NÚMEROS PERFECTOS

JHONATAN COLLAZOS RAMÍREZ

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN

DEPARTAMENTO DE MATEMÁTICAS

POPAYÁN, CAUCA

2015

NÚMEROS PERFECTOS

TRABAJO DE GRADO

En modalidad de Seminario de Grado

presentado como requisito para optar al título de Matemático

JHONATAN COLLAZOS RAMÍREZ

Director:

JHON JAIRO BRAVO GRIJALBA

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN

DEPARTAMENTO DE MATEMÁTICAS

POPAYÁN, CAUCA

2015

Nota de aceptación

Director:

Dr. Jhon Jairo Bravo Grijalba

Jurados:

Dr. Carlos Alberto Trujillo Solarte

Mg. Maribel Díaz Noguera

Fecha de sustentación: Octubre 22 de 2015

Dedicado a ECOZ.

Agradecimientos

A los profesores Jhon Jairo Bravo Grijalba y Diego Fernando Ruíz, por su constante colaboración y apoyo en la realización de este trabajo. Han sido una fuente de gran inspiración, tanto en la parte matemática como en la parte humana al compartir sus conocimientos y experiencias.

A mi familia, Adriana Cruz y a la comunidad de A.A por el apoyo incondicional que siempre me ha brindado durante estos años.

Solo por la gracia de Dios.

Resumen

Un *número perfecto* es un entero positivo n tal que la suma de todos los divisores positivos de n es igual a $2n$. En este trabajo de grado se estudian algunas propiedades aritméticas de los números perfectos, entre las cuales se destaca la caracterización de los números perfectos pares, los cuales tienen la forma $2^{p-1}(2^p - 1)$ donde $2^p - 1$ es un número primo. Hasta el momento se conoce una cantidad finita de números perfectos pares. En la actualidad no se conocen números perfectos impares, sin embargo, mostramos algunas características que deberían tener los números perfectos impares en caso de que existan. Finalmente, hacemos un estudio detallado del trabajo del profesor Florian Luca "*Perfect Fibonacci and Lucas numbers*" del año 2000, en el cual se prueba, entre otras cosas, que no hay números de Fibonacci que sean perfectos.

Notación

La notación que usaremos en este documento es la estándar en teoría de números. Aunque la mayoría de notación será introducida en su momento, a continuación presentamos una lista de los símbolos más comunes que usaremos en este trabajo de grado.

$\mathbb{N}$, $\mathbb{Z}^+$	Conjunto de números naturales $\{1, 2, \ldots\}$.
$a \mid b$	a divide b, a es un divisor de b, b es un múltiplo de a.
$a \equiv b \pmod{n}$	a es congruente con b módulo n.
$\left(\dfrac{a}{p}\right)$	Símbolo de Legendre de a con respecto a p.
$\operatorname{mcd}(a, b)$	Máximo común divisor de a y b.
$\sigma(n)$	Suma de los divisores positivos de n.
$\phi(n)$	Número de enteros positivos menores o iguales a n y coprimos con n.
$w(n)$	Número de primos distintos que dividen a n.
$I(n)$	Índice de abundancia de n, es decir la suma de los inversos de todos los divisores de n.
$\log x$	Logaritmo de x en base 10.
p, q	Números primos mayores que uno.
$f(x) = O(g(x))$	$f(x)$ es O mayúscula de $g(x)$.
$\prod_{i=1}^{r} p_i^{\alpha_i}$	El producto $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.
$\sum_{j=0}^{s} q_i^j$	La suma $1 + q_i + \cdots + q_i^s$.
$\displaystyle\sum_{d \mid n} f(d)$	La suma de los valores de la función f en todos los divisores de n.

Índice general

Capítulo 1

Introducción

Un entero positivo que tienen la propiedad de que es igual a la suma de todos sus divisores propios positivos, se denomina *número perfecto*. Los números perfectos fueron estudiados por Pitágoras y sus discípulos, más por sus propiedades místicas que por sus propias propiedades teóricas. La definición original de número perfecto estaba dada en términos de "partes divisibles" de un número [3]. Por ejemplo, las partes divisibles de 10 son: 1, 2 y 5, ya que $1 = \frac{10}{10}$, $2 = \frac{10}{5}$ y $5 = \frac{10}{2}$. Note que 10 no es una parte divisible de 10 porque no se puede obtener como una fracción entre 10 y un entero positivo mayor que 1.

Los primeros conocimientos matemáticos de los que se tiene información referente a los números perfectos aparecen en los *Elementos de Euclides* escritos alrededor del año 300 a.c. En la antigua Grecia sólo se había descubierto los siguientes números perfectos:

$$\begin{aligned}
6 &= 1 + 2 + 3;\\
28 &= 1 + 2 + 4 + 7 + 14;\\
496 &= 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248;\\
8128 &= 1 + 2 + 4 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064.
\end{aligned}$$

De este modo era natural pensar que existían pocos números perfectos. Era necesario entonces preguntarse qué propiedades tenían para tratar de caracterizarlos. Euclides observó que

$$6 = 2 \cdot 3 = 2^{2-1} \cdot (2^2 - 1);$$

$$28 = 4 \cdot 7 = 2^{3-1} \cdot (2^3 - 1);$$

$$496 = 16 \cdot 31 = 2^{5-1} \cdot (2^5 - 1);$$

$$8128 = 64 \cdot 127 = 2^{7-1} \cdot (2^7 - 1).$$

Con esa información Euclides probó que

“Si $2^k - 1$ es primo y $N = 2^{k-1}(2^k - 1)$, entonces N es perfecto”.

A los números primos de la forma $M_p := 2^p - 1$ se les conoce como primos de Mersenne. La historia de la búsqueda de primos de Mersenne se puede dividir en dos fases; el antes y el después de la llegada de los computadores. En el tiempo donde no existían las computadoras, la búsqueda de primos de Mersenne era tediosa y llena de errores. En el año 1588 se verificó que M_{17} y M_{19} eran primos. En 1772, Euler probó que M_{31} era un número primo usando divisiones hasta 46337, donde $46337 \leqslant \sqrt{M_{31}}$.

En 1644 el monje francés Marin Mersenne, en su libro Cogitata Physica-Mathematica, afirmó que los números M_p son primos para $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, y compuestos para todos los demás valores de p menores que 257. No se sabe cómo pudo llegar a esa conclusión, pero con el tiempo se probó que M_{67} y M_{257} no son primos, mientras que M_{61}, M_{89} y M_{107} sí lo son.

Pasaron muchos años para probar que M_{67} no era primo. En 1876 Lucas usa el test que había desarrollado para mostrar ese hecho sin encontrar su descomposición en factores primos. Tuvieron que pasar 27 años para encontrar la factorización de M_{67}, la cual fue realizada por Frank Nelson Cole en 1903, en una de las reuniones de la *American Mathematical Society.*

Antes de la llegada de los computadores eran 12 los primos de Mersenne encontrados (el último de ellos fue encontrado en 1914), pero desde de la llegada de los computadores se ha encontrado, a un ritmo aproximado de un primo de Mersenne por cada dos años. Note en la Figura 1.1 que a partir de 1952 gracias a la entrada de los computadores, ha aumentado el número de primos de Mersenne encontrados. Encontrar primos de Mersenne no es un trabajo sencillo; actualmente solo se conocen 48 de ellos. El último primo de Mersenne fue hallado en 2013.

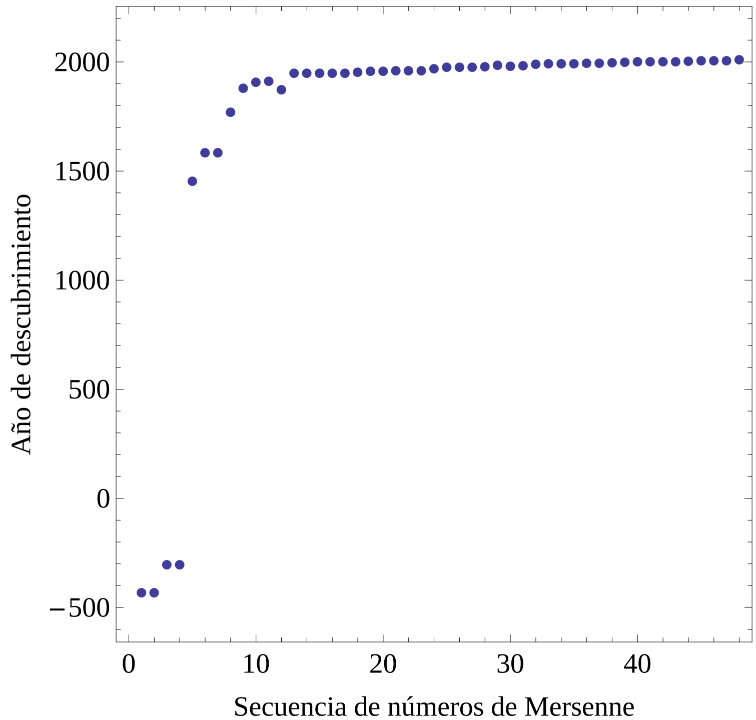

Figura 1.1: Sucesión de los números de Mersenne encontrados en los respectivos años. Datos tomados de [1].

En el año 1952 Raphael Robinson con la ayuda de los computadores encontró cinco primos de Mersenne, además de los que ya se conocían. Él utilizó The National Bureau of Standards Western Automatic Computer (SWAC) con la ayuda de los esposos Derrick H. Lehmer y Emma Trotskaia Lehmer.

Los primos de Mersenne decimotercero y decimocuarto fueron encontrados el primer día que fue utilizada la máquina (30 de enero de 1952), la cual utilizó la prueba de Lucas-Lehmer que permite decidir su primalidad, y los otros tres fueron encontrados en los siguientes nueve meses.

La prueba de Lucas-Lehmer sirve para determinar si un determinado número de Mersenne M_p es primo y consiste en el siguiente algoritmo. Sea $M_p = 2^p - 1$ el número de Mersenne a verificar. Definamos la sucesión s_i para todo $i \geq 0$ de la siguiente manera:

$$s_i = \begin{cases} 4 & \text{si } i = 0 \\ s_{i+1}^2 - 2 & \text{si } i > 0 \end{cases}$$

M_p es primo si y sólo si $s_{p-2} \equiv 0 \pmod{M_p}$. En caso contrario, M_p es compuesto.

El test de Lucas-Lehmer puede ser utilizado con bastante rapidez. Si M_p denota el p-ésimo número de Mersenne, entonces es posible determinar si M_p es un primo de Mersenne usando $O(p^3)$[1] operaciones de bits ([17]).

En comparación con las computadoras de hoy, SWAC era primitiva, su memoria total fue de 1152 bytes, y la mitad de esta memoria era utilizada para los comandos que dirigen el programa.

En el siglo XVIII se produjo un gran avance en el estudio de los números perfectos; Euler logró demostrar que si un entero positivo es perfecto y par, entonces tiene la forma $2^{p-1}(2^p - 1)$, siendo $2^p - 1$ un primo de Mersenne. Es decir, la condición para encontrar números perfectos pares no sólo es necesaria, sino además suficiente.

En cuanto a los números perfectos impares el interrogante es mucho más grande. En los últimos siglos varios resultados han arrojado algo de luz sobre ellos, y cada vez parece más probable que no existan.

En este trabajo de grado estamos interesados en estudiar algunas propiedades de los números perfectos. El trabajo de grado esta organizado de la siguiente manera. En la Introducción (Capitulo 1), hacemos un breve recorrido por la historia de los números perfectos y en el Capitulo 2 presentamos diferentes resultados los cuales caracterizan los números perfectos pares. Posteriormente en el Capítulo 3 estudiamos el concepto de *índice de abundancia* y su relación con los números perfectos.

Finalmente, en los Capítulos 4 y 5 abordamos dos trabajos del profesor Florian Luca, en los cuales se demuestra la inexistencia de números perfectos consecutivos y la inexistencia de números perfectos en las sucesiones de Fibonacci y de Lucas.

