Comportamiento y Características de los polinomios AKS con exponente compuesto $n \in \mathbb{N}$

Jahir G. Medina Lopez
jahir.medina@unitru.edu.pe

Escuela de Informática - UNT, Trujillo, Perú.

Resumen

En este artículo se estudia el comportamiento de los polinomios AKS de exponente generatriz natural compuesto. Se plantea un método de factorización para números semiprimos, su vinculación con los números de Carmichael, además de características relevantes a su comportamiento geométrico en el plano cartesiano.

Palabras claves: polinomio AKS, números semiprimos, prueba de primalidad, números de Carmichael, números compuestos, factorización

1. Introducción

Los polinomios AKS (en honor a las siglas de sus autores), necesarios para la demostración del algoritmo AKS (Agrawal, 2002) tienen un valor importante en el campo de la teoría de números, al ser el primer algoritmo determinista para prueba de primalidad en tiempo polinomial , significando su pertenencia al conjunto de problemas tipo P , lo cual implica su resolución en un *tiempo aceptable* (Kozen, 2006, Lectura 1) , sin embargo la primera aparición de estos polinomios data de 1999, en un trabajo preliminar de uno de los autores del algoritmo AKS, en el artículo *Primality and Identity Testing via Chinese Remaindering* (Agrawal, 1999), que es de donde el presente artículo toma su definición:

$$\mathcal{P}_n(z) = (1+z)^n - 1 - z^n$$

El trabajo realizado aquí se enfoca solo en el polinomio descrito originalmente y su comportamiento cuando su exponente generatriz es un numero compuesto natural, es valido aclarar que la denominación **polinomios AKS** nace de su forma general:

$$\mathcal{P}_n(z) = (a+z)^n - a - z^n$$

$$\text{donde: } \gcd(n, a) = 1$$

Tal como se puede observar, el polinomio AKS es un tipo de binomio con la cualidad de tener por exponente un numero n tal que este es **coprimo** con uno de los elementos indeterminados(a).

Este artículo no enfocara su análisis desde el punto de vista estrictamente polinomial,usando en mayor medida los coeficientes (Fowler, 1996), haciendo empleo del triángulo de pascal y las definiciones combinatorias dadas por newton para los binomios (Coolidge, 1949). En el conjunto de los números compuesto, existen dos subconjuntos: los semiprimos y los Carmichael, estos números presentan comportamientos específicamente interesantes al ser relacionados con los polinomios AKS.

Como nota final, se debe aclarar el presente trabajo aun esta en proceso, por lo que muchas demostraciones se encuentran pendientes; para respaldar las conclusiones (donde sea necesario) se usar los datos obtenidos mediante calculo computacional.

2. Trabajos relacionados

2.1. Binomio de Newton y Coeficiente Binomial

Considerando la definición de **Binomio de Newton** a partir de el Lema 2 (Coolidge, 1949, pag 11)

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

donde $x \wedge y \in \mathbb{R}$ y $n \in \mathbb{N}$, ademas $\binom{n}{k}$ se define como:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{1}$$

denominado **coeficiente binomial** , a partir del cual se puede completar la definición del **triangulo de pascal** (Fowler, 1996, pag 4) , definiéndose como **el triángulo generado al sumar los dos elementos inmediatamente superiores**, creando un arreglo triangular:

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
 & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & \\
\end{array}$$

Figura 1: Primeras 7 filas correlativas con los coeficientes de $(x+1)^n$ estando $n \in [0, 7]$
fuente: Re-diseño (Burton, 1980, pag. 11)

2.1.1. Propiedades

- La suma de elementos de la fila n es igual a n^n

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \tag{2}$$

- Los elementos del triángulo poseen simetría axial derivado de la propiedad de los coeficientes

$$\binom{n}{i} = \binom{n}{n-i} \tag{3}$$

- De 2 y 3 se puede describir la suma de elementos de una fila como:

$$2(\sum_{i=0}^{\frac{n}{2}-1} \binom{n}{i}) + \binom{n}{\frac{n}{2}} = 2^n \iff n \equiv 0(mod 2) \tag{4}$$

$$2(\sum_{i=0}^{\frac{n-1}{2}} \binom{n}{i}) = 2^n \iff n \equiv 1(mod 2) \tag{5}$$

