Revista Digital: Matemática, Educación e Internet
ISSN: 1659-0643
revistadigitalmatematica@itcr.ac.cr
Instituto Tecnológico de Costa Rica
Costa Rica

Miramontes de León, Gerardo
Sobre la infinitud de los primos extendidos de Germain: un nuevo enfoque
Revista Digital: Matemática, Educación e Internet, vol. 23, núm. 2, 2023, Marzo-Agosto, pp. 1-12
Instituto Tecnológico de Costa Rica
Cartago, Costa Rica

DOI: https://doi.org/10.18845/rdmei.v23i2.6347

Disponible en: https://www.redalyc.org/articulo.oa?id=607971877003

Revista digital
Matemática, Educación e Internet
https://revistas.tec.ac.cr/index.php/matematica
Vol 23, No 2. Marzo, 2023 – Agosto, 2023 ISSN 1659 -0643

Sobre la infinitud de los primos extendidos de Germain: un nuevo enfoque

On the infinity of Germain's extended prime numbers: a novel approach

Gerardo Miramontes de León
gmiram@ieee.org
Universidad Autónoma de Zacatecas
México

Recibido: 22 enero 2022 Aceptado: 1 setiembre 2022

Resumen: La conjetura sobre la infinitud de los primos de Germain, es decir, aquellos que "si p es primo, $2p+1$ también es primo", se trata en este trabajo siguiendo un enfoque novedoso. Primero se observa que hay un número infinito de números p que no son primos de Germain. Por lo tanto, si la cantidad de primos de Germain es infinita, no hay una biyección con todos los números primos. Sin embargo, en este trabajo se muestra que haciendo una extensión a la definición de Germain, sí se obtiene esa biyección. Para lograrlo, se extiende la definición de "$2p+1$" a "$kp+(k-1)$, con $k \geq 2$", los cuales serán definidos como primos extendidos de Germain. Eso nos permite plantear, entre otras, la conjetura de que existe un número infinito de primos extendidos de Germain y su biyección al conjunto infinito de los números primos. La última conjetura plantea que, en la forma $kp+(k-1)$, ningún primo p queda fuera de la categoría de ser primo de Germain.

Palabras Clave: números primos, primos de Germain, infinitud de números primos

Abstract: The conjecture about the infinity of Germain primes, that is, those that "if p is prime, $2p+1$ is also prime", is treated in this work following a novel approach. We first observe that there is an infinite number of primes p that are not Germain primes. Therefore, if the number of Germain primes is infinite, there is no bijection with all primes. However, in this work it is shown that by making an extension to Germain's definition, this bijection is obtained. To achieve this, the definition of "$2p+1$" is extended to "$kp+(k-1)$, with $k \geq 2$", which will be defined as extended Germain primes. This allows us to pose, among others, the conjecture that there is an infinite number of extended Germain primes and their bijection to the infinite set of prime numbers. The last conjecture states that, in the form $kp+(k-1)$, no prime p falls outside the category of being a Germain prime.

Keywords: prime numbers, Germain primes, infinity of prime numbers

1. Introducción

Este trabajo se basa en una pregunta muy antigua ¿se puede generar un número primo a partir de otro? Las razones de tal pregunta son varias, una de ellas, aunque parezca desconectada, es la búsqueda

de nuevos números primos. Se pueden mencionar, al menos, dos casos en los que se busca encontrar un número primo que sea generado a partir de otro. Un primer ejemplo son los números primos de Sophie Germain, los cuales se definen así [1]:

Definición 1

Un número primo p es un número primo de Sophie Germain, si $2p + 1$ también es primo.

Aunque quizá se esperaba que dichos números aparecieran con frecuencia, resultó que en realidad hay muchos números primos que no cumplen con esa definición. Una nota adicional es que a los primos de Germain también se les puede llamar "primos casi dobles" [2].

Un segundo ejemplo son los números de Mersenne (1644) [3]:

Definición 2

Un número primo de Mersenne es un número primo que es una potencia de dos menos 1, es decir, si p es primo, $2^p - 1$ también es primo[a].

[a] En realidad no es suficiente que p sea primo para que $2^p - 1$ sea primo.

Marin Mersenne trató de encontrar una fórmula para todos los primos. Sin embargo, y como en el caso de los primos de Germain, no todos los números primos p de la forma $2^p - 1$ son primos. En el caso de los números de Mersenne, incluso, por ser más bien raros, encontrarlos se ha convertido en una tarea gigantesca, en la que se puede participar gracias a la plataforma GIMPS, Great Internet Mersenne Prime Search [4].

No parece haber un patrón para generar números primos, es decir, no hay una fórmula sencilla. Tampoco es conocido algún "comportamiento definido", que nos diga, por ejemplo, cómo están distribuídos o cuándo va a aparecer el siguiente número primo. En 1845 Joseph Bertrand propuso que para cualquier $n \in \mathbb{N}, n > 3$ siempre existe al menos un número primo p tal que $n < p < 2n - 2$; más aún que para $n > 1$ siempre hay un primo en el intervalo $n < p < 2n$. La formulación que nos interesa es la siguiente: dado el n-ésimo número primo p_n, para $n \geq 1$ se tiene que $p_{n+1} < 2p_n$ [5], lo cual se acerca a la definición de primos de Germain.

