Exploración de algunas conjeturas[♣] sobre los números primos con *DERIVE*

Juana Contreras S.[2]
Claudio del Pino O.[3]
Instituto de Matemática y Física
Universidad de Talca

La teoría de los números es la rama de la matemática que estudia los números enteros y sus propiedades, ocupando un lugar muy especial los números primos.

Los primeros estudios sobre los números primos datan de la época de los antiguos griegos. Una hermosa demostración sobre la existencia de infinitos números primos y de teoremas y propiedades relacionados con estos números fueron realizados por *Euclides* (siglo III, a.C). En esta época se construyeron las primeras tablas de primos, utilizando un método sistemático de eliminación de números compuestos con el fin de determinar los primos menores que un entero dado. Este método es atribuido a Eratóstenes (276-194 a.C.) y es denominado: Criba de Eratóstenes.

La infinitud del conjunto de números primos y su irregular distribución en la sucesión de los enteros, ha preocupado, molestado y maravillado a muchos matemáticos a través de la historia. El estudio de los primos ha contribuido con la generación de numerosos e interesantes problemas, algunos con enunciados tan simples de comprender, que tanto matemáticos como amantes de los números se sienten atraídos por éstos. Sin embargo, muchos de estos problemas, se han constituido en verdaderos desafíos para la comunidad matemática.

En 1912, en el V Congreso de Matemática realizado en Cambridge, el matemático alemán Landau mencionó cuatro problemas de la teoría de los números considerados de un alto grado de dificultad. Estos eran: (1) La conjetura de Goldbach; (2) La conjetura de los primos gemelos; (3) La conjetura: para cada número natural n, siempre existe un primo p tal que $n^2<p<(n+1)^2$. (4) La conjetura: existen infinitos primos de la forma n^2+1. Estas cuatro conjeturas continúan en la actualidad en estado de problemas no resueltos.

El estudio de los números primos se potencia considerablemente al contar con apoyo computacional, especialmente de software de propósitos matemáticos. El programa *DERIVE*, por ejemplo, tiene implementadas una serie de funciones y comandos de teoría de los números y un

---

♣ Por una conjetura se entiende a una suposición (denominada también conclusión) fundamentada en observaciones repetidas de un patrón o procesos muy particulares. Evidentemente, una conjetura puede ser verdadera (se demuestra) o falsa (se refuta).

[2] e-mail: jcontres@pehuenche.utalca.cl
[3] e-mail: cdelpino@pehuenche.utalca.cl

archivo especial *NUMBER.MTH*, conteniendo funciones más específicas. Además, este software permite crear nuevas funciones de propósitos específicos. Es así que, para este trabajo se ha creado el archivo *PRIMOS.MTH* con nuevas funciones, especiales para apoyar los temas tratados.

En este trabajo se presentan ocho conjeturas relacionadas con números primos, incluyendo las mencionadas anteriormente, destacando algunos resultados parciales obtenidos de los intentos realizados con el propósito de probarlas o de refutarlas, y propuestas de actividades relacionadas con el tema, integrando las funciones implementadas en el software *DERIVE* en desarrollo de éstas.

I. La conjetura de los primos gemelos. *Existe un número infinito de primos gemelos.*

Dos números primos *p* y *q*, o el par {p, q}, se denominan *primos gemelos*[4], si y solo si, *p* y *q* difieren en dos unidades. Es decir, primos gemelos son pares o parejas de números **primos** de la forma {p, p+2}.

Ejemplo. Los primeros pares de primos gemelos son: {3, 5}, {5, 7 }, {11, 13 }, {17, 19}, etc.

Actividad 1.1
Determinar todas los pares de primos gemelos {p, p+2} que se encuentran entre 1 y *100*, usando el método de la *Criba de Erastóstenes*.

Notas

- El apoyo de *DERIVE* (o de otro software) resulta muy efectivo para encontrar parejas de primos gemelos, ya sea asistiendo el trabajo "a mano", o bien utilizando funciones especiales. En el archivo *PRIMOS.MTH* se encuentran implementadas dos funciones:

  gemelos(n) que entrega todos los pares de primos gemelos {p, p+2} tal que $1< p < p+2 \quad n$

  gemelo(m, n) que entrega todos los pares de primos gemelos *{p, p+2}* tales que $m \leq p < p+2 \leq n$.

