

ANALYTIC NUMBER THEORY, SPRING 2022

THE CLASS NUMBER ONE PROBLEM

ZEÉV RUDNICK

CONTENTS

1. The class number one problem	1
1.1. Even discriminants with class number one	2
1.2. The class number one problem for odd discriminants	3
2. Dirichlet's class number formula	3
2.1. The Kronecker symbol	3
2.2. Dirichlet's class number formula	5
3. Applying the class number formula	6
3.1. An upper bound for $h(D)$	6
3.2. Lower bounds for $h(D)$	7
4. Littlewood's theorem for $\mathbb{F}_q[t]$	8
4.1. Background	8
4.2. Littlewood's theorem for $\mathbb{F}_q[t]$	9
4.3. Over the integers	11
References	12

1. THE CLASS NUMBER ONE PROBLEM

It is very useful to have only one class of forms with a given discriminant. Using reduction theory, we can quickly check several discriminants and obtain 13 discriminants with class number one, namely

$$-4, -3, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$$

Of these, there are 9 fundamental discriminants with class number one:

$$D = -4, -3, -7, -8, -11, -19, -43, -67, -163$$

and 4 which are non-fundamental: $D = -12, -16, -27, -28$. Gauss' class number one problem (1802) was to show that these are the only ones with class number one.

Additionally, Gauss conjectured that $h(D) \rightarrow \infty$ as $D \rightarrow -\infty$.

1.1. Even discriminants with class number one. Gauss used a different definition of integrality of quadratic forms which resulted in only looking at even discriminants, and E. Landau (1902) showed that the only ones with class number one are $D = -4, -8, -12, -16, -28$. This is quite elementary once we have reduction theory!

Theorem 1.1 (E. Landau, 1902). *The only even negative discriminants with $h(D) = 1$ are $D = -4, -8, -12, -16, -28$.*

Proof. We write $D = -4k$. If $\boxed{k = mn}$ with $1 < m < n$ coprime then $[m, 0, n]$ is reduced, primitive and non-principal so that $h(D) > 1$. So we are left to deal with k not of this form, equivalently (check!) for $k = p^r$ with p prime.

For $\boxed{k = 2^r}$ we compute $h(-4) = h(-8) = h(-16) = 1$, $h(-32) = 2$ so we are left to rule out $h(-4 \cdot 2^r)$ for $r \geq 4$. But then consider the form

$$g = [a, b, c] = [4, 4, 2^{r-2} + 1]$$

which has discriminant $D = -4 \cdot 2^r$ and is clearly primitive (as c is odd while $a = b = 2^2$). We check that g is reduced: Indeed $0 < b = a = 4 \leq c = 2^{r-2} + 1$ provided $r \geq 4$. Thus we have found a nonprincipal reduced primitive form so that $h(-4 \cdot 2^r) \geq 2$ for $r \geq 4$.

We are left with $\boxed{D = -4p^r}$ with p an odd prime. If $\boxed{p^r + 1 = ac}$ with $1 < a < c$ coprime, then

$$[a, 2, c]$$

is primitive, has discriminant $D = 4 - 4ac = 4 - 4(p^r + 1) = -4p^r$, and is reduced since $0 < b = 2 \leq a < c$.

So we are left with $p^r + 1$ a prime power, and since p is odd that means $\boxed{p^r + 1 = 2^s}$. For $s \leq 5$ we check $D = -4p^r = -4(2^s - 1)$ using reduction theory.

s	1	2	3	4	5
D	-4	-12	-28	-60	-124
$h(D)$	1	1	1	2	3

For $s \geq 6$ we have the form

$$[8, 6, 2^{s-3} + 1]$$

which is primitive and has discriminant $6^2 - 4 \cdot 8(2^{s-3} + 1) = 4 - 4 \cdot 2^s = 4 - 4(p^r - 1) = -4p^r = D$, and is reduced since $0 < 6 = b < 8 = a < 2^{s-3} + 1$ if $s \geq 6$. Thus $h(D) > 1$ in this last remaining case. $\square$

1.2. The class number one problem for odd discriminants. We are left to determine odd discriminants with class number one, which is a much harder problem.

