Lecture # 1: Euler factorization, the ζ-function, and the distribution of primes.

Noah Snyder

June 24, 2002

1 Some Elementary Results on the Distribution of Primes

The beginning of Analytic Number Theory can be traced to a paper of Euler's. His investigations began with one of the oldest and most important questions in number theory: "How many primes are there?" For example, on average how many primes are in a given interval of the integers? How far can this distribution vary from the average? How random is this distribution?

A few of these questions can be answered with completely elementary methods. For example, it is easy to see that sequences of the form $(n!+2, n!+3, n!+4, ..., n!+n)$ show that there are arbitrarily long gaps between prime numbers. In contrast is the following result due to Euclid:

Theorem 1.1 (Euclid). *There are infinitely many primes.*

Proof. Suppose there were finitely many primes, $p_1, p_2, \dots p_n$. Then consider the number

$$Q = p_1 \cdots p_n + 1.$$

Clearly this number is not divisible by any prime. But it is also bigger than 1 and so (by descent) must be divisible by some prime. This is a contradiction, therefore there must be infinitely many primes. □

Although this method is certainly adequate to show that there are infinitely many primes, it does not seem to show that there are very many primes, because Q is a relatively large number compared to p_n. To quantify such questions of how the primes distributed, we introduce the following functions:

Definition 1.2. *Let $\pi(x)$ be the number of positive primes less than or equal to x. Let p_n be the nth positive prime.*

Euclid's result, therefore, says that $\lim_{x\to\infty} \pi(x) = \infty$, or, alternately, that p_n is actually defined for all positive n. On the other hand, the result on composites mentioned above says that $\limsup_{n\to\infty} p_n - p_{n-1} = \infty$, or, alternately, that for any n, $\pi(x+n) = \pi(x)$ for infinitely many x.

It will also be very useful to have good notation for approximating the growth of functions.

Definition 1.3. *We say that $f(x) = g(x) + O(h(x))$ if $\frac{f(x)-g(x)}{h(x)}$ is bounded as $x \to \infty$. We say that $f(x) = g(x) + o(h(x))$ if $\frac{f(x)-g(x)}{h(x)}$ goes to zero as $x \to \infty$. We say that $f(x) \sim g(x)$ if $\frac{f(x)}{g(x)}$ goes to 1 as $x \to \infty$.*

Occasionally we will also use these same notations for different limit points (usually as x approaches 0 or 1). Notice that $f(x) \sim g(x)$ is the same as saying $f(x) = g(x) + o(g(x))$. Also notice that $\sim$ (which is called asymptotic equality) is an equivalence relation.

A closer look at Euclid's result allows us to get slightly stronger information on the growth of $\pi(x)$ and p_n.

Proposition 1.4. $p_n < e^{e^n}$. *Hence, $\pi(x) > \log\log x$.*

Proof. This theorem is obvious if $n = 1$. If $n > 1$, Euclid's construction actually says that

$$p_n \leq p_1 \cdot p_2 \cdots p_{n-1} + 1 \leq kp_1 \cdot p_2 \cdots p_{n-1}$$

for any $\frac{7}{6} < k$. Combining the first n such equations, we see that:

$$p_n \leq kp_1 \cdot p_2 \cdots p_{n-1} \leq k^2(p_1 \cdots p_{n-2})^2 \leq k^4(p_1 \cdots p_{n-3})^4 \leq \ldots \leq (2k)^{(2^n)}.$$

Clearly we can pick k such that $2k < e$. □

This result shows that, for example, there are at least 2 primes smaller than 100 or that there are at least 3 primes less than $10,000$. This is clearly a horrible underestimate as $\pi(100) = 25$ and $\pi(10,000) = 1,229$.

There are other classical proofs of the infinitude of primes based on similar constructive methods which give similar bounds. For example, consider Goldbach's proof of Proposition 1.4:

Consider the Fermat numbers, $F_n = 2^{2^n} + 1$. Fermat claimed that these were all prime, but Euler found a counterexample. However, they can still be used to prove the infinitude of primes because of the following lemma:

Lemma 1.5. $\gcd(F_n, F_m) = 1$ *so long as n and m are distinct.*

Proof. Without loss of generality, take $n < m$. Suppose some prime p divides both F_n and F_m. Then $-1 \equiv 2^{2^n} \pmod{p}$ and $-1 \equiv 2^{2^m} \pmod{p}$. Squaring the first equation $m - n$ times shows that $1 \equiv 2^{2^m} \pmod{p}$, which contradicts the second equation (clearly p must be odd since all the Fermat numbers are odd). Therefore, all the Fermat numbers are pairwise relatively prime. □

Now we can conclude another proof of Proposition 1.4 using this lemma. If all the Fermat numbers were relatively prime, then each must be divisible by a different prime from all the others. So, $p_n \leq F_n = 2^{2^n} + 1$. Thus, we have $\pi(x) > \log \log x$.

Challenge 1. *Find other elementary proofs of the prime number theorem and see if any of them give a substantively better bound on the growth of π.*

2 Euler Factorization

Obviously we would like to find a much better lower bound for $\pi(x)$ than $\log \log x$. The first proof of the infinitude of primes which allows us a substantively better bound is Euler's proof which can be found in his book *Introduction to Analysis of the Infinite.* Here he actually shows that $\sum_{p \text{ prime}} 1/p$ diverges.

Since $\sum_{n=1}^{\infty} e^{-e^n}$ clearly converges extremely rapidly, Euler's result will give us a substantively better estimate on the growth of $\pi(x)$. Furthermore, the argument itself is exceptional because it does not use constructive algebraic arguments like Euclid's and Goldbach's, but rather an argument based on the properties of a certain analytic function. Euler argued as follows:

"Let us consider the expression

$$\frac{1}{(1 - \alpha z)(1 - \beta z)(1 - \gamma z) \cdots}.$$

"When the division is carried out, we obtain the series $1 + Az + Bz^2 + Cz^3 + \ldots$. It is clear that the coefficients A, B, C, etc. depend on the numbers α, β, γ, etc. in the following way: A is the sum of the sum of the numbers taken singly; B is the sum of the products taken two at a time; C is the sum of the products taken three at a time, etc., where we do not exclude products of the same factor.

"If for α, β, γ, etc. we substitute the reciprocals of some power of all the primes and let

$$P = \frac{1}{\left(1 - \frac{1}{2^n}\right)\left(1 - \frac{1}{3^n}\right)\left(1 - \frac{1}{5^n}\right) \cdots},$$

then $P = 1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \ldots$, where all natural numbers occur with no exception.

"Because we can express the sum of the series $P = 1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \ldots$ as a product of factors, it is convenient to use logarithms. We have

$$\log P = -\log\left(1 - \frac{1}{2^n}\right) - \log\left(1 - \frac{1}{3^n}\right) - \log\left(1 - \frac{1}{5^n}\right) - \ldots.$$

"If we use natural logarithms, then

$$\log P = 1\left(\frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{5^n} + \ldots\right) + \frac{1}{2}\left(\frac{1}{2^{2n}} + \frac{1}{3^{2n}} + \frac{1}{5^{2n}} + \ldots\right)\ldots$$

"If $n = 1$, then $P = 1 + \frac{1}{2} + \frac{1}{3} + \ldots = \log(\frac{1}{1-1}) = \log(\infty)$. Then

$$\log\log\infty = 1\left(\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \ldots\right) + \frac{1}{2}\left(\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{5^2} + \ldots\right) + \ldots$$

"But these series, except for the first ones, not only have finite sums, but the sum of all of them taken together is still finite, and reasonably small. It follows that the first series $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{5} + \ldots$ has an infinite sum." (Chapter XV of Euler's *Introduction to the Analysis of the Infinite.*)

As is to be expected, Euler's argument lacks rigor at a few points, but in this case the questionable steps are easy to identify and deal with. First we need to place the series which he discusses on a firmer foundation.

Proposition 2.1. *The series*

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

converges uniformly on the interval $[c, \infty)$ *for any* $c > 1$.

Proof. Since n^{-s} is monotonically decreasing for positive s, for any N and M and any $s \geq c > 1$,

$$\sum_{n=N}^{M} n^{-s} \leq \int_N^\infty x^{-s} dx = \frac{N^{1-s}}{s-1} < \frac{1}{c-1},$$

which shows uniform convergence. □

The key step in Euler's proof is the following fact known as the Euler factorization of the zeta function.

Proposition 2.2. *The product* $\prod_p \frac{1}{1-p^{-s}}$ *converges uniformly on the interval* $[c, \infty)$ *for any* $c > 1$. *(Here as always we use the notation* $\prod_p$ *(resp.* $\sum_p$*) to denote a product (resp. sum) over all positive primes.) Furthermore for* $s > 1$,

$$\prod_p \frac{1}{1-p^{-s}} = \zeta(s).$$

Proof. The important points are that $\frac{1}{1-p^{-s}} = \sum_{k=0}^\infty p^{-ks}$ and that every positive integer factors uniquely as a product of prime powers. We consider the finite product,

$$\prod_{p<N} \sum_{k=0}^{\infty} p^{-ks} = \sum_{n \in S_N} n^{-s},$$

where S_N is the set of all integers which are products of primes less than N. But clearly $[1, N) \subseteq S_N$. Therefore,

$$\left| \prod_{p<N} \sum_{k=0}^{\infty} p^{-ks} - \sum_{n<N} n^{-s} \right| = \varepsilon(N, s) < \sum_{n>N} n^{-s} < sN^{1-s}. \tag{2.1}$$

Since the right hand side goes to zero as N gets large, uniformly on the interval $[c, \infty)$ for any $c > 1$, our theorem is proved. □

These two results combine to give us the key formula in the middle of Euler's argument:

$$\log \zeta(s) = \sum_p -\log\left(1 - \frac{1}{p^s}\right). \tag{2.2}$$

Using the Taylor expansion for log is legitimate here because $0 < 1 - \frac{1}{p^s} < 1$, and we can exchange the order of summation because all the series involved converge uniformly and absolutely. Therefore, we find that

$$\begin{aligned}\log \zeta(s) &= \sum_p \sum_{n=1}^{\infty} \frac{1}{np^n s} = \sum_{n=1}^{\infty} \frac{1}{n} \sum_p \frac{1}{p^n s} \\ &= \sum_p \frac{1}{p^s} + \sum_{n=2}^{\infty} \frac{1}{n} \sum_p \frac{1}{p^n s}. \end{aligned} \tag{2.3}$$

Thus far we have simply been rephrasing Euler's arguments in the language of modern analysis. The point where we need to do extra work is at the end. Essentially, we want to take the limit as $s \to 1$. Then the left hand side blows up, while the right hand side consists of the series we're interested in plus some finite part. But, unlike Euler, we can not say the left hand side is $\log\log\infty$.

We can, however, still conclude that

$$\lim_{s\to 1^+} \sum_p \frac{1}{p^s} + \sum_{n=2}^{\infty} \frac{1}{n} \sum_p \frac{1}{p^n s}$$

cannot be finite.

First, we want to show that the terms with $k > 1$ on the right hand side of Equation 2.3 are small under the same limit. This is just another simple integral test:

$$\begin{aligned}\sum_{n=2}^{\infty} \frac{1}{n} \sum_p \frac{1}{p^{ns}} &< \int_2^{\infty} \int_2^{\infty} x^{-1} y^{-sx} dy dx = \int_2^{\infty} s^{-1} x^{-2} 2^{-sx} dx \\ &< \frac{1}{4s} \int_2^{\infty} 2^{-sx} dx = \frac{1}{8s^2} 2^{-2s} < \frac{1}{32}.\end{aligned}$$

So clearly the sum of the rest of the series converges in the limiting case, just as Euler claimed. This implies that $\lim_{s\to 1^+} \sum_p \frac{1}{p^s}$ cannot be finite.

Theorem 2.3 (Euler). $\displaystyle\sum_p \frac{1}{p}$ *diverges.*

Proof. For the sake of contradiction, suppose that $\lim_{N\to\infty} \sum_{p<N} p^{-1}$ were actually finite. Then $\sum_{p>N} p^{-1}$ would give a uniform bound on the term $\sum_{p>N} \frac{1}{p^{-s}}$. Hence, $\sum_p \frac{1}{p^{-s}}$ would converge uniformly for all $s \geq 1$.

Thus the interchange of limits would be valid, and

$$\lim_{N\to\infty} \sum_{p<N} \frac{1}{p^{-1}} = \lim_{N\to\infty} \lim_{s\to 1^+} \sum_{p<N} \frac{1}{p^{-s}} = \lim_{s\to 1^+} \lim_{N\to\infty} \sum_{p<N} \frac{1}{p^{-s}} = \lim_{s\to 1^+} \sum_p \frac{1}{p^s}$$

would also be finite. This is clearly a contradiction. □

This proves the theorem which Euler set out to prove. Already this result shows powerful things such as, p_n grows faster on average than n^r does for any $r > 1$. However, Euler claimed something stronger. Not only did he say that $\sum_p \frac{1}{p}$ diverged, he claimed that it was $\log\log\infty$. By this expression Euler seems to mean, in modern notation, that

$$\sum_{p<N} \frac{1}{p} = \log\log N + O(1).$$

In order to prove this result using Euler's methods, we would simply have to show that the Euler factorization was approximately valid for a finite sum and $s = 1$, i.e.

$$\left| \prod_{p<N} \frac{1}{1-p^{-1}} - \sum_{n<N} n^{-1} \right| < \varepsilon(N, 1)$$

for some nice error function. Alas, a little computation shows that this claim is not true at all. Our computation in Theorem 2.2 shows that the error function $\varepsilon(N, s)$ does not behave well as $s \to 1$.

In order to prove this result we will need a bit more information about the $\zeta(s)$ near $s = 1$. For many of Euler's papers in which he considers the Euler factorization and functions like his ζ-function, rather than considering the series, $\zeta(s) = \sum_n n^{-s}$, he instead looks at an alternating series:

Definition 2.4. $\tilde{\zeta}(s) = \sum_n (-1)^{n+1} n^{-s}$.

This new series has the distinct advantage of converging (conditionally) for all $s > 0$ by the alternating series test. If we group terms in pairs, then the series actually converges absolutely for all $s > 0$.

This new function also has an Euler factorization:

$$\begin{aligned}\tilde{\zeta}(s) = \sum_n (-1)^n n^{-s} &= (1 - 2^{-s} - 4^{-s} - \ldots)(1 + 3^{-s} + 9^{-s} - \ldots)(1 + 5^{-s} + 25^{-s} - \ldots)\ldots \\ &= \left(2 - \frac{1}{1-2^{-s}}\right) \prod_{p\neq 3} \left(\frac{1}{1-p^{-s}}\right). \qquad (2.4)\end{aligned}$$

This factorization is very similar to that of the old ζ-function. In fact, we have the formula

$$\zeta(s) = \frac{\frac{1}{1-2^{-s}}}{2 - \frac{1}{1-2^{-s}}} \tilde{\zeta}(s) = \frac{1}{2 - 2^{1-s} - 1} \tilde{\zeta}(s) = \frac{1}{1 - 2^{1-s}} \tilde{\zeta}(s).$$

This new expression for $\zeta(s)$ now makes sense for any $s > 0$ except for $s = 1$ where it clearly blows up. This lets us get a much firmer grasp on the behavior of ζ near 1.

