

# Aplicación de la descomposición racional univariada a Monstrous Moonshine

John McKay

David Sevilla

## Abstract

This paper shows how to use Computational Algebra techniques, namely the decomposition of rational functions in one variable, to explore a certain set of modular functions, called replicable functions, that arise in Monstrous Moonshine. This is an active topic in Mathematics that links the Monster group and complex analysis due to a surprising relation between the character table of the Monster and the coefficients of the expansions of certain modular functions. In particular, we have computed all the rational relations with coefficients in  $\mathbb{Z}$  between pairs of replicable functions.

## 1 Introducción

Las funciones modulares son objetos clásicos en teoría de números, y resultan de considerar la acción del grupo  $PSL_2(\mathbb{Z})$  sobre el plano hiperbólico (representado, por ejemplo, como el semiplano complejo superior). El estudio de ciertos grupos de transformaciones, conmensurables con  $PSL_2(\mathbb{Z})$  (es decir, aquellos cuya intersección tiene índice finito en ambos) proporciona una clase de funciones que quedan invariantes por ellos, de las que la clásica función  $j$  es representante. En concreto, los normalizadores de todos estos grupos en  $PSL_2(\mathbb{R})$  del subgrupo de matrices triangulares superiores módulo  $N$ .

En los años 70, McKay hizo notar que los coeficientes de ciertos desarrollos en serie de estas funciones (que son de hecho enteros positivos) están relacionados con las entradas de la tabla de caracteres del grupo monstruo  $M$ . Conway y Norton ([5]) formularon diversas conjeturas sobre estas funciones, que fueron probadas entre otras por Borcherds en [4]. A continuación presentamos brevemente algunas definiciones y resultados conocidos.

**Definición 1.1.** Dados  $\omega_1, \omega_2$  períodos de una función doblemente periódica con  $\tau = \omega_2/\omega_1 \in \mathcal{H} = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$ , la función  $J$  (conocida comúnmente como función modular de Klein) es

$$J(\omega_1, \omega_2) = \frac{g_2^3(\omega_1, \omega_2)}{\Delta(\omega_1, \omega_2)},$$

donde  $g_2, g_3$  son los invariantes de la función elíptica de Weierstrass con discriminante  $\Delta = g_2^3 - 27g_3^2$ .

Para cada  $\tau \in \mathcal{H}$ , definimos  $J(\tau) = J(1, \tau) = J(\omega_1, \omega_2)$ .

La función  $j$  se define clásicamente como

$$j(q) = 1728 \cdot J(\sqrt{q}).$$

Los primeros coeficientes de  $j$  son:

$$j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + \dots$$

**Definición 1.2.** El *grupo modular* es el grupo de transformaciones

$$z \rightarrow \frac{az + b}{cz + d}$$

donde  $a, b, c, d \in \mathbb{Z}, ad - bc = 1$ , representado proyectivamente por las matrices  $2 \times 2$  con coeficientes en  $\mathbb{Z}$ .

Las funciones con las que trabajamos son aquellas fijadas por grupos discretos  $G_f$ , es decir,

$$f(\gamma z) = f(z) \forall \gamma \in G_f.$$

En general, hay relaciones polinomiales entre cada dos de estas funciones. En particular, cuando uno de los grupos está contenido en el otro se tiene que una de las funciones se puede escribir como función racional de la otra (si los grupos son simplemente conmensurables, puede ser necesario tomar una potencia de  $q$  en la primera función).

En particular, las funciones replicables surgen como generalización de las funciones modulares relacionadas con el grupo  $\mathbb{M}$  (ver [1]). Nuestra aportación consiste en intentar refinar al máximo el poset de estas 619 funciones, encontrando relaciones entre ellas del tipo  $s_1 = f(s_2)$  con  $f \in \mathbb{C}(x)$  o  $f \in \mathbb{Q}(x)$ , donde  $s_1, s_2$  son series en  $q^{k_1}, q^{k_2}$ , y descomponiendo estas funciones racionales para encontrar cadenas maximales en ese poset.

Nuestros cálculos permiten, entre otras cosas, comprobar si la lista de 619 funciones contiene todas las funciones replicables, o si aparecen funciones de otras características especiales como resultado de este refinamiento.

## 2 Algoritmos

Tenemos el siguiente algoritmo elemental para encontrar relaciones racionales entre dos series en general.

**Algoritmo 2.1.**

ENTRADA: dos funciones replicables  $j_1$  y  $j_2$ .

SALIDA: una función  $f \in \mathbb{Q}(x)$  tal que  $j_1(q^r) = f(j_2(q))$  para algún  $r \in \mathbb{N}$ , si existe.

A. Calcular las áreas  $A_1, A_2$  de las regiones fundamentales de  $j_1$  y  $j_2$  respectivamente. Si  $e = A_2/A_1$  no es un número natural, terminar. Si lo es, sea  $r = 1$ .