[1] Si $g(x) \geq 0$, para todo $x \geq a$, escribimos $f(x) = O(g(x))$, para indicar que el cociente $f(x)/g(x)$ es acotado, para $x \geq a$; esto es, existe una constante $M > 0$ tal que $|f(x)| \leq Mg(x)$ para todo $x \geq a$.

Capítulo 2

Números perfectos pares

La suma de todos los divisores positivos de un número entero $m \in \mathbb{Z}^+$ se llama la función sigma de m, denotada por $\sigma(m)$. Es decir, $\sigma(m) = \sum_{d|m} d$. De esta manera el concepto de número perfecto se puede plantear en términos de la función σ. Formalizamos este concepto como sigue

Definición 2.1. *Un entero positivo N es perfecto si $\sigma(N) = 2N$.*

Notemos que 6 es perfecto porque $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6$.

Los griegos solo conocían 4 números perfectos. Fué Euclides el que probó que si la suma $1+2+2^2+\cdots+2^{p-2}+2^{p-1} = 2^p - 1$ es primo, entonces $2^{p-1}(2^p - 1)$ es perfecto. Consideremos la suma $1 + 2 = 3$. Como 3 es un número primo, entonces $2^{2-1}(2^2 - 1) = 6$ es perfecto.

Es bien conocido que si $2^n - 1$ es primo, entonces n es primo. Sin embargo, si p es primo no necesariamente $2^p - 1$ es un número primo. En efecto $2^{11} - 1 = 23 \cdot 89$ es compuesto a pesar de que 11 es un número primo.

Teorema 2.1. *Si $2^k - 1$ es primo y $N = 2^{k-1}(2^k - 1)$, entonces N es perfecto.*

Demostración. Si $2^k - 1 = p$ es un número primo, entonces $N = 2^{k-1}(2^k - 1) = 2^{k-1}p$.

Por lo tanto los divisores propios N son

$$1, 2, \ldots, 2^{k-1}, p, \ldots, 2^{k-2}p.$$

Si S es suma de los divisores propios de N, entonces

$$
\begin{aligned}
S &= (1+2+4+\cdots+2^{k-1}) + (1+2+4+\cdots+2^{k-2})p \\
&= (2^k-1) + (2^{k-1}-1)p \\
&= p + 2^{k-1}p - p \\
&= 2^{k-1}p = N.
\end{aligned}
$$

Por lo tanto, N es perfecto. $\square$

Definición 2.2. *Sea p primo. A los números primos de la forma $M_p := 2^p - 1$ se les conoce como primos de Mersenne.*

Encontrar primos de Mersenne no es un trabajo sencillo; actualmente solo se conocen 48 de ellos. El último primo de Mersenne fue hallado en 2013 y es $2^{57{,}885{,}161} - 1$, que tiene 17,425,170 cifras [1]. Note que para cada uno de los primos de Mersenne basta aplicar la construcción de Euclides para obtener un número perfecto. De este modo, la búsqueda de números perfectos se puede direccionar a la búsqueda de primos de Mersenne.

En el siglo XVIII se produjo un gran avance en el estudio de los números perfectos, Euler logró demostrar que si un entero positivo es perfecto y par, entonces tiene la forma $2^{p-1}(2^p-1)$, con $2^p - 1$ un primo de Mersenne. Es decir, la condición para encontrar números perfectos pares no sólo es necesaria, sino además suficiente.

Veamos ahora una definición.

Definición 2.3. *En teoría de números, una función aritmética $f : \mathbb{N} \longrightarrow \mathbb{C}$ es multiplicativa si $f(1) = 1$ y $f(x.y) = f(x).f(y)$ siempre que sean x y y primos relativos.*

A continuación mostramos que la función σ es una función multiplicativa.

Teorema 2.2. *La función σ es multiplicativa.*

Demostración. Sean X y Y dos enteros positivos. Sea $x_1, \cdots, x_s$ los divisores positivos de X y $y_1, \cdots, y_t$ los divisores positivos de Y. Entonces, $\sigma(X) = x_1 + \cdots + x_s$ y $\sigma(Y) = y_1 + \cdots + y_t$.

Dado que $\operatorname{mcd}(X, Y) = 1$, entonces los divisores de XY son todos los productos que se obtienen al multiplicar un divisor de X por un divisor de Y, i.e., son todos los productos de la forma $x_i y_j$ donde $i = 1, \ldots, s$; $j = 1, \ldots, t$. Luego

$$
\begin{aligned}
\sigma(XY) &= x_1 y_1 + \cdots + x_1 y_t + x_2 y_1 + \cdots + x_2 y_t + \cdots + x_s y_1 + \cdots + x_s y_t \\
&= x_1(y_1 + y_2 + \cdots + y_t) + x_2(y_1 + y_2 + \cdots + y_t) + \cdots x_s(y_1 + y_2 + \cdots + y_t) \\
&= (x_1 + x_2 + \cdots + x_s)(y_1 + y_2 + \cdots + y_t) \\
&= \sigma(X)\sigma(Y).
\end{aligned}
$$

□

Teorema 2.3. *Si N es un número perfecto par, entonces N se puede escribir de la forma $N = 2^{p-1}(2^p - 1)$, donde $2^p - 1$ es primo.*

Demostración. Si N es un número perfecto par, entonces N se puede escribir de la forma $N = 2^{n-1}m$ con m impar y $n > 1$. Como σ es multiplicativa tenemos que

$$
\begin{aligned}
\sigma(N) &= \sigma(2^{n-1}m) \\
&= \sigma(2^{n-1})\sigma(m) \\
&= \left(\frac{2^n - 1}{2 - 1}\right)\sigma(m) \\
&= (2^n - 1)\sigma(m).
\end{aligned}
$$

Puesto que N es perfecto, tenemos que

$$\sigma(N) = 2N = 2(2^{n-1}m) = 2^n m,$$

de donde

$$2^n m = (2^n - 1)\,\sigma(m).$$

Ya que $2^n - 1$ es impar, $2^n - 1 \mid m$, luego existe $k \in \mathbb{Z}^+$ tal que $m = (2^n - 1)k$. Así

$$(2^n - 1)\sigma(m) = 2^n(2^n - 1)k,$$

de donde

$$\begin{aligned}\sigma(m) &= 2^n k\\ &= (2^n-1)k+k\\ &= m+k.\end{aligned}$$

Pero $k \mid m$, así $\sigma(m) = m+k$ implica que m tiene solo dos divisores; a saber m y k. Luego $k=1$ y por lo tanto $\sigma(m) = m+1$ nos dice que m es primo. De otro lado, como $2^n-1 \mid m$, se tiene que $m = 2^n-1$. En consecuencia $N = 2^{n-1}(2^n-1)$ donde 2^n-1 es primo. □

Los números perfectos están estrechamente relacionados con los números triangulares, los cuales son de la forma $1+2+3+\cdots+n$, donde n es un entero positivo. Estos números son llamados así por la disposición de puntos que forman matrices triangulares (como se muestra en la Figura 2.1).

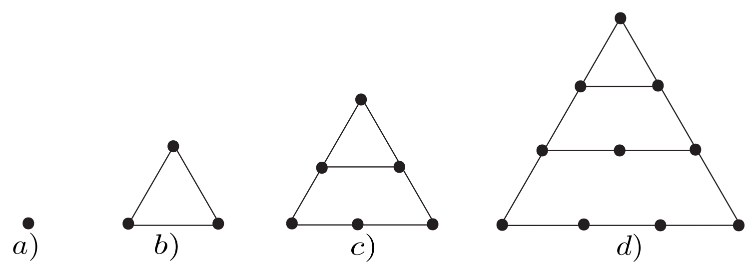

Figura 2.1: Cuatro primeros números triangulares. $a)$ 1, $b)$ 3, $c)$ 6 y $d)$ 10.

Note que cada número triangular T_n está definido por $T_n := n(n+1)/2$. Ahora bien, si N es un número perfecto de la forma $2^{p-1}(2^p-1)$, entonces

$$N = \frac{(2^p-1)\left((2^p-1)+1\right)}{2},$$

mostrando que N es un número triangular. Se puede afirmar entonces que un número perfecto par es un número triangular. Por ejemplo

$$\begin{aligned}1+2+3 &= 6,\\ 1+2+3+4+5+6+7 &= 28,\\ 1+2+3+4+5+6+7+8+9+\cdots+31 &= 496.\end{aligned}$$

También podemos escribir cualquier número perfecto par, mayor a 6, como la suma de cubos de números impares, para ello veamos el Corolario del siguiente Teorema.

Teorema 2.4. *Si* $n = 2^{m-1}(2^m - 1)$*, entonces*

$$n = 1^3 + 3^3 + \cdots + \left(2^{\frac{(m+1)}{2}} - 1\right)^3.$$

Demostración. Sea $k = 2^{\frac{(m-1)}{2}}$. Notemos que $2^{\frac{m+1}{2}} = 2k$, ahora consideremos la siguiente suma

$$\begin{aligned} 1^3 + 2^3 + 3^3 + \cdots + (2k-1)^3 + (2k)^3 &= (1 + 2 + 3 + \cdots + (2k-1) + (2k))^2 \\ &= \left(\frac{1}{2}(2k)(2k+1)\right)^2 \\ &= k^2(2k+1)^2. \end{aligned}$$

Lo cual implica que $1^3 + 2^3 + 3^3 + \cdots + (2k-1)^3$

$$\begin{aligned} &= k^2(2k+1)^2 - (2^3 + 4^3 + \cdots + (2k)^3) \\ &= k^2(2k+1)^2 - 2^3(1^3 + 2^3 + \cdots + k^3) \\ &= k^2(2k+1)^2 - 8(1 + 2 + \cdots + k)^2 \\ &= k^2(2k+1)^2 - 8(\frac{1}{2}k(k+1))^2 \\ &= k^2(2k+1)^2 - 2k^2(k+1)^2 \\ &= k^2(2k^2 - 1). \end{aligned}$$

Sustituyendo $k = 2^{\frac{(m-1)}{2}}$ obtenemos

$$1^3 + 3^3 + \cdots + \left(2^{\frac{(m+1)}{2}} - 1\right)^3 = 2^{m-1}(2^m - 1) = n.$$

$\square$

De esta manera tenemos el siguiente resultado

Corolario 2.1. *Si* $N = 2^{p-1}(2^p - 1)$ *es un número perfecto par, mayor a 6, entonces*

$$N = 1^3 + 3^3 + \cdots + \left(2^{\frac{(p+1)}{2}} - 1\right)^3.$$

Veamos algunos ejemplos:

- $28 = 1^3 + 3^3$, $p = 3$
- $496 = 1^3 + 3^3 + 5^3 + 7^3$, $p = 5$

Teorema 2.5. *Todos los números perfectos pares terminan en* 6 *o en* 8*.*

Demostración. Todos los números perfectos pares tienen la forma $N = 2^{n-1}(2^n - 1)$, donde $2^n - 1$ es un primo de Mersenne. Si $n = 2$, entonces el resultado claramente se verifica. Por lo tanto supongamos que $n \geq 3$. Como n es primo, entonces n es de la forma $4m + 1$ o $4m + 3$. En el primer caso tenemos que

$$\begin{aligned} N = 2^{n-1}(2^n - 1) &= 2^{4m}(2^{4m+1} - 1) \\ &= 16^m(2 \cdot 16^m - 1) \equiv 6^m(2 \cdot 6^m - 1) \equiv 6(12 - 1) \equiv 6 \pmod{10}, \end{aligned}$$

donde hemos usado el hecho de que $6^m \equiv 6 \pmod{10}$, el cual puede ser probado usando inducción sobre m. Análogamente, en el segundo caso tenemos

$$\begin{aligned} N = 2^{n-1}(2^n - 1) &= 2^{4m+2}(2^{4m+3} - 1) \\ &= 4 \cdot 16^m(8 \cdot 16^m - 1) \equiv 4 \cdot 6(8 \cdot 6 - 1) \equiv 4(8 - 1) \equiv 8 \pmod{10}. \end{aligned}$$

Por lo tanto todos los números perfectos pares terminan en 6 o en 8. □

Capítulo 3

Índice de abundancia

En este capítulo se define el concepto de índice de abundancia o radio de abundancia de un número n, el cual nos indica el cociente entre $\sigma(n)$ y n, esto es de gran interés debido a que si n es un número perfecto, el indice abundancia de n es igual a dos.

