UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO

POSGRADO CONJUNTO EN CIENCIAS MATEMÁTICAS
UNAM-UMSNH

SUMA DE CARACTERES Y EL MÍNIMO NO-RESTO CUADRÁTICO

TESIS
QUE PARA OPTAR POR EL GRADO DE:

MAESTRO EN CIENCIAS MATEMÁTICAS

PRESENTA:

LIC. CÉSAR ALFONSO DÍAZ MIJANGOS

DIRECTOR DE TESIS:

DR. MOUBARIZ GARAEV

MORELIA, MICHOACÁN, ENERO 2016.

Índice general

Abstract/Resumen

Abstract. One of the more interesting problems in Number Theory is to study the distribution of the quadratic residues in the complete system of residues modulo a prime $p > 2$. In the present thesis we study the problem of find bounds for the least quadratic non-residue $n(p)$. We exposed the estimates on character sums found by Vinogradov, which allowed him to obtain the bound $n(p) = O_\varepsilon(p^{\frac{1}{2\sqrt{e}}+\varepsilon})$.

We also explain the work of Burgess on the estimate of incomplete character sums, which rest on a powerful result of André Weil. These estimates allowed him to improve the result of Vinogradov to $n(p) = O_\varepsilon(p^{\frac{1}{4\sqrt{e}}+\varepsilon})$.

Finally we pointing out that the problem of find better estimates on $n(p)$ remains open.

Keywords: Quadratic residue, Quadratic non-residue, Dirichlet characters, Character sums, Incomplete sums.

Resumen. Uno de los problemas más interesantes en la Teoría de Números es estudiar la distribución de los restos cuadráticos dentro del sistema completo de restos módulo un primo $p > 2$. En la presente tesis se estudia el problema de determinar cotas para el menor no-resto cuadrático $n(p)$. Se exponen las estimaciones sobre sumas de caracteres halladas por Vinogradov, las cuales le permitieron obtener la estimación $n(p) = O_\varepsilon(p^{\frac{1}{2\sqrt{e}}+\varepsilon})$.

También se explica el trabajo de Burgess sobre la estimación de sumas incompletas de caracteres, el cual se basa en un poderoso resultado de André Weil. Estas estimaciones le permiten mejorar el resultado de Vinogradov a $n(p) = O_\varepsilon(p^{\frac{1}{4\sqrt{e}}+\varepsilon})$.

Finalmente señalamos que el problema de obtener mejores estimaciones de $n(p)$ sigue abierto.

Palabras clave: Resto cuadrático, No-resto cuadrático, Caracteres de Dirichlet, Sumas de caracteres, Sumas incompletas.

Introducción

La presente tesis tiene como principal objetivo estudiar el problema de estimar la magnitud del mínimo no-resto cuadrático positivo $n(p)$, para $p > 2$ un número primo. A pesar de la sencillez con que se enuncia éste problema ha resultado ser bastante complicado de atacar. El primero en considerarlo fue Gauss [4] quien en 1796 obtuvo que $n(p) \leq 2\sqrt{p}$. Este resultado se mantuvo prácticamente sin cambios por más de un siglo, hasta que en 1918 I. M. Vinogradov [5] haciendo uso de estimaciones sobre sumas de caracteres fue capaz de mejorarlo, obteniendo la estimación más precisa

$$n(p) = O_\varepsilon(p^{\frac{1}{2\sqrt{e}}+\varepsilon}) \tag{1}$$

para todo $\varepsilon > 0$. En otras palabras, para cualquier $\varepsilon > 0$ existe una constante $C > 0$ que depende de ε, tal que

$$n(p) < Cp^{\frac{1}{2\sqrt{e}}+\varepsilon}.$$

Este resultado se mantuvo como el mejor hasta 1957 cuando D. A. Burgess [1], haciendo uso de un poderoso teorema de André Weil sobre suma de caracteres evaluados en polinomios, obtiene una mejora sustancial en la estimación de sumas incompletas de caracteres con lo cual consigue reducir el tamaño de la cota hallada por Vinogradov a

$$n(p) = O_\varepsilon(p^{\frac{1}{4\sqrt{e}}+\varepsilon}) \tag{2}$$

para todo $\varepsilon > 0$. Salvo pequeñas mejoras en el factor p^ε esta estimación se mantiene como la mejor hasta el momento.

Vinogradov también propone la siguiente conjetura.

Conjetura 0.1. *Para todo $\varepsilon > 0$ se cumple que $n(p) = O(p^\varepsilon)$.*

Cabe mencionar que en 1942, Yu. V. Linnik [3] demuestra que bajo la asunción de la hipótesis generalizada de Riemann, la conjetura de Vinogradov es cierta.

La tesis consta de dos capítulos, en el capítulo 1 se presentan los resultados que serán necesarios para introducir y atacar el problema del mínimo no-resto cuadrático. Así pues se presenta el símbolo de Legendre y las propiedades de éste que nos interesan para plantear el problema. También en este capítulo aparece el concepto de carácter módulo un primo $p > 2$, mismo que resulta fundamental en la teoría de números.

El capítulo 2 consta de los resultados y técnicas principales en el estudio del mínimo no-resto cuadrático. Se presentan las sumas incompletas de caracteres y se aplican al caso especial del símbolo de Legendre para deducir las estimaciones de $n(p)$.

Durante este trabajo se hace uso de la notación asintótica de Landau, a saber, para $f(x)$ y $g(x) > 0$ funciones definidas en $[A, \infty)$ escribimos $f(x) = O(g(x))$ si existen $x_0 \in [A, \infty)$ y $C > 0$ constante tales que $|f(x)| \leq Cg(x)$ para cada $x \geq x_0$. Y escribimos $f(x) = o(g(x))$ cuando $x \to \infty$, si $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$.

La siguiente notación es utilizada en este trabajo. La parte entera de x se denota por $\lfloor x \rfloor$ y es igual al mayor entero que no es superior a x, el techo de x se denota como $\lceil x \rceil$ y es igual al menor entero que no es inferior a x. Con $\{x\}$ se representa la parte fraccionaria de x la cual está dada por $\{x\} = x - \lfloor x \rfloor$. Con $||x||$ se indica la distancia de x al entero más cercano.

Para p un número primo se denota con $\mathbb{F}_p$ al campo clases residuales módulo p. Con frecuencia los elementos de $\mathbb{F}_p$ serán elegidos como los mínimos representantes no negativos de cada clase residual, es decir, $\{0, 1, 2, ..., p-1\}$. Con ${\mathbb{F}_p}^*$ se denota al grupo cíclico que consta de los elementos de $\mathbb{F}_p$ que son primos relativos con p. Una raíz primitiva módulo p es cualquier generador de ${\mathbb{F}_p}^*$. Dados un entero g raíz primitiva módulo p y n un entero no divisible por p, existe $k \geq 0$ entero tal que $g^k \equiv n \pmod{p}$, tal entero es llamado el índice de n respecto a g módulo p y se denota por $\operatorname{ind}_g n$. Se hace la observación de que el $\operatorname{ind}_g n$ está definido módulo $p-1$, en este trabajo tomaremos siempre el valor que se halle en $\{0, 1, ..., p-2\}$.

Nos apegaremos a la representación usual del anillo de polinomios, es decir, dado un anillo R el anillo de polinomios con coeficientes en R se denota por $R[x]$. Si $f(x) \in R[x] \setminus \{0\}$, el grado de $f(x)$ se denota por $deg\, f$.

Capítulo 1

Preliminares

1.1 Símbolo de Legendre

Consideremos los enteros a, m, n tales que $n > 1$ y $(a, m) = 1$. Se dice que a es un resto de grado n módulo m si la congruencia:

$$x^n \equiv a \ (\texttt{mód}\ m)$$

tiene solución. En caso contrario, a es llamado no-resto de grado n. Cuando $n = 2$ los restos y no-restos se llaman cuadráticos; si $n = 3$, cúbicos; $n = 4$, bicuadráticos. Nosotros solo estaremos interesados en los restos y no-restos cuadráticos módulo un primo $p > 2$.

Notemos que si a es un resto cuadrático módulo p, la congruencia $x^2 \equiv a \ (\texttt{mód}\ p)$ admite dos soluciones. Pues si $x \equiv x_1 \ (\texttt{mód}\ p)$ es solución, entonces $x \equiv -x_1 \ (\texttt{mód}\ p)$ también será solución. Además no puede ocurrir que $x_1 \equiv -x_1 \ (\texttt{mód}\ p)$, pues en este caso tendríamos $2x_1 \equiv 0 \ (\texttt{mód}\ p)$, ya que p es impar se seguiría que $x_1 \equiv 0 \ (\texttt{mód}\ p)$.

Una consecuencia de lo anterior es que en el sistema reducido de restos módulo p hay exactamente $\frac{p-1}{2}$ restos cuadráticos, mismos que son congruentes con los números $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$, y $\frac{p-1}{2}$ no-restos cuadráticos.

