Techniques from Analytic Number Theory

Class Notes from Math 58 / WRS

December 5-7, 2006

1 Chebyshev and the Prime Number Theorem

We begin by proving Chebyshev's version of the prime number theorem.

Theorem 1 (Chebyshev) *There are constants C_1 and C_2 for which*

$$C_1 \frac{x}{\ln x} \leq \pi(x) \leq C_2 \frac{x}{\ln x}$$

for all sufficiently large x.

Actually the Prime Number Theorem says that Theorem 1 holds with $C_1 = 1 - \epsilon$ and $C_2 = 1 + \epsilon$ for any small positive ϵ. We'll prove it for $C_1 = \ln(\sqrt{2}) \approx 0.35$ and $C_2 = 2 \ln 16 \approx 5.5$. It's a start.

Proof. Define

$$M(x) = \text{LCM}\,\{n | n \leq x\} \tag{1}$$

(or $M(x) = 1$ if $x \leq 1$); then for each prime $p \leq x$, $M(x)$ contains a factor of p^k where p^k is the largest power of p that is $\leq x$. For each such p,

$$\sqrt{x} \leq p^k \leq x \tag{2}$$

(because if p^k were less than $\sqrt{x}$, we could square p^k to get a higher power of p still less than x). There are exactly $\pi(x)$ of these prime-power factors, so

$$\sqrt{x}^{\pi(x)} \leq M(x) \leq x^{\pi(x)} \tag{3}$$

or

$$x^{\frac{1}{2}\pi(x)} \leq M(x) \leq x^{\pi(x)}. \tag{4}$$

Define $\psi(x) = \ln(M(x))$ (*Chebyshev's psi function*). Taking logs in (4) gives

$$\frac{1}{2}\pi(x) \ln x \leq \psi(x) \leq \pi(x) \ln x. \tag{5}$$

Turning this around gives bounds on $\pi(x)$:

$$\frac{\psi(x)}{\ln x} \le \pi(x) \le 2\frac{\psi(x)}{\ln x}. \tag{6}$$

(The factor of 2 in (6) can be avoided; it can be replaced by a function of x that approaches 1 as $x \to \infty$. The idea is that the left side of (3) is way too weak, since most of the prime power factors of $M(x)$ are much larger than $\sqrt{x}$. With the factor of 2 neutralized, (6) implies that $\pi(x) \sim \frac{\psi(x)}{\ln x}$, so the PNT is equivalent to the statement that $\psi(x) \sim x$. Most proofs of the PNT are actually proofs that $\psi(x) \sim x$.)

At this stage in class we considered the binomial coefficient $\left(\begin{smallmatrix} 2n \\ n \end{smallmatrix}\right)$, and I didn't quite close the gap between real x and integer $2n$. In these notes we explicitly define $\left(\begin{smallmatrix} x \\ x/2 \end{smallmatrix}\right) = \frac{\lfloor x \rfloor !}{\lfloor x/2 \rfloor !^2}$. If x is an even integer, $x = 2n$, then $\left(\begin{smallmatrix} x \\ x/2 \end{smallmatrix}\right)$ is the same as $\left(\begin{smallmatrix} 2n \\ n \end{smallmatrix}\right)$. This is still true if x is $2n$ plus a fraction, so that $\lfloor x \rfloor = 2n$. But if $\lfloor x \rfloor = 2n+1$, then $\left(\begin{smallmatrix} x \\ x/2 \end{smallmatrix}\right) = n\left(\begin{smallmatrix} 2n \\ n \end{smallmatrix}\right)$. I missed the factor of n in class.

It's easy to show that $2^n \le \left(\begin{smallmatrix} 2n \\ n \end{smallmatrix}\right) \le 2^{2n}$. Here's a fun combinatorial proof, also missed in class: A room contains $2n$ people, arranged into n couples. Then:

- 2^n is the number of subsets containing one person from each couple;
- $\left(\begin{smallmatrix} 2n \\ n \end{smallmatrix}\right)$ is the number of subsets containing n people, regardless of couples;
- 2^{2n} is the number of subsets of all sizes.

So clearly $2^n \le \left(\begin{smallmatrix} 2n \\ n \end{smallmatrix}\right) \le 2^{2n}$. Now if x is any number in $[2n, 2n+2)$ then $\left(\begin{smallmatrix} x \\ x/2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2n \\ n \end{smallmatrix}\right)$ or $n\left(\begin{smallmatrix} 2n \\ n \end{smallmatrix}\right)$, so in any case $\left(\begin{smallmatrix} x \\ x/2 \end{smallmatrix}\right) \le n\left(\begin{smallmatrix} 2n \\ n \end{smallmatrix}\right) \le n2^{2n} \le x2^x$, and since $x < 2^x$ always, this gives

$$\left(\begin{smallmatrix} x \\ x/2 \end{smallmatrix}\right) \le 2^{2x} \tag{7}$$

for every $x \ge 1$.

