Unique Factorization, Non-unique factorization, Introduction to Prime distributions, Dirichlet series and the Zeta-function

September 6, 2012

Recall from last time:

1 A fundamental divisibility lemma

Lemma 1 (The fundamental divisibility lemma) *If a prime p divides a product of two integers $a \cdot b$ then it either divides a or b (or both).*

Proof. If p divides a we're done, so assume that p is relatively prime to a, and therefore there are integers r, s such that

$$(*) \quad 1 = rp + sa.$$

Multiply **(*)** by b, to get

$$(*) \quad b = rpb + sab.$$

and since p divides both terms on the RHS it divides b. QED

There's a subtle afterthought that one can (and perhaps should) have about this lemma. Namely, that this property of a number *dividing a product of two integers if and only if it divides one of them* is satisfied *only* by prime numbers. So, one might take that property as the defining property. We'll discuss this a bit.

Also a bit of "proof-analysis" of the above proof gives us the following adjunction to the fundamental divisibility lemma:

Corollary 1 *Let n be any number relatively prime to a and dividing ab. Then n divides b.*

2 Back to "ord_p"

Recall that for $N \geq 1$ by $ord_p(N)$ we mean the largest exponent e such that p^e divides N, that is, such that

$$N = p^e \cdot N_o$$

for $N_o \in \mathbf{Z}$. It follows that $ord_p(N)$ to is the unique integer e such that

$$N = p^e \cdot N_o$$

for $N_o \in \mathbf{Z}$ with $ord_p(N_o) = 0$. Another was of saying Lemma 1 is:

Lemma 2 *Let a, b be numbers such that $ord_p(a) = ord_p(b) = 0$. Then*

$$ord_p(ab) = 0.$$

We can parlay this into:

Proposition 1 *Let p be a prime and a, b integers. Then:*

$$ord_p(ab) = ord_p(a) + ord_p(b).$$

(I.e., ord_p has a kind of logarithmic property: converting products to sums.)

Proof: Write $a = p^{ord_p(a)}a_o$ and $b = p^{ord_p(b)}b_o$ with $ord_p(a_o) = ord_p(b_o) = 0$. Now,

$$ab = p^{ord_p(a)}p^{ord_p(b)}a_o b_o = p^{ord_p(a)+ord_p(b)}a_o b_o.$$

By Lemma 2, $ord_p(a_o b_o) = 0$ which proves the proposition.

For the next corollary, let's note that the terminology

$$\prod_{p \text{ prime}} p^{a(p)}$$

makes sense if the function

$$p \mapsto a(p) \in \mathbf{Z}$$

is zero for all but finitely many prime numbers p; you get an infinite product of "1"s times a finite product of *actual* powers of prime numbers. We proved, in teh first lecture, that any $N > 1$ is expressible as a finite product of powers of prime numbers, i.e., that any such N can be written as $N = \prod_p p^{a(p)}$ for some function

$$p \mapsto a(p) \in \mathbf{Z}$$

that is zero for all but finitely many prime numbers p. (The proof was by induction using successive factorizations.) We now can show that this expression is unique.

Corollary 2 *Let $N \geq 1$. Then*

$$N = \prod_p p^{ord_p(N)}.$$

Proof: Write $N = \prod_p p^{a(p)}$ and consider any prime number q. Now let's use Proposition 1. Since $ord_q(p) = 1$ or 0 depending on whether p is q or not, we get—by the "logarithmic property "of ord_q—we get that

$$ord_q(N) \;=\; ord_q(\prod_p p^{a(p)}) \;=\; \sum_p ord_q(p^{a(p)}) = a(q).$$

That is, $a(q) = ord_q(N)$. Since this is true for all primes q, the corollary is proved. Another way of expressing the effect of this corollary is to give it as the more traditional:

Theorem 3 *(***Fundamental Theorem of Arithmetic***) Any positive number is expressible in a unique way, except for order of factors, as a product of prime numbers.*

3 First comments on the distribution of primes, Dirichlet Series, and the zeta function

3.1 The 'number' of primes

Define

$$\pi(X) = |\{p \leq X \mid p \text{ prime}\}|,$$

and discuss a bit.