Theorem 2.5. *(cf. Janusz's Number Fields, pp. 144-145)*

$$\lim_{s\to 1} (s-1)\zeta(s) = 1.$$

Proof. If we write

$$(s-1)\zeta(s) = \frac{s-1}{1-2^{1-s}} \tilde{\zeta}(s),$$

the limit as $s \to 1$ actually makes sense. By a standard result from analysis, $\lim_{s\to 1} \tilde{\zeta}(s) = \log 2$. By L'hôpital's rule,

$$\lim_{s\to 1} \frac{s-1}{1-2^{1-s}} = \frac{1}{\log 2}.$$

Thus, $\lim_{s\to 1} (s-1)\zeta(s) = 1$. □

Therefore, by Theorem 2.5, if we consider the series

$$(1-s)\zeta(s) = \sum_n \frac{1-s}{n^s},$$

it will converge uniformly in s for $s \in [1, \infty)$. Hence the error term $(1 - s)\varepsilon(N, s)$ actually does remain bounded as $s \to 1$. Thus we have shown,

Lemma 2.6.

$$\lim_{s\to 1}(1-s)\left|\prod_{p<N}\frac{1}{1-p^{-1}}-\sum_{n<N}n^{-s}\right| < \lim_{s\to 1}\varepsilon(N,s) < \varepsilon(N),$$

for some error function $\varepsilon(N)$ which goes to zero as N gets large.

□

Theorem 2.7.

$$\sum_{p<N}\frac{1}{p} = \log\log N + O(1).$$

Proof. By the lemma for all N and $s>1$,

$$(s-1)\prod_{p<N}\frac{1}{1-p^{-1}} = (s-1)\sum_{n<N}n^{-s} + O(1),$$

where by $O(1)$ we mean the error is bounded as $N\to\infty$ and as $s\to 1^+$. If we take logs of both sides and use an earlier lemma,

$$\log(s-1) + \sum_{p<N}p^{-s} = \log(s-1) + \log\sum_{n<N}n^{-s} + O(1).$$

Now we can cancel the $\log(1-s)$ terms and the terms we are left with are all bounded as $\lim_{s\to 1}$. Thus,

$$\sum_{p<N}\frac{1}{p} = \log\sum_{n<N}n^{-1} + O(1) = \log\log N + O(1).$$

□

Clearly it follows that there are infinitely many primes. In fact, we can extract from this theorem a very good idea of how fast $\pi(x)$ and p_n grow.

We will extend p_n to some monotonic real valued function p_x to get

$$\int_1^X \frac{1}{p_x}dx = \log\log X + O(1). \tag{2.5}$$

We would really like to "differentiate" this equation to get something like

$$\frac{1}{p_x} \approx \frac{d}{dx}\log\log x = \frac{1}{\log x}\frac{1}{x}.$$

This would imply that $p_x \approx x\log x$. However, although integrating preserves estimates, differentiating clearly does not. (For example, consider the fact that $x\sin x = O(x)$, but $\sin x + x\cos x = \frac{d}{dx}x\sin x \neq O(1)$.)

What this does tell us though is that p_n can not grow *significantly faster* than $n\log n$. Similarly, we can see that $\pi(x)$ can not grow significantly slower than $\frac{x}{\log x}$.

This phrase "significantly faster" (resp. slower) can mean any of a number of things, for example,

Proposition 2.8. *For any constant $k>1$ and N, there exists some $n>N$, $p_n \geq kn\log n$.*

Proof. Suppose to the contrary that for some constants $k<1$ and N, $p_n < kn\log n$ for all $n>N$. Thus, if $n>N$,

$$\frac{1}{p_n} < \frac{1}{k}\frac{1}{n\log n}.$$

Integrating yields

$$\sum_{N<n<x} p_n < \frac{1}{k}(\log\log x - \log\log N)$$

for all $x > N$. But by Equation 2.5, this means that for some constant c,

$$\log\log x < c - \frac{1}{k}(\log\log N) + \frac{1}{k}(\log\log x).$$

Since $k > 1$, this last equation is clearly false for large enough x. □

To show a more concrete result, like $p_n \sim n \log n$, one would need to prove something stronger about the smoothness of p_n.

It is worth noting that simply showing that there are infinitely many primes does not require any of the above arguments. We can simply note that if there were finitely many primes, then, by looking at the supposed finite Euler factorization, $\lim_{s\to 1} \zeta(s)$ would be finite.

Throughout this course we will try to emulate Euler's argument, by finding a connection between number theoretic information and analytic functions and then extracting more and more number theoretic information from better and better results concerning these analytic functions.

Lecture # 2: Dirichlet L-functions, Dirichlet Characters and primes in arithmetic progressions.

Noah Snyder

June 26, 2002

1 Elementary Results on Primes in Arithmetic Progressions

Dirichlet considered a question very similar to the one which inspired Euler's introduction of the ζ-function: namely, how the primes are distributed modulo m. The simplest question of this type is whether are there infinitely many primes congruent to a modulo m. Obviously there can only be infinitely many primes of this form if a and m are relatively prime. Unfortunately, this problem turned out to be much more difficult than proving that there are infinitely many primes. Elementary results along the lines of Euclid's proof only sufficed to show very special cases. For example,

Proposition 1.1. *There are infinitely many primes* $p \equiv 3 \pmod 4$.

Proof. Suppose there were only finitely many such primes, $p_1, p_2, \ldots, p_n$. Consider the number

$$Q = 4p_1p_2\ldots p_n - 1.$$

Clearly this number is not divisible by any of the primes which are 3 modulo 4. Thus, $Q \equiv 3 \pmod 4$ is a product of primes all of which are 1 modulo 4. This is clearly a contradiction. □

Proposition 1.2. *There are infinitely many primes* $p \equiv 1 \pmod 4$.

Proof. Here we use the fact from basic number theory that -1 is a square modulo p exactly when $p \equiv 1 \pmod 4$. Again, suppose there were only finitely many primes $p_1, p_2, \ldots, p_n \equiv 1 \pmod 4$. Let

$$Q = (2p_1p_2\ldots p_n)^2 + 1.$$

Clearly Q is not divisible by any of the primes which are 1 modulo 4. Since $-1 \equiv (p_1p_2\ldots p_n)^2 \pmod Q$, any prime which divides Q must be 1 modulo 4. Again, this is a contradiction. □

Although similar methods will work for $m = 3$ or $m = 6$, they are doomed to failure in general. The above arguments generalize only to the following two results:

Proposition 1.3. *Suppose H is a proper subgroup of the group of units $(\mathbb{Z}/m\mathbb{Z})^\times$. Then there exist infinitely many primes which are not in H when reduced modulo m.*

Proof. Suppose there were only finitely many such primes, $p_1, p_2, \ldots, p_n$. Consider the number

$$Q = mp_2 \cdot p_3 \cdots p_n + p_1.$$

Clearly this number is not divisible by any of the primes which are not in H. Thus, $Q \equiv x \pmod m$ is a product of primes all of which are in H. This is clearly a contradiction. □

Proposition 1.4. *There are infinitely many primes congruent to* 1 *modulo m for any m.*

Proof. Let $\Phi_m(x)$ be the mth cyclotomic polynomial (that is the minimal polynomial of a primitive mth root of unity). Suppose there are finitely many primes $p_1, p_2, \ldots, p_n \equiv 1 \pmod m$. Let $N = m \cdot p_1 \cdot p_2 \cdots p_n$. Consider $\Phi_m(N)$. Suppose that a prime q divides $\Phi_m(N)$. Then, modulo q, we must have a primitive mth root of unity. Therefore, $q \equiv 1 \pmod m$. Thus $q = p_i$ for some i. However, none of the p_i can divide $\Phi_m(N)$. This is a contradiction. □

In fact, using class field theory, one can show that it is impossible to find a polynomial which outputs only numbers divisible by primes congruent to $a \pmod{m}$ for a general relatively prime pair a and m.

Rather than trying to use these sorts of elementary proofs, Dirichlet instead tried to adapt Euler's analytic methods to this situation.

2 A Special Case of Dirichlet's Theorem

In particular, Dirichlet wanted to prove

Theorem 2.1. *For any relatively prime positive integers a and m, the series*

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p}$$

diverges.

Let us first consider the particular case $m = 4$. Since we will consider things more rigorously in the general case, here we shall be a bit lax.

The most obvious attempt at modifying Euler's method is to consider the function

$$f_1(s) = \prod_{p \equiv 1\ (4)} \frac{1}{1 - p^{-s}}.$$

By the same arguments as used the last section we can conclude that

$$\sum_{p \equiv 1\ (4)} p^{-s} = \log f_1(s) + O(1).$$

Unfortunately, $f_1(1)$ does not obviously diverge. If we multiply out the Euler product, we see that

$$f_1(s) = \sum_{n \in S} n^{-s},$$

where S is the set of all numbers which are products of primes which are 1 modulo 4. This is entirely unhelpful. We need to find some functions whose Euler factorizations depend only on what the prime is modulo 4, and where the terms in the series do not depend on the prime factorization of n.

Dirichlet's insight was to look at the functions

$$L_1(s) = \sum_{n \text{ odd}} (-1)^{\frac{n-1}{2}} n^{-s} = \prod_{p \equiv 1\ (4)} \frac{1}{1 - p^{-s}} \prod_{p \equiv 3\ (4)} \frac{1}{1 + p^{-s}}$$
$$L_0(s) = \sum_{n \text{ odd}} n^{-s} = \prod_{p \equiv 1\ (4)} \frac{1}{1 - p^{-s}} \prod_{p \equiv 3\ (4)} \frac{1}{1 - p^{-s}} = (1 - 2^{-s})\zeta(s).$$

Just as in the last section, we can take logarithms and use the Taylor series expansion. As in the last section the contribution from quadratic and higher terms in the Taylor series are bounded. Thus,

$$\log L_1(s) = \sum_{p \equiv 1\ (4)} p^{-s} - \sum_{p \equiv 3\ (4)} p^{-s} + O(1)$$
$$\log L_0(s) = \sum_{p \equiv 1\ (4)} p^{-s} + \sum_{p \equiv 3\ (4)} p^{-s} + O(1)$$

Therefore,

$$\frac{1}{2}(\log L_0(s) + \log L_1(s)) = \sum_{p \equiv 1\ (4)} p^{-s} + O(1)$$
$$\frac{1}{2}(\log L_0(s) - \log L_1(s)) = \sum_{p \equiv 3\ (4)} p^{-s} + O(1)$$

Thus in order to prove this special case of Theorem 2.1, we need only show that $\log L_0(s) + \log L_1(s)$ and $\log L_0(s) - \log L_1(s)$ are both unbounded as $s \to 1^+$. Obviously $(1 - 2^{-s})\zeta(s)$ blows up at $s = 1$. Hence we've reduced this problem to showing that $\log L_1(1)$ is finite.

But, $L_1(s)$ is an alternating series; thus, we can bound it by the first two partial sums, i.e. $\frac{2}{3}3^{-s} < L_1(s) < 1$. Thus $\log \frac{2}{3} < \log L_1(1) < 0$, so we have proved Theorem 2.1 for the case of $m = 4$.

3 Some General Results on Dirichlet Series

Before we attack the general proof of Theorem 2.1, it will be useful to have a few technical definitions and results.

Definition 3.1. *A Dirichlet series is a series of the form,*

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

where a_n is some sequence of complex numbers.

We will want to know when a Dirichlet series actually converges. In order to prove this, we will need the following theorem which is the analog for sums of integration by parts.

Theorem 3.2 (Abel Summation Formula or Summation by Parts). *Suppose (a_n) and (b_n) are two sequences. Then $\sum_{n=\ell}^{N} a_n(b_n - b_{n-1}) = a_N b_N - a_\ell b_\ell - \sum_{n=\ell}^{N} b_{n-1}(a_n - a_{n-1})$.*

Proof. To verify this theorem, we simply check that each term $a_i b_j$ occurs with the same multiplicity on both sides. □

Using the notion of a Stieltjes integral we can rewrite the Abel Summation Formula as a generalization of integration by parts.

Definition 3.3. *Let α be a non-decreasing (not necessarily continuous function) on $[a, b]$ and f a function bounded on $[a, b]$. Let P be some partition of $[a, b]$, let $\Delta\alpha_i = \alpha(x_i) - \alpha(x_{i-1})$. Define the upper and lower sums, $U(P, f, \alpha) = \sum_{i=1}^{n} M_i \Delta\alpha_i$ and $U(P, f, \alpha) = \sum_{i=1}^{n} m_i \Delta\alpha_i$, where M_i and m_i are the maximum and minimum respectively of f on the ith interval in the partition. We define the upper and lower Stieltjes integrals to be $\overline{\int_a^b} f d\alpha = glb\ U(P, f, \alpha)$ and $\underline{\int_a^b} f d\alpha = lub\ U(P, f, \alpha)$. If the upper and lower integrals are equal we denote their common value by $\int_a^b f d\alpha$ and say that f is integral with respect to α.*

For our purposes we will only be looking at Stieltjes integrals where either α is differentiable in which case $\int_a^b f d\alpha = \int_a^b f(x)\alpha'(x)dx$ or when α is a step function. In the latter situation the integral is simply a sum over the jumps of the value of the function at that jump times the size of the jump. For example, $\int_a^b f d\lfloor x \rfloor = \sum_{n \in \mathbb{Z} \cap (a,b)} f(n)$. Lastly in the case of α a step function, we shall always take the value of α at each jump to be halfway between the values on either side. Although this is simply a convention, later on it will hopefully become clear why it is such a useful one.

In the context of a Stieltjes integral, summation by parts is simply a special case of integration by parts which holds for all Stieltjes integrals. (This is slightly misleading, in reality one *uses* summation by parts to *prove* this general integration by parts formula.) Generally we will prefer to write things as Stieltjes integrals and use integration by parts, but occasionally we will directly refer to Abel Summation.

Proposition 3.4. *If $\sum a_n n^{-s_0}$ converges, then the Dirichlet series $f(s, a_n)$ converges for all complex numbers s with $Re(s) > s_0$. In fact, this convergence is uniform in any wedge to the right of the point s_0: $\{s : Re(s) > Re(s_0)$ and $0 < \frac{|s-s_0|}{Re(s-s_0)} < M\}$, where M is an arbitrary positive constant. (Since this convergence is uniform, $f(s, a_n)$ is analytic on that region.)*

Proof. Letting M grow arbitrarily shows that the second assertion implies the first. Without loss of generality, we can assume $s_0 = 0$ (since we can look at the Dirichlet series $\sum_n (a_n n^{-s_0}) n^{-s}$). Also, without loss of generality, we can subtract off the first term a_1 and so assume $a_1 = 0$.

Since we are assuming that $\sum_n a_n$ converges for any $\varepsilon > 0$, there exists an integer N such that for any $\ell, m > N$, $|A_{\ell,m}| < \epsilon$.

We want to get a good bound on $|\sum_{n=\ell}^m a_n n^{-s}|$. By Abel's summation formula,

$$\left|\sum_{n=\ell}^{m} a_n n^{-s}\right| = \left|A_{\ell,m} b_m - \sum_{n=\ell}^{m} A_{\ell,m}((n+1)^{-s} - n^{-s})\right| < \epsilon \left(1 + \sum_{n=\ell}^{m} \left|e^{-s\log n} - e^{-s\log(n+1)}\right|\right).$$

To get a bound on that last term, we notice that for any $\alpha > \beta \geq 0$,

$$e^{-\alpha z} - e^{-\beta z} = z \int_{\alpha}^{\beta} e^{-tz} dt.$$

Therefore,

$$\left|e^{-\alpha z} - e^{-\beta z}\right| \leq |z| \int_{\alpha}^{\beta} e^{-t\mathrm{Re}(z)} dt = \frac{|z|}{\mathrm{Re}(z)} \left(e^{-\alpha \mathrm{Re}(z)} - e^{-\beta \mathrm{Re}(z)}\right).$$

Applying this to our particular case, we see that

$$\begin{aligned}\left|\sum_{n=\ell}^{m} a_n n^{-s}\right| &< \epsilon \left(1 + M \sum_{n=\ell}^{m} e^{-\mathrm{Re}(s)\log n} - e^{-\mathrm{Re}(s)\log(n+1)}\right) \\ &= \epsilon \left|1 + M(e^{-\mathrm{Re}(s)\log \ell}) - e^{-\mathrm{Re}(s)\log(m)}\right| < \epsilon(1+M).\end{aligned}$$

Thus for large enough N, this goes to zero independently of s, so the series converges uniformly in this region. □

It turns out that if a function can be written as a Dirichlet series then it can be done so in only one way.

