7
24

UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

FACULTAD DE CIENCIAS

ALGUNOS RESULTADOS SOBRE NUMEROS SEUDOPRIMOS

T E S I S

QUE PARA OBTENER EL TITULO DE

M A T E M A T I C O

P R E S E N T A :

SAUL DIAZ ALVARADO

MEXICO, D. F 1991

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

INDICE.

INTRODUCCION.

Uno de los problemas que desde hace mucho tiempo ha interesado a un gran número de matemáticos, ha sido el de encontrar una manera de determinar cuando un número es primo, o equivalentemente, cuando es compuesto; así dedicados al estudio de estos números han encontrado resultados que parecieran dar solución al problema, sin embargo no es así.

Fermat observó que siempre que n sea un entero primo se cumple con $a^n \equiv a \pmod{n}$ para cualquier número a entero, este resultado, junto con otros, podría pensarse como una forma de saber cuando un número es primo, pues siempre que observáramos que se cumple con esta propiedad podríamos aventurarnos a decir que se trata de un número primo; pero si $a^n \equiv a \pmod{n}$ entonces n no necesariamente es primo. Por otro lado, tenemos tambien que si n es primo cumple con el teorema de Euler, esto es, $a^{n-1} \equiv 1 \pmod{n}$ para toda a talque $(a,n) = 1$.

Así mismo, Fermat advirtió tambien que si $2^m + 1$ es primo, entonces $m = 2^n$; esto, se podría pensar así: "todos los números de la forma $2^{2^n} + 1$ son primos"; sin embargo esto no es cierto, luego, a pesar de que Fermat conjeturó que todos estos números eran primos observamos que no es así.

En otro resultado Mersene nos dice que si un número de la forma $2^m - 1$ es primo entonces m es primo, sin embargo si m es primo $2^m - 1$ no siempre es primo. Hay otros resultados que de igual manera se pudieran pensar como

formas para saber si un un número es o no primo, por ejemplo un número p primo cumple para todo b con:

$$b^{2^j t} \equiv -1 \pmod{p} \quad \text{para alguna} \quad 0 \leq j < s$$

o

$$b^t \equiv 1 \pmod{n}.$$

donde $p - 1 = 2^s t$, $s \geq 0$ t impar; y tambien si p es primo cumple;

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

De todos estos resultados observaremos que el reslproco es falso, esto es, existen números que cumplen estos resultados y son compuestos; a estos números se les llama números seudoprimos y son el propósito de estudio de este trabajo. Para este hecho introduciré lenguaje de teoría de grupos por ser este un lenguaje sencillo y accesible.

CAPITULO I.

NOCIONES GENERALES.

I.1. LEMAS IMPORTANTES .

En esta pequeña sección demostraré algunos lemas importantes sobre enteros que se usarán en los siguientes capítulos.

Lema I.1.

$\forall\, n > 1,\ n < 2^n - 1.$

Demostración:

La demostración se hace por inducción sobre n.

Si $n = 2$, se tiene que $2^2 - 1 = 4 - 1 = 3 > 2$.

Supongamos que $n < 2^n - 1$. (1)

Tenemos que como $n > 1$, $2^n > 1$, entonces sumando en (1) tenemos que

$$n + 1 < 2^n - 1 + 2^n = 2^{n+1} - 1. \quad \blacksquare$$

Lema I.2.

Sean n y d enteros positivos tales que $d \mid n$, entonces para toda $a, b \in \mathbb{Z}$ $a^d - b^d \mid a^n - b^n$.

Demostración:

Como $d \mid n$ existe $k \in \mathbb{Z}$ tal que $dk = n$, entonces

$$(a^d - b^d)(a^{n-d} + a^{n-2d}b^d + \ldots + a^{n-dk}b^{n-d}) =$$

$$a^n + a^{n-d}b^d + \ldots + a^{n-d(k-1)d}b^{n-d}$$

$$- a^{n-d}b^d - \ldots - a^{n-d(k-1)}b^{n-d} - a^{n-dk}b^n$$

$$= a^n - a^{n-dk}b^n = a^n - b^n.$$

es decir,

$$a^d - b^d \mid a^n - b^n. \quad \blacksquare$$

Lema I.3.

$\forall\, n \in \mathbb{N}$,

a) $4 \mid 3^{2n} - 1$.

b) $4 \nmid 3^{2n+1} - 1$.

Demostración:

a)Demostraremos que $3^{2n} \equiv 1 \pmod 4$.

Tenemos que;

$$3 \equiv -1 \pmod 4.$$

luego:

$$3^{2n} \equiv (-1)^{2n} \pmod 4.$$

pero

$$(-1)^{2n} \equiv ((-1)^2)^n \pmod 4.$$

$$((-1)^2)^n \equiv 1 \pmod 4.$$

b)Basta ver que $3^{2n+1} \not\equiv 1 \pmod 4$.

Veamos que:

$$3 \equiv -1 \pmod 4$$

luego;

$$3^{2n+1} \equiv (-1)^{2n+1} \equiv (-1)^{2n}(-1) \not\equiv -1 \pmod 4$$

$$-1 \not\equiv 1 \pmod 4$$

Por lo tanto:

$$3^{2n+1} \not\equiv 1 \quad \blacksquare$$

Lema I.4.

$\forall\, n \in \mathbb{N}$:

a) $8 \mid 5^{2n} - 1$.

b) $8 \nmid 5^{2n+1} - 1$.

c) $16 \nmid 5^{2n+1} - 1$.

Demostración:

a)Veamos que $8 \mid 5^{2n} - 1$ sí y solo sí $5^{2n} \equiv 1 \pmod 8$.

Pero

$$5 \equiv -3 \pmod 8.$$

entonces

$$5^{2n} \equiv (5^2)^n \equiv ((-3)^2)^n$$

$$\equiv (9)^n \equiv 1^n \equiv 1 \pmod 8.$$

b)Demostraremos que $5^{2n+1} \not\equiv 1 \pmod 8$.

Tenemos que

$$5^{2n+1} \equiv 5^{2n} \cdot 5 \equiv (5^2)^n \cdot 5$$

$$\equiv ((-3)^2)^n \cdot 3 \not\equiv 1 \pmod 8.$$

c)Esto se desprende del inciso anterior pue si 16 dividiera a $5^{2n+1} - 1 \ \forall \ n \in \mathbb{Z}$ entonces se tendría que 8 dividiría a $5^{2n+1} - 1 \ \forall \ n \in \mathbb{N}$ lo cual no es posible. ∎

I.4. Teoria de Grupos.

DEFINICION:

Sea G un conjunto no vacío y

$$\cdot : G \times G \longrightarrow G$$

una función, (por comodidad al elemento $\cdot(a,b)$ en G, se le denota ab).Se dice que $(G, \cdot)$ es grupo si cumple con las siguientes condiciones:

a) $a(bc) = (ab)c$

b) Existe un elemento distinguido en G llamado e tal que $ge = eg = g$ $\forall \ g \in G$.

c)$\forall \ g \in G$, $\exists \ g^{-1} \in G$ tal que $gg^{-1} = g^{-1}g = e$

Si además cumple con :

d) $gh = hg \quad \forall \ h,g \in G$

se dice que G es abeliano o conmutativo.

Ejemplos:

·) $(\mathbb{Z},+)$ es grupo, donde el elemento e es 0 y g^{-1} es $-g$.

··) $(\mathbb{N},+)$ no es grupo pues los elementos de $\mathbb{N}$ no tienen inverso.

OBSERVACION:

Si G es grupo el elemento e y los inversos son únicos y en consecuencia $(a^{-1})^{-1}= a$.

Demostración:

Supongamos que existe $e' \in G$ tal que $ae'= e'a = a \ \forall\ a \in G$, entonces $e = ee' = e'$, es decir e es único. Si $a \in G$ e $y \in G$ es tal que $ay = e$, multiplicando por a^{-1} obtenemos $y = a^{-1}$ y por lo tanto como $a^{-1}(a^{-1})^{-1}= e$ entonces $(a^{-1})^{-1}= a$.

DEFINICION:

·) $\forall\ n \in \mathbb{N} \cup \{0\}$ se define g^n por recurrencia de la siguiente manera:

$$g^0 = e \quad , \quad g^n = g^{n-1}g.$$

··) Si $n < 0$ definimos $g^n = (g^{-1})^{-n} = (g^{-n})^{-1}$

Lema I.5

Si g está en un grupo y $n,m \in \mathbb{Z}$, entonces

a) $g^n g^m = g^{n+m}$.

b) $(g^n)^m = g^{nm}$.

Demostración:

Sea $n \in \mathbb{Z}$ fijo pero arbitrario.

a) Supongamos que $m \in \mathbb{N}$, demuestro por inducción sobre m que $g^n g^m = g^{n+m}$.

Si $m = 1$, entonces:

$$g^n g^1 = g^{n+1}$$

por definición, si $n \in \mathbb{N} \cup \{0\}$. Si $n < 0$ entonces $-n > 0$, y por lo tanto $-n - 1 \geq 0$, por lo tanto:

$$g^n g = (g^{-1})^{-n} g = ((g^{-1})^{-n-1} g^{-1})g$$
$$= (g^{-1})^{-n-1} = (g^{-1})^{-(n+1)} = g^{n+1} .$$

Ahora supongamos que $g^n g^m = g^{n+m}$.

Tenemos que

$$g^n g^{m+1} = g^n(g^m g) = (g^n g^m)g = g^{n+m}g = g^{(n+m)+1} = g^{n+(m+1)}$$

Por lo tanto $\forall\, m \in \mathbb{N}$ $g^n g^m = g^{n+m}$.

Además tenemos $g^n g^0 = g^n e = g^n = g^{n+0}$

Ahora supongamos que $m < 0$, entonces $-m > 0$ y notemos que

$$(g^{-1})^{-n}(g^{-1})^{-m} = (g^{-1})^{-(n+m)}$$

de donde

$$g^n g^m = g^{n+m}.$$

En particular se tiene que

$$g^n g^{-n} = g^{n-n} = g^0 = e$$

por lo tanto

$$(g^n)^{-1} = g^{-n}.$$

b) La demostración se hace por inducción sobre m.

Si $m = 1$.

$$(g^n)^1 = g^n = g^{n\cdot 1}$$

Supongamos que $(g^n)^m = g^{nm}$.

Tenemos

$$(g^n)^{m+1} = (g^n)^m g^n = (g^{nm})g^n = g^{nm+n} = g^{n(m+1)}$$

por lo tanto $\forall\, n \in \mathbb{Z}$, $\forall\, m \in \mathbb{N}$, $(g^n)^m = g^{nm}$.

Para $n = 0$ es claro que $(g^n)^0 = e = g^0 = g^{n\cdot 0}$.

Ahora supongamos que $m < 0$, entonces $-m > 0$ y por lo anterior tenemos que

$$(g^n)^m = \left((g^n)^{-1}\right)^{-m} = (g^{-n})^{-m} = g^{(-n)(-m)} = g^{nm}. \quad \blacksquare$$

Lema 1.6.

Si G es grupo, entonces

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Demostación:

La demostración es muy simple ya que

$$(xy)(y^{-1}x^{-1}) = \left(x(yy^{-1})\right)x^{-1} = (xe)x^{-1} = xx^{-1} = e. \quad \blacksquare$$

En particular si G es abeliano el resultado nos dice que

$$(xy)^{-1} = x^{-1}y^{-1}.$$

Teorema I.1.

Sea G grupo abeliano, entonces

$$\forall\, n \in \mathbb{Z} \quad y \quad \forall\, x,y \in G \qquad (xy)^n = x^n y^n$$

Demostración:

Por inducción sobre n.

Si $n = 1$, entonces $(xy)^1 = xy = x^1y^1$.

Supongamos el resultado cierto para n.

Entonces se tiene que

$$(xy)^{n+1} = (xy)^n(xy) = (x^n y^n)(yx) =$$

$$x^n(y^n y)x = (x^n x)(y^n y) = x^{n+1}y^{n+1}$$

Por lo tanto para todo $n \in \mathbb{N}$ es cierto el resultado.

Supongamos que $n \leq 0$, entonces

$$(xy)^n = ((xy)^{-1})^{-n} = (x^{-1}y^{-1})^{-n} =$$

$$(x^{-1})^{-n}(y^{-1})^{-n} = x^n y^n$$

Entonces el resultado es cierto para toda $n \in \mathbb{Z}$. ∎

DEFINICION:

Sea $(G,\cdot)$ grupo y $H \subseteq G$, $H \neq \emptyset$.

Se dice que H es subgrupo de G si $(H, \cdot|_{H\times H})$ es grupo, (escribimos $H \leq G$), donde $\cdot|_{H\times H}: H\times H \longrightarrow G$ es la restricción de $\cdot: G\times G \longrightarrow G$ a $H\times H$, (que en caso de ser H subgrupo $\cdot|_{H\times H}: H\times H \longrightarrow H$).

Ejemplos:

1. $(G,\cdot) = (\mathbb{Z},+)$ y $H = 2\mathbb{Z} = \{n \in \mathbb{Z} \mid n = 2k \text{ p.a. } k \in \mathbb{Z}\}$

Entonces H es subgrupo de $\mathbb{Z}$ ya que:

·) Si $2m, 2n \in 2\mathbb{Z}$, entonces $2m + 2n = 2(n + m) \in 2\mathbb{Z}$.

··) La suma es asociativa pues $2\mathbb{Z}$ es subconjunto de $\mathbb{Z}$.

···) $0 = 2\cdot 0 \in 2\mathbb{Z}$.

····) Si $2n \in 2\mathbb{Z}$, entonces $2(-n) \in 2\mathbb{Z}$ y $2n + 2(-n) = 2(n - n) = 2\cdot 0 = 0$.

2. Sea G grupo y $H \leq G$, entonces $H' \leq H$ implica $H' \leq G$.

3. Si $H \leq G$ entonces:

a) El neutro de $(H,\cdot)$ es el neutro de $(G,\cdot)$.

b) El inverso de h en H es el inverso de h en G.

Teorema I.2.

Sea G grupo y $H \subseteq G$, entonces H es subgrupo de G sí y solo sí

a) $H \neq \varnothing$

b) $g_1 g_2^{-1} \in H \quad \forall\, g_1, g_2 \in H$.

Demostración:

$\Rightarrow$)Supongamos que $H \leq G$ entonces $(H, \cdot|_{H\times H})$ es grupo por lo tanto se verifican las dos condiciones.

$\Leftarrow$) Supongamos a) y b), entonces como $H \neq \varnothing$ $\exists\, g \in H$ y por b) $e = gg^{-1} \in H$. Además se tiene que $eg^{-1} = g^{-1} \in H$, $\forall\, g \in H$.

Sean $g,h \in H$ arbitrarios, entonces $h^{-1} \in H$ y por b) $gh = g(h^{-1})^{-1} \in H$; así que:

$$\begin{array}{ccc} G\times G & \xrightarrow{\quad\cdot\quad} & G \\ \uparrow & \cdot|_{H\times H} & \uparrow \\ H\times H & \xrightarrow{\quad\quad} & H \end{array}$$

conmuta.

Por último, el producto es asociativo pues $H \subseteq G$.

Por lo tanto $H \leq G$. ∎

DEFINICION:

Sa G grupo y $H \leq G$. Sean $g,h \in G$, se dice que g es congruente con h módulo H si $gh^{-1} \in H$. Escribimos

$$g \equiv h \ (mod\ H).$$

Lema I.7.

Sean G grupo y H subgrupo de G . Entonces la relación "$\equiv$ (*mod* H) " es de equivalencia.

Demostración:

·) $g \equiv g \pmod{H}$ pues $e = gg^{-1} \in H$.

··) Supongamos que $g \equiv h \pmod{H}$, entonces $gh^{-1} \in H$, de donde

$$hg^{-1} = (gh^{-1})^{-1} \in H$$

es decir

$$h \equiv g \pmod{H}$$

···)supongamos que $g \equiv h \pmod{H}$ y $h \equiv l \pmod{H}$, entonces

$$gh^{-1} \in H \quad y \quad hl^{-1} \in H$$

de donde

$$gl^{-1} = g(h^{-1}h)l^{-1} = (gh^{-1})(hl^{-1}) \in H.$$

Entonces $g \equiv l \pmod{H}$

Por lo tanto "$\equiv \pmod{H}$" es de equivalencia. ∎

De este lema se concluye que G puede partirse en las clases de equivalencia de la relación "$\equiv \pmod{H}$ ".

DEFINICION:

Sea G grupo y $H \leq G$. Definimos para cada $g \in G$ su clase lateral derecha como

$$Hg = \{hg \mid h \in H\}$$

Del mismo modo se puede definir clase lateral izquierda.

Teorema I.3.

Sean G grupo y $H \leq G$, entonces $x \in Hg$ sí y solo sí

$$x \equiv g \pmod{H}.$$

Demostración:

$x \in Hg \Leftrightarrow x = hg$ para alguna $h \in H \Leftrightarrow xg^{-1} = h \in H$ para alguna $h \in H \Leftrightarrow$

$$x \equiv g \pmod{H}.$$ ∎

De este teorema se desprende el siguiente hecho:

Si $[g]$ denota la clase de equivalencia de g módulo H, entonces $[g] = Hg$.

Teorema I.4.

Dado G grupo y H subgrupo de G existe una función biyectiva entre dos clase laterales derechas cualesquiera.

Demostración:

Sean $g_1, g_2 \in G$, definimos

$$\varphi : Hg_1 \longrightarrow Hg_2$$

dada por

$$\varphi(hg_1) = hg_2$$

Tenemos que si $hg_2 \in Hg_2$, entonces $h \in H$, de donde se tiene que $hg_1 \in Hg_1$ y por definición $\varphi(hg_1) = hg_2$ por lo tanto φ es suprayectiva.

Supongamos que

$$\varphi(hg_1) = \varphi(h'g_1)$$

entonces $hg_2 = h'g_2$ y multiplicando por g_2^{-1} en ambos lados tenemos $h = h'$, de donde se concluye que $hg_1 = h'g_1$. Por lo tanto φ es inyectiva. Por lo tanto φ es biyectiva. ∎

Entonces dos clases de equivalencia módulo H tienen la misma cardinalidad.

Un caso especial de grupos son aquellos que tienen una cantidad finita de elementos.

DEFINICION:

Sea G grupo, se define el orden de G, o(G), como la cardinalidad de G . Una relación que guardan el orden de un grupo finito y los ordenes de sus subgrupos es la siguiente:

Teorema I.5.

Sea G un grupo finito, $H \leq G$, entonces

$$o(H) \mid o(G).$$

Demostración:

Sea H subgrupo de G arbitrario. Como ya se dijo G es la unión ajena de clases laterales derechas y cada clase es finita ya que estan incluidas en G.

Notemos que $He = H$ pues $he = h$ para toda $h \in H$. Por el teorema anterior todas las clase laterales derechas tienen $o(H)$ elementos. Supongamos que hay l distintas clases, entonces

$$o(G) = \underbrace{o(H) + o(H) + \ldots + o(H)}_{l \text{ veces}}$$

de donde, $o(G) = o(H)l$, entonces

$$o(H) \mid o(G). \quad \blacksquare$$

Otro tipo de grupos muy interesante es el de aquellos en los que cada elemento se obtiene como potencia de un elemento fijo. Estos grupos se llaman cíclicos y se hablará de ellos posteriormente.

DEFINICION:

Si G es un grupo y $g \in G$, definimos el subgrupo generado por g como:

$$(g) = \{g^n \mid n \in \mathbb{Z}\}$$

A g se le llama generador de (g).

Lema I.8

Sea G grupo y $g \in G$, entonces el subgrupo generado es un subgrupo de G.

Demostación:

·) Tenemos que $g^0 = e \in (g)$, por lo tanto $(g) \neq \varnothing$.

··) Sean $x, y \in (g)$, entonces $x = g^n$ y $y = g^m$ para algunos $n, m \in \mathbb{Z}$, por lo tanto

$$xy^{-1} = g^n(g^m)^{-1} = g^n g^{-m} = g^{n-m} \in (g).$$

Por lo tanto $(g) \leq G$. $\blacksquare$

DEFINICION:

Sea G grupo. Para cada $g \in G$ se define el orden de g, denotado $o(g)$, como el mínimo entero positivo n tal que $g^n = e$. En caso de no existir se dice que g es de orden infinito.

Lema 1.9.

Si G es grupo y $g \in G$ es de orden n, entonces

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}.$$

Demostración:

Sea $x \in \langle g \rangle$, entonces $x = g^m$ p.a. $m \in \mathbb{Z}$. Por el algoritmo de la división existen enteros q y r tales que

$$m = nq + r \qquad 0 \leq r < n,$$

de donde

$$g^m = g^{nq+r} = g^{nq} g^r = (g^n)^q g^r = eg^r = g^r$$

pero

$$g^r \in \{e, g, g^2, \ldots, g^{n-1}\}$$

de donde

$$g^m \in \{e, g, g^2, \ldots, g^{n-1}\}.$$

Es claro que

$$\{e, g, g^2, \ldots, g^{n-1}\} \subseteq \langle g \rangle$$

por lo tanto

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}. \blacksquare$$

Teorema I.6.

Sea G grupo y supongamos que $g \in G$ es tal que $o(g) = n$.

Entonces si m es tal que $g^m = e$ n divide a m.

Demostración:

Tenemos que

$$m = nq + r \qquad \text{p.a. } q, r \in \mathbb{Z},\ 0 \leq r < n.$$

entonces

$$e = g^m = g^{nq+r} = g^{nq} g^r = g^r$$

lo cual solo es posible si $r = 0$, por lo tanto

$$n \mid m. \blacksquare$$

Teorema I.7.

Supongamos que G es grupo finito, entonces todo elemento $g \in G$ es de orden finito.

