

CS 5000: Lecture 29

Vladimir Kulyukin

Department of Computer Science

Utah State University

Outline

- Fundamental Theorem of Arithmetic
- Unbounded Minimalization

Fundamental Theorem of Arithmetic

Review: Euclid's 1st Theorem

- If a prime divides the product of two positive integers, then the prime divides at least one of the two integers.
- If p/ab , then p/a or p/b .

Fundamental Theorem of Arithmetic (FTA)

Every positive integer greater than 1 is either a prime or can be written as a product of primes. The factorization is unique except for the order.

(Unique Factorization Theorem)

FTA: Examples

$$6 = 2 \cdot 3$$

$$8 = 2^3$$

$$10 = 2^1 \cdot 5^1 = 5^1 \cdot 2^1$$

$$12 = 2^2 \cdot 3 = 3 \cdot 2^2$$

$$1200 = 2^4 \cdot 3 \cdot 5^2$$

FTA: Motivation

$$1200 = 2^4 \cdot 3 \cdot 5^2$$

Any divisor of 1200 is of the form

$2^x \cdot 3^y \cdot 5^z$, where $x \in [0,4]$, $y \in [0,1]$, $z \in [0,2]$.

For example, $2^2 \cdot 3^0 \cdot 5$ is a divisor of 1200.

FTA: Proof

1. We need to prove 2 statements:
 1. Every natural number greater than 1 has a prime factorization, i.e., can be written as a product of primes.
 2. The prime factorization is unique.

FTA: Proof (Part 1)

1. Suppose not every natural number greater than 1 has a prime factorization.

2. By the well-ordering principle, there must be the smallest such number.

Call this number n .

3. n is not a prime, because, if it were, it would have itself as its factorization.

4. So n is a composite.

5. Since n is a composite, $n = ab$, where $a < n$ and $b < n$.

6. Since a and b are positive integers less than n and n is the smallest number that does not have a prime factorization, a and b both have prime factorizations.

FTA: Proof (Part 1)

Conclusion:

n has a prime factorization that consists of the prime factorization of a followed by the prime factorization of b .

FTA: Proof (Part 2)

1. Recall Euclid's 1st Theorem : if p is a prime and $p|ab$, then $p|a$ or $p|b$.
2. Let n be a natural number greater than 1 that has two prime factorizations F_1 and F_2 .
3. $n = F_1 = p_1 \dots p_n = F_2 = q_1 \dots q_m = n$.
4. Take p_1 . $p_1|n$. Thus, $p_1|q_1 \dots q_m$.
5. By Euclid's 1st Theorem, $p_1|q_1$ or $p_1|q_2 \dots q_m$. Since p_1 is a prime, it must be the case that $p_1 = q_1$ or $p_1 = q_i$, $2 \leq i \leq m$.
6. The same trick can be repeated for p_2 , p_3 , etc.

Unbounded Minimalization

Unbounded Minimalization

$$\min_y P(y, x_1, \dots, x_n) \Leftrightarrow$$

The least value of y for which $P(y, x_1, \dots, x_n)$ is true, if there is such a value. If there is no value of y for which $P(y, x_1, \dots, x_n)$ is true, $\min_y P(y, x_1, \dots, x_n)$ is undefined.

Example 1

$$x - y = \min_z [y + z = x]$$

Example 1

$$10 - 7 = \min_z [7 + z = 10] = 3.$$

$$7 - 10 = \min_z [10 + z = 7] = \uparrow.$$

Theorem 7.2 (Ch. 3)

If $P(y, x_1, \dots, x_n)$ is a computable predicate
and if $g(x_1, \dots, x_n) = \min_y P(y, x_1, \dots, x_n)$, then
 g is partially computable.

Theorem 7.2: Proof

[A] IF $P(Y, X_1, \dots, X_n)$ GOTO E

$Y \leftarrow Y + 1$

GOTO A

Theorem 7.2 (Ch. 3): Observations

- Theorem 7.2 in Ch. 3 offers us an important insight into unbounded minimalization.
- Even when a predicate is computable, there is no guarantee that the unbounded minimalization of that predicate will be computable.

Theorem 7.2 (Ch. 3): Observation

Let $P(z,10,7) = 10 + z = 7$.

P is computable. However,

$\min_z [P(z,10,7)]$ is not.

Recommended Reading

- Section 3.7.