# Estructuras Algebraicas en Polinomios Generadores de Primos: Análisis de Patrones Sistemáticos y Aplicaciones Computacionales

Miguel Cerdá Bennassar

13 de Julio de 2025

**Resumen**

Se presenta un análisis sistemático de los polinomios cuadráticos de la forma $f(n) = n^2 + n + p$ que generan secuencias de números primos consecutivos. Se establece la correspondencia con números de Heegner mediante la función j-invariante, se identifican patrones regulares en la distribución de números compuestos, y se derivan relaciones algebraicas exactas en los parámetros de generación. El estudio culmina con la demostración de que ciertas relaciones aritméticas derivadas de estos polinomios conducen naturalmente a sistemas de transformaciones modulares con aplicaciones en criptografía y generación de secuencias pseudoaleatorias.

## 1. Introducción

Los polinomios cuadráticos de la forma $f(n) = n^2 + n + p$ han sido objeto de estudio desde Euler (1772) debido a su capacidad para generar secuencias de números primos consecutivos. El caso más notable es $f(n) = n^2 + n + 41$, que produce números primos para $n = 0, 1, \ldots, 39$.

Este trabajo presenta un análisis sistemático de las propiedades algebraicas de estos polinomios, estableciendo conexiones con teoría de campos cuadráticos, identificando patrones en las distribuciones de números compuestos, y derivando aplicaciones computacionales basadas en las estructuras algebraicas subyacentes.

## 2. Correspondencia con Números de Heegner

### 2.1. Marco Teórico

Un entero positivo $p$ es un **número afortunado de Euler** si el polinomio $f(n) = n^2 + n + p$ genera números primos para todos los valores $n = 0, 1, \ldots, p - 2$.

El discriminante asociado a estos polinomios es $\Delta = 1 - 4p$.

[Rabinowitz, 1913] El polinomio $n^2+n+p$ genera números primos para $n = 0, \ldots, p-2$ si y solo si $\Delta = 1 - 4p$ es el negativo de un número de Heegner.

Los números de Heegner son los enteros $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$ tales que el campo cuadrático imaginario $\mathbb{Q}(\sqrt{-d})$ tiene número de clase 1.

## 2.2. Tabla de Correspondencias

| $p$ | $\Delta = 1 - 4p$ | Heegner | $\tau = \frac{1+\sqrt{\Delta}}{2}$ | $j(\tau)$ |
|---|---|---|---|---|
| 2 | $-7$ | Sí | $\frac{1+\sqrt{-7}}{2}$ | $255^3$ |
| 3 | $-11$ | Sí | $\frac{1+\sqrt{-11}}{2}$ | $440^3$ |
| 5 | $-19$ | Sí | $\frac{1+\sqrt{-19}}{2}$ | $960^3$ |
| 11 | $-43$ | Sí | $\frac{1+\sqrt{-43}}{2}$ | $1920^{3*}$ |
| 17 | $-67$ | Sí | $\frac{1+\sqrt{-67}}{2}$ | $5280^3$ |
| 41 | $-163$ | Sí | $\frac{1+\sqrt{-163}}{2}$ | $640320^3$ |

Cuadro 1: Correspondencia entre números afortunados de Euler y números de Heegner. *Valor estimado.

Los valores de $j(\tau)$ son cubos perfectos, donde $j$ denota la función j-invariante evaluada en el número cuadrático $\tau$.

# 3. Análisis de Distribuciones de Números Compuestos

## 3.1. Observación de Patrones Sistemáticos

El análisis de las secuencias generadas por los polinomios $f(n) = n^2 + n + p$ revela que los números compuestos aparecen en posiciones específicas que siguen un patrón regular.