Pero, si consideramos los números primos de Germain, encontramos que solo algunos números primos p generan un número $2p + 1$ que sea primo. Este es el punto de partida de este trabajo, en el cual se introduce una extensión a los primos de Germain.

El trabajo está organizado de la siguiente manera. En la Sección 2 se calculan algunos números de Germain, y su cardinalidad, para dar una idea de su comportamiento. Como se tiene una conjetura sobre la infinitud de los primos de Germain, se toma un enfoque contrario en la Sección 3, donde se presentan varias demostraciones de la infinitud de los primos que no son primos de Germain. Este nuevo enfoque parte del hecho que es más fácil buscar aquellos números primos que no son primos de Germain que los que sí lo son. En la Sección 4 se definen los primos *completamente no Germain*, y se introduce el conjunto de todos los primos que sí tienen relación con los primos de Germain. Eso es útil para el desarrollo posterior, es decir, para introducir una forma extendida de los primos de Germain, cuya razón se explica en las Secciones 5 y 6. Este enfoque nos permite proponer que la unión de los primos extendidos de Germain contienen a la infinitud de los números primos, la cual ha sido demostrada desde hace siglos por Euclides.

2. Notas preliminares sobre los primos de Germain

Para esta sección y el resto del trabajo se requieren las siguientes definiciones: función contadora de números primos $\pi(n)$, además se designará a un primo de Germain como p_G, y al número primo que se obtiene al hacer $2p+1$ se le designará como p_{sG}, conocido como primo seguro de Germain.

Definición 3

Función contadora de números primos es la función $\pi(n)$ definida como $\pi(n) := \#\{p \in \mathbb{N} \mid p \text{ es un número primo y } p \leq n\}$ y donde $\#\{\,\}$ denota su cardinalidad.

Algunos números primos no son primos de Germain, como el 7, el 13, el 17, y muchos más. Si, por ejemplo, contamos cuántos primos de Germain hay hasta un valor de n dado, encontramos que la densidad de primos de Germain desciende al aumentar n. Como muestra hagamos $n = 100$, entonces $\pi(100) = 25$, es decir, en los 100 primeros números naturales solo hay 25 que son primos. Designando la cantidad (o cardinalidad) de los primos de Germain por $\pi_G(n)$, encontramos que $\pi_G(100) = 10$, es decir, solamente 10 son p_G. Estos cálculos se pueden continuar para valores cada vez más grandes de n. La Tabla 1, tomada de [6], muestra los valores de cardinalidad $\pi(n)$ y $\pi_G(n)$ para diferentes valores de n y en la cuarta columna la razón $\pi_G(n)/\pi(n)$.

Tabla 1: Cardinalidades $\pi(n)$ contra $\pi_G(n)$

n	$\pi(n)$	$\pi_G(n)$	$\pi_G(n)/\pi(n)$
10	4	3	0.750
10^2	25	10	0.400
10^3	168	37	0.220
10^4	1229	190	0.154
10^5	9592	1171	0.122
10^6	78498	7746	0.098
10^7	664579	56032	0.084
10^8	5761455	423140	0.070
10^9	50847534	3308859	0.065

Note que al aumentar n hay un comportamiento asintótico hacia cero en la proporción $\pi_G(n)/\pi(n)$ indicando que $\pi_G(n)$ es mucho menor que $\pi(n)$. Sin embargo, la conjetura de la infinitud de los primos de Germain, de comprobarse, indicaría que ambas cantidades son infinitas.

3. ¿Hay una infinitud de números primos que no son de Germain?

Se considera, en este trabajo, que es más fácil encontrar cuáles primos no pueden ser p_G, en lugar de buscar aquellos que sí lo son. Para ello, tomamos el hecho de que todo número primo p mayor que 3 se puede expresar, ya sea, como $p = 6m - 1$ o como $p = 6m + 1$, donde m es un entero positivo. Note que se ha empleado la conjunción "o", ya que puede haber valores de m en los cuales una de las dos formas no es un número primo. Por ejemplo, con $m = 4$, tenemos $6m - 1 = 23$ que sí es primo, pero $6m + 1 = 25$ el cual no es primo.

Aún así, $m = 4$ sigue siendo válido en la representación de un número primo, en ese caso como $p = 6m - 1$. En este sentido, si se comprueba que m puede ser cualquier entero mayor o igual a 1, m podría ser cualquier entero positivo y por lo tanto podría tender a infinito, cumpliendo con el teorema de Euclides, "existe un número infinito de números primos".

Para el desarrollo de este trabajo, se aplica el siguiente lema [7]:

Lema 1 Todo número primo $p > 3$ se puede escribir como $p = 6m \pm 1$, donde m es un entero positivo.

Una demostración está dada también en [7].