Assuming GRH there is an effective $c > 0$ so that

$$h(D) > c \frac{\sqrt{|D|}}{\log |D|}$$

(Hecke 1918), so that on GRH, Gauss' problem is reduced to checking $h(D)$ for a finite list. Moreover, one can also enumerate all cases with $h(D) = 2$ etc.

Unconditional results: Heilbronn (1934) showed that $h(D) \rightarrow \infty$ as $D \rightarrow -\infty$, so that there are only finitely many fundamental discriminants of class number one. This was done by combining work of Deuring, Mordell and Heilbronn to obtain the the falsity of GRH implies $h(D) \rightarrow \infty$ as $D \rightarrow -\infty$, with the effective lower bound obtained from GRH.

Heilbronn and Linfoot (1934) showed that there are at most 10 fundamental discriminants of class number one (9 were known to Gauss).

Siegel (1935) showed unconditionally that $h(D) \gg_{\epsilon} |D|^{1/2-\epsilon}$ for all $\epsilon > 0$, but his constant was not effective so cannot be used to check that we have obtained all cases with class number one.

The class number one problem was finally settled by Stark (1967) and Baker (1966) (Kurt Heegner had an essentially correct proof in 1952 but was not believed at the time).

The combined work of Goldfeld (1976) and Gross-Zagier (1983) gives effective lower bounds. Oesterlé (1984) gives

$$h(D) > \frac{1}{55} (\log |D|) \prod_{\substack{p|D \\ p \neq D}} \left(1 - \frac{\lfloor 2\sqrt{p} \rfloor}{p+1} \right).$$

This of course is much poorer than the $|D|^{1/2}/\log |D|$ bound conditional on GRH and the ineffective Siegel bound of $|D|^{1/2-\epsilon}$, but is both unconditional and effective.

2. DIRICHLET'S CLASS NUMBER FORMULA

The goal of this section is to state (not prove!) a formula for the class number in terms of the value of a Dirichlet L-function $L(1, \chi_D)$ for a suitable Dirichlet character mod $|D|$.

2.1. The Kronecker symbol. For each discriminant $D = 0, 1 \pmod{4}$, which is not a perfect square (which we assume throughout the rest of

this chapter), we will construct a real Dirichlet character $\chi_D \bmod |D|$, which is nontrivial if D is not a perfect square (e.g. for all $D < 0$).

For $m > 0$ we define the Kronecker symbol $\left(\frac{D}{m}\right)$ by requiring complete multiplicativity in m , that is if $m = p_1^{e_1} \dots p_r^{e_r}$ is the prime factorization then

$$\left(\frac{D}{m}\right) = \prod_{j=1}^r \left(\frac{D}{p_j}\right)^{e_j}.$$

So we need to specify $\left(\frac{D}{p}\right)$ for prime p . This is done by requiring

- $\left(\frac{D}{p}\right) = 0$ if $p \mid D$.
- $\left(\frac{D}{p}\right)$ is the Legendre symbol for odd $p \nmid D$.
- For $p = 2$ and $D = 1 \bmod 4$ we have

$$\left(\frac{D}{2}\right) = \begin{cases} 1, & D = 1 \bmod 8 \\ -1, & D = 5 \bmod 8 \end{cases}$$

Exercise 1. a) For odd D we have $\left(\frac{D}{2}\right) = \left(\frac{2}{|D|}\right)$.

b) If $m > 0$ is odd and coprime to D then the Kronecker symbol is just the Jacobi symbol $\left(\frac{D}{m}\right)$.

We set

$$\chi_D(m) = \left(\frac{D}{m}\right).$$

Lemma 2.1. Let $D = 0, 1 \bmod 4$, $D \neq \square$, $m > 0$ and coprime to D .

For odd D , we have

$$\left(\frac{D}{m}\right) = \left(\frac{m}{|D|}\right)$$

where $\left(\frac{m}{|D|}\right)$ is the Jacobi symbol.

