III. Descomposición en campos cuadráticos y longitud del tramo inicial en los polinomios $n^2 + n + p$

Miguel Cerdá Bennassar

Abril de 2026

Resumen

Se estudia la conexión entre la longitud del tramo inicial de primalidad del polinomio $f_p(n) = n^2 + n + p$ y la aritmética del campo cuadrático $K_p = \mathbb{Q}(\sqrt{1-4p})$. El instrumento central es la tricotomía de los primos en K_p: un primo q es inerte si y solo si no divide ningún término de la sucesión $a_k = p + k(k+1)$; los primos split o ramificados dividen exactamente dos o un término por período respectivamente y son los únicos que pueden causar la ruptura del tramo. Se demuestra que la condición $\ell(p) = p - 1$ —primos afortunados de Euler— es equivalente a que todos los primos $q < p$ sean inertes en K_p. Esta equivalencia admite una demostración elemental, basada en las cotas $a_k \geq p$ y $a_k < p^2$ para $k < p - 1$. La conexión con el teorema de Rabinowitsch —que caracteriza la misma condición mediante el número de clase $h(1-4p) = 1$— se cita sin reproducir. Para los primos ordinarios, se identifica el primo responsable de la ruptura y se obtiene una caracterización efectiva de $\ell(p)$ en términos del primo responsable $q^*(p)$ y sus raíces modulares.

Índice

1. Introducción **2**

2. Preliminares **3**
2.1. Notación de la serie 3
2.2. Herramientas de campos cuadráticos 3
2.3. Notación adicional 4

3. Raíces modulares de f_p y descomposición en $\mathbb{Q}(\sqrt{1-4p})$ **4**

4. El primo responsable de la ruptura **6**
4.1. El caso $p \equiv 1 \pmod 3$ 6
4.2. El caso de primos gemelos 7

5. Reformulación constructiva del teorema de Rabinowitsch **7**
5.1. La desigualdad clave 7
5.2. El teorema central 7
5.3. El contrarrecíproco: existencia del primo responsable 8

6. Verificación para los casos afortunados y ordinarios **9**
6.1. Los casos afortunados 9
6.2. El caso $p = 41$ en detalle 9
6.3. Los casos ordinarios 9
6.4. Ejemplo detallado: $p = 101$ 10

7. Fórmula explícita para $\ell(p)$ **11**
7.1. Los dos casos según la factorización de $4p - 1$ 11

8. Conclusión **12**

1. Introducción

Los dos trabajos anteriores de esta serie han establecido una estructura algebraica precisa para los polinomios cuadráticos $f_p(n) = n^2 + n + p$. El primero [1] analizó la cola de los casos afortunados de Euler ($p \in \{2, 3, 5, 11, 17, 41\}$): compuestos organizados sobre una progresión cuadrática, bloques de primos de longitudes crecientes, y un compuesto centinela $f_p(2p-1) = p \cdot (4p-1)$. El segundo [2] extendió el análisis al caso general: el tramo inicial de primalidad de f_p coincide exactamente con la longitud de la constelación de primos $\{p, p+2, p+6, p+12, \ldots\}$ cuyos términos son los de la sucesión $a_k = p + k(k+1)$.

Ambos trabajos dejaron abierta la pregunta fundamental: ¿qué determina la longitud $\ell(p)$ del tramo inicial? Para los seis casos afortunados, la respuesta es el teorema de Rabinowitsch [3]: $\ell(p) = p - 1$ si y solo si el discriminante $1 - 4p$ es el negativo de un número de Heegner, equivalentemente, si el campo cuadrático $\mathbb{Q}(\sqrt{1-4p})$ tiene número de clase 1 [4]. Para los primos ordinarios, el mecanismo que determina $\ell(p)$ no había sido identificado explícitamente.

El presente trabajo da respuesta a esa pregunta. El instrumento es el comportamiento de los primos en el campo cuadrático $K_p = \mathbb{Q}(\sqrt{1-4p})$, que se clasifica según el símbolo de Legendre del discriminante $D = 1 - 4p$:

- un primo q es *inerte* en K_p si $(D/q) = -1$; en este caso q no divide ningún término a_k;
- un primo q es *split* en K_p si $(D/q) = +1$; en este caso q divide a_k para exactamente dos clases de índices k módulo q;
- un primo q es *ramificado* en K_p si $q \mid D$; en este caso q divide a_k para exactamente una clase de índices k módulo q.

El resultado central es que el tramo inicial de f_p termina en $k = \ell(p)$ precisamente porque existe un primo $q < a_{\ell(p)}$, split o ramificado en K_p, cuya raíz modular cae en esa posición y hace que $a_{\ell(p)}$ sea compuesto. Los primos inertes, por contra, nunca interfieren con el tramo.

