightarrow \mathbf{M}(2,\mathbb{R})$ por un orden de discriminante $d < 0$. Sea $\Gamma \leq \mathbf{SL}(2,\mathbb{R})$ un subgrupo conmensurable con $\Gamma(6,1)$. Por definición, un *parámetro aritmético de uniformización local* en P por la acción de Γ_P es cualquier función

$$q_P(z) := \left(k\frac{z-P}{z-\overline{P}}\right)^{e_P},$$

en donde $e_P = \sharp\overline{\Gamma}_P$ y $k \sim \pi_d$.

Definición. Una función Γ-automorfa se denomina *aritmética en P* si posee un desarrollo en serie de potencias de q_P de coeficientes algebraicos.

Teorema. *Una función Γ-automorfa es aritmética en un punto CM si, y sólo si, es aritmética en todo punto CM.*

G. Frey, presentat per N. Vila

P. Bayer

A. Koblitz i N. Koblitz

P. Bayer i G. Frey

Representació (sènior) del STNB


Trio per amenitzar la festa amb Marcel·lí, Aleix i David

El pastís d'aniversari

Representació (júnior) del STNB