Sobre ciclos en el grafo coprimo de $\mathbb{Z}$

Adriana Aragón
Directora: Dra. Susana Puddu

Departamento de Matemática, FCEyN, UBA (1428)
Buenos Aires, Argentina.
E-mail address: aaragon@dm.uba.ar

RESUMEN. En esta Tesis estudiamos algunas propiedades del Grafo Coprimo de $\mathbb{Z}$. Más precisamente centramos la atención en la existencia de ciclos en dicho grafo. Para garantizar la existencia de ciclos en el Grafo Coprimo de $\mathbb{Z}$, bastará encontrar el máximo cardinal de A, subconjunto de I_n, tal que no contenga ciclos. Así encontrando el máximo subconjunto de I_n con la propiedad de no contener ciclos, garantizamos la existencia de ciclos para subconjuntos A de I_n de cardinal mayor. Estudiamos por separado le existencia de ciclos pares e impares y en cada caso la existencia de un subconjunto A de I_n con la propiedad de no contener tales ciclos. El problema central de esta tesis se desarrolla en el caso de ciclos impares, donde demostramos que si A tiene más de $[\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}]$ elementos queda garantizada la existencia de ciclos impares de casi toda longitud.

Índice general

CAPíTULO 1

Introducción

1. Paul Erdös

El resultado principal del que trata esta Tesis es original de Paul Erdös y Gabor N. Sarkozy, [**6**]

En esta sección nos referiremos a Paul Erdös.

El siguiente texto está extraído principalmente de la wikipedia, para más detalle ver `http://es.wikipedia.org/wiki/Paul_Erd%C5%91s`

Paul Erdös nació en Budapest, Hungría el 26 de marzo de 1913 en el seno de una familia judía (el nombre original de la familia era Engländer). Sus padres, Anna y Lajos Erdös, tuvieron dos hijas, de edades comprendidas entre tres y cinco años, que murieron de fiebre escarlata, apenas unos días antes de Paul nacer. Naturalmente, esto tuvo el efecto de que Lajos y Anna sean extremadamente protectores de Paul. A la edad de 3 años ya sabía sumar y para los 4 ya podía calcular cuantos segundos había vivido una persona. Al pequeño Paul le apasionaban las matemáticas tanto como a sus padres, ambos matemáticos y profesores de dicha ciencia.

Paul tenia poco más de un año de edad cuando la Primera Guerra Mundial estalló. Lajos, su padre, fue capturado por el ejército ruso, cuando atacaron a las tropas Austro-Húngaras. Pasó seis años en cautiverio en Siberia. Mientras Lajos estuvo alejado de la familia, la madre de Paul, Anna trabajaba como docente durante el día. Anna, excesivamente protectora después de la pérdida de sus dos hijas, mantuvo a Paul alejado de la escuela gran parte de sus primeros años y se le proporcionó un tutor para enseñarle en su casa.

Terminada la Primer Gran Guerra, Miklós Horthy, un nacionalista de derecha, asumió el control del país. Su madre fue separada de su puesto de directora de escuela y quedó con gran miedo por su vida y la de su hijo, ya que los hombres de Horthy deambulaban por las calles matando a los comunistas y Judíos. En 1920 Horthy había introducido contra los judíos leyes similares a las que Hitler introduciría en Alemania trece años más tarde. Ese mismo año, Lajos, su padre, regresó a casa después de su cautiverio en Siberia.

El crecimiento de un Judío era cada vez más hostil en la época de entre guerras. Erdös sabía desde temprana edad que un día tendría que salir de Hungría. A pesar de las restricciones a los judíos de entrar en las universidades de Hungría, a Erdös, como ganador de un examen nacional, se

le permitió ingresar en 1930. Estudió para su doctorado en la Universidad Pázmány Péter de Budapest.

Obtuvo su doctorado en 1934, a la edad de 21 años, y dejó Hungría para radicarse en Manchester, Inglaterra debido al recrudecimiento del fascismo en su país de origen y aumentar el odio hacia los judíos. Durante su estadía en Inglaterra, Erdös viajó mucho por el Reino Unido. Se reunió con Hardy en Cambridge en 1934 y Stanislaw Ulam, también en Cambridge, en 1935. Su amistad con Ulam fue importante para presentar a Erdös más tarde, cuando se encontraba en los Estados Unidos.

En 1938 se trasladó a los Estados Unidos, donde habría de pasar los próximos diez años. Ese mismo año aceptó su primer puesto en la Universidad de Princeton. Por esa época, comenzó a desarrollar el hábito de viajar de un campus a otro, visitando matemáticos, costumbre que conservaría hasta su muerte.

A pesar de que quería ver a su madre de nuevo, - su padre había muerto de un ataque al corazón y gran parte de su familia había sido asesinada en el Holocausto - no quería regresar a Hungría a causa de "Joe"(Joseph Stalin). En 1954, sin embargo, se le invitó a una conferencia de matemáticas en Amsterdam. Como extranjero tendría que solicitar un visado de regreso a los Estados Unidos, por lo general una cuestión de rutina. Pero su extensa correspondencia con matemáticos fuera de los Estados Unidos y, en especial, con un matemático de la China comunista, planteó la sospecha de los funcionarios de inmigración durante la época del Macarthismo. Fue miembro del departamento de matemáticas de la Universidad de Notre Dame.

"Los funcionarios de inmigración me realizaron todo tipo de preguntas tontas", recordó Erdös. Le preguntaron acerca de Marx. Él sólo había leído el Manifiesto Comunista y respondió: "Yo no soy competente para juzgar, pero sin duda fue un gran hombre". Como consecuencia su visado se le negó. Obligado a elegir entre la seguridad de sus miembros la Universidad de Notre Dame y la libertad de viajar, no dudó. Asistió a la conferencia y pasó la mayor parte de la siguiente década en el Estado de Israel. Su solicitud de una visa de visitante para asistir a conferencias en los Estados Unidos fueron rechazadas reiteradamente. En 1958 el Departamento de Estado le otorgó un "visado especial"para asistir a una conferencia en Colorado. Durante su estancia un funcionario de inmigración le acompaño a todos lados. En 1962 escribió a sus amigos que, al parecer "la política exterior de EE.UU. insiste en dos puntos: la no admisión de China Roja a la ONU y la no admisión de Paul Erdös a los EE.UU."

Las posesiones materiales no tuvieron importancia para Erdös; premios y otras ganancias eran normalmente donadas para personas necesitadas o como premios para problemas que él mismo proponía. Pasó la mayor parte de su vida como un vagabundo, viajando entre conferencias científicas y casas de colegas matemáticos alrededor del mundo. Típicamente llegaba a la puerta de la casa donde era invitado y decía: mi cerebro esta abierto, permaneciendo

lo suficiente para elaborar algún(os) artículo(s) antes de volver a viajar. En varias ocasiones, preguntaba a su anfitrión a quién debería hacer su siguiente visita.

Él también tenía su propio vocabulario: hablaba de El Libro, un libro imaginario en el cual Dios tenía escritos las pruebas más hermosas de los teoremas matemáticos. En una conferencia de 1985 comentó: No tienes que creer en Dios, pero deberías creer en El Libro. Él mismo dudaba de la existencia de Dios, que llamaba El "Supremo Fascista"(SF) al que acusaba de guardar las pruebas más elegantes sin compartir. Cuando encontraba alguna prueba matemática particularmente hermosa, exclamaba ¡Ésta es una para El Libro!.

Durante varios años persiguió la idea de escribir tal Libro con esas demostraciones que a él le habían gustado más. De hecho, estaba previsto que ese libro se publicara en marzo de 1998, año en el que Erdös cumpliría ochenta y cinco años, pero su inesperada muerte en el verano de 1996 truncó su magnífico proyecto.

Las demostraciones bonitas , a las que se refería Erdös, eran aquellas pruebas que cumplían tres características: que fueran elegantes, fáciles de entender y notoriamente difíciles de resolver.

Los autores de: "El libro de las Demostraciones", son los profesores alemanes Martin Aigner y Günter M.Ziegler pertenecientes a las Universidades de Freie Universität Berlin y Technische Universität Berlin, respectivamente y, especialistas en matemática discreta. Ellos han tenido la osadía de recoger el reto de Erdös y desarrollarlo; además, han incluido muchos de los resultados que el mismo Erdös habría propuesto.

Murió "en acción" de un ataque al corazón el 20 de septiembre de 1996, a la edad de 83, mientras asistía a una conferencia en Varsovia, Polonia. Nunca se casó ni dejó descendencia.

Erdös fue uno de los matemáticos más prolíficos de todos los tiempos. Escribió aproximadamente 1,500 artículos en el transcurso de su vida, colaborando con alrededor de 500 co-autores. Él creía firmemente en las matemáticas como una actividad social.

Paul Erdös solía decir: "¿Por qué son bonitos los números? Es como preguntar por qué la Novena Sinfonía de Beethoven es bonita. Si no ves por qué, nadie podrá decírtelo. Yo sé que los números son bonitos. Si no son bonitos, nada lo es."

Debido a sus numerosos aportes, colaboradores y amigos inventaron el número de Erdös como un homenaje con tintes de humor matemático: Erdös tiene asignado el número 0, todas aquellos que colaboraron en algún artículo con él tienen el 1, alguien que haya colaborado con alguno de sus colaboradores tiene el 2, y así sucesivamente.... Sencillas estimaciones comprueban que el 90 % de los matemáticos activos tienen un número de Erdös menor

que 8 (parece sorprendente si uno no conoce la teoría de Seis grados de separación).

2. Introducción y definiciones

Consideremos el anillo de los números enteros $\mathbb{Z}$. En él, definimos el siguiente grafo: tomamos como vértices a los mismos elementos de $\mathbb{Z}$ y diremos que dos vértices $a, b \in \mathbb{Z}$ están conectados por una rama si y sólo si $(a, b) = 1$ donde (a, b) denota el máximo común divisor entre a y b. A tal grafo se lo llama el *grafo coprimo de* $\mathbb{Z}$ y lo notaremos por $\mathcal{G}$.

Llamaremos $I_n = \{1, \ldots, n\}$. Si $A \subset I_n$, el grafo coprimo de A es el grafo inducido por el grafo coprimo de $\mathbb{Z}$ en A y lo notaremos por $\mathcal{G}(A)$.

Es el propósito de esta Tesis estudiar algunas propiedades del grafo $\mathcal{G}$.

Recientemente ha recibido mucha atención el estudio de varios grafos de enteros (ver [**8**]). El grafo más popular parece ser el grafo coprimo, pero hay muchos problemas atractivos y resultados sobre el grado de los divisores (ver, por ejemplo, [**4, 5, 10, 11**]).

Se han estudiado varios subgrafos del grafo coprimo. Tal vez el primer problema de este tipo fue formulado en 1962 por P. Erdös, [**3**]: Dado $k \in \mathbb{Z}$, ¿Cuál es el conjunto A de mayor cardinal contenido en I_n tal que no contenga ningún subgrafo completo de k vértices. Se puede encontrar una definición de subgrafos completos en el capítulo 3, Definición 3.5

Llamando p_i al $i-$ésimo primo positivo, si definimos el siguiente conjunto

$$A_k := \{m \in I_n \ : \ p_i | m \text{ para algún } i \leq k-1\}$$

demostraremos en el Capítulo 4, sección 2, que A_k tiene la propiedad de que no contiene ningún subgrafo completo de k vértices.

Ahora surge naturalmente la siguiente pregunta: ¿Es A_k el mayor conjunto contenido en I_n con esta propiedad?

La respuesta es que no, en general. Ver [**1**]. Sin embargo, se puede ver fácilmente que para $k = 2$ y $k = 3$ la respuesta es afirmativa. Este hecho se demuestra en esta Tesis en la seccion 2 del capítulo 4 y recientemente, esta misma propiedad fue demostrada para $k = 4$ (ver [**12**]).

Otra cuestión de interés son los ciclos en $\mathcal{G}(A)$. Para una definición precisa de ciclos en un grafo, ver la Definición 3.3.

El caso de los ciclos de longitud par (C_{2l}) no es difícil de resolver, al menos para ciclos no demasiado largos. Este problema está estudiado en el Capítulo 5.

Una pregunta interesante sería: Cúal es el subconjunto $A \subseteq I_n$ de cardinal más grande tal que no contenga ciclos pares?

Probaremos, en el Capítulo 5, que si l no es demasiado grande, el conjunto A de mayor cardinal contenido en I_n tal que no contenga ciclos pares tiene $[\frac{n}{2}] + l - 1$ cantidad de elementos.

Más precisamente el máximo $A \subseteq I_n$ tal que $C_{2l} \not\subset \mathcal{G}(A)$ debe ser de cardinal $[\frac{n}{2}] + l - 1$.

Este cardinal se alcanza tomando todos los números pares y los primeros l primos.

Sobre los ciclos impares nos interesa responder la misma pregunta: ¿Cuál es el conjunto $A \subset I_n$ más grande tal que no contenga ciclos impares?

En el caso de ciclos de longitud 3 (triángulos), los ciclos son además subgrafos completos y veremos en el Capítulo 4, Sección 2, que el mayor $A \subset I_n$ tal que $C_3 \not\subset \mathcal{G}(A)$ es $A_3 = \{m \in I_n \ : \ 2|m \text{ o } 3|m\}$ que tiene cardinal $\sharp A_3 = [\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}]$.

Es decir que para garantizar la existencia de un triángulo en $A \subset I_n$ se necesita $\sharp A \geq [\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + 1$.

Sorprendentemente este cardinal garantiza la existencia de ciclos impares de *casi toda* longitud. Este es el resultado principal de esta Tesis y dedicaremos los capítulos 6, 7 y 8 a su prueba. Este resultado es original de Paul Erdös y Gabor N. Sarkozy [**6**].

3. Organización de la Tesis

Esta Tesis está organizada de la siguiente manera.

Luego de esta introducción, en el Capítulo 2 repasaremos la noción de Funciones Aritméticas y algunas de sus propiedades elementales. Así mismo definiremos algunas de las funciones aritméticas más usuales que nos serán de utilidad en el trabajo.

En el Capítulo 3 daremos algunas definiciones básicas de los grafos y algunas de sus propiedades.

En el Capítulo 4 daremos la definición formal del grafo coprimo de $\mathbb{Z}$, estudiaremos algunas de sus propiedades y hallaremos un conjunto de cardinal máximo con la propiedad de no contener un subgrafo completo de 2 y 3 elementos.

En el Capítulo 5, encontraremos un conjunto de cardinal máximo con la propiedad de no contener ciclos pares de longitud $2l$ para l chico.

Finalmente, en los capítulos restantes, estudiaremos el problema central de la Tesis. Dar un conjunto de cardinal máximo con la propiedad de no contener ciclos impares.

CAPíTULO 2

Funciones Aritméticas

1. Generalidades

Al estudiar las propiedades aritméticas de los números enteros, aparecen naturalmente ciertas funciones definidas sobre el conjunto de los números naturales a valores en un anillo conmutativo, a las que llamaremos, funciones aritméticas. En otras palabras, si A es un anillo conmutativo, una función aritmética a valores en A es una función de $\mathbb{N}$ en A.

Ejemplos:

1. La función aritmética τ, a valores en $\mathbb{Z}$, definida por $\tau(n) = \sharp\{\, d \in \mathbb{N} \,/\, d \mid n \,\}$, es decir, $\tau(n)$ es la cantidad de divisores positivos de n
2. La función aritmética σ, a valores en $\mathbb{Z}$, definida por
$$\sigma(n) = \sum_{d \in \{m \in \mathbb{N} / m \mid n\}} d,$$
es decir, $\sigma(n)$ es la suma de los divisores positivos de n
3. La función aritmética ϕ, a valores en $\mathbb{Z}$, definida por
$$\phi(n) = \sharp\{\, m \in \mathbb{N} \,/\, m \leq n \text{ y } mcd(m,n) = 1 \,\}$$
es decir, $\phi(n)$ es la cantidad de números naturales menores o iguales que n que son coprimos con n (función de Euler)
4. La función aritmética ϵ, a valores en cualquier anillo conmutativo A, definida por $\epsilon(n) = 1$ para todo $n \in \mathbb{N}$
5. La función aritmética ι, a valores en $\mathbb{Z}$, definida por $\iota(n) = n$
6. La función aritmética π, a valores en $\mathbb{Z}$, definida por
$$\pi(n) = \sharp\{p \in \mathbb{N} \,/\, p \text{ es primo y } p \leq n\}$$
es decir, $\pi(n)$ es la cantidad de números primos menores o iguales que n

Notación: Si $n \in \mathbb{N}$ y α es una función aritmética a valores en A, el símbolo $\sum_{d|n} \alpha(d)$ denota $\sum_{d \in \{m \in \mathbb{N} / m|n\}} \alpha(d)$

Por ejemplo, $\sum_{d|12} \pi(d) = \pi(1) + \pi(2) + \pi(3) + \pi(4) + \pi(6) + \pi(12) = 0 + 1 + 2 + 2 + 3 + 5 = 13$

Con esta notación se tiene que $\tau(n) = \sum_{d|n} 1$ y $\sigma(n) = \sum_{d|n} d$

Observemos que $\sum_{d|n} \alpha(d) = \sum_{d|n} \alpha(\frac{n}{d})$

DEFINICIÓN 2.1. *Diremos que una función aritmética α, a valores en un anillo conmutativo A, es multiplicativa si $\forall\, n, m \in \mathbb{N}$ tales que $(n, m) = 1$ se verifica que $\alpha(n.m) = \alpha(n).\alpha(m)$*

LEMA 2.1. *Sean $n, m \in \mathbb{N}$ tales que $(n, m) = 1$. Si $\{n_1, \ldots, n_r\}$ es el conjunto de los divisores positivos de n y $\{m_1, \ldots, m_s\}$ es el conjunto de los divisores positivos de m, entonces $\{\, n_i.m_j \,/\, 1 \leq i \leq r, \quad 1 \leq j \leq s \,\}$ es el conjunto de los divisores positivos de $n.m$. Además, si $n_i.m_j = n_k.m_t \quad (1 \leq i, k \leq r \ , \ 1 \leq j, t \leq s)$ entonces $i = k$ y $j = t$.*

DEMOSTRACIÓN. Es claro que $\forall\, 1 \leq i \leq r, \quad 1 \leq j \leq s$, $n_i.m_j \mid n.m$ pues $n_i \mid n$ y $m_j \mid m$. Recíprocamente, si d es un divisor positivo de $n.m$, como $(d, n) \mid n$ y $(d, m) \mid m$, entonces $\exists i, j \,/\, 1 \leq i \leq r\,,\ 1 \leq j \leq s$ tales que $(d, n) = n_i$ y $(d, m) = m_j$.

Luego, $n_i \mid d$ y $m_j \mid d$ y por lo tanto $n_i.m_j \mid d$ pues $(n_i, m_j) = 1$ ya que n y m son coprimos.

Por otra parte, sean $a, b, k, t \in \mathbb{Z}$ tales que $n_i = d.a + n.b$ y $m_j = d.k + m.t$. Entonces $n_i.m_j = (d.a + n.b)(d.k + m.t) = d(a.d.k + a.m.t + n.b.k) + n.m.b.t$ y, como $d \mid n.m$, resulta que $d \mid n_i.m_j$ y por lo tanto $d = n_i.m_j$.

Si $n_i.m_j = n_k.m_t \quad (1 \leq i, k \leq r \ , \ 1 \leq j, t \leq s)$ entonces $n_i \mid n_k.m_t$ y como $(n_i, m_t) = 1$ entonces $n_i \mid n_k$. Análogamente resulta que $n_k \mid n_i$, por lo tanto $n_i = n_k$ y en consecuencia $m_j = m_t$. Luego $i = k$ y $j = t$. □

PROPOSICIÓN 2.1. *Las funciones aritméticas τ, σ y ϕ definidas anteriormente son multiplicativas.*

DEMOSTRACIÓN. Dados $n, m \in \mathbb{N}$ tales que $(n, m) = 1$, sean $\{n_1, \ldots, n_r\}$ el conjunto de los divisores positivos de n y $\{m_1, \ldots, m_s\}$ el conjunto de los divisores positivos de m. Entonces, aplicando el Lema 2.1, se tiene que

$$\tau(n.m) = r.s = \tau(n).(m)$$

y

$$\sigma(n.m) = \sum_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} n_i.m_j = \left(\sum_{1 \leq i \leq r} n_i \right) \left(\sum_{1 \leq j \leq s} m_j \right) = \sigma(n).\sigma(m)$$

Veamos ahora que $\phi(n.m) = \phi(n).\phi(m)$.

Es claro que esto es cierto cuando $n = 1$ o $m = 1$ ya que $\phi(1) = 1$. Supongamos entonces que $n > 1$ y que $m > 1$.

Sean

$$C_n = \{k \in \mathbb{N} \,/\, k \leq n \text{ y } (k,n) = 1\}$$
$$C_m = \{k \in \mathbb{N} \,/\, k \leq m \text{ y } (k,m) = 1\}$$
$$C_{nm} = \{k \in \mathbb{N} \,/\, k \leq n.m \text{ y } (k,n.m) = 1\}$$

Sea $\psi : C_{nm} \longrightarrow C_n \times C_m$ la aplicación definida por $\psi(k) = (r_n(k), r_m(k))$, donde $r_n(k)$ y $r_m(k)$ son los restos de la división de k por n y m respectivamente.

Como $\phi(n.m) = \sharp C_{nm}$ y $\phi(n).\phi(m) = \sharp(C_n \times C_m)$, basta ver que ψ está bien definida y que es biyectiva.

Observemos que si $(k, n.m) = 1$ entonces $(k,n) = 1$ y $(k,m) = 1$. Por lo tanto, siendo $n > 1$ y $m > 1$, $\forall\, k \in C_{nm}$ es $r_n(k) \neq 0$ y $r_m(k) \neq 0$, $(r_n(k), n) = (k,n) = 1$ y $(r_m(k), m) = (k,m) = 1$. Esto muestra que ψ está bien definida.

Si $k_1, k_2 \in C_{nm}$ son tales que $\psi(k_1) = \psi(k_2)$ entonces $r_n(k_1) = r_n(k_2)$ y $r_m(k_1) = r_m(k_2)$, de donde $n \mid k_1 - k_2$ y $m \mid k_1 - k_2$. Siendo n y m coprimos, resulta que $n.m \mid k_1 - k_2$. Pero $-n.m \leq -k_2 < k_1 - k_2 < k_1 \leq n.m$. Por lo tanto, debe ser $k_1 - k_2 = 0$ con lo que $k_1 = k_2$. Luego, ψ es inyectiva.

Por otra parte, dado $(a,b) \in C_n \times C_m$, sea $k \in \mathbb{Z}$, $0 \leq k < n.m$ tal que $k \equiv a\ (n)$ y $k \equiv b\ (m)$ (la existencia de un tal k está garantizada por el Teorema Chino del Resto). Como $(a,n) = 1$ y $n > 1$ entonces $n \not| \ a$, de donde resulta que $k \neq 0$.

Como $k \equiv a\ (n)$ y $(a,n) = 1$ entonces $(k,n) = 1$. Análogamente, $(k,m) = 1$. Luego, $(k, n.m) = 1$.

Por último, como $0 < a < n$ (pues $a \in C_n$ y $n > 1$) y $k \equiv a\ (n)$ entonces $a = r_n(k)$. Del mismo modo, $b = r_m(k)$.

Luego, $k \in C_{nm}$ y $\psi(k) = (a,b)$, lo que prueba que ψ es suryectiva. □

Proposición 2.2. *Sea ϕ la función de Euler. Entonces*

$$\phi(n) = \begin{cases} 1 & \text{si } n = 1 \\ \displaystyle\prod_{i=1}^{r} (p_i - 1).p_i^{\alpha_i - 1} & \text{si } n = \displaystyle\prod_{i=1}^{r} p_i^{\alpha_i},\ \text{con } \alpha_i \in \mathbb{N} \\ & \text{y } p_1, \ldots, p_r \text{ primos distintos} \end{cases}$$

Demostración. Como ϕ es multiplicativa, basta calcular $\phi(p^r)$ para todo primo p y $r \in \mathbb{N}_0$.

Si $r = 0$ entonces $\phi(p^r) = \phi(1) = \sharp\{m \in \mathbb{N} \,/\, m \leq 1 \text{ y } (m,1) = 1\} = 1$ y si $r \geq 1$ entonces

$$\begin{aligned} \phi(p^r) &= \sharp\{m \in \mathbb{N} \,/\, m \leq p^r \text{ y } (m, p^r) = 1\} \\ &= \sharp\{1,\ 2,\ 3, \ldots,\ p^r\} - \sharp\{p,\ 2p,\ 3p, \ldots,\ p^{r-1}.p\} \\ &= p^r - p^{r-1} = (p-1).p^{r-1}, \end{aligned}$$

como queríamos demostrar. □

2. Convolución de funciones aritméticas

Sea A un anillo conmutativo.

DEFINICIÓN 2.2. *Si α y γ son funciones aritméticas a valores en A, definimos la función aritmética (a valores en A) $\alpha * \gamma$ en la forma:*

$$(\alpha * \gamma)(n) = \sum_{d|n} \alpha(\frac{n}{d}).\gamma(d)$$

Ejemplo: Sean ι y ε las funciones aritméticas a valores en $\mathbb{Z}$ definidas por

$$\iota(n) = n$$
$$\varepsilon(n) = 1$$

Entonces se tiene que $\tau = \varepsilon * \varepsilon$ y $\sigma = \varepsilon * \iota$

Resulta que la operación $*$, llamada convolución, es asociativa y conmutativa. Veamos que tiene elemento neutro.

En efecto, sea χ la función aritmética a valores en A definida por

$$\chi(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$$

Entonces $(\chi * \alpha)(n) = \sum_{d|n} \chi(\frac{n}{d})\alpha(d) = \alpha(n)$

PROPOSICIÓN 2.3. *Sean α y β dos funciones aritméticas a valores en A. Si α y β son multiplicativas entonces $\alpha * \beta$ es multiplicativa.*

DEMOSTRACIÓN. Sean $n, m \in \mathbb{N}$ tales que $(n, m) = 1$. Sea $\{n_1, \ldots, n_r\}$ el conjunto de los divisores positivos de n y sea $\{m_1, \ldots, m_s\}$ el conjunto de los divisores positivos de m. Entonces, $(n_i, m_j) = 1 = (\frac{n}{n_i}, \frac{m}{m_j}) \quad \forall\, 1 \leq i \leq r,\ 1 \leq j \leq s$ pues $(n, m) = 1$.

Luego, utilizando el Lema 2.1, resulta que

$$\begin{aligned}(\alpha * \beta)(n.m) &= \sum_{d|n.m} \alpha(\frac{n.m}{d}).\beta(d) = \sum_{\substack{1\leq i\leq r\\ 1\leq j\leq s}} \alpha(\frac{n.m}{n_i.m_j}).\beta(n_i.m_j)\\ &= \sum_{\substack{1\leq i\leq r\\ 1\leq j\leq s}} \alpha(\frac{n}{n_i}).\alpha(\frac{m}{m_j}).\beta(n_i).\beta(m_j)\\ &= \left(\sum_{1\leq i\leq r} \alpha(\frac{n}{n_i}).\beta(n_i)\right)\left(\sum_{1\leq j\leq s} \alpha(\frac{m}{m_j}).\beta(m_j)\right)\\ &= \left(\sum_{d|n} \alpha(\frac{n}{d}).\beta(d)\right)\left(\sum_{d|m} \alpha(\frac{m}{d}).\beta(d)\right)\\ &= (\alpha * \beta)(n).(\alpha * \beta)(m)\end{aligned}$$

como queríamos demostrar. □

PROPOSICIÓN 2.4. *Para todo $n \in \mathbb{N}$, ϕ la función de Euler, verifica:* $\sum_{d|n} \phi(d) = n$

DEMOSTRACIÓN. Como $\sum_{d|n} \phi(d) = (\varepsilon * \phi)(n)$ entonces $\sum_{d|n} \phi(d) = n$ para todo $n \in \mathbb{N}$ si y sólo si $\varepsilon * \phi = \iota$

Siendo ϕ y ε multiplicativas entonces, por la Proposición 2.3, $\varepsilon * \phi$ es multiplicativa, y como ι es multiplicativa entonces $\varepsilon * \phi = \iota$ si y sólo si $(\varepsilon * \phi)(p^r) = \iota(p^r)$ para todo primo p y $r \in \mathbb{N}_0$.

Pero

$$\begin{aligned}(\varepsilon * \phi)(p^r) &= \sum_{d|p^r} \phi(d) = \sum_{j=0}^{r} \phi(p^j) = 1 + \sum_{j=1}^{r} p^{j-1}(p-1)\\ &= 1 + (p-1).\sum_{j=1}^{r} p^{j-1} = 1 + (p-1).\sum_{i=0}^{r-1} p^i = 1 + (p-1).\frac{p^r - 1}{p-1}\\ &= 1 + p^r - 1 = p^r = \iota(p^r)\end{aligned}$$

Por lo tanto, $\varepsilon * \phi = \iota$. □

COROLARIO 2.1. *Si $n \in \mathbb{N}$ entonces, para todo $d \in \mathbb{N}$ tal que $d \mid n$, en $\mathbb{Z}_n$ hay exactamente $\phi(d)$ elementos de orden d.*

DEMOSTRACIÓN. Para cada $d \in \mathbb{N}$ tal que $d \mid n$ sea $A_d = \{a \in \mathbb{Z}_n \,/\, ord(a) = d\}$

Afirmación: $\sharp A_d \geq \phi(d)$. En efecto, si $d \in \mathbb{N}$ tal que $d \mid n$ entonces, $\forall\, i \in \mathbb{N} \,/\, 1 \leq i \leq d$ y $(d, i) = 1$, se tiene que $ord(\frac{n.i}{d}) = d$.

Luego $\{\frac{n.i}{d} / i \in \mathbb{N},\ i \leq d \text{ y } (d,i) = 1\}$, que tiene $\phi(d)$ elementos, está contenido en A_d. Por lo tanto, $\sharp A_d \geq \phi(d)$

Como $\mathbb{Z}_n = \bigcup_{d|n} A_d$ y esta unión es disjunta, entonces $n = \sum_{d|n} \sharp A_d$.

Si para algún $d \in \mathbb{N}$ tal que $d \mid n$ fuera $\sharp A_d > \phi(d)$ entonces $n = \sum_{d|n} \sharp A_d > \sum_{d|n} \phi(d)$. Pero $\sum_{d|n} \phi(d) = n$ por la Proposición 2.4. Luego debe ser $\sharp A_d = \phi(d)\ \forall d \in \mathbb{N}$ tal que $d \mid n$. □

PROPOSICIÓN 2.5. *Sea α una función aritmética a valores en A. Entonces α es inversible respecto de la operación $*$ (i.e., existe una función aritmética γ a valores en A tal que $\alpha * \gamma = \chi$) si y sólo si $\alpha(1)$ es una unidad del anillo A.*

DEMOSTRACIÓN. Si existe una función aritmética γ a valores en A tal que $\alpha * \gamma = \chi$ entonces $(\alpha * \gamma)(1) = \chi(1)$, de donde resulta que $\sum_{d|1} \alpha(\frac{1}{d}).\gamma(d) = \chi(1)$. Luego, $\alpha(1).\gamma(1) = 1$ y, por lo tanto, $\alpha(1)$ es una unidad de A.

Recíprocamente, si $\alpha(1)$ es una unidad de A, sea $a \in A$ el inverso de $\alpha(1)$. Definimos $\gamma : \mathbb{N} \longrightarrow A$ inductivamente en la forma:

$$\gamma(1) = a$$
$$\gamma(n) = (-a).\sum_{\substack{d|n \\ d \neq n}} \alpha(\frac{n}{d}).\gamma(d) \qquad \text{si } n > 1$$

Esta γ verifica que $\alpha * \gamma = \chi$. □

OBSERVACIÓN 2.1. *Si una función aritmética α es inversible, entonces tiene una única inversa que será notada α^{-1}.*

PROPOSICIÓN 2.6. *Sea α una función aritmética a valores en A. Si α es inversible y multiplicativa entonces α^{-1} es multiplicativa*

DEMOSTRACIÓN. Como α es inversible entonces $\alpha(1)$ es una unidad de A y como α es multiplicativa, entonces $\alpha(1) = \alpha(1{,}1) = \alpha(1).\alpha(1)$. Por lo tanto debe ser $\alpha(1) = 1$.