Demostración. Todo entero positivo $n \geq 6$ se puede expresar como 6m+k, donde $k = 0, 1$,...,5 y $m \geq 1$. Los números $6m$, $6m + 2$, $6m + 3$ y $6m + 4$ son compuestos ya que son divisibles entre 2, entre 3 o ambos, es decir, $6m = 2 \times 3m$, $6m+2 = 2(3m+1)$, $6m+3 = 3(2m+1)$, $6m+4 = 2(3m+2)$. Mientras que $6m + 1$ y $6m + 5$ son, ya sea primos (por ejemplo $6 \times 1 + 1 = 7$, $6 \times 2 - 1 = 11$) o compuestos (por ejemplo $6m + 5$ es divisible por 5 si m es múltiplo de 5, $6m + 1$ es divisible por 3 si la suma de dígitos decimales es divisible por 3). Por otro lado, $6m+5$ se puede escribir como $6(m+1)-1$. Todos los primos menores que 5, es decir el 2 y 3, no se pueden expresar como $p = 6m \pm 1$ donde m es un entero positivo. Esto significa que todo número primo $p \geq 5$ puede ser expresado como $p = 6m \pm 1$, donde $m \in \mathbb{N}$. □

Otro resultado útil es la siguiente observación:

Observación 1
Para todo $p > 5$ ningún número primo tiene terminación en 5.

Con base en estas representaciones, ahora podemos considerar cuáles primos no pueden ser primos de Germain. Específicamente, se hace la proposición:

Proposición 1
Todos aquellos números primos que puedan expresarse como $p = 6m+1$ no pueden ser primos de Germain.

Demostración. Sea $p = 6m+1$, de modo que la definición de p_G nos pide calcular $2p+1$, para obtener:

$$\begin{aligned} 2p + 1 &= 2(6m + 1) + 1 \\ &= 12m + 3 \\ &= 3(4m + 1) \end{aligned}$$

entonces se obtiene un número múltiplo de 3, y por lo tanto no es primo. □

Por otro lado, para algunos valores enteros positivos de m, se obtiene un primo con ambas formas, es decir, con $6m-1$ y con $6m+1$. Cuando ocurre eso, entonces $6m-1$ y $6m+1$ forman un par de primos gemelos[1]; un primo gemelo menor $6m - 1$ y un primo gemelo mayor $6m + 1$. Esta representación $(6m - 1, 6m + 1)$ de primos gemelos, es válida para los pares de gemelos después del par (3,5). Cuando para algún valor de m, alguno de los dos no sea primo, entonces ese primo simplemente no es un primo gemelo (recuerde el ejemplo con $m = 4$, para $p = 23$).

Entre los pares de primos gemelos $(6m - 1, 6m + 1)$, en la Proposicion 1 se demostró que el gemelo mayor $6m + 1$, nunca puede ser primo de Germain. Ahora, el primo gemelo menor, y para cualquier otro número primo, hacemos la siguiente proposición:

[1]Dos números primos consecutivos son gemelos si su diferencia es igual a 2.

Proposición 2

Ningún número primo p con terminación en 7, puede ser primo de Germain, p_G.

Demostración. Sea un número primo con terminación en 7, dado por $p = 10a + 7$, donde a es un número entero, entonces al hacer $2p + 1$ tenemos

$$\begin{aligned} 2p + 1 &= 2(10a + 7) + 1 \\ &= 20a + 15 \end{aligned}$$

de modo que $2p + 1$ será siempre un número con terminación en 5, y ningún número primo tiene terminación en 5, como se estableció en la Observación 1. □

En este punto cabe hacer la pregunta: ¿hay una infinidad de números primos que terminan en 7 o de la forma $6m + 1$? Una respuesta afirmativa puede ser la prueba de la infinitud de los números primos que no son primos de Germain, es decir, se puede establecer la conjetura:

Conjetura 1

El número de primos $p \neq p_G$ es infinito.

En la Conjetura 1, se dice que del infinito número de primos hay muchos que no son primos de Germain, y como se ha demostrado por Euclides que hay infinitos números primos, se puede decir que tiene que haber un número infinito de primos que no son primos de Germain. En este trabajo se propone que aún si se cumple la infinitud de los números primos de Germain, el conjunto también excluye a una gran cantidad de primos, pero al haber un número infinito de números primos, se mantendría también la infinitud de los números primos tales que $2p + 1$ es primo. Una conclusión plausible es que $\pi_G(n)$ es mucho menor que $\pi(n)$, siendo ambos infinitos cuando n tienda a infinito. Más aún, si la cantidad de primos de Germain es infinita, no hay una biyección con la infinitud de los números primos.

4. Unión entre los p_G y sus p_{sG}

El objetivo planteado es encontrar una forma alternativa a los primos de Germain, de modo que se pueda extender el número de primos p que generen otro número primo. Sin embargo, en esta sección se comienza por analizar, incluyendo un ejercicio numérico, si al considerar todos los primos de Germain, sean p_G y/o p_{sG} aumenta su cardinalidad. Así, a partir de un conjunto finito de números primos se analiza su relación a otro conjunto de primos p_G.

Sea el conjunto ordenado $\mathbf{P}$ de números primos, cuyos elementos están dados por:

$\mathbf{P} = \{p | p \leq n\}$, donde p es primo y $n \in \mathbb{N}$ con un valor dado.

