¿Quieres ganar un millón de dólares ? ¡Resuelve el problema de los timbres !

J.L. Ramírez Alfonsín

IMAG, Université de Montpellier, Francia
UMI J.-C. Yaccoz - CNRS/IMPA, Brasil

Mérida, 16 Octubre 2019

Problema de los timbres : propuesto por Ian Stewart

How hard can it be?

Deliver the solution to an everyday puzzle and you could win the biggest prize in mathematics, says **Ian Stewart**

EVER since a Babylonian scribe decided to teach his students arithmetic by setting them problems using the formula "I found a stone but did not weigh it..." mathematicians have celebrated the hidden depths of apparently everyday problems. They have found inspiration in slicing pies, tying knots and spinning coins. But even mathematicians have been surprised by the depth of the mystery that lurks behind an innocent question about postage stamps.

Suppose that your post office sells stamps with just two values: 2 cents and 5 cents. By combining these values, you can make up almost any whole number of cents. For example, to post a letter costing 9¢, you could stick one 5¢ stamp and two 2¢ stamps on the envelope. Two values that you cannot achieve are 1¢ and 3¢ – and in fact these are the only impossible amounts. You can produce any even amount using 2¢ stamps – given a big enough envelope – and any odd value from 5¢ upwards, using one 5¢ stamp and multiple 2¢ stamps.

This example is typical. Given an unlimited supply of stamps, there is always some key value above which any total can be achieved by sticking the right combination of stamps on the envelope. This is also true if you have more than two denominations of stamp available.

But the million-dollar question is this: with *n* denominations of stamps available, what is that key value? The first person to consider a simple version of this question was James Joseph Sylvester in 1883 (to be precise, he was dealing with coins, but for our purposes we'll stick with stamps). Sylvester came up with a simple formula for finding this key value when dealing with just two denominations (see "Pushing the envelope", page 48).

In its general form, the postage-stamp problem really could be a million-dollar question: the Clay Mathematics Institute in Cambridge, Massachusetts, is offering exactly that amount to anyone who can solve a problem that is logically equivalent to it. We now have tantalising new hints that the postage-stamp problem – and therefore, perhaps, the related million-dollar enigma – might not be as daunting as it appears. So considering how to pay for posting our mail might lead to a breakthrough in one of the most significant mathematical problems of the 21st century.

It will never compute

The issue centres around the cost of solving a problem – not in dollars and cents, but in computational effort. We measure the difficulty of a calculation by the number of basic computational steps needed to complete it: for a particular size of problem – often measured in terms of the number of digits in the number to be crunched – what is the "running time" of the algorithm concerned? If the problem concerns 50-digit numbers rather than 25-digit numbers, say, how much longer does the algorithm take to get the answer? What about 100-digit numbers, or any number of digits? It should be noted that this running time is an abstract notion, related but not equivalent to the actual time taken by any given computer.

In broad terms, a computational method is practical – "efficient" or "easy", if you prefer to look at it that way – if the running time grows in step with some fixed power of the number of digits required to pose the question. For example, an algorithm for testing a number *n* to see whether it is prime may have a running time linked to the sixth power of the number of digits of *n*.

Such algorithms are said to be "class P", where the "P" stands for "polynomial". Algorithms that run in polynomial time are relatively stable: they do not get wildly slower with small increases in the size of the input. In contrast, non-P algorithms are generally impractical – "inefficient" or "hard" – and become unmanageable with relatively small increases in input size. It's not quite that straightforward, because some non-P algorithms are pretty efficient until the input size gets very big indeed, while some P algorithms depend on a parameter which is so large that they couldn't actually run within a human lifetime. Nevertheless, the distinction between P and non-P seems to be the most basic and important distinction in problems about the efficiency of algorithms – a way to formalise the intuitive ideas of "easy to compute" versus "hard to compute".

Are there any such things as truly hard problems? Yes, several kinds. The obvious ones are hard for a simple reason, such as printing out the answer takes too long. A good example is "print all ways to rearrange this list of symbols". With the 52 symbols in a pack of cards, the list would contain 80,658,175,170,943,878,571,660,636,856,403,766,975,289,505,440,883,277,824,000,000,000,000 arrangements, and you'd have to print the lot. These types of problem have to be excluded, which we do by introducing another class of algorithm, confusingly called NP, which run in "nondeterministic polynomial" time.

A problem is NP if any proposed solution can be checked to determine whether it is right or wrong, in polynomial time – that is, in reasonable time. A rough analogy is solving a jigsaw puzzle. However long it takes to work out how to fit the pieces together – the nondeterministic aspect – a brief glance at the result usually reveals whether it is correct.

All this classification has led to a rather fundamental question, and whoever cracks it will take the Clay prize: is NP really any different from P? To put it plainly, if it is easy to check the accuracy of any proposed ▸

Problema de los timbres

Dados n timbres de valores $a_1, \ldots, a_n$ con $\gcd(a_1, \ldots, a_n) = 1$ (tenemos tantos timbres de valor a_i como queramos)
¿Cuál es el entero mas grande a partir del cual cualquier valor puede ser alcanzada pegando una combinación exacta de timbress en el sobre ?

Problema de los timbres

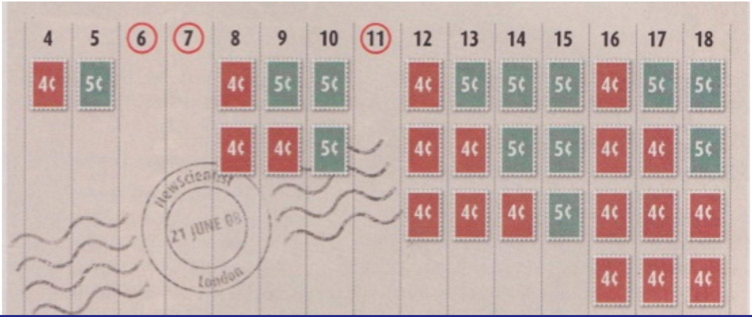
Dados n timbres de valores $a_1, \ldots, a_n$ con $\gcd(a_1, \ldots, a_n) = 1$ (tenemos tantos timbres de valor a_i como queramos)
¿Cuál es el entero mas grande a partir del cual cualquier valor puede ser alcanzada pegando una combinación exacta de timbress en el sobre ?

Ejemplo : Dos timbres de 4¢ y 5¢

Problema de los timbres

Dados n timbres de valores $a_1, \ldots, a_n$ con $\gcd(a_1, \ldots, a_n) = 1$ (tenemos tantos timbres de valor a_i como queramos)
¿Cuál es el entero mas grande a partir del cual cualquier valor puede ser alcanzada pegando una combinación exacta de timbress en el sobre ?

Ejemplo : Dos timbres de 4¢ y 5¢



Problema diofántico de Frobenius

Sean $a_1, \ldots, a_n$ enteros positivos. Diremos que el entero s es representable por $a_1, \ldots, a_n$ si existen enteros $x_i \geq 0$ tales que

$$s = \sum_{i=1}^{n} x_i a_i.$$

Problema diofántico de Frobenius

Sean $a_1, \ldots, a_n$ enteros positivos. Diremos que el entero s es representable por $a_1, \ldots, a_n$ si existen enteros $x_i \geq 0$ tales que

$$s = \sum_{i=1}^{n} x_i a_i.$$

Supongamos que $\gcd(a_1, \ldots, a_n) = 1$.

Problema diofántico de Frobenius

Sean $a_1, \ldots, a_n$ enteros positivos. Diremos que el entero s es representable por $a_1, \ldots, a_n$ si existen enteros $x_i \geq 0$ tales que

$$s = \sum_{i=1}^{n} x_i a_i.$$

Supongamos que $\gcd(a_1, \ldots, a_n) = 1$. El célebre **problema diofántico de Frobenius** plantea encontrar el entero más grande que **<u>no</u>** es representable por $a_1, \ldots, a_n$.

