UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN CIENCIAS MATEMÁTICAS Y DE LA ESPECIALIZACIÓN EN ESTADÍSTICA APLICADA

FUNCIONES DE CONTEO PARA DOS PROBLEMAS DIOFÁNTICOS DE LOS NÚMEROS DE FIBONACCI

TESIS
QUE PARA OPTAR POR EL GRADO DE
DOCTOR EN CIENCIAS

PRESENTA
JUAN JOSÉ ALBA GONZÁLEZ

TUTOR PRINCIPAL: DR. FLORIAN LUCA
UNIVERSIDAD DE WITWATERSRAND

COMITÉ TUTOR:
DR. EUGENIO BALANZARIO GUTIÉRREZ
CENTRO DE CIENCIAS MATEMÁTICAS, UNAM

DR. FRANCISCO MARMOLEJO RIVAS
INSTITUTO DE MATEMÁTICAS, UNAM

MÉXICO, D.F., ENERO DE 2016

Funciones de conteo para dos problemas diofánticos de los números de Fibonacci

M. en C. Juan José Alba González
Tutor principal: Dr. Florian Luca

Octubre de 2015

Índice general

Capítulo 1

Introducción

Los números de Fibonacci $\{F_n\}_{n\geq 0}$ se definen mediante las relaciones

$$F_0 = 0,\ F_1 = 1$$

y

$$F_{n+2} = F_{n+1} + F_n \quad \text{para todo} \quad n \geq 0.$$

En este trabajo de investigación se estudian desde un punto de vista analítico dos problemas diofánticos acerca de los números de Fibonacci.

El primero consiste en estudiar los valores de n tales que $n \mid F_n$. Se puede encontrar una caracterización recursiva de dichos enteros en [S]. Para estudiar este problema desde el punto de vista analítico consideramos la función de conteo de dichos enteros, es decir,

$$\#\mathcal{N}(x) = \#\{n \leq x : n \mid F_n\}$$

y encontramos cotas asintóticas superiores e inferiores para dicha función.

Los resultados que se dan en el trabajo se publicaron en [ALPS] y son mucho más generales pues se dan dichas cotas no solamente para la sucesión de Fibonacci sino para sucesiones con relaciones de recurrencia lineales homogéneas de cualquier orden.

El segundo problema consiste en estudiar la ecuación $u^2 + nv^2 = F_n$. Es fácil encontrar una infinidad de valores de n para los cuales la ecuación tiene solución. Desde el punto de vista analítico nos interesa entonces hacer una estimación de la función de conteo de dichas n's, es decir,

$$\#\mathcal{M}(x) = \#\{n \leq x : \text{la ecuación } u^2 + nv^2 = F_n \text{ tiene solución}\}.$$

Los resultados obtenidos acerca de este problema se pueden encontrar en [AL] y [ABL].

1.1. Resultados

Para una sucesión $\{u_n\}_{n\geq 0}$ definimos $\mathcal{N}_u = \{n \geq 1 : n \mid u_n\}$. Además, dado un conjunto de enteros $\mathcal{A}$, denotamos con $\mathcal{A}(x)$ al conjunto $\mathcal{A} \cap [1, x]$.

Los resultados que se obtuvieron en la investigación están dados por los siguientes teoremas.

Teorema 1.1. *Para todo $k \geq 2$ existe una constante positiva $c_0(k)$ que depende sólo de k tal que si el polinomio característico de una sucesión lineal recurrente no degenerada $\{u_n\}_{n\geq 0}$ de orden k tiene sólo raíces simples entonces se tiene la cota*

$$\#\mathcal{N}_u(x) \leq c_0(k)\frac{x}{\log x}$$

para $x \geq 2$. En particular, $\mathcal{N}_u$ tiene densidad 0.

En el caso de una sucesión de Lucas se puede dar una mejor cota. Sea $L(x) = \exp(\sqrt{\log x \log\log x})$, entonces se tiene el siguiente teorema:

Teorema 1.2. *Sea $\{u_n\}_{n\geq 0}$ una sucesión de Lucas. Entonces la desigualdad*

$$\#\mathcal{N}_u(x) \leq \frac{x}{L(x)^{1+o(1)}}$$

se cumple cuando $x \to \infty$.

También se tienen cotas inferiores dadas por los siguientes teoremas.

Teorema 1.3. *Existe un conjunto de enteros $\mathcal{L}$ tal que $\mathcal{L} \subset \mathcal{N}_u$ para toda sucesión de Lucas u_n con $Q = \pm 1$, y se cumple que*

$$\#\mathcal{N}_u(x) \geq \#\mathcal{L}(x) \geq x^{1/4+o(1)}.$$

Por otra parte, tenemos una cota inferior más holgada para una familia más grande de sucesiones de Lucas. Aquí Δ_u denota el discriminante de la sucesión de Lucas.

Teorema 1.4. *Sea $\{u_n\}_{n\geq 0}$ una sucesión de Lucas con $\Delta_u \neq 1$. Entonces existen constantes positivas c_1 y x_0 que dependen de la sucesión tales que para todo $x > x_0$ se tiene que*

$$\#\mathcal{N}_u(x) \geq \exp(c_1(\log\log x)^2).$$

Para el segundo problema, definimos

$$\mathcal{M} = \{n \geq 0 : \text{la ecuación } u^2 + nv^2 = F_n \text{ tiene solución}\}.$$

El siguiente teorema nos da cotas para $\#\mathcal{M}(x)$.

Teorema 1.5. *Se cumplen las siguientes estimaciones*

$$\frac{x}{\log x} \ll \#\mathcal{M}(x) \ll \frac{x}{(\log x)^{0.06}}.$$

Capítulo 2

Notación y Antecedentes

A lo largo de este trabajo se usará la siguiente notación.

Dado n un entero positivo, $\tau(n)$ denota el número de divisores positivos de n y $\varphi(n)$ es la función de Euler, que cuenta el número de enteros en el intervalo $[1, n]$ que son primos relativos con n. La función $\omega(n)$ denota el número de divisores primos de n sin contar multiplicidad, es decir, si se tiene la factorización $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ dada por el teorema fundamental de la aritmética, entonces $\omega(n) = r$, con la convención de que $\omega(1) = 0$.

Denotamos el máximo común divisor de dos o más enteros simplemente con $(a_1, a_2, \ldots, a_n)$ y el mínimo común múltiplo con $[a_1, a_2, \ldots, a_n]$.

Denotaremos por p y q solamente a números primos, en particular una suma de la forma $\sum_p$ denota una suma donde el índice corre sobre los primos.

Para un número real x definimos, como es usual, $\pi(x)$ como el número de primos menores o iguales que x. La función θ de Chebyshev se define mediante $\theta(x) = \sum_{p \leq x} \log p$.

$P(n)$ es el máximo factor primo de n con la convención de que $P(0) = P(1) = 1$. Dado un número real y, decimos que n es *y-suave* si $P(n) \leq y$, y denotamos con Ψ a la función de conteo de los números y-suaves, $\Psi(x, y) = \#\{1 \leq n \leq x : P(n) \leq y\}$.

Usaremos resultados de la teoría básica de números acerca de divisibilidad, números primos y congruencias, así como resultados importantes como el Teorema Chino del Residuo, el pequeño Teorema de Fermat, el Criterio de Euler, las propiedades del símbolo $\left(\frac{\bullet}{p}\right)$ de Legendre, y el Teorema de Reciprocidad Cuadrática de Gauss.

Todos estos resultados se pueden encontrar en la mayoría de los libros

introductorios de Teoría de Números, como por ejemplo [NZM].

Dado un campo $\mathbb{K}$ y un polinomio $p(x) \in \mathbb{K}[x]$, denotamos con $\partial(p(x))$ el grado de $p(x)$, con la convención de que $\partial(0) = -\infty$. El discriminante de un polinomio $\Delta(p(x))$ de grado n es el producto $a^{2n-2}\prod_{i<j}(\alpha_i - \alpha_j)^2$ donde a es el coeficiente principal y las α_i's son las raíces del polinomio. Para un polinomio $p(x) \in \mathbb{Z}[x]$, el contenido de $p(x)$ es el máximo común divisor de sus coeficientes.

Si $\mathbb{L}$ es una extensión algebraica de $\mathbb{K}$, escribimos $N_{\mathbb{L}/\mathbb{K}}(\gamma)$ para denotar a la norma de un elemento $\gamma \in \mathbb{L}$ con respecto a $\mathbb{K}$. Cuando $\mathbb{K} = \mathbb{Q}$ y se sobreentiende qué campo es $\mathbb{L}$, denotamos la norma simplemente con $N(\gamma)$.

Para un campo numérico $\mathbb{K}$ denotamos con $\mathcal{O}_{\mathbb{K}}$ al anillo de enteros algebraicos de $\mathbb{K}$.

2.1. Sucesiones Recurrentes Lineales Homogeneas

Sea $\{u_n\}_{n\geq 0}$ una sucesión que satisface la relación de recurrencia lineal homogénea

$$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_{k-1}u_{n+1} + a_k u_n, \qquad \text{para} \quad n = 0, 1, \ldots, \quad (2.1)$$

donde $a_1, \ldots, a_k$ son enteros y $a_k \neq 0$.

Las siguientes definiciones y resultados acerca de estas sucesiones se pueden encontrar en [EPSW].

A la sucesión (2.1), le asociamos su *polinomio característico*

$$f_u(X) = X^k - a_1 X^{k-1} - \cdots - a_{k-1}X - a_k = \prod_{i=1}^{m}(X - \alpha_i)^{\sigma_i} \in \mathbb{Z}[X],$$

donde $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$ son las raíces de $f_u(X)$ con multiplicidades $\sigma_1, \ldots, \sigma_m$, respectivamente.

Se sabe que el n-ésimo término de la sucesión se puede expresar como

$$u_n = \sum_{i=1}^{m} A_i(n)\alpha_i^n, \qquad \text{para} \quad n = 0, 1, \ldots, \quad (2.2)$$

donde $A_i(X)$ es un polinomio de grado a lo más $\sigma_i - 1$ para cada $i = 1, \ldots, m$, con coeficientes en $\mathbb{K} = \mathbb{Q}[\alpha_1, \ldots, \alpha_m]$.

Definimos

$$D_u(x_1, \ldots, x_k) = \det(\alpha_i^{x_j})_{1\leq i,j\leq k}.$$

y dado un primo p, con $(p, a_k) = 1$, definimos $T_u(p)$ como el máximo entero no negativo T tal que

$$p \nmid \prod_{0 \le x_2, \ldots, x_k \le T} \text{máx}\{1, |N(D_u(0, x_2, \ldots, x_k))|\}$$

donde $x_2, \ldots, x_k$ son enteros en $[0, T]$.

Se sabe que dicho T existe.

Como $\alpha_1, \ldots, \alpha_k$ son enteros algebráicos en $\mathbb{K}$, se sigue que los números $N(D_u(0, x_2, \ldots, x_k))$ son enteros.

Nótese que $T_u(p) = 0$ si y sólo si $k = 2$ y p divide a $\Delta_u = (\alpha_1 - \alpha_2)^2$.

Decimos que $\{u_n\}_{n \ge 0}$ es una *sucesión de Lucas* si $k = 2$, $u_0 = 0$, $u_1 = 1$ y $(a_1, a_2) = 1$. Si α_1/α_2 no es una raíz de la unidad decimos que la sucesión es *no degenerada* y en general sobreentenderemos que ese es el caso cuando se hable de una de estas sucesiones.

Las sucesiones de Lucas resultan una sucesión de divisibilidad fuerte, es decir, cumplen que $(u_n, u_m) = \left|u_{(n,m)}\right|$. Como consecuencia de esto se sigue que si $n \mid m$ entonces $u_n \mid u_m$.

Para las sucesiones de Lucas, (2.2) toma la forma

$$u_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2}$$

y se conoce como la fórmula de Binet.

Cuando $\{u_n\}_{n \ge 0}$ es una sucesión de Lucas se cumple que

$$|N(D_u(0, x_2))| = |\alpha_2^{x_2} - \alpha_1^{x_2}|^2 = |\Delta_u|^2 |u_{x_2}|^2, \qquad x_2 = 1, 2, \ldots.$$

De modo que si p no divide al discriminante $\Delta_u = (\alpha_1 - \alpha_2)^2 = a_1^2 + 4a_2$ de la sucesión $\{u_n\}_{n \ge 0}$, entonces $T_u(p) + 1$ es de hecho el menor entero positivo ℓ tal que $p \mid u_\ell$. Este número es llamado el *índice de aparición* de p en $\{u_n\}_{n \ge 0}$ y se denota por $z_u(p)$. El índice de aparición $z_u(m)$ se puede definir también para compuestos m de la misma manera, es decir, como el menor entero positivo ℓ tal que $m \mid u_\ell$. Dicho entero existe para todos los enteros positivos m primos relativos con a_2, y tiene la importante propiedad de que $m \mid u_n$ si y sólo si $z_u(m) \mid n$. Se sabe también que si p es un primo impar entonces $z(p) \mid p - \left(\dfrac{\Delta_u}{p}\right)$.

Sea p un primo tal que $p \nmid \Delta_u$. Decimos que p es un divisor primitivo de un elemento u_n de la sucesión si se tiene que $p \mid u_n$ pero $p \nmid u_k$ para $1 \le k < n$.

De la definición se sigue que $z_u(p) = n$ y por lo tanto se cumple que $p \equiv \pm 1 \pmod{n}$.

El siguiente es uno de los resultados más importantes de la teoría de las sucesiones de Lucas, se debe a Zsygmondy, Birkhoff, Vandiver, Carmichael, Bilu, Harnot y Voutier.

Teorema 2.1 (Divisor Primitivo)**.** *Sea $\{u_n\}_{n\geq 0}$ una sucesión de Lucas no degenerada. Si $n > 30$, entonces u_n tiene un divisor primitivo.*

El teorema completo de hecho enuncia cuáles son todas las sucesiones para las cuales hay excepciones cuando $n \leq 30$ (y cuáles son estas excepciones). El teorema se puede consultar en [BHV].

En el caso de la sucesión de Fibonacci, usamos $z(m)$ para el índice de aparición. Entonces $z(m)$ existe para todo m y tenemos que $m \mid F_n$ si y sólo si $z(m) \mid n$. Además, se sabe que $z(p^a) \mid p^{a-1}(p - e_p)$, donde $e_p = \left(\frac{p}{5}\right)$, y que $z(p^a) = p^b z(p)$, donde $b = \text{mín}\{0, a - f_p\}$ y $p^{f_p} \| F_{z(p)}$. Para n en general se tiene que

$$z(n) = [z(p^{a_p}) : p^{a_p} \| n].$$

Dado un primo p, definimos t_p como el periodo mínimo de la sucesión de Fibonacci módulo p. Se sabe que $t_p \in \{z(p),\ 2z(p),\ 4z(p)\}$ (vease [R]).

2.2. Teoría Analítica de Números

Usaremos la notación de Landau O, la notación o y los símbolos de Vinogradov con el significado usual en Teoría Analítica de Números.

Haremos uso de las propiedades de la integral de Riemann-Stieltjes, para aproximar sumas mediante integrales. En particular, como consecuencia de la fórmula de integración por partes tenemos la fórmula de Abel:

Teorema 2.2 (Abel)**.** *Sea a una función aritmética y f una función de clase $\mathcal{C}^1$. Entonces*

$$\sum_{x<n\leq y} a(n)f(n) = A(t)f(t)\Big|_x^y - \int_x^y A(t)f'(t)\mathrm{d}t$$

donde $A(x) = \sum_{n\leq x} a(n)$.

Necesitaremos usar que $\varphi(n)/n \gg 1/\log\log x$ para todo $n \leq x$. Esto es consecuencia del orden mínimo de la función φ de Euler (véase [T]):

$$\liminf_{n\to\infty} \frac{\varphi(n)}{n/\log\log n} = e^{-\gamma}.$$

Los siguientes teoremas se conocen como los Teoremas de Mertens y su demostración se pueden encontrar en [T]:

Teorema 2.3 (Primer Teorema de Mertens)**.** *Para $x \geq 2$ se tiene que*

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1).$$

Teorema 2.4 (Segundo Teorema de Mertens)**.** *Existe una constante M tal que para $x \geq 2$ se tiene que*

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + M + O\left(\frac{1}{\log x}\right).$$

M se conoce como la constante de Mertens.

Teorema 2.5 (Tercer Teorema de Mertens)**.** *Para $x \geq 2$ se tiene que*

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x} \left(1 + O\left(\frac{1}{\log x}\right)\right)$$

donde γ es la constante de Euler.

El siguiente hecho conocido acerca de ω es el Lema 2.3 en [EP] para el caso de $p - 1$; el caso de $p + 1$ es análogo:

Teorema 2.6. *Para $x \geq 3$ se tiene que*

$$\sum_{p \leq x} \frac{\omega(p \pm 1)}{p} \ll (\log \log x)^2.$$

El Teorema del Número Primo se puede enunciar de muchas maneras equivalentes, aquí haremos uso de las distintas formas llamándoles siempre con el mismo nombre. Estos resultados se pueden encontrar en [T].