Por su parte, el conjunto $\mathbf{P}$ tiene su propia cardinalidad dada por $\pi(n)$. A partir de $\mathbf{P}$ se obtiene el conjunto $\mathbf{G}$ cuyos elementos serán los números primos de Germain extraídos de $\mathbf{P}$, es decir, $\mathbf{G} \subseteq \mathbf{P}$ y cuyos elementos están dados por

$$\mathbf{G} = \{p | p = p_G\}. \tag{1}$$

Igual que $\mathbf{P}$, el conjunto $\mathbf{G}$ tiene su cardinalidad en $\pi_G(n)$. El conjunto $\mathbf{G}$ genera un conjunto $\mathbf{S}$ a partir de la condición "$2p + 1$ es primo", es decir, el conjunto $\mathbf{S}$ es el conjunto seguro de Germain, cuyos elementos están dados por

$$\mathbf{S} = \{p | 2p + 1 = p_{sG}\}. \tag{2}$$

Entonces $\mathbf{S}$ tiene la misma cardinalidad $\pi_G(n)$ pero cuyos elementos, algunos, pueden ser iguales a los elementos de $\mathbf{G}$. La unión $\mathbf{E} = \mathbf{G} \cup \mathbf{S}$ tendrá una cardinalidad $\pi_{\mathbf{E}}(n)$. Interesa comparar el total de los números primos de Germain, es decir, los generados como p_{sG} y los generadores p_G. Pero $\pi_{\mathbf{E}}(n)$ no es la suma $\pi_G(n) + \pi_{sG}(n)$ ya que puede haber intersección entre $\mathbf{G}$ y $\mathbf{S}$. Al obtener $\mathbf{E}$, deseamos saber si en la lista se han perdido algunos primos, ya que esto puede suceder, puesto que no todos los primos son primos de Germain.

Cabe hacer un paréntesis para definir una clase importante de número primos, los cuales no tienen relación con los primos de Germain. Al hacer la unión $\mathbf{E} = \mathbf{G} \cup \mathbf{S}$, solo aparecen aquellos p que son p_G, p_{sG} o ambos. Por ejemplo, $p = 7$ no es primo de Germain pero es primo seguro de Germain, p_{sG}, ya que se obtiene a partir de $p = 3$, $(2 \times 3 + 1 = 7)$, entonces sí aparece en el conjunto $\mathbf{E}$. Por lo anterior, la diferencia $\pi(n) - \pi_{\mathbf{E}}(n)$ indicará cuántos de esos primos no se relacionan con los primos de Germain, de ningún modo. El primer ejemplo que aparece es el número primo $p = 13$, el cual no es p_G y tampoco es p_{sG} de ningún otro primo anterior.

Conviene definir la siguiente clase de números primos, la cual será designada por p_{cnG}, es decir, primos *completamente no Germain*:

Definición 4

Un número primo p será *completamente no Germain*, p_{cnG}, si:

$$p \text{ es tal que } \begin{cases} 2p+1, \text{ no es primo.} \\ \dfrac{p-1}{2}, \text{no es primo.} \end{cases}$$

Lo interesante es que la cantidad de primos p_{cnG} es mucho muy grande, y aumenta al aumentar n.

En ese orden de ideas, se compara la cardinalidad entre $\pi_{\mathbf{E}}(n)$ y el total de primos para calcular la proporción $\pi_{\mathbf{E}}(n)/\pi(n)$, al mismo tiempo que se obtiene $\pi_{cnG}(n)$, la cual aumenta con n. Finalmente se comparan los conjuntos $\mathbf{E}$ y $\mathbf{P}$; los elementos de este último que no estén en $\mathbf{E}$ serán los primos p_{cnG}.

4.1. Ejemplos numéricos

Ejemplo 1

Sea $n = 10$. Entonces $\mathbf{P} = \{2, 3, 5, 7\}$. Por lo tanto $\pi(10) = 4$. De aquí obtenemos $\mathbf{G} = \{2, 3, 5\}$ y $\pi_G(10) = 3$. Los primos generados son primos seguros de Germain formando el conjunto $\mathbf{S} = \{5, 7, 11\}$, con cardinalidad $\pi_{sG}(10) = \pi_G(10) = 3$. Prosiguiendo, $\mathbf{E} = \mathbf{G} \cup \mathbf{S} = \{2, 3, 5, 7, 11\}$, con $\pi_{\mathbf{E}}(10) = 5$. Observe que la cardinalidad $\pi_{\mathbf{E}}(10) = 5$ es mayor a la cardinalidad original $\pi(10) = 4$. Sin embargo, se comparan los elementos de $\mathbf{P}$ que no están en $\mathbf{E}$, y haciendo un ajuste en $\mathbf{E}$, se obtiene $\dfrac{\pi_{\mathbf{E}}(10)}{\pi(10)} = \dfrac{4}{4} = 1$.

En el Ejemplo 1, al unir los conjuntos de primos de Germain $\mathbf{G}$ y de primos seguros de Germain $\mathbf{S}$, se obtiene la lista completa de números primos desde el 2 hasta el 7; no se perdió ninguno, pero eso cambia al aumentar n, como se muestra en el siguiente ejemplo.

