

Lecture # 8 and 9: Ideals and the Class Number Formula.

Noah Snyder

July 22, 2002

1 Another Solution to the $n = x^2 + y^2$ Question

There's a different way to go about the problem of finding all ways of writing $n = x^2 + y^2$. Recall that in the Gaussian integers $\mathbb{Z}[i]$ we have an automorphism $\alpha \mapsto \bar{\alpha}$. Thus the function $N\alpha = \alpha\bar{\alpha} = x^2 + y^2$ is multiplicative. Thus our question is just to find all ways of writing n as a norm from the Gaussian integers. To answer this question we need to know a little about the structure of $\mathbb{Z}[i]$.

(Note that by inducting on the norm every number factors into a product of primes.)

Proposition 1.1. $\mathbb{Z}[i]$ is a Euclidean domain, therefore it is a PID, and a UFD.

Proof. Take any Gaussian integers $\alpha = \alpha_1 + \alpha_2 i$ and $\beta = \beta_1 + \beta_2 i$. By the division algorithm in the integers one can choose $q, r' \in \mathbb{Z}[i]$ such that $\bar{\beta}\alpha = N\beta q + r'$ with $r'_1 \leq \frac{1}{2}N\beta$ and $r'_2 \leq \frac{1}{2}N\beta$. Thus, $Nr' \leq \frac{1}{2}N\beta^2$. Since $r' = \bar{\beta}\alpha - N\beta q$ we can write $r' = \bar{\beta}r$. Thus we can write $\alpha = \beta q + r$ with $Nr \leq \frac{1}{2}N\beta$. Thus $\mathbb{Z}[i]$ is Euclidean. By standard arguments it must also be a PID and a UFD. \square

Thus if we factor n into a product of primes in $\mathbb{Z}[i]$ we only need to check whether each prime also pairs with one of its conjugates. To do this we need to get some handle on what the primes in $\mathbb{Z}[i]$ are like.

Proposition 1.2. Any prime $\pi \in \mathbb{Z}[i]$ divides exactly one prime $p \in \mathbb{Z}$.

Proof. $\pi\bar{\pi} = N\pi = \prod_i p_i^{a_i}$. Thus, by unique factorization, we must have $\pi|p_i$ for some i . Suppose $\pi|p$ and $\pi|q$ for two distinct primes. Then choose x and y so that $px + qy = 1$. Thus $\pi|1$ which is a contradiction. \square

Thus in order to find all the primes in $\mathbb{Z}[i]$ it is enough to find how each prime in \mathbb{Z} factors in $\mathbb{Z}[i]$.

Proposition 1.3. If p is a prime in \mathbb{Z} it factors into primes in $\mathbb{Z}[i]$ as follows:

$$p = \begin{cases} p & \text{if } p \equiv 3 \pmod{4} \\ \pi\bar{\pi} \text{ (with } \pi \neq u\bar{\pi}) & \text{if } p \equiv 1 \pmod{4} \\ \pi\bar{\pi} \text{ (with } \pi = u\bar{\pi}) & \text{if } p \equiv 2 \pmod{4} \end{cases}$$

Proof. Notice that

$$\mathbb{Z}[i]/p = \mathbb{Z}[x]/(x^2 + 1, p) = \mathbb{Z}/p[x]/(x^2 + 1).$$

If we know how p factors in $\mathbb{Z}[i]$ then we know the structure of $\mathbb{Z}[i]/p$ (that is, field, product of two fields, or ring with nilpotent elements). Similarly if we know how $(x^2 + 1)$ factors in $\mathbb{Z}/p[x]$ we can recover the structure of $\mathbb{Z}[i]/p$. Therefore we must have that $\mathbb{Z}[i]/p$ must factor in $\mathbb{Z}[i]$ exactly how $(x^2 + 1)$ factors in $\mathbb{Z}/p[x]$. By the quadratic formula the latter is given by whether -4 is a square modulo p . The result follows. \square

Notice that this gives a way of finding which n can be written as $x^2 + y^2$ and how many ways we can write it this way. If we factor n into primes in \mathbb{Z} then each prime which is 1 modulo p can be written as the norm of π and $\bar{\pi}$. Each prime which is 3 modulo 4 must appear with its conjugate (itself) and so the exponent must be even and still you can only write it as a norm one way. The prime 2 can appear to any power, but it can only be written as a norm one way. Since there are exactly 4 units (its easy

to see that α is a unit iff $N\alpha = 1$), its easy to see that n can be written as a norm iff it every prime 3 mod 4 appears to an even power and it can be written in $4 \cdot 2^x$ where x is the number of primes 1 mod 4 dividing n .