Teorema 2.7 (Teorema del Número Primo)**.** *Se tiene que*

$$\pi(x) \sim \frac{x}{\log x}$$

cuando $x \to \infty$.

Equivalentemente, en términos de la función θ de Chebyshev,

$$\theta(x) \sim x$$

cuando $x \to \infty$.

Y tambien equivalentemente, si p_n *denota el* n*-ésimo primo, se tiene que*

$$p_n \sim n \log n$$

cuando $n \to \infty$.

Para ℓ y $k \geq 1$ y primos relativos definimos $\pi(x, k, \ell)$ como el número de primos $p \leq x$ congruentes con ℓ módulo k. Con esta notación tenemos los siguientes teoremas:

Teorema 2.8. *Si* ℓ *y* $k \geq 1$ *son primos relativos, se tiene que*

$$\pi(x, k, \ell) \sim \frac{\pi(x)}{\varphi(k)}$$

cuando $x \to \infty$.

Vamos a necesitar las siguientes consecuencias del teorema de Brun-Titchmarsh (véanse los Lemas 2.4 y 2.5 de [BKW]).

Teorema 2.9 (Brun-Titchmarsh)**.**

(i) Para $(\ell, k) = 1$ *y* $1 \leq \ell \leq k < x$*, tenemos*

$$\pi(x, k, \ell) \leq \frac{3x}{\varphi(k) \log(x/k)}.$$

(ii) La cota

$$\sum_{\substack{p \leq x \\ p \equiv \pm 1 \pmod{k}}} \frac{1}{p} \ll \frac{\log \log x}{\varphi(k)},$$

se cumple uniformemente para $x \geq k \geq 3$.

El Teorema de Densidad de Chebotarev, que se puede consultar en [N], afirma lo siguiente:

Teorema 2.10 (Chebotarev)**.** *Sea* f *un polinomio mónico con coeficientes enteros y discriminante* Δ *distinto de* 0*. Sea* C *una clase de conjugación del grupo de Galois* G *de* f*. Entonces, el conjunto de primos* p *que no dividen a* Δ *para los cuales* σ_p*, el automorfismo de Frobenius, pertenece a* C *tiene densidad igual a* $|C|/|G|$.

El resultado conocido como la Criba de Brun es un teorema muy general y muy técnico, pero tiene muchos corolarios más sencillos que se citan con este nombre. Este resultado y dichos corolarios se pueden encontrar en [HR]. Nosotros usaremos la siguiente forma de la criba de Brun (vease ejercicio 6.18 de [P]):

Teorema 2.11 (Criba de Brun)**.** *Sea $k \geq 1$ un entero fijo, y sea $y \leq x$. Supongamos que para cada $p \leq y$ tenemos escogidas $k_p \leq k$ clases de congruencia módulo p, con $k_p < p$. Entonces el número de enteros positivos $n \leq x$ que evitan todas estas clases de congruencia está acotado por*

$$Cx \prod_{p \leq y} \left(1 - \frac{k_p}{p}\right)$$

donde la constante C es independiente de las clases de congruencia escogidas para cada primo.

Acerca de los números suaves se tiene el siguiente resultado [CEP, Corolario del Teorema 3.1]:

Teorema 2.12. *Para $x \geq y > 1$, se tiene que*

$$\Psi(x, y) = x \exp(-(1 + o(1))u \log u)$$

uniformemente en el intervalo $y > (\log x)^2$ siempre y cuando $u \to \infty$, donde $u = \log x / \log y$.

Y usaremos la siguiente una cota, que es más floja pero más sencilla

Teorema 2.13. *Para todo $x \geq y \geq 2$ se tiene que*

$$\Psi(x, y) \ll x \exp(-u/2)$$

donde $u = \log x / \log y$.

Vamos a necesitar más adelante resultados conocidos acerca de la distribución de valores *y-suaves* de $p^2 - 1$ para primos p. Denotamos con $\Pi(x, y)$ al número de primos $p \leq x$ para los que $p^2 - 1$ es y-suave. Es de esperarse que los números $p^2 - 1$ con p primo se comporten como enteros "aleatorios" desde el punto de vista del tamaño de sus factores primos, por lo que es razonable suponer que el comportamiento de $\Pi(x, y)$ será como el de la función de conteo de los enteros suaves.

Más concretamente, tenemos el siguiente

Teorema 2.14. *Para $v \in [1, 4/3)$ se tiene que*

$$\Pi(y^v, y) \geq y^{v+o(1)}$$

cuando $y \to \infty$.

Este resultado es consecuencia del Teorema 1.2 de [DMT].

Necesitaremos también información acerca del número de divisores de primos trasladados que se encuentran en un intervalo dado. Para esto, definimos

$$H(x, y, z) = \#\{n \leq x \ : \ d \mid n \text{ para algún } d \in (y, z)\},$$

y dado un entero fijo $\lambda \neq 0$ definimos

$$H(x, y, z; P_\lambda) = \#\{p \leq x \ : \ d \mid p + \lambda \text{ para algún } d \in (y, z)\}.$$

Los siguientes resultados se encuentran en los Teoremas 1 y 6 de [F].

Teorema 2.15. *Si $100 \leq y \leq x^{1/2}$, y $2y \leq z \leq y^2$, entonces*

$$H(x, y, z) \asymp xu^\delta (\log 2/u)^{-3/2},$$

donde u está definido implicitamente por $z = y^{1+u}$ y

$$\delta = 1 - \frac{1 + \log\log 2}{\log 2} = 0.086071\ldots .$$

Además, si $1 \leq y \leq x^{1/2}$ entonces se tiene que

$$H(x, y, z; P_\lambda) \ll_\lambda \frac{H(x, y, z)}{\log x}.$$

siempre que $y + (\log y)^{2/3} \leq z \leq x$

Para una progresión aritmética c (mód d), definimos $t_{c,d,p}$ como el periodo mínimo de la sucesión $(F_{c+dn})_{n\geq 0}$ módulo p. El siguiente resultado se sigue de la cota dada en la página 86 de [EPSW], basada en los resultados de [Sh].

Teorema 2.16. *Se tiene, uniformemente para enteros $c \geq 0$, $d \geq 1$ y $p \geq 3$ primo, la siguiente cota:*

$$\sum_{k=1}^{t_{c,d,p}} \left(\frac{F_{c+dk}}{p}\right) \ll \sqrt{p}.$$

Capítulo 3

Primer Problema

El caso de las sucesiones con raíces múltiples presenta problemas para las cotas superiores de $\mathcal{N}_u(x)$,

Por ejemplo, la sucesión $u_n = n2^n$ para todo $n \geq 0$, con polinomio característico $f_u(X) = (X-2)^2$ muestra que $\mathcal{N}_u$ puede consistir en el conjunto de todos los enteros positivos.

Sea $D \in \mathbb{N}$ el común denominador de todos los coeficientes de los polinomios $A_i(X)$ para $i = 1, \ldots, m$. Así, los coeficientes de los polinomios $DA_i(X)$ son enteros algebraicos. Entonces

$$Du_n = \sum_{i=1}^{m} DA_i(0)\alpha_i^n + \sum_{i=1}^{m} D(A_i(n) - A_i(0))\alpha_i^n.$$

Si $n \in \mathcal{N}_u$, entonces $n \mid Du_n$. Como n divide al entero algebraico

$$\sum_{i=1}^{m} D(A_i(n) - A_i(0))\alpha_i^n,$$

se sigue que n divide a

$$\sum_{i=1}^{m} DA_i(0)\alpha_i^n.$$

Si este valor es idénticamente 0 (es decir, $A_i(0) = 0$ para todo $i = 1, \ldots, m$), entonces estamos en una situación similar a la del ejemplo $u_n = n2^n$. En este caso, $\mathcal{N}_u$ contiene por lo menos una proporción positiva de los enteros positivos (todos los enteros n primos relativos con D). De lo contrario, definimos

$$w_n = \sum_{i=0}^{m} DA_i(0)\alpha_i^n \qquad \text{para} \quad n = 0, 1, \ldots.$$

Un poco de teoría de Galois muestra que w_n es un entero para todo $n \geq 0$, y la sucesión $\{w_n\}_{n\geq 0}$ satisface la relación de recurrencia lineal de orden $\ell = \#\{1 \leq i \leq m : A_i(0) \neq 0\}$ con coeficientes enteros, que además tiene solamente raíces simples. Entonces, $\mathcal{N}_u \subseteq \mathcal{N}_w$, y por lo tanto no hay pérdida de generalidad para las pruebas de las cotas superiores cuando se consideran solamente sucesiones de recurrencia sin raíces repetidas.

Veamos entonces el caso en el que $f_u(X)$ tiene solamente raíces simples. En este caso, la relación (2.2) se vuelve

$$u_n = \sum_{i=1}^{k} A_i \alpha_i^n, \qquad \text{para} \quad n = 0, 1, \ldots, \tag{3.1}$$

donde $A_1, \ldots, A_k$ son constantes en K. Podemos suponer que ninguna de ellas es 0, de lo contrario la sucesión $\{u_n\}_{n\geq 0}$ satisface una relación de recurrencia lineal de orden menor.

Definimos

$$\Delta_u = \prod_{1\leq i<j\leq k} (\alpha_i - \alpha_j)^2 = \operatorname{disc}(f_u), \tag{3.2}$$

el discriminante de la sucesión $\{u_n\}_{n\geq 0}$, y del polinomio $f_u(X)$. Se sabe que Δ_u es un entero. También supondremos que $(u_n)_{n\geq 0}$ es no degenerada, es decir, que α_i/α_j no es una raíz de la unidad para ningunos $1 \leq i < j \leq m$.

De aquí en adelante sólo consideraremos sucesiones lineales de recurrencia con raíces simples y no degeneradas.

Cuando $k = 2$, $u_0 = 0$, $u_1 = 1$ y $(a_1, a_2) = 1$, la sucesión $\{u_n\}_{n\geq 0}$ se conoce como una *sucesión de Lucas*. La fórmula (3.1) de su término general es

$$u_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2}, \qquad \text{para} \quad n = 0, 1, \ldots. \tag{3.3}$$

Es decir, $A_1 = 1/(\alpha_1 - \alpha_2)$ y $A_2 = -1/(\alpha_1 - \alpha_2)$ en la fórmula del término general (3.1).

En el caso de una sucesión de Lucas $(u_n)_{n\geq 0}$, la estructura del conjunto $\mathcal{N}_u$ se describe de manera recursiva en [S] de la siguiente manera.

Para $n \in \mathcal{N}_u$, sea $\mathcal{S}_n$ el conjunto de primos que dividen a $u_n\Delta_u$. Los elementos *básicos* de $\mathcal{N}_u$ son 1 y 6 si $a_1 \equiv 3 \pmod 6$ y $a_2 \equiv \pm 1 \pmod 6$, son 1 y 12 si $a_1 \equiv \pm 1 \pmod 6$ y $a_2 \equiv 1 \pmod 6$ y es sólamente el 1 en el resto de los casos. Con esta terminología, se tiene que:

Teorema 3.1. *Todo elemento de $\mathcal{N}_u$ es de la forma $bp_1p_2\cdots p_r$ para algún $r \geq 0$, con b un elemento* básico *de N_u, y para $i = 1, \ldots, r$, los números $bp_1p_2\cdots p_{i-1}$ están también en $\mathcal{N}_u$ y p_i está en $\mathcal{S}_{bp_1p_2\cdots p_{i-1}}$.*

El problema de divisibilidad de los términos de una sucesión de recurrencia lineal entre funciones aritméticas de sus indices se estudió en [LS], y en [L] el caso especial de los números de Fibonacci.

Obsérvese que si $k = 1$, entonces $u_n = A_1 a_1^n$ para todo $n \geq 0$, con $A_1 \neq 0$ y $a_1 \notin \{0, \pm 1\}$. Su polinomio característico es $f_u(X) = X - a_1$. Es fácil ver que en este caso, $\#\mathcal{N}_u(x) = O((\log x)^{\omega(|a_1|)})$. Así que de ahora en adelante podemos suponer que $k \geq 2$.

Obsérvese también que para la sucesión $u_n = 2^n - 2$, con polinomio característico $f_u(X) = (X-1)(X-2)$, el pequeño teorema de Fermat implica que todos los primos están en $\mathcal{N}_u$, así que el Teorema del Número Primo y las estimaciones para la distribución de los pseudoprimos [1] muestran que es posible que ocurra que $\#\mathcal{N}_u(x) = (1 + o(1))x/\log x$ cuando $x \to \infty$.

Para cualquier $\gamma \in (0, 1)$, definimos

$$\mathcal{P}_{u,\gamma} = \{p \ : \ T_u(p) < p^\gamma\}.$$

Lema 1. *Para $x^\gamma, y \geq 2$, se tienen las estimaciones*

$$\#\{p : T_u(p) \leq y\} \ll \frac{y^k}{\log y}, \quad \#\mathcal{P}_{u,\gamma}(x) \ll \frac{x^{k\gamma}}{\gamma \log x}$$

donde la constante implícita depende sólo de la sucesión $\{u_n\}_{n\geq 0}$.

Demostración. Es claro que la segunda desigualdad se sigue de la primera poniendo $y = x^\gamma$, por lo que basta probar la primera. Supongamos que $T_u(p) \leq y$. Entonces para algunos enteros $x_2, \ldots, x_k$ en el intervalo $[1, y+1]$ se tiene que

$$p \mid \text{máx}\{1, |N_{\mathbb{K}/\mathbb{Q}}(D_u(0, x_2, \ldots, x_k))|\}.$$

De esto se sigue que

$$\prod_{T_u(p)\leq y} p \mid \prod_{1\leq x_2,\ldots,x_k\leq y+1} \text{máx}\{1, |N_{\mathbb{K}/\mathbb{Q}}(D_u(0, x_2, \ldots, x_k))|\}. \tag{3.4}$$

Hay, cuando mucho, $(y+1)^{k-1} = O(y^{k-1})$ posibilidades para las $(k-1)$-tuplas $(x_2, \ldots, x_k)$. Para cada una de estas $(k-1)$-tuplas, tenemos que

$$|N_{\mathbb{K}/\mathbb{Q}}(D_u(0, x_2, \ldots, x_k))| = \exp(O(y)).$$

[1] Un pseudoprimo es un número compuesto n que divide a $2^n - 2$. En [L1] se demuestra que existen muy pocos pseudoprimos en comparación con los primos.

Por lo tanto, el lado derecho de la ecuación (3.4) es $\exp(O(y^k))$. Tomando logaritmos en la desigualdad que se sigue de la divisibilidad (3.4), tenemos que

$$\sum_{T_u(p)\leq y} \log p = O(y^k).$$

Si existen en total n primos en esta suma y si p_i denota al i-ésimo primo, entonces

$$\sum_{i=1}^{n} \log p_i = O(y^k),$$

es decir, $\theta(p_n) \ll y^k$. Del Teorema de Número Primo se sigue que $p_n \ll y^k$ y que $n \ll y^k/(k \log y)$, que es lo que queríamos probar. □

El parámetro $T_u(p)$ es útil para acotar el número de soluciones $n \in [1, x]$ de la congruencia $u_n \equiv 0 \pmod{p}$. Por ejemplo, se tiene el siguiente resultado [EPSW, Teorema 5.11].

Lema 2. *Existe una constante $c_2(k)$ que depende sólo de k con la siguiente propiedad. Supóngase que $\{u_n\}_{n\geq 0}$ es una sucesión recurrente lineal de orden k que satisface (2.1), que p es un primo que no divide a $a_k\Delta_u$ y que existe un entero positivo s tal que u_s no es múltiplo de p. Entonces, para todo $x \geq 1$ el número de soluciones $R(x, p)$ de la congruencia*

$$u_n \equiv 0 \pmod{p} \qquad con \quad 1 \leq n \leq x$$

cumple la desigualdad

$$R_u(x, p) \leq c_2(k) \left(\frac{x}{T_u(p)} + 1 \right).$$

La constante $c_2(k)$ se puede escoger como el máximo entre k y una cota superior para el número de soluciones enteras $0 < x_2 < \cdots < x_k$ de la ecuación

$$D_u(0, x_2, \ldots, x_k) = 0, \tag{3.5}$$

que se sabe que existe, es finito y depende sólo de k y no de los números $\alpha_1, \ldots, \alpha_k$.

Cuando $\{u_n\}_{n\geq 0}$ es una sucesión de Lucas, definimos

$$\mathcal{Q}_{u,\gamma} = \{p \ : \ z_u(p) \leq p^\gamma\}.$$

Como consecuencia de las observaciones anteriores al Lema 1 se sigue que $\#\mathcal{Q}_{u,\gamma}(x) = \#\mathcal{P}_{u,\gamma}(x) + O(1)$. Por lo tanto, el Lema 1 implica el siguiente resultado.

Lema 3. *Para $x > 1$, se cumple*

$$\#\mathcal{Q}_{u,\gamma}(x) \ll \frac{x^{2\gamma}}{\log x}$$

donde la constante implicada depende sólo de la sucesión $\{u_n\}_{n\geq 0}$.