Demostración:

Sea $g \in G$, consideremos

$$S = \{g, g^2, \ldots, g^{o(G)}\} \leq G$$

Si todos los elementos de S son distintos entonces la cardinalidad de S es exactamente $o(G)$, por lo tanto $S = G$, de donde $e \in S$, es decir $g^j = e$ p.a. $1 \leq j \leq o(G)$.

Si $g^n = g^m$ con $1 \leq n, m \leq o(G)$, supongamos que $n < m$ entonces si hacemos $j = n - m$, entonces $1 \leq j \leq o(G)$ y

$$g^j = g^{n-m} = e,$$

por el principio del buen orden existe un entero mínimo m $1 \leq m \leq o(G)$ tal que $g^m = e$ entonces $o(g) = m$. ∎

Teorema I.8.

Sea G de orden finito entonces $\forall\, g \in G$ se tiene

$$o(g) \mid o(G).$$

Demostración:

Sea $g \in G$ arbitrario, entonces

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{o(g)-1}\} \leq G$$

entonces

$$o(g) = o(\langle g \rangle) \mid o(G).$$ ∎

Por último introduciremos la noción de grupo cíclico así como algunas de sus propiedades importantes.

DEFINICION:

Se dice que un grupo G es cíclico si existe $g \in G$ tal que $\langle g \rangle = G$.

Ejemplo:

$G = \mathbb{Z}$ esta generado por el elemento 1, es decir $\langle 1 \rangle = \mathbb{Z}$, tambien $\langle -1 \rangle = \mathbb{Z}$.

Notemos que un grupo finito G es cíclico sí y solo sí existe $g \in G$ tal que $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$, donde $o(G) = n$.

Teorema I.9.

Sea G grupo finito, supongamos que $o(G) = p$, con p primo, entonces G es cíclico.

Demostración:

Como el orden de G es mayor que 1 por ser primo, entonces existe $g \in G$ tal que $g \neq e$, así se tiene que

$$o(g) \mid o(G) = p$$

Como p es primo, entonces

$$o(g) = \begin{cases} 1 \\ p \end{cases}$$

$o(g) \neq 1$, puesto que $g \neq e$, por lo tanto $o(g) = p$ luego

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{p-1}\} = G$$

por lo tanto G es cíclico. ∎

De la demostración del teorema se desprende que todo elemento distinto de e en un grupo de orden primo es generador , es decir un grupo de orden primo p tiene $p - 1$ generadores.

El siguiente resultado nos da la cantidad de generadores en un grupo cíclico.

Teorema I.10.

Sea G grupo y $g \in G$, entonces

$$o(g^j) = \frac{o(g)}{(j, o(g))}$$

Demostración:

Sea $m = o(g^j)$ y $n = o(g)$ entonces, como $(g^j)^{n/(j,n)} = (g^n)^{j/(j,n)} = e$

se tiene que

$$m \mid \frac{n}{(j,n)}$$

Por otro lado se tiene que $g^{jm} = (g^j)^m = e$, por lo tanto

$$n \mid jm$$

de donde

$$\frac{n}{(j,n)} \mid \frac{j}{(j,n)} m$$

pero

$$\left(\frac{n}{(j,n)}\ ,\ \frac{j}{(j,n)}\right) = 1$$

entonces

$$\frac{n}{(j,n)} \mid m$$

por lo tanto

$$o(g^j) = m = \frac{n}{(j,n)} \ . \ \blacksquare$$

Corolario I.10.1.

Sea G grupo cíclico de orden n con generador g, entonces existen $\phi(n)$ generadores de G.

Demostración:

Tenemos que un elemento en G es generador de G si y solo si es de orden n, además todos los elementos de G son de la forma g^j con $0 \leq j < n$, y

$$o(g^j) = \frac{n}{(j,n)}$$

entonces $o(g^j) = n$ si y sólo si $(j,n) = 1$, pero hay precisamente $\phi(n)$ enteros primos relativos con n menores que n, por lo tanto hay $\phi(n)$ generadores de G. $\blacksquare$

Teorema I.11.

Sea G grupo abeliano y supongamos que $g,h \in G$ son de orden finito, entonces existe $z \in G$ tal que $o(z) = [n,m]$.

Demostración:

Supongamos que $n = o(g)$ y $o(h) = m$, supongamos que $(n,m) = 1$, sea $s = o(gh)$, entonces como

$$(gh)^{nm} = (g^n)^m(h^m)^n = e \quad \text{ya que G es abeliano}$$

s divide a $nm = [n,m]$.

Por otro lado

$$o(g^m) = \frac{n}{(n,m)} = n \quad y \quad o(h^n) = \frac{m}{(n,m)} = m$$

de donde

$$(gh)^m = g^m h^m = g^m \quad y \quad (gh)^n = g^n h^n = h^n$$

por lo tanto $(gh)^m$ y $(gh)^n$ tienen orden n y m respectivamente.

Tenemos

$$\left((gh)^n\right)^s = \left((gh)^s\right)^n = e \quad \text{y} \quad \left((gh)^n\right)^s = \left((gh)^s\right)^n = e$$

entonces

$$n \mid s \quad \text{y} \quad m \mid s$$

de donde $nm = [n,m] \mid s$.

De lo anterior se concluye que el orden de $z = xy$ es $[n,m]$.

Ahora supongamos que n y m son arbitrarios.

Supongamos que

$$n = p_1^{a_1} p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}$$

$$m = p_1^{b_1} p_2^{b_2} \cdot \ldots \cdot p_r^{b_r}$$

la descomposición de n y m en factores primos respectivamente, entonces

$$[n,m] = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdot \ldots \cdot p_r^{\max(a_r,b_r)}.$$

Definamos n_0, m_0 como sigue:

$$n_0 = p_1^{c_1} p_2^{c_2} \cdot \ldots \cdot p_r^{c_r}$$

donde

$$c_j = \begin{cases} a_j & \text{si } \max(a_j,b_j) = a_j. \\ 0 & \text{si } \max(a_j,b_j) \text{ no es } a_j. \end{cases}$$

$$m_0 = p_1^{d_1} p_2^{d_2} \cdot \ldots \cdot p_r^{d_r}$$

donde

$$d_j = \begin{cases} b_j & \text{si } p_j \mid n_0. \\ 0 & \text{si } p_j \mid n_0. \end{cases}$$

Notemos que n_0, m_0 no tienen divisores comunes, entonces $(n_0, m_0) = 1$ y además $n_0 m_0 = [n,m]$

Sean $n_1 = \frac{n}{n_0}$ $m_1 = \frac{m}{m_0}$, entonces

$$o(g^{n_1}) = \frac{n}{(n_1,n)} = \frac{n}{n_1} = n_0$$

$o(h^{m_1}) = \frac{m}{(m_1,m)} = \frac{m}{m_1} = m_0$ Y por lo anterior

$o(g^{n_1}h^{m_1}) = n_0 m_0 = [n,m]$ Por lo tanto $z = g^{n_1}h^{m_1}$ tiene orden $[n,m]$. ∎

Teorema I.12

Sea G un grupo abeliano finito. Supongamos que la ecuación $x^n = e$, tiene a lo más n soluciones distintas, en G entonces G es cíclico.

Demostración:

Sea $g \in G$ un elemento de orden máximo, (dicho g existe pues el orden de los elementos de G esta acotado por o(G)), ahora demostraré que $\langle g \rangle = G$.

supongamos que $n = o(g)$, entonces $\forall\ i = 1,\ldots,n$ $(g^i)^n = (g^n)^i = e^i = e$, entonces $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$ contiene todas las soluciones de $x^n = e$.

Sea $h \in G$ arbitrario y sea $o(h) = m$, por el teorema anterior existe $k \in G$ cuyo orden es $[n,m]$, pero $[n,m] \geq n$, y n es máximo, entonces $n = [n,m]$ de donde

$$n = [n,m] = \frac{nm}{(n,m)}$$

por lo tanto $(n,m) = m$, es decir, m divide a n, entonces existe $t \in \mathbb{Z}$ tal que $n = mt$, de aquí

$$h^n = h^{mt} = (h^m)^t = e$$

de donde $h \in \langle g \rangle$, por lo tanto $\langle g \rangle = G$. ∎

Notemos que para un elemento de orden finito g de un grupo G se tiene $g^i = g^j$ implica que $g^{i-j} = e$, por lo tanto $o(g)$ divide a $i - j$ es decir

$$i \equiv j \pmod{o(g)}.$$

Además si $0 \leq i, j < o(g)$ entonces $g^i = g^j$ implica $i = j$.

DEFINICIÓN:

Sea $G = \{e, g, g^2, \ldots, g^{n-1}\}$, definimos para cada $x \in G$ el índice de x para la base g, $(i_g(x))$, como el entero $j \in \{0,1,\ldots,n-1\}$, tal que $g^j = x$.

Teorema I.13.

Sean G grupo cíclico de orden n y g generador de G, entonces

·) $i_g(e) = 0$.

··) $i_g(ab) \equiv i_g(a) + i_g(b) \pmod{n}$

$\cdots$) $i_n(a^k) \equiv k i_n(a) \pmod{n}$ $(k \in \mathbb{N})$

Demostración:

·)Tenemos que $g^{i_n(e)} = e$, entonces

$$n = o(g) \mid i_n(e)$$

y $i_n(e) < n$, por lo tanto

$$i_n(e) = 0 .$$

··) Se tiene que $g^{i_n(ab)} = ab$, $g^{i_n(a)} = a$ y $g^{i_n(b)} = b$, de donde

$$g^{i_n(ab)} = ab = g^{i_n(a)} g^{i_n(b)} = g^{i_n(a)+i_n(b)}$$

por lo tanto

$$i_n(ab) \equiv i_n(a) + i_n(b) \pmod{n}$$

$\cdots$) La demostración se hace por inducción sobre k.

Para $k = 1$ es obvio y $k = 2$ es el inciso anterior.

Supongamos que

$$i_n(a^k) \equiv k i_n(a) \pmod{n}$$

entonces

$$i_n(a^{k+1}) = i_n(a^k a) \equiv i_n(a^k) + i_n(a) \equiv$$

$$k i_n(a) + i_n(a) \equiv (k+1) i_n(a) \pmod{n}$$

por lo tanto $\forall\, n \in \mathbb{N}$

$$i_n(a^n) \equiv n i_n(a) \pmod{n}. \quad \blacksquare$$

DEFINICION:

Sea G grupo y k entero positivo, se dice que $a \in G$ tiene raíz k-ésima si la ecuación $x^k = a$ tiene solución en G.

x_0 se llama raíz k-ésima de a si $x_0^k = a$.

Teorema I.14.

Si G es cíclico de orden finito n, entonces $a \in G$ tiene una raíz k-ésima si y solo si $a^{n/d} = e$ donde $d = (n,k)$.

Demostración:

⇒)Sea $g \in G$ generador, supongamos que x_0 es raíz k-ésima

$\cdots\cdot$) Es conmutativo.

Pero no todos los elementos tienen inverso, por ejemplo; en $\mathbb{Z}_4$ el elemento 2 no tiene inverso ya que

$$2^2 = 4 \equiv 0 \pmod 4$$

y si existiera $x \in \mathbb{Z}_4$ tal que

$$X \cdot 2 \equiv 1 \pmod 4$$

entonces

$$X \cdot 2^2 \equiv (X \cdot 2)2 \equiv 2 \equiv X \cdot 0 \equiv 0 \pmod 4$$

lo cual nos indica que 2 y 0 son lo mismo en $\mathbb{Z}_4$, y esto es falso, por lo tanto 2 no puede tener inverso; sin embargo si $x \in \mathbb{Z}_n$ es tal que $(x,n) = 1$, existen $r,s \in \mathbb{Z}$ tales que

$$1 = xr + ns$$

entonces

$$xr \equiv 1 \pmod n$$

luego, el residuo de r módulo n es el inverso de x.

Denotemos $(\mathbb{Z}_n, \cdot)$ el conjunto de residuos módulo n primos con n, entoces $(\mathbb{Z}_n, \cdot)$ resulta ser un grupo llamado el grupo de unides de $\mathbb{Z}_n$.

Notemos que existen $\phi(n)$ enteros positivos menores que n y primos con n, entonces $o((\mathbb{Z}_n, \cdot)) = \phi(n)$ y si n es primo el orden es $n-1$.

Teorema I.15. (Euler).

Sea n entero positivo entonces

$$a^{\phi(n)} \equiv 1 \pmod n$$

para todo a primo relativo con n.

Demostración:

Sea a primo relativo con n, entonces $a \in (\mathbb{Z}_n, \cdot)$ y tenemos que $o((\mathbb{Z}_n, \cdot)) = \phi(n)$, por lo tanto

$$a^{\phi(n)} \equiv 1 \pmod n. \quad \blacksquare$$

Teorema I.16. (Fermat).

Sea p primo, entonces para todo $a \in \mathbb{Z}$

$$a^p \equiv a \pmod p.$$

Demostración:

Sea $a \in \mathbb{Z}$, tenemos dos casos

·) $p \mid a$.

··) $p \nmid a$.

Si se cumple lo primero

$$a \equiv 0 \pmod{p}$$

de donde

$$a^p \equiv 0 \equiv a \pmod{p}.$$

Si p no divide a a, $a \in (\mathbb{Z}_p, \cdot)$ y como $o\big((\mathbb{Z}_p, \cdot)\big) = \phi(p) = p - 1$, se tiene

$$a^{p-1} \equiv 1 \pmod{p}$$

o bien

$$a^p \equiv a \pmod{p}. \quad \blacksquare$$

En los resultados siguientes de la presente sección se encotraremos todas las n para las cuales el grupo $(\mathbb{Z}_n, \cdot)$ resulta ser cíclico.

Teorema I.17.

$(\mathbb{Z}_n, \cdot)$ es cíclico si y sólo si n es 2, 4, p^r o $2p^r$, con p primo impar.

La demostración de este teorema esta dada por los siguientes resultados.

Teorema I.18.

Si p es primo, $(\mathbb{Z}_p, \cdot)$ es cíclico.

Para demostrar este teorema probaremos lo siguiente:

Lema I.10.

Para todo $n \in \mathbb{N}$ un polinomio $f(x)$ de grado n cuyo coeficiente principal no es divisible por p tiene a lo más n raices módulo n, es decir, $f(x) \equiv 0 \pmod{p}$ tiene a lo más n soluciones.

Demostración:

Para demostrar esto consideremos para cada $n \in \mathbb{N}$

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \qquad p \nmid a_n$$

Demostrarmos usando inducción sobre el grado de f que

$f(x) \equiv 0 \pmod{p}$ tiene a lo más n soluciones incongruentes.

$n = 1$.

Como $p \nmid a_n$, $(p, a_n) = 1$, esto es existen x_0, $y_0 \in \mathbb{Z}$ tales que

$$1 = px_0 + a_n y_0$$

multiplicando por $-a_0$ se tiene:

$$-a_0 = p(-a_0 x_0) + a_n(-a_0 y_0)$$

o bien

$$p(a_0 y_0) = a_n(-a_0 y_0) + a_0$$

esto es

$$p \mid a_n(-a_0 y_0) + a_0$$

por tanto

$$f(-a_0 y_0) \equiv 0 \pmod{p}.$$

Supongamos que z es tal que

$$f(z) \equiv 0 \pmod{p},$$

entonces

$$a_n z \equiv a_n(-a_0 y_0) \pmod{p}$$

es decir

$$p \mid a_n(z + a_0 y_0)$$

y como $p \nmid a_n$ se tiene que $p \mid z + a_0 y_0$ o bien

$$z \equiv -a_0 y_0 \pmod{p}.$$

Ahora supongamos que todo f de grado $n - 1$ tiene a lo más $n - 1$ soluciones incongruentes.

Supongamos que $f(x)$ tiene grado n y supongamos que $c_0, c_1, \ldots, c_n$ son $n + 1$ raíces incongruentes, entonces tenemos que

$$f(x) = (x - c_0)h(x)$$

con

$$h(x) = (a_n x^{n-1} + (a_n c_0 + a_{n-1})x^{n-2} + \ldots + (a_n c_0^{n-1} + \ldots + a_2 c_0 + a_1)x$$

de este hecho tenemos que

$$f(c_i) = (c_k - c_0)h(c_k) \equiv 0 \pmod{p}, \quad \forall\, k = 1, \ldots, n$$

es decir,

$$p \mid (c_k - c_0)h(c_k),$$

entonces

$$p \mid (c_i - c_s)$$

ó

$$p \mid h(c_i),$$

pero

$$p \nmid (c_i - c_s)$$

pues

$$c_i \equiv c_s \pmod{p},$$

por tanto

$$p \mid h(c_i)$$

o bien

$$h(c_i) \equiv 0 \pmod{p} \quad \forall\, i$$

pues $h(x) \equiv 0 \pmod{p}$ a lo mas tiene $n - 1$ soluciones incongruentes.

Por tanto $f(x) \equiv 0 \pmod{p}$ tiene a lo mas n soluciones. ■

Demostración (del Teorema):

Ahora la demostracion es sencilla pue si consideramos $f(x) = x^n - 1$

por el *Lema* anterior a lo mas existen n soluciones incongruentes de

$$x^n \equiv 1 \pmod{p}$$

o con el lenguaje de $(\mathbb{Z}p, \cdot)$ existen a lo más n soluciones de

$$x^n = 1$$

por lo que concluimos que $(\mathbb{Z}p, \cdot)$ es cíclico. ■

Teorema I.19.

Sea p primo impar entonces $(\mathbb{Z}p^r, \cdot)$ es cíclico.

Demostración:

Sea g generador de $(\mathbb{Z}p, \cdot)$, demostraré que g o $g + p$ es generador de $(\mathbb{Z}p^r, \cdot)$.

Como $g \in (\mathbb{Z}_p, \cdot)$, entonces $(g,p) = 1$, entonces $(g,p^2) = 1$, por lo tanto $g \in (\mathbb{Z}_{p^2}, \cdot)$.

Sea $n = o(g)$ en $(\mathbb{Z}_{p^2}, \cdot)$, entonces

$$n \mid o((\mathbb{Z}_{p^2}, \cdot)) = p(p-1)$$

además, como

$$g^n \equiv 1 \pmod{p^2}$$

se tiene

$$p \mid p^2 \mid g^n - 1$$

de donde

$$g^n \equiv 1 \pmod{p}$$

entonces

$$p - 1 = o(g) \mid n$$

entonces $\exists\, k_1, k_2 \in \mathbb{Z}$ tales $(p-1)k_1 = n$ y $nk_2 = p(p-1)$, de donde se tiene que

$$(p-1)k_1k_2 = nk_2 = p(p-1),$$

por lo tanto

$k_1k_2 = p$, es decir, k_1 divie a p entnce k_1 tiene ls siuientes posibilidades: $k_1 = \begin{cases} 1 \\ p \end{cases}$

o

$$n = \begin{cases} p-1 \\ p(p-1) \end{cases}$$

Si $n = p(p-1)$, entonces g genera a $(\mathbb{Z}_{p^2}, \cdot)$. Supongamos que $n = p - 1$.

Sea $x = g + p$, entonces

$$x \equiv g \pmod{p}$$

es decir, x es generador de $(\mathbb{Z}_p, \cdot)$ y por la misma razón de antes $x \in (\mathbb{Z}_{p^2}, \cdot)$.

Siguiendo el mismo razonamiento $o(x)$ en $(\mathbb{Z}_{p^2}, \cdot)$ es $p - 1$ o $p(p-1)$. Supongamos que $o(x) = p - 1$, entonces

$$x^{p-1} \equiv 1 \pmod{p^2}$$

por otro lado

$$
\begin{aligned}
x^{p-1} &\equiv (g + p)^{p-1} \\
&= \sum_{i=0}^{p-1} \frac{(p-1)!}{i!(p-1-i)!} g^{p-1-i} p^i \\
&\equiv g^{p-1} + (p-1) g^{p-2} p + \sum_{i=2}^{p-1} \frac{(p-1)!}{i!(p-1-i)!} g^{p-1-i} p^i \\
&\equiv g^{p-1} + (p-1) g^{p-2} p \pmod{p^2}
\end{aligned}
$$

ya que

$$
\sum_{i=2}^{p-1} \frac{(p-1)!}{i!(p-1-i)!} g^{p-1-i} p^i \equiv 0 \pmod{p^2}
$$

por lo tanto

$$
\begin{aligned}
1 &\equiv g^{p-1} + (p-1) g^{p-2} p \\
&\equiv g^{p-1} + p^2 g^{p-2} - p g^{p-2} \pmod{p^2}
\end{aligned}
$$

pero

$$
g^{p-1} \equiv 1 \pmod{p^2}
$$

entonces

$$
1 \equiv 1 - p g^{p-2} \pmod{p^2}
$$

de donde

$$
p g^{p-2} \equiv 0 \pmod{p^2}
$$

por lo tanto $\exists\, k \in \mathbb{Z}$ tal que $p^2 k = p g^{p-2}$, es decir $pk = g^{p-2}$, de donde,

$$
g^{p-2} \equiv 0 \pmod{p}
$$

lo cual no es posible pues g genera a $(\mathbb{Z}_p, \cdot)$. Por lo tanto el orden de x es $p(p-1) = \phi(\mathbb{Z}_{p^2}, \cdot)$, entonces x genera a $(\mathbb{Z}_{p^2}, \cdot)$. ∎

Ahora encontrar un generador para $(\mathbb{Z}_{p^k}, \cdot)$ con $k > 2$ es fácil como nos muestra el siguiente resultado.

Teorema I.20.

Sea p primo impar, entonces $(\mathbb{Z}_{p^k}, \cdot)$ es cíclico para todo k positivo.

Demostración:

El teorema para los casos $k = 1, 2$ ya se demostró antes, entonces $\exists\, g \in (\mathbb{Z}_{p^2}, \cdot)$ tal que $\langle g \rangle = (\mathbb{Z}_{p^2}, \cdot)$. Demostraremos que $\langle g \rangle = (\mathbb{Z}_{p^k}, \cdot)$, para todo $k \geq 3$.

