q-SEUDOPRIMALIDAD VS ω-PRIMALIDAD

Luz Elena Domínguez Rave

UNIVERSIDAD DEL VALLE
FACULTAD DE CIENCIAS NATURALES Y EXACTAS
2017

q-SEUDOPRIMALIDAD VS ω-PRIMALIDAD

Luz Elena Domínguez Rave
dominguez.luz@correounivalle.edu.co

Trabajo Presentado ante el Departamento de Matemáticas como parte de los requerimientos para obtener el título de Magister en Ciencias Matemática de la

Universidad del Valle

Director: Juan Miguel Velásquez Soto

UNIVERSIDAD DEL VALLE
FACULTAD DE CIENCIAS NATURALES Y EXACTAS
2017

Para....
Mamá, Papá, Isa y Sarita

Índice general

Introducción I

1. Preliminares 1

1.1. Resultados básicos 1

1.2. Grupos 5

2. Criterios determinísticos de primalidad 7

3. Seudoprimalidad 13

3.1. Seudoprimalidad de Fermat 13

3.2. Seudoprimos Fuertes 19

4. q-seudoprimos vs ω-Primos 27

4.1. q-Seudoprimos 27

4.2. ω-primos 31

5. Conclusiones 41

Introducción

Desde sus origenes, la Teoría de Números ha tratado de resolver dos grandes problemas: el primero de estos es determinar si un número es compuesto o no y el segundo es, sabiendo que el número es compuesto, encontrar su descomposición en factores primos. En el artículo 329 de las DISQUISITIONES ARITHMETICAE de Carl F. Gauss, se destaca la importancia de resolver estos problemas, pero además se menciona que los métodos desarrollados para la solución de estos han sido laboriosos y algo tediosos para números "grandes". A través del desarrollo tecnológico y la llegada de los computadores el ser humano se ha interesado por implementar algoritmos que se acercan a la solución de dichos problemas basados en teoremas como el Teorema de Pocklington, Teorema de Lucas-Lehmer, entre otros, pero a pesar de estos avances, en términos generales el problema sigue sin solución, ya que siempre es posible encontrar números para los cuales ni los algoritmos actuales, ni la capacidad de computo desarrollada hasta el momento pueden determinar su primalidad. Este hecho ha motivado el desarrollo de teorías que permitan por lo menos saber si un número es compuesto sin saber cuales son sus factores, o decir con una alta probabilidad que un número es primo.

Tal como lo proponen Richard Crandall y Carl Pomerance en su libro "Prime Number A Computacional Perspective" [4], si $S(n)$ es una afirmación sobre el número n y adicionalmente se tiene una proposición de la forma "Si n es un número primo, entonces se cumple $S(n)$", se dice que un número compuesto n es seudoprimo de clase S, si n también satisface la propiedad S. Es claro que existen diferentes tipos de números seudoprimos, entre los que se destacan, por sus aplicaciones y cercanía con los números primos, los seudoprimos de Fermat, los seudoprimos Fuertes, los de Frobenius, entre otros. Los números seudoprimos para una determinada propiedad S, son más cercanos a ser números primos que los números que no satisfacen S, por esta razón es útil estudiar las diferentes clases de seudoprimalidad.

En el presente trabajo se propone estudiar dos clases de seudoprimalidad: q-seudoprimos definidos en [3] y ω-primalidad introducida por Pedro Berrizbeitia en [1]. De ambos conceptos se estudiarán algunas de sus propiedades.

En la primera parte del documento se presentan varios conceptos básicos de la Teoría de Números, herramientas que serán de gran utilidad durante todo el trabajo.

En el segundo capítulo se describen los principales criterios determinísticos de primalidad más conocidos.

En la tercera parte, estudia la seudoprimalidad. La primera de ellas es la debida al Pequeño Teorema de Fermat, llamada seudoprimalidad de Fermat. Este concepto se puede

refinar un poco más y así se define la seudoprimalidad fuerte, que es el segundo tipo de seudoprimalidad que se estudia.

Finalmente, en el cuarto capítulo se presenta la generalización de seudoprimo fuerte, introducida por Castillo, García y Velásquez en [3] llamada q-seudoprimalidad y se introduce el concepto de ω-primo, se presentan algunas de sus propiedades, donde se hace un estudio comparativo entre dicho concepto y el de q-seudoprimo.

Capítulo 1

Preliminares

En el presente capítulo se exponen una serie de nociones y resultados básicos de la teoría elemental de números, con el fin de tener una mejor comprensión de los temas a tratar en los siguientes capítulos. Por tratarse de temas bastante conocidos se omitirán casi la totalidad de las pruebas, las mismas pueden encontrarse en cualquier texto introductorio a la teoría de números, por lo que se sugeriere [2], y [9]. El lector familiarizado con la teoría de números puede pasar directamente al siguiente capítulo.

1.1. Resultados básicos

Sean a, n números enteros, se dice que a es un divisor o un factor de n si existe un entero b tal que $n = ab$ y se denota por $a \mid n$. Si un entero n sólo tiene como divisores al 1 y al mismo n, se dice que es un número *primo*, en caso contrario se dice que es *compuesto*.

Desde los tiempos de Euclides se sabe que los números primos constituyen una base multiplicativa para los enteros.

Teorema 1 (Teorema Fundamental de la Aritmética)**.** *Todo número entero mayor que* 1 *es primo o es el producto de números primos; esta representación es única, salvo el orden de los factores.*

El *algoritmo de la división*, establece que para enteros a, b, con $b > 0$, existen enteros únicos q y r, con $0 \leq r < b$, tales que $a = qb + r$.

Dados enteros a, b el *máximo común divisor* de a y b, denotado por (a, b), es un entero positivo d que cumple las siguientes dos condiciones:

- *i*) $d \mid a$, $d \mid b$
- *ii*) si c es otro entero tal que $c \mid a$ y $c \mid b$ entonces $c \mid d$.

El siguiente resultado es clave a la hora de calcular el máximo común divisor entre dos enteros, ya que es la base del algoritmo de Euclides.

Proposición 2. *Sean a, b, c y d enteros, si $a = bc + d$ entonces $(a, b) = (b, d)$.*

A partir de la proposición anterior se puede probar el siguiente resultado.

Teorema 3 (Algoritmo de Euclides)**.** *Sean a_0, a_1, enteros con $a_1 \neq 0$ y sean*

$$\begin{array}{ll} a_0 = a_1q_1 + a_2 & con \quad 0 < a_2 < a_1 \\ a_1 = a_2q_2 + a_3 & con \quad 0 < a_3 < a_2 \\ \vdots & \vdots \\ a_{i-2} = a_{i-1}q_{i-1} + a_i & con \quad 0 < a_i < a_{i-1} \\ a_{i-1} = a_iq_i & \end{array}$$

Entonces a_i, el último residuo diferente de cero, verifica que $a_i = (a_0, a_1)$. Es más, existen enteros x, y tales que $(a_0, a_1) = a_0x + a_1y$. Ésta última relación se conoce como identidad de Bezout.

Teorema 4. *Sean a, b y c números enteros y $d = (a, b)$, la ecuación Diofántica $ax + by = c$ tiene solución en los enteros si y sólo si $d \mid c$. Más aún, si x_0, y_0 es solución particular de dicha ecuación, entonces todas las otras soluciones están dadas por*

$$x = x_0 + \left(\frac{b}{d}\right)t, \qquad y = y_0 - \left(\frac{a}{d}\right)t$$

donde t es un entero arbitrario.

El algoritmo de la división induce de manera natural una relación de equivalencia sobre los enteros cuando se deja fijo el divisor, así: si $n > 1$ es un entero, se dice que dos enteros a, b son *congruentes módulo n*, si ellos dejan el mismo residuo al ser divididos por n. Si este es el caso se escribe $a \equiv b \mod n$.

La clase de equivalencia de $a \mod n$ se llama clase residual de a módulo n y se denota $[a]$ o $\bar{a}$. Es claro que: $\bar{a} = \{b \in \mathbb{Z} : a \equiv b \mod n\}$.

El conjunto de todas las clases residuales módulo n se denota por $\mathbb{Z}_n$ o $\mathbb{Z}/n\mathbb{Z}$. Por lo tanto, $\mathbb{Z}_n := \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$. Generalmente, por abuso de notación, se escribe $\mathbb{Z}_n$ en la forma abreviada $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$.

En la siguiente proposición se consignan algunas propiedades básicas de la relación de congruencia módulo n.

Proposición 5. *Sean a, b, c, d y $n > 1$ números enteros, entonces:*

1. *Si $a \equiv b \mod n$ y $c \equiv d \mod n$, entonces $a + c \equiv b + d \mod n$ y $ac \equiv bd \mod n$.*
2. *Si $a \equiv b \mod n$, entonces $a^k \equiv b^k \mod n$ para todo $k \in \mathbb{N}$.*
3. *Si $a \equiv b \mod n$ y $c \in \mathbb{Z}$, entonces $ac \equiv bc \mod n$.*

4. Para $p(x) \in \mathbb{Z}[x]$, si $a \equiv b \mod n$, entonces $p(a) \equiv p(b) \mod n$.

Adicionalmente, si a, b, c, n son enteros tales que $ca \equiv cb \mod n$, entonces

$$a \equiv b \mod \frac{n}{(n,c)}.$$

Así las cosas, si $(n, c) = 1$ y $ca \equiv cb \mod n$, entonces $a \equiv b \mod n$.

Tal como en el caso de las ecuaciones, las propiedades anteriores permiten resolver ecuaciones en congruencias. Las ecuaciones de la forma $ax \equiv b \mod n$ son llamadas *congruencias lineales*, una solución de esta es un entero x_0 tal que $ax_0 \equiv b \mod n$.

En el siguiente teorema se dan condiciones necesarias y suficientes para que una congruencia lineal tenga solución.

Teorema 6. *Sean a, b y $n > 1$ números enteros y $d = (a, n)$, entonces la congruencia lineal $ax \equiv b \mod n$ tiene solución si, y sólo si, $d \mid b$. En tal caso, la ecuación tiene exactamente d soluciones incongruentes módulo n.*

Demostración. Dado que la congruencia lineal $ax \equiv b \mod n$ es equivalente a la ecuación Diofántica $ax - ny = b$, por el Teorema 4 ésta ecuación tiene solución, si y sólo si $d \mid b$, más aún, si x_0, y_0 son tales que $ax_0 - ny_0 = b$, las demás soluciones están dadas por $x = x_0 + \left(\frac{n}{d}\right) t$; $y = y_0 - \left(\frac{a}{d}\right) t$ para cualquier $t \in \mathbb{Z}$.

Es claro que x_0, $x_0 + \frac{n}{d}$, $x_0 + \frac{2n}{d}$, ..., $x_0 + \frac{(d-1)n}{d}$ son enteros no congruentes módulo n, y son solución de $ax \equiv b \mod n$, adicionalmente si $x = x_0 + (\frac{n}{d})t$ es una solución de la congruencia lineal, por el algoritmo de la división se tiene $t = qd + t'$, con $0 \leq t' \leq d - 1$, así que

$$\begin{aligned} x = x_0 + \frac{n}{d}t &= x_0 + \frac{n}{d}(qd + t') \\ &= x_0 + nq + \frac{n}{d}t' \\ &\equiv x_0 + \frac{n}{d}t' \mod n. \end{aligned}$$

□

El siguiente teorema establece condiciones para que un sistema de congruencias lineales tenga solución.

Teorema 7 (Teorema Chino del Resto)**.** *Sean $m_1, m_2, ..., m_r$ números enteros, positivos, primos relativos dos a dos. Entonces el sistema de congruencias*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_r \mod m_r \end{aligned}$$

tiene solución única módulo $M = m_1 m_2 \cdots m_r$.

Demostración. Para la construcción de la solución del sistema, considere $M_k = \dfrac{M}{m_k} = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_r$, dado que $(m_j, m_k) = 1$ para $j \neq k$ se tiene que $(M_k, m_k) = 1$, por lo tanto cada ecuación $M_k y \equiv 1 \mod m_k$ tiene solución, digamos que y_k es dicha solución; consideremos $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r$, entonces el entero x es solución simultánea de las congruencias, note que $m_k \mid M_j$ para $k \neq j$ así $M_j \equiv 0 \mod m_k$ por lo tanto $x \equiv a_k M_k y_k \equiv a_k \mod m_k$.

Para ver que la solución es única salvo congruencias módulo M, sean x_0 y x_1 soluciones del sistema de congruencias, entonces para cada k se tiene $x_0 \equiv x_1 \equiv a_k \mod m_k$, esto es, $m_k \mid (x_0 - x_1)$ y por lo tanto $M \mid (x_0 - x_1)$, es decir $x_0 \equiv x_1 \mod M$. □

Un conjunto destacado cuando se trabaja con congruencias módulo n es el conjunto de *unidades* módulo n,

$$\mathbb{U}_n := \{\overline{a} \in \mathbb{Z}_n : \ (a, n) = 1\}.$$

Se puede ver fácilmente, que $\mathbb{U}_n$ es un grupo abeliano bajo la multiplicación usual de clase de congruencias.

Si $n > 1$ es un entero, se define $\phi(n)$, *la función de Euler*, como el cardinal de $\mathbb{U}_n$, y $\phi(1) = 1$. Es posible probar que ϕ es una función multiplicativa, es decir, si m, n son enteros primos relativos entonces, $\phi(nm) = \phi(n)\phi(m)$. Por lo tanto, si $n = \prod_{i=1}^{r} p_i^{e_i}$, con p_i primo y e_i entero positivo entonces $\phi(n) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1)$.

Uno de los resultados más importantes de Teoría de Números, debido a Euler, es el siguiente.