If $D = 2^b u$ with u odd and $b \geq 2$ then

$$\left(\frac{D}{m}\right) = \left(\frac{2}{m}\right)^b (-1)^{\frac{u-1}{2} \cdot \frac{m-1}{2}} \left(\frac{m}{|u|}\right).$$

Proposition 2.2. χ_D is a Dirichlet character mod $|D|$, that is if $m_1 = m_2 \bmod D$ then $\left(\frac{D}{m_1}\right) = \left(\frac{D}{m_2}\right)$.

Proof. We may assume that m_1 (hence m_2) is coprime to D , otherwise both $\chi_D(m_i) = 0$.

For odd D , we have $\left(\frac{D}{m_i}\right) = \left(\frac{m_i}{|D|}\right)$ by Lemma 2.1, and therefore the claim follows by the analogous property of the Jacobi symbol.

For $D = 2^b u$ even (u odd, $b \geq 2$), by Lemma 2.1 we have

$$\left(\frac{D}{m_i}\right) = \left(\frac{2}{m_i}\right)^b (-1)^{\frac{u-1}{2} \cdot \frac{m_i-1}{2}} \left(\frac{m_i}{|u|}\right).$$

Now $\left(\frac{m_1}{|u|}\right) = \left(\frac{m_2}{|u|}\right)$ since $m_1 = m_2 \pmod{|u|}$ (being congruent mod D). Also $m_1 = m_2 \pmod{4}$ (since $4 \mid D$) so that

$$(-1)^{\frac{|u|-1}{2} \cdot \frac{m_1-1}{2}} = (-1)^{\frac{|u|-1}{2} \cdot \frac{m_2-1}{2}}.$$

Finally, if $b = 2$ then $\left(\frac{2}{m_i}\right)^2 = 1$, while for $b > 2$ we are guaranteed $m_1 = m_2 \pmod{8}$ from $m_1 = m_2 \pmod{D}$, so that by the property of the Jacobi symbol, $\left(\frac{2}{m_1}\right) = \left(\frac{2}{m_2}\right)$. Thus we have $\left(\frac{D}{m_1}\right) = \left(\frac{D}{m_2}\right)$ for even D . $\square$

Another important property is that

Lemma 2.3. χ_D is nontrivial, that is there is some $m > 0$, coprime to D , so that $\chi_D(m) = -1$.

Lemma 2.4. For $m, n > 0$ with $n = -m \pmod{D}$, we have

$$\left(\frac{D}{n}\right) = \begin{cases} \left(\frac{D}{m}\right), & D > 0 \\ -\left(\frac{D}{m}\right), & D < 0 \end{cases}.$$

That is, χ_D is an even character if $D > 0$, and an odd character if $D < 0$.

The Kronecker symbol counts the solutions of quadratic congruences (recall that k is represented by some form of discriminant D iff $x^2 = D \pmod{4k}$ is solvable):

Proposition 2.5. Let $k > 0$ be coprime to D . Then the number of solutions of $x^2 = D \pmod{4k}$ is $2 \sum_{f|k} \left(\frac{D}{f}\right)$.

This follows from the Chinese Remainder Theorem and Hensel's lemma.

A final note: All real Dirichlet characters are Kronecker symbols.

2.2. Dirichlet's class number formula. Dirichlet's Class Number Formula expresses $L(1, \chi_D)$ in terms of the class number $h(D)$ and manifestly displays the non-vanishing of $L(1, \chi_D)$.

Theorem 2.6. Let $D < 0$ be a discriminant. Then

$$L(1, \chi_D) = \frac{2\pi}{w_D} \frac{h(D)}{\sqrt{|D|}}$$

where $w_{-4} = 4$, $w_{-3} = 6$, and $w_D = 2$ otherwise.

There is an analogous formula for positive (fundamental) discriminants:

$$L(1, \chi_D) = \frac{2h(D) \log \epsilon_D}{\sqrt{|D|}}$$

with ϵ_D being the fundamental solution of Pellian equation $t^2 - Du^2 = 4$, which is the solution of $t^2 - Du^2 = 4$ with $t_0, u_0 > 0$ and u_0 having the minimal value; all solutions are $\pm \epsilon_D^n$, $n \in \mathbb{Z}$. For $D < 0$ a fundamental discriminant, this is the fundamental unit of $\mathbb{Q}(\sqrt{D})$.