Proposition 3.5. *cf. [?, Thm. 11.4] Suppose that $\sum_n \frac{a_n}{n^s} = 0$ on some right halfplane Re$(s) > \sigma_0$. Then, $a_n = 0$ for all n. Therefore, if we have two Dirichlet series with $\sum_n \frac{b_n}{n^s} = \sum_n \frac{c_n}{n^s}$ for all Re$(s) > \sigma_0$, then $b_n = c_n$ for all n.*

Proof. Without loss of generality, by considering $a_n n^{-\sigma_0}$ we can assume that $\sigma_0 = 0$. Thus, in order to have $\sum_n \frac{a_n}{n^s}$ converge near $s = 0$, we must have $a_n = O(1)$. Now suppose that a_N is the first non-zero term. Then

$$0 = a_N N^{-s} \left(1 + \sum_{n \geq N} \frac{a_n}{a_N} \left(\frac{n}{N}\right)^{-s}\right).$$

Multiplying by N^s we get

$$0 = a_N \left(1 + \sum_{n \geq N} \frac{a_n}{a_N} \left(\frac{n}{N}\right)^{-s}\right).$$

Now send $s \to +\infty + 0i$. Each of the terms in the sum dies exponentially. Therefore, since the coefficients are bounded, the whole sum dies. Therefore, $0 = a_N$. This is a contradiction; therefore, $a_n = 0$ for all n.

For the second conclusion, we simply consider the Dirichlet series $\sum_n \frac{b_n - c_n}{n^s} = 0$, from which it follows that $b_n - c_n = 0$ and thus $b_n = c_n$ for all n. □

Definition 3.6. *A sequence a_n is called multiplicative if $a_n a_m = a_{nm}$ for all relatively prime positive integers n and m. Similarly, a sequence a_n is called strongly multiplicative if $a_n a_m = a_{nm}$ for all pairs of positive integers.*

Theorem 3.7. *If a_n is multiplicative then the Dirichlet series $f(s, a_n)$ has the Euler factorization:*

$$f(s, a_n) = \prod_p \sum_{\ell=1}^{\infty} \frac{a_{p^k}}{p^{sk}}.$$

Furthermore if a_n is strongly multiplicative, summing this geometric series we see that

$$f(s, a_n) = \prod_p \frac{1}{1 - \frac{a_p}{p^s}}.$$

Proof. The proof here is identical to the proof of Theorem **??**. □

Finally we have a formula for the product of two Dirichlet series.

Proposition 3.8. $f(s, a_n)f(s, b_n) = f(s, \sum_{d|n} a_d b_{\frac{n}{d}})$.

Proof. By definition,

$$f(s, a_n)f(s, b_n) = \sum_{m=1}^{\infty} \sum_{\ell=1}^{\infty} \frac{a_m b_\ell}{(m\ell)^s}.$$

Make a change of variables $n = m\ell$ and $d = m$ to get,

$$f(s, a_n)f(s, b_n) = \sum_{n=1}^{\infty} \sum_{d|n} \frac{a_d b_{\frac{n}{d}}}{n^s} = f(s, \sum_{d|n} a_d b_{\frac{n}{d}}).$$

□

4 Dirichlet's L-series

In order to generalize Dirichlet's argument from the case of $m = 4$ to a general m, we should look at all Dirichlet series with particularly nice Euler factorizations in which a_p depends only on what n is modulo m and vanishes when $p|m$. From our results above, it is clear that we should be looking at the series corresponding to sequences of the following form:

Definition 4.1. *Let a Dirichlet character modulo m be any function from $\chi:\ \mathbb{Z} \to \mathbb{C}$ with the properties:*

1. *If n and m are not relatively prime, then $\chi(n) = 0$.*
2. *If n and m are relatively prime, then $|\chi(n)| = 1$.*
3. *If n_1 and n_2 are any two positive integers, then $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$.*

If we restrict a Dirichlet character to $(\mathbb{Z}/m\mathbb{Z})^\times$ we get a homomorphism. (By abuse of notation, we will also call it $\chi:\ (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$.) Furthermore, if one considers any homomorphism $\chi:\ (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ it will be a Dirichlet character modulo k for any $m|k$. If χ is an injective homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \hookrightarrow \mathbb{C}^\times$, then we say that the corresponding Dirichlet character is a primitive character modulo m. The homomorphism sending everything to 1 and the corresponding Dirichlet character will both be called trivial.

The above notion of homomorphisms $\chi:\ (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ generalizes to the more general notion of an abelian group character, which is a homomorphism $\chi:\ G \to \mathbb{C}^\times$ where G is an abelian group.

As far as I can tell, the linguistic history of this term *character* is quite the opposite of what one might expect. The notion of a Dirichlet character came before the notion of a general character, and the name *character* seems to come from the fact that it is a generalization of the *quadratic character* that is the quadratic nature of a number modulo m.

Definition 4.2. *If χ is a Dirichlet character modulo m, then define the Dirichlet L-series*

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

If χ_0 is the trivial character modulo m, then obviously

$$L(s,\chi_0) = \prod_{p|m} \left(1 - \frac{\chi(p)}{p^s}\right) \zeta(s)$$

converges for any $\mathrm{Re}(s) > 1$.

For a nontrivial character, we certainly could get the same region of convergence since $\sum_n \chi(n) n^{-s} < \sum_n |\chi(n)| n^{-s}$. However, we might hope to find some cancellation and be able to find a larger region of convergence.

Lemma 4.3 (Dirichlet). *If G is an abelian group, and χ is a nontrivial character of that group, then*

$$\sum_{g \in G} \chi(g) = 0.$$

Proof. For any $h \in G$, notice that

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg).$$

But, as g runs over all of G, so does hg. Hence,

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g).$$

Therefore, either $\chi(h) = 1$ or $\sum_{g \in G} \chi(g) = 0$. Since χ is nontrivial, we can choose h so that the former condition is not true. Thus the lemma is proved. □

Corollary 4.4. *If χ is a nontrivial Dirichlet character modulo m, then $L(s,\chi)$ converges for $Re(s) > 0$.*

Proof. By Lemma 4.3, we know that $\sum_n \chi(n)$ is bounded. Thus, $\sum_n \chi(n) n^{-s}$ converges for any positive s, which by Proposition 3.4 is enough. □

5 Reducing Dirichlet's Theorem to an Analytic Theorem

Now that we have proved enough technical results, we can return to Dirichlet's original question. Following Euler, we notice that

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

Again the Taylor series expansion is valid, and our estimate on the terms still holds:

$$\left| \sum_{n=2}^{\infty} \frac{1}{n} \sum_p \frac{\chi(p)}{p^{ns}} \right| < \int_2^{\infty} \int_2^{\infty} x^{-1} y^{-sx} dy dx < \frac{1}{32}.$$

Therefore,

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

To get Dirichlet's result, we need to write $f_a(s) = \sum_{p \equiv a\ (m)} p^{-s}$ as a sum of $\log L(s,\chi)$ for various χ. We know that

$$\log L(s,\chi) = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a) f_a(s) + O(1).$$

In order to get this result, Dirichlet noticed and proved a finite analog of Fourier inversion called the orthogonality of characters.

Theorem 5.1 (Dirichlet). *If χ_1 and χ_2 are distinct characters of a finite abelian group G, then*

$$\sum_{g\in G} \chi_1(g)\chi_2(g)^{-1} = 0.$$

Furthermore, if we let G^* denote the dual group of characters of G, then, if $g \neq h$,

$$\sum_{\chi\in G^*} \chi(gh^{-1}) = 0.$$

Proof. The first assertion follows immediately from applying Lemma 4.3 to the character $\chi_1\chi_2^{-1}$. Together with the obvious fact that $\sum_{g\in G}\chi(g)\chi(g)^{-1} = |G|$, this implies that the matrix $(\frac{\chi(g)}{|G|})_{\chi,g}$ has orthogonal rows. By the structure theorem for finite abelian groups, it is easy to see that $|G| = |G^*|$ (since it is obvious for cyclic groups). Thus this matrix is a square matrix. By standard linear algebra we know that having orthogonal columns is the same as having orthogonal rows and the second half of the result follows. □

Thus by Theorem 5.1, we see that the characters χ are all linearly independent and thus form a basis of the space of all complex valued functions on G. In particular,

$$\frac{1}{|G|}\sum_{\chi\in G^*} \chi(h^{-1})\chi(g) = \begin{cases} 1 & \text{if g=h} \\ 0 & \text{otherwise} \end{cases}.$$

Therefore, if we let $G = (\mathbb{Z}/m\mathbb{Z})^\times$,

$$f_a(s) = \frac{1}{|G|}\sum_{\chi\in G^*} \chi(a^{-1})\log L(s,\chi) + O(1).$$

Since $\log L(1,\chi_0)$ blows up, and $\log L(1,\chi) < \infty$ for all nontrivial characters, all that remains is to show that $\log L(1,\chi) > -\infty$. That is to say, we have shown that Theorem 2.1 is equivalent to the following theorem:

Theorem 5.2 (Dirichlet). *If χ is a nontrivial Dirichlet character, then $L(1,\chi)\neq 0$.*

Proof. First we claim that for every m there is at worst one χ with $L(1,\chi) = 0$. Notice that

$$\sum_{\chi\in G^*}\log L(s,\chi) = \varphi(m)\sum_{k=1}^{\infty}\frac{1}{k}\sum_{p:\ p^k\equiv 1\ (m)} p^{-ks} > 0.$$

Now we already know that $\lim_{s\to 1^+}(s-1)L(s,\chi_0)$ is finite. Hence, $\log L(s,\chi_0) = \log\frac{1}{s-1} + O(1)$. But we know by Theorem 3.4 that for all the other $\chi\neq\chi_0$, $L(s,\chi)$ are analytic near 1. Therefore, for all of these, $\log L(s,\chi)$ either goes to $-\infty$ or is bounded.

Suppose one of these series, for instance $L(s,\tau)$, had a zero at 1. Since it is analytic, by considering the Taylor expansion, $\frac{L(s,\tau)}{s-1}$ is analytic and bounded at 1. Hence, $\log L(s,\tau) = -\log(s-1) + O(1)$. So, if we had $L(1,\tau_1) = L(1,\tau_2) = 0$, then

$$\sum_{\chi\in G^*}\log L(s,\chi) = \log(s-1) - 2\log(s-1) + \varepsilon(s),$$

where $\varepsilon(s)$ is either bounded or goes to $-\infty$ as $s\to 1^+$. Thus, the right hand side would be negative for small enough s, and we've reached a contradiction.

Notice that this proves the theorem for every character whose image is not contained in the reals. In this case there is a distinct character $\bar{\chi}(n) = \overline{\chi(n)}$ with $L(1,\chi) = 0 \iff L(1,\bar{\chi}) = 0$.

Furthermore, this shows that there is at worst 1 primitive Dirichlet character with $L(s,\chi) = 0$. If there were two, say one primitive modulo m_1 and the other primitive modulo m_2, then we could consider both of them as Dirichlet characters modulo m_1m_2. Thus their L-series modulo m_1m_2 would differ from the originals by only finitely many terms. Thus there would be two different Dirichlet L-series modulo $m_1 m_2$ with $L(1, \chi) = 0$, which is a contradiction.

So we have proven this theorem for all but one primitive character which must be real. Any real primitive character modulo m must have, for g a generator of $\mathbb{Z}/m\mathbb{Z}$, $\chi(g^k) = (-1)^k$. Clearly, this means $\chi(a)$ is 1 or -1 exactly when a is a square or a non-square respective. Thus, $\chi(a) = \left(\frac{a}{m}\right)$.

Dirichlet spent several years trying to prove that $L(1, \left(\frac{\cdot}{m}\right)) \neq 0$. Eventually he was able to prove this using his famous class number formula, which we will prove (in part) in a later lecture. In next week's homework we will give Dirichlet's proof in the special case of m is prime. Finally the next week in homework we will be giving a much faster modern proof of the general case. □

Lecture # 3: A Review of Fourier Analysis.

Noah Snyder

July 1, 2002

For a more in-depth presentation of this subject material, see any standard intermediate analysis textbook. For example, Lang's *Undergraduate Analysis* or *Real and Functional Analysis.* This particular treatment is adapted from Tom Brennan's notes on Analytic Number Theory.

1 Fourier Series

Suppose f is a continuous function of a real variable which is periodic with period one. These function can be identified with function on the unit circle. Fourier attempted to write such functions as a sum of simple functions like sines and cosines. In particular, suppose we could write

$$f(x) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi inx}.$$

To recover to coefficients a_n Fourier noticed that $\int_0^1 e^{2\pi inx}dx = \delta_{n0}$. Thus, $\int_0^1 \sum_{n\in\mathbb{Z}} a_n e^{2\pi inx}dx = a_0$, and

$$\int_0^1 \left(\sum_{n\in\mathbb{Z}} a_n e^{2\pi inx}\right) e^{-2\pi imx}dx = a_m.$$

Therefore, if one can express f as a sum of these exponentials, then

$$a_m = \int_0^1 f(x)e^{-2\pi imx}dx.$$

Definition 1.1. *The nth Fourier coefficient of f is $\hat{f}(n) = \int_0^1 f(x)e^{-2\pi inx}dx$.*

Our goal is to show that $\sum_{n\in\mathbb{Z}} \hat{f}(n)e^{2\pi inx}$ converges uniformly to f, so long as we put adequate conditions on f. Let $C^k(S^1)$ denote the k-times continuously differentiable functions of period 1.

Proposition 1.2. *For $f \in C^0(S^1)$, $\lim\limits_{|n|\to\infty} \hat{f}(n) = 0$.*

Proof. We can put the sup metric on $C^0(S^1)$. With this topology, $\lim\limits_{|n|\to\infty} \hat{f}(n)$ is a continuous function of f. Thus in order to show that it is 0 it is enough to show this on a dense subset. However, the space of linear combinations of characteristic functions of intervals is dense, hence it suffices to prove this theorem on this set. Furthermore, since $\lim\limits_{|n|\to\infty} \hat{f}(n)$ is linear, it is enough to show this fact for individual characteristic functions of intervals.

So consider $f(x)$ the characteristic function of the interval $[a, b]$. By the definition,

$$\hat{f}(n) = \int_a^b e^{-2\pi inx}dx = \frac{1}{-2\pi in}\left(e^{-2\pi inb} - e^{-2\pi ina}\right).$$

Therefore, $|\hat{f}(n)| < \frac{1}{\pi|n|}$. Thus, $\lim\limits_{|n|\to\infty} \hat{f}(n) = 0$. □

Definition 1.3 (The Dirichlet Kernel). *Let* $D_N(t) = \sum_{|n|\leq N} e^{2\pi int}$.

