Paseando entre la Matemática Recreativa y la Programación Recreativa[1]

Blas Ruiz Dpto. de Lenguajes y Ciencias de la Computación. Universidad de Málaga.

blas@lcc.uma.es

Resumen.- La Programación Recreativa ($\mathcal{P}ro\mathcal{R}ec$) es la disciplina que motiva el estudio de la programación de computadores a través de problemas lúdicos. Los problemas típicos que estudia esta disciplina son similares a los de la Matemática Recreativa ($\mathcal{M}at\mathcal{R}ec$), lo que lleva a veces a identificar ambas disciplinas. Sin embargo, los métodos de una y otra pueden llegar a ser muy diferentes. El objetivo de la $\mathcal{P}ro\mathcal{R}ec$ es escribir programas, mientras que en la $\mathcal{M}at\mathcal{R}ec$ podemos ayudarnos de éstos para enunciar conjeturas sobre la solución.

Desde una visión educativa son muy interesantes aquellos problemas que motivan de forma natural el estudio elemental de resultados notables de la teoría de números ($\mathcal{T}eo\mathcal{N}um$), entendiendo por *elemental* cuando solo es necesario para la comprensión del resultado un conocimiento básico del álgebra: por ejemplo, la conjetura de Goldbach o el teorema de Dirichlet.

La escritura de programas de ordenador utilizando un lenguaje de programación próximo a la notación matemática (como por ejemplo Haskell) constituye un primer paso a la solución del problema, ya que obtenemos con poco esfuerzo sencillos y elegantes programas tan próximos

[1]Resumen, transparencias, y referencias utilizadas en la conferencia de clausura de las XIV CEAM (*Congreso de Enseñanza y Aprendizaje de las Matemáticas*), Málaga, 4-6 de Julio de 2012. Este trabajo ha sido sufragado en parte por los Proyectos de Investigación nacionales ReSCUE TIN2008-05932 y P07-TIC03131.

a la descripción del problema que su corrección es inmediata. Estos programas conducen a un primer análisis del problema estableciendo conjeturas sobre la solución.

Desafortunadamente, para los problemas que analizamos, tales programas pueden ser *casi* inútiles si son extraordinariamente ineficientes. Pero estas conjeturas permiten refinar posteriormente el programa, y así sucesivamente se obtiene una interacción $\mathcal{M}at\mathcal{R}ec\leftrightharpoons\mathcal{P}ro\mathcal{R}ec$ cíclica mutuamente enriquecedora.

Interesa a veces en este proceso de interacción usar resultados célebres de la $\mathcal{T}eo\mathcal{N}um$ ya que conducen a propiedades de fácil comprobación computacional, que *casi* caracterizan a las soluciones y que derivan en programas eficientes.

Pero lo más importante es que esta interacción $\mathcal{M}at\mathcal{R}ec\leftrightharpoons\mathcal{P}ro\mathcal{R}ec$ desarrolla de forma natural un modelo matemático del problema.

Exponemos en esta conferencia dos problemas que ilustran la interacción $\mathcal{M}at\mathcal{R}ec\leftrightharpoons\mathcal{P}ro\mathcal{R}ec$ a través de la $\mathcal{T}eo\mathcal{N}um$. Uno de ello es un puzzle lógico: el problema PS de Freudenthal; el otro es un problema aritmético/combinatorio: la distribución de los Números l–Separables (aquellos naturales tales que sus divisores positivos pueden repartirse en l grupos disjuntos con idéntica suma).

Palabras clave: programación recreativa, matemática recreativa, puzzles lógicos, teoría de números.

Paseando entre la Matemática Recreativa y la Programación Recreativa

Blas Ruiz Dpto. de Lenguajes y Ciencias de la Computación. Universidad de Málaga.

blas@lcc.uma.es

Programación Recreativa $\equiv$ *Computer Recreations* (*Juegos de Ordenador*)

Alexander Dewdney la populariza en *Scientific American* en 80's.

Sustituyó a *Mathematical Games*, de M. Gardner ¡25 años!

"Martin Gardner, gurú de los juegos matemáticos ..."
Abel Grau
El País, 25 de mayo de 2010

El paseo $\mathcal{M}at\mathcal{R}ec \leftrightarrows \mathcal{P}ro\mathcal{R}ec$

- Comenzamos con pautas de la $\mathcal{M}at\mathcal{R}ec$: con lápiz y papel, o ¡en la cabeza!, construimos un modelo matemático.
- Con poco esfuerzo producimos programas *Haskell* que describen el modelo, próximos al problema, y correctos por construcción.
- Desafortunadamente, para los problemas que expondré, estos programas pueden ser ineficientes.
- Pero . . . conducen a alguna conjetura sobre la solución.

. . .

- Probada la conjetura, pasa a ser una *propiedad* de la solución.
- La *propiedad* debe ser *esencial*:
  (1) de comprobación computacional sencilla,
  (2) *casi* debe caracterizar a las soluciones.
- Refinamos el programa introduciendo tal *propiedad esencial* para acelerar su ejecución.
- Nuevas ejecuciones/*experimentos* permiten obtener más conjeturas,

  . . . y así cíclicamente . . .

  ¡ Con nuestros programas enunciamos nuevos resultados,
  y construimos sus pruebas!

Este paseo $\mathcal{MR} \leftrightarrows \mathcal{PR}$ deriva en una investigación matemática experimental de calidad, usando resultados elementales

Recordemos a Vladímir Arnold (1937–2010):

> *Las matemáticas son una parte de la física. La física es una ciencia experimental, parte de las ciencias naturales. Las matemáticas son la parte de la física en la que los experimentos son más baratos.*
>
> Arnold, el matemático que amaba los problemas
> Manuel de León,
> El País, 11 de Junio 2010

Algunos resultados esenciales de la $\mathcal{TN}$ son difíciles de motivar.

El profesor de Matemáticas/Programación debe valorar:

- ♢ el interés formativo y didáctico de sus demostraciones,
- ♢ la importancia de sus aplicaciones

Ilustraremos el paseo $\mathcal{MR} \leftrightarrows \mathcal{PR}$ con dos puzzles:

- El puzzle lógico P-S de Freudenthal.
- Un problema de reparto en Zumkia, original problema aritmético/combinatorio.

y como de ésta interacción aparecen de forma natural resultados fundamentales de la $\mathcal{TN}$.

El puzzle lógico P-S de Hans Freudenthal

(No. 223, Nieuw Archief Voor Wiskunde, 17, 1969)

$\mathcal{A}$ comunica a dos personas $\mathcal{S}$ y $\mathcal{P}$:

♢ *He tomado dos naturales x e y verificando*

$$1 < x < y, \qquad x + y \leq 100.$$

♢ *Daré a $\mathcal{P}$ el producto $x\,y$, y a $\mathcal{S}$ la suma $x + y$.*

Al cabo de un tiempo *escuchamos el siguiente diálogo:*

$\mathcal{P}$.- No sé tu suma.
$\mathcal{S}$.- Ya lo sabía.
$\mathcal{P}$.- Ahora ya sé tu suma.
$\mathcal{S}$.- Y yo tu producto.

Encontrar el par (x, y).

Obsérvese la elegancia del enunciado

Escudriñando la aritmética del puzzle P-S.

La conjetura de Goldbach.

$\left.\begin{array}{l}\mathcal{P}\text{.- No sé tu suma.}\\ \mathcal{S}\text{.- Ya lo sabía.}\end{array}\right\} \equiv \quad \mathcal{S}$.- No sabes mi suma.

¡Si $\mathcal{S}$ tuviera la suma de dos números primos, $\mathcal{P}$ podría tener el producto de dos primos!