2.2. Polinomio AKS

Definiéndose la familia de polinomios AKS como todo polinomio de la forma:

$$\mathcal{P}_n(z) = (a+z)^n - a - z^n$$

$$\text{donde: } \gcd(n, a) = 1$$

$$n \wedge a \in \mathbb{N}$$

y el polinomio AKS original (Agrawal, 1999, pag. 3)

$$\mathcal{P}_n(z) = (1+z)^n - 1 - z^n \tag{6}$$

reescribiéndolo de la forma:

$$\mathcal{P}_n(z) = \sum_{j=1}^{n-1} \binom{n}{j} z^j$$

y a su término general de la forma:

$$t_j = \binom{n}{j} z^j$$

donde $\binom{n}{j}$ es un **coeficiente entero** ,pues $n \wedge j \in \mathbb{N}$.

Además $z \in \mathbb{X}$, $\mathbb{X}$ es un **grupo** donde z representa un elemento cualquiera, denominado *indeterminada* (Robinson, 2003, pag. 100).

2.2.1. Caso Particular

Sea n un **numero primo** definido en $\mathbb{N}$ y usando el lema 3.1 (Agrawal, 2002, pag. 4) cumple que:

$$\mathcal{P}_n(z) \equiv 0(\mathbf{mod}\ n) \rightarrow \mathcal{P}_n(z) \text{ es identicamente nulo}$$

2.3. Definiciones Adicionales

- Se define un numero compuesto como semiprimo, si es de la forma:

$$n = p \cdot q$$

$$p \wedge q \text{ son primos}$$

3. Propuesta

3.1. Definición de un Triángulo Modular AKS

Presentando la idea de un **Triangulo de Pascal Modular del Polinomio AKS** o **AKS-MPT**, definido como:

> El arreglo triangular que se forma al sustituir los elementos clásicos de un triángulo de pascal (coeficientes binomiales de $(x+1)^n$) por los coeficientes del **polinomio AKS original** y aplicando sobre todos ellos la *operación modulo con respecto a su número de fila*.

De esta definición y su sucesivo cálculo obtiene dos tipos de filas en el triángulo:

- Una fila de 0's cuando n es **primo**
- Una fila con valores **enteros** menores a n , cuando n es **compuesto**

3	0	0	0	0															
4	0	0	2	0	0														
5	0	0	0	0	0	0													
6	0	0	3	2	3	0	0												
7	0	0	0	0	0	0	0	0											
8	0	0	4	0	6	0	4	0	0										
9	0	0	0	3	0	0	3	0	0	0									
10	0	0	5	0	0	2	0	0	5	0	0								
11	0	0	0	0	0	0	0	0	0	0	0	0							
12	0	0	6	4	3	0	0	0	3	4	6	0	0						
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0					
14	0	0	7	0	7	0	7	2	7	0	7	0	7	0	0				
15	0	0	0	5	0	3	10	0	0	10	3	0	5	0	0	0			
16	0	0	8	0	12	0	8	0	6	0	8	0	12	0	8	0	0		
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
18	0	0	9	6	0	0	6	0	0	2	0	0	6	0	0	6	9	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	10	0	5	4	0	0	10	0	16	0	10	0	0	4	5	0	10	0	0

Figura 2: Triangulo generado desde la fila 3 hasta la fila 20, resaltado en azul las filas de orden primo

fuente: Propio

De manera formal, un elemento cualquiera de una fila cualquiera del **AKS-MPT** se define:

$$t_j(n) = \binom{n}{j} (\mathbf{mod}\ n) \tag{7}$$

$$n \wedge j \in \mathbb{N}$$

De la definición original para el **polinomio AKS** se sabe que:

- si n es **primo**

$$t_j(n) = 0 \vee \binom{n}{j} \equiv 0(\mathbf{mod}\ n) \tag{8}$$

- si n es **compuesto**

$$\exists!\ \ t_j(n) \neq 0 \vee \binom{n}{j} \equiv m(\mathbf{mod}\ n) \tag{9}$$

donde $m \in [1, n-1]$

3.2. Operaciones Asociadas y Características de AKS-MPT

3.2.1. Número de Elementos

Si en un triángulo de pascal normal, el número de elementos es siempre igual al *número de orden de la fila aumentado en una unidad*, en el **AKS-MPT**, este número varia a causa de las características de su polinomio generatriz (definición 6) , de donde se puede observar pierde el primer y último elemento los cuales son la unidad, adicionalmente en la definición 7 se observa que cuando $j = 1$:

$$\binom{n}{1}(\mathbf{mod}\ n) = \binom{n}{n-1}(\mathbf{mod}\ n) = n(\mathbf{mod}\ n) = 0 \tag{10}$$

Por lo tanto el número de **elementos significativos** (aparente) es:

$$(n+1) - 4$$

$$n - 3$$

pero por el comportamiento combinatorio de los coeficientes binomiales, puede existir algún coeficiente que no se encuentre en los extremos que cumpla:

$$\binom{n}{j} = 0(\mathbf{mod}\ n)$$

definiendo asi, que el número de elementos es:

$$\#nro \leq n - 3 \tag{11}$$

3.2.2. Características de los Coeficientes

mediante un cálculo asistido por computadora de las primeras 7000 filas del **AKS-MPT** se observa que:

$$j \cdot (t_j(n)) \equiv 0(\mathbf{mod}\ n)\ ,\ \forall\ n \text{ compuesto} \tag{12}$$

Sin embargo un caso importante ocurre cuando:

sea n un **numero compuesto semiprimo** y $t_j(n)$ un elemento de la fila n del AKS-MPT, se cumple que si $t_j(n)$ es el **primer número no nulo desde la izquierda** en su fila correspondiente del AKS-MPT entonces:

$$j \cdot t_j(n) = n \tag{13}$$

siendo j el menor factor primo y $t_j(n)$ el mayor

3.2.3. Suma de elementos AKS-MPT

Para un triángulo de Pascal Común, modificando 2 usando 10:

$$\sum_{k=2}^{n-2} \binom{n}{k} + \binom{n}{1} + \binom{n}{n-1} + 1 + 1 = 2^n$$

$$\sum_{k=2}^{n-2} \binom{n}{k} + 2(n) + 2 = 2^n$$

$$\sum_{k=2}^{n-2} \binom{n}{k} = 2^n - 2(n) - 2 \tag{14}$$

Usando la definición 7 y la propiedad distributiva respecto a la suma del módulo:

$$(\sum_{i=2}^{n-2} \binom{n}{j} (\mathbf{mod}\ n))(\mathbf{mod}\ n) = (2^n - 2(n) - 2)(\mathbf{mod}\ n)$$

$$\sum_{i=2}^{n-2} \binom{n}{j} (\mathbf{mod}\ n) \equiv (2^n - 2(n) - 2)(\mathbf{mod}\ n) \tag{15}$$

cuando n es primo todos los elementos son 0 (def. 8)

$$\sum_{i=2}^{n-2} \binom{n}{j} (\mathbf{mod}\ n) = 0$$

$$(2^n - 2(n) - 2)(\mathbf{mod}\ n) = 0$$

$$\Rightarrow (2^n - 2(n) - 2) \equiv 0 (\mathbf{mod}\ n) \tag{16}$$

cuando n es primo.