Notice that $D_N \in C^0(S^1)$ and that $\int_0^1 D_N(t)dt = 1$. Finally, by summing the geometric series and using a trig identity, we see

$$D_N(t) = \frac{\sin(2\pi(N+\frac{1}{2})t)}{\sin(\pi t)} = \cos(2\pi Nt) + \cot(\pi t)\sin(2\pi Nt).$$

Proposition 1.4. *Suppose* $f \in C^1(S^1)$*, and define the* N*th partial sum of the Fourier series of* f *to be* $s_N(x,f) = \sum_{|n|\leq N} \hat{f}(n)e^{2\pi ix}$. *These partial sums converge to* f *pointwise.*

Proof. Notice in terms of the Dirichlet kernel,

$$\begin{aligned} s_N(x,f) &= \sum_{|n|\leq N} e^{2\pi inx}\int_0^1 f(t)e^{-2\pi int}dt = \int_0^1 f(t)D_N(x-t)dt \\ &= \int_{-x}^{1-x} f(x+u)D_N(u)du = \int_0^1 f(x+u)D_N(u)du. \end{aligned}$$

Therefore,

$$\left|\int_0^1 f(x+t)D_N(t)dt - f(x)\right| = \left|\int_0^1 (f(x+t)-f(x))(\cos(2\pi Nt)+\cot(\pi t)\sin(2\pi Nt))dt\right|.$$

If we let $g_1 = (f(x+t)-f(x))$ and $g_2 = g_1\cot(\pi t)$, then

$$\left|\int_0^1 f(x+t)D_N(t)dt - f(x)\right| = \left|\text{Re}(\hat{g}_1(N)) + \text{Im}(\hat{g}_2(N))\right|.$$

Notice that g_1 and hence g_2 are both in $C^0(S^1)$, thus by Proposition 1.2 $\left|\int_0^1 f(x+t)D_N(t)dt - f(x)\right| \to 0$ as we had hoped. □

2 Fourier Integrals

Similarly, one might hope to express any function on the real line in terms of generalized exponentials of the form $e^{2\pi ixt}$, however one can no longer expect x to be an integer or else one could only get periodic functions. That is we would like to be able to write $f(x) = \int_{\mathbb{R}} g(y)e^{2\pi ixy}dy$ for some function g. In order to recover the function g, one can try integrating with respect to x over the whole real line. Since $\int_{\mathbb{R}} e^{2\pi ixy}dx = \delta(y)$ (where δ is the dirac Delta function), $\int_{\mathbb{R}} f(x)dx = g(0)$ and $\int_{\mathbb{R}} f(x)e^{-2\pi ixy}dx = g(y)$. This result is called the Fourier inversion formula. Obviously have not yet given a rigorous proof.

Definition 2.1. *If* $f \in L_1(\mathbb{R})$ *then we define the Fourier transform* $\hat{f}(y) = \int_{\mathbb{R}} f(x)e^{-2\pi ixy}dx$.

Unfortunately the notation for the Fourier transform and the Fourier coefficients are identical. One can distinguish the two situations by looking at f and seeing whether it is a function on the circle or on the real line.

Proposition 2.2. *If* $f \in L^1(\mathbb{R})$ *then* $\lim_{|y|\to\infty} \hat{f}(y) = 0$.

Proof. As with the analogous result for Fourier series we first note that $\lim_{|y|\to\infty} \hat{f}(y)$ is a continuous and linear function. Therefore it suffices to prove this result for f the characteristic function of $[a,b]$. Again, $\int_{\mathbb{R}} f(x)e^{-2\pi ixy}dx = \int_a^b e^{-2\pi ixy} = \frac{1}{-2\pi in}\left(e^{-2\pi inb} - e^{-2\pi ina}\right)$. Therefore, $|\hat{f}(n)| < \frac{1}{\pi|n|}$. Thus, $\lim_{|n|\to\infty} \hat{f}(n) = 0$. □

Before proving the Fourier inversion formula we will need to have a family of functions whose transform is known, just as we knew the Fourier series for the Dirichlet kernel.

Proposition 2.3. *Let c be any complex number with $Re(c) > 0$. Let $f_c(x) = e^{-c\pi|x|^2}$ Then, its Fourier transform is $\hat{f}_c(y) = \frac{1}{\sqrt{c}}e^{-\pi y^2/c} = \frac{1}{\sqrt{c}}f_{\frac{1}{c}}$.*

Proof. Notice,

$$\hat{f}(y) = \int_{\mathbb{R}} e^{-c\pi|x|^2}e^{2\pi ixy}dx = \frac{1}{\sqrt{c}}e^{-\pi y^2/c}\int_{\mathbb{R}} e^{-(x-iy/c)^2}dx.$$

The last integral can be evaluated with Cauchy's theorem. Let γ_T be the parallelogram whose corners are $\pm T$ and $\pm T + iy/c$. Let $g(z) = e^{-\pi(z-iy/c)^2}$. Then $g(z)$ is holomorphic and its integral around γ_T is zero. The integral of $g(z)$ along the left and right sides of γ_T goes to zero as $T \to \infty$. Therefore, $\int_{\mathbb{R}} e^{-\pi(x-iy/c)^2}dx = \int_{\mathbb{R}} e^{-\pi x^2}dx$. In order to evaluate this last integral, make the change of variables $u = \pi x^2$ to get

$$\int_{\mathbb{R}} e^{-\pi x^2}dx = \frac{1}{2\sqrt{\pi}}\int_{\mathbb{R}} e^u u^{-1/2}du = \frac{1}{2\sqrt{\pi}}2\Gamma\left(\frac{1}{2}\right) = 1.$$

Therefore, $\hat{f}(y) = \frac{1}{\sqrt{c}}e^{-\pi y^2/c}$. □

Theorem 2.4 (Fourier Inversion). *If f and $\hat{f}$ are in $L^1(\mathbb{R})$, then $f(x) = \int_{\mathbb{R}} \hat{f}(y)e^{2\pi ixy}dy$.*

Proof. Notice,

$$\int_{\mathbb{R}} \hat{f}(y)e^{2\pi ixy}dy = \lim_{\varepsilon\to 0^+}\int_{\mathbb{R}} \hat{f}(y)f_\varepsilon(y)e^{2\pi ixy}dy.$$

Using the definition of $\hat{f}(y)$, we can rewrite the second integral as

$$\int_{\mathbb{R}}\left(\int_{\mathbb{R}} f(te^{-2\pi ity}dt\right)f_\varepsilon(y)e^{2\pi ixy}dy.$$

Because all integrals converge absolutely by Fubini we can switch the order of integration to get

$$\int_{\mathbb{R}} f(t)\left(\in_{\mathbb{R}} f_\varepsilon(y)e^{-2\pi i(t-x)y}dy\right)dt.$$

The inner integral is just $\hat{f}_\varepsilon(t-x) = \frac{1}{\sqrt{\varepsilon}}f_{\frac{1}{\varepsilon}}(t-x) = \frac{1}{\sqrt{\varepsilon}}f_{\frac{1}{\varepsilon}}(x-t)$. Thus our favorite integral becomes

$$\frac{1}{\sqrt{\varepsilon}}\int_{\mathbb{R}} f(t)f_{\frac{1}{\sqrt{\varepsilon}}}(x-t)dt.$$

Make the change of variables $t \mapsto \sqrt{\varepsilon}(x-t)$ to get

$$\int_{\mathbb{R}} \hat{f}(y)e^{2\pi ixy}dy = \lim_{\varepsilon\to 0^+}\int_{\mathbb{R}} f(x-\sqrt{\varepsilon}t)e^{-\pi t^2}dt = f(x).$$

□

Now notice that this result only holds up to differing by a function with trivial integral. In particular, if f is a step function we are not guaranteed that we get back from Fourier inversion the same values on the jumps. However, Fourier inversion does give some canonical choice of value on these jump points. To calculate this value notice that in the last step there will be different limits depending on whether t is positive or negative. The final value gotten is thus $\frac{1}{2}(f(x^+) + f(x^-))$. Thus the natural choice for step functions if we want them to behave well under Fourier transforms is to choose the value at each jump to be halfway between the other two values. For the rest of the course we will take this convention any time we discuss step functions.

3 General Theory

Thus far we have seen several examples of "Fourier Theories" in the form $\hat{f}(y) = \int_G f(x)\phi(x,y)d\mu$. The following table shows exactly what each term is for each case:

Fourier Theory:	G is	$f(x)$ domain:	$\hat{f}(y)$ domain:	$\phi(x,y)$ is:	$d\mu$ is:
Fourier Series (one direction)	S^1	S^1	$\mathbb{Z}$	$e^{-2\pi xy}$	dx
Fourier Series (the other direction)	$\mathbb{Z}$	$\mathbb{Z}$	S^1	$e^{2\pi xy}$	$d\lfloor y \rfloor$
Fourier Integrals	$\mathbb{R}$	$\mathbb{R}$	$\mathbb{R}$	$e^{2\pi xy}$	dx
Orthogonality of Characters	G	G	G^*	$\chi(g)$	$\frac{1}{\lvert G \rvert}dg$

All of these situations fall into the following general idea. Let G be a Locally Compact Abelian Lie Group. Let G^* be the group of continuous homomorphisms from G to S^1. Choose $d\mu$ to be the normalized Haar measure on G. Define the Fourier transform of $f : G \to \mathbb{C}$ to be $\hat{f}(y) = \int_G y(x)d\mu$. One can prove that under suitable conditions $G^{**} = G$. Thus we can apply this transforming process twice. As in all of the above cases the function we recover is $f(-x)$.

4 Melin Transform

The only remaining group for which we will need a Fourier theory for is the positive reals under multiplication, which we shall denote $\mathbb{R}_+^\times$. Characters on this group take the form x^s where s is a complex number. Thus we expect a Fourier theory of the following form:

Definition 4.1. *Take $f : \mathbb{R}_+^\times \to \mathbb{C}$. Define the Mellin transform (where it converges) to be $F(s) = \int_0^\infty f(x)x^s \frac{dx}{x}$.*

Notice that if this converges for s_0 then it converges for the halfplane to the right of s_0.

Definition 4.2. *Take F a function from a right halfplane in $\mathbb{C}$ to $\mathbb{C}$. Define the inverse Mellin transform to be (for σ such that it actually converges) $f(x) = \frac{1}{2\pi i}\int_{\sigma - i\infty}^{\sigma + i\infty} F(s)x^{-s}ds$.*

Theorem 4.3 (Mellin Inversion Formula). *Let $f : \mathbb{R}_+^\times \to \mathbb{C}$ be a function and $s = \sigma + it$ be a complex number such that the Mellin transform f is defined. Furthermore assume the integral $\int_{-\infty}^\infty F(\sigma + it)dt$ converges absolutely. Then*

$$f(x) = \frac{1}{2\pi i}\int_{\sigma - i\infty}^{\sigma + i\infty} F(s)x^{-s}ds.$$

Proof. As explained above one can prove this result from a more general theory. However, since $\mathbb{R}_+^\times$ is isomorphic to $\mathbb{R}$ under the logarithm map, we can deduce this result from traditional Fourier inversion. Make the change of variable $x = e^{2\pi u}$ to get

$$F(s) = \int_{\mathbb{R}} (2\pi f(e^{-2\pi u})e^{-2\pi u\sigma})e^{-2\pi ut}du.$$

By Fourier inversion

$$2\pi f(e^{-2\pi u})e^{-2\pi u\sigma} = \int_{\mathbb{R}} F(\sigma + it)e^{2\pi iut}dt.$$

Changing variables back to $x = e^{2\pi u}$ and rearranging terms yields,

$$f(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} F(\sigma + it)x^{-(\sigma + it)}dt.$$

□

5 Poisson Summation Formula

Before turning to our main result we need one lemma.

Proposition 5.1. *If $f \in C^2(\mathbb{R})$ and $f, f', f'' \in L^1(\mathbb{R})$, then $|\hat{f}(y)| \leq c(1+|y|)^{-2}$ for some constant c which depends on f.*

Proof. We simply apply integration by parts.

$$\begin{aligned}
|\hat{f}(y) = \left|\int_{\mathbb{R}} f(x)e^{-2\pi ixy}dx\right| &\leq \int_{|x|<1} |f(x)|dx + \frac{1}{|2\pi y|}\left|\int_{|x|\geq 1} f'(x)e^{-2\pi ixy}dx\right| \\
&\leq C + \frac{1}{|2\pi y|^2}\left|\int_{|x|\geq 1} f''(x)e^{-2\pi ixy}dx\right|.
\end{aligned}$$

Therefore, $|\hat{f}(y)| \leq c(1+|x|)^{-2}$. □

Theorem 5.2 (Poisson Summation Formula). *Let $f \in C^2(\mathbb{R})$ be a function for which $|f(x)|$, $|f'(x)|$, and $|f''(x)|$ are all bounded by $c(1+|x|)^{-2}$ for some fixed constant c. Then, letting $\hat{f}$ be the Fourier transform,*

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n).$$

Proof. Let $F(x) = \sum_{k\in\mathbb{Z}} f(x+k)$. Because of our bound on $f(x)$, F must converge uniformly to a continuous function which clearly is periodic with period 1. Furthermore, since its first two derivatives are also nicely bounded, F is a twice continuously differentiable function. Thus we can apply Theorem 1.4 to get

$$F(x) = \sum_{n\in\mathbb{Z}} \hat{F}(n)e^{2\pi inx},$$

for all $x \in \mathbb{R}$.

We turn to calculating $\hat{F}(n)$. Notice,

$$\hat{F}(n) = \int_0^1 f(\theta+k)e^{-2\pi in\theta}d\theta = \int_{\mathbb{R}} f(\theta)e^{-2\pi in\theta}d\theta = \hat{f}(n).$$

(The switching of summation and integration is justified because of the bound we have on $|f(x)|$.) Therefore,

$$\sum_{k\in\mathbb{Z}} f(x+k) = F(x) = \sum_{n\in\mathbb{Z}} \hat{f}(n)e^{2\pi inx}.$$

Taking $x = 0$ gives our result. □

6 Two Applications of Poussin Summation

Proposition 6.1. $\sum_{n=1}^{\infty} \frac{1}{\varepsilon^2+n^2} = -\frac{\pi}{2\varepsilon} - \frac{1}{2\varepsilon^2} + \frac{\pi}{\varepsilon}\frac{1}{1-e^{-2\pi\varepsilon}}$.

Proof. Let $f(x) = e^{-2\pi ixy}$. By definition,

$$\begin{aligned}
\hat{f}(y) = \int_{\mathbb{R}} f(x)e^{-2\pi xy}dx &= \int_0^{\infty} e^{-2\pi(\varepsilon+iy)x}dx + \int_0^{\infty} e^{-2\pi(\varepsilon-iy)x}dx \\
&= \frac{1}{2\pi(\varepsilon+iy)} + \frac{1}{2\pi(\varepsilon-iy)} = \frac{\varepsilon}{\pi(\varepsilon^2+y^2)}.
\end{aligned}$$

Now we can apply the Poisson summation formula to get

$$\frac{2\varepsilon}{\pi}\sum_{n=1}^{\infty}\frac{1}{\varepsilon^2+n^2} + \frac{1}{\varepsilon\pi} = \sum_{n\in\mathbb{Z}} \hat{f}(n) = \sum_{n\in\mathbb{Z}} f(n) = -1 + \frac{2}{1-e^{-2\pi\varepsilon}}.$$

Rearranging we see that,

$$\sum_{n=1}^{\infty} \frac{1}{\varepsilon^2 + n^2} = -\frac{\pi}{2\varepsilon} - \frac{1}{2\varepsilon^2} + \frac{\pi}{\varepsilon} \frac{1}{1 - e^{-2\pi\varepsilon}}.$$

□

Although we shall need this full result at some point later, one nice application is that we can compute $\zeta(2)$. If we expand the last term as a Taylor series in ε, we get,

$$\sum_{n=1}^{\infty} \frac{1}{\varepsilon^2 + n^2} = -\frac{\pi}{2\varepsilon} - \frac{1}{2\varepsilon^2} + \frac{\pi}{\varepsilon} \frac{1}{2\pi\varepsilon} \left(1 + \pi\varepsilon + \frac{1}{3}\pi^2\varepsilon + \dots\right) = \frac{\pi^2}{6} + O(\varepsilon).$$

Therefore, $\zeta(2) = \frac{\pi^2}{6}$.

Our second application is the functional equation of the Jacobi theta function.