- Por ejemplo, para determinar todos los pares de primos gemelos que se encuentran entre 1 y 50 usando la función gemelos(n),
  - Se escribe la expresión *gemelos(50)=* en la línea de trabajo de *DERIVE*
  - A continuación se presiona la tecla *ENTER*
  - En la ventana de álgebra de *DERIVE* aparece lo siguiente:

$$gemelos(50) = \mathbf{[[3, 5], [5, 7], [11, 13], [17, 19], [29, 31], [41, 43]]}$$

- Ejecutando gemelo(1,50) se obtiene el mismo resultado.
- Para determina la cantidad de primos gemelos menores que n, se ejecuta la expresión *dimension(gemelos*(n)).

[4] El nombre de *primos gemelos* se atribuye a Paul Stäckel (1892-1919).

Observaciones
Es importante señalar que entorno a esta conjetura se han realizado muchos trabajos. Algunos resultados obtenidos son:

a) La suma (serie) de los recíprocos (inversos multiplicativos) de los primos de cada par de primos gemelos converge.
Es decir: *(1/3 + 1/5) + (1/5 + 1/7) + (1/7 + 1/13)* + ... converge a una constante real B, llamada *constante de Brun*. [Brun, 1919].

Nota
- Brent (1975, 1976) calculó un valor aproximado de la constante de Brun considerando 10^{11} parejas de primos gemelos, obteniendo aproximadamente $1.90216054 \pm 0.00000050$
- En el archivo *PRIMOS.MTH* se encuentra la función *brun(n)* que calcula un valor aproximado de la *constante* de *Brun* considerando primos gemelos menores que n.

b) Todo par de primos gemelos, a excepción del primer par (3,5), es de la forma {6n-1, 6n+1}.

c) Si $n \geq 2$, entonces, los enteros *{n, n+2}* forman un par de números gemelos, si y solo si, *n(n+2)* es factor de *4((n-1)! +1) +n*. [Clement, 1949].

d) Existen infinitos números primos *p*, tales que *p+2* es primo o es producto de dos números primos [Chen, 1966].

e) Una de las parejas con primos gemelos más grandes (con *11713* dígitos) es:
$\{ 242206083 \times 2^{38880} - 1,\ 242206083 \times 2^{38880} + 1 \}$ [Indlekofer y Jarai, 1995].

Actividad 1.3
1. Determinar todos los pares de primos gemelos entre 710 y 750.
2. Probar que si {p,p+2} es un par de primos gemelos con p>2, entonces existe n en IN, tal que p=6n-1
3. Determinar la veracidad o falsedad de la siguiente afirmación: "para cada número natural, el par {6n-1, 6n+1} es un par de primos gemelos".
4. Al representar los pares de primos gemelos (p,p+2), con p>2, en el plano cartesiano, éstos se encuentran sobre una recta. Justificar esta afirmación y determinar la ecuación de la recta que los contiene.
5. Determinar un valor aproximado de la *constante de Brun* considerando las parejas de primos gemelos menores que *100*, y luego las menores que *1000*.

II. Conjetura de Polignac[5]. *Todo número par m, se puede expresar de infinitas maneras como diferencia de dos primos consecutivos.*

[5] En 1849, Alphonse de Polignac estableció esta conjetura más generalizada.

O equivalentemente, dado cualquier número par *m*, existen infinitas parejas de números de primos *consecutivos* que difieren en *m* unidades.

Nota: Para *m=2*, se obtiene la conjetura de los primos gemelos.

Actividad 2.1
Determinar las parejas de primos consecutivos *{p,q}*, menores que *100* que difieren en *4* unidades.

Nota

- En el archivo *PRIMOS.MTH* se encuentra implementada la función *pares(a,b,m)* que permite determinar todas las parejas de primos consecutivos {p, q} entre a y b que difieren en m unidades.

  Por ejemplo, ejecutando *pares(1,100,4)* se obtiene:

  pares(1,100, 4) = [[7, 11], [13, 17], [19, 23]; [37, 4], [43, 47], [67, 71], [79, 83]]

  y ejecutando *pares(100,200,6)* se obtiene, todas las parejas de primos consecutivos entre 200 y 300 que difieren en 6 unidades:

  pares(100, 200, 6) = [[131, 137], [151, 157], [157, 163], [167, 173], [173, 179]]

Actividad 2.2
Al ejecutar pares(1,1000,20) se obtiene: *pares(1,1000,20) = [887, 907].* Interprete el resultado obtenido.

