CMPSCI 250: Introduction to Computation

Lecture #15: The Fundamental Theorem of Arithmetic
David Mix Barrington
27 February 2012

The Fundamental Theorem of Arithmetic

- Statement of the Theorem
- Existence of a Factorization
- A Recursive Algorithm for Factorization
- Uniqueness of Factorization: Why a Problem?
- The Atomicity Lemma
- Finishing the Proof

Statement of the Theorem

- The **Fundamental Theorem of Arithmetic** says that any positive natural has a *unique* factorization as a product of prime numbers. That is, any positive natural n can be expressed as $p_1 \times p_2 \times \ldots \times p_k$ where each of the numbers p_i is prime, and there cannot be two "different" factorizations of the same n.

- What exactly does "unique" mean in this context? We can write 60, for example, as $3 \times 2 \times 5 \times 2$, or as $5 \times 2 \times 2 \times 3$, or as $2 \times 2 \times 3 \times 5$, and these are different sequences of primes. But each one of them contains two 2's, a 3, and a 5. Our definition of **unique factorization** is that any two factorizations contain the same primes and the same number of each prime.

- The prime factorization of 1 contains 0 primes (an empty product always gives 1). The prime factorization of a prime number has just one prime, itself. The prime factorization of a composite number has more than one prime, or more than one copy of the same prime, or both.

Existence of a Factorization

- Proving the Fundamental Theorem requires two subproofs. We need to prove that at least one factorization exists, and that any two factorizations of n have the same number of each prime.

- The first part is fairly easy. Let n be an arbitrary positive natural. If $n = 1$ or if n is prime, we are done. Otherwise n is composite, which means *by definition* that there exist numbers x and y, each greater than 1, such that $n = x \times y$. Clearly x and y must each be smaller than n.

- If we can *recursively* get prime factorizations of x and y, all we need to do is to put the two factorizations together with another × sign, and we have a factorization of n.

- The recursion cannot go on forever because we keep factoring smaller numbers.

A Recursive Algorithm for Factorization

- Here is some pseudo-Java code, using the `natural` data type. The base of the recursion is when n is 0 or 1. The method sets d to 2 and then increases it until it reaches a value that divides evenly into n. (This has to happen eventually because n divides itself.) Then it prints d, now the smallest prime divisor of n, and recurses on n/d. Note that we use the “square root” trick -- if d gets bigger than the square root of n we jump straight to n.

```
public void factor (natural n) {
// Prints prime factors in ascending order, one per line
   if (n <= 1) return;
   natural d = 2;
   while (n % d != 0) {
      d++;
      if (d * d > n) d = n;}
   System.out.println (d);
   factor (n/d);
   return;}
```

Uniqueness of Factorization: Why a Problem?

- The problem with proving the uniqueness of factorization is that we have heard all our lives that the result is true.

- Consider the two numbers $17 \times 19 \times 23 \times 29$ and $3 \times 5^3 \times 7 \times 83$, each of which is an odd number somewhere around 200,000. We could calculate these two numbers and show that they are not equal, but why is it *impossible* that they be equal?

- We'd like to say "3 divides the number on the right, but not the number on the left". The first is obvious, but the second *assumes* uniqueness of factorization, which we have not yet proved.

- In this special case we can see that the decimal for the number on the right ends in 5, while the one for the number in the left does not. We could also *calculate* the remainder mod 3 for the number on the left, which won't be 0. This latter approach will be what we will generalize for our proof.

The Atomicity Lemma

- Remember that the word **atomic** comes from the Greek for "indivisible". The **Atomicity Lemma** says that if a prime number p divides a product $a \times b$, then p divides either a or b (or both). That is, p is "atomic" in that its property of dividing $a \times b$ cannot be split -- it cannot partially divide a and partially divide b.

- We will prove this lemma by contrapositive. We let p, a, and b be arbitrary, assume that p is prime, and assume that p does *not* divide either a or b. If we can prove that p then does not divide $a \times b$, we will have the contrapositive.

- If a prime number p does not divide either a or b, it must be relatively prime to each. So by the Inverse Theorem, there must exist numbers x and y such that $ax \equiv 1 \pmod{p}$ and $by \equiv 1 \pmod{p}$. We can just multiply to get $axby \equiv 1 \pmod{p}$.

- Now we know that p cannot divide ab, because then we would have $ab \equiv 0 \pmod{p}$ and thus $axby \equiv 0 \pmod{p}$, contradicting $axby \equiv 1 \pmod{p}$.

Finishing the Proof

- Suppose now that a positive natural n has two different prime factorizations: $n = p_1 \times \ldots \times p_k = q_1 \times \ldots q_m$. We want to show that k = m and that the p's include the same number of each prime as the q's.

- We begin by *cancelling* any prime that occurs both among the p's and among the q's. To be able to do this we must know that $(xz = yz) \rightarrow (x = y)$ whenever z is positive. To do this we prove the contrapositive $(x \neq y) \rightarrow (xz \neq yz)$, which we can do be letting x be the smaller of x and y and writing $y = x + c$ for some positive c. Then $yz = xz + cz$, and thus $xz \neq yz$ because cz, the product of two positive numbers, is positive.

- So we can cancel any primes on both sides. This continues until either everything has cancelled on both side (which is what will happen if the factorizations are the same), we empty one side with one or more primes left on the other (which is impossible), or we have a prime p on one side which divides a product of one or more primes on the other. This last case contradicts the Atomicity Lemma, since no prime divides a different prime.