Universidad Nacional Autónoma de México

Posgrado en Ciencias Matemáticas

SOBRE ALGUNAS ECUACIONES DIOFÁNTICAS.

TESIS

QUE PARA OPTAR POR EL GRADO DE:

DOCTOR EN CIENCIAS

Presenta:

M. C. SERGIO GUZMÁN SÁNCHEZ

Director de Tesis

Dr. FLORIAN LUCA

(Centro de Ciencias matemáticas)

Miembros del Comité Tutor

Dr. ALBERTO GERARDO RAGGI CARDENAS

(Centro de Ciencias matemáticas)

Dr. LUIS VALERO ELIZONDO

(Posgrado en Ciencias Matemáticas)

MÉXICO D. F., JUNIO 2014

Índice general

Agradecimientos

Estoy muy agradecido con mi asesor el Dr. Florian Luca, por sus enseñanzas tanto académicas como personales. También agradezco a mis padres y en general a toda mi familia por todo su apoyo. Sin duda debo mencionar que agradezco mucho el apoyo que me brindaron todos mis amigos durante estos años.

Introducción

Para un entero positivo n, escribimos $\sigma(n)$ como la suma de los divisores de n. El número n es llamado *perfecto* si $\sigma(n) = 2n$. No se sabe si hay un número infinito de números perfectos.

Para un entero $g > 1$ un *repdígito* en base g es un entero positivo N tal que todos sus dígitos en base g son iguales. Esto es, N tiene la forma

$$N = d\left(\frac{g^m - 1}{g - 1}\right), \qquad \text{donde} \qquad m \geq 1, \quad \text{y} \quad d \in \{1, 2, \ldots, g - 1\}. \tag{0.1}$$

Se ha trabajado en la pregunta sobre la existencia de repdígitos perfectos dada una base $g > 1$. En [**15**], Pollack probó que dada una base $g > 1$ hay únicamente una cantidad finita de repdígitos en dicha base los cuales son perfectos. Su prueba es efectiva y usa resultados de ecuaciones diofánticas los cuales fueron probados usando cotas inferiores de formas lineales en logaritmos. Hasta ahora, no ha sido calculada una cota superior explícita para la solución más grande en función de g.

Posterior al trabajo de Pollack, en [**3**], Broughan y Zhou han calculado repdígitos perfectos en base g para $g \in \{2, \ldots, 10\}$. El método aplicado en [**3**] es usando restricciones modulares o resolviendo varias ecuaciones diofánticas exponenciales muy particulares.

Estos trabajos son la motivación para el trabajo realizado en el Capítulo 2 donde presentaremos un algoritmo para calcular los repdígitos perfectos en base g. Como un ejemplo, extenderemos los cálculos realizados en [**3**] a las bases $g \in [2, 333]$. Como resultado del trabajo, también daremos algunas cotas teóricas sobre el repdígito perfecto más grande en base g y la cantidad de repdígitos perfectos en base g, ambas cotas en función de la base.

Dada una sucesión recurrente binaria no degenerada $(u_n)_{n\geq 0}$ (ver Sección 2), en [**7**], Luca y Grossman demostraron que para cualesquiera enteros positivos fijos K y ℓ, la ecuación diofántica

$$u_n = \sum_{i=1}^{\ell} a_i m_i! \quad \text{donde} \quad |a_i| \leq K \quad \text{para toda} \quad i = 1, \ldots, \ell$$

tiene una cantidad finita de soluciones $(n, m_1, \ldots, m_\ell)$. Además, dichas soluciones pueden ser calculadas. En [**7**], tomando $K = 1$, $\ell = 2$ y como sucesión recurrente binaria la famosa sucesión de Fibonacci se mostró que $F_{12} = 4! + 5!$ es el término más grande de dicha sucesión que es suma

o diferencia de dos factoriales. Además, en [**2**] se mostró que $F_7 = 1! + 3! + 3!$ es el número de Fibonacci más grande que es suma de tres factoriales.

Sea $P = \{p_1, \ldots, p_k\}$ un conjunto finito de números primos tales que $p_1 < \cdots < p_k$. Denotaremos por S al conjunto de todos los enteros racionales cuyos factores primos están en P, dichos enteros serán llamados S-unidades. En particular, $0 \notin S$ pero $\{\pm 1\} \subset S$.

La ecuación diofántica

$$u_n = s_1 + \cdots + s_\ell \quad \text{con} \quad s_i \in S \quad \text{para todo} \quad i = 1, \ldots, \ell \tag{0.2}$$

puede ser tratada usando la teoría de ecuaciones en S-unidades. Esta ecuación podría tener un número infinito de soluciones, como por ejemplo cuando $\ell = 2$ y

$$u_n = 2^n + 3^n,$$

donde $u_0 = 2,\ u_1 = 5,\ u_{n+2} = 5u_{n+1} - 6u_n$, y $P = \{2, 3\}$. Para eliminar estas soluciones, llamaremos a una solución de la ecuación (0.2) *solución no degenerada* si se cumple de manera simultánea que $\sum_{i\in I} s_i \neq 0$ y $c\alpha^n + \sum_{i\in I} s_i \neq 0$ (donde c y α se definen en la Sección 2) para todos los subconjuntos no vacíos I de $\{1, \ldots, \ell\}$. Entonces el teorema principal concerniente a la finitud de las soluciones no degeneradas de ecuaciones en S-unidades implica que la ecuación (0.2) tiene un número finito de soluciones $(n, s_1, \ldots, s_\ell)$ las cuales son no degeneradas y $\text{mcd}(s_1, \ldots, s_\ell) \leq K$. Esto fue publicado de manera independiente en [**6**] y [**18**]. Sin embargo, este resultado no es efectivo y no sabemos cómo hacerlo efectivo. En particular, no sabemos cómo calcular todas las soluciones enteras positivas (n, a, b) de la ecuación

$$F_n = 2^a + 3^b,$$

la cual es un ejemplo particular de la ecuación (0.2) tomando como sucesión recurrente binaria la sucesión de Fibonacci y el conjunto de primos $P = \{2, 3\}$. En este problema, estudiaremos el problema híbrido que consiste en representar a u_n como una suma de un factorial y una S-unidad. Más precisamente, queremos resolver la ecuación diofántica

$$u_n = Am! + Bs \quad \text{donde} \quad s \in S \quad \text{y} \quad A, B \in \mathbb{Z}, \quad \text{máx}\{|A|, |B|\} \leq K, \tag{0.3}$$

donde $(u_n)_{n\geq 0}$ es una sucesión recurrente binaria no degenerada sujeta a las restricciones $\Delta > 0$, $\text{mcd}(r, t) = 1$ y K es un entero fijo (donde r, s y Δ se definen en la Sección 2) .

En el Capítulo 3 veremos que bajo ciertas restricciones, la ecuación (0.3) tiene únicamente una cantidad finita de soluciones. Para este trabajo usamos formas lineales en logaritmos para dar una cota sobre la más grande solución de la ecuación.

Como ejemplo numérico, fijamos $P = \{2, 3, 5, 7\}$ y $K = 1$ y como sucesión recurrente binaria tomamos la famosa sucesión de Fibonacci, encontrando así que $n = 24$ es la solución más grande a la ecuación (0.3), obteniendo $m = 8$ y $s = 2^5 3^3 7^1$ así tenemos

$$F_{24} = 8! + 2^5 3^3 7^1.$$

Para este ejemplo en particular, aplicamos la cota general encontrada, la cual resulta ser muy grande. Para encontrar la solución $n = 24$ tuvimos que reducir la cota y emplear otros argumentos para llegar a la solución mencionada.

Capítulo 1

Preliminares

En este capítulo presentaremos algunas definiciones y resultados necesarios para demostrar los teoremas principales del trabajo.

1. Ecuaciones de Pell

En el algoritmo para detectar repdígitos perfectos que presentaremos más adelante, usaremos algunos resultados bien conocidos sobre ecuaciones de Pell.

Sea $D > 1$ un entero positivo que no es un cuadrado perfecto, entonces es bien conocido que la ecuación

$$X^2 - DY^2 = \pm 1, \tag{1.1}$$

tiene un número infinito de soluciones cuando el signo en el lado derecho es positivo, cuando es negativo, la ecuación tiene solución solamente si el período de la fracción continua de $\sqrt{D}$ es impar y en este caso, la ecuación también tiene un número infinito de soluciones.

Se puede probar que si (x_1, y_1) y (x_2, y_2) son soluciones de la ecuación (1.1) con x_1, y_1, x_2, y_2 enteros positivos, entonces es equivalente: (i) $|x_1| < |x_2|$ (ii) $|y_1| < |y_2|$. Entonces se sigue de la equivalencia de (i) y (ii) que si la ecuación (1.1) tiene soluciones, hay una solución en la cual X y Y toman su menor valor entero positivo. A dicha solución (x_1, y_1) le llamaremos la *solución minimal positiva*

Si existe solución con $\varepsilon = -1$ y (x_1, y_1) es la solución mínima correspondiente a $\varepsilon = -1$ entonces, la solución mínima para $\varepsilon = 1$ será $(2x_1^2 + 1, 2x_1y_1)$.

Como mencionamos anteriormente, cuando la ecuación (1.1) tiene solución, se tiene un número infinito de soluciones enteras positivas (x, y). Más aún, todas las soluciones son de la forma (x_n, y_n), donde

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n \qquad \text{para toda} \qquad n \geq 1. \tag{1.2}$$

A continuación daremos una cota para la solución mínima de una ecuación de Pell la cual fue establecida en [**11**, Lemma 1]. Esta cota es suficiente para nuestros propósitos.

Lema 1. *Sea $d > 1$ un entero que no es un cuadrado perfecto. Entonces la solución mínima positiva (x_0, y_0) de la ecuación de Pell $X^2 - dY^2 = 1$, satisface $x_0 + y_0\sqrt{d} < d^{3\sqrt{d}}$.*

Demostración. Sea $\eta := x_0 + y_0\sqrt{d}$. Ahora empezaremos asumiendo que $d \equiv 0,\ 1 \pmod 4$. Por el Teorema de Schur [**8**, Teorema 13.5, Pagina 329], si $(u, v) := (u_0, v_0)$ es la mínima solución entera positiva de la ecuación $U^2 - dV^2 = 4$ (la cual siempre existe [**9**, Teorema 1.3]), entonces escribiendo

$$\varepsilon := \frac{u_0 + v_0\sqrt{d}}{2},$$

tenemos que $\varepsilon < d^{\sqrt{d}}$. Ahora veremos como se deduce la conclusión deseada.

Distinguiremos tres casos.

Caso 1. v_0 es par. Entonces u_0 también lo es. Sea $(x, y) := (u_0/2, v_0/2)$, tenemos que $x^2 - dy^2 = 1$, así $\eta \leq x + y\sqrt{d} = \varepsilon < d^{\sqrt{d}}$.

Caso 2. v_0 es impar y u_0 es par. Entonces $4 \mid d$. Además,

$$\varepsilon^2 = \left(\frac{u_0^2 + dv_0^2}{4}\right) + \left(\frac{2u_0v_0}{4}\right)\sqrt{d} =: x + y\sqrt{d}.$$

Claramente, $x,\ y$ son enteros y $x^2 - dy^2 = 1$. Así, $\eta \leq \varepsilon^2 < d^{2\sqrt{d}}$ en este caso.

Caso 3. v_0 es impar y u_0 es impar. Entonces $d \equiv 5 \pmod 8$. Así,

$$\varepsilon^3 = \left(\frac{u_0(u_0^2 + 3dv_0^2)}{8}\right) + \left(\frac{v_0(3u_0^2 + dv_0^2)}{8}\right)\sqrt{d} =: x + y\sqrt{d},$$

donde $x,\ y$ son enteros positivos con $x^2 - dy^2 = 1$. Así, $\eta \leq x + y\sqrt{d} = \varepsilon^3 < d^{3\sqrt{d}}$, que es lo que queríamos probar.

Ahora asumamos que $d \equiv 2, 3 \pmod 4$, y sea (u_0, v_0) la solución mínima entera positiva de la ecuación $U^2 - dV^2 = 4$. Entonces V debe ser par pues si V fuera impar entonces también lo sería U. Reduciendo la ecuación de arriba módulo 4 tendríamos que $d \equiv 1 \pmod 4$, pero este no es el caso que estamos considerando. Así, $(s, t) := (u_0, v_0/2)$ es una solución entera positiva de $S^2 - (4d)T^2 = 4$. Por otra parte, para cada solución entera positiva (s, t) de la ecuación de arriba, el par $(u, v) := (s, 2t)$ es solución entera positiva de la ecuación $U^2 - dV^2 = 4$. Así, por el Teorema de Schur aplicado a $4d$, el cual es congruente con 0 módulo 4, tenemos que

$$\varepsilon = \frac{1}{2}(u_0 + (v_0/2)\sqrt{4d}) < (4d)^{\sqrt{4d}} = (4d)^{2\sqrt{d}}.$$

Observemos que $(x, y) = (u_0/2, v_0/2)$ es una solución entera positiva de $X^2 - dY^2 = 1$, donde tenemos que $\eta \leq \varepsilon \leq (4d)^{2\sqrt{d}}$. Como la desigualdad $(4d)^{2\sqrt{d}} < d^{3\sqrt{d}}$ se mantiene para toda $d > 16$,

sólo nos falta estudiar los casos cuando d esta en el conjunto $\{2, 3, 6, 7, 10, 11, 14, 15\}$. Para cada uno de estos valores, uno puede comprobar directamente que $\eta < d^{3\sqrt{d}}$. □

Sean $A > 1$ y $B > 1$ enteros tal que ninguno de ellos es un cuadrado perfecto. Consideremos la ecuación diofántica

$$AX^2 - BY^2 = \pm 1. \tag{1.3}$$

Como los roles de A y B en la ecuación (1.3) son intercambiables, podemos asumir que el signo en el lado derecho de la ecuación es $+1$.

De manera similar a llas soluciones de la ecuación (1.1), decimos que (x_1, y_1) es *solución mínima positiva* de (1.3), si $X = x_1$ y $Y = y_1$ toman su menor valor entero positivo.

Es conocido que si la ecuación (1.3) tiene una solución entera, entonces la ecuación tiene una infinidad de soluciones enteras positivas. Walker muestra en [**20**], que para hallar la solución mínima (x, y) de la ecuación (1.3), en caso de existir, primero debemos encontrar la solución mínima (r, s) de la ecuación

$$X^2 - ABY^2 = 1.$$

Entonces, la solución (x, y) debe satisfacer

$$(x\sqrt{A} + y\sqrt{B})^2 = r + s\sqrt{AB}.$$

Esto significa que (x, y) será la solución del sistema

$$\begin{cases} Ax^2 + By^2 = & r \\ 2xy = & s. \end{cases}$$

Además, una vez encontrada la solución mínima (x, y) de (1.3), todas sus soluciones positivas son de la forma (x_m, y_m) para algún entero impar $m \geq 1$, donde

$$x_m\sqrt{A} + y_m\sqrt{B} = (x\sqrt{A} + y\sqrt{B})^m.$$

2. Sucesiones recurrentes binarias

Una suceción recurrente binaria $(u_n)_{n\geq 0}$ es una sucesión de enteros tales que

$$u_{n+2} = ru_{n+1} + tu_n \quad \text{para } n \geq 0, \tag{2.1}$$

donde r y t son enteros no cero tales que $\Delta = r^2 + 4t \neq 0$. Sean α y β las raíces del polinomio característico $x^2 - rx - t$, con la convención que $|\alpha| \geq |\beta|$. Es bien conocido que existen constantes c y d tales que

$$u_n = c\alpha^n + d\beta^n \quad \text{para toda } n \geq 0, \tag{2.2}$$

donde

$$c = \frac{u_1 - u_0\beta}{\alpha - \beta} \qquad \text{y} \qquad d = \frac{u_0\alpha - u_1}{\alpha - \beta}. \tag{2.3}$$

La sucesión $(u_n)_{n\geq 0}$ es llamada *no degenerad*a si $cd\alpha\beta \neq 0$ y α/β no es raíz de la unidad.

2.1. Sucesiones de Lucas. Una sucesión de Lucas, es una sucesión recurrente binaria con condiciones iniciales $u_0 = 0,\ u_1 = 1$ donde $r,\ t$ son primos relativos.

En el caso de una sucesión de Lucas, el término general dado por la ecuación (2.2) se ve como

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{para} \quad n = 0, 1, \ldots.$$

Para cada entero positivo k, definimos el orden de aparición de k, denotado por $z(k)$, al menor entero positivo ℓ tal que $k|u_\ell$. Cuando dicho entero no existe se escribirá $z(k) = \infty$.

Recordemos que si a es un entero y p es un primo impar, entonces el símbolo de Legendre $(a|p)$ se define como

1. $(a|p) = 0$ si $p \mid a$.
2. $(a|p) = 1$ si $p \nmid a$ y existe x entero tal que $x^2 \equiv a \pmod{p}$.
3. $(a|p) = -1$ en otro caso.

A continuación enunciaremos algunos resultados conocidos sobre las propiedades más importantes de divisibilidad para las sucesiones de Lucas. Para su demostración véase [**12**].

Teorema. *Sea p un número primo y $\Delta = r^2 + 4t$. Se satisfacen las siguientes propiedades:*

1. *Si $p \mid t$, entonces $p \nmid u_n$ para todo $n \geq 1$.*
2. *Si $p \mid \Delta$, entonces $p \mid u_p$.*
3. *Si p impar tal que $p \nmid \Delta t$ y $(\Delta|p) = 1$ o $p = 2$ y $p \nmid \Delta t$, entonces $p \mid u_{p-1}$.*
4. *Si p es un primo impar no cubierto por 1, 2 o 3, entonces $p \mid u_{p+1}$.*

Proposición 2. *Para todos los enteros positivos m y n se tiene que*

$$mcd(u_m, u_n) = u_{mcd(m,n)}.$$

Observemos que de estos resultados se tiene que si p es un primo que no divide a t, entonces $z(p) \neq \infty$, además, si m es cualquier otro entero tal que $p \mid u_m$, entonces $z(p) \mid m$. En particular, $z(p) \mid p - (\Delta|p)$.

Proposición 3. *1. Si $m \mid n$ y p es un primo tal que $p \mid mcd(u_m, u_n/u_m)$, entonces $p \mid n/m$.*

2. *Si $p > 2$ es primo y $p \mid u_n$, entonces $p \| u_{np}/u_n$ (donde el símbolo $\|$ significa que $p \mid u_{np}/u_n$ y $p^2 \nmid u_{np}/u_n$).*

Ejemplo 1. *Si tomamos $r = 1$ y $t = 1$ obtenemos la famosa sucesión de Fibonacci denotada por $(F_n)_{n\geq 0}$. En este caso obtenemos $\alpha = \frac{1+\sqrt{5}}{2}$ y $\beta = \frac{1-\sqrt{5}}{2}$ y el término general de la sucesión está dado por*

$$F_n = \frac{1}{\sqrt{5}}\alpha^n - \frac{1}{\sqrt{5}}\beta^n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Ejemplo 2. *Sea $g > 1$ entero, si $r = g + 1$ y $t = -g$, entonces*

$$x^2 - rx - t = x^2 - (g+1)x + g = (x - g)(x - 1).$$

En este caso, tenemos $\alpha = g$ y $\beta = 1$ por tanto, se sigue que

$$u_n = \frac{g^n - 1}{g - 1} \qquad \text{para toda} \quad n \geq 0.$$

Esta sucesión es conocida como la sucesión de repunits, la sucesión de números de dígitos repetidos en base g, cuyo dígito es 1.

Observemos que dado un primo p, se tiene que $p \mid u_n$ para algún $n \geq 1$ si y solo si $p \nmid g$.