Ejemplo 2

Sea $n = 100$. Ahora se tiene que $\pi(100) = 25$ y los elementos de $\mathbf{P}$ son: $\mathbf{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$. Los conjuntos $\mathbf{G}$ y $\mathbf{S}$ son: $\mathbf{G} = \{2, 3, 5, 11, 23, 29, 41, 53, 83, 89\}$, $\mathbf{S} = \{5, 7, 11, 23, 47, 59, 83, 107, 167, 179\}$ y $\pi_G(100) = 10$. Entonces, para $p \leq 100$, $\mathbf{E} = \{2, 3, 5, 7, 11, 23, 29, 41, 47, 53, 59, 83, 89\}$, eliminando aquellos $p > 100$, y nos queda $\pi_{\mathbf{E}}(100) = 13$. Finalmente $\frac{\pi_{\mathbf{E}}(100)}{\pi(100)} = \frac{13}{25} = 0.52$, pero ahora sí hay elementos en $\mathbf{P}$ que no están en $\mathbf{E}$ y así $\pi_{cnG}(100) = 12$ es la cantidad de primos que son *completamente no Germain*.

En la Tabla 2 se muestran los resultados de la comparación entre $\pi_{\mathbf{E}}(n)$ y $\pi(n)$ para diferentes valores de n. En la quinta columna se incluye la cantidad de primos p_{cnG}, es decir, que no son primos de Germain de ningún tipo.

Tabla 2: Números primos que no son p_G ni p_{sG}.

n	$\pi(n)$	$\pi_{\mathbf{E}}(n)$	$\pi_{\mathbf{E}}(n)/\pi(n)$	$\pi_{cnG}(n)$
10^2	25	13	0.52	12
10^3	168	55	0.33	113
10^4	1229	277	0.23	952
10^5	9592	1715	0.18	7877
10^6	78498	11364	0.14	67134
10^7	664579	82437	0.12	582142
10^8	5761455	624740	0.11	5136715
10^9	50847534	4894233	0.10	45953301

Según se muestra en la Tabla 2, al aumentar n, hay cada vez un mayor número de primos que caen en la categoría de ser p_{cnG}. Se deja abierta al lector la demostración de que la cantidad de estos puede ser infinita, como se indica en la Conjetura 1.

En la siguiente sección se busca extender la definición de los números de Germain, de modo que se vayan encontrando cada vez más números primos que generen otro número primo.

5. Números primos extendidos de Germain

En este trabajo se amplía la definición de número primo de Germain de "p tal que $2p + 1$ sea primo" a una nueva definición: "p tal que $3p + 2$ sea primo". Se trata de encontrar algunos números que, en la forma anterior, no eran primos de Germain, y que en la nueva forma sí entreguen nuevos números primos. Por ejemplo, sea $p = 7$, que no es número p_G, entonces en la nueva forma se obtiene $3p+2 = 23$, el cual sí es número primo. Designemos a estos números *primos extendidos de Germain* como p_{Gx}.

Repitiendo los cálculos para $p < 100$, los números p_{Gx}, $(3p+2)$ son: $\mathbf{Gx} = \{3, 5, 7, 13, 17, 19, 23, 29, 37, 43, 59, 79, 83, 89, 97\}$, y sus correspondientes números primos seguros extendidos de Germain p_{sGx} son: $\mathbf{S_x} = \{11, 17, 23, 41, 53, 59, 71, 89, 113, 131, 179, 239, 251, 269, 293\}$. Aunque algunos primos de Germain desaparecieron (por ejemplo el 2 y el 11), ahora se obtienen 15 números primos que generan números primos, en lugar de 10. Así que en este caso $\pi_{Gx}(100) = 15$, el cual se puede comparar con $\pi_G(100) = 10$ de la Tabla 1.

Al realizar más cálculos para los primos extendidos p_{Gx}, se obtuvo un comportamiento muy similar al anterior. Los resultados se muestran en la Tabla 3, y se observa solo un ligero incremento en la proporción $\pi_{\mathbf{Ex}}(n)/\pi(n)$, donde $\pi_{\mathbf{Ex}}(n)$ es la cantidad de primos extendidos de Germain, de la forma

$3p+2$. La quinta columna muestra la cantidad de primos que son p_{cnG}, donde también se observa una reducción respecto al caso $2p+1$, pero la tendencia hacia arriba se mantiene al aumentar n.

Tabla 3: Números primos que no son p_{Gx} ni p_{sGx} en $3p+2$.

n	$\pi(n)$	$\pi_{\mathbf{Ex}}(n)$	$\pi_{\mathbf{Ex}}(n)/\pi(n)$	$\pi_{cnG}(n)$
10^2	25	19	0.76	6
10^3	168	85	0.51	83
10^4	1229	470	0.38	759
10^5	9592	2982	0.31	6610
10^6	78498	20199	0.26	58299
10^7	664579	145822	0.22	518757
10^8	5761455	1105405	0.19	4656050
10^9	50847534	8650259	0.17	42197275

5.1. Generalización de los números primos extendidos de Germain

La extensión propuesta se puede continuar como $4p+3$, $5p+4$, entre otras, y se obtienen resultados similares. Con estas nuevas formas (clases) se obtienen otros números primos a partir de números primos anteriores. Cabe aclarar, que no se trata de reemplazar a la forma original, sino de agregar nuevas formas, y su justificación se verá en la siguiente sección.