On the other side we have proved $2^{(x/2)} \le \left(\begin{smallmatrix} x \\ x/2 \end{smallmatrix}\right)$ only when x is an even integer. But it's true whenever $4 \le x \le 6$, and the right side more than doubles whenever x increases by 2, so we have

$$2^{(x/2)} \le \left(\begin{smallmatrix} x \\ x/2 \end{smallmatrix}\right) \tag{8}$$

whenever $x \ge 4$.

(Both (7) and (8) are unnecessarily weak bounds. By using Stirling's formula for factorials, I think we can show that

$$\frac{2^x}{4\sqrt{x}} \le \left(\begin{smallmatrix} x \\ x/2 \end{smallmatrix}\right) \le 2^x\sqrt{x}. \tag{9}$$

These are much tighter bounds, but as I write this, I haven't actually checked the details.)

Now let's do some prime counting in the expression $\left(\begin{array}{c} x \\ x/2 \end{array} \right) = \frac{\lfloor x \rfloor !}{\lfloor x/2 \rfloor !^2}$. Every prime or prime power p^k in the range $x/2 < p^k \leq x$ contributes p to the numerator, and nothing to the denominator. These are exactly the contributions to $M(x)$ that haven't already occurred in $M(x/2)$, so we have

$$\frac{M(x)}{M(x/2)} \leq \left(\begin{array}{c} x \\ x/2 \end{array} \right). \tag{10}$$

On the other hand, every prime power p^k can appear at most once more in the numerator than in the denominator, so

$$\left(\begin{array}{c} x \\ x/2 \end{array} \right) \leq M(x). \tag{11}$$

These inequalities may take a while to absorb. What's going on is that p appears in the numerator $\lfloor x/p \rfloor$ times, but it appears in the denominator $2\lfloor (x/2)/p \rfloor$ times. What is the relationship between these numbers? If x/p rounds down to an even integer, then they are the same: $\lfloor x/p \rfloor = 2\lfloor (x/2)/p \rfloor$. But if x/p rounds down to an odd integer, then $\lfloor x/p \rfloor = 2\lfloor (x/2)/p \rfloor + 1$. So, the difference between the number of appearances of p (or p^k) in the numerator and the number of appearances in the denominator is always either 0 or 1. If it were always 1 (and always 1 for prime powers, too) we would have equality in (11).

(Continuing one more step gives

$$\left(\begin{array}{c} x \\ x/2 \end{array} \right) = \left(\frac{M(x)}{M(x/2)} \right) \left(\frac{M(x/3)}{M(x/4)} \right) \left(\frac{M(x/5)}{M(x/6)} \right) \cdots \tag{12}$$

which is actually a finite product because eventually, all the factors are 1/1. In logs,

$$\ln \left(\begin{array}{c} x \\ x/2 \end{array} \right) = \psi(x) - \psi(x/2) + \psi(x/3) - \psi(x/4) + \psi(x/5) - \psi(x/6) + \cdots. \tag{13}$$

The last expression is a finite sum and is actually exact. It's also an alternating sequence with terms that decrease in absolute value, so any two consecutive partial sums surround its true value. In our main argument, we're just using the first two partial sums. It must be possible to use the entire series to good advantage, but I don't know how, yet.)

Let's combine (10) and (7) and then take logs:

$$\frac{Mx}{M(x/2)} \leq 2^{2x} \tag{14}$$

$$\psi(x) - \psi(x/2) \leq 2x \ln 2. \tag{15}$$

Since this holds for every $x \geq 1$ — well, really for every $x > 0$ — we can run a cascade:

$$\psi(x) \leq 2x \ln 2 + \psi(x/2)$$

$$\begin{aligned} &\leq 2x\ln 2 + 2\frac{x}{2}\ln 2 + \psi(x/4) \\ &\leq 2x\ln 2 + 2\frac{x}{2}\ln 2 + 2\frac{x}{4}\ln 2 + \cdots \\ &\leq 4x\ln 2 \\ &= x\ln 16. \end{aligned} \tag{16}$$

The other side is quicker; just combine (11) and (8) and take logs to get

$$\begin{aligned} 2^{x/2} &\leq M(x) \\ x\ln\sqrt{2} &\leq \psi(x) \end{aligned} \tag{17}$$

when $x \geq 4$.