Si p es un primo dividiendo a $g - 1$, entonces $z(p^a) = p^a$. Si p es un primo que no divide a $g - 1$, entonces $z(p) \mid p - 1$. (Excluimos el caso $p \mid g$ ya que en ese caso $z(p) = \infty$.) Más aún, si

$$u_{z(p)} = p^{e_p} \prod_{\substack{r \mid u_{z(p)} \\ r \neq p}} r^{e_r},$$

entonces tenemos que para toda $a \geq 1$, $z(p^a) = p^{\max\{0, a-e_p\}} z(p)$, lo cual implica que $p^{\max\{0,a-e_p\}} \| z(p^a)$.

Por lo tanto, si $k = \prod_{p\mid k} p^{a_q}$ tenemos que $z(k) = \operatorname{mcm}[z(p^{a_p}) : p \mid k]$.

El ejemplo anterior nos da una sucesión muy particular que será muy útil y será estudiada más adelante. A continuación definimos para un número libre de cuadrados $k > 1$ el parámetro $Z(k)$ asociado a la sucesión de repunits, el cual está muy relacionado con el orden de aparición $z(k)$, como se muestra a continuación. Escribimos

$$u_{z(k)} = \prod_{p\mid k} p^{e_p} \prod_{\substack{q \nmid k \\ q \mid g-1}} q^{f_q} \prod_{\substack{r \mid u_{z(k)} \\ r \nmid k(g-1)}} r^{g_r}.$$

Entonces definimos

$$Z(k) := z(k) \prod_{\substack{p\mid k \\ e_p \equiv 0 \pmod 2}} p \prod_{\substack{q \nmid k \\ q \mid g-1 \\ f_q \equiv 1 \pmod 2}} q.$$

Ejemplo 3. *Con la notación usada para las soluciones de la ecuación* (1.1)*, sea* $\alpha := x_1 + y_1\sqrt{D}$ *y* $\beta := x_1 - y_1\sqrt{D}$*. Conjugando la relación de arriba (es decir, reemplazando* $\sqrt{D}$ *por* $-\sqrt{D}$*) y resolviendo para* x_n *y* y_n *en* (1.2)*, tenemos que*

$$y_n = \frac{\alpha^n - \beta^n}{2\sqrt{D}} = y_1\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right).$$

Definamos $u_n := y_n/y_1$ *para toda* $n \geq 1$ *y* $u_0 := 0$*, al hacer esto, observamos que se tiene que* $\{u_n\}_{n\geq 0}$ *forma una sucesión de Lucas. Más aún,*

$$x_n = \frac{\alpha^n + \beta^n}{2} = \frac{\alpha^{2n} - \beta^{2n}}{2(\alpha^n - \beta^n)} = \frac{u_{2n}}{2u_n} \qquad \text{para toda} \quad n \geq 1.$$

2.2. Sucesiones de Lehmer. Unas sucesiones muy parecidas a las sucesiones de Lucas son las llamadas *sucesiones de Lehmer*. Para definir las sucesiones de Lehmer, asumimos otra vez que r y t son enteros no cero y primos relativos tal que $r > 0$ y $\Delta := r + 4t \neq 0$, sean α y β las dos raíces de la ecuación característica $x^2 - \sqrt{r}x - t = 0$. Asumimos otra vez que α/β no es raíz de la unidad. Pongamos

$$v_n = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta}, & \text{si} \quad n \equiv 1 \pmod 2, \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, & \text{si} \quad n \equiv 0 \pmod 2. \end{cases}$$

La sucesión $\{v_n\}_{n\geq 0}$ es llamada sucesión de Lehmer y consiste de enteros.

Al igual que en las sucesiones de Lucas, se define para cada entero positivo k, el orden de aparición de k en la sucesión $\{v_n\}_{n\geq 0}$ denotado por $z(k)$ al menor entero positivo ℓ tal que $k|v_\ell$, cuando dicho entero no existe se escribirá $z(k) = \infty$. Este orden de aparición satisface propiedades similares a las que se tienen cuando la sucesión es de Lucas, como por ejemplo, $z(p) \mid p - (\Delta|p)$.

Ejemplo 4. *Usando la notación usada para encontrar la solución mínima de la ecuación* (1.3)*, si definimos* $\alpha := x_1\sqrt{A} + y_1\sqrt{B}$ *y* $\beta := x_1\sqrt{A} - y_1\sqrt{B}$*, tenemos que* $r = \alpha + \beta = 2x_1\sqrt{A} = \sqrt{4Ax_1^2}$ *y* $t = -\alpha\beta = -1$*. Además,*

$$y_m = \frac{\alpha^m - \beta^m}{2\sqrt{B}} = y_1\left(\frac{\alpha^m - \beta^m}{\alpha - \beta}\right) \qquad \text{para todo impar} \quad m \geq 1.$$

Observemos que si definimos $v_m := y_m/y_1$ *para* $m \geq 1$ *entero impar, entonces* $\{v_m\}_{m\geq 1 \text{ impar}}$ *es la subsucesión de índices impares de una sucesión de Lehmer cuyas raíces son* α *y* β*.*

Además,

$$x_m = \frac{\alpha^m + \beta^m}{2\sqrt{A}} = x_1\frac{\alpha^m - (-\beta)^m}{\alpha - (-\beta)}.$$

Si definimos $w_m := x_m/x_1$ *para enteros impares* $m \geq 1$*, entonces* $\{w_m\}_{m\geq 1 \text{ impar}}$ *es la subsucesión de índices impares de la sucesión de Lehmer con raíces* α *y* $-\beta$*. Notemos que* $\alpha + (-\beta) = 2y_1\sqrt{B} = \sqrt{4By_1^2}$*, entonces podríamos tomar* $r = 4By_1^2$ *y* $t = -\alpha(-\beta) = 1$*.*

3. Teorema del divisor primitivo

Dado $n > 0$ y una sucesión de Lucas o Lehmer $(u_n)_{n\geq 0}$, un divisor *primitivo* de u_n es definido como un divisor primo p de u_n tal que p no divide a Δ y p no divide a u_m para cualquier entero positivo $m < n$.

El siguiente resultado se debe a Carmichael (ver [**4**]). Usando la notación usada en la Sección 2 se tiene:

Teorema (Carmichael). *Si α y β son reales y $n \neq 1, 2, 6$, entonces u_n tiene al menos un divisor primitivo excepto cuando $n = 12$, $r = 1$ y $t = 1$.*

De la observación hecha posterior a la Proposición 2, se tiene que un divisor primitivo de u_n tiene la propiedad de que $p \equiv \pm 1 \pmod{n}$. Cuando α y β son enteros racionales, la congruencia más precisa es $p \equiv 1 \pmod{n}$ que se mantiene para cada divisor primitivo p de u_n. En este caso particular, u_n tiene un divisor primitivo para toda $n > 6$. En particular, la desigualdad $p \geq n - 1$ se conserva para cada divisor primitivo p de u_n, y se tiene una mejor desigualdad $p \geq n + 1$ que se mantiene cuando las raíces α y β son enteros racionales.

Un teorema similar fue demostrado para sucesiones de Lehmer por Morgan Ward en [**21**]. Diremos que una sucesión de Lehmer es *excepcional* si contiene términos de índice mayor a dos sin divisores primitivos. Cada uno de estos índices es llamado *índice excepcional*. Usando la notación de la Subsección 2.2, sea

$$R = \begin{cases} |4rt| & \text{si } t > 0 \\ |4\Delta t| & \text{si } t < 0, \end{cases}$$

entonces el resultado de Ward es:

Teorema (Ward). *Si α y β son reales, la sucesión $\{v_n\}_{n\geq 0}$ puede ser excepcional si $R < 16$. Un término de $\{v_n\}_{n\geq 0}$ siempre tiene un divisor primitivo si su índice es mayor que 18.*

Para el caso de las sucesiones de Lehmer también se tiene que un divisor primitivo de u_n tiene la propiedad de que $p \equiv \pm 1 \pmod{n}$.

Los teoremas anteriores han sido extendidos a sucesiones de Lucas y Lehmer con raíces complejas no reales por Bilu, Hanrot y Voutier [**1**].

Teorema (Bilu, Hanrot y Voutier). *Si α y β son complejas y $\{u_n\}_{n\geq 0}$ sucesión de Lucas o Lehmer, entonces u_n tiene un divisor primitivo para toda $n \geq 31$. Más aún, hay únicamente un número finito de tríadas (n, α, β) con $5 \leq n \leq 30$, pero $n \neq 6$ tales que u_n carece de divisor primitivo para el correspondiente par de raíces (α, β), que son reales o complejas conjugadas, y todas las excepciones son listadas en* [**1**].

Ejemplo 5. *Para la sucesión de repunits del Ejemplo 2, se tiene por el Teorema de Carmichael que u_n es múltiplo de un primo $p \geq n+1$ para toda $n \geq 7$.*

Lema 4. *Sea $g > 1$ entero y x_n solución entera positiva de la ecuación de Pell $X^2 - DY^2 = 1$ (donde D es un entero positivo libre de cuadrados). Si x_n no tiene factores excediendo g, entonces $n \leq \max\{6, (g+1)/2\}$.*

Demostración. Recordemos del Ejemplo 3 que $x_n = \frac{u_{2n}}{2u_n}$, donde u_n es una sucesión de Lucas. Aplicando el Teorema de Carmichael, se tiene que para $n > 3$, u_{2n} tiene un divisor primitivo p que satisface $p \equiv \pm 1 \pmod{2n}$. Por lo tanto $2n - 1 \leq p < g$, de donde se obtiene el resultado deseado. □

Lema 5. *Sea $g > 1$ entero y x_n solución entera positiva de la ecuación de Pell $AX^2 - BY^2 = 1$ (donde A y B son enteros positivos libres de cuadrados). Si x_n no tiene factores excediendo g, entonces $n \leq \max\{12, g+1\}$.*

Demostración. Del Ejemplo 4, tenemos $\{w_m\}_{m\geq 1 \text{ impar}}$ es la subsucesión de índices impares de la sucesión de Lehmer donde $w_m := x_m/x_1$. Por el Teorema de Ward, sabemos que para $m \geq 12$, w_m tiene un divisor primitivo p que satisface $p \equiv \pm 1 \pmod{m}$. Dicho primo divide a x_m, por lo tanto $m - 1 \leq p < g$, de donde se obtiene el resultado deseado. □

4. Formas lineales en logaritmos de números algebraicos.

En 1900, el matemático alemán David Hilbert presento una lista de 23 problemas. El séptimo de ellos es sobre la pregunta de cuando α^β es trascendente para $\alpha \neq 0, 1$ algebraico y β es un número algebraico irracional. El primer avance significativo fue hecho por Gelfond en 1929, en dicho trabajo él mostró que α^β es trascendente donde $\alpha \neq 0, 1$ algebraico y β cualquier irracional cuadrático imaginario. Este resultado fue extendido a irracionales cuadráticos reales por Kuzmin en 1930. El problema fue resuelto completamente por Gelfond y Schneider de manera independiente en 1934.

El Teorema de Gelfond-Schneider muestra que para cualesquiera números algebraicos diferentes de cero $\alpha_1, \alpha_2, \beta_1, \beta_2$ con $\log\alpha_1, \log\alpha_2$ linealmente independientes sobre los racionales, se tiene

$$\beta_1 \log\alpha_1 + \beta_2 \log\alpha_2 \neq 0.$$

Posterior a esto, se conjeturó que se podría obtener un teorema análogo para una suma de más logaritmos de números algebraicos y más aún, se vio que ésto podría tener varias aplicaciones. Esta conjetura fue probada por Alan Baker en 1966, enunciándose dicho teorema de la siguiente forma

Teorema. *Sean $\alpha_1, \ldots, \alpha_n$ números algebraicos diferentes de cero tales que $\log \alpha_1, \ldots, \log \alpha_n$ son linealmente independientes sobre los racionales, entonces $1, \log \alpha_1, \ldots, \log \alpha_n$ son linealmente independientes sobre el campo de todos los números algebraicos.*

Posteriormente se empezó a trabajar en el problema de encontrar cotas inferiores para las combinaciones lineales de los logaritmos de números algebraicos.

A continuación daremos un resultado sobre este problema. Antes que nada, daremos algunas definiciones para fijar la notación usada para este resultado.

Sea η un número algebraico de grado d, cuyo polinomio mínimo sobre los enteros es

$$g(x) = a_0 \prod_{i=1}^{d} (x - \eta^{(i)}).$$

La altura logarítmica de η es

$$h(\eta) := \frac{1}{d}\left(\log |a_0| + \sum_{i=1}^{d} \log \max\{|\eta^{(i)}|, 1\}\right).$$

Sea $\mathbb{L}$ un campo de números algebraicos y $d_{\mathbb{L}}$ el grado de dicho campo. Sean $\eta_1, \eta_2, \ldots, \eta_l \in \mathbb{L}$ no 0 o 1 y $d_1, \ldots, d_l$ enteros diferentes de 0. Sea

$$D = \max\{|d_1|, \ldots, |d_l|\},$$

pongamos

$$\Lambda = \prod_{i=1}^{l} \eta_i^{d_i} - 1.$$

Sean $A_1, \ldots, A_l$ enteros positivos tales que

$$A_j \geq h'(\eta_j) := \max\{d_{\mathbb{L}} h(\eta_j), |\log \eta_j|, 0{,}16\} \quad \text{para} \quad j = 1, \ldots l.$$

El siguiente resultado se debe a Matveev [**14**].

Teorema (Matveev). *Si $\Lambda \neq 0$ y $\mathbb{L} \subset \mathbb{R}$, entonces*

$$\log |\Lambda| > -1{,}4 \cdot 30^{l+3} l^{4{,}5} d_{\mathbb{L}}^2 (1 + \log d_{\mathbb{L}})(1 + \log D) A_1 A_2 \cdots A_l.$$

También necesitaremos una version p-adica análoga al Teorema de Matveev, la cual fue dada por Kunrui Yu [**22**]. Sea π un ideal primo en el anillo de enteros $O_{\mathbb{L}}$ de enteros algebraicos en el campo L. Sean e_π y f_π los índices de ramificación e inercia de π, respectivamente. Sea $p \in \mathbb{Z}$ el único primo tal que $\pi|p$. Entonces

$$p^{d_{\mathbb{L}}} = \prod_{i=1}^{k} \pi_i^{e_i},$$

donde $\pi_1, \ldots, \pi_k$ son ideales primos en $O_{\mathbb{L}}$. Por convención, podemos tomar $\pi = \pi_1$, en dicho caso, $e_\pi = e_1$. Si $\eta \in \mathbb{L}$, $\mu_\pi(\eta)$ es el orden en el cual π aparece en la factorización en primos del ideal fraccional $\eta O_{\mathbb{L}}$. Cuando π es un primo racional, entenderemos que el campo $\mathbb{L}$ es el campo $\mathbb{Q}$ de números racionales. Sean

$$H_j \geq \max\{h(\eta_j), \log p\} \qquad j = 1, \ldots, l.$$

El siguiente resultado se debe a Yu [**22**].

Teorema (Yu). *Si $\Lambda \neq 0$, entonces*

$$\mu_\pi(\Lambda) \leq 19(20\sqrt{l+1}d_{\mathbb{L}})^{2(l+1)} e_\pi^{l-1} \frac{p^{f_\pi}}{(f_\pi \log p)^2} \log(e^5 l d_{\mathbb{L}}) H_1 \cdots H_l \log D.$$

Para una sucesión recurrente binaria $(u_n)_{n\geq 0}$, los valores de n para los cuales $u_n = 0$ no son buenos para nuestros argumentos, por lo que necesitamos acotarlos. Para ello, necesitaremos cotas sobre las alturas de algunos números involucrados en la sucesión y entonces calcularemos una cota sobre

$$\max\{h(\alpha),\ h(\beta),\ h(\alpha/\beta),\ h(c),\ h(d),\ h(c/d)\}.$$

Sea $(u_n)_{n\geq 0}$ una sucesión recurrente binaria no degenerada tal que $\Delta > 0$ y sea

$$Y := \max\{|r|, |t|, |u_0|, |u_1|\}. \tag{4.1}$$

Lema 6. *Si α, β, c y d son los parámetros mencionados de una sucesión recurrente binaria, entonces*

$$\max\{h(\alpha), h(\beta), h(\alpha/\beta), h(c), h(d), h(c/d)\} < 8\log(Y+2). \tag{4.2}$$

Demostración. Si α es racional, entonces α y β son enteros y $|\beta| \geq 1$. En consecuencia, $1 \leq |\alpha| \leq |t| \leq Y$, $1 \leq |\beta| < |\alpha| \leq Y$, lo cual inmediatamente implica que

$$\max\{h(\alpha), h(\beta), h(\alpha/\beta)\} < \log(Y+2). \tag{4.3}$$

Más aún, $|\alpha - \beta| < 2|\alpha| \leq 2Y < (Y+2)^2$, y

$$\max\{|u_1 - u_0\beta|, |u_1 - u_0\alpha|\} < |\alpha|(|u_0| + |u_1|) < 2Y^2 < (Y+2)^3. \tag{4.4}$$

Esto muestra que

$$\max\{h(c), h(d), h(c/d)\} < 3\log(Y+2). \tag{4.5}$$

A continuación asumimos que $\alpha \notin \mathbb{Q}$. Entonces α y β son enteros algebraicos conjugados. Si $|\beta| > 1$, entonces $|\alpha| < |t| < Y$, y también $|\beta| < |\alpha| < Y$. De otra forma, $|\beta| < 1$, por lo tanto $|\alpha| = |r - \beta| \leq |r| + |\beta| < Y + 1$. Por tanto, en ambos casos, $|\beta| < |\alpha| < Y + 1$. Esto muestra que $h(\alpha) = h(\beta) < \log(Y+2)$. Más aún, c y d son números algebraicos conjugados, los cuales son raíces del polinomio cuadrático

$$\Delta x^2 - \Delta u_0 x + (u_0^2 t - u_0 u_1 r - u_1^2).$$

Como $|\alpha - \beta| = \sqrt{\Delta} \geq 1$, de (4.4), se sigue que $\max\{|c|, |d|\} < (Y+2)^3$. Puesto que $|\Delta| < Y^2 + 4Y < (Y+2)^2$, tenemos que

$$h(c) = h(d) \leq \frac{1}{2}\left(\log \Delta + \log \max\{|c|, 1\} + \log\{|d|, 1\}\right) < 4\log(Y+2). \tag{4.6}$$

Para los cocientes, usamos que

$$h(\alpha/\beta) \leq h(\alpha) + h(1/\beta) = 2h(\alpha) < 2\log(Y+2),$$

y

$$h(c/d) \leq h(c) + h(1/d) = 2h(c) < 8\log(Y+2),$$

las cuales junto con (4.3), (4.5) y (4.6) terminan la demostración. □

A continuación asumiremos que r y t son primos relativos.