Un conocido teorema de Lagrange en teoría elemental de números afirma que para p primo y $f(x) \in \mathbb{Z}[x]$, la congruencia $f(x) \equiv 0 \ (\texttt{mód}\ p)$ tiene a lo más $deg\, f(x)$ soluciones incongruentes. Una aplicación de este resultado, del pequeño teorema de Fermat y lo expuesto en el párrafo anterior nos permiten obtener la siguiente proposición.

Proposición 1.1. *El entero a es un resto cuadrático módulo p si y sólo si*

$$a^{\frac{p-1}{2}} \equiv 1 \ (\texttt{mód}\ p).$$

Definición 1.1. *Sea $p > 2$ primo y a un entero. El símbolo de Legendre $\left(\frac{a}{p}\right)$ se define*

por:

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{si } \ a \equiv 0 \ (\texttt{mód}\ p). \\ 1 & \text{si } a \textit{ es resto cuadrático.} \\ -1 & \text{si } a \textit{ es no-resto cuadrático.} \end{cases} \tag{1.1}$$

En el siguiente teorema se enuncian algunas de las propiedades básicas del símbolo de Legendre.

Teorema 1.1. *Sea $p > 2$ primo. Entonces las siguientes afirmaciones tienen lugar*

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (\texttt{mód}\ p)$.

2. *Si* $a \equiv b \ (\texttt{mód}\ p)$, *entonces* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

3. *Para cualesquiera* $a, b \in \mathbb{Z}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

En el presente trabajo será de gran importancia el estudio de sumas que involucran al símbolo de Legendre. Entre las sumas más sencillas están las siguientes.

Teorema 1.2. *Sea $p > 2$ primo y k entero con $(k, p) = 1$. Entonces*

a) $\displaystyle\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$

b) $\displaystyle\sum_{a=1}^{p-1} \left(\frac{a(a+k)}{p}\right) = -1.$

Demostración: a) Se sigue de que hay el mismo número de restos cuadráticos que de no-restos cuadráticos.

b) Dado $a \not\equiv 0 \pmod{p}$ sea a^* el entero positivo mínimo con $aa^* \equiv 1 \pmod{p}$. Entonces

$$\begin{aligned}\sum_{a=1}^{p-1}\left(\frac{a(a+k)}{p}\right) &= \sum_{a=1}^{p-1}\left(\frac{a(a+k)}{p}\right)\left(\frac{a^*a^*}{p}\right)\\ &= \sum_{a=1}^{p-1}\left(\frac{aa^*(a+k)a^*}{p}\right)\\ &= \sum_{a=1}^{p-1}\left(\frac{1+ka^*}{p}\right)\\ &= \sum_{n=1}^{p-1}\left(\frac{1+n}{p}\right)\\ &= -\left(\frac{1}{p}\right)\\ &= -1.\end{aligned}$$

□

1.2 Caracteres

Definición 1.2. *Sea m entero positivo. Un carácter de Dirichlet módulo m es una función $\chi : \mathbb{Z} \to \mathbb{C}$ que no es identicamente cero y que satisface:*

1. $\chi(n) = 0$, *si* $(n, m) > 1$.
2. $\chi(n + m) = \chi(n)$.
3. $\chi(nr) = \chi(n)\chi(r)$.

Por definición se tiene que $\chi(0) = 0$ para cualquier carácter χ. Además si n es tal que $\chi(n) \neq 0$, entonces como $\chi(n) = \chi(n)\chi(1)$, se tiene que $\chi(1) = 1$.

Nosotros estaremos interesados en los caracteres módulo un primo $p > 2$. En este caso tenemos que si χ es un carácter y g una raíz primitiva módulo p, entonces

$$\chi(g)^{p-1} = \chi(g^{p-1}) = \chi(1) = 1.$$

Luego $\chi(g)$ es una raíz $(p-1)$-ésima de la unidad. Sabemos que para todo $n \not\equiv 0 \pmod{p}$ existe $k = \operatorname{ind}_g n$ tal que $n = g^k$. Ahora para cada $a = 0, 1, ..., p-2$ sean

$$\chi_a(n) = \begin{cases} 0 & \text{si } n \equiv 0 \pmod{p}. \\ e^{2\pi i \frac{ind_g\ n}{p-1} a} & \text{si } n \not\equiv 0 \pmod{p}. \end{cases} \tag{1.2}$$

De este modo quedan definidos $p-1$ caracteres distintos módulo p.

Reciprocamente, es fácil ver que para cada $a \in \{0,1,2,...,p-2\}$ fijo, la función $\chi_a(n)$ definida de esta manera satisface los requisitos de la Definición 1.2. De este modo quedan definidos todos los caracteres módulo p, habiendo por lo tanto $p-1$ de ellos. Nótese que en particular el conjunto de caracteres no depende de la elección de la raíz primitiva g.

Al carácter χ_0 se le llama *carácter principal*. El *orden* de un carácter χ es el menor entero positivo d tal que $\chi^d = \chi_0$.

Proposición 1.2. *Sea $p > 2$ primo, entonces $\chi(n) = \left(\frac{n}{p}\right)$ es un carácter de orden 2.*

Demostración: Que χ es carácter se sigue de la definición del símbolo de Legendre y de los puntos 2 y 3 del Teorema 1.1. Solo resta ver que su orden es 2, pero esto es claro pues $\left(\frac{n}{p}\right)^2 = 1$ si $(n,p) = 1$ y $\left(\frac{n}{p}\right)^2 = 0$ si $(n,p) = p$. Además como $p > 2$ siempre habrá no-restos cuadráticos con lo que el orden de χ no puede ser 1. □

1.3 Teorema de Chebyshev sobre distribución de los números primos

Teorema 1.3 (Fórmula de Sumación Parcial)**.** *Sea c_n un conjunto de números complejos y $f(u) \in \mathrm{C}^1[a,b]$. Entonces*

$$\sum_{a<n\leq b} c_n f(n) = -\int_a^b \mathbf{C}(u) f'(u)du + \mathbf{C}(b)f(b)$$

donde $\mathbf{C}(u) = \sum_{a<n\leq u} c_n$.

Demostración: Se tiene que

$$\begin{aligned}\mathbf{C}(b)f(b) - \sum_{a<n\leq b} c_n f(n) &= \sum_{a<n\leq b} c_n \left(f(b) - f(n)\right) = \sum_{a<n\leq b} c_n \int_n^b f'(u)du \\ &= \sum_{a<n\leq b} c_n \int_a^b g(u,n) f'(u)du\end{aligned}$$

donde $g(u,n) = \begin{cases} 1 & \text{si } n \leq u \leq b \\ \\ 0 & \text{si } a < u < n \end{cases}$.

Entonces

$$\begin{aligned}\mathbf{C}(b)f(b) - \sum_{a<n\leq b} c_n f(n) &= \int_a^b \sum_{a<n\leq b} c_n g(u,n) f'(u)du \\ &= \int_a^b \sum_{a<n\leq u} c_n f'(u)du \\ &= \int_a^b \mathbf{C}(u)f'(u)du.\end{aligned}$$

□

Teorema 1.4 (Fórmula de Sumación de Euler)**.** *Sea* $f(u) \in \mathrm{C}^1[\mathrm{a},\mathrm{b}]$*, se tiene que*

$$\sum_{a<n\leq b} f(n) = \int_a^b f(u)\ du + \rho(b)f(b) - \rho(a)f(a) - \int_a^b \rho(u)f'(u)\ du \tag{1.3}$$

donde $\rho(u) = \frac{1}{2} - \{u\}$.

Más aún si se cumple que $f(u) \in \mathrm{C}^2[\mathrm{a},\mathrm{b}]$*, entonces*

$$\sum_{a<n\leq b} f(n) = \int_a^b f(u)\ du + \rho(b)f(b) - \rho(a)f(a) + \sigma(a)f'(a) - \sigma(b)f'(b) + \int_a^b \sigma(u)f''(u)\ du \tag{1.4}$$

donde $\sigma(u) = \displaystyle\int_0^u \rho(t)\ dt$.

