ALGUNOS TÓPICOS EN TEORÍA DE NÚMEROS: NÚMEROS MERSENNE, TEOREMA DIRICHLET, NÚMEROS FERMAT.

Some topics in number theory: Mersenne numbers, Dirichlet's Theorem, Fermat Numbers.

RESUMEN
En esta parte hacemos un breve estudio de los números de Mersenne, encontramos una relación importante en su forma en lo que hemos denominado zoom y después hacemos una relación sencilla con los números de Fermat. Después estudiamos el teorema de Dirichlet y simplificamos su forma.

PALABRAS CLAVES: Primo de Mersenne, Fermat, teorema Dirichlet.

CAMPO ELIAS GONZALEZ PINEDA
Mg. Matemáticas,
Profesor Asociado
Universidad Tecnológica de Pereira
cegp@utp.edu.co
SANDRA MILENA GARCIA
Lic Matemáticas y Física,
Profesor Auxiliar
Universidad Tecnológica de Pereira
Junio13san@hotmail.com

ABSTRACT
This part is a brief study of Mersenne numbers, we found an important relationship in your way in what we call the zoom and then make a simple relation with Fermat numbers. Then we study the Dirichlet theorem and simplified form..

KEYWORDS: *Dirichlet's theorem, Mersenne prime, Fermat*

1. INTRODUCCIÓN

La Teoría de Números bien conocida como la reina de las Matemáticas tiene diversidad de problemas aún sin resolver y diversidad de aplicaciones nuevas que influyen casi todas las áreas del conocimiento. Aunque hay muchos teoremas y resultados ya conocidos como lo es el Teorema de Dirichlet y los números de Mersenne aún se puede decir más acerca de ellos. Cada día resultan nuevos resultados que aclaran o mejoran el entendimiento de un teorema o un procedimiento. Precisamente en este artículo presentamos un estudio breve del teorema de Dirichlet y resumimos su forma. También hacemos un detallado estudio de los números de Mersenne y generalizamos el teorema que encontró Fermat respecto de los números de Mersenne. También escribimos una breve relación entre los números de Mersenne y de los de Fermat.

2. CONTENIDO

2.1. EL TEOREMA DE DIRICHLET Y SUS CONSECUENCIAS.

Recordemos que el teorema de Dirichlet, dice que si m.c.d $\{a, b\} = 1$, la sucesión $p(n) = a + bn$ contiene infinitos números primos, de hecho el caso $4n + 1$ y $4n - 1$ son casos particulares que se pueden demostrar relativamente fácil. Del teorema de Dirichlet podemos ver que hay infinitos números primos de la forma:

1. $pn + 1$ donde p es un número primo.
2. $p^t n + 1$ donde p es un numero primo y t un entero positivo.
3. $4pn + 1$ donde p es un número primo.
4. $(p_1 \cdot p_2 \cdots p_t)n + 1$ donde p_i es un número primo.
5. $pm + q$ donde p, q son números primos.
6. si p es primo y no es factor de 10^l, $10^l m + p$
7. $4p + 1$ con p primo. Nótese que $((4,1)) = 1$ y $pm + 1$ debe ser impar por lo que m es par, en este caso $m = 4$. En general existen infinitos primos de la forma $2tp + 1$ con p primo. Un resultado similar se tiene para $2tp - 1$.

2.1.1 Zoom Al Teorema De Dirichlet.

Para comenzar nuestro estudio es conveniente enunciar un resultado que nos muestra una interesante propiedad de la suma de números impares.

Teorema 2.1.

1. Sean a, c enteros impares positivos entonces;
   a. $\frac{a+c}{2}$ es par si y solo si $\frac{a-c}{2}$ es impar.
   b. $\frac{a+c}{2}$ es impar si y solo si $\frac{a-c}{2}$ es par.

2. Si a, c son pares $\frac{a+c}{2}$ y $\frac{a-c}{2}$ tiene la misma paridad.

Demostración. Se propone como ejercicio.