We use these bounds on $\psi(x)$ along with (6) to get

$$\left(\ln\sqrt{2}\right)\frac{x}{\ln x} \leq \pi(x) \leq (2\ln 16)\frac{x}{\ln x}. \tag{18}$$

These constants are about 0.35 and 5.5. □

It is possible to get much better constants by doing the work to banish that "2" in (6) and by using the bounds based on Stirling's formula. But we can't make the constants approach 1 unless we go beyond the second partial sum of our series for $\binom{x}{x/2}$. I don't know whether that approach eventually leads to a proof of the prime number theorem.

2 Euler Products and Dirichlet's Theorem

This is nonsense:

$$\begin{aligned} &1+2+3+4+5+\cdots = \\ &\quad (1+2+2^2+2^3+\cdots)(1+3+3^2+3^3+\cdots)(1+5+\cdots)(1+7+\cdots)(1+11+\cdots)\cdots \end{aligned} \tag{19}$$

because neither side even comes close to converging. But it really wants to be true. Note that there is one factor on the right side for each prime, and each factor includes a term for each power of its prime. So, when we multiply it out, the (finite) terms of the product are of the form $p_1^{a_1}p_2^{a_2}p_3^{a_3}\cdots p_k^{a_k}$. (We get some infinite terms, too, but that's just one more reason that (19) is nonsense.) Since each number n on the left can be represented in exactly one way as

$$n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\cdots p_k^{a_k} \tag{20}$$

the equation seems to have some promise.

We can salvage it by taking any completely multiplicative function, say g, and substituting its values for the integers in (19). Then $g(1) = 1$ and $g(p^k) = g(p)^k$ always, and

the equation becomes

$$g(1) + g(2) + g(3) + \cdots = \\ (1 + g(2) + g(2)^2 + \cdots)(1 + g(3) + g(3)^2 + \cdots)(1 + g(5) + g(5)^2 + \cdots)(1 + g(7) + g(7)^2 + \cdots)\cdots \tag{21}$$

Now if n has the prime factorization given above, then

$$g(n) = g(p_1)^{a_1} g(p_2)^{a_2} g(p_3)^{a_3} \cdots g(p_k)^{a_k}. \tag{22}$$

Each term $g(n)$ appears once on the left of (21) and each term $g(p_1)^{a_1} g(p_2)^{a_2} g(p_3)^{a_3} \cdots g(p_k)^{a_k}$ appears once on the right. In fact, (21) is true whenever the left side converges absolutely.

The factors on the right of (21) are geometric series, so they can be simplified. For example,

$$1 + g(2) + g(2)^2 + g(2)^3 + \cdots = \frac{1}{1 - g(2)}. \tag{23}$$

This means that we can write (21) in this compact form:

$$\sum_{n \geq 1} g(n) = \prod_{p \text{ prime}} \left(\frac{1}{1 - g(p)} \right). \tag{24}$$

The representation on the right is called an *Euler product,* or an *Euler product representation* of the series $\sum g(n)$. You can do this with any series whose terms are given by a completely multiplicative function. When the series converges absolutely, it is equal to the corresponding Euler product.

Consider an example. Pick a real number $s \geq 1$, and let $g(n) = 1/n^s$. Then g is completely multiplicative, and the left side of (21) becomes

$$\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \cdots. \tag{25}$$

When $s = 1$, this series is the harmonic series, which diverges. But when $s > 1$, the series converges absolutely (as can be proven by the integral test). In that case it defines the famous *Riemann zeta function,* $\zeta(s)$. (Using that name and notation gives to s a more prominent role than we prefer, so we will use them sparingly. In these notes we prefer to think of s as an afterthought whose main purpose is to make our series converge.) The Euler product representation of this series is

$$\sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(\frac{1}{1 - \frac{1}{p^s}} \right) \tag{26}$$

which is a true statement when $s > 1$.

Here is an application of this line of reasoning.

Theorem 2 *There are infinitely many primes.*

Proof. When $s \to 1^+$, the left side of (26) approaches ∞; that is, it becomes arbitrarily large. So the right side must become arbitrarily large, too. But each factor on the right approaches an easily computed finite limit as $s \to 1^+$. So, in order to become arbitrarily large, the product on the right must have infinitely many factors. □

We can do better.