Definition 1.4.

$$\zeta_{\mathbb{Z}[i]}(s) = \sum_{\alpha \in \mathbb{Z}[i] \setminus \{0\}} N\alpha^{-s}.$$

Since the norm is multiplicative and the Gaussian integers have unique factorization there is an Euler factorization for this ζ function.

$$\zeta_{\mathbb{Z}[i]}(s) = 4 \prod_{\pi} \frac{1}{1 - N\pi^{-s}}$$

where π ranges over the Gaussian primes, but we only count each set of associates (π , $-\pi$, $i\pi$, and $-i\pi$) once. By our result classifying the primes in $\mathbb{Z}[i]$,

$$\begin{aligned} \zeta_{\mathbb{Z}[i]}(s) &= 4 \prod_{p \equiv 1 \pmod{4}} \left(\frac{1}{1 - p^{-s}} \right)^2 \prod_{p \equiv 2 \pmod{4}} \frac{1}{1 - p^{-s}} \prod_{p \equiv 3 \pmod{4}} \frac{1}{1 - p^{-2s}} \\ &= 4 \prod_p \frac{1}{1 - p^{-s}} \prod_p \frac{1}{1 + \left(\frac{-4}{p}\right) p^{-s}} \\ &= 4\zeta(s)L\left(1, \left(\frac{-4}{\cdot}\right)\right). \end{aligned}$$

Since the lefthand side is a generating function for the number of solutions to $n = x^2 + y^2$ this equation encodes a formula for the number of solutions to $n = x^2 + y^2$.

Further notice that this formula is exactly the formula which we used to get the class number formula.

2 Factorization in $\mathbb{Z}[\sqrt{d}]$.

We would like to go through the same argument for $\mathbb{Z}[\sqrt{d}]$. To do so we need unique factorization. But, for example

$$2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Notice that if one tried to prove the division algorithm here you would get a problem exactly when you had a remainder which looked like $(\frac{1}{2} + \frac{1}{2}\sqrt{-3})\beta$. This suggests that one instead look at $\mathbb{Z}[\frac{1}{2} + \frac{\sqrt{-3}}{2}]$. Notice that numbers of the form $a + b\left(\frac{1}{2} + \frac{\sqrt{-3}}{2}\right)$ are in fact closed under multiplication and addition, and one can easily show that this domain is euclidian. Furthermore, the norm of these elements is always an integer and so we can use induction.

So suppose we're given a ring $\mathbb{Z}[\sqrt{d}]$ how many extra rational points of $\mathbb{Q}[\sqrt{d}]$ can we throw in while staying closed under multiplication and having integral norms? It is easy to see that we must then have $\alpha + \bar{\alpha} \in \mathbb{Z}$ and $N\alpha \in \mathbb{Z}$. Combining these two conditions means that the biggest such ring we can find is,

$$\mathcal{O}_{\sqrt{d}} = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod{4} \\ \mathbb{Z}\left[\frac{1}{2} + \frac{\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod{4} \end{cases}.$$

Notice that in these two cases the generator of this ring has minimal polynomials $x^2 - d$ and $x^2 + x + \frac{1-d}{4}$. Furthermore, the former of these two has discriminant $4d$ while the latter has discriminant d .

However, even with these added points one still does not get unique factorization. For example we have the following non-unique factorization:

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Kummer wanted to fix this problem by adding in additional symbols called "ideal primes" to restore unique factorization. Thus we would have, $2 \cdot 3 = p_1 p_2 p_3 p_4 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ and thus no

contradiction to unique factorization. Now when do we need such factors? If α is irreducible by $\mathcal{O}_{\sqrt{d}}/\alpha$ is not a field then we need some ideal prime factor of α . Thus these “ideal primes” correspond to maps $\mathcal{O}_{\sqrt{d}} \rightarrow \mathbb{F}_q$ and we say that $p|\alpha$ if this map factors through $\mathcal{O}_{\sqrt{d}}/\alpha$.

Dedekind realized that its much nicer to look at the kernels of these maps which are called ideals.

3 Ideals in Quadratic Number Fields

Unless otherwise noted we are always looking at the ring $\mathcal{O}_{\sqrt{d}}$. Most of these results are not true for a general domain.