Luego, por la Proposición 2.5, α^{-1} es la función definida inductivamente por

$$\alpha^{-1}(1) = 1$$
$$\alpha^{-1}(n) = -\sum_{\substack{d|n \\ d \neq n}} \alpha(\frac{n}{d}).\alpha^{-1}(d) \qquad \text{si } n > 1$$

Veamos ahora que α^{-1} es multiplicativa. Supongamos que existen $a, b \in \mathbb{N}$ tales que $mcd(a,b) = 1$ y $\alpha^{-1}(a.b) \neq \alpha^{-1}(a).\alpha^{-1}(b)$. Entonces el conjunto

$$S = \{n \in \mathbb{N} / \exists m \in \mathbb{N} :\ m < n, (n,m) = 1 \text{ y } \alpha^{-1}(n.m) \neq \alpha^{-1}(n).\alpha^{-1}(m)\}$$

es no vacío.

En efecto, como $(a,b) = 1$ y $\alpha^{-1}(a.b) \neq \alpha^{-1}(a).\alpha^{-1}(b)$ entonces $a \neq b$ pues $\alpha^{-1}(1) = 1$. Luego, $a < b$, y en tal caso $b \in S$ o $b < a$, y por lo tanto $a \in S$.

Sea $n = min\, S$ y sea m el menor número natural tal que $m < n$, $(n,m) = 1$ y $\alpha^{-1}(n.m) \neq \alpha^{-1}(n).\alpha^{-1}(m)$.

Entonces $n > 1$ y $m > 1$, pues si $n = 1$ o $m = 1$, $\alpha^{-1}(n.m) = \alpha^{-1}(n).\alpha^{-1}(m)$ ya que $\alpha^{-1}(1) = 1$. Además, $\forall k,t \in \mathbb{N}$ tales que $k \mid n$, $t \mid m$ y $k < n$ o $t < m$ se tiene que $\alpha(\frac{n}{k}.\frac{m}{t}) = \alpha(\frac{n}{k}).\alpha(\frac{m}{t})$ y $\alpha^{-1}(k.t) = \alpha^{-1}(k).\alpha^{-1}(t)$.

En efecto, como $(n,m) = 1$, si $k \mid n$ y $t \mid n$ entonces $(\frac{n}{k}, \frac{m}{t}) = 1$ y $(k,t) = 1$. Luego, $\alpha(\frac{n}{k}.\frac{m}{t}) = \alpha(\frac{n}{k}).\alpha(\frac{m}{t})$, pues α es multiplicativa.

Para ver que $\alpha^{-1}(k.t) = \alpha^{-1}(k).\alpha^{-1}(t)$, analizaremos las tres posibilidades: $k = t$, $k < t$ y $t < k$

Primer caso: $k = t$

Como $(k,t) = 1$ entonces debe ser $k = t = 1$. Luego $\alpha^{-1}(k.t) = \alpha^{-1}(k).\alpha^{-1}(t)$ ya que $\alpha^{-1}(1) = 1$

Segundo caso: $k < t$

Como $t \leq m$ pues $t \mid m$ y como $m < n$ entonces $t < n$. Luego $t \notin S$. Siendo $k < t$ y $(k,t) = 1$ entonces $\alpha^{-1}(k.t) = \alpha^{-1}(k).\alpha^{-1}(t)$

Tercer caso: $t < k$

Si $k < n$ entonces $k \notin S$. Siendo $t < k$ y $(k,t) = 1$ entonces $\alpha^{-1}(k.t) = \alpha^{-1}(k).\alpha^{-1}(t)$

Si $k \geq n$, como $k \mid n$ y como $k < n$ o $t < m$ entonces debe ser $k = n$ y $t < m$.

Como m es el menor natural tal que $m < n$, $(n,m) = 1$ y $\alpha^{-1}(n.m) \neq \alpha^{-1}(n).\alpha^{-1}(m)$ y como $t < m$ y satisface $t < n$ (pues $t < k$ y $k = n$) y $mcd(n,t) = mcd(k,t) = 1$ entonces $\alpha^{-1}(n.t) = \alpha^{-1}(n).\alpha^{-1}(t)$. Luego, teniendo en cuenta que $k = n$, resulta que $\alpha^{-1}(k.t) = \alpha^{-1}(k).\alpha^{-1}(t)$

Por último observemos que, por el Lema 2.1, $\sum_{d|n.m} \alpha(\frac{n.m}{d}).\alpha^{-1}(d) = \sum_{\substack{k|n \\ t|n}} \alpha(\frac{n.m}{k.t}).\alpha^{-1}(k.t)$ Luego, como $n.m > 1$,

$$\begin{aligned}
\alpha^{-1}(n.m) &= -\sum_{\substack{d|n.m \\ d\neq n.m}} \alpha(\frac{n.m}{d}).\alpha^{-1}(d) \\
&= -\sum_{\substack{k|n;t|m \\ k<n\vee t<m}} \alpha(\frac{n.m}{k.t}).\alpha^{-1}(k.t) \\
&= -\sum_{\substack{k|n;t|m \\ k<n\vee t<m}} \alpha(\frac{n}{k}).\alpha(\frac{m}{t}).\alpha^{-1}(k).\alpha^{-1}(t) \\
&= -\sum_{\substack{k|n \\ t|m}} \alpha(\frac{n}{k}).\alpha^{-1}(k).\alpha(\frac{m}{t}).\alpha^{-1}(t) + \alpha^{-1}(n).\alpha^{-1}(m) \\
&= -\left(\sum_{k|n} \alpha(\frac{n}{k}).\alpha^{-1}(k)\right).\left(\sum_{t|m} \alpha(\frac{m}{t}).\alpha^{-1}(t)\right) + \alpha^{-1}(n).\alpha^{-1}(m) \\
&= \alpha^{-1}(n).\alpha^{-1}(m)
\end{aligned}$$

ya que

$$\sum_{k|n} \alpha(\frac{n}{k}).\alpha^{-1}(k) = (\alpha * \alpha^{-1})(n) = \chi(n) = 0$$

pues $n > 1$ y

$$\sum_{t|m} \alpha(\frac{m}{t}).\alpha^{-1}(t) = (\alpha * \alpha^{-1})(m) = \chi(m) = 0$$

pues $m > 1$.

Luego, $\alpha^{-1}(n.m) = \alpha^{-1}(n).\alpha^{-1}(m)$, lo que contradice la elección de n y m. Por lo tanto, $\forall a, b \in \mathbb{N}$ tales que $(a, b) = 1$ vale $\alpha^{-1}(a.b) = \alpha^{-1}(a).\alpha^{-1}(b)$. □

Observación 2.2. *Si A es un dominio íntegro y α es una función aritmética a valores en A, no nula y multiplicativa, entonces α es inversible y α^{-1} es multiplicativa.*

En efecto, si $\alpha(1) = 0, \forall\, n \in \mathbb{N}$ se tiene que $\alpha(n) = \alpha(n,1) = \alpha(n).\alpha(1) = 0$, ya que α es multiplicativa.

Luego, siendo α no nula, debe ser $\alpha(1) \neq 0$ y como $\alpha(1) = \alpha(1,1) = \alpha(1).\alpha(1)$, entonces $\alpha(1).[1 - \alpha(1)] = 0$. Por lo tanto debe ser $\alpha(1) = 1$ pues A es íntegro y $\alpha(1) \neq 0$. Luego, por la Proposición 2.5, α es inversible y, por la Proposición 2.6, α^{-1} es multiplicativa.

3. Fórmula de inversión de Möbius

El siguiente problema fue resuelto por A. F. Möbius (1790-1868), quien era alumno de Gauss.

Supongamos que dos funciones aritméticas α y β, a valores en un anillo conmutativo A, satisfacen

$$\alpha(n) = \sum_{d|n} \beta(d)$$

para todo $n \in \mathbb{N}$.
¿Es posible 'invertir' la serie y expresar a β como una función de α?

Para resolver este problema, consideremos la función aritmética ε definida por $\varepsilon(n) = 1$ para todo $n \in \mathbb{N}$. Como $\varepsilon(1) = 1$, por la Proposición 2.5 resulta que ε es inversible. Sea $\mu = \varepsilon^{-1}$

Observando que

$$\alpha(n) = \sum_{d|n} \beta(d) = \sum_{d|n} \varepsilon(\frac{n}{d}).\beta(d) = (\varepsilon * \beta)(n)$$

para todo $n \in \mathbb{N}$, resulta que $\mu * \alpha = \mu * (\varepsilon * \beta) = (\mu * \varepsilon) * \beta = \chi * \beta = \beta$, de donde

$$\beta(n) = \sum_{d|n} \mu(\frac{n}{d}).\alpha(d)$$

para todo $n \in \mathbb{N}$. (Fórmula de inversión de Möbius)

La función μ, llamada la función de Möbius, juega un papel importante en la solución de muchos problemas en Teoría de Números.

Observación 2.3. *La función de Möbius, μ, es multiplicativa.*

En efecto, como ε es inversible y multiplicativa entonces, por la Proposición 2.6, $\mu = \varepsilon^{-1}$ es multiplicativa.

Proposición 2.7. *Para todo $n \in \mathbb{N}$, con ϕ la función de Euler, se verifica: $\phi(n) = \sum_{d|n} \mu(\frac{n}{d}).d$*

Demostración. Por la Proposición 2.4, $\iota(n) = n = \sum_{d|n} \phi(d)$ para todo $n \in \mathbb{N}$. Luego, aplicando la fórmula de inversión de Möbius, resulta que, para todo $n \in \mathbb{N}$,

$$\phi(n) = \sum_{d|n} \mu(\frac{n}{d}).\iota(d) = \sum_{d|n} \mu(\frac{n}{d}).d$$

lo que completa la demostración. □

OBSERVACIÓN 2.4. *Con las notaciones anteriores, podemos escribir*

$$\phi(n) = \sum_{d|n} \mu(d).\iota(\frac{n}{d}) = \sum_{d|n} \mu(d).\frac{n}{d}$$

Es decir

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$$

PROPOSICIÓN 2.8. *Con las notaciones anteriores tenemos*

$$\frac{\phi(n)}{n} = \prod_{p|n} (1 - \frac{1}{p})$$

DEMOSTRACIÓN. Teníamos que $\phi(n) = \prod_{i=1}^{r} (p_i - 1).p_i^{\alpha_i - 1}$ si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, con $\alpha_i \in \mathbb{N}$ y $p_1, \ldots, p_r$ primos distintos y $n \neq 1$. Luego

$$\frac{\phi(n)}{n} = \frac{\prod_{i=1}^{r} (p_i - 1).p_i^{\alpha_i - 1}}{\prod_{i=1}^{r} p_i^{\alpha_i}} = \prod_{i=1}^{r} (p_i - 1).\frac{p_i^{\alpha_i - 1}}{p_i^{\alpha_i}} = \prod_{i=1}^{r} (1 - \frac{1}{p_i}) = \prod_{p|n} (1 - \frac{1}{p})$$

□

Notación: Si $(K, +, \cdot)$ es un cuerpo, con K^* denotaremos el conjunto de los elementos no nulos de K

OBSERVACIÓN 2.5. *Si $(K, +, \cdot)$ es un cuerpo entonces $(K^*, \cdot)$ es un grupo abeliano*

COROLARIO 2.2. *Sea $(K, +, \cdot)$ un cuerpo. Si G es un subgrupo finito de K^* entonces G es cíclico.*

DEMOSTRACIÓN. Sea m el orden de G. Sea $\psi : \mathbb{N} \longrightarrow \mathbb{Z}$ la función aritmética definida por $\psi(n) = \sharp\{\, x \in G \,/\, x \text{ tiene orden } n \,\}$

Afirmación: Para todo $d \in \mathbb{N}$ tal que $d \mid m$, $(\varepsilon * \psi)(d) = d$

En efecto, sea $d \in \mathbb{N}$ tal que $d \mid m$. Entonces

$$(\varepsilon * \psi)(d) = \sum_{k|d} \psi(k) = \sum_{k|d} \sharp\{\, x \in G \,/\, x \text{ tiene orden } k \,\}$$

$$= \sharp \left(\bigcup_{k|d} \{\, x \in G \,/\, x \text{ tiene orden } k \,\} \right)$$

ya que $\bigcup_{k|d} \{\, x \in G \,/\, x \text{ tiene orden } k \,\}$ es una unión disjunta.

Como

$$\bigcup_{k|d}\{\, x \in G \,/\, x \text{ tiene orden } k \,\} = \{\, x \in G \,/\, x^d = 1 \,\}$$

basta probar entonces que $\{\, x \in G \,/\, x^d = 1 \,\}$ tiene d elementos.

Para ello, consideremos el polinomio $X^d - 1 \in K[X]$. Como es un polinomio de grado d con coeficientes en el cuerpo K, no puede tener más de d raíces en K.

Luego, $\sharp\{\, x \in G \,/\, x^d = 1 \,\} \leq d$

Por otra parte, como $d \mid m$ entonces $X^d - 1 \mid X^m - 1$ en $K[X]$. Sea $f \in K[X]$ tal que $X^m - 1 = (X^d - 1).f$

Luego,

$$G = \{\, x \in G \,/\, x^m = 1 \,\} = \{\, x \in G \,/\, x^d = 1 \,\} \cup \{\, x \in G \,/\, f(x) = 0 \,\}$$

de donde

$$\begin{aligned} m = \sharp G &\leq \sharp\{\, x \in G \,/\, x^d = 1 \,\} + \sharp\{\, x \in G \,/\, f(x) = 0 \,\} \\ &\leq \sharp\{\, x \in G \,/\, x^d = 1 \,\} + m - d \end{aligned}$$

ya que f es un polinomio con coeficientes en K de grado $m - d$.

Por lo tanto, $\sharp\{\, x \in G \,/\, x^d = 1 \,\} \geq d$, lo que concluye la demostración de nuestra afirmación.

Veamos ahora que G es cíclico. Como el orden de G es m, basta probar que existe en G un elemento de orden m, es decir, basta probar que $\psi(m) \geq 1$.

Ahora bien,

$$\begin{aligned} \psi(m) = (\chi * \psi)(m) &= ((\mu * \varepsilon) * \psi)\,(m) = (\mu * (\varepsilon * \psi))\,(m) \\ &= \sum_{d|m} \mu(\frac{m}{d}).(\varepsilon * \psi)(d) = \sum_{d|m} \mu(\frac{m}{d}).d \end{aligned}$$

ya que para todo $d \in \mathbb{N}$ tal que $d \mid m$, $(\varepsilon * \psi)(d) = d$

Pero $\displaystyle\sum_{d|n} \mu(\frac{n}{d}).d = \phi(m)$ por la Proposición 2.7 y por lo tanto $\psi(m) = \phi(m) \geq 1$ como queríamos probar. □

Observación 2.6. *Si α y β son funciones aritméticas a valores A que satisfacen*

$$\alpha(n) = \sum_{d|n} \beta(d)$$

para todo $n \in \mathbb{N}$, entonces α es multiplicativa si y sólo si β lo es.

En efecto, como $\alpha = \varepsilon * \beta$, si β es multiplicativa entonces α también lo es por la Proposición 2.3.

Recíprocamente, si α es multiplicativa, como $\beta = \mu * \alpha$ (pues $\alpha = \varepsilon * \beta$ y $\mu = \varepsilon^{-1}$) entonces β es multiplicativa.

La siguiente proposición da una fórmula para calcular el valor de $\mu(n)$

PROPOSICIÓN 2.9. *Sea μ la función de Möbius. Entonces*

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n \text{ es el producto de } k \text{ primos distintos} \\ 0 & \text{si existe un primo } p \text{ tal que } p^2 \mid n \end{cases}$$

DEMOSTRACIÓN. Observemos que, como μ es multiplicativa, basta calcular $\mu(p^r)$ para todo primo p y $r \in \mathbb{N}_0$. Como $\varepsilon * \mu = \chi$, para todo $n \in \mathbb{N}$ se tiene que

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$$

Por lo tanto, $\mu(1) = \sum_{d|1} \mu(d) = 1$ y, para todo $n > 1$, $\sum_{d|n} \mu(d) = 0$.

Luego, si p es un primo, $\mu(p) = -1$ ya que $1 + \mu(p) = \sum_{d|p} \mu(d) = 0$ y, para todo $r \geq 2$, $\mu(p^r) = \sum_{d|p^r} \mu(d) - \sum_{d|p^{r-1}} \mu(d) = 0$ pues $p^r > 1$ y $p^{r-1} > 1$. □

CAPíTULO 3

Grafos

1. Conceptos básicos de la teoría de grafos.

En este capítulo veremos algunas definiciones que se uasarán luego en el dasarrollo de los capítulos siguientes.

DEFINICIÓN 3.1. *Un* grafo *es un par* (V, E) *donde* V *es un conjunto finito y los elementos de* E *son pares de elementos distintos de* V*. Llamaremos* vértices *o* nodos *a los elementos de* V *y* ramas, arcos *o también* flechas *a los elementos de* E*.*

Cuando nos importe el orden en las ramas, los elementos de E *serán pares ordenados y diremos que el grafo es* dirigido*. Cuando no nos importe el orden, los elementos de* E *serán pares no ordenados y diremos que el grafo es* no dirigido*. En ambos casos usaremos la notación* (v, w) *para indicar una rama con la convención de que si el grafo es dirigido nos estamos refiriendo al par ordenado (en cuyo caso* (v, w) *y* (w, v) *denotan ramas distintas) y si es no dirigido nos estamos refiriendo al par no ordenado (en cuyo caso* (v, w) *y* (w, v) *denotan la misma rama).*

DEFINICIÓN 3.2. *Diremos que* $\mathcal{H}$ *es un subgrafo de* $\mathcal{G}$ *y escribiremos* $\mathcal{H} \subset \mathcal{G}$ *si* $\mathcal{V}(\mathcal{H}) \subset \mathcal{V}(\mathcal{G})$ *y* $E(\mathcal{H}) \subset E(\mathcal{G})$*.*

DEFINICIÓN 3.3. *Sea* $G = (V, E)$ *un grafo. Dados* $v, w \in V$ *diremos que una sucesión* $\mathcal{C} = (e_1, \ldots, e_n)$ *de elementos de* E *es un* camino *en* G *de* v *a* w *si* $e_1 = (v, w)$ *o* $e_1 = (w, v)$ *cuando* $n = 1$*, o si* $e_i \neq e_{i+1}$ *para todo* $1 \leq i \leq n-1$ *y existen* $v_1, \ldots v_{n-1} \in V$ *tales que* $e_1 = (v, v_1)$ *o* $e_1 = (v_1, v)$*,* $e_n = (v_{n-1}, w)$ *o* $e_n = (w, v_{n-1})$ *y* $e_i = (v_{i-1}, v_i)$ *o* $e_i = (v_i, v_{i-1})$ *para todo* i *tal que* $2 \leq i \leq n-1$ *cuando* $n > 1$*. En tal caso diremos que* $v, v_1, \ldots, v_{n-1}$ *y* w *son los vértices del camino* $\mathcal{C}$*.*

Si $v, v_1, \ldots, v_{n-1}$ *y* w *son todos distintos diremos que el camino es* simple*. Si* $v = w$ *y* $v, v_1, \ldots, v_{n-1}$ *son todos distintos diremos que el camino es un* ciclo *o también que es un* circuito*.*

Cuando el grafo es dirigido y $e_1 = (v, v_1)$*,* $e_n = (v_{n-1}, w)$ *y* $e_i = (v_{i-1}, v_i)$ *para todo* i *tal que* $2 \leq i \leq n-1$ *si* $n > 1$*, o cuando* $e_1 = (v, w)$ *si* $n = 1$ *diremos que* $\mathcal{C}$ *es un* camino dirigido *de* v *a* w*. Es decir, en un grafo dirigido tenemos los conceptos de camino y camino dirigido. Análogamente se definen los conceptos de* camino dirigido simple *y* ciclo dirigido*.*

Diremos que un grafo G *es* acíclico *si no existe ningún ciclo (dirigido o no) en* G*.*

DEFINICIÓN 3.4. *Diremos que un grafo $G = (V, E)$ es* conexo *si para todo par de vértices $u, v \in V$, $u \neq v$, existe un camino en G de u a v.*

Diremos que el grafo es fuertemente conexo *si para todo par de vértices $u, v \in V$, $u \neq v$, existe un camino dirigido en G de u a v. Observemos que este concepto sólo tiene sentido en el caso de un grafo dirigido.*

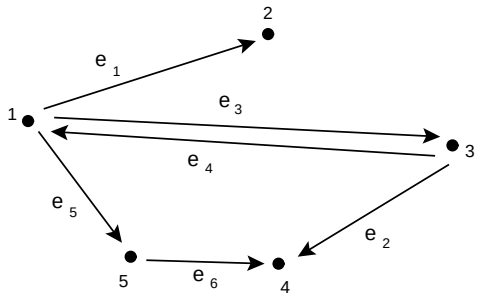
DEFINICIÓN 3.5. *Un grafo $G = (V, E)$ se dice* completo *si para todo par de vértices $u, v \in V$, $u \neq v$, vale que $(u, v) \in E$.*

OBSERVACIÓN 3.1. *Si $G = (V, E)$ es un grafo completo y $m = \sharp V$ entonces*

$$\sharp E = \begin{cases} \binom{m}{2} = \frac{m(m-1)}{2} & \text{si } G \text{ es no dirigido} \\ \\ \binom{m}{2}, 2! = m(m-1) & \text{si } G \text{ es dirigido} \end{cases}$$

Antes de continuar veamos algunos ejemplos.

EJEMPLO 3.1. *Consideremos el siguiente grafo dirigido $G = (V, E)$, con vértices 1, 2, 3, 4 y 5 y ramas $e_1 = (1, 2)$, $e_2 = (3, 4)$, $e_3 = (1, 3)$, $e_4 = (3, 1)$, $e_5 = (1, 5)$ y $e_6 = (5, 4)$, es decir $V = \{1, 2, 3, 4, 5\}$ y $E = \{(1, 2), (3, 4), (1, 3), (3, 1), (1, 5), (5, 4)\}$, al que representaremos gráficamente en la forma*



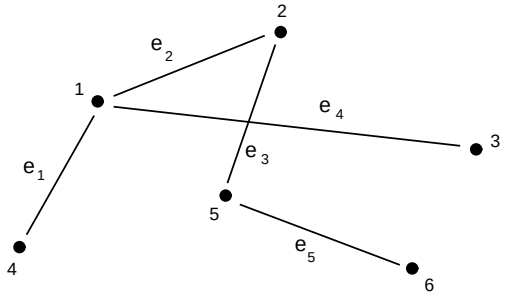
Este es un grafo dirigido, conexo, pero no fuertemente conexo (no hay un camino dirigido de 2 a 3).

La sucesión (e_1, e_3) es un camino simple de 2 a 3. Este camino no es dirigido. El grafo no es acíclico: la sucesión (e_5, e_6, e_2, e_3) es un ciclo. Este ciclo no es un ciclo dirigido.

La sucesión (e_4, e_5, e_6) es un camino dirigido simple de 3 a 4. La sucesión (e_3, e_4) es un ciclo dirigido. La sucesión $(e_1, e_4, e_2, e_6, e_5)$ es un camino de 2 a 1. Este camino no es dirigido ni simple.

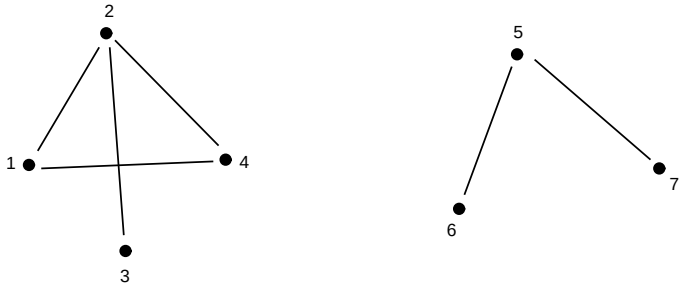
El grafo no es completo: $(2, 1) \notin E$.

EJEMPLO 3.2. *Consideremos el grafo no dirigido $G = (V, E)$, con vértices 1, 2, 3, 4, 5 y 6 y ramas $e_1 = (1, 4)$, $e_2 = (1, 2)$, $e_3 = (2, 5)$, $e_4 = (1, 3)$ y $e_5 = (5, 6)$ $V = \{1, 2, 3, 4, 5, 6\}$ y $E = \{(1, 4), (1, 2), (2, 5), (1, 3), (5, 6)\}$, al que representaremos gráficamente en la forma*



Este es un grafo no dirigido, conexo y acíclico. No es completo: $(4,5) \notin E$. *La sucesión* (e_1, e_2, e_3, e_5) *es un camino simple de 4 a 6.*

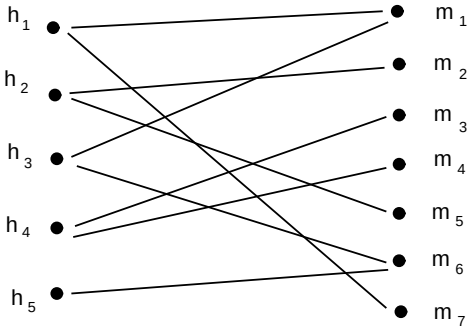
Ejemplo 3.3. *Consideremos el grafo*



Este es un grafo no dirigido. No es conexo (no existe ningún camino que una 1 y 7) sino que tiene dos componentes conexas, una conteniendo un ciclo (el ciclo $(1,2),(2,4),(4,1)$*) y otra acíclica.*

Definición 3.6. *Diremos que* $G = (V, E)$ *es un* grafo bipartito *si existen dos conjuntos disjuntos* P *y* Q *tales que* $V = P \cup Q$ *y toda rama* $e \in E$ *tiene un extremo en* P *y el otro extremo en* Q*.*

Ejemplo 3.4. *El grafo*



es bipartito. En este caso

$$P = \{h_1, h_2, h_3, h_4, h_5\} \quad y \quad Q = \{m_1, m_2, m_3, m_4, m_5, m_6, m_7\}.$$

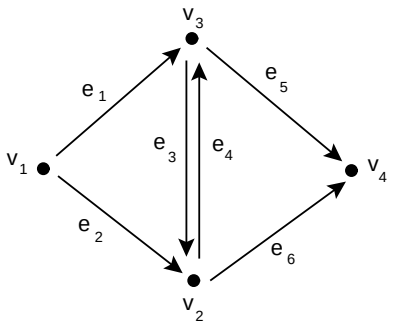
Definición 3.7. *Sea* $G = (V, E)$ *un grafo dirigido. Si* $(u, v) \in E$ *diremos que* u *es la* cola *y que* v *es la* punta *de la flecha* (u, v)*.*

A cada grafo dirigido $G = (V, E)$ le podemos asociar una matriz que contiene toda la información sobre el grafo. Esta matriz se llama la matriz de incidencia vértice-rama *de G.*

Si $V = \{v_1, \ldots, v_m\}$ y $E = \{e_1, \ldots, e_n\}$, la matriz de incidencia vértice-rama de G es la matriz $||a_{ij}|| \in \mathbb{R}^{m\times n}$, definida por

$$a_{ij} = \begin{cases} 1 & \text{si } v_i \text{ es la cola de } e_j \\ -1 & \text{si } v_i \text{ es la punta de } e_j \\ 0 & \text{en otro caso} \end{cases}$$

Ejemplo 3.5. *Dado el grafo*



su matriz de incidencia vértice-rama es la matriz

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 & 1 \\ -1 & 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 \end{pmatrix}$$

Observación 3.2. *La matriz de incidencia vértice-rama de un grafo G tiene, en cada columna, un 1, un -1 y el resto de los coeficientes nulos. Esto se debe a que cada rama tiene una sola cola y una sola punta. Luego, en una matriz de incidencia vértice-rama la suma de todas las columnas es cero.*

CAPíTULO 4

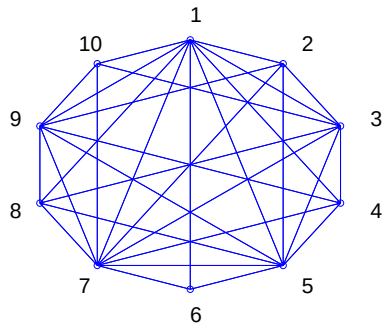
El grafo coprimo de $\mathbb{Z}$

1. El grafo coprimo de $\mathbb{Z}$

El grafo coprimo de $\mathbb{Z}$ es el grafo $\mathcal{G} = (\mathcal{V}, E)$ con $\mathcal{V} = \mathbb{Z}$ y ramas definidas tales que $a, b \in \mathcal{V}$ están conectados por una rama si y sólo si $(a, b) = 1$ donde (a, b) denota el máximo común divisor entra a y b.

Llamaremos $I_n = \{1, \ldots, n\}$. Si $A \subset I_n$, el grafo coprimo de A es el grafo inducido por el grafo coprimo de $\mathbb{Z}$ en A.

EJEMPLO 4.1. *Si* $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, *entonces* $\mathcal{G}(A)$ *es*



Usaremos las siguientes notaciones:

1. $A(m, n) = \{a \in A \mid a \equiv n \ (m)\}$.
2. $\phi(n) =$ función de Euler.
3. $\omega(n) =$ número de factores primos distintos de n.
4. $\mu(n) =$ función de Moëbius.
5. $\mathcal{V}(\mathcal{G})$ y $E(\mathcal{G})$ denotan los conjuntos de vértices y de ramas de $\mathcal{G}$ respectivamente.
6. $K_n =$ grafo completo de n vértices.
7. $C_n =$ ciclo simple de n vértices.
8. Si A es un conjunto, notaremos $\sharp A = |A| =$ cardinal de A, indistintamente
9. $K(m, n) =$ grafo bipartito de U y V con $\sharp U = m$ y $\sharp V = n$.

DEFINICIÓN 4.1. *Diremos que* $\mathcal{H}$ *es un subgrafo de* $\mathcal{G}$ *y escribiremos* $\mathcal{H} \subset \mathcal{G}$ *si* $\mathcal{V}(\mathcal{H}) \subset \mathcal{V}(\mathcal{G})$ *y* $E(\mathcal{H}) \subset E(\mathcal{G})$.

Recientemente ha recibido mucha atención el estudio de varios grafos de enteros. El grafo más popular parece ser el grafo coprimo, pero hay muchos problemas atractivos y resultados sobre el grado de los divisores.

Se han estudiado varios subgrafos del grafo coprimo. Tal vez el primer problema de este tipo fue formulado en 1962: Dado $k \in \mathbb{Z}$, ¿Cuál es el mayor $A \subset I_n$ tal que $K_k \not\subset \mathcal{G}(A)$? O sea, cuál es el mayor subconjunto de I_n tal que no contiene ningún subgrafo completo de $k-$vértices.

2. Subgrafos completos

En esta sección mostraremos la existencia de un conjunto $A_k \subseteq I_n$ tal que para todo k no contiene subgrafos completos de k vértices. Además probaremos que con $k = 2$ y $k = 3$, este conjunto A_k tiene cardinal máximo tal que $K_k \not\subset \mathcal{G}(A)$

Si llamamos p_i al $i-$ésimo primo positivo, se puede ver que el conjunto

$$A_k = \{m \in I_n \ : \ p_i | m \text{ para algún } i \leq k-1\}$$

tiene la propiedad de que $K_k \not\subset \mathcal{G}(A_k)$. En efecto, si existe un $k \in \mathbb{N}$ tal que $K_k \subset \mathcal{G}(A_k)$, tendríamos entonces $a_1, \ldots, a_k \in I_n$, $a_1, \ldots, a_k \in A_k$ distintos con a_i vértices de K_k.

Ahora, dado $a_i \in A_k$ existe p alguno de los primeros $k-1$ primos positivos tales que $p|a_i$ y eligiendo el menor de estos primos, queda definida la aplicación

$$f : \{a_1, \ldots, a_k\} \to \{p_1, \ldots, p_{k-1}\}$$

definida como

$$f(a_i) = \text{mín}\left\{p \in \{p_1, \ldots, p_{k-1}\} \ : \ p|a_i\right\}.$$

Es decir, que a cada a_i le asigna el menor primo entre los primeros $k-1$ primos positivos que lo divide.

Ahora, f está definida desde un conjunto de k elementos en un conjunto de $k-1$ elementos. Luego, f no puede ser inyectiva. En consecuencia, existen $a_i, a_j \in A_k$ distintos tales que $f(a_i) = f(a_j)$. Es decir, $(a_i, a_j) \neq 1$.

Esto contradice el hecho de que K_k es completo.

Hemos demostrado entonces el siguiente resultado:

Proposición 4.1. *Sea p_i el $i-$ésimo primo positivo. El conjunto $A_k = \{m \in I_n \mid p_i|m$ para algún $i \leq k-1\}$ no contiene ningún subgrafo completo de k vértices.*

Surge naturalmente la siguiente pregunta: ¿Es A_k el mayor conjunto contenido en I_n con esta porpiedad?