3.3. Números de Carmichael

En la definición 16 se puede observar una ecuación relativamente semejante al pequeño teorema de Fermat para pruebas de primalidad (Burton, 1980, pag. 97)

$$a^{n-1} = 1 (\mathbf{mod}\ n) \tag{17}$$

cuando n es primo.
Siendo $a \wedge n$ **coprimos** , esto significa que $\gcd(a, n) = 1$ y dado que en la ecuación 16 se sabe n es primo al igual que 2 (para evitar ambigüedades $n \geq 3$, esto no afecta las definiciones ya dadas) se deduce que $\gcd(2, n)$ siempre será 1 y por tanto coprimos.

Los números de Carmichael se definen como todo numero n que cumple la ecuación 17 sin ser primo (Carmichael, 1912), se sabe que estos números son relativamente escasos en comparación con los números primos.

En concordancia con el calculo asistido por computadora de las primeras 7000 filas del **AKS-MPT** se puede contrastar que los **números de Carmichael** menores a 7000

$$561, 1105, 1729, 2465, 2821, 6601$$

tienen una coincidencia del $100\,\%$ de fallos al ser estos probados en la ecuación 16, mientras que para los demás valores actúan de la forma esperada. Por consiguiente es valido inferir que la ecuación 16 tiene similar comportamiento matemático en su rango que **el pequeño teorema de Fermat** [17].

3.3.1. Filas AKS-MPT de orden Carmichael

En las primeras 7000 filas, solo aparecen 6 polinomios AKS de exponen n siendo n un numero de Carmichael; usando AKS-MPT se obtiene los polinomios (por comprensión):

- $n = 561$
$$\sum_{k=2}^{599} \binom{561}{k} z^k$$
- $n = 1105$
$$\sum_{k=2}^{1103} \binom{1105}{k} z^k$$
- $n = 1729$
$$\sum_{k=2}^{1727} \binom{1729}{k} z^k$$
- $n = 2465$
$$\sum_{k=2}^{2463} \binom{2465}{k} z^k$$
- $n = 2821$
$$\sum_{k=2}^{2819} \binom{2821}{k} z^k$$
- $n = 6601$
$$\sum_{k=2}^{6599} \binom{6601}{k} z^k$$

Por una corazonada se calculó el $\gcd(n, \binom{n}{k})$ para todos sus coeficientes, con la idea de que dichos coeficientes serian coprimos de n, sin embargo, se observo que si bien no eran coprimos tenían la siguiente característica :

$$n = \gcd(n, t_k(n)) \cdot k \tag{18}$$

pero también se observo que:

$$\gcd(n, t_k(n)) = t_k(n)$$

por lo que para el caso de las filas AKS-MPT de orden Carmichael la ecuación 18 se simplifica a:

$$n = t_k(n) \cdot k \tag{19}$$

resultado similar a si el exponente fuese semiprimo (ecuación 13)

4. Resultados

4.1. Computacionales

En la sección anterior se revisó y determino el comportamiento aritmético del polinomio AKS con respecto a sus coeficientes y los números de Carmichael, en esta parte, se mostrará el comportamiento geométrico.