III. ***La conjetura de Goldbach.*** *Todo número par mayor que 2 se puede expresar como suma de dos números primos.*

Esta conjetura, una de las más famosas de la teoría de los números (y de la matemática), fue establecida en *1742*, en una carta escrita por *Christian Goldbach* (*1690-1764*) al matemático suizo *Leonard Euler*.

Ejemplo.: *4=2+2, 6=3+3, 8=3+5, 10=5+5, 10=3+7,* etc.

A pesar del gran tiempo dedicado por *Euler* para probarla, no tuvo éxito. Desde su divulgación, muchos matemáticos han trabajado en este problema. Sin embargo, hasta el día de hoy, no ha sido posible demostrarla o refutarla. Esta conjetura es reconocida como uno de los problemas más difíciles de la matemática.

Con la ayuda del computador, se ha verificado la conjetura de *Goldbach* para números extremadamente grandes (hasta aproximadamente al *100.000.000.000.000*)

En el archivo *PRIMOS.MTH* se encuentra implementada la función: *goldbach(n)* que permite lo siguiente: "dado un número par n; al ejecutar *goldbach*(n) se muestra en la ventana de *DERIVE* todas las posibles descomposiciones de n como suma de dos números primos".

Por ejemplo, al ejecutar *goldbach(100)* se obtiene:

$$goldbach(100) = [[3, 97], [11, 89], [17, 83], [29, 7], [41, 59], [47, 53]]$$

Observaciones
Algunos resultados obtenidos de trabajos realizados entorno a esta conjetura son, entre otros, los siguientes:

a) Si *n* es un número impar suficientemente grande, entonces *n* puede expresarse como suma de tres números primos. Se deduce de esto que, cualquier número par suficientemente grande es suma de 4 números primos o menos. [Vinogradov, 1937].

b) Todo número par *suficientemente grande* puede expresarse como suma de un número primo más un entero que tiene dos factores primos. [Chen, 1966].

c) Verificación de la conjetura de *Goldbach* para todos los enteros menores que $4 \cdot 10^{11}$. [Sinisalo, 1993]

d) Todo número par se puede expresar como suma de seis o menos números primos. [Ramaré, 1995].

e) Otra conjetura derivada de la conjetura de Goldbach. **G**: Todo número impar mayor que 5 puede expresarse como la suma de tres o menos números primos.
Notar que, si la conjetura de Goldbach es verdadera, entonces **G** es verdadera. **G** es llamada conjetura de Goldbach impar.

Actividad 3.1
Verificar que la conjetura se cumple para los números n=150 y n=200, presentando para cada número, una sola descomposición como suma de primos.

IV. *Existen infinitos números primos de la forma $n^2 +1$.*

Este problema también es considerado en el grupo de los difíciles de tratar.

Ejemplo. Los primeros números primos de esta forma son: *2, 5, 17, 37, 101, 197, 257, 401,* que corresponden a los valores de *n = 1, 2, 4, 6, 10, 14, 16, 20,* ......

Un resultado parcial obtenido en relación a la conjetura es el siguiente:

Existen infinitos números enteros n tal que n^2+1 se factoriza como producto de a lo más dos factores primos.

Nota

En el archivo *PRIMOS.MTH* se encuentran las funciones:

- *cuad*(n) que entrega los n primeros números primos que son sucesores de un cuadrado perfecto
- *cdn(m)* entrega todos los primos de la forma n^2+1 menores que *m*.

Actividad 4.1

1. Determinar todos los números primos de la forma n^2+1, tal que n sea impar.
2. ¿Existen primos de la forma n^2+1, entre 150 y 200?
3. Sea n mayor que 1. Considerar valores de n tal que n es un cubo perfecto, por ejemplo; n=8. ¿Qué puede decir de n^2+1?

Nota

- Un importante resultado relacionado con la determinación de números primos en una serie de números enteros, se enuncia en el siguiente teorema: "En toda progresión aritmética $(a, a+b, a+2b, a+3b, \ldots)$ siendo a y b primos relativos (o coprimos), existen infinitos números primos". [Dirichlet, 1837].
- La progresión anterior se puede expresar: $s_m = a + bm$ donde $m = 0,1,2,3,4$, etc. o bien, en la forma: $s_m = a + b(m-1)$ donde $m=1,2,3,4,5$, etc.