Proposition 3.1. *Any ideal in $\mathcal{O}_{\sqrt{d}}$ can be written as $\alpha\mathbb{Z} + \beta\mathbb{Z}$.*

Proof. Any ideal is a sublattice of the ring of integers, and any two-dimensional lattice can be written in this form. \square

If A and B are ideals in $\mathcal{O}_{\sqrt{d}}$ let $\bar{A} = \{\bar{\alpha} : \alpha \in A\}$. Let $AB = \{\sum_{i=1}^k \alpha_i \beta_i : k \in \mathbb{Z}^+, \alpha_i \in A, \beta_i \in B\}$. Let $(A, B) = \{\alpha + \beta : \alpha \in A, \beta \in B\}$. Notice that all of these are ideals.

Proposition 3.2. *$NA = n\mathcal{O}$ for some rational integer n .*

Proof. Notice that for some α and β in \mathcal{O} we have $A = (\alpha, \beta)$. Thus $NA = (\alpha\bar{\alpha}, \alpha\bar{\beta}, \beta\bar{\alpha}, \beta\bar{\beta})$. We want to find some rational integer $n \in NA$ such that $\frac{\alpha\bar{\alpha}}{n}, \frac{\alpha\bar{\beta}}{n}, \frac{\beta\bar{\alpha}}{n}, \frac{\beta\bar{\beta}}{n}$ are all in \mathcal{O} . That is to say we need the traces and norms of all of those numbers to be in \mathbb{Z} . Thus we only need $n|\alpha\bar{\alpha}, n|\beta\bar{\beta}$ and $n|(\alpha\bar{\beta} + \beta\bar{\alpha})$. Thus we let $n = \gcd(\alpha\bar{\alpha}, \beta\bar{\beta}, \alpha\bar{\beta} + \beta\bar{\alpha})$ this is clearly in A and we’ve shown that $A \supseteq n\mathcal{O}$, thus $A = n\mathcal{O}$. \square

Proposition 3.3. *In $\mathcal{O}_{\sqrt{d}}$, $AB = AC$ then $B = C$.*

Proof. If $AB = AC$, then $nB = \bar{A}AB = \bar{A}AC = nC$ for some integer n . But then one can easily see that every element of B is an element of C and vice versa. \square

Proposition 3.4. *In $\mathcal{O}_{\sqrt{d}}$, $A|B$ iff $A \supseteq B$.*

Proof. The forward direction is true in any domain. If $AC = B$ then choose any $\beta \in B$. By definition $\beta = \sum_i \alpha_i \gamma_i$ for some $\alpha_i \in A$ and $\gamma_i \in C$. But $\gamma_i \in \mathcal{O}$, therefore $\beta \in A$.

Now we prove the backwards direction. First assume that $A = \alpha\mathcal{O}$ is principal. So we’re assuming that $\alpha\mathcal{O} \supseteq B$. Therefore, for all $\beta \in B$, $\beta = \alpha\gamma$ for some $\gamma \in \mathcal{O}$. Let $C = \{\gamma : \alpha\gamma \in B\}$. C is an ideal and $B = \alpha C$, so $A|B$.

Now suppose A is any ideal. $A \supseteq B$, so $n\mathcal{O} = \bar{A}A \supseteq \bar{A}B$. Thus for some ideal C , $nC = \bar{A}B$. Therefore, $\bar{A}AC = nC = \bar{A}B$, so by our last lemma $AC = B$. \square

Definition 3.5. *$A \neq \mathcal{O}$ is called irreducible if $A = BC$ implies $B = \mathcal{O}$ or $C = \mathcal{O}$. $P \neq \mathcal{O}$ is called prime if $P|AB$ implies $P|A$ or $P|B$.*

Obviously any ideal factors as a product of irreducible ideals. On the other hand any factorization into prime ideals is clearly unique. Thus we need only show that these two concepts coincide in $\mathcal{O}_{\sqrt{d}}$.

Proposition 3.6. *An ideal P is prime iff $\alpha\beta \in P$ implies $\alpha \in P$ or $\beta \in P$.*

Proof. If $\alpha\beta$ is in P , then by our lemma $P|(\alpha)(\beta)$. Therefore by the definition of prime $P|(\alpha)$ or $P|(\beta)$. Using the lemma again $\alpha \in P$ or $\beta \in P$.