Este análisis conduce a una reformulación constructiva del teorema de Rabinowitsch: $\ell(p) = p - 1$ si y solo si todos los primos $q < p$ son inertes en K_p, lo que es equivalente a $h(D) = 1$. La reformulación es constructiva en el sentido de que identifica, para cada primo ordinario, el primo específico responsable de la ruptura del tramo, algo que el enunciado clásico no proporciona.

La sección 2 recoge los preliminares algebraicos necesarios. La sección 3 establece la tricotomía inerte/split/ramificado para los primos de K_p y sus consecuencias sobre la sucesión (a_k). La sección 4 caracteriza el primo responsable de la ruptura del tramo para primos ordinarios. La sección 5 formula y demuestra la reformulación constructiva del teorema de Rabinowitsch. La sección 6 ilustra los resultados con ejemplos explícitos para los casos afortunados y varios primos ordinarios. La sección 8 cierra con las conclusiones.

2. Preliminares

Esta sección recoge, sin demostraciones, los elementos necesarios de los trabajos anteriores y de la teoría de campos cuadráticos.

2.1. Notación de la serie

A lo largo de esta serie, p denota siempre un primo y se trabaja con el polinomio cuadrático

$$f_p(n) = n^2 + n + p$$

y la sucesión

$$a_k = p + k(k+1), \qquad k \geq 0,$$

que satisface $f_p(k) = a_k$ para todo $k \geq 0$ [2]. Las diferencias son $a_{k+1} - a_k = 2(k+1)$, de modo que los gaps forman la sucesión $2, 4, 6, 8, \ldots$

Definición 1 (Tramo inicial)**.** *Se llama* tramo inicial *de f_p al mayor segmento $a_0, a_1, \ldots, a_{\ell-1}$ formado enteramente por números primos. Su longitud se denota $\ell(p)$.*

El discriminante de f_p como polinomio cuadrático es

$$D = 1 - 4p.$$

Este es el objeto central del análisis: determina tanto la aritmética del campo cuadrático $K_p = \mathbb{Q}(\sqrt{D})$ como el comportamiento de la sucesión (a_k) módulo primos.

2.2. Herramientas de campos cuadráticos

Se recogen aquí los resultados estándar de la teoría de campos cuadráticos que se usarán en las secciones siguientes. Las demostraciones pueden consultarse en [5].

Definición 2 (Campo cuadrático asociado a p)**.** *Sea $D = 1 - 4p$. Se define el campo cuadrático imaginario*

$$K_p = \mathbb{Q}(\sqrt{D}).$$

Para los valores de p considerados, $D < 0$ y el campo es imaginario. El número de clase $h(D)$ mide el grado de no unicidad de la factorización en el anillo de enteros de K_p.

Definición 3 (Símbolo de Legendre)**.** *Sea q un primo impar y D un entero con $q \nmid D$. El símbolo de Legendre*

$$\left(\frac{D}{q}\right) = \begin{cases} +1 & \text{si } D \text{ es residuo cuadrático módulo } q, \\ -1 & \text{si } D \text{ es no residuo cuadrático módulo } q. \end{cases}$$

Para $q = 2$ se usa la condición sobre D mód 8: $(D/2) = +1$ si $D \equiv 1 \pmod 8$, $(D/2) = -1$ si $D \equiv 5 \pmod 8$, y $q = 2$ ramifica si $D \equiv 0 \pmod 4$.

Proposición 1 (Tricotomía de primos en K_p, [5])**.** *Sea q un primo y $D = 1 - 4p$.*

1. *Si $q \mid D$: q es* ramificado *en K_p.*
2. *Si $q \nmid D$ y $(D/q) = +1$: q es* descompuesto *(split) en K_p.*
3. *Si $q \nmid D$ y $(D/q) = -1$: q es* inerte *en K_p.*

Teorema 1 (Rabinowitsch, 1913 [3])**.** *$\ell(p) = p - 1$ si y solo si $h(D) = 1$, es decir, si y solo si K_p tiene número de clase 1. Por la clasificación de Stark [4], esto ocurre exactamente para $p \in \{2, 3, 5, 11, 17, 41\}$.*

2.3. Notación adicional

Para un primo q y un entero p, se denota por $\mathcal{R}(q, p)$ el conjunto de *raíces modulares de f_p módulo q*:

$$\mathcal{R}(q, p) = \big\{k \in \{0, 1, \ldots, q-1\} : q \mid f_p(k)\big\}.$$

Equivalentemente, $\mathcal{R}(q, p)$ es el conjunto de soluciones de $x^2 + x + p \equiv 0 \pmod q$. En términos de (a_k): $k \in \mathcal{R}(q, p)$ si y solo si $q \mid a_k$.