La respuesta es que no, en general. Ver [**1**]. Sin embargo, se puede ver fácilmente que para $k = 2$ y $k = 3$ la respuesta es afirmativa y recientemente fue demostrado que para $k = 4$ también (ver [**12**])

Finalicemos esta sección con la demostración de los casos $k = 2$ y $k = 3$.

Lamaremos $f(n, k-1) = \sharp A_k$

Observemos que con $k = 2$ queda

$$\sharp A_2 = f(n, 1) = \sharp\{\{m \in I_n \ : \ 2|m\} = [\frac{n}{2}].$$

Con $k = 3$ tenemos $\sharp A_3 = f(n, 2) = \sharp\{\{m \in I_n \ : \ 2|m \text{ o } 3|m\} = [\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}]$.

Demostración del caso $k = 2$. En este caso, $A_2 = \{m \in I_n \ : \ 2|m\}$. Es decir, A_2 es el conjunto de los números pares menores o iguales a n.

Este conjunto cumple:

1. $K_2 \not\subset \mathcal{G}(A_2)$.
2. A_2 es el mayor con esta propiedad.

La propiedad (1) fue demostrada para todo k en la proposición 4.1. Sin embargo en este caso se observa fácilmente ya que A_2 es el conjunto de todos los pares y por lo tanto no existen en A_2 dos elementos coprimos.

Para ver (2), supongamos que tenemos $B \subset I_n$ con $\sharp B > \sharp A = [\frac{n}{2}]$. O sea $\sharp B \geq [\frac{n}{2}] + 1$. Quiero ver que existen $a, b \in B$ tal que $(a, b) = 1$. La prueba la haremos en dos casos: Si $1 \in B$ o si $1 \notin B$.

Caso 1: Si $1 \in B$ entonces para cualquier $b \in B$ tenemos $(b, 1) = 1$ y por lo tanto tendríamos un K_2 si $\sharp B \geq 2$. Pero $\sharp B \geq [\frac{n}{2}] + 1 \geq 2$ si $n \geq 2$.

Caso 2: Si $1 \notin B$ afirmamos que existe $b \in B$ tal que $b + 1 \in B$. En efecto, si no fuera así, la diferencia entre dos elementos cualesquiera de B sería mayor o igual que 2, entonces como $1 \notin B$ se tendría $\sharp B \leq [\frac{n}{2}]$ lo que es un absurdo ya que $\sharp B \geq [\frac{n}{2}] + 1$.

Luego, B contiene dos elementos consecutivos b y $b+1$ y como $(b, b+1) = 1$ se concluye que B contiene un K_2. □

Demostración del caso $k = 3$. En este caso, el conjunto seria $A_3 = \{m \in I_n \ : \ 2|m \text{ o } 3|m\}$ y $\sharp A_3 = [\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}]$.

Este conjunto cumple:

1. $K_3 \not\subset \mathcal{G}(A_3)$.
2. A_3 es el mayor con esta propiedad.

La propiedad (1) fue demostrada para todo k en la proposición 4.1.

Para ver (2), supongamos que tenemos $B \subset I_n$ con $\sharp B > \sharp A$. O sea $\sharp B \geq [\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + 1$. Quiero ver que existe un $K_3 \subset \mathcal{G}(B)$.

Al igual que en la demostración anterior, dividiremos la prueba en dos casos: $1 \in B$ y $1 \notin B$.

Caso 1: Si $1 \in B$ para encontrar un $K_3 \subset \mathcal{G}(B)$ basta encontrar $a, b \in B$, $a \neq 1$, $b \neq 1$ tal que $(a, b) = 1$.

Como $1 \in B$ consideramos $\bar{B} = B - \{1\}$. Observemos que $\sharp\bar{B} = \sharp B - 1$ y como $\sharp B \geq [\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + 1$, entonces

$$\sharp\bar{B} \geq [\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] \geq [\frac{n}{2}] + 1,$$

ya que como $n \geq 3$, $[\frac{n}{3}] - [\frac{n}{6}] \geq 1$.

Entonces $\bar{B}$ es un subconjunto de I_n con cardinal $\sharp\bar{B} \geq [\frac{n}{2}] + 1$. Luego por lo hecho para el caso $k = 2$, $\bar{B}$ contiene un K_2. O sea existen $a, b \in B$, $a \neq 1$, $b \neq 1$ tal que $(a, b) = 1$.

Entonces $\{1, a, b\}$ forman un K_3 contenido en $\mathcal{G}(B)$.

Caso 2: Supongamos que $1 \notin B$. Dividiremos este dos subcasos, dependiendo si $2 \in B$ o $2 \notin B$.

Caso 2.1: Supongamos que $2 \in B$. Afirmamos que existe $b \in B$, b impar, tal que $b + 2 \in B$ o $b + 4 \in B$.

En efecto, si esto no ocurriera la diferencia entre cualesquiera dos impares de B es por lo menos 6. Entonces B puede contener a lo sumo $[\frac{n-3}{6}]$ impares, y B puede contener a lo sumo $[\frac{n}{2}]$pares. Luego sería: $\sharp B \leq [\frac{n-3}{6}] + [\frac{n}{2}]$.

Ahora $\sharp B \geq [\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + 1$. Entonces debería ser

$$[\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + 1 \leq [\frac{n-3}{6}] + [\frac{n}{2}].$$

Esto se cumple si y sólo si

$$[\frac{n}{3}] - [\frac{n}{6}] + 1 \leq [\frac{n-3}{6}]$$

que es equivalente a

$$1 + [\frac{n}{3}] \leq [\frac{n-3}{6}] + [\frac{n}{6}]$$

Usando la desigualdad $[x] \leq x < [x] + 1$, concluimos

$$\frac{n}{3} < 1 + [\frac{n}{3}] \leq [\frac{n-3}{6}] + [\frac{n}{6}] \leq \frac{n-3}{6} + \frac{n}{6} = \frac{2n-3}{6}$$

lo que es un absurdo.

Entonces B contiene dos impares cuya diferencia es 2 o 4. Es decir, existe $b \in B$ impar tal que $b+2 \in B$ o $b+4 \in B$ y además resulta que $(b, b+2) = 1$ y $(b, b+4) = 1$, con lo cual $\{2, b, b+2\}$ o $\{2, b, b+4\}$ serían $K_3 \subset B$.

Caso 2.2: Supongamos que $1 \notin B$ y $2 \notin B$, con lo cual $B \subset \{3, \ldots, n\}$.

Vamos a partir a B como una unión disjunta de conjuntos de 6 elementos. Sean

$$\begin{aligned} I_0 &= \{3, 4, 5, 6, 7, 8\} \\ I_1 &= \{9, 10, 11, 12, 13, 14\} \\ &\vdots \\ I_k &= \{3 + 6k, 4 + 6k, \ldots, r + 3 + 6k\} \end{aligned}$$

donde r es el resto de dividir $n - 3$ por 6. El último conjunto, I_k, tiene 6 elementos si $n = 6k + 8$, es decir si $n - 3 = 6k + 5$.

En general, se tiene $n - 3 = 6k + r$ con $0 \leq r \leq 5$ y entonces I_k tiene $r + 1$ elementos.

Luego, tenemos

$$\{3,\dots,n\} = \biguplus_{j=0}^{k} I_j,$$

con lo cual

$$B = \biguplus_{j=0}^{k} (B \cap I_j) \quad \text{y} \quad \sharp B = \sum_{j=0}^{k} \sharp(B \cap I_j).$$

Vamos a contar cuántos elementos de B puede haber en cada I_j.

Supongamos primero que en cada I_j hay a lo sumo 4 elementos de B. Es decir, $\sharp(B \cap I_j) \leq 4$, $j = 0,\dots,k-1$ y $\sharp(B \cap I_k) \leq \text{mín}\{4, r+1\}$.

Luego se tiene

$$\begin{aligned}\sharp B &= \sum_{j=0}^{k} \sharp(B \cap I_j) = \sum_{j=0}^{k-1} \sharp(B \cap I_j) + \sharp(B \cap I_k) \\ &\leq \sum_{j=0}^{k-1} 4 + \text{mín}\{4, r+1\} = 4k + \text{mín}\{4, r+1\}.\end{aligned}$$

Usando ahora $\sharp B \geq [\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + 1$, obtenemos

$$[\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + 1 \leq 4k + \text{mín}\{4, r+1\}. \tag{4.1}$$

Observemos ahora que $k = [\frac{n-3}{6}]$ y consideremos los casos que corresponden a cada posible valor de r.

1^{er} *caso:* $r = 0$, con lo cual $n = 6k+3$.

Tenemos

$$[\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + 1 = (3k+1) + (2k+1) - k + 1 = 4k+3,$$

y de (4.1) obtenemos

$$4k + 3 \leq 4k + \text{mín}\{4, r+1\} = 4k+1$$

lo que es un absurdo.

2^{do} *caso:* $r = 1$, con lo cual $n = 6k+4$.

Tenemos

$$[\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + 1 = (3k+2) + (2k+1) - k + 1 = 4k+4,$$

y de (4.1) obtenemos

$$4k + 4 \leq 4k + \text{mín}\{4, r+1\} = 4k+2$$

lo que es un absurdo.

3^{er} *caso:* $r = 2$, con lo cual $n = 6k+5$.

Tenemos

$$[\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + 1 = (3k+2) + (2k+1) - k + 1 = 4k+4,$$

y de (4.1) obtenemos

$$4k + 4 \leq 4k + \text{mín}\{4, r + 1\} = 4k + 3$$

lo que es un absurdo.

4^{to} *caso:* $r = 3$, con lo cual $n = 6k + 5$.

Tenemos

$$[\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + 1 = (3k + 3) + (2k + 2) - (k + 1) + 1 = 4k + 5,$$

y de (4.1) obtenemos

$$4k + 5 \leq 4k + \text{mín}\{4, r + 1\} = 4k + 4$$

lo que es un absurdo.

5^{do} *caso:* $r = 4$, con lo cual $n = 6k + 7$.

Tenemos

$$[\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + 1 = (3k + 3) + (2k + 2) - (k + 1) + 1 = 4k + 5,$$

y de (4.1) obtenemos

$$4k + 5 \leq 4k + \text{mín}\{4, r + 1\} = 4k + 4$$

lo que es un absurdo.

6^{to} *(¡y último!) caso:* $r = 5$, con lo cual $n = 6k + 8$.

Tenemos

$$[\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + 1 = (3k + 4) + (2k + 2) - (k + 1) + 1 = 4k + 6,$$

y de (4.1) obtenemos

$$4k + 6 \leq 4k + \text{mín}\{4, r + 1\} = 4k + 4$$

lo que es un absurdo.

Luego debe existir j, $0 \leq j \leq k$, tal que $\sharp(B \cap I_j) \geq 5$. Es decir, que para ese I_j a lo sumo un elemento no pertenece a B.

Escribamos $I_j = \{6j + 3, 6j + 4, 6j + 5, 6j + 6, 6j + 7, 6j + 8\}$ (si $j = k$ entonces podría no estar el $6j + 8$).

Si $6j + 3 \notin B$ entonces $6j + 5$, $6j + 6$, $6j + 7 \in B$ y forman un K_3. El mismo K_3 se encontrará en B si $6j + 4$ o $6j + 8$ no están en B.

Si $6j + 5 \notin B$ entonces $6j + 3$, $6j + 4$, $6j + 7 \in B$ y forman un K_3. El mismo K_3 se encontrará en B si $6j + 6 \notin B$.

Finalmente, si $6j + 7 \notin B$, tenemos que $6j + 3$, $6j + 4$, $6j + 4 \in B$ forman un K_3.

Esto finaliza la demostración. □

CAPíTULO 5

Ciclos pares

En esta sección, investigamos otra cuestión natural sobre el grafo coprimo de $\mathbb{Z}$: ¿Qué se puede decir sobre los ciclos en $\mathcal{G}(A)$?

El caso de los ciclos pares (C_{2l}) no es difícil de resolver usando los resultados conocidos (al menos para ciclos no demasiado largos).

Una pregunta a resolver sería: Cúal será el subconjunto $A \subseteq I_n$ más grande que no contenga ciclos pares?

Probaremos que si l no es demasiado grande, el conjunto A de mas grande cardinal contenido en I_n tal que no contenga ciclos pares tiene $[\frac{n}{2}] + l - 1$ cantidad de elementos.

Más precisamente si $l \leq \frac{1}{10}\ln(\ln(n))$ el máximo $A \subseteq I_n$ tal que $C_{2l} \not\subset \mathcal{G}(A)$ debe ser de cardinal $f(n,1) + l - 1 = [\frac{n}{2}] + l - 1$.

Este cardinal se alcanza tomando todos los números pares y los primeros l primos.

Es decir tomemos A así:

$$A = \{m \in I_n \ : \ 2|m\} \cup \{p_1, \ldots, p_l\},$$

donde $\{p_1, p_2, \ldots, p_i, \ldots\}$ denota el conjunto de los primos positivos ordenados en forma creciente.

Veamos que el grafo generado por A no contiene ciclos pares. En efecto, si $\mathcal{G}(A)$ contuviera ciclos de $2l$ vértices, entonces existen $a_1, \ldots, a_{2l}$ elementos de A tales que

$$(a_1, a_2) = (a_2, a_3) = \cdots = (a_{2l-1}, a_{2l}) = (a_{2l}, a_1) = 1.$$

Ahora bien, en A hay exactamente $l - 1$ impares, entonces entre los a_i hay como mínimo $2l - (l-1)$ números pares. O sea que entre los a_i hay por lo menos $l + 1$ números pares.

Pero entonces, si tomo los conjuntos

$$\{a_1, a_2\}; \ \{a_3, a_4\}; \ \ldots; \ \{a_{2l-1}, a_{2l}\}$$

son l conjuntos disjuntos. Luego en alguno de ellos debe haber dos pares, o sea existe i tal que a_i y a_{i+1} son pares. Es decir, $(a_i, a_{i+1}) \neq 1$ lo que es un absurdo.

Hemos demostrado que $C_{2l} \not\subset \mathcal{G}(A)$.

Ahora queremos responder la siguiente pregunta: ¿Es A el subconjunto más grande con la propiedad de el grafo inducido por él no contiene ciclos pares?

Calculemos el cardinal de A.

$$\sharp A = \sharp\{m \in I_n \ : \ 2|m\} + \sharp\{p_1, \ldots, p_l\} - 1 = [\frac{n}{2}] + l - 1$$

Recordemos que $f(n,k) = \sharp\{m \in I_n \ : \ p_i|m \text{ para algún } i \leq k\}$. Luego $f(n,1) = [\frac{n}{2}]$.

Probemos que para n suficientemente grande, A es efectivamente el conjunto más grande con la propiedad de no contener ciclos pares de longitud $2l$ si l no es demasiado grande. Más precisamente, si $l \leq \frac{1}{10}\ln(\ln(n))$.

O sea, veremos que si $l \leq \frac{1}{10}\ln(\ln(n))$ y supongamos existe $B \subset \{1, \ldots, n\}$ es tal que $\sharp B > [\frac{n}{2}] + l - 1$ (i.e. $\sharp B \geq [\frac{n}{2}] + l$) entonces existe C_{2l} ciclo par, $C_{2l} \subset B$ para n suficientemente grande. Vamos a usar siguiente teorema cuya prueba se puede ver en [**7**].

TEOREMA 5.1. *Existe un n_0 tal que, para todo $n \geq n_0$ y $C \subset I_n$ tal que $\sharp C > f(n,1)$, $\sharp C(2,1) = s > 0$, entonces, si $r = \text{mín}\{s, \frac{1}{10}\ln(\ln(n)\}$, $K(r,r) \subset \mathcal{G}(C)$.*

Veamos ahora que B está en las condiciones del Teorema 5.1.

- $\sharp B \geq [\frac{n}{2}] + l = f(n,1) + l > f(n,1)$, ya que $l \geq 1$.
- $\sharp B(2,1) = \{b \in B \ : \ b \equiv 1 \ (2)\} > 0$, ya que si $\sharp B(2,1) = 0$, $\Rightarrow \sharp B \leq [\frac{n}{2}]$, lo que es absurdo.

Entonces estamos en las condiciones del Teorema 5.1, y por lo tanto, existe un n_0 tal que, si $n \geq n_0$, tomando $r = \text{mín}\{s, \frac{1}{10}\ln(\ln(n)\} \Rightarrow K(r,r) \subset \mathcal{G}(B)$.

Ahora, en general vale que si $K(r,r) \subset \mathcal{G}(B)$ y $k < r$, entonces $K(k,k) \subset \mathcal{G}(B)$. En efecto, $K(k,k)$ es el subgrafo completo de $K(r,r)$ que resulta de quedarme con los primeros k vértices.

Veamos ahora que $l \leq s$.

Escribiendo $B = \{b \in B \ : \ b \equiv 1 \ (2)\} \uplus \{b \in B \ : \ 2|b\}$, obtenemos tomando cardinal,

$$\sharp B = s + \sharp\{b \in B \ : \ 2|b\} \leq s + f(n,1), \tag{5.1}$$

Ya que $f(n,1) = [\frac{n}{2}] = \sharp\{m \in I_n : \ 2|m\}$.

Ahora como B, $\sharp B \geq f(n,1) + l$ y junto con (5.1) obtenemos

$$f(n,1) + l \leq f(n,1) + s \qquad \Rightarrow \qquad l \leq s.$$

Luego, si $l \leq \frac{1}{10}\ln(\ln(n))$ tenemos que $l \leq \text{mín}\{s, \frac{1}{10}\ln(\ln(n))\} = r$ y por lo tanto, por el Teorema 5.1 obtenemos $K(l,l) \subset \mathcal{G}(B)$.

Ahora, es un hecho general que si $K(l,l) \subset \mathcal{G}(B)$ entonces $C_{2l} \subset \mathcal{G}(B)$, ya que $K(l,l)$ es un subgrafo de $\mathcal{G}(B)$ bipartito de U y V con $\sharp U = \sharp V = l$, tal que $V(K_{ll}) \subseteq V(B)$ y $E(K_{ll}) \subseteq E(B)$ Es decir, si $U = \{a_1, \ldots, a_l\}$ y $V = \{b_1, \ldots, b_l\}$ con $a_i, b_j \in B$ para $i, j = 1, \ldots, l$, como $K(l,l)$ es completo se tiene que $(a_i, b_j) = 1$ para todo $i, j = 1, \ldots, l$.

Luego se puede armar un $2l-$ciclo de la siguiente manera:

$\mathcal{V}(C_{2l}) = \{a_1, b_1, a_2, b_2, \ldots, a_l, b_l\}$,

$E(C_{2l}) = \{[a_1, b_1]; [b_1, a_2]; [a_2, b_2]; [b_2, a_3]; \ldots; [b_{l-1}, a_l]; [a_l, b_l]; [b_l, a_1]\}$.

Entonces hemos construido $C_{2l} \subset \mathcal{G}(B)$.

En conclusión, hemos demostrado el siguiente teorema.

TEOREMA 5.2. *Si* $A = \{m \in I_n \ : \ 2|m\} \cup \{p_1, \ldots, p_l\}$ *donde* p_i *denota al* $i-$*ésimo primo positivo, entonces* $\mathcal{G}(A)$ *no posee ciclos pares. Notemos que* $\sharp A = [\frac{n}{2}] + l - 1$. *Y para* n *suficientemente grande y* $l \leq \frac{1}{10}\ln(\ln(n))$, A *es el mayor subconjunto de* I_n *con esa propiedad.*

CAPíTULO 6

Ciclos impares

En esta sección intentaremos dar una respuesta a la pregunta ¿cuál será el conjunto $A \subset I_n$ más grande tal que no contenga ciclos impares?

En el caso de ciclos de longitud 3 (triángulos), vimos en la Sección 2 que el mayor $A \subset I_n$ tal que $C_3 = K_3 \not\subset \mathcal{G}(A)$ es $A_3 = \{m \in I_n \ : \ 2|m \text{ o } 3|m\}$ que tiene cardinal $\sharp A_3 = f(n,2) = [\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}]$.

Es decir que para garantizar la existencia de un triángulo en $A \subset I_n$ se necesita $\sharp A \geq f(n,2) + 1$.

Sorprendentemente este cardinal garantiza la existencia de ciclos impares de *casi toda* longitud. Más precisamente, se tiene:

TEOREMA 6.1. *Existen constantes c_0 y n_0 tales que, para todo $n \geq n_0$ y para todo $A \subset I_n$ con $\sharp A \geq f(n,2) + 1$, se tiene que existe un $2l+1-$ciclo $C_{2l+1} \subset \mathcal{G}(A)$ para todo $l \leq c_0 n$.*

Sería interesante determinar el valor óptimo de la constante c_0. Un posible valor para la misma es $c_0 = \frac{1}{6}$. La cota $c_0 \leq \frac{1}{6}$ es el contenido del siguiente lema.

LEMA 6.1. *Sea c_0 la constante definida en el Teorema 6.1. Entonces se tiene $c_0 \leq \frac{1}{6}$.*

DEMOSTRACIÓN. Si $c_0 > \frac{1}{6}$, podemos encontrar un conjunto $A \subseteq I_n$ con $\sharp A \geq f(n,2) + 1$ tal que $C_{2l+1} \not\subseteq G(A)$, para $l > \frac{1}{6}n$

Tomemos $n \in \mathbb{N}$ tal que $6|n$ y definimos $A \subset I_n$ como

$$A = \{m \in I_n \ : \ 2|m\} \cup \{2k-1 \ : \ 1 \leq k \leq \frac{n}{6} + 1\}.$$

Se tiene

$$\sharp A = \frac{n}{2} + \frac{n}{6} + 1 = \frac{n}{2} + \frac{n}{3} - \frac{n}{6} + 1 = [\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + 1 = f(n,2) + 1.$$

Veamos que si $l > \frac{1}{6}n$ entonces $C_{2l+1} \not\subset \mathcal{G}(A)$. En efecto, supongamos que $C_{2l+1} \subset \mathcal{G}(A)$ y sea k la cantidad de elementos impares en C_{2l+1}. Luego $k \leq \frac{n}{6} + 1$. Entonces la cantidad de pares en C_{2l+1} es

$$2l + 1 - k \geq 2(\frac{n}{6} + 1) + 1 - (\frac{n}{6} + 1) = \frac{n}{6} + 2.$$

Pero en un ciclo, no puede haber dos pares ligados, luego debe haber por lo menos un impar por cada par. Pero la cantidad de pares en C_{2l+1} es mayor

o igual a $\frac{n}{6}+2$ y la cantidad de impares es menor o igual a $\frac{n}{6}+1$ lo que es un absurdo. □

En la demostración del Teorema 6.1 distinguiremos dos casos dependiendo del tamaño de $\sharp A(6,1)+\sharp A(6,5)$.

El Teorema 6.1 será una consecuencia de dos los siguientes resultados.

TEOREMA 6.2. *Existen constantes c_1, c_2 y n_1 tales que si $n \geq n_1$*

$$\sharp A(6,1) = s_1, \quad \sharp A(6,5) = s_2, \quad 1 \leq s_1 + s_2 \leq c_1 n$$

y $\sharp A > f(n,2)$, entonces $C_{2l+1} \subset \mathcal{G}(A)$ para todo $l \leq c_2 n$.

TEOREMA 6.3. *Para todo $\varepsilon > 0$, existe $n \in \mathbb{N}$ y constantes $c_3 = c_3(\varepsilon)$ y $n_2 = n_2(\varepsilon)$ tales que si $n \geq n_2$*

$$\sharp A(6,1) = s_1, \quad \sharp A(6,5) = s_2, \quad s_1 + s_2 \geq \varepsilon n$$

y $\sharp A > f(n,2)$, entonces $C_{2l+1} \subset \mathcal{G}(A)$ para todo $l \leq c_3 n$.

Veamos que efectivamente los Teoremas 6.2 y 6.3 implican el Teorema 6.1.

Demostración del Teorema 6.1. Sea $A \subset I_n$ tal que $\sharp A > f(n,2)$ y llamemos $s_1 = \sharp A(6,1)$ y $s_2 = \sharp A(6,5)$.

Si se tiene que $1 \leq s_1 + s_2 \leq c_1 n$ con c_1 dada por el Teorema 6.2, entonces se puede aplicar el Teorema 6.2 y se obtiene que existe c_2 y n_1 tal que para todo $n \geq n_1$,

$$C_{2l+1} \subset \mathcal{G}(A) \qquad \text{para todo } l \leq c_2 n.$$

Si en cambio se tiene que $s_1 + s_2 > c_1 n$, se aplica el Teorema 6.3 con $\varepsilon < c_1$ y se obtiene que existe $n_2 = n_2(\varepsilon)$ y $c_3 = c_3(\varepsilon)$ tales que para todo $n \geq n_2$,

$$C_{2l+1} \subset \mathcal{G}(A) \qquad \text{para todo } l \leq c_3 n.$$

Luego el Teorema 6.1 queda probado tomando $n_0 = \text{máx}\{n_1, n_2\}$ y $c_0 = \text{mín}\{c_2, c_3\}$. □

Debemos entonces demostrar los Teoremas 6.2 y 6.3. Haremos estas demostraciones en los siguientes dos capítulos.

CAPíTULO 7

Demostración del Teorema 6.2

En este capítulo demostraremos el Teorema 6.2.

Podemos suponer, sin pérdida de generalidad, que $s_1 = \max\{s_1, s_2\}$.

Una idea general de la demostracón es construir el ciclo $C_{2l+1} \subset \mathcal{G}(A)$ tomando primero $a \in A(6,1)$ con $\phi(a)$ relativamente grande y los restantes $2l$ elementos los elegiremos alternadamente en $A(6,2)$ y $A(6,3)$.

Necesitaremos el siguiente lema:

LEMA 7.1. *Existe una constante c_4 tal que el número de enteros $k \in I_n$ tales que $\phi(k)/k < 1/t$ es menor que $n\exp(-\exp(c_4 t))$.*

Si $t > 2$, la constante c_4 se puede tomar independiente de t.

La demostración del Lema 7.1 se puede encontrar en [**2**].

Aplicamos el Lema 7.1 con

$$t = \frac{1}{c_4} \ln\left(\ln\left(\frac{2n}{s_1}\right)\right). \tag{7.1}$$

Observemos que si c_1 es chico, es decir $c_1 < 2\exp(-\exp(2c_4))$, entonces como $s_1 \leq s_1 + s_2 \leq c_1 n$ tenemos $s_1 < 2\exp(-\exp(2c_4))n$.

Esto implica $2 < \frac{1}{c_4}\ln\left(\ln\left(\frac{2n}{s_1}\right)\right) = t$. Por lo tanto $t > 2$.

Luego, aplicando el Lema 7.1 tenemos que

$$\sharp\left\{k \in I_n \ : \ \frac{\phi(k)}{k} < \frac{1}{t}\right\} < \frac{s_1}{2}. \tag{7.2}$$

Ahora

$$\begin{aligned} A(6,1) = &\left(A(6,1) \cap \left\{k \in I_n \ : \ \frac{\phi(k)}{k} < \frac{1}{t}\right\}\right) \\ &\uplus \left(A(6,1) \cap \left\{k \in I_n \ : \ \frac{\phi(k)}{k} \geq \frac{1}{t}\right\}\right). \end{aligned} \tag{7.3}$$

Tomando cardinal en (7.3) y usando (7.2) obtenemos

$$s_1 < \frac{s_1}{2} + \sharp\left(A(6,1) \cap \left\{k \in I_n \ : \ \frac{\phi(k)}{k} \geq \frac{1}{t}\right\}\right),$$

de donde se obtiene

$$\sharp\left(A(6,1) \cap \left\{k \in I_n \ : \ \frac{\phi(k)}{k} \geq \frac{1}{t}\right\}\right) > \frac{s_1}{2}.$$

Luego concluimos que existe $a \in A(6,1)$ tal que $\phi(a)/a \geq 1/t$.

Sea ahora $B = \{u \in \mathbb{Z} \ : \ 6u+2 \in I_n \text{ y } (6u+2,a) = 1\}$. Queremos calcular $\sharp B$. Este es el contenido del siguiente lema.

LEMA 7.2. *Sea* $B = \{u \in \mathbb{Z} \ : \ 6u+2 \in I_n \ y \ (6u+2,a) = 1\}$. *Entonces*

$$\sharp B = \sum_{d|a} \mu(d) g_1(n,d), \tag{7.4}$$

donde $g_1(n,d) = \sharp\{v \in \mathbb{Z} \ : \ 6v+2 \in I_n \ y \ d|6v+2\}$.

DEMOSTRACIÓN. Usaremos la fórmula de inversión de Mœbious. Definimos

$$\beta(m) = \sharp\{b \in I_n \ : \ b \equiv 2 \ (6) \text{ y } m(b,a) = a\}.$$

Con esta definición, se tiene que $\beta(a) = \sharp B$.

Pues $\sharp B = \sharp\{u \in \mathbb{Z} \ : \ 6u+2 \in I_n \text{ y } (6u+2,a) = 1\} = \sharp\{b \in I_n \ : \ b \equiv 2 \ (6) \text{ y } \ (b,a) = 1\} = \sharp\{b \in I_n \ : \ b \equiv 2 \ (6) \text{ y } \ (b,a)a = a1\} = \beta(a)$

Definamos ahora

$$\alpha(m) = \sharp\{b \in I_n \ : \ b \equiv 2 \ (6) \text{ y } a|mb\}.$$

Con esta definición, para d divisor de a, se tiene que $\alpha(\frac{a}{d}) = g_1(n,d)$. En efecto

$$\begin{aligned} g_1(n,d) &= \sharp\{v \in \mathbb{Z} \ : \ 6v+2 \in I_n \text{ y } d|6v+2\} \\ &= \sharp\{b \in I_n \ : \ b \equiv 2 \ (6) \text{ y } d|b\} \\ &= \sharp\{b \in I_n \ : \ b \equiv 2 \ (6) \text{ y } a\Big|\frac{ab}{d}\} \\ &= \alpha(\frac{a}{d}). \end{aligned}$$

Si ahora vemos que

$$\alpha(m) = \sum_{d|m} \beta(d), \tag{7.5}$$

entonces, por la fórmula de inversión de Mœbius,

$$\beta(m) = \sum_{d|m} \mu(d)\alpha(\frac{m}{d})$$

y, evaluando β en a, se obtiene

$$\sharp B = \beta(a) = \sum_{d|a} \mu(d)\alpha(\frac{a}{d}) = \sum_{d|a} \mu(d) g_1(n,d).$$

Debemos entonces verificar (7.5). La idea es partir al conjunto $\{b \in I_n \ : \ b \equiv 2 \ (6) \text{ y } a|mb\}$ como una unión disjunta de conjuntos de cardinal $\beta(d)$. Más precisamente,

$$\{b \in I_n \ : \ b \equiv 2 \ (6) \text{ y } a|mb\} = \biguplus_{d|m} \{b \in I_n \ : \ b \equiv 2 \ (6) \text{ y } d(b,a) = a\}. \tag{7.6}$$

En efecto, si $d(b,a) = a$ para algún d divisor de m, se tiene que $a = d(b,a)|mb$.

Recíprocamente si $b \in I_n$ es tal que $b \equiv 2\ (6)$ y $a|mb$ tenemos que $d(b,a) = a$ para algún d divisor de m, puesto que como $(a,b)|a$, existe $d \in \mathbb{Z}$ tal que $a = (a,b)d$ y es fácil ver que d verifica lo pedido.

Que la unión es disjunta es evidente.

Tomando ahora cardinal en (7.6) obtenemos

$$\begin{aligned}\alpha(m) &= \sharp\{b \in I_n \ :\ b \equiv 2\ (6) \text{ y } a|mb\} \\ &= \sum_{d|m} \sharp\{b \in I_n \ :\ b \equiv 2\ (6) \text{ y } d(b,a) = a\} \\ &= \sum_{d|m} \beta(d),\end{aligned}$$

como queríamos demostrar. □

Tratemos ahora de encontrar una cota para $g_1(n,d)$.

$g_1(n,d) = \sharp\{b \in I_n \ :\ b \equiv 2\ (6) \text{ y } d|b\} = \sharp\{b \in I_n \ :\ b \equiv 2\ (6) \text{ y } b \equiv 0\ (d)\}$.

Veamos como son todos los $b \in \mathbb{Z}$ soluciones del sistema

$$\begin{cases} b \equiv 2 & (6) \\ b \equiv 0 & (d) \end{cases} \tag{7.7}$$

Como $(a,6) = 1$ y d es un divisor de a, sigue que $(d,6) = 1$ entonces, por el Teorema Chino del Resto, el sistema (7.7) tiene una única solución $b_0 \in [0, 6d)$ (más precisamente $b_0 \in [2, 6d)$, ya que $b_0 \neq 0$ y $b_0 \neq 1$) y todas las soluciones son de la forma

$$b = b_0 + k6d \qquad (k \in \mathbb{Z}).$$

En conclusión,

$g_1(n,d) = \sharp\{b \in I_n \ :\ b = b_0 + k6d\ (k \in \mathbb{Z})\} = \sharp\{k \in \mathbb{Z} \ :\ 1 \leq b_0 + k6d \leq n\}$.

