

Introduction to Analytic Number Theory
Math 531 Lecture Notes, Fall 2005

A.J. Hildebrand
Department of Mathematics
University of Illinois

<http://www.math.uiuc.edu/~hildebr/ant>

Version 2006.09.01

Chapter 0

Primes and the Fundamental Theorem of Arithmetic

Primes constitute the holy grail of analytic number theory, and many of the famous theorems and problems in number theory are statements about primes. Analytic number theory provides some powerful tools to study prime numbers, and most of our current (still rather limited) knowledge of primes has been obtained using these tools.

In this chapter, we give a precise definition of the concept of a prime, and we state the Fundamental Theorem of Arithmetic, which says that every integer greater than 1 has a unique (up to order) representation as a product of primes. We conclude the chapter by proving the infinitude of primes.

The material presented in this chapter belongs to elementary (rather than analytic) number theory, but we include it here in order to make the course as self-contained as possible.

0.1 Divisibility and primes

In order to define the concept of a prime, we first need to define the notion of divisibility.

Given two integers $d \neq 0$ and n , we say that d **divides** n or n **is divisible by** d , if there exists an integer m such that $n = dm$. We write $d|n$ if d divides n , and $d \nmid n$ if d does not divide n .

Note that divisibility by 0 is not defined, but the integer n in the above definition may be 0 (in which case n is divisible by any non-zero integer d) or negative (in which case $d|n$ is equivalent to $d|(-n)$).

While the above definition allows for the number d in the relation “ $d|n$ ”

to be negative, it is clear that $d|n$ if and only if $(-d)|n$, so there is a one-to-one correspondence between the positive and negative divisors of an integer n . In particular, no information is lost by focusing on the *positive* divisors of a given integer, and it will be convenient to restrict the notion of a divisor to that of a positive divisor. We therefore make the following convention: *Unless otherwise specified, by a divisor of an integer we mean a positive divisor, and in a notation like $d|n$ the variable d represents a positive divisor of n .* This convention allows us, for example, to write the sum-of-divisors function $\sigma(n)$ (defined as the sum of all *positive* divisors of n) simply as $\sigma(n) = \sum_{d|n} d$, without having to add the extra condition $d > 0$ under the summation symbol.

The **greatest common divisor (gcd)** of two integers a and b that are not both zero is the unique integer $d > 0$ satisfying (i) $d|a$ and $d|b$, and (ii) if $c|a$ and $c|b$, then $c|d$. The gcd of a and b is denoted by (a, b) . If $(a, b) = 1$, then a and b are said to be **relatively prime** or **coprime**.

The **least common multiple (lcm)** of two non-zero integers a and b is the unique integer $m > 0$ satisfying (i) $a|m$ and $b|m$, and (ii) if $a|n$ and $b|n$, then $m|n$. The lcm of a and b is denoted by $[a, b]$.

The gcd and the lcm of more than two integers are defined in an analogous manner.

An integer $n > 1$ is called **prime** (or a **prime number**) if its only positive divisors are the trivial ones, namely 1 and n .

The sequence of primes, according to this (commonly accepted) definition is thus 2, 3, 5, 7, 11, \dots . Note, in particular, that 1 is not a prime, nor is 0 or any negative integer.

Primes in other algebraic structures. The notion of a “prime” can be defined in quite general algebraic structures. All that is needed for such a definition to make sense is an analog of the multiplication operation (so that divisibility can be defined), and the notion of “units” (which serve as “trivial” divisors, analogous to the numbers ± 1 among the integers). One can then define a prime as any element in the given structure that can only be factored in a trivial way, in the sense that one of the factors is a unit. The best-known examples of such structures are algebraic integers, which behave in many respects like the ordinary integers, and which form the subject of a separate branch of number theory, **algebraic number theory**.

Another example is given by the ring of polynomials with integer coefficients, with multiplication of ordinary polynomials as ring operation and the constant polynomials ± 1 as “units”. The “primes” in such a polynomial

ring turn out to be the irreducible (over \mathbb{Z}) polynomials.

0.2 The Fundamental Theorem of Arithmetic

As the name suggests, this result, which we now state, is of fundamental importance in number theory, and many of the results in later chapters depend in a crucial way on this theorem and would fail if the theorem were false.

Theorem 0.1 (Fundamental Theorem of Arithmetic). *Every integer $n > 1$ can be written as a product of primes, and the representation is unique up to the order of the factors.*

The proof of this result, while elementary, is somewhat involved, and we will not give it here. (It can be found in any text on elementary number theory.) We only note here that the crux of the proof lies in showing the *uniqueness* of a prime factorization; the proof of the *existence* of such a factorization is an easy exercise in induction.

Notation. There are several common ways to denote the prime factorization guaranteed by the Fundamental Theorem of Arithmetic. First, we can write the prime factorization of an integer $n \geq 2$ as

$$n = p_1 \dots p_r,$$

where the p_i 's are primes, but *not necessarily distinct*.

In most situations it is more useful to combine identical factors in the above representation and write

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r},$$

where, this time, the p_i 's are *distinct* primes, and the exponents α_i positive integers.

