Elementary Number Theory : §3

Henry Slayer | University of California, Santa Cruz

Primes and Prime Decomposition

Primes are often referred to as the atoms of the integers, and the analogy could be no less fitting. All integers and rational numbers can be decomposed into primes, and just as a molecule is defined by its distinct atomic signature, the prime decomposition belonging to each number is unique. Some of this may be familiar from previous courses, or even from high school. We develop existence and uniqueness of prime decomposition with the following collection of facts and observations.

Definition 1. *A prime number is a natural number p such that (i) p is not zero or 1, and (ii), the only divisors of p are 1 and itself.*

Proposition 1. *Every nonzero integer has finitely many divisors.*

Proof. For the proof, we consider divisors in terms of absolute value. Suppose that we have two numbers, a and b. If $a \,|\, b$, then $a \leq b$. As the greatest divisor of any number is itself, it follows that any and all other divisors must be smaller than the number itself. So, there must be finitely many such divisors. □

Proposition 2. *Every nonzero number that isn't 1 has a prime factorization.*

Proof. We can consider positive integers not equal to zero or 1, as we are considering divisibility primarily in terms of absolute value. Walking through the numbers, we can see that every number we encounter is either prime (2, 3, 5, . . .), or composite. When we arrive at a prime number, we know by the definition of a prime that it is its own decomposition. When we arrive at a composite number, we stop, and break that number down into composite factors, dividing and dividing and dividing our divisors and dividends until we have found the elements that can no longer be divided, which are primes. We know that we'll eventually bottom out, because each number has finitely many divisors, and we know that all of these numbers are prime, because we've divided as much as we possibly can. So, every integer is itself prime, or the product of primes. □

Proposition 3. *Let N be a natural number greater than 1. If N is composite, then N has a prime factor $p \leq \lfloor\sqrt{N}\rfloor$.*

Proof. Assume that N is composite. So, $N = ab$ for a pair of positive integers a and b, where both a and b are greater than 1. We claim that $a \leq \lfloor\sqrt{N}\rfloor$ or $b \leq \lfloor\sqrt{N}\rfloor$. Suppose, to the contrary, that this wasn't the case. Then, $a \geq b > \lfloor\sqrt{N}\rfloor$, which would imply that $ab > N$, which is impossible. Now, as $a > 1$, a must have some prime factor p, such that $p \leq a \leq \lfloor\sqrt{N}\rfloor$. As $p \,|\, a$, and $a \,|\, N$, it follows that $p \,|\, N$, and so N must have a prime factor $p \leq \lfloor\sqrt{N}\rfloor$. □

Now, try to convince yourself why any integer N not equal to zero or one cannot have a prime factor *larger* than $\lfloor\sqrt{|N|}\rfloor$, unless N itself is prime.
Having established that every number *has* a factorization in terms of primes, we now want to investigate whether or not this factorization is unique.

Lemma 1 (Euclid's Lemma)**.** *Suppose that a, b, c are integers, and $GCD\,(a, b) = 1$. Then, if $a \,|\, bc$, it follows that $a \,|\, c$.*

Proof. As the GCD of a and b is 1, we know from the previous section that $ax + by = 1$, for some choice of integers x and y. Scaling by c,

$$(ac)x + (bc)y = c$$

As $a \,|\, acx$ and $a \,|\, bcy$ (by assumption), we know that a must divide c, too. □

Lemma 2 (Euclid's Lemma, now for primes)**.** *Let p, c, b be integers, where p is a prime number. Then, if $p \,|\, bc$, $p \,|\, b$ or $p \,|\, c$ (or both.*

Proof. Suppose that $p \,|\, b$. Then we're done. If $p \not| \, b$, then p and b must be coprime, and so $p \,|\, c$ by Euclid's lemma. □

The lemmas above suggest an important observation. If a prime number divides any product of integers, say $p \,|\, a_1 a_2 a_3 \cdots a_n$, then $p \,|\, a_i$ for some $1 \leq i \leq n$. This makes sense. If this weren't the case, then somehow parts of p would need to be distributed across one or more integers. However, numbers can't share fractions of a prime between each other, because a prime can't be split into such factors.
Having gathered these observations, we are ready to prove the uniqueness of prime decomposition. From here forwards, we will typically denote the prime factorization of a number as $a = 2^{e_2} 3^{e_3} \cdots$, where each e_i is the exponent of a prime factor.

Theorem 3 (Uniqueness of Prime Decomposition)**.** *Each number has a unique factorization into primes. That is, if e_i and f_i are natural numbers, and*

$$N = 2^{e_2} 3^{e_3} 5^{e_5} \cdots p^{e_p} = 2^{f_2} 3^{f_3} 5^{f_5} \cdots p^{f_p}$$

Then $e_p = f_p$ for each prime factor p.