Sean a, b enteros positivos primos relativos. Hagamos

$$P(m) = a + bm \quad (1)$$

Fecha de Recepción: 12 de Mayo de 2011
Fecha de Aceptación: 29 de Agosto de 2011

Sabemos por el Teorema de Dirichlet que (1) contiene infinitos números primos. Una observación detallada de la ecuación (1) nos permite enunciar lo siguiente.

Teorema 2.2. En la ecuación (1) es suficiente considerar a impar y b par y $a < b$.

Demostración. Consideremos las siguientes situaciones:

1. a, b no pueden ser pares simultáneamente.
2. Si a es par y b impar, m tiene que ser impar. Sea $m = 2t + 1$ entonces,

$$\begin{aligned} P(t) &= a + b(2t + 1) \\ &= a + 1 + 2bt \\ &= a' + b't \end{aligned}$$

Donde a' es impar y b' par.

3. a impar y b impar. En este caso m tiene que ser par, sea $m = 2t$, luego,

$$\begin{aligned} P(t) &= a + b(2t) \\ &= a + 2bt \\ &= a + b't \end{aligned}$$

Donde b' es par.

Así todas las posibilidades conducen a que a es impar y b par. Si $a > b$ por el algoritmo de la división tenemos

$$a = bq + r, \qquad 0 \leq r < b$$

Por lo que

$$p(m) = bq + r + bm = b(m + q) + r$$

Nótese que r es impar. Esto completa la prueba.

Ejemplo 2.1.

1. La sucesión $p(t) = 2t + 1$ contiene todos los números primos impares.

2. Todo primo impar se encuentra en la sucesión $p(m) = 4m + 1$ o en la sucesión $p(n) = 4n - 1$

Para completar el análisis de la ecuación (1) basta considerar ahora el caso $\frac{b}{2}$ par y $\frac{b}{2}$ impar. Sin embargo nótese que m puede ser par o impar.

Hagamos $p(m) = a + bm, \quad p(n) = c + bn$ (supondremos siempre $a < b$, a impar, b par). Consideremos los siguientes casos

$\frac{a+c}{2}$ par y $b = 4t$. En este caso.

$$\mathrm{P} = \frac{p(m)+p(n)}{2} = \frac{a+c}{2} + \frac{b(m+n)}{2} = \frac{a+c}{2} + 2t(m+n)$$

$$\mathrm{I} = \frac{p(m)-p(n)}{2} = \frac{a-c}{2} + \frac{b(m-n)}{2} = \frac{a-c}{2} + 2t(m-n)$$

Donde P es par e I impar. Es importante resaltar que

$$P + I = p(m), \qquad P - I = p(n), \qquad 2P = p(m) + p(n)$$

En este caso m, n pueden ser pares o impares.

2. $\frac{a+c}{2}$ par y $b = 4t + 2$. En este caso.

$$P = \frac{p(m)+p(n)}{2} = \frac{a+c}{2} + \frac{b(m+n)}{2} = \frac{a+c}{2} + (2t+1)(m+n)$$

$$I = \frac{p(m)-p(n)}{2} = \frac{a-c}{2} + \frac{b(m-n)}{2} = \frac{a-c}{2} + (2t+1)(m-n)$$

Si queremos que P sea par y por tanto I impar entonces m, n tiene que ser pares a la vez o impares a la vez.

3. $\frac{a+c}{2}$ par y $b = 4t + 2$, Pero, $m + n$ es impar entonces,

$$I = \frac{p(m)+p(n)}{2} = \frac{a+c}{2} + \frac{b(m+n)}{2} = \frac{a+c}{2} + (2t+1)(m+n)$$

$$P = \frac{p(m)-p(n)}{2} = \frac{a-c}{2} + \frac{b(m-n)}{2} = \frac{a-c}{2} + (2t+1)(m-n)$$

Con I impar y P par. Si $m = 2q, n = 2h + 1$ entonces, $p(m) = a + 4(2t + 1)q$, $p(n) = a + b + 4(2t + 1)h$.