Lema 7. *Si $u_n = 0$, entonces $n \leq 16(Y+2)\log(Y+2)$.*

Demostración. Supongamos que $n \geq 16(Y+2)\log(Y+2)$. Entonces $u_n = 0$ implica

$$\left|\frac{\alpha}{\beta}\right|^n = \left|\frac{d}{c}\right|.$$

Como $|\alpha| > 1$ y $\beta = r - \alpha$, tenemos que $|\beta| \leq |\alpha| - 1$, de modo que

$$\left|\frac{\alpha}{\beta}\right| \geq 1 + \frac{1}{|\alpha| - 1} > 1 + \frac{1}{Y+1}.$$

Así,

$$\left|\frac{\alpha}{\beta}\right|^n > \left(1 + \frac{1}{Y+1}\right)^n > e^{n/(Y+2)},$$

donde usamos el hecho que $(1 + 1/z)^{z+1} > e$ para todo real $z > 1$. Siempre que $h(d/c) < 8\log(Y+2)$ (ver Lema 6), obtenemos que $|d/c| < (Y+2)^{16}$. Entonces,

$$e^{n/(Y+2)} < \left|\frac{\alpha}{\beta}\right|^n = \left|\frac{d}{c}\right| < (Y+2)^{16},$$

dando $n < 16(Y+2)\log(Y+2)$, que es lo que queríamos probar. □

Lema 8. *Sea p un primo. Si $n \geq 16(Y+2)\log(Y+2)$, entonces*

$$\mu_p(u_n) < 2{,}7 \cdot 10^{13} \frac{p^2(\log p + 8\log(Y+2))^2 \log n}{(\log p)^2}.$$

Demostración. Sea π un ideal primo en $\mathbb{L} = \mathbb{Q}(\alpha)$ sobre p. Como $r = \alpha + \beta$ y $t = -\alpha\beta$ son coprimos, se sigue que π no divide a α o β. Sin pérdida de generalidad, asumimos que π no divide a α, ya que el caso cuando π no divide a β se puede tratar de manera similar. Entonces

$$\mu_p(u_n) \leq \mu_\pi(c\alpha^n + d\beta^n) = \mu_\pi(c) + \mu_\pi(1 - (-cd^{-1})^{-1}(\alpha\beta^{-1})^{-n}). \tag{4.7}$$

Claramente,

$$\mu_\pi(c) \leq \mu_\pi(u_0\beta - u_1),$$

entonces

$$p^{\mu_\pi(c)} \leq N_{\mathbb{L}/\mathbb{Q}}(\pi)^{\mu_\pi(c)} \leq N_{\mathbb{L}/\mathbb{Q}}(u_0\beta - u_1) \leq 2Y^3 + Y^2 < (Y+2)^4,$$

así obtenemos que

$$\mu_\pi(c) \leq \frac{4\log(Y+2)}{\log p}. \tag{4.8}$$

Una desigualdad similar se mantiene con d en lugar de c. Esto acota el primer término del lado derecho de (4.7). Para el segundo término, sea

$$\Lambda = 1 - (-cd^{-1})^{-1}(\alpha\beta^{-1})^{-n}. \tag{4.9}$$

El hecho que $\Lambda \neq 0$ es consecuencia del Lema 7 y nuestra hipótesis sobre n. Entonces, estamos preparados para aplicar el Teorema de Yu para acotar la expresión $\mu_\pi(\Lambda)$. Para esto, en la notación de dicho teorema, sean $l = 2$, $\eta_1 = -cd^{-1}$, $\eta_2 = \alpha/\beta$, $d_1 = -1$, $d_2 = -n$, $\mathbb{L} = \mathbb{Q}(\alpha)$, $d_\mathbb{L} \leq 2$, $f_\pi \leq 2$, $e_\pi \leq 2$, $D = n$. Por el Lema 6, podemos tomar $H_1 = H_2 = \log p + 8\log(Y+2)$.

Aplicando el Teorema de Yu, tenemos

$$\mu_\pi(\Lambda) < 19 \cdot (20\sqrt{3} \cdot 2)^6 \cdot 2\frac{p^2}{(\log p)^2} \log(4e^5)(\log p + 8\log(Y+2))^2 \log n. \tag{4.10}$$

Las desigualdades (4.7), (4.8) y (4.10), nos dan que

$$\mu_p(u_n) < 2{,}7 \cdot 10^{13} \frac{p^2}{(\log p)^2}(\log p + 8\log(Y+2))^2 \log n,$$

que es lo que queríamos probar. □

Finalmente, necesitaremos una cota inferior para $|u_n|$.

LEMA 9. *Sea* $n \geq 16(Y+2)\log(Y+2)$. *Entonces*

$$|u_n| > |\alpha|^{n-C_0 \log n},$$

donde podemos tomar

$$C_0 = 4 \cdot 10^{11} \log(Y+2).$$

DEMOSTRACIÓN. Escribimos

$$|u_n| = |c||\alpha|^n |1 - (-cd^{-1})^{-1}(\beta/\alpha)^n|,$$

entonces

$$\log |u_n| = n \log |\alpha| + \log |c| + \log |\Lambda|. \tag{4.11}$$

Como antes, el hecho que $\Lambda \neq 0$ es consecuencia del Lema 7. Por el Lema 6, obtenemos inmediatamente que

$$\log |c| > -16 \log(Y+2) > -34 \log(Y+2) \log |\alpha|,$$

donde usamos el hecho que $|\alpha| \geq (1+\sqrt{5})/2$. Para $\log |\Lambda|$, usamos el Teorema de Matveev tomando $\mathbb{L} = \mathbb{Q}(\alpha) \subset \mathbb{R}$ (observar que α y β son reales ya que $\Delta > 0$), $l = 2$, $\eta_1 = -cd^{-1}$, $\eta_2 = \alpha/\beta$, $d_1 = -1$, $d_2 = -n$. Tenemos que $D = n$, $d_{\mathbb{L}} \leq 2$. Más aún, por el Lema 6, podemos tomar $A_1 = 16 \log(Y+2)$ y $A_2 = 2 \log |\alpha| = 4h(\alpha) (\geq 2h(\alpha/\beta)$. Entonces, obtenemos

$$\begin{aligned} \log |\Lambda| &> -1{,}4 \cdot 30^5 \cdot 2^{4{,}5} \cdot 4(1+\log 2)(1+\log D)(16 \log(Y+2))(2 \log |\alpha|) \\ &> -3{,}4 \cdot 10^{11} \log |\alpha| \log n. \end{aligned}$$

Entonces,

$$\begin{aligned} \log c + \log |\Lambda| &> -\Big(34 \log(Y+2) + 3{,}4 \cdot 10^{11} \log(Y+2) \log n\Big) \log |\alpha| \\ &> -4 \cdot 10^{11} \log(Y+2) \log n \log |\alpha|, \end{aligned}$$

que junto con (4.11) implica la cota inferior deseada. □

5. Otros resultados

En esta Sección, mostraremos un resultado debido a Ljunggren presentado en [**10**] que nos será muy útil para resolver algunas ecuaciones diofánticas que surgen a lo largo del desarrollo del algoritmo para detectar repdígitos perfectos.

TEOREMA (Ljunggren). *Las únicas soluciones enteras positivas a la ecuación*

$$\frac{x^n - 1}{x - 1} = y^2, \qquad \text{con} \quad x > 1 \quad y \quad n \geq 3$$

son $(x, n, y) = (7, 4, 20)$ *y* $(3, 5, 11)$.

Ahora demostraremos un par de desigualdades que nos serán muy útiles más adelante.

LEMA 10. *Si $T > 3$ y*

$$\frac{x}{\log x} < T, \qquad \textit{entonces} \qquad x < 2T \log T. \tag{5.1}$$

DEMOSTRACIÓN. Supongamos que $x \geq 2T \log T$. Entonces $x > 6$. Como $x \mapsto x/\log x$ es creciente para $x > e$, tenemos que

$$T > \frac{x}{\log x} \geq \frac{2T \log T}{\log(2T \log T)}.$$

Esto nos da que $2 \log T > T$, lo cual es falso para $T > 3$. □

LEMA 11. *Si $m \geq 1$, $T > (4m^2)^m$ y*

$$\frac{x}{(\log x)^m} < T, \quad \textit{entonces} \quad x < 2^m T (\log T)^m.$$

DEMOSTRACIÓN. El caso $m = 1$ es dado por el lema anterior, entonces podemos asumir que $m \geq 2$. Supongamos lo contrario, es decir, $x \geq 2^m T (\log T)^m$. Como $x \mapsto x/(\log x)^m$ es creciente cuando $x > e^m$, tenemos que

$$T > \frac{x}{(\log x)^m} \geq \frac{2^m T (\log T)^m}{(\log(2^m T (\log T)^m))^m}.$$

Cancelando un factor T en la expresión de arriba, tomando raíces m-ésimas y exponenciando, tenemos una desigualdad equivalente a

$$2^m (\log T)^m > T, \quad \text{o} \quad 2 \log T > T^{1/m}.$$

Con $W = T^{1/m}$, la última desigualdad es equivalente a

$$W < (2m) \log W,$$

la cual, por el Lemma 10 (notemos que $2m \geq 4 > 3$) nos da que $W < 4m \log(2m)$. Esto implica que $T < (4m \log(2m))^m$. Ahora, es suficiente notar que esto contradice la hipótesis sobre T, ya que $\log(2m) < m$ para toda $m \geq 1$. □

Capítulo 2

Repdígitos perfectos

Como se mencionó antes, en [**3**], se han calculado repdígitos perfectos en base g para $g \in \{2, \ldots, 10\}$. El método de [**3**] es usando restricciones modulares o resolviendo varias ecuaciones exponenciales diofánticas particulares dependiendo fuertemente del valor de la base.

En este trabajo, presentaremos un algoritmo para calcular todos los repdígitos perfectos en base g. Como un ejemplo, extenderemos los cálculos de [**3**] a las bases $g \in [2, 333]$. Como resultado del trabajo, también daremos algunas cotas teóricas tales como

Teorema 1. (i) *El número perfecto más grande de la forma* $N = d\left(\frac{g^m-1}{g-1}\right)$*satisface*

$$N < g^{g^{g^{g^3}}}. \tag{0.2}$$

(ii) *El número de repdígitos perfectos en base* g *es a lo más* $4g^5$.

A lo largo de este capítulo, usaremos p, q y r, con o sin índices, para números primos.

1. Repdígitos perfectos pares

Un resultado conocido de Euclides y Euler dice que un número perfecto par es necesariamente de la forma $2^{p-1}(2^p - 1)$, donde $2^p - 1$ es primo. Esto es, para encontrar repdígitos perfectos pares necesitamos resolver la ecuación

$$N = d\left(\frac{g^m - 1}{g - 1}\right) = 2^{p-1}(2^p - 1), \quad d \in \{1, \ldots, g - 1\}, \text{y } 2^p - 1 \text{ primo}. \tag{1.1}$$

La siguiente proposición es conocida, apareció en [**15**, Lema 7] y extiende [**3**, Lema 5], pero la incluimos por conveniencia para el lector.

Proposición 12. *Todas las soluciones* N *de la ecuación* (1.1) *son tales que* $m = 1$ *y en este caso* $g > N$ *arbitrario y* $d = N$*, o* $m = 2$*. En el caso* $m = 2$ *se tiene que* $d = 2^a$ *y* $g + 1 = 2^b(2^p - 1)$ *donde* a *y* b *son enteros no negativos tales que* $a + b = p - 1$ *y* $N = 2^a + 2^a g$.

Demostración. Sea N un repdígito perfecto par en base g. El caso $m = 1$ no necesita prueba. Cuando $m = 2$, tenemos que $N = d(g+1) = 2^{p-1}(2^p-1)$ y 2^p-1 es primo. Siempre que $2^p-1 > 2^{p-1}$

y $g+1>d$, se tiene que 2^p-1 divide a $g+1$. Entonces, d es un divisor de 2^{p-1}, por eso $d=2^a$ para algún $a\in\{1,\ldots,p-1\}$, lo cual nos da que $g+1=2^b(2^p-1)$ con $b=p-1-a$.

Ahora veremos que el caso $m\geq 3$ no es posible. Es claro que 2^p-1 debe dividir a $(g^m-1)/(g-1)$, de otra manera, si dividiera a d, tendríamos

$$g>d\geq 2^p-1>\sqrt{N}\geq\left(\frac{g^m-1}{g-1}\right)^{1/2}=\sqrt{g^{m-1}+\cdots+1}>g^{(m-1)/2}\geq g,$$

lo cual es imposible. En consecuencia, $(g^m-1)/(g-1)=2^b(2^p-1)$ para algún entero no negativo b. Si m es impar o m es par pero g es par, entonces $(g^m-1)/(g-1)$ es impar, por eso $b=0$. Por lo tanto, $d=2^{p-1}<g$, entonces

$$2^p-1=\frac{g^m-1}{g-1}=g^{m-1}+\cdots+1>g^{m-1}\geq g^2>2^{2p-2},$$

lo cual es falso para toda $p\geq 2$. En consecuencia, g debe ser impar y m debe ser par. Escribamos $m=2m_1$. Entonces tenemos que

$$2^b(2^p-1)=\frac{g^{2m_1}-1}{g-1}=(g^{m_1}+1)\left(\frac{g^{m_1}-1}{g-1}\right).$$

En el miembro derecho, el primer factor es mayor que el segundo factor y en el miembro izquierdo, $2^p-1>2^b$ y 2^p-1 es primo. Por lo tanto, 2^p-1 debe dividir a $g^{m_1}+1$, y tenemos que $g^{m_1}+1=2^c(2^p-1)$ y $(g^{m_1}-1)/(g-1)=2^e$ para algunos enteros positivos c y e. De hecho, $c>0$ porque g es impar y $e>0$ porque $m_1=m/2>1$. Siempre que $(g^{m_1}-1)/(g-1)$ es par y g es impar, tenemos que m_1 es par. Por lo tanto, $m_1=2m_2$, y entonces $2^c(2^p-1)=g^{m_1}+1=g^{2m_2}+1\equiv 2 \pmod 8$. Ahora obtenemos que $c=1$, entonces $2^p-1\equiv 1 \pmod 4$, pero esto es falso para cualquier primo $p\geq 2$.

Esto finaliza la prueba de la proposición. □

2. El caso de repdígitos perfectos impares con p el primo de Euler chico

Hasta ahora no se sabe si hay números perfectos impares, pero se sabe que si los hay debe ser de la forma $p\square$, donde p es llamado el primo de Euler y usamos $\square$ para un cuadrado perfecto. Más aún, se sabe que $p\equiv 1 \pmod 4$. Entonces, siguiendo por ejemplo Pollack [**15**], consideremos la ecuación diofántica

$$d\left(\frac{g^m-1}{g-1}\right)=p\square,\qquad \text{donde}\quad d\in\{1,\ldots,g-1\},\quad \text{y}\quad p\text{ es primo.} \tag{2.1}$$

La ecuación (2.1) implica que

$$\frac{g^m-1}{g-1}=c_{d,p}\square, \tag{2.2}$$

donde $c_{d,p}$ es algún entero libre de cuadrados que puede ser determinado fácilmente en términos de p y d. Para determinarlo, escribamos $d = d_1 d_2^2$ donde d_1 es libre de cuadrados. Entonces $c_{d,p} = pd_1$ si $p \nmid d_1$ y $c_{d,p} = d_1/p$ si $p \mid d_1$.

Ahora distinguiremos varios casos. Diremos que el primo de Euler p es *chico* si $p \leq g$. En la siguiente Sección, consideraremos el caso $p > g$ (en este caso diremos que p es grande).

Desde ahora, asumiremos que $g > 2$, porque si $g = 2$, entonces $d = 1$ y $N = 2^m - 1$ para algún $m \geq 2$, pero estos números son congruentes con 3 módulo 4, y por tanto no pueden ser números perfectos impares.

Proposición 13. *Si el primo de Euler p satisface $p \leq g$, entonces cada solución de la ecuación* (2.1) *satisface* $m \leq \max\{144g^2, 12g^3\}$.

Demostración. Notemos que el caso $p = g$ no puede suceder, ya que si $p = g$, entonces p no puede dividir a d (ya que $d < g = p$) y p es coprimo con $(g^m - 1)/(g - 1) = 1 + g + \cdots + g^{m-1} = 1 + p + \cdots + p^{m-1}$. Entonces, asumimos que $p < g$.

Ahora suponemos que d y p son fijos y consideremos la ecuación (2.1) con una ecuación en la variable m. Reescribiendo la ecuación (2.2) como

$$g^m - (g-1)c_{d,p}\square = 1. \tag{2.3}$$

Cuando m es par, la ecuación de arriba tiene la forma

$$X^2 - DY^2 = 1, \tag{2.4}$$

donde $D := (g-1)c_{d,p}$, y $X := g^{m/2}$. Podemos asumir que D no es un cuadrado perfecto, de otra forma la ecuación de arriba no tiene solución no trivial. Por lo tanto, estamos en el caso de una ecuación de Pell como en el Ejemplo 3, usando la notación de dicho ejemplo, tenemos que $x_n = g^{m/2}$. Por lo tanto, x_n no tiene factores excediendo a g. Por el Lema 4 tenemos que $n \leq \max\{6, (g+1)/2\}$. Sea

$$\alpha := x_1 + y_1\sqrt{D}.$$

Por el Lema 1, $\alpha < D^{3\sqrt{D}}$. Como D divide a $(g-1)dp$, tenemos que $D < g(g-1)^2$. Entonces

$$g^{m/2} = x_n < \alpha^n < D^{3n\sqrt{D}} < (g^3)^{3n\sqrt{g(g-1)^2}} \leq g^{9n(g-1)g^{1/2}},$$

dando $m \leq 18(g-1)g^{1/2}n$. Como $n \leq \max\{6, (g+1)/2\}$, tenemos que $m \leq \max\{108g^{3/2}, 9g^{5/2}\}$.

Lo mismo se mantiene cuando m es impar y g es un cuadrado perfecto. Ahora asumiremos que m es impar y g no es un cuadrado. Entonces la ecuación (2.3) puede ser escrita como

$$AX^2 - BY^2 = 1, \tag{2.5}$$

donde $A := g$, $B := (g-1)c_{d,p}$, y $X := g^{(m-1)/2}$. Ahora B no es un cuadrado, en dado caso, la ecuación se vería como $g^m - 1 = \square$, la cual no tiene solución por el resultado de la ecuación de Catalan. Entonces, estamos en el caso del Ejemplo 4. Así, si $x_n = g^{(m-1)/2}$, por el Lema 5 tenemos que $n \leq \max\{12, g+1\}$. Es bien conocido que si

$$\eta := x_1\sqrt{A} + y_1\sqrt{B}, \tag{2.6}$$

entonces $\eta^2 = u_1 + v_1\sqrt{AB}$ es tal que (u_1, v_1) es la solución mínima positiva (u, v) de la ecuación del Pell $U^2 - DV^2 = 1$ con $D := AB$ (ver [**20**]). En particular,

$$\eta^2 < D^{3\sqrt{D}}.$$

Notemos que $D = g(g-1)c_{d,p} < g^2(g-1)^2$. En consecuencia,

$$g^{(m-1)/2} = x_n < \eta^n < D^{(3n/2)\sqrt{D}} < (g^4)^{(3n/2)\sqrt{g^2(g-1)^2}} < g^{6ng(g-1)},$$

lo cual nos da $m - 1 < 12ng(g-1)$. Como $n \leq \max\{12, g+1\}$, tenemos que $m \leq \max\{144g^2, 12g^3\}$, lo cual completa la prueba de esta proposición. □

Observación 1. Observemos que la cota de la Proposición 13 tiene un mérito teórico ya que es explícita en g. Es muy probable que en la práctica esta cota no sea muy útil sin embargo más adelante la enunciaremos para la demostración del Teorema 1. No obstante, la demostración es muy útil. Para cada d y p, calculemos $c_{d,p}$ y generemos la solución mínima de las ecuaciones tipo Pell implicadas por (2.3), la referenciaremos como ecuación (2.4) cuando m es par o g es un cuadrado perfecto, o por la ecuación (2.5) cuando g no es un cuadrado y m es impar (la última ecuación podría no tener soluciones, pero eso lo podemos saber calculando la solución mínima de la ecuación de Pell y verificar por medio de la relación que se da después de la definición de η en (2.6)). Entonces uno puede evaluar x_n para toda $n \leq \max\{6, (g+1)/2\}$ (o $n \leq \max\{12, g+1\}$, respectivamente), y verificar para cuales de estos valores de n se tiene que x_n una potencia g. Este algoritmo detectará candidatos potenciales para m tal que $N = du_m$ es impar, perfecto y el primo de Euler p es chico.

3. El caso de repdígitos perfectos impares con p el primo de Euler grande

Desde ahora, asumiremos que el primo de Euler p satisface $p > g$ y du_m es impar, donde $u_m := (g^m - 1)/(g-1)$. Por lo tanto, $c_d := c_{d,p}/p$ no depende de p porque d es menor que g, por lo tanto también menor que p, en particular es coprimo con p. Distinguiremos y trataremos esta parte en tres casos los cuales estarán en orden creciente de complejidad.

