Small residues of Dirichlet characters

Candidate:
Iancu Andrei-Mihai

Supervisor:
Prof. Yuri Bilu

ALGANT MASTER THESIS, JULY 2016

Contents

Introduction

The study of residues and nonresidues of Dirichlet characters dates back to the early 19th century when Gauss used a bound on the smallest χ-nonresidues where χ is the Legendre symbol $(\frac{\cdot}{p})$ and p is a prime $\equiv 1(mod\, 8)$ required for his first proof of the quadratic reciprocity law.

Later work of Linnik and Vinogradov succeeded in giving a bound $l \ll_\epsilon p^{\frac{1}{4}+\varepsilon}$ for the smallest prime quadratic residue l i.e. $\chi(l) = 1$ where χ is a quadratic character modulo a prime p.

In the first section, we give a lower bound for prime residues of quadratic characters based on an improved version of Burgess's bound.

As a consequence of Chebotarev's density theorem, the proportion of rational primes that split completely in a number field K is given by $\frac{1}{[L:\mathbb{Q}]}$, where L is the normal closure of $K/\mathbb{Q}$, hence one could ask for an estimate of the smallest such prime. Following the work of mathematician Paul Pollack, we prove as a main result in section 3, that in the special case when K is an abelian number field, we have that $p \ll_{\varepsilon,k} D^{\frac{1}{4}+\varepsilon}$, where $k = [K : \mathbb{Q}]$. To see this, we heavily rely on Siegel's Theorem on lower bounds for the L-series $L(1, \chi)$. A drawback of this is that the constant appearing in Theorem 3.1 is not effective. This can be improved though if one is allowed to exclude certain bad moduli. For instance, there can be established a lower bound of the form $(\log q)^{-\mathcal{O}(1)} \ll L(1, \chi)$ after excluding one bad moduli q in each hyperdyadic range $2^{100^k} \leq q \leq 2^{100^{k+1}}$ $\forall k \in \mathbb{N}$, which is due to a result of Landau(see [7], pp. 362-363) By the same reason, we can have effectiveness in Theorem 3.1 if all the characters appearing in the decomposition of $\zeta_K(s)$ have odd order, thus not being real. In particular, this holds true when $[K : \mathbb{Q}]$ is odd.

1 Bounds for small prime character residues

1.1 Burgess's bound

We want to prove the following theorem([12], Theorem 1.3)

Theorem 1.1. *Let $\varepsilon \geq 0$ and let $A \geq 0$. There is an $m_0 = m_0(\varepsilon, A)$ with the following property: If $m \geq m_0$ and χ is a quadratic character modulo m, then there are at least $(\log m)^A$ primes $l \leq m^{\frac{1}{4}+\varepsilon}$ with $\chi(l) = 1$.*

In doing so, we need some some additional results, mainly a modified version of Burgess's bound below obtained by Norton([8]). Let χ be a Dirichlet character. Then we define

$$S_N(x, \chi) = \sum_{y=N+1}^{N+x} \chi(y)$$

for any integers N, x with $x \geq 1$.

Theorem 1.2. *(Burgess) Let n,x be positive integers, let N be any integer and let ε be any positive real number. Let χ be a nonprincipal Dirichlet character mod n. Then*

$$\left|S_N(x, \chi)\right| \ll_{\varepsilon,t} x^{1-\frac{1}{t}} n^{\frac{t+1}{4t^2}+\varepsilon} \tag{1.1}$$

for each of the values $t = 1, 2, 3$(the implied constant depends at most on ε and t). Furthermore, if n is cubefree, then (1.1) holds for any positive integer t.

This theorem has important applications in number theory and as mentioned, we will prove the following, stronger version of (1.1) that holds for any positive integers n, x, t and any nonprincipal character χ mod n, which actually gives several improved estimates in questions about the structure of the multiplicative group mod n.

Theorem 1.3. *Let n, k, N, x be any integers with n, k, x positive and let χ be a nonprincipal character mod n such that χ^k is principal. Then*

$$\left|S_N(x, \chi)\right| \ll_{\varepsilon,t} R_k(n)^{\frac{1}{t}} x^{1-\frac{1}{t}} n^{\frac{t+1}{4t^2}+\varepsilon} \tag{1.2}$$

for any positive integer t, where

$$R_k(n) = \min\{M(n)^{\frac{3}{4}}, Q(k)^{\frac{9}{8}}\}$$

and

$$M(n) = \prod_{p^e || n, e \geq 2} p^e$$

$$Q(k) = \prod_{p^e || k, e \geq 3} p^e$$

In particular, if $x \geq R_k(n)^{\frac{1}{4}+\delta}$ for $\delta > 0$, then

$$\left|S_N(x, \chi)\right| \ll_\delta x n^{-\delta^2(1+2\delta)^{-1}} \tag{1.3}$$

We need 2 useful lemmas.

Lemma 1.4. *Suppose that n, q, m are positive integers with $n = qm$ and $gcd(q, m) = 1$. If χ is a character mod n, then χ admits a unique representation $\chi = \theta\xi$, where θ is a character mod q and ξ is a character mod m. Furthermore, χ is primitive iff both θ and ξ are primitive.*

This lemma is an easy application of the Chinese Remainder Theorem. For details, see[4], pp.220-221.

Lemma 1.5. *Let χ be a primitive character mod n, where n is a positive integer greater than 1. Let N, x, t be any integers with x, t positive. Then*

$$\left|S_N(x,\chi)\right| \ll_{\varepsilon,t} M(n)^{\frac{3}{4t}} x^{1-\frac{1}{t}} n^{\frac{t+1}{4t^2}+\varepsilon}$$

where M(n) is defined as before.

Proof. Write $M(n) = m$ and let

$$q = \prod_{p^e || n, e\leq 2} p^e$$

By the definition of $M(n)$, we have that $n = qm$, with $gcd(q, m) = 1$.

Notice that if $x < m$, then

$$m^{\frac{3}{4t}} x^{1-\frac{1}{t}} n^{\frac{t+1}{4t^2}+\varepsilon} > m^{\frac{3}{4t}} x^{1-\frac{1}{t}} m^{\frac{1}{4t}} = m^{\frac{1}{t}} x^{1-\frac{1}{t}} > x^{\frac{1}{t}} x^{1-\frac{1}{t}} = x \geq |S_N(x,\chi)|$$

So we may assume that $m \leq x$ and observe that if $m = n$, then

$$m^{\frac{3}{4t}} x^{1-\frac{1}{t}} n^{\frac{t+1}{4t^2}+\varepsilon} > n^{\frac{3}{4t}} n^{1-\frac{1}{t}} n^{\frac{t+1}{4t^2}+\varepsilon} = n^{\frac{1}{4t^2}+1+\varepsilon} > n \geq |S_N(x,\chi)|$$

Hence we must have $m < n$ and $q > 1$. By the previous lemma, χ can be represented in an unique way as a product $\chi = \theta\xi$, where θ is a primitive character mod q and ξ is a primitive character mod m.

Since $gcd(q, m) = 1$, we have that for any nonzero integer a, there exists a unique integer $b, 1 \leq b \leq m$ such that $a \equiv -bq (\text{mod } m)$.

Using the decomposition of χ we have the following

$$|S_N(x,\chi)| = |\sum_{a=1}^{m} \sum_{\substack{N<a\leq N+x \\ a\equiv -bq (mod\, m)}} \theta(a)\xi(a)| \leq \sum_{a=1}^{m} |\sum_{\substack{N<a\leq N+x \\ a\equiv -bq (mod\, m)}} \theta(a)|$$

Writing $a = cm - bq$, we have that $\theta(a) = \theta(c)\theta(m)$ so

$$|S_N(x,\chi)| \leq \sum_{a=1}^{m} |\sum_{\frac{N+bq}{m}<c\leq \frac{N+bq+x}{m}} \theta(c)| \tag{1.4}$$

Notice the following

$$\sum_{\frac{N+bq}{m}<c\leq \frac{N+bq+x}{m}} \theta(c) = S_{\lfloor \frac{N+bq}{m} \rfloor}(\left\lfloor \frac{x}{m} \right\rfloor, \theta)$$

By applying Theorem 1.2, we have

$$\left|S_{\lfloor \frac{N+bq}{m} \rfloor}(\left\lfloor \frac{x}{m} \right\rfloor, \theta)\right| \ll_{\varepsilon,t} M(q)^{\frac{3}{4}} \left\lfloor \frac{x}{m} \right\rfloor^{1-\frac{1}{t}} q^{\frac{t+1}{4t^2}+\varepsilon}$$

Therefore, since q is cubefree, we obtain

$$\begin{aligned}\left|S_{\lfloor \frac{N+bq}{m} \rfloor}(\left\lfloor \frac{x}{m} \right\rfloor, \theta)\right| \ll_{\varepsilon,t} (\frac{x}{m})^{1-\frac{1}{t}} q^{\frac{t+1}{4t^2}+\varepsilon} &= (\frac{x}{m})^{1-\frac{1}{t}} \frac{n}{m}^{\frac{t+1}{4t^2}+\varepsilon} \\ &= m^{-1+\frac{1}{t}-\frac{t+1}{4t^2}-\varepsilon} x^{1-\frac{1}{t}} n^{\frac{t+1}{4t^2}+\varepsilon}\end{aligned}$$

Applying this in (1.4) we get

$$|S_N(x,\chi)| \ll_{\varepsilon,t} \sum_{a=1}^{m} m^{-1+\frac{1}{t}-\frac{t+1}{4t^2}-\varepsilon} x^{1-\frac{1}{t}} n^{\frac{t+1}{4t^2}+\varepsilon} = m \cdot m^{-1+\frac{3}{4t}-\frac{1}{4t^2}-\varepsilon} x^{1-\frac{1}{t}} n^{\frac{t+1}{4t^2}+\varepsilon}$$

$$= m^{\frac{3}{4t}-\frac{1}{4t^2}-\varepsilon}x^{1-\frac{1}{t}}n^{\frac{t+1}{4t^2}+\varepsilon}$$

But
$$m^{\frac{3}{4t}-\frac{1}{4t^2}-\varepsilon}x^{1-\frac{1}{t}}n^{\frac{t+1}{4t^2}+\varepsilon} \ll_{\varepsilon,t} m^{\frac{3}{4t}}x^{1-\frac{1}{t}}n^{\frac{t+1}{4t^2}+\varepsilon} = M(n)^{\frac{3}{4t}}x^{1-\frac{1}{t}}n^{\frac{t+1}{4t^2}+\varepsilon}$$

which concludes the proof. □

Lemma 1.6. *Let N, x, t be any integers with x, t positive and let χ be a nonprincipal character mod n with conductor f. Then*

$$\left|S_N(x,\chi)\right| \ll_{\varepsilon,t} 2^{\omega(n)}M(f)^{\frac{3}{4t}}x^{1-\frac{1}{t}}n^{\frac{t+1}{4t^2}+\varepsilon} \tag{1.5}$$

where $\omega(n)$ is the number of distinct prime factors of n.

Proof. Let ξ be a primitive character mod f which induces χ and let

$$q = \prod_{p|n, p\nmid d} p$$

Then we can decompose χ as $\chi = \theta\xi$, where θ is the principal character mod q.

Using the representation

$$\theta(y) = \sum_{e|gcd(y,q)} \mu(e) = \sum_{e|y, e|q} \mu(e)$$

where μ is the *Möbius* function, we get the following

$$|S_N(x,\chi)| = |\sum_{y=N+1}^{N+x} \chi(y)|$$

$$= |\sum_{y=N+1}^{N+x} \theta(y)\xi(y)|$$

$$= |\sum_{y=N+1}^{N+x} (\sum_{e|y,e|q} \mu(e)) \cdot \xi(y)|$$

So we have that
$$|S_N(x,\chi)| = |\sum_{\frac{N}{e}<z<\frac{N+x}{e}} (\sum_{e|q} \mu(e)) \cdot \xi(z)|$$
$$= |\sum_{e|q} \mu(e)| \cdot |\sum_{\frac{N}{e}<z<\frac{N+x}{e}} \xi(z)|$$

But the last quantity is smaller than

$$\sum_{e|q} |\sum_{\frac{N}{e}<z<\frac{N+x}{e}} \xi(z)| = \sum_{e|q} |S_{\lfloor\frac{N}{e}\rfloor}(\left\lfloor\frac{x}{e}\right\rfloor, \xi)| \tag{1.6}$$

By the previous lemma, we have

$$\left|S_{\lfloor\frac{N}{e}\rfloor}(\left\lfloor\frac{x}{e}\right\rfloor, \xi)\right| \ll_{\varepsilon,t} M(f)^{\frac{3}{4t}} \left\lfloor\frac{x}{e}\right\rfloor^{1-\frac{1}{t}} f^{\frac{t+1}{4t^2}+\varepsilon}$$

and since $e \geq 1$ we get that

$$\left|S_{\lfloor\frac{N}{e}\rfloor}(\left\lfloor\frac{x}{e}\right\rfloor, \xi)\right| \ll_{\varepsilon,t} M(f)^{\frac{3}{4t}}x^{1-\frac{1}{t}}f^{\frac{t+1}{4t^2}+\varepsilon} \tag{1.7}$$

From (1.6) and (1.7) we therefore obtain that

$$|S_N(x,\chi)| \ll_{\varepsilon,t} \sum_{e|q} M(f)^{\frac{3}{4t}} x^{1-\frac{1}{t}} f^{\frac{t+1}{4t^2}+\varepsilon}$$

and since

$$\sum_{e|q} 1 = 2^{\omega(q)} \leq 2^{\omega(n)}$$

we conclude that

$$\left|S_N(x,\chi)\right| \ll_{\varepsilon,t} 2^{\omega(n)} M(f)^{\frac{3}{4t}} x^{1-\frac{1}{t}} n^{\frac{t+1}{4t^2}+\varepsilon}$$

□

Notice that for any divisor d of a positive integer n, we have that $M(d)|M(n)$. This simply follows from the definition of $M(n)$. Now, since $2^{\omega(n)} \ll_\varepsilon n^\varepsilon$, we remark that we can get (1.2) from Lemma 1.6 with $R_k(n)$ replaced by $M(n)^{\frac{3}{4}}$. More work is required though to prove the theorem in its entirety.

Let n, k be positive integers and denote $(\mathbb{Z}/n\mathbb{Z})^\times$ by $C(n)$. Let $C_k(n) \leq C(n)$ be the subgroup of the kth powers and write $v := v_k(n) = [C(n) : C_k(n)]$.

As a straightforward application of the Chinese Remainder Theorem, it can be showed that v_k is multiplicative and therefore the next lemma characterizes v_k completely.

Lemma 1.7.

$$v_k(n) = \begin{cases} 1 & \text{if } n = 2 \\ gcd(k, \varphi(p^a)) & \text{if } n = p^a \text{ for } p \text{ odd prime and } a \geq 1 \\ gcd(k,2)gcd(k,2^{a-2}) & \text{if } n = 2^a, a \geq 2 \end{cases}$$

Proof. Suppose that $n = p^a$, where p is an odd prime and $a \geq 1$. Let g be a primitive root mod p^a and let t be a positive integer. Then $y = g^t$ is a kth power mod p^a iff the congruence $t \equiv mk (\text{mod } p^a)$ is solvable for the integer m. But a well known result in elementary number theory, which can be proved for example using Dirichlet's approximation theorem, tells us that this congruence has solutions iff $d = gcd(k, \varphi(p^a))|t$.

Hence $C_k(p^a)$ is represented by the numbers $g^{dr}, 0 \leq r < \frac{\varphi(p^a)}{d}$ so $|C_k(p^a)| = \frac{\varphi(p^a)}{d}$. Therefore

$$v_k(p^a) = [C(p^a) : C_k(p^a)] = d = gcd(k, \varphi(p^a))$$

It is known that for $a \geq 3$, $C(2^a) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{a-2}\mathbb{Z} =< \widehat{-1}, \widehat{5} >$. So any element $x \in C(2^a)$ can be written uniquely as

$$x \equiv (-1)^\alpha 5^\beta (mod\, 2^a)$$

where $\alpha \in \{0,1\}$ and $\beta \in \{0,1,...,2^{a-2}-1\}$. Notice that this also holds for $a = 2$ since $C(4) = \{\hat{1}, \hat{3}\} =< \widehat{-1} >$.

In the same manner as before, we easily get that

$$v_k(2^a) = gcd(k,2)gcd(k,2^{a-2})\, for\, a \geq 2$$

Finally, $v_k(2) = [C(2) : C_k(2)] = 1$. □

We now give the proof of Theorem 1.3

Proof. Consider the prime decomposition of n:

$$n = p_1^{a_1} \cdot ... \cdot p_r^{a_r}$$

where $r \geq 1, a_i \geq 1 \forall\, i \in \overline{1,r}$ and $p_1, ..., p_r$ are primes with $p_1 < ... < p_r$.
Moreover, write
$$k = p_1^{k_1} \cdot ... \cdot p_r^{k_r} k'$$
where $k_i \in \mathbb{N}\ \ \forall\, i \in \overline{1,r}$ and $k' \geq 1$ such that $(k', p_1 \cdot ... \cdot p_r) = 1$. Now, for each $i \in \overline{1,r}$, define
$$\gamma_i = \begin{cases} min\{a_i, k_i+1\} & \text{if } p_i \text{ is odd} \\ min\{a_i, k_i+2\} & \text{if } p_i = 2 \end{cases}$$
Furthermore, let
$$\lambda := \lambda_k(n) = \begin{cases} 2 & \text{if } n \text{ is even and } k \text{ is odd} \\ 1 & \text{otherwise} \end{cases}$$
and define
$$n_k = \prod_{i=\lambda}^{r} p_i^{\gamma_i}$$
with the convention that $n_k = 1$ if the product is empty. Let d be the conductor of χ. We show that $d|n_k$. Indeed, since $n = p_1^{a_1} \cdot ... \cdot p_r^{a_r}$, we can write
$$\chi = \chi_1 \cdot ... \cdot \chi_r$$
where χ_i is a character mod $p_i^{a_i}\ \forall\, i \in \overline{1,r}$. By the definition of the conductor, we have that
$$f_\chi = \prod_{i=1}^{r} f_{\chi_i}$$
where f_θ denotes the conductor of the character θ. Also notice that χ_i^k is principal $\forall i \in \overline{1,r}$.