On the other hand suppose P satisfies the condition $\alpha\beta \in P$ implies $\alpha \in P$ or $\beta \in P$ and $P|AB$. Further suppose $P \nmid A$ and $P \nmid B$. Thus $P \not\supseteq A$ and $P \not\supseteq B$. Hence there exist $\alpha \in A$ and $\beta \in B$ such that $\alpha \notin P$ and $\beta \notin P$. Hence $\alpha\beta \notin P$. This is a contradiction. \square

This definition is the usual definition of a prime ideal. Further note that this means that P is prime if and only if \mathcal{O}/P is a domain.

Proposition 3.7. *An ideal A is irreducible if and only if it is maximal (that is not properly contained in any ideal other than \mathcal{O}).*

Proof. Again we just use the lemma. Irreducible says that A is maximal with respect to the divides partial ordering. But since divides is the same as contains this is equivalent to saying its maximal. \square

Notice that maximal ideals are characterized by the fact that when you mod out by them you get a field (the only kind of domain with no nontrivial proper ideals).

Proposition 3.8. *An ideal is prime if and only if its irreducible.*

Proof. We've shown that an ideal is prime if and only if when you mod out by it you get a domain. We've also seen that an ideal is irreducible if and only if when you mod out by it you get a field. However, $NA \subseteq A$ and \mathcal{O}/NA has $N\alpha^2$ elements, thus \mathcal{O}/A has finitely many elements. But any finite domain is a field. \square

Thus we have proved:

Theorem 3.9. *Ideals in $\mathcal{O}_{\sqrt{d}}$ factor uniquely as a product of prime ideals.*

4 Class Number Formula

Now we can argue just as we did in $\mathbb{Z}[i]$ and a prime p factors in $\mathcal{O}_{\sqrt{d}}$ exactly how $x^2 - d$ factors in $\mathbb{Z}/p[x]$. Furthermore, by unique factorization the zeta function attached to this ring will have an Euler factorization. Thus, if $D < 0$ is congruent to 0 or 1 modulo 4 and w is the number of units in $\mathcal{O}_{\sqrt{D}}$,

$$\begin{aligned} \zeta_{\mathcal{O}_{\sqrt{D}}}(s) &= \sum_A NA^{-s} = \prod_P \frac{1}{1 - NP^{-s}} \\ &= \prod_{\left(\frac{D}{p}\right)=1} \left(\frac{1}{1 - p^{-s}} \right)^2 \prod_{\left(\frac{D}{p}\right)=1} \frac{1}{1 - p^{-s}} \prod_{\left(\frac{D}{p}\right)=1} \frac{1}{1 - p^{-2s}} \\ &= \zeta(s)L\left(s, \left(\frac{D}{\cdot}\right)\right). \end{aligned}$$

Again the righthand side has a finite limit if you multiply by $(s - 1)$ and then send s to 1. We would like to evaluate this limit of the lefthand side. However dealing with a sum over all ideals is rather unruly. We would like to be able to write this in terms of the elements of $\mathcal{O}_{\sqrt{d}}$.

Notice that since ideals factor uniquely as a product of primes, one can consider the group of fractional ideals, that is to say the free abelian group generated by prime ideals. Furthermore the principal fractional ideals are a subgroup. Thus we can consider the ideal class group C which is the fractional ideals modulo the principal fractional ideals.

Thus we can write any ideal as an element of the class group times a principal fractional ideal. This gets very close to expressing this sum as a sum over elements. In fact,

$$\sum_A NA^{-s} = \sum_{A \in C} \frac{1}{w} \sum_{\alpha \in K: \alpha A \subseteq \mathcal{O}} N(\alpha A)^{-s}.$$

Now $\alpha A \subseteq \mathcal{O}$ exactly when $\alpha NA \subseteq \bar{A}$. Thus we can rewrite this,

$$\zeta_{\mathcal{O}_{\sqrt{D}}}(s) = \sum_{A \in C} \frac{NA^s}{w} \sum_{\alpha \in \bar{A}} N\alpha^{-s}.$$

By our lemma relating the Dirichlet density to the actual density the limit of that last sum times $(s - 1)$ is just (assuming this latter quantity exists):

$$\lim_{N \rightarrow \infty} \sum_{A \in C} \frac{NA^s}{w} \frac{f_A(N)}{N},$$

where $f_A(N)$ is the number of elements of \bar{A} with norm smaller than N . But \bar{A} is just a lattice whose fundamental parallelogram has area NA . (This fact is easy to show for primes, a bit more work for prime powers and then the Chinese remainder theorem gives you the full result.) Furthermore the condition that $N\alpha \leq N$ is that the point lie inside an ellipse with volume $\frac{2\pi}{\sqrt{D}}$. Thus by exactly the same arguments as the last section this limit is $\frac{2\pi h(D)}{w\sqrt{D}}$, where $h(D)$ is the size of the class group (which much be finite for this sum to converge). Therefore, taking this limit of both sides,