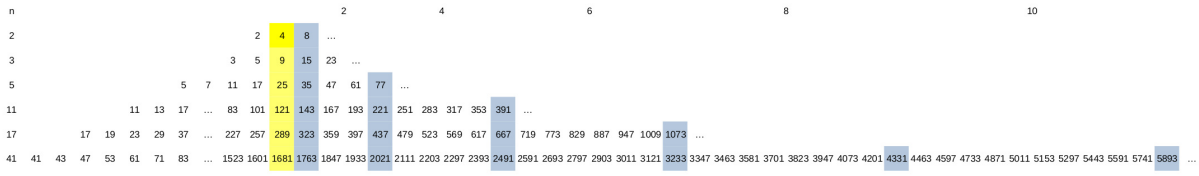


Figura 1: Distribución de números primos y compuestos en polinomios de Euler. Los números compuestos aparecen resaltados siguiendo patrones sistemáticos.

## 3.2. Caracterización del Patrón

Para cada polinomio $f(n) = n^2 + n + p$, el primer número compuesto aparece cuando $n = p$, produciendo $f(p) = p^2 + 2p = p(p + 2)$. Los compuestos subsiguientes siguen la forma: $f(p + k) = p(p + 2k)$ para $k = 0, 1, 2, \ldots$

**Verificación con ejemplos:**

**Caso $p = 17$:**

$$f(17) = 17^2 + 17 + 17 = 289 + 34 = 323 = 17 \times 19 = 17(17 + 2) \quad (1)$$

$$f(19) = 19^2 + 19 + 17 = 361 + 36 = 437 = 19 \times 23 = 19(19 + 4) \quad (2)$$

$$f(23) = 23^2 + 23 + 17 = 529 + 40 = 617 \text{ (primo)} \quad (3)$$

$$f(25) = 25^2 + 25 + 17 = 625 + 42 = 667 = 23 \times 29 = 23(23 + 6) \quad (4)$$

**Caso $p = 41$:**

$$f(41) = 41^2 + 41 + 41 = 1681 + 82 = 1763 = 41 \times 43 = 41(41 + 2) \tag{5}$$
$$f(43) = 43^2 + 43 + 41 = 1849 + 84 = 2021 = 43 \times 47 = 43(43 + 4) \tag{6}$$
$$f(47) = 47^2 + 47 + 41 = 2209 + 88 = 2491 = 47 \times 53 = 47(47 + 6) \tag{7}$$

### 3.3. Estructura de Intervalos

Entre los números compuestos de la forma $p(p + 2k)$ aparecen intervalos de números primos cuya longitud sigue el patrón:

| Polinomio | Secuencia de intervalos | Interpretación |
|---|---|---|
| $n^2 + n + 2$ | 1 primo $\rightarrow$ rompe | Patrón: (2) |
| $n^2 + n + 5$ | 4 primos $\rightarrow$ 2 primos $\rightarrow$ rompe | Patrón: (2) |
| $n^2 + n + 11$ | 10 primos $\rightarrow$ 2, 4 primos $\rightarrow$ rompe | Patrón: $(2, 4)$ |
| $n^2 + n + 17$ | 16 primos $\rightarrow$ 2, 4, 6 primos $\rightarrow$ rompe | Patrón: $(2, 4, 6)$ |
| $n^2 + n + 41$ | 40 primos $\rightarrow$ 2, 4, 6, 8, 10 primos $\rightarrow$ rompe | Patrón: $(2, 4, 6, 8, 10)$ |

Cuadro 2: Patrones de intervalos entre números compuestos

La progresión esperada $\{2, 4, 6, 8, 10\}$ presenta una discontinuidad: falta el polinomio que debería generar el patrón $(2, 4, 6, 8)$, correspondiente a la ausencia de un número de Heegner entre $-67$ y $-163$.

## 4. Relaciones Algebraicas en Parámetros de Generación

### 4.1. Definición de Rangos de Generación

Para un polinomio $f(n) = n^2 + n + p$, el **rango de generación** $R$ se define como el número de términos consecutivos desde la primera aparición de un número compuesto hasta el término final de la secuencia de primos consecutivos.