Problema diofántico de Frobenius

Sean $a_1, \ldots, a_n$ enteros positivos. Diremos que el entero s es representable por $a_1, \ldots, a_n$ si existen enteros $x_i \geq 0$ tales que

$$s = \sum_{i=1}^{n} x_i a_i.$$

Supongamos que $\gcd(a_1, \ldots, a_n) = 1$. El célebre **problema diofántico de Frobenius** plantea encontrar el entero más grande que **no** es representable por $a_1, \ldots, a_n$. (denotado como $g(a_1, \ldots, a_n)$ y llamado número de Frobenius).

Problema diofántico de Frobenius

Sean $a_1, \ldots, a_n$ enteros positivos. Diremos que el entero s es representable por $a_1, \ldots, a_n$ si existen enteros $x_i \geq 0$ tales que

$$s = \sum_{i=1}^{n} x_i a_i.$$

Supongamos que $\gcd(a_1, \ldots, a_n) = 1$. El célebre **problema diofántico de Frobenius** plantea encontrar el entero más grande que **no** es representable por $a_1, \ldots, a_n$. (denotado como $g(a_1, \ldots, a_n)$ y llamado número de Frobenius).

Ejemplo : $a_1 = 3$, $a_2 = 8$

Problema diofántico de Frobenius

Sean $a_1, \ldots, a_n$ enteros positivos. Diremos que el entero s es representable por $a_1, \ldots, a_n$ si existen enteros $x_i \geq 0$ tales que

$$s = \sum_{i=1}^{n} x_i a_i.$$

Supongamos que $\gcd(a_1, \ldots, a_n) = 1$. El célebre **problema diofántico de Frobenius** plantea encontrar el entero más grande que **no** es representable por $a_1, \ldots, a_n$. (denotado como $g(a_1, \ldots, a_n)$ y llamado número de Frobenius).

Ejemplo : $a_1 = 3$, $a_2 = 8$

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 $\cdots$

Problema diofántico de Frobenius

Sean $a_1, \ldots, a_n$ enteros positivos. Diremos que el entero s es representable por $a_1, \ldots, a_n$ si existen enteros $x_i \geq 0$ tales que

$$s = \sum_{i=1}^{n} x_i a_i.$$

Supongamos que $\gcd(a_1, \ldots, a_n) = 1$. El célebre **problema diofántico de Frobenius** plantea encontrar el entero más grande que **no** es representable por $a_1, \ldots, a_n$. (denotado como $g(a_1, \ldots, a_n)$ y llamado número de Frobenius).

Ejemplo : $a_1 = 3$, $a_2 = 8$

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 $\cdots$ Entonces $g(3, 8) = 13$.

Teorema $g(a_1, \ldots, a_n)$ existe y es finito.

Teorema $g(a_1, \ldots, a_n)$ existe y es finito.

Prueba (idea). Como $\gcd(a_1, \ldots, a_n) = 1$ entonces

$m_1 a_1 + \cdots + m_n a_n = 1$ para algún $m_i \in \mathbb{Z}$

Teorema $g(a_1, \ldots, a_n)$ existe y es finito.

Prueba (idea). Como $\gcd(a_1, \ldots, a_n) = 1$ entonces

$m_1 a_1 + \cdots + m_n a_n = 1$ para algún $m_i \in \mathbb{Z}$

Sea P y $-Q$ la suma de términes positivos y negativos respectivamente (por lo que $P - Q = 1$).

Teorema $g(a_1, \ldots, a_n)$ existe y es finito.

Prueba (idea). Como $\gcd(a_1, \ldots, a_n) = 1$ entonces

$m_1 a_1 + \cdots + m_n a_n = 1$ para algún $m_i \in \mathbb{Z}$

Sea P y $-Q$ la suma de términes positivos y negativos respectivamente (por lo que $P - Q = 1$).

Sea $k \geq 0$, tenemos que $(a_1 - 1)Q + k = (a_1 - 1)Q + ha_1 + k'$ con $h \geq 0$ y $0 < k' < a_1$.

Teorema $g(a_1, \ldots, a_n)$ existe y es finito.

Prueba (idea). Como $\gcd(a_1, \ldots, a_n) = 1$ entonces

$m_1 a_1 + \cdots + m_n a_n = 1$ para algún $m_i \in \mathbb{Z}$

Sea P y $-Q$ la suma de términes positivos y negativos respectivamente (por lo que $P - Q = 1$).

Sea $k \geq 0$, tenemos que $(a_1 - 1)Q + k = (a_1 - 1)Q + ha_1 + k'$ con $h \geq 0$ y $0 < k' < a_1$.

Entonces, $(a_1 - 1)Q + k = ha_1 + (a_1 - 1 - k')Q + k'P$.

Algoritmos

Cuando $n = 3$

- Selmer, Bayer, 1978
- Rödseth, 1978
- Davison, 1994
- Scarf, Shallcross, 1993

Algoritmos

Cuando $n = 3$

- Selmer, Bayer, 1978
- Rödseth, 1978
- Davison, 1994
- Scarf, Shallcross, 1993

Cuando $n \geq 4$

- Heap, Lynn, 1964
- Wilf, 1978
- Nijenhuis, 1979
- Greenberg, 1980
- Killingbergto, 2000
- Einstein, Lichtblau, Strzebonski, Wagon, 2007
- Roune, 2008

Los algoritmos más rápidos

Método de Einstein, Lichtblau, Strzebonski, Wagon (2008)

Calcula $g(a_1, \ldots, a_4)$ números con 100 cifras en algunos segundos

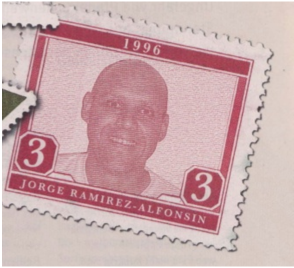
Calcula $g(a_1, \ldots, a_{10})$ números con 10 cifras en dos días

Los algoritmos más rápidos

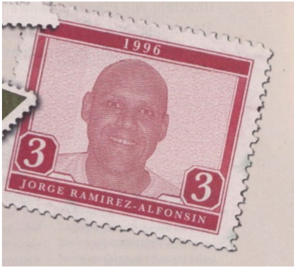
Método de Roune (2008)

Calcula $g(a_1, \ldots, a_4)$ números con 10 000 cifras en algunos segundos

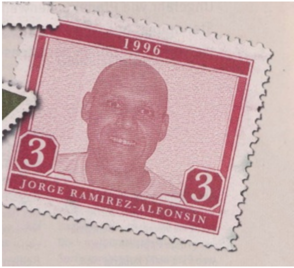
Calcula $g(a_1, \ldots, a_{13})$ números con 10 cifras en algunos días



Teorema (R.A., 1996) $g(a_1, \ldots, a_n)$ es $\mathcal{NP}$-difícil.



Teorema (R.A., 1996) $g(a_1, \ldots, a_n)$ es $\mathcal{NP}$-difícil.
La existencia de un método polinomial para calcular $g(a_1, \ldots, a_n)$ implicaría que ¡$\mathcal{NP} = \mathcal{P}$! Esto daría una respuesta negativa a la pregunta : ¿es verdad que $\mathcal{NP} \neq \mathcal{P}$?



Teorema (R.A., 1996) $g(a_1, \ldots, a_n)$ es $\mathcal{NP}$-difícil.
La existencia de un método polinomial para calcular $g(a_1, \ldots, a_n)$ implicaría que ¡$\mathcal{NP} = \mathcal{P}$! Esto daría una respuesta negativa a la pregunta : ¿es verdad que $\mathcal{NP} \neq \mathcal{P}$?
Uno de los siete famosos problemas por los que el Instituto Clay (USA) ofrece un premio de 1 millón de dólares por la solución de cada uno de los problemas.

Método de Kannan

Teorema (Kannan, 1992) Existe un algoritmo polinomial que détermina $g(a_1, \ldots, a_n)$ cuando $n \geq 2$ es **fijo**.

Sea P un conjunto cerrado y acotado de $\mathbb{R}^n$ y sea L una latiz de dimensión n también en $\mathbb{R}^n$.