Theorem 3 $\displaystyle\sum_{p \text{ prime}} \frac{1}{p} = \infty.$

Proof. Take logs in (26):

$$\begin{aligned} \ln\left(\sum_{n\geq 1} \frac{1}{n^s}\right) &= \sum_{p \text{ prime}} \ln\left(\frac{1}{1-\frac{1}{p^s}}\right) \\ &\approx \sum_{p \text{ prime}} \frac{1}{p^s}. \end{aligned} \tag{27}$$

The approximation comes from the Taylor series for $\ln\left(\frac{1}{1-x}\right)$. We'll skip the details, but the approximation is close enough for our purpose. Since the left side approaches ∞ as $s \to 1^+$, so does the right side. □

Now let's try this with a different multiplicative function. Let

$$g(n) = \frac{\chi(n)}{n^s}$$

with

$$\chi(n) = \begin{cases} 0 & \text{if } n \text{ even} \\ -1 & \text{if } n \equiv 3 \pmod 4 \\ +1 & \text{if } n \equiv 1 \pmod 4 \end{cases} \tag{28}$$

The function χ is completely multiplicative, so the term $\chi(n)/n^s$ is completely multiplicative. The Euler product is

$$\begin{aligned} &1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \cdots = \\ &\quad \left(1 - \frac{1}{3^s} + \frac{1}{(3^s)^2} - \cdots\right)\left(1 + \frac{1}{5^s} + \frac{1}{(5^s)^2} - \cdots\right)\left(1 - \frac{1}{7^s} + \frac{1}{(7^s)^2} - \cdots\right)\cdots. \end{aligned} \tag{29}$$

The right side has one factor for every odd prime, and the factor has alternating signs if the prime is $\equiv 3 \pmod 4$, and all positive signs if the prime is $\equiv 1 \pmod 4$. We can thus write

$$1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \cdots = \prod_{\substack{p \text{ prime} \\ p \equiv 3 \pmod 4}} \left(\frac{1}{1 + \frac{1}{p^s}} \right) \prod_{\substack{p \text{ prime} \\ p \equiv 1 \pmod 4}} \left(\frac{1}{1 - \frac{1}{p^s}} \right). \tag{30}$$

Now, when $s = 1$ the left side of this equation converges conditionally to a finite, non-zero number. (That's easy to prove because the series is an alternating series with decreasing absolute values. According to the Theoretical Computer Science Cheat Sheet, it actually converges to $\pi/4$.) It isn't as easy as it looks to prove that the limit of the left side when $s \to 1+$ is the same finite, non-zero, value, but it is true and can be proved by elementary means. (We don't need Abel's theorem.)

Approximating as before,

$$\ln\left(1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \cdots\right) \approx -\left(\sum_{\substack{p \text{ prime} \\ p \equiv 3 \pmod 4}} \frac{1}{p^s} \right) + \left(\sum_{\substack{p \text{ prime} \\ p \equiv 1 \pmod 4}} \frac{1}{p^s} \right). \tag{31}$$

Taking the limit as $s \to 1+$:

$$\text{some finite number} = -\left(\sum_{\substack{p \text{ prime} \\ p \equiv 3 \pmod 4}} \frac{1}{p} \right) + \left(\sum_{\substack{p \text{ prime} \\ p \equiv 1 \pmod 4}} \frac{1}{p} \right). \tag{32}$$

Write the right side of the last equation as $-A + B$. We have just proved that if $-A + B$ exists, it must be finite. So, it cannot be the case that one of A and B is finite, and the other infinite. But $A + B$ is the sum from Theorem 3, so A and B can't both be finite. So, they are both infinite. So, both sums have infinitely many terms.

Theorem 4 (Dirichlet, mod 4) *There are infinitely many primes of the form $4k + 1$, and infinitely many primes of the form $4k + 3$. Furthermore,*

$$\sum_{\substack{p \text{ prime} \\ p \equiv 1 \pmod 4}} \frac{1}{p} = \infty \qquad \textit{and} \qquad \sum_{\substack{p \text{ prime} \\ p \equiv 3 \pmod 4}} \frac{1}{p} = \infty.$$

□

Yes, we proved the first two claims before, by elementary means. But this method gives a stronger result, and it generalizes to all arithmetic progressions. After surmounting a few obstacles it gives the full version of Dirichlet's theorem.

3 Dirichlet Series and Convolutions

A *Dirichlet series* is a series of the form

$$\sum_{n \geq 1} \frac{a_n}{n^s} = \frac{a_1}{1^s} + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \frac{a_4}{4^s} + \frac{a_5}{5^s} + \frac{a_6}{6^s} + \cdots \tag{33}$$

The a_n's in the numerators are called the *coefficients.* You might think of them as the values of an arithmetic function: $a_n = g(n)$. You can make a Dirichlet series out of any sequence $\{a_n\}$ or arithmetic function $g(n)$. Many techniques involve freely jumping back and forth between these forms:

$$\text{sequence } a_1, a_2, \ldots \longleftrightarrow \text{arithmetic function } g(n) = a_n \longleftrightarrow \text{Dirichlet series } \frac{a_1}{1^s} + \frac{a_2}{2^s} \cdots.$$

We often think of a Dirichlet series as defining a function of s:

$$f(s) = \sum_{n \geq 1} \frac{a_n}{n^s} \tag{34}$$

valid for those s for which the sum converges. But for now, we would rather treat s as an annoying detail than as a central player.