Let y be a positive integer such that $\exists\, i \in \overline{1,r}$ such that $p_i \nmid y$. Then y is a kth power mod $p_i^{a_i}$ iff y is a kth power mod $p_i^{\gamma_i}$. To see this, observe that if $p_i \nmid y$, then there exists a positive integer t such that $y = g^t$, where g is a primitive root mod $p_i^{a_i}$. Hence, as in the proof of Lemma 1.7, $y = g^t$ is a kth power mod $p_i^{a_i}$ if and only if $d = gcd(k, \varphi(p_i^{a_i}))|t$.

Similarly, $y = g^t$ is a kth power mod $p_i^{\gamma_i}$ if and only if the congruence $t \equiv m'k (mod\, p_i^{\gamma_i})$ is solvable for the integer m' iff $d' = gcd(k, \varphi(p_i^{\gamma_i}))|t$.

So from the above, it suffices to show that $d|t \Leftrightarrow d'|t$. It can be easily seen that for a, b, c non-zero integers with $gcd(b, c) = 1$ we have that
$$gcd(ab, c) = gcd(a, c) \tag{1.8}$$
Now we have the following
$$\begin{aligned} d &= gcd(k, \varphi(p_i^{a_i})) \\ &= gcd(p_1^{k_1} \cdot ... \cdot p_r^{k_r} k', p_i^{a_i - 1}(p_i - 1)) \\ &= gcd(\frac{k}{p_i^{k_i}} \cdot p_i^{k_i}, p_i^{a_i-1}(p_i - 1)) \\ &= p_i^{min\{k_i, a_i - 1\}} gcd(\frac{k}{p_i^{k_i}}, p_i - 1) \\ &= p_i^{\gamma_i - 1} gcd(\frac{k}{p_i^{k_i}}, p_i - 1) \end{aligned}$$
But then, putting $a = \frac{k}{p_i^{k_i}}, b = p_i^{k_i}, c = p_i - 1$ in (1.8) yields
$$gcd(\frac{k}{p_i^{k_i}}, p_i - 1) = gcd(\frac{k}{p_i^{k_i}} p_i^{k_i}, p_i - 1) = gcd(k, p_i - 1)$$

So $d = p_i^{\gamma_i - 1} gcd(k, p_i - 1)$.
On the other hand

$$\begin{aligned} d' &= gcd(k, \varphi(p_i^{\gamma_i})) \\ &= gcd(k, p_i^{\gamma_i - 1}(p_i - 1)) \\ &= p_i^{min\{k_i, \gamma_i - 1\}} gcd(k, p_i - 1) \end{aligned}$$

But, by definition, $\gamma_i \leq k_i + 1$ so $\gamma_i - 1 \leq \ k_i$ and therefore

$$d' = p_i^{\gamma_i - 1} gcd(k, p_i - 1)$$

So $d = d'$ and this shows that y is a kth power mod $p_i^{a_i}$ iff y is a kth power mod $p_i^{\gamma_i}$. It follows that if $y \equiv 1 (mod\, p_i^{\gamma_i})$ then $\chi_i(y) = 1$ so by the definition of the conductor we get that $f_{\chi_i} | p_i^{\gamma_i}$.

Now, if $p_1 = 2$ and k is odd, then by Lemma 1.7, any odd y is a kth power mod $p_1^{a_1}$ so χ_1 is principal and $f_{\chi_1} = 1$.

Combining these results we get that $f_\chi = d | n_k$.

For another way to prove this fact using the number $\Omega_k(d)$ of primitive characters $\chi (mod\ d)$ such that χ^k is principal, see [8].

Since $d | n_k$, it follows that $M(d) \leq M(n_k)$. Also, observe that $\omega(n) \leq \omega(n_k) + 1$ since $\lambda \leq 2$.

By applying Lemma 1.6 for the character χ and using the fact that $2^{\omega(m)} \ll_\varepsilon m^\varepsilon$ for a positive integer m we obtain

$$\left| S_N(x, \chi) \right| \ll_{\varepsilon, t} M(n_k)^{\frac{3}{4t}} x^{1 - \frac{1}{t}} n_k^{\frac{t+1}{4t^2} + \varepsilon} \quad \forall t \in \mathbb{N}^* \tag{1.9}$$

Clearly $n_k | n$ and therefore $M(n_k) | M(n)$. Let us prove that $M(n_k) \leq 8 Q(k)^{\frac{3}{2}}$.

To show this, consider the two possible cases:

Case 1. n is odd or n is even and k is odd.

Then for each $i \in \overline{\lambda, r}$ and $\gamma_i \geq 3$, we must have that p_i is odd and $k_i \geq 2$. But $\gamma_i = min\{a_i, k_i + 1\}$ so

$$\gamma_i \leq k_i + 1 \leq \frac{3}{2} k_i \qquad \text{since } k_i \geq 2$$

Hence

$$\prod_{\substack{p^e || n_k \\ e \geq 3}} p_e = M(n_k) \leq \prod_{\substack{\lambda \leq i \leq r \\ k_i \geq 2}} p_i^{\frac{3}{2} k_i} = (\prod_{\substack{\lambda \leq i \leq r \\ k_i \geq 2}} p_i^{k_i})^{\frac{3}{2}}$$

But by the definition of $Q(k)$, we have that

$$Q(k) \geq \prod_{\substack{\lambda \leq i \leq r \\ k_i \geq 2}} p_i^{k_i}$$

so

$$M(n_k) \leq (\prod_{\substack{\lambda \leq i \leq r \\ k_i \geq 2}} p_i^{k_i})^{\frac{3}{2}} \leq Q(k)^{\frac{3}{2}} \tag{1.10}$$

Case 2. n and k are both even.

Then $\lambda = 1$ and $p_1 = 2$. If $\gamma_1 < 3$, we have that

$$M(n_k) = \prod_{\substack{p^e || n_k \\ e \geq 3}} p_e = \prod_{\substack{2 \leq i \leq r \\ \gamma_i \geq 3}} p_i^{\gamma_i}$$

and as in the first case we obtain that

$$M(n_k) \leq Q(k)^{\frac{3}{2}} \tag{1.11}$$

If $\gamma_1 = 3$, then

$$M(n_k) = \prod_{\substack{p^e || n_k \\ e \geq 3}} p_e = 2^3 \cdot \prod_{\substack{2 \leq i \leq r \\ \gamma_i \geq 3}} p_i^{\gamma_i} \leq 2^3 \cdot \prod_{\substack{2 \leq i \leq r \\ k_i \geq 3}} p_i^{\frac{3}{2}k_i} = 8(\prod_{\substack{2 \leq i \leq r \\ \gamma_i \geq 3}} p_i^{k_i})^{\frac{3}{2}} \leq 8Q(k)^{\frac{3}{2}} \tag{1.12}$$

If $\gamma_1 = min\{a_1, k_1 + 2\} \geq 4$, then $k_1 \geq 2$, hence $1 + \frac{3}{2}f_1 = f_1 + (\frac{f_1}{2} + 1) \geq f_1 + 2 \geq \gamma_1$. Therefore we obtain

$$M(n_k) = 2^{\gamma_1} \cdot \prod_{\substack{2 \leq i \leq r \\ \gamma_i \geq 3}} p_i^{\gamma_i} \leq 2^{1+\frac{3}{2}f_1} \cdot \prod_{\substack{2 \leq i \leq r \\ k_i \geq 2}} p_i^{\frac{3}{2}k_i} = 2(\prod_{\substack{1 \leq i \leq r \\ k_i \geq 2}} p_i^{k_i})^{\frac{3}{2}} \leq 2Q(k)^{\frac{3}{2}} \tag{1.13}$$

From $(1.10), (1.11), (1.12)$ and (1.13) we conclude that

$$M(n_k) \leq 8Q(k)^{\frac{3}{2}} \tag{1.14}$$

So we have that

$$M(n_k)^{\frac{3}{4}} \leq 8^{\frac{3}{4}} Q(k)^{\frac{9}{8}}$$

and since $n_k \leq n$ and $M(n_k) \leq M(n)$, by setting $R_k(m) = min\{M(n)^{\frac{3}{4}}, Q(K)^{\frac{9}{8}}\}$ and using (1.9) we obtain

$$\left|S_N(x, \chi)\right| \ll_{\varepsilon,t} R_k(n)^{\frac{1}{t}} x^{1-\frac{1}{t}} n^{\frac{t+1}{4t^2}+\varepsilon}$$

which is precisely the main statement of Theorem 1.3.

As for the remaining part of the theorem, observe that if $x \geq R_k(n) n^{\frac{1}{4}+\delta}$ for some $\delta > 0$, then $R_k(n) \leq x n^{-\frac{1}{4}-\delta}$ and from (1.2) we get

$$\left|S_N(x, \chi)\right| \ll_{\varepsilon,t} (x n^{-\frac{1}{4}-\delta})^{\frac{1}{t}} x^{1-\frac{1}{t}} n^{\frac{t+1}{4t^2}+\varepsilon} = x n^{\frac{t+1}{4t^2}+\varepsilon-\frac{1}{4t}-\frac{\delta}{t}} = x n^{\frac{1}{4t^2}+\varepsilon-\frac{\delta}{t}}$$

So

$$\left|S_N(x, \chi)\right| \ll_{\varepsilon,t} x n^{f(t)+\varepsilon}$$

where $f : (0, +\infty) \longrightarrow \mathbb{R}$, $f(t) = \frac{1}{4t^2} - \frac{\delta}{t}$.

Since the derivative of f is

$$f'(t) = \frac{\delta}{t^2} - \frac{1}{2t^3} = \frac{2\delta t - 1}{t^3}$$

we have that f is increasing for $t \geq \frac{1}{2\delta}$ so for $t = \lceil \frac{1}{2\delta} \rceil$ we have

$$\begin{aligned} f(t) \leq f(\frac{1}{2\delta} + 1) &= \frac{1}{4 \cdot (1 + \frac{1}{2\delta})^2} - \frac{\delta}{1 + \frac{1}{2\delta}} \\ &= \frac{\delta^2}{(2\delta+1)^2} - \frac{2\delta^2}{2\delta+1} \\ &= \frac{\delta^2 - 2\delta^2(2\delta+1)}{(2\delta+1)^2} \\ &= -\frac{\delta^2(4\delta+1}{(2\delta+1)^2} < -\frac{\delta^2(2\delta+1}{(2\delta+1)^2} = -\delta^2(1+2\delta)^{-1} \end{aligned}$$

So we have that

$$\left|S_N(x, \chi)\right| \ll_{\varepsilon} x n^{-\delta^2(1+2\delta)^{-1}+\varepsilon}$$

and (1.3) follows for an appropriate choice of $\varepsilon = \varepsilon(\delta)$. $\square$

Corollary 1.8. *Let $q > 1, \chi$ a primitive character modulo q of order dividing k and let $\delta \in (0, \frac{1}{3}]$. Then, for $x \geq q^{\frac{1}{4}+\delta}$, we have that*

$$\Big|\sum_{n\leq x}\chi(n)\Big| \ll_{\delta,k} x^{1-\delta^2} \tag{1.15}$$

Proof. Applying Theorem 1.3 with $N = 0$ reads

$$\big|S_0(x,\chi)\big| = \Big|\sum_{1\leq n\leq x}\chi(n)\Big| \ll_{\varepsilon,t} R_k(q)^{\frac{1}{t}} x^{1-\frac{1}{t}} q^{\frac{t+1}{4t^2}+\varepsilon} \quad \forall t \in \mathbb{N}, t \geq 1$$

Hence

$$\Big|\sum_{n\leq x}\chi(n)\Big| \ll_{\varepsilon,t,k} x^{1-\frac{1}{t}} q^{\frac{t+1}{4t^2}+\varepsilon} \quad \forall t \in \mathbb{N}, t \geq 1$$

Since $x \geq q^{\frac{1}{4}+\varepsilon}$, we have that

$$q^{\frac{t+1}{4t^2}+\varepsilon} \leq x^{\frac{\frac{t+1}{4t^2}+\varepsilon}{\frac{1}{4}+\delta}}$$

Thus

$$\Big|\sum_{n\leq x}\chi(n)\Big| \ll_{\varepsilon,t,k} x^{1-\frac{1}{t}} x^{\frac{\frac{t+1}{4t^2}+\varepsilon}{\frac{1}{4}+\delta}} = x \cdot x^{\frac{\frac{1}{4t^2}-\frac{\delta}{t}+\varepsilon}{\frac{1}{4}+\delta}}$$

Since this holds for any $t \in \mathbb{N}, t \geq 1$ and for any $\varepsilon > 0$, choosing $t = \lceil\frac{1}{2\delta}\rceil$, $\varepsilon = \frac{\delta^2}{60}$ and keeping in mind that $\delta \in (0, \frac{1}{3}]$, we have that

$$t < \frac{1}{2\delta} + 1 = \frac{1}{\delta}(\frac{1}{2} + \delta) \leq \frac{1}{\delta}\Big(\frac{1}{2} + \frac{1}{3}\Big) = \frac{5}{6\delta}$$

Hence

$$\frac{1}{4t^2} - \frac{\delta}{t} = \frac{1}{t}\Big(\frac{1}{4t} - \delta\Big) \leq \frac{1}{t}\Big(\frac{\delta}{2} - \delta\Big) = -\frac{\delta}{2t} \leq -\frac{\delta}{2}\frac{6\delta}{5} = -\frac{3}{5}\delta^2$$

So

$$\frac{1}{4t^2} - \frac{\delta}{t} + \varepsilon \leq -\frac{3}{5}\delta^2 + \frac{\delta^2}{60} = -\frac{7}{12}\delta^2$$

But then, since $\frac{1}{4} + \delta \leq \frac{1}{4} + \frac{1}{3} = \frac{7}{12}$, we have that

$$\frac{\frac{1}{4t^2} - \frac{\delta}{t} + \varepsilon}{\frac{1}{4} + \delta} \leq -\delta^2$$

which completes the proof. □

This corollary is a very important consequence of Burgess's bound as it is heavily used in the third section to obtain the main result of this paper.

We continue with an application of Theorem 1.3

Theorem 1.9. *Let χ be a nonprincipal character mod n. Let m, h be any integers with h positive and suppose that χ is constant on $\{y|m < y \leq m + h$ and $gcd(y, n) = 1\}$. Then $h \ll_\varepsilon n^{\frac{1}{4}+\varepsilon}$.*

This theorem generalizes a result of Burgess who obtained the bound $h^{\frac{1}{4}} \log p$ for the particular case when $n = p$ is a prime and also a result of Norton on consecutive power residues(see[9], Theorem 4).

Proof. Let χ be a nonprincipal character mod n of order k which satisfies the condition in the hypothesis and let p be a prime factor of k.

Consider θ, the principal character mod n and define a character ξ mod n, $\xi = \chi^{\frac{k}{p}}$. Then ξ has order p and it must be constant on $\{y|m < y \leq m+h \textit{ and } gcd(y,n) = 1\}$. But then

$$S_m(h,\xi) = S_m(h,\theta) \tag{1.16}$$

By the representation of θ used in the proof of Lemma 1.6, we have

$$\begin{aligned}
S_m(h,\theta) &= \sum_{y=m+1}^{m+h} \theta(y) \\
&= \sum_{y=m+1}^{m+h} \sum_{d|y,d|n} \mu(d) \\
&= \sum_{\substack{y=m+1 \\ gcd(y,n)=1}}^{m+h} \sum_{d|y,d|n} \mu(d) + \sum_{\substack{y=m+1 \\ gcd(y,n)>1}}^{m+h} \sum_{d|y,d|n} \mu(d) \\
&= \sum_{\substack{y=m+1 \\ gcd(y,n)=1}}^{m+h} 1 \ + \sum_{\substack{y=m+1 \\ gcd(y,n)>1}}^{m+h} \sum_{d|gcd(y,n)} \mu(d)
\end{aligned} \tag{1.17}$$

Since there are $\varphi(n)$ numbers relatively prime to n in any length n interval $[kn+1,(k+1)n]$, we can estimate the first term in (1.17) by $\frac{h}{n}\varphi(n)$.

As for the second one, we have that

$$\sum_{d|gcd(y,n)} \mu(d) \leq \sum_{d|gcd(y,n)} 1 = 2^{\omega(gcd(y,n))}$$

So

$$\sum_{\substack{y=m+1 \\ gcd(y,n)>1}}^{m+h} \sum_{d|gcd(y,n)} \mu(d) \leq \sum_{\substack{y=m+1 \\ gcd(y,n)>1}}^{m+h} 2^{\omega(gcd(y,n))}$$

and this can be bounded in terms of n^{ε} for any $\varepsilon > 0$.