3.1. El caso cuando m es par. Tenemos el siguiente resultado.

Proposición 14. *Si el primo de Euler p satisface $p > g$ y m es par, entonces se tiene que* $m \leq \max\{216g^{3/2}, 18g^{5/2}\}$.

Demostración. Escribiendo $m = 2m_1$, tenemos

$$c_d p\square = \frac{g^m - 1}{g - 1} = \left(\frac{g^{m_1} - 1}{g - 1}\right)(g^{m_1} + 1).$$

Los dos factores del miembro derecho son coprimos porque su máximo común divisor divide a $(g^{m_1} + 1) - (g^{m_1} - 1) = 2$ y ambos son impares. Así, existe algún divisor λ_d de c_d tal que

$$\frac{g^{m_1} - 1}{g - 1} = \lambda_d\square, \qquad \text{o} \qquad g^{m_1} + 1 = \lambda_d\square. \tag{3.1}$$

Si ocurre lo primero, entonces se puede proceder de manera similar al caso cuando p era chico. Reescribamos la ecuación de la izquierda como

$$g^{m_1} - (g - 1)\lambda_d\square = 1,$$

la cual es de la forma $X^2 - DY^2 = 1$ con $X := g^{m_1/2}$ y $D = (g - 1)\lambda_d \leq (g - 1)^2$ si m_1 es par o $g = \square$, o de la forma $AX^2 - BY^2 = 1$ con $A := g$, $X := g^{(m_1-1)/2}$ y $B := (g - 1)\lambda_d$, entonces $D = AB = g(g - 1)\lambda_d \leq g(g - 1)^2$ dado que m_1 es impar y $g \neq \square$. Usando el mismo método que en la prueba de la Proposición 13 resulta que $m \leq \max\{144g, 12g^2\}$ en el caso que m_1 es par o $g = \square$, y $m \leq \max\{216g^{3/2}, 18g^{5/2}\}$ en el caso que m_1 es impar y $g \neq \square$, esto nos da la conclusión deseada.

El caso de la segunda ecuación en (3.1) es similar. Reescribamos dicha ecuación como $g^{m_1} - \lambda_d\square = -1$, reconocemos que esta ecuación es de la forma $X^2 - DY^2 = -1$, con $X := g^{m_1/2}$, $D = \lambda_d \leq g - 1$, dado que m_1 es par o $g = \square$, o de la forma $AX^2 - BY^2 = -1$ con $A := g$, $X := g^{(m_1-1)/2}$ y $B := \lambda_d$, entonces $D = AB = g\lambda_d \leq g(g - 1)$ dado que m_1 es impar y $g \neq \square$. Notemos que en el último caso podríamos asumir que $B = \lambda_d$ no es un cuadrado, ya que si lo fuera, entonces tendríamos que $g^{m_1} - \square = -1$, lo cual da que $m_1 = 1$ (entonces, $m = 2$, lo cual satisface la conclusión de la proposición), o nos da una solución no trivial de la ecuación de Catalan, y la única posibilidad es $2^3 - 3^2 = -1$, entonces $m_1 = 3$ y $g = 2$, lo cual no puede ser ya que $g > 2$. Otra vez, usando el método de la Proposición 13 resulta que $m \leq \max\{72g^{1/2}, 12g^{3/2}\}$ en el caso que m_1 es par o $g = \square$, y $m \leq \max\{144g, 24g^2\}$ en caso que m_1 es impar y $g \neq \square$. □

Observación 2. Consideraciones similares a las mencionadas en la observación 1 con respecto al cálculo de todos los posibles valores de m se aplican también a este caso.

3.2. El caso cuando $d = \square$. En lo que resta de este capítulo, m es impar. Como $d = \square$, tenemos que $c_d = 1$. Probaremos el siguiente resultado.

Proposición 15. *Si $d = \square$, entonces $m = q$ es un primo, o $m = q^2$, donde q es un primo dividiendo a $g - 1$.*

Demostración. Asumimos que m no es un primo y sea q su mínimo factor primo. Observemos que q es impar. Entonces

$$p\square = \frac{g^m - 1}{g - 1} = \left(\frac{g^m - 1}{g^{m/q} - 1}\right)\left(\frac{g^{m/q} - 1}{g - 1}\right), \tag{3.2}$$

donde, al igual que antes, p es el primo de Euler. A continuación veremos que los dos factores del miembro derecho son coprimos o su máximo común divisor es exactamente q, y esto se mantiene únicamente cuando $q \mid g - 1$. Más aún, en ese caso q divide exactamente al primer factor. Para ver esto, sea P un factor primo común de los dos factores que aparecen en el miembro derecho de (3.2). Sea $a := g^{m/q}$. Entonces P divide a $a - 1$ y también a $(a^q - 1)/(a - 1) = (g^m - 1)/(g^{m/q} - 1)$. Como

$$\frac{a^q - 1}{a - 1} = 1 + a + \cdots + a^{q-1} \equiv q \pmod{a - 1},$$

tenemos que P divide a q, por lo tanto, $P = q$. Ahora, q divide a $g^{m/q} - 1$ y por el Teorema Pequeño de Fermat, q también divide a $g^{q-1} - 1$. Por la propiedad de las sucesiones de Lucas expuesta en la Proposición 2, se tiene que q divide a

$$\operatorname{mcd}(g^{m/q} - 1, g^{q-1} - 1) = g^{\operatorname{mcd}(m/q, q-1)} - 1,$$

y, como q es el factor primo más chico de m, tenemos que $\operatorname{mcd}(m/q, q-1) = 1$. Por lo tanto, q divide $g - 1$. Finalmente, para ver que en el último caso q aparece con el exponente 1 en la factorización de el primer factor, observemos que dicho factor se puede escribir como

$$\left(\frac{g^m - 1}{g^{m/q} - 1}\right) = \left(\frac{(g^m - 1)/(g - 1)}{(g^{m/q} - 1)/(g - 1)}\right).$$

Aplicando la Proposición 3 obtenemos que en este caso q divide de manera exacta al primer factor.

Regresando a (3.2), si los dos factores del miembro derecho son coprimos, se debe tener que el primer factor o el segundo es un cuadrado. Por el Teorema de Ljunggren y como el exponente de m es impar, se sigue que $m/q = 1$, lo cual es lo que queríamos probar, o $g = 3$ y $m/q = 5$. La segunda posibilidad nos da que $m = 5q$, entonces $m \in \{15, 25\}$. Sin embargo, ninguno de los números $(3^{15} - 1)/2$ o $(3^{25} - 1)/2$ es de la forma $p\square$. En consecuencia, esta posibilidad no puede ocurrir, y por lo tanto $m = q$ es un primo.

Ahora veamos el caso cuando el máximo común divisor de los dos factores del miembro derecho de (3.2) es precisamente q. Como $q < g < p$, q debe aparecer con exponente par en $(g^m - 1)/(g - 1)$, y como este aparece con exponente 1 en el primer factor del miembro derecho de (3.2), se sigue que q debe dividir también al segundo factor. Se sigue fácilmente que $q \mid m/q$. Por lo tanto, $q^2 \mid m$. Ahora reescribimos la ecuación (3.2) como

$$p\square = \frac{g^m - 1}{g - 1} = \left(\frac{g^m - 1}{g^{m/q^2} - 1}\right)\left(\frac{g^{m/q^2} - 1}{g - 1}\right). \tag{3.3}$$

Por un argumento similar al usado al principio de la prueba de esta proposición, el máximo común divisor de los dos factores del miembro derecho de (3.3) es una potencia de q. Es fácil ver que el exponente de q en $(g^m - 1)/(g^{m/q^2} - 1)$ es exactamente 2. Como el exponente de q en $(g^m - 1)/(g - 1)$ es par, se sigue que el exponente de q en $(g^{m/q^2} - 1)/(g - 1)$ también es par. Estos argumentos muestran que $(g^m - 1)/(g^{m/q^2} - 1)$ es cuadrado, o $(g^{m/q^2} - 1)/(g - 1)$ es un cuadrado. Asumamos que $m > q^2$, la única posibilidad, usando el Teorema de Ljunggren, es $g = 3$ y $m/q^2 = 5$, por lo tanto $m = 5q^2$. Sin embargo, q debe dividir a $g - 1 = 2$, y esto es falso ya que m debe ser impar. La conclusión es que $m = q^2$ debe mantenerse en este caso y que q divide $g - 1$, lo cual es lo que queríamos probar. □

Ahora daremos una cota para m.

Proposición 16. *Si $d = \square$, entonces $m < \max\{g^2, 8g\log(4g)\}$.*

Demostración. Aplicamos la Proposición 15. Si $m = q^2$ para algún primo $q \mid g - 1$, entonces obviamente $m < g^2$. Asumamos que $m = q$ es primo. Podemos asumir también que $q > g$.

En particular, q no divide a $g - 1$. Sea

$$N = d\left(\frac{g^q - 1}{g - 1}\right) = d\prod_{i=1}^{k} Q_i^{\alpha_i} =: dM,$$

donde $Q_1 < \cdots < Q_k$ son primos. Es claro que si Q es un primo dividiendo a M, entonces $g^q \equiv 1 \pmod{Q}$, por lo tanto $q \mid Q - 1$, o $Q \mid g - 1$. La segunda posibilidad implica que $q = Q$, entonces q divide a $g - 1$, lo cual no puede ser. Por lo tanto, $Q_i \equiv 1 \pmod{q}$ para toda $i = 1, \ldots, k$. Así tenemos que

$$g^q > \frac{g^q - 1}{g - 1} = M \geq (2q + 1)^k,$$

entonces

$$k < \frac{q\log g}{\log(2q + 1)}. \tag{3.4}$$

Ahora observemos que d y M son coprimos. Si no lo fueran, tendríamos que d sería divisible por algún primo Q, entonces $d \geq Q \geq 2q + 1 > 2d$, lo cual es imposible.

Por ello,

$$\sigma(N) = \sigma(d)\sigma(M).$$

Como d es un divisor propio de un número perfecto N, tenemos que $\sigma(d) < 2d$, por lo tanto $\sigma(d) \leq 2d - 1$. Tenemos que

$$2 = \frac{\sigma(N)}{N} = \left(\frac{\sigma(d)}{d}\right)\left(\frac{\sigma(M)}{M}\right) \leq \left(\frac{2d-1}{d}\right)\left(\frac{\sigma(M)}{M}\right),$$

Entonces

$$\frac{\sigma(M)}{M} \geq \frac{2d}{2d-1} = 1 + \frac{1}{2d-1} > 1 + \frac{1}{2g}.$$

Como $\sigma(M)/M < M/\phi(M)$, tenemos que

$$1 + \frac{1}{2g} < \frac{M}{\phi(M)} = \prod_{i=1}^{k}\left(1 + \frac{1}{Q_i - 1}\right).$$

Tomando logaritmos y usando la desigualdad

$$x/2 < \log(1+x) < x \quad \text{es válida} \quad \forall x \in (0,1),$$

junto con (3.4) y el hecho de que $q > g$, obtenemos que

$$\begin{aligned}
\frac{1}{4g} &< \log\left(1 + \frac{1}{2g}\right) < \sum_{i=1}^{k} \log\left(1 + \frac{1}{Q_i - 1}\right) < \sum_{i=1}^{k} \frac{1}{Q_i - 1} \\
&< \frac{1}{2q}\sum_{i=1}^{k}\frac{1}{i} < \frac{1}{2q}\left(1 + \int_1^k \frac{dt}{t}\right) = \frac{1}{2q}(1 + \log k) \\
&< \frac{1}{2q}\left(1 + \log\left(\frac{q\log g}{\log(2q+1)}\right)\right) < \frac{1}{2q}\log(eq)
\end{aligned}$$

(aquí usamos el hecho que $q > g$ y por tanto $\log(2q+1) > \log g$), lo cual implica

$$q < 2g\log(eq) < 4g\log q, \tag{3.5}$$

donde la última desigualdad se sigue porque $q \geq 3 > e$.

Aplicando el Lema 11 a la desigualdad (3.5), la cual puede ser reescrita como $q/\log q < 4g$, tenemos que $q < 8g\log(4g)$, que es el resultado deseado. □

3.3. El caso cuando m es impar y $d \neq \square$. A lo largo de esta Sección, en lugar de c_d escribiremos c y estudiaremos la ecuación

$$u_m = cp\square, \tag{3.6}$$

donde $\{u_n\}_{n\geq 0}$ es la sucesión de Lucas de término general $u_n = (g^n - 1)/(g-1)$ para toda $n \geq 0$ del Ejemplo 2 presentado en la Subsección 2.1, $c \in \{2, \ldots, g-1\}$ es libre de cuadrados y $p > g$ es un primo. Luego, usaremos el hecho de que du_m es perfecto para algún $d \leq g - 1$ tal que $dc = \square$.

Observemos que podemos asumir $g \geq 4$, ya que si $g = 3$, tendríamos que $d = 1$, este caso fue tratado en la Subsección 3.2, o $d = 2$ es el caso en el que N es par, y este caso fue tratado en Sección 1.

A continuación trabajaremos con el parámetro $Z(k)$ definido en la Subsección 2.1.

Proposición 17. *Supongamos que k es libre de cuadrados y que para algún $m \geq 1$ tenemos que*

$$u_m = \prod_{p|k} p^{a_p} \prod_{\substack{q \nmid k \\ q|g-1}} q^{b_q} \prod_{\substack{r|u_m \\ r \nmid k(g-1)}} r^{c_r},$$

donde a_p es impar para toda $p \mid k$ y b_q es par para toda $q \nmid k$ con $q \mid (g-1)$. Entonces:

(i) *$Z(k) \mid m$;*
(ii) *Si $m = Z(k) \prod_{p|k(g-1)} p^{\alpha_p} \prod_{\substack{q|m \\ q \nmid k(g-1)}} q^{\beta_q}$, entonces α_p es par para todos los primos $p \mid k(g-1)$.*

Demostración. Como a_p es impar, se sigue que $a_p \geq 1$, por lo tanto k divide a u_m. Así, $z(k)$ divide a m. Por lo tanto, como $u_{z(k)} \mid u_m$, tenemos que $a_p \geq e_p$. Si e_p es par, entonces como a_p es impar, se sigue que $a_p \geq e_p + 1$, y $e_p \geq 1$ ya que $k \mid u_{z(k)}$. Así, para estos p, se debe tener que $z(p^{e_p+1}) = pz(p) \mid m$.

Como $z(k) \mid m$, también tenemos que $b_q \geq f_q$. Pero $q \mid g-1$ entonces $z(q^{f_q}) = q^{f_q} \| u_{z(k)}$, y se deduce que $q^{f_q} \| z(k)$. De manera similar, $q^{b_q} \| m$. Consecuentemente, si f_q es impar, entonces $b_q \geq f_q + 1$, porque b_q es par, entonces, $q^{f_q+1} \mid m$. Por lo tanto, m es un múltiplo de

$$A := \text{mcm}[a : a \in \mathcal{A}],$$

donde $\mathcal{A}$ es el siguiente conjunto de números

$$\begin{aligned} \mathcal{A} &:= \{z(k)\} \cup \{pz(p) : p \mid k \text{ y } e_p \equiv 0 \pmod 2\} \\ &\cup \{q^{f_q+1} : q \nmid k,\ q \mid (g-1) \text{ y } f_q \equiv 1 \pmod 2\}. \end{aligned}$$

Sin embargo, es fácil ver que el mínimo común múltiplo de arriba es precisamente $Z(k)$. Esto prueba (i). La parte (ii) es también inmediata. □

Tenemos el siguiente corolario.

Corolario 18. *Si m da una solución a la ecuación $u_m = cp\square$ con un primo $p > g$ y un entero libre de cuadrados c con $1 \leq c \leq g-1$, entonces m es un múltiplo de $Z(c)$. Más aún, los exponentes de los primos dividiendo a $c(g-1)$ aparecen en la factorización de $m/Z(c)$ con exponente par.*

Esto sugiere hacer lo siguiente. Dado un impar libre de cuadrados $k > 1$, sea $\mathcal{M}_k$ el conjunto de enteros positivos impares m tales que la relación

$$u_m = k\delta_m\square \quad \text{se mantiene con} \quad \mu^2(k\delta_m) = 1 \quad \text{y} \quad \text{mcd}(\delta_m, g-1) = 1. \tag{3.7}$$

Usamos la función de Möbius $\mu(n)$ con su significado estándar, esto es 0 si n no es libre de cuadrados, y es $(-1)^{\omega(n)}$, donde $\omega(n)$ es el número de distintos factores primos de n, en caso que n sea libre de cuadrados. De lo dicho arriba, tenemos que $Z(k)$ divide a m para todos los enteros $m \in \mathcal{M}_k$. Más aún, si m_1 divide a m_2 y ambos están en $\mathcal{M}_k$, entonces todos los factores primos dividiendo a $k(g-1)$ aparecen con exponente par en m_2/m_1. Entonces, tiene sentido estudiar qué pasa con δ_{m_1} y δ_{m_2} en el caso cuando m_2/m_1 es un primo que no divide a $g-1$, o el cuadrado de un primo que divide a $k(g-1)$.

Tenemos la siguiente proposición, la cual puede ser pensada como una generalización de la Proposición 15.

Proposición 19. *Sea $k > 1$ un impar libre de cuadrados y sean m_1, m_2 enteros impares positivos. Supongamos que*

$$u_{m_1} = k\delta_{m_1}\square, \qquad y \qquad u_{m_2} = k\delta_{m_2}\square,$$

donde

$$\mu^2(k\delta_{m_1}) = \mu^2(k\delta_{m_2}) = mcd(\delta_{m_1}, g-1) = mcd(\delta_{m_2}, g-1) = 1,$$

y $m_2 = m_1 t$, con t siendo un primo que no divide a $k(g-1)$, o el cuadrado de un primo que divide a $k(g-1)$. Entonces $\omega(\delta_{m_2}) \geq \omega(\delta_{m_1})$. La última desigualdad siempre es estricta excepto posiblemente cuando t es un factor primo de δ_{m_1}.

Demostración. Para empezar, escribamos $m = p_1 p_2 \cdots p_s$, con $3 \leq p_1 \leq p_2 \leq \cdots \leq p_s$ y

$$u_m = \left(\frac{u_m}{u_{m/p_1}}\right)\left(\frac{u_{m/p_1}}{u_{m/(p_1p_2)}}\right)\cdots\left(\frac{u_{m/(p_1\cdots p_{s-1})}}{u_{m/(p_1\cdots p_s)}}\right) =: N_{m,1}\cdots N_{m,s}.$$

La observación principal es que $\text{mcd}(N_{m,i}, N_{m,j}) = 1$ para todas $1 \leq i < j \leq s$ excepto cuando $p_i = \cdots = p_j := q$ es un factor primo de $g-1$. En dicho caso, $q \| N_{m,\ell}$ para toda $\ell = i, i+1, \ldots, j$. En efecto, si $q \mid \text{mcd}(N_{m,i}, N_{m,j})$, entonces $q \mid u_{m/(p_1\cdots p_{j-1})} \mid u_{m/(p_1\cdots p_i)}$ (porque $i < j$) y también $q \mid N_{m,i} = u_{m/(p_1\cdots p_{i-1})}/u_{m/(p_1\cdots p_i)}$ (donde $p_0 := 1$). Por lo tanto,

$$q \mid \text{mcd}\left(u_{m/(p_1\cdots p_i)}, \frac{u_{m/(p_1\cdots p_{i-1})}}{u_{m/(p_1\cdots p_i)}}\right).$$

Es bien conocido y fácil de ver que esto es posible únicamente cuando $q = p_i$. Ahora $q \mid g^{m/(p_1\cdots p_{j-1})} - 1 = g^{p_j\cdots p_s} - 1$, y $q \mid g^{p_i - 1} - 1$, por tanto $q \mid g^{\text{mcd}(p_i-1, p_j\cdots p_s)} - 1$. Como $p_i - 1$ y $p_j \cdots p_s$ son coprimos, tenemos que $q \mid g - 1$. Como $q \mid u_{m/p_1\cdots p_{j-1}}/u_{m/(p_1\cdots p_j)}$ y $q \mid g-1$, se sigue que $q = p_j$. Por lo tanto, $q = p_i = \cdots = p_j$, lo cual es lo que habíamos dicho. El resto de la afirmación, $q \| N_{\ell,m}$ para

$\ell = i, i+1, \ldots, j$, es también claro. (Este argumento ha aparecido antes en varias partes como por ejemplo en la demostración del Lema 3 en [**13**])

Ahora escribamos

$$N_{m,i} = A_{m,i}B_{m,i}\square, \qquad \text{para} \qquad i = 1, \ldots, s,$$

donde $\mu^2(A_{m,i}B_{m,i}) = 1$, todos los factores primos de $B_{m,i}$ dividen a $g-1$, y $A_{m,i}$ es coprimo con $g-1$. Como se tiene que para cada primo impar p y cada entero positivo l, $p \mid g-1$ implica que los exponentes de p en las factorizaciones de l y u_l son los mismos, se sigue fácilmente que $B_{m,i} = p_i$ o 1 de acuerdo a si p_i divide $g-1$ o no. Además, por la observación hecha arriba, cada pareja de enteros positivos $A_{m,1}, \ldots, A_{m,s}$ son coprimos.