3. Raíces modulares de f_p y descomposición en $\mathbb{Q}(\sqrt{1-4p})$

Esta sección establece la conexión algebraica fundamental entre las raíces modulares de f_p y el comportamiento de los primos en el campo $K_p = \mathbb{Q}(\sqrt{D})$, $D = 1-4p$.

Teorema 2 (Tricotomía de raíces modulares)**.** *Sea p un primo, $D = 1 - 4p$ y q un primo. El cardinal $|\mathcal{R}(q, p)|$ está determinado por el comportamiento de q en K_p:*

1. *Si q es inerte en K_p: $|\mathcal{R}(q, p)| = 0$. El primo q no divide ningún término a_k.*
2. *Si q es descompuesto en K_p: $|\mathcal{R}(q, p)| = 2$. El primo q divide exactamente dos clases de términos a_k por período de longitud q.*
3. *Si q es ramificado en K_p: $|\mathcal{R}(q, p)| = 1$. El primo q divide exactamente una clase de términos a_k por período de longitud q.*

Demostración. La condición $q \mid a_k$ equivale a $f_p(k) \equiv 0 \pmod{q}$, es decir, a

$$k^2 + k + p \equiv 0 \pmod{q}.$$

Completando el cuadrado,

$$(2k+1)^2 \equiv 1 - 4p = D \pmod{q}.$$

Caso q impar, $q \nmid D$: La ecuación $(2k+1)^2 \equiv D \pmod{q}$ tiene solución si y solo si D es residuo cuadrático módulo q, es decir, si y solo si $(D/q) = +1$. Si $(D/q) = +1$ (caso descompuesto): hay exactamente dos raíces cuadradas de D módulo q, dando dos valores distintos de $2k+1$ y por tanto dos valores de k en $\{0, \ldots, q-1\}$. Si $(D/q) = -1$ (caso inerte): no hay raíces cuadradas de D módulo q, y la ecuación no tiene solución.
Caso $q \mid D$: La ecuación se reduce a $(2k+1)^2 \equiv 0 \pmod{q}$, con solución única $k \equiv (q-1)/2 \pmod{q}$.
Caso $q = 2$: Si $p > 2$ es impar, $k^2 + k = k(k+1)$ es siempre par, luego $f_p(k) \equiv p \equiv 1 \pmod{2}$. Por tanto 2 no divide ningún a_k, es decir, $|\mathcal{R}(2,p)| = 0$. Esto es consistente con que $D = 1 - 4p \equiv 5 \pmod{8}$ para todo primo impar p, y $D \equiv 5 \pmod{8}$ implica que 2 es inerte en K_p [5]. □

Corolario 1 (Fórmula explícita de las raíces)**.** *Sea q un primo impar y p un primo con $q \nmid D$.*

- *Si q es descompuesto y r es una raíz cuadrada de D módulo q (con $1 \le r \le q-1$), entonces*

$$\mathcal{R}(q,p) = \left\{ \frac{r-1}{2} \bmod q, \quad \frac{-r-1}{2} \bmod q \right\},$$

  donde las divisiones son módulo q.

- *Si q es ramificado ($q \mid D$), entonces*

$$\mathcal{R}(q,p) = \left\{ \frac{q-1}{2} \right\}.$$

Demostración. Las dos expresiones se obtienen despejando k de $(2k+1) \equiv \pm r \pmod{q}$ y de $(2k+1) \equiv 0 \pmod{q}$, respectivamente. □

Observación 1 (El propio p siempre es descompuesto)**.** *Para todo primo $p > 2$, el propio p es descompuesto en K_p. En efecto, $D = 1 - 4p \equiv 1 \pmod{p}$, y 1 es siempre un residuo cuadrático, luego $(D/p) = +1$. Las dos raíces de f_p módulo p son $k \equiv 0 \pmod{p}$ y $k \equiv p-1 \pmod{p}$. La primera da $a_0 = p$ (primo), y la segunda da $a_{p-1} = p + (p-1)p = p^2$ (compuesto): estos son precisamente el inicio del tramo y el primer compuesto de la cola.*

Corolario 2 (Los primos inertes no interfieren)**.** *Si q es inerte en K_p, entonces q no divide ningún término $a_k = p + k(k+1)$ para ningún $k \ge 0$. En particular, los primos inertes no pueden causar la ruptura del tramo inicial.*

4. El primo responsable de la ruptura

El Corolario 2 establece que los primos inertes no pueden causar la ruptura del tramo. Esta sección identifica exactamente qué primo la causa y con qué mecanismo.