Definition 6.2. *Let $\theta(z) = \sum_{n\in\mathbb{Z}} e^{i\pi n^2 z}$.*

Notice that this sum converges for all z in the upper halfplane, because $|\theta(z)| < 1 + 2\int_0^\infty e^{-t\mathrm{Im}(z)} dt = 1 + \frac{2}{\mathrm{Im}(z)}$.

Proposition 6.3. *$\theta(z)$ satisfies the symmetry:*

$$\theta(-1/z) = \sqrt{-iz}\theta(z).$$

Here the square root denotes the usual branch which is positive on $\mathbb{R}^+$.

Proof. Let $f_z(x) = e^{i\pi|x|^2 z}$. Recall that $\hat{f}_z(y) = \frac{1}{\sqrt{-iz}} f_{\frac{1}{z}}(y)$.

Now we apply the Poussin summation formula:

$$\theta(z) = \sum_{m\in\mathbb{Z}} f_z(m) = \sum_{m\in\mathbb{Z}} \hat{f}_z(m) = \frac{1}{\sqrt{-iz}} \sum_{m\in\mathbb{Z}} e^{-i\pi m^2/z} = \frac{1}{\sqrt{-iz}} \theta(-1/z).$$

Therefore, $\sqrt{-iz}\theta(z) = \theta(-1/z)$. □

Lecture # 4: The Analytic Continuation and Functional Equation of Riemann's Zeta Function.

Noah Snyder

July 3, 2002

As we mentioned before, by getting more information about the ζ-function we can recover more information about prime numbers. In this lecture we will explain how to extend the ζ-function to the entire complex plane, look at some of its basic properties there, and discuss how Riemann outlined using these properties to get good information about the prime numbers.

1 Continuing ζ to the Line $\mathrm{Re}(s) = 0$.

Theorem 1.1. *The ζ-function can be meromorphically continued to the right halfplane $Re(s) > 0$ with a simple pole of order 1 at $s = 1$ and no others.*

Proof. Let $\zeta_2(s) = -1^{-s} + 2^{-3} - 3^{-s} + 4^{-s} - \ldots$. By our earlier result, this converges for $\mathrm{Re}(s) > 0$. Notice that

$$\zeta(s) + \zeta_2(s) = 2\sum_{2|n} n^{-s} = 2\frac{\frac{1}{1-2^{-s}} - 1}{\frac{1}{1-2^{-s}}}\zeta(s).$$

Therefore, $\zeta(s) + \zeta_2(s) = 2^{1-s}\zeta(s)$. Hence, $\zeta(s) = \frac{1}{2^{1-s}-1}\zeta_2(s)$. The righthand side makes sense for any $\mathrm{Re}(s) > 0$ except for possible simple poles at $s = 1 + 2\pi i \log_2(n)$ for $n \in \mathbb{Z}$.

But we can go through a similar argument for 3. That is, let $\zeta_3(s) = -1^{-s} - 2^{-s} + 2 \cdot 3^{-s} - 4^{-s} - \ldots$. Again this converges for $\mathrm{Re}(s) > 0$. Furthermore,

$$\zeta(s) + \zeta_3(s) = 3\frac{\frac{1}{1-3^{-s}} - 1}{\frac{1}{1-3^{-s}}}\zeta(s).$$

Therefore, $\zeta(s) = \frac{1}{3^{1-s}-1}\zeta_3(s)$. This expression makes sense for any $\mathrm{Re}(s) > 0$ except for possible simple poles at $s = 1 + 2\pi i \log_3(n)$ for $n \in \mathbb{Z}$.

Combining these two results, we've shown that $\zeta(s)$ can be continued to $\mathrm{Re}(s) > 0$ with poles only at numbers both of the form $s = 1 + 2\pi i \log_3(n)$ and $s = 1 + 2\pi i \log_2(m)$. Thus we need to find any integers m and n such that $\log_3(n) = \log_2(m)$. That is to say, $2^n = 3^m$. By unique factorization, this only happens when $n = m = 0$. Thus the only pole is at $s = 1$. □

There is another proof of this result.

Proof. Notice that $\zeta(s) = \int_{1^-}^{\infty} x^{-s} d\lfloor x \rfloor$. Integrating by parts, we see $\zeta(s) = s\int_{1^-}^{\infty} x^{-s-1}\lfloor x \rfloor dx$. Notice that $\lfloor x \rfloor = x - \{x\}$ where $\{x\}$ denotes the fractional part. Therefore,

$$\zeta(s) = s\int_{1^-}^{\infty} x^{-s} dx - s\int_{1^-}^{\infty} x^{-s-1}\lfloor x \rfloor dx = -1 + \frac{1}{1-s} - s\int_{1^-}^{\infty} x^{-s-1}\lfloor x \rfloor dx.$$

Notice that this last integral is bounded by $\int_{1^-}^{\infty} x^{-s-1} dx$, and so converges for any $\mathrm{Re}(s) > 0$. Thus we have a formula which agrees with ζ and makes sense on the halfplane $\mathrm{Re}(s) > 0$ except for a simple pole at $s = 1$. □

2 Continuing Beyond Re$(s) = 0$ and the Functional Equation

Theorem 2.1 (Functional Equation of the ζ-function). *The ζ-function can be meromorphically continued to the entire complex plane with a single pole at $s = 1$. Furthermore, this function satisfies the functional equation*

$$\Gamma(s)\pi^{-s}\zeta(2s) = \Gamma\left(\frac{1}{2} - s\right)\pi^{-\frac{1}{2}+s}\zeta(1-2s).$$

Proof. Take the definition of the Gamma function and make the change of variables $x \to n^2\pi x$ to get

$$n^{-2s}\pi^{-s}\Gamma(s) = \int_0^\infty e^{-n^2\pi x}x^s\frac{dx}{x}.$$

Again we sum over all n and use uniform convergence to interchange sum and integral to get

$$\zeta(2s)\pi^{-s}\Gamma(s) = \int_0^\infty \frac{1}{2}(\theta(ix) - 1)x^s\frac{dx}{x}.$$

Now we can apply the functional equation of the θ function to the right hand side:

$$\begin{aligned}\zeta(2s)\pi^{-s}\Gamma(s) &= \int_0^\infty \frac{1}{2}(\theta(ix)-1)x^s\frac{dx}{x} = \int_0^1 \frac{1}{2}(\theta(ix)-1)x^s\frac{dx}{x} + \int_1^\infty \frac{1}{2}(\theta(ix)-1)x^s\frac{dx}{x} \\ &= \int_1^\infty \frac{1}{2}(\theta(-1/ix)-1)x^{-s}\frac{dx}{x} + \int_1^\infty \frac{1}{2}(\theta(ix)-1)x^s\frac{dx}{x} \\ &= \int_1^\infty \frac{1}{2}(x^{\frac{1}{2}}\theta(ix)-1)x^{-s}\frac{dx}{x} + \int_1^\infty \frac{1}{2}(\theta(ix)-1)x^s\frac{dx}{x} \\ &= \int_1^\infty \frac{1}{2}(\theta(ix)-1)(x^{\frac{1}{2}-s}+x^s)\frac{dx}{x} + \int_1^\infty \frac{1}{2}(-x^{\frac{1}{2}-s}-x^{-s})\frac{dx}{x} \\ &= -\frac{1}{2(\frac{1}{2}-s)} - \frac{1}{2s} + \int_1^\infty \frac{1}{2}(\theta(ix)-1)(x^{\frac{1}{2}-s}+x^s)\frac{dx}{x}.\end{aligned}$$

Notice that the right hand side is defined and analytic for all of $\mathbb{C}$ except for simple poles at $s = 0$ and $s = \frac{1}{2}$. Thus we have given another analytic continuation of ζ to the complex plane except for $s = 1$ (the pole at 0 coming from the Γ factor). But more importantly, this formula is clearly symmetric under the change of variables $s \to \frac{1}{2} - s$ and our theorem is proved. Making the change of variables back from $2s \to s$, we see that the completed ζ-function $\pi^{-s/2}\Gamma(s/2)\zeta(s)$ is symmetric about the line Re$(s) = 1/2$ and only has poles at $s = 0$ and $s = 1$. □

This proof is Riemann's second proof of the analytic continuation and functional equation of the ζ-function. Week 3's homework will work through his first proof.

Definition 2.2. *Let* $\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s)$.

Notice that $\xi(s)$ is holomorphic on the entire complex plane, furthermore, it satisfies the functional equation $\xi(s) = \xi(1-2)$. Often it will be more useful to consider this function than the original ζ-function.

3 The Zeroes of the Zeta Function

Proposition 3.1. $\zeta(s) \neq 0$ *for any* $Re(s) > 1$.

Proof. Since Re$(s) > 1$ we can use the Euler factorization $\zeta(s) = \prod_p \frac{1}{1-p^{-s}}$. We need only show that $\log\zeta(s)$ is finite. But, $\log\zeta(s) = \sum_p\sum_{k=1}^\infty \frac{1}{k}p^{-ks}$, and this last sum is clearly bounded. □

Therefore, by the functional equation, the only zeroes of the ζ function with $\mathrm{Re}(s) < 0$ are those which come from the poles of the Γ function. Thus outside the strip $0 \leq \mathrm{Re}(s) \leq 1$ the only zeroes of the ζ-function lie at $s = 2, 4, \ldots$ and these are simple zeroes of order 1. These are called the "trivial zeroes."

Of the remaining zeroes, Riemann remarked, that it was likely that they all lie on the line $\mathrm{Re}(s) = \frac{1}{2}$. This is the celebrated Riemann Hypothesis, which remains open to this day (with a million dollar bounty on its head).

4 A Brief Tangent: Möbius Inversion

Definition 4.1. *If f and g are functions from the natural numbers to say $\mathbb{C}$, let $f \star g(n) = \sum_{d|n} f(d) g(\frac{n}{d})$.*

Recall that $f(s,a)f(s,b) = f(s, a \star b)$. Thus $\star$ must be associative and commutative. Furthermore, since the function 1 is the identity under multiplication, the sequence $\varepsilon(n)$ which is 1 if $n = 1$ and zero otherwise is the multiplicative identity. One can easily show by hand that a sequence has a $\star$ inverse exactly when $a_1 \neq 0$. In particular the function $1(n) = 1$ has a star inverse which we will call μ. Notice that the property defining μ is that $\sum_{d|n} \mu(d) = \varepsilon(n)$. By hand one can compute that $\mu(n) = (-1)^{\text{number of prime factors}}$ if n is square free, and $\mu(n) = 0$ otherwise.

Theorem 4.2 (Möbius Inversion). *If $f(n) = \sum_{d|n} g(d)$, then $g(n) = \sum_{d|n} \mu(n/d) g(d)$.*

Proof. We are given that $g \star 1 = f$. Therefore, $g \star 1 \star \mu = f \star \mu$. But $1 \star \mu = \varepsilon$ the identity, thus $g = f \star \mu$ which is exactly what we are trying to prove. □

There are several other versions of Möbius inversion which we will be using.

Corollary 4.3. *If $f(x) = \sum_{n=1}^{\infty} g(x/n)$ then $g(x) = \sum_{n=1}^{\infty} \mu(n) f(x/n)$.*

Proof. First plug in the formula for $f(x)$ to see,

$$\sum_{n=1}^{\infty} \mu(n) f(x/n) = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \mu(n) g(x/mn).$$

Now let $\ell = mn$ and $d = m$. Thus,

$$\sum_{n=1}^{\infty} \mu(n) f(x/n) = \sum_{\ell=1}^{\infty} \sum_{d|\ell} \mu(d) g(x/\ell) = \sum_{\ell=1}^{\infty} g(x/\ell) \sum_{d|\ell} \mu(d) = g(x).$$

□

5 Riemann's Argument

Riemann used his analytically continued ζ-function to sketch an argument which would give an actual formula for $\pi(x)$ and suggest how to prove the prime number theorem. This argument is highly unrigorous at points, but it is crucial to understanding the development of the rest of the theory.

Notice that $\log \zeta(s) = \sum_p \sum_n \frac{1}{n} p^{-ns}$ for $\mathrm{Re}(s) > 1$. Letting $J(x)$ be the number of prime powers less than x, notice that $\log \zeta(s) = \int_0^\infty x^{-s} dJ(x)$ again for $\mathrm{Re}(s) > 1$. Now use integration by parts to get

$$\log \zeta(s) = s \int_0^\infty J(x) x^{-s-1} dx.$$

Now this is a Mellin transform, so, assuming some technical results, we should be able to use Melin inversion. Thus,

$$J(x) = \frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} \frac{\log \zeta(s)}{s} x^s ds.$$

This converges when $\sigma > 1$.

Thus in order to find a formula for $J(x)$ we need only get a better formula for $\log\zeta(s)$.

Riemann claimed that $\xi(s) = \xi(0)\prod_\rho \left(1 - \frac{s}{\rho}\right)$, where the product is taken over all roots of the ξ function (that is, over all nontrivial zeroes of the ζ-function). This product does not converge absolutely, and we should pair any terms with $im(\rho)$ positive with a corresponding term with negative imaginary part to get a convergent product. The proof of this product formula basically depends on getting nice bounds on the growth of the number of zeroes.

Now we notice that,

$$\zeta(s) = 2\frac{1}{s(s-1)}\pi^{s/2}\frac{1}{\Gamma(s/2)}\xi(s) = 2\frac{1}{s(s-1)}\pi^{s/2}\frac{1}{\Gamma(s/2)}\xi(0)\prod_\rho\left(1 - \frac{s}{\rho}\right).$$

Therefore,

$$\log\zeta(s) = \log 2 - \log s - \log(s-1) + \frac{s}{2}\log\pi - \log\Gamma(s/2) + \log\xi(0) + \sum_\rho \log\left(1 - \frac{s}{\rho}\right).$$

We want to substitute this into our integral formula and evaluate termwise, however doing so would lead to divergent integrals (for example in the $\frac{s}{2}\log\pi$ term). Thus Riemann first integrated by parts to get,

$$J(x) = -\frac{1}{2\pi i}\cdot\frac{1}{\log x}\int_{\sigma-i\infty}^{\sigma+i\infty}\frac{d}{ds}\left(\frac{\log\zeta(s)}{s}\right)x^s ds.$$

Now we can substitute our formula for $\zeta(s)$ and evaluate term by term. With a good bit of work, Riemann evaluated these integrals and got the formula,

$$J(x) = \mathrm{Li}(x) - \sum_\rho \mathrm{Li}(x^\rho) + \int_x^\infty \frac{1}{t(t^2-1)\log t}dt - \log 2.$$

Notice that $J(x) = \sum_{n=1}^\infty \frac{1}{n}\pi(x^{\frac{1}{n}})$. We can invert this formula to get, $\pi(x) = \sum_{n=1}^\infty \mu(n)\frac{1}{n}J(x^{1/n})$.

This gives us a formula for $\pi(x)$. Its dominant term is $\sum_{n=1}^\infty \mu(n)\frac{1}{n}\mathrm{Li}(x^{1/n})$. This would show the prime number theorem if we could actually prove that this term was dominant. The key to proving this is to show that the $\sum_\rho \mathrm{Li}(x^\rho)$ terms are each smaller, that is to say we need to show that $\mathrm{Re}(\rho) < 1$.

Lectures # 5 and 6: The Prime Number Theorem.

Noah Snyder

July 8, 2002

1 Riemann's Argument

Riemann used his analytically continued ζ-function to sketch an argument which would give an actual formula for $\pi(x)$ and suggest how to prove the prime number theorem. This argument is highly unrigorous at points, but it is crucial to understanding the development of the rest of the theory.

