

El tramo inicial de primos de los polinomios $n^2 + n + p$

Miguel Cerdá Bennassar

Abril de 2026 (revisado en octubre de 2026)

Resumen

Para un primo p , sea $f_p(n) = n^2 + n + p$ y sea $\ell(p)$ el número de valores $f_p(0), f_p(1), \dots$ que son primos antes del primer valor compuesto. Se dan dos descripciones de $\ell(p)$. La primera la expresa mediante los restos de p módulo los primos $q < p$: el primo q divide $f_p(j)$ si y solo si $p \equiv -j(j+1) \pmod{q}$, y $\ell(p)$ es el menor j para el que esto ocurre con algún $q < p$. Esta descripción se lee en el cuerpo $\mathbb{Q}(\sqrt{1-4p})$ según que q sea inerte, ramificado o descompuesto. La segunda expresa $\ell(p)$ mediante las formas cuadráticas reducidas de discriminante $1-4p$, y conduce, por el argumento clásico, al teorema de Rabinowitsch sobre los seis primos con $\ell(p) = p-1$. Se incluyen datos sobre los discriminantes no fundamentales y una observación sobre la predicción de Hardy y Littlewood para los primos con tramo inicial largo.

1. Introducción

Euler observó que $n^2 + n + 41$ es primo para $n = 0, 1, \dots, 39$. Para un primo p , el polinomio $f_p(n) = n^2 + n + p$ cumple $f_p(p-1) = p^2$, de modo que a lo sumo sus $p-1$ primeros valores pueden ser primos. El teorema de Rabinowitsch [6] caracteriza los primos para los que esto ocurre: son aquellos para los que $4p-1$ es un número de Heegner, es decir, un entero d libre de cuadrados tal que $\mathbb{Q}(\sqrt{-d})$ tiene número de clase 1. Por los trabajos de Heegner [4] y Stark [8], esos primos son exactamente 2, 3, 5, 11, 17, 41. Una exposición detallada de estos resultados se encuentra en [7].

Para los demás primos, el tramo inicial de valores primos es más corto, y en este escrito se estudia su longitud $\ell(p)$ para un primo cualquiera. La sección 3 reduce el problema a los primos $q < p$ y lo expresa mediante congruencias explícitas. La sección 4 interpreta esas congruencias en el cuerpo cuadrático $\mathbb{Q}(\sqrt{1-4p})$ y recoge datos sobre el papel de los factores de $4p-1$. La sección 5 expresa $\ell(p)$ mediante las formas cuadráticas reducidas de discriminante $1-4p$ y obtiene de ahí el teorema de Rabinowitsch. La sección 6 reúne ejemplos, y la sección 7 relaciona los primos con tramo inicial largo con la conjetura de las k -uplas de primos. La estructura de los valores de f_p después del tramo inicial, en el caso de los seis primos de Rabinowitsch, se estudia en otro escrito [2].

2. Notación

Sea p un primo. Escribimos

$$f_p(n) = n^2 + n + p, \quad a_k = f_p(k) = p + k(k+1) \quad (k \geq 0), \quad D = 1 - 4p.$$

La sucesión $a_0 = p, a_1 = p + 2, a_2 = p + 6, a_3 = p + 12, \dots$ es creciente, con $a_k \geq p$ para todo k .

Definición 1. Se llama tramo inicial de f_p al mayor segmento $a_0, a_1, \dots, a_{\ell-1}$ formado por primos. Su longitud se denota $\ell(p)$; así, $a_{\ell(p)}$ es el primer valor compuesto.

Como $a_{p-1} = p^2$, se tiene $\ell(p) \leq p - 1$. Si $\ell(p) < p - 1$, el menor factor primo de $a_{\ell(p)}$ se denota $q^*(p)$.

Usaremos dos identidades elementales:

$$a_n - a_m = (n - m)(n + m + 1), \quad 4a_k = (2k + 1)^2 - D. \quad (1)$$

La primera muestra que si un primo q divide a_m , también divide a_n para todo $n \equiv m$ y todo $n \equiv -1 - m \pmod{q}$. En particular, las posiciones $k \geq 0$ con $q \mid a_k$, si existen, forman a lo sumo dos clases módulo q , simétricas respecto de $(q - 1)/2$, y la menor de ellas es como máximo $(q - 1)/2$. Denotamos por $r(q, p)$ esa menor posición, y escribimos $r(q, p) = \infty$ si q no divide ningún a_k .