Definición 4 (Primo responsable)**.** *Sea p un primo con $\ell(p) \geq 1$. Se llama* primo responsable de la ruptura *al menor factor primo de $a_{\ell(p)}$. Se denota $q^*(p)$.*

Dado que $a_{\ell(p)}$ es compuesto por definición de $\ell(p)$, el primo $q^*(p)$ existe y satisface $q^*(p) < a_{\ell(p)}$.

Teorema 3 (Caracterización del primo responsable)**.** *Sea p un primo y $q^*(p)$ el primo responsable de la ruptura. Entonces:*

1. *$q^*(p)$ es split o ramificado en K_p.*
2. *$\ell(p) \in \mathcal{R}(q^*(p), p)$, es decir, $\ell(p)$ es una raíz de f_p módulo $q^*(p)$.*
3. *Ningún primo $q < a_k$ divide a_k para $k < \ell(p)$, salvo que $a_k = q$ (valor primo).*

Demostración. (1) $q^*(p) \mid a_{\ell(p)}$ significa que $\ell(p)$ es una raíz de f_p módulo $q^*(p)$, es decir, $\ell(p) \in \mathcal{R}(q^*(p), p)$. Por el Teorema 2, esto implica que $q^*(p)$ no es inerte; es por tanto split o ramificado.

(2) Se sigue directamente de la definición de $\mathcal{R}$.

(3) Para $k < \ell(p)$, a_k es primo por definición del tramo. Un primo $q < a_k$ que divide a_k satisfaría necesariamente $a_k = q$ (el único divisor propio de un primo es él mismo). □

Observación 2 (Dos mecanismos de ruptura)**.** *Según el tipo de $q^*(p)$ en K_p, la ruptura puede producirse por dos mecanismos distintos.*
Ruptura por primo ramificado. *Si $q^*(p)$ es ramificado en K_p (es decir, $q^*(p) \mid D$), la raíz de f_p módulo $q^*(p)$ es única: $\mathcal{R}(q^*(p), p) = \{(q^*(p) - 1)/2\}$. La ruptura ocurre exactamente en $\ell(p) = (q^*(p) - 1)/2$.*
Ruptura por primo descompuesto. *Si $q^*(p)$ es descompuesto en K_p, $\mathcal{R}(q^*(p), p) = \{r_1, r_2\}$ con dos raíces. La ruptura ocurre en la menor de las dos raíces que cae en el tramo, es decir, en $\ell(p) = \min(r_1, r_2)$ sujeto a que $a_{\ell(p)}$ sea compuesto.*

4.1. El caso $p \equiv 1 \pmod 3$

El caso más frecuente admite una descripción completamente explícita, que unifica la Proposición 6.1 de [2] con la teoría de campos.

Proposición 2 (Ruptura por $q = 3$ para $p \equiv 1 \pmod 3$)**.** *Sea $p > 3$ un primo con $p \equiv 1 \pmod 3$. Entonces $q = 3$ es ramificado en K_p, con raíz $k = 1$, y $\ell(p) = 1$.*

Demostración. $D = 1 - 4p \equiv 1 - p \pmod 3$. Para $p \equiv 1 \pmod 3$: $D \equiv 0 \pmod 3$, luego $3 \mid D$ y $q = 3$ es ramificado. Por el Corolario 1, la raíz única de f_p módulo 3 es $k = (3 - 1)/2 = 1$. Por tanto $3 \mid a_1 = p + 2$. Como $a_1 = p + 2 > 3$ (pues $p > 1$), a_1 es compuesto y $\ell(p) = 1$. □

4.2. El caso de primos gemelos

Para los primos $p \equiv 2 \pmod 3$, el primo $q = 3$ es inerte y nunca rompe el tramo. Si además $(p, p+2)$ es un par de primos gemelos ($\ell(p) \geq 2$), la ruptura es causada por el siguiente primo pequeño cuya raíz modular cae en $k = 2$. La siguiente tabla ilustra los mecanismos:

p	$a_2 = p+6$	$q^*(p)$	tipo en K_p	$\mathcal{R}(q^*, p)$
29	35	5	ramificado	$\{2\}$
59	65	5	ramificado	$\{2\}$
71	77	7	descompuesto	$\{2, 4\}$
137	143	11	descompuesto	$\{2, 8\}$
149	155	5	ramificado	$\{2\}$

En todos los casos $\ell(p) = 2$ coincide con la raíz mínima de $q^*(p)$ dentro del tramo.

5. Reformulación constructiva del teorema de Rabinowitsch

Esta sección formula y demuestra el resultado central del paper.

5.1. La desigualdad clave

El análisis descansa sobre una observación elemental pero decisiva.

Lema 1 (Cota inferior de la sucesión (a_k))**.** *Para todo primo p y todo $k \geq 0$,*

$$a_k = p + k(k+1) \geq p.$$

En particular, si $q < p$ es un primo que divide a_k, entonces $a_k > q$ y a_k es compuesto.