Por la conjetura Goldbach ($\mathcal{G}$), $\mathcal{S}$ no puede tener una suma par, ... al menos hasta sumas ¡enormes!:

$$x + y < 12 \cdot 10^{17}$$ (Oliveira e Silva, 2008):

... y a partir de sumas ¡más enormes!:

$$x + y > 3{,}3 \cdot 10^{43000}$$ (Chen y Wang 1989)

¿Hay alguna suma par solución en el *modesto* intervalo

$$12 \cdot 10^{17} \leq s \leq 3{,}3 \cdot 10^{43000} \quad ?$$

Algo de historia del puzzle P-S

wikipedia $\rightsquigarrow$ Hans Freudenthal (1905–1990)
$\rightsquigarrow$ *Impossible puzzle* (acuñado por M Gardner)
$\rightsquigarrow$ publicaciones recientes.
Nieuw Archief Voor Wiskunde $\rightsquigarrow$ Freudenthal
$\rightsquigarrow$ Hans van Ditmarsch (lógica epistémica, 2009, 2007)

Hans Freudenthal publica en 1970 una solución correcta basada en la enviada por J Boersma; usa conjuntos *filtrados* (estrategia hacia adelante) con las sucesivas frases.

En la literatura sobre $\mathcal{MR}$ rápidamente aparecieron variantes del problema P-S, y también entre los pioneros de la IA, ya que se consideraba un laboratorio para la

Representación del razonamiento *infinitamente inteligente*

Versión de John McCarthy

John McCarthy (1927-2011) divulgó el puzzle P-S a través de XEROX PARC en los 70, y lo publica en *Formalization of two puzzles involving knowledge, 1978-1981*.

$$\ldots \qquad 1 < x \leq \boxed{y \leq 99} \qquad \ldots$$

$\mathcal{P}$.- *No sé los números.*
$\mathcal{S}$.- *Ya lo sabía. Yo tampoco sé los números.*
$\mathcal{P}$.- *Ahora ya los conozco.*
$\mathcal{S}$.- *Ahora yo también.*

- Hace referencia a los factores ... pero $x(s-x) = p$
- Añade Yo tampoco sé los números
- Cambia la restricción $\boxed{x + y \leq 100}$ ¡ESENCIAL!

(McCarthy añade en 2008 una nota citando el original)

Versión de Martin Gardner

A Pride of Problems, Including One that is Virtually Impossible
(Scientific American, 1979)

$$\ldots \qquad 1 < x \leq y \leq 100 \qquad \ldots$$

$\mathcal{S}$.- *No sabes mi suma.*
$\mathcal{P}$.- *Sé tu suma.*
$\mathcal{S}$.- *Sé tu producto.*

Si suponemos $1 < x \leq \boxed{y \leq t}$, entonces

- No hay solución si $t < 62$.
- La solución es única para los valores $62 \leq t \leq 1680$:
  $x = 4, y = 13$, (*palos* y *cartas* de cada palo de la baraja.)
- Para valores mayores de $t > 1680$ aparecen nuevas soluciones.

¿Podemos "demostrar" los resultados anteriores?

Resolviendo el puzzle P-S con lápiz y papel

$$\ldots \qquad 1 < x < y \leq t \qquad \ldots$$

$\mathcal{S}$.- *No sabes mi suma.*
$\mathcal{P}$.- *Sé tu suma.*
$\mathcal{S}$.- *Sé tu producto.*

El observador puede utilizar la *estrategia hacia adelante*:

♢ partiendo del *espacio de búsqueda*

$$\xi = \{(x+y, xy) \,|\, x, y \in \mathbb{N}, 2 \leq x < y \leq t\}$$

♢ cribará este espacio sucesivamente con cada frase.

Necesitamos:

- representar el espacio de búsqueda.
- describir la criba asociada a cada frase (representación del razonamiento).

♠ Representemos ξ con una tabla $p \diagdown s$, con marcas para los pares compatibles.

$p \diagdown s$	5	6	7	8	9	10	11	12	13
6	+								
8		+							
10			+						
12			+	+					
14					+				
15				+					
18					+				
20					+				
21						+			
24						+			
28							+		
30							+		
35								+	
42									+

$$t = 7$$

$$\bigotimes 7 = \{10, 12\}$$

$$\bigoplus 12 = \{7, 8\}$$

$\mathcal{P}$.- *No sé tu suma*: eliminamos las filas con una sola marca.

$\mathcal{S}$.- *No sabes mi suma*: eliminamos cualquier suma que tenga algún producto compatible con una sola marca; deja el espacio vacío; no hay solución.

La manipulación de la tabla es *incómoda*, incluso para t pequeño.

Representaremos ξ con árboles de Freudenthal.

Árboles de Freudenthal

Cada suma tiene por hijos sus productos compatibles, y éstos tienen por hijos sus sumas compatibles (cada suma es abuela de sí misma).

Para $\boxed{t = 14}$, el árbol $\mathcal{F}(11)$ es:

$$\mathcal{F}(11) \qquad p = \overbrace{\underbrace{18}_{9\ 11} \quad \underbrace{24}_{10\ 11\ 14} \quad \underbrace{28}_{11\ 16} \quad \underbrace{30}_{11\ 13}}^{s=11}$$

Al principio tendremos un árbol para cada suma posible

$$\mathcal{F}(5) \qquad \mathcal{F}(6) \qquad \ldots \qquad \mathcal{F}(26) \qquad \mathcal{F}(27)$$

Cada frase elimina hijos, o nietos, y por ello abuelos (árboles completos).

La magia de la frase *No sabes mi suma*

Queremos modelar el comportamiento inteligente del orador que dice la frase *No sabes mi suma*

¡Cada producto compatible con mi suma tiene varias sumas compatibles!

¿Y en términos algebraicos?

Usaremos los conjuntos de compatibles:

$$\bigoplus p = \{x + y \mid 2 \leq x < y \leq t, xy = p\}$$
$$\bigotimes s = \{xy \mid 2 \leq x < y \leq t, x + y = s\}$$

Por ejemplo, para $t = 14$

$$\bigotimes 7 = \{10, 12\}, \qquad \bigoplus 30 = \{11, 13\}$$

Pero somos tan inteligentes como los oradores, y capturamos el razonamiento con los siguientes predicados:

$$f_1(s) \equiv \forall p \bigotimes s.|\bigoplus p| \geq 2 \qquad \mathcal{S}\text{.- No sabes mi suma}$$
$$f_2(p) \equiv |s : s \bigoplus p, f_1(s)| = 1 \qquad \mathcal{P}\text{.- Sé tu suma}$$
$$f_3(s) \equiv |p : p \bigotimes s, f_2(p)| = 1 \qquad \mathcal{S}\text{.- Sé tu producto}$$

Cotas para las sumas. El postulado de Bertrand

El postulado de Joseph Bertrand (1845) o Teorema de Chebyshev (1850) dice

$$\forall n : n > 3 : \mathcal{P}(n, 2n-2)$$

De aquí $\mathcal{P}_t \doteq \{p \text{ primo} \,|\, p \leq t < 2p-2\} \neq \varnothing$, para $t \geq 5$.

En efecto: sea $\alpha \doteq \max\{p \text{ primo} \,|\, p \leq t\}$. Si fuera $t \geq 2\alpha - 2 > \alpha$, ya que existe un primo β verificando $t \geq 2\alpha - 2 > \beta > \alpha$, el máximo no sería α.

Sea pues p primo, con $p \leq t < 2p$.

Veamos que

$$\boxed{2 + p \leq s \leq t + p} \;\Rightarrow\; |\bigoplus p(s-p)| = 1$$

de donde s es incompatible con la frase "*No sabes mi suma*".

En efecto: $\bigoplus p(s-p) = \{pk + q : k \geq 1, ...\}$. Si $k > 1$, $pk \geq 2p > t$, y pk no es un sumando válido.

Recordemos: si p primo, $p \leq t < 2p$, excluimos las sumas

$$\boxed{2+p \leq s \leq t+p}$$

Ejemplo: para $t = 14$, $\{p \text{ primo} \,|\, p \leq 14 < 2p\} = \{11, 13\}$

$2+p$		s		$t+p$
$13 = 2+11$	$\leq$	s	$\leq$	$14+11 = 25$
$15 = 2+13$	$\leq$	s	$\leq$	$14+13 = 27$

Los intervalos *se pisan*, excluimos las sumas $13 \leq s \leq 27$, y solo quedarán $s < 13$.