Proof. Suppose that N is some integer, with two prime decompositions.

$$N = 2^{e_2} 3^{e_3} 5^{e_5} \cdots p^{e_p} = 2^{f_2} 3^{f_3} 5^{f_5} \cdots p^{f_p}$$

We want to show that the exponents are equal, across both factorizations. For any given pair of exponents e_p, f_p, either $e_p \leq f_p$ or $f_p \leq e_p$. So, we'll assume without loss of generality that $e_p \leq f_p$, and we let d denote the difference, $d = f_p - e_p$. So, what happens if we divide N by p^{e_p}?

$$\frac{N}{p^{e_p}} = 2^{e_2}3^{e_3}5^{e_5}\cdots 1 = 2^{e_2}3^{e_3}5^{e_5}\cdots p^d$$

We claim that d must be zero. Why is this the case?
If it weren't the case that d was zero, then p would divide the product on the right hand side. If p divided the product on the right hand side, then it would also need to divide a product on the left. But, the left has no factors of p, because they've already been divided out. By Euclid's lemma, we know that $p \mid a_1 a_2 \cdots a_n$ if and only if $p \mid a_i$ for one of the factors a_i. All of the factors in the left-hand product are prime, so p divides none of them. Thus, d must be zero, which implies that $e_p = f_p$, as desired. □

Decomposition and Divisibility

The beauty of prime decomposition is that it enables us to view the integers in terms of a signature string of exponents, the trace of the prime decomposition. This allows us to re-discover the properties of divisibility in a new and powerful way, and recast the *LCM* and *GCD* in terms of minimum and maximum exponents.

If a divides b, then every prime power of a must divide every prime power of b in their respective decompositions. In other words, if $a = 2^{e_2}3^{e_3}\cdots$ and $b = 2^{f_2}3^{f_3}\cdots$, and $a \mid b$, then $e_p \leq f_p$ for every prime p.

Proposition 4. *Let a and b be positive integers with prime decompositions*

$$a = 2^{e_2}3^{e_3}\cdots \qquad b = 2^{f_2}3^{f_3}\cdots$$

Then, $a \mid b$ if and only if $e_p \leq f_p$ for each prime p.

Proof. Divisibility always implies a third party. Assume $a \mid b$. Then, $b = ac$ for some other integer c. c, in turn, possesses its own unique prime decomposition, say $c = 2^{g_2}3^{g_3}\cdots$.
If $b = ac$, then it follows that

$$ac = 2^{e_2+g_2}3^{e_3+g_3}\cdots = 2^{f_2}3^{f_3}\cdots = b$$

By what we know of prime factorization, this implies that $e_p + g_p = f_p$, which is only possible if $e_p \leq f_p$. Conversely, suppose that $e_p \leq f_p$ for each prime p. Denoting the difference by $d_p = f_p - e_p$, it follows that we can construct a factor $c = 2^{d_2}3^{d_3}\cdots$ such that $ac = b$, which implies that $a \mid b$. □

Prime decomposition enables us to consider divisibility in terms of inequality, and multiplicity in terms of addition. This perspective offers an alternative and equivalent definition for the greatest common divisor and least common multiple.

Corollary 1. *Let a and b be integers, with prime factorizations $a = 2^{e_2}3^{e_3}\cdots$, $b = 2^{f_2}3^{f_3}\cdots$. Then,*

$$GCD\,(a,b) = 2^{min(e_2,f_2)}3^{min(e_3,f_3)}\ldots$$

$$LCM\,(a,b) = 2^{max(e_2,f_2)}3^{max(e_3,f_3)}\ldots$$

Where min and max represent the minimum, and maximum of each pair of exponents, respectively.

Proof. We prove the case for the GCD, leaving the LCM for the reader. Suppose that $g = GCD\,(a,b)$. Naturally, as g is an integer, it can be factored into primes, say

$$g = 2^{h_2}3^{h_3}\cdots$$

What can we say about g? We know that g divides both a and b, certainly, so $h_p \leq e_p$, $h_p \leq f_p$. But we also know that g is divided by every other divisor of a and b. Among all divisors, it is the maximum. So, in terms of exponents, h_p cannot be greater than e_p or f_p, and yet, it must be the greatest possible between the two, which is precisely $min(e_p, f_p)$. □

In summary, all integers (and rational numbers, as we will see) afford a unique decomposition into primes. In turn, this decomposition allows us to explore divisibility relationships as a consequence of the exponents, giving new perspective on some old definitions.

Exercise. *Let a and b be integers. Then, if $GCD\,(a,b) = 1$, $GCD\,(a^m, b^n) = 1$ for all positive integers m, n.*

(Hint: $GCD\,(a,b) = 1 \Rightarrow min(e_p, f_p) = 0$).