3.1. Demostración del Teorema 1.1

Suponemos que x es grande. Partimos el conjunto $\mathcal{N}_u(x)$ en varios subconjuntos. Sea $y = x^{1/\log\log x}$. Definimos

$$\begin{aligned}
\mathcal{N}_1(x) &= \{n \leq x \ : \ P(n) \leq y\};\\
\mathcal{N}_2(x) &= \{n \leq x \ : \ n \notin \mathcal{N}_1(x) \ \text{ y } \ P(n) \in \mathcal{P}_{u,1/(k+1)}\};\\
\mathcal{N}_3(x) &= \mathcal{N}(x) \setminus \left(\cup_{i=1}^{2} \mathcal{N}_i(x)\right).
\end{aligned}$$

Ahora acotaremos las cardinalidades de cada uno de estos conjuntos. Para $\mathcal{N}_1(x)$, por el Teorema 2.12, tenemos

$$\#\mathcal{N}_1(x) = \Psi(x,y) = x\exp(-(1+o(1))v\log v) = o\left(\frac{x}{\log x}\right) \tag{3.6}$$

cuando $x \to \infty$, donde

$$v = \frac{\log x}{\log y} = \log\log x.$$

Ahora consideremos $n \in \mathcal{N}_2(x)$. Entonces $n = pm$, donde $p = P(n) \geq$ máx$\{y, P(m)\}$. En particular, $p \leq x/m$ por lo que $m \leq x/y$. Como también tenemos que $p \in \mathcal{P}_{u,1/(k+1)}(x/m)$, el Lema 1 implica que el número de tales primos $p \leq x/m$ es $O\left((x/m)^{k/(k+1)}\right)$, donde la constante depende de la sucesión $\{u_n\}_{n\geq 0}$. Sumando la desigualdad anterior sobre todos los posibles valores de $m \leq x/y$, tenemos que

$$\begin{aligned}
\#\mathcal{N}_2(x) &\leq x^{k/(k+1)} \sum_{1\leq m\leq x/y} \frac{1}{m^{k/(k+1)}} \ll x^{k/(k+1)} \int_1^{x/y} \frac{\mathrm{d}t}{t^{k/(k+1)}}\\
&= ((k+1)x^{k/(k+1)})t^{1/(k+1)}\Big|_1^{x/y} \ll \frac{x}{y^{1/(k+1)}}.
\end{aligned} \tag{3.7}$$

Tomemos ahora $n \in \mathcal{N}_3(x)$. Como antes, tenemos $n = pm$, donde $p = P(n) > y$. Supongamos que x (y por lo tanto y) es suficientemente grande. Entonces, $m \leq x/p < x/y$. Como $n \in \mathcal{N}_u$, tenemos que $n \mid u_n$, por lo

tanto $p \mid u_n$. Además, $T_u(p) \geq p^{1/(k+1)}$. Fijemos p y contemos el número de posibilidades para m. Para esto, sea $\{w_\ell\}_{\ell \geq 0}$ la sucesión definida como $w_\ell = u_{p\ell}$ para todo $\ell \geq 0$. Esta es una sucesión de recurrencia lineal de orden k. Nos gustaría aplicarle el Lema 2 para acotar el número de soluciones de la congruencia

$$w_m \equiv 0 \pmod{p}, \qquad \text{donde} \quad 1 \leq m \leq x/p.$$

Si se cumplen las hipótesis del Lema 2, este número, denotado por $R_w(x/p, p)$ cumpliría

$$R_w(x/p, p) \leq c_2(k) \left(\frac{x}{pT_w(p)} + 1 \right).$$

Veamos que se cumplen las condiciones del Lema 2. Notese que si $\alpha_1, \ldots, \alpha_k$ son las raíces características de $\{u_n\}_{n \geq 0}$, entonces $\alpha_1^p, \ldots, \alpha_k^p$ son las raíces características de $\{w_\ell\}_{\ell \geq 1}$. Se sigue que

$$f_w(X) = \prod_{i=1}^{k} (X - \alpha_i^p).$$

En particular, el término $a_{w,k}$ correspondiente a la sucesión $\{w_\ell\}_{\ell \geq 1}$ satisface $a_{w,k} = a_k^p$ siempre que $y > 2$. Si suponemos además que $y > |a_k|$, tenemos que p no divide a a_k, y por lo tanto p tampoco divide a $a_{w,k}$. Ahora observemos que

$$\Delta_w = \prod_{1 \leq i < j \leq k} (\alpha_i^p - \alpha_j^p).$$

Módulo p, se tiene

$$\Delta_w \equiv \left(\prod_{1 \leq i < j \leq k} (\alpha_i - \alpha_j) \right)^p \equiv \Delta_u^p \pmod{p}.$$

De esta congruencia se sigue que $p \mid \Delta_w$ si y sólo si $p \mid \Delta_u$. Entonces, tomando x suficientemente grande como para que $y > |\Delta_u|$, tendremos que $p \nmid \Delta_u$, y por lo tanto $p \nmid \Delta_w$.

Hasta el momento, hemos comprobado que p no divide a $a_{w,k}\Delta_w$, que es la primera parte de la hipótesis del Lema 2.

Veamos que se cumple la siguiente parte de la hipótesis.

Como $p \nmid \Delta_u$, el polinomio característico $f_u(X)$ de $\{u_\ell\}_{\ell \geq 0}$ tiene solamente raíces simples módulo p. Además, p tampoco divide al último coeficiente

a_k de la recurrencia para $\{u_n\}_{n\geq 0}$, por lo que la sucesión es puramente periódica módulo p. Sea t_p su periodo mínimo módulo p. Se sabe que t_p es primo relativo con p. De hecho, t_p es un divisor del número

$$[p^i - 1 : i = 1, 2, \ldots, k].$$

Escojamos $n_0 > 0$ tal que $u_{n_0} \neq 0$. Sea x suficientemente grande de manera que $y > |u_{n_0}|$. Como $p > y$, tenemos que $p \nmid u_{n_0}$. Y como $(p, t_p) = 1$, existe un entero s con $sp \equiv n_0 \pmod{t_p}$. Entonces,

$$w_s = u_{sp} \equiv u_{n_0} \pmod{p}.$$

En particular, w_s es primo relativo con p. Por lo tanto, para x suficientemente grande, la segunda parte de la hipótesis del Lema 2 se cumple para la sucesión $\{w_\ell\}_{\ell\geq 0}$.

Ahora mostraremos que

$$R_w(x, p) \leq c_2(k) \left(\frac{x}{T_u(p)} + 1 \right), \tag{3.8}$$

que es la conclusión del Lema 2 con $T_w(p)$ remplazado por $T_u(p)$. Observese primero que $T_u(p)$ y $T_w(p)$ existen porque p no divide a a_k. Además, de las congruencias

$$\begin{aligned} D_w(x_1, \ldots, x_k) &= \det(\alpha_i^{px_j})_{1\leq i,j\leq k} \equiv (\det(\alpha_i^{x_j}))^p \pmod{p} \\ &\equiv D_u(x_1, \ldots, x_k)^p \pmod{p}, \end{aligned}$$

se sigue que si $0 < x_2 < \cdots < x_k$ son cualesquiera enteros positivos, entonces $p \mid N_{\mathbb{K}/\mathbb{Q}}(D_u(0, x_2, \ldots, x_k))$ si y sólo si $p \mid N_{\mathbb{K}/\mathbb{Q}}(D_w(0, x_2, \ldots, x_k))$. En particular, si el conjunto

$$\mathcal{Z}_u = \{(0, x_2, \ldots, x_k) \in \mathbb{Z}^k : 0 < x_2 < \cdots < x_k \text{ y } D_u(0, x_2, \ldots, x_k) = 0\}$$

es vacío, entonces $\mathcal{Z}_w$ es vacío también (de hecho, $\mathcal{Z}_w$ puede pensarse como el subconjunto de $\mathcal{Z}_u$ cuyos elementos son vectores con todas sus entradas múltiplos de p), así pues, $T_u(p) = T_w(p)$, y la desigualdad (3.8) se tiene por el Lema 2. Supongamos ahora que $\mathcal{Z}_u$ es no vacío. Para p grande (y por lo tanto, para x grande), el conjunto $\mathcal{Z}_w$ es vacío pues el número de soluciones de la ecuación (3.5) es finito. Sea $\mathcal{I}$ cualquier intervalo de longitud $T_u(p)$ y sean $n_1 < n_2 < \cdots < n_\ell$ todos los enteros en $\mathcal{I}$ tales que $w_n \equiv 0 \pmod{p}$. Supongamos que $\ell \geq k$. Entonces tenemos

$$\sum_{j=1}^{k} c_j \alpha_j^{pn_i} \equiv 0 \pmod{p} \quad i = 1, 2, \ldots, k-1 \text{ y algunos } i \in \{k, k+1, \ldots, \ell\}.$$

Sea π cualquier ideal primo que divida a p en $\mathcal{O}_K$ y considerense las congruencias anteriores como un sistema de k ecuaciones en las incógnitas $(c_1\alpha_1^{pn_1}, c_2\alpha_2^{pn_1}, \ldots, c_k\alpha_k^{pn_1})$ en $\mathcal{O}_K/\pi$. Aquí, p es suficientemente grande de manera que los denominadores de $c_1, \ldots, c_k$ son invertibles módulo p. Para p grande, la solución anterior del sistema es distinta de 0 en $(\mathcal{O}_K/\pi)^k$, así que podemos concluir que $\pi \mid D_w(0, x_2, \ldots, x_k)$, donde

$$x_2 = n_2 - n_1, \quad x_3 = n_3 - n_1, \quad \ldots, \quad x_{k-1} = n_k - n_1 \quad \text{y} \quad x_k = n_i - n_1.$$

Entonces, $p \mid N_{K/\mathbb{Q}}(\pi) \mid N_{K/\mathbb{Q}}(D_w(0, x_2, \ldots, x_k))$. Como $x_k = n_i - n_1 < T_u(p)$, tenemos que $D_u(0, x_2, \ldots, x_k) = 0$. Sin embargo, hay a lo más $c_2(k)$ posibilidades para el vector $(0, x_2, \ldots, x_k)$ (vease el párrafo de la ecuación (3.5)), de ahí que hay a lo más $c_2(k)$ posibilidades para $n_i - n_1$, y por lo tanto, también para $i \leq \ell$. Entonces, $\ell \leq c_2(k)$, lo que muestra que $\mathcal{I}$ contiene a lo más $c_2(k)$ soluciones de la congruencia $w_n \equiv 0 \pmod{p}$. Esto demuestra la desigualdad (3.8).

Como $n \in \mathcal{N}_3(x)$, tenemos que $T_u(p) \geq p^{1/(k+1)}$.

La desigualdad (3.8) ahora nos dice que el número de elecciones para m una vez que p está fijo es

$$R_w(x/p, p) \leq c_2(k) \left(\frac{x}{p^{1+1/(k+1)}} + 1 \right).$$

En resumen, tenemos que

$$\begin{aligned} \mathcal{N}_3(x) &\leq \sum_{y \leq p \leq x} c_2(k) \left(\frac{x}{p^{1+1/(k+1)}} + 1 \right) \\ &\leq c_2(k) \left(\pi(x) + x \sum_{y \leq p} \frac{1}{p^{1+1/(k+1)}} \right) \\ &\leq c_2(k) \left(\pi(x) + x \int_y^\infty \frac{\mathrm{d}t}{t^{1+1/(k+1)}} \right). \end{aligned}$$

Por lo tanto

$$\mathcal{N}_3(x) \leq c_2(k) \left(\pi(x) + O\left(\frac{(k+1)x}{y^{1/(k+1)}} \right) \right). \tag{3.9}$$

Comparando (3.6), (3.7) y (3.9), tenemos que

$$\#\mathcal{N}(x) \leq c_2(k)\pi(x) + \frac{x}{\exp((1+o(1))v \log v)} + O\left(\frac{x}{y^{1/(k+1)}} \right) \tag{3.10}$$

cuando $x \to \infty$, donde las constantes implicadas dependen de la recurrencia para $\{u_n\}_{n\geq 0}$. Como elegimos $y = x^{1/\log\log x}$, el segundo y tercer término del lado derecho de (3.10) son ambos $o(\pi(x))$ cuando $x \to \infty$ y esto termina la prueba del teorema.

3.2. Demostración del Teorema 1.2

Dividamos a los números $n \in \mathcal{N}_u(x)$ en varias clases:

(i) $\mathcal{N}_1(x) = \{n \in \mathcal{N}_u(x) : P(n) \leq L(x)^{1/2}\}$;

(ii) $\mathcal{N}_2(x) = \{n \in \mathcal{N}_u(x) : P(n) \geq L(x)^3\}$;

(iii) $\mathcal{N}_3(x) = \mathcal{N}_u(x) \setminus (\mathcal{N}_1(x) \cup \mathcal{N}_2(x))$.

Por el Teorema 2.12 tenemos que

$$\#\mathcal{N}_1(x) \leq \Psi(x, L(x)^{1/2}) \leq \frac{x}{L(x)^{1+o(1)}}$$

cuando $x \to \infty$.

Si $n \in \mathcal{N}_u$ y $p \mid n$, tenemos que $n \equiv 0 \pmod{p}$ y $n \equiv 0 \pmod{z_u(p)}$. Si p no divide al discriminante del polinomio característico de u (y por lo tanto, para p suficientemente grande), tenemos que $z_u(p) \mid p \pm 1$, por lo que $(p, z_u(p)) = 1$. Entonces, las condiciones $n \in \mathcal{N}_u$, $p \mid n$, y p suficientemente grande obligan a que $n \equiv 0 \pmod{pz_u(p)}$. De donde, si p es suficientemente grande, el número de n's con $n \in \mathcal{N}_u(x)$ tales que $P(n) = p$ es a lo más $\Psi(x/pz_u(p), p) \leq x/pz_u(p)$.

Entonces, para x grande, se tiene que

$$\#\mathcal{N}_2(x) \leq \sum_{p > L(x)^3} \frac{x}{pz_u(p)} = \sum_{\substack{p > L(x)^3 \\ z_u(p) \leq L(x)}} \frac{x}{pz_u(p)} + \sum_{\substack{p > L(x)^3 \\ z_u(p) > L(x)}} \frac{x}{pz_u(p)}.$$

Por el Lema 1 la primera suma del lado derecho tiene cuando mucho $L(x)^2$ sumandos para x grande, y cada sumando es menor o igual que $x/L(x)^3$, por lo que dicha suma está acotada por $x/L(x)$. La segunda suma tiene sumandos menores que $x/pL(x)$ y la suma $1/p$ es del orden de $\log\log x$, por lo que esta suma es $x/L(x)^{1+o(1)}$ cuando $x \to \infty$. Por lo tanto, $\#\mathcal{N}_2(x) \leq x/L(x)^{1+o(1)}$ cuando $x \to \infty$.

Para cada entero no negativo j, definimos $I_j = [2^j, 2^{j+1})$. Ahora cubrimos $I = [L(x)^{1/2}, L(x)^3)$ con estos intervalos diádicos, y definimos a_j mediante $2^j = L(x)^{a_j}$. Supondremos que j recorre sólamente los enteros en

los que I_j intersecta a I. Para cualquier entero k, sea $\mathcal{P}_{j,k}$ el conjunto de primos $p \in I_j$ con $z_u(p) \in I_k$. Observese que, por el Lema 1, tenemos que $\#\mathcal{P}_{j,k} \ll 4^k$.

Se sigue que

$$\#\mathcal{N}_3(x) \leq \sum_j \sum_k \sum_{p \in \mathcal{P}_{j,k}} \sum_{\substack{n \in \mathcal{N}_u(x) \\ P(n)=p}} 1 \leq \sum_j \sum_k \sum_{p \in \mathcal{P}_{j,k}} \Psi\left(\frac{x}{pz_u(p)}, p\right)$$
$$\leq \sum_j \sum_k \sum_{p \in \mathcal{P}_{j,k}} \frac{x}{pz_u(p)L(x)^{1/(2a_j)+o(1)}},$$

cuando $x \to \infty$, donde se uso el Teorema 2.12 para la última desigualdad.

Para $k > j/2$, acotamos

$$\sum_{p \in \mathcal{P}_{j,k}} \frac{1}{pz_u(p)} \leq 2^{-k} \sum_{p \in I_j} \frac{1}{p} \leq 2^{-k}$$

para x grande. Para $k \leq j/2$, tenemos

$$\sum_{p \in \mathcal{P}_{j,k}} \frac{1}{pz_u(p)} \ll \frac{4^k}{2^j 2^k} = 2^{k-j},$$

pues el número de sumandos es del orden de 4^k, como se hizo ver anteriormente.

Entonces,

$$\begin{aligned} \sum_k \sum_{p \in \mathcal{P}_{j,k}} \frac{1}{pz_u(p)} &= \sum_{k > j/2} \sum_{p \in \mathcal{P}_{j,k}} \frac{1}{pz_u(p)} + \sum_{k \leq j/2} \sum_{p \in \mathcal{P}_{j,k}} \frac{1}{pz_u(p)} \\ &\ll 2^{-j/2} = L(x)^{-a_j/2}. \end{aligned}$$

Tenemos finalmente que

$$\#\mathcal{N}_3(x) \leq \sum_j \frac{x}{L(x)^{a_j/2+1/(2a_j)+o(1)}} \qquad \text{cuando} \qquad x \to \infty.$$

Como el mínimo de $t/2 + 1/(2t)$ para $t > 0$ es 1 y se alcanza cuando $t = 1$, concluimos que $\#\mathcal{N}_3(x) \leq x/L(x)^{1+o(1)}$ cuando $x \to \infty$. Esto, junto con las estimaciones anteriores de $\#\mathcal{N}_1(x)$ y $\#\mathcal{N}_2(x)$, completa la prueba.