3. Reducción a los primos menores que p

Lema 1. Para $0 \leq k \leq p - 2$, el valor a_k es compuesto si y solo si lo divide algún primo $q < p$.

Demostración. Se tiene $p \leq a_k \leq p + (p - 2)(p - 1) < p^2$. Si a_k es compuesto, su menor factor primo q cumple $q^2 \leq a_k < p^2$, luego $q < p$. Recíprocamente, si $q < p$ divide a_k , como $a_k \geq p > q$, el valor a_k es compuesto. $\square$

Teorema 1. Para todo primo p ,

$$\ell(p) = \min\left(\{p - 1\} \cup \{r(q, p) : q < p \text{ primo}\}\right).$$

Si $\ell(p) < p - 1$, entonces $q^*(p) < p$ y $\ell(p) = r(q^*(p), p)$.

Demostración. Por el lema 1, para $k \leq p - 2$ el valor a_k es compuesto exactamente cuando k es una posición r con $q \mid a_r$ para algún primo $q < p$; la menor de esas posiciones es el mínimo de los $r(q, p)$. Si ninguna es menor que $p - 1$, el primer compuesto es $a_{p-1} = p^2$. La segunda afirmación es la primera parte de la demostración del lema 1 aplicada a $k = \ell(p)$, junto con el hecho de que ninguna posición anterior a $\ell(p)$ es divisible por $q^*(p)$. $\square$

La condición de divisibilidad es una congruencia explícita sobre p :

$$q \mid a_j \iff p \equiv -j(j + 1) \pmod{q}. \quad (2)$$

Proposición 1. Sea q un primo y, para $0 \leq j \leq (q-1)/2$, sea $c_j(q) = -j(j+1) \pmod{q}$. Los $\lfloor (q+1)/2 \rfloor$ valores $c_j(q)$ son distintos, y

$$r(q, p) = j \iff p \equiv c_j(q) \pmod{q}.$$

Si $p \pmod{q}$ no es ninguno de ellos, q no divide ningún valor de f_p .

Demostración. Por la primera identidad de (1), $c_i(q) \equiv c_j(q)$ equivale a $(j-i)(i+j+1) \equiv 0 \pmod{q}$. Para $0 \leq i < j \leq (q-1)/2$ se tiene $0 < j-i < q$ y $0 < i+j+1 \leq q-1$, luego los valores son distintos. Si $p \equiv c_j(q)$, entonces $q \mid a_j$ por (2), y ninguna posición menor es raíz, pues daría otro valor $c_i(q)$ igual a $p \pmod{q}$. Por último, la menor raíz, si existe, es como máximo $(q-1)/2$. $\square$

La tabla siguiente da los valores $c_j(q)$ para los primeros primos impares. Si $p \equiv c_j(q) \pmod{q}$, el primo q divide a_j y es la primera posición en que lo hace.

j	$c_j(3)$	$c_j(5)$	$c_j(7)$	$c_j(11)$	$c_j(13)$	$c_j(17)$
0	0	0	0	0	0	0
1	1	3	5	9	11	15
2		4	1	5	7	11
3			2	10	1	5
4				2	6	14
5				3	9	4
6					10	9
7						12
8						13

La fila $j = 0$ corresponde a $q \mid p$ y no interviene cuando $q < p$. La fila $j = 1$ es $c_1(q) = q - 2$, es decir, $q \mid p + 2$; como $p + 2$, si es compuesto, tiene un factor primo menor que p , se obtiene que $\ell(p) \geq 2$ si y solo si $p + 2$ es primo. Con $q = 3$, la condición $p \equiv 1 \pmod{3}$ con $p > 3$ da $\ell(p) = 1$. El valor de la última fila de cada columna es $c_{(q-1)/2}(q) \equiv 4^{-1} \pmod{q}$, que corresponde a $q \mid 4p - 1$, como se verá en la sección siguiente.

Reuniendo el teorema 1 y la proposición 1:

Corolario 1. $\ell(p)$ es el menor entero $j \geq 1$ tal que $p \equiv -j(j+1) \pmod{q}$ para algún primo $q < p$ con $j \leq (q-1)/2$, o bien $p-1$ si no existe tal j . En particular, $\ell(p)$ depende solo de los restos de p módulo los primos menores que p .