Por inducción demostraremos lo siguiente:

$$\forall\ k \geq 2 \qquad g^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$$

Notemos que

$$g^{p-1} = g^{p^0(p-1)} \not\equiv 1 \pmod{p^2}$$

pues $o(g) = p(p-1)$.

Supongamos esto cierto para $k > 2$, como $g \in (\mathbb{Z}p^k, \cdot)$, entonces $(g, p^2) = 1$, de donde $(g, p^{k-1}) = 1$ para todo $k \geq 3$ de aquí tenemos $g \in (\mathbb{Z}p^{k-1}, \cdot)$, entonces

$$g^{\varphi(p^{k-1})} = g^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}}$$

entonces existe $q \in \mathbb{Z}$ tal que

$$g^{p^{k-2}(p-1)} = 1 + p^{k-1}q$$

y $p \nmid q$ pues si $p \mid q$, entonces

$$g^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$$

lo cual no es posible, por lo tanto p no puede dividir a q.

Entonces

$$\begin{aligned} g^{p^{k-1}(p-1)} &= g^{p(p^{k-2}(p-1))} \\ &= \left(g^{p^{k-2}(p-1)} \right)^p = (1 + p^{k-1}q)^p \\ &= \sum_{i=0}^{p} \frac{p!}{i!(p-i)!} \left(p^{k-1}q\right)^i \\ &= \sum_{i=0}^{p} \frac{p!}{i!(p-i)!} p^{i(k-1)} q^i \\ &= 1 + p(p^{k-1}q) + \sum_{i=2}^{p} \frac{p!}{i!(p-i)!} p^{i(k-1)} q^i \end{aligned}$$

pero

$$\sum_{i=0}^{p} \frac{p!}{i!(p-i)!} p^{i(k-1)} q^i \equiv 0 \pmod{p^{k+1}}$$

pues si $i \geq 2$ entonces $ik - i \geq 2k - 2 > k + 1$

ya que $k + 1 > 2k - 2$ implica que $3 > k$, pero estamos suponiendo $k \geq 3$.

Por lo tanto

$$g^{p^{k-1}(p-1)} \equiv 1 + p^k q \pmod{p^{k+1}}$$

y si

$$g^{p^{k-1}(p-1)} \equiv 1 \pmod{p^{k+1}}$$

entonces

$$p^k q \equiv 0 \pmod{p^{k+1}}$$

es decir, $p^k q = p^{k+1} t$ p.a. $t \in \mathbb{Z}$, de donde $q = pt$ lo cual no es posible, por lo tanto

$$g^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$$

Ahora demostraremos que g genera a $(\mathbb{Z}_{p^k}, \cdot)$ $\forall\, k \geq 2$.

$(g, p^k) = 1$ pues $g \in (\mathbb{Z}p^k, \cdot)$, entonces $(g, p^k) = 1$ para toda $k \geq 2$, es decir $g \in (\mathbb{Z}_{p^k}, \cdot)$ para toda $k \geq 2$.

Tomemos $k \geq 2$ arbitraria, sea $n = o(g)$ en $(\mathbb{Z}_{p^k}, \cdot)$, entonces

$$n \mid o\left((\mathbb{Z}_{p^k}, \cdot)\right) = p^{k-1}(p-1)$$

y

$$g^n \equiv 1 \pmod{p^k}$$

como $k \geq 2$, entonces

$$p^2 \mid p^k \mid g^n - 1$$

de donde

$$g^n \equiv 1 \pmod{p^2}$$

entonces

$$o(g) = p(p-1) \mid n.$$

Por lo tanto $\exists\, k_1, k_2 \in \mathbb{Z}$ tales que

$$p(p-1)k_1 = n \qquad \text{y} \qquad nk_2 = p^{k-1}(p-1)$$

de donde

$$p(p-1)k_1k_2 = nk_2 = p^{k-1}(p-1)$$

es decir, $k_1k_2 = p^{k-2}$, así k_1 divide a p^{k-2}, entonces $k_1 = p^t$ con $0 \leq t \leq k-2$, de aquí $n = p^t(p-1)$ $1 \leq t \leq k-1$.

Supongamos $t < k-1$, entonces $0 \leq k-2-t$, de donde

$$1 \equiv g^n \equiv g^{p^t(p-1)} \pmod{p^k}$$

esto es

$$1 \equiv \left(g^{p(1-1)}\right)^{p^{k-1}} \pmod{p^k}$$

como $k \geq 2$, entonces

$$g^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$$

por lo tanto $n = p^{k-1}(p-1)$ ■

Teorema I.21.

Sea p primo impar, entonces $(\mathbb{Z}_{2p^k}, \cdot)$ es cíclico.

Demostración:

Notemos que $\phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k)$ pues $(2, p^k) = 1$, por lo tanto $o\left((\mathbb{Z}_{2p^k}, \cdot)\right) = o\left((\mathbb{Z}_{p^k}, \cdot)\right)$.

Sea g generador de $(\mathbb{Z}_{p^k}, \cdot)$, supongamos que g es impar entonces $(g,2) = 1$ y como $g \in (\mathbb{Z}_{p^k}, \cdot)$ $(g, p^k) = 1$, de donde existen $x_0, x_1, y_0, y_1 \in \mathbb{Z}$ tales que

$$1 = gx_0 + 2x_1$$

$$1 = gy_0 + p^k y_1$$

entonces

$$1 = g^2 x_0 y_0 + 2gx_1 y_0 + p^k g x_0 y_1 + 2p^k x_1 y_1$$

$$1 = g(gx_0 y_0 + 2x_1 y_0 + p^k x_0 y_1) + 2p^k x_1 y_1$$

por lo tanto $(g, 2p^k) = 1$, es decir $g \in (\mathbb{Z}_{2p^k}, \cdot)$.

Sea $n = o(g)$ en $(\mathbb{Z}_{2p^k}, \cdot)$ entonces

$$n \mid o\left((\mathbb{Z}_{2p^k}, \cdot)\right) = o\left((\mathbb{Z}_{p^k}, \cdot)\right) = \phi(p^k)$$

$$g^n \equiv 1 \pmod{2p^k}$$

entonces

$$p^k \mid 2p^k \mid g^n - 1$$

es decir

$$g^n \equiv 1 \pmod{p^k}$$

de donde

$$\phi(p^k) \mid n$$

por lo tanto $n = \phi(p^k)$, así que g genera a $(\mathbb{Z}_{2p^k}, \cdot)$.

Si g es par entonces $x = g + p^k$ es impar y

$$x \equiv g \pmod{p^k}$$

es decir x es generador impar de $(\mathbb{Z}_{p^k}, \cdot)$, y por el razonamiento anterior x genera a $(\mathbb{Z}_{2p^k}, \cdot)$.

Por lo tanto $(\mathbb{Z}_{2p^k}, \cdot)$ es cíclico. ∎

Hasta aquí tenemos que si n es 2, 4, p^k o $2p^k$, entonces $(\mathbb{Z}_n, \cdot)$ es cíclico, el recíproco se prueba en los siguientes resultados.

Teorema I.22.

Sea $k > 2$, entonces el grupo $(\mathbb{Z}_{2^k}, \cdot)$ no es cíclico.

Demostración:

Para demostrar esta afirmación basta probar que ningun elemento de $(\mathbb{Z}_{2^k}, \cdot)$ tiene orden $o\big((\mathbb{Z}_{2^k}, \cdot)\big) = \phi(2^k) = 2^{k-1}$. Demostremos usando inducción que

$$a^{2^{k-2}} \equiv 1 \pmod{2^k} \qquad \forall\, a \in (\mathbb{Z}_{2^k}, \cdot),\ \forall\, k > 2.$$

Sea $a \in (\mathbb{Z}_{2^k}, \cdot)$ arbitrario.

$k = 3$.

Como $a \in (\mathbb{Z}_{2^k}, \cdot)$, $(a, 2^k) = 1$, entonces a es impar, es decir, $\exists\ s \in \mathbb{Z}$ tal que $a = 2s + 1$, entonces

$$a^2 = (2s + 1)^2 = 4s^2 + 4s + 1 = 4s(s + 1) + 1$$

y s o $s + 1$ es par, entonces $a^2 = 8t + 1$ p.a. $t \in \mathbb{Z}$, es decir

$$a^2 \equiv 1 \pmod{2^3}$$

Supongamos que

$$a^{2^{k-2}} \equiv 1 \pmod{2^k} \qquad k > 3.$$

entonces

$$2^k \mid a^{2^{k-2}} - 1$$

de aquí, $\exists\ t \in \mathbb{Z}$ tal que $a^{2^{k-2}} = 2^k t + 1$, entonces

$$a^{2^{k-1}} = \left(a^{2^{k-2}}\right)^2 = (2^k t + 1)^2$$
$$= 2^{2k} t^2 + 2^{k+1} t + 1$$
$$= 2^{k+1}(2^{k-1} t^2 + t) + 1 \equiv 1 \pmod{2^{k+1}}$$

por lo tanto $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ $\forall\, a \in (\mathbb{Z}_{2^k}, \cdot)$

entonces $o(a) \leq 2^{k-2} < 2^{k-1}$, de donde ningun $a \in (\mathbb{Z}2^k,\cdot)$, con $k > 2$ puede generar a $(\mathbb{Z}2^k,\cdot)$, por lo tanto $(\mathbb{Z}2^k,\cdot)$ no es ciclico. ∎

Teorema I.23.

Sea n entero positivo, si $(\mathbb{Z}n,\cdot)$ es ciclico, entonces $n = 2^{e_1}p^{e_2}$, con p primo impar y $e_1 = 0$ o 1; o bien $n = 4$.

Demostración:

Supongamos que $n = p_1^{e_1}p_2^{e_2}\cdot\ldots\cdot p_r^{e_r}$ la descomposición de n en potencias de primos, supongamos que existe $g \in (\mathbb{Z}n,\cdot)$ generador, entonces $o(g) = \phi(n)$, por el teorema de Euler tenemos

$$g^{\phi(p_j^{e_j})} \equiv 1 \pmod{p_j^{e_j}} \qquad \forall\ j = 1,\ldots,k.$$

Sea $N = [\phi(p_1^{e_1}),\phi(p_2^{e_2}),\ldots,\phi(p_r^{e_r})]$ entonces

$$\phi(p_j^{e_j}) \mid N = [\phi(p_1^{e_1}),\phi(p_2^{e_2}),\ldots,\phi(p_r^{e_r})]$$

es decir, para cada $0 \leq j \leq k$, $\exists\ t_j$ tal que $N = \phi(p_j^{e_j})t_j$ de aquí que

$$g^N = g^{\phi(p_j^{e_j})t_j} = \left(g^{\phi(p_j^{e_j})}\right)^{t_j} \equiv 1 \pmod{p_j^{e_j}} \qquad \forall\ j = 1,\ldots,k$$

entonces,

$$g^N \equiv 1 \pmod{n}$$

de aquí que

$$\phi(n) \leq N = [\phi(p_1^{e_1}),\phi(p_2^{e_2}),\ldots,\phi(p_r^{e_r})]$$

pero

$$N = [\phi(p_1^{e_1}),\phi(p_2^{e_2}),\ldots,\phi(p_r^{e_r})] \leq \phi(n) = \phi(p_1^{e_1})\phi(p_2^{e_2})\cdot\ldots\cdot\phi(p_r^{e_r})$$

por lo tanto

$$\phi(p_1^{e_1})\phi(p_2^{e_2})\cdot\ldots\cdot\phi(p_r^{e_r}) = [\phi(p_1^{e_1}),\phi(p_2^{e_2}),\ldots,\phi(p_r^{e_r})]$$

de aquí que los $\phi(p_j^{e_j})$ sean primos relativos entre si.

Si $p_i \neq p_j$ impares ,tenemos que

$$\phi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1) \quad y \quad \phi(p_j^{e_j}) = p_j^{e_j-1}(p_j - 1)$$

son ambos pares lo cual no puede pasar, por lo tanto $n = 2^{e_1}p^{e_2}$.

Ahora si $e_1 \geq 2$ y $e_2 \geq 1$, se tiene $\phi(2^{e_1}) = 2^{e_1-1}$ y $\phi(p_2^{e_2})$ son ambos

pares, lo cual no es posible, por lo tanto $e_1 < 2$ o $e_2 = 0$ y ya se probo que e_1 no puede ser mayor que 2.

Por lo tanto n es 4, o es de la forma $2p^{e_1}$. ∎

Con esto terminamos la demostración del Teorema I.17.

CAPITULO II.

NUMEROS SEUDOPRIMOS.

En este capítulo retomaremos la definición de número seudoprimo para estudiar algunas propiedades y consecuencias de éstas.

En la primera sección se demostrará que existe una infinidad de seudoprimos para cualquier base y una forma de construirlos; en las dos restantes se estudiaran dos tipos de números, números de Fermat y números de Mersenne que bajo ciertas condiciones resultan ser seudoprimos para la base 2.

II.1. SEUDOPRIMOS.

DEFINICION:

Sea b **entero positivo, si** n **es un entero compuesto positivo y**

$$b^n \equiv b \pmod{n}$$

se dice que n **es seudoprimo para la base** b.

Ejemplo:

91 es seudoprimo para la base 3, pues $3^{91} \equiv 3 \pmod{91}$, ya que $91 = 7 \cdot 13$ y por el teorema de Euler

$$3^6 \equiv 1 \pmod{7}$$

$$3^{12} \equiv 1 \pmod{13}$$

de aquí

$$3^{90} = (3^6)^{15} \equiv 1 \pmod 7$$

además

$$3^3 = 27 \equiv 1 \pmod{13}$$

entonces

$$3^{90} = 3^{12\cdot 7+6} = (3^{12})^7 (3^3)^2 \equiv 1 \pmod{13}$$

por lo tanto

$3^{90} \equiv 1 \pmod{91}$. 341 es seudoprimo para la base 2, pues $2^{341} \equiv 2 \pmod{341}$. $341 = 11\cdot 31$, por otro lado

$$2^{10} \equiv 1 \pmod{11} \quad \text{y} \quad 2^5 = 32 \equiv 1 \pmod{31}$$

entonces

$$2^{340} = (2^{10})^{34} \equiv 1 \pmod{11}$$

y

$$2^{340} = (2^5)^{68} \equiv 1 \pmod{31}$$

por lo tanto

$$2^{340} \equiv 1 \pmod{341}.$$

Si consideramos el grupo multiplicativo $(\mathbb{Z}_n, \cdot)$, n es seudoprimo para la base $b \in (\mathbb{Z}_n, \cdot)$ si n es compuesto y $b^{n-1} = 1$ en $\mathbb{Z}_n$.

Si tenemos un entero x tal que $(x,n) = 1$, por el algoritmo de la división existen $q, b \in \mathbb{Z}$ tales que;

$$x = nq + b \quad \text{y} \quad 0 \leq b < n$$

esto es, $x \equiv b \pmod n$. Por esa razón solo se considerarán en lo subsecuente bases $0 \leq b < n$. Además si $d = (b,n)$ se tiene que

$$d \mid b \quad \text{y} \quad d \mid n$$

implica que $d \mid (nq + b) = x$

entonces $d = 1$, es decir, $(b,n) = 1$, así que, $b \in (\mathbb{Z}_n, \cdot)$.

A continuación se verá que las bases para un seudoprimo forman un conjunto cerrado bajo el producto.

Teorema II.1.

Si n es seudoprimo para las bases b_1 y b_2, entonces n es seudoprimo para la base $b_1 b_2$.

Demostración:

Supongamos que n es seudoprimo para las bases b_1 y b_2, entonces;

$$b_1^n \equiv b_1 \pmod{n} \quad y \quad b_2^n \equiv b_2 \pmod{n}$$

Por lo tanto

$$(b_1b_2)^n \equiv b_1^n b_2^n \equiv b_1b_2 \pmod{n}. \blacksquare$$

Teorema II.2.

Sea n entero positivo compuesto.

a) Sea b positivo tal que $(b,n) = 1$, entonces;

n es seudoprimo para la base b si y sólo si el orden de b en $(\mathbb{Z}_n, \cdot)$ divide a $n - 1$.

b)Sea $b \in (\mathbb{Z}_n, \cdot)$ entonces;

n es seudoprimo para la base b si y sólo si n es seudoprimo para la base b^{-1}.

c)Sean $b_1, b_2 \in (\mathbb{Z}_n, \cdot)$ y supongamos que n es seudoprimo para las bases b_1 y b_2, entonces;

n es seudoprimo para la base $b_1b_2^{-1}$.

Demostración:

a)Sea b positivo tal que $(b,n) = 1$. Supongase que n es seudoprimo para la base b entonces,

$$b^n \equiv b \pmod{n}$$

y como $(b,n) = 1$ se tiene que;

$$b^{n-1} \equiv 1 \pmod{n}$$

luego el orden de b en $(\mathbb{Z}_n, \cdot)$ divide a $n - 1$.

Reciprocamente si el orden de b divide a $n - 1$ existe $k \in \mathbb{Z}$ tal que $o(b)k = n - 1$, entonces,

$$b^{n-1} = b^{o(b)k} \equiv 1 \pmod{n}$$

b)Sea $b \in (\mathbb{Z}_n, \cdot)$ y supongamos que n es seudoprimo para la base b, esto es;

$$b^n \equiv b \pmod{n}$$

multiplicando por $(b^{-1})^{n+1}$ tenemos

$$(b^{-1}) \equiv (b^{-1})^{n+1}b^n \equiv (b^{-1})^{n+1}b \equiv (b^{-1})^n \pmod{n}$$

Así n es seudoprimo para la base b^{-1}.

c)Este resultado es consecuencia directa del teorema II.1 junto con el inciso b. ■

Corolario II.2.1.

Sea n entero positivo compuesto y sea

$S = \{b \in (\mathbb{Z}_n, \cdot) \mid n$ es seudoprimo para la base $b\}$,

entonces S es subgrupo de $(\mathbb{Z}_n, \cdot)$.

Demostración:

Claramente n es seudoprimo para la base 1.

Del teorema anterior, si n es seudoprimo para las bases $b_1, b_2 \in (\mathbb{Z}_n, \cdot)$, n es seudoprimo para la base $b_1b_2^{-1}$. ■

Para enteros compuestos que sean el cuadrado de un primo es muy fácil determinar si se trata de un seudoprimo para alguna base, como se ve en el siguiente resultado.

Teorema II.3.

Sea p primo y sea $b \in (\mathbb{Z}_{p^2}, \cdot)$ entonces p^2 es seudoprimo para la base b si y solo si

$$b^{p-1} \equiv 1 \pmod{p^2}$$

Demostración:

Primero supongamos que p^2 es seudoprimo para la base b, entonces

$$b^{p^2} \equiv b \pmod{p^2}$$

o bien

$$b^{p^2-1} \equiv 1 \pmod{p^2}$$

así

$$1 \equiv b^{p^2-1} \equiv b^{(p-1)(p+1)} \equiv b^{p(p-1)+(p-1)} \equiv$$

$$b^{p^2-1} b^{(p-1)} \pmod{p^2}$$

y como el orden de $(\mathbb{Z}_{p^2}, \cdot)$ es $p(p-1)$, entonces

$$b^{p(p-1)} \equiv 1 \pmod{p^2},$$

por lo que

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

Notemos que este argumento es reversible, por tanto p^2 es seudoprimo para la base b si y solo si

$$b^{p-1} \equiv b \pmod{p^2}$$ ■

Dado un seudoprimo se puede encontrar otro a partir de éste como se ve en los siguientes resultados:

Primero considero la base 2 para posteriormente hacerlo para cualquier base.

Teorema II.4.

Sea n entero seudoprimo para la base 2, entonces;

$2^n - 1$ es seudoprimo para la base 2.

Demostración:

Sea $M = 2^n - 1$, como n es seudoprimo para la base 2, en particular n es compuesto.

Entonces $\exists\, d$ divisor propio de n. Por el *Lema* I.2 tenemos que

$$2^d - 1 \mid 2^n - 1$$

además $2^d - 1 \neq 1$ puesto que $d > 1$, y $2^d - 1 \neq 2^n - 1$ ya que $d \neq n$, es decir, M tiene un divisor propio, luego M es compuesto.

Ahora, ya que

$$2^n \equiv 2 \pmod{n},$$

$$n \mid 2^n - 2$$

es decir, existe $k \in \mathbb{Z}$ tal que

$$nk = 2^n - 2.$$

$$M - 1 = 2^n - 2 = nk,$$

de aquí que;

$$n \mid M - 1.$$

Por el *Lema* I.2.

$$M = 2^n - 1 \mid 2^{M-1} - 1,$$

entonces

$$2^{M-1} \equiv 1 \pmod{M}$$

Por tanto M es seudoprimo para para la base 2. ∎

El siguiente teorema nos prueba lo anterior para cualquier base:

Teorema II.5.

Sea n entero positivo, y b entero tal que $(b-1,n) = 1$ si n es seudoprimo para la base b, entonces

$$N = \frac{b^n-1}{b-1}$$

es seudoprimo para la base b.

Demostración:

Primero notemos que N es entero pues $b - 1 \mid b^n - 1$, (*Lema* I.2). Como n es seudoprimo para la base b, en particular n es compuesto, es decir, $\exists$ d divisor propio de n y por el *Lema* I.2. $b^d - 1 \mid b^n - 1$, ésto es, existe $k \in \mathbb{Z}$ tal que $(b^d - 1)k = b^n - 1$, de ésto se desprende que

$$\frac{b^n - 1}{b - 1} k = \frac{b^n - 1}{b - 1} = N$$

por lo tanto N es compuesto.