Teorema 8 (Teorema de Euler)**.** *Sean a y n enteros positivos primos relativos, entonces*

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

Demostración. Sean n un número entero mayor que 1 y $\mathbb{U}_n := \{a_1, a_2, \ldots, a_{\phi(n)}\}$, dado que $(a, n) = 1$, entonces $a\mathbb{U}_n = \{aa_1, aa_2, \ldots, aa_{\phi(n)}\}$ coincide con $\mathbb{U}_n$. Por lo tanto

$$(aa_1)(aa_2)\cdots(aa_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} \mod n$$

de aquí que $a^{\phi(n)}(a_1 a_2 \cdots a_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} \mod n$ y como $(a_i, n) = 1$, se sigue que $a^{\phi(n)} \equiv 1 \mod n$.

□

Corolario 9 (Pequeño Teorema de Fermat)**.** *Si p es un número primo, entonces para cada número entero a se cumple*

$$a^{p-1} \equiv 1 \mod p.$$

1.2. Grupos

Si $(G, \cdot)$ es un grupo, con $|G|$ se denota el orden de G, es decir, el número de elementos de G. Si $a \in G$, con $|a|$ se denota el orden del elemento a, esto es, $|a|$ es el menor entero positivo tal que $a^{|a|} = 1$, donde 1 es el elemento neutro del grupo G. El grupo G se dice que es cíclico si existe un elemento g, en G, tal que $G = \{g^n : n \in \mathbb{Z}\}$. En este caso el grupo G es el *grupo cíclico generado por* g y que g *es un generador de* G. Si $H \subseteq G$ y H con la misma operación de G es un grupo, se dice que H es un subgrupo de G. Si G es un grupo finito y H es un subconjunto no vacío de G, una condición necesaria y suficiente para que H sea un subgrupo de G es que H sea cerrado bajo la operación del grupo, esto es: si a, $b \in H$ entonces $ab \in H$.

Cabe resaltar que si en $\mathbb{Z}_n$ se define una operación suma mediante $\bar{a} + \bar{b} = \overline{a+b}$ entonces, $\mathbb{Z}_n$ se dota de estructura de grupo aditivo cíclico, con elemento neutro $\bar{0}$. Además, el inverso aditivo de $\bar{a}$ es $\overline{n-a}$.

Teorema 10. *Sea n un entero positivo. El grupo $\mathbb{U}_n$ es cíclico si, y sólo si, n pertenece al conjunto $\{2, 4, p^n, 2p^n\}$.*

Si $\mathbb{U}_m$ es cíclico, un generador de él se llama una *raíz primitiva módulo m*. Si $a \in \mathbb{U}_m$ el orden de a, en este grupo, se llama el *orden de a módulo m* y se denota $|a|_m$. Un resultado fundamental en teoría de grupos finitos es el llamado Teorema de Lagrange, el cual establece que si G es un grupo finito y H es un subgrupo de G, entonces, $|H| \mid |G|$. En particular, si a es un elemento del grupo finito G, entonces $|a| \mid |G|$. Por lo tanto, el orden de a módulo m es un divisor de $\phi(m)$. A partir de la definición de orden de un elemento y del algoritmo de la división en $\mathbb{Z}$ se prueba el siguiente resultado.

Teorema 11. *Sea G un grupo, con elemento neutro 1, y $a \in G$ de orden h, entonces $a^t = 1$ si y sólo si $h \mid t$.*

Terminamos esta sección contando la cantidad de soluciones de la ecuación $x^n - 1 = 0$ en un grupo cíclico finito.

Teorema 12. *Sean G un grupo cíclico de orden n, k un entero y $d = (k, n)$, entonces la ecuación $x^k - 1 = 0$ tiene exactamente d soluciones en G.*

Demostración. Como G es un grupo cíclico de orden n, existe $g \in G$ de orden n. Supongamos que $x_0 = g^t$ es solución de la ecuación, esto es, $g^{tk} = 1$, por el Teorema 11, se tiene que $n \mid tk$, así $\frac{n}{d} \mid t\frac{k}{d}$ y ya que $\left(\frac{n}{d}, \frac{k}{d}\right) = 1$, entonces $\frac{n}{d} \mid t$, por lo tanto

$$t \in \left\{\frac{n}{d}, 2\frac{n}{d}, 3\frac{n}{d}, \ldots, (d-1)\frac{n}{d}, n\right\}$$

de manera que, $x^k - 1 = 0$ tiene exactamente $d = (n, k)$ soluciones en G a saber:

$$\left\{g^{\frac{n}{d}}, g^{2\frac{n}{d}}, \ldots, g^{(d-1)\frac{n}{d}}, g^n = 1\right\}.$$

□

Corolario 13. *Sean $n \in \mathbb{N}$ y p un número primo, $n = p^k t$ donde p no divide a t, entonces las congruencias $x^{n-1} \equiv 1 \mod p$ y $x^{n-1} \equiv 1 \mod p^k$ tienen la misma cantidad de soluciones.*

Demostración. Por el Teorema 12 el número de soluciones de $x^{n-1} \equiv 1 \mod p^k$ es $(n-1, \varphi(p^k)) = (n-1, p^{k-1}(p-1)) = (n-1, p-1)$ y el número de soluciones de la ecuación $x^{n-1} \equiv 1 \mod p$ es $(n-1, p-1)$, por lo tanto tienen la misma cantidad de soluciones. □

Capítulo 2

Criterios determinísticos de primalidad

En el estudio de la primalidad se han desarrollado varios resultados que permiten saber cuando un número es primo.

Uno de los primeros algorítmos para hallar los números primos menores que un número n dado, es la Criba de Eratóstenes, esta consiste en formar una tabla con todos los números naturales comprendidos entre 2 y n, y se van tachando los números que no son primos de la siguiente manera: comenzando por el 2, se tachan todos sus múltiplos hasta n; comenzando de nuevo, cuando se encuentra un número entero que no ha sido tachado, ese número es declarado primo, y se procede a tachar todos sus múltiplos, así sucesivamente hasta llegar a la raíz cuadrada del número n. Este algoritmo es poco eficiente para encontrar primos que tengan más de cinco cifras.

A continuación varios resultados que dan condiciones suficientes y necesarioas para que un entero sea primo.

Teorema 14. *(Teorema de Wilson-Lagrange 1771). Un entero p mayor que 1 es primo si, y sólo si*

$$(p-1)! \equiv -1 \mod p.$$

Demostración. Suponga que p es un número primo. Sea $a \in \{1, 2, \ldots, p-1\}$, si $a \neq 1$ y $a \neq p-1$, se tiene que la congruencia $ax \equiv 1 \mod p$ tiene solución, pues $(a, p) = 1$, así que cada $a \in \{2, 3, \ldots, p-2\}$ existe $r \in \{2, 3, \ldots, p-2\}$ tal que $ar \equiv 1 \mod p$ multiplicando cada una de estas congruencias se tiene:

$$2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \mod p.$$

Además se tiene que $p - 1 \equiv -1 \mod p$, multiplicando ambas congruencias obtenemos:

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdot 4 \cdots (p-2)(p-1) &\equiv (1)(-1) \mod p \\ (p-1)! &\equiv -1 \mod p. \end{aligned}$$

Recíprocamente, sea p es un número compuesto, por lo tanto p tiene un divisor d con $1 < d < p$, dado que $d \leq p-1$, entonces d es un factor de $(p-1)!$, así $d \mid (p-1)!$. Por hipótesis se tiene $p \mid (p-1)!+1$ entonces $d \mid (p-1)!+1$, esto implica que $d \mid 1$ pero $d \neq 1$. Por lo tanto p no es un número compuesto. □

Este criterio es poco eficiente y complicado aplicarlo, ya que el factorial crece rápidamente y para números de más o menos 4 cifras el factorial es bastante grande.

Teorema 15 (Teorema de Lucas 1876)**.** *Sean a y n enteros primos relativos, con $n > 1$. Si*

$$a^{n-1} \equiv 1 \mod n \tag{2.1}$$

y, para todo primo $q|n-1$, se cumple que:

$$a^{(n-1)/q} \not\equiv 1 \mod n \tag{2.2}$$

entonces, n es primo.

Demostración. Sea $M = \{e \in \mathbb{N} : a^e \equiv 1 \mod n\}$, es claro que, $n-1 \in M$ y que M es un subgrupo cíclico de $\mathbb{Z}$, así que existe d elemento mínimo de M. Si $d < n-1$ entonces $d \mid n-1$ y d divide por lo menos a uno de los números $\frac{n-1}{q}$ para q divisor primo de $n-1$, y por lo tanto $\frac{n-1}{d} \in M$ lo que contradice (2.2). Por lo tanto $d = n-1$.

Como $(a, n) = 1$ se tiene $a^{\phi(n)} \equiv 1 \mod n$, por lo tanto $\phi(n) \in M$ y como $\phi(n) \leq n-1 = d$, se tiene que $\phi(n) = n-1$, ya que d es el menor entero positivo perteneciente a M. En conclusión, n es un número primo. □

Existen dos inconvenientes principales al aplicar el Teorema de Lucas, el primero es encontrar un a que satisfaga las condiciones establecidas en el teorema, el segundo es encontrar la factorización de $n-1$. Por lo tanto hay dos formas de mejorar el Teorema de Lucas: debilitar las condiciones de a, o tener una factorización parcial de $n-1$.

El siguiente teorema establece mejoras a las condiciones con respecto a la base a.

Teorema 16. *Sea n un entero. Si para cada divisor q_i de $n-1$ existe un entero a_i tal que*

$$a_i^{n-1} \equiv 1 \mod n \quad y \quad a_i^{(n-1)/q_i} \not\equiv 1 \mod n$$

entonces, n es primo.

Demostración. Suponga que, $n-1 = q_1^{k_1} q_2^{k_2} \cdots q_r^{k_r}$ la descomposición en factores primos distintos de $n-1$ donde k_i son números enteros para $i = 1, ..., k$. Sea $h_i = |a_i|_n$, por hipótesis se tiene que $h_i \mid n-1$ y $h_i \nmid \frac{n-1}{q_i}$ por lo tanto $q_i^{k_i} \mid h_i$, pero para cada i se tiene que $h_i \mid \phi(n)$, así $q_i^{k_i} \mid \phi(n)$. Quiere decir $n-1 \mid \phi(n)$, por lo tanto n es primo. □

Ejemplo 17. Si $n = 47$, entonces $n - 1 = 46 = 2 \times 23$, para ver si n es un número primo, por el anterior teorema, para un divisor q_i de los divisores de $n-1$ se debe cumplir $a_i^{n-1} \equiv 1$ mód n y $a_i^{(n-1)/q_i} \not\equiv 1$ mód n.

En efecto, si $q_1 = 2$, entonces $a = 5$ cumple

$$a^{46} \equiv 1 \quad \text{mód } 47 \qquad \text{y} \qquad a^{23} \not\equiv 1 \quad \text{mód } 47.$$

Si $q_2 = 23$, se tiene que $a = 2$ cumple

$$a^{46} \equiv 1 \quad \text{mód } 47 \qquad \text{y} \qquad a^{2} \not\equiv 1 \quad \text{mód } 47$$

Por lo tanto, $n = 47$ es un número primo.

Por otra parte, si $n = 561$, se tiene que $n - 1 = 560 = 2^4 \times 5 \times 7$. A pesar que $a = 5$ satisface

$$a^{560} \equiv 1 \quad \text{mód } 561 \qquad \text{y} \qquad a^{280} \not\equiv 1 \quad \text{mód } 561$$

y $a = 7$ satistace

$$a^{560} \equiv 1 \quad \text{mód } 561 \qquad \text{y} \qquad a^{112} \not\equiv 1 \quad \text{mód } 561$$

, no existe un entero a, tal que

$$a^{560} \equiv 1 \quad \text{mód } 561 \qquad \text{y} \qquad a^{80} \not\equiv 1 \quad \text{mód } 561.$$

Y por el teorema anterior no se puede decidir si 561 es primo.

El Teorema de Lucas es útil cuando $n-1$ tiene una factorización simple, como lo tiene los números de Fermat F_n. Los siguientes resultados brindan herramientas para dar un criterio de primalidad para los números de Fermat.

Proposición 18. *Sea $F_n = 2^{2^n}+1$ el $n-$ésimo número de Fermat, entonces $F_n \equiv 5$ mód 12 para todo $n \geq 1$.*

Demostración. Si $n = 1$, $F_1 = 5 \equiv 5$ mód 12. Por inducción sobre n, se supone que $F_n \equiv 5$ mód 12,

$$F_{n+1} = 2^{2^{n+1}} + 1 = (2^{2^n})^2 + 1 = (F_n + 1)^2 + 1 \equiv 4^2 + 1 \equiv 5 \quad \text{mód } 12$$

□

Como consecuencia de esto hecho y del hecho que 3 es un no residuo cuadrático módulo p para un número primo $p > 3$, tal que, $p \equiv \pm 5$ mód 12 se tiene:

Ejemplo 19 (Pepin, 1877)**.** Una condición suficiente y necesaria para que un número de Fermat $F_n = 2^{2^n} + 1$ para $n \geq 1$, sea primo es:

$$3^{2^{2^n}-1} \equiv -1 \mod F_n.$$

Por el Teorema 15, F_n es primo si y sólo si existe un entero a tal que

$$a^{\frac{F_n-1}{2}} = a^{2^{2^n}-1} \not\equiv 1 \mod F_n \qquad (1)$$

y

$$a^{(F_n-1)} = a^{2^{2^n}} \equiv 1 \mod F_n \qquad (2).$$

Si $x = a^{2^{2^n}-1}$, se reduce el problema a encontrar un entero x tal que $x^2 - 1 \equiv 0 \mod F_n$ y $x \not\equiv 1 \mod F_n$. Si F_n es primo entonces x es un elemento de un anillo sin divisores de cero y por lo tanto la congruencia

$$x^2 - 1 = (x-1)(x+1) \equiv 0 \mod F_n$$

tendrá solamente dos soluciones:

$$x \equiv 1 \mod F_n \text{ y } x \equiv -1 \mod F_n$$

así se pretende encontrar un entero a tal que $x = a^{\frac{F_n-1}{2}} \equiv -1 \mod F_n$, es decir, a es un no residuo cuadrático módulo F_n y por la observación anterios se tiene que 3 es un no residuo cuadrático módulo F_n, luego si $a = 3$ se satisfacen las condiciones requeridas y con esto se concluye el ejercicio.