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

5 The Correspondence Between Forms and Ideals

As we have seen above the class number formula for quadratic forms has an analogue for ideals in quadratic imaginary fields and the question of how you can write numbers in the form $x^2 + ny^2$ can be answered (sort of) using either theory. Thus we might expect there is a closer correspondence going on. If one considers an ideal $A = \{\alpha x + \beta y\}$ in $\mathcal{O}_{\sqrt{D}}$ the norm is going to be some quadratic form. Furthermore if one has a quadratic form like $x^2 + y^2$ these numbers are exactly the image of the norm from some ideal in some quadratic number field. We make this correspondence explicit as follows.

Definition 5.1. *If A is an ideal in $\mathcal{O}_{\sqrt{D}}$ with a chosen ordered basis $A = \alpha\mathbb{Z} + \beta\mathbb{Z}$, then let $f_{\alpha,\beta}(x, y) = \frac{1}{N(A)}N(\alpha x + \beta y)$.*

Proposition 5.2. *$f_{\alpha,\beta}$ is a primitive BQF.*

Proof. Multiplying out the definition of the norm,

$$f_{\alpha,\beta}(x, y) = \frac{1}{N(A)}N(\alpha\bar{\alpha}x^2 + (\alpha\bar{\beta} + \bar{\alpha}\beta)xy + \beta\bar{\beta}y^2).$$

All of these coefficients are fixed under conjugation and thus lie in \mathbb{Z} , we need only show that their gcd is exactly $N(A)$. But this is precisely what we proved when we showed that $NA = n\mathcal{O}$. \square

Proposition 5.3. *The discriminant of $f_{\alpha,\beta}$ is D .*

Proof. The discriminant of $f_{\alpha,\beta}$ is by definition

$$\frac{1}{NA^2}(\alpha\bar{\beta} + \bar{\alpha}\beta)^2 - 4N\alpha N\beta = \frac{1}{NA^2}(\alpha\bar{\beta} - \bar{\alpha}\beta)^2.$$

This last expression is the determinant of the matrix $\begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix}$. Since $\alpha\mathbb{Z} + \beta\mathbb{Z}$ is a sublattice of the lattice \mathcal{O} , for some matrix M ,

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = M \begin{pmatrix} 1 \\ \frac{D}{2} + \frac{\sqrt{D}}{2} \end{pmatrix}.$$

Therefore,

$$\det \begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix} = \det M \det \begin{pmatrix} \frac{D}{2} + \frac{\sqrt{D}}{2} & 1 \\ \frac{D}{2} - \frac{\sqrt{D}}{2} & 1 \end{pmatrix}.$$

Furthermore, $\det M = \pm NA$ because its absolute value is the index $[\mathcal{O} : A]$. Thus,

$$\det \begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix} = \pm \frac{NA}{\sqrt{D}}.$$

Plugging this into the formula for the discriminant gives our result. \square

In order to fix

$$\det \begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix} = +\frac{NA}{\sqrt{D}}$$

we notice that by interchanging α and β we switch the sign of the \sqrt{D} term. Thus for one choice of ordering we can require the plus sign here. Such a basis is called oriented.

Proposition 5.4. *The image of the map $(\alpha, \beta) \mapsto f_{\alpha, \beta}$ from oriented bases of ideals is all primitive (positive definite) quadratic forms with discriminant D .*

Proof. Suppose $Q = (a, b, c)$ is some primitive BQF with discriminant D (positive definite if $D < 0$). Let $A = 2a\mathbb{Z} + (b \pm \sqrt{D})\mathbb{Z}$ with the sign chose so that this basis is oriented. We assume for the moment that A is an ideal. Then

$$f_A(x, y) = \frac{1}{NA}N(2ax + (b \pm \sqrt{D}y)) = \frac{1}{NA}(4a^2 + 4abxy + 4acy^2).$$

Furthermore, we have already shown $NA = \gcd(4a^2, 4ab, 4ac) = 4|a|$ since Q is primitive. Therefore, $f_A = \pm Q$ and by looking at the sign of a one can easily see $f_A = Q$.