La idea para acotar $g_1(n,d)$ va a ser meter $\{k \in \mathbb{Z} \ :\ 1 \leq b_0 + k6d \leq n\}$ entre dos conjuntos convenientes para obtener cotas por arriba y por abajo. Vemos la cota inferior primero. Es claro que

$$\{k \in \mathbb{Z} \ :\ 0 \leq k \leq \frac{n-2}{6d} - 1\} \subset \{k \in \mathbb{Z} \ :\ 1 \leq b_0 + k6d \leq n\}. \tag{7.8}$$

En efecto, si $0 \leq k \leq \frac{n-2}{6d} - 1$ entonces, usando que $1 \leq b_0 < 6d$ obtenemos

$$1 \leq b_0 \leq b_0 + k6d \leq b_0 + (\frac{n-2}{6d} - 1)6d = b_0 + n - 2 - 6d \leq n - 2 < n.$$

Ahora, para la cota superior, afirmamos que

$$\{k \in \mathbb{Z} \ :\ 1 \leq b_0 + k6d \leq n\} \subset \{k \in \mathbb{Z} \ :\ 0 \leq k \leq \frac{n-2}{6d}\}. \tag{7.9}$$

En efecto, si $1 \leq b_0 + k6d$, tenemos (usando que $b_0 < 6d$)

$$k \geq \frac{1 - b_0}{6d} > \frac{1}{6d} - 1 > -1,$$

y si $b_0 + k6d \leq n$, tenemos (usando que $b_0 \geq 2$)

$$k \leq \frac{n - b_0}{6d} \leq \frac{n-2}{6d}.$$

En conclusión

$$-1 < k \leq \frac{n-2}{6d} \quad \Rightarrow \quad 0 \leq k \leq \frac{n-2}{6d}.$$

Tomando cardinal en (7.8) y (7.9) se obtiene,

$$\left[\frac{n-2}{6d} - 1\right] + 1 \leq g_1(n,d) \leq \left[\frac{n-2}{6d}\right] + 1.$$

Ahora, usando que $[x-1] = [x] - 1$ concluimos

$$\left[\frac{n-2}{6d}\right] \leq g_1(n,d) \leq \left[\frac{n-2}{6d}\right] + 1. \tag{7.10}$$

Finalmente, usando $x - 1 < [x] \leq x$ en (7.10) se obtiene

$$\left| g_1(n,d) - \frac{n-2}{6d} \right| \leq 1. \tag{7.11}$$

Queremos ahora acotar el número de sumandos en (7.4). Para ello vamos ahora a utilizar el siguiente lema cuya prueba se encuentra en [**9**], pág. 394.

LEMA 7.3. *Existe $n_3 \in \mathbb{N}$ tal que si $n \geq n_3$ entonces*

$$\omega(n) < 2\frac{\ln(n)}{\ln(\ln(n))}.$$

Para calcular la cantidad de sumandos no nulos en (7.4) debemos calcular $\sharp\{d \in \mathbb{N} \,:\, d|a \text{ y } \mu(d) \neq 0\}$. Ahora, $\mu(d) \neq 0$ si y sólo si, d no contiene primos al cuadrado en su factorización, i.e. $d = \prod_{i=1}^{r} p_i^{\beta_i}$ con $\beta_i = 0, 1$. Luego

$$\begin{aligned}\sharp\{d \in \mathbb{N} \,:\, d|a \text{ y } \mu(d) \neq 0\} &= \sharp\{d \in \mathbb{N} \,:\, d|a \text{ y } d = \prod_{i=1}^{r} p_i^{\beta_i} \text{ con } \beta_i = 0,1\} \\ &= 2^{\omega(a)}.\end{aligned}$$

OBSERVACIÓN 7.1. *Sea $n_3 \in \mathbb{N}$ dado por el Lema 7.3. Podemos suponer que $n_3 \geq e^e$ ya que si $n_3 < e^e$, como el Lema 7.3 vale para todo $n \geq n_3$ en particular vale para todo $n \geq e^e$.*

OBSERVACIÓN 7.2. *La función $h(x) = \frac{\ln(x)}{\ln(\ln(x))}$ $(x > 1)$, es creciente en $(e^e, +\infty)$. Luego si $e^e \leq n_3 \leq a \leq n$ se tiene que*

$$\frac{\ln(a)}{\ln(\ln(a))} \leq \frac{\ln(n)}{\ln(\ln(n))}.$$

OBSERVACIÓN 7.3. *Afirmamos que si $n > 2n_3$ y $a \leq n$ entonces $\omega(a) < 2\frac{\ln(n)}{\ln(\ln(n))}$.*

En efecto, si $a \geq n_3$ es inmediato a partir del Lema 7.3 y de la monotonía dada por la Observación 7.2. Si $a < n_3$, existe $c \in \mathbb{N}$ tal que $n_3 < ac < 2n_3$ con lo cual $\omega(a) \leq \omega(ac) < 2\frac{\ln(ac)}{\ln(\ln(ac))} < 2\frac{\ln(n)}{\ln(\ln(n))}$.

Como consecuencia de las observaciones 7.1, 7.2 y 7.3 tenemos que si $n > 2n_3$ y $a < n$, entonces

$$\sharp\{d \in \mathbb{N} \ : \ d|a \text{ y } \mu(d) \neq 0\} = 2^{\omega(a)} < 2^{2\frac{\ln(n)}{\ln(\ln(n))}}$$

Usemos este hecho y la cota para g_1 obtenida en (7.11) para acotar el cardinal de B. Por (7.4) tenemos

$$\begin{aligned}
\sharp B &= \sum_{d|a} \mu(d) g_1(n,d) \\
&= \sum_{d|a,\ \mu(d)>0} \mu(d) g_1(n,d) + \sum_{d|a,\ \mu(d)<0} \mu(d) g_1(n,d) \\
&= \qquad\qquad I \qquad\quad + \qquad\qquad II.
\end{aligned}$$

Acotemos primero I. Por (7.11) tenemos, si $\mu(d) > 0$,

$$\mu(d) g_1(n,d) \geq \mu(d)\frac{n-2}{6d} - \mu(d).$$

Entonces, como $\mu(d) = 1$ si $\mu(d) > 0$,

$$\begin{aligned}
I &= \sum_{d|a,\ \mu(d)>0} \mu(d) g_1(n,d) \\
&\geq \sum_{d|a,\ \mu(d)>0} \Big(\mu(d)\frac{n-2}{6d} - \mu(d)\Big) \qquad (7.12) \\
&= \frac{n-2}{6} \sum_{d|a,\ \mu(d)>0} \frac{\mu(d)}{d} - \sum_{d|a,\ \mu(d)>0} 1.
\end{aligned}$$

Para acotar II se razona de manera análoga. Por (7.11) se tiene, si $\mu(d) < 0$,

$$\mu(d) g_1(n,d) \geq \mu(d)\frac{n-2}{6d} + \mu(d).$$

Con lo cual, como $\mu(d) = -1$ si $\mu(d) < 0$,

$$\begin{aligned}
II &= \sum_{d|a,\ \mu(d)<0} \mu(d) g_1(n,d) \\
&\geq \sum_{d|a,\ \mu(d)<0} \Big(\mu(d)\frac{n-2}{6d} + \mu(d)\Big) \qquad (7.13) \\
&= \frac{n-2}{6} \sum_{d|a,\ \mu(d)<0} \frac{\mu(d)}{d} - \sum_{d|a,\ \mu(d)<0} 1.
\end{aligned}$$

Luego, por (7.12) y (7.13) obtenemos

$$I + II \geq \frac{n-2}{6} \sum_{d|a,\ \mu(d)\neq 0} \frac{\mu(d)}{d} - \sum_{d|a,\ \mu(d)\neq 0} 1.$$

Por otro lado,

$$\sum_{d|a,\ \mu(d)\neq 0} 1 = \sharp\{d \in \mathbb{Z} \ :\ d|a \text{ y } \mu(d) \neq 0\} = 2^{\omega(a)} < 2^{\frac{2\ln(n)}{\ln(\ln(n))}},$$

luego

$$I + II \geq \frac{n-2}{6} \sum_{d|a,\ \mu(d)\neq 0} \frac{\mu(d)}{d} - 2^{\frac{2\ln(n)}{\ln(\ln(n))}}.$$

Recordemos que, por lo visto en la sección de funciones aritméticas,

$$\frac{\phi(a)}{a} = \sum_{d|a} \frac{\mu(d)}{d},$$

con lo cual nos queda

$$I + II \geq \frac{n-2}{6}\frac{\phi(a)}{a} - 2^{\frac{2\ln(n)}{\ln(\ln(n))}}.$$

Recordemos ahora, que $\frac{\phi(a)}{a} \geq \frac{1}{t}$. Finalmente obtenemos

$$\sharp B \geq \frac{n-2}{6t} - 2^{\frac{2\ln(n)}{\ln(\ln(n))}}.$$

Veamos ahora que, si n es suficientemente grande, se tiene que

$$\frac{n-2}{6t} - 2^{\frac{2\ln(n)}{\ln(\ln(n))}} \geq \frac{n}{7t}. \tag{7.14}$$

En efecto, (7.14) es equivalente a

$$n \geq 42\, t\, 2^{\frac{2\ln(n)}{\ln(\ln(n))}} + 14.$$

Como $t = \frac{1}{c_4}\ln(\ln(\frac{2n}{s_1}))$, (7.14) resulta equivalente a

$$n \geq \frac{42}{c_4} \ln\left(\ln\left(\frac{2n}{s_1}\right)\right) 2^{\frac{2\ln(n)}{\ln(\ln(n))}} + 14. \tag{7.15}$$

Acotemos:

- Se puede ver que si $n \geq e^{e^8}$, entonces
$$2^{\frac{2\ln(n)}{\ln(\ln(n))}} \leq \sqrt[4]{n}$$
- también para n grande y usando $s_1 \geq 1$, así $\frac{2n}{s_1} \leq 2n$, se puede demostrar
$$\frac{42}{c_4} \ln\left(\ln\left(\frac{2n}{s_1}\right)\right) \leq \sqrt[4]{n}.$$
- y además si $n \geq 28$, tenemos $14 \leq \frac{n}{2}$

Luego, juntando estas tres cotas tenemos que para n suficientemente grande

$$\frac{42}{c_4}\ln\left(\ln\left(\frac{2n}{s_1}\right)\right)2^{\frac{2\ln(n)}{\ln(\ln(n))}}+14\leq\sqrt[4]{n}\sqrt[4]{n}+\frac{n}{2}\leq n.$$

Lo que prueba entonces que (7.15) vale.

Hemos entonces demostrado el siguiente lema.

LEMA 7.4. *Con las notaciones del Lema 7.2, se tiene*

$$\sharp B\geq\frac{n}{7t}$$

donde t viene dado por (7.1)*, para todo n suficientemente grande.*

Vamos ahora a tratar de controlar

$$\sharp(B\cap A)=\sharp\{b\in I_n\ :\ b\equiv 2\ (6),\ (b,a)=1\text{ y }b\in A\}.$$

Para ello necesitamos las siguientes definiciones: Teníamos

$$\begin{aligned}s_1&=\sharp A(6,1)=\sharp\{b\in A\ :\ b\equiv 1\ (6)\},\\ s_2&=\sharp A(6,5)=\sharp\{b\in A\ :\ b\equiv 5\ (6)\}.\end{aligned}$$

Definimos

$$\begin{aligned}s_3&=\sharp A(6,0)=\sharp\{b\in A\ :\ b\equiv 0\ (6)\},\\ s_4&=\sharp A(6,2)=\sharp\{b\in A\ :\ b\equiv 2\ (6)\},\\ s_5&=\sharp A(6,3)=\sharp\{b\in A\ :\ b\equiv 3\ (6)\},\\ s_6&=\sharp A(6,4)=\sharp\{b\in A\ :\ b\equiv 4\ (6)\},\end{aligned}$$

y también

$$\begin{aligned}s'_1&=\sharp\{b\in I_n\setminus A\ :\ b\equiv 1\ (6)\},\\ s'_2&=\sharp\{b\in I_n\setminus A\ :\ b\equiv 5\ (6)\},\\ s'_3&=\sharp\{b\in I_n\setminus A\ :\ b\equiv 0\ (6)\},\\ s'_4&=\sharp\{b\in I_n\setminus A\ :\ b\equiv 2\ (6)\},\\ s'_5&=\sharp\{b\in I_n\setminus A\ :\ b\equiv 3\ (6)\},\\ s'_6&=\sharp\{b\in I_n\setminus A\ :\ b\equiv 4\ (6)\}.\end{aligned}$$

Resulta, claramente, que $\sharp A=s_1+s_2+s_3+s_4+s_5+s_6$ y recordando $f(n,2)=\sharp\{m\leq n\ :\ 2|m\text{ o }3|m\}$ podemos escribir $f(n,2)=s_3+s_4+s_5+s_6+s'_3+s'_4+s'_5+s'_6$. Ahora tenámos, por hipótesis, que $\sharp A>f(n,2)$. Entonces resulta que

$$s_1+s_2>s'_3+s'_4+s'_5+s'_6\geq s'_4. \tag{7.16}$$

Si llamamos $A'=I_n\setminus A$, tenemos

$$B=(B\cap A)\uplus(B\cap A')$$

y, tomando cardinal, nos queda

$$\sharp B = \sharp(B \cap A) + \sharp(B \cap A').$$

Por otro lado, tenemos

$$\sharp(B \cap A') \leq s_4'. \tag{7.17}$$

Entonces, por (7.17) y (7.16) nos queda

$$\sharp(B \cap A) = \sharp B - \sharp(B \cap A') \geq \sharp B - s_4' \geq \sharp B - (s_1 + s_2).$$

Finalmente, usando el Lema 7.4, nos queda

$$\sharp(B \cap A) \geq \frac{n}{7t} - (s_1 + s_2).$$

Veamos que, si c_1 es suficientemente pequeño, tenemos

$$\frac{n}{7t} - (s_1 + s_2) \geq \frac{n}{8t}. \tag{7.18}$$

En efecto, (7.18) es equivalente a

$$t \leq \frac{n}{(s_1 + s_2)\,56},$$

y, recordando (7.1),

$$\frac{1}{c_4} \ln\left(\ln\left(\frac{2n}{s_1}\right)\right) \leq \frac{n}{(s_1 + s_2)\,56}. \tag{7.19}$$

La desigualdad (7.19) es una consecuencia de la siguiente observación:

Observación 7.4. *Existe $k_2 > 0$ tal que para todo $x \geq k_2$,*

$$\frac{1}{c_4} \ln(\ln(2x)) \leq \sqrt{\frac{x}{2 \cdot 56}}.$$

La demostración de la Observación 7.4 es evidente.

Ahora, la desigualdad (7.19) estará demostrada, si vemos que $\frac{n}{s_1} \geq k_2$ puesto que, en ese caso, tendríamos

$$t = \frac{1}{c_4} \ln\left(\ln\left(\frac{2n}{s_1}\right)\right) \leq \sqrt{\frac{n}{2s_1 \cdot 56}} \leq \sqrt{\frac{n}{(s_1 + s_2)\,56}} \leq \frac{n}{(s_1 + s_2)\,56}. \tag{7.20}$$

ya que $\frac{n}{(s_1+s_2)\,56} \geq \frac{1}{c_1\,56} \geq 1$ si c_1 es pequeño.

Veamos que efectivamente $\frac{n}{s_1} \geq k_2$. Si c_1 es pequeño ($c_1 \leq \frac{1}{k_2}$), se tiene

$$s_1 \leq s_1 + s_2 \leq c_1 n \leq \frac{n}{k_2},$$

como queríamos.

Hemos demostrado el siguiente lema

LEMA 7.5. *Con las notaciones del Lema 7.2, se tiene*

$$\sharp(B \cap A) \geq \frac{n}{8t}$$

donde t viene dado por (7.1)*, para todo n suficientemente grande, si c_1 es pequeño.*

Tomemos ahora

$$t' = \frac{1}{c_4} \ln\left(\ln\left(\frac{2n}{\frac{n}{8t}}\right)\right), \tag{7.21}$$

resulta entonces que $t > t'$. En efecto,usando (7.18),

$$s_1 \leq s_1 + s_2 \leq \frac{n}{7t} - \frac{n}{8t} < \frac{n}{8t},$$

luego

$$\frac{2n}{s_1} > \frac{2n}{\frac{n}{8t}},$$

lo que implica

$$t = \frac{1}{c_4} \ln\left(\ln\left(\frac{2n}{s_1}\right)\right) > \frac{1}{c_4} \ln\left(\ln\left(\frac{2n}{\frac{n}{8t}}\right)\right) = t'.$$

Volvemos ahora a aplicar el Lema 7.1 con t' para obtener

$$\sharp\Big\{k \in I_n \ : \ \frac{\phi(k)}{k} < \frac{1}{t'}\Big\} < \frac{n}{16t}. \tag{7.22}$$

Ahora,

$$\begin{aligned} B \cap A = &\left((B \cap A) \cap \Big\{k \in I_n \ : \ \frac{\phi(k)}{k} < \frac{1}{t'}\Big\}\right) \\ &\uplus \left((B \cap A) \cap \Big\{k \in I_n \ : \ \frac{\phi(k)}{k} \geq \frac{1}{t'}\Big\}\right) \\ =&\bar{A}_1 \uplus \bar{A}_2. \end{aligned}$$

Tomando cardinal nos queda

$$\sharp(B \cap A) = \sharp\bar{A}_1 + \sharp\bar{A}_2,$$

pero, usando el Lema 7.5 y (7.22), se obtiene

$$\sharp\bar{A}_2 = \sharp(B \cap A) - \sharp\bar{A}_1 > \frac{n}{8t} - \frac{n}{16t} = \frac{n}{16t}.$$

Y resulta que $\frac{n}{16t} \geq 1$ para n suficientemente grande, ya que como $t = \frac{1}{c_4} \ln\left(\ln\left(\frac{2n}{s_1}\right)\right)$, es fácil ver que para n grande vale $n \geq 16\frac{1}{c_4} \ln\left(\ln\left(\frac{2n}{s_1}\right)\right)$

Luego existen por lo menos $\frac{n}{16t}$ enteros $b \in I_n$ tales que

$$b \equiv 2 \ (6), \quad b \in A, \quad (b, a) = 1 \quad \text{y} \quad \frac{\phi(b)}{b} \geq \frac{1}{t'} > \frac{1}{t}.$$

Elijamos b_1 alguno de esos enteros. Como $(b_1, a) = 1$ existe un "lazo" entre a y b_1.

Tomemos ahora $t'' = \frac{1}{c_4}\ln(\ln(\frac{1}{c_1}))$. Aplicando el Lema 7.1 con t'', obtenemos que el número de enteros $k \in I_n$ tales que $\frac{\phi(k)}{k} < \frac{1}{t''}$ es a lo sumo nc_1. Entonces

$$\begin{aligned} A(6,2) =& \left(A(6,2) \cap \left\{ k \in I_n \ : \ \frac{\phi(k)}{k} < \frac{1}{t''} \right\} \right) \\ & \uplus \left(A(6,2) \cap \left\{ k \in I_n \ : \ \frac{\phi(k)}{k} \geq \frac{1}{t''} \right\} \right) \\ =& A^1(6,2) \uplus A^2(6,2). \end{aligned}$$

Tomando cardinal, nos queda

$$\sharp A^2(6,2) = \sharp A(6,2) - \sharp A^1(6,2),$$

pero $A^1(6,2) \subset \left\{ k \in I_n \ : \ \frac{\phi(k)}{k} < \frac{1}{t''} \right\}$, luego $\sharp A^1(6,2) < nc_1$.

Por lo tanto, tenemos que

$$\sharp A^2(6,2) \geq \sharp A(6,2) - nc_1. \tag{7.23}$$

Controlemos ahora $\sharp A(6,2)$. Resulta que

$$\sharp I_n(6,2) = s_4 + s_4',$$

entonces, por (7.16), tenemos

$$s_4 = \sharp A(6,2) = \sharp I_n(6,2) - s_4' \geq \sharp I_n(6,2) - (s_1 + s_2).$$

Con lo cual, por (7.23) y dado que $s_1 + s_2 \leq c_1 n$, se tiene

$$\sharp A^2(6,2) \geq \sharp I_n(6,2) - 2c_1 n. \tag{7.24}$$

Veamos ahora que $\sharp I_n(6,2) = \left[\frac{n-2}{6}\right] + 1$. En efecto

$$\begin{aligned} \sharp I_n(6,2) &= \sharp \left\{ b \in I_n \ : \ b \equiv 2 \ (6) \right\} \\ &= \sharp \left\{ t \in \mathbb{Z} \ : \ 1 \leq 6t + 2 \leq n \right\} \\ &= \sharp \left\{ t \in \mathbb{Z} \ : \ -\frac{1}{6} \leq t \leq \frac{n-2}{6} \right\} \\ &= \left[\frac{n-2}{6} \right] + 1. \end{aligned}$$

Finalmente, de (7.24) obtenemos

$$\sharp A^2(6,2) \geq \left[\frac{n-2}{6} \right] + 1 - 2c_1 n.$$

Ahora, es fácil ver que, si n es suficientemente grande y c_1 es pequeño ($n \geq 28$ y $c_1 \leq \frac{1}{168}$) se tiene

$$\left[\frac{n-2}{6} \right] + 1 - 2c_1 n \geq \frac{n}{7}.$$

Luego obtenemos

$$\sharp A^2(6,2) = \sharp \left(A(6,2) \cap \left\{ k \in I_n \ : \ \frac{\phi(k)}{k} \geq \frac{1}{t''} \right\} \right) \geq \frac{n}{7},$$

si $n \geq 28$ y $c_1 \leq \frac{1}{168}$.

Ahora si $c_2 < \frac{1}{7}$ (donde c_2 es la dada por el Teorema 6.2), tenemos $c_2 n < \frac{n}{7}$, luego como l es $l \leq c_2 n < \frac{n}{7}$. Entonces podemos elegir $l-1$ elementos distintos en $A^2(6,2)$.

Elegimos entonces $b_2, b_3, \ldots, b_l \in A^2(6,2)$ distintos.

Hasta ahora para la construcción de nuestro $2l+1-ciclo$, tenemos elegidos $a, b_1, b_2, b_3, \ldots, b_l$, tales que :

- $a \in A(6,1)$ con $\phi(a)$ relativamente grande
- $b_1 \in A(6,2)$ tal que $(b_1, a) = 1$ con $\phi(b_1)$ relativamente grande también.
- los restantes b_i para $i = 2, ...l$ los elegimos en $b_i \in A^2(6,2)$

Luego definimos $b_{l+1} = a$ y llamamos $e_i := [b_i, b_{i+1}]$, $i = 1, \ldots, l$.

Ahora debemos construir un conjunto donde elegir los restantes $f_1, \ldots, f_l$ elementos de tal manera que la secuencia

$$a,\ b_1,\ f_1,\ b_2,\ f_2, \ldots,\ b_l,\ f_l$$

forme un C_{2l+1} ciclo contenido en $G(A)$ Para esto necesitamos que f_i verifique que $(b_i, f_i) = 1$ y también que $(f_i, b_{i+1}) = 1$. Este hecho queda garantizado si elegimos f_i tales que $(f_i, e_i) = 1$ Pues si $p|b_i$ entonces $p|e_i$, luego si tenemos $(f_i, e_i) = 1$, entonces $p \not| f_i$, con lo cual vale $(b_i, f_i) = 1$. De la misma manera se puede ver $(f_i, b_{i+1}) = 1$.

Construimos entonces el siguiente conjunto:

$$C_i = \{b \in I_n :\ b \equiv 3\ (6) \text{ y } (b, e_i) = 1\}.$$

Análogamente al Lema 7.2 se tiene

LEMA 7.6. *Si* $C_i = \{b \in I_n :\ b \equiv 3\ (6)\ y\ (b, e_i) = 1\}$. *Entonces se tiene*

$$\sharp C_i = \sum_{d|e_i} \mu(d) g_2(n, d),$$

donde $g_2(n,d) = \sharp\{b \in I_n\ :\ b \equiv 3\ (6)\ y\ d|b\}$.

DEMOSTRACIÓN. La idea es similar a la prueba del Lema 7.2. Definimos

$$\beta_i(m) = \sharp\{b \in I_n :\ b \equiv 3\ (6) \text{ y } m(b, e_i) = e_i\}.$$

Con esta definición, se tiene que $\beta_i(e_i) = \sharp C_i$.

Razonando igual que en el Lema 7.2 se tiene que

$$g_2(n,d) = \sharp\{b \in I_n\ :\ b \equiv 3\ (6) \text{ y } e_i | \frac{be_i}{d}\}.$$

Luego, si definimos

$$\alpha_i(m) = \sharp\{b \in I_n\ :\ b \equiv 3\ (6) \text{ y } e_i | mb\},$$

tenemos que $\alpha_i(\frac{e_i}{d}) = g_2(n,d)$.

Entonces, si vemos que

$$\alpha_i(m) = \sum_{d|m} \beta_i(d), \tag{7.25}$$

por la fórmula de inversión, obtendríamos

$$\beta_i(m) = \sum_{d|m} \mu(d)\alpha_i(\frac{m}{d}),$$

que evaluando en e_i da

$$\sharp C_i = \beta_i(e_i) = \sum_{d|e_i} \mu(d)\alpha_i(\frac{e_i}{d}) = \sum_{d|e_i} \mu(d) g_2(n,d),$$

como queremos demostrar en este lema.

Afirmamos que vale la siguiente igualdad de conjuntos,

$$\{b \in I_n \ : \ b \equiv 3 \ (6) \text{ y } e_i | mb\} = \biguplus_{d|m} \{b \in I_n \ : \ b \equiv 3 \ (6) \text{ y } d(e_i, b) = e_i\}. \tag{7.26}$$

En efecto, si $b \in I_n$ es tal que $b \equiv 3 \ (6)$ y $d(e_i, b) = e_i$ para algún d divisor de m, tenemos $m = dq$, entonces $mb = dqb$. Por otro lado, $b = (b, e_i)t$, entonces

$$mb = dq(b, e_i)t = e_i qt,$$

con lo cual $e_i | mb$.

Recíprocamente, sea $b \in I_n$ tal que $b \equiv 3 \ (6)$ y $e_i | mb$. Ahora $e_i = (e_i, b)q$ y como $e_i | mb$ se tiene que

$$q = \frac{e_i}{(e_i, b)} \Big| \frac{mb}{(e_i, b)}.$$

Ahora

$$\Big(\frac{e_i}{(e_i, b)}, \frac{b}{(e_i, b)}\Big) = 1,$$

entonces $q|m$ y cumple $q(e_i, b) = e_i$.

Hemos demostrado (7.26). Finalmente, tomando ahora cardinal en (7.26), obtenemos (7.25).

Esto finaliza la demostración. □

Observemos que como $b_i \in A(6, 2)$, tenemos que $b_i = 6v_i + 2$ para algún $v_i \in \mathbb{Z}$. Con lo cual $2|b_i$ y $3 \not| b_i$.

Ahora, vamos a tratar de acotar g_2 usando las mismas ideas que se usaron para acotar g_1. Recordemos que para d divisor de e_i

$$g_2(n, d) = \sharp\{b \in I_n \ : \ b \equiv 3 \ (6) \text{ y } d|b\} = \sharp\{b \in I_n \ : \ b \equiv 3 \ (6) \text{ y } b \equiv 0 \ (d)\}.$$

Luego debemos resolver el sistema

$$\begin{cases} b \equiv 3 \ (6), \\ b \equiv 0 \ (d). \end{cases}$$

Este sistema tendrá solución o no dependiendo de $(6, d)$. Más aún, por el Teorema Chino del Resto, el sistema tiene solución si y sólo si $(6, d)|3$.

Calculemos entonces $(6, d)$. Como d es un divisor de $e_i = [b_i, b_{i+1}]$ y como $2|b_i$ y $b_i|e_i$ para todo $i = 1, \ldots, l$, entonces $2|e_i$. Luego, d que es un divisor de e_i podría ser par o impar, pero si $2|d$, se tendría $(6, d) \neq 1$ y a demás $(6, d) \neq 3$, ya que $3 \not| d$. Pues si $3|d$, entonces $3|e_i = [b_i, b_i + 1]$, pero al ser 3 primo se tiene que $3|b_i$ o $3|b_{i+1}$ lo que es un absurdo seguún la observación anterior con lo cual el sistema no tendría solución.

Es decir, si d es par, $g_2(n, d) = 0$.

Ahora, si d es impar, los posibles valores de $(6, d)$ son 1 o 3. Pero como se dijo antes $3 \not| d$. Luego $(6, d) = 1$ y el sistema tiene solución única $b_0 \in [0, 6d)$ y todas las soluciones son de la forma $b = b_0 + k6d$ con $k \in \mathbb{Z}$. En conclusión, si d es impar,

$$g_2(n, d) = \sharp\{k \in \mathbb{Z} \ : \ 1 \leq b_0 + k6d \leq n\}.$$

Veamos ahora que

$$\{k \in \mathbb{Z} \ : \ 0 \leq k \leq \frac{n-3}{6d} - 1\} \subset \{k \in \mathbb{Z} \ : \ 1 \leq b_0 + k6d \leq n\} \tag{7.27}$$

y

$$\{k \in \mathbb{Z} \ : \ 1 \leq b_0 + k6d \leq n\} \subset \{k \in \mathbb{Z} \ : \ 0 \leq k \leq \frac{n-3}{6d}\}. \tag{7.28}$$

En efecto, si $0 \leq k \leq \frac{n-3}{6d} - 1$, entonces

$$1 \leq b_0 \leq b_0 + k6d \leq b_0 + n - 3 - 6d < n - 3 < n,$$

lo que prueba (7.27).

Por otro lado, si $1 \leq b_0 + k6d \leq n$, entonces

$$-1 < \frac{1}{6d} - 1 < \frac{1}{6d} - \frac{b_0}{6d} = \frac{1 - b_0}{6d} \leq k \leq \frac{n - b_0}{6d} \leq \frac{n-3}{6d},$$

pues $b_0 \geq 3$, lo que prueba (7.28).

Tomando cardinal en (7.27) – (7.28) obtenemos

$$\left[\frac{n-3}{6d}\right] \leq g_2(n, d) \leq \left[\frac{n-3}{6d}\right] + 1,$$

que, usando $[x] \leq x < [x] + 1$ implica

$$\frac{n-3}{6d} - 1 \leq g_2(n, d) \leq \frac{n-3}{6d} + 1.$$

O sea

$$-1 \leq g_2(n, d) - \frac{n-3}{6d} \leq 1.$$

Llamemos $\varepsilon = g_2(n, d) - \frac{n-3}{6d}$. Tenemos entonces $g_2(n, d) = \frac{n-3}{6d} + \varepsilon$ con $|\varepsilon| \leq 1$ para d impar.

Resumiendo, hemos probado el siguiente lema

LEMA 7.7. *Sea $g_2(n,d)$ la función definida en el Lema 7.6. Entonces se tiene*

$$g_2(n,d) = \begin{cases} 0 & \text{si } d \text{ es par} \\ \frac{n-3}{6d} + \varepsilon & \text{en otro caso,} \end{cases}$$

donde $|\varepsilon| \leq 1$.