Actividad 4.2

En la progresión aritmética (3 + 4m) = (3, 7, 10, ...)

1. Encontrar los cinco primeros números primos que aparecen en esta sucesión.
2. De los veinte primeros términos de la sucesión ¿cuántos son primos?, ¿cuáles son esos números primos? y ¿qué lugares ocupan en la sucesión?

Nota. La función DIR3(a,b,n) se encuentra definida en el archivo PRIMOS.MTH. Esta función entrega los n primeros número primos de la progresión aritmética {a + bx /x en IN}

Actividad 4.3

1. Determinar el 100 avo número primo en la sucesión (3 + 4m)
2. Considerar las sucesiones $a_m = 4+7m$ y $b_m = 3+8m$. Se tiene que: existen r, s en IN tal que $a_r = b_s = p$, donde p es primo.
   Verifique esta afirmación, determinando el menor número primo p, que pertenece a ambas sucesiones, y que lugar ocupa este elemento en cada una.

Observaciones

a) Una conjetura de contenido más general es la llamada *Conjetura de Patrones de Primos* cuyo enunciado es: "Sea *S* un conjunto finito de enteros, que no contiene a todos los posibles restos de dividir un entero por algún primo *p*. Se conjetura que, existe un número infinito de enteros *k* tal que *{k+s / s en S}* son primos".

Nota.

- La conjetura de los *primos gemelos* es un caso particular de la conjetura de patrones de primos, basta considerar S={0,2}.

- La conjetura *de patrones de primos,* implica la existencia de conjuntos finitos, con una cantidad arbitraria de elementos, tal que sus elementos están en progresión aritmética y son números primos (progresiones aritméticas de primos).

Ejemplo: (*199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089*) es una progresión aritmética de *10* términos de primos con diferencia *210*.

b) En la determinación de *largos* conjuntos de primos que aparecen en términos consecutivos de una progresión aritmética, y en la determinación de largos conjuntos de primos consecutivos en progresión aritmética, se han realizado varios trabajos.

Ejemplo. Considerar la sucesión: (*11.410.337.850.553 + 4.609.098.694.200 n*), con n = 0, 1,2,3, ... etc., que es una progresión aritmética de números enteros..

Los primeros *23* primeros elementos[6] de esta sucesión son:

[11410337850553, 16019436544753, 20628535238953, 25237633933153, 29846732627353, 34455831321553, 39064930015753, 43674028709953, 48283127404153, 52892226098353, 57501324792553, 62110423486753, 66719522180953, 71328620875153, 75937719569353, 80546818263553, 85155916957753, 89765015651953, 94374114346153, 98983213040353, 103592311734553, 108201410428753, 112810509122953]

Y, al ejecutar DIR3(a,b,23) entrega los 23 primeros números primos de la sucesión.

DIR3*(11410337850553, 4609098694200, 23) =*
[11410337850553, 16019436544753, 20628535238953, 25237633933153, 29846732627353, 34455831321553, 39064930015753, 43674028709953, 48283127404153, 52892226098353, 57501324792553, 62110423486753, 66719522180953, 71328620875153, 75937719569353, 80546818263553, 85155916957753, 89765015651953, 94374114346153, 98983213040353, 103592311734553, 108201410428753, 131246903899753]

se puede observar que los 22 primeros términos de la progresión aritmética son primos [Pritchard et al., 1995].

Hasta el año 1995, este era el conjunto más grande de primos (conjunto de 22 números primos) en progresión aritmética, conocido hasta esa fecha.

Actividad 4.4
Considerar la sucesión estudiada por Pritchard del ejemplo anterior,

[6] Para listar estos elementos se ha ejecutado *VECTOR*(11410337850553 + 4609098694200·n, n, 0, 22) en *DERIVE*.

1. Sabiendo que el siguiente número primo de la progresión dada es el número *131246903899753*. ¿Qué lugar ocupa en la sucesión?.
2. ¿Qué se puede afirmar respecto del 23 avo término de la sucesión dada?.