En el siguiente teorema, conocido como el Teorema de Pocklington, se exige una factorización parcial de $n - 1 = fr$, donde f está completamente factorizado. Si $f > r$ se puede garantizar la primalidad de n.

Teorema 20 (Teorema de Pocklington-Lehmer, 1928)**.** *Sea n un entero y $n-1 = fr$, donde se conoce la factorización prima de f, esto es, $f = q_1^{k_1} q_2^{k_2} \cdots q_s^{k_s}$. Si para cada primo q_i existe un entero a_i tal que*

$$a_i^{n-1} \equiv 1 \mod n$$

y

$$(a_i^{(n-1)/q_i} - 1, n) = 1.$$

Entonces, todo factor primo p de n es congruente con 1 módulo f.

Demostración. Si $p \mid n$ y $q \mid f$, con p y q primos, sean a_i tal que cumple las condiciones del teorema y $e = |a_i|_p$, así que $e \mid p-1$ y por la primera condición de la hipótesis $e \mid n-1$, por lo tanto $\frac{n-1}{e} \in \mathbb{Z}$. De la segunda condición de la hipótesis y del hecho que $p \mid n$ se tiene $a_i^{\frac{n-1}{q}} - 1 \not\equiv 0 \mod p$, así que $e \nmid \frac{n-1}{q}$. Sea s la mayor potencia de q que divide a f, entonces $q^s \mid n-1$ y $q \nmid \frac{n-1}{e}$ así que $q^s \mid e$ y como $e \mid p-1$, se tiene $q^s \mid p-1$. Como se cumple para todo primo $q \mid f$ se tiene que $f \mid p-1$. □

Corolario 21. *Si $f > r$ y se mantiene las hipótesis del teorema anterior, entonces n es primo.*

Demostración. Sea p el menor primo que divide a n y supongamos que n es compuesto, entonces $p \leq \sqrt{n}$. Pero, como $f^2 > n-1$, entonces $f \geq \sqrt{n}$ y del Teorema 20 se tiene que $f \mid p-1$, es decir $p > p-1 \geq f$, lo cual es un absurdo, por lo tanto n es primo. □

Corolario 22 (Proth, 1878)**.** *Sea $N = 2^m h + 1$ un entero. Si existe un entero a tal que*

$$a^{\frac{N-1}{2}} \equiv -1 \mod N$$

entonces, todo primo p divisor de N, es de la forma $2^m t + 1$, con t entero positivo.

Demostración. Si en el Teorema 20 se toma a $f = 2^m$, veamos que se cumplen todas las hipótesis, en efecto, dado que $a^{\frac{N-1}{2}} \equiv -1 \mod N$, entonces $a^{N-1} \equiv 1 \mod n$ y además se cumple $\left(a^{\frac{N-1}{2}}, 2^m h + 1\right) = 1$ por lo tanto todo divisor primo p de N es de la forma $2^m t + 1$. □

Capítulo 3

Seudoprimalidad

En el capítulo anterior se presentaron varios resultados que permiten determinar cuándo un número es primo, pero dadas las condiciones que se deben cumplir son muchas las desventajas que se tiene al aplicar estos criterios determinísticos, por ejemplo, en ocasiones se necesita saber la factorización completa de $n-1$, o bien encontrar un número natural que cumpla varias condiciones a la vez. En este capítulo se desarrolla un concepto que se acerca bastante al de primalidad y en ciertos casos se puede decir cuándo un número es compuesto, aún sin conocer sus factores.

En general, si $S(n)$ es una afirmación "fácilmente" verificable sobre el número n y si se tiene un teorema de la forma "Si n es un número primo entonces $S(n)$ es cierto", es válido preguntarse por la existencia de números compuestos que cumplen la propiedad S, dichos números son conocidos como seudoprimos de clase S.

En las siguentes secciones se estudiarán algunos tipos de seudoprimalidad y se contarán las bases para las cuales tales primalidades ocurren, los resultados son tomados del documento "ARITMETICA: UN ENFOQUE COMPUTACIONAL" escrito por el profesor Gilberto García, [5].

3.1. Seudoprimalidad de Fermat

El hecho que $a^b \mod n$ pueda calcularse de forma rápida computacionalmente, es fundamental en muchos resultados y algoritmos en la teoría de números, uno de estos es el Pequeño Teorema de Fermat, el cuál permite distinguir números primos de compuestos.

Teorema 23. *(Pequeño Teorema de Fermat) Si n es un número primo, entonces para todo entero a primo relativo con n, se cumple*

$$a^{n-1} \equiv 1 \mod n.$$

De hecho, sea n un número entero, si se toma al azar un número $a \in \mathbb{Z}$, al calcular el máximo común divisor entre n y a existen dos posibilidades, la primera es que dicho máximo

común divisor sea diferente de 1, en este caso, el número n es compuesto y uno de sus factores es el máximo común divisor; la segunda es que el máximo común divisor entre a y n es 1, para esta opción, por el Pequeño Teorema de Fermat, se calcula $a^{n-1} \mod n$, si dicho valor no es 1, se puede asegurar que n es un número compuesto, en caso contrario no se puede decidir acerca de la primalidad n, si un número n cumplen esta condición para un valor fijo de a se le llama **probable primo** base a.

Definición 24. Sean n y a números enteros, con n compuesto y $(a, n) = 1$. Se dice que n es seudoprimo de Fermat, o símplemente seudoprimo base a, si se cumple $a^{n-1} \equiv 1 \mod n$.

Por ejemplo, 91 es seudoprimo base 3, note que: $(91, 3) = 1$, y dado que $91 = 7 \times 13$, $3^6 \equiv 1$ mód 7 y $3^3 \equiv 1 \mod 13$, elevando convenientemente y haciendo uso de las propiedades de la congruencia se sigue que $3^{90} \equiv 1 \mod 91$.

En la siguiente tabla se presentan algunas bases de seudoprimalidad para algunos números.

a	n
2	341, 561, 645
3	91, 121, 286
4	15, 85, 91
5	4, 124, 217
10	9, 33, 91
15	14, 341, 742
20	21, 57, 133

Para ampliar esta tabla ver `http://oeis.org/wiki/Table_of_Fermat_pseudoprimes`.

Se puede contar la cantidad de bases para las que un número dado es seudoprimo, para esto se define

$$Bsp(n) := \left\{1 \leq a < n : \ (a, n) = 1 \text{ y } a^{n-1} \equiv 1 \mod n\right\}. \tag{3.1}$$

Por ejempo, si $n = 9$, dado que

$$\begin{array}{lll} 1^8 \equiv 1 \mod 9; & 2^8 \equiv 4 \mod 9; & 4^8 \equiv 7 \mod 9 \\ 5^8 \equiv 7 \mod 9; & 7^8 \equiv 4 \mod 9; & 8^8 \equiv 1 \mod 9 \end{array}$$

se tiene que $Bsp(9) = \{1, 8\}$.

En el siguiente lema se muestra que el conjunto de bases de seudoprimalidad para un entero fijo n, tiene estructura de grupo.

Lema 25. *Sea n un entero mayor que 1, entonces $Bsp(n) = \{1 \leq a < n : \ (a, n) = 1$ y $a^{n-1} \equiv 1 \mod n\}$. es un subgrupo de $\mathbb{U}_n$.*

Demostración. Es claro que $Bsp(n) \subset \mathbb{U}_n$. Por otra parte, sean $a, b \in Bsp(n)$, entonces $(a,n) = 1$, $(b,n) = 1$, $a^{n-1} \equiv 1 \mod n$ y $b^{n-1} \equiv 1 \mod n$, dado que $\mathbb{U}_n$ es grupo se tiene que $(ab^{-1}, n) = 1$, además

$$(ab^{-1})^{n-1} = (b^{-1})^{n-1}a^{n-1} = (b^{n-1})^{-1}a^{n-1} \equiv (1)^{-1}1 \equiv 1 \mod n$$

por lo tanto $ab^{-1} \in Bsp(n)$. □

Como consecuencia del lema anterior, para un número fijo n, $|Bsp(n)|$ es finito, más aún es un divisor de $\phi(n)$.

De otro lado, si a es un entero fijo, se puede probar que existen infinitos seudoprimos de Fermat base a. Una de tales pruebas es el siguiente teorema.

Teorema 26 (Cipolla, 1904)**.** *Sean p un número primo, a un número entero tal que $p \nmid a(a^2-1)$ y sean $n_1 = \dfrac{a^p - 1}{a-1}$ y $n_2 = \dfrac{a^p + 1}{a+1}$, entonces $n = n_1 n_2$ es seudoprimo base a.*

Demostración. Claramente n es un número compuesto. Veamos que $a^{n-1} \equiv 1 \mod n$. Por la hipótesis, se tiene

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

Dado que p es un número primo y $(a,p) = 1$, por el Pequeño Teorema de Fermat se tiene que,

$$a^{2p} \equiv a^2 \mod p$$

por lo tanto p divide a $a^{2p} - a^2 = (n-1)(a^2-1)$, pero p no divide a $a^2 - 1$, así que p divide a $n - 1$.

Por otra parte, dado que $n = \dfrac{a^{2p} - 1}{a^2 - 1} = 1 + a^2 + \cdots + a^{2(p-1)}$ y p es impar, entonces $n-1$ se puede expresar como la suma de una cantidad par de términos de la misma paridad, así $n - 1$ es par, en consecuencia $2p$ divide a $n - 1$, por lo tanto $a^{2p} - 1$ divide a $a^{n-1} - 1$, pero $a^{2p} - 1$ es un múltiplo de n, luego $n | a^{n-1} - 1$. □

El siguiente teorema da una caracterización de los números seudoprimos por medio de la solución de la ecuación $x^k - 1 = 0$.

Teorema 27. *Sean $a \geq 2$ y n un número compuesto con $(a,n) = 1$. n es seudoprimo base a si, y sólo si, para todo primo p divisor de n se cumple*

$$a^{n/p-1} \equiv 1 \mod p.$$

Demostración. Suponga que n es seudoprimo base a, $a^{n-1} \equiv 1 \mod p$, y dado que $a^n = (a^p)^{n/p} \equiv a^{n/p} \mod p$, se tiene

$$\begin{aligned} a^{n-1} &\equiv a^n a^{-1} \quad \text{mód } p \\ &\equiv a^{n/p} a^{-1} \quad \text{mód } p \\ &\equiv a^{(n/p)-1} \quad \text{mód } p \end{aligned}$$

por lo tanto $a^{(n/p)-1} \equiv 1 \mod p$.

Recíprocamente, suponga que para todo primo $p|n$, se cumple $a^{(n/p)-1} \equiv 1 \mod p$, y dado que $a^p \equiv a \mod p$, entonces

$$(a^p)^{(n/p)-1} \equiv a^{(n/p)-1} \quad \text{mód } p.$$

Por otra parte, $a^{n-p} = a^n (a^p)^{-1}$, así $a^{n-p} \equiv a^n a^{-1} \mod p$, lo que permite concluir que $a^{n-1} \equiv 1 \mod p$. □

Corolario 28. *Si $n = pq$ y $t = (p-1, q-1)$, entonces las bases de seudoprimalidad para n son justamente las soluciones de la ecuación $x^t \equiv 1 \mod n$.*

Demostración. Sea n un seudoprimo base a, esto es, $(a, n) = 1$ y $a^{n-1} \equiv 1 \mod n$. Por el teorema anterior se tiene que $a^{p-1} \equiv 1 \mod q$ y $a^{q-1} \equiv 1 \mod p$, quiere decir, $|a|_q \mid p-1$ y $|a|_p \mid q-1$.

Por el Pequeño Teorema de Fermat se tiene $a^{q-1} \equiv 1 \mod q$ y $a^{p-1} \equiv 1 \mod p$, esto implica, $|a|_q \mid q-1$ y $|a|_p \mid p-1$. Como consecuancia de lo anterior $|a|_q \mid (p-1, q-1)$ y $|a|_p \mid (p-1, q-1)$, así $a^t \equiv 1 \mod n$. Las bases de seudoprimalidad de n son las soluciones de la ecuación $x^t \equiv 1 \mod n$. □

De ahora en adelante $\nu_p(n)$ denota la máxima potencia con que aparece p en la descomposición en factores primos de n.

Por ejemplo: $140625 = 3^2 \times 5^6$, se tiene que $\nu_5(140625) = 6$ y $\nu_3(140625) = 2$.

El siguiente teorema cuenta las bases de seudoprimalidad para un número n.

Teorema 29. *Sea $n = \prod_{i=1}^{r} p_i^{k_i}$ donde p_j son números primos para $0 \leq j \leq r$, entonces*

$$|Bsp(n)| = \prod_{i=1}^{r} (n-1, p_i - 1).$$

Demostración. Para encontrar la cantidad de bases de seudoprimalidad para n se cuentan cuántos enteros primos relativos con n son solución de la congruencia $x^{n-1} - 1 \equiv 0 \mod n$. Para esto, en virtud del Teorema Chino del Residuo se debe determinar la cantidad de soluciones de $x^{n-1} - 1 \equiv 0 \mod p_i^{\alpha_i}$ para $i = 1, \ldots, r$.

Por el Corolario 13 basta contar la cantidad de soluciones de la congruencia $x^{n-1} \equiv 1 \mod p_i$, para $i = 1, \ldots, r$ y esta congruencia tiene solución si $x^{n-1} - 1 = 0$ tiene solución en

$\mathbb{Z}_{p_i}$, en efecto, por el Teorema 12 la cantidad de soluciones es $(n-1, \phi(p_i)) = (n-1, p_i - 1)$. Por lo tanto, $x^{n-1} - 1 \equiv 0 \mod n$ tiene $\prod_{i=1}^{r}(n-1, p_i - 1)$ soluciones. □

Ejemplo 30. Sea $n = 4095 = 3^2 \times 5 \times 7 \times 13$. La cantidad de bases de seudoprimalidad para n es 16, quiere decir que existen solo 16 números primos relativos a 4095 de los 1728 posibles que lo hacen ser un número seudoprimo. Este hecho hace que el número sea "fácil" de identificar como compuesto.