Para estimar el cardinal de $C_i = \{b \in I_n \ : \ b \equiv 3 \ (6) \text{ y } (b, e_i) = 1\}$, de acuerdo a los Lemas 7.6 y 7.7 necesitamos estimar la cantidad de sumandos no nulos en

$$\sum_{d|e_i} \mu(d) g_2(n,d).$$

Es decir, queremos estimar

$$\sharp\{d \in \mathbb{N} \ : \ d|e_i \text{ y } \mu(d) \neq 0\}.$$

Ahora bien,

$$\begin{aligned} \sharp\{d \in \mathbb{N} \ : d|e_i \text{ y } \mu(d) \neq 0\} & \\ &= \sharp\{d \in \mathbb{N} \ : \ d|e_i \text{ y } d = \prod_{j=1}^{r} p_i^{\beta_i} \text{ con } 0 \leq \beta_i \leq 1\} \\ &= 2^{\omega(e_i)} \end{aligned} \tag{7.29}$$

Usando ahora la Observación 7.3, como $e_i \leq n^2$ (dado que $e_i = [b_i, b_{i+1}] \leq b_i b_{i+1} \leq n^2$) y $n^2 > n > 2n_3$, se obtiene:

$$\omega(e_i) \leq \frac{2\ln(n^2)}{\ln(\ln(n^2))} < \frac{4\ln(n)}{\ln(\ln(n))},$$

con lo cual

$$2^{\omega(e_i)} < 2^{\frac{4\ln(n)}{\ln(\ln(n))}}. \tag{7.30}$$

Luego,

$$\begin{aligned} \sharp C_i &= \sharp\{b \in I_n \ : \ b \equiv 3 \ (6) \text{ y } (b, e_i) = 1\} \\ &= \sum_{d|e_i} \mu(d) g_2(n,d) \\ &= \sum_{d|e_i, 2\not|d} \mu(d) g_2(n,d) \\ &= \sum_{d|e_i, 2\not|d, \mu(d)>0} \mu(d) g_2(n,d) + \sum_{d|e_i, \ 2\not|d, \mu(d)<0} \mu(d) g_2(n,d) \\ &= \qquad I \qquad + \qquad II. \end{aligned}$$

Acotemos primero I. Por el Lema 7.7, tenemos

$$\begin{aligned} I &= \sum_{d|e_i, 2\not|d, \mu(d)>0} \mu(d) g_2(n,d) \\ &\geq \sum_{d|e_i, 2\not|d, \mu(d)>0} \mu(d)\frac{n-3}{6d} - \mu(d) \\ &= \frac{n-3}{6} \sum_{d|e_i, 2\not|d, \mu(d)>0} \frac{\mu(d)}{d} - \sum_{d|e_i, 2\not|d, \mu(d)>0} 1. \end{aligned}$$

Acotemos ahora II. Por el Lema 7.7, obtenemos

$$\begin{aligned} II &= \sum_{d|e_i, 2\not|d, \mu(d)<0} \mu(d) g_2(n,d) \\ &\geq \sum_{d|e_i, 2\not|d, \mu(d)<0} \mu(d)\frac{n-3}{6d} + \mu(d) \\ &= \frac{n-3}{6} \sum_{d|e_i, 2\not|d, \mu(d)<0} \frac{\mu(d)}{d} - \sum_{d|e_i, 2\not|d, \mu(d)<0} 1. \end{aligned}$$

Juntando todo, nos queda

$$I + II \geq \frac{n-3}{6} \sum_{d|e_i, 2\not|d, \mu(d)\neq 0} \frac{\mu(d)}{d} - \sum_{d|e_i, 2\not|d, \mu(d)\neq 0} 1.$$

Por (7.29) y (7.30) sigue que

$$\begin{aligned} \sum_{d|e_i, 2\not|d, \mu(d)\neq 0} 1 &= \sharp\{d \in \mathbb{N} \ : \ d|e_i, \ 2 \not| d \text{ y } \mu(d) \neq 0\} \\ &\leq \sharp\{d \in \mathbb{N} \ : \ d|e_i \text{ y } \mu(d) \neq 0\} \\ &\leq 2^{\omega(e_i)} \\ &\leq 2^{\frac{4\ln(n)}{\ln(\ln(n))}}, \end{aligned}$$

de donde

$$I + II \geq \frac{n-3}{6} \sum_{d|e_i, 2\not|d, \mu(d)\neq 0} \frac{\mu(d)}{d} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}}. \tag{7.31}$$

Ahora, usamos la siguiente propiedad de las funciones aritméticas, demostrada en el capitulo 1, Observación 2.4, tenemos:

$$\frac{\phi(e_i)}{e_i} = \sum_{d|ei} \frac{\mu(d)}{d} \tag{7.32}$$

de la que se deduce la Proposición 2.8

$$\frac{\phi(e_i)}{e_i} = \prod_{p|e_i} (1 - \frac{1}{p}). \tag{7.33}$$

Ahora, como $\mu(d) = 0$ si $4|d$,

$$\begin{aligned}\frac{\phi(e_i)}{e_i} &= \sum_{d|ei} \frac{\mu(d)}{d} = \sum_{d|ei,\ 2|d} \frac{\mu(d)}{d} + \sum_{d|ei,\ 2\not|d} \frac{\mu(d)}{d} \\ &= \sum_{2k|ei,\ 2\not|k} \frac{\mu(2k)}{2k} + \sum_{d|ei,\ 2\not|d} \frac{\mu(d)}{d} \\ &= -\frac{1}{2} \sum_{2k|ei,\ 2\not|k} \frac{\mu(k)}{k} + \sum_{d|ei,\ 2\not|d} \frac{\mu(d)}{d} \\ &= -\frac{1}{2} \sum_{k|ei,\ 2\not|k} \frac{\mu(k)}{k} + \sum_{d|ei,\ 2\not|d} \frac{\mu(d)}{d} \\ &= \frac{1}{2} \sum_{d|ei,\ 2\not|d} \frac{\mu(d)}{d}\end{aligned}$$

Con lo cual, por (7.33),

$$2\prod_{p|e_i}(1-\frac{1}{p}) = \sum_{d|e_i,\ 2\not|d} \frac{\mu(d)}{d}$$

Observemos que

$$2\prod_{p|e_i}(1-\frac{1}{p}) = 2\prod_{p|e_i,\ p\neq 2}(1-\frac{1}{p})\cdot(1-\frac{1}{2}) = \prod_{p|e_i,\ p\neq 2}(1-\frac{1}{p})$$

de donde se obtiene

$$\prod_{p|e_i,\ p\neq 2}(1-\frac{1}{p}) = \sum_{d|e_i,\ 2\not|d} \frac{\mu(d)}{d}. \tag{7.34}$$

Ahora, como $e_i = [b_i; b_{i+1}]$,

$$\begin{aligned}\{p \text{ primo } :\ p|e_i\} =& \{p \text{ primo } :\ p|b_i\} \cup \{p \text{ primo } :\ p|b_{i+1}\} \\ =& \{p \text{ primo } :\ p|b_i \text{ y } p\not|b_{i+1}\} \cup \{p \text{ primo } :\ p\not|b_i \text{ y } p|b_{i+1}\} \\ & \cup \{p \text{ primo } :\ p|b_i \text{ y } p|b_{i+1}\} \quad \text{(unión disjunta)}\end{aligned}$$

Luego,

$$\prod_{p|e_i}(1-\frac{1}{p}) = \prod_{p|b_i,\ p\not|b_{i+1}}(1-\frac{1}{p}) \times \prod_{p|b_{i+1},\ p\not|b_i}(1-\frac{1}{p}) \times \prod_{p|b_{i+1},\ p|b_i}(1-\frac{1}{p}). \tag{7.35}$$

Ahora, resulta que como $1 - \frac{1}{p} \leq 1$, para todo p primo, entonces

$$\prod_{p|b_{i+1},\ p|b_i}(1-\frac{1}{p}) \leq 1$$

Luego

$$\prod_{p|b_{i+1}}(1-\frac{1}{p}) = \prod_{p|b_{i+1},\ p\not|b_i}(1-\frac{1}{p}) \times \prod_{p|b_{i+1},\ p|b_i}(1-\frac{1}{p}) \leq \prod_{p|b_{i+1},\ p\not|b_i}(1-\frac{1}{p}).$$

Con lo cual multiplicando a ambos miembros por $\prod_{p|b_i}(1-\frac{1}{p})$, obtenemos

$$\prod_{p|b_i}(1-\frac{1}{p}) \times \prod_{p|b_{i+1}}(1-\frac{1}{p}) \leq \prod_{p|b_{i+1},\ p\not|b_i}(1-\frac{1}{p}) \times \prod_{p|b_i}(1-\frac{1}{p}),$$

Más precisamente, desarrollando el segundo miembro obtenemos:

$$\prod_{p|b_i}(1-\frac{1}{p}) \times \prod_{p|b_{i+1}}(1-\frac{1}{p}) \leq \prod_{p|b_{i+1},\ p\not|b_i}(1-\frac{1}{p}) \times \prod_{p|b_i,\ p\not|b_{i+1}}(1-\frac{1}{p}) \times \prod_{p|b_i,\ p|b_{i+1}}(1-\frac{1}{p}).$$

Luego, por (7.35), tenemos

$$\prod_{p|b_i}(1-\frac{1}{p}) \times \prod_{p|b_{i+1}}(1-\frac{1}{p}) \leq \prod_{p|e_i}(1-\frac{1}{p}). \tag{7.36}$$

Ahora, volviendo a la ecuación (7.31), tenemos, por (7.34)

$$I + II \geq \frac{n-3}{6} \sum_{d|e_i, 2\not|d, \mu(d)\neq 0} \frac{\mu(d)}{d} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}}$$

$$= \frac{n-3}{6} \prod_{p|e_i,\ p\neq 2}(1-\frac{1}{p}) - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} \tag{7.37}$$

Por otra parte, tenemos

$$\prod_{p|e_i,\ p\neq 2}(1-\frac{1}{p}) \geq \prod_{p|e_i}(1-\frac{1}{p}) \tag{7.38}$$

pues

$$\begin{aligned}\prod_{p|e_i}(1-\frac{1}{p}) &= (1-\frac{1}{2}) \times \prod_{p|e_i,\ p\neq 2}(1-\frac{1}{p}) \\ &= \frac{1}{2} \times \prod_{p|e_i,\ p\neq 2}(1-\frac{1}{p}) \\ &\leq \prod_{p|e_i,\ p\neq 2}(1-\frac{1}{p}).\end{aligned}$$

Luego, por (7.38), (7.36) y (7.33) tenemos

$$\begin{aligned}\frac{n-3}{6}\prod_{p|e_i,\ p\neq 2}(1-\frac{1}{p})-2^{\frac{4\ln(n)}{\ln(\ln(n))}} &\geq \frac{n-3}{6}\prod_{p|e_i}(1-\frac{1}{p})-2^{\frac{4\ln(n)}{\ln(\ln(n))}}\\ &\geq \frac{n-3}{6}\prod_{p|b_i}(1-\frac{1}{p})\times\prod_{p|b_{i+1}}(1-\frac{1}{p})-2^{\frac{4\ln(n)}{\ln(\ln(n))}}\\ &= \frac{n-3}{6}\frac{\phi(b_i)}{b_i}\frac{\phi(b_{i+1})}{b_{i+1}}-2^{\frac{4\ln(n)}{\ln(\ln(n))}}.\end{aligned}$$

Volviendo a (7.37) nos queda

$$I+II\geq \frac{n-3}{6}\frac{\phi(b_i)}{b_i}\frac{\phi(b_{i+1})}{b_{i+1}}-2^{\frac{4\ln(n)}{\ln(\ln(n))}}. \tag{7.39}$$

Ahora, por otra parte,

$$\begin{aligned}&\sharp\{b\in I_n\ :\ b\equiv 3\ (6)\text{ y }(b,e_i)=1\}\\ &\quad=\sharp\{b\in I_n\ :\ b\equiv 3\ (6)\ ;\ (b,e_i)=1\ ;\ b\in A\}\\ &\qquad+\sharp\{b\in I_n\ :\ b\equiv 3\ (6)\ ;\ (b,e_i)=1\ ;\ b\notin A\}\end{aligned}$$

y tenemos:

$$\sharp\{b\in I_n\ :\ b\equiv 3\ (6)\ ;\ (b,e_i)=1\ ;\ b\notin A\}\leq\sharp\{b\in I_n\setminus A\ :\ b\equiv 3\ (6)\}=s_5'.$$

Por lo tanto

$$\begin{aligned}&\sharp\{b\in I_n\ :\ b\equiv 3\ (6)\ ;\ (b,e_i)=1\ ;\ b\in A\}\\ &\qquad\geq\sharp\{b\in I_n\ :\ b\equiv 3\ (6)\text{ y }(b,e_i)=1\}-s_5'.\end{aligned}$$

Pero, según (7.16)

$$s_1+s_2>s_3'+s_4'+s_5'+s_6'\geq s_5'$$

de donde

$$-s_5'\geq-(s_1+s_2).$$

Entonces

$$\begin{aligned}&\sharp\{b\in I_n\ :\ b\equiv 3\ (6)\ ;\ (b,e_i)=1\ ;\ b\in A\}\\ &\qquad\geq\sharp\{b\in I_n\ :\ b\equiv 3\ (6)\text{ y }(b,e_i)=1\}-(s_1+s_2).\end{aligned}$$

O lo que es lo mismo,

$$\begin{aligned}\sum_{\substack{u:\,6u+3\leq n,\,(6u+3,e_i)=1,\\ 6u+3\in A}}1 &\geq\sharp\{b\in I_n\ :\ b\equiv 3\ (6)\text{ y }(b,e_i)=1\}-(s_1+s_2)\\ &\geq\frac{n-3}{6}\ \frac{\phi(b_i)}{b_i}\ \frac{\phi(b_{i+1})}{b_{i+1}}-2^{\frac{4\ln(n)}{\ln(\ln(n))}}-(s_1+s_2)\end{aligned}$$

Acotemos ahora $\frac{\phi(b_i)}{b_i}$, para los distintos valores de i.

- Si $i = 1$, $\frac{\phi(b_1)}{b_1} \geq \frac{1}{t'}$ por la elección de b_1. Y por la elección de b_2, $\frac{\phi(b_2)}{b_2} \geq \frac{1}{t''}$

  Entonces nos queda

$$\sum_{\substack{u:\, 6u+3\leq n,\, (6u+3,e_1)=1,\\ 6u+3\in A}} 1 \geq \frac{n-3}{6}\ \frac{1}{t'}\ \frac{1}{t''} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} - (s_1+s_2).$$

  Ahora para n suficientemente grande,

$$\frac{n-3}{6}\ \frac{1}{t'}\ \frac{1}{t''} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} - (s_1+s_2) \geq \frac{n}{7tt''} - (s_1+s_2). \tag{7.40}$$

  En efecto, como $t > t'$, tenemos

$$\frac{n-3}{6}\ \frac{1}{t'}\ \frac{1}{t''} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} \geq \frac{n-3}{6}\ \frac{1}{t}\ \frac{1}{t''} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}}.$$

  Luego, (7.40) es una consecuencia de

$$\frac{n-3}{6}\ \frac{1}{t}\ \frac{1}{t''} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} \geq \frac{n}{7tt''}. \tag{7.41}$$

  Pero, (7.41) es equivalente a

$$\begin{aligned}
(\frac{n}{6} - \frac{1}{2})\frac{1}{tt''} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} - \frac{n}{7tt''} \geq 0 \quad &\Leftrightarrow \\
\frac{n}{6tt''} - \frac{n}{7tt''} \geq \frac{1}{2tt''} + 2^{\frac{4\ln(n)}{\ln(\ln(n))}} \quad &\Leftrightarrow \\
\frac{n}{42tt''} \geq \frac{1}{2tt''} + 2^{\frac{4\ln(n)}{\ln(\ln(n))}} \quad &\Leftrightarrow \\
n \geq 21 + 2^{\frac{4\ln(n)}{\ln(\ln(n))}} 42tt''
\end{aligned}$$

  Recordemos que $t = \frac{1}{c_4}\ln(\ln(\frac{2n}{s_1}))$ y $t'' = \frac{1}{c_4}\ln(\ln(\frac{1}{c_1}))$, de donde (7.41) resulta equivalente a

$$n \geq \left(2^{\frac{4\ln(n)}{\ln(\ln(n))}}\right)\left(\frac{42}{c_4^2}\ln(\ln(\frac{2n}{s_1}))\right)\left(\ln(\ln(\frac{1}{c_1}))\right) + 21 = ABC + D.$$

  Ahora, si $n \geq 42$ entonces $D \leq \frac{n}{2}$.

  Veremos que $A, B, C \leq \sqrt[6]{n}$ y luego $ABC \leq \sqrt{n}$.

  Es fácil ver que si $n \geq e^{e^{24}}$ entonces $A \leq \sqrt[6]{n}$. En efecto, si $n \geq e^{e^{24}}$, entonces $\ln(n) \geq e^{24}$, luego $\ln(\ln(n)) \geq 24$. De donde se obtiene

$$\frac{4\ln(n)}{\ln(\ln(n))} \leq \frac{4\ln(n)}{24} = \frac{1}{6}\ln(n).$$

  Luego

$$e^{\frac{4\ln(n)}{\ln(\ln(n))}} \leq e^{\frac{\ln(n)}{6}} = \sqrt[6]{n}$$

  Finalmente,

$$A = 2^{\frac{4\ln(n)}{\ln(\ln(n))}} \leq e^{\frac{4\ln(n)}{\ln(\ln(n))}} \leq \sqrt[6]{n}.$$

Veamos ahora que $B \leq \sqrt[6]{n}$. Como $s_1 \geq 1$, entonces $\frac{2n}{s_1} \leq 2n$ y luego $\ln(\ln(\frac{2n}{s_1})) \leq \ln(2n)$.Entonces

$$B = \frac{42}{c_4^2} \ln(\ln(\frac{2n}{s_1})) \leq \frac{42}{c_4^2} \ln(2n).$$

Luego, la afirmación es inmediata del hecho de que

$$\frac{42}{c_4^2} \ln(2n) \leq \sqrt[6]{n},$$

para n suficientemente grande.

Falta ver que $C \leq \sqrt[6]{n}$, donde $C = \ln(\ln(\frac{1}{c_1}))$.

Por hipótesis, se tiene $1 \leq s_1 + s_2 \leq c_1 n$, luego

$$\frac{1}{c_1} \leq n.$$

Entonces

$$C \leq \ln(\frac{1}{c_1}) \leq \ln(n) \leq \sqrt[6]{n},$$

si n es grande.

Juntando todos los cálculos,

$$ABC + D \leq \sqrt{n} + \frac{n}{2} \leq n,$$

para n grande. Hemos entonces demostrado (7.40).

Ahora, si tomamos c_1 pequeño, obtenemos

$$\frac{n}{7tt''} - (s_1 + s_2) \geq \frac{n}{8tt''}. \tag{7.42}$$

En efecto, (7.42) es equivalente a

$$\begin{aligned} \frac{n}{7tt''} - \frac{n}{8tt''} \geq s_1 + s_2 \quad &\Leftrightarrow \\ \frac{n}{56tt''} \geq s_1 + s_2 \quad &\Leftrightarrow \\ \frac{n}{56(s_1 + s_2)} \geq tt''. & \end{aligned}$$

Debemos ver

$$tt'' \leq \frac{n}{56(s_1 + s_2)} \tag{7.43}$$

Si c_1 es suficientemente pequeño, por (7.20),

$$t \leq \sqrt{\frac{n}{(s_1 + s_2)56}}.$$

Veamos ahora que

$$t'' \leq \sqrt{\frac{n}{(s_1 + s_2)56}}.$$

Pero

$$t'' = \frac{1}{c_4}\ln(\ln(\frac{1}{c_1})) \leq \frac{1}{c_4}\ln(\frac{1}{c_1}).$$

Ahora, como para x grande se tiene $\frac{1}{c_4}\ln(x) \leq \sqrt{\frac{x}{56}}$, sigue que

$$t'' \leq \frac{1}{c_4}\ln(\frac{1}{c_1}) \leq \sqrt{\frac{1}{56c_1}}$$

si c_1 es pequeño. Finalmente, usando que $s_1 + s_2 \leq c_1 n$ tenemos

$$t'' \leq \sqrt{\frac{1}{56c_1}} = \sqrt{\frac{n}{56c_1 n}} \leq \sqrt{\frac{n}{56(s_1+s_2)}}.$$

Hemos probado (7.43) con lo cual queda demostrada la desigualdad (7.42).

En conclusión, para el caso $i = 1$ obtenemos la cota

$$\begin{aligned} \sum_{\substack{u:\, 6u+3\leq n,\, (6u+3,e_1)=1,\\ 6u+3\in A}} 1 &\geq \frac{n-3}{6}\frac{1}{tt''} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} - (s_1+s_2) \\ &\geq \frac{n}{7tt''} - (s_1+s_2) \\ &\geq \frac{n}{8tt''} \end{aligned} \tag{7.44}$$

si n es suficientemente grande y c_1 suficientemente chico.

- Para $i = l$ nos queda:

$$\begin{aligned} &\sum_{\substack{u:\, 6u+3\leq n,(6u+3,e_l)=1,\\ 6u+3\in A}} 1 \\ &\geq \frac{n-3}{6}\ \frac{\phi(b_l)}{b_l}\ \frac{\phi(b_{l+1})}{b_{l+1}} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} - (s_1+s_2) \\ &= \frac{n-3}{6}\ \frac{\phi(b_l)}{b_l}\ \frac{\phi(a)}{a} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} - (s_1+s_2) \end{aligned}$$

Usando $\frac{\phi(b_l)}{b_l} \geq \frac{1}{t''}$ y $\frac{\phi(a)}{a} \geq \frac{1}{t}$, nos queda:

$$\sum_{\substack{u:\, 6u+3\leq n,(6u+3,e_l)=1,\\ 6u+3\in A}} 1 \geq \frac{n-3}{6}\ \frac{1}{t''}\ \frac{1}{t} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} - (s_1+s_2).$$

En conclusión, usando (7.41) y (7.42), como antes, para el caso $i = l$ obtenemos:

$$\begin{aligned}\sum_{\substack{u:\, 6u+3\le n,(6u+3,e_l)=1,\\ 6u+3\in A}} 1 &\ge \frac{n-3}{6}\frac{1}{tt''} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} - (s_1+s_2)\\ &\ge \frac{n}{7tt''} - (s_1+s_2)\\ &\ge \frac{n}{8tt''}\end{aligned} \tag{7.45}$$

si n es suficientemente grande y c_1 suficientemente chico.

- Si $1 < i < l$:
  Teníamos

$$\sum_{\substack{u:\, 6u+3\le n,(6u+3,e_i)=1,\\ 6u+3\in A}} 1 \ge \frac{n-3}{6}\,\frac{\phi(b_i)}{b_i}\,\frac{\phi(b_{i+1})}{b_{i+1}} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} - (s_1+s_2). \tag{7.46}$$

  Ahora si $2 \le i \le l-i$; $\frac{\phi(b_i)}{b_i} \ge \frac{1}{t''}$, por elección de b_i.
  Entonces la desigualdad (7.46) queda:

$$\ge \frac{n-3}{6}\,\frac{1}{t''}\,\frac{1}{t''} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} - (s_1+s_2).$$

  Veamos ahora que para n suficientemente grande vale:

$$\frac{n-3}{6}\,\frac{1}{(t'')^2} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} \ge \frac{n}{7(t'')^2}. \tag{7.47}$$

  Esto es equivalente a

$$\frac{n-3}{6}\,\frac{1}{(t'')^2} - \frac{n}{7(t'')^2} \ge 2^{\frac{4\ln(n)}{\ln(\ln(n))}}.$$

$$\Leftrightarrow$$

$$\frac{n}{6(t'')^2} - \frac{n}{7(t'')^2} \ge 2^{\frac{4\ln(n)}{\ln(\ln(n))}} + \frac{1}{2(t'')^2}$$

$$\Leftrightarrow$$

$$\frac{n}{42(t'')^2} \ge 2^{\frac{4\ln(n)}{\ln(\ln(n))}} + \frac{1}{2(t'')^2}$$

$$\Leftrightarrow$$

$$n \ge 2^{\frac{4\ln(n)}{\ln(\ln(n))}} 42(t'')^2 + 21$$

  pero $t'' = \frac{1}{c_4}\ln(\ln(\frac{1}{c_1}))$

  Luego la desigualdad que queremos ver resulta equivalente a

$$n \ge \left(2^{\frac{4\ln(n)}{\ln(\ln(n))}}\right)\left(\frac{42}{c_4^2}\left(\ln(\ln(\frac{1}{c_1}))\right)^2\right) + 21 = AB + C.$$

  Ahora si $n \ge 42$, entonces $C = 21 \le \frac{n}{2}$.

  Veamos que $A, B \le \sqrt[4]{n}$ así $AB + C \le \sqrt{n} + \frac{n}{2} \le n.$, para n grande.

Demostramos anteriormente que si $n \geq e^{e^{24}}$ entonces $A \leq \sqrt[6]{n}$. Usando este hecho tenemos entonces, $A \leq \sqrt[6]{n} \leq \sqrt[4]{n}$, para n grande.

Veamos ahora que $B < \sqrt[4]{n}$

En efecto, usando que $1 \leq c_1 n$ y $\ln(n) \leq n$, tenemos:

$$B = \frac{42}{c_4^2}\left(\ln(\ln(\frac{1}{c_1}))\right)^2 \leq \frac{42}{c_4^2}\left(\ln(\ln(n))\right)^2 \leq \frac{42}{c_4^2}\left(\ln(n)\right)^2.$$

Luego la afirmación es inmediata del hecho $\frac{42}{c_4^2}\left(\ln(n)\right)^2 \leq \sqrt[4]{n}$, para n suficientemente grande.

Luego tenemos $AB + C \leq \sqrt[4]{n}\sqrt[4]{n} + \frac{n}{2} \leq \sqrt{n} + \frac{n}{2} \leq n$, para n suficientemente grande.

Queda probada entonces la desigualdad (7.47), que decía:

$$\frac{n-3}{6}\ \frac{1}{(t'')^2} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}}\ \geq \frac{n}{7(t'')^2}.$$

Con lo cual

$$\frac{n-3}{6}\ \frac{1}{(t'')^2} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} - (s_1+s_2)\ \geq \frac{n}{7(t'')^2} - (s_1+s_2).$$

Veamos ahora

$$\frac{n}{7(t'')^2} - (s_1+s_2) \geq \frac{n}{8(t'')^2} \tag{7.48}$$

para n suficientemente grande y c_1 suficientemente chico. Ahora

$$\frac{n}{7(t'')^2} - (s_1+s_2) \geq \frac{n}{8(t'')^2}$$

$\Leftrightarrow$

$$\frac{n}{56(t'')^2} \geq (s_1+s_2)$$

$\Leftrightarrow$

$$\frac{n}{(s_1+s_2)56} \geq (t'')^2 \tag{7.49}$$

Veamos esto:

Para c_1 chico, tenemos para t'':

$$t'' = \frac{1}{c_4}\ln(\ln(\frac{1}{c_1})) \leq \frac{1}{c_4}\ln(\frac{1}{c_1}).$$

Ahora, como para x grande se tiene $\frac{1}{c_4}\ln(x) \leq \sqrt{\frac{x}{56}}$, sigue que

$$t'' \leq \frac{1}{c_4}\ln(\frac{1}{c_1}) \leq \sqrt{\frac{1}{56c_1}}$$

si c_1 es pequeño.

Finalmente, usando que $s_1 + s_2 \leq c_1 n$ tenemos

$$t'' \leq \sqrt{\frac{1}{56c_1}} = \sqrt{\frac{n}{56c_1 n}} \leq \sqrt{\frac{n}{56(s_1+s_2)}}.$$

Con lo cual obtenemos

$$(t'')^2 \leq \frac{n}{56(s_1+s_2)},$$

como queríamos ver en (7.49). Hemos probado entonces (7.48).

Juntando todo, (7.47), y (7.48), para $1 < i < l$, teníamos, según (7.46):

$$\begin{aligned} \sum_{\substack{u:\, 6u+3\leq n,\, (6u+3,e_i)=1,\\ 6u+3\in A}} 1 \geq \\ \frac{n-3}{6}\ \frac{\phi(b_i)}{b_i}\ \frac{\phi(b_{i+1})}{b_{i+1}} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} - (s_1+s_2) \geq \\ \frac{n-3}{6}\ \frac{1}{(t'')^2} - 2^{\frac{4\ln(n)}{\ln(\ln(n))}} - (s_1+s_2) \geq \\ \frac{n}{7(t'')^2} - (s_1+s_2) \geq \\ \frac{n}{8(t'')^2}. \end{aligned}$$

Todo esto con n suficientemente grande y c_1 suficientemente chico.

En conclusión para el caso $1 < i < l$ tenemos la siguiente cota:

$$\sum_{\substack{u:\, 6u+3\leq n,\, (6u+3,e_i)=1,\\ 6u+3\in A}} 1 \geq \frac{n}{8(t'')^2} \tag{7.50}$$

Para n suficientemente grande y c_1 suficientemente chico.

Veamos que si c_2 es suficientemente pequeño podemos elegir distintos f_i para $1 \leq i \leq l$, según los casos anteriores.

Para el caso $i = 1$ teníamos según (7.44)

$$\sum_{\substack{u:\, 6u+3\leq n,\, (6u+3,e_i)=1,\\ 6u+3\in A}} 1 \geq \frac{n}{8tt''}$$

y

$$\sharp\{u:\, 6u+3 \leq n,\, (6u+3,e_i)=1, 6u+3\in A\} = \sum_{\substack{u:\, 6u+3\leq n,\, (6u+3,e_i)=1,\\ 6u+3\in A}} 1$$

Veamos que $8tt'' \leq n$, así $\frac{n}{8tt''} \geq 1$ y por lo tanto podemos elegir un elemento en $\{u:\, 6u+3 \leq n,\, (6u+3,e_i)=1,\, 6u+3\in A\}$.

En efecto

$$8tt'' = 8\frac{1}{c_4}\ln(\ln(\frac{2n}{s_1}))\frac{1}{c_4}\ln(\ln(\frac{1}{c_1})).$$

Ahora como $s_1 \geq 1$,

$$\begin{aligned}\frac{2n}{s_1} &\leq 2n.\\ \ln(\frac{2n}{s_1}) &\leq \ln(2n) \leq n.\\ \ln(\ln(\frac{2n}{s_1})) &\leq \ln(2n) \leq 2\ln(n).\end{aligned}$$

Además, como

$$\begin{aligned}1 \leq nc_1 \ \Rightarrow \frac{1}{c_1} &\leq n\\ \ln(\frac{1}{c_1}) &\leq \ln(n) \leq n\\ \ln(\ln(\frac{1}{c_1})) &\leq \ln(n).\end{aligned}$$

Luego juntando todo, tenemos:

$$8tt'' = 8\frac{1}{c_4}\ln(\ln(\frac{2n}{s_1}))\frac{1}{c_4}\ln(\ln(\frac{1}{c_1})) \leq \frac{16}{c_4^2}\ln^2(n) \leq n$$

agrandando n si fuera necesario ya que la función $y = \ln^2(x)$, crece mas lento que la función $y = x$.

Entonces obtuvimos que $8tt'' \leq n$ y por lo tanto (7.44) queda:

$$\sum_{\substack{u:\, 6u+3\leq n,\, (6u+3,e_i)=1,\\ 6u+3\in A}} 1 \geq \frac{n}{8tt''} \geq 1$$

Entonces el conjunto

$$\{u :\, 6u+3 \leq n,\, (6u+3, e_i) = 1,\, 6u+3 \in A\}$$

tiene por lo menos un elemento.

Luego podemos entonces, elegir f_1 ahí. Es decir $f_1 \in \{b \in I_n \ : \ b \equiv 3\ (6)\ ;\ (b, e_i) = 1\ ;\ b \in A\}$

Por otro lado con $i = l$ teníamos la misma cota (7.45):

$$\sum_{\substack{u:\, 6u+3\leq n,\\ (6u+3,e_l)=1,\, 6u+3\in A}} 1 \geq \frac{n}{8tt''} \geq 1$$

Entonces, con el mismo argumento podemos elegir f_l ahí.

Es decir elegimos $f_l \in \{b \in I_n \ : \ b \equiv 3\ (6)\ ;\ (b, e_l) = 1\ ;\ b \in A\}$.

Veamos ahora como justificamos la existencia de los $l-2$ elementos restantes para construir el $2l+1-ciclo \subseteq G(A)$

Teníamos para $1 < i < l$:

$$\sum_{\substack{u:\, 6u+3\leq n,\, (6u+3,e_i)=1,\\ 6u+3\in A}} 1 \geq \frac{n}{8(t'')^2}$$

Veamos que si c_2 es suficientemente chico, resulta $\frac{n}{8(t'')^2} \geq l \geq l-2$, Y, por lo tanto, podemos elegir $l-2$ cosas ahí.

Basta ajustar entonces c_2 tal que garantice que $\frac{n}{8(t'')^2} \geq l$. Según hipótesis debe ser $l \leq c_2 n$. Entonces bastara tomar c_2 tal que $\frac{1}{8(t'')^2} \geq c_2$ Ahora como c_1 ya está fijo, resulta $t'' = \frac{1}{c_4}\ln(\ln(\frac{1}{c_1})) \in R$, luego, bastará elegir $c_2 \leq \frac{1}{8(t'')^2}$. Así $c_2 n \leq \frac{n}{8(t'')^2}$ y por lo tanto si $l \leq c_2 n$ resulta $l \leq c_2 n \leq \frac{n}{8(t'')^2}$

Entonces como habíamos afirmado, podemos entonces elegir $l-2$ cosas en $\{b \in I_n \ : \ b \equiv 3\ (6) (b, e_i) = 1\ ;\ b \in A\}$

Elegimos entonces f_i con $1 < i < l\ \ ;\ \ f_i \in \{b \in I_n \ : \ b \equiv 3\ (6)\ ,\ (b, e_i) = 1\ ;\ b \in A\}$.