Demostración. $k(k+1) \geq 0$ para todo $k \geq 0$, luego $a_k \geq p$. Si $q < p \leq a_k$ y $q \mid a_k$, entonces q es un divisor propio de a_k, y por tanto a_k es compuesto. □

5.2. El teorema central

Teorema 4 (Equivalencia elemental)**.** *Sea $p > 2$ un primo y $D = 1 - 4p$. Las siguientes afirmaciones son equivalentes:*

1. *$\ell(p) = p - 1$.*
2. *Todos los primos $q < p$ son inertes en $K_p = \mathbb{Q}(\sqrt{D})$.*

Ambas son además equivalentes a $h(D) = 1$ (teorema de Rabinowitsch [3] y clasificación de Stark [4]), pero esta última equivalencia no se demuestra aquí.

Demostración. (1) $\Rightarrow$ (2)**:** Supóngase $\ell(p) = p-1$, es decir, $a_0, a_1, \ldots, a_{p-2}$ son todos primos. Sea $q < p$ un primo. Si q no fuera inerte, existiría una raíz $k^* \in \mathcal{R}(q,p)$ con $0 \le k^* \le q-1 < p-1$. Entonces $q \mid a_{k^*}$ y, por el Lema 1, $a_{k^*} \ge p > q$, luego a_{k^*} sería compuesto. Esto contradice la primalidad del tramo. Por tanto q es inerte.

(2) $\Rightarrow$ (1)**:** Supóngase que todos los primos $q < p$ son inertes en K_p. Por el Corolario 2, ningún $q < p$ divide ningún a_k. Sea $0 \le k \le p-2$. Todos los factores primos de a_k son entonces $\ge p$. Pero

$$a_k = p + k(k+1) \le a_{p-2} = p^2 - 2p + 2 < p^2,$$

luego $a_k < p^2$. Si a_k tuviera dos factores primos $q_1, q_2 \ge p$, se tendría $a_k \ge q_1 q_2 \ge p^2$, contradicción. Por tanto a_k tiene exactamente un factor primo, es decir, a_k es primo. Esto se cumple para todo $k \le p-2$, luego $\ell(p) = p-1$. □

Observación 3 (Sobre la equivalencia con $h(D) = 1$)**.** *La equivalencia entre (1) y $h(D) = 1$ es el contenido del teorema de Rabinowitsch. Combinada con el teorema clásico de Rabinowitsch, la equivalencia anterior sitúa la condición de inercia total de los primos $q < p$ dentro del marco del número de clase $h(D) = 1$ [3, 4]. Conviene precisar que $h(D) = 1$ debe entenderse aquí como "$D = 1 - 4p$ es un discriminante de Heegner", es decir, un discriminante fundamental con número de clase 1. Para los primos p con $D = 1-4p$ no fundamental (por ejemplo $p = 7$, donde $D = -27 = -3 \times 3^2$), el campo $\mathbb{Q}(\sqrt{D_{fund}})$ puede tener número de clase 1 y aun así existir primos no inertes menores que p; ese fenómeno, ligado al conductor del orden $\mathbb{Z}[(1+\sqrt{D})/2]$, queda fuera del alcance de este trabajo. Este paper no necesita ni reproduce esas pruebas: los resultados sobre el primo responsable y la fórmula para $\ell(p)$ se deducen directamente de la equivalencia (1) $\leftrightarrow$ (2) demostrada aquí.*

5.3. El contrarrecíproco: existencia del primo responsable

Corolario 3 (El primo responsable existe y es menor que p)**.** *Sea p un primo ordinario, es decir, $\ell(p) < p-1$. Entonces el primo responsable $q^*(p)$ satisface $q^*(p) < p$, es split o ramificado en K_p, y $\ell(p) \in \mathcal{R}(q^*(p), p)$.*

Demostración. Como $a_{\ell(p)}$ es compuesto por definición, tiene un factor primo $q^* = q^*(p)$. Como $a_{\ell(p)} \ge p$ (Lema 1) y $q^* \mid a_{\ell(p)}$, el valor $a_{\ell(p)} > q^*$. Por el Teorema 2, q^* no es inerte (pues $q^* \mid a_{\ell(p)}$ implica $\ell(p) \in \mathcal{R}(q^*, p)$ y el conjunto de raíces es no vacío). Por tanto q^* es split o ramificado, y $\ell(p) \in \mathcal{R}(q^*, p)$.