Definición 3.1. *El índice de abundancia o radio de abundancia de un entero positivo n se define por*

$$I(n) = \frac{\sigma(n)}{n}.$$

Veamos algunos ejemplos:

- $I(36) = \frac{\sigma(36)}{36} = \frac{91}{36}$.
- $I(1034) = \frac{\sigma(1024)}{1024} = \frac{2047}{2047}$.
- $I(2145) = \frac{\sigma(2145)}{2145} = \frac{4032}{2145}$.

Debido a que la función sigma es una función multiplicativa, entonces el índice de abundancia también lo es. Note que un número es perfecto si y solo si su índice de abundancia es igual a 2, esto es, si $I(n) = 2$.

Cuando $I(n)$ es un entero $r > 2$, se dice que n es un número *multiperfecto de índice r*. Por ejemplo, 120 es un número multiperfecto de índice 3, ya que $I(n) = 3$. El estudio de números multiperfectos fue tratado inicialmente por Descartes y Fermat en el siglo XVII, y se desarrollo alrededor del año 1900. Una bibliografía detallada se puede encontrar en [7].

Definición 3.2. *Sea $n \in \mathbb{Z}^+$, si el índice de abundancia $I(n)$ es menor que 2, entonces decimos que n es deficiente, mientras que sí $I(n)$ es mayor que 2 decimos que n es abundante.*

Veamos algunos ejemplos:

- $I(36) = \dfrac{91}{36} > 2$, luego $n = 36$ es un número abundante.
- $I(1034) = \dfrac{\sigma(1024)}{1024} = \dfrac{2047}{2047} < 2$, luego $n = 1034$ es un número deficiente.

Mostremos algunos lemas importantes que describen algunas propiedades del índice de abundancia. Una de ellas es que el índice de abundancia nos indica la suma de los inversos de los divisores de n.

Lema 3.1. *Para todo $n \geq 1$ tenemos que*

$$\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d}.$$

Demostración. Observemos que si d recorre los divisores de n, entonces n/d también. Por lo tanto

$$\frac{\sigma(n)}{n} = \frac{1}{n}\sum_{d|n} d = \frac{1}{n}\sum_{d|n} \frac{n}{d} = \sum_{d|n} \frac{1}{d}.$$

□

Lema 3.2. *Sean $m, n \in \mathbb{Z}^+$, si $m \mid n$, entonces $\dfrac{\sigma(m)}{m} \leqslant \dfrac{\sigma(n)}{n}$. La igualdad se obtiene cuando $m = n$.*

Demostración. Por el Lema 3.1, tenemos que

$$\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d} \quad \text{y} \quad \frac{\sigma(m)}{m} = \sum_{d^*|m} \frac{1}{d^*}.$$

Como $m \mid n$, entonces

$$\sum_{d|n} \frac{1}{d} \geq \sum_{d^*|m} \frac{1}{d^*},$$

esto es

$$\frac{\sigma(n)}{n} \geq \frac{\sigma(m)}{m}.$$

$\square$

Lema 3.3. *El índice de abundancia toma valores arbitrariamente grandes.*

Demostración. Sea $n \in \mathbb{Z}^+$ y consideremos el número $n!$. Por Lema 3.1, tenemos que

$$\frac{\sigma(n!)}{n!} = \sum_{d|n!} \frac{1}{d} \geqslant \sum_{i=1}^{n} \frac{1}{i}.$$

La última cantidad es una suma parcial de una serie armónica que diverge hacia el infinito, luego la fracción $\frac{\sigma(n!)}{n!}$ se puede hacer tan grande como queramos. $\square$

Lema 3.4. *Para cualquier potencia prima p^α, las siguientes desigualdades se cumplen*

$$1 < \frac{p+1}{p} \leq \frac{\sigma(p^\alpha)}{p^\alpha} < \frac{p}{p-1}.$$

Donde p es un número primo y $\alpha \geq 1$

Demostración. Primero que todo, $\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^{\alpha-1} + p^\alpha = \dfrac{p^{\alpha+1}-1}{p-1}$.
Note que la primera desigualdad se cumple para cualquier primo p.

Para mostrar que $\frac{p+1}{p} \leq \frac{\sigma(p^\alpha)}{p^\alpha}$, observemos que

$$p^\alpha + p^{\alpha-1} < 1 + p + p^2 + \cdots + p^{\alpha-1} + p^\alpha,$$

de donde

$$p^\alpha + p^{\alpha-1} < \sigma(p^\alpha).$$

Por lo tanto

$$p^\alpha \left(1 + \frac{1}{p}\right) < \sigma(p^\alpha),$$

y así

$$1 + \frac{1}{p} < \frac{\sigma(p^\alpha)}{p^\alpha},$$

esto es,

$$\frac{p+1}{p} < \frac{\sigma(p^\alpha)}{p^\alpha}.$$

Por otro lado

$$p - \frac{1}{p^\alpha} < p,$$

luego

$$\frac{p^{\alpha+1}-1}{p^\alpha}\left(\frac{1}{p-1}\right) < p\left(\frac{1}{p-1}\right).$$

Como $\sigma(p^k) = \dfrac{p^{k+1}-1}{p-1}$, se concluye que

$$\frac{\sigma(p^\alpha)}{p^\alpha} < \frac{p}{p-1}.$$

$\square$

Como el índice de abundancia de un número entero positivo es un número racional. En los próximos resultados se resumen gran parte de lo que se conoce acerca de la distribución de estos racionales [5].

Teorema 3.1. *Sean* $k, m \in \mathbb{Z}^+$. *Si* $\operatorname{mcd}(k,m) = 1$ *y* $m < k < \sigma(m)$, *entonces* $\dfrac{k}{m}$ *no puede ser el número de abundancia de ningún número entero.*

Demostración. Supongamos que $I(n) = k/m$, para algún entero $n \geq 1$. Entonces $kn = m\sigma(n)$, lo que significa que $m \mid kn$ y así $m \mid n$ ya que $\operatorname{mcd}(k,m) = 1$. Se sigue del Lema 3.2 que,

$$\frac{\sigma(m)}{m} \leqslant \frac{\sigma(n)}{n} = \frac{k}{m},$$

por lo tanto, $\sigma(m) \leq k$, lo cual es una contradicción ya que $k < \sigma(m)$ por hipótesis. $\square$

Corolario 3.1. *Sea* $m > 1$. *El racional* $(m+1)/m$ *es un índice de abundancia de un entero positivo, si y solo si,* m *es un número primo.*

Demostración. Si $m > 1$ es primo, entonces $I(m) = (m+1)/m$. Recíprocamente, si m fuese un número compuesto, entonces $m < m+1 < \sigma(m)$. Luego, por el Teorema 3.1, tenemos que $(m+1)/m$ no es un índice de abundancia de ningún número entero positivo. $\square$

Corolario 3.2. *Si* m *es primo, entonces* $(m+1)/m$ *es el índice de abundancia únicamente de* m.

Demostración. Sea p un número primo positivo tal que

$$I(p) = \frac{\sigma(p)}{p} = \frac{p+1}{p} = \frac{m+1}{m}.$$

Entonces $m(p+1) = p(m+1)$, y como $m \nmid m+1$ se deduce que $m \mid p$. En consecuencia $p = m$. $\square$

Definición 3.3. *Un número racional mayor que* 1 *se dice que es una abundancia prohibida si no se encuentra dentro del rango de la función* $I(n)$.

Lema 3.5. *Sea* $m \geq 1$ *un entero y* p *un primo tal que* $p > 2m$. *Entonces en cualquier conjunto de* $2m$ *enteros consecutivos hay al menos un entero primo relativo con* pm.

Demostración. Sea S cualquier conjunto de $2m$ enteros consecutivos. Si $p > 2m$ entonces hay como máximo un múltiplo de p en S, pero S contiene al menos dos enteros primos relativos con m, uno de los cuales es primo relativo con p y, por lo tanto también a pm. $\square$

Teorema 3.2. *El conjunto de abundancias prohibidas es denso en el intervalo* $(1, \infty)$.

Demostración. Sean $x \geq 1$ y $\epsilon > 0$ dos números reales. La idea de la prueba es mostrar un racional en el intervalo $(x - \epsilon, x + \epsilon)$ que no es un índice de abundancia (es una abundancia prohibida).

Como conjunto de índices de abundancia $I(n)$, $n > 1$, es denso en el intervalo $(1, \infty)$[15]. Entonces existe $m > 1$, tal que el índice de abundancia $I(m) = \dfrac{\sigma(m)}{m}$ pertenece al intervalo $(x - \frac{\epsilon}{2}, x + \frac{\epsilon}{2})$. Para cada primo $p > 2m$, tenemos que

$$x - \frac{\epsilon}{2} < \frac{\sigma(m)}{m} < \frac{\sigma(pm)}{pm} = \left(1 + \frac{1}{p}\right)\frac{\sigma(m)}{m} < \left(1 + \frac{1}{p}\right)\left(x + \frac{\epsilon}{2}\right).$$

Si además escogemos $p > \dfrac{2x+\epsilon}{\epsilon}$, entonces $\left(1 + \dfrac{1}{p}\right)\left(x + \dfrac{\epsilon}{2}\right) < x + \epsilon$. Así,

$$x - \frac{\epsilon}{2} < \frac{\sigma(pm)}{pm} < x + \epsilon.$$

Aplicando el Lema 3.5, $\sigma(pm) - k$ es primo relativo con pm para algún k, con $1 \leq k \leq 2m$. Para este mismo k, tenemos

$$\sigma(pm) - k \geq \sigma(pm) - 2m \geq (p+1)(m+1) - 2m > pm,$$

pues $p > 2m$. Por lo tanto, por el Teorema 3.1,

$$\frac{\sigma(pm) - k}{pm}$$

no puede ser el índice de abundancia de ningún número entero positivo. Por lo tanto tenemos

$$\frac{\sigma(pm) - k}{pm} \geq \frac{\sigma(pm) - 2m}{pm} = \frac{\sigma(pm)}{pm} - \frac{2}{p} > x - \frac{\epsilon}{2} - \frac{2}{p}.$$

Si $p \geq \frac{4}{\epsilon}$, tenemos que $x - \frac{\epsilon}{2} - \frac{2}{p} \geq x - \epsilon$. En este caso

$$\frac{\sigma(pm) - k}{pm} > x - \epsilon.$$

En consecuencia, todas las desigualdades anteriores se satisfacen si elegimos

$$p > \text{máx}\left\{2m, \frac{2x + \epsilon}{\epsilon}, \frac{4}{\epsilon}\right\}.$$

En conclusión

$$x - \epsilon < \frac{\sigma(pm) - k}{pm} < \frac{\sigma(pm)}{pm} < x + \epsilon.$$

Esto proporciona un racional $\frac{\sigma(pm) - k}{pm}$ el cual es una abundancia prohibida.

$\square$

Capítulo 4

Números perfectos impares

El índice de abundancia nos ayuda a encontrar algunas características que debiera tener un número perfecto impar en caso de que exista. En este capitulo damos a conocer una alguna de ellas. No sabemos si en realidad los números perfectos impares existan, pero a través de los años se han estudiado las propiedades de estos en caso de que existieran. Veamos algunas de ellas.