- Para $t = 14$, con la frase *"No sabes mi suma"* solo consideramos las sumas $s < 13$, es decir,

$$5, 6, 7, 8, 9, 10, 11, 12$$

- La frase *"No sabes mi suma"* elimina
  - Las sumas extremas $(5, 6, 2t - 2, 2t - 1)$, y quedan

$$7, 8, 9, 10, 11, 12$$

  - las que admiten una descomposición en suma de dos primos distintos, en particular, las pares > 6 (conjetura de Goldbach), y las que $s - 2$ es primo, y solo queda $s = 11$, y un único árbol.

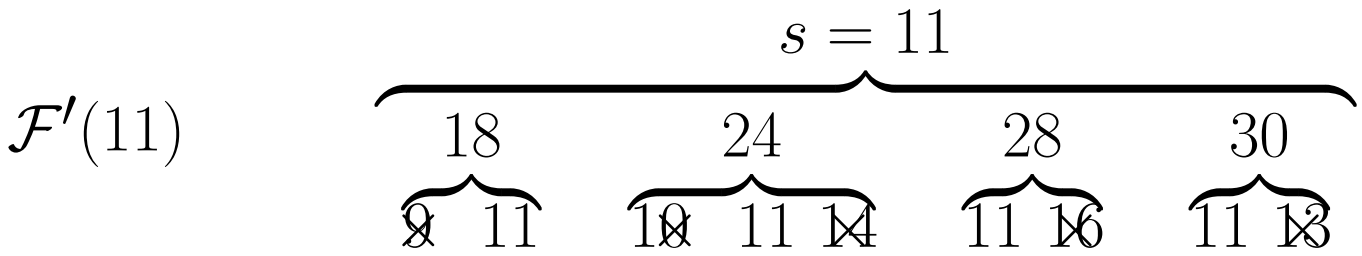
Si procedemos igual para $t = 100$, quedan 11 sumas:

$$[11, 17, 23, 27, 29, 35, 37, 41, 47, 51, 53]$$

¡Solamente 51 no es válida!

Es decir, el predicado "s impar y $s-2$ compuesto" es decisivo: fácil de computar, es necesario para $f_1(s)$, y *casi* suficiente.

Para $t = 14$ el único árbol tras la primera criba es:



(suprimimos los nietos/sumas 9, 10, 14, 16, 13: son incompatibles con la frase "No sabes mi suma").

$\mathcal{P}$.- *Sé tu suma*: no filtra nada ¡En efecto, siempre es 11!

$\mathcal{S}$.- *Sé tu producto*, elimina la suma que queda, y no hay solución para $t = 14$.

Tiene solución el diálogo:

$\mathcal{S}$.- No sabes mi suma.

$\mathcal{P}$.- Sé tu suma.

¡Pero un observador no conocerá el producto!

♠ En general, si

$$\mathcal{P}_t \doteq \{p \text{ primo} \,|\, p \leq t < 2p\}$$

excluimos las sumas

$$2 + \min \mathcal{P}_t \leq s \leq t + \max \mathcal{P}_t$$

Es decir, las sumas posibles quedan reducidas a la 4ª parte.

¡Atención con la conjetura de Goldbach!

Obsérvese: Si $s \leq 2 + t$

♢ Entonces podemos aplicar la conjetura $\mathcal{G}$, ya que si s es suma de dos primos distintos α, β, éstos serán $\leq t$.

♢ $f_1(s) \Rightarrow s$ impar, $s - 2$ compuesto, y $s < 2 + \min \mathcal{P}_t$

¿ Cómo demostrar $f_1(s) \Rightarrow s \leq 2 + t$?

¡ Necesitamos una conjetura adicional!

♠ Existencia de primos en intervalos $(\alpha, \alpha + \alpha^\theta)$

Entre las conjeturas célebres relacionadas con la de Ludvig Opperman (1882), son interesantes las de la forma:

$$\mathcal{XO}^\theta \doteq \forall \alpha : \alpha \geq N_\theta, \alpha \text{ primo} : \mathcal{P}(\alpha, \alpha + \alpha^\theta)$$

Mozzochi (1986) la probó para $\theta = 1051/1920 = 0{,}5479\ldots$.
Lou y Yao (1993) la prueban para $\theta = 6/11 = 0{,}5454\ldots$.

Nosotros hemos usado la *conjetura* para $\theta = 0{,}5$:

$$\boxed{\mathcal{XO} \doteq \forall \alpha : \alpha \geq 127, \alpha \text{ primo} : \mathcal{P}(\alpha, \alpha + \sqrt{\alpha})}$$

Teorema 3.- Admitiendo $\mathcal{XO}$, $f_1(s) \Rightarrow s \leq t$, luego

$f_1(s) \Rightarrow s < 2 + \min\{p \text{ primo} \,|\, p \leq t < 2p\} \wedge s-2$ compuesto

Y admitiendo además $\mathcal{G}$,

$f_1(s) \Rightarrow s$ impar, $\qquad f_1^\infty(s) \equiv s$ impar $\wedge\ s - 2$ compuesto

♠ Conexiones con la conjetura de Goldbach

Consideremos el predicado de la primera frase del diálogo de M Gardner sin cota $(1 < x < y)$:

$$f_1^{\infty}(s) \equiv \forall p \bigotimes s.|\bigoplus p| \geq 2 \qquad \mathcal{S}\text{.- No sabes mi suma}$$

y la conjetura Goldbach en su forma débil $(\mathcal{G}^{\delta})$:
El doble de un primo (> 3) *es suma de dos primos distintos.*

Teorema 4.- Se verifica $\mathcal{G} \Rightarrow \mathcal{C} \Rightarrow \mathcal{G}^{\delta}$, donde

$$\mathcal{C} \doteq \forall s : s > 4 : f_1^{\infty}(s) \Longleftrightarrow s \text{ impar } \wedge\, s-2 \text{ no primo}$$

Consecuencias:

- Si $\mathcal{G}^{\delta} \Rightarrow \mathcal{G}$, entonces $\mathcal{C}$ caracteriza las dos conjeturas.
- Admitiendo $\mathcal{G}$, escribimos programas muy rápidos.

Dada una suma s, estaremos seguros si s es o no una suma solución, si se satisface:

$\text{máx}\{s' : p \in \bigotimes s, s' \in \bigoplus p\} < 12{\cdot}10^{17}$(Oliveira e Silva, 2008)

Razonando hacia atrás

Para el problema de McCarthy (4 frases) definiremos cuatro funciones de conjuntos,

$$V_1, V_2, V_3, V_4 : \mathbb{N} \longrightarrow 2^{\mathbb{N}}$$

$V_1(p) = \{$ sumas que pensó $\mathcal{P}$: compatibles con p que certifican la frase *No sé tu suma* $\}$

♢ Primera frase:

$$\begin{aligned} V_1(p) &= S, \quad \text{si } |S| \geq 2, \text{ donde } S = \bigoplus p \\ &= \emptyset, \quad \text{en otro caso} \end{aligned}$$

Si (p, s) es un par solución, $s \in V_1(p)$
(no recíprocamente).