Ahora sea $n = 341 = 11 \times 31$. Se tiene que $|Bsp(n)| = 100$ y $\phi(341) = 300$; en este caso las bases de seudoprimalidad es mucho mayor que en el caso anterior así la probabilidad de decidir si n es compuesto es mucho menor que en el caso anterior.

Al tener las bases de seudoprimalida surge la pregunta: ¿Existen números enteros n tal que el conjunto de bases de seudoprimalidad coincide con el conjunto de las unidades? El siguiente teorema da las condiciones que se deben considerar para que la respuesta sea afirmativa.

Teorema 31 (Teorema de Korselt)**.** *Sea* $n = \prod_{i=1}^{r} p_i^{k_i}$ *su descomposición en factores primos tal que cumple* $Bsp(n) = \mathbb{U}_n$ *si y sólo si* n *es un entero positivo, compuesto, libre de cuadrado y para cada primo* p *divisor de* n *se tiene que* $p - 1$ *divide a* $n - 1$.

Demostración. Suponga que existe un n tal que $Bsp(n) = \mathbb{U}_n$, en primer lugar, consedere que n no es libre de cuadrado, esto es, existe p un número primo tal que $p \mid n$ y $p^2 \mid n$, dado que la función $\phi(n)$ es multiplicativa y $\phi(p^\alpha) = p^{\alpha-1}(p-1)$, entonces $p \mid \phi(n) = \prod_{p_i}(n-1, p_i - 1)$, por lo tanto existe un p_i tal que $p \mid (n-1, p_i - 1)$, en consecuencia $p \mid n - 1$, así $p \mid 1$ pero $p > 1$, se concluye que n es libre de cuadrado.

Sea p un número primo divisor de n, por el Teorema de Fermat $a^{p-1} \equiv 1 \mod p$ para $a \in \mathbb{Z}$ primo relativo con p, quiere decir, $|a|_p \mid p - 1$. Por otra parte $a^{n-1} \equiv 1 \mod n$ y dado que $p \mid n$ se tiene que $a^{n-1} \equiv 1 \mod p$, así $|a|_p$ divide a $n - 1$, se concluye que $p - 1 \mid n - 1$.

Recíprocamente, sea n es un número compuesto, libre de cuadrado y que para cada primo p divisor de n, se tiene que $p - 1$ divide a $n - 1$. Se debe ver que $a^n \equiv a \mod n$ para todo entero a primo relativo con n. Dado que n es libre de cuadrado, basta demostrar que $a^n \equiv a$ mód p para todo entero a y todo primo p divisor de n. Si a no es divisible por p se tiene $a^{p-1} \equiv 1 \mod p$ y dado que $p - 1 \mid n - 1$ tenemos $a^{n-1} \equiv 1 \mod p$. □

Ejemplo 32. Sea $n = 561$, este número cumple con las dos condiciones del Teorema 31:

i) Es libre de cuadrado ya que $n = 561 = 3 \times 11 \times 17$.

ii) Se tiene $560 = 280 \times 2 = 56 \times 10 = 35 \times 16$, esto es, para todo p primo divisor de n, $p - 1$ divide a $n - 1$.

Además de esto, para $b \in \mathbb{Z}$ con $(b, 561) = 1$ se tiene que $b^{561-1} \equiv 1 \mod 561$, en efecto, como $(b, 561) = 1$ entonces $(b, 3) = 1$, $(b, 11) = 1$ y $(b, 17) = 1$. Por el Pequeño Teorema de Fermat $b^2 \equiv 1 \mod 3$, $b^{10} \equiv 1 \mod 11$ y $b^{16} \equiv 1 \mod 17$. Por lo tanto

$$b^{560} = (b^2)^{280} \equiv 1 \mod 3$$
$$b^{560} = (b^{10})^{53} \equiv 1 \mod 11$$
$$b^{560} = (b^{16})^{35} \equiv 1 \mod 17.$$

El anterior ejemplo permite dar cuenta que existen números seudoprimos para todas las posibles bases, "seudoprimos absolutos", quiénes son estos números? son infinitos? que propiedades cumplen?

Definición 33. Un número entero compuesto n tal que satisface $b^{n-1} \equiv 1 \mod n$ para todos los enteros positivos b primos relativos con n, es llamado número de Carmichael o seudoprimo absoluto.

Ejemplo 34. El primer número de Carmichael es el 561. Los siguientes números de Carmichael son 1105, 1729, 2465, ..., la lista es infinita.

Simplificando las condiciones del Teorema de Korselt 31 se tiene una caracterización de los números de Carmichael:

Teorema 35. *Si $n = pqr$, donde p, q, r son números primos impares distintos, entonces n es de Carmichael si, y sólo si $p - 1$ divide a $qr - 1$, $q - 1$ divide a $pr - 1$ y $r - 1$ divide a $pq - 1$.*

Demostración. Por el Teorema 31, n es de Carmichael si y sólo si $p-1$, $q-1$ y $r-1$ dividen a $n-1$ pero $n-1 = pqr-1 = pq(r-1)+pq-1 = pr(q-1)+pr-1 = qr(p-1)+qr-1$. Por lo tanto si $p-1$ divide a $n-1$ y también divide a $qr(p-1)$, entonces necesariamente divide al otro sumando $qr-1$, recíprocamente, si $p-1$ divide a $qr-1$, como divide al segundo sumando, entonces divide a la suma, que es $n-1$. De forma análoga se razona con $q-1$ y $r-1$. □

Se puede probar que

$$c(m) = (12m + 7)(36m + 13)(48m + 27)$$
$$c(m) = (6m + 7)(12m + 13)(18m + 19)$$
$$c(m) = (30m + 7)(60m + 13)(150m + 31)$$

Son números de Carmichael si cada uno de los factores son números primo. Por ejemplo si $m = 0$, el número $c(0) = 7 \times 13 \times 19 = 1729$ es un número de Carmichael.

Richard Pinch tiene la más grande lista de números de Carmichael. Para ver más detalle de estos números se puede dirigir a `http://oeis.org/A002997`.

3.2. Seudoprimos Fuertes

Considere $p \geq 2$ un primo, y $p-1 = 2^s t$ con $(2,t) = 1$, y sea a es un entero no divisible por p, entonces $a^{p-1} \equiv 1 \mod p$, o lo que es lo mismo $a^{2^s t} \equiv 1 \mod p$, factorizando como diferencias de cuadrados tantas veces como sea posible se tiene:

$$\begin{aligned} p \mid a^{2^s t} - 1 &\Leftrightarrow p \mid \left(a^{2^{s-1}t} - 1\right)\left(a^{2^{s-1}t} + 1\right) \\ &\Leftrightarrow p \mid \left(a^{2^{s-1}t} + 1\right)\left(a^{2^{s-2}t} - 1\right)\left(a^{2^{s-2}t} + 1\right) \\ &\vdots \\ &\Leftrightarrow p \mid \left(a^{2^{s-1}t} + 1\right)\left(a^{2^{s-2}t} + 1\right)\left(a^{2^{s-3}t} + 1\right)\cdots\left(a^t + 1\right)\left(a^t - 1\right). \end{aligned}$$

y como p es primo, se puede afirmar que

$$p \mid a^t - 1 \qquad \text{ó} \qquad \text{existe } i \text{ con } 0 \leq i \leq s-1 \text{ tal que } p \mid a^{2^i t} + 1,$$

equivalentemente

$$a^t \equiv 1 \mod p \qquad \text{ó} \qquad \text{existe } i \text{ con } 0 \leq i \leq s-1 \text{ tal que } a^{2^i t} \equiv -1 \mod p.$$

Ésta reescritura del Pequeño Teorema de Fermat permite definir, a la luz de la seudoprimalidad, una nueva clase de seudoprimos, los seudoprimos fuertes.

Definición 36. Sean a, n enteros, n compuesto y $(a,n) = 1$, se dice que n es seudoprimo fuerte en base a, si al escribir $n - 1 = 2^s t$, con $(2,t) = 1$, se cumple una de las siguientes condiciones:
i.) $a^t \equiv 1 \mod p$ ó
ii.) Existe i con $0 \leq i \leq s-1$ tal que $a^{2^i t} \equiv -1 \mod p$.

Notación: En lo sucesivo, cuando n sea seudoprimo fuerte base a, se escribirá $n \in Spf(a)$. Adicionalmente, al conjunto de bases de seudoprimalidad fuerte para un número fijo n se lo denotará por $Bspf(n)$, esto es,

$$Bspf(n) := \{a \in \mathbb{Z} \ : \ (a,n) = 1 \text{ y } n \text{ es seudoprimo fuerte base } a\}.$$

Note que si n es seudoprimo fuerte base a, entonces n es seudoprimo de Fermat base a, ya que si existe $i < s$, para el cual $a^{2^i t} \equiv -1 \mod n$, se elige $k > 1$ tal que $i + k = s$, se tiene que

$$(a^{2^i t})^{2^k} \equiv (-1)^{2^k} \mod n \Leftrightarrow a^{n-1} \equiv 1 \mod n.$$

el caso $a^t \equiv 1 \mod n$ se resuelve con un argumento similar.

Teorema 37. *Sea n un número entero, si n es seudoprimo base 2, entonces $m = 2^n - 1$ es seudoprimo fuerte base 2.*

Demostración. Dado que n es compuesto, existen enteros $l > 1$, $k > 1$ para los cuales $n = lk$, y por tanto $2^l - 1 \mid 2^n - 1 = m$, es decir m es compuesto. Además $m - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2t$, y como por hipótesis $2^{n-1} \equiv 1 \mod n$, se sigue que $n \mid 2^{n-1} - 1$, o lo que es lo mismo $n \mid t$, y en consecuencia $2^n - 1 \mid 2^t - 1$. □

Es fácil ver que $n \in \mathbb{Z}$, los números de Fermat, $F_n := 2^{2^n} + 1$ son primos ó seudoprimos fuertes base 2.

El siguiente resultado es un criterio de seudoprimalidad fuerte para potencias de un primo.

Lema 38. *Sean p un número primo impar, $n > 1$, a un entero primo relativo con p, entonces $p^n \in Spf(a)$ si, y sólo si $p^n \in Sp(a)$.*

Demostración. Suponga que $a^{p^n-1} \equiv 1 \mod p^n$, si $p^n - 1 = 2^s t$, se tiene que $a^{2^s t} \equiv 1 \mod p^n$ y es equivalente a $(a^{2^{s-1}t})^2 \equiv 1 \mod p^n$, entonces

$$a^{2^{s-1}t} \equiv 1 \mod p^n \quad \text{ó} \quad a^{2^{s-1}t} \equiv -1 \mod p^n.$$

En el caso que se cumpla $a^{2^{s-1}t} \equiv -1 \mod p^n$ se tiene el enunciado. En el caso contrario se tiene que $(a^{2^{s-1}t})^2 \equiv 1 \mod p^n$ y de nuevo

$$a^{2^{s-2}t} \equiv 1 \mod p^n \quad \text{ó} \quad a^{2^{s-2}t} \equiv -1 \mod p^n.$$

En general se cumple que:

$$p^n \mid a^{2^i t} + 1$$

para algún $0 \leq i \leq s - 1$ ó

$$p^n \mid b^t - 1$$

esto es, $p^n \in Spf(a)$. □

Encontrar números seudoprimos fuertes es una tarea a la que se han dedicado varios investigadores a nivel mundial, un ejemplo de esto son los matemáticos Yupeing Jiang y Yingpu Deng, en su artículo "*Strong pseudoprimes to the first eight prime bases*" [6] definen

$$\Psi_k = min\{n \in Spf(p_j) : 1 \leq j \leq k\}$$

como el menor número que es seudoprimo fuerte en las bases de los primeros k primos a la misma vez.

Por ejemplo $\Psi_2 = 1373653$, este número es el menor seudoprimo fuerte en base 2 y 3. $\Psi_3 = 25326001$, es el menor seudoprimo fuerte en base 2, 3 y 5. Hasta la fecha sólo se ha encontrado hasta Ψ_{12}.

Al igual que en la seudoprimalidad de Fermat, se pueden contar la cantidad de bases de seudoprimalidad fuerte para un entero fijo n.

Para ilustrar el método de conteo que se usará en este caso, considere primero $n = pq$ el producto de dos primos impares diferentes y sea $n - 1 = 2^{s_n} t_n$ con t_n impar, y expresiones similares para $p - 1$ y $q - 1$. Sea $s = min\{s_p, s_q\}$, (note que $s \geq 1$), y sea $(a, b)^*$ el mayor impar que es divisor común de a y b. Como

$$n - 1 = pq - 1 = p(q - 1) + (p - 1) = q(p - 1) + (q - 1)$$

se sigue que

$$(n - 1, p - 1)^* = (n - 1, q - 1)^* = (p - 1, q - 1)^* = (t_p, t_q).$$

Sea $t = (t_p, t_q)$ y $b \in \mathbb{U}_n$ tal que n es $Spf(b)$. Entonces

$$b^{t_n} \equiv 1 \mod n \tag{1}$$

ó

$$b^{2^i t_n} \equiv -1 \mod n \text{ para algún } i = 0, 1, \ldots, s_n - 1 \tag{2}$$

Si ocurre (1), entonces

$$b^{t_n} \equiv 1 \mod p \text{ y } b^{t_n} \equiv 1 \mod q,$$

ahora, la cantidad de elementos b tales que $b^{t_n} \equiv 1 \mod p$ es exactamente

$$(t_n, p - 1) = (n - 1, p - 1)^* = t.$$

De manera similar, hay exactamente

$$(t_n, q - 1) = (n - 1, q - 1)^* = t$$

elementos b tales que $b^{t_n} \equiv 1 \mod q$.