Teorema 4.1. *Si n un entero positivo tal que $\sigma(n)$ y n son a la vez impares, entonces n debe ser un cuadrado*

Demostración. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ la descomposición en factores primos de n. Como n es impar entonces $p_i^{\alpha_i}$ es impar para $1 \leqslant i \leq k$. Además como $\sigma(n)$ es impar y

$$\sigma(n) = \sigma(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2}) \dots \sigma(p_k^{\alpha_k}),$$

entonces cada $\sigma(p_i^{\alpha_i})$ es impar, $1 \leqslant i \leq k$. Puesto que $\sigma(p_i^{\alpha_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}$, entonces $p_i + p_i^2 + \cdots + p_i^{\alpha_i}$ es un número par, así α_i es un número par para $1 \leqslant i \leq k$. $\square$

Teorema 4.2. *Si $I(n) = \dfrac{5}{3}$ para algún entero positivo n, entonces $5n$ es un número perfecto impar.*

Demostración. Sea n un entero positivo. Como $3\sigma(n) = 5n$, entonces $3 \mid n$. Sí n fuese par, entonces tendríamos que $6 \mid n$ y aplicando el Lema 3.2 tenemos

$$\frac{\sigma(n)}{n} \geq \frac{\sigma(6)}{6} = 2,$$

lo cual es una contradicción pues $I(n) = \dfrac{5}{3}$. Así n es impar, de donde $5n$ también es impar. Por tanto $\sigma(n)$ es impar ya que $3\sigma(n) = 5n$. Puesto que la función $\sigma(n)$ es multiplicativa, si $\sigma(n)$ y n son a la vez impares, entonces n debe de ser un cuadrado, por lo tanto $3^2 \mid n$. Ahora bien, si 5 divide a n, entonces $3^2 \cdot 5 \mid n$. Nuevamente aplicando el Lema 3.2, tenemos que

$$I(n) = \frac{\sigma(n)}{n} \geq \frac{\sigma(3^2 \cdot 5)}{3^2 \cdot 5} = \frac{26}{15} > \frac{5}{3}.$$

Contradiciendo el hecho de que $I(n) = \dfrac{5}{3}$, por lo tanto $\operatorname{mcd}(5, n) = 1$, así

$$\frac{\sigma(5n)}{5n} = \frac{\sigma(5)\sigma(n)}{5n} = \frac{6}{5} \cdot \frac{5}{3} = 2,$$

lo que significa que $5n$ es un número perfecto impar. $\square$

Observemos que si N es un número perfecto con factorización canónica $N = \prod_{i=1}^{w(N)} P_i^{\alpha_i}$, donde $w(N)$ es el número de primos distintos que dividen a N, entonces aplicando la función σ a la igualdad anterior obtenemos

$$\sigma(N) = \sigma\left(\prod_{i=1}^{w(N)} P_i^{\alpha_i}\right).$$

Como N es un número perfecto y σ es una función multiplicativa, entonces

$$2N = \prod_{i=1}^{w(N)} \sigma\left(P_i^{\alpha_i}\right).$$

Aplicando el Lema 3.4, obtenemos

$$2N < \prod_{i=1}^{w(N)} \frac{P_i^{\alpha_i+1}}{P_i - 1} = N \prod_{i=1}^{w(N)} \frac{P_i}{P_i - 1}.$$

Así

$$2 < \prod_{i=1}^{w(N)} \frac{P_i}{P_i - 1}.$$

El resultado anterior lo podemos simplificar como sigue.

Lema 4.1. *Si N es un número perfecto con factorización canónica $N = \prod_{i=1}^{w(N)} P_i^{\alpha_i}$, entonces*

$$2 < \prod_{i=1}^{w(N)} \frac{P_i}{P_i - 1} = \prod_{i=1}^{w(N)} \left(1 + \frac{1}{P_i - 1}\right).$$

Lema 4.2. *Si N es un número perfecto con factorización canónica $N = \prod_{i=1}^{w(N)} P_i^{\alpha_i}$, entonces*

$$2 \geq \prod_{i=1}^{w(N)} \left(1 + \frac{1}{P_i} + \cdots + \frac{1}{P_i^{\beta_i}}\right),$$

donde $0 \leq \beta_i \leq \alpha_i$, $\forall i$.

Demostración. Sea N un número perfecto con factorización canónica $N = \prod_{i=1}^{w(N)} P_i^{\alpha_i}$. Debido a que la función índice de abundancia es multiplicativa, ademas por ser N un número perfecto, se cumple que

$$\begin{aligned}
2 = I(N) &= I(\prod_{i=1}^{w(N)} P_i^{\alpha_i}) \\
&= \prod_{i=1}^{w(N)} I(P_i^{\alpha_i}) \\
&= \prod_{i=1}^{w(N)} \frac{\sigma(P_i^{\alpha_i})}{P_i^{\alpha_i}} \\
&= \prod_{i=1}^{w(N)} \left(1 + \frac{1}{P_i} + \cdots + \frac{1}{P_i^{\alpha_i}}\right) \\
&\geq \prod_{i=1}^{w(N)} \left(1 + \frac{1}{P_i} + \cdots + \frac{1}{P_i^{\beta_i}}\right), 0 \leq \beta_i \leq \alpha_i, \forall i.
\end{aligned}$$

Así

$$2 \geq \prod_{i=1}^{w(N)} \left(1 + \frac{1}{P_i} + \cdots + \frac{1}{P_i^{\beta_i}}\right),$$

donde $0 \leq \beta_i \leq \alpha_i$, $\forall i$. □

4.1. Número de factores primos distintos de un número perfecto impar

Al considerar que características deben de tener los números perfectos impares en caso de que existan, los Lemas 4.1 y 4.2 proporcionan límites inferiores para $w(N)$. De hecho, usando estos lemas se obtienen mayores límites inferiores para el número de distintos factores primos de un número perfecto impar. A continuación probaremos que un número perfecto impar debe tener al menos tres factores primos distintos.

Teorema 4.3. *Si N es un número perfecto impar, entonces $w(N) \geq 3$.*

Demostración. Sea N un número perfecto impar. Como las potencias primas son deficientes, $w(N) \geqslant 2$. Supongamos que $w(N) = 2$. Puesto que N es impar tenemos que $P_1 \geqslant 3$ y $P_2 \geqslant 5$ donde $N = P_1^{\alpha_1} P_2^{\alpha_2}$ es la factorización canónica de N. Usando el Lema 4.1 tenemos que

$$\begin{aligned} 2 < \prod_{i=1}^{w(N)} \frac{P_i}{P_i - 1} = \prod_{i=1}^{2} \frac{P_i}{P_i - 1} &= \left(\frac{P_1}{P_1 - 1}\right)\left(\frac{P_2}{P_2 - 1}\right) \\ &= \left(\frac{1}{1 - \dfrac{1}{P_1}}\right)\left(\frac{1}{1 - \dfrac{1}{P_2}}\right) \\ &\leqslant \left(\frac{1}{1 - \dfrac{1}{3}}\right)\left(\frac{1}{1 - \dfrac{1}{5}}\right) \\ &= 1{,}875 < 2. \end{aligned}$$

Así, $2 < 2$ lo cual es una contradicción. En consecuencia, $w(N) \geq 3$.

□

Teorema 4.4. *Si N es un número perfecto impar, entonces $w(N) \geq 4$.*

Demostración. Sea N un número perfecto impar. Del teorema anterior se sigue que $w(N) \geq 3$. Supongamos que $w(N) = 3$. Ya que N es impar, $P_1 \geqslant 3$, $P_2 \geqslant 5$ y $P_3 \geqslant 7$ donde $N = P_1^{\alpha_1} P_2^{\alpha_2} P_3^{\alpha_3}$ es la factorización canónica de N. Del Lema 4.1 tenemos que:

$$
\begin{aligned}
2 < \prod_{i=1}^{w(N)} \frac{P_i}{P_i - 1} = \prod_{i=1}^{3} \frac{P_i}{P_i - 1} &= \left(\frac{P_1}{P_1 - 1}\right)\left(\frac{P_2}{P_2 - 1}\right)\left(\frac{P_3}{P_3 - 1}\right) \\
&= \left(\frac{1}{1 - \frac{1}{P_1}}\right)\left(\frac{1}{1 - \frac{1}{P_2}}\right)\left(\frac{1}{1 - \frac{1}{P_3}}\right) \\
&\leqslant \left(\frac{1}{1 - \frac{1}{3}}\right)\left(\frac{1}{1 - \frac{1}{5}}\right)\left(\frac{1}{1 - \frac{1}{7}}\right) \\
&= \frac{35}{16} = 2{,}1875,
\end{aligned}
$$

lo cual no es una contradicción. Ahora bien, supongamos que $P_1 \geqslant 5$, $P_2 \geqslant 7$ y $P_3 \geqslant 11$. Usando nuevamente el Lema 4.1 obtenemos que $2 < \left(\frac{5}{4}\right)\left(\frac{7}{6}\right)\left(\frac{11}{10}\right) = \frac{77}{48}$, obteniendo una contradicción. En consecuencia $P_1 = 3$. Si asumimos que $P_2 \geq 7$ llegamos a que

$$
2 < \left(\frac{3}{2}\right)\left(\frac{7}{6}\right)\left(\frac{11}{10}\right) = \frac{77}{40},
$$

lo cual es una contradicción. Por lo tanto se debe de tener que $P_2 = 5$, y así $P_3 \geqslant 7$. Nuevamente aplicando el Lema 4.1 y no asignando un valor primo para P_3 obtenemos que

$$
2 < \left(\frac{3}{2}\right)\left(\frac{5}{4}\right)\frac{P_3}{P_3 - 1} \Longleftrightarrow \frac{16}{15} < \frac{P_3}{P_3 - 1}.
$$

Resolviendo la anterior desigualdad obtenemos que $P_3 < 16$. Puesto que P_3 es primo se debe de dar uno de los siguientes 3 casos:

Caso 1. $\mathbf{N = 3^{\alpha_1} 5^{\alpha_2} 7^{\alpha_3}}$

Como N es impar, entonces 4 no divide a $\sigma(N) = \sigma(3^{\alpha_1})\sigma(5^{\alpha_2})\sigma(7^{\alpha_3}) = 2N = 2 \cdot 3^{\alpha_1} 5^{\alpha_2} 7^{\alpha_3}$. En particular, $4 \nmid \sigma(3^{\alpha_1})$ y $4 \nmid \sigma(7^{\alpha_3})$. Pero $\sigma(3^{\alpha_1}) = 4$ para $\alpha_1 = 1$ y $\sigma(7^{\alpha_3}) = 8$ para $\alpha_3 = 1$. Así, $\alpha_1 \geq 2$ y $\alpha_3 \geq 2$. Usando el Lema 4.2 con $\beta_1 = 2$, $\beta_2 = 1$ y $\beta_3 = 2$ tenemos que:

$$
2 \geq \left(1 + \frac{1}{3} + \frac{1}{3^2}\right)\left(1 + \frac{1}{5}\right)\left(1 + \frac{1}{7} + \frac{1}{7^2}\right) = \frac{494}{245},
$$

lo cual no es posible. Luego no hay un número perfecto impar de la forma $N = 3^{\alpha_1} 5^{\alpha_2} 7^{\alpha_3}$.

Caso 2. $\mathbf{N = 3^{\alpha_1} 5^{\alpha_2} 11^{\alpha_3}}$

1. *Usando el Lema 4.1 con* $\alpha_2 = 1$ *tenemos* $2 < \left(\frac{3}{2}\right)\left(\frac{\sigma(5^{\alpha_2})}{5^{\alpha_2}}\right)\left(\frac{11}{10}\right) = \frac{99}{50}$*, lo cual es una contradicción.*

2. *Sea* $\alpha_2 \geq 2$*. Para* $\alpha_1 = 1, 2, 3$*, tenemos que* $\sigma(3^{\alpha_1}) = 4, 13, 40$*. Puesto que* $4 \nmid \sigma(N)$*,* $\alpha_1 \neq 1$ *y* $\alpha_1 \neq 3$*. También,* $13 \nmid \sigma(N) = 2(N) = 2 \cdot 3^{\alpha_1}5^{\alpha_2}11^{\alpha_3}$ *y por lo tanto,* $13 \nmid \sigma(3^{\alpha_1})$*. Así* $\alpha_1 \neq 2$*, lo cual implica que* $\alpha_1 \geq 4$*. De igual manera,* $\sigma(11^{\alpha_3}) = 12$ *para* $\alpha_3 = 1$*, lo que contradice el hecho de que* $4 \nmid \sigma(11^{\alpha_3})$*. Así,* $\alpha_3 \geq 2$*. Usando ahora el Lema 4.2 con* $\beta_1 = 4$*,* $\beta_2 = 2$ *y* $\beta_3 = 2$ *resulta que:*

$$2 \geq \left(1 + \frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + \frac{1}{3^4}\right)\left(1 + \frac{1}{5} + \frac{1}{5^2}\right)\left(1 + \frac{1}{11} + \frac{1}{11^2}\right) = \frac{4123}{2005},$$

lo cual es una contradicción. Por lo tanto no hay un número perfecto impar de la forma $N = 3^{\alpha_1}5^{\alpha_2}11^{\alpha_3}$*.*

Caso 3. $\mathbf{N = 3^{\alpha_1}5^{\alpha_2}13^{\alpha_3}}$

1. *Usando el Lema 4.1 con* $\alpha_2 = 1$ *tenemos* $2 < \frac{3}{2}\frac{\sigma(5^{\alpha_2})}{5^{\alpha_2}}\frac{13}{12} = \frac{3}{2}\frac{6}{5}\frac{13}{12} = \frac{39}{20}$*, lo cual es una contradicción.*

2. *Sea* $\alpha_2 \geq 2$*. De manera similar a lo que obtuvimos en el Caso 2.2, tenemos* $\alpha_1 \neq 1, 3$*.*

   - $\alpha_1 = 2$*. Del Lema 4.1, tenemos que*

     $$2 < \frac{\sigma(3^{\alpha_1})}{3^{\alpha_1}}\frac{5}{4}\frac{13}{12} = \frac{13}{9}\frac{5}{4}\frac{13}{12} = \frac{845}{432},$$

     lo cual no es posible.