Notice that $\log\zeta(s) = \sum_p \sum_n \frac{1}{n} p^{-ns}$ for $\mathrm{Re}(s) > 1$. Letting $J(x) = \sum_{p^k \leq x} \frac{1}{k}$, notice that $\log\zeta(s) = \int_0^\infty x^{-s} dJ(x)$ again for $\mathrm{Re}(s) > 1$. Now use integration by parts to get

$$\log\zeta(s) = s\int_0^\infty J(x)x^{-s-1}dx.$$

Now this is a Mellin transform, so, assuming some technical results, we should be able to use Melin inversion. Thus,

$$J(x) = \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} \frac{\log\zeta(s)}{s} x^s ds.$$

This converges when $\sigma > 1$.

Thus in order to find a formula for $J(x)$ we need only get a better formula for $\log\zeta(s)$.

Riemann claimed that $\xi(s) = \xi(0)\prod_\rho \left(1 - \frac{s}{\rho}\right)$, where the product is taken over all roots of the ξ function (that is, over all nontrivial zeroes of the ζ-function). This product does not converge absolutely, and we should pair any terms with $im(\rho)$ positive with a corresponding term with negative imaginary part to get a convergent product. The proof of this product formula basically depends on getting nice bounds on the growth of the number of zeroes.

Now we notice that,

$$\zeta(s) = 2\frac{1}{s(s-1)}\pi^{s/2}\frac{1}{\Gamma(s/2)}\xi(s) = 2\frac{1}{s(s-1)}\pi^{s/2}\frac{1}{\Gamma(s/2)}\xi(0)\prod_\rho\left(1-\frac{s}{\rho}\right).$$

Therefore,

$$\log\zeta(s) = \log 2 - \log s - \log(s-1) + \frac{s}{2}\log\pi - \log\Gamma(s/2) + \log\xi(0) + \sum_\rho \log\left(1 - \frac{s}{\rho}\right).$$

We want to substitute this into our integral formula and evaluate termwise, however doing so would lead to divergent integrals (for example in the $\frac{s}{2}\log\pi$ term). Thus Riemann first integrated by parts to get,

$$J(x) = -\frac{1}{2\pi i}\cdot\frac{1}{\log x}\int_{\sigma-i\infty}^{\sigma+i\infty}\frac{d}{ds}\left(\frac{\log\zeta(s)}{s}\right)x^s ds.$$

Now we can substitute our formula for $\zeta(s)$ and evaluate term by term. With a good bit of work, Riemann evaluated these integrals and got the formula,

$$J(x) = \mathrm{Li}(x) - \sum_\rho \mathrm{Li}(x^\rho) + \int_x^\infty \frac{1}{t(t^2-1)\log t}dt - \log 2.$$

Notice that $J(x) = \sum_{n=1}^{\infty} \frac{1}{n}\pi(x^{\frac{1}{n}})$. We can invert this formula to get, $\pi(x) = \sum_{n=1}^{\infty} \mu(n)\frac{1}{n}J(x^{1/n})$.

This gives us a formula for $\pi(x)$. Its dominant term is $\sum_{n=1}^{\infty} \mu(n)\frac{1}{n}\mathrm{Li}(x^{1/n})$. This would show the prime number theorem if we could actually prove that this term was dominant. The key to proving this is to show that the $\sum_{\rho} \mathrm{Li}(x^{\rho})$ terms are each smaller, that is to say we need to show that $\mathrm{Re}(\rho) < 1$.

2 Chebyshev's Functions

Before Riemann's work the only significant progress towards the prime number theorem was made by Chebyshev who proved that, for sufficiently large x and some constants $c_1 < 1 < c_2$, $c_1\frac{x}{\log x} \leq \pi(x) \leq c_2\frac{x}{\log x}$. To prove this he introduced two functions which are crucial in later proofs of prime number theory. Recall that we conjecture that the chances that a number n is prime is roughly $\frac{1}{\log n}$. Thus, if we counted each prime as $\log p$ instead of as 1, then we would get a better behaved function.

Definition 2.1. *Let $\theta(n) = \sum_{p \leq n} \log p$ (where, as usual, at jumps we define the function to be halfway in between the two values).*

As we've seen from Riemann's argument it is often simpler to count prime powers instead of primes.

Definition 2.2. *Let $\psi(n) = \sum_{p^k \leq n} \log p$.*

There is another way of writing ψ in terms of Von Mangoldt's Λ function.

Definition 2.3. *Let*

$$\Lambda(n) = \begin{cases} \log n & \textit{if } n \textit{ is a prime power} \\ 0 & \textit{else} \end{cases}.$$

Clearly $\psi(x) = \sum_{x \leq n} \Lambda(n)$.

First we notice that one can express each of the functions ψ, θ, π, and J in terms of any of the others.

Proposition 2.4.

$$J(x) = \sum_{n=1}^{\infty} \frac{1}{n}\pi(x^{1/n}).$$

$$\pi(x) = \sum_{n=1}^{\infty} \mu(n)\frac{1}{n}\pi(x^{1/n}).$$

$$\psi(x) = \sum_{n=1}^{\infty} \theta(x^{1/n}).$$

$$\theta(x) = \sum_{n=1}^{\infty} \mu(n)\psi(x^{1/n}).$$

Proof. We've already shown the first two, and the proof of the second two are exactly the same. □

Proposition 2.5.

$$\pi(x) = \frac{\theta(x)}{\log x} + \int_0^{\infty} \frac{\theta(t)}{t(\log t)^2}dt.$$

$$J(x) = \frac{\psi(x)}{\log x} + \int_0^{\infty} \frac{\psi(t)}{t(\log t)^2}dt.$$

$$\psi(x) = J(x)\log x - \int_0^{x} \frac{J(t)}{t}dt.$$

$$\theta(x) = \pi(x)\log x - \int_0^{x} \frac{\pi(t)}{t}.$$

Proof. Notice that $\pi(x) = \int_0^x \frac{1}{\log t} d\theta(t)$. The theorem follows from integration by parts. Similarly $J(x) = \int_0^x \frac{1}{\log t} d\psi(t)$, and we integrate by parts again. Conversely, $\theta(x) = \int_0^x \log t d\pi(t)$ and $\psi(x) = \int_0^x \log t dJ(t)$. Integrating these by parts gives the second two equations. □

Since θ and ψ are trivially $O(x \log x)$ and π and J are trivially $O(x)$ we can rewrite these equations in terms of error estimates. The long and short of all of this is that to prove the prime number theorem it is enough to prove any of $\pi \sim \text{Li}(x)$, $J(x) \sim \text{Li}(x)$, $\theta(x) \sim x$, or $\psi(x) \sim x$. Furthermore, given any explicit error terms in the above approximations we can find explicit error terms for all of the other approximations. As it turns out ψ is the easiest function to deal with.

Proposition 2.6. *For any n, $\sum_{d|n} \Lambda(d) = \log n$.*

Proof. Notice that $n = \prod_{p|n} p^k$ where k is the largest number such that $p^k|n$. Thus, $n = \prod p^k|np$. Taking the logarithm shows that $\log n = \sum_{d|n} \Lambda(d)$.

There is another way of looking at this identity. In shorthand this proposition claims $\Lambda \star 1 = \log n$. Thus it is equivalent to some identity involving Dirichlet series. Notice that

$$\sum_{n=1}^{\infty} \Lambda(n) n^{-s} = \sum_p \sum_{m=1}^{\infty} (\log p) p^{-ms} = -\frac{\zeta'(s)}{\zeta(s)}.$$

Also

$$\sum_{n=1}^{\infty} \log n = \zeta'(s).$$

Therefore, $f(s, \Lambda)\zeta(s) = f(s, \log n)$ exactly as we had hoped to show. □

Before leaving this last proof we notice that one of the equations can be rewritten

$$-\frac{\zeta'(s)}{\zeta(s)} = \int_0^{\infty} x^{-s} d\psi(x).$$

3 Chebyshev's Theorem

Theorem 3.1. *For sufficiently large x and some constants $c_1 < 1 < c_2$, $c_1 \leq \frac{\psi(x)}{x} \leq c_2$.*

Proof. Chebyshev noticed that if we sum $\sum_{d|n} \Lambda(d) = \log n$ over all $n \leq x$, then

$$T(x) = \sum_{m \leq x} \Lambda(m) \left\lfloor \frac{x}{m} \right\rfloor = \sum_{n \leq x} \log n = \log \lfloor x \rfloor !.$$

By Stirling's formula

$$T(x) = \log \lfloor x \rfloor ! = x \log x - x + O(\log x).$$

Notice that

$$T(x) = \sum_{m \leq x} \sum_{n \leq \frac{x}{m}} \Lambda(m) = \sum_{n \leq x} \sum_{m \leq \frac{x}{n}} \Lambda(m) = \sum_{n \leq x} \psi\left(\frac{x}{n}\right).$$

Therefore, by Möbius inversion,

$$\psi(x) = \sum_{n=1}^{\infty} \mu(n) T\left(\frac{x}{n}\right).$$

This suggests that finite expressions which have several terms from $\sum_{n=1}^{\infty} \mu(n) T\left(\frac{x}{n}\right)$ will give good approximations to ψ. But we also want good cancellations when we plug in the approximation from Stirling's formula. For example, it would be informative to look at expressions of the following form:

$$T(x) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{2}\right),$$

$$T(x) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) + T\left(\frac{x}{6}\right),$$
$$T(x) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) + T\left(\frac{x}{30}\right), \text{ etc.}$$

We will look at the first expression $T(x) - 2T\left(\frac{x}{2}\right)$. Chebyshev looked at the third expression and was able to get constants c_1 and c_2 closer to 1. Notice,

$$T(x) - 2T\left(\frac{x}{2}\right) = \sum_{m \le x} \Lambda(m) \left(\left\lfloor \frac{x}{m} \right\rfloor - \left\lfloor \frac{x}{2m} \right\rfloor \right).$$

The lefthand side is $x \log 2 + O(\log x)$. The righthand side is

$$\sum_{m \le x} \Lambda(m) \left(\left\lfloor \frac{x}{m} \right\rfloor - \left\lfloor \frac{x}{2m} \right\rfloor \right) \le \sum_{m \le x} \Lambda(m) = \psi(x).$$

Therefore, for large x and any constant $\varepsilon > 0$,

$$\log 2 - \varepsilon \le \frac{\psi(x)}{x}.$$

In particular, we can take $c_1 = .69$.

Similarly, the righthand side is

$$\sum_{m \le x} \Lambda(m) \left(\left\lfloor \frac{x}{m} \right\rfloor - \left\lfloor \frac{x}{2m} \right\rfloor \right) \ge \sum_{\frac{1}{2}x \le m \le x} \Lambda(m) = \psi(x) - \psi\left(\frac{x}{2}\right).$$

Therefore, $\psi(x) - \psi\left(\frac{x}{2}\right) \le x \log 2 + O(\log x)$. Summing these estimates yields,

$$\psi(x) \le x \cdot 2 \log 2 + O(\log^2 x).$$

In particular, we can take $c_2 = 1.38$. □

By our previous results relating ψ and π, we also get that

$$.79 \cdot \frac{x}{\log x} \le \pi(x) \le 1.38 \cdot \frac{x}{\log x}.$$

4 Reducing the Prime Number Theorem to Facts About $\zeta(s)$.

Recall that

$$-\frac{\zeta'(s)}{\zeta(s)} = \int_0^\infty x^{-s} d\psi(x).$$

Integrate by parts to see that

$$-\frac{\zeta'(s)}{\zeta(s)} = s \int_0^\infty \psi(x) x^{-s-1} dx.$$

Our general method of attack is to rewrite this as a Mellin transform and then use Mellin inversion to retrieve $\psi(x)$ in terms of $\zeta(s)$. However, to make certain integrals behave well later on, we first make a slight change. Integrates by parts again to notice that

$$-\frac{\zeta'(s)}{\zeta(s)} = s^2 \int_0^\infty \left(\int_0^x \frac{\psi(t)}{t} dt \right) x^{-s-1} dx.$$

Definition 4.1. *Let* $\phi(x) = \int_0^x \frac{\psi(t)}{t} dt$.

Therefore we have

$$-\frac{\zeta'(s)}{\zeta(s)} = s^2 \int_0^\infty \phi(x) x^{-s-1} dx.$$

To write this as a Mellin transform we make the change of variables $s \mapsto 1-s$. Therefore,

$$-\frac{\zeta'(1-s)}{\zeta(1-s)} \frac{1}{(1-s)^2} = \int_0^\infty \frac{\phi(x)}{x} x^{-s} \frac{dx}{x}.$$

In order to apply Mellin inversion we must check to see that the technical conditions of that theorem are satisfied. Notice that since $\psi(x) = O(x \log x)$ we have $\frac{\phi(x)}{x} = O(\log x)$. Therefore the integrand in the Mellin transform converges absolutely for $\Re(s) < 0$. Also,

$$\left| \frac{\zeta'(s)}{\zeta(s)} \right| \leq \sum_{n=1}^{\infty} (\log n) n^{-\sigma}.$$

Thus, for any positive ε, in the region $\mathrm{Re}(s) \geq 1 + \varepsilon$, the function $\frac{\zeta'(s)}{\zeta(s)}$ is bounded by an absolute constant. Therefore, the integral

$$\int_{\sigma - i\infty}^{\sigma + i\infty} \frac{\zeta'(1-s)}{\zeta(1-s)} \frac{1}{(1-s)^2} dx$$

converges absolutely for any $\sigma < 0$. Therefore the conditions of Mellin inversion are satisfied and,

$$\frac{\phi(x)}{x} = -\frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} \frac{\zeta'(1-s)}{\zeta(1-s)} \frac{1}{(1-s)^2} x^{-s} ds,$$

for any $\mathrm{Re}(s) < 0$.

Now we can change variables back $s \mapsto 1-s$ and multiply both sides by x to get,

Proposition 4.2. *For any s with $Re(s) > 1$ the following integral converges absolutely and*

$$\phi(x) = -\frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} \frac{\zeta'(s)}{\zeta(s)} \frac{1}{s^2} x^s dx.$$

□

Notice that thus far we could have gone through the argument with $\psi(x)$ instead of $\phi(x)$ and the resulting formula would have a $1/s$ instead of $1/s^2$.

Our argument from here on in consists of several parts. First we will assume that there are no zeroes of the ζ function on the line $\mathrm{Re}(s) = 1$. We will prove this in the next section. Thus the only pole of the integrand in the halfplane $\mathrm{Re}(s) \geq 0$ is $s = 1$. We can subtract off this pole to get a term which contributes the dominant term x. The remaining integral we can move all the way to the line $\mathrm{Re}(s) = 1$. Then we will get an explicit bound on this integral. This will give us an approximation for $\phi(x)$. Finally we will need to extract an estimate for $\psi(x)$ from our knowledge concerning $\psi(x)$.

So notice that

$$\phi(x) = \frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} \frac{1}{s-1} \frac{1}{s^2} x^s dx - \frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} \left(\frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s-1} \right) \frac{1}{s^2} x^s dx.$$

The first integral can be written as the limit of an integral about the rectangle with corners $1+1/T \pm iT$ and $-T \pm iT$. The integrals along all but the right side die very quickly. Thus our integral is the sum of the residues to the left of $\mathrm{Re}(s) = 2$. The only poles are at $s = 0$ and $s = 1$. To this end expand $x^s = e^{s \log x} = 1 + s \log x + s^2 \log^2 x + \ldots$. Thus the residue at $s = 0$ is $-\log x$. At $s = 1$ the residue is x. Therefore this integral contributes the term $x - \log x$.

(The notes that I am basing this on say that this integral is $x - \log x - 1$. I cannot find out where the -1 comes from, but I do not trust my ability to do complex analysis very well, and so that is probably right. Nonetheless since we are only interested in approximation the -1 will not matter.)