Demostración: Para probar la Fórmula (1.3) apliquemos la fórmula de sumación parcial con $c_n = 1$. Observemos que

$$\begin{aligned}\mathbf{C}(u) = \sum_{a<n\leq u} 1 &= [u] - [a] = (u - \{u\}) - (a - \{a\}) = u - a + \frac{1}{2} - \{u\} - \frac{1}{2} + \{a\} \\ &= u - a + \rho(u) - \rho(a).\end{aligned}$$

Entonces sustituyendo en la fórmula de sumación parcial e integrando por partes se tiene

$$\begin{aligned}\sum_{a<n\leq b} f(n) &= -\int_a^b (u - a - \rho(a) + \rho(u))f'(u)\ du + (b - a + \rho(b) - \rho(a))f(b) \\ &= -(u - a - \rho(a))f(u)\Big|_a^b + \int_a^b f(u)\ du - \int_a^b \rho(u)f'(u)\ du + \\ &+ (b - a + \rho(b) - \rho(a))f(b) \\ &= \int_a^b f(u)\ du + \rho(b)f(b) - \rho(a)f(a) - \int_a^b \rho(u)f'(u)\ du.\end{aligned}$$

Para la Fórmula (1.4) obsérvese que la integración por partes nos da

$$\begin{aligned}\int_a^b \rho(u)f'(u)\,du &= \left(\int_0^u \rho(t)\,dt\right) f'(u)|_a^b - \int_a^b \left(\int_0^u \rho(t)\,dt\right) f''(u)\,du \\ &= \sigma(b)f'(b) - \sigma(a)f'(a) - \int_a^b \sigma(u)f''(u)\,du.\end{aligned}$$

Luego sustituyendo esta igualdad en (1.3) se obtiene el resultado. □

Proposición 1.3. *Sea n entero positivo. Entonces*

$$n! = \prod_p p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots} \tag{1.5}$$

donde el producto corre en los números primos.

Demostración: Observemos que dados n entero positivo y p un primo, la máxima potencia k de p que divide a $n!$ está dada por

$$k = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + ...$$

En efecto, entre los números $1, 2, ..., n$ exactamente $\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor$ son divisibles por p^i pero no por p^{i+1}. De este modo, si k es la mayor potencia de p que divide a $n!$ se tiene

$$\begin{aligned}k &= \left(\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor\right) + 2\left(\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor\right) + 3\left(\left\lfloor \frac{n}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^4} \right\rfloor\right) + ... \\ &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + ...\end{aligned}$$

Esta observación implica que $n! = \prod_p p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots}$. □

Definición 1.3. *Para $x > 0$ la función ψ de Chebyshev se define por la fórmula*

$$\psi(x) = \sum_{m \geq 1} \sum_{\substack{p \\ p^m \leq x \\ primo}} \log p \tag{1.6}$$

Proposición 1.4. *Sea n entero positivo. Se cumple que*

$$\log n! = \psi(n) + \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{3}\right) + ...$$

Demostración: Por la Proposición 1.3 se tiene

$$\log n! = \log \prod_p p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots} = \sum_{p \text{ primo}} \left(\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + ... \right) \log p$$
$$= \sum_{p \text{ primo}} \log p \sum_{m \geq 1} \left\lfloor \frac{n}{p^m} \right\rfloor .$$

Por otro lado

$$\sum_{t \geq 1} \psi\left(\frac{n}{t}\right) = \sum_{t \geq 1} \sum_{m \geq 1} \sum_{\substack{p^m \leq \frac{n}{t} \\ p \text{ primo}}} \log p = \sum_{p \text{ primo}} \sum_{t \geq 1} \sum_{m \geq 1} \sum_{p^m t \leq n} \log p$$
$$= \sum_{p \text{ primo}} \log p \sum_{t \geq 1} \sum_{m \geq 1} \sum_{p^m t \leq n} 1 = \sum_{p \text{ primo}} \log p \sum_{m \geq 1} \sum_{t \geq 1} \sum_{p^m t \leq n} 1$$
$$= \sum_{p \text{ primo}} \log p \sum_{m \geq 1} \sum_{t \geq 1} \sum_{1 \leq t \leq \frac{n}{p^m}} 1$$
$$= \sum_{p \text{ primo}} \log p \sum_{m \geq 1} \left\lfloor \frac{n}{p^m} \right\rfloor$$

Por lo tanto ambas expresiones coinciden. □

Teorema 1.5. *Sea $n > 1$ entero, se cumple que*

$$\log n! = n \log n - n + \frac{1}{2} \log n + 1 + O\left(\frac{1}{n}\right).$$

Demostración: Obsérvese que $\log n! = \sum_{1 < t \leq n} \log t$. Luego aplicando la segunda fórmula de sumación de Euler con $f(u) = \log u$ se tiene

$$\log n! = \int_1^n \log u \; du + \rho(n) \log n - \rho(1) \log + \sigma(1) \frac{1}{1} - \sigma(n) \frac{1}{n} + \int_1^n \sigma(u) \left(\log u\right)'' \; du$$

Ahora obsérvese que $\sigma(n) = 0$ para n entero, y $0 \leq \sigma(u) \leq \frac{1}{8}$. Entonces

$$\log n! = (u \log u - u)|_1^n + \frac{1}{2} \log n + \int_1^n \sigma(u) \left(\frac{1}{u}\right)' \; du$$
$$= n \log n - n + 1 + \frac{1}{2} \log n + O\left(\frac{1}{n}\right).$$

Por lo tanto

$$\log n! = n \log n - n + \frac{1}{2} \log n + 1 + O\left(\frac{1}{n}\right).$$

□

Los resultados anteriores nos permiten obtener la siguiente estimación de Chebyshev acerca de la función $\psi(x)$.

Teorema 1.6 (Chebyshev)**.** *Existen constantes positivas A, B tales que*

$$An \leq \psi(n) \leq Bn.$$

Demostración: Por los Teoremas 1.4 y 1.5 se tiene

$$\psi(n) + \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{3}\right) + \psi\left(\frac{n}{4}\right) + ... = n\log n - n + \theta_1(n)\log n, \tag{1.7}$$

con $|\theta_1(n)| \leq 2$ digamos. Ahora si multiplicamos (1.7) por 2 y sustituimos n por $\frac{n}{2}$ se obtiene

$$2\left(\psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{4}\right) + \psi\left(\frac{n}{6}\right) + ...\right) = n\log\frac{n}{2} - n + \theta_2(n)\log\frac{n}{2}, \tag{1.8}$$

donde $|\theta_2(n)| \leq 4$.

Restando (1.8) de (1.7) se llega a

$$\psi(n) - \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{3}\right) - \psi\left(\frac{n}{4}\right) + ... = n\log 2 + \theta_3(n)\log 2, \tag{1.9}$$

con $|\theta_3(n)| \leq 6$. Ahora obsérvese que

$$\left(\psi\left(\frac{n}{3}\right) - \psi\left(\frac{n}{2}\right)\right) + \left(\psi\left(\frac{n}{5}\right) - \psi\left(\frac{n}{4}\right)\right) + \left(\psi\left(\frac{n}{7}\right) - \psi\left(\frac{n}{6}\right)\right) + ... \leq 0.$$

De esto se sigue que

$$\begin{aligned}\psi(n) &\geq \psi(n) - \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{3}\right) - \psi\left(\frac{n}{4}\right) + ... \\ &\geq n\log 2 - 6\log 2 \\ &\geq \frac{1}{3}n.\end{aligned} \tag{1.10}$$

Donde la última desigualdad se verifica para $n \geq 12$. Además como

$$\begin{aligned}\psi(n) - \psi\left(\frac{n}{2}\right) &\leq \psi(n) - \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{3}\right) - \psi\left(\frac{n}{4}\right) + ... \\ &\leq n\log 2 + 6\log 2 \\ &\leq 7n,\end{aligned}$$

tenemos

$$\begin{aligned}\psi(n) - \psi\left(\frac{n}{2}\right) &\leq 7n \\ \psi\left(\frac{n}{2}\right) - \psi\left(\frac{n}{4}\right) &\leq 7\left(\frac{n}{2}\right) \\ \psi\left(\frac{n}{4}\right) - \psi\left(\frac{n}{6}\right) &\leq 7\left(\frac{n}{4}\right) \\ &\vdots\end{aligned}$$

Sumando sobre ambos lados de estas desigualdades se llega a

$$\psi(n) \leq 7n\left(1 + \frac{1}{2} + \frac{1}{2^2} + ...\right) = 14n. \tag{1.11}$$

El teorema se sigue ahora de las desigualdades (1.10) y (1.11). □

1.4 Estimaciones de Mertens

A continuación se presentan dos resultados de Mertens acerca de la distribución de los números primos. La segunda de estas estimaciones será clave en la obtención de las cotas del mínimo no-resto cuadrático que se expondrán en el próximo capítulo.

Teorema 1.7 (Mertens)**.** *Para $x \geq 2$ se cumple* $\displaystyle\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1)$.