Es posible que usando los métodos de [ELP] y [GP] se puedan obtener mejores estimaciones.

3.3. Demostración del Teorema 1.3

Como $a_2 = \pm 1$, se tiene que para cualquier entero m, la sucesión u es puramente periódica módulo m. Así que el índice de aparición $z_u(m)$ existe para todos los enteros positivos m. Además, usando la fórmula (3.3) se puede ver que para cualquier potencia de primo $q = p^k$ tenemos

$$z_u(p^k) \mid z_u(p)p^{k-1}. \tag{3.11}$$

Definimos, para todo $y \geq 1$

$$M_y = [m : \ m \leq y].$$

Decimos que un entero positivo n es L-*especial* si es de la forma $n = 2sM_y$ para algún $y \geq 3$ y para algún entero positivo s libre de cuadrados que cumpla que $(s, M_y) = 1$ y que para todo primo $p \mid s$ se tiene $p^2 - 1 \mid M_y$. Sea $\mathcal{L}$ el conjunto de todos los números L-especiales.

Demostraremos ahora que $\mathcal{L} \subset \mathcal{N}_u$ para cualquier sucesión u con $a_2 = \pm 1$. Para probar esto basta mostrar que para cualquier $n = 2sM_y \in \mathcal{L}$ y para cualquier potencia de primo $q \mid n$, se tiene que $z_u(q) \mid n$. Esto es fácil si $q \mid s$, porque entonces $q = p$ es primo y entonces, o bien $z_u(p) = p$ (cuando $p \mid \Delta_u$) o bien $z_u(p) \mid p \pm 1$. Y como $p^2 - 1 \mid M_y$, en cualquiera de los casos tenemos $z_u(p) \mid n$.

Supongamos ahora que $q \mid 2M_y$, consideramos dos casos:

- Cuando q es impar, tenemos $q \mid M_y$ por lo que $q \leq y$. Escribimos $q = p^k$ con p primo, de manera que (3.11) implica $z_u(q) \mid (p-1)p^{k-1}, p^k$ o $(p+1)p^{k-1}$. Tenemos $p^{k-1} \leq y$ y si $p + 1 \leq y$, entonces $z(q) \mid M_y$. El único caso que no se cubre es cuando $p + 1 > y$ (y entonces $p \in (y-1, y]$), $k = 1$, $z_u(p) = p+1$. Escribimos $p+1 = 2^j m$ con m impar. Entonces $2^j \mid 2M_y$ y $m \mid 2M_y$, por lo que $p+1 \mid 2M_y$. Así, en cualquiera de los casos, $z_u(q) \mid 2M_y$ y $z_u(q) \mid n$.

- Cuando q es par, tenemos $q = 2^k$ y $q \mid 2M_y$, entonces, como $z_u(2) \in \{2, 3\}$, se sigue de (3.11) que $z_u(2^k) \mid 2^k$ o $z_u(2^k) \mid 3 \cdot 2^{k-1}$. Como $y \geq 3$, en cualquier caso tenemos $z_u(q) \mid 2M_y$.

Ahora usamos el método de Erdős [ER] para demostrar que el conjunto $\mathcal{L}$ es bastante grande. Definimos

$$y = \frac{\log x}{\log \log x} \qquad \text{y} \qquad z = y^v.$$

Decimos que q es una potencia de primo *propia* si $q = p^k$ para un primo p y un entero $k \geq 2$.

Definimos $\mathcal{P}$ como el conjunto de primos p tales que:

- $p \in [y+1, z]$;
- $p^2 - 1$ es y-suave;
- $p^2 - 1$ no es divisible por ninguna potencia de primo propia $q > y$.

Obsérvese que si q es una potencia de primo propia y $q \mid p^2 - 1$, entonces $q \mid p \pm 1$, a menos que q se par, en cuyo caso tenemos $q/2 \mid p \pm 1$. Como claramente hay a lo más $O(t^{1/2})$ potencias de primo propias $q \leq t$, hay solamente $O(zy^{-1/2})$ primos $p \leq z$ para los cuales $p^2 - 1$ es divisible por una potencia de primo propia $q > y$. Entonces, por el Teorema 2.14, tenemos que

$$\#\mathcal{P} \geq \Pi(z, y) - y + O(zy^{-1/2}) = z^{1+o(1)},$$

cuando $x \to \infty$.

Es claro también que para cualquier entero positivo s libre de cuadrados formado por primos $p \in \mathcal{P}$, el entero $n = 2sM_y$ es L-especial.

Tomamos ahora el conjunto $\mathcal{L}_v(x)$ de todos estos enteros L-especiales $n = 2sM_y$, donde s está formado por

$$r = \left\lfloor \frac{\log x - 2y}{\log z} \right\rfloor$$

primos distintos de $\mathcal{P}$. Por el Teorema del Número Primo se tiene que $M_y = \exp((1 + o(1))y)$ cuando $x \to \infty$, por lo que para x suficientemente grande tenemos que $n \leq x$ para todo $n \in \mathcal{L}_v(x)$.

Podemos entonces acotar la cardinalidad de $\mathcal{L}_v(x)$ como sigue

$$\#\mathcal{L}_v(x) \geq \binom{\#\mathcal{P}}{r} \geq \left(\frac{\#\mathcal{P}}{r}\right)^r.$$

Como

$$r = (v^{-1} + o(1))\frac{\log x}{\log\log x} \qquad \text{y} \qquad \frac{\#\mathcal{P}}{r} = (\log x)^{v-1+o(1)}$$

cuando $x \to \infty$, tenemos que $\#\mathcal{L}_v(x) \geq x^{1-1/v+o(1)}$ cuando $x \to \infty$. Finalmente observamos que $\mathcal{L}_v(x) \subset \mathcal{L}(x)$ y esto concluye la prueba.

3.4. Demostración del Teorema 1.4

Como $\Delta_u \equiv 0, 1 \pmod 4$ y $\Delta_u \neq 0,\ 1$, se tiene que $|\Delta_u| > 1$. Sea r un factor primo de Δ_u. Entonces $r^k \in \mathcal{N}_u$ para todo $k \geq 0$ (vease [Lu, páginas 210 y 295]). Sea k un entero positivo grande, y consideremos $u_{r^{k+4}}$. Por el Teorema 2.1, u_n tiene un divisor primitivo p para $n \geq 31$ y dicho primo p cumple que $p \equiv \pm 1 \pmod n$. Como hay, cuando mucho, 5 valores de $k \geq 0$ tales que $r^k \leq 30$ para el mismo entero $r > 1$, y como $u_m \mid u_n$ si $m \mid n$, tenemos que $u_{r^{k+4}}$ tiene por lo menos $\tau(r^{k+4}) - 5 = k$ factores primos $p \neq r$. Digamos que son $p_1 < \cdots < p_k$. Supongamos que $|\alpha_1| \geq |\alpha_2|$. Para n grande, tenemos que $|\alpha_1|^{n/2} < |u_n| < 2|\alpha_1|^n$ [EPSW, Teorema 2.3]. Si $\beta_1, \ldots, \beta_k$ son exponentes no negativos tales que

$$\beta_i \leq \frac{\log(x/r^{k+4})}{k \log p_i},$$

entonces $r^{k+4} p_1^{\beta_1} \cdots p_k^{\beta_k} \leq x$ está en $\mathcal{N}_u$ [Lu, Página 210], y está contado en $\#\mathcal{N}_u(x)$. Por lo tanto,

$$\begin{aligned}
\#\mathcal{N}_u(x) &\geq \prod_{i=1}^{k} \left(\left\lfloor \frac{\log(x/r^{k+4})}{k \log p_i} \right\rfloor + 1 \right) \geq \left(\frac{\log(x/r^{k+4})}{k} \right)^k \frac{1}{\prod_{i=1}^{k} \log p_i} \\
&\geq \left(\frac{\log(x/r^{k+4})}{2r^{k+4} \log |\alpha_1|} \right)^k,
\end{aligned}$$

donde la última desigualdad se sigue de lo siguiente

$$\begin{aligned}
\prod_{i=1}^{k} \log p_i \leq \left(\frac{1}{k} \sum_{i=1}^{k} \log p_i \right)^k &\leq \left(\frac{\log(|u_{r^{k+4}}|)}{k} \right)^k \\
&< \left(\frac{r^{k+4} \log |\alpha_1| + \log 2}{k} \right)^k \\
&< \left(\frac{2r^{k+4} \log |\alpha_1|}{k} \right)^k,
\end{aligned}$$

para $k \geq 2$. Aquí se ha usado también que $|u_n| < 2|\alpha_1|^n$ para todo $n \geq 1$ con $n = r^{k+4}$.

Sea $c_3 = 2 \log |\alpha_1|$. La cota para $\#\mathcal{N}_u(x)$ se puede escribir como

$$\begin{aligned}
\#\mathcal{N}_u(x) &\geq \left(\frac{\log x}{r^{k+4} c_3} + O\left(\frac{k}{r^k} \right) \right)^k = \left(\frac{\log x}{r^{k+4} c_3} \right)^k \left(1 + O\left(\frac{k^2}{\log x} \right) \right) \\
&\gg \left(\frac{\log x}{r^{k+4} c_3} \right)^k
\end{aligned}$$

siempre y cuando

$$k = o(\sqrt{\log x}), \tag{3.12}$$

cuando $x \to \infty$, lo cual supondremos. Ahora observemos que

$$\left(\frac{\log x}{r^{k+4}c_3}\right)^k = \exp\left(k\log(\log x/c_3) - k(k+4)\log r\right).$$

Sea $A = \log(\log x/c_3)$. La función $f(t) = tA - t(t+4)\log r$ alcanza su máximo en $t = (A - 4\log r)/(2\log r) = A/(2\log r) - 2$. Así, tomando $k = \lfloor A/(2\log r) - 2 \rfloor$ (de modo que se cumple (3.12)), obtenemos que $f(k) = f(t) + O(f'(t)) = A^2/(4\log r) + O(A)$, y entonces

$$\begin{aligned}\#\mathcal{N}_u(x) &\geq \exp\left(\frac{(\log(\log x/c_3))^2}{4\log r} + O(\log\log x)\right)\\ &= \exp\left(\frac{(\log\log x)^2}{4\log r} + O(\log\log x)\right),\end{aligned}$$

lo cual implica el teorema con cualquier constante $c_1 < 1/(4\log r)$.

3.5. Observaciones

Como se había mencionado, $\#\mathcal{N}_u(x)$ puede llegar a ser muy grande bajo ciertas condiciones. Nótese que la sucesión $u_n = 2^n - 2$ tiene la propiedad de que $u_1 = 0$. La siguiente proposición nos da una generalización de esto.

Proposición 1. *Sean $k \geq 2$ y $\{u_n\}_{n\geq 0}$ una sucesión lineal recurrente de orden k que cumple la relación* (2.1)*. Supongamos que existe un entero positivo n_0 primo relativo con a_k tal que $u_{n_0} = 0$. Entonces*

$$\#\mathcal{N}_u(x) \gg x/\log x,$$

donde la constante implícita depende de la sucesión $\{u_n\}_{n\geq 0}$.

Demostración. Como n_0 es primo relativo con a_k, se tiene que $\{u_n\}_{n\geq 0}$ es puramente periódica módulo n_0. Sea t_{n_0} su periodo. Ahora consideremos $\mathcal{R}_u$ el conjunto de los primos $p \equiv 1 \pmod{t_{n_0}}$ tales que $f_u(X)$ se descompone en factores lineales módulo p. Dicho de otra manera, $\mathcal{R}_u$ es el conjunto de los primos p tales que el polinomio $f_u(X)(X^{t_{n_0}} - 1)$ se descompone en factores lineales módulo p. El conjunto de dichos primos tiene densidad positiva dentro de los primos por el Teorema 2.10. Se afirma que

$$\mathcal{S}_u \subseteq \mathcal{N}_u, \tag{3.13}$$

donde

$$\mathcal{S}_u = \{pn_0 : p \in \mathcal{R}_u \text{ y } p > n_0|\Delta_u|\}.$$

Dicha inclusión nos da la cota buscada pues

$$\#\mathcal{N}_u(x) \geq \#\mathcal{R}_u(x/n_0) + O(1) \gg x/\log x.$$

Supongamos entonces que $p > n_0|\Delta_u|$ está en $\mathcal{R}_u$. Entonces $p \equiv 1 \pmod{t_{n_0}}$, de donde $p = 1 + \lambda t_{n_0}$ para algún entero positivo λ. Entonces $pn_0 = n_0 + \lambda n_0 t_{n_0}$ y como $\{u_n\}_{n\geq 1}$ es puramente periódica con periodo t_{n_0} módulo n_0, tenemos que

$$u_{pn_0} = u_{n_0+\lambda n_0 t_{n_0}} \equiv u_{n_0} = 0 \pmod{n_0}. \tag{3.14}$$

Ahora, como el polinomio $f_u(X)$ se descompone en factores lineales módulo p, tenemos que $\alpha_i^p \equiv \alpha_i \pmod{p}$ para todo $i = 1, \ldots, k$. En particular, $\alpha_i^{pn_0} \equiv \alpha_i^{n_0} \pmod{p}$ para todo $i = 1, \ldots, k$. Como los denominadores de los coeficientes A_i, $i = 1, \ldots, k$, en (3.1) son divisores de Δ_u y $p > |\Delta_u|$, se sigue que dichos denominadores son invertibles módulo p, por lo que $A_i\alpha_i^{pn_0} \equiv A_i\alpha_i^{n_0} \pmod{p}$ para todo $i = 1, \ldots, k$. Sumando estas congruencias para $i = 1, \ldots, k$, obtenemos

$$u_{pn_0} = \sum_{i=1}^{k} A_i\alpha_i^{pn_0} \equiv \sum_{i=1}^{k} A_i\alpha_i^{n_0} \equiv u_{n_0} = 0 \pmod{p}. \tag{3.15}$$

De las congruencias (3.14) y (3.15), obtenemos que p y n_0 dividen a u_{pn_0}, y como p es primo relativo con n_0, concluimos que $pn_0 \mid u_{pn_0}$. □

La condición de que n_0 sea primo relativo con a_k no es necesaria, como lo muestra la sucesión con término general

$$u_n = 10^n - 7^n - 2 \cdot 5^n - 1 \qquad \text{para todo} \quad n \geq 0,$$

en la cuál podemos tomar $n_0 = 2$. En este caso $k = 4$,

$$f_u(X) = (X - 10)(X - 7)(X - 5)(X - 1),$$

y n_0 no es primo relativo con $a_4 = -350$, sin embargo se puede comprobar que $2p \mid u_{2p}$ para todos los primos $p \geq 11$.

Sea $\mathcal{K}_u(x)$ el conjunto de los enteros $n \leq x$ tales que $n \mid u_n$ y n *no* es de la forma pn_0, donde p es primo y $u_{n_0} = 0$. Veamos que en las condiciones del Teorema 1.1, podemos obtener una cota superior para $\#\mathcal{K}_u(x)$ menor que la que tenemos para $\#\mathcal{N}_u(x)$ si agregamos una hipótesis más.

Proposición 2. *Sea $\{u_n\}_{n\geq 0}$ una sucesión lineal recurrente de orden k cuyo polinomio característico se descompone en factores lineales en $\mathbb{Z}[X]$. Entonces existe una constante positiva c_4 que depende sólo de k tal que para todo x suficientemente grande, tenemos que $\#\mathcal{K}_u(x) \leq x/L(x)^{c_4}$.*

Demostración. Sea $y = L(x)$. Partimos a $\mathcal{K}_u(x)$ en los siguientes conjuntos:

$$\begin{aligned}\mathcal{K}_1(x) &= \{n \in \mathcal{K}_u(x) : P(n) \leq y\};\\ \mathcal{K}_2(x) &= \{n \in \mathcal{K}_u(x) : \text{ existe un primo } p \mid n,\ p > y,\ pT_u(p) \leq kx\};\\ \mathcal{K}_3(x) &= \mathcal{K}_u(x) \setminus (\mathcal{K}_1(x) \cup \mathcal{K}_2(x)).\end{aligned}$$

Como en la demostración del Teorema 1.2, vemos que, por el Teorema 2.12, tenemos que $\#\mathcal{K}_1(x) \leq x/L(x)^{1/2+o(1)}$ cuando $x \to \infty$.