Asumamos ahora que $m \in \mathcal{M}_k$, es decir, $u_m = k\delta_m\square$ con $\mu^2(k\delta_m) = \text{mcd}(\delta_m, g-1) = 1$. Entonces, como $k = \text{mcd}(k, g-1) \cdot (k/\text{mcd}(k, g-1))$, tenemos que

$$\prod_{i=1}^{s} B_{m,i} = \text{mcd}(k, g-1)\square \qquad \text{y} \qquad \prod_{i=1}^{s} A_{m,i} = \left(\frac{k}{\text{mcd}(k, g-1)}\right)\delta_m\square$$

(los $\square$ que están más a la derecha son de hecho iguales a 1). Asumamos ahora que $m := m_1$ y que $m_2 := m_1 t$ está también en $\mathcal{M}_k$. Asumamos también que $t = q$ es un primo con $q \nmid g-1$.

Observemos la expresión

$$u_{m_2} = N_{m_2,1} \cdots N_{m_2,s+1}$$

y comparemos esta factorización con

$$u_{m_1} = N_{m_1,1} \cdots N_{m_1,s}$$

de u_{m_1}. Sea i_0 el mínimo índice en $\{0, 1, \ldots, s\}$ para el cual la desigualdad $p_i \le q < p_{i+1}$ se mantiene, donde $p_0 := 1$ y $p_{s+1} := \infty$. Observemos que i_0 es el único índice i tal que la desigualdad $p_i < q < p_{i+1}$ se mantiene en el caso que $q \nmid m_1$, mientras que i_0 es el mínimo índice i para el cual $p_i = q$ en caso de que $q \mid m_1$. En los casos extremos $i_0 = 0$ e $i_0 = s$ leemos que $q < p_1$ y $q \ge p_s$, respectivamente. Tenemos que $N_{m_2,\ell+1} = N_{m_1,\ell}$ para toda $\ell \ge i_0 + 1$. Si $1 \le \ell \le i_0$, Entonces

$$N_{m_2,\ell} = \frac{u_{drq}}{u_{dq}} \qquad \text{y} \qquad N_{m_1,\ell} = \frac{u_{dr}}{u_d},$$

donde $d := p_{\ell+1} \cdots p_s$ y $r := p_\ell$. Veamos que $N_{m_1,\ell} \mid N_{m_2,\ell}$ para toda $\ell = 1, \ldots, i_0 - 1$. En efecto, si $q \ne r$ esto es cierto aun cuando $\ell := i_0$ porque entonces

$$\frac{N_{m_2,\ell}}{N_{m_1,\ell}} = \frac{u_{dqr}u_d}{u_{dq}u_{dr}} = \frac{(g^{dqr}-1)(g^d-1)}{(g^{dq}-1)(g^{dr}-1)} = \Phi_{qr}(g^d) \in \mathbb{Z}, \tag{3.8}$$

donde $\Phi_{qr}(X)$ es el polinomio ciclotómico cuyas raíces son las raíces primitivas de la unidad de orden qr. Por lo tanto, $N_{m_1,\ell} \mid N_{m_2,\ell}$ para toda $\ell = 1, \ldots, i_0$, si $q \ne r$. Por otro lado, el caso $q = r$ conduce a $p_{i_0} \le q = r = p_\ell$, así $\ell \ge i_0$ y esto es posible cuando $\ell \le i_0$ que solo es posible cuando

$\ell = i_0$. Así, la relación de divisibilidad $N_{m_1,\ell} \mid N_{m_2,\ell}$ se mantiene para toda $\ell = 1, \ldots, i_0 - 1$, y uno puede verificar que $N_{m_2,i_0+1} = N_{m_1,i_0}$ en el caso de que $q = p_{i_0} \mid m_1$.

Así, resumiendo, mostramos que

$$N_{m_2,\ell} = N_{m_1,\ell-1} \qquad \text{para toda} \qquad \begin{cases} i_0 + 2 \leq \ell \leq s + 1, & \text{si} \quad q \nmid m_1, \\ i_0 + 1 \leq \ell \leq s + 1, & \text{si} \quad q \mid m_1, \end{cases}$$

y que

$$N_{m_1,\ell} \mid N_{m_2,\ell} \qquad \text{para toda} \qquad \begin{cases} 1 \leq \ell \leq i_0, & \text{si} \quad q \nmid m_1, \\ 1 \leq \ell \leq i_0 - 1, & \text{si} \quad q \mid m_1. \end{cases}$$

Sea $j_0 := i_0$ si q no divide a m_1 y $j_0 := i_0 - 1$ si q divide a m_1. Recordemos que estamos asumiendo que q no divide a $g - 1$.

Primero trataremos el caso cuando q no divide a δ_{m_1}. Entonces los exponentes de todos los primos dividiendo a δ_{m_1} en u_{m_1} y u_{m_2} son los mismos.

Esto muestra que

$$\begin{aligned} &A_{m_2,\ell} = A_{m_1,\ell-1} \text{ y } B_{m_2,\ell} = B_{m_1,\ell-1}, \text{ para toda } j_0 + 2 \leq \ell \leq s + 1, \\ &A_{m_1,\ell} \mid A_{m_2,\ell} \text{ y } B_{m_2,\ell} = B_{m_1,\ell}, \quad \text{para toda } 1 \leq \ell \leq j_0. \end{aligned} \tag{3.9}$$

Sin embargo, todavía tenemos que considerar el número

$$N_{m_2,j_0+1} = A_{m_2,j_0+1} B_{m_2,j_0+1} \square.$$

Por lo que mostramos arriba, y como estamos asumiendo que q no divide a $g - 1$, tenemos que $B_{m_2,j_0+1} = 1$. Además, el número N_{m_2,j_0+1} no es un cuadrado perfecto por el Teorema de Ljunggren (recordemos que las dos soluciones excepcionales de la ecuación $(x^n - 1)/(x - 1) = y^2$ con $x > 1$ y $n > 2$ son $(x, n) = (3, 5)$ y $(7, 4)$, las cuales no aplican en nuestro argumento ya que estamos considerando que $g \geq 4$ y que los exponentes son impares). Por lo tanto, $A_{m_2,j_0+1} > 1$, y como

$$\prod_{\ell=1}^{s+1} B_{m_2,\ell} = \prod_{\ell=1}^{s} B_{m_1,\ell} = \operatorname{mcd}(k, g - 1)\square,$$

tenemos que

$$\frac{\delta_{m_2} k}{\operatorname{mcd}(k, g - 1)} = \prod_{\ell=1}^{s+1} A_{m_2,\ell} \text{ es múltiplo propio de } \prod_{\ell=1}^{s} A_{m_1,\ell} = \frac{\delta_{m_1} k}{\operatorname{mcd}(k, g - 1)}.$$

Notemos que hemos usado el hecho de que $A_{m_i,\ell}$ son coprimos y libres de cuadrados, así el cuadrado $\square$ en las ecuaciones para sus productos con $i = 1, 2$ en cada caso es 1, así dichos cuadrados no interfieren.) Así, vemos que si $t = q$ y $q \nmid \delta_{m_1}$, entonces $\delta_{m_2}/\delta_{m_1} > 1$ es un entero, así $\omega(\delta_{m_2}) > \omega(\delta_{m_1})$.

Pequeñas variaciones a este argumento sirven para el resto de los casos. Por ejemplo, supongamos que todavía tenemos $t = q$ pero $q \mid \delta_{m_1}$. Supongamos primero que q no divide a m_1, así $j_0 = i_0$. Con la notación de arriba, sea i_1 el único índice $i \in \{1, \ldots, s\}$ tal que $q \mid A_{m_1,i_1}$. Entonces $q \mid N_{m_1,i_1}$. No es difícil verificar que p_{i_1} es el mínimo factor primo del índice de aparición $z(q)$ de q en $\{u_n\}_{n\geq 0}$. Notemos que $z(q) \leq q - 1 < q$, por lo tanto $q > p_{i_1}$. En particular, $i_1 \leq i_0$. Así, como N_{m_1,i_1} es divisible por q a un exponente impar y $m_2 = m_1 q$, se sigue que N_{m_2,i_1} es divisible por q a un exponente par. Todo permanece igual que antes, así las relaciones (3.9) se mantienen para toda $\ell \in \{1, 2, \ldots, s+1\}$ excepto para $\ell = j_0 + 1$ y $\ell = i_1$, cuando $\ell = i_1$, tenemos que $A_{m_1,i_1}/q \mid A_{m_2,i_1}$ (y $B_{m_2,i_1} = B_{m_1,i_1}$). Así, aquí perdimos un primo de δ_{m_1} (le llamemos q), pero ganamos al menos un primo de A_{m_2,j_0+1}. Esto muestra que $\omega(\delta_{m_2}) \geq \omega(\delta_{m_1})$, pero ya no es cierto que δ_{m_1} divide a δ_{m_2} en este caso (aunque δ_{m_1}/q divide a δ_{m_2}).

Ahora asumamos que todavía estamos en el caso que $t = q$ divide a δ_{m_1}, pero que $q \mid m_1$. Entonces $j_0 = i_0 - 1$ y $i_1 < i_0$. Con la misma notación de antes, tenemos otra vez que $q \mid N_{m_1,i_1}$. Sin embargo, recordando que $q^{e_q} \| u_{z(q)}$, se sigue que $q^a \| m_1$, donde $a \geq 1$ es algún entero tal que $a + e_q \equiv 1 \pmod 2$. Como $p_{i_1} < q$, se sigue que $m_1/(p_1 \cdots p_{i_1-1})$ es un múltiplo de $z(q)q^a$, mientras que $m_2/(p_1 \cdots p_{i_1-1})$ es un múltiplo de $z(q)q^{a+1}$. Así, las relaciones (3.9) se mantienen para toda $\ell \in \{1, \ldots, s+1\}$ excepto para $\ell = j_0 + 1$ y $\ell = i_1$, mientras que para $\ell = i_1$, tenemos, como en el caso anterior, que $A_{m_1,i_1}/q \mid A_{m_2,i_1}$ (y $B_{m_2,i_1} = B_{m_1,i_1}$). Así, otra vez perdemos un primo de δ_{m_1} (le llamemos a este primo q), pero ganamos al menos otro primo de $A_{m_2,j_0+1} > 1$. Así, otra vez tenemos que $\omega(\delta_{m_2}) \geq \omega(\delta_{m_1})$.

Ahora vamos a esbozar el caso cuando $t = q^2$ y q divide a $k(g-1)$. Mantendremos la notación i_0 como el mínimo índice i en $\{0, \ldots, s\}$ tal que $p_i \leq q < p_{i+1}$. Entonces como en el caso anterior, uno argumenta que existe $j_0 \in \{0, \ldots, s+2\}$ tal que

$$N_{m_2,\ell} = N_{m_1,\ell-2} \qquad \text{para toda} \qquad \ell \in \{j_0 + 3, \ldots, s+2\}, \tag{3.10}$$

y

$$N_{m_1,\ell} \mid N_{m_2,\ell} \qquad \text{para toda} \qquad \ell \in \{1, \ldots, j_0\}. \tag{3.11}$$

Aquí, otra vez $j_0 := i_0$ si q es coprimo con m_1 y $j_0 := i_0 - 1$ si $q \mid m_1$. Para la relación de divisibilidad (3.11), uno usa el hecho de que el polinomio

$$\frac{(X^{q^2 r} - 1)(X - 1)}{(X^{q^2} - 1)(X^r - 1)} = \Phi_{q^2 r}(X)\Phi_{qr}(X) \qquad \text{tiene coeficientes enteros,}$$

en lugar del argumento de la relación (3.8). Por lo tanto, $A_{m_2,\ell} = A_{m_1,\ell-2}$ y $B_{m_2,\ell} = B_{m_1,\ell-2}$ para toda $\ell \in \{j_0 + 3, \ldots, s+2\}$. Por argumentos similares a los anteriores, tenemos fácilmente que cuando

q divide a $g-1$, y q no divide a δ_{m_1}, tenemos también que $A_{m_1,\ell} \mid A_{m_2,\ell}$ y $B_{m_1,\ell} = B_{m_2,\ell}$ para toda $\ell \in \{1,\dots,j_0\}$.

Cuando q divide a $k/\mathrm{mcd}(k,g-1)$, una conclusión similar puede ser deducida de la siguiente forma. Primero observemos que $q \mid k \mid g^{m_1}-1$ y $q \mid g^{q-1}-1$ por el pequeño Teorema de Fermat. Por lo tanto, $q \mid g^{\mathrm{mcd}(m_1,q-1)}-1$ y como $q \nmid g-1$, se sigue que $q \mid u_{\mathrm{mcd}(m_1,q-1)}$. En otras palabras, $i_0 > 0$ y $q \mid u_{p_1\dots p_{j_0}}$. Ahora, cada una de las expresiones $N_{m_1,\ell}$ para $\ell \in \{1,\dots,j_0\}$ es de la forma $(g^{dr}-1)/(g^d-1)$ para algún primo $r < q$ y su correspondiente $N_{m_2,\ell}$ es de la forma $(g^{drq^2}-1)/(g^{dq^2}-1)$. Ahora es fácil verificar que el exponente del primo q tiene la misma clase residual módulo 2 en la factorización de $N_{m_1,\ell}$ y $N_{m_2,\ell}$, respectivamente, lo cual implica que $A_{m_1,\ell} \mid A_{m_2,\ell}$ para $\ell \in \{1,\dots,j_0\}$. Todavía tenemos que analizar N_{m_2,j_0+1} y N_{m_2,j_0+2}. Como $q \mid k(g-1)$, tenemos que $B_{m_2,j_0+2} = B_{m_2,j_0+1}$ y su valor común es q o 1 de acuerdo a si q divide a $(g-1)$ o $k/\mathrm{mcd}(k,g-1)$, respectivamente.

Recordemos que A_{m_2,j_0+1} y A_{m_2,j_0+2} son coprimos. Si fuera cierto que A_{m_2,j_0+1} y A_{m_2,j_0+2} son 1, deberíamos tener que con algún divisor d de m_1 (aquí, $d := p_{i_0+1}\cdots p_s$ si $q \nmid m_1$ y $d := p_{i_0}\cdots p_s$ cuando $q \mid m_1$), se tendría que

$$\frac{g^{dq}-1}{g^d-1} = B_{m_2,j_0+2}\square, \qquad \text{y} \qquad \frac{g^{dq^2}-1}{g^{dq}-1} = B_{m_2,j_0+1}\square.$$

Por el Teorema de Ljunggren, ninguno de B_{m_2,j_0+2} o B_{m_2,j_0+1} pueden ser 1 así ambos deben ser q. Al multiplicar las relaciones de arriba, obtendríamos $(g^{dq^2}-1)/(g^d-1) = \square$, lo cual es imposible. Así, $e := A_{m_2,j_0+1}A_{m_2,j_0+2} > 1$. Porque, como hemos visto, $A_{m_1,\ell} | A_{m_2,\ell}$ para $1 \le \ell \le j_0$ y $A_{m_1,\ell} = A_{m_2,\ell+2}$ para $j_0+1 \le \ell \le s$, el producto de $A_{m_1,\ell}$ divide al producto de $A_{m_2,\ell}/e$. Como $e > 1$, tenemos que el cociente de $A_{m_1,\ell}$ sobre $A_{m_2,\ell}$ es mayor que 1. Pero este cociente es también el cociente $\delta_{m_2}/\delta_{m_1}$. Como δ_{m_1} y δ_{m_2} son libres de cuadrados, se sigue que $\omega(\delta_{m_2}) > \omega(\delta_{m_1})$. □

El siguiente corolario es de interés:

Corolario 20. (i) *Si $m_1 \mid m_2$ están en $\mathcal{M}_k$, $m_2/m_1 > 1$ y $\delta_{m_1} = 1$, entonces $\delta_{m_2} > 1$.*

(ii) *Si $m_1 \mid m_2$ están en $\mathcal{M}_k$, $m_2/m_1 > 1$ y $\delta_{m_1} > g$ es primo, entonces $\delta_{m_2} > 1$, además, si es primo se tiene $m_2 = m_1\delta_{m_1}$.*

Demostración. La parte (i) es inmediata. De hecho, sea $r \mid m_2/m_1$ y supongamos que $u_{m_2} = k\square$. Entonces $r^2 \mid m_2/m_1$ si r divide a $k(g-1)$. Sea $t := r^2$ si r divide a $k(g-1)$ y $t := r$ en otro caso. Entonces $m_1 t \mid m_2$, y $\delta_{m_1} = 1$, entonces por la Proposición 19, tenemos que $\delta_{m_1 t} > 1$. Por lo tanto, $\omega(\delta_{m_1 t}) \ge 1$. Por inducción sobre el número de factores primos de $m_2/(m_1 t)$ usando la Proposición 19, tenemos que $\omega(\delta_{m_2}) \ge 1$, lo cual nos da una contradicción.

Para (ii), denotemos con p a δ_{m_1}. Sea r algún factor primo de m_2/m_1. Otra vez, sea $t := r^2$ si r divide a $k(g-1)$ y $t := r$ en otro caso. Entonces $m_1 t$ divide a m_2.

Más aún, por la Proposición 19, si $r \neq p$ entonces $\omega(\delta_{m_1 t}) \geq 2$.

Ahora, por inducción sobre el número de factores primos de $m_2/(m_1 t)$, por la Proposición 19 tenemos que $\omega(\delta_{m_2}) \geq 2$, lo cual nos da una contradicción. Por lo tanto, debemos tener que $r = p$.

Pero entonces esto es cierto para cada factor primo de m_2/m_1, así $m_2 = m_1 p^a$ para algún $a \geq 1$.

Ahora mostraremos que $a = 1$. Asumamos que no. La Proposición 19 muestra que $u_{m_1} = kp\square$ y $u_{pm_1} = kq\square$, donde $q = \delta_{m_1 p}$ es un primo. Entones q no es el mismo primo que p (de hecho, $q \equiv 1 \pmod{p}$ como $p > g$). Por lo tanto, por la Proposición 19 aplicada a $m_1 p$ y $m_1 p^2$, tenemos que $\omega(\delta_{m_1 p^2}) > \omega(\delta_{m_1 p}) = 1$.