Nota

Otras funciones que se encuentran definidas en *PRIMOS.MTH* son:

- *DIR4(a,b,n)* que entrega los n primeros números primos de la progresión aritmética {a + bx / x en IN}
- *DIR5(a,b,n)* que entrega todos los elementos que son números primos de entre los n primeros términos de la sucesión

Observaciones

a) La sucesión más *larga* de <u>primos consecutivos</u> y <u>en progresión aritmética</u> encontrada hasta el año 1998 contiene *10* términos [Dubner, Forbes, Toplic, 1998]..

b) El más "*pequeño*" conjunto con seis primos consecutivos y en progresión aritmética corresponde al formado por los seis primeros términos de la sucesión: 121174811+30n

V. *Existe al menos un número primo entre n^2 y $(n + 1)^2$.*

Al igual que el problema anterior, esta conjetura es considerada difícil de probar o de refutar.

Ejemplo

Los primos más pequeños entre n^2 y $(n+1)^2$ para $n = 1, 2, 3, 4, 5, 6, ...,$ son *2, 5, 11, 17, 29, 37, 53, 67, 83, ...*

Observaciones

Algunos resultados parciales obtenidos son:

a) Para todo número entero P que es primo o se factoriza como producto de dos primos (semiprimo) existe un entero n tal que $n^2<P<(n+1)^2$. [Chen, 1975]

b) Dado un entero positivo n. Siempre existe un número primo p entre $n\text{-}n^k$ y n, donde $k=23/42$.

Ejemplo: Para n=10, $10 - 10^{23/42} = 6.471264979$, existe p=7

Nota.

- En el archivo PRIMOS.MTH se encuentra definida la función *entre(n)* que entrega todos los números primos entre n^2 y $(n+1)^2$.

Ejemplo. Al ejecutar *entre(15)* se obtienen todos los números primos entre 15^2 y 16^2: *entre(15)=[227, 229, 233, 239, 241, 251]*

Nota

- Un problema algo más simple que el anterior, es la conjetura de *Bertrand*: "existe al menos un número primo entre *n* y *2n*".
  Esta dejó de ser conjetura, al ser probada por *Chebyshev* (1821-1894), incorporándose como una nueva proposición en la teoría de los números.
- En el archivo *PRIMOS.MTH* se encuentra implementada la función: *bertrand(n)* que entrega todos los números primos entre *n* y *2n*.

VI. *Existen infinitos números perfectos.*

Un entero positivo *n* es un *número perfecto*[7], si y solo si, la suma de todos sus divisores positivos es *2n*.

Por ejemplo: *6* es un número perfecto (el primer número perfecto) ya que los divisores positivos de *6* son *1, 2, 3, 6,* y la suma de ellos es $1+2+3+6=12=2*6$.

Actividad 6.1
Determinar todos los números perfectos menores que *100*.

Observaciones

a) El estudio de los números perfectos tiene relación con una clase especial de números primos, como se verá más adelante.

b) Euclides probó que si $2^n - 1$ es primo, entonces, el número $2^{n-1}(2^n - 1)$ es un número perfecto. Notar que sustituyendo *n* por *2*, se obtiene el número perfecto *6*.

c) Muy posterior a esta época, *Euler* (en 1747) demostró que, todo número perfecto par es de la forma $2^{n-1}(2^n - 1)$, donde $2^n - 1$ es un número primo.

   Por lo tanto, de existir infinitos números primos de esta forma, existirían infinitos números perfectos pares, y por ende infinitos números perfectos.

d) Una propiedad muy interesante de los números perfectos es la siguiente:

   La suma de los recíprocos (inversos multiplicativos) de los divisores positivos de un número perfecto es *2*.

Nota.

- En el archivo *NUMBER.MTH* de *DERIVE* se encuentra definida la función *perfect(n)* que entrega el *n-ésimo* número perfecto (sólo hasta el 38-avo número perfecto).

Actividad 6.2
Verificar el resultado anterior para el número perfecto $n=6$, y luego para n=28.

---

[7] Los números perfectos fueron presentados por Euclides en su obra Elementos

Actividad 6.3

a) Sea *n un número perfecto.* Determine la suma de todos los divisores de n

b) Sea *n un entero que se descompone como producto de dos números primos (considere los siguientes casos: (caso 1): es decir, $n=p^2$. (caso 2): $n=pq$, donde* p y q son primos distintos. Para cada caso, calcule la suma de todos los divisores de *n* y luego determine todos los números de esa forma que son perfectos, si es que existen.

Observaciones

a) Una de las conjeturas más antiguas relacionadas con números perfectos, que en nuestros días se ha convertido en interrogante es: ¿Existen números perfectos impares?

b) Una conjetura que directamente daría respuesta a la interrogante sobre números perfectos impares es la *Conjetura de Ore*.