Using the notation $p^m || n$ if p^m is the exact power of p that divides n (i.e., $p^m | n$, but $p^{m+1} \nmid n$), we can write the above representation as

$$n = \prod_{p^m || n} p^m.$$

Yet another useful representation of the prime factorization of n is

$$n = \prod_p p^{\alpha(p)},$$

where the product is extended over *all* prime numbers and the exponents $\alpha(p)$ are nonnegative integers with $\alpha(p) \neq 0$ for at most finitely many p .

The last notation is particularly convenient when working with the greatest common divisor or the least common multiple, since these concepts have a simple description in terms of this notation: Indeed, if n and m are positive integers with prime factorization $n = \prod_p p^{\alpha(p)}$ and $m = \prod_p p^{\beta(p)}$, then the gcd and lcm of n and m are given by

$$(n, m) = \prod_p p^{\min(\alpha(p), \beta(p))}, \quad [n, m] = \prod_p p^{\max(\alpha(p), \beta(p))},$$

respectively. Similarly, divisibility is easily characterized in terms of the exponents arising in the representation: Given $n = \prod_p p^{\alpha(p)}$ and $m = \prod_p p^{\beta(p)}$, we have $m|n$ if and only if $\beta(p) \leq \alpha(p)$ for all p .

With the convention that an empty product is to be interpreted as 1, all of the above formulas remain valid when $n = 1$.

Unique factorization in more general algebraic structures. As mentioned above, the concept of a prime can be defined in very general algebraic structures. One can then ask if an analog of the Fundamental Theorem of Arithmetic also holds in these structures. It turns out that the existence part of this result, i.e., the assertion that every (non-unit) element in the given structure has a representation as a product of “prime” elements, remains valid under very general conditions. By contrast, the uniqueness of such a representation (up to the order of the factors or multiplication by units) is no longer guaranteed and can fail, even in some simple examples. For instance, in the ring of algebraic integers $\{n + m\sqrt{6}i : m, n \in \mathbb{Z}\}$, the number 10 can be factored as $10 = 2 \cdot 5$ and $10 = (2 + i\sqrt{6})(2 - i\sqrt{6})$, and one can show that each of the four factors $2, 5, 2 \pm i\sqrt{6}$ arising here are “primes” in the appropriate sense.

Beurling generalized primes. By the Fundamental Theorem of Arithmetic the positive integers are exactly the products of the form $(*) \prod_{i \in I} p_i^{\alpha_i}$, where $p_1 < p_2 < \dots$ is the sequence of primes, I a finite (possibly empty) subset of the positive integers, and the exponents α_i are positive integers. This characterization of the positive integers suggests the following generalization of the concepts of a “prime” and a (positive) “integer”, which was first proposed some 50 years ago by Arne Beurling. Instead of starting with an appropriate analog of the integers and then trying to define a notion of a

prime, the idea of Beurling was to start with an appropriate generalization of the primes and then define generalized integers as above in terms of these generalized primes. Specifically, let $\mathcal{P} = \{p_1 < p_2 < \dots\}$ be an arbitrary sequence of positive numbers (which need not even be integers), and let $\mathbb{N}_{\mathcal{P}}$ be the set of all finite products of the form $(*)$ with the p_i 's taken from \mathcal{P} . Then \mathcal{P} is called a system of *Beurling generalized primes*, and $\mathbb{N}_{\mathcal{P}}$ the associated system of *Beurling generalized integers*. One can study such systems in great generality, and ask, for instance, how the “growth” of such a sequence of generalized primes is related with that of the associated sequence of generalized integers.

0.3 The infinitude of primes

We conclude this chapter with a proof of the infinitude of primes, a result first proved some two thousand years ago by Euclid.

Theorem 0.2. *There are infinitely many primes.*

Proof. We give here a somewhat nonstandard proof, which, while not as short as some other proofs, has a distinctly analytic flavor. It is based on the following lemma, which is of interest in its own right.

Lemma 0.3. *Let $\mathcal{P} = \{p_1, \dots, p_k\}$ be a finite set of primes, let*

$$\mathbb{N}_{\mathcal{P}} = \{n \in \mathbb{N} : p|n \Rightarrow p \in \mathcal{P}\},$$

i.e., $\mathbb{N}_{\mathcal{P}}$ is the set of positive integers all of whose prime factors belong to the set \mathcal{P} (note that $1 \in \mathbb{N}_{\mathcal{P}}$), and let

$$N_{\mathcal{P}}(x) = \#\{n \in \mathbb{N}_{\mathcal{P}} : n \leq x\} \quad (x \geq 1).$$

Then there exist constants c and x_0 (depending on \mathcal{P}) such that $N_{\mathcal{P}}(x) \leq c(\log x)^k$ for $x \geq x_0$.