♢ Segunda frase: los productos que pensó $\mathcal{S}$ a partir de su suma,

$$V_2(s) = \bigotimes s, \text{ si } \forall p \otimes s. |\bigoplus p| \geq 2 \qquad \textit{ya lo sabía}$$
$$\wedge$$
$$|p : p \otimes s, s \in V_1(p)| \geq 2 \quad \textit{no sé tu producto}$$
$$= \emptyset, \text{ en otro caso}$$

♢ Cuarta frase:

$$V_4(s) = P, \text{ si } |P| = 1$$
$$= \emptyset, \text{ en otro caso}$$
$$\text{donde } P = \{p : p \otimes s, s \in V_3(p)\}$$

En consecuencia, el conjunto de pares que verifican el diálogo es

$$\mathcal{S}_t = \{(p, s) \mid s \in \Sigma_t, p \in V_4(s)\}$$

La definición de $\mathcal{S}_t$ permite *construir* las soluciones

Un programa *Haskell*

La descripción por comprensión de los conjuntos puede trasladarse directamente a *Haskell* a través de listas por comprensión

$$
\begin{array}{l}
v2\ s \mid varios\ [p \mid p \in ps,\ s\ `elem`\ v1\ p]\ \&\& \\
\qquad and\ [varios(sum\_de\ p) \mid p \in ps] \qquad\qquad = ps \\
\qquad \mid otherwise \qquad\qquad\qquad\qquad\qquad\qquad = [\,]\ where\ ps = pro\_de\ s
\end{array}
$$

— Se tu producto

$$
\begin{array}{l}
v4\ s \mid uno\ pp \qquad\qquad\qquad = pp \\
\qquad \mid otherwise \qquad\qquad\qquad = [\,]
\end{array}
$$

$$where\ pp = [p \mid p \in pro\_de\ s,\ s\ `elem`\ v3\ p]$$

— Búsqueda vía *backtracking*

$$sol = [(p, s) \mid s \in [5\,..\,2 * t - 1],\ p \in v4\ s]$$

La elección $s \in [5\,..\,2 * t - 1]$ es mejorable.

De nuevo la interacción $\mathcal{PR} \rightleftarrows \mathcal{MR}$

El programa es *extraordinariamente lento*: cómputo innecesario.

Lema 2.-. (¡PLAUSIBLE!)

(a) $V_4(s) \subset V_2(s)$ (b) $V_3(p) \subset V_1(p)$

El lema muestra la consistencia de las afirmaciones de los oradores.

¡Podemos añadir estos resultados al programa!

— Por (a):

$$sol = [(p, s) |\ s \in [5 .. 2 * t - 1],\ v2\ s \neq [\,],\ p \in v4\ s]$$

El Lema 2(a) es decisivo: un programa 100 veces más rápido.

La forma de las soluciones

p	s	10000	20000	30000/40000	∞
52	17	2^2+13	E	E	E
244	65	2^2+61	E	E	E
1168	89	2^4+73	E	E	E
1776	127	2^4+3*37	E	E	E
4672	137	2^6+73	E	E	E
5494	149	$\boxed{2*41+67}$			
4192	163	2^5+131	E	E	E
2608	179	2^4+163	E	E	E
724	185				2^2+181
8128	191	2^6+127	E	E	E
916	233	2^2+229	E	E	E
1912	247				2^3+239
3328	269		2^8+13	E	E
15424	305				2^6+241
23136	337		$\boxed{2^5*3+241}$		
9952	343		2^5+311	E	E
3352	427			2^3+419	E
3592	457				2^3+449

Abundan las soluciones $(x,y)=(2^k,\beta)$ (β primo) y son estables, así como $(2^k,3^q\beta)$. Las sumas son muy pequeñas.

♠ La versión de Martin Gardner

Lema 1.- $$p' \in V_2(s) \Longleftrightarrow p' \otimes s \wedge \underbrace{\forall p \otimes s.|\bigoplus p| \geq 2}_{f_1(s)}$$

Por tanto, $V_2(s)$ puede reescribirse en la forma

$$\begin{aligned} V_2(s) &= \bigotimes s, \text{ si } f_1(s) \\ &= \emptyset, \text{ en otro caso} \end{aligned}$$

que se corresponde con el diálogo que propuso Martin Gardner

$\mathcal{S}$.- No sabes mi suma.
$\mathcal{P}$.- Ya sé tu suma.
$\mathcal{S}$.- Y yo tu producto.

Los problemas de J McCarthy y de M Gardner son equivalentes

Otra a vez $\mathcal{MR}\leftrightarrows\mathcal{PR}$. La variante de Dick Hess

Consideremos los predicados para el siguiente diálogo sin cota $(1 < x < y)$:

$$f_1(s) \equiv \forall p \bigotimes s.|\bigoplus p| \geq 2 \qquad \mathcal{S}\text{.- No sabes mi suma}$$
$$f_2(p) \equiv |s : s \bigoplus p, f_1(s)| > 1 \qquad \mathcal{P}\text{.- No sé tu suma}$$
$$f_3(s) \equiv |p : p \bigotimes s, f_2(p)| = 1 \qquad \mathcal{S}\text{.- Sé tu producto}$$

Nuestro programa HASKELL solo encontró la solución $s = 11$, $p = 30$, y ... ¡$f_3(s)$ falla a partir de $s = 17$!

Teorema 4.- Admitiendo $\mathcal{G}$, $f_3(s) \Rightarrow s \leq 17$, y el problema $\mathcal{H}$ tiene una única solución: $s = 11, p = 30$.

¿Será única la solución para $s > 12 \cdot 10^{17}$?

¿Conduce esto a $\mathcal{G}$?

♠ Edsger Wybe Dijkstra (1930 - 2002) cuenta cómo resolvió durante una duermevela el problema P-S original ($x + y \leq 100$).

Reconoce que tardó 6 horas, y otras tantas en *copiar* la solución.

Antes de exponer la solución dice:

> *Más tarde me enteré de que algunas personas cuando se enfrentan a este problema, en lugar de resolverlo por sí mismos, con o sin lápiz y papel, llegan a extremos tales como escribir un programa informático para ello.*
>
> *A problem solved in my head*, EWD666, 1976.

Un breve preludio

God Created The Integers
Stephen Hawking, 2005

Hace 2300 años ocurrió un decisivo hecho en la historia de las matemáticas: la aparición de

Elementos, Euclides (325–265 a.C.)

. . . transformó la matemática desde la numerología
a una ciencia deductiva
Introduction to Analytic Number Theory
Tom Apostol, 1976

Hasta 1950, tras la Biblia, *Elementos* fue la obra más vendida.

Elementos es una colección de 13 libros, 500 resultados.

Los libros VII, IX y X están dedicados a la teoría de números.

El libro IX contiene dos joyas de la matemática que aún hoy día nos sorprenden:

- la demostración de la infinitud de los números primos.
- una solución parcial a un problema de Pitágoras: encontrar todos los números perfectos.

n es *perfecto* si es la suma de sus partes.

$\partial\, 6 = \{1, 2, 3, 6\}$, y $6 = 1 + 2 + 3$ es perfecto.

$$n \text{ es perfecto sii } \sigma n = 2n$$

Proposición 36 del libro IX:

Si $2^{k+1}-1$ es primo, $2^k(2^{k+1}-1)$ es perfecto.

Leonhard Euler (1707–1783): los únicos números perfectos pares son los descritos por Euclides.

¿Existe algún número perfecto impar?

Quizás el problema más célebre de la $\mathcal{TN}$ aún no resuelto.

Variantes de los perfectos:

perfectos-múltiples: $\sigma n = l \cdot n$

abundantes: $\sigma n \geq l \cdot n$

...

Es difícil aportar resultados originales o problemas no resueltos.

Proponer buenos problemas aún no resueltos es un arte difícil. El balance entre trivial y no-resuelto es delicado.

Richard Guy, *Unsolved Problems in Number Theory*, 1994

Pál Erdös (1913-1996) aportó *buenos* problemas no resueltos, y ¡ofrecía recompensas! (junto a Euler, uno de los matemáticos más prolíficos.)

Un problema de reparto en Zumkia

El presidente de la república de Zumkia durante su larga vida ha logrado obtener una *hermosa* colección formada por un ejemplar de cada uno de los billetes de sus país; la colección asciende a un total de la nada despreciable cantidad de 1,249,920 zumkios. El zumkio, la moneda de Zumkia, está disponible en billetes de un zumkio y múltiplos de solo 3, 5 o 7 zumkios (existe el billete de 15 zumkios, pero no el de 10.) Cómo debe repartir el presidente la colección entre sus dos hijos en forma equitativa.