4. Un análisis similar se tiene cuando $\frac{a+c}{2}$ es impar. Se deja al lector.

Ejemplo 2.2.

1. El caso especial ocurre cuando $p(m) = 4m \pm 1$, $p(n) = 4n \pm 1$. Para el primer caso

$\mathrm{p}(m) + p(n) = 4(m + n) \pm 2$ luego,

$$\mathrm{I} = \frac{p(m)+p(n)}{2} = 2(m+n) \pm 1$$

$$\mathrm{P} = \frac{p(m)-p(n)}{2} = 2(m-n).$$

2. Sean $p(m) = 4m + 1$, $p(n) = 4n - 1$ entonces,

$$\mathrm{P} = \frac{p(m)+p(n)}{2} = 2(m+n)$$

$$\mathrm{I} = \frac{p(m)-p(n)}{2} = 2(m-n) + 1.$$

3. Podemos hacer $p(m) = 2m + 1$, $p(n) = 2n - 1$ y este incluye los dos casos anteriores.

Del estudio anterior podemos enunciar la siguiente conjetura que equivale a la conjetura de Golbach:

Conjetura: Para todo P par (impar) mayor o igual 4(5), existe un impar (par) I de tal manera que

$$P + I = P_1, \qquad P - I = P_2$$

Donde P_1, P_2 son números primos.

2.2 Números de Mersenne

En esta parte hacemos un breve estudio de los números de Mersenne, especialmente aquellos que son primos y deduciremos algunos resultados relativos a ellos.

Para comenzar nuestro estudio consideremos el siguiente resultado elemental de la teoría de Números.

1. Todo impar I es de la forma $4n + 1$ o de la forma $4n - 1$.

2. Existen infinitos primos de la forma $4n + 1$ e infinitos de la forma $4n - 1$.

3. Todo primo impar o es de la forma $4n + 1$ o de la forma $4n - 1$ pero no de ambas a la vez.

4. Si a, b son primos relativos entonces $p(n) = a + bn$ contiene infinitos primos.

La demostración del resultado anterior se deja como consulta para el lector. Sin embargo, hacemos notar que el caso 1) es una simple consecuencia del algoritmo de la división. Como todo primo distinto de 2 es impar, se deduce que todo primo es de la forma indicada en 1). De aquí se deduce inmediatamente que existen infinitos primos de la forma $4m + 1$ o de la forma $4n - 1$ (¿por qué?) Sin embargo la parte 2) se puede demostrar de manera relativamente fácil. Es claro que el literal 2) es un caso particular de 4) el cual es llamado Teorema de Dirichlet quien lo demostró en el año1837 utilizando herramientas de la variable compleja. Recordemos que los números de Mersenne tienen la forma.

$$Mp = 2^p - 1 = q \quad (2)$$

La expresión (2) puede escribirse como

$$2^p - 1 = q \Leftrightarrow 4(2^{p-2}) - 1 = q$$

Es decir, todo primo de Mersenne es de la forma $4k - 1$. Dividiendo q entre p cuando q es primo vemos que $q = pl + 1$, resultado cierto que probaremos más adelante. Es decir,

$$2^p - 1 = pl + 1 \quad (3)$$

El resultado dado en (3) fue probado por Fermat. Es importante recordar que el hecho de que p sea primo no implica que M_p sea primo, el caso trivial es $2^{11} - 1 = 2047 = (23)(89)$. Nosotros generalizaremos este resultado. En la ecuación anterior podemos escribir

$$pl = 2^p - 2$$

Como $2^p - 2$ es par y p es primo impar, entonces l tiene que ser par. Sin embargo, $\frac{l}{2}$ es impar, puesto que

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

Podemos definir

$$l(p) = \frac{2^p - 2}{p}$$

Por ejemplo, $l(11) = \frac{2046}{11} = 186$. Resumiendo tenemos, para p primo impar

1. $2^p - 1 = pl + 1$

2. l es par.

3. $\frac{l}{2}$ es impar.