Ahora construimos la siguiente secuencia:

$$a,\ b_1,\ f_1,\ b_2,\ f_2, \ldots,\ b_l,\ f_l$$

Esta secuencia forma un C_{2l+1} ciclo contenido en $G(A)$, ya que:

- son $2l+1$ elementos en A
- $(b_i, f_i) = 1$, para $1 \leq i \leq l$. Ya que si $p|b_i$, como $b_i\,|[\,b_i; b_{i+1}] = e_i$ $\Rightarrow p|e_i$, pero como por elección de f_i es $(f_i, e_i) = 1$, entonces $p \not| f_i$
- $(f_i, b_{i+1}) = 1$, para $1 \leq i < l$. Ya que, de la misma manera, si $p|b_{i+1}$ como $b_{i+1}|e_i$ tenemos que $p|e_i$ y como $(f_i, e_i) = 1$, entonces $p \not| f_i$
- $(a, b_1) = 1$, por elección de b_1, y
- $(f_l, a) = 1$. Igual que antes ya que $[b_l; a] = e_l$

Esto finaliza la demostración del Teorema 6.2. □

CAPíTULO 8

Demostración del Teorema 6.3

En este capítulo haremos la demostración del Teorema 6.3. Con esto queda terminada la prueba del Teorema 6.1.

Teníamos por hipótesis $S_1 + S_2 \geq \epsilon\ n$. Entonces algún $S_i \geq \frac{\epsilon}{2}n$.Ya que si $S_1 < \frac{\epsilon}{2}n$ y $S_2 < \frac{\epsilon}{2}n \Rightarrow S_1 + S_2 < \epsilon\ n$. Asumimos entonces que $S_2 \geq \frac{\epsilon}{2}n$.El caso en que sea $S_1 \geq \frac{\epsilon}{2}n$ es similar. Llamamos P_r al producto de los primos menores o iguales que r, o sea

$$P_r = \prod_{p:primo \leq r} p.$$

Ejemplos de P_r:

$$\begin{aligned}
P_1 &= \emptyset \\
P_2 &= \prod_{p:primo \leq 2} p = 2 \\
P_3 &= \prod_{p:primo \leq 3} p = 2 \cdot 3 = 6 \\
P_4 &= \prod_{p:primo \leq 4} p = P_3 = 2 \cdot 3 = 6 \\
P_5 &= \prod_{p:primo \leq 5} p = 2 \cdot 3 \cdot 5 = 30 \\
P_6 &= P_5 \\
P_7 &= P_5 \cdot 7 = 210 \\
P_8 &= P_7 = 210 \\
P_9 &= P_8 = P_7 = 210
\end{aligned}$$

La idea de la demostración es primero encontrar tres enteros positivos j_1, j_2, j_3 tales que $(j_1, j_2) = (j_2, j_3) = (j_3, j_1) = 1$, (O sea un K_3), con $\sharp A(p_r, j_i) = \sharp\{a \in A \mid a \equiv j_i\ (p_r)\}$ grande para cada $i : 1, 2, 3$.

Luego si $1 \leq l \leq c_3 n$, construimos un C_{2l+1} en $G(A)$ así: primero elegimos $a \in A(p_r, j_1)$ y luego los restantes $2l$ numeros serán elegidos alternadamente de $A(p_r, j_2)$ y $A(p_r, j_3)$.

Vamos a necesitar el siguiente lema:

LEMA 8.1. *Para todo $\sigma > 0$ y $\delta > 0$ existe $r_0 = r_0(\sigma; \delta)$, tal que si $r \geq r_0$, $n \geq n_4(\sigma, \delta, r)$ y $u = 1, 2, \ldots, P_r$, entonces, para todos excepto $\frac{\sigma n}{p_r}$ enteros k tales que $1 \leq k \leq n$ y $k \equiv u\ (p_r)$, tenemos*

$$\alpha(k) = \prod_{p\ :p|k\ ;p>r} \left(1 - \frac{1}{p}\right) > 1 - \delta.$$

Este lema puede ser encontrado en [**7**].

Ahora probemos el Teorema 6.3, par esto, usaremos el lema 8.1 con $\sigma = \frac{\epsilon}{8}$ y $\delta = \frac{\epsilon}{8}$.Con lo cual existe $r_0 = r_0(\frac{\epsilon}{8}; \frac{\epsilon}{8})$, tal que si $r \geq r_0$, $n \geq n_4(\sigma, \delta, r)$, se cumple el lema. Sea entonces $r \geq r_0$ del lema ; podemos suponer $r \geq 3$ así $\frac{P_r}{6} \in Z$

1. Probaremos:

$$\biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+1) = A(6,1)$$

Veamos: Si $a \in A$ tal que $a \equiv 6i+1\ (P_r)$, para algún i. Entonces $a = k \cdot P_r + (6i+1)$. Como $6|P_r$, entonces $a \equiv 1\ (6)$. Y por lo tanto $a \in A(6,1)$.

Además si $a \in A(6,1)$, veamos también que $a \in A(P_r, 6i+1)$; para algún $i = 1, \cdots, \frac{P_r}{6}$. Como $a \equiv 1\ (6)$, entonces existe $j \in Z$ tal que $a = 6j+1$. Tomemos $h = r_{\frac{P_r}{6}}(j)$, esto dice que $j = k \cdot \frac{P_r}{6} + h$, donde $0 \leq h < \frac{P_r}{6}$.

Entonces $a = 6j + 1 = 6(k\frac{P_r}{6} + h) + 1 = kP_r + 6h + 1$.
Luego $6h + 1 = r_{P_r}(a)$, siempre que $0 \leq 6h + 1 < P_r$.
Pero

$$\begin{aligned} 0 \leq & h < \frac{P_r}{6}, \text{ luego} \\ 1 \leq & 6h + 1 < P_r + 1, \text{ con lo cual} \\ 1 \leq & 6h + 1 \leq P_r. \end{aligned}$$

Ahora $6h+1 \neq P_r$, pues $6|P_r$, entonces $1 \leq 6h+1 < P_r$, y por lo tanto $6h + 1 = r_{p_r}(a)$, o sea $a \equiv 6h + 1\ (P_r)$, con $h = 0, \cdots, \frac{P_r}{6} - 1$ Si $h = 1, \cdots, \frac{P_r}{6} - 1$, tomemos $h = i$. Y en consecuencia $a \in A(P_r, 6i + 1)$. Si $h = 0$, entonces $a \in A(P_r, 6i + 1)$, con $i = \frac{P_r}{6}$. Ya que, reescribiendo 1 modulo P_r, tenemos $a \equiv 1 \equiv P_r + 1 \equiv 6(\frac{P_r}{6}) + 1\ \ (P_r)$

Acabamos de probar entonces:

$$\biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+1) = A(6,1).$$

2. De la misma manera podemos probar:

$$\biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+2) = A(6,2).$$

Veamos:

Si $a \in A$ tal que $a \equiv 6i+2\ (P_r)$, para algún i, entonces $a = k \cdot P_r + (6i+2)$.Como $6|P_r$, entonces $a \equiv 2\ (6)$. Y por lo tanto $a \in A(6,2)$.

Si $a \in A(6,2)$, entonces $a \in A$ y $a \equiv 2\ (6)$. Queremos ver que $a \in A(P_r, 6i+2)$, para algún $1 \leq i \leq \frac{P_r}{6}$. Como $a \equiv 2\ (6)$, entonces existe $j \in Z$ tal que $a = 6j+2$. Tomemos $h = r_{\frac{P_r}{6}}(j)$, así $j = k \cdot \frac{P_r}{6} + h$, donde $0 \leq h < \frac{P_r}{6}$.

Teníamos entonces $a = 6j+2 = 6(k\frac{P_r}{6}+h)+2 = kP_r+6h+2$.
Ahora $6h+2 = r_{P_r}(a)$, siempre que $0 \leq 6h+2 < P_r$.
Pero

$$\begin{aligned} 0 \leq & h < \frac{P_r}{6}, \text{ luego} \\ 2 \leq & 6h+2 < P_r+2, \text{ con lo cual} \\ 2 \leq & 6h+2 \leq P_r+1. \end{aligned}$$

Esto nos da tres opciones para la cota superior de $6h+2$ es $6h+2 = P_r+1$, o $6h+2 = P_r$, o $6h+2 < P_r$.

Veamos que $6h+2 \neq P_r+1$.

Como $6h+2 \equiv 2\ (6)$ y $P_r+1 \equiv 1\ (6)$, entonces $6h+2 \neq P_r+1$. De la misma manera como $6h+2 \equiv 2\ (6)$ y $P_r \equiv 0\ (6)$, obtenemos $6h+2 \neq P_r$. Luego $6h+2 < P_r$ y por lo tanto $6h+2 = \text{resto}_{P_r}(a)$. O sea $a \in A(P_r, 6h+2)$, así $a \equiv 6h+2\ (P_r)$ con h tal que $0 \leq k < \frac{P_r}{6}$.

- Si $h = 0$ entonces $a \equiv 2\ (P_r)$.Con lo cual podemos escribir $a \equiv 2 \equiv P_r+2 \equiv 6\big(\frac{P_r}{6}\big)+2\ (P_r)$. Luego $a \equiv 6i+2\ (P_r)$ con $i = \frac{P_r}{6}$ y por lo tanto $a \in \biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+2)$.
- Si $0 < h < \frac{P_r}{6}$ entonces $a \equiv 6h+2\ (P_r)$ y por lo tanto $a \in \biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+2)$ con $i = h$.

De la misma manera podemos probar:

3.

$$\biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+3) = A(6,3).$$

Análogamente:

4.
$$\biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+4) = A(6,4).$$

Y

5.
$$\biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+5) = A(6,5).$$

Como también

6.
$$\biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i) = A(6,0).$$

Por otro lado, reescalando convenientemente, tenemos:

$$\biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+5) = \biguplus_{j=1}^{\frac{P_r}{6}} A(P_r, 6j-1) = A(6,5)$$

Ya que

$$\begin{aligned}\biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+5) &= \biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6(i+1)-1) \\ &= \biguplus_{j=2}^{\frac{P_r}{6}+1} A(P_r, 6j-1) \\ &= \biguplus_{j=2}^{\frac{P_r}{6}} A(P_r, 6j-1) \uplus A(P_r, P_r+5)\end{aligned}$$

y $A(P_r, P_r+5) = A(P_r, 5)$ es el termino $j = 1$ de la sumatoria $\biguplus_{j=1}^{\frac{P_r}{6}} A(P_r, 6j-1)$.

Luego tenemos:

$$\biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+5) = \biguplus_{j=1}^{\frac{P_r}{6}} A(P_r, 6j-1) = A(6,5)$$

Escribiendo los siguientes conjuntos como uniones de conjuntos, según (1), (2), (3), (4), (5) y (6) tenemos:

$$A(6,5) \biguplus A(6,0) \biguplus A(6,1) \biguplus A(6,2) \biguplus A(6,3) \biguplus A(6,4) \biguplus A(6,5) =$$

$$\biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i-1) \uplus \biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i) \uplus \biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+1) \uplus \biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+2) \uplus$$
$$\biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+3) \uplus \biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+4) \uplus \biguplus_{i=1}^{\frac{P_r}{6}} A(P_r, 6i+5) =$$
$$A(6,5) \uplus \biguplus_{i=0}^{5} A(6,i)$$

Tomando cardinal, queda:

$$\begin{aligned} |A| + |A(6,5)| =& |A(6,5)| + |A(6,0)| + |A(6,1)| + \cdots + |A(6,5)| \\ =& \sum_{i=1}^{\frac{P_r}{6}} \big(|A(P_r, 6i-1)| + |A(P_r, 6i)| + |A(P_r, 6i+1)| \\ & + |A(P_r, 6i+2)| + |A(P_r, 6i+3)| \\ & + |A(P_r, 6i+4)| + |A(P_r, 6i+5)| \big) \end{aligned}$$

Ahora recordemos que $|A(6,5)| = S_2$, y por hipótesis, teníamos $|A| > f(n,2)$ y $f(n,2) = [\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}]$

Entonces queda $|A| + |A(6,5)| > f(n,2) + S_2 = [\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] + S_2$.

Ahora, planteando casos de congruencia modulo seis para n, se puede ver que

$$f(n,2) = [\frac{n}{2}] + [\frac{n}{3}] - [\frac{n}{6}] > \frac{2n}{3} - 2$$

Luego $f(n,2) + S_2 > \frac{2n}{3} - 2 + S_2 \geq \frac{2n}{3} - 2 + \frac{\epsilon n}{2}$, ya que estamos suponiendo $S_2 \geq \frac{\epsilon n}{2}$.

Con lo cual tenemos $|A| + |A(6,5)| > f(n,2) + S_2 > \frac{2n}{3} - 2 + \frac{\epsilon n}{2}$.

En conclusión :

$$|A| + |A(6,5)| > \frac{2n}{3} - 2 + \frac{\epsilon n}{2} \tag{8.1}$$

Ahora, si todos los sumandos desde $i = 1$ hasta $\frac{P_r}{6}$, del tipo

$$|A(P_r, 6i-1)| + |A(P_r, 6i)| + ... + |A(P_r, 6i+4)| + |A(P_r, 6i+5)|$$

fueran menor o igual que $\frac{\frac{2n}{3} - 2 + \frac{\epsilon n}{2}}{\frac{P_r}{6}}$, entonces quedaría

$$|A| + |A(6,5)| \leq \frac{P_r}{6} \left(\frac{\frac{2n}{3} - 2 + \frac{\epsilon n}{2}}{\frac{P_r}{6}} \right) = \frac{2n}{3} - 2 + \frac{\epsilon n}{2}$$

Lo que es un absurdo, según (8.1).

Luego, existe un i_0, $1 \leq i_0 \leq \frac{P_r}{6}$, para el cual, el sumando

$$|A(P_r, 6i_0 - 1)| + |A(P_r, 6i_0)| + |A(P_r, 6i_0 + 1)| + \cdots + |A(P_r, 6i_0 + 5)| > \frac{\frac{2n}{3} - 2 + \frac{\epsilon n}{2}}{\frac{P_r}{6}} = \frac{4n}{P_r} - \frac{12}{P_r} + \frac{3n\epsilon}{P_r}$$

Es decir para este i_0 se tiene la siguiente desigualdad:

(8.2)
$$|A(P_r, 6i_0 - 1)| + |A(P_r, 6i_0)| + |A(P_r, 6i_0 + 1)| + \cdots + |A(P_r, 6i_0 + 5)| > \frac{4n}{P_r} - \frac{12}{P_r} + \frac{3n\epsilon}{P_r}$$

Veamos ahora la siguiente observación:

Observación 8.1. *Para todo u, se tiene:* $|A(P_r, u)| < \frac{n}{P_r} + 1$

Pues: $|A(P_r, u)| = |A(P_r, u')|$ con u' tal que $1 \leq u' \leq P_r$ y $u' \equiv u(P_r)$ y $|A(P_r, u')| \subseteq \{b \in I_n \ : \ b \equiv u' \ (P_r)\} = \{k : \ 1 \leq P_r k + u' \leq n\}$ Ahora usando que $0 < \frac{u'}{P_r} \leq 1$ tenemos $\{k : \ 1 \leq P_r k + u' \leq n\} \subseteq \{k : \ -1 < k < \frac{n}{P_r}\} \subseteq \{k : 0 \leq k \leq \frac{n}{P_r} - 1\}$. Tomando cardinal obtenemos $|A(P_r, u)| \leq [\frac{n}{P_r} - 1] + 1 \leq \frac{n}{P_r}$ Probamos entonces que para todo u se cumple:

$$|A(P_r, u)| < \frac{n}{P_r} + 1$$

De esto ultimo y según (8.2) se tiene la siguiente afirmación:

Afirmación :

(8.3)
$$\begin{aligned} &\text{Existen tres enteros } j_1, j_2, j_3 \text{ tales que} \\ &6i_0 - 1 \leq j_1 < j_2 < j_3 \leq 6i_0 + 5; \\ &(j_1; j_2) = (j_2; j_3) = (j_1; j_3) = 1 \quad y \\ &|A(P_r; j_i)| > \frac{\epsilon}{2}\frac{n}{P_r}, \ \forall i : 1, 2, 3 \end{aligned}$$

Veámoslo:

- 1er Caso:

Si $|A(P_r; 6i_0 - 1)| \leq \frac{\epsilon n}{2P_r}$.
Entonces podemos acotar la siguiente suma así:

$$|A(P_r; 6i_0)| + \cdots + |A(P_r; 6i_0 + 5)| > \frac{4n}{P_r} + \frac{5\epsilon n}{2P_r} - \frac{12}{P_r}$$

ya que según (8.2) teníamos:

$$|A(P_r, 6i_0 - 1)| + |A(P_r, 6i_0)| + |A(P_r, 6i_0 + 1)| + \cdots + |A(P_r, 6i_0 + 5)| > \frac{\frac{2n}{3} - 2 + \frac{\epsilon n}{2}}{\frac{P_r}{6}} = \frac{4n}{P_r} + \frac{3\epsilon n}{P_r} - \frac{12}{P_r}$$

Ahora si $|A(P_r; 6i_0 - 1)| \leq \frac{\epsilon n}{2P_r}$, entonces

$$-|A(P_r; 6i_0 - 1)| \geq -\frac{\epsilon n}{2P_r}$$

Luego restando $|A(P_r; 6i_0 - 1)|$ queda:

$$\begin{aligned} |A(P_r; 6i_0)| + \cdots + |A(P_r; 6i_0 + 5)| &> \frac{4n}{P_r} + \frac{3\epsilon n}{P_r} - \frac{12}{P_r} - |A(P_r; 6i_0 - 1)| \\ &\geq \frac{4n}{P_r} + \frac{3\epsilon n}{P_r} - \frac{12}{P_r} - \frac{\epsilon n}{2P_r} \\ &= \frac{4n}{P_r} + \frac{5\epsilon n}{2P_r} - \frac{12}{P_r} \end{aligned}$$

Por lo tanto queda:

$$|A(P_r; 6i_0)| + \cdots + |A(P_r; 6i_0 + 5)| > \frac{4n}{P_r} + \frac{5\epsilon n}{2P_r} - \frac{12}{P_r} \tag{8.4}$$

Ahora afirmamos que existen 5 numeros u_1, u_2, u_3, u_4, u_5 dentro del conjunto $\{0, 1, 2, 3, 4, 5\}$ tales que

$$|A(P_r; 6i_0 + u_i)| > \frac{\epsilon n}{2P_r} \tag{8.5}$$

para todo $i = 1...,5$

Ya que si esto no ocurriera quiere decir que de los 6 elementos del conjunto $\{0, 1, 2, 3, 4, 5\}$ hay por lo menos 2 elementos u_i donde $|A(P_r; 6i_0 + u_i)| \leq \frac{\epsilon n}{2P_r}$, usando esto y usando lo que teníamos en (8.1) que para todo u se cumple: $|A(P_r, u)| < \frac{n}{P_r} + 1$ podemos acotar la suma superiormente usando estas dos desigualdades de la siguiente manera:

$$\begin{aligned} |A(P_r; 6i_0)| + \cdots + |A(P_r; 6i_0 + 5)| &< 4\left(\frac{n}{P_r} + 1\right) + 2\left(\frac{\epsilon n}{2P_r}\right) \\ &= 4\frac{n}{P_r} + \epsilon\frac{n}{P_r} + 4 \end{aligned}$$

Esta cota contradice (8.4), pues: Recién obtuvimos $|A(P_r; 6i_0)| + \cdots + |A(P_r; 6i_0 + 5)| < 4\frac{n}{P_r} + \epsilon\frac{n}{P_r} + 4$, y según (8.4) teníamos:

$$|A(P_r; 6i_0)| + \cdots + |A(P_r; 6i_0 + 5)| > \frac{4n}{P_r} + \frac{5\epsilon n}{2P_r} - \frac{12}{P_r}$$

Entonces debería pasar

$$\frac{4n}{P_r} + \frac{5\epsilon n}{2P_r} - \frac{12}{P_r} < 4\frac{n}{P_r} + \epsilon\frac{n}{P_r} + 4.$$

Cancelando y haciendo cuentas tenemos la siguiente desigualdad equivalente:

$$0 < \frac{\epsilon n}{P_r} - 5\frac{\epsilon n}{2P_r} + \frac{12}{P_r} + 4$$

Esto se da si y sólo si $3\frac{\epsilon n}{2P_r} - \frac{12}{P_r} < 4$ Lo que es equivalente a

$$\frac{3}{2}\epsilon n - 12 < 4P_r$$

Esto se cumple si y solo si $n < \frac{8P_r+24}{3\epsilon}$

Luego, bastara elegir n suficientemente grande. Es decir tomamos $n_2(\epsilon) > \frac{8P_r+24}{3\epsilon}$ así, si $n \geq n_2(\epsilon)$ obtenemos un absurdo.

Probamos hasta ahora la existencia de 5 numeros enteros $u_1, \ldots, u_5$ dentro del conjunto $\{0, 1, 2, 3, 4, 5\}$ tales que

$$|A(P_r; 6i_0 + u_i)| > \frac{\epsilon n}{2P_r}$$

para todo $i = 1, \ldots, 5$, según afirmamos en (8.5)

Veamos que $6i_0 + u_1 < 6i_0 + u_2 < \cdots < 6i_0 + u_5$ contiene una subsucesión de tres numeros j_1, j_2, j_3 coprimos de a pares donde vale

$$|A(P_r; j_i)| > \frac{\epsilon n}{2P_r}, \ \forall i : 1, 2, 3$$

como queríamos probar en (8.3).

Hasta ahora tenemos 5 numeros u_1, u_2, u_3, u_4, u_5 dentro del conjunto $\{0, 1, 2, 3, 4, 5\}$ tales que según (8.5) cumplen:

$$|A(P_r; 6i_0 + u_i)| > \frac{\epsilon n}{2P_r}$$

para todo $i = 1, \ldots, 5$. Con lo cual ordenando los u_i, tenemos: $6i_0 + u_1 < 6i_0 + u_2 < 6i_0 + u_3 < 6i_0 + u_4 < 6i_0 + u_5$. De esta secuencia necesitamos extraer tres coprimos de a pares, es decir un K_3.

Veamos por casos:

- Si el elemento de $\{0, 1, 2, 3, 4, 5\}$ que no es ningún u_i es el 0, entonces $1 = u_1 < 2 = u_2 < 3 = u_3 < \cdots$.

  Tenemos entonces la secuencia de cinco elementos: $\{6i_0+1, 6i_0+2, 6i_0+3, 6i_0+4, 6i_0+5\}$, dentro de la cual $\{6i_0+1, 6i_0+2, 6i_0+3\}$ forman un K_3

- Si el elemento de $\{0, 1, 2, 3, 4, 5\}$ que no es ningún u_i es el 1, la secuencia sería: $\{6i_0, 6i_0+2, 6i_0+3, 6i_0+4, 6i_0+5\}$, y de acá podemos extraer el siguiente $K_3 : \{6i_0 + 3, 6i_0 + 4, 6i_0 + 5\}$

- Si el elemento de $\{0, 1, 2, 3, 4, 5\}$ que no es ningún u_i es el 2, la secuencia sería: $\{6i_0, 6i_0+1, 6i_0+3, 6i_0+4, 6i_0+5\}$, y de acá $\{6i_0 + 3, 6i_0 + 4, 6i_0 + 5\}$ son un K_3.

- Si el elemento de $\{0, 1, 2, 3, 4, 5\}$ que no es ningún u_i es el 3, la secuencia sería: $\{6i_0, 6i_0+1, 6i_0+2, 6i_0+4, 6i_0+5\}$, y de acá $\{6i_0 + 1, 6i_0 + 2, 6i_0 + 5\}$ son un K_3.

- Si el elemento de $\{0,1,2,3,4,5\}$ que no es ningún u_i es el 4, la secuencia queda: $\{6i_0, 6i_0+1, 6i_0+2, 6i_0+3, 6i_0+5\}$, y de acá $\{6i_0+1, 6i_0+2, 6i_0+3\}$ son un K_3.
- Si el elemento de $\{0,1,2,3,4,5\}$ que no es ningún u_i es el 5, la secuencia queda: $\{6i_0, 6i_0+1, 6i_0+2, 6i_0+3, 6i_0+4\}$, y de acá $\{6i_0+1, 6i_0+2, 6i_0+3\}$ son un K_3.

Por lo tanto para este 1er Caso suponiendo : $|A(P_r; 6i_0-1)| \leq \frac{\epsilon n}{2P_r}$, hemos probado la afirmación de los j_i

- 2do Caso:

Si $|A(P_r; 6i_0+5)| \leq \frac{\epsilon n}{2P_r}$ es similar.

Ya que según (8.2)y restando ahora $|A(P_r; 6i_0+5)|$ podemos acotar la suma como antes:

$$|A(P_r; 6i_0-1)| + |A(P_r; 6i_0| + \cdots + |A(P_r; 6i_0+4)| > \frac{4n}{P_r} + \frac{5\epsilon n}{2P_r} - \frac{12}{P_r}$$

Esto implica, igual que en el caso 1, que existen 5 numeros $u_1, \cdots, u_5$ tales que $-1 \leq u_1 < \cdots < u_5 \leq 4$ que verifican:

$$|A(P_r; 6i_0+u_i)| > \frac{\epsilon n}{2P_r} \tag{8.6}$$

para todo $i = 1, \ldots, 5$, ya que si esto no pasara, igual que antes, hay dos o mas objetos u_i para los cuales podemos acotar:

$$|A(P_r; 6i_0+u_i)| \leq \frac{\epsilon n}{2P_r}$$

y además teníamos según la Observación 8.1 que para todo u se cumple: $|A(P_r, u)| < \frac{n}{P_r} + 1$.

Luego la suma queda: $|A(P_r; 6i_0-1)| + |A(P_r; 6i_0| + \cdots + |A(P_r; 6i_0+4)| < 4\left(\frac{n}{P_r}+1\right) + 2\left(\frac{\epsilon n}{2P_r}\right) = 4\frac{n}{P_r} + \epsilon\frac{n}{P_r} + 4$ lo que contradice (8.4) como antes.

Tenemos hasta ahora 5 numeros u_1, u_2, u_3, u_4, u_5 dentro del conjunto $\{0,1,2,3,4,5\}$ tales que, según (8.5), cumplen:

$$|A(P_r; 6i_0+u_i)| > \frac{\epsilon n}{2P_r}$$

para todo $i = 1, \ldots, 5$. Con lo cual ordenando los u_i, tenemos: $6i_0+u_1 < 6i_0+u_2 < 6i_0+u_3 < 6i_0+u_4 < 6i_0+u_5$. De esta secuencia, como antes, para poder demostrar la afirmación (8.3) necesitamos extraer un K_3

Veamos:

- Si el elemento de $\{-1,0,1,2,3,4\}$ que no es u_i es el -1 la secuencia queda: $\{6i_0, 6i_0+1, 6i_0+2, 6i_0+3, 6i_0+4\}$ donde $\{6i_0+1, 6i_0+2, 6i_0+3\}$ forman un K_3.
- El mismo K_3 sirve si el elemento de $\{-1,0,1,2,3,4\}$ que no es u_i es el 0.

- Si el elemento de $\{-1,0,1,2,3,4\}$ que no es u_i es el 1 la secuencia queda: $\{6i_0-1, 6i_0, 6i_0+2, 6i_0+3, 6i_0+4\}$ acá $\{6i_0-1, 6i_0+3, 6i_0+4\}$ forman un K_3.
- Si el elemento de $\{-1,0,1,2,3,4\}$ que no es u_i es el 2 el mismo K_3 sirve.
- Si el elemento de $\{-1,0,1,2,3,4\}$ que no es u_i es el 3 la secuencia queda: $\{6i_0-1, 6i_0, 6i_0+1, 6i_0+2, 6i_0+4\}$ acá $\{6i_0-1, 6i_0+1, 6i_0+2\}$ forman un K_3.
- Si el elemento de $\{-1,0,1,2,3,4\}$ que no es u_i es el 4 el mismo K_3 sirve.

  En consecuencia, igual que antes, la secuencia $\{6i_0+u_1, 6i_0+u_2, 6i_0+u_3, 6i_0+u_4, 6i_0+u_5\}$; donde $-1 \leq u_1 < u_2 < u_3 < u_4 < u_5 \leq 4$, contiene una subsecuencia j_1, j_2, j_3 de tres elementos coprimos de a pares donde se cumple: $|A(P_r; j_i)| > \frac{\epsilon}{2}\frac{n}{P_r},\ \forall i : 1,2,3$

- 3er Caso (si no se dan los casos 1 y 2):

Es decir si $|A(P_r; 6i_0-1)| > \frac{\epsilon n}{2P_r}$ y $|A(P_r; 6i_0+5)| > \frac{\epsilon n}{2P_r}$

En este caso elegimos $j_1 = 6i_0 - 1$ y $j_3 = 6i_0 + 5$. Para j_2 elegiremos alguno de los enteros: $6i_0+1, 6i_0+2$ o $6i_0+3$ para el cual $|A(P_r; j_2)| > \frac{\epsilon n}{2P_r}$

Un j_2 así, existe pues sino, para estos tres enteros tendríamos: $|A(P_r; 6i_0+1)| \leq \frac{\epsilon n}{2P_r}$ y $|A(P_r; 6i_0+2)| \leq \frac{\epsilon n}{2P_r}$ y $|A(P_r; 6i_0+3)| \leq \frac{\epsilon n}{2P_r}$ Con lo cual tendríamos, en particular, dos miembros de la suma $|A(P_r; 6i_0)| + \cdots + |A(P_r; 6i_0+5)|$ para acotar con menor o igual a $\frac{\epsilon n}{2P_r}$. Así la suma quedaría: $|A(P_r; 6i_0)| + \cdots + |A(P_r; 6i_0+5)| < 4\left(\frac{n}{P_r}+1\right) + 2\left(\frac{\epsilon n}{2P_r}\right) = 4\frac{n}{P_r} + \epsilon\frac{n}{P_r} + 4.$

Esto contradice (8.4) como el Caso 1.

Luego, la **Afirmación de los** j_i (8.3)es cierta!!! Es decir existen tres enteros j_1, j_2, j_3 tales que $6i_0 - 1 \leq j_1 < j_2 < j_3 \leq 6i_0 + 5$; $(j_1; j_2) = (j_2; j_3) = (j_1; j_3) = 1$ y

$$|A(P_r; j_i)| > \frac{\epsilon}{2}\frac{n}{P_r},\ \forall i : 1,2,3$$

Como j_1 puede no pertenecer al conjunto $\{1, 2, \ldots, P_r\}$; tomamos congruencia modulo P_r a j_1 y llamamos $\tilde{j_1} \equiv j_1$. (P_r) así resulta $\tilde{j_1} < P_r$.Luego aplicando el Lema (8.1)con $u = \tilde{j_1}$, $\delta = \frac{\epsilon}{8}$ y $\sigma = \frac{\epsilon}{8}$, tenemos la existencia de de un conjunto B (de excepciones), de $\sharp B = \frac{\epsilon n}{8P_r}$ tal que para todo k tales que $1 \leq k \leq n$ y $k \equiv \tilde{j_1}\ (P_r)$, y $k \notin B$ tenemos

$$\alpha(k) = \prod_{p\ :p|k\ ;p>r} \left(1 - \frac{1}{p}\right)\ > 1 - \delta.$$

Entonces para todo $a \in A(P_r, j_1) - B$ vale que:

$$\alpha(a) = \prod_{p\ :p|a\ ;p>r} \left(1 - \frac{1}{p}\right)\ > 1 - \delta.$$

Observamos que por elección $\tilde{j_1}$no es cero. Así $\tilde{j_1} \in \{1, 2, \cdots, P_r\}$ y por lo tanto podemos usar el lema con $u = \tilde{j_1}$.

Elegimos $a \in A(P_r, j_1) - B$, así para este a tenemos

$$\alpha(a) = \prod_{p\ :p|a\ ;p>r} \left(1 - \frac{1}{p}\right)\ > 1 - \frac{\epsilon}{8}. \tag{8.7}$$

Observemos que es posible elegir a así, pues $\big(A(P_r, j_1) - B\big) \neq \emptyset$ ya que por elección de j_1 se cumple que $\sharp A(P_r, j_1) > \frac{\epsilon n}{2P_r} > \frac{\epsilon n}{8P_r} = \sharp B$.