Imitando ahora la demostración del Teorema 1.1, vemos que

$$\#\mathcal{K}_2(x) \ll \sum_{\substack{y<p\leq x\\ pT_u(p)\leq kx}} \left(\frac{x}{pT_u(p)} + 1\right) \ll \sum_{y<p\leq x} \frac{x}{pT_u(p)}.$$

Partimos esta suma en dos, dependiendo de si $p \in \mathcal{P}_{u,1/(k+1)}$ o no. El Lema 1 nos dice que $\#\mathcal{P}_{u,1/(k+1)}(t) \ll t^{k/(k+1)}/\log t$. Entonces,

$$\sum_{\substack{y<p\leq x\\ p\in\mathcal{P}_{u,1/(k+1)}}} \frac{x}{pT_u(p)} \leq \sum_{\substack{y<p\leq x\\ p\in\mathcal{P}_{u,1/(k+1)}}} \frac{x}{p} \ll \frac{x}{y^{1/(k+1)}},$$

y

$$\sum_{\substack{y<p\leq x\\ p\notin\mathcal{P}_{u,1/(k+1)}}} \frac{x}{pT_u(p)} \leq \sum_{y<p\leq x} \frac{x}{py^{1/(k+1)}} \ll \frac{x\log_2 x}{y^{1/(k+1)}}.$$

Por lo tanto,

$$\#\mathcal{K}_2(x) \ll \frac{x}{L(x)^{1/(k+1)+o(1)}} \qquad \text{cuando} \qquad x \to \infty.$$

Tomemos ahora $n \in \mathcal{K}_3(x)$. Sea $p \mid n$ tal que $pT_u(p) > kx$. Usando que $T_u(p) \leq kt_p$ y que $t_p \mid p-1$ (pues f_u se descompone en factores lineales sobre $\mathbb{Z}[X]$), tenemos que

$$kx < pT_u(p) \leq kpt_p \leq kp^2,$$

de modo que $p > \sqrt{x}$. Entonces n puede tener a lo más un factor primo p tal que $pT_u(p) > kx$. Por lo tanto, si $n \in \mathcal{K}_3(x)$, podemos suponer que $n = mp$

donde $p > \sqrt{x} > m$, y $P(m) \leq y$. Además, podemos suponer que $u_m \neq 0$. Como $p \mid u_{pm}$ y $t_p \mid p-1$, tenemos que $p \mid u_m$. Por otra parte, el número de factores primos de u_m es $O(m)$. Como el número de enteros n en $\mathcal{K}_3(x)$ que tienen un divisor primo p con estas propiedades es $O(x/(pT_u(p))+1) = O(1)$, tenemos que

$$\#\mathcal{K}_3(x) \ll \sum_{\substack{m<\sqrt{x} \\ P(m)\leq y}} m \leq \sqrt{x}\,\Psi(\sqrt{x}, y) = \frac{x}{L(x)^{1/4+o(1)}} \quad \text{cuando} \quad x \to \infty,$$

por el Teorema 2.12. Esto termina la demostración el teorema escogiendo, por ejemplo, $c_4 = \min\{1/5, 1/(k+2)\}$. □

Finalmente, consideremos un polinomio no constante $g(X) \in \mathbb{Z}[X]$ y la generalización

$$\mathcal{N}_{u,g} = \{n \geq 1 \ : \ g(n) \mid u_n\}.$$

Sea $y < x^{1/2}$ y obsérvese que por el Teorema 2.11, existen a lo más

$$N_1 \ll x\left(\frac{\log y}{\log x}\right) \tag{3.16}$$

valores de $n \leq x$ tales que $g(n)$ no tiene un divisor primo en el intervalo $[y, x^{1/2}]$. Obsérvese también que para un primo p que no divide al contenido de g, la divisibilidad $p \mid g(n)$ coloca a n en a lo más $\partial(g)$ progresiones aritméticas. Entonces, por el Lema 2, el número de las n's restantes tales que $n \leq x$ y $g(n) \mid u_n$ se puede estimar como sigue

$$N_2 \leq \sum_{p\in[y,x^{1/2}]} \sum_{\substack{n\leq x \\ p\mid g(n) \\ p\mid u_n}} 1 \ll \sum_{p\in[y,x^{1/2}]} \left(\frac{x}{pT_u(p)}+1\right) \ll x \sum_{p\in[y,x^{1/2}]} \frac{1}{pT_u(p)} + O(x^{1/2}).$$

Usando el Lema 1 para $\gamma \in (0,1)$ y la estimación trivial $T_u(p) \gg \log p$, obtenemos

$$\sum_{p\in[z,2z]} \frac{1}{pT_u(p)} \leq \frac{1}{z} \sum_{p\in[z,2z]} \frac{1}{T_u(p)} \ll \frac{1}{z}\left(\frac{z^{k\gamma}}{(\log z)^2} + \frac{z^{1-\gamma}}{\log z}\right).$$

Escogemos γ de manera que

$$z^\gamma = (z \log z)^{1/(k+1)},$$

para obtener

$$\frac{1}{z}\sum_{p\in[z,2z]}\frac{1}{pT_u(p)} \ll z^{-1/(k+1)}(\log z)^{-(k+2)/(k+1)}.$$

Sumando sobre los intervalos diádicos, tenemos que

$$\sum_{p\in[y,x^{1/2}]}\frac{1}{pT_u(p)} \ll y^{-1/(k+1)}(\log y)^{-(k+2)/(k+1)}.$$

Por lo tanto,

$$N_2 \ll xy^{-1/(k+1)}(\log y)^{-(k+2)/(k+1)} + x^{1/2}. \tag{3.17}$$

Tomando $y = (\log x)^{k+1}$, concluimos de (3.16) y (3.17) la cota

$$\#\mathcal{N}_{u,g}(x) \le N_1 + N_2 \ll x\left(\frac{\log\log x}{\log x}\right). \tag{3.18}$$

Sería interesante tratar de mejorar la cota (3.18) para que se acerque a la del Teorema 1.1, pero la prueba del Teorema 1.1 no funciona en general por la posible existencia de divisores primos grandes de $g(n)$.

Capítulo 4

Segundo Problema

4.1. Introducción

La ecuación diofantina $F_n = f(x)$ donde $f(X) \in \mathbb{Q}[X]$ ha sido estudiada para distintos polinomios $f(X)$. Nemes y Pethő [NP] clasificaron todos los polinomios $f(X)$ tales que dicha ecuación tiene una infinidad de soluciones enteras (n, x) con $n \geq 0$. Los números de Fibonacci F_n que son suma de tres cuadrados se investigaron en [RO].

Dado un entero fijo d, los números de Fibonacci F_n de la forma $x^2 + dy^2$ para algunos enteros x y y se investigaron en [BL]. Específicamente, los autores definen $\mathcal{M}_d$ como el conjunto de los enteros $n > 0$ tales que $F_n = x^2 + dy^2$ para algunos enteros x y y, y estudian el conjunto $\mathcal{D}$ de los enteros d tales que $\mathcal{M}_d$ tiene densidad inferior positiva.

En este trabajo se estudian los enteros positivos n para los cuales se tiene una representación "diagonal" $F_n = u^2 + nv^2$ para algunos enteros u y v. Definamos entonces

$$\mathcal{M} = \{n \geq 1 : F_n = u^2 + nv^2 \text{ para algunos enteros } u,\ v\}.$$

Probaremos las siguientes cotas

$$\frac{x}{\log x} \ll \#\mathcal{M}(x) \ll \frac{x}{(\log x)^{0.06}}.$$

4.2. Resultados Preliminares

Con la notación $\mathcal{P}_y = \{p : z(p) \leq y\}$ el Lema 1 tiene como caso particular para la sucesión de Fibonacci el siguiente Lema:

Lema 4. *Se cumple que*

$$\#\mathcal{P}_y \ll \frac{y^2}{\log y}$$

para todo $y \geq 2$.

También necesitaremos la siguiente congruencia.

Lema 5. *Para todo entero* m *y para todo primo* p *se tiene que* $F_{pm} \equiv F_p F_m \pmod{p}$.

Demostración. Usando la identidad 11 de la página 10 de [BQ] y el teorema de Fermat, tenemos que

$$F_{pm} = \sum_{k=0}^{p} \binom{p}{k} F_m^k F_{m-1}^{p-k} F_k \equiv F_m^p F_p \equiv F_m F_p \pmod{p}.$$

□

A continuación probamos que $t_{c,d,p} = t_p/(d, t_p)$ siempre que $z(p) \nmid d$.

Lema 6. *Sean* $c \geq 0,\ d > 0$ *enteros y* $p > 5$ *un primo tal que* $z(p) \nmid d$, *entonces* $t_{c,d,p} = t_p/(d, t_p)$.

Demostración. Sean $\alpha = (1+\sqrt{5})/2,\ \beta = (1-\sqrt{5})/2$ y $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. Es fácil ver que $\{F_{c+nd}\}_{n\geq 0}$ es una sucesión lineal recurrente de orden 2 con polinomio característico $x^2 - (\alpha^d + \beta^d)x + (-1)^d$ y que $\{F_{c+nd}\}_{n\geq 0}$ es puramente periódica módulo p. Por lo tanto, $\{F_{c+nd}\}_{n\geq 0}$ es periódica módulo p con periodo $T(= t_{c,d,p})$ si y sólo si $F_c \equiv F_{c+dT} \pmod{p}$, $F_{c+d} \equiv F_{c+d+dT} \pmod{p}$, y T es mínimo con esta propiedad. Sea π un primo en $\mathcal{O}_{\mathbb{K}}$ que divida a p. Definiendo $u = \alpha^{dT} - 1,\ v = \beta^{dT} - 1$, y usando la fórmula de Binet podemos reescribir las congruencias anteriores como

$$\begin{aligned} \alpha^c u - \beta^c v &\equiv 0 \pmod{\pi} \\ \alpha^{c+d} u - \beta^{c+d} v &\equiv 0 \pmod{\pi}. \end{aligned}$$

El determinante de este sistema de ecuaciones (en u y v) es $(\alpha\beta)^c(\alpha^d - \beta^d) = (-1)^c\sqrt{5}F_d$, que es distinto de 0 módulo π porque $\pi \mid p, p > 5$ y como $z(p) \nmid d$, $p \nmid F_d$. Esto demuestra que $u \equiv 0 \pmod{\pi}$ y $v \equiv 0 \pmod{\pi}$. En particular, T es el orden de (α^d, β^d) en $\mathcal{O}_{\mathbb{K}}/\pi \times \mathcal{O}_{\mathbb{K}}/\pi$. Un argumento similar con $c = 0$ y $d = 1$ demuestra que t_p es el orden de (α, β) en $\mathcal{O}_{\mathbb{K}}/\pi \times \mathcal{O}_{\mathbb{K}}/\pi$. Por lo tanto, $T = t_p/(d, t_p)$. □

4.3. Demostración del Teorema 1.5

4.3.1. Cota Superior

Empezamos por descartar varios subconjuntos de enteros $n \in [1, x]$ que nos estorban para trabajar en el problema.

Sean x un número real positivo grande, $y_1 = \exp(\log x / \log\log x)$ y definimos

$$\mathcal{M}_1(x) = \{n \leq x : P(n) \leq y_1\}.$$

Observese que $u = \log x / \log y_1 = \log\log x$, así que por el Teorema 2.13, tenemos que

$$\#\mathcal{M}_1(x) = \Psi(x, y_1) \ll x \exp(-u/2) = \frac{x}{(\log x)^{1/2}}. \tag{4.1}$$

Ahora tomamos $z_1 = (\log x)^3$. Consideremos $\alpha \in (0, 1)$ cuyo valor determinaremos después. Definimos ahora

$$\mathcal{M}_2(x) = \{n \leq x : p^2 \mid n \text{ para algún primo } p > z_1^\alpha\}.$$

Si $n \in \mathcal{M}_2(x)$ entonces $p^2 \mid n$ para algún primo $p \geq z_1^\alpha$. Si fijamos p, el número de dichas n's es $\lfloor x/p^2 \rfloor \leq x/p^2$. Entonces

$$\#\mathcal{M}_2(x) \leq \sum_{z_1^\alpha \leq p \leq x^{1/2}} \frac{x}{p^2} \leq x \sum_{m \geq z_1^\alpha} \frac{1}{m^2} \ll \frac{x}{z_1^\alpha} = \frac{x}{(\log x)^{3\alpha}}. \tag{4.2}$$

A continuación definimos

$$\mathcal{P} = \{p : z(p) < p^{1/3}\}.$$

Por el Lema 4, tenemos que

$$\#\mathcal{P}(x) = \#\{p \leq x : z(p) < x^{1/3}\} = \#\mathcal{P}_{x^{1/3}} \ll \frac{x^{2/3}}{\log x}.$$

Y definimos

$$\mathcal{M}_3(x) = \{n \leq x : p \mid n \text{ para algún } p \in \mathcal{P} \text{ con } p \geq z_1\}.$$

El número de enteros $n \le x$ que son múltiplos p es $\lfloor x/p \rfloor \le x/p$. Sumando sobre todos los posibles valores de p tenemos que

$$\begin{aligned}\#\mathcal{M}_3(x) &\le \sum_{\substack{z_1 \le p \le x \\ p \in \mathcal{P}}} \frac{x}{p} = x \int_{z_1}^{x} \frac{\mathrm{d}\#\mathcal{P}(t)}{t} = x \left(\frac{\#\mathcal{P}(t)}{t}\Big|_{z_1}^{x} + \int_{z_1}^{x} \frac{\#\mathcal{P}(t)}{t^2}\mathrm{d}t \right) \\ &\ll x \left(\frac{\#\mathcal{P}(x)}{x} + \int_{z_1}^{x} \frac{\mathrm{d}t}{t^{4/3}} \right) \ll x \left(\frac{1}{x^{1/3}\log x} + \left(-\frac{3}{t^{1/3}}\Big|_{t=z_1}^{t=x} \right) \right) \\ &\ll \frac{x^{2/3}}{\log x} + \frac{3x}{z_1^{1/3}} \ll \frac{x}{\log x}. \end{aligned} \tag{4.3}$$

Ahora definimos el conjunto

$$\mathcal{M}_4(x) = \{n \le x : n \notin \mathcal{M}_3(x) \text{ y } p \mid (n, F_n) \text{ para algún } p > z_1\}.$$

Si $n \in \mathcal{M}_4(x)$, entonces $p \mid (n, F_n)$ para algún $p > z_1$. Como $n \notin \mathcal{M}_3(x)$, tenemos que $p \notin \mathcal{P}$, por lo que $z(p) > p^{1/3} > z_1^{1/3}$. Para x grande, tenemos que $z(p) > z_1^{1/3} > 5$, y entonces $z(p) \mid p \pm 1$. En particular, p and $z(p)$ son primos relativos, y como $p \mid n$ y $p \mid F_n$; entonces, $z(p) \mid n$, y podemos concluir que $pz(p) \mid n$. Para un primo fijo p, el número de estos enteros n es $\lfloor x/pz(p) \rfloor \le x/pz(p)$. Sumando sobre todos los posibles valores de p, tenemos que

$$\#\mathcal{M}_4(x) \le \sum_{\substack{p > z_1 \\ pz(p) \le x}} \frac{x}{pz(p)} \le \sum_{p > z_1} \frac{x}{p^{4/3}} \ll \frac{x}{z_1^{1/3}} = \frac{x}{\log x}. \tag{4.4}$$

Supongamos por el momento que $n \le x$ no está en $\bigcup_{i=1}^{4} \mathcal{M}_i(x)$. Y supongamos que

$$F_n = u^2 + nv^2 \tag{4.5}$$

para algunos enteros u y v (que dependen de n). Para x grande, tenemos que $y > z_1$, y como $n \notin \mathcal{M}_1(x)$, existe un primo $p > z_1$ tal que $p \mid n$. Como $n \notin \mathcal{M}_2(x) \cup \mathcal{M}_4(x)$, tenemos que $p \| n$ y $p \nmid F_n$. Así que podemos poner $n = pm$, donde $(m, p) = 1$. Reduciendo la ecuación (4.5) módulo p, tenemos que

$$F_n \equiv u^2 \pmod{p}$$

con $u \not\equiv 0 \pmod{p}$. Por lo tanto,

$$\left(\frac{F_n}{p} \right) = 1.$$

Por el Lema 5, tenemos que

$$1 = \left(\frac{F_n}{p}\right) = \left(\frac{F_p F_m}{p}\right) = \left(\frac{F_p}{p}\right)\left(\frac{F_m}{p}\right),$$

y por lo tanto

$$\left(\frac{F_m}{p}\right) = \left(\frac{F_p}{p}\right). \tag{4.6}$$

Como consecuencia de esto tenemos que en cualquier representación de n de la forma $n = mp$, con $p > z_1$, el carácter cuadrático de F_m módulo p está determinado de manera única por p. Para usar de manera eficiente esta información necesitamos remover aún mas enteros $n \le x$.