Podemos por ahora enunciar el siguiente resultado el cual demostraremos en esta parte.

Teorema 2.3

1. Sea p un número primo.

a) Sea $2^p - 1 = q$. Si q es primo entonces $2^p - 1 = pl + 1$

b) $pDq - 1$

c) $l(p) = \frac{2^p - 2}{p}$ es un número par para cada primo p Además, $l(p)$ es divisible por 2 y 3. Es decir, por 6.

d) Si M_p es primo entonces, $2^p - 1 = 6pl_1 + 1$ con l impar.

2. Ningún primo de la forma $4t + 1$ es de un primo de Mersenne.

3. Ningún primo de la forma $4t - 1$ con t impar es de un primo de Mersenne.

4. Ningún primo de la forma $6pl + 1$ con l par es primo de Mersenne

5. Ningún primo de la forma $4t - 1$ con t par que tenga divisores distintos de potencias de dos es de un primo de Mersenne.

6. Los primos de Mersenne son escasos al comparar con el número de primos.

7. Todo número primo de Mersenne distinto de 3 termina en 1 o en 7. Más aún, $2^p - 1$ con p impar termina en 1 o en 7.

p	2^p-1	$l(p)=\frac{2^p-2}{p}$	$4k-1$
2	3	1	$4(1)-1$
3	7	2	$4(2)-1$
5	31	6	$4(8)-1$
7	127	18	$4(32)-1$
13	8191	630	$4(2048)-1$
17	131071	7710	$4(32768)-1$
19	524287	27594	$4(131072)-1$
31	2147483647	69273666	$4(536870912)-1$

Para una demostración sencilla de la parte dos del teorema anterior, recordemos que

$$a \equiv b(modm) \Leftrightarrow mD(a-b)$$

Donde D significa divide. De aquí se deduce fácilmente que el residuo de dividir a entre m es igual al residuo de dividir b entre m. Esto lo denotamos

$$res\left(\frac{a}{m}\right) = res\left(\frac{b}{m}\right)$$

Si φ es la función fi de Euler, tenemos el teorema de Fermat cuya demostración puede consultarse en cualquier libro de Teoría de Números,

Teorema 2.4. *Si el máximo común divisor entre a y m es* 1 *entonces,*

$$a^{\varphi(m)} \equiv 1(mod\ m)$$

En particular si p es primo $\varphi(p) = p-1$, luego $a^{p-1} \equiv 1(mod\ p)$. Si hacemos $a = 2$ encontramos.

$$pD(2^{p-1}-1) \Leftrightarrow pl_1 = 2^{p-1}-1 \Leftrightarrow p(2l_1) = 2^p - 2$$
$$\Leftrightarrow pl + 1 = 2^p - 1$$

Veamos por qué $l(p)$ es divisible por 6. En primer lugar tenemos,

Teorema 2.5. $a^{2n}-1$ es divisible por $a+1$ y por $a-1$

Demostración. La prueba es por inducción. Hagamos $P(n) = a^{2n}-1$. El resultado es cierto para $n = 1$. En efecto, pues $P(1) = a^2 - 1 = (a+1)(a-1)$. Supongamos que $P(n) = a^{2n}-1$ es cierta. Ahora:

$$P(n+1) = a^{2n+2} - 1 = a^{2n}(a^2 - 1 + 1) - 1$$
$$= a^{2n} - 1 + a^{2n}(a^2 - 1)$$

Y el resultado es cierto para $n+1$.

Como caso particular $2^{2n}-1$ es divisible por tres. Del teorema anterior tenemos que.

$a^{2n}-1 = l(a+1)(a-1) \leftrightarrow a^{2n+1} - a =$
$la(a+1)(a-1)$.

Pero sabemos que el producto de tres enteros consecutivos es divisible por 6. Por tanto $(a-1)\ (a)\ (a+1)$ es divisible por 6 y podemos escribir entonces,

$$a^{2n+1} - a = l_1(a+1)(a-1) = l_2 \cdot 6l_1 = 6l$$

Ejemplo 2.3.