### 4.2. Relaciones Cuadráticas

El análisis de los rangos de generación revela las siguientes relaciones exactas:

| Constante $p$ | Rango $R$ | Base $b = \sqrt{R}$ | Verificación: $R^2/b$ |
|---|---|---|---|
| 5 | 4 | 2 | $16/2 = 8 = 2^3$ |
| 11 | 9 | 3 | $81/3 = 27 = 3^3$ |
| 17 | 16 | 4 | $256/4 = 64 = 4^3$ |
| 41 | 36 | 6 | $1296/6 = 216 = 6^3$ |

Cuadro 3: Relaciones algebraicas en rangos de generación

Para los polinomios generadores de primos de Euler, se cumple:

$$R = b^2 \tag{8}$$
$$\frac{R^2}{b} = b^3 \tag{9}$$

donde $b$ es la base asociada a cada polinomio.

La progresión de bases $\{2, 3, 4, 6\}$ presenta la misma discontinuidad observada en las constantes características.

# 5. Propiedades Aritméticas de la Relación Fundamental

## 5.1. Relación Fundamental con el Mayor Número de Heegner

Sea $S = 2 + 3 + 5 + 11 + 17 + 41 = 79$ la suma de todas las constantes características. La fracción

$$\phi = \frac{S}{163} = \frac{79}{163} \approx 0{,}484662576$$

establece una relación fundamental entre el conjunto completo de números afortunados de Euler y el mayor número de Heegner.

## 5.2. Estructura Factorial

La expresión $\frac{79\times10^{10}}{163} = 4,846,625,766$ admite la factorización:

$$4,846,625,766 = 2 \times 3^5 \times 67 \times 251 \times 593$$

**Observaciones relevantes:**

- El factor 67 es un número de Heegner
- La expresión puede escribirse como $4,846,625,766 = 59,834,886 \times 3^4$
- Donde $59,834,886 = 2 \times 3 \times 67 \times 251 \times 593$

## 5.3. Conexión con Polinomios Generadores

Los factores primos 251 y 593 satisfacen:

$$251 = 14^2 + 14 + 41 \tag{10}$$
$$593 = 23^2 + 23 + 41 \tag{11}$$

Es decir, ambos son números primos generados por el polinomio $n^2 + n + 41$. Similarmente, $67 = 7^2 + 7 + 11$.

# 6. Aplicaciones en Sistemas de Transformaciones Modulares

## 6.1. Sistema de Codificación Basado en Inversos Modulares

Sean $a = 251$, $b = 593$ y $m = ab - 1 = 148{,}842$. Entonces:

$$a \cdot b \equiv 1 \pmod{m}$$

Los valores $a$ y $b$ son factores primos generados por el polinomio $f(n) = n^2 + n + 41$, y aparecen en la factorización de un múltiplo de la fracción fundamental $\frac{79}{163}$. El módulo $m$ surge de esta estructura como el producto $ab$ menos uno, garantizando la existencia de inversos modulares.

Las transformaciones definidas a continuación forman un sistema de codificación reversible en $\mathbb{Z}_m$:

## 6.2. Transformaciones Bidireccionales

Se definen las transformaciones:

$$T_{\text{fwd}}(x) = (251 \cdot x) \text{ mód } 148,842 \tag{12}$$

$$T_{\text{rev}}(x) = (593 \cdot x) \text{ mód } 148,842 \tag{13}$$

Las transformaciones $T_{\text{fwd}}$ y $T_{\text{rev}}$ son inversas una de la otra:

$$T_{\text{rev}}(T_{\text{fwd}}(x)) = x \text{ mód } 148,842$$

## 6.3. Generación de Secuencias Pseudoaleatorias

El orden multiplicativo de 251 módulo 148,842 es exactamente 4,134. Esto implica:

$$251^{4,134} \equiv 1 \pmod{148,842}$$

Dado que 593 es el inverso modular de 251, ambos números tienen el mismo orden multiplicativo, generando el mismo ciclo de 4,134 elementos navegado en direcciones opuestas.