Therefore, given our assumption that $\zeta(1 + it) \neq 0$, we have proved:

Proposition 4.3.

$$\phi(x) = x - \log x - \frac{x}{2\pi i} \int_{-\infty}^{i\infty} \left(\frac{\zeta'(1+it)}{\zeta(1+it)} + \frac{1}{it} \right) \frac{1}{(1+it)^2} e^{it \log x} dx.$$

□

In order to estimate this last integral we will need a few estimates on the size of $\zeta(s)$ and $\zeta'(s)$. These will be proved in the next section. Thus we will make the following assumptions:

Proposition 4.4. *Letting $s = \sigma + it$ as usual, we have the bound $\zeta^(k)(s) = O(\log^k t)$ in the region $\sigma > 1 - \frac{1}{\log t}$ and $t > 2$. Also we have $\frac{1}{\zeta(s)} = O(\log^7 t)$ in the region $\sigma \geq 1$ and $t > 2$.*

Proposition 4.5. *For any integer k, $\phi(x) = x + O\left(\frac{x}{(\log x)^k}\right)$.*

Proof. Let

$$f(t) = \frac{1}{2\pi i} \left(\frac{\zeta'(1+it)}{\zeta(1+it)} + \frac{1}{it} \right) \frac{1}{(1+it)^2}.$$

Recall that $\phi(x) = \int_{\mathbb{R}} f(t) e^{it \log x}$. Since the second term is rapidly oscillating, if we can get a decent bound on $f(t)$ we should get a very good bound on $\phi(x)$. From our estimates concerning ζ and its derivatives,

$$f^(k)(t) = O\left(\frac{\log t}{(1+t)^2} \right).$$

Therefore for each k there is a constant $C(k)$ with

$$\int_{\mathbb{R}} |f^(k)(t)| dt \leq C(k).$$

Now we integrate by parts k times to see that,

$$\int_{\mathbb{R}} f(t) e^{it \log x} dt = \frac{1}{(-i \log x)^k} \int_{\mathbb{R}} f^(k)(t) e^{it \log x}.$$

Therefore,

$$\left| \int_{\mathbb{R}} f(t) e^{it \log x} \right| \leq \frac{C(k)}{\log^k x}.$$

Combining this with our earlier results yields our required results. □

Notice that had we attempted to run through the above argument with ψ the final integral would not have converged absolutely. One would still expect the oscillatory term to cancel things out, but proving this would be more difficult.

All that remains to do (other than the analytic results put off till next section) is to turn this estimate for ϕ into an estimate for ψ. It is perhaps surprising that one can do this, since we are essentially differentiating an approximation. But since ψ behaves so nicely we can in fact do this.

Theorem 4.6. *For any integer k, $\psi(x) = x + O(\frac{x}{\log^{k/2} x})$.*

Proof. Suppose the $\varepsilon(x)$ is any function satisfying $0 < \varepsilon(x) \leq \frac{x}{2}$. Let $g_k(x) = \frac{x}{\log^k x}$. We have proved that for all sufficiently large x and some constant C,

$$x - Cg_k(x) \leq \phi(x) \leq x - Cg_k(x).$$

Therefore, since $g_k(2x) \leq g_k(x)$,

$$\phi(x + \varepsilon(x)) - \phi(x) \leq \varepsilon(x) + Cg_k(x + \varepsilon(x)) + Cg_k(x) \leq \varepsilon(x) + 3Cg_k(x).$$

On the other hand, since ψ is an increasing function,

$$\phi(x+\varepsilon(x))-\phi(x)=\int_x^{x+\varepsilon(x)}\frac{\psi(t)}{t}dt\geq\psi(x)\frac{\varepsilon(x)}{x+\varepsilon(x)}.$$

Combining these two equations shows that

$$\psi(x)\leq x+\varepsilon(x)+3Cg_k(x)\frac{x+\varepsilon(x)}{\varepsilon(x)}\leq x+\varepsilon(x)+\frac{6Cxg_k(x)}{\varepsilon(x)}.$$

Considering $\phi(x)-\phi(x-\varepsilon(x))$ in the same way yields

$$\phi(x)\geq x-\frac{2Cxg_k(x)}{\varepsilon(x)}.$$

Now we can choose $\varepsilon(x)$ in such a way to minimize the error term. The best such choice is $\varepsilon(x)=c\sqrt{xg_k(x)}$ where we choose c small enough so that we still have $\varepsilon(x)\leq\frac{x}{2}$. Plugging this expression into our previous results yields the theorem. □

This is equivalent to the prime number theorem. Plugging our estimate for ψ into our previous relations,

$$\pi(x)=\frac{x}{\log x}+\int_2^x\frac{1}{\log^2 t}dt+O\left(\frac{x}{\log^k x}\right).$$

However, by integration by parts, $\mathrm{Li}(x)=\frac{x}{\log x}+\int_2^x\frac{1}{\log^2 t}dt+O(1)$. Therefore, we have

$$\pi(x)=\mathrm{Li}(x)+O\left(\frac{x}{\log^k x}\right).$$

Notice that the approximation $\pi(x)=\frac{x}{\log x}$ only holds, a priori, up to $O\left(\frac{x}{\log^2 x}\right)$.

5 Some Facts About $\zeta(s)$.

Proposition 5.1. *For any real t, $\zeta(1+it)\neq 0$.*

Proof. Throughout this proof any time we use the symbol c it means a particular constant which may change from equation to equation.

Recall that

$$\log\zeta(s)\geq\sum_p p^{-s}+c.$$

Therefore,

$$\mathrm{Re}\zeta(s)\geq\sum_p\frac{\cos t\log p}{p^\sigma}+c.$$

If $s=1+it$ were a zero of the zeta function, then $\lim_{\sigma\to1^+}\log\zeta(\sigma+it)=-\infty$. Therefore,

$$\lim_{\sigma\to1^+}\frac{\cos t\log p}{p^\sigma}=-\infty.$$

This implies that the vast majority of numbers $\cos t\log p$ are near -1. Therefore, nearly all the numbers $\log p$ would lie near the points of the arithmetic progression $(2n+1)t^{-1}\pi$. This is impossible because this regularity would suggest that $\cos(2t\log p)$ were nearly 1 for the vast majority of primes. This in turn suggests that $\zeta(s)$ has a pole at $s=1+2it$.

Now we make this argument rigorous. Suppose $\zeta(s)$ had a zero at $s=1+it$, then $\zeta(s)/(s-1-it)$ would be analytic near $s=1+it$. In particular, taking the real part of log of $\zeta(s)/(s-1-it)$, we see that

$$\sum_p\frac{\cos(t\log p)}{p^\sigma}<\log(\sigma-1)+c.$$

Let $\delta > 0$ be some small positive number. Let S_1 be the sum of $p^{-\sigma}$ over all primes which satisfy $|(2n+1)\pi - t \log p| < \delta$ for some integer n, and let S_2 be the sum over primes which do not satisfy this condition. For terms in the second sum $\cos(t \log p) > -\cos\delta$. Therefore,

$$-S_1 - (\cos\delta)S_2 < \log(\sigma - 1) + K.$$

On the other hand, since there is a simple pole at 1, we have $S_1 + S_2 < -\log(\sigma - 1) + c$. Therefore,

$$-S_1 - (\cos\delta)S_2 < -S_1 - S_2 + c.$$

Therefore,

$$S_2 < \frac{c}{1 - \cos\delta}.$$

However, since $1+2\pi it$ is not a pole of $\zeta(s)$, the real part of $\log\zeta(s)$ is bounded above near $s = 1+2it$. Therefore

$$\sum_p \frac{\cos 2t \log p}{p^\sigma} < c.$$

Again we can split this sum up over the two sets of primes. For primes of the first type $\cos(2t \log p) > \cos 2\delta > 0$. Therefore,

$$S_1 \cos 2\delta - S_2 < c.$$

Therefore,

$$S_1 < \frac{c}{(1 - \cos\delta)\cos 2\delta}.$$

Hence, for some constant depending on δ, $S_1 + S_2 < C(\delta)$. Letting σ approach 1 makes the lefthand side blow up which is a contradiction.

For a more clever but perhaps less informative proof that a zero at $\zeta(1+it)$ would force a pole at $\zeta(1+2it)$ look at the proof of this result on one of the next few copied pages. □

The proofs of the following two results are on the next few photocopied pages.

Proposition 5.2. *Letting $s = \sigma + it$ as usual, we have the bound $\zeta^(k)(s) = O(\log^k t)$ in the region $\sigma > 1 - \frac{1}{\log t}$ and $t > 2$.*

Proposition 5.3. *Letting $s = \sigma + it$ as usual, we have the bound $\frac{1}{\zeta(s)} = O(\log^7 t)$ in the region $\sigma \geq 1$ and $t > 2$.*

Lectures # 7: The Class Number Formula For Positive Definite Binary Quadratic Forms.

Noah Snyder

July 17, 2002

1 Definitions

Definition 1.1. *A binary quadratic form (BQF) is a function $Q(x,y) = ax^2+bxy+cy^2$ (with $a,b,c \in \mathbb{Z}$) and will be denoted (a,b,c).*

These BQFs were first studied in an attempt to generalize Fermat's theorem that $n = x^2+y^2$ if and only if when we write $n = \prod p^{a_p}$ the exponent a_p is even for every prime $p \equiv 1 \pmod 4$.

Definition 1.2. *We say that a BQF Q represents a number n when there exist integers x and y such that $Q(x,y) = n$. If x and y are relatively prime then we say that Q properly represents n.*

Notice that if $d = \gcd(x,y)$ then $Q(x,y) = n$ if and only if $Q(\frac{x}{d},\frac{y}{d}) = \frac{n^2}{d}$. Since the latter representation is proper, to find all numbers represented by Q it is enough to find all the numbers it properly represents.

The basic question in the theory of BQF's is to find all numbers represented by a form Q and to find how many different ways there are to represent each of these numbers.

Definition 1.3. *If $Q = (a,b,c)$ is a BQF, we define the associated matrix (which by abuse of notation we will denote Q) to be*

$$\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}.$$

Proposition 1.4. *Let $v = \begin{pmatrix} x \\ y \end{pmatrix}$. Then*

$$Q(x,y) = v^T Q v.$$

Proof. This simply says that $ax^2+bxy+cy^2 = ax^2 + \frac{b}{2}xy + \frac{b}{2}yx + cy^2$. □

Notice that this means if we change variables $\begin{pmatrix} x' \\ y' \end{pmatrix} = v' = Av$ (the entries of A are integers) then $Q(x',y') = (Av)^T QAv = v^T(A^TQA)v$. Therefore, if Q represents a number then so does A^TQA. In particular, if A has an inverse with integer entries, then we get that Q and A^TQA represent all the same numbers. Clearly if A has an inverse B with integer entries, then $\det A \det B = \det AB = 1$, thus $\det A = \pm 1$. Furthermore one can easily show that if $\det A = \pm 1$ then A has an integer inverse. Lagrange defined two forms Q and Q' to be equivalent if there exists A with determinant ± 1 such that $A^TQA = Q'$. Gauss strengthened this notion as follows.

Definition 1.5. *We say that two forms Q and Q' are properly equivalent if there exists a matrix A such that $A^TQA = Q'$ and $\det A = 1$. If there exists a matrix A such that $A^TQA = Q'$ and $\det A = -1$ then we call the two BQFs improperly equivalent. Unless otherwise noted, when we say equivalent we mean properly equivalent.*

Notice that two BQFs can be both properly and improperly equivalent, for example $(1,0,1)$ is equivalent to itself under the identity transformation and under the transformation $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, thus it is improperly equivalent to itself.

Furthermore notice that proper equivalence is an equivalence relation (while improper equivalence is not).

Notice that if two forms Q and Q' are equivalent, then $\det Q' = \det A^T \det Q \det A = \det Q$. This suggests the following definition.

Definition 1.6. *The discriminant of a form Q is the integer $D_Q = -4 \det Q = b^2 - 4ac$.*

We have already proved that the discriminant is defined up to equivalence.

Notice that $D_Q \equiv b^2 \equiv 0$ or $1 \pmod 4$. Furthermore, if D_Q is a perfect square then Q factors as the product of two linear forms. Since the theory is trivial in this case we only consider forms Q with D_Q nonsquare.

Henceforth the number D will always denote a non-square integer congruent to 0 or 1 modulo 4.

Proposition 1.7. *Let $D = D_Q$ for some fixed form Q. If $D > 0$ then Q represents both positive and negative numbers. If $d < 0$ and $a > 0$ then Q represents only nonnegative numbers. If $d < 0$ and $a < 0$ then Q represents only nonpositive numbers.*

Proof. If $D > 0$ then $F(1,0) = a$ and $F(b,-2a) = -Da$. These two numbers have opposite signs. If $D < 0$ notice that $4aQ(x,y) = (2ax+by)^2 - dy^2 \geq 0$, from which the result follows. □

Definition 1.8. *If $D_Q > 0$ then we call Q indefinite. If $d < 0$ and $a > 0$ then Q is called positive definite. If $d < 0$ and $a < 0$ then Q is called negative definite.*

Since positive and negative definite forms are simply negatives of each other, we can ignore negative definite forms. In this week's lectures we will only be considering positive definite forms, indefinite forms will be dealt with in one of the projects. Many of the following results also hold for indefinite forms, finding which ones will be left as an exercise to the reader.

Finally we call a BQF primitive if a, b, and c are relatively prime. Again, if they weren't we could factor out the common factor and study that quadratic form and recover all the information about the original form. Thus from now on we will only consider

2 Class Number

Suppose we consider one particular equivalence class of BQFs. We would like to be able to pick a particularly nice representative of this class with small coefficients.

Theorem 2.1. *Every class contains a form for which $|b| \leq |a| \leq c$.*

Proof. Choose a form (a_0, b_0, c_0) belonging to the class in question. Let a be a nonzero number represented by (a_0, b_0, c_0) with minimal absolute value. Thus

$$a = a_0 r^2 + b_0 rt + c_o t^2.$$

We must have $\gcd(r,t) = 1$ or else $\frac{a}{\gcd(r,t)}$ would be represented contradicting minimality. Therefore we can find numbers u and t such that $ru - st = 1$.

A simple computation shows that $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ takes (a_0, b_0, c_0) to (a, b', c') for some integers b' and c'.

Now the transformation $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ takes (a, b', c') to $(a, 2ah + b', c(h))$. Thus for suitably chosen h, the second coefficient can be made smaller in absolute value than b. Therefore, we have found an element of the class (a,b,c) with $|b| \leq |a|$. Since $c \neq 0$ can be represented by Q we get $|a| \leq |c|$ as we had hoped to show. □

Therefore the number of distinct primary equivalence classes with a given discriminant is finite. This number is called the class number and will be denoted $h(D)$.

If $D =\equiv 0 \pmod 4$ then $(D, 0, 1)$ has discriminant D and if $D \equiv 1 \pmod 4$ then $(1, 1, \frac{1-D}{4})$ has discriminant D. Thus for any D, $h(D) > 0$.

Letting $\chi(n) = \left(\frac{D}{n}\right)$ Our goal is to give a formula for $h(D)$ in terms of $L(1, chi)$. As a consequence we will see that $L(1, \chi) \neq 0$.

3 Which Numbers are Represented by Some Form With Discriminant D.

Theorem 3.1. *The numbers properly represented by Q are exactly the numbers a' which appear as the first term of forms equivalent to Q.*

Proof. If $Q = (a, b, c) \sim (a', b', c')$ via the matrix $A = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$, then $n = Q(r, t)$. Since $\det A = 1$, this representation is proper.