3. APPLYING THE CLASS NUMBER FORMULA

3.1. An upper bound for $h(D)$. Let $D < 0$ be a discriminant. Using reduction theory, we obtained an upper bound on the class number of $h(D) \ll |D|$. We improve it by using Dirichlet's class number formula:

Theorem 3.1. *As $D \rightarrow -\infty$, $h(D) \ll \sqrt{|D|} \log |D|$.*

Proof. From the class number formula, it suffices to show that $|L(1, \chi_D)| \ll \log |D|$. Using summation by parts, we have (that was the analytic continuation)

$$L(1, \chi) = \sum_n \frac{\chi_D(n)}{n} = \frac{S(t)}{t} \Big|_1^\infty + \int_1^\infty \frac{S(t)}{t^2} dt$$

with

$$S(t) := \sum_{n \leq t} \chi_D(n).$$

Since χ_D is a nontrivial character mod $|D|$, the orthogonality relations give

$$|S(t)| \leq \min(t, |D|).$$

Hence the boundary term is $O(1)$. We divide the domain of integration in $\int_1^\infty \frac{S(t)}{t^2} dt$ to $1 \leq t \leq Y$ and $t > Y$, where we will take $Y \approx |D|$:

$$\left| \int_1^\infty \frac{S(t)}{t^2} dt \right| \leq \int_1^Y \frac{|S(t)|}{t^2} dt + \int_Y^\infty \frac{|S(t)|}{t^2} dt$$

For $1 \leq t \leq Y$, we use $|S(t)| \leq t$, while for $t > Y$ we use $|S(t)| \ll |D|$. We obtain

$$\begin{aligned} L(1, \chi_D) &\ll \int_1^Y \frac{t}{t^2} dt + \int_Y^\infty \frac{|D|}{t^2} dt \\ &\ll \log Y + \frac{|D|}{Y}. \end{aligned}$$

Taking $Y \approx |D|$ gives $L(1, \chi_D) \ll \log |D|$. □

3.2. Lower bounds for $h(D)$. Gauss conjectured that $h(D) \rightarrow \infty$ as $D \rightarrow -\infty$. This was proved (Hecke/Landau 1918) assuming GRH, moreover there is an effective $c > 0$ so that $h(D) > c\sqrt{|D|}/\log |D|$, so that on GRH Gauss' problem is reduced to checking $h(D)$ for a finite list. Moreover, one can also enumerate all cases with $h(D) = 2$ etc. Heilbronn (1934) showed (unconditionally) that $h(D) \rightarrow \infty$ as $D \rightarrow -\infty$.

By the class number formula, for $D < -12$, $\pi h(D) = |D|^{1/2} L(1, \chi_D)$, hence to show $h(D) \rightarrow \infty$ is equivalent to showing $|D|^{1/2} L(1, \chi_D) \rightarrow \infty$ as $D \rightarrow -\infty$.

Siegel (1935) proved that for any $\epsilon > 0$, there is some $C(\epsilon) > 0$ (ineffective!) so that

$$L(1, \chi_D) \geq C(\epsilon) |D|^{-\epsilon}$$

so that $h(D) \geq C(\epsilon) |D|^{1/2-\epsilon}$ as $D \rightarrow -\infty$.