Queda por mostrar que $q^* < p$. Por el Teorema 4, como p es ordinario, existe un primo $q < p$ no inerte en K_p. Su raíz mínima $k_0 = \min \mathcal{R}(q,p) \le q-1 < p-1$ satisface $q \mid a_{k_0}$. Si $k_0 < \ell(p)$, entonces $q \mid a_{k_0}$ con $a_{k_0} \ge p > q$ haría a_{k_0} compuesto, contradiciendo la primalidad del tramo. Por tanto $k_0 \ge \ell(p)$. Ahora bien, $k_0 = \ell(p)$ implica $q \mid a_{\ell(p)}$, luego $q \ge q^*$ (por ser q^* el menor factor de $a_{\ell(p)}$). Si $k_0 > \ell(p)$ para todo primo $q < p$ no inerte, entonces ningún primo $< p$ divide $a_{\ell(p)}$; pero entonces todos los factores de $a_{\ell(p)}$ serían $\ge p$, y por $a_{\ell(p)} < p^2$, $a_{\ell(p)}$ sería primo, contradiciendo que es compuesto. Por tanto algún primo $q < p$ divide $a_{\ell(p)}$, y $q^* \le q < p$. □

6. Verificación para los casos afortunados y ordinarios

Esta sección ilustra los teoremas de las secciones anteriores mediante ejemplos explícitos.

6.1. Los casos afortunados

Para los primos afortunados, el Teorema 4 predice que todos los primos $q < p$ son inertes en K_p. La siguiente tabla confirma esto para $p \in \{5, 11, 17, 41\}$:

p	$D = 1 - 4p$	primos $q < p$	todos inertes	$\ell(p)$
5	-19	$2, 3$	sí	4
11	-43	$2, 3, 5, 7$	sí	10
17	-67	$2, 3, 5, 7, 11, 13$	sí	16
41	-163	$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$	sí	40

En todos los casos, el único primo descompuesto pequeño es el propio p, con raíces $k = 0$ (da $a_0 = p$, primo) y $k = p - 1$ (da $a_{p-1} = p^2$, inicio de la cola).

6.2. El caso $p = 41$ en detalle

Para $p = 41$, $D = -163$ (primo), los doce primos $q < 41$ son todos inertes:

$$q \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37\} \;\Rightarrow\; \left(\frac{-163}{q}\right) = -1.$$

Por el Teorema 4, el tramo inicial tiene longitud $\ell(41) = 40 = p - 1$: los cuarenta valores $a_0 = 41, a_1 = 43, \ldots, a_{39} = 1601$ son todos primos.

El primer primo no inerte tras el tramo es el propio $q = 41$ (descompuesto, raíces $k = 0$ y $k = 40$) y el primo ramificado $q = 163 = |D|$, con raíz única $k = (163 - 1)/2 = 81 = 2p - 1$. Este último da el compuesto centinela:

$$a_{81} = f_{41}(81) = 6683 = 41 \times 163 = p \cdot |\Delta|,$$

en perfecta consistencia con el compuesto centinela demostrado en [1].

6.3. Los casos ordinarios

La siguiente tabla recoge el primo responsable $q^*(p)$, su tipo en K_p, sus raíces modulares y el valor compuesto $a_{\ell(p)}$ para una selección de primos ordinarios:

p	$\ell(p)$	$q^*(p)$	tipo en K_p	$\mathcal{R}(q^*,p)$	$a_{\ell(p)}$
7	1	3	ramificado	$\{1\}$	$9 = 3^2$
13	1	3	ramificado	$\{1\}$	$15 = 3 \times 5$
19	1	3	ramificado	$\{1\}$	$21 = 3 \times 7$
23	1	5	descompuesto	$\{1,3\}$	$25 = 5^2$
29	2	5	ramificado	$\{2\}$	$35 = 5 \times 7$
43	1	3	ramificado	$\{1\}$	$45 = 3^2 \times 5$
59	2	5	ramificado	$\{2\}$	$65 = 5 \times 13$
71	2	7	descompuesto	$\{2,4\}$	$77 = 7 \times 11$
83	1	5	descompuesto	$\{1,3\}$	$85 = 5 \times 17$
101	4	11	descompuesto	$\{4,6\}$	$121 = 11^2$
107	3	7	ramificado	$\{3\}$	$119 = 7 \times 17$

En cada caso, $\ell(p)$ coincide con la raíz mínima de $q^*(p)$ dentro del tramo, y $q^*(p) < p$ en todos los casos, confirmando el Corolario 3.