Generalizando, la extensión se puede llevar a la forma

$$p_{Gk} = kp + (k-1), \text{con } k \geq 2 \tag{3}$$

donde k es un entero y reemplaza al subíndice x. Si hacemos $k=1$ regresamos a los números primos originales, así que para ajustarnos al criterio de Germain, se propone $k \geq 2$.

En la sección anterior se vio que algunos p que no generaban otro primo como $2p+1$, en la forma alternativa $3p+2$ sí lo hacen. Para ilustrar la extensión a otros valores de k, sea $k=4$, usando la notación propuesta en (3), para $p=5$ tenemos $p_{G4} = 4\times 5+3 = 23$, el cual es primo. Esto no se cumple con todos los p, de ahí la búsqueda para ver en cuáles sí se cumple y sobre todo cuántas veces se cumple para una n dada, donde n es el número deseado en $\pi(n)$. En lugar del uso de tablas, en la Figura 1 se muestran los resultados para varios valores de k, y para n desde 100 hasta 10^8. Es evidente que el cambio de la forma $2p+1$ a $kp+(k-1)$, con $k \geq 2$, no reduce de manera significativa el número de primos que no son, ahora, "primos extendidos de Germain".

El resultado no es completamente inesperado, ya que en la forma alternativa $kp+(k-1)$ también se pueden encontrar primos p que no serán primos (extendidos) de Germain. En cada caso, es decir, para cada valor de k, se conjetura que habrá un número infinito de primos p que no generan otro número primo, exactamente igual que en el caso original $2p+1$. La demostración queda abierta pero, de manera inicial, se propone el siguiente procedimiento.

Sea p_{G3} el primo extendido de Germain clase 3, es decir, de la forma $3p+2$. Aquellos números primos p con terminación en 1, no serán primos extendidos de Germain de esta clase ($k=3$), ya que generan un número con terminación en 5, y como ya se observó, y además es conocido, ningún número (después del 5) que termine en 5 es primo.

Demostración. Sea un número primo dado por $p = 10a+1$, donde a es un número entero. Al hacer $3p+2$ se tiene:

$$\begin{aligned} 3p+2 &= 3(10a+1)+2 \\ &= 30a+5 \end{aligned}$$

y por lo tanto no es primo porque termina en 5. □

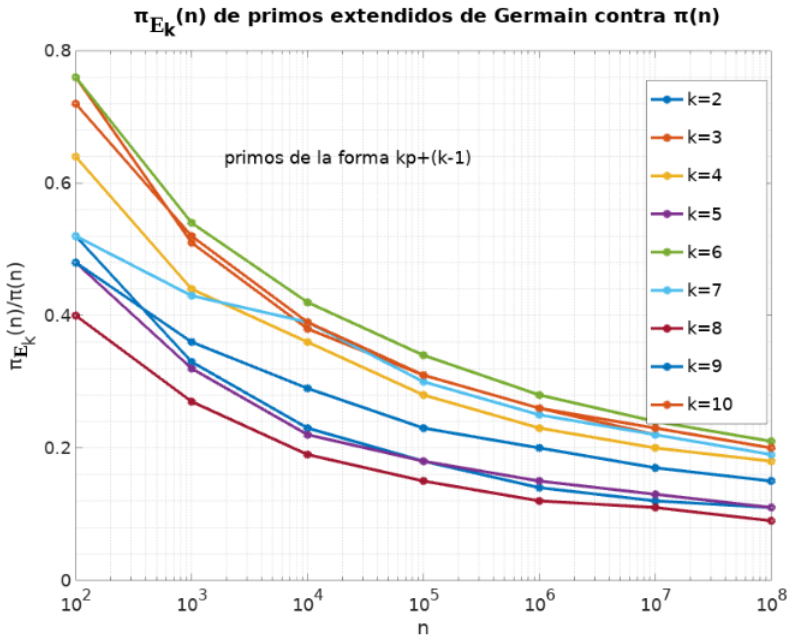

Figura 1: Comportamiento de la proporción entre primos extendidos de Germain y $\pi(n)$ para varios valores de k y de n. (Elaboración propia).

En resumen, cada clase k de Germain tendrá ciertos valores de p para los cuales no cumplan la definición. Esto se muestra, para algunos valores de k, en la Tabla 4. Nuevamente se confirma que hay un gran número de primos que no generan otro primo clase Germain, que bien podrían llamarse "casi múltiplo", siguiendo la terminología del término "casi doble."

Tabla 4: Primos que no son p_{Gk}.

clase $kp+(k-1)$	primo p que no es clase k Germain
$2p+1$	$p = 6m+1$ y/o terminado en 7
$3p+2$	p terminado en 1
$4p+3$	p terminado en 3
$5p+4$	forma $p = 6m+1$
$7p+6$	p terminado en 7
$\vdots$	$\vdots$

6. Unión de primos extendidos de Germain clase k

Finalmente, se propone hacer la unión de todas las formas extendidas de primos de Germain, para obtener todos los números primos, al menos, hasta $p \leq n$.