Sea

$$\begin{aligned}\mathcal{M}_5(x) = \{n \le x \ : \ & n \notin \mathcal{M}_2(x) \text{ y existe } q > z_1^{\alpha},\ q \mid (z(p_1), z(p_2)) \\ & \text{con } \ p_1 \neq p_2 \ \text{ y } \ p_1 p_2 \mid n, \ \text{ ó } \ q \mid (n, z(n))\}.\end{aligned}$$

Supongamos que $n \in \mathcal{M}_5(x)$. Observese que si x es grande, entonces q también es grande, y la condición $q \mid z(p)$ implica que $q \mid p \pm 1$. Por lo tanto, $p \equiv \pm 1 \pmod q$. Además, como $q^2 \nmid n$, porque $n \notin \mathcal{M}_2(x)$, y ya que para todos los enteros positivos a y primos p se tiene que $z(p^a) = p^b z(p)$ para algún entero no negativo $b < a$ (que depende de p y de a), se sigue que $q \mid z(n)$, y por lo tanto $q \mid z(p)$ para algún factor primo p de n. Entonces, si $n \in \mathcal{M}_5(x)$, entonces, o bien existen dos factores primos distintos de n, digamos p_1 y p_2, y un primo $q > z_1^{\alpha}$ tal que $p_i \equiv \pm 1 \pmod q$ para $i = 1, 2$, o bien $q \mid n$ y $q \mid z(p)$ para algún factor primo p de n. Consideremos el primer caso y sea $\mathcal{M}_{5,1}(x)$ el conjunto de los $n \le x$ que caen en dicho caso. Si p_1 y p_2 están fijos, el número de dichas $n \le x$ es $\lfloor x/p_1p_2 \rfloor \le x/p_1p_2$. Dejando $q > z_1^{\alpha}$ fijo y sumando la desigualdad anterior sobre todas las parejas de primos (p_1, p_2) con $p_1p_2 \le x$ y $p_i \equiv \pm 1 \pmod q$ para $i = 1, 2$, y luego sumando sobre todos los primos $q > z_1^{\alpha}$ obtenemos la siguiente cota

$$\begin{aligned}\#\mathcal{M}_{5,1}(x) &\le \sum_{q > z_1^{\alpha}} \sum_{\substack{p_1 \neq p_2 \\ p_1p_2 \le x \\ p_i \equiv \pm 1 \pmod q}} \frac{x}{p_1p_2} \le x \sum_{q > z_1^{\alpha}} \left(\sum_{\substack{p \le x \\ p \equiv \pm 1 \pmod q}} \frac{1}{p} \right)^2 \\ &\ll x \sum_{q > z_1^{\alpha}} \left(\frac{\log\log x}{q-1} \right)^2 \ll x(\log\log x)^2 \sum_{q > z_1^{\alpha}} \frac{1}{q^2} \\ &\ll \frac{x(\log\log x)^2}{z_1^{\alpha}} = \frac{x(\log\log x)^2}{(\log x)^{3\alpha}}, \end{aligned} \tag{4.7}$$

donde hemos usado la desigualdad (ii) del Teorema 2.9. Consideremos ahora el segundo caso y sea $\mathcal{M}_{5,2}(x)$ el conjunto de las $n \leq x$ que caen en este segundo caso. Entonces n es divisible entre algunos primos p y $q \geq z_1^\alpha$, con $q \mid z(p)$. Para p y q fijos, el número de dichas $n \leq x$ es cuando mucho x/pq. Sumando sobre todos los q que dividen a $z(p)$ (y por lo tanto, a $p-1$ o $p+1$) y que son mayores que z_1^α, y luego sobre todos los primos $p \leq x$, obtenemos que

$$\#\mathcal{M}_{5,2}(x) \leq \sum_{p \leq x} \sum_{\substack{q \mid z(p) \\ q > z_1^\alpha}} \frac{x}{pq} \leq \frac{x}{z_1^\alpha} \sum_{p \leq x} \frac{\omega(p-1) + \omega(p+1)}{p} \ll \frac{x(\log\log x)^2}{(\log x)^{3\alpha}}, \tag{4.8}$$

donde la última cota se sigue del Teorema 2.6.

Recopilando los resultados (4.7) y (4.8), obtenemos que

$$\#\mathcal{M}_5(x) \ll \frac{x(\log\log x)^2}{(\log x)^{3\alpha}}. \tag{4.9}$$

Dado un primo p ponemos $z(p) = a_p b_p$ donde $P(a_p) \leq (\log p)^3$ y b_p tiene sólamente factores primos mayores que $(\log p)^3$. Sea $z_2 = \exp(18(\log\log x)^2)$ y definimos

$$\mathcal{M}_6(x) = \{n \leq x : a_p > z_2 \text{ para algún primo } p \mid n\}.$$

Consideremos $n \in \mathcal{M}_6(x)$. Entonces existe un factor primo p de n tal que $a_p > z_2$. Como $a_p \mid p \pm 1$ para x grande, tenemos que $p \equiv \pm 1 \pmod{a_p}$. Entonces, $p = \pm 1 + a_p\lambda$ para algún entero positivo λ. Fijando $a = a_p$ y λ, el número de $n \leq x$ con estos parámetros es cuando mucho

$$\frac{x}{1 + a_p\lambda} + \frac{x}{-1 + a_p\lambda} \leq \frac{3x}{a_p\lambda}$$

para x suficientemente grande. Obsérvese que a_p está en el conjunto

$$A = \{a \leq x : a > z_2 : P(a) \leq z_1\}.$$

Sumando sobre todos los posibles valores de a y λ, tenemos que

$$\begin{aligned} \#\mathcal{M}_6(x) &\leq \sum_{\substack{a \in A \\ 1 \leq \lambda \leq x}} \frac{3x}{a\lambda} \leq 3x \left(\sum_{\substack{z_2 < a \leq x \\ P(a) \leq z_1}} \frac{1}{a} \right) \left(\sum_{1 \leq \lambda \leq x} \frac{1}{\lambda} \right) \\ &\ll x \log x \int_{z_2}^{x} \frac{\mathrm{d}\Psi(t, z_1)}{t} \\ &\ll x \log x \left(\frac{\Psi(t, z_1)}{t} \Big|_{t=z_2}^{t=x} + \int_{z_2}^{x} \frac{\Psi(t, z_1)}{t^2} \mathrm{d}t \right). \end{aligned} \tag{4.10}$$

Como $t \geq z_2$, tenemos que

$$\frac{\log t}{\log z_1} \geq \frac{18(\log\log x)^2}{3\log\log x} = 6\log\log x.$$

Por el Teorema 2.13 se sigue que

$$\Psi(t, z_1) \ll t\exp\left(-\frac{\log t}{2\log z_1}\right) \leq \frac{t}{(\log x)^3}$$

para todo $t \in [z_2, x]$. Usando esto en (4.10), obtenemos

$$\#\mathcal{M}_6(x) \ll x\log x\left(\frac{1}{(\log x)^3} + \frac{1}{(\log x)^3}\int_{z_2}^{x}\frac{\mathrm{d}t}{t}\right) \ll \frac{x}{\log x}. \tag{4.11}$$

Ahora definimos $z_3 = \exp((\log x)^\alpha)$ y vamos a descartar a los enteros positivos n que tienen un factor primo $p > z_3$ para el cuál $z(p)$ es "pequeño" en un sentido que se precisará después. Tomamos $c = 20\alpha^{-2}$ y definimos los siguientes conjuntos de primos

$$\begin{aligned}
\mathcal{Q}_1 &= \left\{p : z(p) < \frac{p^{1/2}}{\log p}\right\};\\
\mathcal{Q}_2 &= \left\{p : \frac{p^{1/2}}{\log p} < z(p) < p^{1/2}\exp\left(c(\log\log p)^2\right)\right\}.
\end{aligned}$$

Necesitaremos cotas para los tamaños de $\mathcal{Q}_1(t)$ y $\mathcal{Q}_2(t)$. Para $\#\mathcal{Q}_1(t)$, tenemos

$$\#\mathcal{Q}_1(t) \leq \#\left\{p \leq t : z(p) \leq \frac{t^{1/2}}{\log t}\right\} \leq \#\mathcal{P}_{t^{1/2}/\log t} \ll \frac{t}{(\log t)^3}, \tag{4.12}$$

por el Lema 4 con $y = t^{1/2}/\log t$. Para $\#\mathcal{Q}_2(t)$, primero consideramos $\mathcal{Q}_2 \cap [t/2, t]$. Sea p un primo en $\mathcal{Q}_2 \cap [t/2, t]$ donde t es grande. Entonces

$$\begin{aligned}
z(p) &> \frac{p^{1/2}}{\log p} > \frac{t^{1/2}}{2^{1/2}\log(t/2)} > \frac{t^{1/2}}{2\log t};\\
z(p) &< p^{1/2}\exp\left(c(\log\log p)^2\right) < t^{1/2}\exp\left(c(\log\log t)^2\right).
\end{aligned}$$

Como $t^{1/2}/(2\log t) > 5$ para t grande, tenemos que $z(p) \mid p\pm 1$. En particular, estos primos p tienen la propiedad de que $p+1$ o $p-1$ tiene un dividor en el intervalo (y, z), donde $y = t^{1/2}/(2\log t)$ y $z = t^{1/2}\exp\left(c(\log\log t)^2\right)$. Para

acotar la cantidad de dichos primos usamos el Lema 2.15. Las hipótesis del lema se satisfacen (con $x = t$) siempre que $t > \exp(5300)$. Tenemos que

$$\begin{aligned} u &= \frac{\log z}{\log y} - 1 = \frac{\log(t^{1/2}\exp\left(c(\log\log t)^2\right)}{\log(t^{1/2}/(2\log t))} - 1 \\ &= \frac{\log t^{1/2} + c(\log\log t)^2}{\log t^{1/2} - \log\log t - \log 2} - 1 \\ &= \frac{c(\log\log t)^2 + \log\log t + \log 2}{\log t^{1/2} - \log\log t - \log 2} \\ &= (2c + o(1))\frac{(\log\log t)^2}{\log t} \end{aligned}$$

cuando $t \to \infty$. Entonces, por el Lema 2.15,

$$\begin{aligned} H(t,y,z) &\ll tu^{\delta}\log(2/u)^{-3/2} \\ &\ll t\left(\frac{(\log\log t)^2}{\log t}\right)^{\delta}\left(\log\left(O\left(\frac{\log t}{(\log\log t)^2}\right)\right)\right)^{-3/2} \\ &\ll \frac{t}{(\log t)^{\delta}(\log\log t)^{3/2-2\delta}} \ll \frac{t}{(\log t)^{\delta}}, \end{aligned}$$

y

$$\#(\mathcal{Q}_2 \cap [t/2,t]) \le \sum_{\lambda\in\{\pm 1\}} H(t,y,z,P_\lambda) \ll \frac{H(t,y,z)}{\log t} \ll \frac{t}{(\log t)^{1+\delta}}. \quad (4.13)$$

Remplazando t por $t/2$, y luego por $t/4$, etc. y sumando las desigualdades, obtenemos

$$\#\mathcal{Q}_2(t) \ll \frac{t}{(\log t)^{1+\delta}}. \quad (4.14)$$

Comparando (4.14) con (4.12), vemos que si ponemos $\mathcal{Q}_3 = \mathcal{Q}_1 \cup \mathcal{Q}_2$, entonces

$$\#\mathcal{Q}_3(t) \le \#\mathcal{Q}_1(t) + \#\mathcal{Q}_2(t) \ll \frac{t}{(\log t)^{1+\delta}}.$$

Ahora definimos

$$\mathcal{M}_7(x) = \{n \le x : \text{ existe } \ p > z_3,\ p \mid n,\ p \in \mathcal{Q}_3\}.$$

Si $n \in \mathcal{M}_7(x)$, entonces $p \mid n$ para algún primo $p > z_3$ en $\mathcal{Q}_3$. Si fijamos p, hay $\lfloor x/p \rfloor \le x/p$ posibles valores para $n \le x$. Sumando estas desigualdades

para todos los posibles valores de p, tenemos

$$\begin{aligned}
\#\mathcal{M}_7(x) &\leq \sum_{\substack{z_3\leq p\leq x\\ p\in\mathcal{Q}_3}} \frac{x}{p} = x\int_{z_3}^{x} \frac{\mathrm{d}(\#\mathcal{Q}_3(t))}{t} \\
&= x\left(\frac{\#\mathcal{Q}_3(t)}{t}\Big|_{t=z_3}^{t=x} + \int_{z_3}^{x} \frac{\#\mathcal{Q}_3(t)}{t^2}\mathrm{d}t\right) \\
&\ll x\left(\frac{1}{(\log t)^{1+\delta}}\Big|_{t=z_3}^{t=x} + \int_{z_3}^{x} \frac{\mathrm{d}t}{t(\log t)^{1+\delta}}\right) \\
&\ll x\left(\frac{1}{(\log x)^{1+\delta}} + \left(-\frac{1}{\delta(\log t)^{\delta}}\Big|_{t=z_3}^{t=x}\right)\right) \\
&\ll \frac{x}{(\log z_3)^{\delta}} = \frac{x}{(\log x)^{\alpha\delta}}. \qquad (4.15)
\end{aligned}$$

Sea $\beta \in (0, 1-\alpha)$ y definimos $K = \lfloor \beta \log\log x \rfloor$, $y_2 = \exp(\log x/(\log\log x)^2)$, $\mathcal{I} = (z_3, y_2)$ y

$$\omega_{\mathcal{I}}(n) = \sum_{\substack{p\in\mathcal{I}\\ p|n}} 1.$$

Sea

$$\mathcal{M}_8(x) = \{n \leq x : n \notin \mathcal{M}_2(x), \omega_{\mathcal{I}}(n) < K\}.$$

La siguiente prueba de (4.19) imita la prueba de los Teoremas 08 y 09 de [HT].

Sea $n \in \mathcal{M}_8(x)$. Como $n \notin \mathcal{M}_2(x)$, se tiene $p^2 \nmid n$ para $p > z_1$. Para x suficientemente grande, tenemos que $z_3 > z_1$, por lo que si $p \in \mathcal{I}$ divide a n, entonces $p^2 \nmid n$. Entonces, para x suficientemente grande, podemos descomponer a n de manera única como $n = uv$, donde v no tiene primos de $\mathcal{I}$ y u es libre de cuadrados y tiene $\ell < K$ factores primos, todos en $\mathcal{I}$. Fijemos u. Entonces $v \leq x/u$ y observese que

$$\frac{x}{u} \geq \frac{x}{y_2^K} \geq y_2,$$

para x suficientemente grande. En particular, $\mathcal{I} \subset [1, x/u]$. Por el teorema 2.11, el número de posibles elecciones para v es de orden a lo más

$$\frac{x}{u}\prod_{p\in\mathcal{I}}\left(1-\frac{1}{p}\right) \ll \frac{x}{u}\exp(-S), \qquad (4.16)$$

donde

$$S = \sum_{p\in\mathcal{I}} \frac{1}{p}.$$

Por el Segundo Teorema de Mertens, tenemos que

$$S = \log\log y_2 - \log\log z_3 + o(1) = (1-\alpha)\log\log x - 2\log\log\log x + o(1) \tag{4.17}$$

cuando $x \to \infty$. Entonces,

$$\exp(S) = (1+o(1))\frac{(\log x)^{1-\alpha}}{(\log\log x)^2} \quad \text{cuando} \quad x \to \infty.$$

Sea $\mathcal{U}$ el conjunto de las u's que estamos considerando, es decir, libres de cuadrados y con menos de K factores primos, todos en $\mathcal{I}$. Sumando la desigualdad (4.16) sobre todos los $u \in \mathcal{U}$, obtenemos

$$\begin{aligned} \#\mathcal{M}_8(x) &\ll \frac{x(\log\log x)^2}{(\log x)^{1-\alpha}} \sum_{u\in\mathcal{U}} \frac{1}{u} \le \frac{x(\log\log x)^2}{(\log x)^{1-\alpha}} \sum_{\ell<K} \frac{1}{\ell!} \left(\sum_{p\in\mathcal{I}} \frac{1}{p}\right)^{\ell} \\ &= \frac{x(\log\log x)^2}{(\log x)^{1-\alpha}} \sum_{\ell<K} \frac{1}{\ell!} S^{\ell}. \end{aligned} \tag{4.18}$$