En la práctica, sin embargo, determinar $\ell(p)$ a partir de este corolario no es más sencillo que buscar directamente el primer valor compuesto de la sucesión.

4. Lectura en el cuerpo cuadrático

Sea $K_p = \mathbb{Q}(\sqrt{D})$, con $D = 1 - 4p$. Para p impar se tiene $D \equiv 5 \pmod{8}$ y todos los a_k son impares, de modo que $q = 2$ no interviene. Para q impar, la segunda identidad de (1) da

$$q \mid a_k \iff (2k+1)^2 \equiv D \pmod{q},$$

y se obtienen tres casos, según la descomposición de q en K_p [5]. Si D no es un resto cuadrático módulo q (q inerte), q no divide ningún a_k . Si $q \mid D$ (q ramificado), la única clase de raíces es $2k + 1 \equiv 0$, es decir, $r(q, p) = (q - 1)/2$; es la última fila de la tabla anterior. Si D es un resto cuadrático no nulo (q descompuesto), hay dos clases de raíces, j y $q - 1 - j$, con $j < (q - 1)/2$. Con esta lectura, el teorema 1 toma la forma siguiente.

Corolario 2. Sea p un primo con $\ell(p) < p - 1$, y sean

$$\begin{aligned}\mathcal{A}(p) &= \{(q - 1)/2 : q < p \text{ primo}, q \mid D\}, \\ \mathcal{B}(p) &= \{r(q, p) : q < p \text{ primo descompuesto en } K_p\}.\end{aligned}$$

Entonces $\ell(p) = \min(\mathcal{A}(p) \cup \mathcal{B}(p))$. Además, $\ell(p) = p - 1$ si y solo si todos los primos $q < p$ son inertes en K_p .

La última afirmación es la parte elemental de las demostraciones del teorema de Rabinowitsch [7].

Observación 1 (El menor factor de $4p - 1$). Sea q_D el menor factor primo de $4p - 1$. Si $4p - 1$ es compuesto, $q_D \leq \sqrt{4p - 1} < p$ para $p \geq 5$, y por el corolario 2,

$$\ell(p) \leq \frac{q_D - 1}{2}.$$

La igualdad se da cuando $q^*(p)$ es ramificado; en otro caso, el tramo lo corta antes un primo descompuesto. Entre los 162 primos $p < 1000$ con $\ell(p) < p - 1$, el primo $q^*(p)$ divide a $4p - 1$ en 95 casos.

Observación 2 (Discriminantes no fundamentales). Como $D \equiv 1 \pmod{4}$, el discriminante D es fundamental si y solo si $4p - 1$ es libre de cuadrados. Si $q^2 \mid 4p - 1$ para algún primo q , el anillo $\mathbb{Z}[(1 + \sqrt{D})/2]$ es un orden no maximal de K_p , pero el cálculo anterior no depende de ello: todo factor primo de $4p - 1$, del discriminante del cuerpo o del conductor, produce la raíz $(q - 1)/2$. Hay 75 primos $p < 2000$ con $4p - 1$ no libre de cuadrados; en 70 de ellos $\ell(p) = (q_D - 1)/2$, y las excepciones son 233, 719, 1301, 1373 y 1409. Por ejemplo, para $p = 233$ se tiene $4p - 1 = 7^2 \cdot 19$, de modo que la cota es 3, pero $a_1 = 235 = 5 \cdot 47$ y $\ell(233) = 1$.

5. Formas cuadráticas reducidas

Una forma cuadrática binaria $ax^2 + bxy + cy^2$, que denotamos (a, b, c) , tiene discriminante $b^2 - 4ac$. Si este es negativo y $a > 0$, la forma es *reducida* cuando $|b| \leq a \leq c$, con $b \geq 0$ si $|b| = a$ o $a = c$. Toda forma definida positiva es equivalente a una única forma reducida, y el número de clase $h(D)$ es el número de formas reducidas primitivas de discriminante D [1].