   - $\alpha_1 \geq 4$*. Suponiendo* $\alpha_3 = 1$ *se sigue que* $\sigma(13^{\alpha_3}) = 14 = 2 \cdot 7$*. Luego,*

     $$7 \mid \sigma(13^{\alpha_3}) \mid \sigma(N) = 2N = 2 \cdot 3^{\alpha_1}5^{\alpha_2}13^{\alpha_3},$$

     lo cual es contradictorio. En consecuencia, $\alpha_3 \geq 2$*.*

     Nuevamente usando el Lema 4.2 con $\beta_1 = 4$*,* $\beta_2 = 2$ *y* $\beta_3 = 2$ *tenemos que:*

     $$2 \geq \left(1 + \frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + \frac{1}{3^4}\right)\left(1 + \frac{1}{5} + \frac{1}{5^2}\right)\left(1 + \frac{1}{13} + \frac{1}{13^2}\right) = \frac{228811}{114075},$$

     lo cual es absurdo. Por lo tanto no hay un número perfecto impar de la forma $N = 3^{\alpha_1}5^{\alpha_2}13^{\alpha_3}$*.*

$\square$

De esta manera, no hay un número perfecto impar con exactamente tres factores primos distintos. En otras palabras, un número perfecto impar debe tener al menos cuatro factores primos distintos [5].

A continuación presentamos los resultados más recientes de una cota superior para los números perfectos impares por Nielsen [12] y un cota inferior por Brent [2] ,

$$10^{300} < N < 2^{4^{w(N)}}.$$

Así,

$$w(N) > \left(\frac{2 + \log(3) - \log(\log(2))}{\log(4)}\right) > 4{,}9804,$$

lo que implica que $w(N) \geq 5$ ya que $w(N)$ debe de ser un entero.

Hay un proyecto llevado a cabo en *http://www.oddperfect.org/*, organizado por William Lipp, el cual busca mejorar la cota inferior de un número perfecto impar a 10^{500}, incluso 10^{600}. De hecho en el 2006, Nielsen [13] fue capaz de demostrar que $w(N) \geq 9$.

4.2. Caracterización de Euler de un número perfecto impar

Euler también trató de realizar algunos avances en el problema de la existencia de números perfectos impares. Él demostró que cualquier número perfecto impar N debe de tener la forma

$$N = (4m + 1)^{4k+1} b^2,$$

donde $4m + 1$ es primo y $\text{mcd}(4m + 1, b) = 1$.

Teorema 4.5 (Euler)**.** *Sea N un número perfecto impar. Entonces la descomposición en factores primos de N tiene la forma*

$$N = q^{4e+1} p_1^{2a_1} \cdots p_r^{2a_r}, \quad \textit{donde} \quad q \equiv 1 \pmod 4.$$

Demostración. Sea $N = l_1^{e_1} l_2^{e_2} \cdots l_s^{e_s}$ para algunos primos $l_1, l_2, \cdots, l_s$. Ya que N es impar todos los l_k son impares. Como N es un número perfecto impar y σ es multiplicativa se deduce que $\sigma(N) = 2N$ y

$$\sigma(N) = \sigma(l_1^{e_1} l_2^{e_2} \cdots l_s^{e_s}) = \sigma(l_1^{e_1})\sigma(l_2^{e_2}) \cdots \sigma(l_s^{e_s}).$$

Observemos que

$$\sigma(l^e) = 1 + l + l^2 + \cdots + l^e$$

es una suma de $e+1$ números impares. Esta expresión es impar solo si e es un número par. Ya que

$$\sigma(l_1^{e_1} l_2^{e_2} \cdots l_s^{e_s}) = \sigma(l_1^{e_1})\sigma(l_2^{e_2}) \cdots \sigma(l_s^{e_s}) = 2l_1^{e_1} l_2^{e_2} \cdots l_s^{e_s},$$

solamente podemos obtener un factor de 2. Así que los e_i son pares, excepto uno, digamos e_1. De este modo

$$N = l_1^{e_1} p_1^{2a_1} \cdots p_r^{2a_r}.$$

Notemos que $2 \mid \sigma(l_1^{e_1})$, pero $4 \nmid \sigma(l_1^{e_1})$. Ya que l_1 es impar, e_1 es impar. Ahora, reduciendo la relación anterior módulo 4 observamos que

$$l_1 \equiv 1 \pmod{4} \text{ o } l_1 \equiv -1 \pmod{4}.$$

Pero si $l_1 \equiv -1 \pmod{4}$, entonces

$$\sigma(l_1^{e_1}) = 1 + l_1 + l_1^2 + l_1^3 + \cdots + l_1^{e_1-1} + l^{e_1} \equiv 1 + (-1) + 1 + (-1) + \cdots + 1 + (-1) \equiv 0 \pmod{4},$$

lo cual es una contradicción, ya que $4 \nmid \sigma(l_1^{e_1})$. Así $l_1 \equiv 1 \pmod{4}$. Ahora

$$\sigma(l_1^{e_1}) = 1 + l_1 + l_1^2 + l_1^3 + \cdots + l_1^{e_1-1} + l^{e_1} \equiv 1 + 1 + 1 + 1 + \cdots + 1 + 1 \equiv e_1 + 1 \pmod{4},$$

ya que e_1 es impar. De lo anterior

$$e_1 + 1 \equiv 0 \pmod{4} \text{ o } e_1 + 1 \equiv 2 \pmod{4}.$$

Sí $e_1 + 1 \equiv 0 \pmod{4}$, entonces $4 \mid \sigma(l_1^{e_1})$, que es nuevamente una contradicción.

Así

$$e_1 + 1 \equiv 2 \pmod{4} \Leftrightarrow e_1 + 1 = 4e + 2, \text{ es decir } e_1 = 4e + 1.$$

Por lo tanto

$$N = q^{4e+1} p_1^{2a_1} \cdots p_r 2^{a_r}, \text{ donde } q \equiv 1 (\mod 4).$$

□

En el Teorema 4.5, q es llamado el número primo especial de Euler, mientras que q^{4e+1} es llamado el factor de Euler.

Capítulo 5

Inexistencia de números perfectos en algunos casos especiales

En este capítulo presentamos en detalle dos trabajos del Profesor Dr. Florian Luca, en los cuales se demuestra que no existen dos números perfectos consecutivos [11], ni tampoco números perfectos en las sucesiones de Fibonacci y de Lucas [10].

5.1. Inexistencia de números perfectos consecutivos

En esta sección demostraremos que no existen dos números perfectos consecutivos. Para tal efecto, recordemos que en el Teorema 2.3 se prueba que n es un número perfecto par, si y sólo si, n es de la forma $2^{p-1}(2^p-1)$ donde 2^p-1 es primo. De esta manera, para probar que no existen números perfectos consecutivos, es suficiente demostrar que $M = 2^{p-1}(2^p-1)+1$ y $N = 2^{p-1}(2^p-1)-1$ no son perfectos cuando 2^p-1 es primo.

Notemos que si $p = 2$, entonces $M = 2^{2-1}(2^2-1)+1 = 7$, $N = 2^{2-1}(2^2-1)-1 = 5$, y es claro que ni 5 ni 7 son números perfectos.

Si p es un número primo impar tenemos

$$2^{p-1}(2^p-1) \equiv 4^{\frac{(p-1)}{2}}\left(2\cdot 4^{\frac{(p-1)}{2}}-1\right) \equiv 4(2\cdot 4-1) \equiv 4 \pmod{12}, \tag{5.1}$$

ya que cada potencia de 4 es congruente con 4 módulo 12.

De lo anterior deducimos que $M \equiv -1 \pmod 3$ y por lo tanto M no es un cuadrado. Además

$$\sigma(M) = \sum_{d|M,\ d<\sqrt{M}} \left(d + \frac{M}{d} \right).$$

La congruencia

$$d\left(\frac{M}{d}\right) \equiv -1 \pmod 3$$

implica que para cada d divisor de M, la congruencia módulo 3 de d y M/d es $\{1, -1\}$. Luego, $\sigma(M) \equiv 0 \pmod 3$. Por otra parte, $2M \equiv 2(-1) \equiv 1 \pmod 3$, así que

$$\sigma(M) \neq 2M.$$

Esto es, M no es perfecto.

Usando nuevamente (5.1) tenemos que

$$N \equiv -1 \pmod 4,$$

y así N no es un cuadrado. En consecuencia

$$\sigma(N) = \sum_{d|N,\ d<\sqrt{N}} \left(d + \frac{N}{d} \right).$$

Similarmente, la congruencia

$$d\left(\frac{N}{d}\right) \equiv -1 \pmod 4$$

implica que para cada d divisor de N, la congruencia módulo 4 de d y N/d es $\{1, -1\}$. Luego

$$\sigma(N) \equiv 0 \pmod 4.$$

Por otra parte

$$2N \equiv 2(-1) \equiv 2 \pmod 4,$$

y por consiguiente

$$\sigma(N) \neq 2N.$$

Esto es, N no es perfecto.

En las siguientes secciones mostramos que la sucesión de Fibonacci y la sucesión de Lucas no contienen ningún número perfecto.

5.2. Algunas identidades de las Sucesiones de Fibonacci y de Lucas

En las siguientes pruebas utilizamos algunas propiedades de la sucesión de Fibonacci y de Lucas. Algunas pruebas están incluidas en el documento y otras serán referenciadas para el lector interesado.

Denotemos mediante

$$(F_n)_{n\geq 0} \text{ y } (L_n)_{n\geq 0}$$

las sucesiones de Fibonacci y de Lucas, respectivamente.

La sucesión $(F_n)_{n\geq 0}$ está definida por

$$F_0 = 0, \quad F_1 = 1 \quad \text{y} \quad F_{n+2} = F_{n+1} + F_n, \quad \text{para todo } n \geq 0,$$

mientras que la sucesión $(L_n)_{n\geq 0}$ está dada por

$$L_0 = 2, \quad L_1 = 1 \quad \text{y} \quad L_{n+2} = L_{n+1} + L_n, \quad \text{para todo } n \geq 0.$$

Determinar una expresión que permitiera calcular en una cantidad fija de pasos cualquier número de Fibonacci y de Lucas fue un problema que ocupó a algunos matemáticos durante los siglos XVIII y XIX. El descubrimiento de una expresión con estas características se le atribuye a Jacques P. M. Binet. Las expresiones son las siguientes para la sucesión de Fibonacci y Lucas, respectivamente

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}} \quad \text{y} \quad L_n = \alpha^n + \beta^n, \quad \text{para todo} \quad n \geq 0. \tag{5.2}$$

Donde

$$\alpha = \frac{1+\sqrt{5}}{2} \quad \text{y} \quad \beta = \frac{1-\sqrt{5}}{2},$$

son las raíces del polinomio característico

$$x^2 - x - 1 = 0.$$

Miremos ahora algunas identidades que cumplen las sucesiones de Fibonacci y de Lucas, las cuales son bien conocidas.