Hence we have the estimate

$$\left|S_m(h,\theta)\right| = \frac{h}{n}\varphi(n) + \mathcal{O}_{\varepsilon}(n^{\varepsilon})$$

On the other hand, Theorem 1.3 gives us

$$\left|S_m(h,\xi)\right| \ll_{\varepsilon,t} h^{1-\frac{1}{t}} n^{\frac{t+1}{4t^2}+\varepsilon} \quad \forall t \in \mathbb{N}^*$$

So from these last results and (1.15) we get that

$$\frac{h}{n}\varphi(n) \ll_{\varepsilon,t} h^{-\frac{1}{t}} n^{\frac{t+1}{4t^2}+\varepsilon}$$

Hence

$$h^{\frac{1}{t}} \ll_{\varepsilon,t} n^{\frac{t+1}{4t^2}+\varepsilon}$$

So

$$h \ll_{\varepsilon,t} n^{\frac{t+1}{4t}+\varepsilon t} = n^{\frac{1}{4}+\frac{1}{4t}+\varepsilon}$$

Choosing t as an appropriate function of ε, we get the desired result. $\square$

Theorem 1.9 can be generalized as follows:

Theorem 1.10. *Let K be a real valued function on the positive integers such that*

$$1 \leq K(n) \ll_{\varepsilon} n^{\varepsilon} \quad \forall n \in \mathbb{N}^*$$

Let χ be a nonprincipal character mod n of order k. Let m, h be any integers with h positive and suppose that χ takes at most $min\{k-1, K(n)\}$ distinct values on the set $\{y|m < y \leq m+h$ and $gcd(y,n) = 1\}$. Then $h \ll_{\varepsilon} n^{\frac{1}{4}+\varepsilon}$.

For details of the proof of this theorem, see [10].

1.2 Dirichlet's hyperbola method

Let f, g, h be multiplicative functions such that $f = g \star h$, where $\star$ denotes the Dirichlet convolution of g and h i.e.

$$(g \star h)(n) = \sum_{d|n} g(d)h(\frac{n}{d}) = \sum_{ab=n} g(a)h(b)$$

where the sum extends on all positive divisors of n or equivalently over all pairs (a, b) of positive integers whose product is n. For more on the Dirichlet convolution also known as Dirichlet product, see [5].

Dirichlet's hyperbola method (typically shortened to hyperbola method) is a way to compute $\sum_{n\leq x} f(n)$ using the Dirichlet convolution $f = g \star h$.

Theorem 1.11. *(Dirichlet's hyperbola method). Let f, g, h be multiplicative functions as above and write*

$$G(X) = \sum_{1\leq n\leq X} g(n) \quad \textit{and} \quad H(X) = \sum_{1\leq n\leq X} h(n)$$

Then

$$\begin{aligned}\sum_{1\leq n\leq X} f(n) &= \sum_{1\leq n\leq X} (g \star h)(n) \\ &= \sum_{1\leq a\leq y} g(a)H(\frac{x}{a}) + \sum_{1\leq b\leq \frac{X}{y}} h(b)G(\frac{X}{b}) - G(y)H(\frac{X}{y}) \quad \forall\ 1 \leq y \leq X \qquad (1.18)\end{aligned}$$

Proof. We have that

$$\begin{aligned}\sum_{1\leq n\leq X} f(n) &= \sum_{1\leq n\leq X} (g \star h)(n) \\ &= \sum_{1\leq n\leq X} \sum_{ab=n} g(a)h(b) \\ &= \sum_{1\leq ab\leq X} g(a)h(b)\end{aligned}$$

where the sum is over the set

$$\mathcal{M} = \{(a, b) \in (\mathbb{N}^*)^2 | ab \leq X\}$$

The name of the method comes from the fact that $\mathcal{M}$ is the set of positive integer pairs under the hyperbola $xy = X$.

Let $1 \leq y \leq X$ and $(a, b) \in \mathcal{M}$. Then we must have $a \leq y$ or $b \leq \frac{X}{y}$, otherwise $ab > X$. Hence we can write $\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2$ where

$$\mathcal{M}_1 = \{(a, b) \in (\mathbb{N}^*)^2 | ab \leq X \ \textit{and} \ a \leq y\}$$

$$\mathcal{M}_2 = \{(a,b) \in (\mathbb{N}^*)^2 | ab \leq X \ \ and \ \ b \leq \frac{X}{y}\}$$

Therefore, by the inclusion-exclusion principle we have

$$\begin{aligned}\sum_{(a,b)\in\mathcal{M}} g(a)h(b) &= \sum_{(a,b)\in\mathcal{M}_1\cup\mathcal{M}_2} g(a)h(b) \\ &= \sum_{(a,b)\in\mathcal{M}_1} g(a)h(b) + \sum_{(a,b)\in\mathcal{M}_2} g(a)h(b) - \sum_{(a,b)\in\mathcal{M}_1\cap\mathcal{M}_2} g(a)h(b)\end{aligned}$$

But

$$\begin{aligned}\mathcal{M}_1 \cap \mathcal{M}_2 &= \{(a,b) \in (\mathbb{N}^*)^2 | ab \leq X, a \leq y, b \leq \frac{X}{y}\} \\ &= \{(a,b) \in (\mathbb{N}^*)^2 | a \leq y, b \leq \frac{X}{y}\}\end{aligned}$$

Finally

$$\begin{aligned}\sum_{(a,b)\in\mathcal{M}} g(a)h(b) &= \sum_{ab\leq X}\sum_{a\leq y} g(a)h(b) + \sum_{ab\leq X}\sum_{b\leq\frac{X}{y}} g(a)h(b) - \sum_{a\leq x}\sum_{b\leq\frac{X}{y}} g(a)h(b) \\ &= \sum_{a\leq y} g(a) \sum_{b\leq\frac{X}{a}} h(b) + \sum_{b\leq\frac{X}{y}} h(b) \sum_{a\leq\frac{X}{b}} g(a) - \sum_{a\leq y} g(a) \sum_{b\leq\frac{X}{y}} H(b) \\ &= \sum_{a\leq y} g(a)H(\frac{X}{a}) + \sum_{b\leq\frac{X}{y}} h(b)G(\frac{X}{b}) - G(y)H(\frac{X}{y})\end{aligned}$$

□

Using the hyperbola method, a nice and quite straightforward result can be obtained on $\tau(n)$, the divisor function, namely

Theorem 1.12. *For any $X \geq 1$ we have*

$$\sum_{1\leq n\leq X} \tau(n) = X\log X + (2\gamma - 1)X + \mathcal{O}(X^{\frac{1}{2}})$$

where γ is the Euler-Mascheroni constant.

Given a character χ, we define $r_\chi : \mathbb{Z} \longrightarrow \mathbb{C}$, $r_\chi(n) = \sum_{d|n}\chi(d)$. It follows then that

$$r_\chi(n) = \prod_{p^e||n} (1 + \chi(p) + ... + \chi(p)^e) \tag{1.19}$$

so r_χ is multiplicative.

Notice that for a quadratic character χ, (1.19) tells us that $r_\chi(n) \geq 0 \ \forall n \in \mathbb{Z}$ and in fact we can give a complete characterization of r_χ:

$$r_\chi(n) = \begin{cases} 0 & \text{if } \exists \text{ prime } p \mid n \text{ such that } v_p(n) \text{ is odd and } \chi(p) = -1 \\ \tau(n) & \text{if all the primes } p \mid n \text{ are residues} \\ \tau(\frac{n}{m}), & \text{otherwise} \end{cases}$$

Here $\tau(n)$ represents as usual, the number of divisors of n, $v_p(n)$ is the valuation of n at p and

$$m = \prod_{\substack{p^e||n \\ \chi(p)=1}} p^e$$

Proposition 1.13. *For any $\varepsilon > 0$,if χ is a quadratic character mod m and $x \geq m^{\frac{1}{4}+\varepsilon}$, then there exists a constant $\eta = \eta(\varepsilon) > 0$ such that*

$$\sum_{n \leq x} r_\chi(n) = L(1,\chi)x + \mathcal{O}_\varepsilon(x^{1-\eta})$$

Proof. Let $\alpha = \frac{\frac{1}{4}+\frac{\varepsilon}{2}}{\frac{1}{4}+\varepsilon} \in (0,1)$ and let $y = x^\alpha$. Then

$$y = x^\alpha \geq (m^{\frac{1}{4}+\varepsilon})^\alpha = m^{\frac{1}{4}+\frac{\varepsilon}{2}}$$

Put $z = \frac{x}{y}$ and remark that from the definition of r_χ and of the Dirichlet convolution, we have that $r_\chi = \chi \star 1$. But then, by Dirichlet's hyperbola method, putting $g \equiv \chi$ and $h \equiv 1$ in (1.18) gives us

$$\sum_{n \leq x} r_\chi(n) = \sum_{n \leq x} (\chi \star 1)(n) = \sum_{a \leq y} \chi(a) \sum_{b \leq \frac{x}{a}} 1 \; + \sum_{b \leq z} \sum_{a \leq \frac{x}{b}} \chi(a) - \sum_{a \leq y} \chi(a) \sum_{b \leq z} 1 \qquad (1.20)$$

Observe that by putting $k = 2$ in Theorem 1.3, we have that $1 \leq R_2(m) \leq Q(2)^{\frac{9}{8}} = 1$ since 2 is cubefree. Hence, by using (1.2), we get the following estimate

$$\sum_{d \leq w} \chi(d) \ll_{\varepsilon,t} w^{1-\frac{1}{t}} m^{\frac{t+1}{4t^2}+\varepsilon} \quad \forall w, t \text{ positive integers}$$

Consider now an integer $w \geq y$. Since $y \geq m^{\frac{1}{4}+\frac{\varepsilon}{2}}$ we have that $w \geq m^{\frac{1}{4}+\frac{\varepsilon}{2}}$ so for big enough t there is a constant $\theta = \theta(\varepsilon) > 0$ such that

$$\sum_{d \leq w} \chi(d) \ll_\varepsilon w^{1-\theta} \quad \forall w \geq y \qquad (1.21)$$

Notice that if $1 \leq b \leq z = \frac{x}{y}$ then $y \leq \frac{x}{b}$, so we can apply (1.21) for the second double sum in (1.20) and get

$$\sum_{b \leq z} \sum_{a \leq \frac{x}{b}} \chi(a) \ll_\varepsilon \sum_{b \leq z} (\frac{x}{b})^{1-\theta} = x^{1-\theta} \sum_{b \leq z} b^{\theta-1} \leq x^{1-\theta} \cdot z \cdot z^{\theta-1} = z(\frac{z}{x})^{\theta-1} = x(\frac{z}{x})^\theta = xy^{-\theta}$$

Similarly, applying (1.21) for the third double sum in (1.20) we get

$$\sum_{a \leq y} \chi(a) \sum_{b \leq z} 1 \leq z \sum_{a \leq y} \chi(a) \ll_\varepsilon zy^{1-\theta} = xy^{-\theta}$$

For the first double sum in (1.20) we have

$$\begin{aligned} \sum_{a \leq y} \chi(a) \sum_{b \leq \frac{x}{a}} 1 &= \sum_{a \leq y} \chi(a)(\frac{x}{a} + \mathcal{O}(1)) \\ &= x \sum_{a \leq y} \frac{\chi(a)}{a} + \mathcal{O}(1) \sum_{a \leq y} \chi(a) \\ &= x(L(1,\chi) - \sum_{a > y} \frac{\chi(a)}{a}) + \mathcal{O}(y) \\ &= xL(1,\chi) + \mathcal{O}_\varepsilon(xy^{-\theta}) + \mathcal{O}(y) \end{aligned}$$

From these 3 estimations of the double sums in (1.20) we deduce that

$$\sum_{n \leq x} r_\chi(n) = xL(1,\chi) + \mathcal{O}_\varepsilon(xy^{-\theta}) + \mathcal{O}(y)$$

$$= xL(1,\chi) + \mathcal{O}_\varepsilon(x \cdot x^{-\alpha\theta}) + \mathcal{O}(x^\alpha)$$
$$= xL(1,\chi) + \mathcal{O}_\varepsilon(x^{1-\alpha\theta}) + \mathcal{O}(x^\alpha)$$

Letting $\eta = min\{\alpha\theta, 1-\alpha\}$, we have that

$$\begin{aligned} max\{x^\alpha, x^{1-\alpha\theta}\} &= max\{x^{1-(1-\alpha)}, x^{1-\alpha\theta}\} \\ &= x^{1-min\{\alpha\theta, 1-\alpha\}} \\ &= x^\eta \end{aligned}$$

Hence this and the last estimate yield

$$\sum_{n\leq x} r_\chi(n) = L(1,\chi)x + \mathcal{O}_\varepsilon(x^{1-\eta})$$

□

Together with Corollary 1.8, the following result of Siegel is used to prove both the final results of this section as well as the main result of the paper. The downside of using this theorem is that the constant appearing in the statement is generally non-effective.

1.3 Siegel's Theorem

Theorem 1.14. *(Siegel) For any $\varepsilon > 0$, there exists a constant $C(\varepsilon) > 0$ such that $C(\varepsilon)q^{-\varepsilon} \leq |L(1,\chi)|$ for any primitive character χ modulo q.*

Proof. Let $\chi_1 \neq \chi_2$ be primitive non-principal real characters modulo q_1 and q_2 respectively. Define

$$\begin{aligned} F(s) &= \zeta(s)L(s,\chi_1)L(s,\chi_2)L(s,\chi_1\chi_2) \\ &= \prod_p \left(1-\frac{1}{p^s}\right)^{-1}\left(1-\frac{\chi_1(p)}{p^s}\right)^{-1}\left(1-\frac{\chi_2(p)}{p^s}\right)^{-1}\left(1-\frac{\chi_1(p)\chi_2(p)}{p^s}\right)^{-1} \end{aligned}$$

We can thus write

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

with $a_0 = 1$ and $a_n \geq 0 \, \forall n \geq 2$. Notice that $F(s)$ has a simple pole at $s = 1$ with

$$Res_{s=1}F(s) = L(1,\chi_1)L(1,\chi_2)L(1,\chi_1\chi_2) = \lambda$$

and it is regular on $\mathbb{C} \setminus \{1\}$. We show that $\exists \alpha \in (0,1)$ and $A, B, C > 0$ such that

$$F(s) > A - \frac{B\lambda}{1-s}(q_1q_2)^{C(1-s)} \tag{1.22}$$

holds for any $s \in (\alpha, 1)$.

Since $F(s)$ has nonnegative Dirichlet series, its Taylor expansion at $s_0 = 2$ is

$$F(s) = \sum_{k=0}^{\infty}(b_k - \lambda)(2-s)^k \quad \forall s \in \mathbb{C}$$

where $b_0 = F(2) > 1$ and $b_k > 0 \, \forall k \geq 0$. F is entire except for a simple pole of residue λ at $s = 1$ so we have

$$F(s) - \frac{\lambda}{s-1} = \sum_{k=0}^{\infty}(b_k - \lambda)(2-s)^k \quad \forall s \in \mathbb{C}$$

Consider this equality on the circle $|s-2| = \frac{3}{2}$. The trivial bounds $L(s,\chi_1) \ll q_1$, $L(s,\chi_2) \ll q_2$, $L(s,\chi_1\chi_2) \ll q_1q_2$ and the fact that $\zeta(s)$ is bounded on $|s-2| = \frac{3}{2}$ give us that $F(s) \ll (q_1q_2)^2$, hence the same holds for $F(s) - \frac{\lambda}{s-1}$. Thus

$$|b_k - \lambda| \ll \left(\frac{2}{3}\right)^k (q_1q_2)^2$$

Then

$$\sum_{k=M}^{\infty} |b_k - \lambda|(2-s)^k \ll (q_1q_2)^2 \Big(\frac{2}{3}(2-\alpha)\Big)^M$$

for any $s \in (\alpha, 1)$, where $\alpha \in (\frac{1}{2}, 1)$ is fixed. Consequently, since $b_0 > 1$ and $b_k \geq 0\,\forall k$, we have

$$F(s) - \frac{\lambda}{s-1} \geq 1 - \lambda + (b_1-\lambda)(2-s) + ... + (b_{M-1}-\lambda)(2-s)^{M-1} - \mathcal{O}((q_1q_2)^2)\Big(\frac{2}{3}(2-\alpha)\Big)^M$$

Hence

$$F(s) - \frac{\lambda}{s-1} \geq 1 - \lambda(1 + (2-s) + ... + (2-s)^{M-1}) - \mathcal{O}((q_1q_2)^2)\Big(\frac{2}{3}(2-\alpha)\Big)^M$$

So

$$F(s) - \frac{\lambda}{s-1} \geq 1 - \lambda\frac{(2-s)^M - 1}{1-s} - \mathcal{O}((q_1q_2)^2)\Big(\frac{2}{3}(2-\alpha)\Big)^M$$

Let M be the largest integer such that the error estimate is $< \frac{1}{2}$. Then

$$F(s) > \frac{\lambda}{s-1} + 1 - \lambda\frac{(2-s)^M - 1}{1-s} - \frac{1}{2} = \frac{1}{2} - \frac{\lambda}{1-s}(2-s)^M$$

But

$$(2-s)^M = e^{M\log(2-s)} \leq e^{M(2-s-1)}$$

and since

$$e^M \ll (q_1q_2)^{\mathcal{O}(1)}$$

this concludes the proof of (1.22).