Lema 2. Sea (a, b, c) una forma reducida de discriminante $D = 1 - 4p$. Entonces b es impar, $a \leq \sqrt{(4p - 1)/3}$ y

$$ac = a_k \quad \text{con } k = \frac{|b| - 1}{2}.$$

La única forma reducida con $a = 1$ es la forma principal $(1, 1, p)$.

Demostración. De $b^2 - 4ac = 1 - 4p$ se sigue que b es impar y $ac = (b^2 - 1)/4 + p = p + k(k+1)$. De $|b| \leq a \leq c$ se obtiene $4p - 1 = 4ac - b^2 \geq 3a^2$. Si $a = 1$, entonces $|b| \leq 1$, luego $b = 1$ y $c = p$. $\square$

Teorema 2. *Sea p un primo. Si existen formas reducidas de discriminante $1 - 4p$ distintas de la principal, entonces*

$$\ell(p) = \min \left\{ \frac{|b|-1}{2} : (a, b, c) \text{ reducida, } a \geq 2 \right\},$$

y $q^*(p)$ es el menor valor de a entre las formas reducidas con $|b| = 2\ell(p) + 1$. Si la única forma reducida es la principal, entonces $\ell(p) = p - 1$.

Demostración. Si (a, b, c) es reducida con $a \geq 2$, el lema 2 da $a_k = ac$ con $2 \leq a \leq c$, de modo que a_k es compuesto y $\ell(p) \leq k = (|b| - 1)/2$. Como además $k \leq (a - 1)/2 < p - 1$, la existencia de una tal forma implica $\ell(p) < p - 1$.

Recíprocamente, supongamos $\ell = \ell(p) < p - 1$ y sean $q = q^*(p)$ y $c' = a_\ell/q$. La forma $(q, 2\ell + 1, c')$ tiene discriminante $(2\ell + 1)^2 - 4a_\ell = 1 - 4p$. Por el teorema 1, $q < p$ y $\ell = r(q, p) \leq (q - 1)/2$, es decir, $2\ell + 1 \leq q$; y $c' \geq q$ porque a_ℓ es compuesto y q es su menor factor primo. Como $b = 2\ell + 1 > 0$, la forma es reducida, y da el valor ℓ en el mínimo. Cualquier otra forma reducida $(a, \pm(2\ell + 1), c)$ cumple $ac = a_\ell$ con $a \geq 2$, luego $a \geq q$. $\square$

En el teorema intervienen también las formas no primitivas. Si $g^2 \mid D$ con $g > 1$, la forma $(g, g, g(1 - D/g^2)/4)$ es reducida y no primitiva, pues $|D|/g^2 \geq 3$. Por tanto, la forma principal es la única forma reducida de discriminante D si y solo si D es fundamental y $h(D) = 1$. Con el teorema 2 se obtiene así el argumento clásico del teorema de Rabinowitsch [6, 7].

Corolario 3 (Rabinowitsch). $\ell(p) = p - 1$ si y solo si $4p - 1$ es libre de cuadrados y $h(1 - 4p) = 1$, es decir, si y solo si $4p - 1$ es un número de Heegner. Por la determinación de los cuerpos cuadráticos imaginarios de número de clase 1 [4, 8], esto ocurre exactamente para $p \in \{2, 3, 5, 11, 17, 41\}$.

Cuando D es fundamental y $h(D) = 2$ hay una única forma reducida no principal (a, b, c) , y el teorema 2 da directamente $\ell(p) = (|b| - 1)/2$ y $q^*(p) = a$. Así ocurre, por ejemplo, para $p = 13, 23, 29, 31, 47, 59, 67, 101, 107$; para $p = 101$, la forma $(11, 9, 11)$ da $\ell(101) = 4$ y $a_4 = 121 = 11 \cdot 11$.

6. Ejemplos

La tabla siguiente recoge seis primos que ilustran los distintos casos. En cada uno se indica la factorización de $4p - 1$, la longitud del tramo, el primer valor compuesto, el tipo de $q^*(p)$ en K_p , la congruencia que lo determina y las formas reducidas no principales que realizan el mínimo del teorema 2.