Si b_1 (respectivamente b_2) es tal que $b_1^{t_n} \equiv 1 \mod p$ (respectivamente $b_2^{t_n} \equiv 1 \mod q$). Sea b tal que $b \equiv b_1 \mod p$ y $b \equiv b_2 \mod q$, la existencia de b la garantiza el Teorema Chino del Residuo, entonces

$$b^{t_n} \equiv 1 \mod p \text{ y } b^{t_n} \equiv 1 \mod q$$

luego $b^{t_n} \equiv 1 \mod n$ y $n \in Spf(b)$. Por lo tanto, en este caso n es seudoprimo fuerte para t^2 bases b.

Si ocurre la condición (2), entonces

$$b^{t_n} \equiv -1 \mod n \text{ ó } b^{2t_n} \equiv -1 \mod n \text{ ó } \ldots \text{ ó } b^{2^{(s_n-1)}t_n} \equiv -1 \mod n$$

Si $b^{t_n} \equiv -1 \mod n$ entonces $b^{2t_n} \equiv 1 \mod n$, así que $b^{2t_n} \equiv 1 \mod p$ y $b^{2t_n} \equiv 1 \mod q$. Elementos b tales que $b^{2t_n} \equiv 1 \mod p$ hay

$$(2t_n, p-1) = (2t_n, 2^{s_p}t_p) = 2(t_n, t_p) = 2t$$

de estos elementos deben eliminarse los t elementos para los cuales $b^{t_n} \equiv 1 \mod p$, así sólo hay t elementos b tales que $b^{t_n} \equiv -1 \mod p$. Similarmente hay t elementos b tales que $b^{t_n} \equiv -1 \mod q$. Utilizando nuevamente el Teorema Chino del Residuo, se prueba que hay t^2 elementos b, tales que $b^{t_n} \equiv -1 \mod n$.

Si $b^{2t_n} \equiv -1 \mod n$ entonces $b^{2^2t_n} \equiv 1 \mod n$ y por tanto $b^{2^2t_n} \equiv 1 \mod p$ y $b^{2^2t_n} \equiv 1 \mod q$. Así, elementos b tales que $b^{2^2t_n} \equiv 1 \mod p$ hay

$$(2^2t_n, p-1) = (2^2t_n, 2^{s_p}t_p) = 2^2t.$$

De estos 2^2t elementos hay que eliminar los $2t$ elementos b para los cuales $b^{2t_n} \equiv 1 \mod p$, quedan $2t$ (ó ninguno según que $s_p > 1$ o $s_p = 1$), elementos b tales que $b^{2^2t_n} \equiv -1 \mod p$, similarmente hay $2t$ (ó ninguno según que $s_q > 1$ o $s_q = 1$) elementos b tales que $b^{2^2t_n} \equiv -1 \mod q$. Obsérvese la incidencia de $s = mins_p, s_q$. Por lo tanto, hay $(2t)^2$ (o ninguna) bases b tales que $b^{2^2t_n} \equiv -1 \mod n$. Continuando así, se tiene que el número de bases b para las que n es seudoprimo fuerte es

$$t^2 + t^2 + 4t^2 + 4^2t^2 + \cdots + 4^{s-1}t^2.$$

El número total de bases es

$$(1 + (1 + 4 + 4^2 + \cdots + 4^{s-1}))t^2$$

o sea

$$\left(1 + \frac{4^s - 1}{4 - 1}\right) t^2.$$

De la discusión previa se tiene el siguiente resultado.

Lema 39. *Sea $n = pq$, con $p = 2^{s_p}t_p + 1$ y $q = 2^{s_q}t_q + 1$ primos impares distintos y t_p, t_q impares, sean además $t = (t_p, t_q)$ y $s = min\{s_p, s_q\}$, entonces n seudoprimo fuerte para*

$$\left(1 + \frac{4^h - 1}{3}\right) t^2$$

bases b en $\mathbb{U}_n$.

El resultado anterior se puede generalizar en la siguiente forma, se omite la prueba del mismo, pues se consigue haciendo un razonamiento similar al del Lema en cuestión.

Teorema 40. *Sean $n = p_1^{a_1}p_2^{a_2}\ldots p_w^{a_w}$ un entero impar, donde $p_1 = 2^{s_{p_1}}t_{p_1}+1$, $p_2 = 2^{s_{p_2}}t_{p_2}+1$, $\ldots$, $p_w = 2^{s_{p_w}}t_{p_w} + 1$, con t_{p_i} impar para cada $i = 1, \ldots, w$ son primos impares distintos,*

sea además $T_{p_i} = (t_n, t_{p_i})$ *y* $s = \min\{s_{p_1}, s_{p_2}, \ldots, s_{p_w}\}$, *entonces la cantidad de bases de seudoprimalidad fuerte de* n *es*

$$\left(1 + \frac{2^{sw} - 1}{s^w - 1}\right) \prod_{i=1}^{w} T_{p_i},$$

es decir

$$|Bspf(n)| = \left(1 + \frac{2^{sw} - 1}{s^w - 1}\right) \prod_{i=1}^{w} T_{p_i}$$

Ejemplo 41. Como $221 = 13 \times 17$, en este caso: $p - 1 = 12 = 3 \times 4$, $q - 1 = 16 = 2^4$, $t = (3, 1) = 1$, $s = min\{2, 4\} = 2$, entonces

$$|Bspf(221)| = 1 + \left(\frac{4^2 - 1}{3}\right) = 6.$$

Teorema 42 (Rabín, 1980)**.** *Sea* n *un número entero impar, entonces*

$$\frac{|Bspf(n)|}{n-1} \leq \frac{1}{4}.$$

Demostración. Para la prueba se distinguen tres casos de acuerdo a la factorización de n, así:

Caso 1. n no es libre de cuadrados. Existe p número primo divisor de n tal que p^2 divide a n. Suponga que n es seudoprimo fuerte base a, por lo tanto también se cumple $a^{n-1} \equiv 1 \mod n$, además dado que $p^2 \mid n$, entonces $a^{n-1} \equiv 1 \mod p^2$ y esta congruencia tiene $(n-1, p(p-1)) = d$ soluciones, como $p \nmid n-1$ entonces $d = (n-1, p-1)$, así las cosas:

$$\begin{aligned} \frac{|Bspf(n)|}{n-1} &< \frac{d}{n-1} \\ &< \frac{p-1}{n-1} \\ &< \frac{p-1}{p^2-1} \\ &< \frac{1}{p+1} < \frac{1}{4} \end{aligned} \tag{3.2}$$

Caso 2. n libre de cuadrados. Esto es, $n = p_1 p_2 \cdots p_w$ donde $p_i \neq p_j$ para $i \neq j$. En primera instancia se supone que $n = pq$ y n es seudoprimo fuerte base a

$$\begin{aligned}
\frac{|Bspf(n)|}{n-1} &\leq \frac{|Bspf(n)|}{\phi(n)} \\
&= \frac{\left(1+\left(\frac{4^s-1}{3}\right)\right)t^2}{\phi(p)\phi(q)} \\
&= \frac{\left(1+\frac{2^{2s}-1}{3}\right)(t_p,t_q)^2}{(p-1)(q-1)} \\
&= \frac{\left(1+\frac{2^{2s}-1}{3}\right)(t_p,t_q)^2}{(2^{s_p}t_p)(2^{s_q}t_q)} \qquad \text{dado que } (t_p,t_q) \leq t_p \\
&\leq \frac{1+\frac{2^{2s}-1}{3}}{2^{s_p}2^{s_q}}.
\end{aligned} \tag{3.3}$$

Sin perdida de generalidad se supone que $s = s_p = min\{s_p, s_q\} < s_q$, por lo tanto

$$\begin{aligned}
\frac{1+\frac{2^{2s}-1}{3}}{2^{s_p}2^{s_q}} &\leq \frac{1+\frac{2^{2s}-1}{3}}{2^{2s_p+1}} \\
&= \frac{2+2^{2s}}{2^{2s+1}} \\
&= \frac{1}{2^{2s}} + \frac{1}{2} \\
&\leq \frac{1}{2} + \frac{1}{2} \\
&= \frac{1}{4}.
\end{aligned}$$

Ahora se supone que $s_p = s_q$ y que $p < q$, entonces $(n-1, t_p) = (n-1, t_q) = (t_p, t_q)$, además $t_p \neq t_q$ ya que $p \neq q$.

Por lo tanto, dado que $(t_p, t_q) \mid t_p$, entonces $t_p = k(t_p, t_q)$ pero como t_p es impar se tiene que $3(t_p, t_q) \leq t_q$, así:

$$\begin{aligned}
|Bspf(n)| &\leq \frac{1+\dfrac{2^{2s}-1}{3}}{2^{2s}t_pt_q}3^{-1}t_pt_q \\
&= \frac{\dfrac{1}{3}+\dfrac{2^{2s}-1}{9}}{2^{2s}} \\
&= 2^{-2s}\left(\frac{2^{2s}+2}{9}\right) \\
&= \frac{1}{9}\left(1+\frac{2}{2^{2s-1}}\right) \\
&\leq \frac{1}{9}\left(1+\frac{1}{2}\right) \\
&\leq \frac{1}{4}.
\end{aligned}$$

Por lo anterior se concluye que

$$\frac{|Bspf(n)|}{n-1} \leq \frac{1}{4}.$$

Caso 3. Si $n = \prod_{i=1}^{w} p_i$, $w > 2$ con todos los p_i son distintos, sea $p_i - 1 = 2^{s_{p_i}}t_{p_i}$ y suponga que $s_1 \leq s_i$ para todo $i = 1, \ldots, w$

$$\begin{aligned}
\frac{|Bspf(n)|}{n-1} &\leq \frac{|Bspf(n)|}{\phi(n)} \\
&= \frac{\left(1+\dfrac{2^{sw}-1}{2^w-1}\right)\displaystyle\prod_{i=1}^{w}(n-1,t_i)}{\phi(n)} \\
&= \frac{\left(1+\dfrac{2^{sw}-1}{2^w-1}\right)\displaystyle\prod_{i=1}^{w}(n-1,t_i)}{\displaystyle\prod_{i=1}^{w}2^{s_i}\prod_{i=1}^{w}t_i} \\
&\leq \frac{\left(1+\dfrac{2^{sw}-1}{2^w-1}\right)}{2^{sw}} \\
&\leq \frac{1}{2^{w-1}} \\
&\leq \frac{1}{4}.
\end{aligned}$$

Por lo tanto, para todo $n \in \mathbb{Z}$ se tiene

$$\frac{|Bspf(n)|}{n-1} \leq \frac{1}{4}.$$

□

El Teorema anterior, permite desarrollar un test probabilístico de primalidad, llamado *Test de Miller-Rabin.*

Terminamos este capítulo presentando una caracterización de los seudoprimos fuertes, la cual será generalizada en el siguiente capítulo.

Teorema 43. *Un entero compuesto impar n es seudoprimo fuerte base a si, y sólo si, n es seudoprimo base a y existe un entero no negativo k tal que para todo primo p divisor de n se cumple $\nu_2(|a|_{p^{\nu_p(n)}}) = \nu_2(|a|_p) = k$.*

Demostración. Suponga que $n = 2^s t + 1$, $a \in Bsp(n)$ y que existe un entero k tal que $\nu_2(|a|_{p^{\nu_p(n)}}) = \nu_2(|a|_p) = k$ para un primo p divisor de n, considere dos casos para k: Si $k = 0$ entonces $|a|_n$ es impar, además dado que $a^{n-1} \equiv 1 \mod n$ entonces $a^t \equiv 1 \mod n$, por lo tanto $a \in Bspf(n)$. Si $k > 0$, entonces $|a|_{p^{\nu_p(n)}} = 2^k s_p$, es decir, $a^{2^k s_p}$ satisface la ecuación $x^2 \equiv 1 \mod p^{\nu_p(n)}$, ésta tiene dos soluciones en $\mathbb{U}_{p^{\nu_p(n)}}$, por lo tanto $a^{2^{k-1} s_p} \equiv -1$ mód $p^{\nu_p(n)}$ para todo primo p divisor de n, esto es, $a^{2^{k-1} s_p} \equiv -1 \mod n$ así se concluye que $a \in Bspf(n)$.

Recíprocamente, si $a \in Bspf(n)$ se tiene que $a \in Bsp(n)$ entonces existe i tal que $a^{2^i t} \equiv -1 \mod n$ ó $a^t \equiv 1 \mod n$. Si se cumple la segunda congruencia se tiene que para todo primo p divisor de n se cumple $|a|_{p^{\nu_p(n)}}$ divide a t luego $k = 0$. Si se cumple la primera congruencia se tiene $\nu_2(|a|_{p^{\nu_p(n)}}) = i + 1$. □

Capítulo 4

q-seudoprimos vs ω-Primos

En este capítulo se hace la presentación de los números q-seudoprimos definidos por Castillo, García y Velásquez en [3], y de los ω-primos definidos por Berrizbeitia y Berry en [1], se hará una comparación entre dichos conceptos mostrando las ventajas de los q-seudoprimos sobre los w-primos.

4.1. q-Seudoprimos

La caracterización de la seudoprimalidad fuerte presentada en el Teorema 43, expone que un número n es seudoprimo fuerte base a si y sólo si el exponente con que aparece 2 en el orden de a módulo p, es constante para todo primo p divisor de n. Este hecho sugiere la siguiente generalización de la seudoprimalidad fuerte.

Definición 44. Sean $n > 1$, a enteros con $(n, a) = 1$ con $a^{n-1} \equiv 1 \mod n$ y sea q un primo tal que para todo p divisor de n, q divide a $p - 1$. Se dice que n es q-seudoprimo base a, si n es compuesto y existe un entero no negativo k tal que para todo primo p divisor de n, se cumple que $\nu_q(|a|_p) = k$.