Ahora vamos a buscar algún elemento coprimo con a perteneciente a $A(P_r, j_2)$ Para esto, estimamos por abajo el número de soluciones de

$$(a; \mathbf{b}_x) = 1;\ \mathbf{b}_x \in A(P_r, j_2)$$

Llamamos $C = \{\mathbf{b}_x : \mathbf{b}_x \in A(P_r, j_2)\ ;\ (a; \mathbf{b}_x) = 1\}$.

Luego $\sharp C = \sharp\{h : h \in A(P_r, j_2)\ ;\ (h, a) = 1\}$.

Queremos obtener una cota inferior para $\sharp C$ para poder elegir cosas en C

Tenemos $C \subseteq A(P_r, j_2)$ y podemos escribir

$$A(P_r, j_2) = \{h : h \in A(P_r, j_2)\ ;\ (h, a) = 1\} \biguplus \{h : h \in A(P_r, j_2)\ ;\ (h, a) > 1\}.$$

Entonces $\sharp C = \sharp A(P_r, j_2) - \sharp\{h : h \in A(P_r, j_2)\ ;\ (h, a) > 1\}$. Resulta que: $\{h : h \in A(P_r, j_2)\ ;\ (h, a) > 1\} \subseteq \{h \in I_n;\ h \equiv j_2\ (P_r);\ (h, a) > 1\}$.

Entonces

$$\begin{aligned}
\sharp C &= \sharp A(P_r, j_2) - \sharp\{h : h \in A(P_r, j_2)\ ;\ (h, a) > 1\} \\
&\geq \sharp A(P_r, j_2) - \sharp\{d \in I_n;\ d \equiv j_2\ (P_r);\ (d, a) > 1\} \\
&= \sharp A(P_r, j_2) - \sum_{\substack{d \leq n;\ d \equiv j_2\ (P_r), \\ (a,d) > 1}} 1
\end{aligned}$$

Ahora:

$$\sum_{\substack{d \leq n;\ d \equiv j_2\ (P_r), \\ (a,d) > 1}} 1 = \sum_{d \leq n;\ d \equiv j_2\ (P_r)} 1 - \sum_{\substack{d \leq n;\ d \equiv j_2\ (P_r), \\ (a,d) = 1}} 1$$

Lo que es igual:

$$= \sum_{d \leq n;\ d \equiv j_2\ (P_r)} 1 - \sharp\{d \in I_n :\ d \equiv j_2\ (P_r), (a, d) = 1\}$$

Ahora tratemos de acotar $\sharp\{d \in I_n :\ d \equiv j_2\ (P_r),\ (a, d) = 1\}$. Para esto vamos a usar la fórmula de inversión de Moëbius.

Previamente definamos las siguientes funciones:

Llamamos $h(P_r, j, z) = \sharp\{d \in I_n : d \equiv j\ \ (P_r)\ ;\ (z, d) = 1\}$.

Luego $h(P_r, j_2, a) = \sharp\{d \in I_n : d \equiv j_2\ \ (P_r)\ ;\ (a, d) = 1\}$, y podemos escribir $h(P_r, j_2, a) = \sharp\{d \in I_n : d \equiv j_2\ \ (P_r)\ ;\ a(a, d) = a\}$.

Definimos: $\beta(m) = \sharp\{b \in I_n : b \equiv j_2\ (P_r)$ y $m(a; b) = a\}$

Con esta definición $\beta(a) = h(P_r, j_2, a)$

Luego, para calcular h que es $\beta(a)$ necesitamos tener una función aritmética α tal que $\alpha(m) = \sum_{d|m} \beta(d)$, así por la fórmula de inversión, resulta $\beta(m) = \sum_{d|m} \mu(d)\alpha(\frac{m}{d})$

Definimos entonces:

$$\alpha(m) = \sharp\{b \in I_n : b \equiv j_2 \ (P_r) \text{ y } a|mb\}$$

Tenemos:

$$\begin{aligned}\sum_{d|m} \beta(d) &= \sum_{d|m} \sharp\{b \in I_n : b \equiv j_2 \ (P_r) \text{ y } d(a;b) = a\} \\ &= \sharp \biguplus_{d|m} \{b \in I_n : b \equiv j_2 \ (P_r) \text{ y } d(a;b) = a\}\end{aligned}$$

y tenemos la siguiente igualdad de conjuntos:

$$\biguplus_{d|m} \{b \in I_n : b \equiv j_2 \ (P_r) \text{ y } d(a;b) = a\} = \{b \in I_n : b \equiv j_2 \ (P_r) \text{ y } a|mb\}$$

En efecto, si $b \in I_n$ tq $b \equiv j_2 \ (P_r)$ y $d(a;b) = a$ para algún d divisor de m, como $d|m$ y $(a;b)|b$ tenemos $d(a;b)|mb$.

Luego como d es tal que $d(a;b) = a$ tenemos $a|mb$ y de la misma manera si $b \in I_n : b \equiv j_2 \ (P_r)$ y $a|mb$. Queremos encontrar algún d divisor de m tal que $d(a;b) = a$. Proponemos $q = \frac{a}{(a;b)}$.

Claramente $q \in Z$. Veamos que $q|m$.

Como $a|mb$ tenemos $\frac{a}{(a;b)} | \frac{mb}{(a;b)}$ y como $\left(\frac{a}{(a;b)} : \frac{b}{(a;b)}\right) = 1$. Entonces $\frac{a}{(a;b)}|m$. O sea $q|m$ y claramente q verifica $q(a;b) = a$. Por lo tanto este sería el divisor de m que estábamos buscando.

Así probamos la siguiente igualdad de cardinales:

$$\sharp \biguplus_{d|m} \{b \in I_n : b \equiv j_2 \ (P_r) \text{ y } d(a;b) = a\} = \sharp\{b \in I_n : b \equiv j_2 \ (P_r) \text{ y } a|mb\}.$$

Con lo cual habiendo definido α como arriba tenemos:

$$\sum_{d|m} \beta(d) = \alpha(m)$$

Luego por la Fórmula de Inversión tenemos:

$$\beta(m) = \sum_{d|m} \mu(d)\alpha(\frac{m}{d}).$$

Evaluando en a queda:

$$\beta(a) = \sum_{d|a} \mu(d)\alpha(\frac{a}{d})$$

Tratemos ahora de ver que es $\alpha(\frac{a}{d})$.

$$\alpha(\frac{a}{d}) = \sharp\{b \in I_n : b \equiv j_2 \ (P_r) \text{ y } a|\frac{a}{d}b\}$$

Ahora,

$$\begin{aligned} a|\frac{a}{d}b &\Leftrightarrow \frac{a}{d}b = aq \text{ para algun } q \in Z \\ &\Leftrightarrow \frac{a}{d}b = \frac{a}{d}dq \\ &\Leftrightarrow \frac{a}{d}(b - dq) = 0 \\ &\Leftrightarrow d|b \end{aligned}$$

Entonces podemos escribir, para d divisor de a:

$$\alpha(\frac{a}{d}) = \sharp\{b \in I_n : b \equiv j_2 \ (P_r) \text{ y } d|b\} = \sharp\{b \in I_n : b \equiv j_2 \ (P_r) \text{ y } b \equiv 0 \ (d)\}$$

Llamemos $g(n,d) = \sharp\{b \in I_n : b \equiv j_2 \ (P_r) \text{ y } b \equiv 0 \ (d)\}$

Calculemos entonces $g(n,d) = \alpha(\frac{a}{d})$

Para esto debemos resolver el sistema

$$\begin{cases} b \equiv j_2 \ (P_r), \\ b \equiv 0 \ (d). \end{cases}$$

Este sistema tendrá solución o no dependiendo de (P_r, d). Más aún, por el Teorema Chino del Resto, el sistema tiene solución si y sólo si $(P_r, d)|j_2$.

Calculemos entonces (P_r, d).

Si $(P_r, d) \neq 1$ afirmamos que el sistema no tiene solución, ya que si existe b solución, b se puede escribir:

$$\begin{aligned} b &= dk \\ b &= qP_r + j_2, \end{aligned}$$

con k y $q \in Z$.

Ahora como $(P_r, d) \neq 1$ entonces existe p primo tal que $p|(P_r, d)$. Luego $p|P_r$ y por lo tanto $p \leq r$; además $p|d$ y como $d|a$, entonces $p|a$. Y como $p|d$ entonces $p|b$; luego $p|j_2$.

Ahora $a \in A(P_r, j_1)$ o sea $a = kP_r + j_1$ para algún $k \in Z$ y como $p|a$ y $p|P_r$, entonces $p|j_1$, lo cual es absurdo ya que $(j_1, j_2) = 1$.

Luego, si $(P_r, d) \neq 1$ el sistema no tiene solución y por lo tanto $\alpha(\frac{a}{d}) = 0$.

Ahora si $(P_r, d) = 1$, el sistema tiene solución única $b_0 \in [0, P_r d)$ y todas las soluciones son de la forma $b = b_0 + kP_r d$ con $k \in \mathbb{Z}$.

Luego

$$\alpha(\frac{a}{d}) = \sharp\{b \in I_n : b \equiv j_2 \ (P_r) \text{ y } b \equiv 0 \ (d)\} = \sharp\{k \in \mathbb{Z} \ : \ 1 \leq b_0 + kP_r d \leq n\}.$$

Veamos ahora que

$$\{k \in \mathbb{Z} \ : \ 0 \leq k \leq \frac{n}{P_r d} - 1\} \subset \{k \in \mathbb{Z} \ : \ 1 \leq b_0 + kP_r d \leq n\} \tag{8.8}$$

y

$$\{k \in \mathbb{Z} \ : \ 1 \leq b_0 + kP_r d \leq n\} \subset \{k \in \mathbb{Z} \ : \ 0 \leq k \leq \frac{n}{P_r d}\}. \tag{8.9}$$

En efecto, si $0 \leq k \leq \frac{n}{P_r d} - 1$, entonces

$$1 \leq b_0 \leq b_0 + kP_r d \leq b_0 + n - P_r d < n,$$

Resulta que $b_0 \geq 1$ pues $b_0 \neq 0$,ya que por elección, $j_2 = 6i_0 + t$ con $t = 1, 2, 3, 4$ y por lo tanto $j_2 \not\equiv 0 \ (P_r)$ y a demás $b_0 - P_r d < 0$, lo que prueba (8.8).

Por otro lado, si $1 \leq b_0 + kP_r d \leq n$, entonces

$$-1 < \frac{1}{P_r d} - 1 < \frac{1}{P_r d} - \frac{b_0}{P_r d} = \frac{1 - b_0}{P_r d} \leq k \leq \frac{n - b_0}{P_r d} \leq \frac{n}{P_r d},$$

lo que prueba (8.9).

Tomando cardinal en (8.8) – (8.9) obtenemos

$$\left[\frac{n}{P_r d}\right] \leq \alpha(\frac{a}{d}) \leq \left[\frac{n}{P_r d}\right] + 1,$$

que, usando $[x] \leq x < [x] + 1$ implica

$$\frac{n}{P_r d} - 1 \leq \alpha(\frac{a}{d}) \leq \frac{n}{P_r d} + 1.$$

O sea

$$-1 \leq \alpha(\frac{a}{d}) - \frac{n}{P_r d} \leq 1.$$

Llamemos $\varepsilon = \alpha(\frac{a}{d}) - \frac{n}{P_r d}$. Tenemos entonces

$$\alpha(\frac{a}{d}) = \frac{n}{P_r d} + \varepsilon$$

con $|\varepsilon| \leq 1$ para d tal que $(P_r, d) = 1$.

Hemos probado entonces el siguiente lema:

LEMA 8.2. *Sea $g(n, d) = \alpha(\frac{a}{d})$ definidas como arriba, se tiene*

$$\alpha(\frac{a}{d}) = \begin{cases} 0 & \text{si } (P_r, d) \neq 1 \\ \frac{n}{P_r d} + \varepsilon & \text{si } (P_r, d) = 1 \end{cases}$$

donde $|\varepsilon| \leq 1$.

Retomando

$$\begin{aligned} \beta(a) &= \sum_{d|a} \mu(d)\alpha(\frac{a}{d}) \\ &= \sum_{\substack{d|a, \mu(d)>0, \\ (P_r,d)=1}} \mu(d)\alpha(\frac{a}{d}) + \sum_{\substack{d|a, \mu(d)<0, \\ (P_r,d)=1}} \mu(d)\alpha(\frac{a}{d}) \\ &= \qquad I \qquad + \qquad II. \end{aligned}$$

Buscamos ahora acotar inferiormente $\beta(a)$.

Usando que $\alpha(\frac{a}{d}) \geq \frac{n}{P_r d} - 1$, tenemos

$$\mu(d)\alpha(\frac{a}{d}) \geq \mu(d)\frac{n}{P_r d} - \mu(d)$$

para $\mu(d) > 0$

Y usando que $\alpha(\frac{a}{d}) \leq \frac{n}{P_r d} + 1$ y $\mu(d) < 0$, tenemos

$$\mu(d)\alpha(\frac{a}{d}) \geq \mu(d)\frac{n}{P_r d} + \mu(d)$$

Entonces nos queda:

$$I + II \geq \sum_{\substack{d|a,\mu(d)>0,\\(P_r,d)=1}} \mu(d)\frac{n}{P_r d} - \mu(d) + \sum_{\substack{d|a,\mu(d)<0,\\(P_r,d)=1}} \mu(d)\frac{n}{P_r d} + \mu(d)$$

Lo que es igual a:

$$\sum_{\substack{d|a,\mu(d)\neq 0,\\(P_r,d)=1}} \mu(d)\frac{n}{P_r d} - \sum_{\substack{d|a,\mu(d)>0,\\(P_r,d)=1}} 1 + \sum_{\substack{d|a,\mu(d)<0,\\(P_r,d)=1}} -1 =$$

$$= \frac{n}{P_r} \sum_{d|a,(P_r,d)=1} \frac{\mu(d)}{d} - \sum_{\substack{d|a,\mu(d)\neq 0,\\(P_r,d)=1}} 1 \tag{8.10}$$

Ahora acotemos $\sum_{\substack{d|a,\mu(d)\neq 0,\\(P_r,d)=1}} 1$.

Resulta que:

$$\sum_{\substack{d|a,\mu(d)\neq 0,\\(P_r,d)=1}} 1 = \sharp\{d \in Z \ : \ \mu(d) \neq 0; \ d|a; \ (d, P_r) = 1\}$$

$$\leq \sharp\{d \in Z \ : \ \mu(d) \neq 0, \ d|a\} = 2^{w(a)}$$

Usando esto (8.10) queda:

$$\geq \frac{n}{P_r} \sum_{\substack{d|a,\mu(d)\neq 0,\\(P_r,d)=1}} \frac{\mu(d)}{d} - 2^{w(a)}$$

Es decir, juntando todo tenemos:

$$I + II \geq \frac{n}{P_r} \sum_{\substack{d|a,(P_r,d)=1,\\ \mu(d)\neq 0}} \frac{\mu(d)}{d} - 2^{w(a)}$$

Ahora recordemos que: $I + II = \beta(a) = h(P_r, j_2, a)$. Con lo cual tenemos la siguiente desigualdad:

$$h(P_r, j_2, a) - \frac{n}{P_r} \sum_{\substack{d|a,(P_r,d)=1,\\ \mu(d)\neq 0}} \frac{\mu(d)}{d} \geq -2^{w(a)} \tag{8.11}$$

Calculemos ahora $\sum_{\substack{d|a,(P_r,d)=1,\\ \mu(d)\neq 0}} \frac{\mu(d)}{d}$. Escribiendo $a = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_m^{\alpha_m}\acute{a}$ con $P_r = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_m^{\alpha_m}$ primos y $p_m \leq r$ tenemos que como $(P_r, d) = 1$, entonces $d|a \Leftrightarrow d|\acute{a}$. Con lo cual usando esto y la propiedad de las funciones aritméticas 2.4 la sumatoria que queremos calcular queda:

$$\sum_{\substack{d|a,(P_r,d)=1,\\ \mu(d)\neq 0}} \frac{\mu(d)}{d} = \sum_{d|a,(P_r,d)=1} \frac{\mu(d)}{d} = \sum_{d|\acute{a}} \frac{\mu(d)}{d} = \frac{\phi(\acute{a})}{\acute{a}}$$

Y según (7.33)

$$\frac{\phi(\acute{a})}{\acute{a}} = \prod_{p|\acute{a}}(1-\frac{1}{p}) = \prod_{p|a,p>r}(1-\frac{1}{p})$$

Entonces quedó:

$$\sum_{\substack{d|a,(P_r,d)=1,\\ \mu(d)\neq 0}} \frac{\mu(d)}{d} = \prod_{p|a,p>r}(1-\frac{1}{p})$$

con lo cual reescribiendo la desigualdad (8.11), queda:

$$h(P_r, j_2, a) \geq \frac{n}{P_r}\prod_{p|a,p>r}(1-\frac{1}{p}) - 2^{w(a)}$$

Ahora según vimos en la Observación 7.3 existe n_3 tal que si $n \geq 2n_3$ y $a \leq n$ (cosa que vale ya que $a \in A(P_r, j_1) \subseteq I_n$), entonces se tiene $\omega(a) < 2\frac{\ln(n)}{\ln(\ln(n))}$. Con lo cual, si n es suficientemente grande tenemos $\omega(a) < 2\frac{\ln(n)}{\ln(\ln(n))}$. Luego, juntando todo, la desigualdad anterior queda:

$$h(P_r, j_2, a) - \frac{n}{P_r}\prod_{p|a,p>r}(1-\frac{1}{p}) \geq -2^{w(a)} > -2^{2^{\frac{\ln(n)}{\ln(\ln(n))}}}$$

Por lo tanto

$$h(P_r, j_2, a) > \frac{n}{P_r}\prod_{p|a,p>r}(1-\frac{1}{p}) - 2^{2^{\frac{\ln(n)}{\ln(\ln(n))}}}$$

Recordemos ahora que según la aplicación del Lema (8.1), con $\delta = \frac{\epsilon}{8}$, habíamos elegido a tal que verifica :$\prod_{p|a,p>r}(1-\frac{1}{p}) > 1-\frac{\epsilon}{8}$ Entonces la desigualdad anterior queda:

$$h(P_r, j_2, a) > \frac{n}{P_r}\prod_{p|a,p>r}(1-\frac{1}{p}) - 2^{2^{\frac{\ln(n)}{\ln(\ln(n))}}} > \frac{n}{P_r}(1-\frac{\epsilon}{8}) - 2^{2^{\frac{\ln(n)}{\ln(\ln(n))}}}$$

Afirmamos ahora que para n grande vale:

$$\frac{n}{P_r}(1-\frac{\epsilon}{8}) - 2^{2^{\frac{\ln(n)}{\ln(\ln(n))}}} > (1-\frac{\epsilon}{4})\frac{n}{P_r} \tag{8.12}$$

Primero tenemos que si n es suficientemente grande, ie si $n \geq \exp(\exp 8)$, entonces $2\frac{\ln(n)}{\ln(\ln(n))} \leq 2\frac{\ln(n)}{8} = \frac{\ln(n)}{4}$. Luego, para n grande tenemos la siguiente cota:

$$2^{2^{\frac{\ln(n)}{\ln(\ln(n))}}} < \exp(2\frac{\ln(n)}{\ln(\ln(n))}) \leq \sqrt[4]{n}$$

Entonces queda:

$$\frac{n}{P_r}(1-\frac{\epsilon}{8}) - 2^{2^{\frac{\ln(n)}{\ln(\ln(n))}}} > \frac{n}{P_r}(1-\frac{\epsilon}{8}) - \sqrt[4]{n}$$

Veamos ahora que

$$\frac{n}{P_r}(1-\frac{\epsilon}{8}) - \sqrt[4]{n} > \left(1-\frac{\epsilon}{4}\right)\frac{n}{P_r}$$

Esto ocurre si y sólo si

$$\begin{aligned} -\frac{\epsilon n}{8P_r} - \sqrt[4]{n} &> -\frac{\epsilon n}{4P_r} \\ \Leftrightarrow \frac{\epsilon n}{8P_r} &> \sqrt[4]{n} \\ \Leftrightarrow \frac{n}{\sqrt[4]{n}} &> \frac{8P_r}{\epsilon} \\ \Leftrightarrow n^{\frac{3}{4}} &> \frac{8P_r}{\epsilon} \\ \Leftrightarrow n^3 &> \left(\frac{8P_r}{\epsilon}\right)^4 \\ \Leftrightarrow n &> \sqrt[3]{\left(\frac{8P_r}{\epsilon}\right)^4} \end{aligned}$$

Bastará pedir entonces $n_2(\epsilon) > \sqrt[3]{\left(\frac{8P_r}{\epsilon}\right)^4}$, así si $n \geq n_2(\epsilon)$ vale la afirmación (8.12) Y por lo tanto hemos probado que para n suficientemente grande, tenemos

$$h(P_r, j_2, a) > (1-\frac{\epsilon}{4})\frac{n}{P_r} \tag{8.13}$$

Ahora con estas notaciones $\sharp C$ queda:

$$\begin{aligned} \sharp C &= \sharp A(P_r, j_2) - \sharp\{h : h \in A(P_r, j_2)\ ;\ (h,a) > 1\} \\ &\geq \sharp A(P_r, j_2) - \sharp\{d \in I_n;\ d \equiv j_2\ (P_r);\ (d,a) > 1\} \\ &= \sharp A(P_r, j_2) - \sum_{\substack{d \leq n;\ d \equiv j_2\ (P_r), \\ (a,d)>1}} 1 \end{aligned}$$

Ahora:

$$\sum_{\substack{d \leq n;\ d \equiv j_2\ (P_r), \\ (a,d)>1}} 1 = \sum_{d \leq n;\ d \equiv j_2\ (P_r)} 1 - \sum_{\substack{d \leq n;\ d \equiv j_2\ (P_r), \\ (a,d)=1}} 1$$

Lo que es igual:

$$= \sum_{d\leq n;\ d\equiv j_2\ (P_r)} 1 - \sharp\{d\in I_n:\ d\equiv j_2\ (P_r),\ (a,d)=1\}$$

$$= \sum_{d\leq n;\ d\equiv j_2\ (P_r)} 1 - h(P_r;j_2;a)$$

Juntando todo y volviendo a tratar de acotar el $\sharp C$, tenemos:

$$\sharp C \geq \sharp A(P_r,j_2) - \sum_{\substack{d\leq n;\ d\equiv j_2\ (P_r),\\ (a,d)>1}} 1$$

$$= \sharp A(P_r,j_2) - \left\{ \sum_{d\leq n;\ d\equiv j_2\ (P_r)} 1 - h(P_r;j_2;a) \right\}$$

$$= \sharp A(P_r,j_2) - \sum_{d\leq n;\ d\equiv j_2\ (P_r)} 1 + h(P_r;j_2;a)$$

Ahora acotemos:

1. por un lado por elección de j_2, teníamos:

$$\sharp A(P_r,j_2) > \frac{\epsilon n}{2P_r}$$

2. podemos escribir la suma:

$$\sum_{d\leq n;\ d\equiv j_2\ (P_r)} 1 = \sharp\{k:\ k\in I_n;\ k\equiv j_2\ (P_r)\}$$

$$= \sharp\{k:\ k\in I_n;\ k = hP_r + \tilde{j_2} \text{ con } \tilde{j_2}\equiv j_2\ (P_r) \text{ y} \tilde{j_2}\in[1,P_r]\}$$

$$= \sharp\{hP_r+\tilde{j_2} : 1\leq hP_r+\tilde{j_2}\leq n\}$$

$$= \sharp\{h : 1\leq hP_r+\tilde{j_2}\leq n\}$$

Ahora resulta:

$$\{h : 1\leq hP_r+\tilde{j_2}\leq n\} \subseteq \{h : 0\leq h < \frac{n}{P_r}\} \tag{8.14}$$

Pues si h es tal que $1\leq hP_r+\tilde{j_2}\leq n$, entonces $h\geq \frac{1-\tilde{j_2}}{P_r} = \frac{1}{P_r} - \frac{\tilde{j_2}}{P_r}$, ahora como $\tilde{j_2}\leq P_r$ entonces $\frac{\tilde{j_2}}{P_r}\leq 1$, luego $h\geq \frac{1-\tilde{j_2}}{P_r} = \frac{1}{P_r} - \frac{\tilde{j_2}}{P_r} \geq \frac{1}{P_r} - 1 > -1$ y por lo tanto $h\geq 0$. De la misma manera, si h es tal que $1\leq hP_r+\tilde{j_2}\leq n$, entonces $h\leq \frac{n-\tilde{j_2}}{P_r} = \frac{n}{P_r} - \frac{\tilde{j_2}}{P_r}$. Ahora como $\frac{\tilde{j_2}}{P_r}\geq \frac{1}{P_r}$, luego $h\leq \frac{n-\tilde{j_2}}{P_r} = \frac{n}{P_r} - \frac{\tilde{j_2}}{P_r} < \frac{n}{P_r}$ Hemos probado entonces la inclusión de (8.14).

Volviendo entonces a acotar la suma, tenemos:

$$\sum_{d\leq n;\ d\equiv j_2\ (P_r)} 1 \leq \sharp\{h : 0\leq h < \frac{n}{P_r}\} \leq \frac{n}{P_r} < \frac{n}{P_r} + 1$$

Luego

$$\sum_{d\leq n;\ d\equiv j_2\ (P_r)} 1 < \frac{n}{P_r} + 1$$

Con lo cual

$$-\sum_{d\leq n;\ d\equiv j_2\ (P_r)} 1 > -\frac{n}{P_r} - 1$$

3. para la cota de h según (8.13) teníamos, para n grande

$$h(P_r, j_2, a) > (1 - \frac{\epsilon}{4})\frac{n}{P_r}$$

Luego acotando con (1), (2) y (3) el $\sharp C$ tenemos:

$$\begin{aligned}\sharp C &\geq \sharp A(P_r, j_2) - \sum_{d\leq n;\ d\equiv j_2\ (P_r)} 1 + h(P_r; j_2; a)\\ &> \frac{\epsilon n}{2P_r} - \frac{n}{P_r} - 1 + (1 - \frac{\epsilon}{4})\frac{n}{P_r}\\ &= \frac{\epsilon n}{4P_r} - 1\end{aligned}$$

Y con n suficientemente grande podemos acotar $\frac{\epsilon n}{4P_r} - 1 > \frac{\epsilon n}{5P_r}$. Ya que

$$\begin{aligned}\frac{\epsilon n}{4P_r} - 1 &> \frac{\epsilon n}{5P_r}\\ \Leftrightarrow \frac{\epsilon n}{4P_r} - \frac{\epsilon n}{5P_r} &> 1\\ \Leftrightarrow \frac{\epsilon n}{20P_r} &> 1\\ \Leftrightarrow n &> \frac{20P_r}{\epsilon}\end{aligned}$$

Luego, bastará entonces pedir $n_2(\epsilon) > \frac{20P_r}{\epsilon}$, así si $n \geq n_2(\epsilon)$ se cumple que

$$\sharp C > \frac{\epsilon n}{5P_r} \tag{8.15}$$

Aplicando ahora el Lema 8.1con $u = \tilde{j_2}$, tal que $\tilde{j_2} \equiv j_2\ (P_r)$ y$\tilde{j_2} \in (0, P_r]$ tenemos la existencia de de un conjunto B (de excepciones) de $\sharp B = \frac{\epsilon n}{8P_r}$ tal que para todo k tales que $1 \leq k \leq n$ y $k \equiv \tilde{j_2}\ (P_r)$, y $k \notin B$ tenemos

$$\alpha(k) = \prod_{p\ :p|k\ ;p>r} \left(1 - \frac{1}{p}\right) > 1 - \frac{\epsilon}{8}$$

En particular para todo $k \in A(P_r, \tilde{j_2}) - B = A(P_r, j_2) - B$ y k tal que $(k : a) = 1$; siempre que exista un k así. Tomemos entonces el conjunto: $\{k :\ k \in A(P_r; j_2)\ ;\ (k : a) = 1\} - B$. Deberíamos poder mostrar que este conjunto es distinto de vacío. Veamos:

$\sharp\{k:\ k\in A(P_r;j_2)\ ;\ (k:a)=1\}=\sharp C$ que según (8.15) es $\sharp C>\frac{\epsilon n}{5P_r}$. Y en B hay $\frac{\epsilon n}{8P_r}$ elementos. Luego como $\frac{\epsilon n}{5P_r}>\frac{\epsilon n}{8P_r}$ el conjunto.

$$\{k:\ k\in A(P_r;j_2)\ ;\ (k:a)=1\}-B\neq\emptyset.$$

Veamos ahora que este conjunto $\{k:\ k\in A(P_r;j_2)\ ;\ (k:a)=1\}-B$ contiene por lo menos l elementos. Ahora

$$\begin{aligned}\sharp\big(\{k:\ k\in A(P_r;j_2)\ ;\ (k:a)=1\}-B\big)\\ \geq\sharp\{k:\ k\in A(P_r;j_2)\ ;\ (k:a)=1\}-\sharp B\end{aligned}$$

y acotando esta resta es $>\frac{\epsilon n}{5P_r}-\frac{\epsilon n}{8P_r}$ Queremos mostrar que este conjunto $\{k:\ k\in A(P_r;j_2)\ ;\ (k:a)=1\}-B$ contiene l cosas y esto ocurre si

$$\frac{\epsilon n}{5P_r}-\frac{\epsilon n}{8P_r}=\frac{3\epsilon n}{40P_r}\geq l$$

Veamos:

$$\frac{3\epsilon n}{40P_r}\geq l\Leftrightarrow l\leq\frac{3\epsilon n}{40P_r}$$

Ahora por hipótesis l debe cumplir $l\leq c_3(\epsilon)n$, luego bastará pedir que $c_3(\epsilon)\leq\frac{3\epsilon}{40P_r}$ así se cumple:

$$l\leq c_3(\epsilon)n\leq\frac{3\epsilon}{40P_r}n$$

Y por lo tanto podemos elegir l cosas en

$$\big(\{k:\ k\in A(P_r;j_2)\ ;\ (k:a)=1\}-B\big)$$

Elegimos entonces $b_1,b_2,b_3,\ldots,b_l$ que satisfacen:

$$(a:b_i)=1,\qquad b_i\in A(P_r,j_2)\qquad\text{y}$$

$$\prod_{p|b_i,\ p>r}\big(1-\frac{1}{p}\big)>1-\frac{\epsilon}{8}\ \text{ para todo } 1\leq i\leq l \tag{8.16}$$

Ahora la prueba sigue de manera análoga a lo que se hace en la demostración del Teorema 6.2.

Como antes, para la construcción de nuestro $2l+1-ciclo$, tenemos elegidos $a,b_1,b_2,b_3,\ldots,b_l$, definimos $b_{l+1}=a$ y llamamos $e_i:=[b_i,b_{i+1}]$, $i=1,\ldots,l$.

Debemos construir entonces un conjunto donde elegir los restantes f_i, $i=1,\ldots,l$, elementos de tal manera que la secuencia

$$a,b_1,f_1,b_2,f_2,\ldots,b_l,f_l$$

forme un C_{2l+1} ciclo contenido en $\mathcal{G}(A)$. Para esto necesitamos que f_i verifique que $(b_i,f_i)=1$ y también que $(f_i,b_{i+1})=1$. Este hecho queda garantizado si elegimos f_i tales que $(f_i,e_i)=1$. Pues si $p|b_i$ entonces $p|e_i$, luego si tenemos $(f_i,e_i)=1$, entonces $p\not|f_i$, con lo cual vale $(b_i,f_i)=1$. De la misma manera se puede ver $(f_i,b_{i+1})=1$.