Demostración: Notemos que de los Teoremas 1.4 y 1.5 se tiene

$$\begin{aligned} n\log n - n + O(\log n) &= \sum_{\substack{p \leq n \\ p \text{ primo}}} \left(\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + ...\right) \log p \\ &= \sum_{\substack{p \leq n \\ p \text{ primo}}} \left(\frac{n}{p} - \left\{\frac{n}{p}\right\} + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + ...\right) \log p \\ &= \sum_{\substack{p \leq n \\ p \text{ primo}}} \frac{n}{p} \log p - \sum_{\substack{p \leq n \\ p \text{ primo}}} \left\{\frac{n}{p}\right\} \log p + O\left(\sum_{\substack{p \leq n \\ p \text{ primo}}} \frac{n}{p^2} (\log p)^2\right) \\ &= n \sum_{\substack{p \leq n \\ p \text{ primo}}} \frac{\log p}{p} + O\left(\sum_{\substack{p \leq n \\ p \text{ primo}}} \log p\right) + O(n) \end{aligned} \tag{1.12}$$

$$= n \sum_{\substack{p \leq n \\ p \text{ primo}}} \frac{\log p}{p} + O(n).$$

La última igualdad se sigue del Teorema 1.6, pues

$$\sum_{\substack{p \leq n \\ p \text{ primo}}} \log p \leq \psi(n) = O(n).$$

Por lo tanto

$$n \sum_{\substack{p \leq n \\ p \text{ primo}}} \frac{\log p}{p} + O(n) = n \log n - n + O(\log n).$$

El resultado se obtiene al dividir esta última igualdad entre n. □

Teorema 1.8 (Mertens)**.** *Existe una constante C tal que para $x \geq 2$ se cumple*

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

Demostración: Aplicando la fórmula de sumación parcial con

$$f(u) = \frac{1}{\log u} \quad \text{y} \quad c_n = \begin{cases} \frac{\log n}{n} & \text{si } n \text{ es primo,} \\ \\ 0 & \text{en otro caso,} \end{cases}$$

se tiene que $\mathbf{C}(x) = \sum_{p \leq x} \frac{\log p}{p}$. Entonces

$$\begin{aligned}
\sum_{p \leq x} \frac{1}{p} &= \sum_{\frac{3}{2} < n \leq x} c_n f(n) = -\int_{\frac{3}{2}}^{x} \frac{\mathbf{C}(u)}{u \log^2 u} du + \mathbf{C}(x) \frac{1}{x} \\
&= \int_{\frac{3}{2}}^{x} \frac{\log u + O(1)}{u \log^2 u} du + \frac{\log x + O(1)}{\log x} \\
&= \int_{\frac{3}{2}}^{x} \frac{du}{u \log u} + \int_{\frac{3}{2}}^{x} \frac{O(1)}{u \log^2 u} du + 1 + O\left(\frac{1}{\log x}\right) \\
&= \log \log u \Big|_{\frac{3}{2}}^{x} + \int_{\frac{3}{2}}^{\infty} \frac{O(1)}{u \log^2 u} du - \int_{x}^{\infty} \frac{O(1)}{u \log^2 u} du + 1 + O\left(\frac{1}{\log x}\right) \\
&= \log \log x - \log \log \frac{3}{2} + 1 + C_1 + O\left(\int_{x}^{\infty} \frac{du}{u \log^2 u}\right) + O\left(\frac{1}{\log x}\right) \\
&= \log \log x + C + O\left(\frac{1}{\log x}\right).
\end{aligned}$$

□

1.5 La función divisor

Definición 1.4. *La función divisor $\tau(n)$ está definida como el número de divisores positivos de n. Obsérvese que si $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ es la descomposición canónica de n, entonces*

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1).$$

El siguiente teorema nos da información sobre el comportamiento asintótico de la función divisor. Esta información será utilizada en el siguiente capítulo para estimar el número de soluciones a ciertas congruencias.

Teorema 1.9. *Para cada $\varepsilon > 0$ existe $C = C(\varepsilon)$ tal que $\tau(n) \leq Cn^{\varepsilon}$.*

Demostración: Sean $\varepsilon > 0$ y $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ la descomposición canónica de n. Entonces

$$\frac{\tau(n)}{n^{\varepsilon}} = \frac{(\alpha_1 + 1)}{p_1^{\alpha_1 \varepsilon}} ... \frac{(\alpha_k + 1)}{p_k^{\alpha_k \varepsilon}} = \prod_{\substack{\alpha \geq 1 \\ p \text{ primo tal que } \frac{\alpha+1}{p^{\alpha\varepsilon}} \geq 1}} \frac{\alpha + 1}{p^{\alpha\varepsilon}}. \tag{1.13}$$

Como $\frac{\alpha+1}{2^{\alpha\varepsilon}} \geq 1$, entonces $\alpha + 1 \geq 2^{\alpha\varepsilon} \geq e^{\frac{\alpha\varepsilon}{2}} \geq 1 + \frac{\left(\frac{\alpha\varepsilon}{2}\right)^2}{2}$. Luego

$$\alpha \leq \frac{8}{\varepsilon^2}. \tag{1.14}$$

También se tiene que $\frac{\alpha+1}{p^{\alpha\varepsilon}} \geq 1$, entonces

$$\alpha + 1 \geq p^{\alpha\varepsilon} = e^{\alpha\varepsilon \log p} \geq 1 + \alpha\varepsilon \log p.$$

Se sigue que

$$p \leq e^{\frac{1}{\varepsilon}} \tag{1.15}$$

Además

$$\frac{\alpha + 1}{p^{\alpha\varepsilon}} \leq \frac{2\alpha}{2^{\alpha\varepsilon}} \leq \frac{2\alpha}{\alpha\varepsilon \log 2} \leq \frac{3}{\varepsilon}. \tag{1.16}$$

De (1.14), (1.15) y (1.16) se tiene

$$\frac{\tau(n)}{n^{\varepsilon}} \leq \prod_{\substack{\alpha \leq \frac{8}{\varepsilon^2} \\ p \leq e^{\frac{1}{\varepsilon}}}} \frac{3}{\varepsilon} = C. \qquad \square$$

Capítulo 2

Suma de caracteres y el mínimo no-resto cuadrático

Por lo visto en el capítulo anterior para $p > 2$ primo hay $\frac{p-1}{2}$ restos y no-restos cuadráticos módulo p. Uno de los problemas más importantes en Teoría Analítica de los Números es determinar cómo se distribuyen los restos y no-restos cuadráticos dentro del sistema reducido $1, 2, ..., p-1$. En particular uno está interesado en conocer la distribución de éstos en intervalos de longitud pequeña, para este problema uno puede centrar la atención en determinar cuál es el orden de magnitud del mínimo no-resto cuadrático positivo $n(p)$ para un primo p grande.

La manera natural de estimar a $n(p)$ es mediante sumas de símbolos de Legendre, lo cual es un caso particular de suma de caracteres.

2.1 Estimaciones de sumas de caracteres

Teorema 2.1. *Sean p primo y Q enteros tales que $1 < Q < p$. Considérese la suma $S = \sum_{x=0}^{p-1} S_x^2$, donde $S_x = \sum_{z=0}^{Q-1} \left(\frac{x+z}{p}\right)$. Entonces $S = (p-Q)Q$.*

Demostración: Tenemos que

$$S = \sum_{x=0}^{p-1} \left(\sum_{z=0}^{Q-1} \left(\frac{x+z}{p}\right)\right)^2 = \sum_{x=0}^{p-1} \sum_{z=0}^{Q-1} \sum_{z_1=0}^{Q-1} \left(\frac{(x+z)(x+z_1)}{p}\right)$$
$$= \sum_{z=0}^{Q-1} \sum_{z_1=0}^{Q-1} \sum_{x=0}^{p-1} \left(\frac{(x+z)(x+z_1)}{p}\right).$$

Para $z \in \{0, 1, 2, ..., Q-1\}$ fijo, si x recorre el sistema completo de restos módulo p,

entonces $x+z$ también lo hará. Luego, sustituyendo $y=x+z$, podemos escribir

$$S=\sum_{z=0}^{Q-1}\sum_{z_1=0}^{Q-1}\sum_{y=0}^{p-1}\left(\frac{y(y+z_1-z)}{p}\right)=(p-1)Q+(-1)(Q^2-Q)=(p-Q)Q. \qquad \square$$

Este teorema nos permite obtener una primer estimación no trivial para $n(p)$. En efecto, si aceptamos que los elementos $1,2,...,2Q$ son restos cuadráticos, por el resultado anterior tendríamos que:

$$(p-Q)Q=\sum_{x=0}^{p-1}S_x^2\geq\sum_{x=1}^{Q+1}S_x^2=\sum_{x=1}^{Q+1}\left(\sum_{z=0}^{Q-1}\left(\frac{x+z}{p}\right)\right)^2=(Q+1)Q^2.$$

Luego, $p-Q\geq(Q+1)Q=Q^2+Q$, entonces $p\geq Q^2+2Q$. Como p es primo no puede ser igual a Q^2+2Q, tampoco puede ser igual a $Q^2+2Q+1=(Q+1)^2$, ya que ambos son compuestos. Así se debe tener que $p>(Q+1)^2$. Y de esta desigualdad se sigue que $Q+1<\sqrt{p}$ o equivalentemente $Q+1\leq[\sqrt{p}]$. Pero esto es falso para $Q=[\sqrt{p}]$, luego $n(p)\leq 2[\sqrt{p}]$.