Fix $\varepsilon > 0$. Then, Siegel's Theorem is trivial if there is no modulus q_ε and real character χ_ε mod q_ε such that $L(s,\chi_\varepsilon)$ has a zero in $\big(1 - \frac{\varepsilon}{2C}, 1\big)$. So we can assume that $L(s,\chi_\varepsilon)$ has a zero β_ε. Then, for $q_\varepsilon = q_2, \chi_\varepsilon = \chi_2$, let β be a zero of $L(s,\chi_2)$, hence $F(\beta) = 0$.

Then (1.22) reads

$$0 > A - \frac{B\lambda}{1-\beta}(q_1q_2)^{C(1-\beta)}$$

Thus

$$\lambda > \frac{A}{B}(1-\beta)(q_1q_2)^{-C(1-\beta)}$$

Therefore

$$L(1,\chi_1)L(1,\chi_2)L(1,\chi_1\chi_2) > \frac{A}{B}(1-\beta)(q_1q_2)^{-C(1-\beta)}$$

Using the trivial bounds $L(1,\chi_2) \ll \log q_2$, $L(1,\chi_1\chi_2) \ll \log q_1q_2$ we obtain

$$L(1,\chi_1) > Mq_1^{-C(1-\beta)}\frac{1}{\log q_1}\frac{1}{\log q_1q_2}$$

and since $\log q_1 \in o(q_1^\delta)$, $\log q_1q_2 \in o((q_1q_2)^\delta)$ $\forall\delta > 0$, we conclude that

$$L(1,\chi_1) \gg q_1^{-\varepsilon}$$

$\square$

Definition 1.15. *For a positive integer n, we define $P^+(n)$ to be the largest prime factor of n, with the convention that $P(1) = 1$. We say that n is $y-smooth$ or $y-friable$ if $P^+(n) \leq y$.*

For $x \geq y \geq 2$ define the de Bruijn function $\Psi(x, y) = |\{n \leq x | P^+(n) \leq y\}|$. A result of de Bruijn([1]) states that for a fixed $\theta \geq 1$ we have that

$$\Psi(x, , (\log x)^\theta) = x^{1-\frac{1}{\theta}+o(1)} \quad as\ x \longrightarrow \infty \tag{1.23}$$

1.4 Proof of Theorem 1.1

Let $\varepsilon \in (0, \frac{1}{4})$ and let χ be a quadratic character mod n. Let $x = m^{\frac{1}{4}+\varepsilon}$ and set

$$q = \prod_{\substack{p \text{ prime} \\ p \leq x \\ \chi(p)=1}} p$$

Then it suffices to prove that $\omega(q) \geq (\log m)^A$. Suppose then that $\omega(q) < (\log m)^A$. Choose $S \subseteq [1, x]$ such that $Supp(r_\chi) \subseteq S$ on $[1, x]$ and let $M = max\{r_\chi(n) | n \in S\}$.

As seen before, $r_\chi(n) \geq 0 \ \forall n \in \mathbb{N}^*$ so we have that

$$0 \leq \sum_{n \leq x} r_\chi(n) \leq |S|M$$

But from our characterization of r_χ, we can choose $S = \{n \leq x | p || n \Rightarrow p | mq\}$. Now, each element n of S can be written as a product $n = n_1 n_2$ of a squarefree divisor n_1 of mq and a squarefull divisor n_2 of mq. Notice that the number of elements of S for which $n_2 > x^{\frac{1}{2}}$ is $\mathcal{O}(x^{\frac{3}{4}})$ and let us consider the remaining elements of S.

Given n_2, we have at most d choices for n_1, where d is the number of squarefree integers in $[1, \frac{x}{n_2}]$ composed of the first $\omega(mq)$ primes. Since $\omega(q) < (\log m)^A$ and $\omega(mq) \leq \omega(m) + \omega(q)$, we get that $\omega(mq) < \omega(m) + (\log m)^A$.

But $x = m^{\frac{1}{4}+\varepsilon}$, so

$$\omega(mq) < \omega(m) + (\log(x^c)^A$$

where $c = \frac{1}{\frac{1}{4}+\varepsilon}$.

Since $2^{\omega(m)} \ll_\varepsilon m^\varepsilon \leq x^{4\varepsilon}$, we therefore obtain

$$\omega(mq) < \log_2(x^{4\varepsilon}) + c^A \log^A x = 4\varepsilon \log_2 x + c^A log^A x$$

Hence, for large enough x, all the first $\omega(mq)$ primes are $\leq (\log x)^{A+1}$ so the number of choices of n_1 for a fixed n_2 is at most $\Psi(\frac{x}{n_2}, (\log x)^{A+1})$. But then, from (1.23) for $\theta = A+1$ we get

$$\Psi(x, (\log x)^{A+1}) = x^{1-\frac{1}{A+1}+o(1)}$$

Since

$$\Psi(x, (\log x)^{A+1}) \geq \Psi(\frac{x}{n_2}, (\log x)^{A+1})$$

and keeping in mind that $\frac{x}{n_2} \geq x^{\frac{1}{2}}$, for large enough x we have

$$\Psi(\frac{x}{n_2}, (\log x)^{A+1}) \leq (\frac{x}{n_2})^{1-\frac{1}{A+2}}$$

So we have that

$$|S| \ll x^{\frac{3}{4}} + x^{1-\frac{1}{A+2}} \ll x^\alpha$$

where $\alpha = max\{\frac{3}{4}, 1 - \frac{1}{A+2}\}$. Let $\beta = 1 - \alpha$. Then we have that

$$r_\chi(n) = \sum_{d|n} \chi(d) \leq \sum_{d|n} 1 = \tau(n) \ll x^{\frac{\beta}{2}}$$

Hence

$$\sum_{n \leq x} r_\chi(n) \ll |S|M \ll x^\alpha x^{\frac{\beta}{2}} = x^\alpha \cdot x^{\frac{1-\alpha}{2}} = x^{\frac{\alpha+1}{2}}$$

But then, by Proposition 1.13, this implies

$$xL(1,\chi) + \mathcal{O}_\varepsilon(x^{1-\eta}) \ll x^{\frac{\alpha+1}{2}}$$

So we obtain

$$L(1,\chi) \ll x^\gamma$$

where $\gamma = \frac{\alpha-1}{2} < 0$ since $\alpha < 1$, which contradicts Siegel's theorem. Therefore we conclude that $\omega(q) \geq (\log m)^A$ as desired.

In the same setup as Theorem 1.1, but for primes character residues smaller than m we have

Proposition 1.16. *Let χ be a quadratic character mod m. Then*

$$\sum_{\substack{p \leq m \\ \chi(p)=1}} \frac{1}{p} \geq \frac{1}{2} \log(\frac{\varphi(m)}{m} L(1,\chi) \log m) + \mathcal{O}(1)$$

To prove this, we need the following lemma

Lemma 1.17. *Let f be a non-negative multiplicative function which for suitable constants A, B satisfies*

$$(1) \sum_{p \leq y} f(p) \log p \leq Ay \quad \forall y \geq 0$$

$$(2) \sum_{p} \sum_{e \geq 2} \frac{f(p^e)}{p^e} \log p^e \leq B$$

Then

$$\sum_{n \leq x} f(n) \leq (A + B + 1) \frac{x}{\log x} \sum_{n \leq x} \frac{f(n)}{n} \quad \forall x > 1$$

Proof. Let

$$S(x) := \sum_{n \leq x} f(n) \quad \textit{and} \quad L(x) := \sum_{n \leq x} \frac{f(n)}{n}$$

Clearly $S(x) \leq xL(x)$. Furthermore

$$\begin{aligned} S(x) \log x &= \sum_{n \leq x} f(n) \log x \\ &= \sum_{n \leq x} f(n) \log \frac{x}{n} + \sum_{n \leq x} f(n) \log n \\ &= \sum_{n \leq x} f(n) \log \frac{x}{n} + \sum_{n \leq x} f(n) \sum_{p||n} \log p + \sum_{n \leq x} f(n) \sum_{\substack{p^e||n \\ e \geq 2}} \log p^e \end{aligned}$$

For $1 \leq n \leq x$, we have that $\log \frac{x}{n} < \frac{x}{n}$ hence

$$\sum_{n \leq x} f(n) \log \frac{x}{n} \leq \sum_{n \leq x} f(n) \frac{x}{n} = xL(x)$$

Writing $n = mp$ where p is a prime divisor of n and using the first condition in the statement we have that

$$\sum_{n \leq x} f(n) \sum_{p || n} \log p = \sum_{m \leq x} \sum_{\substack{p \leq \frac{x}{m} \\ p \nmid m}} f(p) \log p \leq \sum_{m \leq x} f(m) A \frac{x}{m} \leq \sum_{m \leq x} f(m) A \frac{x}{m} \leq mL(x) A \frac{x}{m} = AxL(x)$$

Finally

$$\begin{aligned}
\sum_{n \leq x} f(n) \sum_{\substack{p^e || n \\ e \geq 2}} \log p^e = \sum_{p} \sum_{e \geq 2} f(p^e) \log p^e \cdot \sum_{\substack{m \leq \frac{x}{p^e} \\ p \nmid m}} f(m) &\leq \sum_{p} \sum_{e \geq 2} f(p^e) \log p^e S(\frac{x}{p^e}) \\
&\leq \sum_{p} \sum_{e \geq 2} f(p^e) \log p^e \frac{x}{p^e} L((\frac{x}{p^e}) \\
&\leq \sum_{p} \sum_{e \geq 2} \frac{f(p^e)}{p^e} xL(x) \\
&\leq BxL(x)
\end{aligned}$$

Summing up the results we conclude that

$$S(x) \log x \leq (A + B + 1) xL(x)$$

Hence

$$\sum_{n \leq x} f(n) \leq (A + B + 1) \frac{x}{\log x} \sum_{n \leq x} \frac{f(n)}{n} \quad \forall x > 1$$

$\square$

Proof of Proposition 1.16
Let us consider the function that we introduced earlier,

$$r = r_\chi(n) = \sum_{d | n} \chi(d) = \sum_{p^e || n} (1 + \chi(p) + \ldots + \chi(p)^e)$$

Then r satisfies the conditions of Lemma 1.17, hence, for some constants A, B we have that

$$\sum_{n \leq m} r(n) \leq (A + B + 1) \frac{m}{\log m} \sum_{n \leq m} \frac{r(n)}{n}$$

So

$$\frac{1}{m} \sum_{n \leq m} r(n) \ll \frac{1}{\log m} \sum_{n \leq m} \frac{r(n)}{n}$$

Proposition 1.13 gives us

$$L(1, \chi) \ll \frac{1}{m} \sum_{n \leq m} r(n)$$

Thus

$$L(1, \chi) \ll \frac{1}{\log m} \sum_{n \leq m} \frac{r(n)}{n}$$

So it suffices to show that

$$\sum_{n\le m}\frac{r(n)}{n}\ll\frac{m}{\varphi(m)}\exp\Big(2\sum_{\substack{p\le m\\ p\,\text{prime}\\ \chi(p)=1}}\frac{1}{p}\Big)$$

We have that

$$\sum_{n=1}^{\infty}\frac{r(n)}{n^s}=(\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s})(\sum_{n=1}^{\infty}\frac{1}{n^s})$$

But for $s\to1^+$, we have that $\zeta(s)\sim\frac{1}{s-1}$. Indeed, for $k\ge1$, set

$$a_k(s)=\frac{1}{k^s}-\int_{k-1}^{k}\frac{dt}{t^s}$$

Then, by Taylor's formula to order 2, we have that

$$a_k(s)\sim\frac{s}{2}k^{-s-1}$$

as $s\to+\infty$, hence $\sum_{k\ge2}a_k(s)$ converges for $s>0$. For $s>1$ we have

$$\begin{aligned}\sum_{k\ge2}a_k(s)&=\sum_{k\ge2}\frac{1}{k^s}-\int_1^{\infty}\frac{dt}{t^s}\\&=\zeta(s)-1-\frac{1}{s-1}\end{aligned}$$

Since the series on the left converges normally for $s\ge\varepsilon>0$, by analytic continuation of $\zeta(s)$, it follows that the equality holds for all $s>0$.

Using the Taylor expansion of a_k around $s_0=1$, we obtain the following power series in $s-s_0=s-1$:

$$a_k(s)=\sum_{m\ge0}\frac{(-1)^m}{m!}\Big(\frac{(\log k)^m}{k}-\frac{(\log k)^{m+1}-(\log k-1)^{m+1}}{m+1}\Big)(s-1)^m$$

Thus, by absolute convergence, we can reorder the terms of the double sum $\sum_{k\ge2}a_k(s)$ and get

$$\sum_{k\ge2}a_k(s)=\zeta(s)-1-\frac{1}{s-1}=\sum_{m\ge0}\frac{(-1)^m}{m!}\gamma_m(s-1)^m$$

where we define

$$\begin{aligned}\gamma_m&=\sum_{k\ge2}\Big(\frac{(\log k)^m}{k}-\frac{(\log k)^{m+1}-(\log k-1)^{m+1}}{m+1}\Big)\\&=\lim_{N\to+\infty}\Big(\sum_{k=2}^{N}\frac{(\log k)^m}{k}-\frac{(\log N)^{m+1}}{m+1}\Big)\end{aligned}$$

Notice that in particular, $\gamma_0=\gamma-1$, where γ is the Euler-Mascheroni constant. Furthermore, by the Euler-MacLaurin summation formula, the limit defining γ_m exists, hence

$$\begin{aligned}\zeta(s)&=\frac{1}{s-1}+\sum_{m\ge0}\frac{(-1)^m}{m!}\gamma_m(s-1)^m\\&=\frac{1}{s-1}+\gamma+\mathcal{O}(s-1)\end{aligned}$$

Therefore
$$L(s,\chi)\zeta(s) \sim \frac{L(1,\chi)}{s-1}$$
as $s \to 1^+$.

Using Perron's formula we have
$$\begin{aligned}
\sum_{n\le x} r(n) &= \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} (\sum_{n=1}^{\infty} \frac{r(n)}{n^s})\frac{x^s}{s}ds \\
&= \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} L(s,\chi)\zeta(s)\frac{x^s}{s}ds \\
&= \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{L(1,\chi)}{s-1}\frac{x^s}{s}ds \\
&= L(1,\chi)\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{x^s}{s(s-1)}ds \\
&\sim L(1,\chi)x \qquad (1.24)
\end{aligned}$$

Moreover, Abel summation gives us
$$\begin{aligned}
\sum_{n\le x} \frac{r(n)}{n} &= \frac{R(x)}{x} - \int_1^x (\sum_{n\le t} r(n))(\frac{1}{t})'dt \\
&= \frac{R(x)}{x} + \int_1^x (\sum_{n\le t} r(n))\frac{1}{t^2}dt
\end{aligned}$$

where $R(x) = \sum_{n\le x} r(n)$. But from (1.24), we have that
$$\begin{aligned}
\int_1^x (\sum_{n\le t} r(n))\frac{1}{t^2}dt &= \int_1^x (L(1,\chi)t)t^{-2}dt \\
&= L(1,\chi)\log x
\end{aligned}$$

Hence
$$\sum_{n\le x} \frac{r(n)}{n} \sim L(1,\chi)\log x \qquad (1.25)$$

Now, the Prime Number Theorem gives the following
$$\sum_{\substack{p\le m \\ p \text{ prime} \\ \chi(p)=1}} \frac{1}{p} \sim C \sum_{\substack{p\le m \\ p \text{ prime}}} \frac{1}{p} \sim C\log\log x$$

with $C = \frac{1}{\varphi(m)}$, which combined with (1.25) gives us the desired estimate.

2 The Dedekind zeta function

2.1 Preliminaries

In this section, we explain how the Dedekind zeta function associated to a number field decomposes, which is of vital importance to prove the main theorem in section 3.

Definition 2.1. *Let K be a number field and $\mathcal{O}_K$ its ring of integers. The Dedekind zeta function of K, $\zeta_K(s)$ is defined to be the analytic continuation of the series*

$$\sum_{I \subseteq \mathcal{O}_K} \frac{1}{(N_{K/\mathbb{Q}}(I))^s}$$

where I ranges over all non-zero integral ideals of K and $N_{K/\mathbb{Q}}(I) = |\mathcal{O}_K : I|$ is the norm of I.

ζ_K converges for $Re(s) > 1$ and has a meromorphic continuation to the whole plane with a unique simple pole at $s = 1$. Furthermore, if $k = [K : \mathbb{Q}]$, r_1 is the number of real embeddings and r_2 is the number of pairs of complex embeddings of K, then ζ_K satisfies the following functional equation

$$A^s \Gamma(\frac{s}{2})^{r_1} \Gamma(s)^{r_2} \zeta_K(s) = A^{1-s} \Gamma(\frac{1-s}{2})^{r_1} \Gamma(1-s)^{r_2} \zeta_K(1-s) \tag{2.1}$$

where

$$A = 2^{-r_2} \pi^{-\frac{k}{2}} \sqrt{|disc(K)|}$$

For details of this result, see [6], p. 254.

Assume that K is a non-trivial abelian extension of $\mathbb{Q}$ with $D > 1$, where $D = |disc(K)|$ is the absolute value of the discriminant. Let $k = [K : \mathbb{Q}]$ and consider $\zeta_K(s)$, the Dedekind zeta function of K. Then, by the Kronecker-Weber theorem, there exists an integer n(which we choose minimal) such that $K \subseteq \mathbb{Q}(\xi_n)$, the n-th cyclotomic field.