Sea P un conjunto cerrado y acotado de $\mathbb{R}^n$ y sea L una latiz de dimensión n también en $\mathbb{R}^n$.
El más pequeño real positivo t tal que $tP + L$ sea igual a $\mathbb{R}^n$ es llamado covering radius de P con respecto a L (denotado por $\mu(P, L)$).

Sea P un conjunto cerrado y acotado de $\mathbb{R}^n$ y sea L una latiz de dimensión n también en $\mathbb{R}^n$.
El más pequeño real positivo t tal que $tP + L$ sea igual a $\mathbb{R}^n$ es llamado covering radius de P con respecto a L (denotado por $\mu(P, L)$).
Teorema (Kannan, 1992) Sean

$$L = \{(x_1, \ldots, x_{n-1}) | x_i \text{ enteros y } \sum_{i=1}^{n-1} a_i x_i \equiv 0 \bmod a_n\} \text{ y}$$

$$S = \{(x_1, \ldots, x_{n-1}) | x_i \geq 0 \text{ reales y } \sum_{i=1}^{n-1} a_i x_i \leq 1\}.$$

Sea P un conjunto cerrado y acotado de $\mathbb{R}^n$ y sea L una latiz de dimensión n también en $\mathbb{R}^n$.

El más pequeño real positivo t tal que $tP + L$ sea igual a $\mathbb{R}^n$ es llamado covering radius de P con respecto a L (denotado por $\mu(P, L)$).

Teorema (Kannan, 1992) Sean

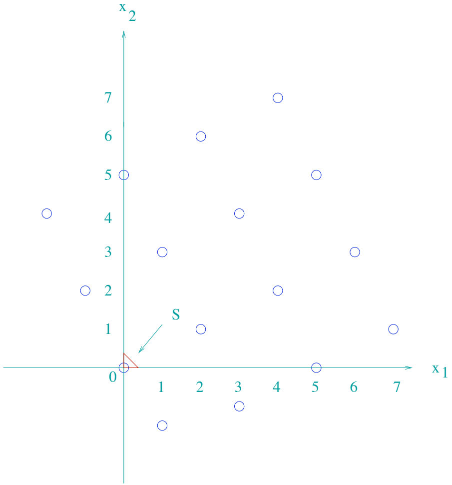
$$L = \{(x_1, \ldots, x_{n-1}) | x_i \text{ enteros y } \sum_{i=1}^{n-1} a_i x_i \equiv 0 \bmod a_n\} \text{ y}$$

$$S = \{(x_1, \ldots, x_{n-1}) | x_i \geq 0 \text{ reales y } \sum_{i=1}^{n-1} a_i x_i \leq 1\}.$$

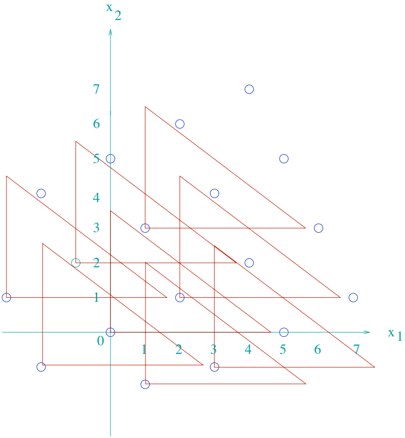
Entonces, $\mu(S, L) = g(a_1, \ldots, a_n) + a_1 + \cdots + a_n$.

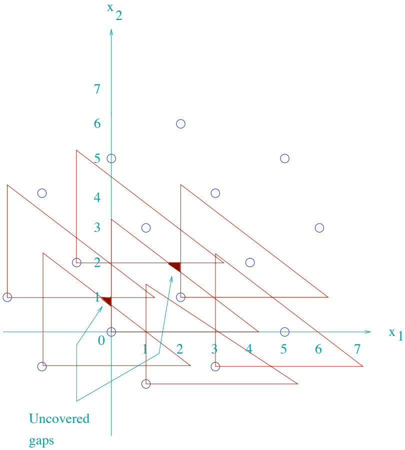
Ejemplo : Sean $a_1 = 3, a_2 = 4$ y $a_3 = 5$.

Ejemplo : Sean $a_1 = 3, a_2 = 4$ y $a_3 = 5$.



Ejemplo cont ... Notemos que $14S$ cubre el plano pero $13S$ no lo cubre. Entonces, $\mu(L,S)=14$ y $g(3,4,5)=2$.



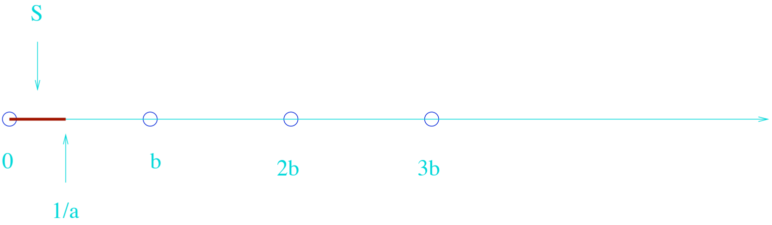


Fórmulas

Fórmulas

Teorema (Sylvester, 1883) $g(a, b) = ab - a - b$.

Prueba Sea a, b dos enteros positivos tales que $\gcd(a, b) = 1$.



El más pequeño real t tal que tS cubre el intervalo $[0, b]$ es ab.

Entonces, $g(a, b) = \mu(S, L) - a - b = ab - a - b$.

Pregunta : ¿Existe una fórmula similar para $g(a_1, a_2, a_3)$?

Pregunta : ¿Existe una fórmula similar para $g(a_1, a_2, a_3)$?

Teorema (Curtis, 1990) No existe un conjunto finito de polinomios $\{h_1, \ldots, h_m\}$ tales que para cada tripleta a_1, a_2, a_3 hay alguna i tal que $h_i(a_1, a_2, a_3) = g(a_1, a_2, a_3)$.

Pregunta : ¿Existe una fórmula similar para $g(a_1, a_2, a_3)$?

Teorema (Curtis, 1990) No existe un conjunto finito de polinomios $\{h_1, \ldots, h_m\}$ tales que para cada tripleta a_1, a_2, a_3 hay alguna i tal que $h_i(a_1, a_2, a_3) = g(a_1, a_2, a_3)$.

Pregunta : ¿Existe una fórmula **semi-explicita** para $g(a_1, a_2, a_3)$?

Sean L_1, L_2 y L_3 los enteros positivos más pequeños tales que existen enteros $x_{ij} \geq 0$, $1 \leq i, j \leq 3$, $i \neq j$ con

$$\begin{aligned} L_1 a_1 &= x_{12} a_2 + x_{13} a_3, \\ L_2 a_2 &= x_{21} a_1 + x_{23} a_3, \\ L_3 a_3 &= x_{31} a_1 + x_{32} a_2. \end{aligned}$$

Sean L_1, L_2 y L_3 los enteros positivos más pequeños tales que existen enteros $x_{ij} \geq 0$, $1 \leq i, j \leq 3$, $i \neq j$ con

$$\begin{aligned} L_1 a_1 &= x_{12} a_2 + x_{13} a_3, \\ L_2 a_2 &= x_{21} a_1 + x_{23} a_3, \\ L_3 a_3 &= x_{31} a_1 + x_{32} a_2. \end{aligned}$$

Teorema (Denham 2000, R.A., Rødseth 2008) Sean a_1, a_2, a_3 enteros positivos primos relativos y $\{i, j, k\} = \{1, 2, 3\}$. Entonces,

$$g(a_1, a_2, a_3) = \begin{cases} \max\{L_i a_i + x_{jk} a_k, L_j a_j + x_{ik} a_k\} - \sum_{n=1}^{3} a_n & \text{si } x_{ij} > 0 \\ & \text{para todo } i, j, \\ L_j a_j + L_i a_i - \sum_{n=1}^{3} a_n & \text{si } x_{ij} = 0. \end{cases}$$

Huecos

Huecos

Un semigrupo numérico es un subconjunto $\mathcal{S}$ de $\mathbb{N}$ que contiene al cero, que es estable bajo adiciones y con complemento finito $\mathbb{N} \setminus \mathcal{S}$.