4.1.1. Polinomio AKS General con $\mathbb{X} = \mathbb{R}$

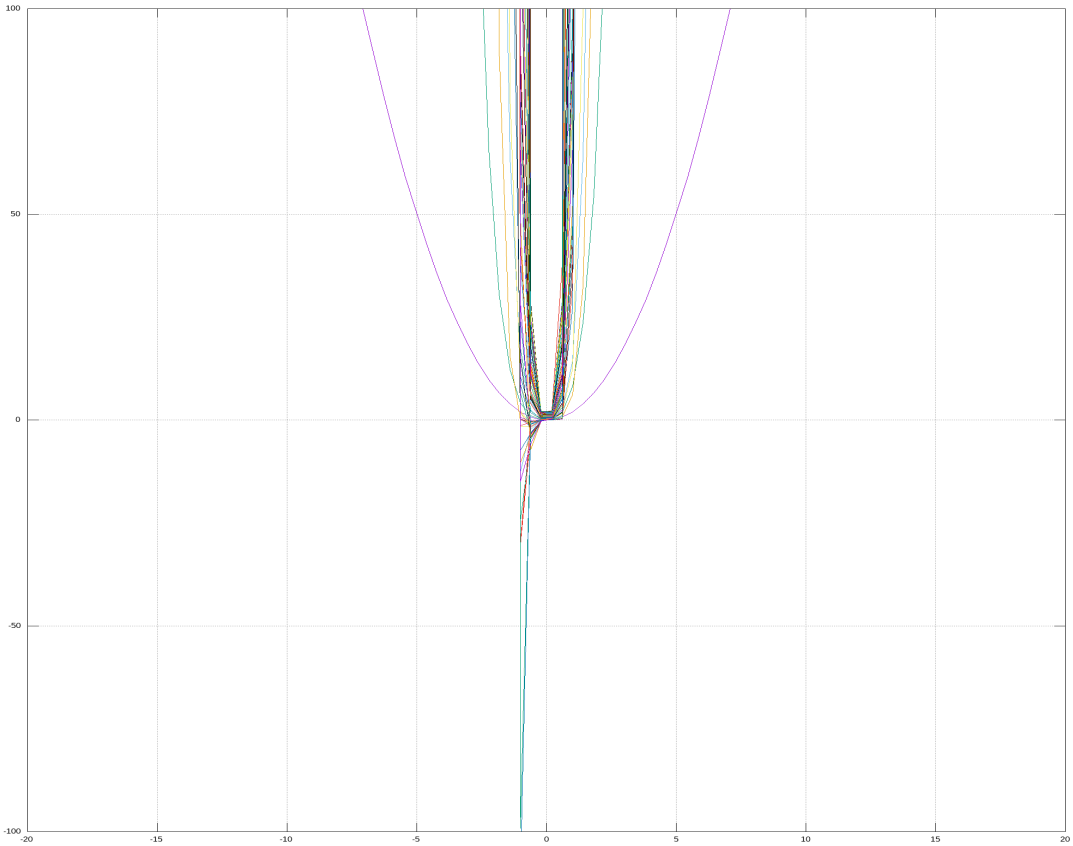

Figura 3: Grafica de los polinomios AKS cuando $n \in [3, 100]$ y $x \in \mathbb{R}$
fuente: Propio

En esta imagen se puede observar que cuando un polinomio AKS se opera sobre los $\mathbb{R}$ su comportamiento geométrico no difiere en nada de los binomios comunes

4.1.2. Polinomio AKS-MPT con $\mathbb{X} = \mathbb{R}$

En este caso en particular, donde la operación $(\mathbf{mod}\ n)$ resulta relevante, pues es quien aparentemente genera la tendencia de $\mathcal{P}_n(z)$ a acumularse cerca del eje x , en otras palabras, tender hacia 0.