Consideremos

$$N - 1 = \frac{b^n - 1}{b - 1} - 1 = \frac{b^n - 1 - b + 1}{b - 1} = \frac{b^n - b}{b - 1}$$

como n es seudoprimo para la base b tenemos que se cumple

$$b^n \equiv b \pmod{n}$$

es decir,

$$n \mid b^n - b$$

entonces existe un entero l tal que $nl = b^n - b$, así que

$$N - 1 = \frac{b^n - b}{b - 1} = \frac{nl}{b - 1}$$

y como $(b - 1,n) = 1$, entonces

$$\frac{l}{b - 1} \quad \text{es entero,}$$

$$\therefore \quad n \mid N - 1.$$

Del *Lema* I.2 se sigue que

$$b^n - 1 \mid b^{N-1} - 1$$

entonces se tiene que $b^{N-1} - 1 = (b^n - 1)m$ p.a. $m \in \mathbb{Z}$. Por tanto

$$b^{N-1} - 1 = \frac{b^n - 1}{b - 1}(b - 1)m = N[(b - 1)m]$$

es decir,

$$b^{N-1} \equiv 1 \pmod{N}$$

así que

$$b^N \equiv b \pmod{N}$$

N es seudoprimo para la base b. ∎

Los números seudoprimos, al igual que otros tipos de enteros, constituyen un conjunto infinito como se vé abajo.

El siguiente lema nos servirá para demostrar que hay una infinidad de seudoprimos para las bases 2, 3 y 5. Despues probaremos el resultado para bases arbitrarias.

Lema II.1.

Si $n \geq 1$ e impar, entonces

a) $(2, \frac{3^n-1}{3-1}) = 1$.

b) $(4, \frac{5^n-1}{5-1}) = 1$.

Demostración:

a) Sea $d = (4, 3^n - 1)$, entonces d divide a 4 así que se tiene alguna de las siguientes posibilidades: $d = \begin{cases} 1 \\ 2 \\ 4 \end{cases}$

si $d = 4$ entonces

$$4 \mid 3^n - 1$$

lo cual no es posible según el *Lema* I.4. ya que n es impar.

Por lo tanto $d = 1$ o $d = 2$, pero claramente 2 divide a $3^n - 1$, de donde $d = 2$.

De aquí que

$$(2, \frac{3^n-1}{3-1}) = 1$$

b) Sea $d = (16, 5^n - 1)$ entonces d divide a $16 = 2^4$, así que d puede ser:

$$d = \begin{cases} 1 \\ 2 \\ 4 \\ 8 \\ 16 \end{cases}$$

vamos a probar que d no puede ser 8.

Si $d = 8$, entonces

$$8 \mid 5^n - 1$$

lo cual no puede pasar por el *Lema* I.4

Por lo tanto tenemos que $d \neq 8$. Ahora d no puede ser 16 ya que si $d = 16$

$$8 \mid 16 \mid 5^n - 1$$

lo cual no es posible.

Por el *Lema* I.4

$$4 \mid 5^n - 1$$

por lo tanto $d = 4$, de donde

$$4 = (16, 5^n - 1)$$

así que

$$(4, \frac{5^n - 1}{5 - 1}) = 1. \quad \blacksquare$$

Corolario II.5.1.

a) Existe un número infinito de seudoprimos para la base 2.

b) Existe un número infinito de seudoprimos para la base 3.

c) Existe un número infinito de seudoprimos para la base 5.

Demostración:

a) Para demostrar éste inciso, observemos que si $n > 1$ entonces; $n < 2^n - 1$ (*Lema* I.3), y sabemos que $n = 341$ es seudoprimo para la base 2.

De esta forma se puede generar una cadena infinita de seudoprimos para la base 2.

$$341 < 2^{341} - 1 < 2^{2^{341}-1} - 1 < \ldots$$

b) Como antes, tenemos que si $n > 1$ entonces por *Lema* I.5 $2n + 1 < 3^n$ de donde

$$n < \frac{3^n-1}{3-1}$$

y usando el teorema anterior junto con el lema se tiene que si n es seudoprimo para la base 3, entonces $\frac{3^n-1}{3-1}$ es seudoprimo para la base 3,

$$\frac{3^{\frac{3^n-1}{3-1}}-1}{3-1}$$

es seudoprimo para la base 3, etc., como $n = 91$ es seudoprimo para la base 3 entonces si hacemos

$$n_1 = 91,\ n_2 = \frac{3^{n_1}-1}{3-1},\ n_3 = \frac{3^{n_2}-1}{3-1},\ \ldots$$

entonces

$$n_1 < n_2 < n_3 < \ldots$$

es una cadena infinita de seudoprimos para la base 3.

c) De nuevo tenemos que $4n + 1 < 5^n \quad \forall\, n \in \mathbb{N}$, (segun *Lema* I.5) de aquí que $n < \frac{5^n-1}{5-1} \quad \forall\, n \in \mathbb{N}$.

Tenemos que

$$561 = 3 \cdot 11 \cdot 17$$

$$5^2 \equiv 1 \pmod 3$$

$$5^{10} \equiv 1 \pmod{11}$$

$$5^{16} \equiv 1 \pmod{17}$$

entonces

$$5^{560} = (5^2)^{280} \equiv 1 \pmod 3$$

$$5^{560} = (5^{10})^{56} \equiv 1 \pmod{11}$$

$$5^{560} = (5^{16})^{35} \equiv 1 \pmod{17}$$

por lo tanto

$$5^{560} \equiv 1 \pmod{561}$$

de donde

$5^5 \equiv 5 \pmod{561}$. Esto es: 561 es seudoprimo para la base 5. Por el teorema y lema anteriores

$$n_1 = 561,\ n_2 = \frac{5^{n_1}-1}{5-1},\ n_3 = \frac{5^{n_2}-1}{5-1}, \ldots.$$

todos son seudoprimos para la base 5 y además

$$n_1 < n_2 < n_3 < \ldots$$

son un conjunto infinito de seudoprimos para la base 5. ■

Tenemos hasta aquí una forma de construir seudoprimos para algunas bases a partir de un seudoprimo dado. El siguiente teorema nos dá una forma de construir seudoprimos para cualquier base.

Notemos que si $b = 1$ entonces cualquier entero compuesto positivo es seudoprimo para la base 1. Por esta razón en el teorema sólo se consideran bases mayores que 1.

Teorema II.6.

Sea b entero mayor que 1 y p primo tal que

$$p \nmid b(b^2 - 1)$$

entonces

$$n = \frac{b^{2p} - 1}{b^2 - 1}$$

es seudoprimo para la base b.

Demostración:

Notemoa que $p \neq 2$, pues b o $b^2 - 1$ es par.

Tenemos que n es entero ya que

$$2 \mid 2p$$

y por el *Lema* I.2. tenemos que

$$b^2 - 1 \mid b^{2p} - 1.$$

Además

$$n = \frac{b^{2p} - 1}{b^2 - 1} = \frac{b^p - 1}{b - 1}\,\frac{b^p + 1}{b + 1}$$

Por lo tanto n es compuesto.

Ya que

$$n - 1 = \frac{b^{2p} - 1}{b^2 - 1} - 1 = \frac{b^{2p} - 1 - b^2 + 1}{b^2 - 1} = \frac{b^{2p} - b^2}{b^2 - 1},$$

entonces

$$(b^2 - 1)(n - 1) = b^{2p} - b^2$$

y como p es primo tenemos

$$b^p \equiv b \pmod{p}$$

así que

$$b^{2p} \equiv b^2 \pmod{p}$$

es decir

$$p \mid b^{2p} - b^2 = (b^2 - 1)(n - 1).$$

Como además

$$p \nmid b^2 - 1$$

pues

$$p \nmid b(b^2 - 1)$$

se sigue que

$$p \mid n - 1$$

Ahora notemos que

$$(b^t - 1)(b^{(n-2)t} + b^{(n-3)t} + \ldots + b^t + b^t) =$$
$$b^{(n-1)t} + b^{(n-2)t} + b^{(n-3)t} + \ldots + b^{3t} + b^t$$
$$- b^{(n-2)t} - b^{(n-3)t} - \ldots - b^{2t} - b^t =$$
$$b^{(n-1)t} - b^t.$$

Por lo tanto

$$n - 1 = \frac{b^{(n-1)t} - b^t}{b^t - 1} = \underbrace{b^{(n-2)t} + b^{(n-3)t} + \ldots + b^t + b^t}_{p-1 \text{ sumandos}}$$

Como $p - 1$ es par, entonces $n - 1$ es suma par de potencias de b, por lo tanto $n - 1$ es par, es decir,

$$2 \mid n - 1$$

y como

$$p \mid n - 1$$

con $(p,2) = 1$ entonces,

$$2p \mid n - 1 .$$

Por el *Lema* 1.2.

$$b^{2p} - 1 \mid b^{n-1} - 1 .$$

Como

$$b^{2p} - 1 = \frac{b^{2p} - 1}{b^2 - 1}(b^2 - 1) .$$

esto implica que

$$n = \frac{b^{kp}-1}{b^{k}-1} \mid b^{n-1}-1.$$

Por lo tanto

$$b^{n-1} \equiv 1 \pmod{n}$$

entonces

$$b^{n} \equiv b \pmod{n} .$$

Por lo tanto n es seudoprimo para la base b. ∎

Lema II.1.

Sea x entero positivo, entonces existe una infinidad de primos que no dividen a x.

Demostración:

La demostración se sigue de el siguiente hecho:

El teorema fundamental de la aritmética nos dice que todo número positivo mayor que 1 se escribe como un producto finito de potencias de primos de manera única, por lo tanto la cantidad de primos que no dividen a un entero es infinito, ya que hay una infinidad de primos. ∎

Teorema II.7.

Para todo entero b positivo, existe una infinidad de enteros seudoprimos para la base b.

Demostración:

Sea $b > 0$, si $b = 1$ es obvio que existe una infinidad de seudoprimos para la base 1.

Supongamos que $b > 1$. Por el lema anterior existe una infinidad de primos que no dividen a $b(b^{k}-1)$, por el teorema anterior

$$n_{b} = \frac{b^{kp}-1}{b^{k}-1}$$

es seudoprimo para la base b para cada p primo que no divida a $b(b^{2}-1)$. Por lo tanto existe una infinidad de seudoprimos para la base b. ∎

Ejemplos:

Si $b = 2$, entonces $p = 5$ no divide a $2(2^{2}-1)$, por lo tanto

$$n = \frac{2^{k\cdot 5}-1}{2^{k}-1} = \frac{2^{10}-1}{3} = 341$$

es seudoprimo para la base 2.

Si $b = 3$, $p = 5$ no divide a $3(3^2-1)$, por lo tanto

$$n = \frac{3^{2\cdot 5}-1}{3^2-1} = \frac{3^{10}-1}{8} = 7381$$

es seudoprimo para la base 3.

Para finalizar esta sección vale la pena notar que no todos los seudoprimos son de la forma

$$\frac{b^{2p}-1}{b^2-1}$$

con p no es divisor de $b(2^{2-1})$, por ejemplo 91 es seudoprimo para la base 3 y si

$$91 = \frac{b^{2p}-1}{b^2-1} = \frac{b^{2p}-1}{8}$$

entonces

$$728 = 8\cdot 91 = 3^{2p}-1$$

es decir $727 = 3^{2p}$

Por otro lado, tenemos que $727 = 3^6 = 3^{2\cdot 3}$, esto diría que $3^{2p} = 3^{2\cdot 3} \Leftrightarrow 2p = 2\cdot 3$, así que $p = 3$, sin embargo

$$3 \mid 3(3^2-1) = 24 .$$

II.2. Números de Fermat.

Teorema II.8.

Sea n entero positivo. Si $2^n + 1$ es primo, entonces n es una potencia de 2.

Demostración:

Supongamos que 2^n+1 es primo, si resulta que $2^n+1 = 3$, entonces $n = 1 = 2^0$.

Supongamos que $n > 1$. Sea $d > 1$ divisor de n y supongamos que d es impar, entonces, como

$$d \mid n$$

$\exists\, k \in \mathbb{Z}$ tal que dk, además como $d \neq 1$ se tiene que $1 < k$ y como d es impar

$$(2^{s}+1)((2^{s})^{t-1}-(2^{s})^{t-2}+\ldots+(2^{s})^{2}-(2^{s})^{1}+(2^{s})^{0})$$

$$=(2^{s}+1)((2^{s})^{t-1}-(2^{s})^{t-2}+\ldots+(2^{s})^{2}-2^{s}+1)$$

$$=(2^{s})^{t}-(2^{s})^{t-1}+\ldots+(2^{s})^{3}-(2^{s})^{2}+2^{s}$$

$$+(2^{s})^{2}-(2^{s})^{1}+\ldots+(2^{s})^{2}-2^{s}+1$$

$$=(2^{s})^{t}+1=2^{st}+1=2^{n}+1$$

po lo tanto

$$2^{k}+1 \mid 2^{n}+1 \quad \forall$$

pues estamos suponiendo que $2^{n}+1$ es primo, por lo tanto d es par, si es divisor de n, por lo tanto $n=2^{m}$ p.a. $m \in \mathbb{N} \cup \{0\}$ que es lo que se quería probar. ■

Conclulmos que: si $2^{m}+1$ es primo entonces es de la forma $2^{(2^{r})}+1$.

DEFINICION:

Para cada $n \geq 0$ se define el *n-ésimo* entero de Fermat como

$$F_{n}=2^{2^{n}}+1.$$

Ejemplos:

$$F_{0}=2^{2^{0}}+1=3.$$

$$F_{1}=2^{2^{1}}+1=5.$$

$$F_{2}=2^{2^{2}}+1=17.$$

Fermat conjeturó que todos estos números son primos, pero desafortunadamente ésto es falso como lo muestra el siguiente teorema:

Teorema II.9.

El quinto entero de Fermat $F_{5}=2^{2^{5}}+1$ es divisible por 641.

Demostración:

Notemos que

$$641=16+625=2^{4}+5^{4}$$

y

$$641=640+1=5\cdot 128+1=5\cdot 2^{7}+1$$

de aquí que

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 =$$
$$2^4 2^{28} + 1 = (641 - 5^4)2^{28} + 1 =$$
$$641 \cdot 2^{28} - 5^4(2^7)^4 + 1 =$$
$$641 \cdot 2^{28} - (641 - 1)^4 + 1 =$$
$$641 \cdot 2^{28} - (641^4 - 4 \cdot 641^3 + 6 \cdot 641^2 - 4 \cdot 641 + 1) + 1 =$$
$$641(2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4) - 1 + 1 =$$
$$641(2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4).$$

Por lo tanto

$$641 \mid F_5. \quad \blacksquare$$

En el capítulo V daré una condición necesaria y suficiente para que F_n sea primo.

El siguiente resultado nos dice de que forma son los divisores primos de un entero de Fermat.

Teorema II.10.

Sea $F_n = 2^{2^n} + 1$ un entero de Fermat, entonces los divisores primos de F_n son de la forma $2^{n+1}k + 1$, $k \in \mathbb{Z}$.

Demostración:

Sea p divisor primo de F_n, entonces

$$p \mid F_n = 2^{2^n} + 1$$

notemos que $p \neq 2$, pues F_n es impar. Como

$$p \mid 2^{2^n} + 1$$

se tiene

$$2^{2^n} \equiv -1 \pmod{p}$$

de aquí que

$$(2^{2^n})^r \equiv (-1)^r \equiv 1 \pmod{p}$$

por lo tanto

$$2^{2^{n+1}} \equiv 1 \pmod{p}.$$

Como $p \neq 2$, entonces $(2,p) = 1$, por lo tanto $2 \in (\mathbb{Z}_p, \cdot)$, entonces

$$o(2) \mid 2^{n+1},$$

por lo tanto $o(2) = 2^m$ para alguna $0 < m \leq n + 1$. Supongamos que $m < n + 1$, es decir que $m \leq n$, así que $n - m \geq 0$ y por lo tanto $2^{n-m} \geq 1$.

Como $o(2) = 2^m$ se tiene

$$2^{2^m} \equiv 1 \pmod{p}$$

entonces

$$(2^{2^m})^{2^{n-m}} \equiv 1 \pmod{p}$$

pero

$$(2^{2^m})^{2^{n-m}} \equiv 2^{2^m 2^{n-m}} \equiv 2^{2^n} \equiv -1 \pmod{p}$$

por lo tanto

$$1 \equiv -1 \pmod{p} \quad \nabla_0 \quad \text{pues} \quad p \neq 2.$$

Entonces $m = n + 1$, por lo tanto $o(2) = 2^{n+1}$.

Como $p \neq 2$ se tiene que $(p,2) = 1$, entonces

$$2^{p-1} \equiv 1 \pmod{p},$$

entonces

$$2^{n+1} = o(2) \mid p - 1 .$$

Por lo tanto $\exists\, k \in \mathbb{Z}$ tal que $2^{n+1}k = p - 1$, de donde se concluye que

$$p = 2^{n+1}k + 1$$

■

En el capítulo V demostraremos que $p = 2^{n+2}k + 1$ cuando $n \geq 3$.

Teorema II.11.

$\forall\, n \in \mathbb{N}$.

$$F_0F_1 \cdot \ldots \cdot F_{n-1} = F_n - 2.$$

Demostración:

La demostración se hace por inducción.

$n = 1$.

$$F_1 - 2 = 2^{2^1} + 1 - 2 = 3 = 2^{2^1} + 1 = F_0$$

Supongamos que

$$F_0F_1 \cdot \ldots \cdot F_{n-1} = F_n - 2$$

Tenemos que

$$F_0F_1 \cdot \ldots \cdot F_{n-1}F_n = (F_0F_1 \cdot \ldots \cdot F_{n-1})F_n =$$

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

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

$$2^{2^{n+1}} + 1 - 2 = F_{n+1} - 2$$

lo cual completa la demostración. ∎

Teorema II.12.

Si $n \neq m$ entonces

$$(F_n, F_m) = 1.$$

Demostración:

Sin perdida de generalidad podemos suponer $m < n$.

Por el teorema anterior

$$F_{n'} \mid F_n - 2 \quad \forall\ 0 \leq n' < n.$$

Como $m < n$ entonces

$$F_m \mid F_n - 2,$$

es decir, $\exists\ k \in \mathbb{Z}$ tal que $F_m \cdot k = F_n - 2$.

Sea $d = (F_m, F_n)$ entonces

$$d \mid F_m \ \text{ y } \ d \mid F_n$$

por lo tanto

$$d \mid F_m \cdot k = F_n - 2 \ \text{ y } \ d \mid F_n.$$

Entonces $d \mid 2$ luego $d = 1$ o $d = 2$.

Si $d = 2$, entonces

$$2 \mid F_n = 2^{2^n} + 1$$

lo cual no es posible. Por lo tanto $d = 1$.

Lo cual completa la demostración. ∎

Teorema II.13.

Sea $n \geq 0$ entonces $F_n = 2^{2^n} + 1$ es primo o es seudoprimo para la base 2.

Demostración:

Notemos que

$$2^{F_n} = 2^{2^{2^n}+1} = 2 \cdot 2^{2^{2^n}} =$$

$$2 \cdot 2^{2^{2^n}} + 2 - 2 = 2(2^{2^{2^n}} + 1) - 2 =$$

$$2\cdot F_{2^n} - 2 = F_{2^n} + (F_{2^n} - 2) \equiv F_{2^n} \equiv 2 \pmod{F_n}$$

puesto que $n < 2^n$ (*Lema* I.3) y $F_{2^n} - 2$ es dividido por F_n.

Por lo tanto

$$2^{F_n} \equiv 2 \pmod{F_n}$$

es decir F_n es seudoprimo para la base 2, si F_n no es primo. ∎

II.3. Números de Mersenne.

DEFINICION:

Sea m un entero positivo, entonces el número

$$M_m = 2^m - 1$$

es llamado el m-ésimo número de Mersenne.

Si para p primo $Mp = 2^p - 1$ también es primo, entonces a M_p se le llama primo de Mersenne. Esta definición es adecuada en vista del Teorema II.14.

Ejemplos:

$M_1 = 2^1 - 1 = 1$.

$M_2 = 2^2 - 1 = 3$.

$M_3 = 2^3 - 1 = 7$.

$M_4 = 2^4 - 1 = 15$.

En los ejemplos M_2 y M_3 son primos de Mersenne.

Teorema II.14.

Sea n entero positivo, entonces $M_n = 2^n - 1$ primo implica que n es primo.

Demostración:

Haré la demostración por contra puesta.

Supongamos que n es compuesto entonces $n = ab$ con $1 < a < n$ y $1 < b < n$, por lo tanto

$$M_n = 2^n - 1 = 2^{ab} - 1 .$$

Por el *Lema* I.2.

$$2^a - 1 \mid 2^{ab} - 1 ,$$

de ésto se sigue que $M_n = 2^n - 1$ es compuesto. ∎

Desafortunadamente el recíproco de este teorema no es válido por ejemplo:

$$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89.$$

es decir, M_{11} no es primo, sin embargo, 11 es primo.

En el siguiente resultado se dara la forma que tienen los divisores primos de un número de Mersenne M_p cuando p es primo.

Teorema II.15.

Sea p primo, entonces los divisores primos de

$$M_p = 2^p - 1$$

son de la forma $2kp + 1$, con $k > 0$.

Demostración:

Sea q divisor primo de $M_p = 2^p - 1$, por lo tanto

$$q \mid 2^p - 1$$

esto es

$$2^p \equiv 1 \ (mod\ q) .$$

Además $q \neq 2$, pues si $q = 2$ tendríamos que

$$2 \nmid 2^p - 1$$

lo cual no es posible, por lo tanto $(q,2) = 1$, entonces $2 \in (Z_q, \cdot)$. Como

$$2^p \equiv 1 \ (mod\ q)$$

se tiene que el orden de 2 divide a p, pero p es primo. por lo tanto $o(2) = p$ así que

$$p \mid q - 1 .$$

Además $q - 1$ es par, ésto es

$$2 \mid q - 1$$

por lo tanto

$2p \mid q - 1$. $\therefore$ $\exists\, k \in \mathbb{Z}$ tal que $2pk = q - 1$, es decir, $q = 2pk + 1$. ■

Teorema II.16.