Observese que para $\ell < K$, tenemos, por (4.17),

$$\frac{S^{\ell+1}/(\ell+1)!}{S^{\ell}/\ell!} = \frac{S}{\ell+1} \ge \frac{(1-\alpha)\log\log x - 2\log\log\log x + o(1)}{\beta\log\log x + 1} > \eta$$

para x suficientemente grande, donde podemos escoger cualquier $\eta \in (1, (1-\alpha)/\beta)$, por lo tanto, la última suma en (4.18) está dominada por el término correspondiente a $\ell = K$. Entonces, usando que $K! \ge (K/e)^K$, tenemos

$$\begin{aligned} \#\mathcal{M}_8(x) &\ll \frac{x(\log\log x)^2}{(\log x)^{1-\alpha}} \frac{S^K}{K!} \ll \frac{x(\log\log x)^2}{(\log x)^{1-\alpha}} \\ &\times \left(\frac{e(1-\alpha)\log\log x - 2e\log\log\log x + o(1)}{\beta\log\log x + O(1)}\right)^{\beta\log\log x + O(1)} \\ &\ll \frac{x(\log\log x)^2}{(\log x)^{1-\alpha}} \left(\frac{e(1-\alpha)}{\beta} + O\left(\frac{\log\log\log x}{\log\log x}\right)\right)^{\beta\log\log x + O(1)} \\ &\ll \frac{x(\log\log x)^{O(1)}}{(\log x)^{\gamma}}, \end{aligned} \tag{4.19}$$

donde

$$\gamma = 1 - \alpha - \beta\log\left(\frac{e(1-\alpha)}{\beta}\right).$$

Finalmente consideramos $\mathcal{M}_9(x) = \mathcal{M}(x) \setminus \left(\bigcup_{i=1}^{8} \mathcal{M}_i(x) \right)$. Sea $n \in \mathcal{M}_9(x)$. Podemos escribir como $n = mP$, donde $P = P(n) > y_1$ (porque $n \notin \mathcal{M}_1(x)$), y $P \nmid m$ para x suficientemente grande (porque $n \notin \mathcal{M}_2(x)$ y $y_1 > z_1$ para x suficientemente grande). Fijemos m. Observemos que $y_1 > y_2$ para todo $x > e$. Como $n \notin \mathcal{M}_8(x)$, existen K factores primos de m todos en $\mathcal{I}$. Sea $p_1, \ldots, p_K$ los más pequeños de estos primos. Definimos

$$U(m) = [t(p_1), \ldots, t(p_K)].$$

Recordemos que $t(p_i) = \delta(p_i) z(p_i)$, donde $\delta(p_i) \in \{1, 2, 4\}$ para cada $i = 1, \ldots, K$. Además, $z(p_i) = a_{p_i} b_{p_i}$ para cada $i = 1, \ldots, K$, donde a_{p_i} es $(\log p_i)^3$-suave y todos los factores primos de b_{p_i} son mayores que $(\log p_i)^3$. Ahora, como $n \notin \mathcal{M}_6(x)$, se tiene que $a_{p_i} \leq z_2$ para cada $i = 1, \ldots, K$. Como todos los factores primos de b_{p_i} son mayores que

$$(\log p_i)^3 \geq (\log z_3)^3 = (\log x)^{3\alpha} = z_1^{\alpha} \quad \text{para todo} \quad i = 1, \ldots, K,$$

y como $n \notin \mathcal{M}_5(x)$, se tiene que b_{p_i} y b_{p_j} son primos relativos para cualesquiera $i \neq j$ en $\{1, 2, \ldots, K\}$. Entonces,

$$U(m) \mid [\delta(p_1) a_{p_1}, \ldots, \delta(p_K) a_{p_K}] b_{p_1} \cdots b_{p_K}.$$

Definiendo

$$V(m) = [\delta(p_1) a_{p_1}, \ldots, \delta(p_K) a_{p_K}]$$

observamos que

$$V(m) \leq 4 \prod_{i=1}^{K} a_{p_i} \leq 4 z_2^K = 4 \exp\left(18\beta (\log\log x)^3\right).$$

Por lo tanto $V(m) < y_1$ para x suficientemente grande. Consideremos P en una clase de congruencia fija $w \pmod{V(m)}$, donde $w \in \{1, 2, \ldots, V(m)\}$ y es primo relativo con $V(m)$. Entonces $P \leq x/m$ y $P \equiv w \pmod{V(m)}$. Esto nos dice que $P = w + V(m)\lambda$ para algún entero $\lambda \geq 1$. Entonces,

$$n = mP = p_i \left(m/p_i (w + V(m)\lambda)\right) \quad \text{para todo} \quad i = 1, \ldots, K.$$

Tomamos $c_i = wm/p_i$ y $d_i = V(m)m/p_i$ para $i = 1, \ldots, K$. Por (4.6), tenemos que

$$\left(\frac{F_{c_i + d_i \lambda}}{p_i} \right) = \left(\frac{F_{p_i}}{p_i} \right). \tag{4.20}$$

Observemos que como $n \notin \mathcal{M}_7(x)$, tenemos que

$$b_{p_i} = \frac{z(p_i)}{a_{p_i}} \geq p_i^{1/2} \exp(c(\log\log p_i)^2) z_2^{-1}.$$

Pero

$$\begin{aligned} \exp(c(\log\log p_i)^2) z_2^{-1} &\geq \exp(c(\log\log z_3)^2) z_2^{-1} \\ &= \exp(c\alpha^2(\log\log x)^2) z_2^{-1} \\ &= \exp(2(\log\log x)^2). \end{aligned}$$

Entonces,

$$b_{p_i} \geq p_i^{1/2} \exp(2(\log\log x)^2) \quad \text{para todo} \quad i = 1, \ldots, K. \tag{4.21}$$

Ahora veremos que el periodo t_{c_i,d_i,p_i} de $(F_{c_i+d_ik})_{k\geq 0}$ módulo p_i es

$$t_{c_i,d_i,p_i} = \frac{t_{p_i}}{(t_{p_i}, V(m)m/p_i)} = b_{p_i} \quad \text{para todo} \quad i = 1, \ldots, K. \tag{4.22}$$

Para esto, usamos el Lema 6. Es claro que $p_i > 5$ para x suficientemente grande (basta que $z_3 > 5$). Veamos que $z(p_i) \nmid d_i$. Si este no fuera el caso, tendríamos que $b_{p_i} \mid z(p_i) \mid d_i \mid V(m)m$. Sin embargo, el divisor $b_{p_i} > 1$ de $z(p_i)$ es divisible sólo entre primos $q > z_1^{\alpha}$, y dichos primos no pueden dividir a m, porque entonces dividirían a n y a $z(n)$, lo cual no es posible porque $n \notin \mathcal{M}_5(x)$, y tampoco pueden a $V(m)$ pues entonces dividirían a a_{p_j} para algún j (necesariamente distinto de i), y por tanto a $z(p_j)$ para algún $j \neq i$ contradiciendo otra vez que $n \notin \mathcal{M}_5(x)$. Esto prueba 4.22.

Definimos

$$\begin{aligned} A_i^+ &= \left\{ \lambda \bmod b_{p_i} : \left(\frac{F_{c_i+d_i\lambda}}{p}\right) = 1 \right\}, \\ A_i^- &= \left\{ \lambda \bmod b_{p_i} : \left(\frac{F_{c_i+d_i\lambda}}{p}\right) = -1 \right\}. \end{aligned}$$

Tenemos que

$$\#A_i^+ + \#A_i^- = b_{p_i} \quad \text{y} \quad |\#A_i^+ - \#A_i^-| = O(p_i^{1/2}),$$

por el Lema 2.16. Tenemos entonces que

$$\#A_i^{\pm} = \frac{b_{p_i}}{2} + O(p_i^{1/2}) = \frac{b_{p_i}}{2}\left(1 + O\left(\frac{1}{\exp(2(\log\log x)^2)}\right)\right), \tag{4.23}$$

como consecuencia de (4.21). Observese que para cada i fijo, por (4.20), la clase de residuos λ (mód b_{p_i}) esta en A_i^+ o A_i^- dependiendo de si $\left(\frac{F_{p_i}}{p_i}\right)$ es $+1$ o -1 respectivamente. Tomemos $\varepsilon_i \in \{+,-\}$ el signo de $\left(\frac{F_{p_i}}{p_i}\right)$. Para cada $i = 1,\dots,K$, fijemos $\mu_i \in A_i^{\varepsilon_i}$. Contemos el número de primos P tales que $\lambda \equiv \mu_i$ (mód b_{p_i}) para $i = 1,\dots,K$. Por el Teorema Chino del Residuo (recordemos que b_{p_i} y b_{p_j} son primos relativos si $i \neq j$), el sistema de congruencias anterior es equivalente a la congruencia

$$\lambda \equiv \mu_0 \pmod{B(m)},$$

donde $B(m) = b_{p_1} \cdots b_{p_K}$ y $\mu_0 = \mu_0(\mu_1,\dots,\mu_K)$. Entonces,

$$P = w + V(m)\mu_0 + V(m)B(m)k, \tag{4.24}$$

para algún entero no negativo k. Podemos suponer que $w + V(m)\mu_0$ es primo relativo con $V(m)B(m)$, pues de otra manera habría a lo más un primo en esta progresión. Entonces $P \leq x/m$ está en una progresión fija módulo $V(m)B(m)$. Observese que $b_{p_i} < p_i$ para cada $i = 1,\dots,K$ si x es suficientemente grande. Entonces

$$\begin{aligned} V(m)B(m) &\leq 4\exp(18\beta(\log\log x)^3)y_2^K \\ &\leq 4\exp\left(\frac{\beta\log x}{\log\log x} + 18\beta(\log\log x)^3\right) \\ &< \exp\left(\frac{\eta\log x}{\log\log x}\right) \end{aligned} \tag{4.25}$$

para cualquier $\eta \in (\beta,1)$ fijo, si x es suficientemente grande. En particular,

$$V(m)B(m) < y_1 < x/m$$

para todo x suficientemente grande. Entonces el número de primos $P \leq x/m$ de la forma (4.24) es, por el Teorema 2.9 (i),

$$\pi(x/m, V(m)B(m), w + V(m)\mu_0) \ll \frac{x/m}{\varphi(V(m)B(m))\log(x/(mV(m)B(m)))}.$$

Por la desigualdad (4.25) y como $x/m > P > y_1$, tenemos que

$$\frac{x}{mV(m)B(m)} > \frac{y_1}{V(m)B(m)} > \exp\left(\frac{(1-\eta)\log x}{\log\log x}\right).$$

Usando también que $\varphi(\ell)/\ell \gg 1/\log\log x$ para todos los enteros positivos $\ell \leq x$, tenemos que

$$\pi(x/m, V(m)B(m), w + V(m)\mu_0) \ll \frac{x(\log\log x)^2}{mV(m)B(m)\log x}.$$

Ahora fijamos w, sumamos sobre todos los posibles valores de $\mu_i \in A_i^{\varepsilon_i}$, y usamos las desigualdades (4.23)

$$\begin{aligned}
&\sum_{\substack{\mu_i \in A_i^{\varepsilon_i} \\ i=1,\dots,K}} \pi\left(x/m, V(m)B(m), w + V(m)\mu_0\right) \\
\ll\ & \frac{x(\log\log x)^2}{mV(m)\log x} \prod_{i=1}^{K} \frac{\#A_i^{\varepsilon_i}}{b_{p_i}} \\
\ll\ & \frac{x(\log\log x)^2}{mV(m)\log x} \frac{1}{2^K} \left(1 + O\left(\frac{1}{\exp(2(\log\log x)^2)}\right)\right)^{\beta \log\log x} \\
\ll\ & \frac{x(\log\log x)^2}{2^K mV(m)\log x}.
\end{aligned}$$

Sumando ahora sobre las $\varphi(V(m))$ posibles clases de congruencia módulo $V(m)$, y sobre todos los posibles valores de $m < x/y_1$ obtenemos que

$$\begin{aligned}
\#\mathcal{M}_9(x) \ &\ll \sum_{m<x/y_1} \frac{x(\log\log x)^2}{2^K m\log x}\left(\frac{\varphi(V(m))}{V(m)}\right) < \frac{x(\log\log x)^2}{2^K\log x} \sum_{1\leq m\leq x} \frac{1}{m} \\
&\ll \frac{x(\log\log x)^2}{(\log x)^{\beta\log 2}}. \qquad (4.26)
\end{aligned}$$

Comparando las cotas (4.1), (4.2), (4.3), (4.4), (4.9), (4.11), (4.15), (4.19), (4.26), obtenemos

$$\#\mathcal{M}(x) \ll \frac{x}{(\log x)^{\min\{\alpha\delta, \gamma, \beta\log 2\}}}.$$

Escogemos α y β de manera que $\alpha\delta = \gamma = \beta\log 2$. Entonces, $\beta = \alpha\delta/\log 2$, y tenemos que

$$\alpha\delta = 1 - \alpha - \frac{\alpha\delta}{\log 2}\log\left(\frac{e(1-\alpha)\log 2}{\alpha\delta}\right).$$

Esta ecuación tiene dos soluciones en el intervalo $(0,1)$, pero sólo una de ellas cumple que $\beta < 1-\alpha$. Esa solución es $\alpha = 0.7504\ldots$, que nos da $\alpha\delta = 0.0645\ldots$ y esto termina la prueba de la cota superior de $\#\mathcal{M}(x)$.

4.3.2. Cota Inferior

Para obtener una cota inferior muy holgada de manera sencilla podemos ver que $p^2 \in \mathcal{M}$ para todo $p > 5$. Para esto tomamos $n = (p^2-1)/2$ en la conocida identidad

$$F_{2n+1} = F_{n+1}^2 + F_n^2, \tag{4.27}$$

y obtenemos

$$F_{p^2} = F_{(p^2+1)/2}^2 + F_{(p^2-1)/2}^2 = u^2 + p^2 v^2, \quad (u, v) = (F_{(p^2+1)/2}, F_{(p^2-1)/2}/p).$$

Como $z(p) \mid p \pm 1$ para todo $p > 5$, se tiene que $z(p) \mid (p^2-1)/2$, por lo que $v = F_{(p^2-1)/2}/p$ es entero, y por lo tanto $p^2 \in \mathcal{M}$.

Como consecuencia del Teorema del Número Primo (Teorema 2.7), obtenemos la cota

$$\frac{\sqrt{x}}{\log x} \ll \#\mathcal{M}(x)$$

Cálculos con la ayuda de la computadora muestran que, para primos $p < 350$, $p \in \mathcal{M}$ si $p = 2$ ó $p \equiv 1 \pmod 4$ y que $p \notin \mathcal{M}$ si $p \equiv 3 \pmod 4$. Esto sugiere la siguiente conjetura:

Conjetura. *Un primo p está en $\mathcal{M}$ si y sólo si $p = 2$ ó $p \equiv 1 \pmod 4$.*

Veamos que si $p \equiv 3 \pmod 4$ y además $p \equiv \pm 2 \pmod 5$, entonces efectivamente $F_p = x^2 + py^2$ no tiene solución. De tenerse esta igualdad, tendríamos que $F_p \equiv x^2 \pmod p$, por lo que $\left(\frac{F_p}{p}\right) = 1$. Por otra parte, como

$$F_p \equiv 5^{(p-1)/2} \equiv \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{\pm 2}{5}\right) = -1 \pmod p$$

tenemos que $\left(\frac{F_p}{p}\right) = \left(\frac{-1}{p}\right) = -1$, lo cual es una contradicción.

Demostrar que para los primos $p \equiv 3 \pmod 4$ y $p \equiv \pm 1 \pmod 5$ la ecuación no tiene solución parece ser más difícil.

Sin embargo, vamos a demostrar que si $p \equiv 1 \pmod 4$ entonces sí ocurre que $p \in \mathcal{M}$.

Como $F_5 = 0^2 + 5 \cdot 1^2$, podemos suponer que $p > 5$. Dado m un entero positivo denotaremos con ζ_m una raíz m-ésima de la unidad. También definimos

$$\mathbb{L} = \mathbb{Q}(\zeta_p, \sqrt{5}, i), \quad \text{donde} \quad i^2 = -1.$$

Dado un entero d, abreviamos $\mathbb{Q}(\sqrt{d})$ como $\mathbb{Q}_d$. Usamos, como antes, α y β para denotar a $\frac{1+\sqrt{5}}{2}$ y $\frac{1-\sqrt{5}}{2}$ respectivamente. Primero probaremos que

$$N_{\mathbb{L}/\mathbb{Q}_5}(\alpha - i\zeta_p) = \alpha^{p-1}F_p, \quad \text{de donde} \quad N(\alpha - i\zeta_p) = F_p^2 \tag{4.28}$$

Empezamos notando que $[\mathbb{L} : \mathbb{Q}] = 4(p-1)$. Y de hecho,

$$G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q}) = \langle\tau\rangle \times \langle\sigma_5\rangle \times \langle\sigma_{-1}\rangle,$$

donde

- $\tau(\zeta_p) = \zeta_p^g$ para algún generador fijo g de $\mathbb{Z}_p^*$, $\tau(\sqrt{5}) = \sqrt{5}$ y $\tau(i) = i$;
- $\sigma_5(\zeta_p) = \zeta_p$, $\sigma_5(\sqrt{5}) = -\sqrt{5}$ y $\sigma_5(i) = i$;
- $\sigma_{-1}(\zeta_p) = \zeta_p$, $\sigma_{-1}(\sqrt{5}) = \sqrt{5}$ y $\sigma_{-1}(i) = -i$.

También observamos que $\mathbb{L} = \mathbb{Q}_5(\zeta_p, i) = \mathbb{Q}_5(\zeta_{4p})$ y que

$$\mathrm{Gal}(\mathbb{L}/\mathbb{Q}_5) = \langle\tau\rangle \times \langle\sigma_{-1}\rangle. \tag{4.29}$$

Tenemos que

$$\alpha^{p-1}F_p = \frac{\alpha^p(\alpha^p - \beta^p)}{\alpha(\alpha - \beta)} = \frac{\alpha^{2p}+1}{\alpha^2+1} = \Phi_{4p}(\alpha),$$

donde $\Phi_n(x)$ es el n-ésimo polinomio ciclotómico. Se puede ver que $i\zeta_p = \exp\left((2(p+4)\pi i/4p\right)$ y $(p+4, p) = 1$, de donde se sigue que $i\zeta_p$ es una raíz $4p$-ésima de la unidad. Entonces

$$\Phi_{4p}(\alpha) = \prod_{\substack{1\le k\le 4p\\(k,4p)=1}} (\alpha - (i\zeta_p)^k).$$

Por (4.29), se puede ver a

$$\{i\zeta_p \mapsto (i\zeta_p)^k : 1 \le k \le 4p,\ (k, 4p) = 1\}$$

como el grupo $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}_5)$, de donde

$$\Phi_{4p}(\alpha) = \prod_{\sigma\in\mathrm{Gal}(\mathbb{L}/\mathbb{Q}_5)} (\alpha - \sigma(i\zeta_p)) = \prod_{\sigma\in\mathrm{Gal}(\mathbb{L}/\mathbb{Q}_5)} \sigma(\alpha - i\zeta_p) = N_{\mathbb{L}/\mathbb{Q}_5}(\alpha - i\zeta_p),$$

lo que prueba (4.28).