- Si el mayor billete ζ es *perfecto* ya tendremos un reparto.
- Un número es de Zumkeller (o 2–separable) si el conjunto de sus factores admite una partición en dos conjuntos con igual suma: 12 no es perfecto, pero $\Sigma\{1,3,4,6\} = \Sigma\{12,2\}$, y por tanto $12 \in \mathcal{Z}$

$\mathcal{Z}$ es infinito: $\Sigma\{1,2,3,p,2p,3p\} = \Sigma\{6,6p\}$, y $6p \in \mathcal{Z}$ si p primo > 3; pero $6p$ no es perfecto: $\sigma(6p) = 12(p+1) \neq 12p$.

En general, siendo $\mathcal{S}_l$ el conjunto de números l-separables,

$m \in \mathcal{S}_l, m \perp p$ primo $\Rightarrow$ $p^k m \in \mathcal{S}_l$ ($\mathcal{S}_l$ es vacío o infinito)

¿Qué problemas hay que resolver?

- Calcular el valor ζ del mayor billete $\zeta = 3^i 5^j 7^k$ sabiendo que sus factores suman $1,249,920$.
- Calcular sus divisores y repartirlos en dos grupos con igual suma, o bien demostrar que no es posible.

Teorema Fundamental de la Aritmética: Todo natural admite una única descomposición en factores primos (DFP):

$n = p_1^{k_1} \cdots p_j^{k_j}, k_i > 0, p_i$ primos distintos, $p_1 < p_2 < \ldots$

Demostración interesante: uso elegante y preciso del principio de inducción.

A partir de la DFP obtenemos la suma de los factores:

$$\sigma(p_1^{k_1} \cdots p_j^{k_j}) = (1 + ... + p_1^{k_1}) \cdots (1 + ... + p_j^{k_j}) \qquad (1)$$

¡cada factor de n aparece una sola vez en el desarrollo!

Calculemos i, j, k de forma que $\sigma(3^i 5^j 7^k) = 1,249,920 = 2^7 3^2 5^1 7^1 31^1$, es decir,

$$\frac{3^{i+1}-1}{3-1}\,\frac{5^{j+1}-1}{5-1}\,\frac{7^{k+1}-1}{7-1} = 2^7 3^2 5^1 7^1 31^1.$$

Razonamientos sencillos ($7 \nmid 7^{k+1}-1 \ldots$) conducen a $\zeta = 3^3 5^5 7$.

- número de factores: $(3+1)(5+1)(1+1) = 48$.
- número de posibles repartos: $2^{48}/2 = 140\ 737\ 488\ 355\ 328$
- y con igual número de billetes: $\binom{48}{24}/2 = 16\ 123\ 801\ 841\ 550$.

¡ No es *aconsejable* estudiar todos los posibles repartos!

¿ Cómo evitamos escudriñar todos los repartos ?

- Estudiar propiedades sencillas de verificar, pero decisivas. Los que las satisfacen los llamaremos candidatos: $\mathcal{C}_l$.
- Diseñar algoritmos rápidos ($O|\partial\, n|$) para decidir la separabilidad, al menos *para casi todos los candidatos*.
- Construir separables a partir de otros.

Propiedades elementales pero decisivas

Si $n \in \mathcal{Z}$, existe una partición $D \uplus D'$ con $\Sigma D = \Sigma D'$; luego:

- $2(\Sigma D) = \sigma\, n$, de donde $\sigma\, n$ es par.
- $\Sigma D \geq n$, y de aquí $\sigma\, n \geq 2n$.

En definitiva:

$$\text{Si } n \in \mathcal{Z}, \text{ entonces } 2 \mid \sigma\, n \wedge \sigma\, n \geq 2n. \tag{2}$$

En general

$$\text{Si } n \in \mathcal{S}_l, \text{ entonces } l \mid \sigma\, n \wedge \sigma\, n \geq l \cdot n. \tag{3}$$

Estas se comprueban directamente a través de la DFP.

Siendo $\boxed{h\, n \doteq \sigma\, n/n}$, definimos el conjunto de l–candidatos

$$\mathcal{C}_l = \{n \in \mathbb{N} \ : \ l \mid \sigma\, n \wedge h\, n \geq l\}$$

Distribución de candidatos y separables

Frecuencias de naturales $n \leq 10^7$ *satisfaciendo* $h\,n \doteq \sigma\,n/n \geq l$.

l	$l \mid \sigma\,n$	$h\,n \geq l$	candidatos	separables	% de separables
2	9 994 602	2 476 741	2 474 422	2 287 889	92.5
3	8 400 034	202 187	191 223	189 705	99.2
4	4 394 309	1 238	1 218	1 218	100.0
5	4 328 053	0	0	0	—

- casi todos los l-abundantes son separables, *pero no son tan abundantes.*
- la condición $h\,n \geq l$ es un buen *filtro*, $l \mid \sigma\,n$ NO.

Hemos comprobado para $n \leq 50,000,000$:

Conjetura 1.- La densidad de $\mathcal{Z}$ es $\simeq 0.229$. Paul Erdös conjetura que la de los abundantes es un irracional de $[0.24750,0.24893]$.

Conjetura 2.- Todo intervalo $[K, K+11]$ contiene un $n \in \mathcal{Z}$.

♣ Generadores y criba

Descompongamos los divisores de p^2m, con $m \perp p$ primo:

$$\partial(p^2m) = D \uplus pD \uplus p^2D, \qquad \text{siendo } D = \partial m$$

Si D es separable, entonces también lo serán pD, p^2D, ...
Por tanto, $m \in \mathcal{S}_l \;\Rightarrow\; p^k m \in \mathcal{S}_l$, y por el TFA

$$\text{Si } m \in \mathcal{S}_l, \text{ con } n \perp m, \text{ entonces } nm \in \mathcal{S}_l \qquad (A)$$

Por otro lado

$$\partial(5^3\boxed{3^3 5^2 7}) \;=\; \partial\boxed{3^3 5^2 7} \;\uplus\; 5^3\partial\boxed{3^3 5^2 7}$$

Luego $3^3 5^2 7 \in \mathcal{S}_l \;\Rightarrow\; 5^3(3^3 5^2 7)$. En general,

$$p^k m \in \mathcal{S}_l \Rightarrow p^{k+s(k+1)} m \in \mathcal{S}_l \qquad (B)$$

estos últimos los llamamos *trasladados*.

(A) y (B) proporcionan nuevos separables; los que no pueden obtenerse así los llamamos **generadores**. Los generadores de $\mathcal{S}_2$ son:

$$6, 12, 20, 28, 40, 48, 56, 70, 80, 88, 90, 104, 112, 126, 176, \ldots$$

♣ Emulando la **criba de Eratóstenes**, computaremos (en forma perezosa) la lista infinita de generadores de $\mathcal{S}_l$.

Por ejemplo, para $\mathcal{S}_2$:

– Se toman inicialmente la secuencia *infinita* ordenada de candidatos $(2|\sigma\, n \wedge \sigma\, n \geq 2 \cdot n)$:

$$6, 12, 20, 24, 28, 30, 40, 42, 48, 54, 56, 60, 66, 70, 78, 80, 84, \ldots$$

– Se toma el primer Zumkeller de esta secuencia (el 6) y se tachan todos sus trasladados y comúltiplos $6m$ $(m \perp 6)$:

$$\not{6}, 12, 20, \not{24}, 28, \not{30}, 40, \not{42}, 48, \not{54}, 56, \not{60}, \not{66}, 70, \not{78}, 80, 84, \ldots$$

El primer Zumkeller no tachado es el siguiente generador ...

¡En pocos minutos obtenemos los 7438 generadores de $\mathcal{Z}$ menores que 1 000 000!

Conjetura 3.- El número de generadores de Zumkeller menores que K es del orden de $0.5 \cdot K^{0.69}$ $(\ll 0.229 \cdot K)$.