Sea p primo, entonces el p-ésimo número de Mersenne es primo o bien seudoprimo para la base 2.

Demostración:

Tenemos que $M_p = 2^p - 1$, entonces $M_p - 1 = 2^p - 2$, por lo tanto $2^{M_p-1} = 2^{2^p-2}$. Por otro lado tenemos que

$$2^p \equiv 2 \pmod{p} .$$

Esto es,

$$p \mid 2^p - 2$$

de donde

$$M_p = 2^p - 1 \mid 2^{2^p-2} - 1 = 2^{M_p-1} - 1 ,$$

$$\therefore \quad 2^{M_p-1} \equiv 1 \pmod{M_p}$$

entonces

$$2^{M_p} \equiv 2 \pmod{M_p}$$

por lo tanto M_p es seudoprimo para la base 2, si M_p no es primo. ■

CAPITULO III.

NUMEROS DE CARMICHAEL.

III.1 NUMEROS DE CARMICHAEL.

El teorema de Euler nos dice que si p es primo se cumple

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{para todo } a \in (Z_p, \cdot)$$

lo cual nos dá una buena aproximación para saber si un número es primo, ya que si

$$a^{n-1} \not\equiv 1 \pmod{n}$$

para algún $a \in (Z_n, \cdot)$, entonces n es compuesto.

Por ejemplo:

$n = 341$.

tenemos que

$$2^{10} = 1024 \equiv 1 \pmod{341}$$

y

$$7^3 = 343 \equiv 2 \pmod{341}$$

así

$$7^{340} = (7^3)^{113}7 \equiv 2^{113}7 \equiv 2^{110}2^27 \equiv 28 \not\equiv 1 \pmod{341}$$

por lo tanto 341 es compuesto.

El recíproco de este teorema es falso, pues hay números compuestos que siguen cumpliendo la congruencia anterior, por ejemplo:

$n = 561 = 3 \cdot 11 \cdot 17$, si $b \in (\mathbb{Z}_n, \cdot)$, entonces b es elemento de $(\mathbb{Z}_3, \cdot)$, $(\mathbb{Z}_{11}, \cdot)$ y de $(\mathbb{Z}_{17}, \cdot)$, de donde

$$b^2 \equiv 1 \pmod 3$$
$$b^{10} \equiv 1 \pmod{11}$$
$$b^{16} \equiv 1 \pmod{17}$$

es decir,

$$b^{560} \equiv (b^2)^{280} \equiv 1 \pmod 3$$
$$b^{560} \equiv (b^{10})^{56} \equiv 1 \pmod{11}$$
$$b^{560} \equiv (b^{16})^{35} \equiv 1 \pmod{17}$$

por lo tanto

$$b^{560} \equiv 1 \pmod{561}.$$

Este tipo de enteros recibe un nombre especial:

DEFINICION:

Sea n entero compuesto positivo, n se llama número de Carmichael si cumple con

$$b^{n-1} \equiv 1 \pmod n \quad \forall\ b \text{ tal que } (b,n) = 1.$$

De nuevo, como b es congruente con algún entero entre cero y $n - 1$, restringiremos nuestra atención a los enteros b tales que $0 \leq b \leq n - 1$. Entonces la definición se puede cambiar por la siguiente:

DEFINICION:

Sea n entero compuesto positivo, n se llama número de Carmichael si cumple con

$$b^{n-1} \equiv 1 \pmod n \quad \forall\ b \in (\mathbb{Z}_n, \cdot).$$

A través de los siguientes resultados se puede observar que los números de Carmichael se descomponen como un producto de más de tres primos distintos donde cada uno de ellos no aparece más de una vez en dicha

descomposición.

DEFINICION:

·) Un entero k se llama cuadrado perfecto si $k = m^2$ para algun $m \in \mathbb{Z}$.

··) Se dice que el entero n es libre de cuadrados si no es dividido por ningun cuadrado perfecto distinto de 1.

Lema III.1.

n es libre de cuadrados si y sólo si

$$n = \pm\, p_1 p_2 \cdot \ldots \cdot p_k$$

donde p_i's son primos y $p_i \neq p_j$ cuando $i \neq j$.

Demostración:

$\Longrightarrow$)Consideremos a $n = \pm\, p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$, su descomposición como potencias de primos.

Supongamos que $e_j \geq 2$ p.a. $j \in \{1, \ldots, k\}$, entonces

$$p^2 \mid p^{e_j} \mid n \,,$$

lo cual no es posible, pues n es libre de cuadrados, por lo tanto

$$n = \pm\, p_1 p_2 \cdot \ldots \cdot p_k \,.$$

$\Longleftarrow$) Si n no es libre de cuadrados entonces $m^2 \mid n$, así que si p primo divide a m entonces $p^2 \mid m^2 \mid n$. ∎

Proposición III.1. *(Teorema Chino del residuo).*

Sean $m_1, m_2, \ldots, m_k$ enteros positivos tales que $(m_i, m_j) = 1$ siempre que $i \neq j$, entonces el sistema

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_k} \end{aligned}$$

tiene solución, además cualquier par de soluciones son congruentes modulo $M = m_1 m_2 \cdot \ldots \cdot m_k$.

Demostración:

Primero supongamos que x_0, x_1 son soluciones del sistema,

entonces

$$x_0 \equiv x_i \pmod{m_i} \quad \forall\, j = 1,\ldots,n$$

es decir

$$m_j \mid x_0 - x_i \quad \forall\, j = 1,\ldots,n$$

de donde

$$[m_1, m_2, \ldots, m_n] = M \mid x_0 - x_i$$

es decir,

$$x_0 \equiv x_i \pmod{M} .$$

Ahora, para cada $i = 1,\ldots,n$, hacemos $M_i = \frac{M}{m_i}$, entonces $(M_i, m_i) = 1$, de aquí, $\exists\, x_i, y_i \in \mathbb{Z}$ tales que

$$1 = M_i x_i + m_i y_i$$

entonces

$$M_i x_i \equiv 1 \pmod{m_i} ,$$

por lo tanto

$$a_i M_i x_i \equiv a_i \pmod{m_i} .$$

Sea $x = \sum_{i=1}^{n} a_i M_i x_i$. Como $m_j \mid M_i$, siempre que $i \neq j$, entonces

$$x \equiv a_j M_j x_j \equiv a_j \pmod{m_j} \quad \forall\, j = 1,\ldots,n$$

es decir x es solución del sistema. ∎

Teorema III.1.

Si n es de Carmichael, entonces n es libre de cuadrados.

Demostración:

Por contraposición.

Supongamos que $m^2 \mid n$, entonces $p^2 \mid n \quad \forall\ p$ primo divisor de m.

Tomemos p cualquier divisor primo de m.

Sea $g \in (\mathbb{Z}_{p^e}, \cdot)$ generador, entonces $o(g) = p(p - 1)$ en $(\mathbb{Z}_{p^e}, \cdot)$. Hacemos

$$n = \prod_{\substack{q \text{ primo} \\ q \mid n \\ q \neq p}} q$$

entonces por el teorema Chino del residuo 3 b tal que

$$b \equiv g \pmod{p^2}$$

$$b \equiv 1 \pmod{n_1} \qquad (1)$$

por lo tanto

$$b \in (\mathbb{Z}_{p^2}, \cdot) \quad y \quad o(b) = p(p-1)$$

y además

$$1 = b - nt \quad \text{para alguna} \quad t \in \mathbb{Z} \text{ por (1)}$$

así que

$$(b, p^2) = 1 \ , \ (b, n_1) = 1$$

por lo tanto

$$(b, n) = 1 \ .$$

Supongamos que n es de Carmichael, luego

$$b^{n-1} \equiv 1 \pmod{n}$$

y como $p^2 \mid n$ entonces

$$b^{n-1} \equiv 1 \pmod{p^2}$$

de aquí

$$o(b) = p(p-1) \mid n - 1$$

esto implica que $p \mid n - 1$, lo cual no puede pasar, pues $p \mid n$ por lo tanto n no puede ser de Carmichael. ∎

Teorema III.2.

Sea n positivo libre de cuadrados, entonces n es de Carmichael sí y solo sí $p - 1 \mid n - 1$ para todo p primo que divida a n.

Demostración :

Primero supongamos que $p_j - 1 \mid n - 1 \ \forall \ j = 1,2,\ldots,k$ luego, para cada $j = 1,2,\ldots,k$ $\exists \ t_j$ tal que $(p_j - 1)t_j = n - 1$.

Sea $(b,n) = 1$, entonces

$$(b,p_j) = 1 \quad \forall \quad j = 1,2,\ldots,k$$

de aquí

$$b^{p_j-1} \equiv 1 \pmod{p_j} \quad \forall \; j = 1,2,\ldots,k$$

así

$$b^{n-1} \equiv b^{(p_j-1)t_j} \equiv \left(b^{p_j-1}\right)^{t_j} \equiv 1 \pmod{p_j} \quad \forall \; j = 1,2,\ldots,k$$

es decir

$$b^{n-1} \equiv 1 \pmod{n}$$

por lo tanto, n es de Carmichael.

Ahora supongamos que n es de Carmichael.

Sea p primo divisor de n, y g generador de $(\mathbb{Z}_p,\cdot)$.

Como $(p,\frac{n}{p}) = 1$, $\exists\, b$ tal que

$$b \equiv g \pmod{p}$$

$$b \equiv 1 \pmod{\frac{n}{p}}$$

entonces

$$o(g) = o(b) = p - 1 \quad y \quad (b,n) = 1$$

pues

$$(b,\frac{n}{p}) = 1 \quad y \quad (b,p) = 1.$$

Como n es de Carmichael

$$b^{n-1} \equiv 1 \pmod{n}$$

de aquí

$$b^{n-1} \equiv 1 \pmod{p}$$

por lo tanto

$$o(b) = p - 1 \mid n - 1. \blacksquare$$

Teorema III.3.

Si n es de Carmichael, entonces n es producto de más de dos primos distintos.

Demostración:

Supongamos que $n = pq$, y p , q son primos distintos; sin pérdida de generalidad podemos suponer $p < q$.

Por ser n de Carmichael se tiene que

$$q - 1 \mid n - 1$$

es decir

$$n - 1 \equiv 0 \pmod{q - 1}.$$

Además

$$n - 1 = pq - 1 = p(q - 1 + 1) - 1 \equiv p - 1 \pmod{q - 1}$$

pues

$$q - 1 + 1 \equiv 1 \pmod{q - 1}$$

de aquí

$$n - 1 \equiv p - 1 \equiv 0 \pmod{q - 1}$$

es decir:

$$q - 1 \mid p - 1$$

lo cual no es posible, pues $p < q$. ■

En el capítulo anterior pudimos probar la existencia de una infinidad de seudoprimos para una base dada, desafortunadamente no se ha podido probar esto mismo para los números de Carmichael, sin embargo, hay indicios de que existe una infinidad de ellos. Todos los intentos por demostralo son tambien conjeturas.

Observemos el siguiente teorema:

Teorema III.4.

Sea m positivo tal que $6m + 1$, $12m + 1$ y $18m + 1$ son primos, entonces

$$n = (6m + 1)(12m + 1)(18m + 1)$$

es de Carmichael.

Demostración:

En vista del **Teorema III.2.** basta demostrar que $6m$, $12m$ y $18m$ dividen a $n - 1$.

Notemos que

$$\begin{aligned} n - 1 &= (6m + 1)(12m + 1)(18m + 1) - 1 = \\ &(6 \cdot 12m^2 + 18m + 1)(18m + 1) - 1 = \\ &6 \cdot 12 \cdot 18m^3 + (6 \cdot 12 + 18^2)m^2 + 36m + 1 - 1 = \\ &m(6 \cdot 12 \cdot 18m^2 + (6 \cdot 12 + 18^2)m + 36). \end{aligned}$$

Por otro lado

$$6\cdot 12\cdot 18m^3 + (6\cdot 12 + 18^2)m + 36 =$$
$$6(12\cdot 18m^3 + (12 + 3\cdot 18)m + 6) =$$
$$12(6\cdot 18m^3 + (6 + 3^2\cdot 3)m + 3) =$$
$$18(6\cdot 12m^3 + (4 + 18)m + 2 .$$

Por lo tanto $6m$, $12m$ y $18m$ dividen a $n - 1$. ∎

Ejemplos:

Para $m = 1$

$$1729 = 7\cdot 13\cdot 19.$$

$m = 6$

$$294409 = 37\cdot 73\cdot 109.$$

$m = 35$

$$55164051 = 211\cdot 421\cdot 621.$$

$m = 45$

$$118901521 = 271\cdot 541\cdot 811.$$

$m = 51$

$$72947529 = 307\cdot 613\cdot 919.$$

Es natural pensar que existen muchos enteros m que hacen posible que $6m + 1$, $12m + 1$ y $18m + 1$ sean primos, pero esto aún no está demostrado.

Conjetura:

Existe una infinidad de números de Carmichael.

Sin embargo el siguiente resultado nos muestra algunos tipos de número de Carmichael, de los cuales sólo hay una cantidad finita:

Teorema III.5.

Sea r entero primo fijo, entonces existe sólo una cantidad finita de números de Carmichael de la forma rpq, con p y q primos.

Demostración:

Sea r primo, supongamos que rpq es de Carmichael, entonces $p - 1 \mid rpq - 1$ y $q - 1 \mid rpq - 1$, es decir,

$$rpq \equiv 1 \pmod{p - 1}$$
$$rpq \equiv 1 \pmod{q - 1}$$

pero $p \equiv 1 \pmod{p-1}$ y $q \equiv 1 \pmod{q-1}$, por lo tanto

$$rq \equiv 1 \pmod{p-1}$$

$$rp \equiv 1 \pmod{q-1}$$

de aquí $rq = 1 + k(p-1)$ y $rp = 1 + s(q-1)$, de donde

$$\begin{aligned} r^2q &= r + k(rp - r) \\ &= r + k(1 + s(q-1) - r) \\ &= r + k + ksq - ks - kr, \end{aligned}$$

es decir,

$$q = \frac{r + k - ks - kr}{r^2 - ks}$$

y como q es entero positivo se tiene que $r + k - ks - kr < 0$ y $r^2 - ks < 0$ o bien $r + k - ks - kr \geq 0$ y $r^2 - ks > 0$, si pasa $r + k - ks - kr \geq 0$ y $r^2 - ks > 0$, entonces $0 < ks < r^2$ en cuyo caso existe sólo un número finito de parejas (r,s) que cumplen la condicion $0 < ks < r^2$; si pasa $r + k - ks - kr < 0$ y $r^2 - ks < 0$, se tiene

$$\begin{aligned} q &= \frac{r + k - ks - kr}{r^2 - ks} \\ &= \frac{ks + kr - k - r}{ks - r^2} \\ &= 1 + \frac{kr - k + r^2 - r}{ks - r^2} \end{aligned}$$

pero q es entero, por lo tanto debe pasar que

$$ks - r^2 \leq kr - k + r^2 - r$$

de donde $ks - kr + k \leq 2r^2 - r$, es decir, $k(s - r + 1) \leq 2r^2 - r$ y en este caso tambien sólo hay un número finito de parejas (r,s) que cumplan la condición $r + k - ks - kr \geq 0$ y $ks - r^2 > 0$, por lo tanto q sólo puede tomar un número finito de valores y para p pasa lo mismo ■

CAPITULO IV.

SEUDOPRIMOS FUERTES.

IV.1. LA PRUEBA DE MILLER.

Supongamos que p es primo y que $p - 1 = 2^s t$, con $s \geq 0$ y t entero impar, (lo cual siempre es posible ya que todo entero n se descompone de la forma $n = 2^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_i^{\alpha_i}$, con los p_i's primos impares).

Por ser p primo se tiene

$$b^{p-1} \equiv 1 \pmod{p} \quad \forall\, b \text{ tal que } p \nmid b.$$

Si $2^s t = p - 1$ es par, entonces

$$b^{2^{s-1}t} = b^{(p-1)/2} \equiv 1 \pmod{p}$$

o

$$b^{2^{s-1}t} = b^{(p-1)/2} \equiv -1 \pmod{p}$$

Si $2^{s-1}t$ sigue siendo par y además

$$b^{2^{s-1}t} \equiv 1 \pmod{p}$$

se tiene

$$b^{2^{s-2}t} = b^{(p-1)/4} \equiv 1 \pmod{p}$$

o

$$b^{2^{s-2}t} = b^{(p-1)/4} - 1 \pmod{p}$$

y así, si se puede seguir el procedimiento tendríamos que

$$b^t \equiv 1 \pmod{p}.$$

Resumiendo: si p es primo y $p - 1 = 2^s t$, $s \geq 0$ y t impar, se tiene

$$b^{2^j t} \equiv -1 \pmod{p} \quad \text{para alguna} \quad 0 \leq j < s$$

o

$$b^t \equiv 1 \pmod{p}.$$

De todo ésto se puede concluir lo siguiente:

Teorema IV.1.

Sea n entero positivo y $n - 1 = 2^s t$, con $s \geq 0$ y t impar, entonces si

i) $b^{2^j t} \equiv -1 \pmod{n}$ $\forall$ j tal que $0 \leq j < s$

y

ii) $b^t \not\equiv 1 \pmod{n}$ para algun b tal que $(b,n) = 1$, implica que n es compuesto. ∎

El recíproco de este teorema es falso como lo indican los siguiente ejemplos:

1. $n = 2047 = 23 \cdot 89$, y $n - 1 = 2046 = 2 \cdot 1023$.

Tenemos

$$2^{11} = 2048 \equiv 1 \pmod{2047}$$

por lo tanto

$$2^{1023} = (2^{11})^{93} \equiv 1 \pmod{2047}.$$

2. $n = 25$ y $n - 1 = 24 = 2^3 \cdot 3$, además

$$7^2 = 49 \equiv -1 \pmod{25}$$

de aquí

$$7^{2^2 \cdot 3} = (7^2)^3 \equiv (-1)^3 \equiv -1 \pmod{25}.$$

DEFINICION:

Sean n entero positivo tal que $n - 1 = 2^s t$, $s \geq 0$, t impar y b entero, se dice que n cumple con la prueba de Miller para la base b si

$$b^{2^j t} \equiv -1 \pmod{p} \quad \text{para alguna} \quad 0 \le j < s$$

o

$$b^t \equiv 1 \pmod{n}.$$

En caso de ser $n - 1$ impar, se toma sólo la congruencia

$$b^t \equiv 1 \pmod{n}.$$

Corolario IV.1.1.

Si p es primo impar, entonces cumple con la prueba de Miller para toda $b \in (\mathbb{Z}_p, \cdot)$.

Demostración:

La demostración se sigue del **Teorema IV.1.** ya que si p no cumple con la prueba de Miller para alguna b p sería compuesto. ∎

Teorema IV.2.

Si n es entero compuesto positivo y cumple con la prueba de Miller para alguna base b, entonces n es seudoprimo para la base b.

Demostración:

Como n cumple con la prueba de Miller para la base b se tiene

$$b^{2^j t} \equiv -1 \pmod{p} \quad \text{para alguna} \quad 0 \le j < s$$

o

$$b^t \equiv 1 \pmod{n},$$

entonces

$$b^{s-1} = b^{2^{s-1} t} = \left(b^{2^j t}\right)^{2^{s-1-j}} \equiv (-1)^{2^{s-1-j}} \equiv 1 \pmod{n}$$

o

$$b^{s-1} = b^{2^{s-1} t} \equiv \left(b^t\right)^{2^{s-1}} \equiv 1^{2^{s-1}} \equiv 1 \pmod{n}.$$

Por lo tanto

$$b^n \equiv b \pmod{n},$$

es decir, n es seudoprimo para la base b. ∎

Al igual que el subconjunto de bases b en $(\mathbb{Z}_n, \cdot)$ para las cuales n resulta ser seudoprimo para la base b, el subconjunto de bases b en $(\mathbb{Z}_n, \cdot)$ par las cuales n cumple la prueba de Miler resulta ser un grupo.

Teorema IV.3.

Sea n entero positivo, supongamos que n cumple con la prueba de Miller para las bases b_1, b_2, entonces

·) n cumple con la prueba de Miller para la base 1.

··) n cumple con la prueba de Miller para la base $b_1 b_2$.

···) Si $b_1 \in (Z_n, \cdot)$, entonces n cumple con la prueba de Miller para la base b_1^{-1}.

····) Si $b_1, b_2 \in (Z_n, \cdot)$, entonces n cumple con la prueba de Miller para la base $b_1 b_2^{-1}$

Demostración:

Sea $n - 1 = 2^s t$, $s \geq 0$ y t impar.

Como n cumple con la prueba de Miller para las bases b_1, b_2 se tiene

i)

$$\text{a) } b_1^{2^j t} \equiv -1 \pmod{n} \quad \text{p.a. } 0 \leq j < s$$

o

$$\text{b) } b_1^t \equiv 1 \pmod{n}$$

y

ii)

$$\text{a) } b_2^{2^j t} \equiv -1 \pmod{n} \quad \text{p.a. } 0 \leq k < s$$

o

$$\text{b) } b_2^t \equiv 1 \pmod{n}$$

·) Es claro que

$$1^t \equiv 1 \pmod{n}.$$

··) Supongamos que se cumple el inciso *i*a) e inciso *ii*a) supongamos que $k \leq j$, (el caso $k > j$ es análogo), entonces existe $m \in \mathbb{N} \cup \{0\}$ tal que $k + m = j$ de donde $2^k t \leq 2^j t = 2^m(2^k t)$, de aquí que

$$(b_1 b_2)^{2^j t} \equiv b_1^{2^j t} b_2^{2^j t} \equiv b_1^{2^j t} \left(b_2^{2^j t}\right)^{2^m} \equiv 1 \pmod{n}.$$

Si se cumple *i*b) y *ii*b) se tiene

$$(b_1 b_2)^t \equiv b_1^t b_2^t \equiv 1 \pmod{n}.$$

Si pasa *i*a) y *ii*b) tenemos

$$(b_i b_\epsilon)^{2^t} \equiv b_i^{2^t}\left(b_\epsilon^t\right)^2 \equiv 1 \pmod{n},$$

análogamente si pasa *ib)* y *iia)*.