Ejemplo 45. Sea $n = 1891 = 31 \times 61$, entonces $n - 1 = 1890 = 2 \times 3^3 \times 5 \times 7$, se tiene:

- (i) $\nu_2(|3|_{31}) = 1 \qquad \nu_2(|3|_{61}) = 1 \quad$ 1891 es 2-seudoprimo base 3 .
- (ii) $\nu_3(|3|_{31}) = 1 \quad \nu_3(|3|_{61}) = 0 \quad$ 1891 no es 3-seudoprimo base 3.
- (iii) $\nu_5(|3|_{31}) = 1 \qquad \nu_5(|3|_{61}) = 1 \quad$ 1891 es 5-seudoprimo base 3.
- (iv) $\nu_7(|3|_{31}) = 0 \qquad \nu_7(|3|_{61}) = 0 \quad$ 1891 es 7-seudoprimo base 3.

A continuación se presentan los polinomios ciclotómicos y algunas de sus propiedades con el fin de dar una caracterización a la q-seudoprimalidad.

Definición 46. Sean K un campo, p un número primo y n un entero positivo primo relativo con p, y ξ una raíz n-ésima primitiva de la unidad sobre K, entonces el polinomio

$$\Phi_n(x) = \prod_{\substack{s=1 \\ (n,s)=1}}^{n} (x - \xi^s), \tag{4.1}$$

es llamado el n-ésimo polinomio ciclotómico sobre K.

De la definición de polinomio ciclotómico se ve que el grado de $\Phi_n(x)$ es justamente $\phi(n)$.

Teorema 47. *Sea K un campo de característica p y n un entero positivo primo relativo con p. Entonces*

i) $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

ii) Los coeficientes de $\Phi_n(x)$ están en el subcampo primo de K.

El siguiente teorema y corolario se pueden encontrar en [8] y son herramientas fundamentales para la caracterización de la q-seudoprimalidad.

Teorema 48. *Sean m, $b \geq 2$, $n \geq 3$ enteros y p el mayor primo divisor de n. El entero m es divisor de $\Phi_n(b)$ si, y sólo si $b^n \equiv 1 \mod m$ y para todo primo q divisor de m y distinto de p se tiene $|b|_q = n$. Es más, si p divide a m entonces $n = p^e|b|_p$ con $e > 1$.*

Corolario 49. *Sean n, $a \geq 2$ enteros y q un número primo, entonces n es divisor de la evaluación del polinomio ciclotómico $\Phi_q(a)$ si, y sólo si para todo primo p divisor de n, se tiene $|a|_p = q$.*

Ejemplo 50. Por Teorema 47 para un número primo p, se tiene que,

$$\Phi_p(x) = 1 + x + x^2 + x^3 + \cdots + x^{p-1}$$

por lo tanto para una potencia de un número primo, p^r, se obtiene que,

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{\Phi_1(x)\Phi_p(x)\cdots\Phi_{p^{r-1}}(x)} = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1}$$

Con lo descrito anteriormente, se está en condiciones de enunciar y demostrar el teorema que caracteriza los números q-seudoprimos.

Teorema 51. *Sean n un entero compuesto impar, a un entero positivo primo relativo con n y q un divisor primo de $n-1$. Sea $n - 1 = q^s t$ con $(q, t) = 1$, entonces n es q-seudoprimo base a si, y sólo si se cumple una de las siguientes condiciones.*

i) Todo divisor primo de n es congruente con 1 módulo q y $a^t \equiv 1 \mod n$.

ii) Existe i con $0 \leq i \leq s-1$ tal que $n \mid \Phi_q(a^{q^i t})$.

Demostración. Suponga que $n-1 = q^s t$ con $(q,t) = 1$, todo divisor primo de n es congruente con 1 módulo q y $a^t \equiv 1 \mod n$. Dado que p es un divisor de n, entonces $a^t \equiv 1 \mod p$, por lo tanto $\nu_q(|a|_p) = 0$ para todo primo p divisor de n y así n es q-seudoprimo base a.

Por otra parte, si existe i con $0 \leq i \leq s-1$ tal que n divide a $\Phi_q(a^{q^i t})$ entonces por el Corolario 49 se tiene $|a^{q^i t}|_p = q$ para cualquier primo p divisor de n, por lo tanto $\nu_q(|a|_p) = i+1$, en consecuencia n es q-seudoprimo base a.

Recíprocamente, suponga que $n = q^s t + 1$ es q-seudoprimo base a, por lo tanto, $a^{n-1} \equiv 1$ mód n y para p divisor de n y q divisor de $p-1$ se tiene $\nu_q(|a|_p) = k$ donde k es una constante.

- Si $k = 0$, entonces $\nu_q(|a|_p) = 0$, lo cual quiere decir que $|a|_p$ es un divisor de t así, $a^t \equiv 1 \mod p$ y por lo tanto se tiene $a^t \equiv 1 \mod n$.
- Si $k \geq 1$, entonces $\nu_q(|a|_p) = k$ se tiene que $|a|_p = q^k t_1$ para algún t_1 divisor de t y por lo tanto $a^{q^k t} \equiv 1 \mod p$ y $a^{q^{k-1} t} \not\equiv 1 \mod p$ para todo primo p divisor de n, en consecuencia $|a^{q^{k-1} t}|_p = q$ y del Corolario 49 se tiene que n divide a $\Phi_q(a^{q^{k-1} t})$.

□

Ejemplo 52. Para $n = 341$, cuántas y cuáles son las bases de q-seudoprimalidad?

Se tiene que $340 = 5 \times 68$, tomemos $q = 5$, $t = 68$ y $s = 1$.

La primera condición de la caracterización de 5−seudoprimalidad da como bases a los enteros primos relativos con 341 que satisfacen la congruencia $x^{68} \equiv 1 \mod 341$ y estos son $\{1, 32, 309, 340\}$.

La segunda condición del Teorema 51 da como bases de 5-seudoprimalidad a todos aquellos enteros a menores o iguales y primos relativos a 341 que satisfacen la congruencia $\Phi_5(a^{68}) \equiv 0 \mod 341$, para obtener todas las bases, el seudocódigo que se utilizó en MUPAD fue:

```
bqs:=proc(n,q,a)
local b,h;
begin
s:=nu(n-1,q); t:=(n-1)/q^s;
if is(_mod(a^t,n) =1 ) then return(a); end_if;
 for i from 0 to s-1 do
   if is(_mod(polylib::cyclotomic(q, z)(a^(t*q^i)),n) =0) then
     return(a);
   end_if;
 end_for;
return(0)
end_proc
```

y los valores arrojados fueron:

$B = \{1, 2, 4, 8, 15, 16, 23, 27, 29, 30, 32, 35, 39, 46, 47, 54, 58, 60, 61, 63, 64, 70, 78, 85, 89, 91, 92, 94, 95, 97, 101, 108, 109, 116, 120, 122, 123, 125, 126, 128, 139, 140, 147, 151, 153, 156, 157, 159, 163, 170, 171, 178, 182, 184, 185, 188, 190, 194, 201, 202, 213, 215, 216, 218, 219, 221, 225, 232, 233, 240, 244, 246, 247, 249, 250, 252, 256, 263, 271, 277, 278, 280, 281, 283, 287, 294, 295, 302, 306, 309, 311, 312, 314, 318, 325, 326, 333, 337, 339, 340\}$

Por lo tanto, para $n = 341$ existen 68 bases de 5-seudoprimalidad.

Al igual que en la seudoprimalidad de Fermat y la seudoprimalidad fuerte, surge la inquietud por el cardinal de las bases de q-seudoprimalidad, esto es, fijando un n y un q, cuántas bases hacen posible que n sea q-seudoprimo. El siguiente teorema da respuesta a esta inquietud:

Teorema 53. *Sean* $n = \prod_{i=1}^{w} p_i$, *v el exponente con que aparece q en el máximo común divisor de los $p_i - 1$ para $1 \leq i \leq w$, y sea $n - 1 = q^s t$, donde q no divide a t, entonces la cantidad de bases de q-seudoprimalidad para n es:*

$$\prod_{i=1}^{w} (t, p_i - 1) \left(1 + (q-1)^w \left(\frac{q^{wv} - 1}{q^w - 1}\right)\right).$$

Demostración. Para contar las bases de q-seudoprimalidad de n, por el Teorema 51 se tiene que n es q-seudoprimo base a si cumple cualquiera de las siguientes condiciones:

i) $a^t \equiv 1 \mod n$.

ii) Existe i donde $0 \leq i \leq s-1$ tal que n divide a $\Phi_q(a^{q^i t})$

por lo tanto, contar las bases de q-seudoprimalidad para n es contar la cantidad de soluciones de *i)* y *ii)*

Para *i)* la cantidad de soluciones de $a^t \equiv 1 \mod n$, por el Teorema 12 son $\prod_{i=1}^{w} (t, p_i - 1)$.

Para *ii)* se deben encontrar cuantos a satisfacen que n divida a $\Phi_q(a^{q^i t})$ para $0 \leq i \leq s-1$. Del hecho que $\Phi_q(x) = \dfrac{x^q - 1}{x - 1}$ y $(a^{q^i t} - 1, n) = 1$, la condición *ii)* se puede reescribir de la siguiente manera: existe i con $0 \leq i \leq s-1$ tal que $a^{q^{i+1} t} \equiv 1 \mod n$.

Sea $n = p^\alpha b$, se debe contar la cantidad de soluciones de la congruencia $a^{q^{i+1} t} \equiv 1 \mod p^\alpha$, pero no de $a^{q^i t} \equiv 1 \mod p^\alpha$. Por el Teorema 12, la cantidad de soluciones es:

$$\begin{aligned} (q^{i+1} t, \phi(p^\alpha)) - (q^i t, \phi(p^\alpha)) &= q^{i+1} (t, p-1) - q^i (t, p-1) \\ &= q^i (q-1) (t, p-1), \end{aligned}$$

esto es, para todo primo p divisor de n, se tiene que la cantidad de soluciones en este caso es:

$$q^{iw}(q-1)^w \prod_{p|n}(t, p-1).$$

Así, en total, la cantidad de bases de q-seudoprimalidad es:

$$\prod_{i=1}^{w}(t, p_i - 1)\left(1 + (q-1)^w + q^w(q-1)^w + q^{2w}(q-1)^w + \cdots + q^{(v-1)w}(q-1)^w\right)$$

factorizando se obtiene:

$$\prod_{i=1}^{w}(t, p_i - 1)\left(1 + (q-1)^w\left(\frac{q^{vw}-1}{q^w-1}\right)\right).$$

□

Ejemplo 54. Para $n = 79381 = 163 \times 487$ con $q = 3$ se tiene que $n - 1 = 3^4 \times 980$, así, $s = 4$, $t = 980$. $x = (980, 162) \times (980, 486) = 2 \times 2 = 4$ y dado que $(162, 486) = 162 = 2 \times 3^4$, entonces $\nu = 4$. Por el Teorema anterior se tiene que 79381 tiene

$$\begin{aligned} x\left[1 + (q-1)^w\left(\frac{q^{\nu w}-1}{q^w-1}\right)\right] &= 4\left[1 + 2^2\left(\frac{3^8-1}{3^2-1}\right)\right] \\ &= 4(3271) \\ &= 13084 \end{aligned}$$

bases de 3-seudoprimalidad.

4.2. ω-primos

Las definiciones y algunos de los teoremas presentados en esta parte son tomados del artículo [1]. En primer lugar se hacen las considereciones pertinentes para definir el concepto de ω-primo.

Sean $n = \prod_{i=1}^{k} p_i$ la descomposición en factores primos distintos de n, q un número primo divisor de $p_i - 1$ para todo $i = 1, \ldots, k$, $r = q^e$ para e un número entero mayor o igual a 1 y ω un entero de orden r módulo n. Se define el siguiente conjunto:

$$A_r = \{n \in \mathbb{Z} : \ n = p_1 p_2 \cdots p_k \text{ tal que } p_i \equiv 1 \mod r \text{ para } 1 \leq i \leq k\}.$$

La definición de ω-primo dada por Pedro Berrizbeitia y T.G.Berry es la siguiente:

Definición 55. Para $n \in A_r$, sea $n - 1 = q^s t$ donde t no divide a q. Sea $a \in \mathbb{N}$. Decimos que n es ω-primo base a si cumple alguna de las siguientes condiciones:

$$\exists h \in \mathbb{Z} \text{ tal que } a^t \equiv \omega^{qh} \mod n \tag{4.2}$$

ó

$$\exists i, j, (q, j) = 1,\ 0 \leq i \leq s - e,\ 1 \leq j \leq r - 1 \text{ tal que } a^{q^i t} \equiv \omega^j \mod n. \tag{4.3}$$

El objetivo del artículo de Berrizbeitia y Berry [1], es dar una generalización de test de Miller-Rabin para los números ω-primos, con esta idea, la siguiente definición permite dar formalismo a este hecho.

Definición 56. Sea $A \subseteq \mathbb{N}$. Un test elemental probabilístico de primalidad para un entero n en A, denotado (T, A), es una colección $T = \{T_n \ : \ n \in A\}$ de conjuntos con las siguientes propiedades:

1. $T_n \subset \mathbb{Z}_n^*$, para todo n en A.
2. Si $n \in A$ es primo, entonces $T_n = \mathbb{Z}_n^*$.
3. Si $n \in A$, $a \in \mathbb{Z}_n^*$, entonces saber si $a \in T_n$ se puede decidir en tiempo polinomial.

Ejemplo 57. En este ejemplo sea a un entero.

1. El test de Fermat: $(F, \mathbb{N})$ donde
$$F_n = \left\{a \in \mathbb{Z}_n^* \ : \ a^{n-1} \equiv 1 \mod n\right\}.$$
2. El test del r-ésimo orden: $(T(\omega), A_r)$ donde
$$T_n(\omega) = \left\{a \in \mathbb{Z}_n^* \ : \ n \text{ es } \omega\text{-primo base } a\right\}.$$

Observación. Del ejemplo anterior note que $(T(-1), A_2)$ es el test de seudoprimalidad fuerte y $(T(1), \mathbb{N})$ es el test de primalidad de Fermat. Para ambos test hay algoritmos eficientes que permiten saber si un número entero a está en T_n. El análisis del costo computacional no hace parte de nuestro interés para esté trabajo, no obstante el lector interesado puede consultar el texto de Crandall y Pomerance [4] para ver los detalles en ese sentido.