PREVIO 1: Dado un entero positivo n. Se define el medio armónico de los divisores de *n* como: $H(n)=\dfrac{t}{\dfrac{1}{d_1}+\dfrac{1}{d_2}+\cdots+\dfrac{1}{d_t}}$ siendo t el número de divisores positivos de *n*, y $d_1, d_2, ..., d_t$ los *t* divisores positivos de *n*

PREVIO 2: El siguiente teorema relaciona este número con números perfectos: "si *n* es perfecto entonces *H(n)* es un número entero".

Ejercicio: Ilustrar este teorema para los números perfectos 6 y 28.

Conjetura de Ore: "si *n* es impar, entonces *H(n)* no es un entero".

c) De ser cierta la conjetura de Ore, no existirían números perfectos impares.

Notas

- En el texto *Teoría de los Números*, cuyo autor es Peter Barlow, escrito en 1811, en una de páginas aparece lo siguiente; el número "$2^{30}(2^{31}$-1) es el más grande número perfecto descubierto hasta la fecha". ¡Qué maravilla!. En primer lugar, dicho número es perfecto, y en segundo lugar, es destacable que, sin apoyo de tecnología se había probado que el número $2^{31} - 1 = 2147483647$ era primo.
- Los números perfectos pares están muy relacionados con los números primos de Mersenne.

VII. Existen infinitos números primos de Mersenne.

Los números de la forma 2^n*-1* fueron estudiados por *Mersenne*[8] (1588-1648), y son denominados números de Mersenne.

[8] *Marin Mersenne,* monje francés (siglo XVI).

Los números primos de la forma 2^n-1, son llamados *números primos de Mersenne*[9].

La conjetura que data desde entonces es: "el número de *primos* de *Mersenne* es infinito".

Nota.

- La siguiente proposición es verdadera: Si el número de Mersenne $M_n = 2^n-1$ es primo entonces n es un número primo.
  En efecto, si n es compuesto, entonces existen enteros positivos a, b tal que $n=ab$ y $1<a<b<n$. Luego, $2^n-1=2^{ab}-1=(2^a)^b-1=(2^a-1)(2^b+2^{b-1}+ \ldots +1)$, *y por lo tanto* 2^n-1 *sería* compuesto.
- Esta proposición establece que: el conjunto de números primos de Mersenne es subconjunto de $\{2^p - 1$ / p es primo$\}$.

Observaciones

a) Si se denota por *Mersenne(i)* al i-ésimo número primo de *Mersenne*, los seis primeros son:
   Mersenne(1) $= M_2 = 3$ *Mersenne(4)* $= M_7=127$
   Mersenne(2) $= M_3 = 7$ *Mersenne(5)* $= M_{13} = 8191$
   Mersenne(3) $= M_5 = 31$ *Mersenne(6)* $= M_{17}=131071$

b) El número de Mersenne $M_{11} = 2^{11} - 1$ no es primo [año 1536].
   Se puede verificar sin mucha dificultad, a mano o asistido por una calculadora o por *DERIVE* esta afirmación. ¿Qué nos dice esta afirmación?

c) A medida que crece el exponente n, los números de la forma $2^n - 1$ son muy grandes, y por tanto difícil de determinar si son primos o compuestos.

   A continuación se presentan algunos datos relacionados con el descubrimiento de números primos de *Mersenne* a través de la historia:

   ⇒ Los primos de *Mersenne*, el sexto y el séptimo: M_{17} y M_{19} fueron descubiertos por *Cataldi* en el año 1588 (en aquella época no eran llamados primos de Mersenne). Aproximadamente *200* años más tarde, Euler descubrió el octavo primo de Mersenne: M_{31}.

   ⇒ El 12 avo primo de *Mersenne* (un número con *39* dígitos) fue descubierto por *Lucas,* en el año 1876: *Mersenne(12)* $= M_{127} = 2^{127} - 1$

   ⇒ En 1952, con apoyo de tecnología computacional, Robinson probó que los números M_{521}, M_{607}, M_{1279}, M_{2203} y M_{2281} eran números primos. Así, hasta ese año se tenía conocimiento de los primeros 17 números primos de Mersenne.

   ⇒ En 1979 se encontró el 27 avo número de Mersenne. Este número consta de 13395 dígitos: *Mersenne(27)* $= M_{44497} = 2^{44497} - 1$

[9] Un número entero positivo es *primo de Mersenne* si y solo si, es un número de Mersenne que es primo.