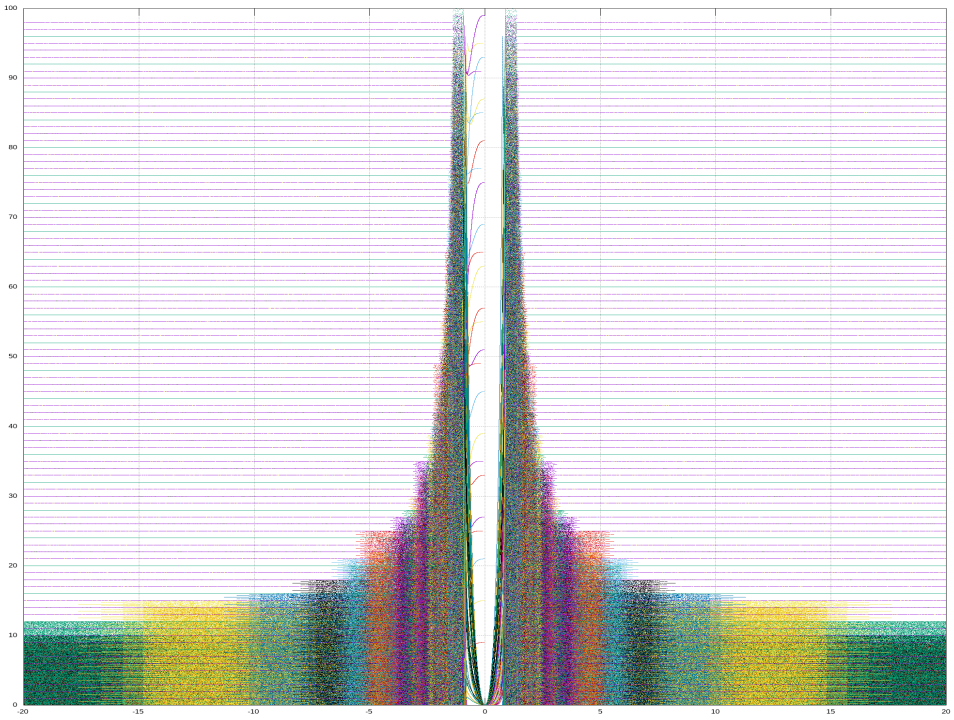

Figura 4: Los coeficientes generados por el AKS-MPT en forma polinomial $x \in [-20, 20] \wedge n \in [3, 100]$

fuente: Propio

Este comportamiento acumulativo puede deberse a la característica de sus coeficientes descrita por la definición 12, de manera que al sustituirse el valor indeterminado solo queda de resto $x^j(\mathbf{mod}\ n)$. Dado que esta expresión se puede escribir como:

$$x^j = l(\mathbf{mod}\ n) \tag{20}$$

estando $l \in \langle 0, n \rangle$, resultado de extender la operación $\mathbf{mod}$ al grupo de los $\mathbb{R}$,trabajando solo con la parte entera y dejando la parte decimal intacta. Ya que en $a' \in [a, a+1]$ la operación $\mathbf{mod}$ extendida se limita a $a' \in [a(\mathbf{mod}\ \mathbf{n}), a+1(\mathbf{mod}\ \mathbf{n})]$ dejando los valores no enteros de la forma

$$a' = a(\mathbf{mod}\ \mathbf{n}) + \sigma \tag{21}$$
$$\sigma \in \langle 0, 1 \rangle$$

si σ es elevando a la potencia j el resultado sigue perteneciendo al intervalo $\langle 0, 1 \rangle$, por consiguiente se puede asumir que solo resulta relevante estudiar la parte de entera residual obtenida en la ecuación 20. Del gráfico y la definición 21 podemos manifestar que el resultado de trabajar sobre los reales tiene relevancia solo la parte entera, la cual es, quien en última instancia se empieza a acumular cerca del eje x o del valor 0 en y. Un explicación mas detallada requeriría cálculos con rangos superiores a $[-20, 20]$ y la demostración analítica de esta convergencia.

4.2. Detalles de Resultados

Dado que los resultados computacionales contienen 7000 columnas y habiendo 4 diferentes tipos, se dejara un enlace hacia **github** , de donde se podrá descargar los datos completos y el script usado para su generación:
enlace: **Comportamiento-y-Caracteristicas-de-los-polinomios-AKS-con-exponente-compuesto-n-N.git**

4.2.1. Script

Amen de no alargar el articulo de forma innecesaria, no se pondrá el script directamente, solo una descripción técnica. El script desarrollado para los cálculos se encuentra escrito en **python** ,para la versión $2{,}7{,}13$,; no se empleó ningún algoritmo especial, sin embargo, para el cálculo de las filas se aposto por operaciones secuenciales que ocupen memoria y no potencia de cálculo.