Huecos

Un semigrupo numérico es un subconjunto $\mathcal{S}$ de $\mathbb{N}$ que contiene al cero, que es estable bajo adiciones y con complemento finito $\mathbb{N} \setminus \mathcal{S}$.

Denotaremos $\langle a_1, \ldots, a_n \rangle$ el semigrupo numérico generado por $a_1, \ldots, a_n$, esto es, el conjunto de enteros que son representables por $a_1, \ldots, a_n$.

Huecos

Un semigrupo numérico es un subconjunto $\mathcal{S}$ de $\mathbb{N}$ que contiene al cero, que es estable bajo adiciones y con complemento finito $\mathbb{N} \setminus \mathcal{S}$.

Denotaremos $\langle a_1, \ldots, a_n \rangle$ el semigrupo numérico generado por $a_1, \ldots, a_n$, esto es, el conjunto de enteros que son representables por $a_1, \ldots, a_n$.

Los elementos $\mathbb{N} \setminus \mathcal{S}$ son llamados huecos de $\mathcal{S}$ y su cardinal, denotado por $k(\mathcal{S})$, es llamado el género de $\mathcal{S}$.

Teorema (Sylvester 1882) $k(\langle a, b\rangle) = \frac{g(a,b)-1}{2}$.

Teorema (Sylvester 1882) $k(\langle a, b\rangle) = \frac{g(a,b)-1}{2}$.

Teorema (Nijenhuis, Wilf 1972) $k(\langle a_1, \ldots, a_n\rangle) \geq \frac{g(a_1,\ldots,a_n)-1}{2}$.

Teorema (Sylvester 1882) $k(\langle a, b\rangle) = \frac{g(a,b)-1}{2}$.

Teorema (Nijenhuis, Wilf 1972) $k(\langle a_1, \ldots, a_n\rangle) \geq \frac{g(a_1,\ldots,a_n)-1}{2}$.

Un semigrupo es simétrico si $k(\langle a_1, \ldots, a_n\rangle) = \frac{g(a_1,\ldots,a_n)-1}{2}$.

Teorema (Sylvester 1882) $k(\langle a, b\rangle) = \frac{g(a,b)-1}{2}$.

Teorema (Nijenhuis, Wilf 1972) $k(\langle a_1, \dots, a_n\rangle) \geq \frac{g(a_1,\dots,a_n)-1}{2}$.

Un semigrupo es simétrico si $k(\langle a_1, \dots, a_n\rangle) = \frac{g(a_1,\dots,a_n)-1}{2}$.

Noción interesante : ramas algebraicas planas, curvas monomiales, anillos locales Noetherianos, teoría de códigos, etc.

Teorema (Sylvester 1882) $k(\langle a, b\rangle) = \frac{g(a,b)-1}{2}$.

Teorema (Nijenhuis, Wilf 1972) $k(\langle a_1, \ldots, a_n\rangle) \geq \frac{g(a_1,\ldots,a_n)-1}{2}$.

Un semigrupo es simétrico si $k(\langle a_1, \ldots, a_n\rangle) = \frac{g(a_1,\ldots,a_n)-1}{2}$.

Noción interesante : ramas algebraicas planas, curvas monomiales, anillos locales Noetherianos, teoría de códigos, etc.

Pregunta : Dado $k \in \mathbb{N}$ ¿cuál es el número n_k de semigrupos numéricos S de género k ?

Teorema (Sylvester 1882) $k(\langle a, b\rangle) = \frac{g(a,b)-1}{2}$.

Teorema (Nijenhuis, Wilf 1972) $k(\langle a_1, \ldots, a_n\rangle) \geq \frac{g(a_1,\ldots,a_n)-1}{2}$.

Un semigrupo es simétrico si $k(\langle a_1, \ldots, a_n\rangle) = \frac{g(a_1,\ldots,a_n)-1}{2}$.

Noción interesante : ramas algebraicas planas, curvas monomiales, anillos locales Noetherianos, teoría de códigos, etc.

Pregunta : Dado $k \in \mathbb{N}$ ¿cuál es el número n_k de semigrupos numéricos S de género k ?

Teorema (Bras-Amorós 2008) Determinó n_k para todo $k \leq 50$.

Teorema (Sylvester 1882) $k(\langle a, b\rangle) = \frac{g(a,b)-1}{2}$.

Teorema (Nijenhuis, Wilf 1972) $k(\langle a_1, \ldots, a_n\rangle) \geq \frac{g(a_1,\ldots,a_n)-1}{2}$.

Un semigrupo es simétrico si $k(\langle a_1, \ldots, a_n\rangle) = \frac{g(a_1,\ldots,a_n)-1}{2}$.

Noción interesante : ramas algebraicas planas, curvas monomiales, anillos locales Noetherianos, teoría de códigos, etc.

Pregunta : Dado $k \in \mathbb{N}$ ¿cuál es el número n_k de semigrupos numéricos S de género k ?

Teorema (Bras-Amorós 2008) Determinó n_k para todo $k \leq 50$.

Conjetura (Bras-Amorós 2008) $n_k \geq n_{k-1} + n_{k-2}$ para todo k (desigualdad **tipo- Fibonacci**)

Sea $n(k,l)$ el número de semigrupos numéricos de género k y con un conjunto minimal generador de cardinal l.

Sea $n(k,l)$ el número de semigrupos numéricos de género k y con un conjunto minimal generador de cardinal l.

Teorema (R.A., Eliahou 2011) $n(2^k, 2) = \frac{s+1}{2}$ donde s es el factor más grande de $k+1$.

Sea $n(k,l)$ el número de semigrupos numéricos de género k y con un conjunto minimal generador de cardinal l.

Teorema (R.A., Eliahou 2011) $n(2^k,2)=\frac{s+1}{2}$ donde s es el factor más grande de $k+1$.

¿Que podemos decir para $n(p^k,2)$ para $p\geq 3$ primo ?

Sea $n(k, l)$ el número de semigrupos numéricos de género k y con un conjunto minimal generador de cardinal l.

Teorema (R.A., Eliahou 2011) $n(2^k, 2) = \frac{s+1}{2}$ donde s es el factor más grande de $k+1$.

¿Que podemos decir para $n(p^k, 2)$ para $p \geq 3$ primo ?

Podemos demostrar que $n(p^k, 2)$ es igual al número de índices $i \in \{0, \ldots, k\}$ tales que

$$\gcd(p^i + 1, 2p^{k-i} + 1) = 1.$$

En el caso $i = k - 1$ con $k = 2^t + 1$ se puede demostrar que

$$\gcd(p^{2^t} + 1, 2p + 1) = \gcd(2^{2^t} + 1, 2p + 1).$$

En el caso $i = k - 1$ con $k = 2^t + 1$ se puede demostrar que

$$\gcd(p^{2^t} + 1, 2p + 1) = \gcd(2^{2^t} + 1, 2p + 1).$$

Entonces para determinar $n(p^k, 2)$ se requiere saber, en particular, cuando $\gcd(2^{2^t} + 1, 2p + 1) = 1$.

En el caso $i = k - 1$ con $k = 2^t + 1$ se puede demostrar que

$$\gcd(p^{2^t} + 1, 2p + 1) = \gcd(2^{2^t} + 1, 2p + 1).$$

Entonces para determinar $n(p^k, 2)$ se requiere saber, en particular, cuando $\gcd(2^{2^t} + 1, 2p + 1) = 1$.

i.e., se requiere saber la factorización del número de Fermat $F_t = 2^{2^t} + 1$.

En el caso $i = k - 1$ con $k = 2^t + 1$ se puede demostrar que

$$\gcd(p^{2^t} + 1, 2p + 1) = \gcd(2^{2^t} + 1, 2p + 1).$$

Entonces para determinar $n(p^k, 2)$ se requiere saber, en particular, cuando $\gcd(2^{2^t} + 1, 2p + 1) = 1$.

i.e., se requiere saber la factorización del número de Fermat $F_t = 2^{2^t} + 1$.