1. $2^{2n}-1$ es divisible por 3.
2. $2^{2n+1}-2$ es divisible por 6.
3. $l(p) = \frac{2^p-2}{p}$con primo impar es divisible por 6.
4. $2^{2n+k} - 2^k$ es divisible por $2^k.3$.
5. En general $a^{2^r n}-1$ es divisible por a^2-1.
6. Como $a^{2n}-1 = (a-1)(a^{2n-1}+a^{2n-2}+\cdots+1) = k(a+1)(a-1)$ entonces vemos que
$a^{2n-1}+a^{2n-2}+\cdots+1$ es divisible por $a+1$.
7. Para todo entero $a \geq 2$ el numero $4(a^{2n-2})-1$ no es primo puesto que es divisible por 3.
8. En conclusión todo primo de Mersenne es de la forma $2^p - 1 = 6pl + 1$, donde p es primo y l es impar.

Recuérdese que en general $a^n - 1$ es primo si y solo si $a = 2$.

2.2.1. Zoom de los números de Mersenne

En esta parte hacemos un zoom de los números de Mersenne, es decir, penetraremos hasta lo más profundo de estos números. Para tal efecto, consideremos una vez más la identidad:

$$a^{2n}-1 = (a-1)(a^{2n-1}+a^{2n-2}+\cdots+1)$$
$$= l_1(a+1)(a-1)$$

De donde concluimos

$$a^{2n}-1 = l_1 a(a+1)(a-1) + a - 1$$
$$= (a-1)[l_1 a(a+1)+1]$$

En particular si $a = 2$ se obtiene

$$2^{2n+1} - 1 = 6l_1 + 1 = 2(3l_1) + 1 = 3(2l_1) + 1$$

Nótese que l_1 es impar, lo cual se deduce del hecho $6l_1 + 1 = 4k - 1 \rightarrow 3l_1 = 2k - 1$.

Más aún

$$l_1 = \frac{2^{2n+1} - 2}{6} = \frac{2^{2n} - 1}{3}$$

Pero l_1 es impar, $l_1 = 2t_1 + 1$ es decir,

$$t_1 = 2t_2, \qquad t_2 = \frac{2^{n-2} - 1}{3}$$

Luego,

$$l_1 = 2t_1 + 1 = 2^2 t_2 + 1, \quad t_2 = \frac{2^{n-2} - 1}{3}$$

Pero t_2 es impar por ser división de impares, luego $t_2 = 2t_3 + 1$. Ósea

$$t_3 = 2\left[\frac{2^{n-1} - 1}{3}\right]$$

Así tenemos,

$$l_1 = 2^2 t_2 + 1 = 2^2(2t_3 + 1) + 1$$
$$= 2^2(2^2 t_4 + 1) + 1$$
$$= 2^4 t_4 + 2^2 + 1, t_4 = \frac{2^{n-4} - 1}{3}$$

Pero $t_4 = 2t_5 + 1$, ósea

$$2t_5 = 2^2\left[\frac{2^{n-6} - 1}{3}\right]$$

Y así,

$$l_1 = 2^4(2t_5 + 1) + 1 = 2^4(2^2 t_6 + 1) + 2^2 + 1$$
$$= 2^6 t_6 + 2^4 2^2 + 1, t_6 = \frac{2^{n-6} - 1}{3}$$

Siguiendo el proceso obtenemos la formula

$$l_1 = 2^{2i} t_{2i} + 2^{2i-2} + 2^{2i-4} + \cdots + 2^2 + 1, t_{2i}$$
$$= \frac{2^{n-2i} - 1}{3}$$

Pero el proceso debe terminar y ocurre cuando $2i = 2n$ y encontramos que

$$l_1 = 2^{2n-2} + 2^{2n-14} + 2^{2n-6} + \cdots + 2^2 + 1$$
$$= \frac{2^{2n-1} + 2^{2n-2} + 2^{2n-3} + \cdots + 2^2 + 2 + 1}{3}$$

$$= \frac{2^{2n+1} - 2}{6} = \frac{2^{2n} - 1}{3}$$

Así tenemos que para $p = 2n + 1$ primo impar

$$2^{2n+1} - 1 =$$
$$6\lfloor 2^{2n-2} + 2^{2n-4} + 2^{2n-6} + \cdots + 2^2 + 1 \rfloor + 1$$