Teorema 2.2 (Gauss)**.** *Sean a entero positivo y $p>2$ primo tales que $(a,p)=1$. Entonces si χ es un carácter no-principal módulo p se cumple*

$$\left|\sum_{x=1}^{p-1}\chi(x)e^{2\pi i\frac{ax}{p}}\right|=\sqrt{p}.$$

Demostración: Sea $W=\sum_{x=1}^{p-1}\chi(x)e^{2\pi i\frac{ax}{p}}$. Entonces

$$|W|^2=\left(\sum_{x=1}^{p-1}\chi(x)e^{2\pi i\frac{ax}{p}}\right)\overline{\left(\sum_{y=1}^{p-1}\chi(y)e^{2\pi i\frac{ay}{p}}\right)}=\sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\chi(x)\overline{\chi}(y)e^{2\pi ia\frac{x-y}{p}}.$$

Obsérvese que $\overline{\chi}(y)=\chi(y^*)$. Además dado x fijo, si r recorre el sistema reducido de restos módulo p, también xr lo hará. Luego sustituyendo $y=rx$, podemos escribir

$$\begin{aligned}|W|^2&=\sum_{x=1}^{p-1}\sum_{r=1}^{p-1}\chi(xx^*r^*)e^{2\pi ia\frac{(1-r)x}{p}}=\sum_{r=1}^{p-1}\sum_{x=0}^{p-1}\chi(r^*)e^{2\pi ia\frac{(1-r)x}{p}}\\&=p+\sum_{r=2}^{p-1}\chi(r^*)\sum_{x=0}^{p-1}e^{2\pi ia\frac{(1-r)x}{p}}.\end{aligned} \tag{2.1}$$

Observemos que

$$\sum_{x=0}^{p-1} e^{2\pi i \frac{ax}{p}} = \begin{cases} p & \text{si } a \equiv 0 \ (\texttt{mód } p) \\ 0 & \text{si } a \not\equiv 0 \ (\texttt{mód } p). \end{cases}$$

Lo cual implica que la última suma en (2.1) es cero, pues cuando $r = 2, 3, ..., p-1$ se tiene que $a(1-r) \not\equiv 0 \ (\texttt{mód } p)$. □

El siguiente resultado de Vinogradov servirá para mejorar la estimación que tenemos para $n(p)$.

Teorema 2.3. *Sean $m \geq 2$ y $L_a, M_a \geq 1$ enteros, entonces*

$$\sum_{a=1}^{m-1} \left| \sum_{x=L_a+1}^{L_a+M_a} e^{2\pi i \frac{ax}{m}} \right| \leq m \log m.$$

Demostración: Observando que la suma interior es la suma de una progresión geométrica se tiene que

$$\sum_{a=1}^{m-1} \left| \sum_{x=L_a+1}^{L_a+M_a} e^{2\pi i \frac{ax}{m}} \right| = \sum_{a=1}^{m-1} \left| e^{2\pi i \frac{a(L_a+1)}{m}} \left(\frac{e^{2\pi i a \frac{M_a}{m}} - 1}{e^{2\pi i \frac{a}{m}} - 1} \right) \right| = \sum_{a=1}^{m-1} \left| \frac{e^{2\pi i \frac{M_a}{m}} - 1}{e^{2\pi i \frac{a}{m}} - 1} \right|.$$

Denotando por $||x||$ a la distancia de x al entero más cercano, se sigue que

$$\begin{aligned} \left| \frac{e^{2\pi i a \frac{M_a}{m}} - 1}{e^{2\pi i \frac{a}{m}} - 1} \right| &= \left| \frac{e^{\pi i a \frac{M_a}{m}} (e^{\pi i a \frac{M_a}{m}} - e^{-\pi i a \frac{M_a}{m}})}{e^{\pi i \frac{a}{m}} (e^{\pi i \frac{a}{m}} - e^{-\pi i \frac{a}{m}})} \right| = \left| \frac{\operatorname{sen} \frac{\pi a M_a}{m}}{\operatorname{sen} \frac{\pi a}{m}} \right| \\ &\leq \frac{1}{\left| \operatorname{sen} \frac{\pi a}{m} \right|} \leq \frac{1}{\operatorname{sen} \left(\pi \| \frac{a}{m} \| \right)} \leq \frac{1}{2 \| \frac{a}{m} \|}, \end{aligned}$$

donde la última desigualdad se obtine gracias a que $\operatorname{sen}(\pi x) \geq 2x$ para $x \in \left[0, \frac{1}{2}\right]$.

Para terminar la demostración se hará uso de la desigualdad: $\frac{1}{a} \leq \log\left(\frac{2a+1}{2a-1}\right)$ para $a > 1$. La cual se sigue de que la función $f(x) = x \log\left(\frac{2x+1}{2x-1}\right) \geq 1$ para $x > 1$. Para ver esto notemos que

$$f'(x) = \log\left(\frac{2x+1}{2x-1}\right) - \frac{4x}{4x^2-1} \quad \text{y} \quad f''(x) = \frac{-4}{4x^2-1}\left(1 - \frac{4x^2+1}{4x^2-1}\right).$$

Luego $f''(x) > 0$ cuando $x > 1$, con lo que $f'(x)$ es creciente y además $f'(x) \to 0$ cuando $x \to \infty$, por tanto $f'(x) < 0$, para $x > 1$. Esto implica que $f(x)$ es decreciente. Además haciendo la sustitución $x = \frac{1}{t}$ y calculando el límite cuando $t \to 0$ con la regla de L'Hôpital se sigue que $f(x) \to 1$ cuando $x \to \infty$. Por lo tanto $f(x) \geq 1$ para cada $x > 1$.

Ahora si m es impar

$$\sum_{a=1}^{m-1}\left|\frac{e^{2\pi i\frac{M_a}{m}}-1}{e^{2\pi i\frac{a}{m}}-1}\right| \leq \sum_{a=1}^{m-1}\frac{1}{2\|\frac{a}{m}\|} = 2\sum_{a=1}^{\frac{m-1}{2}}\frac{1}{2\left(\frac{a}{m}\right)} = m\sum_{a=1}^{\frac{m-1}{2}}\frac{1}{a}.$$

Entonces

$$m\sum_{a=1}^{\frac{m-1}{2}}\frac{1}{a} \leq m\sum_{a=1}^{\frac{m-1}{2}}\left(\log\left(2a+1\right)-\log\left(2a-1\right)\right) = m\log m.$$

Para el caso en que m es par se tiene

$$\begin{aligned}\sum_{a=1}^{m-1}\left|\frac{e^{2\pi i\frac{aM_a}{m}}-1}{e^{2\pi i\frac{a}{m}}-1}\right| &\leq \sum_{a=1}^{m-1}\frac{1}{2\|\frac{a}{m}\|} = 2\sum_{a=1}^{\frac{m-2}{2}}\frac{1}{2\left(\frac{a}{m}\right)}+\frac{1}{2\left(\frac{\frac{m}{2}}{m}\right)}\\ &= m\sum_{a=1}^{\frac{m-2}{2}}\frac{1}{a}+1 \leq m\log(m-1)+1 \leq m\log m. \qquad \square\end{aligned}$$

Teorema 2.4 (Desigualdad de Pólya-Vinogradov)**.** *Sean $p>2$ primo, M un entero positivo y χ carácter no-principal módulo p. Entonces*

$$\left|\sum_{x=L+1}^{L+M}\chi(x)\right| \leq \sqrt{p}\log p.$$

Demostración: Recordemos que

$$\frac{1}{p}\sum_{a=0}^{p-1}e^{2\pi i\frac{a(x-y)}{p}} = \begin{cases} 1 & \text{si } x-y\equiv 0 \ (\texttt{mód}\ p)\\ 0 & \text{si } x-y\not\equiv 0 \ (\texttt{mód}\ p).\end{cases}$$

Luego podemos escribir

$$\begin{aligned}\sum_{x=L+1}^{L+M}\chi(x) &= \sum_{x=L+1}^{L+p}\sum_{y=L+1}^{L+M}\frac{1}{p}\sum_{a=o}^{p-1}\chi(x)e^{2\pi i\frac{a(x-y)}{p}}\\ &= \frac{1}{p}\sum_{a=0}^{p-1}\sum_{y=L+1}^{L+M}e^{-2\pi i\frac{ay}{p}}\sum_{x=L+1}^{L+p}\chi(x)e^{2\pi i\frac{ax}{p}}.\end{aligned}$$