Littlewood (1928) [1] showed that

Theorem 3.2. *if D is a discriminant (not a perfect square), and χ a real non-principal character mod D (e.g. χ_D) then assuming that $L(s, \chi)$ satisfies the Riemann Hypothesis, we have*

$$(1) \quad \frac{1}{\log \log |D|} \ll L(1, \chi) \ll \log \log |D|.$$

For his proof, Littlewood showed that on GRH, we can approximate $L(1, \chi)$ by a short Euler product, from which he deduced Theorem 3.2:

Theorem 3.3. *If $\chi \neq \chi_0$ is real mod D then*

$$(2) \quad L(1, \chi) = \prod_{p \leq (\log |D|)^2} \left(1 - \frac{\chi(p)}{p}\right)^{-1} \left(1 + O\left(\frac{\log \log \log |D|}{\log \log |D|}\right)\right)$$

We show how to use Theorem 3.3 to prove Theorem 3.2: By the short Euler product representation, for any $\chi \neq \chi_0$ we have an upper bound

$$|L(1, \chi)| \ll \prod_{p \leq (\log |D|)^2} \left(1 - \frac{1}{p}\right)^{-1}$$

which by Mertens' theorem, is $\approx \log \log |D|$. Now for χ real we also have $L(1, \chi)$ real and being non-zero it is positive, so that $L(1, \chi) = |L(1, \chi)|$, hence

$$L(1, \chi) \ll \log \log |D|.$$

For the lower bound, we have

$$\left| \left(1 - \frac{\chi(p)}{p}\right)^{-1} \right| \geq \frac{1}{1 + \frac{1}{p}} \approx 1 - \frac{1}{p}$$

and so

$$L(1, \chi) \gg \prod_{p \leq (\log |D|)^2} \left(1 - \frac{1}{p}\right) \approx \frac{1}{\log \log |D|}$$

giving the requested lower bound.

We will explain Theorem 3.3 in the setting of $\mathbb{F}_q[t]$.

4. LITTLEWOOD'S THEOREM FOR $\mathbb{F}_q[t]$

4.1. Background. We first recall Mertens' theorem for $\mathbb{F}_q[t]$:

Exercise 2. Fix q . As $M \rightarrow \infty$,

$$\prod_{\deg P \leq M} \left(1 - \frac{1}{\|P\|}\right) \approx \frac{1}{M}.$$

Let $D \in \mathbb{F}_q[t]$ be a polynomial of positive degree, and χ a non-trivial character mod D . The L-function is

$$L(s, \chi) = \sum_{f \text{ monic}} \chi(f) \|f\|^{-s} = \sum_{f \text{ monic}} \chi(f) u^{\deg f}$$

where $\|f\| = q^{\deg f}$ and $u = q^{-s}$. We saw that $L(s, \chi)$, initially defined for $\operatorname{Re}(s) > 1$, turn out to be a polynomial of degree at most $\deg D - 1$ in u , and hence can be written as

$$L(s, \chi) = \prod_{j=1}^{\deg D - 1} (1 - \alpha_j(\chi)u).$$

The Explicit formula says that

$$\Psi(k; \chi) := \sum_{\deg f = k} \Lambda(f) \chi(f) = - \sum_{j=1}^{\deg D - 1} \alpha_j(\chi)^k$$

The Riemann Hypothesis in this context was proved by Weil in the 1940's and gives that the inverse zeros are bounded by $|\alpha_j| \leq q^{1/2}$. Hence

$$|\Psi(k, \chi)| \leq (\deg D - 1) q^{k/2}.$$

Lemma 4.1. Let $D \in \mathbb{F}_q[t]$ be a polynomial of positive degree, and χ a non-trivial character mod D . Then

$$(3) \quad \left| \sum_{\substack{\deg P = k \\ P \text{ prime}}} \chi(P) \right| \leq \frac{q^{k/2}}{k} \deg D.$$

Proof. For $k = 1$, this follows immediately from the Explicit formula, since the sum is $\Psi(1, \chi)$. So assume that $k \geq 2$.