Actividad 7.1
Si se escribiera *Mersenne*(*27*) en un cuaderno de papel cuadriculado, de *24* cuadraditos de ancho por *32* cuadraditos de largo, y un dígito por cuadradito ¿cuánto ocuparía aproximadamente, la escritura de este número en el cuaderno?

⇒ En 1992, en un artículo del boletín de la Asociación Matemática de Estados Unidos se publicó el descubrimiento del 32 avo primo de *Mersenne*.

⇒ Hasta el año 1998 se habían descubierto *37* números primos de Mersenne en total. El más grande de todos era $M_{3.021.377}$ con *909526* dígitos.

⇒ El 1 de Julio de 1999, se encontró el 38 avo número de Mersenne:

$$M(38) = M_{6.972.593} = 2^{6.972.593} - 1$$

d) Algunas interrogantes relacionadas con los números de Mersenne son:

- ¿Existen números primos doble-Mersenne?
  Un primo es doble-Mersenne es un primo Mersenne M_p tal que $p=M_n$ es un número primo de Mersenne.
  Por ejemplo, $M_{M_2} = M_3 = 2^3 - 1 = 7$ es un número primo *doble-Mersenne*. También lo son: M_7, M_{31}, M_{127}. Sin embargo, $M_{M_{13}} = M_{8191}$ es compuesto.
- ¿Hay infinitos números de Mersenne compuestos?

Nota
El archivo *NUMBER.MTH*, del programa *DERIVE,* contiene la función Mersenne(n) que entrega el n-ésimo número primo de Mersenne, para n menor o igual que *38*.

Por ejemplo, *MERSENNE(10) = 618970019642690137449562111*

Actividad 7.2
1. Probar que M_{67} no es primo (Sugerencia: *193707721* es uno de sus factores).
2. Determinar los cinco primeros números perfectos.

VIII. *Existen infinitos números primos de Fermat.*

Pierre de Fermat[10] (1601-1665), se interesó por estudiar los números enteros de la forma 2^m+1.

Fermat conocía la proposición: "si 2^m+1 es primo entonces m debía ser una potencia de *2*".

En una de sus cartas enviada a Mersenne, Fermat estableció la siguiente conjetura:

"si m es una potencia de 2, entonces 2^m+1 es primo"

[10] Pierre de Fermet, matemático francés, siglo XVII, contemporáneo de Mersenne.

Los números enteros de la forma $F_n = 2^{(2^n)} + 1$ son llamados números de *Fermat*, y los números primos que son de esta forma, se denominan *números primos de Fermat*[11].

Nota.

- Fermat verificó la conjetura planteada para *n= 0, 1, 2, 3 y 4*.
- Alrededor de cien años más tarde, *Euler* (1732) demostró que para *n=5*, el número de Fermat $F_5 = 2^{(2^5)} + 1 = 2^{32} + 1$ es divisible por *641*. *E*s decir, este número de Fermat no es primo, refutando la conjetura de *Fermat*.

Actividad 8.1

Euler [2]. probó que, $(1+ab)a^4 + 1 - a^4b^4 = F_5$ cuando a=2^7, b=5. Verificar que esta expresión permite probar que F_5 no es primo, y determine la factorización completa de este número de Fermat.

Observaciones

a) Posteriormente la conjetura fue reformulada, con el siguiente enunciado: "*Existen infinitos números primos de Fermat*".

b) Con el transcurrir de los años, la siguiente interrogante ha tomado un lugar especial: "¿Existe algún número de Fermat F_n que sea primo, aparte de los cinco ya encontrados?", debido principalmente a que se han encontrado muchos números de Fermat compuestos, y fuera de los cinco primos encontrados no se ha descubierto ninguno nuevo. Actualmente se ha reformulado la conjetura de Fermat como sigue: "Existe un número finito de primos de Fermat".

c) Existe una interesante relación entre los números primos de *Fermat* y un gran problema de geometría: construcciones de polígonos regulares utilizando exclusivamente regla y compás. *Gauss* (1796) probó que si F_n es primo entonces el polígono regular con F_n lados puede ser construido sólo con regla y compás. Posteriormente demostró, que un polígono regular de m lados es constructible usando sólo regla y compás, si y solo si, $m=2^s F_1 F_2 \ldots F_t$ siendo s mayor o igual que *0*, y los factores $F_1, F_2, \ldots, F_t$ son primos de Fermat distintos.