El record en 2010, la factorización de F_t es conocida completamente solo para $t \leq 11$.

(W. Keller, Prime factors $k2^n + 1$ of Fermat numbers F_m and complete factoring status, web page available at `http://www.prothsearch.net/fermat.html`).

Poset

Poset

Sea $(\mathcal{P}, \leq)$ un poset localmente finito, i.e,

- el conjunto $\mathcal{P}$ es ordenado parcialmente por $\leq$,
- para cada $a, b \in \mathcal{P}$ el conjunto $\{c \in \mathcal{P} \mid a \leq c \leq b\}$ es finito.

Poset

Sea $(\mathcal{P}, \leq)$ un poset localmente finito, i.e,

- el conjunto $\mathcal{P}$ es ordenado parcialmente por $\leq$,
- para cada $a, b \in \mathcal{P}$ el conjunto $\{c \in \mathcal{P} \,|\, a \leq c \leq b\}$ es finito.

Una cadena de longitud $l \geq 0$ entre $a, b \in \mathcal{P}$ es

$$\{a = a_0 < a_1 < \cdots < a_l = b\} \subset \mathcal{P}.$$

Sea $c_l(a, b)$ el número de cadenas de longitud l entre a y b.

Poset

Sea $(\mathcal{P}, \leq)$ un poset localmente finito, i.e,

- el conjunto $\mathcal{P}$ es ordenado parcialmente por $\leq$,
- para cada $a, b \in \mathcal{P}$ el conjunto $\{c \in \mathcal{P} \mid a \leq c \leq b\}$ es finito.

Una cadena de longitud $l \geq 0$ entre $a, b \in \mathcal{P}$ es

$$\{a = a_0 < a_1 < \cdots < a_l = b\} \subset \mathcal{P}.$$

Sea $c_l(a, b)$ el número de cadenas de longitud l entre a y b.

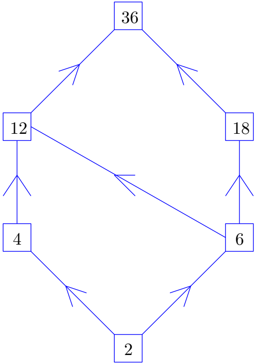
La función de Möbius $\mu_{\mathcal{P}}$ es definida por

$$\mu_{\mathcal{P}} : \mathcal{P} \times \mathcal{P} \longrightarrow \mathbb{Z}$$

$$\mu_{\mathcal{P}}(a, b) = \sum_{l \geq 0} (-1)^l c_l(a, b).$$

Consideremos el poset $(\mathbb{N}, |\,)$ de enteros no negativos ordenados por la divisibilidad, i.e., $a \mid b \iff a$ divide b. Calculemos $\mu_{\mathbb{N}}(2, 36)$. Como $\{c \in \mathbb{N};\ 2 \mid c \mid 36\} = \{2, 4, 6, 12, 18, 36\}$ entonces las cadenas de

- longitud 1 $\rightarrow$ $\{2, 36\}$
- longitud 2 $\left\{\begin{array}{c}\{2,4,36\}\\ \{2,6,36\}\\ \{2,12,36\}\\ \{2,18,36\}\end{array}\right.$
- longitud 3 $\left\{\begin{array}{c}\{2,4,12,36\}\\ \{2,6,12,26\}\\ \{2,6,18,36\}\end{array}\right.$



Obteniendo,

$\mu_{\mathbb{N}}(2, 36) = -c_1(2, 36) + c_2(2, 36) - c_3(2, 36) = -1 + 4 - 3 = 0.$

La función aritmética de Möbius clásica

Dado $n \in \mathbb{N}$ la función aritmética de Möbius $\mu(n)$ es definida como

$$\mu(n) = \begin{cases} 1 & \textit{si } n = 1 \\ (-1)^k & \textit{si } n = p_1 \cdots p_k \text{ con } p_i \textit{ primos diferentes} \\ 0 & \textit{sino } (i.e; n \textit{ admite al menos un factor cuadrado} \\ & \textit{mas grande que uno}) \end{cases}$$

La función aritmética de Möbius clásica

Dado $n \in \mathbb{N}$ la función aritmética de Möbius $\mu(n)$ es definida como

$$\mu(n) = \begin{cases} 1 & si \;\; n = 1 \\ (-1)^k & si \;\; n = p_1 \cdots p_k \text{ con } p_i \; primos \; diferentes \\ 0 & sino \; (i.e; \; n \; admite \; al \; menos \; un \; factor \; cuadrado \\ & mas \; grande \; que \; uno) \end{cases}$$

Ejemplo : $\mu(2) = \mu(7) = -1, \mu(4) = \mu(8) = 0, \mu(6) = \mu(10) = 1$

La función aritmética de Möbius clásica

Dado $n \in \mathbb{N}$ la función aritmética de Möbius $\mu(n)$ es definida como

$$\mu(n) = \begin{cases} 1 & si \;\; n = 1 \\ (-1)^k & si \;\; n = p_1 \cdots p_k \text{ con } p_i \; primos \; diferentes \\ 0 & sino \; (i.e; \; n \; admite \; al \; menos \; un \; factor \; cuadrado \\ & mas \; grande \; que \; uno) \end{cases}$$

Ejemplo : $\mu(2) = \mu(7) = -1, \mu(4) = \mu(8) = 0, \mu(6) = \mu(10) = 1$

La función inversa de Riemann ζ, $s \in \mathbb{C}, Re(s) > 0$

$$\zeta^{-1}(s) = \left(\sum_{n=1}^{+\infty} \frac{1}{n^s}\right)^{-1} = \prod_{p-prime} (1 - p^{-1}) = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^2}.$$

Hay resultados impresionantes que usan μ.

Ejemplo : Para un entero n

$$Pr(n \textit{ no tenga factores cuadrados }) = \frac{6}{\pi^2}$$

Hay resultados impresionantes que usan μ.

Ejemplo : Para un entero n

$$Pr(n \textit{ no tenga factores cuadrados }) = \frac{6}{\pi^2}$$

Para el poset $(\mathbb{N}, |\,)$ tenemos para todo $a, b \in \mathbb{N}$

$$\mu_{\mathbb{N}}(a,b) = \begin{cases} (-1)^r & \text{si } b/a \text{ es el producto de } r \text{ primos distintos} \\ 0 & \text{sino} \end{cases}$$

$\mu_{\mathbb{N}}(2,36) = 0$ porque $36/2 = 18 = 2 \cdot 3^2$

Poset de un semigrupo

Sea $\mathcal{S} := \langle a_1, \ldots, a_n \rangle$ un semigrupo generado por $a_1, \ldots, a_n \in \mathbb{N}$, i.e.,

$$\mathcal{S} := \langle a_1, \ldots, a_n \rangle = \{x_1 a_1 + \cdots + x_n a_n \,|\, x_1, \ldots, x_n \in \mathbb{N}\}.$$

Poset de un semigrupo

Sea $\mathcal{S} := \langle a_1, \ldots, a_n \rangle$ un semigrupo generado por $a_1, \ldots, a_n \in \mathbb{N}$, i.e.,

$$\mathcal{S} := \langle a_1, \ldots, a_n \rangle = \{x_1 a_1 + \cdots + x_n a_n \,|\, x_1, \ldots, x_n \in \mathbb{N}\}.$$

$\mathcal{S}$ induce un orden parcial $\leq_{\mathcal{S}}$ en $\mathbb{N}$ dado por

$$x \leq_{\mathcal{S}} y \Longleftrightarrow y - x \in \mathcal{S}.$$

Denotemos por $\mu_{\mathcal{S}}$ la función de Möbius asociada a $(\mathbb{N}, \leq_{\mathcal{S}})$.