In the explicit formula, we separate out the contribution of primes and bound the rest:

$$\Psi(k, \chi) = k \sum_{\substack{\deg P=k \\ P \text{ prime}}} \chi(P) + \sum_{\substack{d|k \\ d < k}} d \sum_{\substack{\deg P=d \\ P \text{ prime}}} \chi(P^{k/d})$$

The sum over $d < k$ is bounded trivially using $|\chi| \leq 1$ and then arguing as in the Prime Polynomial Theorem

$$\begin{aligned} \left| \sum_{\substack{d|k \\ d < k}} d \sum_{\substack{\deg P=d \\ P \text{ prime}}} \chi(P^{k/d}) \right| &\leq \sum_{\substack{d|k \\ d < k}} d \pi_q(d) \leq \sum_{\substack{d|k \\ d < k}} q^d \leq \sum_{k=1}^{d/2} q^d \\ &= \frac{q^{\lfloor k/2 \rfloor + 1} - q}{q - 1} = \frac{q^{\lfloor k/2 \rfloor} - 1}{1 - 1/q} = q^{\lfloor k/2 \rfloor} \frac{1 - 1/q^{\lfloor k/2 \rfloor}}{1 - 1/q}. \end{aligned}$$

Since $k \geq 2$, we have $\frac{1 - 1/q^{\lfloor k/2 \rfloor}}{1 - 1/q} \leq 1$ and so

$$\left| \Psi(k, \chi) - k \sum_{\substack{\deg P=k \\ P \text{ prime}}} \chi(P) \right| \leq q^{k/2}.$$

Since $|\Psi(k, \chi)| \leq (\deg D - 1)q^{k/2}$ we obtain

$$\left| k \sum_{\substack{\deg P=k \\ P \text{ prime}}} \chi(P) \right| \leq |\Psi(k, \chi)| + q^{k/2} \leq q^{k/2} \deg D$$

as required. $\square$

4.2. Littlewood's theorem for $\mathbb{F}_q[t]$. We will give the analogue of Littlewood's result for $\mathbb{F}_q[t]$ (see [2, Proposition 1.4]):

Theorem 4.2. *Let $D \in \mathbb{F}_q[t]$ of positive degree, and $\chi \neq \chi_0$ a real nonprincipal character mod D . Then*

$$L(1, \chi) = \prod_{\|P\| \ll (\deg D)^2} \left(1 - \frac{\chi(P)}{\|P\|} \right)^{-1} \cdot \left(1 + O\left(\frac{1}{\log_q \deg D} \right) \right).$$

Proof. We deduce from Lemma 4.1 that for $\sigma := \operatorname{Re}(s) > 1/2$, we have a convergent expansion

$$\log L(s, \chi) = \sum_{k \geq 1} A_k(s)$$

where

$$A_k(s) = - \sum_{\deg P=k} \log \left(1 - \frac{\chi(P)}{\|P\|^s} \right)$$

Indeed, this expansion holds for $\sigma > 1$ by Euler's product expansion. Expanding $\log(1-z)^{-1} = z + O(z^2)$ gives for $\sigma > 1/2$ that

$$\begin{aligned} A_k(s) &= \sum_{\deg P=k} \left(\frac{\chi(P)}{\|P\|^s} + O\left(\frac{1}{\|P\|^{2\sigma}}\right) \right) \\ &= \frac{1}{q^{ks}} \sum_{\deg P=k} \chi(P) + O\left(\frac{q^k/k}{q^{2k\sigma}}\right) \\ &\ll \frac{1}{q^{k\sigma}} \frac{q^{k/2}}{k} \deg D + O\left(\frac{1}{kq^{k(2\sigma-1)}}\right) \end{aligned}$$

by (3), hence

$$A_k(s) \ll \frac{\deg D}{kq^{k(\sigma-1/2)}}$$

so that $\sum_{k \geq 1} A_k(s)$ converges absolutely for $\sigma > 1/2$. In particular, for $s = 1$ we obtain a tail estimate

$$\sum_{k > M} A_k(1) \ll \sum_{k > M} \frac{\deg D}{kq^{k/2}} \ll \frac{\deg D}{Mq^{M/2}}.$$

Therefore we find

$$\log L(1, \chi) = - \sum_{1 \leq \deg P \leq M} \log \left(1 - \frac{\chi(P)}{\|P\|} \right) + O\left(\frac{\deg D}{Mq^{M/2}}\right).$$