Como se mostró anteriormente, algunos números primos no están incluidos en algunas clases k de Germain, no como p_G y tampoco como p_{sG}. Al calcular el primo $kp+(k-1)$, con $k > 2$, sí aparecen, ya sea como p_{Gk} o como p_{sGk}. Se plantea que aumentando el valor de k sucesivamente, se obtendrá la lista completa de números primos $p \leq n$.

Se podrá preguntar ¿qué sentido tiene obtener un primo p si ya se tiene previamente una lista? Aunque esto parece repetir lo que ya se tiene, con este ejercicio se logra comprobar que en la totalidad de las clases extendidas de Germain, sí se encuentran todos los números primos.

Sea el conjunto $\mathbf{E}_2 = \mathbf{G}_2 \cup \mathbf{S}_2$, donde, $\mathbf{G}_2$ es el conjunto de primos de Germain y $\mathbf{S}_2$ el conjunto de los primos seguros de Germain de la forma $2p+1$, obtenidos del conjunto $\mathbf{P} = \{p \leq n\}$. Además, se definen todos los conjuntos $\mathbf{E_k} = \mathbf{G_k} \cup \mathbf{S_k}$, con $k \geq 2$, entonces se plantea la siguiente conjetura:

Conjetura 2

La unión de los conjuntos $\mathbf{E_k}$ contendrán a todos los número primos $p \leq n$, es decir,

$$\mathbf{E_T} = \cup_{k\geq 2}\mathbf{E}_k = \mathbf{E}_2 \cup \mathbf{E}_3 \cup \cdots \cup \mathbf{E}_k = \{p|p \leq n\}. \tag{4}$$

En la Conjetura 2, no se trata de encontrar cuántos primos no pertenecen a una clase k, o a todas las clases k, si no que se trata de probar que en los primos extendidos de Germain, están todos los números primos. La forma de ilustrarlo es por medio de un ejemplo, paso a paso.

Ejemplo 3

Sea el conjunto $\mathbf{P} = \{p|p \leq 20\} = \{2,3,5,7,11,13,17,19\}$. Iniciando con la definición de Sophie Germain, $k = 2$. Entonces, $\mathbf{G}_2 = \{2,3,5,11\}$, los primos 13, 17 y 19 no son primos de Germain clase 2; el conjunto de primos seguros de Germain es $\mathbf{S}_2 = \{5,7,11,23\}$. La unión de $\mathbf{G}_2$ y $\mathbf{S}_2$, es $\mathbf{E}_2 = \{2,3,5,7,11,23\}$. Como $\mathbf{S}_k$ puede crecer, al aumentar k, mucho más allá del intervalo de interés, se ignora todo término mayor que el último elemento de $\mathbf{P}$. En este caso se ignora el último término $(23 > 19)$, quedando la unión como $\mathbf{E}_2 = \{2,3,5,7,11\}$. Comparando $\mathbf{E}_2$ con $\mathbf{P}$, hay una diferencia en los términos, así que se continúa con $k = 3$.
El cálculo con $k = 3$ entrega $\mathbf{G}_3 = \{3,5,7,13,17,19\}$ y $\mathbf{S}_3 = \{11,17,23,41,53,59\}$. Luego $\mathbf{E}_3 = \{3,5,7,11,13,17,19,23,41,53,59\}$. Nuevamente, el último término de $\mathbf{E}_3$ es mayor al último término de $\mathbf{P}$, por lo que se elimina el último quedando $\mathbf{E}_3 = \{3,5,7,11,13,17,19,23,41,53\}$. Esta operación se repite hasta que el último término de $\mathbf{E}_3$ sea menor o igual al último término de $\mathbf{P}$, quedando $\mathbf{E}_3 = \{3,5,7,11,13,17,19\}$. La unión de $\mathbf{E}_2$ y $\mathbf{E}_3$ es $\mathbf{E_T} = \{2,3,5,7,11,13,17,19\}$. Se comparan los conjuntos $\mathbf{E_T}$ y $\mathbf{P}$ y se obtiene una relación uno a uno, misma cantidad y mismos números primos. Se requirieron los valores de $k = 2$ y $k = 3$, y no falta ningún primo en $\mathbf{E_T}$ para ese intervalo $p \leq 20$.

El Ejemplo 3, muestra paso a paso el procedimiento a seguir. Para valores más grandes se puede hacer la misma comparación y encontrar hasta qué valor de k es necesario para completar el conjunto original $\mathbf{P}$. En la Tabla 5 se muestran los resultados para varios valores de n y el último valor de k en cada caso.