Por lo tanto n cumple con la prueba de Miller para para la base $b_i b_\epsilon$.

$\cdots$) Tenemos que

$$(b_i^{\cdot})^{2^t} \equiv \left(b_i^{2^j t}\right)^{-1} \equiv -1 \pmod{n} \quad \text{p.a. } 0 \le j < s$$

o

$$(b_i^{\cdot})^t \equiv \left(b_i^t\right)^{-1} \equiv 1 \pmod{n}$$

Por lo tanto n cumple con la prueba de Miller para la base $b_i^{\cdot}$.

$\cdots\cdot$) La demostración es consecuencia directa de $\cdot\cdot$) y $\cdots$). ∎

Corolario IV.3.1.

Sea n entero positivo fijo, si

$R_n = \{b \in (\mathbb{Z}_n, \cdot) \mid n$ cumple con la prueba de Miller para la base $b\}$,

entonces R_n es subgrupo de $(\mathbb{Z}_n, \cdot)$.

No es fácil determinar las bases b para las que n cumple con la prueba de Miller, sin embargo, se puede dar una muy buena estimación de la cantidad de bases para las cuales n cumple con la prueba de Miller.

Lema IV.1.

Sea p primo impar, entonces la congruencia

$$x^n \equiv 1 \pmod{p^k} \quad k \ge 1$$

tiene exactamente $(n, p^{k-1}(p-1))$ soluciones incongruentes.

Demostración:

Como p es primo impar $(\mathbb{Z}_{p^k}, \cdot)$ es cíclico de orden $p^{k-1}(p-1)$, sea g un generador, entonces cualquier solución de la congruencia es de la forma g^i, pero

$$(g^i)^n \equiv 1 \pmod{p^k}$$

si y sólo si $I_g((g^i)^n) \equiv 0 \pmod{p^{k-1}(p-1)}$ si y sólo si

$$n I_g((g^i)^n) \equiv 0 \pmod{p^{k-1}(p-1)}$$

si y sólo si $ni \equiv 0 \pmod{p^{k-1}(p-1)}$ y esta última congruencia siempre tiene solución y además tiene exactamente $(n, p^{k-1}(p-1))$ soluciones. ∎

Lema IV.2.

Si $p \nmid n$, p primo, entonces

$$(n-1, p^k(p-1)) = (n-1, p-1).$$

Demostración:

Sean $d = (n-1, p-1)$ y $d' = (n-1, p^k(p-1))$, entonces d divide a $n-1$ y a $p^k(p-1)$ y por lo tanto a d'. Por otro lado d' divide a $n-1$ y $(d', p) = 1$ pues de otro modo $p \mid d'$ n lo cual no es posible pues, $p \nmid n$, por lo tanto d' divide a $p-1$, de donde $d' \mid d$.

Por lo tanto $d = d'$. ∎

Teorema IV.4.

Sea n entero positivo, impar y compuesto, entonces n cumple con la prueba de Miller a lo más para $\frac{n-1}{4}$ bases b, con $1 \leq b \leq n-1$.

Demostración:

Sea n entero positivo, compuesto e impar, por la demostración **Teorema IV.2.** si n cumple con la prueba de Miller para la base b entonces

$$b^{n-1} \equiv 1 \pmod{n}.$$

Supongamos que n se descompone como potencia de primos como sigue:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}.$$

Por el lema anterior la congruencia

$$x^{n-1} \equiv 1 \pmod{p_i^{\alpha_i}}$$

Tiene

$$(n-1, p_i^{\alpha_i - 1}(p_i - 1)) = (n-1, p_i - 1)$$

soluciones incongruentes y por el teorema Chino del residuo la congruencia

$$x^{n-1} \equiv 1 \pmod{n}$$

tiene exactamente

$$\prod_{i=1}^{r} (n-1, p_i - 1) \quad \text{soluciones.}$$

Supongamos que en la descomposición de n aparece $p_i^{\alpha_i}$, con $\alpha_i \geq 2$.

Dado que n es impar, p_i es impar, entonces $p_i^{\alpha_i - 1} \geq 3$ y $p_i^{\alpha_i} \geq 9$, de donde

$$\frac{1}{p^{\alpha_i - 1}} \leq \frac{1}{3} \quad \text{y} \quad \frac{1}{p^{\alpha_i}} \leq \frac{1}{9} \ ,$$

de aquí

$$\frac{p_i - 1}{p^{\alpha_i}} = \frac{1}{p^{\alpha_i - 1}} - \frac{1}{p^{\alpha_i}} \leq \frac{1}{3} - \frac{1}{9} = \frac{2}{9}$$

entonces

$$p_i - 1 \leq \frac{2}{9} p_i^{\alpha_i}.$$

Por lo tanto

$$\prod_{i=1}^{r} (n-1, p_i - 1) \leq \prod_{i=1}^{r} (p_i - 1) =$$

$$\left(\prod_{\substack{i=1 \\ i \neq k}}^{r} (p_i - 1) \right) (p_i - 1) <$$

$$\left(\prod_{\substack{i=1 \\ i \neq k}}^{r} p_i \right) (p_i - 1) <$$

$$\left(\prod_{\substack{i=1 \\ i \neq k}}^{r} p_i \right) \left(\frac{2}{9} p_i^{\alpha_i} \right) \leq$$

$$\frac{2}{9} \left(\prod_{i=1}^{r} p_i^{\alpha_i} \right) = \frac{2}{9} n.$$

Pero $n \geq p_i^{\alpha_i} \geq 9$, entonces $9n - 8n \geq 9$, de aquí $9n - 9 \geq 8n$, es decir, $9(n-1) \geq 8n$, por lo tanto $\frac{n-1}{4} \geq \frac{2}{9} n$.

De lo anterior

$$\prod_{i=1}^{r} (n-1, p_i - 1) \leq \left(\prod_{\substack{i=1 \\ i \neq k}}^{r} (p_i - 1) \right) \leq \frac{n-1}{4}$$

que es lo que se quería probar.

Ahora supongamos que n es de la forma

$$n = p_1 p_2 \cdot \ldots \cdot p_r$$

y supongamos que para cada $i = 1, \ldots, r$

$$p_i - 1 = 2^{s_i} t_i$$

con $s_i > 0$ y t_i impar, ($s_i > 0$ por que n es impar, de donde p_i todos son impares).

Sin pérdida de generalidad supongamos que $s_1 \leq s_2 \leq \ldots \leq s_r$.

Para cada $i = 1, \ldots, r$, el número de soluciones incongruentes de $x^t \equiv 1 \pmod{p_i}$ es

$$\begin{aligned}(t, p_i - 1) &= (2^0 t, 2^{s_i} t_i) \\ &= 2^{\min(0, s_i)} (t, t_i) \\ &= (t, t_i),\end{aligned}$$

hagamos $T_i = (t, t_i)$; el número de soluciones incongruentes de

$$x^{2^k t} \equiv -1 \pmod{p_i} \quad \text{con} \quad 0 \leq k \leq s_i - 1$$

es

$$\begin{aligned}(2^k t, p_i - 1) &= (2^k t, 2^{s_i} t_i) \\ &= 2^{\min(k, s_i)} (t, t_i) \\ &= 2^k T_i,\end{aligned}$$

pues $k < s_i$.

Por el *Lema* IV.1 y lo anterior la congruencia

$$x^t \equiv 1 \pmod{n}$$

tiene $T_1 T_2 \cdot \ldots \cdot T_r$ soluciones incongruentes y para cada $k = 1, \ldots, s_1 - 1$ la congruencia

$$x^{2^k t} \equiv -1 \pmod{n}$$

tiene

$$2^k T_1 \cdot 2^k T_2 \cdot \ldots \cdot 2^k T_r = 2^{kr} T_1 T_2 \cdot \ldots \cdot T_r$$

soluciones incongruentes, pues $k < s_1 \leq s_2 \leq \ldots \leq s_r$.

Por lo tanto n cumple con la prueba de Miller para a lo más

$$T_1T_2\cdot\ldots\cdot T_r+\left(\sum_{k=0}^{s_1-1}2^{kr}T_1T_2\cdot\ldots\cdot T_r\right)=T_1T_2\cdot\ldots\cdot T_r+\left(\sum_{k=0}^{a-1}2^{kr}\right)T_1T_2\cdot\ldots\cdot T_r$$

$$=T_1T_2\cdot\ldots\cdot T_r\left(1+\sum_{k=0}^{s_1-1}2^{kr}\right)$$

$$=T_1T_2\cdot\ldots\cdot T_r\left(1+\frac{2^{rs_1}-1}{2^r-1}\right)$$

bases b tales que $1\le b\le n-1$.

Por otro lado como $T=\{t_i\mid t_i$ para cada $i=1,\ldots,r$, tenemos que

$$T_1T_2\cdot\ldots\cdot T_r\le t_1t_2\cdot\ldots\cdot t_r$$

y como $s_1\le s_2\le\ldots\le s_r$, entonces

$$\frac{1+\frac{2^{rs_1}-1}{2^r-1}}{2^{s_1+s_2+\ldots+s_r}}\le\frac{1+\frac{2^{rs_1}-1}{2^r-1}}{2^{rs_1}}$$

$$=\frac{1}{2^{rs_1}}+\frac{2^{rs_1}-1}{2^{rs_1}(2^r-1)}$$

$$=\frac{1}{2^{rs_1}}+\frac{2^{rs_1}}{2^{rs_1}(2^r-1)}-\frac{1}{2^{rs_1}(2^r-1)}$$

$$=\frac{1}{2^{rs_1}}+\frac{1}{2^r-1}-\frac{1}{2^{rs_1}(2^r-1)}$$

$$=\frac{2^r-1-1}{2^{rs_1}(2^r-1)}+\frac{1}{2^r-1}$$

$$=\frac{2^r-2}{2^{rs_1}(2^r-1)}+\frac{1}{2^r-1}$$

$$=\frac{2^r-2+2^{rs_1}}{2^{rs_1}(2^r-1)}\le\frac{1}{2^{r-1}}\ .$$

Si $r\ge 3$, $r-1\ge 2$ y $2^{r-1}\ge 4$, de donde $\frac{1}{2^{r-1}}\le\frac{1}{4}$ en cuyo caso

$$T_1T_2\cdot\ldots\cdot T_t\left(\frac{1+\dfrac{2^{rs_1}-1}{2^r-1}}{2^{s_1+s_2+\ldots+s_t}}\right)\leq\frac{t_1t_2\cdot\ldots\cdot t_t}{4}$$

de donde

$$\begin{aligned}T_1T_2\cdot\ldots\cdot T_t\left(1+\frac{2^{rs_1}-1}{2^r-1}\right)&\leq\frac{t_1t_2\cdot\ldots\cdot t_t}{4}\cdot 2^{s_1+s_2+\ldots+s_t}\\&=\frac{2^{s_1}t_1\cdot 2^{s_2}t_2\cdot\ldots\cdot 2^{s_t}t_t}{4}\\&=\frac{(p_1-1)(p_2-1)\cdot\ldots\cdot(p_t-1)}{4}\\&=\frac{\phi(n)}{4}\leq\frac{n-1}{4}\end{aligned}$$

Si $r=2$ y $s_1<s_2$, se tiene

$$\begin{aligned}\frac{1+\dfrac{2^{2s_1}-1}{3}}{2^{s_1+s_2}}&=\frac{1+\dfrac{2^{2s_1}-1}{3}}{2^{2s_1}2^{s_2-s_1}}\\&=\frac{\dfrac{1}{2^{2s_1}}+\dfrac{2^{2s_1}-1}{3\cdot 2^{2s_1}}}{2^{s_2-s_1}}\\&=\frac{\dfrac{1}{2^{2s_1}}+\dfrac{1}{3}-\dfrac{1}{3\cdot 2^{2s_1}}}{2^{s_2-s_1}}\\&=\frac{\dfrac{1}{3}+\dfrac{3-1}{3\cdot 2^{2s_1}}}{2^{s_2-s_1}}\\&=\frac{\dfrac{1}{3}+\dfrac{1}{3\cdot 2^{2s_1-1}}}{2^{s_2-s_1}}\\&\leq\frac{\dfrac{1}{3}+\dfrac{1}{6}}{2}=\frac{\dfrac{3}{6}}{2}=\frac{1}{4}\end{aligned}$$

y de nuevo

$$T_1T_2\left(1+\frac{2^{rs_1}-1}{2^r-1}\right) \le \frac{t_1t_2}{4}2^{s_1+s_2} = \frac{2^{s_1}t_1\cdot 2^{s_2}t_2}{4} = \frac{(p_1-1)(p_2-1)}{4} = \frac{\phi(n)}{4} \le \frac{n-1}{4}.$$

Por último si $r = 2$ y $s_1 = s_2$

$$\frac{1+\frac{2^{2s_1}-1}{3}}{2^{s_1+s_2}} \le \frac{1}{6} < \frac{1}{4}$$

por lo tanto

$$T_1T_2\left(1+\frac{2^{rs_1}-1}{2^r-1}\right) < \frac{t_1t_2}{4}2^{s_1+s_2} = \frac{2^{s_1}t_1\cdot 2^{s_2}t_2}{4} = \frac{(p_1-1)(p_2-1)}{4} = \frac{\phi(n)}{4} \le \frac{n-1}{4}.$$

Por lo tanto n solo puede cumplir con la prueba de Miller para alo más $\frac{n-1}{4}$ bases b tales que $1 \le b \le n-1$. ■

IV.2. Seudoprimos Fuertes.

En la anterior sección vimos que todos los números primos cumplen con la prueba de Miller, se dijo tambien que existian enteros compuestos que cumplen con dicha prueba de estos enteros hablaremos en la presente sección.

DEFINICION:

Si n es entero compuesto positivo y cumple con la prueba de Miller para la base b se le llama seudoprimo fuerte para la base b.

Ejemplos:

1. $n = 2047 = 23\cdot 89$, entonces n es seudoprimo fuerte para la base 2 ya

que $n - 1 = 2046 = 2 \cdot 1023$ y

$$2^{11} = 2048 \equiv 1 \pmod{2047}$$

por lo tanto

$$2^{1023} = (2^{11})^{93} \equiv 1 \pmod{2047}.$$

2. $n = 25$ es seudoprimo fuerte para la base 7 puesto que $n - 1 = 24 = 2^3 \cdot 3$, además

$$7^2 = 49 \equiv -1 \pmod{25}$$

de aquí

$$7^{2^3} = (7^2)^3 \equiv (-1)^3 \equiv -1 \pmod{25}.$$

Como corolario del Teorema IV.3. tenemos que todo seudoprimo fuerte para la base b es seudoprimo para la misma base b, el siguiente lema nos dice que no todo seudoprimo es seudoprimo fuerte.

Lema IV.3.

341 es seudoprimo para la base 2 pero no es seudoprimo fuerte para la base 2.

Demostración:

Tenemos que $n - 1 = 340 = 2^2 \cdot 85$.

Como $(2,11) = (2,31) = 1$, se tiene

$$2^{10} \equiv 1 \pmod{11}$$

$$2^{10} = (2^5)^2 = 32^2 \equiv 1 \pmod{31}$$

de donde

$$2^{170} = (2^{10})^{17} \equiv 1 \pmod{11}$$

$$2^{170} = (2^{10})^{17} \equiv 1 \pmod{31}$$

por lo tanto

$$2^{170} \equiv 1 \not\equiv -1 \pmod{341}$$

ahora

$$2^{85} = (2^{10})^8 2^5 \equiv 2^5 \equiv 32 \pmod{11}$$

$$2^{85} = (2^5)^{13} \equiv 1 \equiv 32 \pmod{31}$$

entonces

$$2^{85} \equiv 32 \not\equiv 1 \pmod{341}$$

por lo tanto 341 no cumple con la prueba de Miller para la base 2, es decir, 341 no es seudoprimo fuerte para la base 2.

Por otro lado, como

$$2^{170} \equiv 1 \pmod{341}$$

entonces

$$2^{340} \equiv 1 \pmod{341}$$

de donde concluimos que 341 es seudoprimo para la base 2. ∎

Por último demostraremos que existe una infinidad de seudoprimos fuertes para la base 2, para ésto demostremos el siguiente teorema.

Teorema IV.5.

Si n es seudoprimo impar para la base 2 entonces $N = 2^n - 1$ es seudoprimo fuerte para la base 2.

Demostración:

Sea n impar y supongamos que n es seudoprimo para la base 2, $n = 1$ claramente es seudoprimo fuerte para la base 2. Supongamos que $n > 1$, entonces

$$2^n \equiv 2 \pmod{n}$$

y como n es impar

$$2^{n-1} \equiv 1 \pmod{n},$$

es decir, n divide a $2^{n-1} - 1$ o bien $2^{n-1} - 1 = nk$ para algún $k \in \mathbb{Z}$.

por otro lado, si $N = 2^n - 1$ se tiene

$$N - 1 = 2^n - 2 = 2^1(2^{n-1} - 1) = 2^1 nk,$$

como $n > 1$ $nk = 2^{n-1} - 1$ es impar y

$$2^{(N-1)/2} = 2^{nk} = (2^n)^k \equiv 1 \pmod{N},$$

ya que

$$2^n = (2^n - 1) + 1 = N + 1 \equiv 1 \pmod{N}.$$

Por lo tanto N cumple con la prueba de Miller para la base 2.

Ahora, como n es compuesto existe un entero $d < n$ tal que $d \mid n$

de donde $2^d - 1 \mid 2^n - 1 = N$, es decir N es compuesto.

Por lo tanto N es seudoprimo fuerte para la base 2. ∎

Corolario IV.5.1.

Si n es seudoprimo fuerte para la base 2, entonces $N = 2^n - 1$ es seudoprimo fuerte para la base 2.

Demostración:

La demostración es inmediata del teorema ya que si n es seudoprimo fuerte para la base 2 en particular es seudoprimo para la base 2 y por el teorema anterior $N = 2^n - 1$ es seudoprimo fuerte para la base 2. ∎

Teorema IV.6.

Existe una infinidad de seudoprimos fuertes para la base 2.

Demostración:

Basta tomar $n_1 = 1387$, que es seudoprimo fuerte para la base 2. Por el corolario anterior $n_2 = 2^{n_1} - 1$ es seudoprimo fuerte para la base 2, $n_3 = 2^{n_2} - 1$ es seudoprimo fuerte para la base 2, etc., de tal suerte que

$$n_1 < n_2 < n_3 < \ldots$$

es una cadena infinita de seudoprimos fuertes para la base 2. ∎

CAPITULO V.

SEUDOPRIMOS DE EULER.

V.1. RECIPROCIDAD CUADRATICA.

DEFINICION:

Sea m entero positivo, si $a \in (\mathbb{Z}_m, \cdot)$ a recibe el nombre de residuo cuadrático módulo m si la congruencia

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

tiene solución. Si no tiene solución se llama residuo no cuadrático, es decir a es residuo cuadrático si a tiene raíz cuadrada en $(\mathbb{Z}_n, \cdot)$ y a es no residuo cuadrático en caso contrario.

Teorema V.1.

Si m es primo, entonces $a \in (\mathbb{Z}_m, \cdot)$ es residuo cuadrático si y sólo si

$$a^{\phi(m)/d} \equiv 1 \pmod{m}$$

donde $d = (2, \phi(m))$.

Demostración:

La demostración es inmediata del Teorema **I.14.** pues decir que a es residuo cuadrático es lo mismo que decir que a tiene raíz cuadrada en $(\mathbb{Z}_n, \cdot)$. ∎

Teorema V.2.

Sea p primo impar y $a \in (\mathbb{Z}_p, \cdot)$, entonces a es residuo cuadrático si y sólo si $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Demostración:

Tenemos que $\phi(p) = p - 1$ y $(2, p-1) = 2$, pues p es impar, luego por el teorema anterior a es residuo cuadrático si y sólo si

$$a^{(p-1)/2} \equiv 1 \pmod{p}. \blacksquare$$

Nos interesa clasificar a todos los enteros primos con p, (p primo impar) de acuerdocon que sean o no residuos cuadráticos, para esto observemos la siguiente definición.

DEFINICION:

Sea p primo impar y $a \in (\mathbb{Z}_n, \cdot)$, el simbolo de Legendre $\left(\frac{a}{p}\right)$ se define como:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{Si } a \text{ es residuo cuadrático.} \\ -1 & \text{Si } a \text{ es no residuo cuadráico.} \end{cases}$$

En el siguiente teorema se enuncian las propiedades básicas de el simbolo de Legendre.

Teorema V.3.

Sea p primo impar y $a, b \in (\mathbb{Z}p, \cdot)$, entonces

$\cdot$) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$ (*Criterio de Euler*).

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

$\cdot\cdot\cdot$) $a \equiv b \pmod{p}$ implica que $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

$\cdot\cdot\cdot\cdot$) $\left(\frac{a^2}{p}\right) = 1$.

——) $\left(\frac{1}{p}\right) = 1$.

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

——) $\left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ si y sólo si } p \equiv 1 \pmod 4 \\ -1 \text{ si y sólo si } p \equiv 1 \pmod 4 \end{cases}$.