Combinaciones unitarias de divisores (solo $\mathcal{S}_2$)

Un número es de Zumkeller sii el 0 se puede representar como **combinación unitaria** de sus factores:

$$0 = 1 - 2 + 3 + 4 + 6 - 12, \qquad \boxed{n \in \mathcal{Z} \iff 0 \in \mathcal{C}(n)}$$

Estudiemos ahora las CU de $p^k m$, donde $m \perp p$ primo.

Sea $X \pm Y = \{x + y, x - y, -x + y, -x - y \mid x \in X, y \in Y\}$

Ejemplo: $\mathcal{C}(5) = \{1\} \pm \{5\} = \{-6, -4, 4, 6\} \equiv \langle 4, 6 \rangle$

$\pm$ es conmutativo, asociativo, . . . , de donde:

$$\mathcal{C}(p^k m) = \mathcal{C}m \pm p\mathcal{C}m \pm \ldots \pm p^k \mathcal{C}m$$

Si aplicamos $\boxed{n \in \mathcal{Z} \iff 0 \in \mathcal{C}(n)}$ debemos calcular muchas combinaciones . . . pero

AJÁ $\boxed{0 \in A \pm pB \text{ sii } 0 \in \frac{1}{p}A \pm B}$

♠ Cocientes Reiterados. Una demostración vía $\mathcal{MR}\leftrightarrows\mathcal{PR}$.

Sabemos $n \in \mathcal{Z} \iff 0 \in \mathcal{C}(n) \equiv M \pm pM \pm p^2M \ldots$ (muchas combinaciones)

AJÁ $\boxed{0 \in A \pm pB \text{ sii } 0 \in \frac{1}{p}A \pm B}$; luego son equivalentes:

$$0 \in M \pm p(M \pm pM) \qquad 0 \in \frac{1}{p}M \pm (M \pm pM) \qquad 0 \in \frac{1}{p}(\frac{1}{p}M \pm M) \pm M$$

En general: $\boxed{p^k m \in \mathcal{Z} \text{ sii } \ 0 \in R_k}$, donde $M = \mathcal{C}m = R_0$,

$$R_1 = \frac{1}{p}R_0 \pm M \ldots$$

¿$3^i5^17^1 \in \mathcal{Z}$? $M = \mathcal{C}(5^17^1)$, ¡computemos con un sencillo programa!:

$$\begin{array}{ll}
R_0 \equiv \mathcal{C}(5^17^1) = \langle 22, 24, 32, 34, 36, 38, 46, 48\rangle & \boxed{\not\ni 0} \\
R_1 = \langle 6, , 64\rangle \equiv \langle 6, 8, 10, \ldots, 62, 64\rangle & \boxed{\not\ni 0} \\
R_2 = \langle 2, , 68\rangle & \boxed{\not\ni 0} \\
R_3 = \langle 0, , 70\rangle = R_4 = R_5 = \ldots & \boxed{\ni 0}
\end{array}$$

– ¡van creciendo!

luego $3^i5^17^1 \in \mathcal{Z} \iff i \geq 3$ ¡una demostración vía $\mathcal{MR}\leftrightarrows\mathcal{PR}$!

Una prueba $\mathcal{MR}\leftrightarrows\mathcal{PR}$ como tributo a Euclides/Euler

Teorema 1.- *Para cada primo impar* p,

$$2^k p \text{ es } 2\text{–separable sii } p \leq 2^{k+1}-1.$$

Demostración.- Usamos:

$$\boxed{2^k p \in \mathcal{Z} \Longleftrightarrow 0 \in \tfrac{1}{p}M \pm M} \text{ , con } M = \mathcal{C}(2^k)$$

Vía HASKELL generamos $\mathcal{C}(2), \mathcal{C}(2^2), \ldots$ y observando, conjeturamos $\mathcal{C}(2^k) = \langle 1, , 2^{k+1}-1\rangle$, que ya se prueba fácilmente por inducción.

- Si $p \leq 2^{k+1}-1$, $p \in \langle 1, , 2^{k+1}-1\rangle = M$, de donde $1 \in \frac{1}{p}M$; y como $1 \in M$, $0 \in \frac{1}{p}M \pm M$. Luego $2^k p \in \mathcal{Z}$.
- Si $p > 2^{k+1}-1$, entonces $\frac{1}{p}M$ es vacío, luego $0 \notin \frac{1}{p}M \pm M$.

¿Cuántos divisores primos tiene un abundante?

El menor 8-abundante par tiene 24 primos y 44 cifras:

$$189754423305609216200380675865179877721600 0$$

$$= 2^{10}3^{5}5^{3}7^{2}11^{2}13^{1}17^{1}19^{1}23^{1}29^{1}31^{1}37^{1}41^{1}43^{1}47^{1}53^{1} 59^{1}61^{1}67^{1}71^{1}73^{1}79^{1}83^{1}89^{1}$$

Todo 9–abundante par debe tener al menos 35 primos, aunque el menor tiene 37 primos, 73 cifras, y es par:

$$4368924363354820808981210203132513655327781713 900627249499856876120704000$$

$$= 2^{10}3^{5}5^{3}7^{3}11^{2}13^{2}17^{2}19^{1}23^{1}29^{1}31^{1}37^{1}41^{1}43^{1}47^{1}53^{1} 59^{1}61^{1}67^{1}71^{1}73^{1}79^{1}83^{1}89^{1}97^{1}101^{1}103^{1}107^{1}109^{1}113^{1} 127^{1}131^{1}137^{1}139^{1}149^{1}151^{1}157^{1}$$

¿Cuántos primos tiene el menor 10-separable impar?

¿Y el menor l-perfecto impar?

De la DFP obtenemos propiedades esenciales de h,

$$h(n\,m) \geq h\,n, \qquad h(q^k) = 1 + \frac{1}{q} + \cdots + \frac{1}{q^k}$$

y la acotación (Sylvester 1888;Carmichael 1907; Dickson 1913):

$$\sum_{1\leq i\leq j} \frac{1}{p_i} < (\frac{1+p_1}{p_1}) \cdots (\frac{1+p_k}{p_k}) \leq h(p_1^{k_1} \ldots p_j^{k_j}) < \prod_{1\leq i\leq j} \frac{p_i}{p_i - 1}$$

♢ Como la serie $\sum_{p\ primo} \frac{1}{p}$ diverge: (Euler 1737; Clarkson 1966)

¡El conjunto de l–abundantes es no vacío, y por tanto, infinito!

♢ Otro ejemplo:

$$h(3^a 5^b 7^d) < \frac{3}{3-1} \cdot \frac{5}{5-1} \cdot \frac{7}{7-1} = \frac{105}{48} < 3$$

¡El presidente de Zumkia no puede repartir entre tres hijos!

♠ La acotación (Sylvester 1888;Carmichael 1907; Dickson 1913)

$$(\frac{1+p_1}{p_1})\dots(\frac{1+p_k}{p_k}) \leq h(p_1^{k_1}\dots p_j^{k_j}) < \sum_{1\leq i\leq j}\frac{p_i}{p_i-1}$$

permite encontrar cotas del número de primos de un abundante.

Un programa HASKELL (basado en redes de procesos) computa valores de estas cotas para candidatos pares e impares:

l	2	3	4	5	...	9	10
$(\underline{P_l}, \overline{P_l})$	(2,2)	(3,6)	(4,11)	(6,24)	...	$\boxed{(35, 553)}$	(55,1245)
$(\underline{I_l}, \overline{I_l})$	(3,5)	$\boxed{(8, 16)}$	(21,51)	(54,166)	...	(2697, 22791)	(?,?)

¡ El presidente de Zumkia no podrá repartir los billetes de su colección entre tres hijos !