We take M minimal so that the O -term is $o(1)$, say

$$M \approx 2 \log_q \deg D$$

for which the O -term is $O(1/M)$, and exponentiating gives the analogue of Littlewood's approximation (2):

$$L(1, \chi) = \prod_{\deg P \leq M} \left(1 - \frac{\chi(P)}{\|P\|} \right)^{-1} \cdot \left(1 + O\left(\frac{1}{M}\right) \right).$$

Now note that the condition $\deg P \leq M \approx 2 \log_q \deg D$ is equivalent to $\|P\| \lesssim (\deg D)^2$. $\square$

4.3. Over the integers. The number field version (Littlewood's original result) is the same argument, using a dyadic subdivision and summation by parts with GRH. One writes for $\sigma = \operatorname{Re}(s) > 1$

$$\log L(s, \chi) = \sum_{k \geq 0} A_k(s)$$

with

$$A_k(s) = \sum_{2^k < p \leq 2^{k+1}} \log \left(1 - \frac{\chi(p)}{p^s} \right)^{-1}.$$

Then expand the logarithm and show that

$$\begin{aligned} A_k(s) &= - \sum_{2^k < p \leq 2^{k+1}} \left(\frac{\chi(p)}{p^s} + O \left(\frac{1}{p^{2\sigma}} \right) \right) \\ &= - \sum_{2^k < p \leq 2^{k+1}} \frac{\chi(p)}{p^s} + O(2^{-(2\sigma-1)k}). \end{aligned}$$

We need GRH to bound the prime sum

$$\theta(\chi, t) := \sum_{p \leq t} \chi(p) \log p.$$

GRH gives that for a nontrivial character mod D , and $|D| \leq t$, then

$$\psi(\chi, t) := \sum_{n \leq t} \Lambda(n) \chi(n) \ll t^{1/2} \log^2(t|D|).$$

Applying a standard argument to bound the contribution of higher prime powers give

$$\left| \sum_{\substack{p^k \leq t \\ k \geq 2}} \chi(p^k) \log p \right| \leq \sum_{\substack{p^k \leq t \\ k \geq 2}} \log p \ll t^{1/2}.$$

Hence we obtain

$$(4) \quad |\theta(\chi, t)| \ll t^{1/2} \log^2(t|D|).$$

Now we use summation by parts to bound $A_k(s)$ for $\sigma > 1/2$

$$\begin{aligned} \sum_{2^k < p \leq 2^{k+1}} \frac{\chi(p)}{p^s} &= \sum_{2^k < p \leq 2^{k+1}} \frac{\chi(p) \log p}{p^s \log p} \\ &= \frac{\theta(\chi, t)}{t^s \log t} \Big|_{2^k}^{2^{k+1}} - \int_{2^k}^{2^{k+1}} \theta(\chi, t) \left(\frac{1}{t^s \log t} \right)' dt \end{aligned}$$

Inserting (4) gives

$$\left| \sum_{2^k < p \leq 2^{k+1}} \frac{\chi(p)}{p^s} \right| \ll 2^{k(1/2-\sigma)} \log^2(|D|2^k)$$

Hence for $\sigma > 1/2$ (in particular, for $s = 1$)

$$|A_k(s)| \ll \frac{\log^2(|D|2^k)}{2^{k(\sigma-1/2)}}.$$

Therefore

$$\log L(s, \chi) = \sum_{p \leq M} \log \left(1 - \frac{\chi(p)}{p^s} \right)^{-1} + O \left(\frac{\log^2(DM)}{M^{\sigma-1/2}} \right).$$

Taking $M \approx (\log |D|)^5$ will give

$$L(1, \chi) = \prod_{p \leq \log^5 |D|} \left(1 - \frac{\chi(p)}{p} \right)^{-1} (1 + o(1))$$

which is (essentially) Littlewood's theorem.

REFERENCES

- [1] Littlewood, J. E. On the class number of the corpus $P(\sqrt{-k})$. Proceedings of the London Mathematical Society 27, no. 1 (1928): 358–372.
- [2] Lumley, Allysa. Complex moments and the distribution of values of $L(1, \chi_D)$ over function fields with applications to class numbers. Mathematika 65 (2019), no. 2, 236–271.