Lema 5.1. *Sean* $(F_n)_{n\geq 0}$ *la sucesión de Fibonacci y* $(L_n)_{n\geq 0}$ *la sucesión de Lucas. Para todo* $n, m \geq 0$ *se cumple que*

(*a*) $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$.

(*b*) $$2^{n-1}F_n = \begin{cases} \binom{n}{1} + \binom{n}{3}5 + \binom{n}{5}5^2 + \cdots + \binom{n}{n-1}5^{\frac{n-2}{2}}, & \textit{si } n \textit{ es par,} \\ \binom{n}{1} + \binom{n}{3}5 + \binom{n}{5}5^2 + \cdots + \binom{n}{n-1}5^{\frac{n-1}{2}}, & \textit{si } n \textit{ es impar.} \end{cases}$$

(*c*) $F_{2n} = F_nL_n$.

(*d*) $L_n^2 - 5F_n^2 = 4(-1)^n$.

Demostración.

(*a*) Fijemos m y hagamos inducción sobre n. Veamos que la propiedad se cumple para $n = 1$ y $n = 2$.

$$F_{m+1} = F_{m-1} + F_m = F_{m-1}F_1 + F_mF_2,$$

$$F_{m+2} = F_{m+1} + F_m = F_{m-1} + F_m + F_m = F_{m-1}F_2 + F_mF_3.$$

Supongamos ahora que la propiedad se cumple para $1 \leq n \leq k$ y veamos que se cumple para $n = k + 1$. En efecto

$$\begin{aligned} F_{m+(k+1)} &= F_{m+k} + F_{m+(k-1)} \\ &= (F_{m-1}F_k + F_mF_{k+1}) + (F_{m-1}F_{k-1} + F_mF_k) \\ &= F_{m-1}(F_k + F_{k-1}) + F_m(F_k + F_{k+1}) \\ &= F_{m-1}F_{k+1} + F_mF_{k+2}. \end{aligned}$$

(*b*) Según la expresión (5.2), tenemos que

$$\begin{aligned} 2^n\sqrt{5}F_n &= (1+\sqrt{5})^n - (1-\sqrt{5})^n \\ &= \sum_{k=0}^{n} \binom{n}{k} \sqrt{5}^k - \sum_{k=0}^{n} \binom{n}{k} (-\sqrt{5})^k \\ &= \sum_{k=0}^{n} \binom{n}{k} \sqrt{5}^k \left(1 - (-1)^k\right). \end{aligned}$$

Cuando k es un número par, los sumandos de la expresión anterior se anulan. Por lo tanto

$$\begin{aligned} 2^n\sqrt{5}F_n &= 2\binom{n}{1}\sqrt{5} + 2\binom{n}{3}\sqrt{5}^3 + 2\binom{n}{5}\sqrt{5}^5 + \cdots \\ &= 2\sqrt{5}\left(\binom{n}{1} + \binom{n}{3}\sqrt{5}^2 + \binom{n}{5}\sqrt{5}^4 + \cdots\right), \end{aligned}$$

de donde

$$2^{n-1}F_n = \binom{n}{1} + \binom{n}{3}5 + \binom{n}{5}5^2 + \cdots$$

(c) Por la primera parte de la expresión (5.2), tenemos que

$$\begin{aligned} F_{2n} &= \frac{1}{\sqrt{5}}\left(\alpha^{2n} - \beta^{2n}\right) \\ &= \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)(\alpha^n + \beta^n) \\ &= F_nL_n. \end{aligned}$$

(d) Según la expresión (5.2), tenemos que

$$F_n^2 = \frac{1}{5}\left(\alpha^n - \beta^n\right)^2 = \frac{1}{5}\left(\alpha^{2n} + \beta^{2n} - 2\alpha^n\beta^n\right),$$

y

$$L_n^2 = \alpha^{2n} + \beta^{2n} + 2\alpha^n\beta^n.$$

Así

$$\begin{aligned} L_n^2 - 5F_n^2 &= \left(\alpha^{2n} + \beta^{2n} + 2\alpha^n\beta^n\right) - \left(\alpha^{2n} + \beta^{2n} - 2\alpha^n\beta^n\right) \\ &= 4(\alpha\beta)^n = 4(-1)^n. \end{aligned}$$

$\square$

Definición 5.1. *Sean p un primo impar y a un entero tal que* $\operatorname{mcd}(a,p) = 1$. *Si la congruencia cuadrática*

$$x^2 \equiv a \pmod{p}$$

tiene solucion, decimos que a es un residuo cuadrático de p. De no tener solución decimos que a no es un residuo cuadrático de p.

Definición 5.2. *Sea p un primo impar y a un entero tal que* $\operatorname{mcd}(a,p)=1$*. El símbolo de Legendre de a con respecto a p, denotado por* $\left(\dfrac{a}{p}\right)$*, se define por*

$$\left(\frac{a}{p}\right)=\begin{cases} 1, & \textit{si } a \textit{ es un residuo cuadrático de } p, \\ -1, & \textit{si } a \textit{ no es un residuo cuadrático de } p. \end{cases}$$

El símbolo de Legendre tiene propiedades importantes. Entre ellas se destaca que es completamente multiplicativo, es decir, para a y b enteros, con $\operatorname{mcd}(p,a)=1$ y $\operatorname{mcd}(p,b)=1$, se cumple que

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Este hecho lo usaremos más adelante. Mostremos algunos resultados que asocian la sucesión de Fibonacci y el Símbolo de Legendre.

Lema 5.2. *Sea $p>5$ un número primo.*

(*a*) *Si* $\left(\dfrac{5}{p}\right)=1$*, entonces* $p\mid F_{p-1}$*.*

(*b*) *Si* $\left(\dfrac{5}{p}\right)=-1$*, entonces* $p\mid F_{p+1}$*.*

(*c*) $F_{p-\left(\frac{5}{p}\right)}\equiv 0 \pmod{p}$.

Demostración.

(*a*) Como 5 es un residuo cuadrático de p, entonces por el criterio de Euler [1]

$$5^{\frac{p-1}{2}}\equiv 1 \pmod{p}.$$

Por el Lema 5.1 (b), tenemos que

$$2^{p-2}F_{p-1}=\binom{p-1}{1}+\binom{p-1}{3}5+\binom{p-1}{5}5^2+\cdots+\binom{p-1}{p-2}5^{\frac{p-3}{2}}.$$

Como

$$\tbinom{p-1}{k}\equiv -1 \pmod{p}, \text{ y como } k \text{ es un numero impar,}$$

[1](Criterio de Euler) $a^{(p-1)/2}\equiv\left(\dfrac{a}{p}\right) \pmod{p}$.

entonces

$$2^{p-2}F_{p-1} \equiv -\left(1+5+5^2+\cdots+5^{\frac{p-3}{2}}\right) \pmod{p}$$
$$\equiv -\left(\frac{5^{\frac{p-1}{2}}-1}{5-1}\right) \equiv 0 \pmod{p}.$$

Es decir $p \mid F_{p-1}$.

(b) Como 5 no es un residuo cuadrático de p, entonces por el criterio de Euler

$$5^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Usando el Lema (5.1) (b). Tenemos

$$2^pF_{p+1} = \binom{p+1}{1} + \binom{p+1}{3}5 + \binom{p+1}{5}5^2 + \cdots + \binom{p+1}{p}5^{\frac{p-1}{2}}$$
$$\equiv 1+5^{\frac{p-1}{2}} \pmod{p} \equiv 0 \pmod{p},$$

y así $p \mid F_{p+1}$.

(c) Consecuencia de los literales (a) y (b).

□

Se define el rango de aparición en la sucesión de Fibonacci de la siguiente manera:

Definición 5.3. *Sea $m > 1$. Al menor índice i tal que $F_i \equiv 0 \pmod{m}$ se le llama el rango de aparición de m en la sucesión de Fibonacci y se denota por $r(m)$.*

El rango de aparición siempre existe [6].

Mostremos algunos resultados relacionado al concepto anterior.

Lema 5.3. *Para todos $n, m \geq 1$ se cumple que*

(a) $m \mid F_n$, si y sólo si, $r(m) \mid n$.

(b) Si $p \neq 5$, entonces $\operatorname{mcd}(r(p), p) = 1$.

Demostración.

(*a*) Supongamos que $m \mid F_n$ y que $r(m) \nmid n$. Por el algoritmo de la división existen enteros a y b tales que

$$n = r(m)a + b, \quad \text{con} \quad 0 < b < r(m).$$

Por el Lema 5.1, tenemos que

$$F_n = F_{r(m)a+b} = F_{r(m)a-1}F_b + F_{r(m)a}F_{b+1}.$$

Como $m \mid F_n$ y $m \mid F_{r(m)a}$, entonces $m \mid F_{r(m)a-1}F_b$.

Sin embargo, $\mathrm{mcd}(F_{r(m)a}, F_{r(m)a-1}) = 1$ ya que cualquier par de enteros consecutivos en la sucesión de Fibonacci son primos relativos, así

$$m \mid F_b$$

lo cual es una contradicción pues $b < r(m)$.

Supongamos ahora que $r(m) \mid n$. Entonces existe $t \in \mathbb{Z}^+$ tal que $n = r(m)t$, entonces $m \mid F_{r(m)} \mid F_{r(m)t} = F_n$.

(*b*) Por el Lema 5.2 (*c*) y el literal (*a*), tenemos que

$$r(p) \mid p - \left(\frac{5}{p}\right).$$

Así $r(p) \mid p \pm 1$ y de esta manera

$$r(p) = p + 1 \quad \text{o} \quad r(p) \leq p - 1 < p.$$

En cualquier caso $\mathrm{mcd}(r(p), p) = 1$.

□

Otras propiedades importantes de la sucesión de Fibonacci y de Lucas son las siguientes:

Lema 5.4. *Para todo $n, m \geq 0$ se cumple que*

(*a*) $\mathrm{mcd}(F_n, F_m) = F_{\mathrm{mcd}(n,m)}$.

(*b*) *Si $m \geq 3$, entonces $F_m \mid F_n$, si y sólo si, $m \mid n$.*

(c) *Sea $m > 2$. Si n/m es impar, entonces $L_m \mid L_n$.*

(d) *Sean $m, n \in \mathbb{Z}^+$ tal que n/m es impar. Si p es un primo tal que $p \mid \operatorname{mcd}(L_m, \dfrac{L_n}{L_m})$, entonces $p \mid n/m$.*

Demostración.

(a) Para mostrar que $\operatorname{mcd}(F_n, F_m) = F_{\operatorname{mcd}(n,m)}$ usamos la siguiente identidad que se cumple en la sucesion de Fibonacci

$$F_{kn+r} = \sum_{h=0}^{k} \binom{k}{h} F_n^h F_{n-1}^{k-h} F_{r+h},$$

donde $k \geq 0$ y $\binom{k}{h}$ es el coeficiente binomial de k en h.

Sean $\operatorname{mcd}(m, n) = g$ y $\operatorname{mcd}(F_m, F_n) = G$, luego existen enteros x y y (no ambos negativos) tales que $xm + yn = g$. Supongamos que $x \geq 0$. Entonces

$$F_g = \sum_{h=0}^{x} \binom{x}{h} F_m^h F_{m-1}^{x-h} F_{yn+h} \equiv 0 \pmod{G}$$

ya que $G \mid F_m$ y $G \mid F_n$. Por lo tanto $G \mid F_g$.

Como $\operatorname{mcd}(m, n) = g$, tenemos que $g \mid m$ y $g \mid n$, entonces $F_g \mid F_m$ y $F_g \mid F_n$, esto es $F_g \mid G$.

Por lo anterior concluimos que $G = F_g$.

(b) $F_m \mid F_n \Leftrightarrow \operatorname{mcd}(F_m, F_n) = F_m \Leftrightarrow F_{\operatorname{mcd}(m,n)} = F_m \Leftrightarrow \operatorname{mcd}(m, n) = m \Leftrightarrow m \mid n$.