Let $G = Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})$ and let $\chi : G \longrightarrow \mathbb{C}^*$ be a Dirichlet character. Then the kernel of χ determines a fixed subfield of $\mathbb{Q}(\xi_n)$ and for any field K as above, there is a group X of Dirichlet characters of G such that K is equal to the intersection of the fixed fields by the kernels of all $\chi \in X$. Moreover, $|X| = k$ and $X \simeq Gal(K/\mathbb{Q})$.

Conversely, given X a finite group of Dirichlet characters of conductors $f_{\chi_1}, ..., f_{\chi_k}$, where $k = |X|$, let $n = lcm(f_{\chi_1}, ..., f_{\chi_k})$. Then X is a subgroup of the characters of $Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})$ and let $H = \bigcap_{\chi \in X} Ker(\chi)$. If K is the fixed field of H, then X coincides with the set of homomorphisms $Gal(K/\mathbb{Q}) \longrightarrow \mathbb{C}^*$.

If G is a finite abelian group, let $\widehat{G}$ be the group of multiplicative homomorphisms from G to $\mathbb{C}^*$.

Lemma 2.2. *If G is a finite abelian group, then $G \simeq \widehat{G}$(noncanonically).*

Proof. By the divisors theorem, G decomposes as

$$G \simeq \bigoplus_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$$

Hence

$$\widehat{G} \simeq \bigoplus_{i=1}^{r} \widehat{\mathbb{Z}/d_i\mathbb{Z}}$$

For $\chi \in \widehat{\mathbb{Z}/d_i\mathbb{Z}}$, we have that $\chi(1)$ determines χ since $\mathbb{Z}/d_i\mathbb{Z}$ additive and cyclic, so since $\chi(1)$ can be any m-th root of unity, it follows that the lemma holds true for any $\mathbb{Z}/m\mathbb{Z}$, hence for G. $\square$

Corollary 2.3. $G \simeq \widehat{\widehat{G}}$*(canonically).*

Proof. Let $g \in G$ and suppose $\chi(g) = 1 \, \forall \chi \in \widehat{G}$. Let $H =< g >$. Then $\widehat{G}$ acts as a set of distinct characters of the quotient G/H. But by the previous lemma, there are at most $|G/H|$ of these, hence $H = \{1\}$ which yields $g = 1$. Therefore G injects into $\widehat{G}$ and the conclusion follows since $|G| = |\widehat{G}| = |\widehat{\widehat{G}}|$. □

Let H be subgroup of G . Then we define

$$H^{\perp} = \{\chi \in \widehat{G} | \chi(h) = 1 \, \forall h \in H\}$$

Clearly, there is an isomorphism $H^{\perp} \simeq \widehat{G/H}$.

Lemma 2.4. $\widehat{H} \simeq \widehat{G}/H^{\perp}$.

Proof. By restriction, there exists a map $\widehat{G} \longrightarrow \widehat{H}$ whose kernel is $H^{\perp}$.
On the other hand,

$$|H^{\perp}| = |\widehat{G/H}| = |G/H| = \frac{|G|}{|H|}$$

Hence

$$|\widehat{H}| = |H| = \frac{|G|}{|H^{\perp}|} = \frac{|\widehat{G}|}{|H^{\perp}|}$$

which gives us the surjectivity as well. □

Another straightforward result is

Lemma 2.5. $(H^{\perp})^{\perp} = H$.

The previous three results hold true for locally compact abelian groups as well, but the proofs are harder since we cannot use counting arguments.

Consider the pairing

$$G \times \widehat{G} \longrightarrow \mathbb{C}^*$$
$$(g, \chi) \longrightarrow \chi(g)$$

Notice that if $\chi(g) = 1 \forall \chi \in \widehat{G}$, then $g = 1$. But then, if $\chi(g) = 1 \forall g \in G$, then clearly $\chi = 1$. Therefore the pairing is nondegenerate.

Let K be a field and X its associated group of Dirichlet characters. Let L be a subfield of K and let

$$Y = \{\chi \in X | \chi(\sigma) = 1 \, \forall \sigma \in Gal(K/L)\}$$

Then

$$\begin{aligned} Y &= Gal(L/K)^{\perp} \\ &= Gal(K/\widehat{\mathbb{Q})/G}al(K/L) \\ &= Ga\widehat{l(L/}\mathbb{Q}) \end{aligned}$$

Conversely, if $Y \subseteq X$ is a subgroup and L the fixed field of $Y^{\perp} = \{g \in Gal(K/\mathbb{Q}) | \chi(g) = 1 \, \forall \chi \in Y\}$, then by Galois theory, we have that $Y^{\perp} = Gal(K/L)$. So

$$Y = (Y^{\perp})^{\perp} = Gal(K/L)^{\perp} = Ga\widehat{l(L/}\mathbb{Q})$$

Therefore there is a one to one correspondence between subgroups of X and subfields of K given by

$$Gal(K/L)^{\perp} \longleftrightarrow L$$

$$Y \longleftrightarrow \text{fixed field of } Y^{\perp}$$

whence a one to one correspondence between groups of Dirichlet characters and subfields of cyclotomic fields.

Since $Gal(L/\mathbb{Q})$ is a finite abelian group, Lemma 2.2 tells us that

$$Y = \widehat{Gal(L/\mathbb{Q})} \simeq Gal(L/\mathbb{Q})$$

although not canonically, thus the preference for the natural nondegenerate pairing $Gal(L/\mathbb{Q}) \times Y \longrightarrow \mathbb{C}^*$.

Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ be the prime decomposition of a positive integer $n \geq 2$. By the Chinese Remainder Theorem we know that

$$(\mathbb{Z}/n\mathbb{Z})^{\times} \simeq \prod_{i=1}^{k} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^{\times}$$

Then given a character χ mod n, decompose it as

$$\chi = \prod_{i=1}^{k} \chi_{p_i}$$

where χ_{p_i} is a Dirichlet character defined mod $p_i^{\alpha_i}$.

For a group X of Dirichlet characters, define

$$X_{p_i} = \{\chi_{p_i} | \chi \in X\} \, \forall i \in \overline{1,k}$$

.

Theorem 2.6. *Let X be a group of Dirichlet characters and K its associated field. If p is a prime number with ramification index e_p in K, then $e_p = |X_p|$.*

Proof. Let $n = lcm(f_\chi)_{\chi \in X}$, where f_χ denotes as usual, the conductor of the character χ. Then $K \subseteq \mathbb{Q}(\zeta_n)$. Decompose n as $n = p^a m$, with $gcd(p, m) = 1$ and consider the composite field $L = K(\zeta_m) = K\mathbb{Q}(\zeta_m)$. Let

$$Y = \{\chi | \chi \text{ character of } (\mathbb{Z}/n\mathbb{Z})^{\times} \text{ with } gcd(f_\chi, p) = 1\}$$

Notice that Y consists in fact of the characters mod m. Then the group of characters of L is generated by X and Y. Hence the group of characters of L is given by the direct product of X_p with the characters of $\mathbb{Q}(\zeta_m)$. So

$$L = \mathbb{Q}(\zeta_m)F$$

the compositum of $\mathbb{Q}(\zeta_m)$ with the field $F \subseteq \mathbb{Q}(\zeta_{p^a})$ associated to X_p.

Observe that the ramification index e_p of p in K is the same as for p in L since p is unramified in $\mathbb{Q}(\zeta_m)$. But p is unramified in L/F, hence e_p is equal to the ramification index of p in F which is $deg(F/\mathbb{Q}) = |X_p|$. □

Corollary 2.7. *Let χ be a Dirichlet character and K its associated field. Then a prime p ramifies in $K \Leftrightarrow \chi(p) = 0$. More generally, given a group X of Dirichlet characters, if L is its associated field, then p is unramified in $L/\mathbb{Q} \Longleftrightarrow \chi(p) \neq 0 \, \forall \chi \in X$.*

Proof. By the previous theorem, we have that p ramifies in $L \Longleftrightarrow X_p \neq 1 \Longleftrightarrow \exists \chi \in X$ with $\chi_p \neq 1 \Longleftrightarrow \exists \chi \in X$ such that $p | f_\chi \Longleftrightarrow \exists \chi \in X$ such that $\chi(p) = 0$. □

Theorem 2.8. *Let X be a group of Dirichlet characters, K its associated field and p a rational prime. Let*

$$X_1 = \{\chi \in X | \chi(p) \neq 0\}$$

$$X_2 = \{\chi \in X | \chi(p) = 1\}$$

Let e_p be the ramification index of p in K and f_p the residue class degree. Then $e_p = [X : X_1]$ and $f_p = [X_1 : X_2]$. In fact, $X/X_1 \simeq$ the inertia group and X_1/X_2 is cyclic of order f_p.

Proof. Let $L \subseteq K$ be the subfield associated to X_1. Corollary 2.7 tells us that L is the maximal subfield of K in which p is unramified. Then L is the fixed field of the inertia group, hence the inertia group is $Gal(K/L)$. Considering the pairing $Gal(K/\mathbb{Q}) \times X \longrightarrow \mathbb{C}^*$, by the Galois correspondence between subgroups and subfields, we have that $X_1 = Gal(K/L)^\perp$. Therefore

$$\begin{aligned} X/X_1 &= \widehat{Gal(K/\mathbb{Q})}/Gal(K/L)^\perp \\ &= \widehat{Gal(K/L)} \\ &\simeq Gal(K/L) \end{aligned}$$

where we made use of Lemma 2.2 and Lemma 2.4.

Since $e_p = |Gal(K/L)|$, the order of the inertia group, we therefore have that $e_p = |X/X_1|$.

Consider now the extension $L/\mathbb{Q}$ which has X_1 as its group of characters. Let $n = lcm(f_\chi)_{\chi \in X_1}$. Since p is unramified in L, we have that $p \nmid n$ and $L \subseteq \mathbb{Q}(\zeta_n)$. Since

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$$

we obtain

$$Gal(L/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times/(Gal(\mathbb{Q}(\zeta_n)/L)$$

Notice that σ_p, the Frobenius map for $L/\mathbb{Q}$ is just the coset of p in $Gal(L/\mathbb{Q})$. Since for $\chi \in X_1$ we have that $\chi(\sigma) = 0 \, \forall \sigma \in Gal(\mathbb{Q}(\zeta_n)/L)$, we get that $\chi(\sigma_p) = \chi(p)$ so $\chi(\sigma_p) = 1 \iff \chi(p) = 1$, hence $X_2 =< \sigma_p >^\perp$ under the pairing $Gal(L/\mathbb{Q}) \times X_1 \longrightarrow \mathbb{C}^*$, where $| < \sigma_p > | = f_p$. Consequently, Lemma 2.4 gives us the isomorphism

$$X_1/X_2 \simeq \widehat{< \sigma_p >}$$

But since $\widehat{< \sigma_p >} \simeq < \sigma_p >$, we obtain

$$|X_1/X_2| = | < \sigma_p > | = f_p$$

$\square$

2.2 Decomposition of the Dedekind zeta function

Theorem 2.9. *Let $K \subseteq \mathbb{Q}(\zeta_n)$ be a number field and let X be the associated group of Dirichlet characters mod n. Then*

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi)$$

Proof. Recall the Euler product expansion of the Dedekind zeta function of K

$$\zeta_K(s) = \prod_{\wp \in \mathcal{O}_K} (1 - \frac{1}{N(\wp)^s})^{-1}$$

We compare the product expansions for each integer prime p. Let $p\mathcal{O}_K = \prod_{i=1}^{g} \wp_i^e$ be the prime factorization of p in K, where each $\wp_i$ has residue class degree f and thus $N(\wp_i) = p^f \; \forall i \in \overline{1, g}$.

Then the Euler factors of $\zeta_K(s)$ corresponding to p are just $(1 - \frac{1}{p^{fs}})^{-g}$. For the L-series, the Euler product expansion is

$$L(s, \chi) = \prod_p (1 - \frac{\chi(p)}{p^s})^{-1}$$

The terms corresponding to p are in this case

$$\prod_{\chi \in X} (1 - \frac{\chi(p)}{p^s})^{-1}$$

Let $X_1 = \{\chi \in X | \chi(p) \neq 0\}$ and $X_2 = \{\chi \in X | \chi(p) = 1\}$. Then only the $\chi \in X_1$ will contribute to the product.

By Theorem 2.8, X_1/X_2 is cyclic of order f and let $\chi_0 \in X_1$ such that its image generates X_1/X_2. Clearly $\chi_0(p) = \zeta_f$, a primitive f-th root of unity. Thus

$$\prod_{i=0}^{f-1} (1 - \frac{\chi_0^i(p)}{p^s})^{-1} = \prod_{i=0}^{f-1} (1 - \frac{\zeta_f^i}{p^s})^{-1} = (1 - \frac{1}{p^{fs}})^{-1}$$

Notice though that taking the product over all $\chi \in X$ is the same as taking it over all $\chi \in X_1$ and since $\chi(p) = 1 \, \forall \chi \in X_2$ and the image of χ_0 generates X_1/X_2, it is the same as taking it g times over the powers of χ_0.

We therefore conclude that the Euler factor at any integer prime p for the product of L-series is $(1 - \frac{1}{p^{fs}})^{-g}$, the same as for $\zeta_K(s)$, which completes the proof of the theorem. □

Corollary 2.10. $L(1, \chi) \neq 0$.

Proof. Let K be the associated field to χ and let k be the order of χ. Then, by Theorem 2.9, we have that

$$\zeta_K(s) = \prod_{i=0}^{k-1} L(s, \chi^i) = \zeta(s) \prod_{i=1}^{k-1} L(s, \chi^i)$$

Since $\zeta(s)$ has only a simple pole at $s = 1$, none of the factors $L(s, \chi^i)$ can vanish at $s = 1$, which yields the desired result. □

2.3 Application to Dirichlet's Theorem on arithmetic progressions

As a popular application of this corollary, we give a proof of Dirichlet's theorem on arithmetic progressions.

Theorem 2.11. *Let a, n be relatively prime positive integers. Then there are infinitely many primes $p \equiv a (mod\, n)$.*

Proof. Let P_a be the set of primes $p \equiv a(mod\, n)$, hence we need to show that P_a is infinite. Consider the function

$$P_a(s) = \sum_{p \in P_a} \frac{1}{p^s}$$

defined for complex s with $Re(s) > 1$. It suffices then to show that for real s we have that $\lim_{s \to 1^+} P_a(s) = +\infty$.

Define the function

$$1_a : \mathbb{Z} \longrightarrow \{0, 1\}$$

the characteristic function of the congruence class $a(mod\, n)$ given by

$$1_a(k) = \begin{cases} 1 & \text{if } k \equiv a(mod\, n) \\ 0 & \text{otherwise} \end{cases}$$

Then for all $k \in \mathbb{Z}$, we have

$$1_a(k) = \sum_{\chi \in X(n)} \frac{\chi(a)^{-1}}{\varphi(n)} \chi(k)$$

where $X(n)$ denotes the group of Dirichlet characters mod n.

Indeed, since χ is completely multiplicative, we have that

$$\sum_{\chi \in X(n)} \frac{\chi(a)^{-1}}{\varphi(n)} \chi(k) = \frac{1}{\varphi(n)} \sum_{\chi \in X(n)} \chi(a^{-1}k)$$

But by the orthogonality property of characters, we have that

$$\sum_{\chi \in X(n)} \chi(a^{-1}k) = \begin{cases} \varphi(n) & \text{if } a^{-1}k \equiv 1(mod\, n) \\ 0 & \text{otherwise} \end{cases}$$

which gives us the formula for 1_a.