B. Sea

$$f = \frac{t^e + a_{e-1}t^{e-1} + \dots + a_0}{t^{e-r} + b_{e-r-1}t^{e-r-1} + \dots + b_0}.$$

Sean  $s_1 = 1/q + \sum_{k=0}^{2e+1} c_k q^k$ ,  $s_2 = 1/q + \sum_{k=0}^{2e+1} d_k q^k$  las series truncadas de  $j_1$  y  $j_2$  respectivamente.

C. Resolver el sistema de ecuaciones lineales en las variables  $a_i, b_j$  dado por la anulaci3n del numerador de  $j_1(q^r) - f(j_2(q))$ . Si tiene soluci3n, devolver el  $f$  correspondiente.

D. Si  $r < e$ , incrementar  $r$  y volver a B. Si no, terminar.

Este es un algoritmo de complejidad baja, ya que las 1reas de las regiones fundamentales son conocidas (f1cilmente computables a partir de generadores de los grupos que las fijan) y calcular los coeficientes se hace a trav1s de la resoluci3n de sistemas de ecuaciones lineales. De esta manera construimos un grafo cuyos nodos son funciones modulares y cuyas aristas vienen dadas por pares de funciones relacionadas de la manera anterior.

El siguiente paso es utilizar un algoritmo propio de descomposici3n de funciones racionales univariadas, eficiente en la pr1ctica, para refinar todo lo posible este grafo. Este algoritmo, cuyos detalles pueden encontrarse en [9], est1 basado en una idea presentada en [2]. Damos a continuaci3n las definiciones y resultados m1s relevantes.

**Definici3n 2.2.** Definimos el *grado* de una funci3n racional como el m1ximo de los grados de su numerador y su denominador, suponiendo que no tienen factores comunes.

Una funci3n racional  $f \in \mathbb{K}(x)$  est1 en *forma normal* si  $\text{gr } f_N > \text{gr } f_D$  y  $f_N(0) = 0$  (por tanto  $f_D(0) \neq 0$ ).

**Lema 2.3.** Dada  $f \in \mathbb{K}(x)$ , si  $\text{gr } f < |\mathbb{K}|$  existen unidades  $u, v$  tales que  $u \circ f \circ v$  est1 en forma normal.

**Teorema 2.4.** Si  $f$  est1 en forma normal, toda descomposici3n suya es equivalente a una descomposici3n en la que ambas componentes est1n en forma normal.

**Teorema 2.5.** Sea  $f = g(h)$  con  $f, g, h$  en forma normal. Entonces  $h_N$  divide a  $f_N$  y  $h_D$  divide a  $f_D$ .

El teorema anterior nos proporciona el algoritmo de descomposici3n antes mencionado.

**Algoritmo 2.6.**

ENTRADA:  $f \in \mathbb{K}(x)$ .

SALIDA: todas las descomposiciones de  $f$  (es decir, al menos un representante de cada clase de equivalencia de descomposiciones).

A. Calcular unidades  $u, v$  como en el Lema 2.3. Sea  $\bar{f} = u \circ f \circ v$ .

B. Factorizar  $\bar{f}_N$  y  $\bar{f}_D$ . Sea  $D = \{(A_1, B_1), \dots, (A_m, B_m)\}$  el conjunto de pares  $(A, B)$  de polinomios m3nicos tales que  $A, B$  dividen a  $\bar{f}_N, \bar{f}_D$  respectivamente.

- C. Para cada  $i \in \{1, \dots, m\}$  comprobar si existe  $g \in \mathbb{K}(x)$  tal que  $\bar{f} = g \circ (A_i/B_i)$ . Si es así, añadir  $(u^{-1}(g), h(v^{-1}))$  a la lista de descomposiciones.
- D. Devolver la lista de descomposiciones (si no se ha encontrado ninguna,  $f$  es indescomponible).

### 3 Resultados

La utilización de esta combinación de técnicas nos ha permitido calcular este grafo refinado descomponiendo las relaciones en  $\mathbb{Q}(x)$  encontradas de acuerdo con este esquema:

$$j_1 \xrightarrow{d,r} j_2 \Rightarrow j_1(q^r) = f(j_2(q)), \text{ gr } f = d$$

$$f = g \circ h \Rightarrow \begin{cases} j_3(q^s) = h(j_2(q)) \\ j_1(q^r) = g(j_3(q^s)) \end{cases}$$

$$j_1 \xrightarrow{\text{gr } g,r/s} j_3 \xrightarrow{\text{gr } h,s} j_2$$

En el primer paso se obtuvieron 2419 relaciones. Se necesitaron aproximadamente 20 horas en un ordenador personal PC Pentium 4 utilizando el software de cálculo simbólico Maple para completar esta etapa; la mayor parte del tiempo se utilizó en el cálculo de coeficientes de las series involucradas por medio de una recurrencia. En la siguiente tabla mostramos los grados de las funciones racionales encontradas:

<i>grado</i>	<i>cantidad</i>	<i>grado</i>	<i>cantidad</i>
2	698	16	52
3	243	18	60
4	422	20	2
5	26	24	71
6	333	28	2
8	178	30	8
9	40	32	4
10	14	36	40
12	209	48	5
14	4	72	2
15	6		

En la etapa de descomposición, tras 30 horas de cálculo se computó el grafo buscado, que consta de 619 nodos y 1202 aristas.