3.2 Formal Dirichlet Series

A "formal Dirichlet Series" (for us) will be an infinite series in the variable s of the form:

$$D(s) \quad = \quad a_1 + \frac{a_2}{2^s} + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \ldots + \frac{a_n}{n^s} + \ldots \quad = \quad \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where the coefficients a_n are complex numbers.

For a while we can think of these things as merely formal where it is clear how to add and multiply two such. E.g.,

$$\{\sum_{n=1}^{\infty}\frac{a_n}{n^s}\}\cdot\{\sum_{n=1}^{\infty}\frac{b_n}{n^s}\}=\{\sum_{n=1}^{\infty}\frac{c_n}{n^s}\},$$

where

$$c_n=\sum_{1\le d\mid n}a_d\cdot b_{n/d}.$$

But, in fact, most of the ones that are of interest to us will have the property that their coefficients a_n grow no faster than *polynomial in* n, which means that they converge absolutely for s large enough. This is also true if you let s range through complex numbers whose real parts are large enough. Although many deep results in number theory are consequences of the behavior of these Dirichlet series as functions of the complex plane (or parts of the complex plane) for some of what we'll say today the convergence isn't even necessary.

3.3 Example: the zeta-function

If the coefficients a_n are all equal to 1, our Dirichlet series is denoted:

$$\zeta(s) \quad = \quad 1+\frac{1}{2^s}+\frac{1}{2^s}+\frac{1}{3^s}+\ldots+\frac{1}{n^s}+\ldots \quad = \quad \sum_{n=1}^{\infty}\frac{1}{n^s}.$$

So:

$$\zeta(1)= \quad = \quad \sum_{n=1}^{\infty}\frac{1}{n}.$$

$$\zeta(2)= \quad = \quad \sum_{n=1}^{\infty}\frac{1}{n^2}.$$

Relate these to $\int_0^{\infty}\frac{dx}{x}$ and $\int_0^{\infty}\frac{dx}{x^2}$ to get

Theorem 4 *The sum of the reciprocals of prime numbers,*

$$\sum_{p\text{ prime}}1/p,$$

diverges.

Proof on page 21 section 3 of Chapter 2 of **[I-R]**. The idea is to form the finite product

$$\lambda(N) := \prod_{p \text{ prime } \leq N} \frac{1}{1-\frac{1}{p}}.$$

That is,

Lemma 3 *Letting $p_1, p_2, \ldots p_{\pi(N)}$ be the set of primes $\leq N$ we have:*

$$\lambda(N) = \sum (p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots p_{\pi(N)}^{a_{\pi(N)}})^{-1}$$

where the sum is over all tuples of non-negative integers $(a_1, a_2, \ldots, a_{\pi(N))})$.

Since any number $n \leq N$ is expressible as such a $p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots p_{\pi(N)}^{a_{\pi(N)}}$ we have that

$$\sum_{n \leq N} 1/n \leq \lambda(N)$$

which gives, for example, that

$$\lambda(N) \to \infty$$

(and therefore we already have as consequence that there are infinitely many primes).

Now form

$$\log(\lambda(N)) = - \sum_{p \text{ prime } \leq N} \log(1 - \frac{1}{p})$$

and break up each summand above as:

$$-\log(1-\frac{1}{p}) \ = \frac{1}{p} + \epsilon_p,$$

where

$$\epsilon_p := \{\frac{1}{2p^2} + \frac{1}{3p^3} + \frac{1}{4p^4} + \ldots\} \quad \leq \quad \{\frac{1}{p^2} + \frac{1}{p^3} + \frac{1}{p^4} + \ldots\} = p^{-2}/(1-p^{-1}) \ \leq 2/p^2.$$

So,

$$\log(\lambda(N)) = \sum_{p \text{ prime } \leq N} \frac{1}{p} + \sum_{p \text{ prime } \leq N} \epsilon_p.$$

Now, $\sum_{p \text{ prime}} \epsilon_p$ converges, say, to $\epsilon < \infty$ and we have

$$\sum_{p \text{ prime}} 1/p \ \geq \log(\lambda(N)) - \epsilon.$$

3.4 Infinite Product Expansion of $\zeta(s)$

One way of expressing the **Unique Factorization Theorem** for **Z** is that we have the following equality between the formal sum on the RHS and the formal product on the LHS:

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{p^s}}.$$

Discuss.