Demostración:

·) Como p es primo y $(a,p) = 1$, tenemos

$$a^{p-1} \equiv 1 \pmod{p}$$

es decir

$$p \mid a^{p-1} - 1 = (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1)$$

por lo tanto

$$p \mid a^{(p-1)/2} - 1$$

o

$$p \mid a^{(p-1)/2} + 1$$

es decir

$$a^{(p-1)/2} \equiv -1 \pmod{p}$$

o

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Si

$$a^{(p-1)/2} \equiv -1 \not\equiv 1 \pmod{p}$$

por el Teorema V.2, a es no residuo cuadrático, por lo tanto

$$\left(\frac{a}{p}\right) = -1 \equiv a^{(p-1)/2} \pmod{p}$$

y si

$$a^{(p-1)/2} \equiv 1 \pmod{p}$$

a es residuo cuadrático, entonces

$$\left(\frac{a}{p}\right) = 1 \equiv a^{(p-1)/2} \pmod{p}.$$

··) $\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2}$

$$\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$$

y como p es impar

$$1 \equiv -1 \pmod{p}$$

por lo tanto

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

···) Supongamos que $a \equiv b \pmod{p}$, entonces si existe x_0 tal que $x_0^2 \equiv a \pmod{p}$ se tiene $x_0^2 \equiv b \pmod{p}$ y resiprocamente, es decir, a es residuo cuadrático si y sólo si b es residuo cuadratico, por lo tanto

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

····) Tenemos que

$$\left(\frac{a^2}{p}\right) = \left(\frac{aa}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^2 = \begin{cases} 1' \\ 0 = 1. \\ (-1)' \end{cases}$$

——) Hacemos $a^2 = 1$, por lo tanto

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

·——) Tenemos sólo dos casos:

$$(-1)^{(p-1)/2} = 1 \text{ o } -1,$$

supongamos que

$$(-1)^{(p-1)/2} = 1 \equiv 1 \pmod{p},$$

entonces de acuerdo con el Teorema V.2. -1 es residuo cuadrático, de donde

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

si $(-1)^{(p-1)/2} = -1 \not\equiv 1 \pmod{p}$ (pues p es impar),

entonces -1 no puede ser residuo cuadrático, por lo tanto

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

··——) Supongamos que

$$p \equiv 1 \pmod{4}$$

entonces p es de la forma $p = 4k + 1$, con $k \in \mathbb{Z}$, de aquí $\frac{p-1}{2} = 2k$, por lo tanto

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

Ahora, si

$$p \equiv -1 \pmod{4}$$

p es de la forma $p = 4k - 1$, de donde $\frac{p-1}{2} = 2k - 1$, por lo tanto

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

Resiprocamente, si $\left(\frac{-1}{p}\right) = 1$, entonces $(-1)^{(p-1)/2} = 1$, lo cual implica que $\frac{p-1}{2} = 2k$ para algun entero k, es decir $p = 4k + 1$ o bien

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

Si $\left(\frac{-1}{p}\right) = -1$, entonces $(-1)^{(p-1)/2} = -1$, de aquí que

$\frac{p-1}{2} = 2k - 1$, o bien $p = 4k - 1$, por lo tanto

$$p \equiv -1 \pmod 4.$$

■

Si p es un primo impar el entero 2 no siempre tiene raíz cuadrada en $(\mathbb{Z}_p, \cdot)$, a continuación veremos que si p cumple con que $\frac{p^2-1}{8}$ sea par el 2 tiene raíz cuadrada, para este echo demostremos el Lema de Gauss.

Teorema V.4. (*Lema de Gauss*

Sea p primo impar y a entero positivo tal que $(a,p) = 1$. Consideremos el conjunto

$$A = \{a, 2a, 3a, \ldots, (\tfrac{p-1}{2})a\}$$

y el conjunto

$$B = \{a_j \in \{1, \ldots, p-1\} \mid a_j \equiv ja \pmod p,\ 1 \le j \le \tfrac{p-1}{2}\}$$

(a B le llamaremos el conjunto de mínimos residuos del conjunto A), supongamos que hay n a_i's tales que $a_i > \frac{p}{2}$, entonces

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Demostración:

Supongamos que $a_{i_1}, a_{i_2}, \ldots, a_{i_n}$ son mayores que $p/2$ y $a_{j_{n+1}}, \ldots, a_{j_{(p-1)/2}}$ son menores o iguales que $p/2$, entonces

$p - a_{i_k} < p - \frac{p}{2} = \frac{p}{2}$, $\forall\ i = 1, \ldots, n$, y tenemos que

$$p - a_{i_k} \equiv a_{j_k} \pmod p \quad \forall\ i \in \{1, \ldots, n\} \quad y \quad \forall\ k \in \{n+1, \ldots, \tfrac{p-1}{2}\}$$

pues si

$$p - a_{i_k} \equiv a_{j_k} \pmod p,$$

se tendría que

$$-j_k a \equiv j_k a \pmod p$$

es decir $p \mid j_k + j_k$, de donde $p \le j_k + j_k \le \frac{p-1}{2}$ lo cual no puede pasar, por lo tanto $p - a_{i_1}, \ldots, p - a_{i_n}, a_{j_{n+1}}, \ldots, a_{j_{(p-1)/2}}$ son los enteros

$1,2,\ldots,\frac{p-1}{2}$ quizás en otro orden, por lo tanto

$$\begin{aligned} 1\cdot 2\cdot\ldots\cdot\frac{p-1}{2} &\equiv (p-a_{j_1})\cdot\ldots\cdot(p-a_{j_n})a_{j_{n+1}}\cdot\ldots\cdot a_{j_{(p-1)/2}} \\ &\equiv (-1)^n a_{j_1}a_{j_2}\cdot\ldots\cdot a_{j_n}a_{j_{n+1}}\cdot\ldots\cdot a_{j_{(p-1)/2}} \\ &\equiv (-1)^n a^{(p-1)/2} j_1 j_2\cdot\ldots\cdot j_{(p-1)/2} \\ &\equiv (-1)^n a^{(p-1)/2}(1\cdot 2\cdot\ldots\cdot\frac{p-1}{2}) \pmod p \end{aligned}$$

de aquí que

$$1 \equiv (-1)^n a^{(p-1)/2} \equiv (-1)^n\left(\frac{a}{p}\right) \pmod p$$

por lo tanto

$$\left(\frac{a}{p}\right) \equiv (-1)^n\left(\frac{a}{p}\right)^2 \equiv (-1)^n \pmod p$$

de donde $\left(\frac{a}{p}\right) = (-1)^n$. ∎

Teorema V.5.

Si p es primo impar

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Demostración:

Consideremos el cobnjunto $A = \{2\cdot 1, 2\cdot 2, \ldots, 2(\frac{p-1}{2})\}$, entonces $2j \leq p/2$ si y sólo si $j \leq p/4$, de aquí que la cantidad de elementos de A menores que $p/2$ es exactamente $\left[\frac{p}{4}\right]$, donde $\left[\frac{p}{4}\right]$ es la parte entera de $p/4$, entonces hay $n = \frac{p-1}{2} - [p/4]$ elementos de A mayores que $p/4$.

Por otro lado, como p es primo tiene las siguientes posibilidades

$$p \equiv \pm 1 \pmod 8$$

o $p \equiv \pm 3 \pmod 8$

si $p \equiv \pm 1 \pmod 8$ se tiene $p = 8k \pm 1$ para algun $k \in \mathbb{Z}$, de donde

$$\begin{aligned} \frac{p^2-1}{8} &= \frac{(8k\pm 1)^2 - 1}{8} \\ &= \frac{64k^2 \pm 16k + 1 - 1}{8} \\ &= 8k^2 \pm 2k \equiv 0 \pmod 2 \end{aligned}$$

y si $p \equiv \pm 3 \pmod 8$, entonces $p = 8k \pm 3$, con $k \in \mathbb{Z}$, por lo tanto

$$\frac{p^2-1}{8} = \frac{(8k \pm 3)^2 - 1}{8}$$

$$= \frac{64k^2 \pm 48k + 9 - 1}{8}$$

$$= 8k^2 \pm 6k + 1 \equiv 1 \pmod 2$$

Por otro lado, si $p = 8k + 1$

$$n = \frac{p-1}{2} - [p/4]$$

$$= 4k - [2k + 1/4]$$

$$= 2k \equiv 0 \pmod 2$$

y si $p = 8k - 1$

$$n = \frac{p-1}{2} - [p/4]$$

$$= 4k - 1 - [2k - 1/4]$$

$$= 4k - 1 - (2k - 1)$$

$$= 2k \equiv 0 \pmod 2$$

ahora si $p = 8k + 3$

$$n = \frac{p-1}{2} - [p/4]$$

$$= 4k + 1 - [2k + 3/4]$$

$$= 2k + 1 \equiv 1 \pmod 2$$

y por último, si $p = 8k - 3$

$$n = \frac{p-1}{2} - [p/4]$$

$$= 4k - 2 - [2k - 3/4]$$

$$= 4k - 2 - (2k - 1)$$

$$= 2k - 1 \equiv 1 \pmod 2$$

por lo tanto

$$n \equiv \frac{p^2-1}{8} \pmod 2$$

de donde

$$\left(\frac{2}{p}\right) = (-1)^n = (-1)^{(p^2-1)/8}. \quad \blacksquare$$

Una consecuencia interesante de este teorema es el siguiente:

Teorema V.6.

Sea $n \geq 2$, entonces los divisores primos del n-ésimo número de Fermat son de la forma $2^{n+2}k + 1$.

Demostración:

Sea p divisor primo de $F_n = 2^{2^n} + 1$, segun el

Teorema II.10 . el orden de 2 en $(\mathbb{Z}_p,\cdot)$ es 2^{n+1} y $p = 2^{n+1}t + 1$, para algún entero t, de aquí que

$$p^2 = 2^{2(n+1)}t^2 + 2^{n+2}t + 1$$

por lo tanto

$$\frac{p^2-1}{8} = 2^{2n-1}t^2 + 2^{n-1}k = 2(2^{2(n-1)}t^2 + 2^{n-2}t)$$

de donde

$$\left\{\frac{2}{p}\right\} = (-1)^{(p^2-1)/8} = 1,$$

es decir, 2 es residuo cuadrático, entonces

$$2^{(p-1)/2} \equiv 1 \ (mod\ p)$$

y como el orden de 2 es 2^{n+1}, tenemos $2^{n+1}k = \frac{p-1}{2}$ para algun entero k, por lo tanto

$$p = 2^{n+2}k + 1. \quad \blacksquare$$

El siguiente teorema no facilita el calculo del simbolo de Legendre para enteros compuestos, figandonos sólo en sus divisores primos.

Lema V.1.

Sea p primo impar y a impar tal que $_0(a,p) = 1$, entonces

$$\left\{\frac{a}{p}\right\} = (-1)^{T(a,p)}$$

donde $T(a,p) = \sum_{i=1}^{(p-1)/2} [ia/p]$.

Demostración:

Sea $A = \{a, 2a, \ldots, (\frac{p-1}{2})a\}$ y

$B = \{u_1, \ldots, u_s, v_1, \ldots, u_t\}$

su conjunto de mínimos residuos de A, donde primeros n son mayores que $p/2$ y los siguientes son menores o iguales.

Para cada $i = 1, \ldots, \frac{p-1}{2}$ se tiene que $ia = p[ia/p] + r_i$ donde $r_i \in B$, además de la demostración del lema de gauss se tiene que los enteros $p - u_1, p - u_2, \ldots, p - u_s, v_1, \ldots, v_t$ son los enteros $1, 2, \ldots, \frac{p-1}{2}$, quizas en otro orden, de donde

$$\sum_{i=1}^{(p-1)/2} i = \sum_{i=1}^{n} (p - u_i) + \sum_{j=1}^{m} v_j = pn - \sum_{i=1}^{n} u_i + \sum_{j=1}^{m} v_j$$

de donde

$$\sum_{i=1}^{(p-1)/2} ia - \sum_{i=1}^{(p-1)/2} i = \sum_{i=1}^{n} (p - u_i) + \sum_{j=1}^{m} v_j$$

$$= \sum_{i=1}^{(p-1)/2} (p[ia/p] + r_i) - pn + \sum_{i=1}^{n} u_i - \sum_{j=1}^{m} v_j$$

$$= \sum_{i=1}^{(p-1)/2} p[ia/p] - pn + 2\sum_{i=1}^{n} u_i$$

$$= pT(a,p) - pn + 2\sum_{i=1}^{n} u_i$$

por lo tanto

$$(a - 1) \sum_{i=1}^{(p-1)/2} i = p(T(a,p) - n) + 2\sum_{i=1}^{n} u_i$$

pero por ser a impar $a - 1$ es par, y de lo anterior

$$2 \mid p(T(a,p) - n)$$

además p es impar, por lo tanto

$$2 \mid T(a,p) - n,$$

es decir,

$$n \equiv T(a,p) \pmod 2,$$

entonces

$$\left(\frac{a}{p}\right) = (-1)^n = (-1)^{T(a,p)}. \quad \blacksquare$$

Teorema V.7. *Ley de la reciprocidad cuadrática*

Sean p, q primos impares, entonces

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

Demostración:

Sea $A = \{(x,y) \in Z \times Z \mid 1 \le x \le \frac{p-1}{2} \text{ y } 1 \le y \le \frac{q-1}{2}\}$, notemos que la cardinalidad de A es $(\frac{p-1}{2})(\frac{q-1}{2})$

Sean A_1, $A_2 \subset A$, dados de la siguiente manera:

$$A_1 = \{(x,y) \in A \mid qx < py\}$$

$$A_2 = \{(x,y) \in A \mid py < qx\}.$$

Notemos que $qx \neq py \quad \forall (x,y) \in A$. pues si $qx = py$ para algun $(x,y) \in A$, entonces $q \mid py$, de donde $q \mid y$ lo cual no es posible pues $y \leq \frac{q-1}{2}$, entonces $A_1 \cap A_2 = \emptyset$ y $A_1 \cup A_2 = A$.

Notemos que la cardinalidad de A_1 es $\sum_{y=1}^{(q-1)/2} [py/q]$ y la cardinalidad de A_2 es $\sum_{x=1}^{(p-1)/2} [qx/p]$, por lo tanto la cardinalidad de A es

$$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) = \sum_{y=1}^{(q-1)/2} [py/q] + \sum_{x=1}^{(p-1)/2} [qx/p].$$

y por el lema anterior

$$\left(\frac{p}{q}\right)\left(\frac{q}{q}\right) = (-1)^{\Sigma[py/q]}(-1)^{\Sigma[qx/p]}$$
$$= (-1)^{((p-1)/2)((q-1)/2)}. \quad \blacksquare$$

La ley de reciprocidad cuadrática se puede expresar tambien así:

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

En el Capitulo II vimos que el quinto número dr Fermat es compuesto, a continuación doy un criterio para determinar cuando un número de Fermat es primo.

Teorema V.8.

Sea $n \geq 1$, entonces $F_n = 2^{2^n} + 1$ es primo si y sólo si

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

Demostración:

$\Leftarrow$) Supongamos que

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$$

entonces

$$3^{F_n-1} \equiv 1 \pmod{F_n}$$

de aquí que $(3^{F_n-1}, F_n) = 1$, entonces $(3, F_n) = 1$.

Sea p primo divisor de F_n, entonces

$$3^{F_n-1} \equiv 1 \pmod{p}$$

y como $(3,F_n) = 1$ se tiene que $(3,p) = 1$, es decir $3 \in (\mathbb{Z}_p,\cdot)$, por lo tanto $o(3) \mid F_n - 1 = 2^{2^n}$ y como

$$3^{(F_n-1)/2} \equiv -1 \not\equiv 1 \pmod{p}$$

pues p es impar, se tiene

$$o(3) \nmid (F_n-1)/2) = 2^{2^n-1}$$

por lo tanto $o(3) = 2^{2^n} = F_n - 1$, entonces $F_n - 1 \leq p - 1$, por lo tanto $F_n \leq p$.

Por otro lado, como $p \mid F_n$, $p \leq F_n$.

Por lo tanto $F_n = p$, es decir, F_n es primo.

$\Rightarrow$) Supongamos que F_n es primo, entonces

$$F_n \equiv 2 \pmod{3}$$

pues si

$$F_n \equiv 1 \pmod{3}$$

se tendría que 3 divide a 2^{2^n} lo cual no es posible o si

$$F_n \equiv 0 \pmod{3}$$

diría que $F_n = 3$, pues F_n es primo, de aquí $2^{2^n} = 2$, es decir $2^n = 1$, o bien $n = 0$ lo cual no es posible.

Por otro lado

$$\left(\frac{3}{F_n}\right) = (-1)^{((F_n-1)/2)((3-1)/2)}\left(\frac{F_n}{3}\right)$$

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

$$= (-1)^{(3^2-1)/8} = -1$$

y por el criterio de euler

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}. \quad \blacksquare$$

Ahora generalizaremos la idea del símbolo de Legendre para enteros no necesariamente primos.

DFINICION:

Sea n entero impar y supongamos que su descomposición en potencias de primos es $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_r^{\alpha_r}$.

Sea a entero tal que $(a,n) = 1$, definimos el simbolo de Jacobi como:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\cdot\ldots\cdot\left(\frac{a}{p_k}\right)^{\alpha_k}.$$

Notemos que la definición si tiene sentido ya que $(a,n) = 1$ implica $(a,p_i) = 1$ para toda $i = 1,\ldots,k$; además si n es primo el simbolo de Legendre coincide con el simbolo de Jacobi, por lo tanto se usara la misma notación.

Teorema V.9.

Sea n entero impar y $a,b \in (\mathbb{Z}n,\cdot)$, entonces

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

$\cdot\cdot$) $a \equiv b \pmod{n}$ implica que $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

$\cdot\cdot\cdot$) $\left(\frac{a^2}{n}\right) = 1$.

$\cdot\cdot\cdot\cdot$) $\left(\frac{1}{n}\right) = 1$.

—) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

—) $\left(\frac{-1}{n}\right) = \begin{cases} 1 \text{ si y sólo si } n \equiv 1 \pmod 4 \\ -1 \text{ si y sólo si } n \equiv 1 \pmod 4 \end{cases}$.

Demostración:

Supongamos que $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$, entonces

$\cdot$)

$$\left(\frac{ab}{n}\right) = \prod_{i=1}^{k}\left(\frac{ab}{p}\right)^{\alpha_i} = \prod_{i=1}^{k}\left(\frac{a}{p}\right)^{\alpha_i}\left(\frac{b}{p}\right)^{\alpha_i}$$
$$= \prod_{i=1}^{k}\left(\frac{a}{p}\right)^{\alpha_i}\prod_{i=1}^{k}\left(\frac{b}{p}\right)^{\alpha_i}$$
$$= \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$

$\cdot\cdot$) Si $a \equiv b \pmod{n}$, se cumple

$$a \equiv b \pmod{p_i} \quad \text{para toda } i = 1,\ldots,k$$

de donde

$$\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right) \quad \text{para toda } i = 1,\ldots,k,$$

por lo tanto

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)^{\alpha_i}$$

$$= \prod_{i=1}^{k}\left(\frac{b}{p_i}\right)^{\alpha_i} = \left(\frac{b}{n}\right)$$

$\cdots$) $\left(\frac{a^s}{n}\right) = \prod_{i=1}^{k}\left(\frac{a^s}{p_i}\right)^{\alpha_i} = 1$, ya que $\left(\frac{a^s}{p_i}\right) = 1 \quad \forall\ i = 1,\ldots,k.$

$\cdots\cdot$) $\left(\frac{1}{n}\right) = \prod_{i=1}^{k}\left(\frac{1}{p_i}\right)^{\alpha_i} = 1$, ya que $\left(\frac{1}{p_i}\right) = 1 \quad \forall\ i = 1,\ldots,k.$

——) $\left(\frac{-1}{n}\right) = \prod_{i=1}^{k}\left(\frac{-1}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{k}((-1)^{(p_i-1)/2})^{\alpha_i} \equiv (-1)^{\sum((p_i-1)/2)\alpha_i}$

por otro lado

$$n = p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_r^{\alpha_r} = \prod\,(1 + (p_i - 1))^{\alpha_i}$$

y como $p_i - 1$ es par para toda i, se tiene

$$(1 + (p_i - 1))^{\alpha_i} \equiv 1 + \alpha_i(p_i - 1) \pmod 4,$$

además

$$(1 + \alpha_i(p_i - 1))(1 + \alpha_j(p_j - 1))$$

$$\equiv 1 + \alpha_i(p_i - 1) + \alpha_j(p_j - 1) \pmod 4,$$

ya que $(p_i - 1)(p_j - 1) \equiv 0 \pmod 4$, por lo tanto

$$n = \prod\,(1 + (p_i - 1))^{\alpha_i} \equiv 1 + \alpha_1(p_1 - 1) + \ldots + \alpha_r(p_r - 1) \pmod 4,$$

es decir

$$4s = (n - 1) - \sum \alpha_i(p_i - 1) \qquad \text{p.a.} \quad s \in \mathbb{Z}$$

de donde

$$2s = \frac{n-1}{2} - \sum \alpha_i\left(\frac{(p_i-1)}{2}\right)$$

o bien

$$\frac{n-1}{2} \equiv \alpha_i\left(\frac{(p_i-1)}{2}\right) \pmod 2$$

por lo tanto

$$\left(\frac{-1}{n}\right) = (-1)^{\sum((p_i-1)/2)\alpha_i} \equiv (-1)^{(n-1)/2}.$$

Desafortunadamente el criterio de Euler ya no es válido con el símbolo de Jacobi, por ejemplo:

$n = 341 = 11\cdot 31$. Tenemos que

$$2^{(341-1)/2} \equiv 2^{170} \equiv 1 \pmod{341}$$

mientras que

$$\left(\frac{2}{341}\right) = \left(\frac{2}{11}\right)\left(\frac{2}{31}\right) =$$
$$(-1)^{(11^2-1)/8}(-1)^{(31^2-1)/2} =$$
$$(-1)^{15}(-1)^{120} = -1$$

por lo tanto

$$\left(\frac{2}{341}\right) \not\equiv 2^{(341-1)/2} (mod\ 341).$$

De los números compuestos que cumplen con el criterio de Euler nos ocuparemos en la siguiente sección.