El interés de los resultados obtenidos es múltiple. Por una parte, las relaciones obtenidas son una buena comprobación de que las tablas de datos conocidas son correctas, dado que no se han encontrado funciones nuevas mediante este método.

Por otra parte, también se han observado interesantes propiedades en algunas de las funciones racionales encontradas. El ejemplo más claro en ese sentido es la relación racional entre las funciones denotadas (1A) y (9B):

$$f = \frac{x^3(x+6)^3(x^2-6x+36)^3}{(x-3)^3(x^2+3x+9)^3}.$$

Durante el último paso fueron encontradas dos descomposiciones completas de  $f$ :

$$f = x^3 \circ \frac{x(x-12)}{x-3} \circ \frac{x(x+6)}{x-3} = \frac{x^3(x+24)}{x-3} \circ \frac{x(x^2-6x+36)}{x^2+3x+9}.$$

Esto significa que la función  $f$  tiene dos cadenas completas de descomposición de distinta longitud. Por lo que sabemos, es el primer ejemplo conocido de función racional en  $\mathbb{Q}(x)$  con esta propiedad; como contraste, es conocido que todas las cadenas completas de descomposición de polinomios con coeficientes en característica cero tienen la misma longitud (ver [7], [8]). Para más detalles al respecto, ver [9].

También es interesante notar que, en algunos casos, para dos series  $s_1, s_2$  encontramos más de una relación, es decir,  $s_1(q) = f_1(s_2(q^{k_1})) = f_2(s_2(q^{k_2}))$  con  $k_1 \neq k_2$ . Con una simple resultante podemos encontrar una relación polinomial del tipo  $P(s_2(q), s_2(q^k)) = 0$ . Estas relaciones tienen un interés propio en la teoría relativa al Monstrous Moonshine, siendo generalizaciones de los clásicos *polinomios modulares* para  $j$ .

Una posible línea de investigación inmediata consiste en calcular todas las descomposiciones de estas funciones en  $\mathbb{C}(x)$ , dado que se espera que las acciones no triviales que surgen sobre los grupos correspondientes proporcionen nuevas funciones de interés. También esperamos poder aplicar otras técnicas de Álgebra Computacional a aspectos relacionados dentro del Monstrous Moonshine.

## References

- [1] D. Alexander, C. Cummins, J. McKay, C. Simons, *Completely replicable functions*. Groups, Combinatorics and Geometry (Durham, 1990), 87–98, London Math. Soc. Lecture Note Ser., 165, Cambridge University Press, Cambridge, 1992.
- [2] C. Alonso, J. Gutiérrez, T. Recio, *A rational function decomposition algorithm by near-separated polynomials*. J. Symbolic Comput. 19 (1995), no. 6, 527–544.
- [3] T. M. Apostol, *Modular functions and Dirichlet series in number theory*. 2nd ed. Springer-Verlag, New York, 1997.
- [4] R. E. Borcherds, *Monstrous Moonshine and monstrous Lie superalgebras*. Invent. Math. 109 (1992), no. 2, 405–444.
- [5] J. H. Conway, S. P. Norton, *Monstrous Moonshine*. Bull. London Math. Soc. 11 (1979), no. 3, 308–339.

- [6] J. Gutiérrez, R. Rubio, D. Sevilla, *Unirational fields of transcendence degree one and functional decomposition*. ISSAC 2001, London, Canada, 167–174.
- [7] J. F. Ritt, *Prime and composite polynomials*. Trans. Amer. Math. Soc. 23 (1922), no. 1, 51–66.
- [8] A. Schinzel, *Polynomials with special regard to reducibility*. Cambridge University Press, New York, 2000.
- [9] D. Sevilla, *Ritt's Theorems and computation of unirational fields*. Ph. D. Thesis Dissertation. University of Cantabria, 2004.

David Sevilla González  
Dpto. de Matemáticas, Estadística y Computación - Facultad de Ciencias  
Universidad de Cantabria  
Av. de los Castros s/n  
39071 Santander (Cantabria)  
david.sevilla@unican.es

John McKay  
Sir George Williams Campus  
1455 De Maisonneuve Blvd. West  
LB 903 15  
Montreal, QC, Canada, H3G 1M8  
mckay@cs.concordia.ca