3.5 Arithmetic Functions related to $\zeta(s)$

1. The divisor function:

$$\nu(n) := \text{the number of positive divisors of } n \quad = \sum_{1 \leq d \mid n} 1.$$

$$\zeta(s)^2 = \sum_{n=1}^{\infty} \frac{\nu(n)}{n^s}.$$

2. The sum-of-divisors function:

$$\sigma(n) := \text{the sum of positive divisors of } n \quad = \sum_{1 \leq d \mid n} d.$$

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

3. The sum-of-k-th powers-of-divisors function:

$$\sigma_k(n) :== \sum_{1 \leq d \mid n} d^k.$$

$$\zeta(s)\zeta(s-k) = \sum_{n=1}^{\infty} \frac{\sigma_k(n)}{n^s}.$$

   So: $\nu(n) = \sigma_0(n)$ and $\sigma(n) = \sigma_1(n)$.

4. The Moebius function $\mu(n)$ which is defined to be 0 if n is not square-free, and $+1$ if n is is a product of an even number of distinct primes[1], and is -1 if n is a product of an odd number of distinct primes.

   The Moebius function defines an operator on functions of positive numbers, as follows: if $f(n)$ is such a function, define:

$$(Mf)(n) := \sum_{1 \leq d \mid n} \mu(d) f(n/d).$$

   To think efficiently about this, we will introduce a certain kind of "multiplication of functions" that we've already encountered in the discussion above about Dirichlet series.

[1] Note that zero is an *even* number.

3.6 Dirichlet Product

Given functions $A : n \mapsto A(n)$ and $B : n \mapsto B(n)$, the formula

$$C(n) = \sum_{1 \leq d \mid n} A(d) \cdot B(n/d)$$

that we have encountered as giving the coefficients of the product of two Dirichlet Series defines a function $C(n)$ that can be thought of as a kind of product of A and B ("$\star$-multiplication"). Not quite following our text's notation, denote it:

$$C := A \star B.$$

This operation is commutative and associative, and there is even a two-sided identity $\mathbf{I}$.

$$(\mathbf{I} : n \mapsto 1 \text{ if } n = 1, \text{ and } 0 \text{ if } n > 1.)$$

In this new notation the ordinary product of two Dirichlet series $\sum_n A(n)/n^s$ and $\sum_n B(n)/n^s$ is

$$\sum_n A \star B(n)/n^s.$$

Also, note that our operation

$$f \mapsto Mf$$

is just $\star$-multiplying f by the Moebius function μ.

Proposition 2 *$\sum_{1 \leq d \mid n} \mu(d) = 0$ if $n > 1$ and is equal to 1 when $n = 1$. In our $\star$-notation, this boils down to saying that if ι is the constant function with value 1 (i.e., $\iota(n) = 1$ for all n) then*

$$M\iota = \mu \star \iota = \mathbf{I}.$$

That is, in terms of $\star$-product, the Moebius function μ is the $\star$-inverse of the constant function ι.

Corollary 5

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

Moebius inversion:

Corollary 6 *For $n \mapsto F(n)$ an arbitrary function and form $f(n) := \sum_{1 \leq d \mid n} f(n/d)$. We can retrieve the original function F from f by*

$$F = Mf.$$

That is,

$$F(n) = \sum_{1 \leq d \mid n} \mu(d) f(n/d).$$

The proof consists in staring at the formula:

$$\iota \star \mu \star f = f.$$