To complete the proof we need to prove that A is an ideal. To do this we need to show that multiplying each of the basis elements by $\frac{D+\sqrt{D}}{2}$ gives something in A . But

$$2a\frac{D+\sqrt{D}}{2} = 2a\frac{D-b}{2} + (b+\sqrt{D})a$$

and

$$(b+\sqrt{D})\frac{D+\sqrt{D}}{2} = 2ac + \frac{b+d}{2}(b+\sqrt{D}).$$

Since b and D have the same parity we're done. \square

All that remains to show is that this correspondence preserves the equivalence class structure. Notice that two oriented bases (α, β) and (α', β') are equivalent if and only if there exists some matrix $M \in \text{SL}_2(\mathbb{Z})$ and a fractional principal ideal $\alpha\mathcal{O}$ such that

$$\alpha M \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix}.$$

Notice that

$$(\alpha x + \beta y) = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}^T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix}^T M^{-T} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Letting

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = M^{-T} \begin{pmatrix} x \\ y \end{pmatrix}$$

we get that $f_{\alpha, \beta} \sim \pm f_{\alpha', \beta'}$ under the transformation M^{-T} where the sign comes from the sign of $N\alpha$. Similarly one can go the other way and one gets that the so called strong equivalence of ideals (where we require that the principal ideal taking one to the other has positive sign) corresponds to proper equivalence of BQFs.

6 Another Proof of the Nonvanishing of $L(1, \chi)$.

Lastly we give a proof of the nonvanishing of $L(1, \chi)$ for χ a nontrivial real Dirichlet series without proving the full class number formula. Notice that the quadratic forms argument showed that there was a nice Dirichlet series expansion of $\frac{L(s, \chi)L(s, \chi_0)}{L(2s, \chi_0)}$. If in fact $L(1, \chi) = 0$, then the lefthand side would be zero at $s = 1$. But the Dirichlet series expansion has only positive terms and its constant term is nonzero.

Theorem 6.1. *If χ is any nontrivial real Dirichlet character modulo m , $L(1, \chi) \neq 0$.*

Proof. Let

$$F(s) = \frac{L(s, \chi)L(s, \chi_0)}{L(2s, \chi_0)}.$$

Assume $L(1, \chi) \neq 0$. Thus $F(s)$ is holomorphic for $\sigma > \frac{1}{2}$. In addition $\lim_{s \rightarrow \frac{1}{2}} F(s) = 0$.

Since χ is real $\chi(p) = \pm 1$. Therefore,

$$L(s, \chi) = \prod_{p:\chi(p)=1} \frac{1}{1-p^{-s}} \prod_{p:\chi(p)=-1} \frac{1}{1+p^{-s}}.$$

Using the Euler factorization for $L(s, \chi_0)$ we get,

$$F(s) = \prod_{p:\chi(p)=1} \frac{1-p^{-2s}}{(1-p^{-s})^2} \prod_{p:\chi(p)=-1} \frac{1-p^{-2s}}{(1+p^{-s})(1-p^{-s})} = \prod_{p:\chi(p)=1} \frac{1+p^{-s}}{1-p^{-s}}.$$

For $\sigma > 1$ we can expand this as a Dirichlet series $F(s) = \sum_n a_n n^{-s}$ where each a_n is nonnegative and $a_1 = 1$ (in fact the Dirichlet series is our old friend 2^μ). Since $F(s)$ is holomorphic in the region $\sigma > \frac{1}{2}$ it has a power series about 2 with radius at least $\frac{3}{2}$. That is to say, $F(s) = \sum_{m=0}^{\infty} \frac{F^{(m)}(2)}{m!} (s-2)^m$. We can explicitly compute the terms of this power series using our Dirichlet series expansion. That is to say,

$$F^{(m)} = \sum_{n=1}^{\infty} a_n (\log n)^m n^{-2} = (-1)^m b_m,$$

where $b_m \geq 0$ and $b_0 \geq a_1 = 1$. Therefore,

$$F(s) = \sum_{m=0}^{\infty} \frac{b_m}{m!} (2-s)^m.$$

Therefore, for real $s \in (\frac{1}{2}, 2)$, $F(s) \geq F(2) \geq b_0 \geq 1$, this contradicts the fact that $\lim_{s \rightarrow \frac{1}{2}} F(s) = 0$. \square