Actividad 8.2

Sea P un polígono regular con n lados, siendo n un número impar.

1. Nombrar siete de tales polígonos tal que P puede construirse utilizando solamente regla y compás.
2. Considerando los números primos de Fermat descubiertos hasta la fecha, ¿cuántos valores puede tomar n, tal que P puede construirse utilizando solamente regla y compás?

---

[11] Un número entero positivo es <u>primo de Fermat</u> si y solo si, es un número de Fermat que es primo.

Actividad 8.3
Uno de los teoremas demostrados por *Fermat* es: "Todo número primo impar se puede expresar de una única manera como la diferencia de dos cuadrados". Ilustrar este teorema para los cinco primeros enteros impares.

Complemento.

Una de las grandes riquezas de la teoría de los números es la cantidad de problemas abiertos que existen en diferentes temáticas, Muchas de las conjeturas que han sido propuestas, han dejado de serlo debido a que han sido demostradas o refutadas,

Una de las más famosas es *"El Último Teorema de Fermat*", establecido como teorema por *Pierre de Fermat*(1601-1665). Este *problema* atrajo la atención y dedicación de grandes matemáticos durante los últimos siglos (400 años aproximadamente). Fue demostrado por *Andrew Wiles (1953-*, Cambridge, Inglaterra) y su demostración se encuentra en el trabajo *Modular elliptic curves and Fermat's Last Theorem*, publicado en los Annals of Mathematics, año 1995.

A continuación se mencionan otros problemas relacionados con números primos, que se encuentran abiertos hasta el momento:

a) Todo entero múltiplo de 6 puede expresarse como la diferencia de dos números primos.
b) ¿Existen infinitas **ternas** de primos consecutivos en progresión aritmética?
c) ¿Existen infinitos números primos de la forma $n!+1$?
d) ¿ Existen infinitos números primos de la forma $n!-1$?
e) ¿Existen infinitos números primos en la sucesión (a_n), donde $a_n=n^2-n+41$?.
f) ¿Existen infinitos números primos en la sucesión (b_n) donde $b_n= n^2-79n+1601$*?*
g) ¿Es infinito el número de primos en la sucesión de *Fibonacci* ?

Actividad 9.1
Determinar los cincuenta primeros números primos de la sucesión $a_n=n^2-n+4$, y el lugar que ocupan. Si se cuenta con el programa *DERIVE* (u otro), realizar la siguiente actividad; de los quinientos primeros elementos de esta sucesión, ¿cuántos son primos? Y ¿qué lugar ocupa el último de estos primos en la sucesión?. Idem, al considerar los mil primeros elementos.

Comentarios Finales

Como el título de este trabajo lo señala, se han presentado algunas conjeturas e interrogantes relacionadas con números primos. Cabe señalar que existe bastante literatura al respecto, especialmente en diversos sitios web que se actualizan periódicamente

Uno de los principales propósitos de este trabajo ha sido, mostrar el estado de avance de algunos famosos problemas de la teoría de los números y como las herramientas computacionales, especialmente los software de propósitos matemáticos, como el programa *DERIVE* por ejemplo, se constituyen en un poderoso recurso que permiten complementar un estudio formal de la teoría involucrada.

Bibliografía

[1] Hardy, G.H. and Wright, E.M. *Introduction to the Theory of Numbers*, 3rd edition. Oxford, Clarendon Press, 1954.
[2] Hua, L. K. *Introduction to Number Theory*. Springer-Verlag. Berlin Heilderberg New York. 1982
[3] Ore, O. *Number Theory and Its History*, New York, McGraw.Hill, 1949.
[4] Stewart, B.M. *Theory of Numbers*. The MacMillan Company, New York. 1965.
[5] Uspensky, J.V. and Heaslet, M.H. *Elementary Number Theory*, New York, McGraw-Hill, 1939.
[6] http://www.utm.edu/research/primes/notes/conjectures/
[7] http://venus.mathsoft.com/asolve/constant/hrdyltl/goldbach.html
[8] http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Prime_numbers.html
[9] http://mathworld.wolfram.com/topics/UnsolvedProblems.html

Nota: En caso que lo requiera, solicitar archivo *PRIMOS.MTH* a las direcciones electrónicas mencionadas.