Ahora veremos que

$$N_{\mathbb{L}/\mathbb{Q}_{-p}}(\alpha - i\zeta_p) = \delta^2 \tag{4.30}$$

para algún elemento $\delta = u + v\sqrt{-p} \in \mathbb{Z}[\sqrt{-p}]$.

Se sabe que $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ es el único subcampo cuadrático de $\mathbb{K} = \mathbb{Q}(\zeta_p)$. Para ver esto, observemos que el discriminante de $\mathbb{K}$, denotado por $d_{\mathbb{K}}$, is $(-1)^{(p-1)/2}p^{p-2}$ (Ejercicio 4.5.10 de [EM]). Como $\mathbb{K}$ es de Galois, tenemos que $\sqrt{d_{\mathbb{K}}} \in \mathbb{K}$, de donde $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p}) \subseteq \mathbb{K}$. Que este sea el único subcampo cuadrático de $\mathbb{K}$ es consecuencia de la correspondencia de Galois, pues el grupo de Galois de $\mathbb{K}/\mathbb{Q}$ es cíclico, por lo que contiene un único subgrupo de índice 2.

Como $p \equiv 1 \pmod 4$ tenemos que $\mathbb{Q}_p$ está contenido en $\mathbb{L}$, y como $i \in \mathbb{L}$, tenemos que $\mathbb{Q}_{-p}$ también es un subcampo de $\mathbb{L}$. Calculemos $N_{\mathbb{L}/\mathbb{Q}_{-p}}(\alpha - i\zeta_p)$.

Para esto, observamos que

$$\mathrm{Gal}(\mathbb{L}/\mathbb{Q}_{-p}) = \langle \tau\sigma_{-1} \rangle \times \langle \sigma_5 \rangle. \tag{4.31}$$

En efecto, tenemos que τ^2 fija a $\sqrt{p}$ pero τ no. Esto nos dice que $\tau(\sqrt{p}) = -\sqrt{p}$. Además, $\sigma_{-1}(i) = -i$, lo que nos dice que $\tau\sigma_{-1}$ deja fijo a $i\sqrt{p}$. Por otra parte, σ_5 fija tanto a i como a ζ_p, y por lo tanto también a $i\sqrt{p}$. Entonces, todos los elementos del subgrupo $\langle \tau\sigma_{-1} \rangle \times \langle \sigma_5 \rangle$ de G fijan a $i\sqrt{p}$. Pero este es un subgrupo de G con $2(p-1) = [\mathbb{L} : \mathbb{Q}_{-p}]$ elementos, por lo que se tiene (4.31).

Tenemos entonces que

$$\begin{aligned}
N_{\mathbb{L}/\mathbb{Q}_{-p}}(\alpha - i\zeta_p) &= \prod_{k=1}^{p-1} \Big(\alpha - (\tau\sigma_{-1})^k(i\zeta_p)\Big)\Big(\beta - (\tau\sigma_{-1})^k(i\zeta_p)\Big) \\
&= \prod_{k=1}^{p-1} \Big(\alpha - \tau^k(\zeta_p)\sigma_{-1}^k(i)\Big)\Big(\beta - \tau^k(\zeta_p)\sigma_{-1}^k(i)\Big) \\
&= \prod_{k=1}^{p-1} \Big(\alpha - (-1)^k i\zeta_p^{g^k}\Big)\Big(\beta - (-1)^k i\zeta_p^{g^k}\Big) \\
&= \prod_{a=1}^{p-1} \left(\alpha - \left(\frac{a}{p}\right) i\zeta_p^a\right)\left(\beta - \left(\frac{a}{p}\right) i\zeta_p^a\right) \\
&= \prod_{a=1}^{(p-1)/2} \left(\alpha - \left(\frac{a}{p}\right) i\zeta_p^a\right)\left(\beta - \left(\frac{a}{p}\right) i\zeta_p^a\right)\left(\alpha - \left(\frac{-a}{p}\right) i\zeta_p^{-a}\right)\left(\beta - \left(\frac{-a}{p}\right) i\zeta_p^{-a}\right).
\end{aligned}$$

Aquí hemos usado que cuando k varía de 1 a $p-1$, g^k también lo hace y que $(-1)^k = \left(\frac{g^k}{p}\right)$. Como $p \equiv 1 \pmod 4$, tenemos que $\left(\frac{-1}{p}\right) = 1$. Usando también que $\alpha\beta = -1$ y que $i = -i^{-1}$, tenemos que $N_{\mathbb{L}/\mathbb{Q}_{-p}}(\alpha - i\zeta_p)$ es

$$\begin{aligned}
&\prod_{a=1}^{(p-1)/2} \left(\alpha - \left(\frac{a}{p}\right) i\zeta_p^a\right)\left(\beta - \left(\frac{a}{p}\right) i\zeta_p^a\right)\left(\alpha - \left(\frac{-a}{p}\right) i\zeta_p^{-a}\right)\left(\beta - \left(\frac{-a}{p}\right) i\zeta_p^{-a}\right) \\
= &\prod_{a=1}^{(p-1)/2} \left(\alpha - \left(\frac{a}{p}\right) i\zeta_p^a\right)\left(\beta - \left(\frac{a}{p}\right) i\zeta_p^a\right)\left(\frac{-1}{\beta} + \left(\frac{a}{p}\right)\frac{1}{i\zeta_p^a}\right)\left(\frac{-1}{\alpha} + \left(\frac{a}{p}\right)\frac{1}{i\zeta_p^a}\right) \\
= &\prod_{a=1}^{(p-1)/2} \left(\alpha - \left(\frac{a}{p}\right) i\zeta_p^a\right)\left(\beta - \left(\frac{a}{p}\right) i\zeta_p^a\right)\left(\frac{\beta - \left(\frac{a}{p}\right) i\zeta_p^a}{\beta\left(\frac{a}{p}\right) i\zeta_p^a}\right)\left(\frac{\alpha - \left(\frac{a}{p}\right) i\zeta_p^a}{\alpha\left(\frac{a}{p}\right) i\zeta_p^a}\right) \\
= &\prod_{a=1}^{(p-1)/2} \left(\alpha - \left(\frac{a}{p}\right) i\zeta_p^a\right)^2 \left(\beta - \left(\frac{a}{p}\right) i\zeta_p^a\right)^2 \zeta_p^{-2a} = \delta^2
\end{aligned}$$

donde

$$\delta = \prod_{a=1}^{(p-1)/2} \left(\alpha - \left(\frac{a}{p}\right) i\zeta_p^a\right)\left(\beta - \left(\frac{a}{p}\right) i\zeta_p^a\right)\zeta_p^{-a}.$$

Es claro que δ es un entero algebráico.

Mostremos ahora que $\delta \in \mathbb{Q}_{-p}$. Para esto, por (4.29), basta probar que $\tau\sigma_{-1}(\delta) = \delta$, pues obviamente σ_5 deja fijo a δ.

Tenemos que $\tau\sigma_{-1}(\delta)$ es igual a

$$
\begin{aligned}
& \prod_{a=1}^{(p-1)/2} \left(\alpha - \left(\frac{a}{p}\right)\sigma_{-1}(i)\tau(\zeta_p^a)\right)\left(\beta - \left(\frac{a}{p}\right)\sigma_{-1}(i)\tau(\zeta_p^a)\right)\tau(\zeta_p^{-a}) \\
= & \prod_{a=1}^{(p-1)/2} \left(\alpha - \left(\frac{a}{p}\right)(-1)\zeta_p^{ga}\right)\left(\beta - \left(\frac{a}{p}\right)(-i)\zeta_p^{ga}\right)\zeta_p^{-ga} \\
= & \prod_{a=1}^{(p-1)} \left(\alpha - \left(\frac{ga}{p}\right)i\zeta_p^{ga}\right)\left(\beta - \left(\frac{ga}{p}\right)i\zeta_p^{ga}\right) \quad \left(\text{ pues } \left(\frac{g}{p}\right) = -1\right) \\
= & \prod_{a=1}^{(p-1)/2} \left(\alpha - \left(\frac{\varepsilon_a a}{p}\right)i\zeta^{\varepsilon_a a}\right)\left(\beta - \left(\frac{\varepsilon_a a}{p}\right)i\zeta_p^{\varepsilon_a a}\right)\zeta_p^{-\varepsilon_a a} \quad (\text{con } \varepsilon_a = \pm 1) \\
= & \prod_{a=1}^{(p-1)/2} \left(\alpha - \left(\frac{a}{p}\right)i\zeta_p^{\varepsilon_a a}\right)\left(\beta - \left(\frac{a}{p}\right)\zeta_p^{\varepsilon_a a}\right)\zeta_p^{-\varepsilon_a a} \quad \left(\left(\frac{\varepsilon_a}{p}\right) = 1\right) \\
= & \prod_{\substack{a=1 \\ \varepsilon_a=1}}^{(p-1)/2} \left(\alpha - \left(\frac{a}{p}\right)i\zeta_p^{a}\right)\left(\beta - \left(\frac{a}{p}\right)i\zeta_p^{a}\right)\zeta_p^{-a} \\
\times & \prod_{\substack{a=1 \\ \varepsilon_a=-1}}^{(p-1)/2} \left(\alpha - \left(\frac{a}{p}\right)i\zeta_p^{-a}\right)\left(\beta - \left(\frac{a}{p}\right)i\zeta_p^{-a}\right)\zeta_p^{a} \\
= & \prod_{\substack{a=1 \\ \varepsilon_a=1}}^{(p-1)/2} \left(\alpha - \left(\frac{a}{p}\right)i\zeta_p^{a}\right)\left(\beta - \left(\frac{a}{p}\right)i\zeta_p^{a}\right)\zeta_p^{-a} \\
\times & \prod_{\substack{a=1 \\ \varepsilon_a=-1}}^{(p-1)/2} \left(\frac{\beta - \left(\frac{a}{p}\right)i\zeta_p^{a}}{\beta\left(\frac{a}{p}\right)i\zeta_p^{a}}\right)\left(\frac{\alpha - \left(\frac{a}{p}\right)i\zeta_p^{a}}{\alpha\left(\frac{a}{p}\right)i\zeta_p^{a}}\right)\zeta_p^{-a} \\
= & \prod_{\substack{a=1 \\ \varepsilon_a=1}}^{(p-1)/2} \left(\alpha - \left(\frac{a}{p}\right)i\zeta_p^{a}\right)\left(\beta - \left(\frac{a}{p}\right)i\zeta_p^{a}\right)\zeta_p^{-a} \\
\times & \prod_{\substack{a=1 \\ \varepsilon_a=-1}}^{(p-1)/2} \left(\alpha - \left(\frac{a}{p}\right)i\zeta_p^{a}\right)\left(\beta - \left(\frac{a}{p}\right)i\zeta_p^{a}\right)\zeta_p^{-a} \\
= & \ \delta,
\end{aligned}
$$

Entonces, como δ es un entero algebráico de $\mathbb{Q}_{-p}$ y $p \equiv 1 \pmod 4$ tene-

mos que $\delta = u + v\sqrt{-p}$ para algunos enteros u y v. Se sigue que

$$\begin{aligned} F_p^2 &= N(\alpha - i\zeta_p) = N_{\mathbb{Q}_{-p}/\mathbb{Q}}(N_{\mathbb{L}/\mathbb{Q}_{-p}}(\alpha - i\zeta_p)) = N_{\mathbb{Q}_{-p}/\mathbb{Q}}(\delta^2) \\ &= \left(N_{\mathbb{Q}_{-p}/\mathbb{Q}}(\delta)\right)^2 = (u^2 + pv^2)^2, \end{aligned}$$

Sacando raíz obtenemos $F_p = u^2 + pv^2$, lo cuál prueba que $p \in \mathcal{M}$. Finalmente, como consecuencia del Teorema 2.8, tenemos que

$$\frac{x}{\log x} \ll \mathcal{M}(x)$$

lo cuál concluye la demostración del Teorema 1.5.

Bibliografía

[ABL] J. J. Alba González, P. Berrizbeitia y F. Luca, *On the formula* $F_p = u^2 + pv^2$, Int. J. Number Theory **11** (2015), 185-191.

[AL] J. J. Alba González y F. Luca, *On positive integers n satisfying the equation* $F_n = x^2 + ny^2$, Contemporary Mathematics **587** (2013), 95-109.

[ALPS] J. J. Alba González, F. Luca, C. Pomerance e I. E. Shparlinski, *On numbers n dividing the nth term of a linear recurrence*, Proc. Edinburgh. Math. Soc. **55** (2012), 271-289.

[BKW] N. L. Bassily, I. Kátai y M. Wijsmuller, *Number of prime divisors of* $\phi_k(n)$*, where* ϕ_k *is the* k*-fold iterate of* ϕ, J. Number Theory **65** (1997), 226-239.

[BHV] Yu. Bilu, G. Hanrot, P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte*, J. Reine Angew Math. **539** (2001), 75-122.

[BL] C. Ballot y F. Luca, *On the equation* $x^2 + dy^2 = F_n$, Acta Arith. **127** (2007), 145-155.

[BQ] A. T. Benjamin y J. J. Quinn, *Proofs that really count. The art of combinatorial proof*, Mathematical Association of America, Washington, DC,(2003).

[CEP] E. R. Canfield, P. Erdős y C. Pomerance, *On a problem of Oppenheim concerning 'Factorisatio Numerorum'*, J. Number Theory **17** (1983), 1-28.

[DMT] C. Dartyge, G. Martin y G. Tenenbaum, *Polynomial values free of large prime factors*, Periodica Math. Hungar. **43** (2001), 111-119.

[ELP] P. Erdős, F. Luca y C. Pomerance, *On the proportion of numbers coprime to a given integer*, Proceedings of the Anatomy of Integers Conference, Montréal, March 2006, J.-M. De Koninck, et al., eds., CRM Proceedings and Lecture Notes, **46** (2008), 47-64.

[EM] M. R. Murty y J. Esmonde, *Problems in Algebraic Number Theory*, Second Edition, Springer (2004).

[EP] P. Erdős and C. Pomerance, *On the normal number of prime factors of $\phi(n)$*, Rocky Mtn. J. Math. **15** (1985), 343-352.

[EPSW] G. Everest, A. van der Poorten, I. E. Shparlinski y T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs **104**, American Mathematical Society (2003).

[ER] P. Erdős, *On the normal number of prime factors of $p-1$ and some other related problems concerning Euler's ϕ function*, Quart. J. Math. (Oxford Ser.) **6** (1935), 205-213.

[F] K. Ford, *The distribution of integers with a divisor in a given interval*, Ann. Math. **168** (2008), 367-433.

[GP] D. Gordon and C. Pomerance, *The distribution of Lucas and elliptic pseudoprimes*, Math. Comp. **57** (1991), 825-838.

[HR] H. Halberstam y H.-E. Richert, *Sieve Methods*, Academic Press, London, (1974).

[HT] R. R. Hall y G. Tenenbaum, *Divisors*, Cambridge University Press, Cambridge, (1988).

[L1] F. Luca, *Números primos y aplicaciones*, Aportaciones Matemáticas, Nivel Avanzado **26** (2004).

[L] F. Luca, *On positive integers n for which $\Omega(n)$ divides F_n*, Fibonacci Quart. **41** (2003), 365-371.

[Lu] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184-240, 289-321.

[LS] F. Luca e I. E. Shparlinski, *Some divisibilities amongst the terms of linear recurrences*, Abh. Math. Sem. Univ. Hamburg, **46** (2006), 143-156.

[N] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, (1999).

[NP] I. Nemes y A. Pethő, *Polynomial values in linear recurrences II*, J. Number Theory **24** (1986), 47-53.

[NZM] I. Niven, H. S. Zuckerman y H. L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley & Sons Inc., New York, (1991).

[P] P. Pollack, *Not Always Buried Deep: A Second Course in Elementary Number Theory*, American Mathematical Society, Providence, (2009) (1981), 587-593.

[POM] C. Pomerance, *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), 587-593.

[R] D. W. Robinson, *The Fibonacci matrix modulo m*, Fibonacci Quart. **1** (1963), 29-36.

[RO] N. Robbins, *On Fibonacci and Lucas numbers which are sums of precisely four squares*, Fibonacci Quart. **21** (1983), 3-5.

[Sh] I. E. Shparlinski, *Distribution of nonresidues and primitive roots in recurrent sequences*, Mat. Zametki **24** (1978), 603-613, 733.

[S] C. Smyth, *Divisibility of terms in Lucas sequences by their subscripts*, Applications of Fibonacci numbers **5** (1993), 515-525.

[T] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, Cambridge, (1995).