Entonces utilizando los teoremas 2.2 y 2.3 se tiene

$$\left|\sum_{x=L+1}^{L+M}\chi(x)\right| \leq \frac{1}{p}\sum_{a=0}^{p-1}\left|\sum_{y=L+1}^{L+M}e^{-2\pi i\frac{ay}{p}}\right|\left|\sum_{x=L+1}^{L+p}\chi(x)e^{2\pi i\frac{ax}{p}}\right| \leq \frac{1}{\sqrt{p}}\sum_{a=0}^{p-1}\left|\sum_{y=L+1}^{L+M}e^{-2\pi i\frac{ay}{p}}\right|$$
$$\leq \sqrt{p}\log p. \qquad \square$$

Corolario 2.1. *Sean $p>2$ primo y $N=\left\lfloor p^{\frac{1}{2}}\log^2 p\right\rfloor$. Entonces la cantidad de no-restos cuadráticos menores o iguales que N está dada por $\left(\frac{1}{2}+O\left(\frac{1}{\log p}\right)\right)N$.*

Demostración: Por el teorema 2.4 se tiene que

$$\left|\sum_{x=1}^{N}\left(\frac{x}{p}\right)\right| \leq p^{\frac{1}{2}}\log p.$$

Si se denota por N_1, N_2 a los restos y no-restos cuadráticos en $1,2,...,N$ respectivamente, se tiene que

$$2N_1=\sum_{x=1}^{N}\left(1+\left(\frac{x}{p}\right)\right)=N+\sum_{x=1}^{N}\left(\frac{x}{p}\right)\leq\left(1+\frac{1}{\log p}\right)N.$$

Por otro lado también se cumple que

$$2N_1=\sum_{x=1}^{N}\left(1+\left(\frac{x}{p}\right)\right)=N+\sum_{x=1}^{N}\left(\frac{x}{p}\right)\geq\left(1-\frac{1}{\log p}\right)N.$$

Luego $2N_1=\left(1+\frac{\theta}{\log p}\right)N$ para algún número $\theta=\theta(N,p)$ con $|\theta|\leq 1$. Como $N_1+N_2=N$ se tiene que

$$2N_2=\left(1-\frac{\theta}{\log p}\right)N.$$

En particular, $N_2=\left(\frac{1}{2}+O\left(\frac{1}{\log p}\right)\right)N$. $\square$

Teorema 2.5 (I. M. Vinogradov)**.** *Para cada $\varepsilon>0$ existe $C_\varepsilon>0$ constante, tal que $n(p)<C_\varepsilon p^{\frac{1}{2\sqrt{e}}+\varepsilon}$ para cada primo $p>2$.*

Demostración: Sean $\varepsilon>0$ y $N=\sqrt{p}\log^2 p$. Por el Corolario 2.1 se tiene que

$$\sum_{\substack{n\leq N\\ n \text{ no-resto}}}1=\left(\frac{1}{2}+O\left(\frac{1}{\log p}\right)\right)N. \tag{2.2}$$

Ahora, por la propiedad multiplicativa del símbolo de Legendre, se sigue que cada no-resto cuadrático tiene un divisor primo que también es no-resto cuadrático. Luego los

no-restos cuadráticos que son menores o iguales a N, tienen al menos un divisor primo q que satisface $n(p) \leq q \leq N$. Entonces

$$\begin{aligned}\left(\frac{1}{2}+O\left(\frac{1}{\log p}\right)\right)N &\leq \sum_{\substack{n(p)\leq q\leq N\\ q \text{ primo}}}\left[\frac{N}{q}\right] < N\sum_{\substack{n(p)\leq q\leq N\\ q \text{ primo}}}\frac{1}{q}\\ &= N\left(\log\left(\frac{\log N}{\log n(p)}\right)+O\left(\frac{1}{\log n(p)}\right)\right).\end{aligned} \tag{2.3}$$

Donde la última igualdad se da gracias a la estimación de Mertens sobre la suma de los recíprocos de los primos, ver Teorema 1.8.

Podemos suponer que $n(p) > p^{\frac{1}{100}}$, pues en otro caso no habría nada que probar. Con esto se tiene que $O\left(\frac{1}{\log n(p)}\right) = O\left(\frac{1}{\log p}\right)$. Entonces

$$\frac{1}{2}+\frac{C}{\log p} < \log\left(\frac{\log N}{\log n(p)}\right)+O\left(\frac{1}{\log p}\right),$$

de donde

$$\frac{1}{2}+O\left(\frac{1}{\log p}\right) < \log\left(\frac{\log N}{\log n(p)}\right).$$

Por tanto

$$e^{\frac{1}{2}+O\left(\frac{1}{\log p}\right)} < \frac{\log N}{\log n(p)}.$$

Finalmente despejando $n(p)$ se obtiene

$$\begin{aligned}n(p) &< N^{e^{-\frac{1}{2}+O\left(\frac{1}{\log p}\right)}} = (p^{\frac{1}{2}}\log^2 p)^{e^{-\frac{1}{2}}e^{O\left(\frac{1}{\log p}\right)}}\\ &= (p^{\frac{1}{2}}\log^2 p)^{e^{-\frac{1}{2}}(1+o(1))} = \left(p^{\frac{1}{2}+o(1)}\right)^{\frac{1+o(1)}{\sqrt{e}}}\\ &= p^{\frac{1}{2\sqrt{e}}+o(1)},\end{aligned}$$

lo cual es equivalente al enunciado del teorema. □

2.2 Estimación de Burgess

El resultado de Vinogradov fue el mejor hasta 1957 cuando Burgess [1] obtiene una mejora sustancial. La estimación de Burgess se basa en un teorema sobre suma de caracteres hallado por Weil [7], este a su vez se obtiene como consecuencia de resultados muy profundos de la teoría de las curvas algebraicas, y su demostración queda fuera del alcance del presente trabajo.

Teorema 2.6 (Weil)**.** *Sea $p > 2$ primo y χ un carácter no-principal módulo p de orden s. Sea además $f(x) \in \mathbb{F}_p[x]$ de grado n tal que $f(x)$ no puede ser escrito en la forma*

$c(h(x))^s$ en $\mathbb{F}_p[x]$. Si r es el número de raíces distintas de $f(x)$ en $\overline{\mathbb{F}}_p$, entonces

$$\left|\sum_{x\in\mathbb{F}_p}\chi(f(x))\right| \leq (r-1)\sqrt{p}.$$

Como una aplicación de este resultado se prueba la siguiente desigualdad que será utilizada con frecuencia en lo sucesivo.

Proposición 2.1. *Sean $p > 2$ primo, L entero positivo y χ un carácter no-principal. Para cualquier entero $k \geq 1$ se cumple que*

$$\sum_{\lambda=1}^{p}\left|\sum_{m=1}^{L}\chi(x)\right|^{2k} \leq k^{2k}L^k p + (2k-1)L^{2k}\sqrt{p}.$$

Demostración: En efecto, se tiene que

$$\begin{aligned}
\sum_{\lambda=1}^{p}\left|\sum_{m=1}^{L}\chi(\lambda+m)\right|^{2k} &= \sum_{\lambda=1}^{p}\left(\sum_{m=1}^{L}\chi(\lambda+m)\right)^k\overline{\left(\sum_{m=1}^{L}\chi(\lambda+m)\right)^k}\\
&= \sum_{\lambda=1}^{p}\sum_{1\leq m_1,\ldots,m_{2k}\leq L}\chi((\lambda+m_1)\ldots(\lambda+m_k))\overline{\chi}((\lambda+m_{k+1})\ldots(\lambda+m_{2k}))\\
&= \sum_{1\leq m_1,\ldots,m_{2k}\leq L}\sum_{\lambda=1}^{p}\chi((\lambda+m_1)\ldots(\lambda+m_k))\overline{\chi}((\lambda+m_{k+1})\ldots(\lambda+m_{2k}))\\
&= S_1 + S_2,
\end{aligned} \tag{2.4}$$

donde

$$S_1 = \sum_{\substack{1\leq m_1,\ldots,m_{2k}\leq L\\ \text{todos los } m_i \text{ se repiten}}}\sum_{\lambda=1}^{p}\chi((\lambda+m_1)\ldots(\lambda+m_k))\overline{\chi}((\lambda+m_{k+1})\ldots(\lambda+m_{2k})),$$

$$S_2 = \sum_{\substack{1\leq m_1,\ldots,m_{2k}\leq L\\ \text{hay un } m_i \text{ que no se repite}}}\sum_{\lambda=1}^{p}\chi((\lambda+m_1)\ldots(\lambda+m_k))\overline{\chi}((\lambda+m_{k+1})\ldots(\lambda+m_{2k})).$$