Then the corresponding identity for $P_a(s)$ is

$$P_a(s) = \sum_{\chi \in X(n)} \frac{\chi(a)^{-1}}{\varphi(n)} \sum_p \frac{\chi(p)}{p^s} \tag{2.2}$$

Now let

$$L(s, \chi) = \prod_p (1 - \frac{\chi(p)}{p^s})^{-1}$$

Taking the logarithm, we obtain

$$\log L(s, \chi) = -\sum_p \log (1 - \frac{\chi(p)}{p^s})$$

By Taylor expansion, we have

$$\log L(s, \chi) = \sum_p \sum_n \frac{1}{n} (\frac{\chi(p)}{p^s})^n$$

Define

$$l(s,\chi) = \sum_p \sum_n \frac{1}{n}(\frac{\chi(p)}{p^s})^n$$

Observe that the $n = 1$ contribution to $l(s,\chi)$ gives us the sum appearing in (2.2). We show that we can disregard all the other terms of $l(s,\chi)$ coming from $n \geq 2$. For this, separate $l(s,\chi)$ as follows:

Let

$$l_1(s,\chi) = \sum_p \frac{\chi(p)}{p^s}$$

and

$$l_{\geq 2}(s,\chi) = \sum_{n\geq 2} \sum_p \frac{1}{n}(\frac{\chi(p)}{p^s})^n$$

Then

$$l(s,\chi) = l_1(s,\chi) + l_{\geq 2}(s,\chi)$$

and

$$P_a(s) = \sum_{\chi \in X(n)} \frac{\chi(a)^{-1}}{\varphi(n)} l_1(s,\chi)$$

We have then that

$$|l_{\geq 2}(s,\chi)| \leq \sum_{n\leq 2} \sum_p \frac{1}{np^n} \leq \sum_p \sum_{n\geq 2} (\frac{1}{p})^n = \sum_p \frac{1}{p^2} \lim_{n\to\infty} \frac{(\frac{1}{p})^n - 1}{\frac{1}{p} - 1}$$

So

$$|l_{\geq 2}(s,\chi)| \leq \sum_p \frac{1}{p^2}\frac{p}{p-1} \leq \sum_p \frac{1}{p^2} \cdot 2 \leq 2\sum_{n\geq 1} \frac{1}{n^2} = \frac{\pi^2}{3} < \infty$$

Hence $l_{\geq 2}(s,\chi)$ is absolutely convergent at $s = 1$ so it is bounded as $s \longrightarrow 1^+$. Consequently, we can disregard the $l_{\geq 2}(s,\chi)$ part of $l(s,\chi)$ and write

$$P_a(s) = \sum_{\chi \in X(n)} \frac{\chi(a)^{-1}}{\varphi(n)} l(s,\chi) + \mathcal{O}(1)$$

Let χ_0 be the principal character mod n. Then we can rewrite

$$P_a(s) = \frac{1}{\varphi(n)} \sum_{p\nmid n} \frac{1}{p^s} + \sum_{\chi \neq \chi_0} l(s,\chi) + \mathcal{O}(1) \tag{2.3}$$

Since $\sum_{p\nmid n} \frac{1}{p^s}$ is up to a finite number of terms, just the sum $\sum_p \frac{1}{p^s}$ and since $\sum_p \frac{1}{p} = +\infty$, we deduce that the first term of the right hand side of (2.3) is unbounded for $s \longrightarrow 1^+$. Thus it would suffice to prove that $l(s,\chi)$ is bounded as $s \longrightarrow 1^+$ for any nonprincipal character χ.

For $s \in \mathbb{R}$, with $|s| < 1$, we have the Taylor expansion

$$-log(1-s) = \sum_{n=1}^{\infty} \frac{s^n}{n}$$

Hence

$$e^{-\sum_{n=1}^{\infty} \frac{s^n}{n}} = 1 - s \quad \forall\, s \in \mathbb{R}, |s| < 1$$

But then, by analytic continuation, the corresponding complex power series gives a well defined logarithm for $s \in \mathbb{C}$ with $|s| < 1$.

Moreover, we have that

$$\lim_{Re(s)\to+\infty} L(s,\chi) = 1$$

which implies that there exists $r > 0$ such that for $Re(s) > r$, we have that $|1-L(s,\chi)| < 1$, thus

$$e^{l(s,\chi)} = L(s,\chi) \quad \text{for } Re(s) > r \tag{2.4}$$

Similarly, by analytic continuation, (2.4) holds true whenever both sides are well-defined analytic functions which is the case for all $s \in \mathbb{C}$ with $Re(s) > 1$.

It is well known that for any nonprincipal character χ, the Dirichlet series for $L(s,\chi)$ is convergent on $Re(s) > 0$. Now, since by Corollary 2.10, $L(1,\chi) \neq 0$, from the above, we obtain

$$L(1,\chi) = \lim_{s\to 1} L(s,\chi) = \lim_{s\to 1} e^{l(s,\chi)}$$

Since $L(s,\chi)$ is analytic and $L(1,\chi) \neq 0$, there exists a small open disk around $L(1,\chi)$ not containing the origin, whence we can choose a branch of the logarithm such that $\log L(s,\chi)$ is well-defined on the preimage of that disk so in particular on a small open disk D around $s = 1$. Consequently, $\log L(1,\chi)$ is a well-defined complex number and since any two logarithms of the same analytic function coincide modulo a constant $C = 2n\pi i$, a multiple of $2\pi i$, we have that

$$l(s,\chi) = \log L(s,\chi) + 2n\pi \quad \text{on } D$$

Therefore, $l(s,\chi)$ is bounded as $s \to 1^+$ for any nonprincipal character $\chi \neq \chi_0$.

We conclude that $P_a(s)$ is unbounded as $s \to 1^+$, hence for real values $s > 1$, we have

$$\lim_{s\to 1^+} P_a(s) = \sum_{p\in P_a} \frac{1}{p} = \infty$$

So P_a is infinite, hence there are infinitely many primes $p \equiv a(mod\, n)$. $\square$

2.4 Conductor-Discriminant Formula

For a Dirichlet character χ of conductor f, consider the Gauss sum

$$\tau(\chi) = \sum_{k=1}^{f} \chi(k) e^{\frac{2\pi i k}{f}} \tag{2.5}$$

and let δ_χ be defined as 0 if $\chi(-1) = 1$ and 1 if $\chi(-1) = -1$. Then the functional equation for the L-series $L(s,\chi)$ is

$$(\frac{f}{\pi})^{\frac{s}{2}} \Gamma(\frac{s+\delta}{2}) L(s,\chi) = W_\chi (\frac{f}{\pi})^{\frac{1-s}{2}} \Gamma(\frac{1-s+\delta}{2}) L(1-s,\overline{\chi}) \tag{2.6}$$

where $W_\chi = \frac{\tau(\chi)}{\sqrt{f} i^{\delta_\chi}}$.

We now show that $|W_\chi| = 1$, which will be used to prove the Conductor-Discriminant formula. The result on W_χ follows from the next two lemmas.

Lemma 2.12. *Let χ be a Dirichlet character of conductor f and consider the Gauss sum $\tau(\chi)$ as in (2.5). Then for any $a \in \mathbb{Z}$*

$$\sum_{k=1}^{f} \overline{\chi}(k) e^{\frac{2\pi i a k}{f}} = \chi(k)\tau(\overline{\chi})$$

Proof. If $gcd(a,f) = 1$, since everything depends only on residue classes mod f, by making a change of variables $c \equiv ab(\text{mod } f)$, the result follows.

Let now $gcd(a,f) = d > 1$. Then both sides vanish. Indeed, this is clear for the right hand side. For the left, notice that if $\chi(y) = 1\, \forall q \equiv 1(\text{mod } \frac{f}{d})$ with $gcd(y,f) = 1$, then χ would be defined mod $\frac{f}{d}$, thus contradicting the definition of the conductor f. Therefore

$\exists y \equiv 1(\text{mod } \frac{f}{d})$ with $gcd(y, f) = 1$ such that $\chi(y) \neq 1$.

Since $dy \equiv d(\text{mod } f)$ and $ay \equiv a(\text{mod } f)$, we have

$$\sum_{k=1}^{f} \overline{\chi}(k) e^{\frac{2\pi i a k}{f}} = \sum_{k=1}^{f} \overline{\chi}(k) e^{\frac{2\pi i a k y}{f}} = \chi(y) \sum_{k=1}^{f} \overline{\chi}(k) e^{\frac{2\pi i a k}{f}}$$

Then since $\chi(y) \neq 1$, we must have that

$$\sum_{k=1}^{f} \overline{\chi}(k) e^{\frac{2\pi i a k}{f}} = 0$$

□

Lemma 2.13. *Let χ be a Dirichlet character of conductor f and let τ be a Gauss sum as in (2.5). Then $|\tau(\chi)| = \sqrt{f}$.*

Proof. Using Lemma 2.12, we have that

$$\begin{aligned}\varphi(f)|\tau(\chi)|^2 &= \sum_{a=1}^{f} |\chi(k)\tau(k)|^2 \\ &= \sum_{a=1}^{f} \sum_{b=1}^{f} \chi(k) e^{\frac{2\pi i a b}{f}} \sum_{c=1}^{f} \overline{\chi}(c) e^{\frac{-2\pi i a c}{f}}\end{aligned}$$

Therefore

$$\begin{aligned}\varphi(f)|\tau(\chi)|^2 &= \sum_{b=1}^{f} \sum_{c=1}^{f} \chi(b)\overline{\chi}(c) \sum_{a=1}^{f} e^{\frac{2\pi i a(b-c)}{f}} \\ &= \sum_{b=1}^{f} \chi(b)\overline{\chi}(b) f = f\varphi(f)\end{aligned}$$

since

$$\chi(b)\overline{\chi}(b) = \begin{cases} 1 & \text{if } gcd(a, f) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Hence $|\tau(\chi)|^2 = f$ so $|\tau(\chi)| = \sqrt{f}$ as desired. □

Corollary 2.14. *Let χ be a Dirichlet character of conductor f and τ as in (2.5). Then $|W_\chi| = 1$.*

Theorem 2.15. *(Conductor-Discriminant Formula) Let K be a number field associated to the group X of Dirichlet characters. Then the discriminant of K is given by*

$$|disc(K)| = \prod_{\chi \in X} f_\chi$$

Proof. Let $\zeta_K(s)$ be the Dedekind zeta function of K. Theorem 2.9 gives us the decomposition

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi)$$

Then substituting in the functional equation (2.1) of $\zeta_K(s)$, we have that

$$A^s \Gamma(\frac{s}{2})^{r_1} \Gamma(s)^{r_2} \prod_{\chi \in X} L(s, \chi) = A^{1-s} \Gamma(\frac{1-s}{2})^{r_1} \Gamma(1-s)^{r_2} \prod_{\chi \in X} L(1-s, \chi) \tag{2.7}$$

where r_1 is the number of real embeddings of K and r_2 is the number of pairs of complex embeddings. Since $K/\mathbb{Q}$ is Galois, either $r_1 = 0$ or $r_2 = 0$.

If $r_1 = 0$, then $r_2 = \frac{k}{2}$, where $k = [K : \mathbb{Q}]$. In this case, half the characters are even and half of them are odd. Taking the product over all even characters, the functional equation (2.6) for the L-series gives

$$\Gamma(\frac{s}{2})^{\frac{k}{2}} \prod_{\substack{\chi \in X \\ \chi(-1)=1}} (\frac{f_\chi}{\pi})^{\frac{s}{2}} L(s,\chi) = \Gamma(\frac{1-s}{2})^{\frac{k}{2}} \prod_{\substack{\chi \in X \\ \chi(-1)=1}} (\frac{f_\chi}{\pi})^{\frac{1-s}{2}} W_\chi L(1-s,\overline{\chi})$$

Similarly, for the odd characters, we have

$$\Gamma(\frac{s+1}{2})^{\frac{k}{2}} \prod_{\substack{\chi \in X \\ \chi(-1)=-1}} (\frac{f_\chi}{\pi})^{\frac{s}{2}} L(s,\chi) = \Gamma(\frac{2-s}{2})^{\frac{k}{2}} \prod_{\substack{\chi \in X \\ \chi(-1)=1}} (\frac{f_\chi}{\pi})^{\frac{1-s}{2}} W_\chi L(1-s,\overline{\chi})$$

From the above two equations, thus taking the sum over all $\chi \in X$, we have

$$(\Gamma(\frac{s}{2})\Gamma(\frac{s+1}{2}))^{\frac{k}{2}} \prod_{\chi \in X} (\frac{f_\chi}{\pi})^{\frac{s}{2}} L(s,\chi) = (\Gamma(\frac{1-s}{2})\Gamma(\frac{2-s}{2}))^{\frac{k}{2}} \prod_{\chi \in X} (\frac{f_\chi}{\pi})^{\frac{1-s}{2}} W_\chi L(1-s,\overline{\chi}) \quad (2.8)$$

Using the duplication formula

$$\Gamma(s)\Gamma(s+\frac{1}{2}) = 2^{1-s}\sqrt{\pi}\Gamma(2s)$$

(2.8) becomes

$$(2^{1-s}\sqrt{\pi}\Gamma(s))^{\frac{k}{2}} \prod_{\chi \in X} (\frac{f_\chi}{\pi})^{\frac{s}{2}} L(s,\chi) = (2^{s}\sqrt{\pi}\Gamma(1-s))^{\frac{k}{2}} \prod_{\chi \in X} (\frac{f_\chi}{\pi})^{\frac{1-s}{2}} W_\chi L(1-s,\overline{\chi})$$

Since $r_1 = 0$, equation (2.7) reads

$$A^s\Gamma(s)^{\frac{k}{2}} \prod_{\chi \in X} L(s,\chi) = A^{1-s}\Gamma(1-s)^{\frac{k}{2}} \prod_{\chi \in X} L(1-s,\chi)$$

Comparing the last two equations, we must have that

$$\frac{2^{\frac{k(1-s)}{2}}(\prod_{\chi\in X}\frac{f_\chi}{\pi})^{\frac{s}{2}}}{A^s} = \frac{2^{\frac{ks}{2}}(\prod_{\chi\in X}\frac{f_\chi}{\pi})^{\frac{1-s}{2}}\prod_{\chi\in X}W_\chi}{A^{1-s}}$$

Hence

$$2^{\frac{k(1-s)-ks}{2}}(\prod_{\chi \in X}\frac{f_\chi}{\pi})^{\frac{2s-1}{2}} = A^{2s-1}\prod_{\chi \in X} W_\chi$$

So

$$(\frac{1}{2^k}\prod_{\chi \in X}\frac{f_\chi}{\pi})^{\frac{2s-1}{2}} = A^{2s-1}\prod_{\chi \in X} W_\chi$$

Since the left hand side of the above equation is a positive real number, we must have that $\prod_{\chi\in X} W_\chi \in \mathbb{R}_+$, but Corollary 2.14 tells us that $|W_\chi| = 1\,\forall\chi \in X$ so we must have that $\prod_{\chi\in X} W_\chi = 1$. Thus

$$\frac{1}{2^k}\prod_{\chi \in X}\frac{f_\chi}{\pi} = A^2$$

and since

$$A = 2^{-\frac{k}{2}}\pi^{-\frac{k}{2}}\sqrt{|disc(K)|}$$

we obtain

$$\prod_{\chi\in X}\frac{f_\chi}{\pi}=\pi^{-k}|disc(K)|$$

Hence $|disc(K)|=\prod_{\chi\in X}\frac{f_\chi}{\pi}$ as desired.

Consider now the second case when $r_2=0$. Then K is a totally real number field of degree k and all the characters are even. So taking the product over all characters $\chi\in X$, the functional equations for the L-series read

$$\Gamma(\frac{s}{2})^k\prod_{\chi\in X}(\frac{f_\chi}{\pi})^{\frac{s}{2}}L(s,\chi)=\Gamma(\frac{1-s}{2})^k\prod_{\chi\in X}(\frac{f_\chi}{\pi})^{\frac{1-s}{2}}W_\chi L(1-s,\overline{\chi})$$

Moreover, (2.7) becomes

$$A^s\Gamma(\frac{s}{2})^k\prod_{\chi\in X}L(s,\chi)=A^{1-s}\Gamma(\frac{1-s}{2})^k\prod_{\chi\in X}L(1-s,\chi)$$

Comparing the last two equations, we get that

$$\frac{(\prod_{\chi\in X}\frac{f_\chi}{\pi})^{\frac{s}{2}}}{A^s}=\frac{(\prod_{\chi\in X}\frac{f_\chi}{\pi})^{\frac{1-s}{2}}\prod_{\chi\in X}W_\chi}{A^{1-s}}$$

Thus

$$(\prod_{\chi\in X}\frac{f_\chi}{\pi})^{\frac{2s-1}{2}}=A^{2s-1}\prod_{\chi\in x}W_\chi$$

As in the previous case, we have that $\prod_{\chi\in X}W_\chi=1$ and therefore

$$A^2=\prod_{\chi\in X}\frac{f_\chi}{\pi}$$

Since $r_2=0$, we have that

$$A=\pi^{-\frac{k}{2}}\sqrt{|disc(K)|}$$

whence substituting A in the last equation completes the proof. $\square$

3 Smallest completely splitting prime in an abelian number field

3.1 First estimate for Theorem 3.1

In this section, we prove our main result:

Proposition 3.1. *Let K be an abelian number field of degree k. Then, for any $\varepsilon > 0$, the smallest prime p that splits completely in K satisfies*

$$p \ll_{\varepsilon,k} D^{\frac{1}{4}+\varepsilon}$$

where $D = |disc(K)|$, the absolute value of the discriminant.

Let $K/\mathbb{Q}$ be a nontrivial abelian extension of degree k and let $X = \{\chi_1, ..., \chi_k\}$ be the associated group of Dirichlet characters, where $\chi_1 \equiv 1$ is the trivial character. For each $\chi_i \in X$, let $q_i = f_{\chi_i}$, the conductor of χ_i. In particular, $q_1 = 1$. Then Theorem 2.9 tells us that the Dedekind zeta function of K decomposes as

$$\zeta_K(s) = \zeta(s) \prod_{i=2}^{k} L(s, \chi_i) \tag{3.1}$$

We can assume that $\varepsilon \in (0, \frac{2}{3})$. Let $D = |disc(K)|$. Then, by the conductor-discriminant formula, we have that

$$D = q_1 q_2 \cdots q_k = q_2 \cdots q_k$$

For each $i \in \overline{2, k}$ let

$$y_i = max\{q_i^{\frac{1}{4}+\frac{\varepsilon}{2}}, D^{\frac{\varepsilon}{2k}}\}$$

and set

$$y = \prod_{i=2}^{k} y_i$$

Then we have that

$$D^{\frac{1}{4}+\frac{\varepsilon}{2}} = (q_2 \cdots q_k)^{\frac{1}{4}+\frac{\varepsilon}{2}} \le \prod_{i=2}^{k} y_i = y$$

On the other hand, if $i_1, ..., i_r$ are the indexes for which $y_i = q_i^{\frac{1}{4}+\frac{\varepsilon}{2}}$ where $r \in \overline{0, k-1}$ then

$$\begin{aligned} y &= y_{i_1} \cdots y_{i_r} D^{\frac{\varepsilon}{2k}(k-1-r)} \\ &= q_{i_1} \cdots q_{i_r} D^{\frac{\varepsilon}{2k}(k-1-r)} \end{aligned} \tag{3.2}$$

But then $y < D^{\frac{1}{4}+\varepsilon}$. Indeed, from (3.2), this is equivalent to proving

$$\begin{aligned} (q_{i_1} \cdots q_{i_r})^{\frac{1}{4}+\frac{\varepsilon}{2}} < D^{\frac{1}{4}+\varepsilon-\frac{\varepsilon}{2k}(k-1-r)} &= D^{\frac{1}{4}+\varepsilon-\frac{\varepsilon}{2}+\varepsilon\frac{r+1}{2k}} \\ &= D^{\frac{1}{4}+\varepsilon+\varepsilon\frac{r+1}{2k}} \end{aligned}$$

And this is clear since

$$D = q_2 \cdots q_k \ge q_{i_1} \cdots q_{i_r}$$

and $\varepsilon \frac{r+1}{2k} > 0$.