(c) Si n/m es impar, entonces existe t impar tal que $n = mt$. Ahora bien,

$$\begin{aligned}
\frac{L_n}{L_m} = \frac{\alpha^n + \beta^n}{\alpha^m + \beta^m} &= \frac{(\alpha^m)^t + (\beta^m)^t}{\alpha^m + \beta^m} \\
&= \frac{(\alpha^m + \beta^m)\left(\alpha^{m(t-1)} - \alpha^{m(t-2)}\beta^m + \cdots + \beta^{m(t-1)}\right)}{\alpha^m + \beta^m} \\
&= \alpha^{m(t-1)} - \alpha^{m(t-2)}\beta^m + \cdots + \beta^{m(t-1)}.
\end{aligned}$$

La parte izquierda de la expresión anterior es racional y la parte derecha es un entero algebraico[2] ya que α y β son enteros algebraicos, por ser raíces de $x^2 - x - 1 = 0$. Y como

[2]Un entero algebraico es un número complejo que es la raíz de algún polinomio mónico con coeficientes en $\mathbb{Z}$

los únicos enteros algebraicos que son racionales son los enteros, se deduce que la parte derecha es un entero. Esto es, $L_m \mid L_n$.

(d) Finalmente para probar (d) observamos que $\alpha^m \equiv -\beta^m \pmod{p}$ ya que $p \mid L_m$. Además $m \mid n$ y n/m es impar, entonces $n = ml$ con l impar. De donde

$$\begin{aligned} \frac{L_n}{L_m} = \frac{\alpha^n + \beta^n}{\alpha^m + \beta^m} &= \frac{(\alpha^m)^l + (\beta^m)^l}{\alpha^m + \beta^m} \\ &= \alpha^{m(l-1)} - \alpha^{m(l-2)}\beta^m + \cdots + \beta^{m(l-1)} \\ &\equiv l\alpha^{m(l-1)} \equiv l\beta^{m(l-1)} \equiv 0 \pmod{p}. \end{aligned}$$

En consecuencia, $p^2 \mid l^2(\alpha\beta)^{m(l-1)}$ y así $p \mid l$.

□

5.3. Inexistencia de números perfectos pares en las sucesiones de Fibonacci y Lucas

Supongamos que existe un número perfecto par que pertenece a la sucesión Fibonacci o a la sucesión de Lucas. Recordemos que todo número perfecto par tiene la forma $2^{p-1}(2^p - 1)$ con $2^p - 1$ primo. Así con $p = 2$ o $p = 3$ obtenemos los números perfectos 6 y 28 respectivamente, los cuales no pertenecen ni a la sucesión de Fibonacci ni a la sucesión de Lucas.

Supongamos que $p \geq 5$. Por una parte, la igualdad $L_n = 2^{p-1}(2^p - 1)$ no es posible para estos valores primos de p, debido a que ningún elemento de la sucesión de Lucas es divisible entre 8. Lo anterior se debe a que la sucesión de Lucas es periódica vista módulo un entero positivo m. En particular, si $m = 8$, entonces los primeros números de Lucas módulo 8 son

$$2, 1, 3, 4, 7, 3, 2, 5, 7, 4, 3, 7, 2, 1, 3, 4, 7, 3, 2, 5, 7, 4, 3, 7 \ldots$$

Luego, no existe un número de Lucas que sea divisible por 8, ya que la sucesión de Lucas módulo 8 es periódica, y no aparece el cero. Por lo tanto no aparecerá en ningún momento. Es decir, no existe un número de Lucas que sea divisible por 8.

Por otra parte, $F_n = 2^{p-1}(2^p - 1)$ implica que $16 \mid F_n$, entonces por Lema (5.3)

$$r(16) \mid n,$$

esto es

$$12 \mid n.$$

Así $4 \mid n$, y en consecuencia

$$3 = F_4 \mid F_n = 2^{p-1}(2^p - 1),$$

lo cual no es posible debido a que $p \geq 5$ y $2^p - 1$ es primo.

En conclusión, ni la sucesión de Fibonacci ni la sucesión de Lucas contienen números perfectos pares.

5.4. Inexistencia de números perfectos impares en las sucesiones de Fibonacci y Lucas

Resta demostrar que las sucesiones de Fibonacci y de Lucas tampoco contienen ningún número perfecto impar. No se sabe si existen números perfectos impares. Sin embargo, por el Teorema 4.5 se concluye que si m es un número perfecto impar, entonces éste debe ser de la forma

$$m = p_1 x^2 \tag{5.3}$$

para algún número primo p_1 tal que $p_1 \equiv 1 \pmod{4}$.

Luego si F_n o L_n es un número perfecto impar, entonces es de la forma $p_1 x^2$ para algún primo p_1 tal que $p_1 \equiv 1 \pmod{4}$. Así el resto del trabajo consiste en demostrar que no existen números de Fibonacci ni de Lucas de la forma antes descrita.

5.4.1. Clases de cuadrados de Fibonacci y números de Lucas

En esta sección recordamos algunos resultados sobre los elementos de la sucesión de Fibonacci y Lucas de la forma dx^2 donde d es un entero libre de cuadrados.

El primer resultado lo dio Cohn [4], quien mostró que $F_1 = F_2 = 1$ y $F_{12} = 144$ son los únicos cuadrados en la sucesión de Fibonacci. Veinte años más tarde, Robbins [16] probó el siguiente resultado.

Teorema 5.1. *Supongamos que $F_n = p_1 x^2$ para algún número primo impar p_1 y algún entero $x \neq 0$. Entonces $n \in \{4, 25\}$ o $n = p$ es un número primo.*

Si bien no se encuentra un resultado especifico en los artículos de Robbins respecto a la sucesión de Lucas, podemos utilizar los siguientes resultados generales de Ribenboim [14] relativa a las clases de cuadrados de Fibonacci y números de Lucas.

Teorema 5.2. *Sea $d \geq 1$ un número entero libre de cuadrados.*

1. *Si $F_m = dx^2$ y $F_n = dy^2$, para algunos enteros positivos m, n, x, y, entonces $d = 1$ y $m, n \in \{1, 2, 12\}$ o $d = 2$ y $m, n \in \{3, 6\}$ o $m = n$.*

2. *Si $L_m = dx^2$ y $L_n = dy^2$, para algunos enteros positivos m, n, x, y, entonces $d = 1$ y $m, n \in \{1, 3\}$ o $d = 2$ y $m, n \in \{0, 6\}$ o $m = n$.*

Teniendo en cuenta lo anterior se prueba el siguiente lema.

Lema 5.5. *Si F_n o L_n es un número perfecto impar, entonces n es un número primo.*

Demostración. Supongamos primero que F_n es un número perfecto impar. Por (5.3), tenemos que

$$F_n = p_1 x^2,$$

para algún primo p_1. Por el Teorema 5.1 concluimos que $n \in \{4, 25\}$ o $n = p$ es un número primo. El caso $n \in \{4, 25\}$ no es posible debido a que ninguno de los números F_4 o F_{25} es perfecto. Por lo tanto n es un número primo.

Ahora miremos el caso donde L_n es un número perfecto impar. En este caso

$$L_n = p_1 x^2$$

para algún primo p_1 tal que

$$p_1 \equiv 1 \pmod{4}.$$

En particular,

$$L_n \equiv 1 \pmod{4},$$

ya que x es impar, por ser L_n impar.

Además recordemos que la sucesión de Lucas es periódica módulo un entero positivo m. En particular, los primeros números de Lucas módulo 4 son

$$2, 1, 3, 0, 3, 3, 2, 1, 3, 0, 3, 3, \ldots$$

Como lo mencionamos antes la sucesión se repite. En la lista anterior aparece uno en $L_1, L_7, L_{13}, \ldots$, es decir, $L_n \equiv 1 \pmod 4$ si $n \equiv 1 \pmod 6$. Luego n debe de ser, en particular, un número impar.

Sea p el mayor número primo tal que $p \mid n$. Como n es impar, entonces por el Lema 5.4

$$L_p \mid L_n.$$

Afirmamos que L_p es divisible únicamente por números primos más grandes que p. Esto es,

“ si q es un número primo tal que $q \mid L_p$, entonces $q > p$ ”

En efecto, por los Lemas 5.3 y 5.1, tenemos que

$$q \mid L_p \mid F_{2p},$$

de donde

$$r(q) \mid 2p. \tag{5.4}$$

Primero que todo notemos que $q \neq \{2, 3, 5\}$ ya que

- si $q = 2$, entonces $2 \mid L_p \mid L_n$, lo cual no es posible ya que L_n es impar;
- si $q = 3$, entonces $4 = r(3) \mid 2p$, de donde $p = 2$. Así, $2 \mid n$, lo cual no es posible por ser n impar;
- el caso $q = 5$ no es posible ya que ningún elemento de la sucesión de Lucas es divisible entre 5.

En resumen $q > 5$ y en consecuencia por el Lema 5.2 tenemos que $F_{q\pm 1} \equiv 0 \pmod q$. Es decir $q \mid F_{q\pm 1}$ y así

$$r(q) \mid q \pm 1. \tag{5.5}$$

Si $r(q) = 2$, entonces $q \mid F_2 = 1$, lo cual no es posible. Luego $r(q) \neq 2$. Por (5.4) los posibles valores que puede tomar $r(q)$ son p y $2p$. En cualquiera de los dos casos tenemos que $p \mid q \pm 1$ y en consecuencia $p \leq q - 1$, que es lo que queríamos probar. Notemos que el caso $p = q$ no es posible ya que $p \mid q \pm 1$, y el caso $p = q + 1$ no se puede dar por ser p un número impar.

Afirmamos ahora que

$$\operatorname{mcd}\left(L_p, \frac{L_n}{L_p}\right) = 1. \tag{5.6}$$

En efecto, si $d = \operatorname{mcd}\left(L_p, \frac{L_n}{L_p}\right) > 1$, entonces existe un primo q tal que $q \mid d$. Por el Lema 5.4, $q \mid n/p$. Así que $q \leq p$, lo cual es contradictorio ya que $q \mid L_p$ y todos los divisores primos de L_p son mayores a p.

Es decir, L_p y L_n/L_p son primos entre si. Así

$$L_p.\frac{L_n}{L_p} = p_1 x^2,$$

implica que

$$L_p = x_1^2 \quad \text{o} \quad L_p = p_1 x_1^2, \quad \text{para algún divisor } x_1 \text{ de } x.$$

En el caso $L_p = x_1^2$, concluimos por el Teorema 5.2 que $p = 3$, lo cual es imposible pues $L_3 = 4$ es par.

En el caso $L_p = p_1 x_1^2$, concluimos por el Teorema 5.2, que $n = p$ es un número primo, puesto que $L_n = p_1 x^2$. □

En resumen del Lema 5.5 se concluye que es suficiente demostrar, que no hay ningún número perfecto de la forma F_p o L_p para algún primo impar p.

5.4.2. Una desigualdad que implica la función sigma

En esta sección usamos el siguiente resultado presentado por Florian Luca en [9].

Teorema 5.3. *Si $n \geq 1$ un entero positivo, entonces*

$$\sigma(F_n) \leq F_{\sigma(n)}.$$

Corolario 5.1. *No existen números de Fibonacci perfectos impares.*

Demostración. Si F_n es un número perfecto impar, entonces por lo visto anteriormente n debe de ser un número primo, digamos $n = p$. Por lo tanto $\sigma(p) = p + 1$ y en consecuencia por el Teorema 5.3 se tiene que

$$2 = \frac{\sigma(F_p)}{F_p} \leq \frac{F_{\sigma(p)}}{F_p} = \frac{F_{p+1}}{F_p} < 2,$$

lo cual es una contradicción. Por lo tanto no existen números perfectos impares en la sucesión de Fibonacci. □

En [8] y [9] no se prueba que la desigualdad $\sigma(F_n) \leq F_{\sigma(n)}$ se cumple para la sucesión de Lucas. Sin embargo F. Luca en [10] prueba el siguiente resultado que es apropiado para resolver el problema. Veamos.