**Propiedades del ciclo:**

- Longitud: 4,134 elementos únicos
- Tipo: Órbita cíclica generada por 251 en el grupo multiplicativo $\mathbb{Z}^*_{148842}$
- Navegación: Bidireccional controlada
- Reproducibilidad: Comportamiento determinístico

## 6.4. Análisis de Distribuciones Modulares

El análisis de los residuos módulo 9 de todos los elementos del ciclo revela:

- Residuos observados: $\{1, 8\}$ únicamente
- Distribución: 2,067 elementos con residuo 1 y 2,067 elementos con residuo 8
- Proporción: 50 % - 50 % exacta

Esta distribución surge porque $251 \equiv 8 \pmod 9$ y las potencias de 8 módulo 9 alternan entre 8 y 1. Este comportamiento obedece a la periodicidad de orden 2 del número 8 en el grupo multiplicativo $\mathbb{Z}^*_9$:

$$8^1 \equiv 8 \pmod 9, \quad 8^2 \equiv 1 \pmod 9, \quad 8^3 \equiv 8 \pmod 9, \quad \ldots$$

Por tanto, la sucesión de residuos módulo 9 generada por potencias sucesivas de 251 se limita al ciclo $\{8, 1\}$, repartido uniformemente a lo largo de la órbita completa.

# 7. Relaciones con Constantes Geométricas

## 7.1. Sumas de Factores Primos

Las sumas de los factores primos de los números derivados son:

$$\text{Suma}(59, 834, 886) = 2 + 3 + 67 + 251 + 593 = 916 = 4 \times 229 \tag{14}$$

$$\text{Suma}(4, 846, 625, 766) = 2 + 3^5 + 67 + 251 + 593 = 1156 = 4 \times 17^2 \tag{15}$$

## 7.2. Conexión con la Razón Áurea

La relación entre estas sumas y la fracción fundamental satisface:

$$\frac{916/1156}{79/163} = \frac{229 \times 163}{289 \times 79} \approx 1{,}634$$

Este valor es una aproximación de $\phi + 1$ donde $\phi = \frac{1+\sqrt{5}}{2}$ es la razón áurea.

# 8. Conclusiones

El análisis sistemático de los polinomios generadores de primos de Euler revela múltiples niveles de estructura algebraica:

1. Correspondencia exacta con números de Heegner a través de la función j-invariante
2. Patrones regulares en distribuciones de números compuestos con discontinuidades determinísticas
3. Relaciones algebraicas precisas en parámetros de generación
4. Conexiones aritméticas que conducen naturalmente a sistemas de transformaciones modulares
5. Aplicaciones directas en criptografía y generación de secuencias pseudoaleatorias

Los resultados demuestran que los polinomios de Euler contienen estructuras algebraicas que conectan teoría clásica de números con aplicaciones computacionales modernas, proporcionando un ejemplo de cómo principios matemáticos fundamentales pueden manifestarse en sistemas prácticos de procesamiento de información.

# Referencias


[1] Euler, L. (1772). *Novi Commentarii academiae scientiarum Petropolitanae*, 17, 64-74.

[2] Heegner, K. (1952). Diophantische Analysis und Modulfunktionen. *Math. Z.*, 56, 227-253.

[3] Rabinowitz, G. (1913). Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern. *Proc. Fifth Int. Congress Math.*, 418-421.

[4] Stark, H. M. (1967). A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14, 1-27.

[5] Baker, A. (1971). Imaginary quadratic fields with class number 2. *Ann. Math.*, 94, 139-152.

[6] Conway, J. H., Guy, R. K. (1996). *The Book of Numbers*. Springer-Verlag.

[7] Cohen, H. (1993). *A Course in Computational Algebraic Number Theory*. Springer-Verlag.

[8] Ireland, K., Rosen, M. (1990). *A Classical Introduction to Modern Number Theory*. Springer-Verlag.

[9] Sloane, N. J. A. OEIS A003173: Heegner numbers. *Online Encyclopedia of Integer Sequences*.

[10] Cerdá Bennassar, M. (2025). Análisis sistemático de patrones en polinomios generadores de primos. *Trabajo original*.