Tabla 5: Primos extendidos de Germain clase k en $\{p \leq n\}$.

n	k	longitud de $\mathbf{P}$ y de $\mathbf{E_T}$
10^2	7	25
10^3	18	168
10^4	31	1229
10^5	45	9592
10^6	93	78498

En la tercera columna de la Tabla 5, se indica que la longitud, o número de elementos, del conjunto $\mathbf{P}$ es la misma que el conjunto $\mathbf{E_T}$, y cabe aclarar que además de la longitud, ambos contienen exactamente los mismos números primos. De hecho, el algoritmo termina cuando la operación XOR (la cual se emplea en varios lenguajes de programación), entre $\mathbf{E_T}$ y $\mathbf{P}$, devuelve el conjunto vacío, indicando que ambos se han vuelto idénticos[2].

[2]Recuerde que la operación XOR representa la función de desigualdad, es decir, encuentra aquellos elementos que no están en ambos conjuntos.

Los resultados de la Tabla 5 son un impulso para enunciar una conjetura más, ya que se puede proponer que:

Conjetura 3

En el conjunto infinito de números primos y en el conjunto infinito de unión de conjuntos $(\mathbf{E_k})$ de primos extendidos clase k se cumple que

$$\begin{aligned}&\text{Si } \mathbf{P} = \{p | p \leq n,\ n \to \infty\},\ \text{(conjunto infinito de números primos)}\\ &\text{y si}\\ &\mathbf{E_T} = \cup_{k\geq 2}\mathbf{E_k} = \mathbf{E_2} \cup \mathbf{E_3} \cup \cdots \cup \mathbf{E_k},\ \text{con } k \to \infty \qquad (5)\\ &\text{(unión infinita de conjuntos de primos extendidos de Germain)}\\ &\text{entonces } \mathbf{E_T} = \mathbf{P}.\end{aligned}$$

Como consecuencia de la Conjetura 3, se termina haciendo la siguiente:

Conjetura 4

Para cualquier número primo p, sin importar su valor, $\exists$ un entero $k \geq 2$ tal que $kp + (k-1)$ es primo.

Es decir, si un número p no entrega un primo $2p+1$, existe un número con el valor adecuado de k, sin importar la magnitud de ambos, tal que $kp + (k-1)$ es primo. De este modo, no se obtiene un primo "casi doble" [2], si no que se obtendrá un número primo con "casi" multiplicidad k. En este trabajo se recomienda seguir usando el término "primo de Germain" en lugar de primo casi doble, y "primo extendido de Germain" (o primo de Germain clase k) en lugar de primo casi múltiple, para hacer honor a su autora, Sophie Germain.

7. Conclusiones

En este trabajo se siguió un nuevo enfoque en el tema sobre la infinitud de los primos de Germain, al considerar que es más fácil determinar cuáles primos no son primos de Germain, en lugar de los que sí lo son. Algunos aspectos a resaltar son:

- A partir de la definición "p tal que $2p+1$ es primo", se presentaron algunos casos para comprobar que hay primos que nunca son primos de Germain.
- Se definió un conjunto $\mathbf{E}$ cuyos elementos son todos los primos de Germain, es decir, los p_G más los p_{sG} para identificar, de ese modo, los primos que son completamente no Germain. Para ello se comparó la cardinalidad del conjunto $\mathbf{E}$ al conjunto $\mathbf{P}$ de números primos, en un intervalo $p \leq n$ dado.
- Posteriormente, se definieron los primos extendidos de Germain, es decir, se amplió la definición de primo de Germain de "$2p+1$" a "$kp + (k-1)$, $k \geq 2$, entero", definiendo así una clase k de Germain. Finalmente, la unión de las clases extendidas de Germain, unión infinita de conjuntos $\mathbf{E_k}$, designada como $\mathbf{E_T}$, nos permitió plantear una biyección entre esa unión y el conjunto infinito de números primos.
- La última conjetura lograda es que para todo número primo p, existe un valor k tal que en la forma $kp + (k-1)$ se obtiene un número primo. Ningún p queda fuera de la categoría de ser primo de Germain, y más específicamente, k-Germain, con $k \geq 2$.

La conclusión definitiva es que, si la cantidad de primos de Germain $(2p+1)$ es infinita, no hay una biyección con la infinitud de los números primos.

Agradecimientos

Se agradecen las aportaciones de los revisores anónimos, quienes con sus observaciones y correcciones ayudan a mejorar la presentación del trabajo. En especial, se agradece su aportación para aclarar la notación empleada en la demostración de la Proposición 2 y de la página 8.

8. Bibliografía

[1] V. Shoup, *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2009.

[2] L. Günter, "Long chains of nearly doubled primes," *Mathematics of Computation*, vol. 53, no. 1889, pp. 751–759, 1989.

[3] M. Mersenne, "Cogitata physico-mathematica (paris, 1644)," 1644.

[4] "Great internet mersenne prime search," https://www.mersenne.org/legal/.

[5] P. Ribenboim, *Fermat's Last Theorem for Amateurs*. Springer, 1999.

[6] G. Miramontes and D. Miramontes, "Números primos gemelos y primos gemelos de germain," *Revista Digital Matemática Educación e Internet*, vol. 23, no. 1, Agosto 2022 - Febrero 2023 2022.

[7] M. Barylski, "Studies on twin primes in goldbach partitions of even numbers," http://tasmoto.org/research/TwinPrimesInGoldbachPartitions.pdf, 2018.