6.4. Ejemplo detallado: $p = 101$

Para ilustrar la teoría en un caso con $\ell(p) > 2$, se desarrolla completamente el caso $p = 101$:

- $D = 1 - 4 \times 101 = -403 = -(13 \times 31)$. Los primos 13 y 31 son ramificados en K_{101}.
- El primo $q = 11$: $D = -403 \equiv -403 + 37 \times 11 = 4 \pmod{11}$. Como $(4/11) = (2^2/11) = 1$, el primo 11 es descompuesto. Sus raíces modulares son: $\mathcal{R}(11, 101) = \{4, 6\}$, pues $f_{101}(4) = 16 + 4 + 101 = 121 = 11^2$ y $f_{101}(6) = 36 + 6 + 101 = 143 = 11 \times 13$.
- El primo $q = 13$ (ramificado): raíz única $k = (13 - 1)/2 = 6$. Pero $\min \mathcal{R}(11, 101) = 4 < 6$, así que 11 gana.
- Ningún primo $q < 11$ divide ningún a_k para $k < 4$: $a_0 = 101$, $a_1 = 103$, $a_2 = 107$, $a_3 = 113$ (todos primos).
- Por tanto $q^*(101) = 11$ (descompuesto), $\ell(101) = \min\{4, 6\} = 4$, y $a_4 = 121 = 11^2$ es el primer compuesto del tramo.

Observación 4 (El centinela en los casos ordinarios)**.** *Para todo primo p, el primo $q = 4p - 1$ es ramificado (pues $q \mid D = 1 - 4p$), con raíz única $k = (4p - 1 - 1)/2 = 2p - 1$. Este da el compuesto centinela $a_{2p-1} = p \cdot (4p - 1)$, demostrado en [1, 2]. Para los primos ordinarios, el centinela se encuentra mucho más allá del fin del tramo: el tramo termina en $k = \ell(p)$ por el primo $q^*(p) < p$, mientras que el centinela espera en $k = 2p - 1 \gg \ell(p)$.*

7. Fórmula explícita para $\ell(p)$

Los resultados de las secciones anteriores permiten calcular $\ell(p)$ de forma completamente explícita.

Teorema 5 (Fórmula unificada para $\ell(p)$)**.** *Sea p un primo ordinario y $q^*(p)$ el primo responsable. Entonces*

$$\ell(p) = \min \mathcal{R}(q^*(p),\, p).$$

En el caso ramificado, $|\mathcal{R}(q^*, p)| = 1$ y la fórmula se simplifica:

$$q^*(p) \text{ ramificado} \implies \ell(p) = \frac{q^*(p) - 1}{2}.$$

Demostración. Por el Teorema 3, $q^*(p) \mid a_{\ell(p)}$, luego $\ell(p) \in \mathcal{R}(q^*(p), p)$.

Si q^* es ramificado, $\mathcal{R}(q^*, p) = \{(q^* - 1)/2\}$ por el Corolario 1, y por tanto $\ell(p) = (q^* - 1)/2$.

Si q^* es descompuesto, $\mathcal{R}(q^*, p) = \{r_1, r_2\}$ con $r_1 < r_2$. Como $\ell(p) \in \{r_1, r_2\}$, si fuera $\ell(p) = r_2 > r_1$, entonces $r_1 < \ell(p)$ y $q^* \mid a_{r_1}$. Por el Lema 1, $a_{r_1} \geq p > q^*$, luego a_{r_1} sería compuesto, contradiciendo la primalidad del tramo. Por tanto $\ell(p) = r_1 = \min \mathcal{R}(q^*, p)$. □

Corolario 4 (Fórmula explícita en el caso ramificado)**.** *Si el primo responsable $q^*(p)$ es ramificado en K_p (es decir, $q^*(p) \mid 4p - 1$), entonces*

$$q^*(p) = \min\bigl\{q \text{ primo} : q \mid (4p - 1),\ q < p\bigr\}$$

y

$$\ell(p) = \frac{q^*(p) - 1}{2}.$$

Demostración. Todo primo $q \mid D = 1 - 4p$ es ramificado en K_p (Proposición 1). Si q^* es ramificado, es el menor factor primo de $a_{\ell(p)}$. Por la fórmula de la raíz única, $a_{(q^*-1)/2}$ es divisible por q^*. Ningún primo ramificado $q' < q^*$ con $q' \mid (4p-1)$ podría existir: si existiera, su raíz $(q' - 1)/2 < (q^* - 1)/2 = \ell(p)$ caería dentro del tramo y haría $a_{(q'-1)/2}$ compuesto, contradiciendo el tramo. Por tanto q^* es el menor factor primo de $4p - 1$ que es menor que p. □

7.1. Los dos casos según la factorización de $4p - 1$

La fórmula adopta formas especialmente limpias según la estructura de $4p - 1$:

Caso A: $4p - 1$ **tiene un factor primo** $q < p$**.** El primo q es ramificado, $q^*(p) = \min\{q \mid 4p - 1, q < p\}$ y

$$\ell(p) = \frac{q^*(p) - 1}{2}.$$

Caso B: $4p-1$ **es primo o todos sus factores son** $\geq p$**.** No hay primos ramificados menores que p. El primo responsable es split, y

$$\ell(p) = \min \mathcal{R}(q^*(p),\, p)$$

donde $q^*(p)$ es el primo split con raíz mínima más pequeña.