Sean $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ la descomposición en factores primos distintos de n y $n - 1 = q^s t$. Sea $K_m := \{c \in \mathbb{Z}_n^* \ : \ c^m \equiv 1 \mod n\}$ el Kernel de la función m-ésima potencia en $\mathbb{Z}_n^*$. Con esta notación se tiene que $F_n = K_{n-1} = K_t \times K_{q^s}$. Se define un subconjunto B_r de K_{q^s} como:

$$B_r = \{\beta \in K_{q^s} : \ \exists h \text{ tal que } \beta \equiv \omega^{qh} \mod n \qquad \text{ó}$$

$$\exists i, j, (q, j) = 1, 0 \leq i \leq s - e, 1 \leq j \leq r - 1 : \ \beta^{q^i} \equiv \omega^j \mod n\}. \tag{4.4}$$

Con el mismos objetivo inicial, la generalización del test de Miller-Rabin, Berrizbeitia presenta los siguientes lemas.

Lema 58. *Con la notación introducida anteriormente, se tiene:*

$$T_n(\omega) \cong K_t \times B_r.$$

Para cada p_i, sea f_i el exponente de la mayor potencia de q que divide a $p_i - 1$, ya que $n \in A_r$, entonces $f_i \geq e$. Sea $e' = min\{f_i\}$ para $i = 1, \ldots, k$.

Lema 59.

$$|B_r| = q^{e-1} + (q-1)q^{e-1}\left(1 + q^k + q^{2k} + \cdots + q^{(e'-e)k}\right)$$

El siguiente Teorema es la generalización del Test de Miller Rabin para los números ω-primos.

Proposición 60. *Sea $n = \prod_{i=1}^{k} p_i^{\alpha^i}$ la descomposición en factores primos de n, sea q un número primo divisor de todos los $p_i - 1$ para $i = 1, \ldots k$. Con la notación introducida se tiene:*

$$\frac{|T_n(\omega)|}{|F_n|} \leq \frac{1}{r^{k-1}}.$$

Así, la probabilidad de escoger una base de ω-primalidad para un número n entre las posibles bases de seudoprimalidad de Fermat es menor o igual a $\frac{1}{r^{k-1}}$. Dado que $q \geq 2$, $k > 1$ y $r = q^e$ con $e \geq 1$, entonces $\frac{1}{r^{k-1}} \leq \frac{1}{4}$, lo que hace la ω-primalidad una mejora al concepto de seudoprimo fuerte.

En lo que sigue se considera $e = 1$, esto hace que $r = q$ y ω sea una raíz q-ésima de la unidad módulo n.

Por lo tanto, la condición (4.2) de la definición de ω-primalidad se convierte en

$$a^t \equiv 1 \mod n$$

El siguiente lema con las condiciones anteriores, demuestra que ser un número q-seudoprimo implica ser ω-primo.

Lema 61. *Sean n un número entero con $n - 1 = q^s t$ y $a \in \mathbb{Z}$ tal que $(a, n) = 1$. Si n es q-seudoprimo base a, entonces n es ω-primo base a.*

Demostración. Sean $n - 1 = q^s t$ donde $(q, t) = 1$, $a \in \mathbb{Z}$ con $(a, n) = 1$. Suponga que n es $q-$seudoprimo base a, así por el Teorema 51 se tiene que $a^t \equiv 1 \mod n$, dado que $\omega^q \equiv 1$ mód n entonces con $h = 1$ se tiene que

$$a^t \equiv \omega^{qh} \mod n.$$

Suponga ahora, que existe i con $0 \leq i < s$ tal que $\Phi_q(a^{q^i t}) \equiv 0 \mod n$, esto implia que $a^{q^{i+1}t} \equiv 1 \mod n$, equivalentemente,

$$(a^{q^i t})^q \equiv 1 \mod n$$

así, $a^{q^i t}$ es una raíz q-ésima de la unidad módulo n, si se define a ω como $a^{q^i t}$, entonces para $0 \leq j < q$ se cumple $a^{q^i t} \equiv \omega^j \mod n$. □

La pregunta que surge es: ¿el recíproco del lema anterior es cierto?, es decir, ¿las definiciones de $\omega-$primo y q-seudoprimalidad son equivalentes? El siguiente ejemplo permite dar una respuesta parcial de lo que sucede.

Ejemplo 62. Para $n = 341$, cuántas y cuáles son las bases de ω-primalidad?

En este caso $n - 1 = 340 = 5 \times 68$ y se tiene $t = 68$, $r = q = 5$. .

Los posibles valores para a son aquellos valores que son primos relativos con 341.

Para encontrar a ω se buscan las soluciones de la congruencia $x^5 \equiv 1 \mod 341$ excepto $\omega = 1$. Haciendo uso del paquete de MUPAD estos son los seudocódigos:

```
wprimo:=proc(n,w,q,e,a)
local b,h;
begin
if igcd(a,n)>1 then return(a, "no es admisible"); end_if;
if powermod(w,q^e,n)<> 1 then return(w ,"no es admisible"); end_if;
s:=nu(n-1,q); t:=(n-1)/q^s; r:=q^e;
H:={h $ h=0..q^(e-1)-1};
Wqh:={_mod(w^(q*h),n) $ h in H };
if is(_mod(a^t,n) in Wqh) then return(a); end_if;
Wqj:={_mod(w^j,n) $ j in {j $ j=1..r-1} };
for i from 0 to s-e do
  if is(_mod(a^(t*q^i),n) in Wqj) then return(a); end_if;
 end_for;
 return(0)
end_proc
```

```
wprimo2:=proc(n,w,q,e,a)
/* Decide si n es w-primo base a.*/
local b,h;
begin
if igcd(a,n)>1 then return(a, "no es admisible"); end_if;
if powermod(w,q^e,n)<> 1 then return(w ,"no es admisible"); end_if;
s:=nu(n-1,q); t:=(n-1)/q^s; r:=q^e;
if is(_mod(a^t,n) =1 ) then return(a); end_if;
for i from 0 to s do
```

```
  if is(_mod(a^(t*q^i),n) =1) then return(a); end_if;
 end_for
end_proc
```

Los resultados arrojados son:

$W = \{4, 16, 47, 64, 70, 78, 97, 125, 126, 157, 159, 163, 188, 190, 202, 218, 221, 225, 256, 280, 287, 295, 311, 312\}$.

Por la primera condición de ω-primalidad, para cada ω los posibles valores de a son aquellos que satisfacen la congruencia $x^{68} \equiv 1 \mod 341$, así se tiene que $a \in \{1, 32, 309, 340\}$.

Para la segunda condición, las bases de ω-primalidad deben satisfacer la congruencia $x^{68} \equiv \omega^j \mod 341$, para $j = 1, 2, 3, 4$. Se tiene la siguiente lista:

ω	a
4	1, 2, 4, 8, 16, 32, 64, 85, 128, 170, 171, 213, 256, 277, 309, 325, 333, 337, 339, 340
16	1, 2, 4, 8, 16, 32, 64, 85, 128, 170, 171, 213, 256, 277, 309, 325, 333, 337, 339, 340
47	1, 27, 29, 32, 47, 95, 101, 140, 159, 163, 178, 182, 201, 240, 246, 294, 309, 312, 314, 340
64	1, 2, 4, 8, 16, 32, 64, 85, 128, 170, 171, 213, 256, 277, 309, 325, 333, 337, 339, 340
70	1, 32, 46, 58, 60, 70, 108, 126, 147, 151, 190, 194, 215, 233, 271, 281, 283, 295, 309, 340
78	1, 23, 32, 54, 78, 89, 109, 120, 122, 153, 188, 219, 221, 232, 252, 263, 287, 309, 318, 340
97	1, 15, 32, 35, 39, 91, 97, 116, 139, 157, 184, 202, 225, 244, 250, 302, 306, 309, 326, 340
125	1, 30, 32, 61, 63, 92, 94, 123, 125, 156, 185, 216, 218, 247, 249, 278, 280, 309, 311, 340
126	1, 32, 46, 58, 60, 70, 108, 126, 147, 151, 190, 194, 215, 233, 271, 281, 283, 295, 309, 340
157	1, 15, 32, 35, 39, 91, 97, 116, 139, 157, 184, 202, 225, 244, 250, 302, 306, 309, 326, 340
159	1, 27, 29, 32, 47, 95, 101, 140, 159, 163, 178, 182, 201, 240, 246, 294, 309, 312, 314, 340
163	1, 27, 29, 32, 47, 95, 101, 140, 159, 163, 178, 182, 201, 240, 246, 294, 309, 312, 314, 340
188	1, 23, 32, 54, 78, 89, 109, 120, 122, 153, 188, 219, 221, 232, 252, 263, 287, 309, 318, 340
190	1, 32, 46, 58, 60, 70, 108, 126, 147, 151, 190, 194, 215, 233, 271, 281, 283, 295, 309, 340
202	1, 15, 32, 35, 39, 91, 97, 116, 139, 157, 184, 202, 225, 244, 250, 302, 306, 309, 326, 340
218	1, 30, 32, 61, 63, 92, 94, 123, 125, 156, 185, 216, 218, 247, 249, 278, 280, 309, 311, 340
221	1, 23, 32, 54, 78, 89, 109, 120, 122, 153, 188, 219, 221, 232, 252, 263, 287, 309, 318, 340
225	1, 15, 32, 35, 39, 91, 97, 116, 139, 157, 184, 202, 225, 244, 250, 302, 306, 309, 326, 340
256	1, 2, 4, 8, 16, 32, 64, 85, 128, 170, 171, 213, 256, 277, 309, 325, 333, 337, 339, 340
280	1, 30, 32, 61, 63, 92, 94, 123, 125, 156, 185, 216, 218, 247, 249, 278, 280, 309, 311, 340
287	1, 23, 32, 54, 78, 89, 109, 120, 122, 153, 188, 219, 221, 232, 252, 263, 287, 309, 318, 340
295	1, 32, 46, 58, 60, 70, 108, 126, 147, 151, 190, 194, 215, 233, 271, 281, 283, 295, 309, 340
311	1, 30, 32, 61, 63, 92, 94, 123, 125, 156, 185, 216, 218, 247, 249, 278, 280, 309, 311, 340
312	1, 27, 29, 32, 47, 95, 101, 140, 159, 163, 178, 182, 201, 240, 246, 294, 309,312, 314, 340

De lo anterior, se tiene que el conjunto de todas las bases de ω-primalidad para todos los posibles ω es:

$B = \{1, 2, 4, 8, 15, 16, 23, 27, 29, 30, 32, 35, 39, 46, 47, 54, 58, 60, 61, 63, 64, 70, 78, 85, 89, 91, 92, 94, 95, 97, 101, 108, 109, 116, 120, 122, 123, 125, 126, 128, 139, 140, 147, 151, 153, 156, 157, 159, 163, 170, 171, 178, 182, 184, 185, 188, 190, 194, 201, 202, 213, 215, 216, 218, 219, 221, 225, 232, 233, 240, 244, 246, 247, 249, 250, 252, 256, 263, 271, 277, 278, 280, 281, 283, 287, 294, 295, 302, 306, 309, 311, 312, 314, 318, 325, 326, 333, 337, 339, 340\}$.

Por lo tanto para $n = 341$, existen 100 bases de ω-primalidad para todos los posibles ω.

En el Ejemplo 52 se determinó que para $n = 341$ existen 68 bases de $5-$seudoprimalidad, 32 menos que en el caso de ω-primo cuando $q = 5$. Lo cual demuestra que dichos conceptos son distintos.

Los ejemplos anteriores ilustran el hecho que la cantidad de bases de q-seudoprimalidad son menos que las de ω-primalidad. Esto da pie al resultado principal de este trabajo. En la definición de ω-primo se hace la consideración $e = 1$, con esto se tiene $q = r$, con la notación introducida con anterioridad se tiene en general el siguiente resultado,

Proposición 63. *Para un número n entero, la cantidad de bases de q-seudoprimalidad es menor que la cantidad de bases de ω-primalidad.*

Demostración. Sean $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, q un número primo tal que $n - 1 = q^s t$ donde $q | p_i - 1$ para todo $i = 1, \ldots, k$ y a un número entero, primo relativo con n. Recordando; n es ω-primo base a con ω tal que $w^q \equiv 1 \mod n$, si satisface cualquiera de las condiciones: $i)$ $a^t \equiv 1 \mod n$ ó $ii)$ existe $i = 1, \ldots, s-1$ y $j = 1, \ldots q-1$ con $(j, q) = 1$ tal que $a^{q^i t} \equiv w^j \mod n$. Por otra parte, n es q-seudoprimo base a si satisface cualquiera de las siguientes condiciones: $i)$ $a^t \equiv 1 \mod n$ ó $ii)$ existe $i = 0, \ldots s-1$ tal que $n \mid \Phi_q(a^{q^i t})$.

La primera condición para ambos conceptos es la misma, por lo tanto, si se comparan la cantidad de bases de ω-primalidad con las de q-seudoprimalidad, basta mirar la cantidad de soluciones en las congruencias de las segundas condiciones en cada uno de los conceptos.

Así, para el caso de la ω-primalidad, con la condición $e = 1$, la segunda condición es: existe $i = 0, \ldots s-1$ tal que $a^{q^{i+1} t} \equiv 1 \mod n$. En general, la cantidad de soluciones de $x^q - 1 \equiv 0 \mod n$ es la misma que de $x^q - 1 \equiv 0 \mod \prod_{i=1}^{k} p_i^{\alpha_i}$ y por el Teorema Chino del Residuo es el producto de la cantidad de soluciones de $x^q - 1 \equiv 0 \mod p_i^{\alpha_i}$ para $i = 1, ..., k$. Así por el Teorema 12, la cantidad de soluciones es $(q, p_i^{\alpha_i}(p-1)) = (q, p-1) = q$, por lo tanto la congruencia $x^q - 1 \equiv 0 \mod n$ tiene q^k soluciones.