Proof. Note that

$$\mathbb{N}_{\mathcal{P}} = \{p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} : a_i \in \mathbb{N}_0\},$$

and that by the Fundamental Theorem of Arithmetic each element in $\mathbb{N}_{\mathcal{P}}$ corresponds to a *unique* k -tuple (a_1, \dots, a_k) of nonnegative integers. Thus,

$$\begin{aligned} N_{\mathcal{P}}(x) &= \#\{(a_1, \dots, a_k) : a_i \in \mathbb{N}_0, p_1^{a_1} \dots p_k^{a_k} \leq x\} \\ &= \#\{(a_1, \dots, a_k) : a_i \in \mathbb{N}_0, a_1 \log p_1 + \dots + a_k \log p_k \leq \log x\}. \end{aligned}$$

Now note that the inequality $a_1 \log p_1 + \cdots + a_k \log p_k \leq \log x$ implies $a_i \leq \log x / \log p_i \leq \log x / \log 2$ for each i . Hence, for each a_i there are at most $\lceil \log x / \log 2 \rceil + 1$ choices, and the number of tuples (a_1, \dots, a_k) counted in $\mathbb{N}_{\mathcal{P}}(x)$ is therefore

$$\leq \left(\left\lceil \frac{\log x}{\log 2} \right\rceil + 1 \right)^k.$$

If we now restrict x by $x \geq 2$, then $\lceil \log x / \log 2 \rceil + 1 \leq 2 \log x / \log 2$, so the above becomes

$$\leq \left(2 \frac{\log x}{\log 2} \right)^k = (2/\log 2)^k (\log x)^k.$$

This gives the asserted bound for $\mathbb{N}_{\mathcal{P}}(x)$ with $c = (2/\log 2)^k$ and $x_0 = 2$. \square

With this lemma at hand, the infinitude of primes follows easily: If there were only finitely many primes, then we could apply the lemma with \mathcal{P} equal to the set of all primes and, consequently, $\mathbb{N}_{\mathcal{P}}$ the set of all positive integers, so that $\mathbb{N}_{\mathcal{P}}(x) = [x]$ for all $x \geq 1$. But the lemma would give the bound $\mathbb{N}_{\mathcal{P}}(x) \leq c(\log x)^k$ for all $x \geq 2$ with some constant c , and since $(\log x)^k/[x]$ tends to zero as $x \rightarrow \infty$, this is incompatible with the equality $\mathbb{N}_{\mathcal{P}}(x) = [x]$. \square

0.4 Exercises

- 0.1 Show that there exist arbitrarily large intervals that are free of primes, i.e., for every positive integer k there exist k consecutive positive integers none of which is a prime.
- 0.2 Let $p(x) = \sum_{i=0}^k a_i x^i$ be a polynomial with integer coefficients a_i and of degree $k \geq 1$. Show that $p(n)$ is composite for infinitely many integers n .
Remark: With “composite” replaced by “prime”, the question becomes a famous problem that is open (in general) for polynomials of degree at least 2. For example, it is not known whether there are infinitely many primes of the form $p(n) = n^2 + 1$.
- 0.3 Call a set of positive integers a *PC-set* if it has the property that any pair of distinct elements of the set is coprime. Given $x \geq 2$, let $N(x) = \max\{|A| : A \subset [2, x], A \text{ is a PC-set}\}$, i.e., $N(x)$ is the maximal number of integers with the PC property that one can fit into the interval $[2, x]$. Prove that $N(x)$ is equal to $\pi(x)$, the number of primes $\leq x$.
- 0.4 A positive integer n is called squarefull if it satisfies $(*) p|n \Rightarrow p^2|n$. (Note that $n = 1$ is squarefull according to this definition, since 1 has no prime divisors and the above implication is therefore trivially true.)
- (i) Show that n is squarefull if and only if n can be written in the form $n = a^2 b^3$ with $a, b \in \mathbb{N}$.
 - (ii) Find a similar characterization of “ k -full” integers, i.e., integers $n \in \mathbb{N}$ that satisfy $(*)$ with 2 replaced by k (where $k \geq 3$).
- 0.5 Let $\mathcal{P} = \{p_1, \dots, p_k\}$ be a finite set of primes, let

$$\mathbb{N}_{\mathcal{P}} = \{n \in \mathbb{N} : p|n \Rightarrow p \in \mathcal{P}\}$$

i.e., $\mathbb{N}_{\mathcal{P}}$ is the set of positive integers all of whose prime factors belong to the set \mathcal{P} (note that $1 \in \mathbb{N}_{\mathcal{P}}$), and let

$$N_{\mathcal{P}}(x) = \#\{n \in \mathbb{N}_{\mathcal{P}} : n \leq x\} \quad (x \geq 1).$$

In Lemma 0.3 we showed that $N_{\mathcal{P}}(x) \leq c_1(\log x)^k$ for a suitable constant c_1 (depending on the set \mathcal{P} , but not on x) and for all sufficiently large x , say $x \geq x_1$. Prove that a bound of the same type holds in the other direction, i.e., there exist constants $c_2 > 0$ and x_2 , depending on \mathcal{P} , such that $N_{\mathcal{P}}(x) \geq c_2(\log x)^k$ holds for all $x \geq x_2$.