Si todos los números $m_1, \ldots, m_{2k}$ se repiten, entonces a lo más se les pueden asignar k valores distintos. Obsérvese que para k valores fijos $1 \leq m_{i_1}, m_{i_2}, \ldots, m_{i_k} \leq L$, el número de $(2k)$-tuplas que se pueden formar con estos valores dados está acotado por k^{2k}. Luego el número total de $2k$-tuplas $(m_1, \ldots, m_{2k})$ con todos los valores m_i repetidos está acotado por $k^{2k}L^k$. Así

$$|S_1| \leq k^{2k}L^k p. \tag{2.5}$$

Para la segunda suma notemos que

$$|S_2| \leq L^{2k} \left| \sum_{\lambda=1}^{p} \chi((\lambda+m_1)...(\lambda+m_k))\overline{\chi}((\lambda+m_{k+1})...(\lambda+m_{2k})) \right|,$$

donde en la última suma todos los $m_1, m_2, ..., m_{2k}$ son fijos, y entre ellos hay uno que no se repite. Sin pérdida de generalidad podemos suponer que es m_1. Entonces notando que $\overline{\chi}((\lambda+m_{k+1})...(\lambda+m_{2k})) = \chi((\lambda+m_{k+1})^{p-2}...(\lambda+m_{2k})^{p-2})$, tenemos

$$|S_2| \leq L^{2k} \sum_{\lambda=1}^{p} \chi((\lambda+m_1)...(\lambda+m_k)(\lambda+m_{k+1})^{p-2}...(\lambda+m_{2k})^{p-2}).$$

El polinomio $f(x) = (x+m_1)...(x+m_k)(x+m_{k+1})^{p-2}...(x+m_{2k})^{p-2}$ satisface las condiciones del Teorema 2.6 pues tiene al menos un cero simple. Por lo tanto

$$|S_2| \leq (2k-1)L^{2k}\sqrt{p}. \tag{2.6}$$

El resultado se obtiene al insertar las cotas (2.5) y (2.6) en (2.4). □

Lema 2.1. *Sean H, N, K enteros positivos y $f : \mathbb{Z} \to \mathbb{C}$ tal que $|f(x)| \leq 1$ para cada $x \in \mathbb{Z}$. Entonces*

$$\sum_{x=L+1}^{L+H} f(x) = \frac{1}{NK} \sum_{x=L+1}^{L+H} \sum_{y=1}^{N} \sum_{z=1}^{K} f(x+yz) + O(NK).$$

Demostración: Podemos suponer que $NK < H$, ya que en caso contrario la afirmación es evidente. Dados y, z con $yz \leq NK$ tenemos

$$\begin{aligned} \left| \sum_{x=L+1}^{L+H} f(x) - \sum_{x=L+1}^{L+H} f(x+yz) \right| &= \left| \sum_{x=L+1}^{L+yz} f(x) - \sum_{x=L+H+1}^{L+H+yz} f(x) \right| \\ &\leq \left| \sum_{x=L+1}^{L+yz} f(x) \right| + \left| \sum_{x=L+H+1}^{L+H+yz} f(x) \right| \\ &\leq 2yz \leq 2NK. \end{aligned}$$

Entonces

$$\sum_{x=L+1}^{L+H} f(x) = \sum_{x=L+1}^{L+H} f(x+yz) + O(NK).$$

Sumando sobre $1 \leq y \leq N$ y $1 \leq z \leq K$ en ambos lados de ésta igualdad tenemos

$$\begin{aligned} NK \sum_{x=L+1}^{L+H} f(x) &= \sum_{y=1}^{N}\sum_{z=1}^{K}\left(\sum_{x=L+1}^{L+H} f(x+yz) + O(NK)\right) \\ &= \sum_{x=L+1}^{L+H}\sum_{y=1}^{N}\sum_{z=1}^{K} f(x+yz) + O(N^2K^2). \end{aligned}$$

Dividiendo ambas partes por NK se obtiene la afirmación del lema. □

Teorema 2.7 (Burgess)**.** *Sea χ un carácter de Dirichlet no-principal módulo p. Para cada $\varepsilon > 0$, existen $\delta = \delta(\varepsilon) > 0$ y $p_0 = p_0(\varepsilon) > 0$ tales que para cada primo $p > p_0$ y $H > p^{\frac{1}{4}+\varepsilon}$ entero se cumple*

$$\left|\sum_{x=L+1}^{L+H} \chi(x)\right| \leq Hp^{-\delta}.$$

Demostración: Obsérvese que podemos partir el intervalo $[L+1, L+H]$ en intervalos disjuntos de la forma $[L_1+1, L_1+H_1]$ donde

$$\min\left\{p^{\frac{1}{4}+\frac{1}{10}}, p^{\frac{1}{4}+\varepsilon}\right\} < H_1 < 2\min\left\{p^{\frac{1}{4}+\frac{1}{10}}, p^{\frac{1}{4}+\varepsilon}\right\}.$$

De esta observación se sigue que basta demostrar el teorema solo para el caso

$$0 < \varepsilon < \frac{1}{10} \quad \text{y} \quad p^{\frac{1}{4}+\varepsilon} < H < 2p^{\frac{1}{4}+\varepsilon}.$$

Sean $N = \left\lfloor p^{\frac{1}{4}} \right\rfloor$ y $K = \left\lfloor p^{\frac{\varepsilon}{2}} \right\rfloor$. Por el Lema 2.1 se tiene

$$\sum_{x=L+1}^{L+H} \chi(x) = \frac{1}{NK}\sum_{x=L+1}^{L+H}\sum_{y=1}^{N}\sum_{z=1}^{K} \chi(x+yz) + O(NK). \tag{2.7}$$

Sea ahora $W = \sum_{x=L+1}^{L+H}\sum_{y=1}^{N}\sum_{z=1}^{K} \chi(x+yz)$, entonces

$$\begin{aligned} |W| &= \left|\sum_{x=L+1}^{L+H}\sum_{y=1}^{N}\sum_{z=1}^{K} \chi(x+yz)\right| \leq \sum_{x=L+1}^{L+H}\sum_{y=1}^{N}\left|\sum_{z=1}^{K} \chi(xy^*+z)\right| \\ &= \sum_{\lambda\in A} I(\lambda)\left|\sum_{z=1}^{K} \chi(\lambda+z)\right|, \end{aligned}$$

donde

$$A = \{xy^* \ (\texttt{mód}\ p);\ L+1 \leq x \leq L+H,\ 1 \leq y \leq N\},$$

e $I(\lambda)$ es el número de soluciones de la congruencia

$$xy^* \equiv \lambda \ (\texttt{mód}\ p), \quad L+1 \leq x \leq L+H,\ 1 \leq y \leq N. \tag{2.8}$$

Aplicando la desigualdad de Cauchy-Schwarz se tiene

$$|W|^2 \leq \sum_{\lambda \in A} I^2(\lambda) \sum_{\lambda \in A} \left| \sum_{z=1}^{K} \chi(\lambda + z) \right|^2. \tag{2.9}$$

Notemos que $\sum_{\lambda \in A} I^2(\lambda)$ es el número de soluciones de la congruencia

$$x_1 y_1^* \equiv x_2 y_2^* \ (\texttt{mód}\ p), \quad L+1 \leq x_1, x_2 \leq L+H,\ 1 \leq y_1, y_2 \leq N. \tag{2.10}$$

Sea J el número de soluciones de la congruencia (2.10). Definiendo los conjuntos

$$A_1 = \{\lambda \in A;\ I(\lambda) \leq 1\} \quad \text{y} \quad A_2 = \{\lambda \in A;\ I(\lambda) \geq 2\}$$

se tiene

$$J = \sum_{\lambda \in A} I^2(\lambda) = \sum_{\lambda \in A_1} I^2(\lambda) + \sum_{\lambda \in A_2} I^2(\lambda) \leq HN + \sum_{\lambda \in A_2} I^2(\lambda) \tag{2.11}$$

Fijemos una solución $(x_0(\lambda), y_0(\lambda))$ de la congruencia (2.8). Entonces si (x, y) es cualquier otra solución se verifica que

$$x - x_0(\lambda) \equiv (y - y_0(\lambda))\lambda \ (\texttt{mód}\ p), \quad 0 < |x - x_0(\lambda)| \leq H,\ 0 < |y - y_0(\lambda)| < N. \tag{2.12}$$

De aquí se sigue que $I(\lambda) \leq 1 + I_1(\lambda)$, con $I_1(\lambda)$ igual al número de soluciones de

$$xy^* \equiv \lambda \ (\texttt{mód}\ p), \quad 0 < |x| \leq H,\ 0 < |y| \leq N.$$

Obsérvese que para $\lambda \in A_2$ se cumple que $I(\lambda) \leq 2I_1(\lambda)$. Luego sustituyendo en (2.11)

$$J \leq HN + 4 \sum_{\lambda \in A_2} I_1^2(\lambda) = HN + 4J_1. \tag{2.13}$$

Donde J_1 es el número de soluciones de la congruencia

$$|x_1||y_1| \equiv |x_2||y_2| \ (\texttt{mód}\ p), \quad 0 < |x_1|, |x_2| \leq H,\ 0 < |y_1|, |y_2| \leq N. \tag{2.14}$$

Ya que $HN < p$ la congruencia (2.14) se convierte en la igualdad

$$|x_1||y_1| = |x_2||y_2|, \quad 0 < |x_1|, |x_2| \leq H,\ 0 < |y_1|, |y_2| \leq N. \tag{2.15}$$

Para x_2, y_2 fijos, el número de soluciones de $|x_1||y_1| = |x_2||y_2|$ es $4\tau(|x_2||y_2|)$, donde τ es la

función divisor. Del Teorema 1.9 se sigue que $\tau(n) \leq n^{o(1)}$, por lo tanto $J_1 \leq HNp^{o(1)} = (HN)^{1+o(1)}$, pues $HN < p$. Luego sustituyendo en (2.13) se tiene

$$J \leq HN + 4(HN)^{1+o(1)} = HN\left(1 + (HN)^{o(1)}\right).$$

Con esto la desigualdad (2.9) nos queda

$$|W|^2 \leq HN\left(1 + (HN)^{o(1)}\right) \sum_{\lambda \in A} \left| \sum_{z=1}^{K} \chi(\lambda + z) \right|^2 = HN\left(1 + (HN)^{o(1)}\right) W_1, \tag{2.16}$$

donde $W_1 = \displaystyle\sum_{\lambda \in A} \left| \sum_{z=1}^{K} \chi(\lambda + z) \right|^2$.