Poset de un semigrupo

Sea $\mathcal{S} := \langle a_1, \ldots, a_n \rangle$ un semigrupo generado por $a_1, \ldots, a_n \in \mathbb{N}$, i.e.,

$$\mathcal{S} := \langle a_1, \ldots, a_n \rangle = \{x_1 a_1 + \cdots + x_n a_n \,|\, x_1, \ldots, x_n \in \mathbb{N}\}.$$

$\mathcal{S}$ induce un orden parcial $\leq_{\mathcal{S}}$ en $\mathbb{N}$ dado por

$$x \leq_{\mathcal{S}} y \Longleftrightarrow y - x \in \mathcal{S}.$$

Denotemos por $\mu_{\mathcal{S}}$ la función de Möbius asociada a $(\mathbb{N}, \leq_{\mathcal{S}})$.

Se puede verificar que $\mu_{\mathcal{S}}(x, y) = 0$ si $y - x \notin \mathbb{N}$, o bien $\mu_{\mathcal{S}}(x, y) = \mu_{\mathcal{S}}(0, y - x)$ sino. Consideremos entonces la función de Möbius reducida definida

$$\mu_{\mathcal{S}}(x) := \mu_{\mathcal{S}}(0, x) \quad \text{para todo } x \in \mathbb{N}.$$

Série de Hilbert asociado a un semigrupo

Sea $A[\mathcal{S}] = K[z_1, \ldots, z_n]$ el anillo de polinomios sobre un campo K (de caracteristica 0) asociado al semigrupo $\mathcal{S} = \langle a_1, \ldots, a_n \rangle$.

La série de Hilbert de $A[\mathcal{S}]$ es dada por

$$\mathcal{H}_{\mathcal{S}}(z) = \sum_{i \in \mathcal{S}} z^s = \frac{Q(z)}{(1 - z^{a_1}) \cdots (1 - z^{a_n})}.$$

Série de Hilbert asociado a un semigrupo

Sea $A[\mathcal{S}] = K[z_1, \ldots, z_n]$ el anillo de polinomios sobre un campo K (de caracteristica 0) asociado al semigrupo $\mathcal{S} = \langle a_1, \ldots, a_n \rangle$.

La série de Hilbert de $A[\mathcal{S}]$ es dada por

$$\mathcal{H}_{\mathcal{S}}(z) = \sum_{i \in \mathcal{S}} z^s = \frac{Q(z)}{(1 - z^{a_1}) \cdots (1 - z^{a_n})}.$$

Observación

$$g(a_1, \ldots, a_n) = \text{grado de } \; \mathcal{H}_{\mathcal{S}}(z)$$

Ejemplo : Sea $\mathcal{S} = \langle 2, 3\rangle \subset \mathbb{N}$, tenemos que $\mathcal{S} = \{0, 2, 3, 4, 5 \ldots\}$

Ejemplo : Sea $\mathcal{S}=\langle 2,3\rangle\subset\mathbb{N}$, tenemos que $\mathcal{S}=\{0,2,3,4,5\ldots\}$

$$\mathcal{H}_{\mathcal{S}}(t)=\;1\;+\;t^2\;+\;t^3\;+\;t^4\;+\;t^5\;+\cdots$$

Ejemplo : Sea $\mathcal{S} = \langle 2, 3 \rangle \subset \mathbb{N}$, tenemos que $\mathcal{S} = \{0, 2, 3, 4, 5 \ldots\}$

$$
\begin{array}{rccccccccccc}
\mathcal{H}_{\mathcal{S}}(t) = & 1 & + & t^2 & + & t^3 & + & t^4 & + & t^5 & + \cdots \\
t^2\,\mathcal{H}_{\mathcal{S}}(t) = & & & t^2 & + & & & t^4 & + & t^5 & + \cdots
\end{array}
$$

Entonces, $(1 - t^2)\,\mathcal{H}_{\mathcal{S}}(t) = 1 + t^3$, por lo que

$$\mathcal{H}_{\mathcal{S}}(t) = \frac{1 + t^3}{1 - t^2}$$

Funcion de Möbius vs série de Hilbert

Supongamos que podemos escribir

$$\mathcal{H}_{\mathcal{S}}(z) = \frac{\sum_{b\in\Delta} f_b\, z^b}{(1-z^{c_1})\cdots(1-z^{c_k})}$$

para algún conjunto finito $\Delta \subset \mathbb{N}$ y algunos $c_1, \ldots, c_k \in \mathbb{N}$.

Funcion de Möbius vs série de Hilbert

Supongamos que podemos escribir

$$\mathcal{H}_{\mathcal{S}}(z) = \frac{\sum_{b\in\Delta} f_b\, z^b}{(1-z^{c_1})\cdots(1-z^{c_k})}$$

para algún conjunto finito $\Delta \subset \mathbb{N}$ y algunos $c_1, \ldots, c_k \in \mathbb{N}$.

Teorema (Chappelon, Garcia-Marco, Montejano, R.A., 2015)

$$\sum_{b\in\Delta} f_b\ \mu_{\mathcal{S}}(x-b) = 0$$

para todo $x \notin \{\sum_{i\in A} c_i \,|\, A \subset \{1,\ldots,k\}\}$.

Consideremos $\mathcal{G}_{\mathcal{S}}$ la función generatriz de la función de Möbius, i.e.,

$$\mathcal{G}_{\mathcal{S}}(z) := \sum_{b \in \mathbb{N}} \mu_{\mathcal{S}}(b)\, z^{b}.$$

Teorema (Chappelon, Garcia-Marco, Montejano, R.A., 2015)

$$\mathcal{H}_{\mathcal{S}}(z)\; \mathcal{G}_{\mathcal{S}}(z) = 1.$$

Una aplicación a teselaciones

Una aplicación a teselaciones

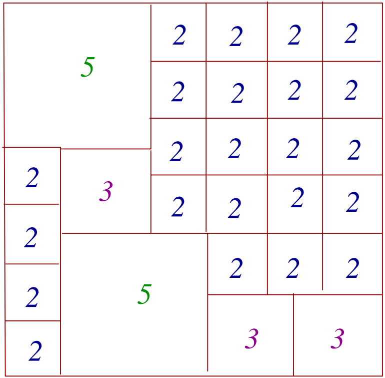
Una teselación es un recubrimiento del plano con figuras planas llamadas teselas o azulejos.

Una aplicación a teselaciones

Una teselación es un recubrimiento del plano con figuras planas llamadas teselas o azulejos.

Sea $R(a, b)$ el rectángulo 2-dimensional de lados a y b. Diremos que el rectángulo R puede ser teselado con azulejos (rectángulos 2-dimensionales más pequuños) $R_1, \ldots R_k$, si R puede ser llenado completamente con copias disjuntas de R_i, $1 \leq i \leq k$, sin usar rotaciones.

Ejemplo : Teselación de $R(13,13)$ con $R(2,2)$, $R(3,3)$ y $R(5,5)$



Pregunta : ¿Existe una función C_R tal que, para cualesquiera enteros $a, b \geq C_R$ el rectángulo $R(a, b)$ puede ser teselado con copias de los rectángulos $R(x, y)$ and $R(u, v)$?

Pregunta : ¿Existe una función C_R tal que, para cualesquiera enteros $a, b \geq C_R$ el rectángulo $R(a, b)$ puede ser teselado con copias de los rectángulos $R(x, y)$ and $R(u, v)$?

El caso especial cuando $x = 4, y = 6, u = 5$ y $v = 7$ fué una de las preguntas del William Mowell Putnam Examination (Problem B-3) en 1991.

Pregunta : ¿Existe una función C_R tal que, para cualesquiera enteros $a, b \geq C_R$ el rectángulo $R(a, b)$ puede ser teselado con copias de los rectángulos $R(x, y)$ and $R(u, v)$?

El caso especial cuando $x = 4, y = 6, u = 5$ y $v = 7$ fué una de las preguntas del William Mowell Putnam Examination (Problem B-3) en 1991.

Teorema (Klosinski, Alexanderson, Larson, 1992) $R(a, b)$ puede ser teselado con $R(4, 6)$ y $R(5, 7)$ si $a, b \geq 2214$.