Para finalizar esta sección demos la generalización de la ley de reciprocidad cuadrática.

Teorema V.10. *Ley de reciprocidad cuadrática para el símbolo de Jacobi*

Sean n, m enteros impares, entonces

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{((n-1)/2)((m-1)/2)}$$

Demostración:

Supongamos que $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_r^{\alpha_r}$ y $m = q_1^{\beta_1}q_2^{\beta_2}\cdot\ldots\cdot q_s^{\beta_s}$

como

$$\left(\frac{n}{m}\right) = \prod_{i=1}^{k}\left(\frac{n}{p_i}\right) = \prod_{i=1}^{k}\left(\frac{p_1^{\alpha_1}\cdot\ldots\cdot p_r^{\alpha_r}}{q_i}\right)$$
$$= \prod_{i=1}^{k}\left[\left(\frac{p_1}{q_i}\right)^{\alpha_1}\left(\frac{p_2}{q_i}\right)^{\alpha_2}\cdot\ldots\cdot\left(\frac{p_r}{q_i}\right)^{\alpha_r}\right]^{\beta_i}$$
$$= \prod_{i=1}^{k}\left(\frac{p_1}{q_i}\right)^{\alpha_1\beta_i}\left(\frac{p_2}{q_i}\right)^{\alpha_2\beta_i}\cdot\ldots\cdot\left(\frac{p_r}{q_i}\right)^{\alpha_r\beta_i}$$
$$= \prod_{i=1}^{k}\prod_{j=1}^{r}\left(\frac{p_j}{q_i}\right)^{\alpha_j\beta_i}$$

y analogamente

$$\left(\frac{m}{n}\right) = = \prod_{i=1}^{k}\prod_{j=1}^{r}\left(\frac{q_i}{p_j}\right)^{\alpha_j\beta_i}$$

de donde

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{k}\prod_{j=1}^{r}\left(\frac{p_i}{q_j}\right)^{\alpha_i\beta_j}\prod_{i=1}^{k}\prod_{j=1}^{r}\left(\frac{q_j}{p_i}\right)^{\alpha_i\beta_j}$$

$$= \prod_{i=1}^{k}\prod_{j=1}^{r}\left(\frac{p_i}{q_j}\right)^{\alpha_i\beta_j}\left(\frac{q_j}{p_i}\right)^{\alpha_i\beta_j}$$

$$= \prod_{i=1}^{k}\prod_{j=1}^{r}\left[\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right]^{\alpha_i\beta_j}$$

$$= \prod_{i=1}^{k}\prod_{j=1}^{r}\left((-1)^{((p_i-1)/2)((q_j-1)/2)}\right)^{\alpha_i\beta_j}$$

$$= (-1)^{\sum_{i=1}^{k}\sum_{j=1}^{r}((p_i-1)/2)\alpha_i((q_j-1)/2)\beta_j}.$$

Pero

$$\sum_{i=1}^{k}\sum_{j=1}^{r}((p_i-1)/2)\alpha_i((q_j-1)/2)\beta_j$$

$$= \left(\sum_{i=1}^{k}((p_i-1)/2)\alpha_i\right)\left(\sum_{j=1}^{r}((q_j-1)/2)\beta_j\right)$$

$$\equiv \frac{n-1}{2}\cdot\frac{m-1}{2} \pmod 2$$

(ver demostración del Teorema V.9. inciso (——)), por lo tanto

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\sum_{i=1}^{k}\sum_{j=1}^{r}((p_i-1)/2)\alpha_i((q_j-1)/2)\beta_j}$$

$$= (-1)^{((n-1)/2)((m-1)/2)}. \quad \blacksquare$$

V.2. Seudoprimos Euler.

Si p es primo impar y $(b,p) = 1$ por el criterio de Euler tenemos

$$\left(\frac{b}{p}\right) \equiv b^{(p-1)/2} \pmod p$$

de donde, un entero positivo n es tal que

$$\left(\frac{b}{n}\right) \equiv b^{(p-1)/2} \pmod n$$

para algun b primo con n, entonces n tiene que ser compuesto. Sin embargo exiten enteros compuestos que cumplen con el criterio de Euler para algún b, por ejemplo:

Si $n = 1105$, entonces $\frac{n-1}{2} = 552$.

Tenemos que $1105 = 5\cdot 13\cdot 17$ y

$$2^4 \equiv 1 \pmod 5$$
$$2^{12} \equiv 1 \pmod{13}$$
$$2^{16} \equiv 1 \pmod{17}$$

por lo tanto

$$2^{(n-1)/2} = 2^{552} = (2^4)^{138} \equiv 1 \pmod 5$$
$$2^{(n-1)/2} = 2^{552} = (2^{12})^{46} \equiv 1 \pmod{13}$$

y además

$$2^4 = 16 \equiv -1 \pmod{17},$$

de donde

$$2^{(n-1)/2} = 2^{552} = (2^4)^{138} \equiv (-1)^{138} \equiv 1 \pmod{17}$$

entonces

$$2^{(n-1)/2} = 1 \pmod n.$$

Por otro lado

$$\left(\frac{2}{1105}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{13}\right)\left(\frac{2}{17}\right)$$
$$\equiv (-1)^{(5^2-1)/2}(-1)^{(13^2-1)/2}(-1)^{(17^2-1)/2}$$
$$\equiv (-1)^3(-1)^{21}(-1)^{30}$$
$$\equiv 1.$$

Por lo tanto

$$\left(\frac{2}{1105}\right) \equiv 2^{(1105-1)/2} \pmod{1105}.$$

DEFINICION:

Un entero compuesto n positivo e impar es llamado seudoprimo de Euler para la base b si cumple con:

$$\left(\frac{b}{n}\right) \equiv b^{(n-1)/2} \pmod n.$$

Como su nombre lo indica, si n es seudoprimo de Euler para la base b, entonces n es a su vez un seudoprimo para la base b como se indica en el siguiente teorema.

Teorema V.11.

Sean n entero positivo, compuesto e impar y b en $(Z_n,\cdot)$. Si

n es seudoprimo de Euler para la base b entonces n es seudoprimo para la base b.

Demostración:

Supongamos que n es seudoprimo de Euler para la base b, entonces

$$\left(\frac{b}{n}\right) \equiv b^{(n-1)/2} (mod\ n)$$

de aquí que

$$1 \equiv \left(\frac{b}{n}\right)^2 \equiv \left(b^{(n-1)/2}\right)^2 \equiv b^{n-1} (mod\ n),$$

es decir

$$b^n \equiv b\ (mod\ n). \blacksquare$$

tiene sentido darle un nuevo nombre a este tipo de números pues existen seudoprimos que no necesariamente son seudoprimos de Euler. Tomemos $n = 341 = 11 \cdot 31$, como ya se vió en el CAPITULO I, n es seudoprimo para la base 2, ahora $\frac{n-1}{2} = 170$ y

$$2^5 = 32 \equiv 1\ (mod\ 341),$$

de donde

$$2^{170} = (2^5)^{34} \equiv 1\ (mod\ 341).$$

Por otro lado, $341 = 344 - 3 = 8 \cdot 43 - 3$, de donde

$$341^2 - 1 = (8 \cdot 43 - 3)^2 =$$
$$8^2 43^2 - 2 \cdot 8 \cdot 43 + 3^2 - 1 =$$
$$8(8 \cdot 43^2 - 2 \cdot 43 + 1).$$

Por lo tanto $\frac{n^2-1}{8} = \frac{341^2-1}{8} = 8 \cdot 43^2 - 2 \cdot 43 + 1$, de aquí que $\frac{n^2-1}{8}$ es impar. Entonces

$$\left(\frac{b}{n}\right) = (-1)^{(n^2-1)/8} = -1,$$

por lo tanto

$$\left(\frac{b}{n}\right) \equiv b^{(n-1)/2}\ (mod\ n).$$

Sin embargo, todo seudoprimo fuerte es seudoprimo de Euler, pomo lo indica el siguiente resultado.

Teorema V.12.

Sea n entero impar compuesto. Si n es seudoprimo fuerte para

la base b, entonces n es seudoprimo de Euler para la base b.

Demostración:

Supongamos que n es seudoprimo fuerte para la base b, supongamos que $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ y $n - 1 = 2^s t$ con $s \geq 1$ y t impar, entonces

$$b^{2^j t} \equiv -1 \pmod{n} \quad \text{p.a. } 0 \leq j \leq s - 1,$$

o

$$b^t \equiv 1 \pmod{n}.$$

Supongamos primero que

$$b^t \equiv 1 \pmod{n}$$

entonces $ru = 1 - b^t$ para alguna $u \in \mathbb{Z}$, de donde $1 = ru + b^t$, es decir, $(b,n) = 1$, entonces $(b,p_i) = 1 \quad \forall\, i = 1,\ldots,k$, o bien $b \in (\mathbb{Z}_{p_i}, \cdot) \quad \forall\, i = 1,\ldots,n$. Sea $i \in \{1,\ldots,k\}$ cualquiera.

Ya que

$$b^t \equiv 1 \pmod{n},$$

entonces

$$b^t \equiv 1 \pmod{p_i} \quad \forall\, i = 1,\ldots,k$$

de aquí

$$o(b) \mid t$$

por lo tanto $o(b)$ es impar.

Como $o((\mathbb{Z}_{p_i}, \cdot)) = p_i - 1$ y $o(b)$ divide a $o((\mathbb{Z}_{p_i}, \cdot))$, entonces $o(b)v = p_i - 1$ para algun $v \in \mathbb{Z}$, como $p_i - 1$ es par y $o(b)$ es impar v tiene que ser par, es decir, $v = 2u$ p.a. $u \in \mathbb{Z}$, por lo tanto $\frac{p_i - 1}{2} = o(b)u$, de donde

$$\left(\frac{b}{p_i}\right) \equiv b^{(p_i-1)/2} \equiv b^{o(b)u} \equiv 1 \pmod{n}.$$

Entonces

$$\left(\frac{b}{p_i}\right) = 1 \quad \forall\, i = 1,\ldots,k,$$

por lo tanto

$$\left(\frac{b}{n}\right) = \prod_{i=1}^{k} \left(\frac{b}{p_i}\right)^{\alpha_i} = 1$$

y

$$b^{(n-1)/2} \equiv b^{2^{s-1}t} \equiv \left(b^t\right)^{2^{s-1}} \equiv 1 \pmod{n}$$

es decir

$$\left(\frac{b}{n}\right) \equiv b^{(n-1)/2} \pmod{n}.$$

Ahora supongamos que

$$b^{2^j t} \not\equiv -1 \pmod{n} \quad \text{p.a.} \quad 0 \leq j \leq s-1.$$

entonces

$$b^{2^j t} \not\equiv -1 \pmod{p_i} \quad \forall\, i = 1, \ldots, k$$

de donde

$$b^{2^{j+1}t} = \left(b^{2^j t}\right)^2 \equiv (-1)^2 \equiv 1 \pmod{p_i}$$

por lo tanto $o(b)$ divide a $2^{j+1}t$ y como

$$b^{2^j t} \not\equiv -1 \not\equiv 1 \pmod{n}$$

$o(b) \nmid 2^j t$.

Supongamos que

$$2^{j+1}t = o(b)u \qquad (u \in \mathbb{Z}),$$

si u fuese de la forma, $u = 2v$ se tendría $2^j t = o(b)v$ lo cual no puede pasar, por lo tanto u es impar, de donde, $(u, 2^{j+1}) = 1$ y como $2^{j+1}t = o(b)u$ tenemos $o(b) = 2^{j+1}(t/u)$, esto es, $2^{j+1} \mid o(b)$ y como

$$o(b) \mid o(\mathbb{Z}p_i, \cdot) = p_i - 1,$$

se tiene 2^{j+1} divide a $p_i - 1$, es decir

$$p_i = 2^{j+1}d_i + 1, \text{ con } d_i \in \mathbb{Z} \ (i = 1, \ldots, k).$$

Por otro lado, como

$$b^{o(b)} \equiv \left(b^{o(b)/2}\right)^2 \equiv 1 \pmod{p_i}$$

y p_i primo implican

$$b^{o(b)/2} \equiv 1 \pmod{p_i}$$

o

$$b^{o(b)/2} \equiv -1 \pmod{p_i}$$

pero el primer caso no puede pasar por que $\frac{o(b)}{2} < o(b)$, por lo tanto

$$b^{o(b)/2} \equiv -1 \pmod{p_i}$$

de aquí que

$$\left(\frac{b}{p_i}\right) \equiv b^{(p_i-1)/2} \equiv b^{(o(b)/2)(p-1)/o(b)}$$

$$\equiv (-1)^{(p-1)/o(b)} \equiv (-1)^{d_i/c} \pmod{p_i}$$

donde $c = \frac{t}{u}$ y como t y u son impares c es impar, entonces $\sqrt[c]{-1} = -1$, por lo tanto $(-1)^{d_i/c} = (-1)^{d_i}$.

Además

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = \prod_{i=1}^{k} (1 + 2^{j+1}d_i)^{\alpha_i}$$

$$= \prod_{i=1}^{k} \left(1 + \alpha_i 2^{j+1}d_i + \sum_{m=2}^{\alpha_i} \binom{\alpha_i}{m} \left(2^{j+1}d_i\right)^m\right)$$

$$\equiv \prod_{i=1}^{k} (1 + 2^{j+1}\alpha_i d_i)$$

$$\equiv (1 + 2^{j+1}\alpha_1 d_1)\prod_{i=2}^{k} (1 + 2^{j+1}\alpha_i d_i)$$

$$\equiv \prod_{i=2}^{k} (1 + 2^{j+1}\alpha_i d_i) + 2^{j+1}\alpha_1 d_1 \prod_{i=2}^{k} (1 + 2^{j+1}\alpha_i d_i)$$

$$\equiv \prod_{i=2}^{k} (1 + 2^{j+1}\alpha_i d_i) + 2^{j+1}\alpha_1 d_1(1 + 2^{j+1}\alpha_2 d_2)\prod_{i=3}^{k} (1 + 2^{j+1}\alpha_i d_i) \equiv \prod_{i=2}^{k} (1 +$$

$$2^{j+1}\alpha_i d_i) + 2^{j+1}\alpha_1 d_1 + 2^{j+2}2^j \alpha_1 \alpha_2 d_1 d_2 \prod_{i=3}^{k} (1 + 2^{j+1}\alpha_i d_i)$$

$$\equiv \prod_{i=2}^{k} (1 + 2^{j+1}\alpha_i d_i) + 2^{j+1}\alpha_1 d_1$$

$$\equiv (1 + 2^{j+1}\alpha_2 d_2)\prod_{i=3}^{k} (1 + 2^{j+1}\alpha_i d_i) + 2^{j+1}\alpha_1 d_1$$

$$\equiv \prod_{i=3}^{k} (1 + 2^{j+1}\alpha_i d_i) + 2^{j+1}\alpha_2 d_2 \prod_{i=3}^{k} (1 + 2^{j+1}\alpha_i d_i) + 2^{j+1}\alpha_1 d_1$$

$$\equiv \prod_{i=3}^{k} (1 + 2^{j+1}\alpha_i d_i) + 2^{j+1}\alpha_2 d_2 + 2^{j+1}\alpha_1 d_1 \equiv$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$(1 + 2^{j+1}\alpha_{k-1} d_{k-1})(1 + 2^{j+1}\alpha_k d_k) + 2^{j+1}\alpha_{k-2} d_{k-2} + \ldots + 2^{j+1}\alpha_2 d_2 +$$

$$2^{j+1}\alpha_1 d_1 \equiv$$

De aquí que

$$2^s t = n - 1 \equiv 2^{j+1} \sum_{i=1}^{k} \alpha_i d_i \pmod{2^{j+2}}$$

entonces

$$2^{j+2} r = 2^s t - 2^{j+1} \sum_{i=1}^{k} \alpha_i d_i \quad \text{p.a.} \quad r \in \mathbb{Z}$$

por lo tanto

$$2r = 2^{s-j-1} t - \sum_{i=1}^{k} \alpha_i d_i ,$$

es decir

$$2^{s-j-1} \equiv \sum_{i=1}^{k} \alpha_i d_i \pmod{2} ,$$

o bien, 2^{s-j-1} y $\sum_{i=1}^{k} \alpha_i d_i$ tienen la misma paridad, entonces

$$b^{(p-1)/2} = b^{2^{j+1}t} = \left(b^{2^j t}\right)^{2^{j+1}}$$
$$\equiv (-1)^{2^{j+1}} \equiv (-1)^{\sum \alpha_i d_i} \pmod{n} ;$$

por otro lado

$$\left(\frac{b}{n}\right) = \prod_{i=1}^{k} \left(\frac{b}{p_i}\right)^{\alpha_i}$$
$$= \prod_{i=1}^{k} \left((-1)^{d_i}\right)^{\alpha_i} = (-1)^{\sum \alpha_i d_i} ,$$

por lo tanto

$$\left(\frac{b}{n}\right) \equiv b^{(n-1)/2} \pmod{n} ,$$

es decir, n es seudoprimo de Euler para la base b.

Esta definición no esta de más pues aunque todo seudoprimo fuerte para la base b es seudoprimo de Euler para esta misma base no todo seudoprimo de Euler es seudoprimo fuerte. Por ejemplo $n = 1105 = 5 \cdot 13 \cdot 17$, que es seudoprimo de Euler para la base 2 no es seudoprimo fuerte para la base 2 como se muestra en seguida:

$n - 1 = 1104 = 2^4 \cdot 69$ y $2^3 \cdot 69 = 552$. Por el teorema de Euler tenemos que

$$2^4 \equiv 1 \pmod{5}$$
$$2^{12} \equiv 1 \pmod{13}$$

de donde

$$2^{552} = (2^4)^{138} \equiv 1 \pmod 5$$

$$2^{552} = (2^{12})^{46} \equiv 1 \pmod{13},$$

además como

$2^4 = 16 \equiv -1 \pmod{17}$ tenemos

$$2^{552} = (2^4)^{138} \equiv (-1)^{138} \equiv 1 \pmod{17}$$

por lo tanto

$$2^{2^3 69} = 2^{552} \equiv 1 \equiv -1 \pmod{1105}.$$

Ahora, $2^3 \cdot 69 = 276 = 24 \cdot 11 + 12$ y como

$$2^4 \equiv 1 \pmod 5$$

$$2^{12} \equiv 1 \pmod{13}$$

$$2^4 \equiv -1 \pmod{17}$$

tenemos

$$2^{24} = (2^4)^6 \equiv 1 \pmod 5$$

$$2^{24} = (2^{12})^2 \equiv 1 \pmod{13}$$

$$2^{24} = (2^4)^6 \equiv 1 \pmod{17}$$

por lo tanto

$$2^{24} \equiv 1 \pmod{1105}$$

de donde

$$2^{2^3 69} = 2^{276} = 2^{24 \cdot 11 + 12} = (2^{24})^{11} 2^{12} \equiv 2^{12}$$

$$= 2^{10} \cdot 4 = 1024 \cdot 4 \equiv -81 \cdot 4 = -324 \equiv 781 \pmod{1105}.$$

Por lo tanto 1105 no puede ser seudoprimo fuerte, sin embargo si n es compuesto y $n \equiv 3 \pmod 4$ ó $\left(\frac{b}{n}\right) = -1$, n es seudoprimo de Euler para la base b si y sólo si n es seudoprimo fuerte para la base b ya que si $n \equiv 3 \pmod 4$, n es de la forma $n = 4k + 3$, de donde $\frac{n-1}{2} = 2k + 1$ que es impar, además, $n - 1 = 2(\frac{n-1}{2})$ y si n es seudoprimo de Euler para la base b, se tiene

$$b^{(n-1)/2} \left(\frac{b}{n}\right) \equiv \pm 1 \pmod n,$$

es decir, n cumple con la prueba de Miller para la base b.

Ahora, si $\left(\frac{b}{n}\right) = -1$, entonces

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \equiv -1 \pmod{n},$$

es decir n cumple con la prueba de Miller para la base b.

Teorema V.13.

Existe una infinidad de seudoprimos de Euler para la base 2.

Demostración:

La demostración se sigue del teorema anterior ya que todo seudoprimo fuerte es de Euler y sabemos que existe una infinidad de seudoprimos fuertes para la base 2. ∎

NOTACION.

$\mathbb{Z}$	Números enteros.
$\mathbb{N}$	Enteros mayores que cero
$d \mid n$	d divide a n.
$a \equiv b \pmod{m}$	a es congruente con b módulo n.
$\mathbb{Z}_n$	El conjunto de residuos módulo n .
$(\mathbb{Z}_n, \cdot)$	El conjunto de residuos módulo n primos con n .
$H \leq G$	H es subgrupo de G.
$g \equiv h \pmod{H}$	g es congruente con h módulo H.
Hg (ó gH)	Clase lateral.
o(G)	Orden del grupo G.
o(g)	Orden del elemento g.
(g)	Subgrupo cíclico generado por g.
$i_g(a)$	Indice de a para la base g.
$\phi(n)$	La función de Euler, para cada $n > 1$ el número de enteros menores que n y primos con n y para 1 $\phi(1) = 1$.
F_n	El n-ésimo número de Fermat.
M_n	El n-ésimo número de Mersenne.
$\left(\frac{a}{n}\right)$	Si n es primo el símbolo de Legendre, si n es compuesto el símbolo de Jacobi.

BIBLIOGRAFIA.

1.- Introduccción a la teoría de los números
Niven y Zuckerman
Editorial limusa.

2.- Elementary Number Theory and its Applications
Kenneth H. Rosen
Addison-Wesley Publishing company.

3.- A Course in Number Theory and Cryptography
Neal Koblitz
Graduate Texts in Mathematics
Editorial Board

4.- Topics in algebra 2nd edition.
I. N. Herstein
John Wiley and Sons, Inc.