Como se describe anteriormente, el cálculo de los coeficientes de los polinomios y elementos del AKS-MPT no emplea el cálculo combinatorio al ser excesivamente demandante la recursión factorial; sin embargo, si se emplea la técnica original del triángulo de pascal de sumas sucesivas.

4.2.2. Tablas de Resultados

- Definiciones 8 y 9 basadas en el archivo **patrón de coeficientes.dat**
- Patrón usado para definir la ecuación 19 y Parte 3.3.1 revisar los archivos **carmichael test.dat** y **carmichael polinomios.dat**
- Grafica de polinomios AKS (figura 3) sobre los $\mathbb{R}$ generada desde el archivo **polinomios Generales.plot**

4.3. Teóricos

El presente artículo trata a todas sus definiciones, ecuaciones y suposiciones como verdaderas, mas no por tanto deben ser tomadas como tales, el trabajo aquí presentado es de carácter descriptivo más que analítico, siendo esta una versión inicial se espera en futuras versiones incluir definiciones y demostraciones completamente analíticas que den un respaldo solido a los cálculos obtenidos vía asistencia computacional.

5. Conclusiones y trabajos futuros

5.1. Conclusiones

El polinomio AKS presenta un gran campo de estudio, no solo para la teoría de números, sino también para la criptografía, en donde se puede emplear en la definición 13 para factorizar los números RSA (Rivest et al., 1978, pag. 5 sección V), caracterizados por ser semiprimos, sin tener que recurrir las divisiones sucesivas. Para este fin, el presente artículo deja a disposición el script usado para generar las n filas del AKS-MPT, si este n fuese un **número RSA** la

factorización quedaría inmediatamente determinada por:

$$j \cdot t_j(n) = n$$

De ser requerido j puede ser obtenido de forma aleatoria y recurri a la formula con la forma:

$$j \cdot \binom{n}{j} = n$$

Aunque esta aplicación resulta en un consumo exagerado de recursos computacionales (sumas sucesivas) se puede optimizar si se analiza con mayor detalle los patrones que oculta los polinomios AKS con exponente compuesto $n \in \mathbb{N}$, el método empleado aquí resulta especialmente favorable durante estudios descriptivos, ya que aun no ofrece directamente ninguna demostración analítica propiamente dicha, el AKS-MPT posee ventaja sobre los métodos polinomiales de análisis cuando se trata de ubicar patrones usando solo la intuición.

5.2. Trabajos futuros

Se sugiere revisar el caso de los exponentes n que sean números de Carmichael, su relativa relación con el pequeño teorema de Fermat puede resultar en la obtención de nuevos patrones.

Finalmente se recomienda re-calcular y re-graficar los valores para los polinomios AKS sobre el grupo de los complejos, quizás el comportamiento con tendencia a acumularse hacia 0 resulte en una serie de curvas cerradas.

Referencias

Agrawal, N. K. N. S. M. (2002). Primes is in p. *Indian Institute of Technology Kanpur Department of Computer Science & Engineering Kanpur-208016, INDIA*.

Agrawal, S. B. M. (1999). Primality and identity testing via chinese remaindering. *Indian Institute of Technology*.

Burton, D. M. (1980). *Elementary Number Theory*. Allyn and Bacon, Inc.

Carmichael, R. D. (1912). On composite numbers p which satisfy the fermat congruence <tex-math>$a^{P-1} \equiv 1 \bmod p$</tex-math>. *The American Mathematical Monthly*, 19(2):22–27.

Coolidge, J. L. (1949). The story of the binomial theorem. *The American Mathematical Monthly*, 56(3):147–157.

Fowler, D. (1996). The binomial coefficient function. *The American Mathematical Monthly*, 103(1):1–17.

Kozen, D. C. (2006). *Theory of Computation*. Springer London.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126.

Robinson, D. J. S. (2003). *An Introduction to Abstract Algebra*. Walter de Gruyter, Department of Mathematics University of Illinois at Urbana-Champaign 1409 W. Green Street Urbana, Illinois 61801-2975 USA.