Por inducción sobre a usando la Proposición 19, tenemos que $\omega(\delta_{m_2}) = \omega(\delta_{m_1 p^a}) \geq \omega(\delta_{m_1 p^2}) \geq 2$, lo cual es una contradicción. □

3.3.1. Un algoritmo para calcular todas las soluciones. Ahora estamos listos para explicar un algoritmo que detecta todos los candidatos para m tales que $N = du_m$ es perfecto. Recordemos que estamos en el caso en que N es impar, $p > g$, $d \neq \square$, m impar y $g \geq 4$.

Regresemos a la ecuación (3.6), es decir, $u_m = cp\square$ con $c = c_d$. Primero eliminaremos tres casos donde restricciones modulares implican que no hay solución: d par, $g \equiv 2 \pmod{4}$ con $d \equiv 1 \pmod{4}$, y $4 \mid g$ con $d \equiv 3 \pmod{4}$.

Observe que, como en este caso $\delta_m = p > g$, se tiene que $\mathrm{mcd}(\delta_m, g-1) = 1$, entonces $m \in \mathcal{M}_c$. Por la Proposición 17, $m_d := Z(c) \mid m$. En consecuencia, $u_{m_d} = c\delta_d\square$ con δ_d libre de cuadrados. Claramente, $m_d \in \mathcal{M}_c$. Sea $m =: m_d n$. Entonces, por el Corolario 18, todos los factores primos de n dividiendo a $c(g-1)$ aparecen con exponente par en n. El objetivo es dar una lista corta que contenga a todos los candidatos para n.

Recordemos que

$$u_{m_d} = c\delta_d\square, \qquad \text{donde} \qquad \mu^2(c\delta_d) = \mathrm{mcd}(\delta_d, g-1) = 1.$$

Si $\omega(\delta_d) \geq 2$, entonces la Proposición 19 más inducción en el número de factores primos de m/m_d, muestra que $\omega(\delta_m) \geq 2$ para toda $m \in \mathcal{M}_c$, entonces no tenemos soluciones para n.

Si δ_d es un primo, entonces el Corolario 20 (ii) muestra que $n \in \{1, \delta_d\}$.

Ahora asumamos que $\delta_d = 1$. Escribamos

$$N = \left(d\frac{g^{m_d}-1}{g-1}\right)\left(\frac{g^{m_d n}-1}{g^{m_d}-1}\right). \tag{3.12}$$

Supongamos primero que los dos factores de la derecha en la relación (3.12) no son coprimos. Sea q un primo dividiendo a dichos factores. Si $q \mid u_{m_d}$, entonces como $q \mid (g^{m_d n}-1)/(g^{m_d}-1) = u_{m_d n}/u_{m_d}$, obtenemos que $r \mid n$, donde $r = q$. Si no, entonces $q \mid d$ y $q \nmid u_{m_d}$, entonces $z(q) \mid m_d n$ y $z(q) \nmid m_d$. Por lo tanto, existe un primo r tal que $r \mid n$, y este primo es q si $q \mid u_{m_d}$, o es un factor primo de $z(q)/\mathrm{mcd}(z(q), m_d)$, donde $q \mid d$. En cualquier caso, podemos decir que n es un múltiplo de t, donde $t := r$, si r no divide a $c(g-1)$, y $t := r^2$, si r divide a $c(g-1)$, y r es un primo como se mencionó anteriormente. Ahora

$$u_{m_d t} = c\delta_{d,t}\square,$$

por el Corolario 20 (i), tenemos que $\delta_{d,t} > 1$. Si $\omega(\delta_{d,t}) \geq 2$, entonces no hay soluciones para n, si $\delta_{d,t}$ es un primo, entonces $n \in \{t, t\delta_{d,t}\}$, por el Corolario 20 (ii).

Ahora asumamos que los dos factores que aparecen en el lado derecho de la ecuación (3.12) son coprimos. Entonces

$$2N = \sigma(N) = \sigma(du_{m_d})\sigma\left(\frac{g^{m_d n}-1}{g^{m_d}-1}\right).$$

Ahora $du_{m_d} < \sigma(du_{m_d}) < 2du_{m_d}$. Sabemos que si $q^a \| du_{m_d}$, entonces $q^a \| 2N$. Por lo tanto, debe existir un número primo q dividiendo a $\sigma(du_{m_d})$ el cual no divide a du_{m_d}. Si este primo es 2, entones $\sigma(u_{m_d n}/u_{m_d})$ es impar, por lo tanto $u_{m_d n}/u_{m_d} = \square$, lo cual no es posible para $n > 1$ por el Teorema de Ljunggren. Por lo tanto, q es impar. Así conseguimos que $q \mid (g^{m_d n}-1)/(g^{m_d}-1)$, por lo tanto $z(q) \mid m_d n$, pero $z(q) \nmid m_d$. Sea r algún factor primo de $z(q)/\mathrm{mcd}(z(q), m_d)$. Entonces n es divisible por t, donde al igual que antes ponemos $t := r$, si r no divide a $c(g-1)$, y $t := r^2$, en otro caso. Ahora escribamos

$$u_{m_d t} = c\delta_{d,t}\square.$$

Entonces $\delta_{d,t} > 1$ por Corolario 20 (i). Si $\omega(\delta_{d,t}) \geq 2$, no hay soluciones para n. Finalmente, si $\delta_{d,t}$ es un primo, entonces $n \in \{t, t\delta_{d,t}\}$, por Corolario 20 (ii).

Esto agota todas las posibilidades, y así todos los candidatos potenciales para m tales que du_m es perfecto.

4. Demostración del Teorema 1

Empezaremos con la parte (i) del Teorema 1. Si N es par, la Proposición 12 muestra que $N < g^2$. Cuando N es impar, entonces $N < g^m$, así es suficiente acotar m. Cuando N es impar y el primo de Euler p es chico, entonces la Proposición 13 muestra que $m < 144g^3 < g^{11}$, cuando $p > g$ es grande pero m es par, entonces $m \leq 216g^{5/2} < g^{11}$ porque $g \geq 2$. Cuando p es grande y $d = \square$, la Proposición 16 muestra que $m < g^2$, o $m < 8g\log(4g) \leq 8g\log(g^3) = 24g\log g < g^{11}$.

Resumiendo, en todos los casos excepto el último cuando N es impar, p grande y $d \neq \square$, tenemos que $m < g^{11} < g^{g^4} < g^{g^{g^2}}$. Así, veamos que el último caso sólo puede ocurrir cuando $g \geq 4$.

Es claro que $z(c_d) \leq c_d \leq g-1$, por lo tanto $m_d = Z(c_d) \leq z(c_d)d(g-1) \leq (g-1)^3$. Por consiguiente, factores primos q de du_{m_d}, o de $\sigma(du_{m_d})$, no exceden $2g^{(g-1)^3}$ porque du_{m_d} divide a un numero perfecto, así cualquier factor primo r de su índice de aparición en u_{m_d} es a lo más tan grande como la misma cota $2g^{(g-1)^3}$. Por lo tanto, con la notación de la Sección 3.3.1, tenemos que $t \leq r \leq 2g^{(g-1)^3}$, o $t = r^2 \leq (g-1)^2$, donde el último caso es únicamente cuando $r \mid (g-1)$. Observemos que $(g-1)^2 < 2g^{(g-1)^3}$ como $g \geq 4$. Así, $m_d t < 2(g-1)^3 g^{(g-1)^3}$, y entonces cualquier factor primo de $u_{m_d t}$ es a lo más

$$g^{2(g-1)^3 g^{(g-1)^3}} < g^{g^{(g-1)^3+4}}. \tag{4.1}$$

Como $g \geq 4$, tenemos que $g^3 > (g-1)^3 + 4$, por lo tanto la expresión que aparece en el lado derecho de la desigualdad (4.1) es menor que $g^{g^{g^3}}$, lo cual completa la prueba de la parte (i) del teorema.

Ahora veamos (ii) del Teorema 1. Si N es par, entonces la Proposición 12 muestra que $m = 1$ y $N < g$, o $m = 2$ y $d = 2^a$ y $g + 1 = 2^b(2^p - 1)$ para algunos enteros no negativos a y b. Podemos ver que cuando $m = 2$, el número N es (en el mejor de los casos) unívocamente determinado. Así, el número de repdígitos perfectos pares en base g es menor que g.

Ahora asumamos que N es impar y que el primo de Euler p es chico, esto es $p < g$. Entonces el número de elecciones para la pareja (d, p) es menor que g^2. Para cada una de estas elecciones, cada m surge como $X_n = g^{\lfloor m/2 \rfloor}$, donde $X = X_n$ surge como la primer coordenada de una solución entera positiva (X, Y) de la ecuación (2.4), o de la ecuación (2.5), dependiendo de la paridad de m. Si $n \geq 7$ en el primer caso, o $n \geq 13$ en el segundo caso, entonces X_n tiene un divisor primitivo, así $X_n = g^{\lfloor m/2 \rfloor}$ puede suceder a lo más para uno de estos valores de n. Por lo tanto, el número de soluciones m cuando (p, d) es dado, es $\leq (6+1) + (13+1) = 20$. Así, tenemos en total a lo más $20g^2$ posibilidades de para dichas soluciones.

Ahora consideraremos el caso cuando N es impar, p es grande y m es par. Dado d, el numero λ_d usado en la prueba de la Proposición 14 es un divisor de c_d, así este puede tener a lo más c_d valores.

Dado λ_d, el número $m = 2m_1$ surge de la relación $X_n = g^{\lfloor m_1/2 \rfloor}$, donde $X = X_n$ es la primer coordenada de una solución entera positiva (X, Y) de una de las dos ecuaciones que surgen de (3.1). El argumento previo muestra que cada una de estas soluciones tiene a lo más 20 soluciones. Así, tenemos a lo más $2 \cdot 20c_d < 40g$ soluciones m para cada valor fijo de d, por lo tanto tenemos un total de a lo más $40g^2$ soluciones en este caso.

Ahora consideraremos el caso cuando N es impar, p es grande y $d = \square$. Entonces, por la Proposición 15 y 16, tenemos que $m = q^2$, donde q es un factor primo de $g-1$, o $m = p <$

$8g\log(4g) \le 8g\log(g^3) = 24g\log g < 24g^2$. El número $g-1$ tiene menos de g factores primos. Así, el número de soluciones en este caso es menor que $24g^2 + g$.

Ahora consideraremos el último caso cuando N es impar, p es grande y $d \neq \square$. Aquí, $g \ge 4$. Dado d, calculamos δ_d. Si $\omega(\delta_d) \ge 2$, no hay soluciones. Si δ_d es un primo, entonces tenemos dos posibilidades para n. Supongamos ahora que $\delta_d = 1$. Tenemos que $m_d = Z(c_d) < g^3$ como vimos en la prueba de la parte (i). Por lo tanto tenemos otra vez que $du_{m_d} < \sigma(du_{m_d}) < 2du_{m_d} < 2g^{m_d} < g^{g^3}$, porque du_{m_d} divide a un número perfecto. Así, el total de factores primos de $du_{m_d}\sigma(du_{m_d})$ es menor que

$$\frac{g^3\log g}{\log 2} + \frac{g^3\log g}{\log 2} < g^4.$$

Aquí, usamos la desigualdad $g^2 \le 2^g$ en la forma $(2\log g)/(\log 2) \le g$ que es válida para toda $g \ge 4$. Cada uno de los factores primos de $du_{m_d}\sigma(du_{m_d})$ determina, usando la Proposición 19, a lo más un valor para t. Para cada uno de estos valores de t, calculamos $u_{m_d t} = c_d\delta_{d,t}\square$, y si $\delta_{d,t}$ es un primo, entonces $m \in \{m_d t, m_d t\delta_{d,t}\}$; en otro caso, no hay solución para dicho t. Así, tenemos a lo más $2(g^4+1)$ posibilidades para d fijo, así obtenemos un total de a lo más $2g^5 + 2g$ posibilidades en este caso.

Resumiendo, el número de soluciones es

$$< g + 20g^2 + 40g^2 + (24g^2 + g) + (2g^5 + 2g) = 2g^5 + 84g^2 + 4g. \tag{4.2}$$

La cota de arriba es menor que $4g^5$ para toda $g \ge 4$. Cuando $g = 3$, el último término $(2g^5 + 2g)$ no aparece en la suma de (4.2), por lo tanto para este caso tenemos que la cota es $84g^2 + 2g < 4g^5$. Esto completa la prueba de (ii) y del teorema.

5. Los cálculos

El algoritmo descrito en la observación al final de la Sección 2 (caso en que el primo de Euler p es chico), observación 2 al final de la Subsección 3.1 (caso en que m es par y p es grande) y en la Subsección 3.3 (caso en que m es impar y p es grande) fueron implementados en Mathematica. No se encontraron números perfectos impares para cada dígito d y valores de g hasta $g = 333$ y la única razón por la cual no se pueden extender estos cálculos para valores más grandes de g es la capacidad de la computadora para hacer los cálculos en un tiempo razonable.

Tuvimos la necesidad de resolver ecuaciones de Pell $x^2 - Dy^2 = \pm 1$ con valores grandes de D, y esto no fue un obstáculo, para ello usamos la función de Mathematica "Reduce". Como era de esperar, algunas veces obtuvimos soluciones fundamentales muy grandes. Cuando resolvimos la ecuación generalizada de Pell $Ax^2 - By^2 = \pm 1$, algunas veces hubo la necesidad de encontrar la raíz cuadrada de un entero muy grande cuando éste era un cuadrado. Para verificar si es un cuadrado

usamos hasta 1000 residuos cuadráticos. Cuando había éxito usamos precisión de aritmética de punto flotante para dar una prueba completa y encontrar la raíz cuadrada cuando ésta existía.

En el cálculo de la función Z evitamos factorizar enteros del orden de 100 o más dígitos, lo cual es muy lento en Mathematica.

Finalmente, dados valores de d y valores muy grandes de m, en el caso cuando m es impar y p grande, necesitamos verificar si los repdígitos

$$N := d\left(\frac{g^m - 1}{g - 1}\right)$$

eran perfectos o no. Para ello usamos una estrategia similar a la utilizada en el siguiente ejemplo, y ésto funcionó en cada caso considerado.

Sea $d = 23,\ g = 54,\ m = 102735452373554407$ así

$$N = 23\left(\frac{54^m - 1}{53}\right).$$

Ahora $23 \mid 54^{m \pmod{\varphi(23)}} - 1$ y $23^2 \nmid 54^{m \pmod{\varphi(23^2)}} - 1$ donde $\varphi(n)$ es la función fi de Euler. Por lo tanto $23^2 \| N$. Pero $\sigma(23^2) = 7 \cdot 79$ y $7 \nmid 54^{m \pmod{\varphi(7)}} - 1$, así N no es perfecto.

Capítulo 3

Combinaciones lineales de factoriales y S-unidades en sucesiones recurrentes binarias

Como mencionamos en la introducción, estamos interesados en resolver la ecuación

$$u_n = Am! + Bs,$$

donde $(u_n)_{n\geq 0}$ es una sucesión recurrente binaria no degenerada sujeta a las restricciones $\Delta > 0$, $\mathrm{mcd}(r,t) = 1$ y K es un entero fijo. En particular, se tiene que $|\alpha| > |\beta|$ y $\mathbb{L} = \mathbb{Q}(\alpha)$ es el campo de los números racionales o un campo cuadrático real. Decimos que n es una *solución trivial* si $c\alpha^n = Bs$ o $d\beta^n = Bs$. Observemos que la ecuación (0.3) podría tener un número infinito de soluciones triviales, como ejemplo de esta situación observemos la sucesión

$$u_n = 6 + 2^n,$$

donde $\{u_n\}_{n\geq 0}$ esta definida por $u_0 = 7,\ u_1 = 8,\ u_{n+2} = 3u_{n+1} - 2u_n$ para toda $n \geq 0$ y $P = \{2\}$. Observemos que para cada $n \geq 1$ se tiene un solución a la ecuación (0.3) tomando $A = B = 1,\ m = 3,\ s = 2^n$. Sin embargo, estas soluciones son triviales. En cuanto a las soluciones no triviales, probaremos que sólo hay una cantidad finita de ellas y dichas soluciones son efectivamente computables. Como resultado adicional, obtenemos un resultado sobre el factor primo más grande de los enteros de la forma $u_n \pm m!$. Sea $P(m)$ el factor primo más grande del entero m con la convención que $P(0) = P(\pm 1) = 1$. Tenemos el siguiente resultado.

Teorema 2. *Sea $\{u_n\}_{n\geq 0}$ una sucesión recurrente binaria no degenerada con polinomio característico $x^2 - rx - t$, donde $\Delta = r^2 + 4t > 0$ y $\mathrm{mcd}(r,t) = 1$. Sea K un entero positivo. Entonces*

$$P(u_n \pm Am!) \geq (1 + o(1))\frac{\log n \log\log n}{\log\log\log n} \tag{0.1}$$

cuando $n \to \infty$ uniformemente, donde A y m son enteros con $m \geq 1$ y $|A| \leq K$.

Teorema 3. *Sea $P = \{p_1, \ldots, p_k\}$ un conjunto finito de primos tales que $p_1 < \cdots < p_k$ y S es el correspondiente conjunto de S-unidades. Sea K un entero positivo. Sea*

$$X = \max\{|r|, |t|, |u_0|, |u_1|, p_k, K, 11\}.$$

Entonces todas las soluciones no triviales de la ecuación (0.3) *tienen la propiedad que*

$$n < e^{12X}.$$

Tomando $K = 1$ y $P = \{2, 3, 5, 7\}$ y considerando la sucesión de Fibonacci, tenemos el siguiente resultado numérico.

Teorema 4. *La solución entera positiva más grande n tal que*

$$F_n = \pm m! \pm 2^a 3^b 5^c 7^d, \qquad a, b, c, d \in \mathbb{Z}_{\geq 0} \tag{0.2}$$

es $n = 24$ *con* $F_{24} = 8! + 2^5 3^3 7^1$.

El resto del capítulo esta organizado como sigue. En la Sección 1, demostraremos los Teoremas 2 y 3, donde usaremos algunos resultados demostrados en la Sección 4 sobre las alturas de $\alpha,\ \beta,\ c,\ d$ y sus cocientes en términos de los valores $r,\ s,\ u_0,\ u_1$. Dichos resultados podrían ser útiles para futuras investigaciones sobre propiedades aritméticas de sucesiones recurrentes binarias. El resultado numérico correspondiente al Teorema 4 es demostrado en la Sección 2.

1. Demostración de los Teoremas 2 y 3

Demostraremos los Teoremas 2 y 3 de manera simultánea. Sea $\pi(X)$ el número de primos $p \leq X$. Claramente, $k = \#P \leq \pi(X)$. Sea $M(X) = e^{\pi(X)\log\log X}$. Por el Teorema de los números primos, $\pi(X) = (1 + o(1))X/\log X$ cuando $X \to \infty$. Es fácil ver que en la notación del Teorema 3, para probar los Teoremas 2 y 3 es suficiente mostrar que cualquier solucion n satisface

$$n \leq \begin{cases} e^{12X} & \text{para toda} \quad X, \\ M(X)^{1+o(1)} & \text{cuando} \quad X \to \infty. \end{cases}$$

Tenemos que $X \geq Y$. Como

$$16(X + 2)\log(X + 2) < e^{12X} \tag{1.1}$$

(porque $X \geq 11$), podemos asumir que $n \geq 16(X + 2)\log(X + 2)$. Entonces, $u_n \neq 0$ por el Lema 7. También es claro que el miembro izquierdo de (1.1) está acotado superiormente por $M(X)^{1+o(1)}$ cuando $X \to \infty$. Distinguiremos varios casos.