Llamamos entonces $e_i = [b_i : b_{i+1}]$, para todo $1 \leq i \leq l$ donde definimos $b_{l+1} = a$, y llamamos $Y_i = \sharp\{y : \ y \in A(P_r, j_3), \ ; (e_i : y) = 1\}$. Como antes, podemos escribir:

$$\begin{aligned} Y_i &= \sharp\{y : \ y \in A(P_r, j_3), \ ; (e_i : y) = 1\} \\ &= \sharp A(P_r, j_3) - \sharp\{y : \ y \in A(P_r, j_3), \ ; (e_i : y) > 1\} \\ &\geq \sharp A(P_r, j_3) - \sharp\{d \in I_n; \ d \equiv j_3 \ (P_r); \ (d, e_i) > 1\} \\ &= \sharp A(P_r, j_3) - \sum_{\substack{d \leq n; \ d \equiv j_3 \ (P_r), \\ (e_i, d) > 1}} 1 \end{aligned}$$

Ahora, como antes:

$$\sum_{\substack{d \leq n; \ d \equiv j_3 \ (P_r), \\ (e_i, d) > 1}} 1 = \sum_{d \leq n; \ d \equiv j_3 \ (P_r)} 1 - \sum_{\substack{d \leq n; \ d \equiv j_3 \ (P_r), \\ (e_i, d) = 1}} 1$$

Lo que es igual:

$$= \sum_{d \leq n; \ d \equiv j_3 \ (P_r)} 1 - \sharp\{d \in I_n : \ d \equiv j_3 \ (P_r), \ (e_i, d) = 1\}$$

Ahora tratemos de acotar $\sharp\{d \in I_n : \ d \equiv j_3 \ (P_r), \ (e_i, d) = 1\}$
Para esto vamos a usar la fórmula de inversión de Moëbius. Previamente definamos las siguientes funciones, como antes:

Llamamos $h(P_r, j, z) = \sharp\{d \in I_n : d \equiv j \ \ (P_r) \ ; (z, d) = 1\}$. Luego $h(P_r, j_3, e_i) = \sharp\{d \in I_n : d \equiv j_3 \ \ (P_r) \ ; (e_i, d) = 1\}$. Y podemos escribir $h(P_r, j_3, e_i) = \sharp\{d \in I_n : d \equiv j_3 \ \ (P_r) \ ; e_i(e_i, d) = e_i\}$.

Definimos: $\beta(m) = \sharp\{b \in I_n : b \equiv j_3 \ (P_r) \text{ y } m(e_i; b) = e_i\}$. Con esta definición $\beta(e_i) = h(P_r, j_3, e_i)$.

Luego, para calcular h que es $\beta(e_i)$ necesitamos tener una función aritmética α tal que $\alpha(m) = \sum_{d|m} \beta(d)$, así por la fórmula de inversión, resulta $\beta(m) = \sum_{d|m} \mu(d)\alpha(\frac{m}{d})$.

Definimos entonces:

$$\alpha(m) = \sharp\{b \in I_n : b \equiv j_3 \ (P_r) \text{ y } e_i | mb\}$$

Tenemos:

$$\begin{aligned} \sum_{d|m} \beta(d) &= \sum_{d|m} \sharp\{b \in I_n : b \equiv j_3 \ (P_r) \text{ y } d(e_i; b) = e_i\} \\ &= \sharp \biguplus_{d|m} \{b \in I_n : b \equiv j_3 \ (P_r) \text{ y } d(e_i; b) = e_i\} \end{aligned}$$

y tenemos, como antes, la siguiente igualdad de conjuntos:

$$\biguplus_{d|m} \{b \in I_n : b \equiv j_3 \ (P_r) \text{ y } d(e_i; b) = e_i\} = \{b \in I_n : b \equiv j_3 \ (P_r) \text{ y } e_i | mb\}$$

En efecto, si $b \in I_n$ tal que $b \equiv j_3 \ (P_r)$ y $d(e_i; b) = e_i$ para algún d divisor de m, como $d|m$ y $(e_i; b)|b$, tenemos $d(e_i; b)|mb$.Luego como d es

tal que $d(e_i;b) = e_i$ tenemos $e_i|mb$. De la misma manera, si $b \in I_n$ es tal que $b \equiv j_3\ (P_r)$ y $e_i|mb$, queremos encontrar algún d divisor de m tal que $d(e_i;b) = e_i$. Proponemos $q = \frac{e_i}{(e_i;b)}$. Claramente $q \in \mathbb{Z}$. Veamos que $q|m$. Como $e_i|mb$ tenemos $\frac{e_i}{(e_i;b)}|\frac{mb}{(e_i;b)}$ y $\left(\frac{e_i}{(e_i;b)}, \frac{b}{(e_i;b)}\right) = 1$. Entonces $\frac{e_i}{(e_i;b)}|m$. O sea $q|m$ y claramente q verifica $q(e_i;b) = e_i$. Por lo tanto este sería el divisor de m que estábamos buscando.

Así probamos la siguiente igualdad de cardinales:

$$\sharp \biguplus_{d|m} \{b \in I_n : b \equiv j_3\ (P_r) \text{ y } d(e_i;b) = e_i\} = \sharp\{b \in I_n : b \equiv j_3\ (P_r) \text{ y } e_i|mb\}.$$

Con lo cual habiendo definido α como arriba tenemos:

$$\sum_{d|m} \beta(d) = \alpha(m)$$

Luego por la Fórmula de Inversión tenemos:

$$\beta(m) = \sum_{d|m} \mu(d)\alpha(\frac{m}{d})$$

Evaluando en e_i queda:

$$\beta(e_i) = \sum_{d|e_i} \mu(d)\alpha(\frac{e_i}{d})$$

Tratemos ahora de ver que es $\alpha(\frac{e_i}{d})$.

$$\alpha(\frac{e_i}{d}) = \sharp\{b \in I_n : b \equiv j_3\ (P_r) \text{ y } e_i|\frac{e_i}{d}b\}$$

Ahora,

$$\begin{aligned} e_i|\frac{e_i}{d}b &\Leftrightarrow \frac{e_i}{d}b = e_i q \text{ para algun } q \in Z \\ &\Leftrightarrow \frac{e_i}{d}b = \frac{e_i}{d}dq \\ &\Leftrightarrow \frac{e_i}{d}(b - dq) = 0 \\ &\Leftrightarrow d|b \end{aligned}$$

Entonces podemos escribir, para d divisor de e_i:

$$\alpha(\frac{e_i}{d}) = \sharp\{b \in I_n : b \equiv j_3\ (P_r) \text{ y } d|b\} = \sharp\{b \in I_n : b \equiv j_3\ (P_r) \text{ y } b \equiv 0\ (d)\}.$$

Llamemos $\tilde{g}(n,d) = \sharp\{b \in I_n : b \equiv j_3\ (P_r) \text{ y } b \equiv 0\ (d)\}$. Calculemos entonces $\tilde{g}(n,d) = \alpha(\frac{e_i}{d})$

Para esto debemos resolver el sistema

$$\begin{cases} b \equiv j_3\ (P_r), \\ b \equiv 0\ (d). \end{cases}$$

Este sistema tendrá solución o no dependiendo de (P_r, d). Más aún, por el Teorema Chino del Resto, como antes, el sistema tiene solución si y sólo si $(P_r, d)|j_3$.

Calculemos entonces (P_r, d).

Si $(P_r, d) \neq 1$ afirmamos que el sistema no tiene solución. Ya que si existe b solución, b se puede escribir:

$$b = dk$$
$$b = qP_r + j_3.$$

Con k y $q \in Z$. Ahora como $(P_r, d) \neq 1$ entonces existe p primo tal que $p|(P_r, d)$. Luego $p|P_r$ y por lo tanto $p \leq r$; además $p|d$ y como $d|e_i$, entonces $p|e_i$.Y como $p|d$ entonces $p|b$; luego $p|j_3$. Además $p|e_i$ con $e_i = [b_i : b_{i+1}]$ y como $b_i b_{i+1} = (b_i : b_{i+1})[b_i : b_{i+1}]$, entonces $p|b_i$ o $p|b_{i+1}$. En cualquiera de los dos casos como b_i y $b_{i+1} \in A(P_r, j_2)$ si $i < l$, entonces $p|j_2$ lo que es un absurdo ya que $(j_2 : j_3) = 1$. Y si $i = l$ $p|b_l$ o $p|b_{l+1}$. Si $p|b_l$ entonces como $b_l \in A(P_r, j_2)$ entonces $p|j_2$ lo que es un absurdo como antes. Si $p|b_{l+1}$ como $b_{l+1} = a$ y como $a \equiv j_1,\ (P_r)$, entonces $p|j_1$ lo que también es un absurdo ya que $(j_1 : j_3) = 1$. Luego, si $(P_r, d) \neq 1$ el sistema no tiene solución y por lo tanto $\alpha(\frac{e_i}{d}) = 0$.

Ahora si $(P_r, d) = 1$, el sistema tiene solución única $b_0 \in [0, P_r d)$ y todas las soluciones son de la forma $b = b_0 + kP_r d$ con $k \in \mathbb{Z}$. Luego

$$\alpha(\frac{e_i}{d}) = \sharp\{b \in I_n : b \equiv j_3\ (P_r) \text{ y } b \equiv 0\ (d)\} = \sharp\{k \in \mathbb{Z}\ :\ 1 \leq b_0 + kP_r d \leq n\}.$$

Análogamente como en el Lema 8.2 se puede ver que :

$$\alpha(\frac{e_i}{d}) = \begin{cases} 0 & \text{si } (P_r, d) \neq 1 \\ \frac{n}{P_r d} + \varepsilon & \text{si } (P_r, d) = 1 \end{cases}$$

donde $|\varepsilon| \leq 1$.

Luego:

$$\begin{aligned} \beta(e_i) &= \sum_{d|e_i} \mu(d)\alpha(\frac{e_i}{d}) \\ &= \sum_{\substack{d|e_i, \mu(d)>0, \\ (P_r,d)=1}} \mu(d)\alpha(\frac{e_i}{d}) + \sum_{\substack{d|e_i, \mu(d)<0, \\ (P_r,d)=1}} \mu(d)\alpha(\frac{e_i}{d}) \\ &= \qquad I \qquad + \qquad II. \end{aligned}$$

Usando que $\alpha(\frac{e_i}{d}) \geq \frac{n}{P_r d} - 1$, tenemos

$$\mu(d)\alpha(\frac{e_i}{d}) \geq \mu(d)\frac{n}{P_r d} - \mu(d)$$

para $\mu(d) > 0$

Y usando que $\alpha(\frac{e_i}{d}) \leq \frac{n}{P_r d} + 1$ y $\mu(d) < 0$, tenemos

$$\mu(d)\alpha(\frac{e_i}{d}) \geq \mu(d)\frac{n}{P_r d} + \mu(d)$$

Entonces nos queda:

$$I + II \geq \sum_{\substack{d|e_i, \mu(d)>0, \\ (P_r,d)=1}} \mu(d)\frac{n}{P_r d} - \mu(d) + \sum_{\substack{d|e_i, \mu(d)<0, \\ (P_r,d)=1}} \mu(d)\frac{n}{P_r d} + \mu(d)$$

Lo que es igual a:

$$\sum_{\substack{d|e_i, \mu(d)\neq 0, \\ (P_r,d)=1}} \mu(d)\frac{n}{P_r d} - \sum_{\substack{d|e_i, \mu(d)>0, \\ (P_r,d)=1}} 1 + \sum_{\substack{d|e_i, \mu(d)<0, \\ (P_r,d)=1}} -1 =$$

$$= \frac{n}{P_r} \sum_{d|e_i,(P_r,d)=1} \frac{\mu(d)}{d} - \sum_{\substack{d|e_i, \mu(d)\neq 0, \\ (P_r,d)=1}} 1 \tag{8.17}$$

Ahora acotemos $\sum_{\substack{d|e_i, \mu(d)\neq 0, \\ (P_r,d)=1}} 1.$

Resulta que:

$$\sum_{\substack{d|e_i, \mu(d)\neq 0, \\ (P_r,d)=1}} 1 = \sharp\{d \in Z \ : \ \mu(d) \neq 0; \ d|e_i; \ (d, P_r) = 1\}$$

$$\leq \sharp\{d \in Z \ : \ \mu(d) \neq 0, \ d|e_i\} = 2^{w(e_i)}$$

Usando esto, (8.17) queda:

$$\geq \frac{n}{P_r} \sum_{\substack{d|e_i, \\ (P_r,d)=1, \mu(d)\neq 0}} \frac{\mu(d)}{d} - 2^{w(e_i)}$$

Luego, juntando todo tenemos:

$$I + II \geq \frac{n}{P_r} \sum_{\substack{d|e_i, \\ (P_r,d)=1, \mu(d)\neq 0}} \frac{\mu(d)}{d} - 2^{w(e_i)}$$

Ahora recordemos que: $I + II = \beta(e_i) = h(P_r, j_3, e_i)$.

Con lo cual tenemos la siguiente desigualdad:

$$h(P_r, j_3, e_i) - \frac{n}{P_r} \sum_{\substack{d|e_i, (P_r,d)=1, \\ \mu(d)\neq 0}} \frac{\mu(d)}{d} \geq -2^{w(e_i)} \tag{8.18}$$

Calculemos ahora $\sum_{\substack{d|e_i, (P_r,d)=1, \\ \mu(d)\neq 0}} \frac{\mu(d)}{d}$

Escribiendo $e_i = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \acute{e}_i$ con $P_r = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ primos y $p_m \leq r$ tenemos que como $(P_r, d) = 1$, entonces $d|e_i \Leftrightarrow d|\acute{e}_i$.

Con lo cual usando esto y la propiedad de las funciones aritméticas (7.32) la sumatoria que queremos calcular queda:

$$\sum_{\substack{d|e_i,(P_r,d)=1,\\ \mu(d)\neq 0}} \frac{\mu(d)}{d} = \sum_{d|e_i,(P_r,d)=1} \frac{\mu(d)}{d} = \sum_{d|e_i'} \frac{\mu(d)}{d} = \frac{\phi(e_i')}{e_i'}$$

Y según (7.33)

$$\frac{\phi(e_i')}{e_i'} = \prod_{p|e_i'}(1-\frac{1}{p}) = \prod_{p|e_i,p>r}(1-\frac{1}{p})$$

Entonces quedó:

$$\sum_{\substack{d|e_i,(P_r,d)=1,\\ \mu(d)\neq 0}} \frac{\mu(d)}{d} = \prod_{p|e_i,p>r}(1-\frac{1}{p})$$

con lo cual reescribiendo la desigualdad (8.18), queda:

$$h(P_r,j_3,e_i) \geq \frac{n}{P_r}\prod_{p|e_i,p>r}(1-\frac{1}{p}) - 2^{w(e_i)}$$

Ahora para acotar a $w(e_i)$ necesitamos otra desigualdad.

Vamos a usar la Observación 7.3, la cual dice que existe n_3 tal que si $n \geq 2n_3$ y $a \leq n$, entonces se tiene $\omega(a) < 2\frac{\ln(n)}{\ln(\ln(n))}$.

Usaremos esta observación con e_i en lugar de a y n^2 en lugar de n Para esto veamos que:

- $e_i \leq n^2$: Pues $e_i = [b_i : b_{i+1}] \leq [b_i : b_{i+1}](b_i : b_{i+1}) = b_i b_{i+1} \leq n^2$
- $n^2 > 2n_3$: Pues si n es grande $n^2 > n$ y $n > 2n_3$.

Luego usando la Observación 7.3, (para n suficientemente grande, $n > 2n_3$), tenemos:

$$\omega(e_i) < 2\frac{\ln(n^2)}{\ln(\ln(n^2))}$$

Ahora como $n < n^2$ entonces $\ln(\ln(n)) < \ln(\ln(n^2))$ y por lo tanto $\frac{1}{\ln(\ln(n))} > \frac{1}{\ln(\ln(n^2))}$. Es así como

$$w(e_i) < \frac{2\ln(n^2)}{\ln(\ln(n^2))} < \frac{2\ln(n^2)}{\ln(\ln(n))} = \frac{4\ln(n)}{\ln(\ln(n))}$$

Con lo cual, si n es suficientemente grande tenemos $\omega(e_i) < 4\frac{\ln(n)}{\ln(\ln(n))}$.

Luego, juntando todo, la desigualdad anterior queda:

$$h(P_r,j_3,e_i) - \frac{n}{P_r}\prod_{p|e_i,p>r}(1-\frac{1}{p}) \geq -2^{w(e_i)} > -2^{4\frac{\ln(n)}{\ln(\ln(n))}}$$

Por lo tanto

$$h(P_r, j_3, e_i) > \frac{n}{P_r} \prod_{p|e_i, p>r} (1 - \frac{1}{p}) - 2^{4\frac{\ln(n)}{\ln(\ln(n))}} \tag{8.19}$$

Tratemos ahora de acotar inferiormente $\prod_{p|e_i, p>r} (1 - \frac{1}{p})$

Observación 8.2. *Resulta que*

$$\prod_{p|e_i, p>r} (1 - \frac{1}{p}) \geq \prod_{p|b_i, p>r} (1 - \frac{1}{p}) \times \prod_{p|b_{i+1}, p>r} (1 - \frac{1}{p})$$

Veamos: como $1 - \frac{1}{p} \leq 1$ entonces

$$\prod_{\substack{p|b_{i+1}, p\not|b_i, \\ p>r}} (1 - \frac{1}{p}) \geq \prod_{\substack{p|b_{i+1}, p|b_i, \\ p>r}} (1 - \frac{1}{p}) \times \prod_{\substack{p|b_{i+1}, p|b_i, \\ p>r}} (1 - \frac{1}{p})$$

y tenemos

$$\prod_{\substack{p|b_{i+1}, p\not|b_i, \\ p>r}} (1 - \frac{1}{p}) \times \prod_{\substack{p|b_{i+1}, p|b_i, \\ p>r}} (1 - \frac{1}{p}) = \prod_{\substack{p|b_{i+1}, \\ p>r}} (1 - \frac{1}{p})$$

Luego

$$\prod_{\substack{p|b_{i+1}, p\not|b_i, \\ p>r}} (1 - \frac{1}{p}) \geq \prod_{\substack{p|b_{i+1}, \\ p>r}} (1 - \frac{1}{p})$$

Es así como

$$\begin{aligned}
\prod_{p|e_i, p>r} (1 - \frac{1}{p}) &= \prod_{\substack{p|b_{i+1}, p\not|b_i, \\ p>r}} (1 - \frac{1}{p}) \times \prod_{\substack{p|b_i, p\not|b_{i+1}, \\ p>r}} (1 - \frac{1}{p}) \times \prod_{\substack{p|b_{i+1}, p|b_i\text{`}, \\ p>r}} (1 - \frac{1}{p}) \\
&= \prod_{\substack{p|b_{i+1}, p\not|b_i, \\ p>r}} (1 - \frac{1}{p}) \times \prod_{p|b_i p>r} (1 - \frac{1}{p}) \\
&\geq \prod_{\substack{p|b_{i+1}, \\ p>r}} (1 - \frac{1}{p}) \times \prod_{p|b_i p>r} (1 - \frac{1}{p})
\end{aligned}$$

Como queríamos ver en la observación.

Luego volviendo a (8.19), tenemos:

$$\begin{aligned}
h(P_r, j_3, e_i) &> \frac{n}{P_r} \prod_{p|e_i, p>r} (1 - \frac{1}{p}) - 2^{4\frac{\ln(n)}{\ln(\ln(n))}} \\
&\geq \frac{n}{P_r} \prod_{p|b_{i+1}, p>r} (1 - \frac{1}{p}) \times \prod_{p|b_i p>r} (1 - \frac{1}{p}) - 2^{4\frac{\ln(n)}{\ln(\ln(n))}}
\end{aligned}$$

Luego, por elección de b_i según (8.16) se cumple:

$$\prod_{p|b_i,\ p>r} \big(1-\frac{1}{p}\big) > 1-\frac{\epsilon}{8}$$

para todo $1 \leq i \leq l$. Así como también para $i = l+1$, ya que $b_{l+1} = a$, y para a teníamos también que $\prod_{p|a,\ p>r} \big(1-\frac{1}{p}\big) > 1-\frac{\epsilon}{8}$

Luego volviendo a $h(P_r, j_3, e_i)$, tenemos

$$h(P_r, j_3, e_i) \geq \frac{n}{P_r}\big(1-\frac{\epsilon}{8}\big)^2 - 2^{4\frac{\ln(n)}{\ln(\ln(n))}}$$

Veamos ahora que con n grande resulta

$$\frac{n}{P_r}\big(1-\frac{\epsilon}{8}\big)^2 - 2^{4\frac{\ln(n)}{\ln(\ln(n))}} > \big(1-\frac{\epsilon}{4}\big)\frac{n}{P_r}$$

Como se demostró en el Teorema 6.2, resulta que si $n \geq e^{e^{24}}$ entonces $2^{\frac{4\ln(n)}{\ln(\ln(n))}} \leq \sqrt[6]{n}$. En efecto, si $n \geq e^{e^{24}}$, entonces $\ln(n) \geq e^{24}$, luego $\ln(\ln(n)) \geq 24$. De donde se obtiene

$$\frac{4\ln(n)}{\ln(\ln(n))} \leq \frac{4\ln(n)}{24} = \frac{1}{6}\ln(n).$$

Luego

$$e^{\frac{4\ln(n)}{\ln(\ln(n))}} \leq e^{\frac{\ln(n)}{6}} = \sqrt[6]{n}$$

Finalmente,

$$2^{\frac{4\ln(n)}{\ln(\ln(n))}} \leq e^{\frac{4\ln(n)}{\ln(\ln(n))}} \leq \sqrt[6]{n}.$$

Entonces si $n \geq e^{e^{24}}$, tenemos

$$\frac{n}{P_r}\big(1-\frac{\epsilon}{8}\big)^2 - 2^{4\frac{\ln(n)}{\ln(\ln(n))}} \geq \frac{n}{P_r}\big(1-\frac{\epsilon}{8}\big)^2 - \sqrt[6]{n}$$

Luego

$$\begin{aligned}
\frac{n}{P_r}\big(1-\frac{\epsilon}{8}\big)^2 - \sqrt[6]{n} &> \big(1-\frac{\epsilon}{4}\big)\frac{n}{P_r} \\
&\Leftrightarrow \frac{\epsilon^2 n}{64P_r} - \sqrt[6]{n} > 0 \\
&\Leftrightarrow \frac{\epsilon^2 n}{64P_r} > \sqrt[6]{n} \\
&\Leftrightarrow n^{\frac{5}{6}} > \frac{64P_r}{\epsilon^2} \\
&\Leftrightarrow n^5 > \big(\frac{64P_r}{\epsilon^2}\big)^6 \\
&\Leftrightarrow n > \sqrt[5]{\big(\frac{64P_r}{\epsilon^2}\big)^6}
\end{aligned}$$

Entonces bastará pedir $n_2(\epsilon) > max\{\sqrt[5]{\left(\frac{64P_r}{\epsilon^2}\right)^6}; e^{e^{24}}\}$, así si $n > n_2(\epsilon)$ se cumple $h(P_r, j_3, e_i) > \left(1 - \frac{\epsilon}{4}\right)\frac{n}{P_r}$

Luego volviendo a nuestro propósito de asegurar suficientes cosas en Y_i Teníamos:

$$\begin{aligned}
Y_i &= \sharp\{y:\ y \in A(P_r, j_3),\ ;\ (e_i : y) = 1\} \\
&= \sharp A(P_r, j_3) - \sharp\{y:\ y \in A(P_r, j_3),\ ;\ (e_i : y) > 1\} \\
&\geq \sharp A(P_r, j_3) - \sharp\{d \in I_n;\ d \equiv j_3\ (P_r);\ (d, e_i) > 1\} \\
&= \sharp A(P_r, j_3) - \sum_{\substack{d \leq n;\ d \equiv j_3\ (P_r) \\ (e_i, d) > 1}} 1 \\
&= \sharp A(P_r, j_3) - \sum_{d \leq n;\ d \equiv j_3\ (P_r)} 1 + \sharp\{d \in I_n:\ d \equiv j_3\ (P_r),\ (e_i, d) = 1\} \\
&= \sharp A(P_r, j_3) - \sum_{d \leq n;\ d \equiv j_3\ (P_r)} 1 + h(P_r, j_3, e_i)
\end{aligned}$$

Es decir

$$Y_i \geq \sharp A(P_r, j_3) - \sum_{d \leq n;\ d \equiv j_3\ (P_r)} 1 + h(P_r, j_3, e_i)$$

Ahora teníamos:

- $\sharp A(P_r, j_3) > \frac{\epsilon n}{2P_r}$ por elección de j_i
- $\sum_{d \leq n;\ d \equiv j_3\ (P_r)} 1 \leq \frac{n}{P_r}$ luego, $\sum_{d \leq n;\ d \equiv j_3\ (P_r)} 1 < \frac{n}{P_r} + 1$
- $h(P_r, j_3, e_i) > \left(1 - \frac{\epsilon}{4}\right)\frac{n}{P_r}$, par n suficientemente grande

Así juntando todo podemos acotar Y_i y queda:

$$\begin{aligned}
Y_i &\geq \sharp A(P_r, j_3) - \sum_{d \leq n;\ d \equiv j_3\ (P_r)} 1 + h(P_r, j_3, e_i) \\
&> \frac{\epsilon n}{2P_r} - \left(\frac{n}{P_r} + 1\right) + \left(1 - \frac{\epsilon}{4}\right)\frac{n}{P_r} \\
&= \frac{\epsilon n}{4P_r} - 1
\end{aligned}$$

Y para n grande podemos acotar

$$\begin{aligned}
\frac{\epsilon n}{4P_r} - 1 &> \frac{\epsilon n}{5P_r} \\
\Leftrightarrow \frac{\epsilon n}{4P_r} - \frac{\epsilon n}{5P_r} &> 1 \\
\Leftrightarrow \frac{\epsilon n}{20P_r} &> 1 \\
\Leftrightarrow n &> \frac{20P_r}{\epsilon}
\end{aligned}$$

Entonces si $n_2(\epsilon)$ es suficientemente grande, es decir $n_2(\epsilon)$ mayor que la más grande de todas las cotas de n que fuimos necesitando resulta que con $n > n_2(\epsilon)$ tenemos $Y_i > \frac{\epsilon n}{5P_r}$Es decir

$$Y_i = \sharp\{y : \ y \in A(P_r, j_3), \ ; (e_i : y) = 1\} > \frac{\epsilon n}{5P_r}$$

Luego, aplicando nuevamente el Lema 8.1 con $u = \tilde{j_3}$, tal que $\tilde{j_3} \equiv j_3 \ (P_r)$ y$\tilde{j_3} \in (0, P_r]$ tenemos la existencia de de un conjunto B (de excepciones) de $\sharp B = \frac{\epsilon n}{8P_r}$ tal que para todo k tales que $1 \leq k \leq n$ y $\ k \equiv \tilde{j_3} \ (P_r)$, y $k \notin B$ tenemos

$$\alpha(k) = \prod_{p \ :p|k \ ;p>r} \left(1 - \frac{1}{p}\right) \ > 1 - \frac{\epsilon}{8} \tag{8.20}$$

En particular para todo $k \in A(P_r, \tilde{j_3}) - B = A(P_r, j_3) - B$ y k tal que $(k : e_i) = 1$; siempre que exista un k así. Tomemos entonces el conjunto: $\{k : \ k \in A(P_r; j_3) \ ; \ (k : e_i) = 1\} - B$. Deberíamos poder mostrar que este conjunto es distinto de vacío. Veamos:

$$\sharp\{k : \ k \in A(P_r; j_3) \ ; \ (k : e_i) = 1\} = \sharp Y_i$$

que según (8.20) es $\sharp Y_i > \frac{\epsilon n}{5P_r}$.

Y en B hay $\frac{\epsilon n}{8P_r}$ elementos.Luego como $\frac{\epsilon n}{5P_r} > \frac{\epsilon n}{8P_r}$ el conjunto $\{k : \ k \in A(P_r; j_3) \ ; \ (k : e_i) = 1\} - B \neq \emptyset$

Veamos ahora que este conjunto $\{k : \ k \in A(P_r; j_3) \ ; \ (k : e_i) = 1\} - B$ contiene por lo menos l elementos.

Ahora

$$\sharp\big(\{k : \ k \in A(P_r; j_3) \ ; \ (k : e_i) = 1\} - B\big) \geq$$
$$\sharp\{k : \ k \in A(P_r; j_3) \ ; \ (k : e_i) = 1\} - \sharp B$$

y acotando esta resta es $> \frac{\epsilon n}{5P_r} - \frac{\epsilon n}{8P_r}$ Queremos mostrar que este conjunto contiene l cosas y esto ocurre si

$$\frac{\epsilon n}{5P_r} - \frac{\epsilon n}{8P_r} = \frac{3\epsilon n}{40P_r} \geq l$$

Igual que antes veamos:

$$\frac{3\epsilon n}{40P_r} \geq l \Leftrightarrow l \leq \frac{3\epsilon n}{40P_r}$$

Ahora por hipótesis l debe cumplir $l \leq c_3(\epsilon)n$, luego bastará pedir que $c_3(\epsilon) \leq \frac{3\epsilon}{40P_r}$ con $c_3(\epsilon)$ así se cumple:

$$l \leq c_3(\epsilon)n \leq \frac{3\epsilon}{40P_r}n$$

Y por lo tanto podemos elegir l cosas en

$$\{k : \ k \in A(P_r; j_3) \ ; \ (k : e_i) = 1\} - B$$

Elegimos entonces $c_1, c_2, c_3, \ldots, c_l$ que satisfacen:

$$(e_i : c_i) = 1 \qquad , \qquad c_i \in A(P_r, j_3) \qquad \text{y}$$

$$\prod_{p|c_i,\ p>r} \left(1 - \frac{1}{p}\right) > 1 - \frac{\epsilon}{8} \text{ para todo} 1 \leq i \leq l \tag{8.21}$$

Entonces ahora con $a, b_1, b_2, \ldots, b_l, c_1, c_2, \ldots, c_l$ que son $2l+1$ elementos formamos el siguiente $2l + 1 - ciclo$:

$$a,\ b_1,\ c_1,\ b_2,\ c_2,\ b_3,\ c_3, \ldots,\ b_l,\ c_l$$

Veamos que efectivamente esta secuencia forma un $2l+1-ciclo$ contenido en $\mathcal{G}(A)$, para esto debemos ver:

- $a, b_1, c_1, b_2, c_2, b_3, c_3, \ldots, b_l, c_l$ pertenecen a A
- $(a, b_1) = 1$. Ya que por elección de b_i verifica $(b_i, a) = 1$. En particular b_1
- $(b_i, c_i) = 1$ para todo $i = 1, \ldots, l$ Pues si existe p tal que $p|b_i$, entonces $p|e_i = [b_i, b_{i+1}]$.Ahora como por elección de los c_i tenemos $(c_i, e_i) = 1$ entonces $p \not| c_i$.Luego $(b_i, c_i) = 1$
- $(c_i, b_{i+1}) = 1$ para todo $i = 1, \ldots, l-1$. Igual que el caso anterior.
- $(c_l, a) = 1$ ya que si $p|a$ entonces $p|[b_l, a] = e_l$. Ahora como $(e_l, c_l) = 1$ entonces $p \not| c_l$

Luego, $a,\ b_1,\ c_1,\ b_2,\ c_2, \ldots,\ b_l,\ c_l$ forman un $2l + 1 - ciclo$ contenido en $\mathcal{G}(A)$

FIN

Bibliografía

[1] R. Ahlswede y L.H. Khachatrian, *On extremal sets without coprimes*, Acta Arithmetica, LXVI.1 (1994), 89–99.

[2] P. Erdös, *Some remarks about additive and multiplicative functions*, Bull. Amer. Math. Soc. (1946), 132–136.

[3] P. Erdös, *Remarks in number theory, IV* (in Hungarian), Mat. Lapok, 13 (1962), 228–255.

[4] P. Erdös, R. Freud y N. Hegyvári, *Arithmetical properties of permutations of integers*, Acta Math. Acad. Sci. Hung., 41 (1983), 169–176.

[5] P. Erdös y C. Pomerance, *Matching the natural numbers up to n with distinct multiples in another interval*, Nederl. Akad. Wetensch. Proc. Ser. A, 83 (1980), 147–161.

[6] P. Erdös and G.N. Sarkozy, *On cycles in the coprime graph of integers*, Electronic J. Combinatorics, 4 (2) (1997), 1–11.

[7] P. Erdös, A. Sárközy and E. Szemerédi, *On some extremal properties of sequences of integers, I*, Ann. Univ. Sci. Budapest Eötvös, 12 (1969), 131–135, *II.*, Publ. Math. Debrecen, 27 (1980), 117–125.

[8] R.L. Graham, M. Grötschel, L. Lovász (editors), Handbook of Combinatorics, MIT Press.

[9] I. Niven, H.S. Zuckerman, H.L. Montgomery, An introduction to the theory of numbers, 5th edition, John Wiley & Sons, 1991.

[10] C. Pomerance, *On the longest simple path in the divisor graph*, Congressus Numerantium, 40 (1983), 291–304.

[11] E. Saias, *Etude du graphe divisoriel, I*, Periodica Math. Hung., por aparecer.

[12] C. Szabó and G. Tóth, *Maximal sequences not containing 4 pairwise coprime integers* (in Hungarian), Mat. Lapok, 32 (1985), 253–257.