Para las bases de q-seudoprimalidad, se sabe que $\Phi_q(x) = \dfrac{x^q - 1}{x - 1}$, por lo tanto, la cantidad de soluciones de $\Phi_q(x) \equiv 0 \mod n$ es la misma que la de $x^q - 1 \equiv 0 \mod n$ menos la cantidad de soluciones de $x - 1 = 0 \mod n$. Por lo anterior, la cantidad de soluciones de $x^q - 1 \equiv 0 \mod p_i^{\alpha_i}$ es q, en consecuencia, $\Phi_q(x) \equiv 0 \mod p_i^{\alpha_i}$ tiene $q - 1$ soluciones, por lo tanto $\Phi_q(x) \equiv 0 \mod n$ tiene $(q-1)^k$ soluciones. □

Con la anterior proposición se concluye el concepto de q-seudoprimo es más refinado que el de ω-primo, ya que al tener menos bases, la probabilidad de saber si el número es

compuesto aumenta.

El siguiente ejemplo, cuenta las bases de q-seudoprimalidad y ω-primalidad del número 1729, número de Carmichael.

Ejemplo 64. Sea $n = 1729$, entonces $n - 1 = 1728 = 3^3 \times 64$.

Para contar las bases a, de ω-primalidad sean, $t = 64$, $s = 3$, $e = 1$, $r = q = 3$, los posibles ω son aquellos que satisfacen la congruencia: $\omega^3 \equiv 1 \mod 1729$:

144, 172, 191, 235, 438, 562, 638, 653, 666, 729, 809, 828, 900, 919, 932, 989, 1075, 1166, 1236, 1303, 1394, 1569, 1626, 1654, 1660, 1717

Ahora, la primera condición que deben cumplir las bases de ω-primalidad con las condiciones establacidas para $n = 1729$, es $a^{64} \equiv 1 \mod 1729$, los valores que satisfacen esta congruencia tal que $(a, n) = 1$ son:

$$\{1, 246, 265, 398, 512, 645, 664, 818, 911, 1065, 1084, 1217, 1331, 1464, 1483, 1728\}.$$

Para la segunda condición se debe cumplir que: existe $j = 1, 2$ tal que $a^{64} \equiv \omega^j \mod 1729$, en efecto, si a está en el siguiente conjuto, cumple la congruencia:

{8, 11, 12, 18, 20, 27, 30, 31, 37, 45, 46, 50, 58, 64, 68, 69, 75, 83, 87, 88, 94, 96, 102, 103, 106, 107, 113, 115, 121, 122, 125, 132, 134, 141, 144, 145, 151, 153, 159, 160, 163, 164, 170, 172, 178, 179, 183, 191, 197, 198, 201, 202, 216, 220, 227, 229, 235, 236, 239, 240, 248, 254, 255, 258, 267, 274, 277, 278, 284, 292, 293, 296, 297, 303, 305, 311, 316, 324, 330, 331, 334, 335, 341, 349, 353, 354, 360, 362, 368, 369, 372, 373, 379, 381, 387, 388, 391, 400, 407, 410, 411, 417, 419, 425, 426, 430, 436, 438, 444, 445, 449, 457, 463, 464, 467, 474, 482, 486, 487, 493, 495, 501, 502, 505, 506, 514, 521, 524, 531, 540, 543, 544, 550, 552, 558, 562, 563, 569, 571, 577, 578, 582, 590, 596, 597, 600, 601, 607, 615, 619, 620, 626, 628, 634, 635, 638, 639, 647, 653, 654, 657, 666, 673, 677, 683, 685, 691, 692, 695, 696, 704, 710, 711, 723, 729, 730, 733, 734, 740, 748, 752, 753, 759, 761, 768, 771, 772, 778, 786, 787, 790, 797, 799, 809, 810, 816, 824, 825, 828, 829, 835, 837, 843, 844, 848, 856, 862, 863, 866, 867, 873, 881, 885, 886, 892, 894, 900, 901, 904, 905, 913, 919, 920, 930, 932, 939, 942, 943, 951, 957, 958, 961, 968, 970, 976, 977, 981, 989, 995, 996, 999, 1000, 1006, 1018, 1019, 1025, 1033, 1034, 1037, 1038, 1044, 1046, 1052, 1056, 1063, 1072, 1075, 1076, 1082, 1090, 1091, 1094, 1095, 1101, 1103, 1109, 1110, 1114, 1122, 1128, 1129, 1132, 1133, 1139, 1147, 1151, 1152, 1158, 1160, 1166, 1167, 1171, 1177, 1179, 1185, 1186, 1189, 1198, 1205, 1208, 1215, 1223, 1224, 1227, 1228, 1234, 1236, 1242, 1243, 1247, 1255, 1262, 1265, 1266, 1272, 1280, 1284, 1285, 1291, 1293, 1299, 1303, 1304, 1310, 1312, 1318, 1319, 1322, 1329, 1338, 1341, 1342, 1348, 1350, 1356, 1357, 1360, 1361, 1367, 1369, 1375, 1376, 1380, 1388, 1394, 1395, 1398, 1399, 1405, 1413, 1418, 1424, 1426, 1432, 1433, 1436, 1437, 1445, 1451, 1452, 1455, 1462, 1471, 1474, 1475, 1481, 1489, 1490, 1493, 1494, 1500, 1502, 1509, 1513, 1527, 1528, 1531, 1532, 1538, 1546, 1550, 1551, 1557, 1559, 1565, 1566, 1569, 1570, 1576, 1578, 1584, 1585, 1588, 1595, 1597, 1604, 1607, 1608, 1614, 1616, 1622, 1623, 1626, 1627, 1633, 1635, 1641, 1642, 1646, 1654, 1660, 1661, 1665, 1671, 1679, 1683, 1684, 1692, 1698, 1699, 1702, 1709, 1711, 1717, 1718, 1721}.

Por lo anterior, la cantidad de bases de ω-primalidad para 1729 son 432.

Para saber la cantidad de bases de q-seudoprimalidad, en primer lugar, se debe saber la cantidad de soluciones de la congruencia $a^{64} \equiv 1 \mod 1729$, y estas son:

$$\{1, 246, 265, 398, 512, 645, 664, 818, 911, 1065, 1084, 1217, 1331, 1464, 1483, 1728\}.$$

La segunda condición que establece si un número es base de q-seudoprimalidad es: existe un $i = 1, 2$ tal que $n \mid \Phi_3(a^{3^i 64})$, por lo tanto, los valores de a que satisfacen la congruencia son:

$\{1, 11, 30, 45, 46, 68, 87, 88, 102, 107, 121, 145, 159, 163, 178, 179, 198, 201, 236, 240,$
$246, 254, 265, 277, 292, 296, 297, 331, 334, 353, 354, 368, 373, 387, 388, 398, 410, 425, 444,$
$445, 464, 487, 501, 512, 543, 544, 562, 563, 578, 600, 620, 634, 635, 639, 645, 653, 654, 664,$
$691, 695, 696, 711, 730, 752, 786, 787, 809, 810, 818, 828, 829, 843, 886, 900, 901, 911, 919,$
$920, 942, 943, 977, 999, 1018, 1033, 1034, 1038, 1065, 1075, 1076, 1084, 1090, 1094, 1095, 1109,$
$1129, 1151, 1166, 1167, 1185, 1186, 1217, 1228, 1242, 1265, 1284, 1285, 1304, 1319, 1331, 1341,$
$1342, 1356, 1361, 1375, 1376, 1395, 1398, 1432, 1433, 1437, 1452, 1464, 1475, 1483, 1489, 1493,$
$1528, 1531, 1550, 1551, 1566, 1570, 1584, 1608, 1622, 1627, 1641, 1642, 1661, 1683, 1684, 1699,$
$1718, 1728\}$

Así las bases de q-seudoprimalidad para 1729 son 144.

A continuación se cuentas las bases de ω-primalidad con las siguientes consideraciones $e = 1$, por lo tanto $q = r$. Así se tiene que un número n es ω-primo base a si satisface alguna de las siguientes condiciones:

$$a^t \equiv 1 \mod n$$

ó

$$\exists 0 \leq i \leq s-1, \text{ tal que } a^{q^{i+1}t} \equiv 1 \mod n \tag{4.5}$$

Lema 65. *La cantidad de bases de ω-primalidad sobre todos los posibles ω para $n = \prod_{i=1}^{m} p_i$ y $n - 1 = q^s t$ es:*

$$\left| \bigcup_{\omega} B\omega p(n) \right| = q^m \prod_{i=1}^{m} (t, p_i - 1) = \left| \{x : \ x^{qt} \equiv 1 \mod n\} \right|$$

Demostración. Sea ω fijo donde $|\omega|_n = q$, para $a \in \mathbb{U}_n$ se deben ver la cantidad de soluciones de las ecuaciones

$$a^t \equiv 1 \mod n \tag{4.6}$$

$$\text{existe } 0 \leq j \leq q-1 \text{ tal que } a^t \equiv \omega^j \mod n \tag{4.7}$$

La cantidad de soluciones de 4.6 está dada por la cantidad de soluciones del sistema

$$\left\{a^t \equiv 1 \mod p_i^{\alpha_i}\right\}_{i=1}^{m}$$

cada una de estas congruencias tiene

$$(t, \phi(p_i^{\alpha_i})) = (t, p_i^{\alpha_i - 1}(p_i - 1)) = (t, p_i - 1)$$

soluciones. Así la congruencia $a^t \equiv 1 \mod n$ tiene $\prod_{i=1}^{m}(t, p_i - 1)$ soluciones.

Para el caso 4.7, con j fijo y dado que $\omega^q \equiv 1 \mod n$, contar la cantidad de soluciones de $a^t \equiv \omega^j \mod n$ es equivalente a contar la cantidad de soluciones de la congruencia $a^{qt} \equiv 1$ mód n, para esto, se debe ver la cantidad de soluciones del sistema

$$\left\{a^{qt} \equiv 1 \mod p_i^{\alpha_i}\right\}_{i=1}^{m}$$

en efecto, cada una de estas ecuaciones tiene

$$(qt, \phi(p_i^{\alpha_i})) = (qt, p_i - 1) = q(t, p_i - 1)$$

soluciones, por lo tanto la cantidad de soluciones de $a^{qt} \equiv 1 \mod n$ es $q\prod_{i=1}^{m}(t, p_i - 1)$.

Dado que existen q^m posibles ω y para cada uno de estos se calculó cuántas bases existen, así la unión de todas las posibles bases sobre todos los posibles ω es:

$$\left|\bigcup_{\omega} B\omega p(n)\right| = q^m \prod_{i=1}^{m}(t, p_i - 1).$$

□

Capítulo 5

Conclusiones

- Al estudiar los conceptos de q-seudoprimalidad base a y ω-primalidad base a, para un entero n y teniendo en cuenta el Lema 61 y los Ejemplos 52 y 62, se concluye que hay menos bases de q-seudoprimalidad que de ω-primalidad, esto es, existen menos bases para las cuales el número n aparenta ser primo. Así decidir si un número es primo o compuesto es más fácil si se hace por el camino de la q-seudoprimalidad. En este sentido el concepto de q-seudoprimalidad es más refinado que el de ω-primo.

- Contrario a lo que inicialmentes se pensó, logramos establecer que los conceptos q-seudoprimalidad y ω-primalidad, NO son equivalentes, en nuestros ejemplos se evidencia no solo que los conceptos son distintos, sino que la q-seudoprimalidad es mejor que la ω-primalidad, ya que al haber menos base de q-seudoprimalidad, números que se camuflan como primos a la luz de un test de ω-primalidad, pueden ser detectados como compuestos en un test de q-seudoprimalidad.

- Como un trabajo futuro, queremos estimar la cota para el cociente $\dfrac{|Bqsp(n)|}{n-1}$, dado que los q-seudoprimos son un refinamiento de los ω-primos, es de esperarse que dicha cota sea más pequeña que la dada por Berrizbeitia en el Teorema 60.

Bibliografía

[1] Pedro Berrizbeitia and T.G.Berry, *Generalized Strong Pseudoprime Tests and Applications*, J. Symbolic Computation, Vol 30, Issue 2, August 2000, Pág 151–160.

[2] David M. Burrton, *Elemenatry Number Theory*, Seventh Edition, The McGraw-Hill companies, 2010.

[3] Jhon H. Castillo, Gilberto Garcia-Pulgarín and Juan Miguel Velásquez-Soto, *De los números de Midy a la primalidad*, Revista Integración, Universidad Industrial de Santander, Vol. 33, No. 1, 2015, pág. 1-10.

[4] Richard Crandall and Carl Pomerance, *Prime Number A Computational Perpective*, Second Edition, Springer, USA, 2005.

[5] Gilberto García P. *ARITMETICA: UN ENFOQUE COMPUTACIONAL*, VIII Coloquio Regional de Matemáticas, Universidad de Nariño. Marzo 1994, Pág 11-25.

[6] Yupeng Jiang and Yingpy Deng, *Strong Pseudoprimes To the Firts Eight Prime Bases*, Mathematics Of Computation, Vol. 83, No 290, November 2014, Pág 2915–2924.

[7] Rudolf Lidl, Haral Niederreiter and P. M. Cohn, *Finite Fields*, Encyclopedia of Mathematics and its applications, Second Edition, vol 20, Cambridge University Press, 1997.

[8] Motose K., *On values of cyclotomic polynimial. II*, Math. J Okayama Uni. No 37 (1995), pág 27-36

[9] Kenneth H. Rosen, *Elemenatry Number Theory and Its Applications*, Sixth Edition, Pearson, 2011.

[10] Vladimir Shevelev, Jhon H. Castillo, Gilberto Garcia Pulgarín and Juan Miguel Velásquez Soto, *Overpseudoprime, and Mersenne and Fermat numbers as primover numbers*, J. Integer Seq. 15 (2012), No. 7, pág 1-10.