Caso 1. $A = 0$. En este caso,

$$|u_n| = |B|s = |B| \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Claramente,

$$\alpha_i \leq \mu_{p_i}(u_n) \leq 2{,}7 \cdot 10^{13} \frac{p_i^2(\log p_i + 8\log(X + 2))^2}{(\log p_i)^2} \log n,$$

por el Lema 8. Siempre que $X \geq 11$ y $p_i \leq X$, tenemos que $p_i/\log p_i \leq X/\log X$, además

$$\begin{aligned}\alpha_i &\leq 2{,}7 \cdot 10^{13} \frac{X^2}{(\log X)^2} \left(\log X + 8\log(X+2)\right)^2 \log n \\ &< 2{,}7 \cdot 10^{13} \cdot 13^2 X^2 \log n \\ &< 4{,}6 \cdot 10^{15} X^2 \log n,\end{aligned}$$

donde usamos el hecho de que $X + 2 < X^{3/2}$ para $X \geq 11$. Por el Lema 9, obtenemos que

$$\begin{aligned}(n - C_0 \log n)\log|\alpha| &< \log|u_n| \leq \log|B| + \sum_{i=1}^{k} \alpha_i \log p_i \\ &< \log X + 4{,}6 \cdot 10^{15} X^2 \pi(X) \log X \log n \\ &< 6 \cdot 10^{15} X^3 \log n,\end{aligned}$$

donde usamos que $\pi(X) < 1{,}3X/\log X$ (ver Corolario 2 en [**16**]). Por lo tanto,

$$\begin{aligned}n &< 4 \cdot 10^{11} \log(X+2) \log n + \frac{6}{\log|\alpha|} \cdot 10^{15} X^3 \log n \\ &< 1{,}3 \cdot 10^{16} X^3 \log n,\end{aligned}$$

donde usamos que $|\alpha| \geq (1 + \sqrt{5})/2$. Por Lema 10, tenemos que

$$\begin{aligned}n &< 2{,}6 \cdot 10^{16} X^3 (\log(1{,}3 \cdot 10^{16}) + 3\log X) \\ &< 2{,}6 \cdot 10^{16} X^3 (\log X)\left(\frac{\log(1{,}3 \cdot 10^{16})}{\log(11)} + 3\right) \\ &< 5 \cdot 10^{17} X^3 \log X. \qquad (1.2)\end{aligned}$$

La última expresión de arriba es $< e^{12X}$ (porque $X \geq 11$) y es a lo más $M(X)^{1+o(1)}$ cuando $X \to \infty$.

Caso 2. $B = 0$. Tenemos que

$$(n - C_0 \log n)\log|\alpha| \leq \log|u_n| = \log(|A|m!) < \log X + m\log m.$$

Asumamos $n < 2C_0 \log n$. Por Lema 10, tenemos que

$$\begin{aligned}n &< 4C_0 \log 2C_0 < 16 \cdot 10^{11} \log(X+2)\left(\log(8 \cdot 10^{11}) + \log(\log(X+2))\right) \\ &< 16 \cdot 10^{11} (\log(X+2))^2 \left(\frac{\log(8 \times 10^{11}) - 1}{\log(13)} + 1\right) \\ &< 2 \cdot 10^{13} (\log(X+2))^2. \qquad (1.3)\end{aligned}$$

Arriba, usamos que $X \geq 11$ y el hecho que $1 + \log z < z$ con $z = \log(X+2)$. Ahora asumamos que $n \geq 2C_0 \log n$. Entonces $n - C_0 \log n \geq n/2$, y entonces

$$0{,}2n < (n/2)\log|\alpha| < \log X + m\log m,$$

donde usamos el hecho que $|\alpha| \geq (1+\sqrt{5})/2$. Como $n \geq 16(X+2)\log(X+2)$, se sigue que $0{,}1n > \log X$. Así,

$$0{,}1n < 0{,}2n - \log X < m \log m,$$

lo cual muestra que

$$m > \frac{0{,}1n}{\log(0{,}1n)} > \frac{n}{10\log n}.$$

Como $n \geq 16(X+2)\log(X+2)$ y $X \geq 11$, se sigue que $m \geq 8$. Así,

$$\mu_2(m!) = \left\lfloor \frac{m}{2} \right\rfloor + \left\lfloor \frac{m}{4} \right\rfloor + \cdots \geq \left\lfloor \frac{m}{2} \right\rfloor + 1 > \frac{m}{2} > \frac{n}{20\log n}, \tag{1.4}$$

recordemos que $\mu_2(m!)$ es la potencia más grande de 2 que divide a $m!$.

Por otra parte, sin duda

$$\begin{aligned} \mu_2(m!) &\leq \mu_2(u_n) < 2{,}7 \cdot 10^{13} \frac{2^2(\log 2 + 8\log(X+2))^2 \log n}{(\log 2)^2} \\ &< 2 \cdot 10^{16}(\log(X+2))^2 \log n, \end{aligned} \tag{1.5}$$

por Lema 8. Comparando (1.4) y (1.5), tenemos que

$$\frac{n}{20\log n} < 2 \cdot 10^{16}(\log(X+2))^2 \log n,$$

o

$$n < 4 \cdot 10^{17}(\log(X+2))^2(\log n)^2.$$

Por Lema 11 (con $m = 2$), tenemos que

$$\begin{aligned} n &< 1{,}6 \cdot 10^{18}(\log(X+2))^2(\log(4 \cdot 10^{17}) + 2\log(\log(X+2)))^2 \\ &< 1{,}6 \cdot 10^{18}(\log(X+2))^3 \left(\frac{\log(4 \cdot 10^{17}) - 2}{\log(13)} + 2 \right)^2 \\ &< 5 \cdot 10^{20}(\log(X+2))^3. \end{aligned} \tag{1.6}$$

Observemos que la cota superior (1.6) es más grande que la cota en (1.3) obtenida en el caso cuando $n < 2C_0 \log n$. Por lo tanto, la expresión (1.6) es una cota superior para n en el Caso 2. La expresión (1.6) es $< e^{12X}$ para toda $X \geq 11$ y es a lo más $M(X)^{1+o(1)}$ cuando $X \to \infty$.

Desde ahora, asumiremos que $AB \neq 0$.

Caso 3. $m! \leq |\alpha|^{n/2}$.

De las ecuaciones (2.2) y (0.3), tenemos que

$$c\alpha^n - Bs = Am! - d\beta^n. \tag{1.7}$$

Como $m! \leq |\alpha|^{n/2}$, tenemos que

$$|c\alpha^n - Bs| \leq K|\alpha|^{n/2} + |d||\beta|^n.$$

Dividiendo por $|c\alpha^n|$, tenemos

$$|1 - Bc^{-1}\alpha^{-n}s| < \frac{K|c|^{-1}}{\sqrt{|\alpha|}^n} + |dc^{-1}|\left|\frac{\beta}{\alpha}\right|^n.$$

Por Lema 6, tenemos que

$$\max\{|c|^{-1}, |dc^{-1}|\} \leq (X+2)^{16}.$$

Por lo tanto

$$\left|\frac{\beta}{\alpha}\right|^n \leq \frac{1}{(1+1/(|\alpha|-1))^n} \leq \frac{1}{(1+1/X)^n} < \frac{1}{e^{n/(X+1)}}.$$

Como $X \geq 11$, tenemos que

$$e^{1/(X+1)} \leq e^{1/6} < \sqrt{(1+\sqrt{5})/2} \leq \sqrt{|\alpha|}.$$

Así tenemos que

$$|1 - Bc^{-1}\alpha^{-n}s| \leq \frac{X(X+2)^{16}}{\sqrt{|\alpha|}^n} + \frac{(X+2)^{16}}{e^{n/(X+1)}} < \frac{(X+2)^{17}}{e^{n/(X+1)}}. \tag{1.8}$$

Como $s \in S$, podemos escribir $s = p_1^{\theta_1} \cdots p_k^{\theta_k}$. De (0.3) y el hecho que estamos en el Caso 3, tenemos que

$$\begin{aligned} 2^{\max_{1\leq i\leq k}\{\theta_i\}} &\leq |p_1^{\theta_1} \cdots p_k^{\theta_k}| = \left|\frac{u_n - Am!}{B}\right| \\ &\leq |c||\alpha|^n + |d||\beta|^n + K|\alpha|^{\frac{n}{2}} \\ &\leq 3X(X+2)|\alpha|^n. \end{aligned}$$

Entonces, usando que $\log|\alpha| \leq 2h(\alpha)$ y (4.3), tenemos que

$$\begin{aligned} \max_{1\leq i\leq k}\{\theta_i\} &< \frac{1}{\log 2}\left(\log((X+2)^3) + n\log|\alpha|\right) \\ &\leq \frac{3\log(X+2)}{\log 2} + \frac{2nh(\alpha)}{\log 2} \\ &\leq 5\log(X+2) + 4n\log(X+2) \\ &< 5n\log(X+2) < n^2. \end{aligned} \tag{1.9}$$

Escribimos $\Lambda = 1 - Bc^{-1}\alpha^{-n}p_1^{\theta_1} \cdots p_k^{\theta_k}$. Observemos que $\Lambda \neq 0$, porque estamos trabajando con soluciones no triviales.

Aplicamos el Teorema de Matveev con los siguientes parametros: $\eta_1 = B$, $\eta_2 = c$, $\eta_3 = \alpha$, $\eta_{3+i} = p_i$ para $i = 1, \ldots k$, los cuales son $l = k+3$ números algebraicos en $\mathbb{L} = \mathbb{Q}(\alpha)$ el cual es un

campo real de grado $d_{\mathbb{L}} \leq 2$. Por (1.9), podemos tomar $D = n^2$. Además, por (4.3) y (4.5), podemos tomar $A_1 = 2\log X$, $A_2 = 6\log(X+2)$, $A_3 = 2\log(X+2)$ y $A_{3+i} = 2\log X$ para $i = 1, \ldots, k$.

Aplicando el Teorema de Matveev, tenemos que

$$\begin{aligned}\log|\Lambda| &> -1{,}4 \cdot 30^{k+6}(k+3)^{4,5} \cdot 2^2(1+\log 2)(1+2\log n) \cdot \\ &\quad (2\log X)(6\log(X+2))(2\log(X+2))(2\log X)^k \\ &> -(1{,}4 \cdot 30^3 \cdot 2^2(1+\log 2) \cdot 9)(60\log(X+2))^{k+3}(k+3)^{4,5}\log n \\ &> -2{,}4 \cdot 10^6(60\log(X+2))^{k+3}(k+3)^{4,5}\log n,\end{aligned}$$

donde usamos el hecho que $1 + 2\log n < 3\log n$. Comparando la última desigualdad con (1.8), tenemos que

$$\frac{n}{X+1} - 17\log(X+2) < 2{,}4 \cdot 10^6(60\log(X+2))^{k+3}(k+3)^{4,5}\log n,$$

lo cual nos da

$$\begin{aligned}n &< 2{,}5 \cdot 10^6(X+1)(60\log X + 2))^{k+3}(k+3)^{4,5}\log n \\ &< 2{,}5 \cdot 10^6(X+1)^{5,5}(60\log(X+2))^{k+3}\log n,\end{aligned}$$

donde usamos el hecho que $k + 3 \leq \pi(X) + 3 < X + 1$ como $X \geq 11$. Aplicando el Lema 10, con $T = 2{,}5 \cdot 10^6(X+1)^{5,5}(60\log(X+2))^{k+3}$, tenemos que

$$n < 5 \cdot 10^6(X+1)^{5,5}(60\log(X+2))^{k+3}\log T,$$

donde

$$\log T = \Big(\log(2{,}5 \cdot 10^6) + 5{,}5\log(X+1) + (k+3)\log(60\log(X+2))\Big).$$

Como $60\log(X+2) < 60(X+1) < (X+1)^3$ para $X \geq 11$ y $\log(2{,}5 \cdot 10^6) < 15$, tenemos

$$\begin{aligned}\log T &< (15 + 5{,}5\log(X+1) + 3(k+3)\log(X+1)) \\ &< \left(3(k+3) + 5{,}5 + \frac{15}{\log(13)}\right)\log(X+1) \\ &< 9k\log(X+1),\end{aligned}$$

como $k = \pi(X) \geq 4$. Esto nos da que

$$n < 6 \cdot 10^7(X+1)^{6,5}(60\log(X+2))^{k+3}. \tag{1.10}$$

El logaritmo del lado derecho es

$$\log(6 \cdot 10^7) + 6{,}5\log(X+1) + (k+3)\log(60\log(X+2)). \tag{1.11}$$

Es claro que esta última expresión es, asintóticamente,

$$(1+o(1))k\log\log X \leq (1+o(1))\log M(X) \qquad (X \to \infty).$$

Esto muestra que

$$n < M(X)^{1+o(1)} \quad \text{cuando} \quad X \to \infty.$$

Como $k \le \pi(X) \le 1{,}25X/\log X + 1$, la expresión es a lo más

$$\log(6 \cdot 10^7) + 6{,}5 \log(X+1) + (1{,}25X/(\log X) + 4) \log(60 \log(X+2))$$

y esta última expresión es menor que $12X$ para $X \ge 11$.

Caso 4. $m! > |\alpha|^{n/2}$.

Como $m^m > m!$, tenemos que

$$m > \frac{n \log \alpha}{2 \log n} > \frac{0{,}24n}{\log n}. \tag{1.12}$$

Asumamos primero que el lado derecho de la expresión de arriba es a lo más $2X$. Entonces

$$\frac{n}{\log n} < 10X,$$

por lo tanto, por Lema 10, tenemos que $n < 20X \log(10X)$. Esta cota para n es menor que e^{12X} para $X \ge 11$ y también menor que $M(X)^{1+o(1)}$ cuando $X \to \infty$. Así, desde ahora asumiremos que

$$m > \frac{0{,}24n}{\log n} > 2X,$$

por lo tanto, en particular, la desigualdad

$$\mu_p(m!) \ge \left\lfloor \frac{m}{p} \right\rfloor \ge \frac{m}{2p} \qquad \text{para toda} \qquad p \le X.$$

Entonces

$$\mu_p(m!) > \frac{n \log \alpha}{4p \log n} > \frac{0{,}12n}{p \log n}. \tag{1.13}$$

Usando el Lema 8, tenemos que

$$\begin{aligned} \mu_p(u_n) &< 2{,}7 \cdot 10^{13} \frac{(X+2)^2}{(\log(X+2))^2} (9 \log(X+2))^2 \log n \\ &< 2{,}7 \cdot 9^2 \cdot 10^{13} (X+2)^2 \log n \\ &< 2{,}2 \cdot 10^{15} (X+2)^2 \log n, \end{aligned} \tag{1.14}$$

donde usamos el hecho que $p/\log p < (X+2)/\log(X+2)$ para todos los primos $p \le X$ y $X \ge 11$.

Asumamos que $\mu_p(m!) \le \mu_p(u_n)$ para algún $p \le p_k$. Entonces, de (1.13) y (1.14), tenemos que

$$n < \frac{2{,}2 \cdot 10^{15}}{0{,}12} (X+2)^3 (\log n)^2 < 1{,}9 \cdot 10^{16} (X+2)^3 (\log n)^2.$$

Aplicando Lema 11 (con $m = 2$), tenemos que

$$\begin{aligned} n &< 4 \cdot 1{,}9 \cdot 10^{16}(X+2)^3(\log(1{,}9 \cdot 10^{16}) + 3\log(X+2))^2 \\ &< 7{,}6 \cdot 10^{16}(X+2)^3(\log(X+2))^2 \left(\frac{\log(1{,}9 \cdot 10^{16})}{\log(13)} + 3\right)^2 \\ &< 2{,}5 \cdot 10^{19}(X+2)^3 \log(X+2)^2. \end{aligned}$$

Esta última expresión es $< e^{12X}$ para toda $X \geq 11$ y es a lo más $M(X)^{1+o(1)}$ cuando $X \to \infty$.

Ahora, asumamos que para toda $p \leq p_k$, la desigualdad $\mu_p(u_n) < \mu_p(m!)$ se mantiene. Como $u_n = Am! + Bs$ y A es un entero, tenemos que $\mu_p(Bs) = \mu_p(u_n)$ para toda $p \leq p_k$. Entonces

$$\mu_p(s) \leq \mu_p(Bs) = \mu_p(u_n) < 2{,}2 \cdot 10^{15}(X+2)^2 \log n$$

por (1.14). Como

$$\log s = \sum_{p \leq p_k} \mu_p(s) \log p,$$

tenemos que

$$\log s < 2{,}2 \cdot 10^{15}(X+2)^2 \log(X+2) \log n. \tag{1.15}$$

Ahora, distinguiremos dos posibilidades.

Caso 4.1. $|t| > 1$.

Es claro que α no es unidad en $\mathbb{L}$. En efecto, si $\mathbb{L} = \mathbb{Q}$, esto es claro ya que $|\alpha| > 1$ y las únicas unidades de $\mathbb{Q}$ son ± 1. En el caso que $\mathbb{L}$ es cuadrático y α es unidad, entonces β es su conjugado y $t = N_{\mathbb{L}}(\alpha) = \pm 1$, lo cual no es el caso que estamos considerando. Sea $\pi \in \mathcal{O}_{\mathbb{L}}$ algún ideal primo dividiendo a α. Como $\mathrm{mcd}(r, t) = 1$, se sigue que $\pi \nmid \alpha - \beta$, así que $\mu_\pi(\alpha - \beta) = 0$, por lo tanto

$$\mu_\pi(c) = \mu_\pi\left(\frac{u_1 - u_0\beta}{\alpha - \beta}\right) = \mu_\pi(u_1 - u_0\beta) \geq 0.$$

Así tenemos que

$$\mu_\pi(c\alpha^n) \geq n. \tag{1.16}$$

Necesitamos una cota superior para $\mu_\pi(d\beta^n - Bs)$. Como $\mathrm{mcd}(r, t) = 1$, tenemos que $\pi \not| \beta$, por lo tanto

$$\begin{aligned} \mu_\pi(d\beta^n - Bs) &= \mu_\pi((d\beta^n)(1 - d^{-1}\beta^{-n}Bs)) \\ &= \mu_\pi(d) + \mu_\pi(1 - d^{-1}\beta^{-n}Bs) \\ &< \frac{4\log(X+2)}{\log 2} + \mu_\pi(1 - d^{-1}\beta^{-n}Bs) \\ &< 6\log(X+2) + \mu_\pi(\Lambda), \end{aligned} \tag{1.17}$$

donde $\Lambda = 1 - d^{-1}\beta^{-n}Bs$ y usamos el análogo de (4.8) con d en lugar de c. Tenemos que $\Lambda \neq 0$ porque estamos trabajando con soluciones no triviales. Sea p el único primo tal que $\pi \mid p$. Observemos que $p \mid t$, por lo tanto $p \leq X$. Aplicamos el Teorema de Yu con los siguientes parámetros: $l = 4$, $\eta_1 = d$, $\eta_2 = \beta$, $\eta_3 = B$, $\eta_4 = s$, $d_1 = -1$, $d_2 = -n$, $d_3 = 1$, $d_4 = 1$, $d_{\mathbb{L}} \leq 2$, $f_\pi \leq 2$, $e_\pi \leq 2$, $D = n$, $H_1 = 3\log(X+2)$, $H_2 = \log(X+2)$, $H_3 = \log X$, $H_4 = \log s$. Aplicando el Teorema de Yu, obtenemos que

$$\begin{aligned}\mu_\pi(\Lambda) &< 19 \cdot (20\sqrt{5}\cdot 2)^{10} \cdot 2^3 \frac{p^2}{(\log p)^2} \log(8e^5) \cdot \\ &\quad (3\log(X+2)) \cdot \log(X+2) \cdot \log X \cdot \log s \cdot \log n \\ &= 1{,}1 \cdot 10^{23}(X+2)^2 \log(X+2) \log s \cdot \log n.\end{aligned}$$

Usando (1.15), obtenemos que

$$\mu_\pi(\Lambda) < 2{,}5 \cdot 10^{38}(X+2)^4(\log(X+2))^2(\log n)^2. \tag{1.18}$$

Entonces, usando la desigualdad (1.18) en (1.17), tenemos que

$$\begin{aligned}\mu_\pi(d\beta^n - Bs) &< 6\log(X+2) + \mu_\pi(\Lambda) \\ &< 2{,}6 \cdot 10^{38}(X+2)^4(\log(X+2))^2(\log n)^2. \end{aligned} \tag{1.19}$$

Como $Am! - c\alpha^n = d\beta^n - Bs$, tenemos que

$$\mu_\pi(d\beta^n - Bs) = \mu_\pi(Am! - c\alpha^n) = \min\{\mu_\pi(Am!), \mu_\pi(c\alpha^n)\} \geq \min\{\mu_\pi(m!), n\}.$$

De (1.19) y (1.13), tenemos que

$$\begin{aligned}\frac{0{,}12n}{p\log n} &< \min\{\mu_\pi(Am!), n\} \leq \mu_\pi(d\beta^n - Bs) \\ &< 2{,}6 \cdot 10^{38}(X+2)^4(\log(X+2))^2(\log n)^2,\end{aligned}$$

lo cual nos da

$$n < 2{,}2 \cdot 10^{39}(X+2)^5(\log(X+2))^2(\log n)^3.$$

El Lema 11 con $T = 2{,}2 \cdot 10^{39}(X+2)^5(\log(X+2))^2$ (y $m = 3$) nos da que

$$n \leq 8 \cdot 2{,}2 \cdot 10^{39}(X+2)^5(\log(X+2))^2(\log T)^3.$$

Ahora

$$\begin{aligned}\log T &= \log(2{,}2 \cdot 10^{39}) + 5\log(X+2) + 2\log\log(X+2) \\ &< \log(X+2)\left(\frac{\log(2{,}2 \cdot 10^{39})}{\log(13)} + 7\right) \\ &< 44\log(X+2),\end{aligned}$$

dando

$$n < 17{,}6 \cdot 44^3 \cdot 10^{39}(X+2)^6(\log(X+2))^4 < 1{,}5 \cdot 10^{45}(X+2)^5(\log(X+2))^5.$$

La última expresión de arriba es $< e^{12X}$ para toda $X \geq 11$ y es a lo más $M(X)^{1+o(1)}$ cuando $X \to \infty$.