The coefficients a_n need not be integers. They can be anything, as long as we can divide them by numbers and add them. Also, if you like, you can allow s or the a_n's to be complex. (Definition: $n^s = \exp(s \ln n)$, where exp is defined by its series representation.)

The "simplest" example has $a_n = 1$ for all n. As noted above, it is the Riemann zeta function, $\zeta(s) = \sum 1/n^s$. This definition of the zeta function works when $s > 1$ (or $\mathrm{Re}(s) > 1$ if s is complex); other definitions are used to extend the zeta function to other values of s. We know that $\zeta(2) = \frac{\pi^2}{6}$ and we know the values of $\zeta(s)$ for other even integers s, but we don't know exact values of $\zeta(s)$ for any other positive real s. We do know that $\zeta(3)$ is irrational.

There is an analogy to power series: If you give a sequence $a_0, a_1, a_2, \ldots$ to functional analysts, they'll make it into a power series: $f(x) = a_0 + a_1 x^1 + a_2 x^2 + \cdots$. Standard theorems then connect the coefficients to the properties of the function; *e.g.,* $a_n = f^{(n)}(0)/n!$. We would like to do the same thing with Dirichlet series. (But note: a Dirichlet series is definitely not a power series.)

Two things are wonderful about Dirichlet series:

- As we have seen, if the a_n's are completely multiplicative ($a_n a_m = a_{nm}$ always) then we have an Euler product,

$$\sum_{n \geq 1} \frac{a_n}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - \frac{a_p}{p^s}} \tag{35}$$

  whenever the left side converges absolutely.

- Multiplying the functions defined by Dirichlet series corresponds to convolution (or "Dirichlet product," $*$) of their coefficient series. That is, if we have

$$\begin{aligned} f(s) &= \frac{a_1}{1^s} + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \frac{a_4}{4^s} + \frac{a_5}{5^s} + \frac{a_6}{6^s} + \cdots \\ g(s) &= \frac{b_1}{1^s} + \frac{b_2}{2^s} + \frac{b_3}{3^s} + \frac{b_4}{4^s} + \frac{b_5}{5^s} + \frac{b_6}{6^s} + \cdots \end{aligned}$$

then

$$f(s)g(s) = \frac{c_1}{1^s} + \frac{c_2}{2^s} + \frac{c_3}{3^s} + \frac{c_4}{4^s} + \frac{c_5}{5^s} + \frac{c_6}{6^s} + \cdots \tag{36}$$

where

$$c_n = \sum_{ij=n} a_i b_j = \sum_{d|n} a_d b_{n/d}. \tag{37}$$

If we use a, b, and c as function names, this translates to $c = a * b$. It happens because, when we multiply the series term-by-term, we find a product term containing $1/n^s$ whenever we combine terms $1/i^s$ and $1/j^s$ with $ij = n$. (Did Dirichlet invent the Dirichlet product because he saw this phenomenon in Dirichlet series? Or did he go looking for series that he could multiply using the Dirichlet product?)

4 Notation for the Gaussian Integers

Write:

$$\begin{aligned}
\mathbb{Z}^+ &= \{1, 2, 3, 4, \ldots\} \\
P &= \text{set of rational primes} = \{2, 3, 5, 7, \ldots\} \\
\mathbb{G} &= \text{set of Gaussian integers} = \{a + bi | a, b \in \mathbb{Z}\} \\
\mathbb{G}^* &= \text{set of nonzero Gaussian integers} = \{a + bi | a, b \in \mathbb{Z}, \text{ not both zero}\} \\
\mathbb{G}P &= \text{a particular set of Gaussian primes, as follows.}
\end{aligned}$$

We want $\mathbb{G}P$ to contain "all" the Gaussian primes up to associates — that is, $\mathbb{G}P$ contains one Gaussian prime from each set of four associates. We'll let $\mathbb{G}P$ contain 7, but not -7, $7i$, or $-7i$. We can be very explicit: $\mathbb{G}P$ contains

- $1 + i$ (which has norm 2)
- p (which has norm p^2) if p is a rational prime with $p \equiv 3 \pmod 4$
- $a + bi$ and $a - bi$ (both with norm p) if $a^2 + b^2 = p$, p a rational prime with $p \equiv 1 \pmod 4$, *and* $a > b > 0$.