Teorema (Labrousse, R.A., 2010) Sean p, q, r, s enteros tales que $\gcd(qs, qr, rs) = \gcd(p, r) = \gcd(p, s) = \gcd(r, s) = 1$. Entonces, $R(a, b)$ puede ser teselado con $R(p, q)$ y $R(r, s)$ si

$$a, b > \max\{2qrs - (qs + qr + rs), ps - p - s, rs - r - s\}.$$

Teorema (Labrousse, R.A., 2010) Sean p, q, r, s enteros tales que $\gcd(qs, qr, rs) = \gcd(p, r) = \gcd(p, s) = \gcd(r, s) = 1$. Entonces, $R(a, b)$ puede ser teselado con $R(p, q)$ y $R(r, s)$ si

$$a, b > \max\{2qrs - (qs + qr + rs), ps - p - s, rs - r - s\}.$$

Caso especial : Si $p = 6, q = 4, r = 5$ y $s = 7$ entonces $R(a, b)$ puede ser teselado con $R(4, 6)$ y $R(5, 7)$ si $a, b > 197$.

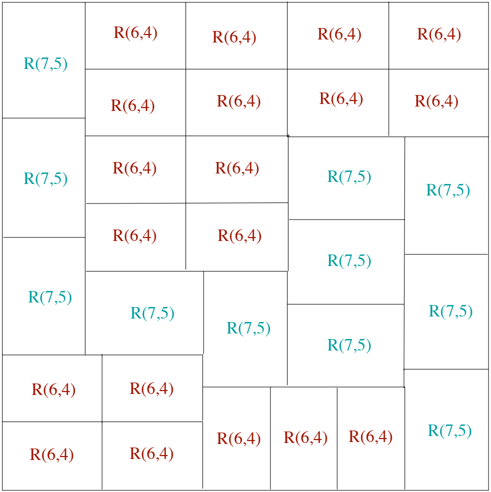
Teorema (Labrousse, R.A., 2010) Sean p, q, r, s enteros tales que $\gcd(qs, qr, rs) = \gcd(p, r) = \gcd(p, s) = \gcd(r, s) = 1$. Entonces, $R(a, b)$ puede ser teselado con $R(p, q)$ y $R(r, s)$ si

$$a, b > \max\{2qrs - (qs + qr + rs), ps - p - s, rs - r - s\}.$$

Caso especial : Si $p = 6, q = 4, r = 5$ y $s = 7$ entonces $R(a, b)$ puede ser teselado con $R(4, 6)$ y $R(5, 7)$ si $a, b > 197$.

Teorema (Narayan, Schwenk, 2002) $R(a, b)$ puede see teselado con $R(4, 6)$ y $R(5, 7)$ si $a, b \geq 33$.

Ejemplo : Teselación de $R(29,29)$ con $R(6,4)$ y $R(7,5)$

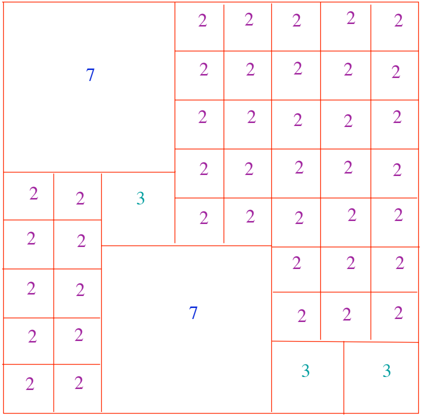


Teorema (Labrousse, R.A., 2010) Sean $1 < a_1 < a_2 < \cdots < a_{n+1}$ enteros positivos primos relativos, $n \geq 1$. Entonces $R(\underbrace{a, \ldots, a}_{n})$ puede ser teselado con $R(\underbrace{a_1, \ldots, a_1}_{n}), \ldots, R(\underbrace{a_{n+1}, \ldots, a_{n+1}}_{n})$ si

$$a > g(A_1, \ldots, A_{n+1}) = nP - \sum_{i=1}^{n+1} A_i$$

donde $A_i = P/a_i$ con $P = \prod_{j=1}^{n+1} a_j$.

Teselación de $R(17,17)$ con $R(2,2), R(3,3)$ y $R(7,7)$.



Toro 2-dimensional

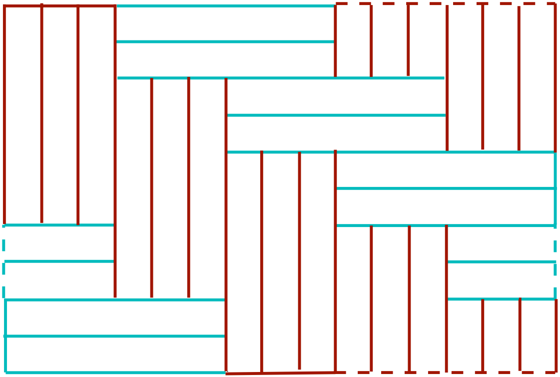
Aquí pensaremos en el toro 2-dimensional $T(a, b)$ de lados a y b como un rectángulo, cuyos lados paralelos son identificados en la forma usual.

Toro 2-dimensional

Aquí pensaremos en el toro 2-dimensional $T(a, b)$ de lados a y b como un rectángulo, cuyos lados paralelos son identificados en la forma usual.

Diremos que el toro T puede ser teselado con rectángulos 2-dimensionales más pequuños $R_1, \ldots R_k$, si T puede ser llenado completamente con copias disjuntas de R_i, $1 \leq i \leq k$, sin usar rotaciones.

Ejemplo : Teselación de $T(15,10)$ con $R(1,6)$



Pregunta : ¿Existe una función $C_T = C_T(x, y, u, v)$ tal que, para cualesquiera enteros $a, b \geq C_T$ el toro $T(a, b)$ puede ser teselado con copias de los rectángulos $R(x, y)$ and $R(u, v)$?

Pregunta : ¿Existe una función $C_T = C_T(x, y, u, v)$ tal que, para cualesquiera enteros $a, b \geq C_T$ el toro $T(a, b)$ puede ser teselado con copias de los rectángulos $R(x, y)$ and $R(u, v)$?

Teorema (Labrousse, R.A., 2010) La función $C_T(x, y, u, v)$ existe si y solamente si $\gcd(xy, uv) = 1$.

Pregunta : ¿Existe una función $C_T = C_T(x, y, u, v)$ tal que, para cualesquiera enteros $a, b \geq C_T$ el toro $T(a, b)$ puede ser teselado con copias de los rectángulos $R(x, y)$ and $R(u, v)$?

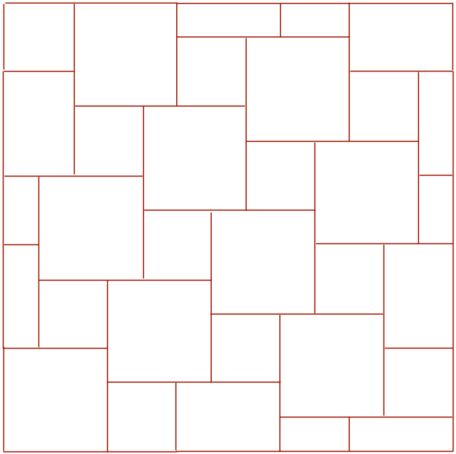
Teorema (Labrousse, R.A., 2010) La función $C_T(x, y, u, v)$ existe si y solamente si $\gcd(xy, uv) = 1$.

Teorema (Labrousse, R.A., 2010) Sean u, v, x y y enters positivos tales que $\gcd(xy, uv) = 1$. Entonces, $T(a, b)$ puede ser teselado con $R(x, y)$ y $R(v, u)$ si

$$a, b \geq \min\{n_1(uv + xy) + 1, n_2(uv + xy) + 1\}$$

donde $n_1 = \max\{vx, uy\}$ y $n_2 = \max\{ux, vy\}$.

Ejemplo : Teselación $T(13,13)$ con $R(2,2)$ y $R(3,3)$



Ya'ab Niib óolal !