Más aun tenemos

$$\frac{2^{2n-2} + 2^{2n-4} + 2^{2n-6} + \cdots + 2^2 + 1}{2n + 1}$$

Es un entero impar. Esto se deduce del hecho

$$2^{n+1} - 1 = 6l_1 + 1 = 6pl + 1$$

3. La función C.E.G.P.

En esta parte definimos una función que nos ilustrará respecto a los números de Mersenne.

Definición3.1. *Definamos $w(p,k) = 2^P - 1 - 2k$ donde P es un número impar.*

Observemos que para p primo y $k = 0$ nos da los números de Mersenne. Dos casos particulares de esta función son

1. Si p es primo $w_1(p,k) = 2^p - 1 - 2k = pl + 1 - 2k$.
2. Si p no es primo $w_1(p,k) = 2^p - 1 - 2k = pl + 7 - 2k$.

Según lo visto en el apartado anterior.

Una simple observación muestra que los números $w(4t + 3, k), t \in \{0,1,2,\ldots\}$terminan en la misma cifra.

De igual forma los números $w(4t + 1, k), t \in \{1,2,\ldots\}$ terminan en la misma cifra. En efecto, para probar esto observemos las potencias de dos:

$$\begin{pmatrix} 2\downarrow & 2^3\downarrow & 2^5\downarrow & 2^7\downarrow & 2^9\downarrow & 2^{11}\downarrow & 2^{13}\downarrow \\ 2 & 8 & 32 & 128 & 512 & 2048 & 8192 \end{pmatrix}$$

Vemos que las potencias impares de dos terminan en 2 y 8 de manera intermedia. Como los números impares forman una sucesión aritmética podemos escribir lo siguiente:

$$a_t = 3 + 4(t-1) = 4t - 1, b_t = 5 + 4(t-1)$$
$$= 4t + 1, para\ t = 1,2,3,\ldots$$

Teorema 3.1. $P(t) = 2^{4t}$ Termina en 6.

Demostración. La prueba es por inducción. Para todo $t = 1$,$p\ (1) = \ 2^4 = 16$. Supongamos que

$P(t) = 2^{4t}$ termina en 6 y vemos que P(t + 1) termina en 6. En efecto, $P(t\ +\ 1) = 2^{4(t+1)} = 2^4 2^{4t}$

Pero 2^{4t} termina en 6 y por hipótesis de inducción, 2^{4t} termina en 6, por lo que el producto termina en 6.

De aquí obtenemos,

Teorema 3.2 El número $2^{4t+1} - 1$ termina en 1 y $2^{4t-1} - 1$termina en 7.

Demostración. Veamos porque esto es cierto. Hagamos

$$p(t) = 2^{4t+1} - 1,\ \ t = 1,2,3 \ldots$$

Observemos que si $t = 1,\quad P\ (t)\ 2^5 - 1 = 31$. Supongamos que el resultado se cumple para t y veamos que se cumple para $t + 1$. Tenemos,

$$P(t + 1) = 2^{4(t+1)+1} - 1 = 2^5 2^{4t} - 1$$

Por la parte anterior 2^{4t} termina en 6, 2^5 termina en 2, luego $2^5\ 2^{4t}$ termina en 2 y $p\ (t + 1)$ termina en 1. De manera similar se muestra que 2^{4t-1} – 1 termina en 7.

Es fácil mostrar que 2^{4t-2} termina en 4. Así tenemos,

Teorema 3.3. El numero entero $2^{4t}(2^{4t+1} - 1)$ termina en 6 y $2^{4t-2}(\ 2^{4t-1} - 1)$ termina en 8.