La siguiente tabla ilustra ambos casos:

p	$4p-1$	factores	q^*	tipo	$\ell(p)$
7	27	3^3	3	ramif.	$(3-1)/2 = 1$
29	115	5×23	5	ramif.	$(5-1)/2 = 2$
107	427	7×61	7	ramif.	$(7-1)/2 = 3$
149	595	$5 \times 7 \times 17$	5	ramif.	$(5-1)/2 = 2$
71	283	283 (primo)	7	split	$\min\{2,4\} = 2$
83	331	331 (primo)	5	split	$\min\{1,3\} = 1$
101	403	13×31	11	split	$\min\{4,6\} = 4$
227	907	907 (primo)	13	split	$\min\{4,8\} = 4$

Observación 5 (Predominio del caso ramificado)**.** *Para los primos ordinarios $p < 1000$, el caso A (primo responsable ramificado) representa aproximadamente el 64 % de los casos. El caso B ocurre cuando $4p-1$ es primo o cuando sus factores primos son todos $\geq p$; en ese caso el primo responsable es siempre split, y no hay fórmula cerrada comparable para $\ell(p)$ (se requiere calcular la raíz cuadrada de $D = 1-4p$ módulo q^*, que no admite expresión algebraica general).*

8. Conclusión

Este trabajo cierra la trilogía sobre los polinomios cuadráticos $f_p(n) = n^2+n+p$ estableciendo la conexión entre la longitud del tramo inicial y la aritmética del campo cuadrático $K_p = \mathbb{Q}(\sqrt{1-4p})$.

Resultados demostrados. El Teorema 2 establece la tricotomía exacta entre el comportamiento de un primo q en K_p y el número de raíces de f_p módulo q. Esta tricotomía, junto con las cotas elementales $a_k \geq p$ y $a_k < p^2$ para $k < p-1$, constituye el fundamento de toda la teoría.

El Teorema 4 prueba elementalmente que $\ell(p) = p-1$ si y solo si todos los primos $q < p$ son inertes en K_p, sin necesidad de usar la teoría de ideales. El Corolario 3 identifica el primo responsable $q^*(p)$ y prueba que siempre satisface $q^*(p) < p$. El Teorema 5 da la fórmula explícita $\ell(p) = \min \mathcal{R}(q^*(p), p)$, que en el caso ramificado se simplifica a $\ell(p) = (q^*(p)-1)/2$.

La trilogía completa. Los tres trabajos de la serie construyen un cuadro coherente:

Paper	Objeto central	Resultado principal
[1]	Cola de los casos afortunados	Estructura cuadrática, centinela $p \cdot \lvert\Delta\rvert$
[2]	Constelaciones y caso general	$f_p(k) = a_k$, clasificación de $\ell(p)$
Este	Descomposición en K_p	Fórmula para $\ell(p)$, equivalencia con Rabinowitsch

El hilo conductor es la sucesión $a_k = p + k(k+1)$: en el primer paper organiza la cola; en el segundo identifica el tramo con una constelación de primos; en este tercero revela que su divisibilidad por primos queda descrita de forma exacta en términos de la aritmética de K_p.

Limitaciones y direcciones abiertas. La equivalencia entre la inercia de todos los $q < p$ y el número de clase $h(D) = 1$ no se demuestra aquí: se cita de Rabinowitsch y de la teoría estándar de campos cuadráticos.

Para el caso split (Caso B de la §7), la fórmula $\ell(p) = \min \mathcal{R}(q^*, p)$ requiere calcular la raíz cuadrada de D módulo q^*, que no admite expresión algebraica cerrada general. Mollin [6] estudió el caso $h(D) = 2$ con métodos análogos y obtuvo resultados similares; extender su análisis al marco de este paper queda como dirección abierta.

Referencias

[1] M. Cerdá Bennassar, *Estructura cuadrática de los compuestos y bloques de primos en polinomios de Euler*, preprint, 2025.

[2] M. Cerdá Bennassar, *Estructura de los polinomios cuadráticos $n^2 + n + p$: constelaciones de primos y compuesto centinela*, preprint, 2025.

[3] G. Rabinowitz, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern*, Proc. Fifth Int. Congress Math., Cambridge, 1913, pp. 418–421.

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

[5] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1990, cap. 5–6.

[6] R. A. Mollin, *Quadratic Polynomials Producing Consecutive Distinct Primes and Class Groups of Complex Quadratic Fields*, Acta Arith. **74** (1996), 17–30.