COMPSCI 250: Introduction to Computation

Lecture #15: The Fundamental Theorem of Arithmetic
David Mix Barrington and Ghazaleh Parvini
10 October 2023

The Fundamental Theorem

- Review EA and Inverses
- 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

Reviewing Inverses

- We have been working with arithmetic where the "numbers" are congruence classes modulo m.
- A class [x] (the set {n: n ≡ x}) has a **multiplicative inverse** if there is another class [y] such that [x][y] = [1], or xy ≡ 1 (mod m).
- The **Inverse Theorem** says that a number z has a multiplicative inverse modulo m if and only if z and m are relatively prime, or gcd(z, m) = 1.

The Inverse Algorithm

- It’s fairly clear that if z and m have a common factor $g > 1$, then a multiplicative inverse for z modulo m is impossible.

- The Euclidean Algorithm is our method to compute gcd’s and thus test for relative primality.

- The **Extended Euclidean Algorithm** takes z and m as inputs and uses the arithmetic from the Euclidean Algorithm, but gets an additional result at each step.

The Inverse Algorithm

- We write each number that occurs as an integer **linear combination** of z and m.
- If z and m are relatively prime, we compute numbers a and b such that az + bm = 1.
- Then a is an inverse of z modulo m and b is an inverse of m modulo z.

```
119 % 65 = 54
65 % 54 = 11
54 % 11 = 10
11 % 10 = 1
10 % 1 = 0
```

```
119 = 1×65 + 54
65 = 1×54 + 11
54 = 4×11 + 10
11 = 1×10 + 1
10 = 10×1 + 0
```

```
119 = 1×119 + 0×65
65 = 0×119 + 1×65
54 = 1×119 - 1×65
11 = -1×119 + 2×65
10 = 5×119 - 9×65
1 = -6×119 + 11×65
```

Review of Chinese Remainder

- If we have two congruences $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$, and m and n are relatively prime, they are equivalent to a single congruence $x \equiv c \pmod{mn}$.
- To compute c, we first find integers y and z such that $ym + zn = 1$.
- Then $c = bym + azn$ works. Modulo m, $c \equiv a[zn] \equiv a$, and modulo b, $c \equiv b[ym] \equiv b$.
- Here's an example with actual numbers.

Chinese Remainder Example

- Let’s have $m = 9$, $n = 5$, $a = 6$, $b = 2$.
- So we want $x \equiv 6 \pmod{9}$ and $x \equiv 2 \pmod{5}$.
- By the Extended EA, we have $9 = 1\cdot9 + 0\cdot5$, $5 = 0\cdot9 + 1\cdot5$, $4 = 1\cdot9 - 1\cdot5$, and $1 = -1\cdot9 + 2\cdot5$. This gives us $y = -1$ and $z = 2$.
- So $c = bym + azn = 2\cdot(-1)\cdot9 + 6\cdot2\cdot5 = -18 + 60 = 42$.
- We might have gotten something off by any multiple of $mn = 45$.

Statement of the FTA

- 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?

Unique Factorization

- We can write 60, for example, as 3 × 2 × 5 × 2, or as 5 × 2 × 2 × 3, or as 2 × 2 × 3 × 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.

Prime Factorizations

- 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.

1 = empty
2 = 2
3 = 3
4 = 2×2
5 = 5
6 = 2×3
7 = 7
8 = 2×2×2
9 = 3×3
10 = 2×5
11 = 11
12 = 2×2×3
13 = 13
14 = 2×7
15 = 3×5
16 = 2×2×2×2

Clicker Question #1

- How many numbers less than 300 are divisible by four distinct primes?
- (a) none
- (b) one
- (c) two
- (d) three

Not the Answer

Clicker Answer #1

- How many numbers less than 300 are divisible by four distinct primes?
- (a) none
- (b) one $210 = 2 \times 3 \times 5 \times 7$, the next is 330
- (c) two
- (d) three

Existence of a Factorization

- For n to be composite means *by definition* that there exist numbers x and y, each greater than 1, such that n = x × 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 Factoring Algorithm

- Here is some pseudo-Java code, using the natural data type.

```
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;}
```

A Recursive Factoring Algorithm

- 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.

Clicker Question #2

- If we call `factor(630)`, which of these numbers will *not* be the argument of a later recursive call to factor?
- (a) 21
- (b) 35
- (c) 105
- (d) 315

Not the Answer

Clicker Answer #2

- If we call `factor(630)`, which of these numbers will *not* be the argument of a later recursive call to factor?
- (a) 21 630/2 = 315, 315/3 = 105,
- (b) 35 105/3 = 35, 35/5 = 7
- (c) 105
- (d) 315

Will This Always Work?

- In COMPSCI 187 we learned three rules for the correctness of a recursive algorithm.
- It must have one or more base cases in which we can see that it does the right thing.
- Its recursion must always reach the base case.
- If we assume that the recursive call is correct, we must then show the original call gets the correct result.

Will This Always Work?

- In the case of our factoring algorithm, the recursive call always is to a smaller natural than the argument of the original call.

- We certainly believe we can’t have infinitely many calls, each to a natural smaller than the previous one.

- But this is actually a profound fact about the naturals, variously called the Least Number Principle or the Law of Mathematical Induction, as we’ll see starting next week.

Why is Uniqueness 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 $3 \times 53 \times 7 \times 83$, 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?

Why is Uniqueness a Problem?

- 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* the 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 9, 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. We will generalize this latter approach 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 × b, then p divides either a or b (or both).
- That is, p is “atomic” in that its property of dividing a × b cannot be split -- it cannot *partially* divide a and *partially* divide b.

Clicker Question #3

- Consider all strings over a non-empty alphabet. We say that a non-empty string w is **atomic** if for any two strings u and v, if w = uv, then either u or v must be equal to w. What are the atomic sets?
- (a) no strings have this property
- (b) only the empty string
- (c) all strings with exactly one letter
- (d) all strings have this property

Not the Answer

Clicker Answer #3

- Consider all strings over a non-empty alphabet. We say that a non-empty string w is **atomic** if for any two strings u and v, if w = uv, then either u or v must be equal to w. What are the atomic sets?
- (a) no strings have this property
- (b) only the empty string we said w is non-empty
- (c) all strings with exactly one letter
- (d) all strings have this property any longer string can be non-trivially factored

Proving the Atomicity Lemma

- 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 also does not divide a × b, we will have the contrapositive.

$$D(p, ab) \to (D(p, a) \lor D(p, b))$$

$$\leftrightarrow$$

$$(\neg D(p, a) \land \neg D(p, b)) \to \neg D(p, ab)$$

Proving the Atomicity Lemma

- 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 ≡ 1 (mod p) and by ≡ 1 (mod p).
- We can just multiply to get axby ≡ 1 (mod p).
- Now we know that p cannot divide ab, because then we would have ab ≡ 0 (mod p) and thus axby ≡ 0 (mod p), contradicting axby ≡ 1 (mod p).

Finishing the FTA 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.

Justifying Cancellation

- To be able to cancel like 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.

Finishing the FTA Proof

- We can cancel any primes that appear on both sides. This continues until one of three things happen:
- (1) Everything has been cancelled on both sides (which will happen if the factorizations are the same).
- (2) We empty one side with one or more primes left on the other (impossible since the empty side is 1).
- (3) We have a prime p on one side, which divides a product of one or more non-p primes on the other. This last case contradicts the Atomicity Lemma.