Aplicando la desigualdad de Hölder y la Proposición 2.1 se obtiene

$$\begin{aligned}
W_1^r &\leq |A|^{r-1} \sum_{\lambda \in A} \left| \sum_{z=1}^{K} \chi(\lambda + z) \right|^{2r} \\
&\leq |A|^{r-1} \sum_{\lambda=1}^{p} \left| \sum_{z=1}^{K} \chi(\lambda + z) \right|^{2r} \\
&\leq |A|^{r-1} \left(r^{2r} K^r p + (2r-1) K^{2r} \sqrt{p} \right) \\
&\leq (HN)^{r-1} \left(r^{2r} K^r p + (2r-1) K^{2r} \sqrt{p} \right) \\
&= (HN)^r K^{2r} \left(\frac{r^{2r} p}{HNK^r} + \frac{(2r-1)\sqrt{p}}{HN} \right).
\end{aligned}$$

Tomando $r = \lceil \frac{1}{\varepsilon} \rceil$ se tiene $K^r > p^{\frac{\varepsilon r}{2}} > p^{\frac{1}{2}}$, con lo que

$$W_1{}^r < (HN)^r K^{2r} p^{\frac{-\varepsilon}{4}}$$

para p primo suficientemente grande en términos de ε. Con este valor de r también se tiene que $(p^{\frac{-\varepsilon}{4}})^{\frac{1}{r}} \leq p^{\frac{-\varepsilon^2}{5}}$ digamos. Entonces

$$|W_1| \leq HNK^2 p^{\frac{-\varepsilon^2}{5}}.$$

Sustituyendo en (2.16) se sigue

$$|W|^2 \leq (HNK)^2 \left(1 + (HN)^{o(1)}\right) p^{\frac{-\varepsilon^2}{5}} \leq (HNK)^2 p^{\frac{-\varepsilon^2}{6}}.$$

Por lo tanto $|W| \leq HNKp^{\frac{-\varepsilon^2}{12}}$ para p primo suficientemente grande en términos de ε.

Sustituyendo en (2.7) se tiene

$$\left|\sum_{x=L+1}^{L+H}\chi(x)\right| \leq \frac{1}{NK}|W| + O(NK) \leq Hp^{\frac{-\varepsilon^2}{12}} + O\left(p^{\frac{1}{4}+\frac{\varepsilon}{2}}\right)$$
$$\leq Hp^{\frac{-\varepsilon^2}{14}},$$

para p primo suficientemente grande en terminos de ε. □

2.3 Mínimo no-resto cuadrático

Teorema 2.8 (Burgess)**.** *Para cada $\varepsilon > 0$ existe $C_\varepsilon > 0$ constante tal que*

$$n(p) < C_\varepsilon p^{\frac{1}{4\sqrt{e}}+\varepsilon}$$

para cada primo $p > 2$.

Demostración: Sea $H = [p^{\frac{1}{4}+\varepsilon}]$, y sea N la cantidad de no-restos cuadráticos módulo p menores o iguales a H. Entonces

$$N = \frac{1}{2}\sum_{1\leq n\leq H}\left(1 - \left(\frac{n}{p}\right)\right) = \frac{H}{2} - \frac{1}{2}\sum_{1\leq n\leq H}\left(\frac{n}{p}\right).$$

Luego

$$\left|N - \frac{H}{2}\right| = \frac{1}{2}\left|\sum_{1\leq n\leq H}\left(\frac{n}{p}\right)\right|.$$

Aplicando la estimación de Burgess a la suma del lado derecho se tiene

$$\left|N - \frac{H}{2}\right| \leq Hp^{-\delta}$$

para algún $\delta > 0$. Luego $N = H\left(\frac{1}{2} + \frac{\theta}{p^\delta}\right)$ para algún $|\theta| \leq \frac{1}{2}$. Repitiendo el argumento de Vinogradov se tiene que cualquier no-resto cuadrático menor o igual que H tiene un divisor primo q que también es un no-resto cuadrático y que satisface $n(p) \leq q \leq H$. Entonces

$$\sum_{\substack{n\leq H\\ n \text{ no-resto}}} 1 = \left(\frac{1}{2} + \frac{\theta}{p^\delta}\right)H \leq \sum_{\substack{n(p)\leq q\leq H\\ q \text{ primo}}}\left[\frac{H}{q}\right] \leq H\sum_{\substack{n(p)\leq q\leq H\\ q \text{ primo}}}\frac{1}{q}$$
$$= H\left(\log\left(\frac{\log H}{\log n(p)}\right) + O\left(\frac{1}{\log n(p)}\right)\right).$$

Podemos suponer que $n(p) \geq p^{\frac{1}{100}}$, de otro modo no habría nada que probar. Con este

supuesto se tiene $O\left(\frac{1}{\log n(p)}\right) = O\left(\frac{1}{\log p}\right)$. Luego

$$\frac{1}{2} + \frac{\theta}{p^{\delta}} \leq \log\left(\frac{\log H}{\log n(p)}\right) + O\left(\frac{1}{\log p}\right)$$

de aquí se sigue

$$\frac{1}{2} + O\left(\frac{1}{\log p}\right) \leq \log\left(\frac{\log H}{\log n(p)}\right)$$

y así

$$e^{\frac{1}{2}+O\left(\frac{1}{\log p}\right)} \leq \frac{\log H}{\log n(p)}.$$

Despejando $n(p)$ se obtiene

$$\begin{aligned} n(p) &\leq (H)^{e^{-\frac{1}{2}+O\left(\frac{1}{\log p}\right)}} = \left(p^{\frac{1}{4}+\varepsilon}\right)^{e^{-\frac{1}{2}}e^{O\left(\frac{1}{\log p}\right)}} \\ &= \left(p^{\frac{1}{4}+\varepsilon}\right)^{\frac{1+o(1)}{\sqrt{e}}} = p^{\frac{1}{4\sqrt{e}}+\frac{\varepsilon}{\sqrt{e}}+o(1)} \\ &< C_{\varepsilon}p^{\frac{1}{4\sqrt{e}}+\varepsilon}. \end{aligned}$$

□

Por último cabe puntualizar que el problema de hallar una mejora considerable al valor de esta cota se mantiene abierto. En los últimos años se han hecho pequeños progresos y se han obtenido algunos refinamientos en el factor p^{ε}, sin embargo el factor $p^{\frac{1}{4\sqrt{e}}}$ no ha sido mejorado, al menos no sin la ayuda de poderosas conjeturas tales como la hipótesis generalizada de Riemann. También hay que señalar que el problema se puede generalizar al caso de módulo compuesto [2].

Bibliografía

[1] D. A. Burgess, "The distribution of quadratic residues and non-residues," *Mathematika* **4** (1957) 106-112.

[2] Yuk-Kam Lau, Jie Wu. "On the least quadratic non-residue," *Int. J. Number Theory* **4 (3)** (2008) 423-435.

[3] Yu. V. Linnik, "A remark on the least quadratic non-residue," C. R. (Doclady) Acad. Sci. URSS (N. S.), **36** (1942) 119-120.

[4] C. F. Gauss, *Disquisitiones Arithmeticae.* Leipzig, Fleisher (1801). English translation: A. A. Clarke, Yale University Press (1966).

[5] I. M. Vinogradov, "Sur la distribution des residus and nonresidus des puissances," *J. Soc. Phys. Math. Univ. Perm.* **1** (1918) 18–28.

[6] I. M. Vinogradov, *Fundamentos de la teoría de los números.* Ed. Mir, 2da. Edición, (1977).

[7] A. Weil, "On some exponential sums," *Proc. N. A. S.* **34 (5)** (1948) 204-207.