By definition, we can write

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where $a_n = \{I \subseteq \mathcal{O}_K \text{ ideal } | N_{K/\mathbb{Q}}(I) = n\}$.

The main idea in proving Theorem 3.1 is to estimate the sum $\sum_{n \le y} a_n$ in two different ways.

Proposition 3.2. *Assume that every prime that splits completely in K exceeds $D^{\frac{1}{4}+\varepsilon}$. Then we have*

$$\sum_{n\le y} a_n \ll_k y^{\frac{3}{4}}$$

Proof. Recall the Euler product of the Dedekind zeta function

$$\zeta_K(s) = \prod_p (1 - \frac{1}{p^{f_p s}})^{-g_p}$$

where f_p is the inertia degree of any prime ideal $\wp$ of $\mathcal{O}_K$ lying above p and g_p is the number of such prime ideals. Therefore

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p (1 - \frac{1}{p^{f_p s}})^{-g_p}$$

Let $p \le y$ be a prime that doesn't split completely in K, hence $p|D$ or $f_p > 1$. From the above equality, it follows that if $n \le y$ and a_n doesn't vanish, we can decompose n as $n = n_1 n_2$, where n_1 is a squarefree divisor of D and n_2 is squarefull. But a result of Golomb on powerfull numbers (see [3]) tells us that

$$|\{n_2 \in \mathbb{N}|_2 \le y \text{ and } n_2 \text{ is squarefull }\}| \ll y^{\frac{1}{2}}$$

Moreover, since $\tau(D) \ll_\varepsilon D^\varepsilon$, we have in particular that $\tau(D) \ll D^{\frac{1}{32}}$. Then

$$A_y = |\{n \in \mathbb{N}|n \le y \text{ such that } a_n \ne 0\}| \ll y^{\frac{1}{2}} D^{\frac{1}{32}}$$

We saw that $D^{\frac{1}{4}+\frac{\varepsilon}{2}} \le y$, thus $D^{\frac{1}{4}} < y$ and therefore

$$A_y \ll y^{\frac{1}{2}} y^{\frac{1}{8}} = y^{\frac{5}{8}}$$

On the other hand, the decomposition (3.1) of $\zeta_K(s)$ gives us

$$a_n = (1 \star \chi_2 \star ... \star \chi_k)(n) \quad \forall n \in \mathbb{N}, n \ge 1$$

where $\star$ denotes the Dirichlet convolution. Hence

$$a_n \le (1 \star 1 \star ... \star 1)(n) = \tau_k(n)$$

where τ_k, the convolution of the function **1** with itself for k-times is known in the literature as the k-fold Piltz divisor function.

Therefore, since

$$\tau_k(n) \le \tau(n)^{k-1} \ll_k n^{\frac{1}{8}}$$

we conclude that

$$\sum_{n\le y} a_n \ll_k y^{\frac{5}{8}} y^{\frac{1}{8}} = y^{\frac{3}{4}}$$

□

3.2 Second estimate for Theorem 3.1

Now we give a second estimate for $\sum_{n\leq y} a_n$ in the following two lemmas. First, remark that since $a_n = (1 \star \chi_2 \star ... \star \chi_k)(n) \quad \forall n \in \mathbb{N}, n \geq 1$, we can write

$$\begin{aligned}
\sum_{n\leq y} a_n &= \sum_{d_2\cdots d_k \leq y} \chi_2(d_2)\cdots\chi_k(d_k) \left\lfloor \frac{y}{d_2\cdots d_k} \right\rfloor \\
&= \sum_{d_2\cdots d_k \leq y} \chi_2(d_2)\cdots\chi_k(d_k) \Big(\frac{y}{d_2\cdots d_k} - \Big\{ \frac{y}{d_2\cdots d_k} \Big\}\Big) \\
&= y \sum_{d_2\cdots d_k \leq y} \frac{\chi_2(d_2)}{d_2}\cdots\frac{\chi_k(d_k)}{d_k} \;-\; \sum_{d_2\cdots d_k \leq y} \chi_2(d_2)\cdots\chi_k(d_k) \Big\{ \frac{y}{d_2\cdots d_k} \Big\}
\end{aligned}$$

Lemma 3.3. *The following holds*

$$\sum_{d_2\cdots d_k \leq y} \frac{\chi_2(d_2)}{d_2}\cdots\frac{\chi_k(d_k)}{d_k} = L(1,\chi_2)\cdots L(1,\chi_k) + \mathcal{O}_{\varepsilon,k}(D^{-\frac{\varepsilon^2}{20k}})$$

Proof. For each $(k-1)$-tuple $(d_2, ..., d_k)$ with $d_2\cdots d_k \leq y$, let

$$\mathcal{U}_{(d_2,...,d_k)} = \{1 \leq i \leq k-1 | y_i < d_i\}$$

and for each $\mathcal{U} \subseteq \overline{2,k}$, let

$$\mathcal{F}(\mathcal{U}) = \{(d_2, .., d_k) | \mathcal{U}_{(d_2,..,d_k)} = \mathcal{U}\}$$

Then we have that

$$\begin{aligned}
\sum_{d_2\cdots d_k \leq y} \frac{\chi_2(d_2)}{d_2}\cdots\frac{\chi_k(d_k)}{d_k} &= \sum_{\mathcal{U}\subseteq\overline{2,k}} \; \sum_{(d_2,...,d_k)\in\mathcal{F}(\mathcal{U})} \frac{\chi_2(d_2)}{d_2}\cdots\frac{\chi_k(d_k)}{d_k} \\
&= \sum_{(d_2,...,d_k)\in\mathcal{F}(\varnothing)} \frac{\chi_2(d_2)}{d_2}\cdots\frac{\chi_k(d_k)}{d_k} + \sum_{\varnothing\neq\mathcal{U}\subseteq\overline{2,k}} \; \sum_{(d_2,...,d_k)\in\mathcal{F}(\mathcal{U})} \frac{\chi_2(d_2)}{d_2}\cdots\frac{\chi_k(d_k)}{d_k}
\end{aligned}$$

By the definition of $\mathcal{F}(\mathcal{U})$, we have that

$$\begin{aligned}
\mathcal{F}(\varnothing) &= \{(d_2, ..., d_k) | \varnothing_{(d_2,...,d_k)} = \varnothing\} \\
&= \{(d_2, .., d_k) | \{2 \leq i \leq k | y_i < d_i\} = \varnothing\} \\
&= \{(d_2, ..., d_k) | d_i \leq y_i \, \forall i \in \overline{2,k}\}
\end{aligned}$$

Hence

$$\begin{aligned}
\sum_{(d_2,...,d_k)\in\mathcal{F}(\varnothing)} \frac{\chi_2(d_2)}{d_2}\cdots\frac{\chi_k(d_k)}{d_k} &= \sum_{\substack{d_i\leq y_i \\ \forall i\in\overline{2,k}}} \frac{\chi_2(d_2)}{d_2}\cdots\frac{\chi_k(d_k)}{d_k} \\
&= \prod_{i=2}^{k} \sum_{d_i\leq y_i} \frac{\chi_i(d_i)}{d_i}
\end{aligned}$$

Let $S_i(t) = \sum_{n\leq t} \chi_i(n) \, \forall i \in \overline{2,k}$. Then, by Corollary 1.8, we have that

$$S_i(N) \ll_{\varepsilon,k} N^{1-\frac{\varepsilon^2}{4}} \, \forall N \geq q_i^{\frac{1}{4}+\frac{\varepsilon}{2}}$$

and since $y_i = max\{q_i^{\frac{1}{4}+\frac{\varepsilon}{2}}, D^{\frac{\varepsilon}{2k}}\}$, it follows that

$$S_i(t) \ll_{\varepsilon,k} t^{1-\frac{\varepsilon^2}{4}} \quad \forall t \geq y_i$$

By using Abel summation we obtain

$$\sum_{y_i < n \leq N} \frac{\chi_i(n)}{n} = \frac{S_i(N)}{N} - \frac{S_i(y_i)}{y_i} - \int_{y_i}^{N} S_i(t)\Big(\frac{1}{t}\Big)' dt$$
$$= \frac{S_i(N)}{N} - \frac{S_i(y_i)}{y_i} + \int_{y_i}^{N} \frac{S_i(t)}{t^2} dt$$

Hence

$$\sum_{n > y_i} \frac{\chi_i(n)}{n} = -\frac{S_i(y_i)}{y_i} + \int_{y_i}^{\infty} \frac{S_i(t)}{t^2} dt$$

since $S_i(N) \ll_{\varepsilon,k} N^{1-\frac{\varepsilon^2}{4}}$.

Therefore

$$L(1,\chi_i) - \sum_{d_i \leq y_i} \frac{\chi_i(d_i)}{d_i} = -\frac{S_i(y_i)}{y_i} + \int_{y_i}^{\infty} \frac{S_i(t)}{t^2} dt$$

Again, using (1.15), we can dispose of the first term in the right hand side. As for the second term, since

$$\int_{y_i}^{\infty} \frac{t^{1-\frac{\varepsilon^2}{4}}}{t^2} dt = -\frac{4}{\varepsilon^2} y_i^{-\frac{\varepsilon^2}{4}}$$

we deduce that

$$-\frac{S_i(y_i)}{y_i} + \int_{y_i}^{\infty} \frac{S_i(t)}{t^2} dt \ll_{\varepsilon,k} y_i^{-\frac{\varepsilon^2}{4}}$$

Hence

$$L(1,\chi_i) - \sum_{d_i \leq y_i} \frac{\chi_i(d_i)}{d_i} \ll_{\varepsilon,k} y_i^{-\frac{\varepsilon^2}{4}}$$

and since by definition, $y_i \geq D^{\frac{\varepsilon}{2k}}$, we get

$$L(1,\chi_i) - \sum_{d_i \leq y_i} \frac{\chi_i(d_i)}{d_i} \ll_{\varepsilon,k} D^{-\frac{\varepsilon^3}{8k}}$$

which means that $\exists M(\varepsilon,k) > 0$ such that

$$\left| L(1,\chi_i) - \sum_{d_i \leq y_i} \frac{\chi_i(d_i)}{d_i} \right| \leq M(\varepsilon,k) D^{-\frac{\varepsilon^3}{8k}}$$

for large enough D. Thus

$$\left| \sum_{d_i \leq y_i} \frac{\chi_i(d_i)}{d_i} \right| - \left| L(1,\chi_i) \right| \leq M(\varepsilon,k) D^{-\frac{\varepsilon^3}{8k}}$$

Consequently

$$\left| \sum_{d_i \leq y_i} \frac{\chi_i(d_i)}{d_i} \right| \leq \left| L(1,\chi_i) \right| + M(\varepsilon,k) D^{-\frac{\varepsilon^3}{8k}} = \left| L(1,\chi_i) \right| \left(1 + \frac{1}{\left| L(1,\chi_i) \right|} M(\varepsilon,k) D^{-\frac{\varepsilon^3}{8k}} \right) \quad (3.3)$$

But Siegel's theorem with $\varepsilon = \frac{\varepsilon^3}{16k}$ reads

$$q_i^{-\frac{\varepsilon^3}{16k}} \ll_{\varepsilon,k} \left| L(1,\chi_i) \right|$$

So $\exists N(\varepsilon,k)>0$ such that for big enough q_i we have

$$q_i^{-\frac{\varepsilon^3}{16k}} \le N(\varepsilon,k)\big|L(1,\chi_i)\big|$$

Then from this and (3.3) we have

$$\Bigg|\sum_{d_i\le y_i}\frac{\chi_i(d_i)}{d_i}\Bigg| \le \big|L(1,\chi_i)\big|\Bigg(1+\frac{M(\varepsilon,k)}{N(\varepsilon,k)}q_i^{\frac{\varepsilon^3}{16k}}D^{-\frac{\varepsilon^3}{8k}}\Bigg)$$

Whence

$$\begin{aligned}\sum_{d_i\le y_i}\frac{\chi_i(d_i)}{d_i} &= L(1,\chi_i)\big(1+\mathcal{O}_{\varepsilon,k}\big(q_i^{\frac{\varepsilon^3}{16k}}D^{-\frac{\varepsilon^3}{8k}}\big)\big)\\ &= L(1,\chi_i)\big(1+\mathcal{O}_{\varepsilon,k}\big(D^{-\frac{\varepsilon^3}{16k}}\big)\big)\end{aligned}$$

where the last equality holds since $q_i \le D = q_2\cdots q_k$.

Then, taking the product over all the characters, we have that

$$\prod_{i=2}^{k}\sum_{d_i\le y_i}\frac{\chi_i(d_i)}{d_i} = L(1,\chi_2)\cdots L(1,\chi_k)\big(1+\mathcal{O}_{\varepsilon,k}\big(D^{-\frac{\varepsilon^3}{16k}}\big)\big)$$

Using the trivial bound $L(1,\chi_i)\ll \log q_i\,\forall i\in\overline{2,k}$ and the fact that $q_i\le D\ \ \forall i\in\overline{2,k}$, we get

$$L(1,\chi_2)\cdots L(1,\chi_k) = \mathcal{O}(\log D^{k-1})$$

Hence

$$\begin{aligned}\prod_{i=2}^{k}\sum_{d_i\le y_i}\frac{\chi_i(d_i)}{d_i} &= L(1,\chi_2)\cdots L(1,\chi_k) + \mathcal{O}((\log D)^{k-1})\mathcal{O}_{\varepsilon,k}\big(D^{-\frac{\varepsilon^3}{16k}}\big)\\ &= L(1,\chi_2)\cdots L(1,\chi_k) + \mathcal{O}_{\varepsilon,k}\big((\log D)^{k-1}D^{-\frac{\varepsilon^3}{16k}}\big)\\ &= L(1,\chi_2)\cdots L(1,\chi_k) + \mathcal{O}_{\varepsilon,k}\big(D^{-\frac{\varepsilon^3}{20k}}\big) \qquad (3.4)\end{aligned}$$

since $(\log D)^{k-1}$ is a polylogarithmic function in D and $f(x)=o(x^{\varepsilon})\,\forall\varepsilon>0$ and $\forall f$ a polylogarithmic function, i.e $f(n)\in\mathbb{Z}[\log n]$.