In our proof of the finiteness of class number we should that if a number a' was properly represented by Q then Q is equivalent to (a', b', c') for some b' and c'. □

Theorem 3.2. *If n is properly representable by $Q = (a, b, c)$ with discriminant D, then $D \equiv \Box \pmod{4|n|}$.*

Proof. By the last theorem there exist some b' and c' such that $(a, b, c) \sim (n, b', c')$. Thus $b'^2 - 4nc' = D$. The theorem follows. □

Theorem 3.3. *If $D \equiv \Box \pmod{4|n|}$, then n is properly by some form of discriminant D.*

Proof. By assumption there exists some integers ℓ and k such that $\ell^2 = D - 4nk$. Therefore the form (n, ℓ, k) has discriminant D and represents n. □

Furthermore, for each choice of $\ell^2 \equiv D \pmod{4n}$ with $0 \leq \ell < 2k$, there is only one form written in the form (n, ℓ, k) with discriminant D.

4 An Application

Theorem 4.1. *An odd prime p can be written in the form $x^2 + y^2$ exactly when $p \equiv 1 \pmod 4$.*

Proof. Let $Q = (1, 0, 1)$. This has discriminant -4. Suppose (a, b, c) is a reduced representative of some equivalence class with discriminant D. Thus $|b| \leq a \leq |c|$ and $b^2 - 4ac = -4$. Thus $b^2 = 4(ac - 1)$. Since $|ac| \geq b^2$ we must have $ac - 1 = 0$. Thus the only such form is $(1, 0, 1)$. Therefore, $h(-4) = 1$. Hence p is representable by $(1, 0, 1)$ if and only if $-4 \equiv \Box \pmod{4p}$. Thus if and only if $\left(\frac{-1}{p}\right) = 1$. By the supplementary law to QR we're done. □

Similarly one can show that $p = x^2 + 2y^2$ exactly when $p \equiv 1$ or $3 \pmod 8$.

5 Number of Representations

We want to find the number of ways in which we can properly represent n by some BQF of fixed discriminant $D < 0$. By arguments we have already made it suffices to find every transformation $A = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ with $\det A = 1$ sending Q to itself. For this to happen we must have

$$a = ar^2 + brt + ct^2,$$

$$b = 2ars + b(1 + 2st) + 2ctu.$$

Therefore we must also have, $0 = ars + bst + ctu$.

We can eliminate b to get, $as = cst^2 - crtu = -ct$. On the other hand we can eliminate c to get, $a(u-r) = bt$. Therefore, $a|ct$ and $a|bt$. If Q is primitive, then $a|t$. Let $t = at'$. Therefore, $s = -ct'$ and $u - r = bt'$. Hence it follows that,

$$(u+r)^2 = (u-r)^2 + 4ur = b^2t'^2 + 4(1+st) = b^2t'^2 + 4(1 - act'^2) = Dt'^2 + 4.$$

Therefore, $(u+r)^2 - Dt'^2 = 4$. If $D = -3$ then there are 6 solutions. If $D = -4$ there are 4 solutions. If $D < -4$ then there are only 2 solutions. We let w denote this number of solutions.

Theorem 5.1. *Suppose n is an integer relatively prime to D. If n is divisible by μ distinct primes each of which has $\left(\frac{D}{p}\right) = 1$ but by no other primes, then n can be represented in $w2^\mu$ distinct ways by a primitive form of discriminant D. Otherwise n cannot be represented by a primitive form of discriminant D.*

Proof. Recall that each pair of solutions of $\ell^2 \equiv D \pmod{4n}$ gives us exactly w ways of representing n by some form of discriminant K. We factor $4n$ as a product of primes and use the Chinese remainder theorem to reduce to counting the number of square roots of D modulo a prime power p^k.

For each odd prime we can write D as a square modulo p^k in exactly $1 + \left(\frac{D}{p}\right)$ ways.

Now we turn our attention to the prime 2. Suppose n is odd. Then the power of two we are looking at is 4. Since $D \equiv 0$ or $1 \pmod 4$ it can be written as a square in exactly 2 ways. If n is even then we are looking modulo at least 8. Since n is relatively prime to D, $D \equiv 1 \pmod 4$. Thus D can be written as a square in $2(1 + \left(\frac{D}{2}\right))$ ways.

By only counting one solution from each pair, for the last two cases we should only consider half the solutions. Thus, for each prime with $\left(\frac{D}{p}\right) = 1$ we pick up 2 solutions, and modulo the product we end up with 2^μ pairs of solutions. Thus the total number of representations is $w2^\mu$. □

It follows that:

Theorem 5.2. *We have*

$$\sum_Q \sum_{x,y} Q(x,y)^{-s} = w \sum_{m=1}^{\infty} \frac{2^\mu}{m^s},$$

where Q runs over each primary class once and x and y run over all relatively prime pairs with $Q(x,y)$ relatively prime to D.

□

The right hand side has an Euler factorization.

$$\sum_{m=1}^{\infty} \frac{2^\mu}{m^s} = \prod_{p:\ \left(\frac{D}{p}\right)=1} 1 + \frac{2}{p^s} + \frac{2}{p^2s} + \ldots = \prod_{p:\ \gcd(p,D)=1 \text{ and } \left(\frac{D}{p}\right)=1} \frac{1+p^{-s}}{1-p^{-s}}.$$

Therefore,

$$\sum_Q \sum_{x,y} Q(x,y)^{-s} = w \prod_{\gcd(p,D)=1} \frac{1+p^{-s}}{1 - \left(\frac{D}{p}\right) p^{-s}} = w \frac{L(s,\chi_0)L(s,\chi}{L(2s,\chi_0)}.$$

If we multiply both sides by $L(2s,\chi_0)$, the left hand side becomes

$$\sum_n \sum_{x,y \text{relatively prime}} (n^2 Q(x,y))^{-s} = \sum_n \sum_{x,y \text{relatively prime}} Q(nx,ny)^{-s} = \sum_{x',y'} Q(x',y'),$$

where each of these sums range over all pairs with Q relatively prime to D and where the last sum ranges over *all* such pairs.

Therefore, (still summing over $Q(x,y)$ relatively prime to D),

$$\sum_Q \sum_{x,y} Q(x,y)^{-s} = wL(s,\chi_0)L(s,\chi).$$

Dirichlet noticed that if you multiply both sides by $(s-1)$ and send $s \to 1^+$ then you get well-defined limit. The righthand side is $\frac{w\varphi(|D|)}{|D|}L(1,\chi)$.

Proposition 5.3. *Suppose a_n is a sequence. Let $f(x) = \sum_{n \leq x}$ such that*

$$\lim_{x\to\infty} \frac{f(x)}{x} \to c.$$

Then

$$\lim_{s\to 1^+} (s-1) \sum_{n=1}^{\infty} \frac{a_n}{n^s} = c.$$

Proof. This proposition states that if some sequence has a well-defined density, then it also has a well-defined Dirichlet density and the two are equal. The converse, however, is not true.

If $f(n-1) < i \leq f(n)$ then let $k_i = n$. Notice that the multiset of all the $k's$ contains the element n exactly a_n times. Thus

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \sum_{i=1}^{\infty} k_i^{-s}.$$

Let $h_n = \frac{n}{k_n}$. We claim $\lim_{n\to\infty} h_n = c$. Notice that $h_{f(n)} = \frac{f(n)}{n}$. Thus the smallest that h_x can get is $\frac{f(n)}{n-1}$. This limit still approaches c.

Notice,

$$\lim_{s\to 1^+} (s-1) \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \lim_{s\to 1^+} (s-1) \sum_{n=1}^{\infty} \frac{h_n^s}{n^s}.$$

The righthand side can be easily evaluated. For any $\varepsilon > 0$ we can choose N large enough such that for all $n \geq N$, $c - \varepsilon < h_n < c + \varepsilon$. With this choice, splitting the sum up into terms less than and greater than N,

$$\lim_{s\to 1^+} (s-1)(c-\varepsilon)^s \zeta(s) \leq \lim_{s\to 1^+} (s-1) \sum_{n=1}^{\infty} \frac{h_n^s}{n^s} \leq \lim_{s\to 1^+} (s-1)(c+\varepsilon)^s \zeta(s).$$

Thus the limit is sandwiched between $c - \varepsilon$ and $c + \varepsilon$ and so goes to c. □

Proposition 5.4. *One can find Q in a given equivalence class such that a is relatively prime to a given number m.*

Proof. This is equivalent to saying that we can choose x and y so that $Q(x,y)$ is relatively prime m. Choose any prime $p|m$. If $p|a$ and $p|c$, then $p \nmid b$, so if we choose x and y both prime to p Q will also be prime to p. If $p \nmid a$ (resp. c) then we can choose x prime to p and y divisible by p (resp. x divisible by p and y prime to p). By the Chinese remainder theorem we can choose x and y subject to the above conditions for every prime $p|m$. □

Theorem 5.5. *For any fixed Q, (taking the sum over $Q(x,y)$ relatively prime to D as usual)*

$$\lim_{s\to 1^+} s \sum_{x,y} Q(x,y)^{-s} = \frac{\varphi(|D|)}{|D|} \frac{2\pi}{\sqrt{|D|}}.$$

Proof. By our first lemma it is enough to compute the ordinary density $\lim_{n\to\infty} \frac{f(n)}{n}$ where $f(n)$ is the number of values $Q(x,y) \leq n$ relatively prime to D.

First we deal with the issue of finding which pairs make $Q(x,y)$ relatively prime to D. Notice that this is just a question of what the values of Q are on $\mathbb{Z}/D\mathbb{Z}$. By our second lemma we can choose our representative Q such that each one has a relatively prime to D.

Suppose D is odd and thus b is odd. Thus $ax^2 + bxy + cy^2$ is relatively prime to D exactly when $2a(ax^2 + bxy + cy^2) = (2ax + by)^2 - Dy^2$ is. Now, no matter what we choose for y we only need to have $(2ax + by)$ relatively prime to D. As x varies this runs through a complete residue system, thus the total number of solutions is $D\varphi(D)$.

Suppose D is even and thus b is even. Thus $ax^2+bxy+cy^2$ is relatively prime to D exactly when $a(ax^2+bxy+cy^2)=(ax+\frac{b}{2}y)^2-\frac{D}{4}y^2$ is. If y is even then it is sufficient to choose $ax+\frac{b}{2}y$ relatively prime to D. This runs through a complete system of residues as x runs through one, thus with y even there are $\frac{D}{2}\varphi(D)$ solutions. If y is odd, and $\frac{D}{4}$ is even, then we are in exactly the same situation and there are $\frac{D}{2}\varphi(D)$ more solutions. If y is odd and $\frac{D}{4}$ is odd then we need to choose $ax+\frac{b}{2}y$ even and relatively prime to $\frac{D}{4}$. Since this expression still runs through a complete residue system modulo D there are $\frac{D}{2}2\varphi\left(\frac{D}{4}\right)=\frac{D}{2}\varphi(D)$. For both of these cases the total number of pairs which give $Q(x,y)$ relatively prime to D is $D\varphi(D)$.

Thus if we let $f_{x_0,y_0}(n)$ denote the number of values $Q(x,y)\le x$ in some particular equivalence class $(x,y)\equiv(x_0,y_0) \pmod{D}$, it is sufficient to prove

$$\lim_{n\to\infty}\frac{f(n)}{n}=\frac{1}{|D|^2}\frac{2\pi}{\sqrt{|D|}}.$$

The condition $Q(x,y)\le n$ says that (x,y) should lie in an ellipse which expands uniformly as n increases. We would thus expect the number of points in some particular equivalence class to be $\frac{1}{|D|^2}Area$. The are of the ellipse is $\frac{2\pi}{\sqrt{|D|}}n$. Thus we would expect $\frac{f(n)}{n}\approx\frac{1}{|D|^2}\frac{2\pi}{\sqrt{|D|}}$.

To make this argument rigorous, divide the plane into squares of side $|D|$. For every square in the interior of the ellipse $Q(x,y)\le n$ we should count it once. For squares on the boundary we may or may not count the square depending on whether the lattice point in our equivalence class lies there. Scaling the whole picture by $\frac{1}{n}$ we are looking at the plane divided into squares of side $\frac{|D|}{n}$ and we want to find the number of squares contained in (and possibly on the boundary) of the ellipse $Q(x,y)\le 1$. By integral calculus, this limit is the area of the ellipse $Q(x,y)\le 1$ regardless of whether we count boundary points. Therefore $\lim_{n\to\infty}\frac{f(n)}{n}=\frac{1}{|D|^2}\frac{2\pi}{\sqrt{|D|}}$.

Thus we've proved our result. □

Theorem 5.6.

$$L(1,\chi)=h(D)\frac{2\pi}{w\sqrt{|D|}}\neq 0$$

and

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

Proof. We have shown that (letting Q run over representatives of each class and x and y range over pairs with $Q(x,y)$ prime to D)

$$\sum_{Q}\sum_{x,y}Q(x,y)^{-s}=wL(s,\chi_0)L(s,\chi).$$

Multiply both sides by $(s-1)$ and send $s\to 1^+$. We have already evaluated these limits, thus

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

Rearranging gives our two formulas. □

Notice, by the methods of homework 2 we can write $L(1,\chi)$ as a finite sum:

$$L(1,\chi)=-\frac{\pi}{\sqrt{|D|}}\sum_{m=1}^{|D|}m\chi(m)=-\frac{\pi}{\sqrt{|D|}}\frac{D}{2-\chi(2)}\sum_{m=1}^{\frac{|D|}{2}}\chi(m).$$

Therefore,

$$h(D)=\frac{1}{2-\chi(2)}\sum_{m=1}^{\frac{|D|}{2}}\chi(D).$$

Notice that since $h(D)$ is positive, most of the squares modulo D lie between 0 and $\frac{|D|}{2}$. Interestingly enough there is no known non-analytic proof of this fact.

This also gives a very quick way of finding a give class number. Unfortunately, the method of simply finding all reduced forms actually works more quickly. Using the functional equation of the L-series, however gives a much more efficient way of computing this value.

Finally we would like to notice that if D is squarefree (except for possibly 4) every form is primary and we could have found a formula for the number of representations of n even when n was not relatively prime to D. In this case D is a square modulo p in one way but not a square p^2 for every prime dividing n and D (unless that prime is 2 in which case it takes a tad more work). Thus we get representations when the number is also a product of primes dividing D each taken to the first power. Plugging this into our equations gives the nicer formula (where we now only sum over x and y not both zero)

$$\sum_{x,y} Q(x,y)^{-s} = \zeta(s)L(s,\chi).$$

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. □

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. □

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:*

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

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 $\mathbb{Z}/p[x]/(x^2+1)$. 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. □

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.

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

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,

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

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 $\mathcal{O}_{\sqrt{d}} \to \mathbb{F}_q$ 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. □

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 $NA = (\alpha\bar{\alpha}, \alpha\bar{b}eta, \beta\bar{\alpha}, \beta\bar{\beta})$. We want to find some rational integer $n \in NA$ such that $\frac{\alpha\bar{\alpha}}{n}, \frac{\alpha\bar{b}eta}{n}, \frac{\beta\bar{\alpha}}{n}, \frac{\beta\bar{\beta}}{n}$ 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 $n|(\alpha\bar{b}eta + \beta\bar{\alpha})$. Thus we let $n = \gcd(\alpha\bar{\alpha}, \beta\bar{\beta}, \alpha\bar{b}eta + \beta\bar{\alpha})$ this is clearly in A and we've shown that $A \supseteq n\mathcal{O}$, thus $A = n\mathcal{O}$. □

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. □

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 $\beta \in B$.

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 $AC = B$. □

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. □

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. □

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 Na^2 elements, thus $\mathcal{O}/A$ has finitely many elements. But any finite domain is a field. □

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 was 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):

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

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 $NA = n\mathcal{O}$. □

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. □

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. □

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 $M \in \mathrm{SL}_2(\mathbb{Z})$ 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 $\lim_{s\to\frac{1}{2}} F(s) = 0$.

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 $\lim_{s\to\frac{1}{2}} F(s) = 0$. □