For example, in the case of $p = 5$, we let in $2 + i$ and $2 - i$, but not $i + 2$ (which is an associate of $2 - i$). We'll use "q" for a typical Gaussian prime to minimize the confusion with rational primes.

Let's practice with these notations, while laying some groundwork for the next section. As usual, let

$$\begin{aligned}
r_2(n) &= \text{number of ways to represent } n \text{ as a sum of two squares} \\
&= \#\{(a, b) | a^2 + b^2 = n\}.
\end{aligned} \tag{38}$$

We count all the ordered pairs, despite the obvious symmetries: for example, $(2, 1)$, $(1, 2)$, $(-2, 1)$, $(1, -2)$, $(2, -1)$, $(-1, 2)$, $(-2, -1)$, $(-1, -2)$ are all distinct ordered pairs, so $r_2(5) = 8$.

The Dirichlet series associated with r_2 is this:

$$\sum_{n\geq 1} \frac{r_2(n)}{n^s} = \frac{4}{1^s} + \frac{4}{2^s} + \frac{0}{3^s} + \frac{4}{4^s} + \frac{8}{5^s} + \frac{0}{6^s} + \frac{0}{7^s} + \frac{4}{6^s} + \frac{4}{9^s} + \cdots. \tag{39}$$

(The $n = 0$ term is missing here. For the obvious reason, it is never welcome in a Dirichlet series.)

Whenever we find an ordered pair (a, b) with $a^2 + b^2 = n$, we find a Gaussian integer $a + bi$ with $N(a + bi) = n$. So

$$\sum_{n\geq 1} \frac{r_2(n)}{n^s} = \sum_{n\geq 1} \frac{\#\{a + bi \in \mathbb{G}^* | N(a + bi) = n\}}{n^s} \tag{40}$$

so

$$\sum_{n\geq 1} \frac{r_2(n)}{n^s} = \sum_{x\in\mathbb{G}^*} \frac{1}{N(x)^s}. \tag{41}$$

That last step may require some thought. On the right side, each nonzero Gaussian integer is counted once, and contributes one term with a numerator of 1. On the left side, the Gaussian integers with the same norm ($N(x) = n$) are grouped together, and since there are $r_2(n)$ of them, they form a term with numerator $r_2(n)$. But we're counting the same things on both sides, so the two sums are equal. (This is a common trick; it's the reason Dirichlet series are often useful for counting things.)

In the next section, we'll work with the sum on the right, in order to understand the sum on the left.

5 In how many ways can n be expressed as a sum of two squares?

If Dirichlet series are fun in the world of integers, they should be even more fun in the world of Gaussian integers.

We have unique factorization in the Gaussian integers, so the reasoning that led to Euler products in integers works just as well for Gaussian integers. The version for Gaussian integers is this: Suppose that $g(x)$ is defined for all $x \in \mathbb{G}^*$ and is completely multiplicative; that is, $g(x)g(y) = g(xy)$ always. Then

$$\sum_{x\in\mathbb{G}^*} g(x) = 4 \prod_{q\in\mathbb{G}P} \frac{1}{1 - g(p)} \tag{42}$$

provided the sum on the left converges absolutely.

Two comments. First, the sum on the right isn't quite like the infinite sums we saw in Math 6; the terms don't have a definite ordering to them, so it is hard to say what we mean by partial sums. To sum the series, you have to put the terms in an arbitrary

order of your own. If the series converges absolutely, you have no problem, but you need to give up any notion of conditional convergence.

Second, what is that factor of 4 doing on the right side of (42)? It is there because, for every unique factorization in the Gaussian integers, there are four Gaussian integers with that factorization — up to units. For example, all four of the Gaussian integers 21, -21, $21i$, $-21i$ have the factorization

$$x = \text{unit} \times 7 \times 3$$

with $7, 3 \in \mathbb{G}P$. When we multiply out the terms on the right, we get one term for each unique factorization, but then we have to multiply by 4 to get one term for each nonzero Gaussian integer. (The same issue would have arisen in $\mathbb{Z}$, but we arbitrarily defined Dirichlet series to have terms only for positive n. If we had included all nonzero n on the left of (21) we would have needed a factor of 2 on the right side.)