Aplicación 2 : método Shell-sort

Aplicación 2 : método Shell-sort

lista a ordenar : 3,2,7,9,8,1,1,5,2,6

Aplicación 2 : método Shell-sort

lista a ordenar : 3,2,7,9,8,1,1,5,2,6

(secuencia de incrementación : 7,3,1)

Aplicación 2 : método Shell-sort

lista a ordenar : 3,2,7,9,8,1,1,5,2,6

(secuencia de incrementación : 7,3,1)

7-ordenado : 3,2,6,9,8,1,1,5,2,6

Aplicación 2 : método Shell-sort

lista a ordenar : 3,2,7,9,8,1,1,5,2,6

(secuencia de incrementación : 7,3,1)

7-ordenado : 3,2,6,9,8,1,1,5,2,6

3-ordenado : 1,2,1,3,5,2,7,8,6,9

Aplicación 2 : método Shell-sort

lista a ordenar : 3,2,7,9,8,1,1,5,2,6

(secuencia de incrementación : 7,3,1)

7-ordenado : 3,2,6,9,8,1,1,5,2,6

3-ordenado : 1,2,1,3,5,2,7,8,6,9

1-ordenado : 1,1,2,2,3,5,6,7,8,9

Aplicación 2 : método Shell-sort

lista a ordenar : 3,2,7,9,8,1,1,5,2,6

(secuencia de incrementación : 7,3,1)

7-ordenado : 3,2,6,9,8,1,1,5,2,6

3-ordenado : 1,2,1,3,5,2,7,8,6,9

1-ordenado : 1,1,2,2,3,5,6,7,8,9

Sea $n_d(a_1,\ldots,a_n)$ el número de múltiplos de d que no son representables por $a_1,\ldots,a_n$.

Lema El número de pasos necesarios para h_j-ordenar N enteros que ya han sido $h_{j+1} - h_{j+2} - \cdots - h_t$-ordenados es

$$O\left(\frac{Nn_{h_j}(h_{j+1}, h_{j+2}, \ldots, h_t)}{h_j}\right).$$

Lema El número de pasos necesarios para h_j-ordenar N enteros que ya han sido $h_{j+1} - h_{j+2} - \cdots - h_t$-ordenados es

$$O\left(\frac{Nn_{h_j}(h_{j+1}, h_{j+2}, \ldots, h_t)}{h_j}\right).$$

Lema Si $\gcd(a_1, \ldots, a_n) = 1$ entonces

$$n_d(a_1, \ldots, a_n) < \frac{g(a_1, \ldots, a_n)}{d}.$$

Lema El número de pasos necesarios para h_j-ordenar N enteros que ya han sido $h_{j+1} - h_{j+2} - \cdots - h_t$-ordenados es

$$O\left(\frac{Nn_{h_j}(h_{j+1}, h_{j+2}, \ldots, h_t)}{h_j}\right).$$

Lema Si $\gcd(a_1, \ldots, a_n) = 1$ entonces

$$n_d(a_1, \ldots, a_n) < \frac{g(a_1, \ldots, a_n)}{d}.$$

Teorema (Incerpi, Sedgewick, 1985) El tiempo de ejecución del Shell-sort es $O(N^{3/2})$ donde N es el número de elementos del arreglo (en promedio y en el peor caso).

Fórmulas para secuencias particulares

Fórmulas para secuencias particulares

(Brauer 1942) $g(a, a+1, \dots, a+k-1) = \left(\left\lfloor \frac{a-2}{k-1} \right\rfloor + 1 \right) a - 1.$

Fórmulas para secuencias particulares

(Brauer 1942) $g(a, a+1, \ldots, a+k-1) = \left(\left\lfloor \frac{a-2}{k-1} \right\rfloor + 1 \right) a - 1.$

(Roberts 1956) Sean $a, d, s \in \mathbb{N}$ con $\gcd(a, d) = 1$.
$g(a, a+d, \ldots, a+sd) = \left(\left\lfloor \frac{a-2}{s} \right\rfloor + 1 \right) a + (d-1)(a-1) - 1.$

Fórmulas para secuencias particulares

(Brauer 1942) $g(a, a+1, \ldots, a+k-1) = \left(\left\lfloor \frac{a-2}{k-1} \right\rfloor + 1\right) a - 1.$

(Roberts 1956) Sean $a, d, s \in \mathbb{N}$ con $\gcd(a, d) = 1$.
$g(a, a+d, \ldots, a+sd) = \left(\left\lfloor \frac{a-2}{s} \right\rfloor + 1\right) a + (d-1)(a-1) - 1.$

(Selmer 1977) Sean $a, h, d, k \in \mathbb{N}^+$ con $\gcd(a, d) = 1$. Entonces,
$g(a, ha+d, ha+2d, \ldots, ha+kd) = ha \left\lfloor \frac{a-2}{k} \right\rfloor + a(h-1) + d(a-1).$

Fórmulas para secuencias particulares

(Brauer 1942) $g(a, a+1, \ldots, a+k-1) = \left(\left\lfloor \frac{a-2}{k-1} \right\rfloor + 1\right) a - 1.$

(Roberts 1956) Sean $a, d, s \in \mathbb{N}$ con $\gcd(a, d) = 1$.
$g(a, a+d, \ldots, a+sd) = \left(\left\lfloor \frac{a-2}{s} \right\rfloor + 1\right) a + (d-1)(a-1) - 1.$

(Selmer 1977) Sean $a, h, d, k \in \mathbb{N}^+$ con $\gcd(a, d) = 1$. Entonces,
$g(a, ha+d, ha+2d, \ldots, ha+kd) = ha \left\lfloor \frac{a-2}{k} \right\rfloor + a(h-1) + d(a-1).$

(R.A., Rødseth 2008) Fórmula semi-explicita para
$g(a, a+d, \ldots, a+kd, c)$ con $\gcd(a, d) = 1$.

Cotas Superiores

Cotas Superiores

(Schur 1942) $g(a_1, \ldots, a_n) \leq (a_1 - 1)(a_n - 1) - 1.$

(Erdős, Graham 1972) $g(a_1, \ldots, a_n) \leq 2a_{n-1} \left\lfloor \frac{a_n}{n} \right\rfloor - a_n.$

(Selmer 1977) $g(a_1, \ldots, a_n) \leq 2a_n \left\lfloor \frac{a_1}{n} \right\rfloor - a_1.$

Cotas Superiores

(Schur 1942) $g(a_1,\ldots,a_n) \leq (a_1-1)(a_n-1)-1.$

(Erdős, Graham 1972) $g(a_1,\ldots,a_n) \leq 2a_{n-1}\left\lfloor \frac{a_n}{n} \right\rfloor - a_n.$

(Selmer 1977) $g(a_1,\ldots,a_n) \leq 2a_n\left\lfloor \frac{a_1}{n} \right\rfloor - a_1.$

Cotas Inferiores

(Hujter 1982)

$$g(a_1,\ldots,a_n) \geq \left(\frac{n-1}{n}\right)\left((n-1)!a_1a_2\cdots a_n\right)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i.$$

(Killingbergtrø 2000)

$$g(a_1,\ldots,a_n) \geq \left((n-1)!a_1a_2\cdots a_n\right)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i.$$

Referencias

- S. Eliahou, J.R.A., Two generator numerical semigroups and Fermat and Marsenne numbers, *SIAM Discrete Mathematics* **25** (2011), 622-630.
- S. Eliahou, J.R.A., On the number of numerical semigroups of prime power genus, *Semigroup Forum* **87** (2013), 171-186.
- D. Labrousse, J.R.A., A tiling problem and the Frobenius number, in *Additive Number Theory, Springer-Verlag* (2010), 203-220.
- J.R.A., El problema diofántico de Frobenius, *La Gaceta de la Real Sociedad Matemática Espanola* **16** (2013), 117-129.
- J.R.A., The complexity of the Frobenius problem, *Combinatorica* **16** (1996), 143-147.
- J.R.A., The diophantine Frobenius problem, *Oxford Lectures Seires in Mathematics* **30** (2005), 243p.