La cota superior normalmente está muy alejada del valor real.
(para $l = 4$ hay abundantes con 4 primos, pero el menor tiene 5)

Menores abundantes con np primos (♣ es el menor separable)

np	$l = 3$	$l = 4$	$l = 5$
3	♣$120 \in \mathcal{S}_3$ $2^1 3^1 5^1$		
4	$420 \in \mathcal{S}_3$ $2^2 3^1 5^1 7^1$	$30\,240 \in \mathcal{S}_4$ $2^5 3^3 5^1 7^1$	
5		♣$27\,720 \in \mathcal{S}_4$ $2^3 3^2 5^1 7^1 11^1$	
6		$120\,120 \in \mathcal{S}_4$ $2^3 3^1 5^1 7^1 11^1 13^1$	$605\,404\,800 \in \mathcal{S}_5$ $2^7 3^3 5^2 7^2 11^1 13^1$
7			$122\,522\,400 \notin \mathcal{S}_5$ $2^5 3^2 5^2 7^1 11^1 13^1 17^1$ ♣$147\,026\,880 \in \mathcal{S}_5$ $2^6 3^3 5^1 7^1 11^1 13^1 17^1$
8			$232\,792\,560 \in \mathcal{S}_5$ $2^4 3^2 5^1 7^1 11^1 13^1 17^1 19^1$

Existen infinitos candidatos. El teorema de Dirichlet

(P.G. Legeune Dirichlet 1837): Si a y b son enteros $(b > 0)$ primos entre sí, entonces la progresión aritmética $a+bk$ contiene una infinidad de números primos.

Luego, existen infinitos primos de la forma $p = -1 + kl$,

y todos satisfacen $l|(1+p) = \sigma(p)$

Por tanto, existe $p \perp m$ tal que $l|\sigma(pm)$.

Si m es abundante, también lo es pm, y pm un candidato.

Es decir,

$\mathcal{C}_l$ es no vacío, y por tanto infinito.

Según T Apóstol: la prueba del Teorema de Dirichlet es el **origen de la teoría analítica de los números**.

♠ Los candidatos no separables son infinitos

Ejecutando nuestro programas vimos que:

♢ Entre los menores 2-candidatos no separables aparecen $(2^1 3^2)p$, para p primo $\geq 41 > 39 = \sigma(2^1 3^2)$.

♢ Para $l = 3, \ldots$ ocurre algo parecido

$\mathcal{MR} \leftrightarrows \mathcal{PR}$ nos lleva a conjeturar:

Si $m \perp p$ primo y $p > \sigma\, m$, entonces $m \notin \mathcal{S}_l \;\Rightarrow\; p^k m \notin \mathcal{S}_l$.

o equivalentemente

$$p^k m \in \mathcal{S}_l \;\Rightarrow\; m \in \mathcal{S}_l$$

Sea una l-separación de las sumas de los divisores de pm:

$$s_1 + p\triangle_1 = s_2 + p\triangle_2 = s_3 + p\triangle_3 = \ldots$$

Entonces $|s_i - s_i|$ es múltiplo de p, y $|s_i - s_i| \leq \sigma m < p$,
Luego $|s_i - s_i| = 0$, $s_i = s_i = \ldots$, y $m \in \mathcal{S}_l$

♠ Construcción de un candidato no separable

PASO 1 Sea $m = p_1^{k_1} \dots p_j^{k_j}$, con $h(m) \geq l$.

PASO 2 Para asegurar que $l \nmid \sigma\, m$, *ajustamos* m:
Si $l \mid \sigma(q^k)$, q primo, entonces $l \nmid \sigma(q^{k+1})$.
Por tanto $\exists m \notin \mathcal{S}_l, hm \geq l$.

PASO 3 Existe $p > \sigma(m)$ tal que $l|\sigma(pm)$. Por ser m abundante, también lo será pm, de donde pm es un candidato.

PASO 4 Como $m \notin S_l$, tendremos que $p\,m \notin S_l$, pero $p\,m \in \mathcal{C}_l$.

Luego $\mathcal{C}_l \subsetneq \mathcal{S}_l$

Casi comprobación voraz de $n \in \mathcal{Z}$

Los algoritmos más sencillos escudriñan en forma combinatoria todas las particiones. Son ineficaces (incluso inútiles).

Estudiemos un algoritmo de comprobación *casi* directa.

Tomemos por ejemplo $n = 80 = 2^4\,5$. En primer lugar comprobamos que es un candidato:

$$\sigma(80) = (2^{4+1} - 1)(1 + 5) = 186 = 2 \cdot 93$$

$$h(80) = 186/80 \simeq 2{,}32 > 2$$

Ahora *repartimos* en dos montones la lista descendente de sus divisores: $[80, 40, 20, 16, 10, 8, 5, 4, 2, 1]$

Comenzamos desde la situación

[80,40,20,16,10,8,5,4,2,1]	93 [ ]	93 [ ]
$[d, ...]$	s [. . .]	s' [. . .]

[80,40,20,16,10,8,5,4,2,1]	93	[ ]	93	[ ]
[40,20,16,10,8,5,4,2,1]	13	[80]	93	[ ]
[10,8,5,4,2,1]	13	[80]	17	[16, 20, 40]
[8,5,4,2,1]	3	[10, 80]	17	[16, 20, 40]
[2,1]	3	[10, 80]	0	[4, 5, 8, 16, 20, 40]
[ ]	0	[1, 2, 10, 80]	0	[4, 5, 8, 16, 20, 40]

Una colosal sorpresa: el algoritmo obtiene una partición correcta casi siempre

$$Main > [\, n \mid n \in [1 \,..\, 10000], \\ esDeZumkeller\ n \neq casiEsDeZumkeller\ n]$$

$$[1190, 1430, 1575, 2090, 3410, 4408, 4510, 5775, 8228, 9765]$$
$$(6{,}04\ secs,\ 346124744\ bytes)$$

♠ Fallos del algoritmo voraz

Para $n \leq 10^K$ se producen $\simeq 0{,}00003125 \cdot 2^K$ fallos

N	*esDeZ*	*casiEsDeZ*	fallos sobre	el	total	% fallos
10,000	0.06	0.06	10	/	2294	0.45
1,000,000	17.02	16.40	4764	/	229026	2.08
10,000,000	359.05	291.03	81914	/	2287889	3.58
20,000,000	8339.50	746.03	185256	/	4577210	4.05

Tiempos de ejecución (segundos) vía ghc-6.10.1, Windows XP, Sony VAIO/CPU Intel U1400 @ 1.20Ghz/1Gb RAM

El algoritmo se amplia a los l-separables

Por ejemplo, $\sigma(120) = 3 \cdot 120$, el algoritmo separa en 3 montones:

[ ]	[120]	[60,40,20]	[30,24,15,12,10,8,6,5,4,3,2,1]

El algoritmo voraz se traslada rápidamente a HASKELL

```
type Factores = [Integer]
type Suma = Integer
casiAdmitePartición :: Factores → Suma → Suma → Bool

casiAdmitePartición []       _ _  = False
casiAdmitePartición (d : ds) s s'
| d == s || d == s'               = True
| d ≤ s                           = casiAdmitePartición ds (s − d) s'
| d ≤ s'                          = casiAdmitePartición ds s (s' − d)
| otherwise                       = False   — FALLO

casiEsDeZumkeller n = par sigma && sigma ≥ 2 * n &&
                      casiAdmitePartición ds ms ms
  where fs    = factoriza n
        sigma = sumaDeDivisores fs
        ds    = divisoresO fs   — ¡decreciente!
        ms    = sigma `quot` 2
```

♠ Para obtener un algoritmo que comprueba $n \in \mathcal{Z}$ en todos los casos, sustituimos $casiAdmitePartición$ por:

$$
\begin{array}{lll}
admitePartición & [\,] & \_\ \_ = False \\
admitePartición & (d : ds)\ s\ s' & \\
\mid d == s \mid\mid d == s' & & = True \\
\mid otherwise & & = d \leq s\ \&\&\ admitePartición\ ds\ (s-d)\ s' \mid\mid \\
 & & \quad d \leq s'\ \&\&\ admitePartición\ ds\ s\ (s'-d)
\end{array}
$$

Ligeros cambios permiten devolver la partición, controlar la misma cardinalidad, . . .

Para $n \leq 10^K$ se producen $\simeq 0{,}00003125 \cdot 2^K$ fallos.