Teorema 5.4. *Si p es un número primo, entonces*

$$\sigma(L_p) < 2L_p.$$

Demostración. El teorema es cierto para $p = 2$ y $p = 3$. Supongamos que $p > 3$ es un número primo. Escribamos a L_p de la siguiente forma

$$L_p = \prod_{i=1}^{k} P_i^{\beta_i},$$

donde $P_1 < \cdots < P_k$, son primos. Note que $P_1 \neq 2$.

Observe además que

$$P_1 \mid L_p \mid F_{2p}. \tag{5.7}$$

Teniendo en cuenta que p es impar y usando el Lema 5.1 tenemos que

$$L_p^2 - 5F_p^2 = -4.$$

Reduciendo la relación anterior módulo P_1, obtenemos

$$-5F_p^2 \equiv -4 \pmod{P_1},$$

de donde

$$(5F_p)^2 \equiv 20 \pmod{P_1}.$$

Por lo tanto la congruencia

$$x^2 \equiv 20 \pmod{P_1},$$

tiene solución. De ahí que

$$\left(\frac{20}{P_1}\right) = 1.$$

Como el símbolo de Legendre es multiplicativo, concluimos que

$$1 = \left(\frac{20}{P_1}\right) = \left(\frac{2^2 \cdot 5}{P_1}\right) = \left(\frac{4}{P_1}\right)\left(\frac{5}{P_1}\right) = \left(\frac{5}{P_1}\right),$$

y así por el Lema 5.2 tenemos que

$$P_1 \mid F_{P_1 - 1}.$$

Como $P_1 \mid F_{2p}$, entonces

$$P_1 \mid \operatorname{mcd}(F_{2p}, F_{P_1-1}) = F_{\operatorname{mcd}(2p, P_1-1)}.$$

Observemos que si $\operatorname{mcd}(2p, P_1 - 1) = 2$, entonces por la expresión anterior tendríamos que $P_1 \mid F_2 = 1$, lo cual no es posible. Si $p \mid P_1 - 1$, entonces $2p \mid P_1 - 1$ por ser P_1 impar. por lo tanto $\operatorname{mcd}(2p, P_1 - 1) = 2p$

De está manera $2p \mid (P_1 - 1)$, y en consecuencia

$$P_1 - 1 \geq 2p.$$

Dado que $L_n < 2^n$ para todos los $n \geq 1$, concluimos que

$$2^p > L_p \geq \prod_{i=1}^{k} P_i \geq P_1^k \geq (2p+1)^k.$$

Por lo tanto,

$$k < \frac{p \log 2}{\log(2p+1)}.$$

Por otra parte

$$\frac{\sigma(p^a)}{p^a} < \frac{p^a}{\phi(p^a)}, \quad \text{para todo} \quad a \geq 1,$$

ya que por el Lema 3.4

$$\frac{\sigma(p^a)}{p^a} < \frac{p}{p-1} = \frac{p^a}{p^{a-1}(p-1)} = \frac{p^a}{\phi(p^a)},$$

Además las funciones σ y ϕ tienen la propiedad de que son multiplicativas, se tiene que

$$\begin{aligned}\frac{\sigma(L_p)}{L_p} < \frac{L_p}{\phi(L_p)} = \prod_{i=1}^{k}\left(1+\frac{1}{P_i-1}\right) &\leq \left(1+\frac{1}{P_1-1}\right)^k \\ &< \left(1+\frac{1}{2p}\right)^{\frac{p\log 2}{\log(2p+1)}} \\ &< e^{\frac{\log 2}{2\log(2p+1)}} \\ &< 2^{\frac{1}{2\log(2p+1)}} \\ &< 2.\end{aligned}$$

En el argumento anterior, por ϕ denotamos la función de Phi de Euler como es usual, es decir $\phi(n)$ cuenta el número de primos relativos con n menores que n. Además hemos utilizado el hecho de que

$$\left(1+\frac{1}{x}\right)^x < e, \quad \text{para } x > 1.$$

De esta manera

$$\sigma(L_p) < 2L_p.$$

$\square$

Finalmente, de lo anterior concluimos que no existen números de Lucas perfectos impares. En efecto, si L_p es perfecto para algún primo p, por lo anterior deducimos que

$$2 = \frac{\sigma(L_p)}{L_p} < 2,$$

lo cual es una contradicción.

Capítulo 6

Resultados y problemas

En este último capítulo se exponen los resultados que consideramos más importantes en el estudio de números perfectos, los cuales se trabajaron en detalle en los capítulos anteriores. Además se plantean algunos problemas relacionados con los números perfectos en sucesiones distintas a $(F_n)_{n\geq 0}$ y $(L_n)_{n\geq 0}$.

6.1. Resultados

Los números perfectos pares se pueden escribir de la siguiente forma $2^{p-1}(2^p-1)$ con 2^p-1 primo. Sin embargo, hasta el momento solo se conocen una cantidad finita de ellos, es decir, no se ha logrado probar que existen infinitos números perfectos pares. Los números de la forma $M_p = 2^p - 1$ se les conocen como números de Mersenne. Cuando M_p es un número primo podemos encontrar un número perfecto par, es decir, cada primo de Mersenne tiene asociado un número perfecto par. De esta manera la búsqueda de números perfectos pares la podemos direccionar a encontrar primos de Mersenne. Actualmente se conocen 48 primos de Mersenne, y por lo tanto se han encontrado 48 números perfectos. En este momento hay un proyecto llamado GIMPS (Great Internet Mersenne Prime Search), el cual busca encontrar números primos de Mersenne con la ayuda de las computadores. El más reciente primo de Mersenne fue encontrado en el año 2013, el cual tiene más de 17 millones de cifras, sobrepasando así en casi 5 millones el número de cifras del primo de Mersenne número 47 de la lista.

Hasta el momento no se ha logrado encontrar ningún número perfecto impar. En el Teorema 4.4 mostramos que si un número perfecto impar existe, entonces este debe tener al menos cuatro factores primos distintos. De hecho en el 2006, Nielsen [13] demostró que el número de factores primos distintos de un número perfecto impar es mayor o igual a 9. Euler demostró que si existe un número perfecto impar , entonces debe tener la forma $p^{\alpha}m^2$, donde p es un número primo tal que $\text{mcd}(p, m) = 1$ y $p \equiv \alpha \equiv 1 \pmod{4}$.

El índice de abundancia de un número perfecto es igual a 2. El índice de abundancia tiene la propiedad de que es denso en el intervalo $(1, \infty)$[15]. Los números que no son índice de abundancia, también son densos en el intervalo $(1, \infty)$. El anterior hecho se prueba en el Teorema 3.2 .

Se prueba que un número perfecto par mayor a 6 se puede escribir como la suma de cubos de números impares. También se probó que un número perfecto par es un número triangular. A pesar de que los números perfectos cumplen con ciertas propiedades; en el Capítulo 5, se mostró que no existen dos números perfectos consecutivos y que no existen números perfectos que sean parte de las sucesiones de Fibonacci y de Lucas.

6.2. Algunos problemas

Dado que cada primo de Mersenne tiene asociado un número perfecto, nos encontramos frente al problema de que los números perfectos parecen ser cada vez más escasos, pues el número perfecto asociado al último numero de Mersenne encontrado tiene cerca de 34 millones de cifras.

Es posible establecer 48 números de Mersenne y por lo tanto construir igual cantidad números perfectos pares ¿Cuántos hay en total? ¿Son finitos o infinitos? Además no se conocen hasta el momento algún numero perfecto impar. Por lo anterior vale la pena insistir en los siguientes problemas de alto interés en la comunidad matemática.

- ¿Los números perfectos pares son infinitos?
- ¿Existe algún número perfecto impar?

De otro lado, recordemos que la sucesión de Fibonacci esta dada por

$$F_0 = 0, \quad F_1 = 0, \quad F_{n+2} = F_{n+1} + F_n,$$

para todo $n \geq 0$. La sucesión de Lucas esta dada por

$$L_0 = 2, \quad L_1 = 1, \quad L_{n+2} = L_{n+1} + L_n,$$

para todo $n \geq 0$.

La pregunta que surge es qué pasa si cambiamos las condiciones iniciales ¿Esa nueva sucesión tiene números perfectos? Por ejemplo, consideremos $(S_n)_{n\geq 0}$ una sucesión de la forma

$$S_0 = a, \quad S_1 = b, \quad S_{n+2} = S_{n+1} + S_n,$$

para todo $n \geq 0$, con $a, b, n \in \mathbb{Z}^+$.

¿$(S_n)_{n\geq 0}$, contiene o no números perfectos? ¿Qué condiciones debe de cumplir a y b para que existan o no números perfectos en $(S_n)_{n\geq 0}$?

6.3. Trabajo futuro

Estudiar la existencia o no de números perfectos en las sucesiones de Pell y Pell-Lucas. La sucesión de Pell $(P_n)_{n\geq 0}$ esta dada por la recurrencia

$$P_0 = 0, \quad P_1 = 1, \quad P_n = 2P_{n-1} + P_{n-2}, \quad \text{para } n \geq 2,$$

mientras que la sucesión asociada, llamada sucesión de Pell-Lucas $(Q_n)_{n\geq 0}$, esta definida por la misma relación de recurrencia pero con condiciones iniciales diferentes.

$$Q_0 = 2, \quad Q_1 = 2, \quad Q_n = 2Q_{n-1} + Q_{n-2}, \quad \text{para } n \geq 2.$$

Analizando los primeros valores vemos que 6 es un número perfecto que pertenece a la sucesión de Pell-Lucas, a saber $Q_2 = 6$.

Conjetura 6.1. *El único número perfecto que aparece en la sucesión de Pell y en la sucesión de Pell-Lucas es $Q_2 = 6$.*

Bibliografía

[1] Great internet mersenne prime search (gimps), 2015.

[2] R. P. Brent, G. L. Cohen, and H. J. J. te Riele. Improved techniques for lower bounds for odd perfect numbers. *Mathematics of Computation*, 57(196):857–868, 1991.

[3] D. M. Burton. The history of mathematics: An introduction. *AMC*, 10:12, 1985.

[4] J. H. E. Cohn. Square fibonacci numbers, etc. *Fibonacci Quarterly*, 2:109–113, 1964.

[5] J. A. Dris. Solving the odd perfect number problem: Some old and new approaches. Master's thesis, De La Salle University–Manila, 2008.

[6] G. Espíndola. Algunos resultados derivados del estudio de la sucesión de fibonacci módulo m. Master's thesis, Universidad Industrial de Santander, 2015.

[7] R. K. Guy. *Unsolved Problems in Number Theory*, volume 1. Springer Science & Business Media, ny, 1994.

[8] F. Luca. Euler indicators of lucas sequences. *Bull. Mat. Soc. Mat. Roumaine*, 40(88):151–163, 1997.

[9] F. Luca. Arithmetic functions of fibonacci and lucas numbers. *Fibonacci Quarterly*, 37(3):265–268, 1999.

[10] F. Luca. Perfect fibonacci and lucas numbers. *Rendiconti del Circolo Matematico di Palermo*, 49(2):313–318, 2000.

[11] F. Luca and F. B. Coghlan. Can two consecutive numbers both be perfect? *The American Mathematical Monthly*, 108(1):80–81, 2001.

[12] P. Nielsen. An upper bound for odd perfect numbers. *Integers*, 3:A14, 2003.

[13] P. Nielsen. Odd perfect numbers have at least nine distinct prime factors. *Mathematics of Computation*, 76(260):2109–2126, 2007.

[14] R. Paulo. Square classes of fibonacci and lucas numbers. *Portugaliae mathematica*, 46(2):159–175, 1989.

[15] L. Richard. Measuring the abundancy of integers. *Mathematics Magazine*, pages 84–92, 1986.

[16] N. Robbins. On fibonacci numbers of the form px^2 where p is prime. *Fibonacci Quarterly*, 37(4):265–268, 1983.

[17] K. H. Rosen. *Elementary Number Theory and Its Applications*. Alternative Text Formats Series. Pearson/Addison Wesley, 2005.