p	$4p - 1$	ℓ	a_ℓ	q^*	congruencia	forma
23	$7 \cdot 13$	1	$25 = 5^2$	5, desc.	$23 \equiv 3 = c_1(5)$	$(5, 3, 5)$
29	$5 \cdot 23$	2	$35 = 5 \cdot 7$	5, ram.	$29 \equiv 4 = c_2(5)$	$(5, 5, 7)$
71	283	2	$77 = 7 \cdot 11$	7, desc.	$71 \equiv 1 = c_2(7)$	$(7, \pm 5, 11)$
101	$13 \cdot 31$	4	$121 = 11^2$	11, desc.	$101 \equiv 2 = c_4(11)$	$(11, 9, 11)$
107	$7 \cdot 61$	3	$119 = 7 \cdot 17$	7, ram.	$107 \equiv 2 = c_3(7)$	$(7, 7, 17)$
227	907	4	$247 = 13 \cdot 19$	13, desc.	$227 \equiv 6 = c_4(13)$	$(13, \pm 9, 19)$

Para $p = 101$, los factores 13 y 31 de $4p - 1$ tienen raíces 6 y 15, de modo que el tramo lo corta antes el primo descompuesto 11, cuya menor raíz es 4. Para $p = 71$ y $p = 227$, el número $4p - 1$ es primo y mayor que p , de modo que el primo responsable es necesariamente descompuesto.

7. Tramos iniciales largos

Para $k \geq 1$ fijo, $\ell(p) \geq k$ significa que los k números

$$p, p + 2, p + 6, \dots, p + (k - 1)k$$

son todos primos. Este patrón es admisible en el sentido de Hardy y Littlewood [3]: para cada primo q , los valores $-j(j + 1)$ mód q con $0 \leq j < k$ son a lo sumo $\lfloor (q + 1)/2 \rfloor$, por la simetría $j \leftrightarrow -1 - j$, y por tanto queda siempre algún resto de p módulo q para el que ningún término es múltiplo de q . La conjetura de las k -uplas de primos predice entonces que, para cada k , hay infinitos primos p con $\ell(p) \geq k$. Para $k = 2$ es la conjetura de los primos gemelos. Ninguno de estos enunciados está demostrado para $k \geq 2$; ni siquiera se sabe que $\ell(p) \geq 2$ ocurra infinitas veces.

8. Conclusiones y cuestiones abiertas

La longitud $\ell(p)$ del tramo inicial de primos de $n^2 + n + p$ es el menor j para el que algún primo $q < p$ cumple $p \equiv -j(j + 1)$ (mód q). Esta descripción se lee en el cuerpo $\mathbb{Q}(\sqrt{1 - 4p})$, donde solo los primos ramificados y descompuestos pueden cortar el tramo, y equivale a otra en términos de las formas cuadráticas reducidas de discriminante $1 - 4p$: $\ell(p)$ es el menor valor de $(|b| - 1)/2$ entre las formas reducidas no principales, y el primo que corta el tramo es el primer coeficiente de la correspondiente. El caso extremo $\ell(p) = p - 1$ es el teorema de Rabinowitsch.

Quedan abiertas, entre otras, las cuestiones siguientes. La primera es la distribución de $\ell(p)$: la frecuencia de los primos con $\ell(p) \geq k$ entre los primos hasta x , para la que la conjetura de Hardy y Littlewood da una predicción asintótica que podría compararse con recuentos numéricos. La segunda es la frecuencia relativa de los dos mecanismos de ruptura, por un factor de $4p - 1$ o por un primo descompuesto, de la que solo se han dado aquí datos para $p < 1000$.

Referencias

- [1] D. A. Buell, *Binary Quadratic Forms: Classical Theory and Modern Computations*, Springer-Verlag, 1989.
- [2] M. Cerdá Bennassar, *Compuestos y bloques de primos en la cola de los polinomios de Euler afortunados*, <https://collatz.es>, 2026.
- [3] G. H. Hardy, J. E. Littlewood, *Some problems of ‘Partitio Numerorum’; III: On the expression of a number as a sum of primes*, Acta Math. **44** (1923), 1–70.
- [4] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227–253.

- [5] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, 2.^a ed., Springer-Verlag, 1990.
- [6] G. Rabinowitz, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern*, Proc. Fifth Int. Congress Math., Cambridge, 1913, pp. 418–421.
- [7] P. Ribenboim, *Euler's famous prime generating polynomial and the class number of imaginary quadratic fields*, L'Enseignement Math. **34** (1988), 23–42.
- [8] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. **14** (1967), 1–27.