Para los fallos, ¡computamos una buena aproximación!

Por ejemplo, para el primer fallo 1190, el algoritmo termina así:

[**5,2,1**]	4	[17,85,1190]	4	[7,10,14,34,35,70,119,170,238,595]

♢ El algoritmo es **voraz** (no puede recuperar un paso erróneo)

♢ Tomando candidatos, se diferencian en *calderilla*:
$\sigma(1190)/2 = 1296$, pero $\Sigma_1 - \Sigma_2 = 2 \;\; (0{,}16\,\%)$

Si el presidente de Zumkia usa este algoritmo *natural* llega a una solución muy descompensada: montones con 42 y 6 billetes.

¡ ... el problema está resuelto !

¿Y si quiere montones con el mismo número de billetes?

Un ejemplo de $\mathcal{PR}\rightleftarrows\mathcal{MR}$: una solución para el presidente

$\partial(3^3 5^5 7)$ tiene $\sim 1{,}6 \cdot 10^{13}$ equi-particiones.
$\partial(3^3 5^2 7)$ tiene $\sim 2{,}7 \cdot 10^{6}$ equi-particiones.

$$\partial(5^3\boxed{3^3 5^2 7}) \;=\; \partial\boxed{3^3 5^2 7} \;\uplus\; 5^3\partial\boxed{3^3 5^2 7}$$

luego, $3^3 5^2 7 \in \mathcal{S}_2 \;\Rightarrow\; 5^3(3^3 5^2 7) \in \mathcal{S}_2$.

Para $3^3 5^2 7$ nuestro programa *Haskell encuentra* rápidamente una separación con el mismo número de divisores:

$$\Sigma\{1, 3, 5, 7, 9, 15, 25, 27, 35, 45, 63, 3^3 5^2 7\}$$
$$= \Sigma\{21, 75, 105, 135, 175, 189, 225, 315, 525, 675, 945, 1575\}$$

Ahora basta añadir los mismos multiplicados por 5^3:

$$\Sigma\{\; 1, 3, 5, 7, 9, 15, 25, 27, 35, 45, 63, 3^3 5^2 7,$$
$$125, 375, 625, 875, 1125, 1875, 3125, 3375, 4375, 5625, 7875, 3^3 5^5 7\} =$$
$$\Sigma\{\; 21, 75, 105, 135, 175, 189, 225, 315, 525, 675, 945, 1575,$$
$$2625, 9375, 13125, 16875, 21875, 23625, 28125, 39375, 65625, 84375, 118125, 196875\}$$

¿Cuales son los límites de nuestros algoritmos?

A través de un *buenos* algoritmos la comprobación $n \in \mathcal{S}_l$ queda reducida a la factorización.

Recordemos pues la siguiente reflexión de Gauss (*Disquisitiones Arithmeticæ*, 1801):

> El problema de distinguir los números primos de los compuestos y su factorización es uno de los problemas más importantes y útiles en la aritmética ... Sin embargo, debemos confesar que todos los métodos que se han propuesto hasta el momento son muy especiales o laboriosos incluso para números pequeños ... La dignidad de la ciencia requiere toda la ayuda para explorar la solución de un problema tan elegante y célebre.

Conclusiones

Es esencial construir un modelo sencillo

La elección de un buen lenguaje traslada el modelo a un programa correcto por construcción

¡Con nuestros programas enunciamos nuevos resultados, y en muchos casos construimos sus pruebas!

La interacción $\mathcal{MR} \leftrightarrows \mathcal{PR}$ proporciona una investigación matemática experimental barata, y de calidad, incluso usando resultados elementales

Recordemos de nuevo a Vladímir Arnold, *el matemático que amaba los problemas*

Las matemáticas son la parte de la física en la que los experimentos son más baratos.

Bibliografía

[1] Albert, A.A. Leonard Eugene Dickson: A Biographical Memoir. Biographical Memoir, pp. 329-345 (1955); National Academy of Sciences, Washington (1994).

[2] Bach, Erich; Miller, Gary and Shallit, Jeffrey. Sums of divisors, perfect numbers and factoring. SIAM Journal on Computing, 15-4, pp. 1143 - 1154 (1986)

[3] Bhaskara, K.P.S. and Peng, Y. On Zumkeller Numbers. En arXiv:0912.0052v1 [math.NT] (2009).

[4] Brassard, G. and Bratley, P. Fundamentals of Algorithmics. Prentice Hall (1996).

[5] Carmichael, R.D. A table of multiply perfect numbers. Bull. Amer. Math. Soc. 13, pp 383-386 (1907).

[6] Carmichael, R.D. Even multiply perfect numbers of five different prime factor. Bull. Amer. Math. Soc. Volume 15, Number 1, 7-8 (1908). Este complementa [5].

[7] Dickson, L.E. Finiteness of the odd perfect and primitive abundant number with n distinct prime factors. Amer. J. Math. vol. 35, pp. 413–422 (1913).

[8] Dickson, L.E. Even abundant numbers. Amer. J. Math. vol. 35 pp. 423–426 (1914).

[9] Dickson, L.E. History of the Theory of Numbers. Carnegie Institute (1919).

[10] Guelfond, A.O. Resolución de ecuaciones en números enteros. Colección *Lecciones populares de matemáticas*. Ed. Mir (1979) (versión española de 1979).

[11] Guy, Richard. Unsolved Problems in Intuitive Mathematics. Vol 1: Unsolved problems in Number Theory. 2ª ed. Springer-Verlag (1994).

[12] Hardy, G.H. Autojustificación de un matemático. Ariel (1981). traducción de *A Mathematician's Apology*, Cambridge Univ. Press (1940).

[13] Hardy, G.H. and Wright, E.M. Introduction to The Theory of Numbers. Oxford University Press, 4ª ed. corregida (1968).

[14] Hawking, Stephen. Dios creó los números. Ed. Crítica (2006). Versión española de *God created the integers*, Penguin (2005).

[15] Knuth, Donald. The Art of Computer Programming; vol. 2, *Seminumerical Algorithms*. Addison Wesley, 2ª ed. (1980).

[16] Lehmer, Derrick Norman. Multiply perfect numbers. Annals of Mathematics, (2), vol. 2 (1901).

[17] Muñoz, R., Ruiz, B. y Muñoz, M.; Combinaciones de divisores y Números de Zumkeller. Actas de XIII CIAM (Congreso de Enseñanza y Aprendizaje de las Matemáticas, Córdoba, Setiembre de 2010).

[18] Pomerance, Carl. On the congruences "$\sigma(n) \equiv a(\bmod n)$ and $n \equiv a(\bmod \phi(n))$. Acta Arith. 26, no. 3, 265–272 (1975).

[19] Pomerance, Carl. Multiply perfect numbers. Mersenne Primes, and Effective Computability. Math. Ann. 226, pp 195-206, Stringer-Verlag (1977).

[20] Pomerance, Carl. Primality testing: Variations on a them of Lucas. Proceed. 13th Meeting of the Fibonacci Association, Congressus Numeratium 201, pp 301-312 (2010)

[21] Puertas Castaños, M.L. *Elementos Libros X-XII.* Ed. Gredos, Madrid (1996).

[22] Ruiz, B.C. et al. Razonando con Haskell. Ed. Thomson (2004). Véase la página del libro en `http://www.lcc.uma.es/RazonandoConHaskell`.

[23] Ruiz, B.C. et al. Some Light On The Conjectures Of Goldbach And Opperman En: Second Mediterranean Conference On Mathematics Education, Vol 1, 65-74 (2000), Nicossia, Chipre.

[24] Ruiz, B.C. et al. From recreational mathematics to recreational programming, and back. International journal of mathematical education in science and technology, Vol. 42, N°. 6, 2011 , págs. 775-787.

[25] Voight, John. Perfect numbers: An elementary introduction (1998) (no publicado).

[26] Voight, J. On the nonexistence of odd perfect numbers. Mass SelectA, A. Math. Soc. (2003).