We now apply (42) when $g(x) = \frac{1}{N(x)^s}$. That is a completely multiplicative function, whatever s is. We get:

$$\sum_{x \in \mathbb{G}^*} \frac{1}{N(x)^s} = 4 \prod_{q \in \mathbb{G}P} \left(\frac{1}{1 - \frac{1}{N(q)^s}} \right). \tag{43}$$

We know what the Gaussian primes are, so we can break out the factors by type:

$$\sum_{x \in \mathbb{G}^*} \frac{1}{N(x)^s} = 4 \begin{pmatrix} \text{term for } 1+i\text{:} \\ \text{(norm 2)} \end{pmatrix} \prod \begin{pmatrix} \text{terms for } p \equiv 3\text{:} \\ \text{one each, norm } p^2 \end{pmatrix} \prod \begin{pmatrix} \text{terms for } p \equiv 1\text{:} \\ \text{two each, norm } p \end{pmatrix} \tag{44}$$

$$= 4 \left(\frac{1}{1 - \frac{1}{2^s}} \right) \prod_{\substack{p \text{ prime} \\ p \equiv 3 \pmod 4}} \left(\frac{1}{1 - \frac{1}{(p^2)^s}} \right) \prod_{\substack{p \text{ prime} \\ p \equiv 1 \pmod 4}} \left(\frac{1}{1 - \frac{1}{p^s}} \right)^2. \tag{45}$$

Combining our results we have

$$\sum_{n \geq 1} \frac{r_2(n)}{n^s} = 4 \left(\frac{1}{1 - \frac{1}{2^s}} \right) \prod_{\substack{p \text{ prime} \\ p \equiv 3 \pmod 4}} \left(\frac{1}{1 - \frac{1}{(p^2)^s}} \right) \prod_{\substack{p \text{ prime} \\ p \equiv 1 \pmod 4}} \left(\frac{1}{1 - \frac{1}{p^s}} \right)^2. \tag{46}$$

THIS IS A STATEMENT ABOUT ORDINARY INTEGERS, and it is true whenever the left side converges absolutely. We're done with the Gaussian integers, for now.

Continuing: The denominator in the middle product in (46) is a difference of squares, so it factors: $1 - \frac{1}{(p^2)^s} = (1 - \frac{1}{p^s})(1 + \frac{1}{p^s})$. Write the last factor with two minus signs: $1 - \frac{1}{(p^2)^s} = (1 - \frac{1}{p^s})(1 - \frac{-1}{p^s})$. If we split up the middle product based on that factorization,

and also split up the last product, we get

$$\sum_{n\geq 1}\frac{r_2(n)}{n^s} = 4\left(\frac{1}{1-\frac{1}{2^s}}\right)\prod_{\substack{p \text{ prime}\\ p\equiv 3 \pmod 4}}\left(\frac{1}{1-\frac{+1}{(p^2)^s}}\right)\prod_{\substack{p \text{ prime}\\ p\equiv 3 \pmod 4}}\left(\frac{1}{1-\frac{-1}{(p^2)^s}}\right)$$
$$\prod_{\substack{p \text{ prime}\\ p\equiv 1 \pmod 4}}\left(\frac{1}{1-\frac{+1}{p^s}}\right)^2\prod_{\substack{p \text{ prime}\\ p\equiv 1 \pmod 4}}\left(\frac{1}{1-\frac{+1}{p^s}}\right)^2. \tag{47}$$

Now recombine these products in a different way:

$$\sum_{n\geq 1}\frac{r_2(n)}{n^s} = 4\prod_{p \text{ prime}}\left(\frac{1}{1-\frac{+1}{(p^2)^s}}\right)\prod_{p \text{ prime}}\left(\frac{1}{1-\frac{\chi(p)}{p^s}}\right)^2. \tag{48}$$

The first, second, and fourth products in (47) have combined to form the first product in (48). The third and fifth products in (47) have formed the second product on in (48). We have made use of the familiar function $\chi(p)$, which is convenient because it is -1 for the $\equiv 3$ primes, and $+1$ for the $\equiv 1$ primes. The last product has conjured up a factor for $p = 2$ out of thin air, but that's OK because $\chi(2) = 0$ which makes the conjured-up factor equal to 1.

Now, look at those two products in (48). They're both Euler products! In fact, they're the same Euler products we used in Section 2. Replacing them with the corresponding Dirichlet series gives

$$\sum_{n\geq 1}\frac{r_2(n)}{n^s} = 4\left(\sum_{n\geq 1}\frac{1}{n^s}\right)\left(\sum_{n\geq 1}\frac{\chi(n)}{n^s}\right) \tag{49}$$

We know what to do with the product of two Dirichlet series.

$$\begin{aligned}\sum_{n\geq 1}\frac{r_2(n)}{n^s} &= 4\sum_{n\geq 1}\frac{(\chi * 1)(n)}{n^s}\\ &= \sum_{n\geq 1}\frac{4\sum_{d|n}\chi(d)}{n^s}.\end{aligned} \tag{50}$$

Here we have found two Dirichlet series which are equal as functions for a range of values of s. (We need to check that the series really do converge for a range of values of s, but that's easy.) That's enough to conclude that the coefficients are equal:

$$r_2(n) = 4\sum_{d|n}\chi(d), \tag{51}$$

or equivalently,

$$r_2(n) = 4\left[\begin{pmatrix}\text{number of factors of n}\\ \text{that are} \equiv 1 \pmod 4\end{pmatrix} - \begin{pmatrix}\text{number of factors of n}\\ \text{that are} \equiv 3 \pmod 4\end{pmatrix}\right] \tag{52}$$

for every $n \geq 1$.