Este resultado nos explica porque todo número perfecto par termina en 6 o en 8. El resultado se puede ver en las matrices abajo.

$$\begin{pmatrix} 2^3-1\downarrow & 2^5-1\downarrow & 2^7-1\downarrow & 2^9-1\downarrow & 2^{11}-1\downarrow & 2^{13}-1\downarrow & 2^{15}-1\downarrow \\ 7 & 31 & 127 & 511 & 2047 & 8191 & 32727 \end{pmatrix}$$

$$\begin{pmatrix} 2^2\downarrow & 4\downarrow & 2^6\downarrow & 2^8\downarrow & 2^{10}\downarrow & 2^{12}\downarrow & 2^{14}\downarrow & 2^{16}\downarrow \\ 4 & 16 & 64 & 256 & 1024 & 4096 & 65536 & 65536 \end{pmatrix}$$

Vemos que $2^{p-1}\ \ (\ 2^p\ - 1)$ termina en 6 o en 8.

Ahora hagamos,

$g(a_{t)} = w\big(a_{t,k}\big) = 2^{4t-1} - 1 - 2k, h(b_t) = w(b_t, k) = 2^{4t+1} - 1 - 2k$.

Los valores permitidos para k son 0, 1, 2, 3, ya que $g(a_1, k) > 0. Si\ k = 0$ sabemos que $g\ (a_t)$ termina en 1. Si $k = 1\ o\ k = 2\ o\ k = 3\ g\ (a_t)$ termina en 9 o 7 o 5 respectivamente y $h\ (b_t)$ termina en 5 o 3 o 1 respectivamente. Además,

$1.\mathrm{h}(b_{(t)}) - g\big(a_{(t)}\big) = 3(2^{4t-1}) + 3g\big(a_{(t)}\big) + 3l_1 donde\ \ l_1 = 1 + 2k$.

2. $g(a_{t+1}) - g(a_t) = 15(2^{4t-1})$.

3. $g(b_{t+1}) - h(b_t) = 15(2^{4t-1})$.

Si permitimos escoger valores para k que hagan $w\ (p, k) > 0$ según el caso se tiene el resultado trivial.

Teorema 3.4. Para cada p impar existe k tal que $w\ (p, k)$ es un número primo.

4. Números de Fermat.

En esta parte estudiamos brevemente los números de Fermat. Sea $2^n\ +\ 1\ =\ q$. No es difícil probar que si q es primo entonces n es una potencia de 2. Definamos q=$2^{2^p} + 1$. Por una observación directa vemos que q= q=$2^{2^p}\ +\ 1 = 2^p l + 1$. De otro lado

$$2^{2^p} + 1 = 4(2^{2^p-2}) + 1$$

De esta observación vamos que existe una relación entre los números de Fermat y los de Mersenne. Observamos que $Mp\ =\ 2^p - 1$ implica $2^p\ =\ Mp\ +\ 1$, por lo que

$$F_p = 2^{M_p+1} + 1$$

Esto nos da partida para estudiar brevemente los siguientes números:

1. Ningún H_p=$2^{M_{p^{-1}}} - 1$ es un numero primo de Mersenne.

2. Si $M_n - 1$ es un primo de Mersenne $G_p = 2^{M_{p^{-1}}} + 1$ no es un primo de Fermat, ya que $M_n - 1$ es divisible por 3.

6. BIBLIOGRAFÍA

[1]. Elementos de Álgebra. Marco Fidel Suárez. Centro Editorial. Universidad del Valle. 1994.

[2]. De los enteros a los dominios, Ruiz, Roberto. Centro Editorial. Universidad del Valle 1994.

[3]. Introducción a la Teoría de los Números. Niven, I. y Zuckerman, H. S., Editorial Limusa-Wiley, México, 1969.

[4]. Teoría de los números. Burton, W. Jones. Centro regional para la ayuda técnica, Agencia para el desarrollo internacional, México 1969.

[5]. Solved and unsolved problems in number theory, Shanks, Daniel, Chelsea publishing company, New York, 1978.