Let us estimate now the contribution coming from nonempty $\mathcal{U}$. Fix such an $\mathcal{U}\subseteq\overline{2,k}$, let $u_0\in\mathcal{U}$ and set

$$P = P((d_2,...,\widehat{d_{u_0}},...d_k)) = \prod_{\substack{i=2\\ i\ne u_0}}^{k} d_i$$

so when we write P, we assume it depends on the $(k-2)$-tuple $(d_2,...,\widehat{d_{u_0}},...d_k)$, where $\widehat{x}$ means that we omit x. Then the triangle inequality gives

$$\begin{aligned}\Bigg|\sum_{(d_2,...,d_k)\in\mathcal{F}(\mathcal{U})}\frac{\chi_2(d_2)}{d_2}\cdots\frac{\chi_k(d_k)}{d_k}\Bigg| &\le \Bigg|\sum_{(d_2,...,d_k)\in\mathcal{F}(\mathcal{U})}\frac{\chi_{u_0}(d_{u_0})}{d_2\cdots d_k}\Bigg| = \Bigg|\sum_{(d_2,...,d_k)\in\mathcal{F}(\mathcal{U})}\frac{1}{P}\frac{\chi_{u_0}(d_{u_0})}{d_{u_0}}\Bigg|\\ &\le \sum_{\substack{(d_2,..,\widehat{d_{u_0}},..,d_k)\\ (d_2,...,d_k)\in\mathcal{F}(\mathcal{U})}}\frac{1}{P}\Bigg|\sum_{y_{u_0}<d_{u_0}\le\frac{y}{P}}\frac{\chi_{u_0}(d_{u_0})}{d_{u_0}}\Bigg|\end{aligned}$$

Then, using Abel's summation formula we have

$$\sum_{y_{u_0}<d_{u_0}\le\frac{y}{P}}\frac{\chi_{u_0}(d_{u_0})}{d_{u_0}} = \frac{S_{u_0}(\frac{y}{P})}{\frac{y}{P}} - \frac{S_{u_0}(y_{u_0})}{y_{u_0}} + \int_{y_{u_0}}^{\frac{y}{P}}\frac{S_{u_0}(t)}{t^2}dt$$

Since $\frac{u}{P} > y_{u_0}$, (1.15) gives us

$$S_{u_0}(\frac{y}{P}) \ll_{\varepsilon,k} \left(\frac{y}{P}\right)^{1-\frac{\varepsilon^2}{4}}$$

Furthermore

$$\int_{y_{u_0}}^{\frac{y}{P}} \frac{S_{u_0}(t)}{t^2} dt \ll_{\varepsilon,k} \int_{y_{u_0}}^{\frac{y}{P}} \frac{t^{1-\frac{\varepsilon^2}{4}}}{t^2} dt = -\frac{4}{\varepsilon^2} t^{-\frac{\varepsilon^2}{4}} \Big|_{y_{u_0}}^{\frac{y}{P}} \ll_{\varepsilon,k} y_{u_0}^{-\frac{\varepsilon^2}{4}}$$

Consequently

$$\sum_{y_{u_0} < d_{u_0} \leq \frac{y}{P}} \frac{\chi_{u_0}(d_{u_0})}{d_{u_0}} \ll_{\varepsilon,k} \left(\frac{y}{P}\right)^{1-\frac{\varepsilon^2}{4}} + y_{u_0}^{-\frac{\varepsilon^2}{4}} \ll y_{u_0}^{-\frac{\varepsilon^2}{4}}$$

Thus

$$\begin{aligned}
\sum_{\substack{(d_2,..,\widehat{d_{u_0}},..,d_k) \\ (d_2,...,d_k)\in\mathcal{F}(\mathcal{U})}} \frac{1}{P} \Bigg| \sum_{y_{u_0} < d_{u_0} \leq \frac{y}{P}} \frac{\chi_{u_0}(d_{u_0})}{d_{u_0}} \Bigg| &\ll_{\varepsilon,k} y_{u_0}^{-\frac{\varepsilon^2}{4}} \sum_{\substack{(d_2,..,\widehat{d_{u_0}},..,d_k) \\ (d_2,...,d_k)\in\mathcal{F}(\mathcal{U})}} \frac{1}{P} \\
&\leq D^{-\frac{\varepsilon^3}{8k}} \Big(\sum_{d\leq y} \frac{1}{d}\Big)^{k-2} \\
&\leq D^{-\frac{\varepsilon^3}{8k}} (1+\log y)^{k-2} \\
&\leq D^{-\frac{\varepsilon^3}{8k}} (\log eD)^{k-2}
\end{aligned}$$

Since $(\log eD)^{k-2}$ is polylogarithmic, we have that $(\log eD)^{k-2} \in o((eD)^{\delta})\,\forall\delta > 0$, so in particular $(\log eD)^{k-2} \in o((eD)^{\frac{\varepsilon^3}{40k}})$, hence

$$D^{-\frac{\varepsilon^3}{8k}} (\log eD)^{k-2} = \mathcal{O}_{\varepsilon,k}\big(D^{-\frac{\varepsilon^3}{10k}}\big)$$

Combining this and (3.4) gives us the desired bound. □

Lemma 3.4. *We have*

$$\sum_{d_2\cdots d_k\leq y} \chi_2(d_2)\cdots\chi_k(d_k)\left\{\frac{y}{d_2\cdots d_k}\right\} \ll_{\varepsilon,k} D^{-\frac{\varepsilon^3}{600k}}$$

Proof. Let $y' = yD^{-\frac{\varepsilon}{4}}$. We first show that we can dispose of the $(k-1)$-tuples $(d_2,...,d_k)$ such that $d_2\cdots d_k \leq y'$.

Indeed, we have that

$$\begin{aligned}
\Bigg| \sum_{d_2\cdots d_k\leq y'} \chi_2(d_2)\cdots\chi_k(d_k)\left\{\frac{y}{d_2\cdots d_k}\right\}\Bigg| &\leq \sum_{d_2\cdots d_k\leq y'} 1 \\
&\leq y'\Big(\sum_{d\leq y'}\frac{1}{d}\Big)^{k-2} \\
&\leq y'(1+\log y')^{k-2} \\
&\leq yD^{-\frac{\varepsilon}{4}}(1+\log D)^{k-2}
\end{aligned}$$

where the last inequality holds since $y' < y < D$.

As seen in the proof of the previous lemma, we have that $(1+\log D)^{k-2} \in o(D^{\delta})\ \ \forall\delta > 0$, so in particular, for $\delta = \frac{\varepsilon}{20}$ we obtain that

$$yD^{-\frac{\varepsilon}{4}}(1+\log D)^{k-2} \ll_{\varepsilon,k} yD^{-\frac{\varepsilon}{4}+\frac{\varepsilon}{20}} = yD^{-\frac{\varepsilon}{5}}$$

Clearly this is negligible compared to our desired bound so we focus on the contribution of $(k-1)$-tuples $(d_2, ..., d_k)$ with $y' < d_2 \cdots d_k \leq y$. Let

$$y'_i = max\{q_i^{\frac{1}{4}+\frac{\varepsilon}{8}}, D^{\frac{\varepsilon}{8k}}\}$$

Then if $d_2 \cdots d_k > y'$, we claim that there exists $i_0 \in \overline{2,k}$ such that $d_{i_0} > y'_{i_0}$.

Suppose this doesn't occur, hence $d_i \leq y'_i \, \forall i \in \overline{2,k}$. Then

$$y' < d_2 \cdots d_k \leq y'_2 \cdots y'_k$$

Hence

$$yD^{-\frac{\varepsilon}{4}} < y'_2 \cdots y'_k$$

We saw that $D^{\frac{1}{4}+\frac{\varepsilon}{2}} \leq y$ and therefore

$$D^{\frac{1}{4}+\frac{\varepsilon}{4}} \leq y'_2 \cdots y'_k$$

Let $r \in \overline{0,k-1}$ and $i_1, ..., i_r \in \overline{2,k}$ such that $y'_i = q_i^{\frac{1}{4}+\frac{\varepsilon}{8}}$. Then

$$y'_2 \cdots y'_k = (q_{i_1} \cdots q_{i_r})^{\frac{1}{4}+\frac{\varepsilon}{8}} D^{\frac{\varepsilon}{8k}(k-1-r)}$$

and since $q_{i_1} \cdots q_{i_r} \leq q_2 \cdots q_k = D$, we get that

$$D^{\frac{1}{4}+\frac{\varepsilon}{4}} \leq D^{\frac{1}{4}+\frac{\varepsilon}{8}} D^{\frac{\varepsilon}{8k}(k-1-r)}$$

Hence

$$1 \leq D^{-\frac{r+1}{8k}}$$

which is clearly a contradiction since $D > 1$. Therefore there is an $i_0 \in \overline{2,k}$ such that $d_{i_0} > y'_{i_0}$ and taking into account that $\left\lfloor \frac{y}{d_2 \cdots d_k} \right\rfloor < \frac{y}{y'}$ for $d_2 \cdots d_k > y'$, similarly to the proof of Lemma 3.3, we can group the remaining $(k-1)$-tuples $(d_2, ..., d_k)$ with $y' < d_2 \cdots d_k \leq y$ as follows:

For each $(k-1)$-tuple, let

$$\mathcal{U}_{(d_2,...,d_k)} = \{2 \leq i \leq k | y'_i < d_i\}$$

Since we proved that there is an $i_0 \in \overline{2,k}$ with $d_{i_0} > y'_{i_0}$ we have that

$$\mathcal{U}_{(d_2,...,d_k)} \neq \varnothing \;\; \forall (d_2, ..., d_k)$$

Now, for each $\varnothing \neq \mathcal{U} \subseteq \overline{2,k}$ and $m \in \mathbb{N}, 1 \leq m < D^{\frac{\varepsilon}{4}} = \frac{y}{y'}$, define

$$\mathcal{F}(\mathcal{U}, m) = \{(d_2, ..., d_k) | \mathcal{U}_{(d_2,...,d_k)} = \mathcal{U} \text{ and } \left\lfloor \frac{y}{d_2 \cdots d_k} \right\rfloor = m\}$$

Then clearly

$$\sum_{y' < d_2 \cdots d_k \leq y} \chi_2(d_2) \cdots \chi_k(d_k) \left\{ \frac{y}{d_2 \cdots d_k} \right\} = \sum_{\mathcal{U}, m} \sum_{(d_2,...,d_k) \in \mathcal{F}(\mathcal{U},m)} \chi_2(d_2) \cdots \chi_k(d_k) \left\{ \frac{y}{d_2 \cdots d_k} \right\}$$

Fix a pair $(\mathcal{U}, m)$, let $u_0 \in \mathcal{U} \neq \varnothing$ and consider a $(k-2)$-tuple $(d_2, ..., \widehat{d_{u_0}}, .., d_k)$ such that $(d_2, ..., d_k) \in \mathcal{F}(\mathcal{U}, m)$ for some d_{u_0}.

Since $u_0 \in \mathcal{U}$, we have that $y'_{u_0} < d_{u_0}$. Furthermore, since $(d_2, ..., d_k) \in \mathcal{F}(\mathcal{U}, m)$, by the definition of $\mathcal{F}(\mathcal{U}, m)$, we have that $\left\lfloor \frac{y}{P d_{u_0}} \right\rfloor = m$, where we set

$$P = P((d_2, .., \widehat{d_{u_0}}, .., d_k)) = \prod_{\substack{i=2 \\ \imath \neq u_0}}^{k} d_i$$

Hence

$$\frac{y}{Pd_{u_0}} < m+1$$

So

$$d_{u_0} > \frac{y}{(m+1)P}$$

Lastly,

$$d_{u_0} > \frac{y'}{P}$$

since $d_2 \cdots d_k > y'$. Thus if we set

$$M = M((d_2, ..., \widehat{d_{u_0}}, .., d_k)) = max\{y'_{u_0}, \frac{y}{(m+1)P}, \frac{y'}{P}\}$$

we have that

$$M < d_{u_0} \leq \frac{y}{mP}$$

where the inequality on the right holds since $\left\lfloor \frac{y}{d_2 \cdots d_k} \right\rfloor = m$. These are precisely the integers d_{u_0} satisfying the condition imposed on the $(k-2)$-tuplets. Consequently, the triangle inequality gives us

$$\Big| \sum_{\mathcal{U},m} \sum_{(d_2,\ldots,d_k)\in\mathcal{F}(\mathcal{U},m)} \chi_2(d_2)\cdots\chi_k(d_k)\Big\{\frac{y}{d_2\cdots d_k}\Big\}\Big|$$

$$\leq \sum_{\substack{(d_2,..,\widehat{d_{u_0}},..,d_k) \\ (d_2,\ldots,d_k)\in\mathcal{F}(\mathcal{U})}} \Big| \sum_{M<d_{u_0}\leq\frac{y}{mP}} \chi_{i_0}(d_{u_0})\Big\{\frac{y}{d_{u_0}P}\Big\}\Big| \tag{3.5}$$

Since

$$\left\lfloor \frac{y}{Pd_{u_0}} \right\rfloor = m$$

is constant, the function $b : \mathbb{N} \longrightarrow [0,1)$, $b(n) = \left\{\frac{y}{nP}\right\}$ is decreasing on the integers d_{u_0} and it is also nonnegative. Then, using Abel's inequality, we have

$$\Big| \sum_{M<d_{u_0}\leq\frac{y}{mP}} \chi_{i_0}(d_{u_0})\Big\{\frac{y}{d_{u_0}P}\Big\}\Big| \leq \max_{M<t\leq\frac{y}{mP}} \Big| \sum_{M<d_{u_0}\leq t} \chi_{u_0}(d_{u_0})\Big|$$

Since

$$M \geq y'_{i_0} \geq q_i^{\frac{1}{4}+\frac{\varepsilon}{8}}$$

Corollary 1.8 gives us

$$\Big| \sum_{M<d_{u_0}\leq t} \chi_{u_0}(d_{u_0})\Big| \ll_{\varepsilon,k} t^{1-\frac{\varepsilon^2}{64}}$$

Whence

$$\max_{M<t\leq\frac{y}{mP}} \Big| \sum_{M<d_{u_0}\leq t} \chi_{u_0}(d_{u_0})\Big| \ll_{\varepsilon,k} \left(\frac{y}{mP}\right)^{1-\frac{\varepsilon^2}{64}} \leq \left(\frac{y}{mP}\right) M^{\frac{\varepsilon^2}{64}} \leq \frac{y}{mP} D^{-\frac{\varepsilon^3}{512k}} \tag{3.6}$$

since

$$D^{\frac{\varepsilon}{8k}} \leq y'_{u_0} \leq M < d_{u_0} \leq \frac{y}{mP}$$

From (3.5) and (3.6), we deduce that the contribution of the pairs $(\mathcal{U}, m)$ is

$$\begin{aligned}
&\ll_{\varepsilon,k} \frac{y}{m} D^{-\frac{\varepsilon^3}{512k}} \sum_{\substack{(d_2,..,\widehat{d_{u_0}},..,d_k) \\ (d_2,...,d_k)\in\mathcal{F}(\mathcal{U},m)}} \frac{1}{P} \\
&\leq \frac{y}{m} D^{-\frac{\varepsilon^3}{512k}} \left(\sum_{d\leq y} \frac{1}{d} \right)^{k-2} \\
&\leq \frac{y}{m} D^{-\frac{\varepsilon^3}{512k}} (1+\log y)^{k-2}
\end{aligned}$$

Finally, summing over all pairs $(\mathcal{U}, m)$, we conclude that the upper bound is

$$\ll_{\varepsilon,k} yD^{-\frac{\varepsilon^3}{512k}} (1+\log y)^{k-2} \ll_{\varepsilon,k} D^{-\frac{\varepsilon^3}{600k}}$$

since

$$(1+\log y)^{k-2} \in o(D^{\delta}) \quad \forall \delta > 0$$

. $\square$

Proof of Theorem 3.1
Lemmas 3.3 and 3.4 give us the estimate

$$\sum_{n\leq y} a_n = yL(1,\chi_2)\cdots L(1,\chi_k) + \mathcal{O}_{\varepsilon,k}(D^{-\frac{\varepsilon^3}{600k}})$$

Assuming that the least prime that splits completely in K is greater than $D^{\frac{1}{4}+\varepsilon}$, by Proposition 3.2, we have that

$$\sum_{n\leq y} a_n \ll_k y^{\frac{3}{4}}$$

Therefore

$$L(1,\chi_2)\cdots L(1,\chi_k) \ll_{\varepsilon,k} y^{-\frac{1}{4}} + D^{-\frac{\varepsilon^3}{600k}}$$

Since

$$D^{\frac{1}{4}} < D^{\frac{1}{4}+\frac{\varepsilon}{2}} \leq y$$

we obtain

$$\begin{aligned}
L(1,\chi_2)\cdots L(1,\chi_k) &\ll_{\varepsilon,k} D^{-\frac{1}{16}} + D^{-\frac{\varepsilon^3}{600k}} \\
&\ll D^{-\frac{\varepsilon^3}{600k}} \qquad (3.7)
\end{aligned}$$

On the other hand, Siegel's theorem with $\varepsilon = \frac{\varepsilon^3}{600k+1}$ gives us

$$q_i^{-\frac{\varepsilon^3}{600k+1}} \ll_{\varepsilon,k} \left|L(1,\chi_i)\right| \quad \forall i \in \overline{2,k}$$

Hence

$$D^{-\frac{\varepsilon^3}{600k+1}} = (q_2\cdots q_k)^{-\frac{\varepsilon^3}{600k+1}} \ll_{\varepsilon,k} \left|L(1,\chi_2)\cdots L(1,\chi_k)\right|$$

which clearly contradicts (3.7)

Therefore the least prime that splits completely in K is $\ll_{\varepsilon,k} D^{\frac{1}{4}+\varepsilon}$.

4 Bibliography

[1] N.G. de Bruijn, On the number of positive integers $\leq$ x and free of prime factors $>$ y. II, Indag.Math. 28 (1966), 239247.

[2] C.F.Gauss: Disquisitiones arithmeticae, Springer-Verlag, 1986.

[3] S. W. Golomb, Powerful numbers, Amer. Math. Monthly 77 (1970), 848855. MR0266878 (421780)

[4] H.Hasse, Vorlesungen uber Zahlentheorie, 2nd ed., Springer, Berlin, 1964.

[5] A.J. Hildebrand: Introduction to Analytic Number Theory, Lecture notes.

[6] S. Lang: Algebraic Number Theory. Addison-Wesley: Reading, MA, 1970

[7] H.L. Montgomery and R.C. Vaughan: Multiplicative number theory. I. Classical theory, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.

[8] K.K. Norton: On the distribution of power residues and non-residues, J. Reine Angew. Math.254 (1972), 188203.

[9] K.K. Norton: Bounds for sequences of consecutive power residues. I , in: Analytic Number Theory, Proc. Sympos. Pure Math. 24, Amer. Math. Soc., Providence, R.I., 1973, 213220.

[10] K.K. Norton: A character-sum estimate and applications, Acta Arithm. 85(1998),51-78.

[11] K.K. Norton: Upper bounds for kth power coset representatives modulo n, Acta Arithm. 85(1998), 161-179.

[12] P. Pollack: Bounds for the first several prime character nonresidues,
http://arxiv.org/pdf/1508.05035v2.pdf.

[13] P. Pollack: The smallest prime that splits completely in an abelian number field, Proc. Amer. Math. Soc. 142(2014), 1925-1934.

[14] G.Tenenbaum: Introduction to analytic and probabilistic number theory, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995.