We proclaimed this formula a month ago in class. Now we have a proof.

6 In how many ways can n be expressed as $a^2 + 2b^2$?

Was that fun? Let's do it again. All of it, from the beginning. We'll try to evaluate

$$\tilde{r}_2(n) = \text{number of ways to represent } n \text{ as a } a^2 + 2b^2,\ a, b \in \mathbb{Z}.$$

Consider the number system

$$\mathbb{H} = \left\{a + b\sqrt{-2} \quad | \quad a, b \in \mathbb{Z}\right\}.$$

We have put $\sqrt{-2}$ in place of $i = \sqrt{-1}$ in the definition of the Gaussian integers.

This system satisfies all of the usual addition and multiplication axioms (not the ordering axioms) and we can prove that it has unique factorization in exactly the same way as we did for the Gaussian integers. There are some differences. There are only two units in $\mathbb{H}$, 1 and -1. ($\mathbb{H}$ doesn't contain i, and $\sqrt{-2}$ isn't a unit.) That means that primes in $\mathbb{H}$ come in pairs, not fours. The number $2 \in \mathbb{H}$ isn't prime, but it factors in a different way: $2 = (\sqrt{-2})(-\sqrt{-2})$. Those factors are both prime; and in fact, they are associates of each other.

The norm in $\mathbb{H}$ is $N(a + b\sqrt{-2}) = a^2 + 2b^2$. It is completely multiplicative.

Some rational primes remain primes in $\mathbb{H}$. If p cannot be written as $p = a^2 + 2b^2$, then p remains prime in $\mathbb{H}$; if p can be written in that way, then p factors as $p = (a + b\sqrt{-2})(a - b\sqrt{-2})$, and those factors are both prime. But which primes can be factored in this way? We can find that out in the same way we worked the $x^2 + y^2$ problem and the answer turns out to be this:

> $p \in P$ can be expressed as a^2+2b^2 for some $a, b \in \mathbb{Z}$ if and only if p is congruent to 1 or 3 $\pmod 8$.

Now repeat all of the steps in the last section, for $\mathbb{H}$ in place of $\mathbb{G}$. What changes? The giant "4" becomes a giant "2", because there are only two units. The definition of χ has to change: it is $\chi(n) = 0$ when n is even, $\chi(n) = +1$ when $n \equiv 1$ or 3 $\pmod 8$, and $\chi(n) = -1$ otherwise. It is still completely multiplicative. All of the sums that covered primes $\equiv 3 \pmod 4$ now cover primes $\equiv 5$ or 7 $\pmod 8$. Nothing else changes, and we finish with

$$\tilde{r}_2(n) = 2\left[\begin{pmatrix}\text{number of factors of n}\\ \text{that are} \equiv 1 \text{ or } 3 \pmod 8\end{pmatrix} - \begin{pmatrix}\text{number of factors of n}\\ \text{that are} \equiv 5 \text{ or } 7 \pmod 8\end{pmatrix}\right] \tag{53}$$

For example, $n = 36$ has three odd factors, 1, 3, and 9. They are all congruent to 1 or 3 (mod 8), so the formula gives

$$\tilde{r}_2(36) = 2 \times 3 = 6.$$

Indeed,

$$\begin{aligned} 36 &= (6)^2 + 2(0)^2 = (-6)^2 + 2(0)^2 \\ &= (2)^2 + 2(4)^2 = (2)^2 + 2(-4)^2 = (-2)^2 + 2(4)^2 = (-2)^2 + 2(-4)^2. \end{aligned}$$

Acknowledgement

Thanks to Jonah Sinick for suggesting most of the above; in particular, Section 2 follows his talk at DMC (Bryn Mawr). Richard Lu suggested Jameson's book, below; his poster on the Prime Number Theorem is now in room 145 and on the web (Math/Stat Dept — people — Stromquist — Math 97 page — posters).

References

For further reading try these:

- Jameson, *The Prime Number Theorem,* Cambridge University Press ca. 2002.
- Apostol, *An Introduction to Analytic Number Theory,* Springer (?).
- Edwards, *The Riemann Zeta Function.*