Caso 4.2 *El caso* $t = \pm 1$.

En este caso, α y β son unidades conjugadas en un campo cuadrático. Entonces, $\beta = \pm\alpha^{-1}$. Escribimos (1.7) como

$$\begin{aligned} Am! &= c\alpha^n + d\beta^n - Bs \\ &= c\alpha^n + \epsilon d\alpha^{-n} - Bs \\ &= c\alpha^{-n}\left(\alpha^{2n} - \frac{Bs}{c}\alpha^n + \varepsilon\frac{d}{c}\right) \\ &= c\alpha^n(1-\alpha^{-n}z_1)(1-\alpha^{-n}z_2), \end{aligned} \tag{1.20}$$

donde $\varepsilon \in \{1,-1\}$ y

$$z_i = \frac{\operatorname{sign}(c)Bs \pm \sqrt{B^2s^2 - 4\varepsilon cd}}{2|c|} \qquad \text{para} \qquad i = 1,2. \tag{1.21}$$

Sea $i \in \{1,2\}$ fijo y sea $\Lambda = 1 - \alpha^{-n}z_i$. Observemos que $\Lambda \neq 0$. Sea $p = 2$ y π ideal primo de $O_{\mathbb{K}}$ tal que $\pi|p$. Aplicamos el Teorema de Yu con los siguientes parámetros: $l = 2$, $\eta_1 = \alpha$, $\eta_2 = z_i$, $\mathbb{L}_i = \mathbb{Q}(\alpha, z_i)$ de grado $d_{\mathbb{L}_i} \leq 4$, $f_\pi \leq 4$, $e_\pi \leq 4$, $D = n$, $H_1 = \log(X+2)$, $H_2 = \max\{h(z_i), \log 2\}$. Necesitaremos estimar $h(z_i)$. Observemos que

$$\pm|u_1 - u_0\beta|z_i = \pm Bs|\alpha - \beta| \pm \sqrt{B^2s^2(\alpha-\beta)^2 - (u_1 - u_0\beta)(u_0\alpha - u_1)}$$

y el lado derecho es un entero algebraico. Como los conjugados de z_i se obtienen al intercambiar el signo $\pm$ que se encuentra en la raíz cuadrada en (1.21) o por intercambiar simultáneamente c y d en la fórmula (1.21), tenemos que el denominador de z_i divide a

$$|u_1 - u_0\beta||u_1 - u_0\alpha| \leq (X+2)^4.$$

Para los conjugados $|z_i'|$ de z_i, tenemos que cada uno de ellos satisface

$$\begin{aligned} |z_i'| &\leq \frac{\sqrt{B^2s^2 + 4|cd|}}{|c|} \leq \frac{|Bs| + 2\sqrt{|cd|}}{|c|} \\ &\leq (1/|c|) \cdot \max\{|Bs|, 2\} \cdot \max\{2\sqrt{|cd|}, 2\}, \end{aligned}$$

así

$$\begin{aligned}\log|z_i'| &\leq \log(1/|c|) + \log \text{máx}\{|Bs|, 2\} + \log \text{máx}\{2\sqrt{|cd|}, 2\} \\ &\leq 2\log(X+2) + \log X + \log s + \log 2 + 2\log(X+2) \\ &\leq 6\log(X+2) + \log s.\end{aligned}$$

En consecuencia,

$$H_2 = h(z_i) \leq \log((X+2)^4) + 6\log(X+2) + \log s < 2{,}5 \cdot 10^{15}(X+2)^3 \log n,$$

donde también utilizamos (1.15).

Aplicando el Teorema de Yu, tenemos que

$$\begin{aligned}\mu_\pi(1-\alpha^{-n}z_i) &< 19(20\sqrt{3}\cdot 4)^6 4\frac{2^4}{(\log 2)^2}\log(8e^5)\log(X+2)H_2\log n \\ &< 3{,}2\cdot 10^{32}(X+2)^3\log(X+2)(\log n)^2 \qquad (i=1,2).\end{aligned}$$

De (1.20), tenemos que

$$\begin{aligned}\mu_2(Am!) &\leq \mu_\pi(c) + \mu_\pi(1-\alpha^{-n}z_1) + \mu_\pi(1-\alpha^{-n}z_2) \\ &\leq \frac{4\log(X+2)}{\log 2} + 6{,}4\cdot 10^{32}(X+2)^3\log(X+2)\log n \\ &< 7\cdot 10^{32}(X+2)^3\log(X+2).\end{aligned}$$

Como tenemos que

$$\frac{0{,}12n}{2\log n} < \mu_2(Am!) < 7\cdot 10^{32}(X+2)^3\log(X+2)\log n,$$

obtenemos

$$n < 1{,}2\cdot 10^{34}(X+2)^3\log(X+2)(\log n)^2.$$

El Lema 11 con $T = 1{,}2\cdot 10^{34}(X+2)^3\log(X+2)$ (y $m=2$), nos da

$$n < 4{,}8\cdot 10^{34}(X+2)^3\log(X+2)(\log T)^2.$$

Como

$$\begin{aligned}\log T &= \log(1{,}2\cdot 10^{34}) + 3\log(X+2) + \log\log(X+2) \\ &< \log(X+2)\left(\frac{\log(1{,}2\cdot 10^{34})}{\log(13)} + 4\right) \\ &< 35\log(X+2),\end{aligned}$$

tenemos que

$$n < 4{,}8 \cdot 35^2 \times 10^{34}(X+2)^3(\log(X+2))^3 < 6 \cdot 10^{37}(X+2)^3(\log(X+2))^3.$$

La última expresión es $< e^{12X}$ para toda $X \geq 11$ y es a lo más $M(X)^{1+o(1)}$ cuando $X \to \infty$. Esto finaliza la prueba de los Teoremas 2 y 3.

2. Demostración del Teorema 4

El Teorema 3 con $X = 11$ nos da inmediatamente que $n < e^{132} < 2{,}2 \cdot 10^{57} := M$, pero esta cota es demasiado grande, entonces necesitaremos reducirla. Por lo tanto, iremos a través de la demostración del Teorema 3. Sea $P = \{2, 3, 5, 7\}$. Primero asumiremos que $n > 10,000$. Cuando $A = 0$, tenemos que $F_n = s$. En particular, $P(F_n) \leq 7$. Es bien conocido, por el Teorema del divisor primitivo de Carmichael, que $P(F_n) \geq n - 1$ para toda $n \geq 13$. Esto muestra que en el caso $A = 0$, no tenemos soluciones con $n > 10,000$. Si $B = 0$, entonces tenemos que $F_n = m!$. Por el resultado de [**7**], tenemos que $n \leq 3$. Por lo tanto, no tenemos soluciones para $n > 10,000$. Desde ahora, $AB \neq 0$.

Asumamos que estamos en el caso $m! \leq \alpha^{\frac{n}{2}}$. Entonces la desigualdad (1.8) deviene

$$|1 - \sqrt{5}^{-1}\alpha^{-n}2^{\theta_1}3^{\theta_2}5^{\theta_3}7^{\theta_4}| < \frac{13^{17}}{e^{n/12}}. \tag{2.1}$$

Como $n > 1000$, el miembro derecho de arriba es $< 1/2$. Sea

$$\Gamma = n\log\alpha + \theta_1\log 2 + \theta_2\log 3 + (\theta_3 - 1/2)\log 5 + \theta_4\log 7.$$

Entonces tenemos fácilmente que

$$|2\Gamma| < \frac{4 \cdot 13^{17}}{e^{n/12}} < \frac{1}{e^{n/12-44}}. \tag{2.2}$$

Observemos que 2Γ es una forma lineal en cinco logaritmos cuyos coeficientes estan acotados por $N = 2M^2 > 2n^2$ por (1.9). Ahora, seguimos el método descrito en [**5**] sobre la aplicación del Algoritmo LLL, el cual nos da una cota inferior para $|2\Gamma|$ cuando los valores absolutos de los coeficientes son menores que N. Entonces, usamos esta cota inferior en (2.2) para obtener una cota superior para n la cual es menor a la cota que teníamos antes. Iteramos este argumento varias veces hasta obtener un valor $n < 10,000$, el cual es una contradicción.

Desde ahora, asumiremos que $\alpha^{n/2} < m!$. Esto nos da que $m > 466$. Como

$$\mu_p(m!) \geq \left\lfloor \frac{m}{p} \right\rfloor + \left\lfloor \frac{m}{p^2} \right\rfloor + \left\lfloor \frac{m}{p^3} \right\rfloor,$$

tenemos que

$$\mu_2(m!) \geq 407, \qquad \mu_3(m!) \geq 223, \quad \mu_5(m!) \geq 114, \quad \mu_7(m!) \geq 76. \tag{2.3}$$

Sea $z(k)$ el orden de aparición del entero k definido en la Sección 2. Es bien conocido que $z(p^\ell) = z(p)p^{\ell-1}$ para todos los primos $p > 2$ y toda $\ell \geq 2$. Para $p = 2$, tenemos que $z(2^\ell) = 3 \cdot 2^{\ell-2}$ para toda $\ell \geq 3$. Además, para $p = 5$ tenemos que $z(5^\ell) = 5^\ell$. Basado en estas observaciones, tenemos que

$$\mu_p(F_n) \leq 2 + \frac{\log n}{\log p} \leq 2 + \frac{\log M}{\log p} \quad \text{para toda} \quad p \in P. \tag{2.4}$$

Las cotas superiores de arriba son menores que 193, 123, 85 y 70 para $p = 2, 3, 5, 7$, respectivamente, comparando éstas con las cotas inferiores (2.3) de $\mu_p(m!)$ para estos cuatro primos p, tenemos que $\mu_p(F_n) < \mu_p(m!)$ para toda $p \in P$, por lo tanto $s \mid F_n$. En particular,

$$s \leq 2^2 \cdot 3 \cdot 7n \leq 84N.$$

Recordamos el siguiente lema de [**2**].

LEMA 21. *Sea s un entero el cual no es de la forma $\pm F_m$ para algún entero positivo $m \geq 3$. Entonces para todos los enteros positivos n, se tiene que*

$$\mu_2(F_n - s) < 1730 \log(6s^2) \max\{10, \log n\}^2. \tag{2.5}$$

En el Lemma 1 en [**2**], sólo se trabajó el caso cuando s es positivo. Una inspección de la prueba de este lema, revela que el lema se mantiene para valores negativos de s. Por lo tanto, supongamos que s no es de la forma $\pm F_m$ para algún entero positivo m. Entonces, por (2.5), tenemos que

$$\begin{aligned} m/2 &\leq \mu_2(m!) = \mu_2(F_n - s) < 1730 \log(6 \cdot 84^2 \cdot N^2) \max\{10, \log n\}^2 \\ &< 5 \cdot 10^5 \max\{10, \log n\}^2. \end{aligned}$$

Esto da

$$m < \max\{10^8, 10^6 (\log n)^2\}.$$

Además,

$$\frac{n \log \alpha}{2} = \log \alpha^{n/2} < \log m! < m \log m.$$

Si $n > 23,000$, entonces $\log n > 10$, y tenemos que

$$n < \frac{2 \cdot 10^6}{\log \alpha} (\log n)^2 \left(\log(10^6) + 2 \log \log n \right),$$

lo cual nos da $n < 10^{11}$. Supongamos ahora que $s = \pm F_\ell$ para algún $\ell \geq 1$. Por el Teorema del divisor primitivo de Carmichael, tenemos que $l \leq 12$. Por lo tanto, tenemos que

$$F_n \pm F_\ell = m!$$

para algún $m > 460$ y algún $\ell \in \{1, \ldots, 12\}$. Verificamos computacionalmente que si esto sucede para algún $\ell \geq 3$, entonces $n \equiv \ell \pmod 2$. Para hacer esto, para cada $\ell \in \{3, \ldots, 12\}$, encontramos un primo $p < 460$ tal que el período de $\{F_n\}_{n \geq 0}$ módulo p es par y tal que si $F_n \equiv \pm F_\ell \pmod p$, entonces $n \equiv \ell \pmod 2$. Ahora, recordemos que

$$F_n \pm F_\ell = F_{(n+\eta_1 \ell)/2} L_{(n+\eta_2 \ell)/2}$$

para algún signo $\eta_1,\ \eta_2 \in \{\pm 1\}$ de acuerdo a las clases de n y ℓ módulo 4. La fórmula de arriba se mantiene también cuando $\ell \in \{1, 2\}$, donde usamos el hecho de que $F_1 = F_2 = 1$ y elegimos para cada n el valor $\ell \in \{1, 2\}$ tal que $n \equiv \ell \pmod 2$. Como 8 no divide a L_ℓ para cada ℓ, tenemos que

$$230 < \frac{m}{2} \leq \mu_2(m!) \leq \mu_2(F_n \pm s) \leq 2 + 2 + \frac{\log(n + \ell)/2}{\log 2} < 4 + \frac{\log N}{\log 2} < 200,$$

lo cual es imposible. Así, $\pm s$ no es un número de Fibonacci. Por lo tanto, llegamos a la conclusión que $\pm s$ no es un número de Fibonacci y $n < 10^{11}$.

Ahora acotaremos los exponentes θ_i para $i = 1, \ldots, 4$ como antes (ver la desigualdad (2.4)), consiguiendo

$$\mu_2(s) < 39, \quad \mu_3(s) < 26, \quad \mu_5(s) < 18 \quad \text{y} \quad \mu_7(s) < 16.$$

Ahora, si p es cualquier primo menor a 460, tenemos que

$$F_n \equiv \pm 2^{\theta_1} 3^{\theta_2} 5^{\theta_3} 7^{\theta_4} \pmod p.$$

Probamos la congruencia de arriba para cada primo $p \leq 460$ y todos los posibles valores de θ_i para $i = 1, \ldots, 4$. Los cálculos confirmaron que s es un número de Fibonacci, lo cual nos da la contradicción final en el caso que $n > 10,000$.

Por tanto, $n \leq 10,000$. Para $m \leq 100$, ejecutamos un código de Mathematica el cual toma todos los pares (n, m) en el rango de arriba tal que $P(F_n \pm m!) \leq 7$. El valor más grande de n fue 24. Supongamos que $m > 100$. Entonces

$$\mu_2(m!) > 50, \quad \mu_3(m!) > 33, \quad \mu_5(m!) > 20 \quad \text{y} \quad \mu_7(m!) > 14.$$

Como

$$\mu_p(F_n) \leq 2 + \frac{\log(10^4)}{\log p} \quad \text{para toda} \quad p \in P,$$

tenemos que $\mu_p(F_n) < \mu_p(m!)$ para toda $p \in P$. Entonces generamos todos los números $s \in S$ tales que $z(s) \leq 10000$ y para cada uno de ellos checamos cuándo $F_n \pm s = m!$ para algún m. Haciendo esto no encontramos nuevas soluciones. Esto completa la demostración del Teorema 4.

Bibliografía

[1] Y. Bilu, G. Hanrot and P. M. Voutier with an appendix by M. Mignotte, 'Existence of primitive divisors of Lucas and Lehmer numbers', *J. reine angew. Math.* **539** (2001), 75–122.

[2] M. Bollman, S. Hernández Hernández and F. Luca *Fibonacci numbers which are sums of three factorials*, Publ. Math. Debrecen **77** (2010), 211–224.

[3] K. A. Broughan and Q. Zhou, 'Odd repdigits to small bases are not perfect', *INTEGERS*, to appear.

[4] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. Math. (2) **15** (1913), 30–70.

[5] H. Cohen, Number Theory Volume I: Tools and Diophantine Equations, Springer, New York, 2007.

[6] J.-H. Evertse, *On sums of S -units and linear recurrences*, Comp. Math. **53** (1984), 225–244.

[7] G. Grossman and F. Luca, *Sums of factorial in binary recurrence sequences*, Journal of Number Theory **93** (2002), 87–107.

[8] L. K. Hua, *Introduction to number theory*, Springer-Verlag, 1982.

[9] M. J. Jacobson, Jr. and H. C. Williams, *Solving the Pell equation*, Springer, 2009.

[10] W. Ljunggren, 'Some theorems on indeterminate equations of the form $\frac{x^n-1}{x-1} = y^q$', *Norsk Mat. Tidsskr.* **25** (1943), 17–20.

[11] F. Luca and M. Křížek, 'On the solutions of the congruence $n^2 \equiv 1 \pmod{\phi^2(n)}$', *Proc. Amer. Math. Soc.* **129** (2001), 2191–2196.

[12] F. Luca, Ecuaciones Diofánticas, XXI Escuela Venezolana de Matemáticas, Venezuela, 2008

[13] F. Luca and P. Pollack, 'Multiperfect numbers with identical digits', *J. Number Theory* **131** (2011), 260–284.

[14] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers II*, Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), 125–180; translation in Izv. Math. **64** (2000), 1217–1269.

[15] P. Pollack, 'Perfect numbers with identical digits', *INTEGERS* **11A** (2011), A18.

[16] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[17] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge University Press, Cambridge 1986.

[18] A.J. van der Poorten and H.P. Schlickewei, *The growth conditions for recurrence sequences*, Macquarie Univ. Math. Rep. 82-0041. North Ryde, Australia.

[19] J. Voight, 'On the nonexistence of odd perfect numbers', *MASS selecta*, 293–300, Amer. Math. Soc., Providence, RI, 2003.

[20] D. T. Walker, 'On the diophantine equation $mX^2 - nY^2 = \pm 1$', *Amer. Math. Monthly* **74** (1967), 504–513.

[21] M. Ward, 'The intrinsic divisors of Lehmer numbers', *Ann. Math. (2)* **62** (1955), 230–236.

[22] K. Yu, *p-adic logarithmic forms and group varieties II*, Acta Arith, **89** (1999), 377–378.