

CS 5000: Lecture 28

Vladimir Kulyukin

Department of Computer Science

Utah State University

Outline

- Number Theory
 - A Bit of History
 - Well-Ordering Principle
 - Bezout's Identity
 - Euclid's Theorems
 - Computing Primes
 - Fundamental Theorem of Arithmetic

Origins of Decimals

“The world owes the decimal notation to the Hindus, and arithmetic as a practical science would have been impossible without the decimal notation. The Arabs first learned that notation from the Hindus and introduced it into Europe. The ancient Greeks and Romans were ignorant of it and consequently never made much progress in numerical science.”

Romesh Chunder Dutt. “A History of Civilization in Ancient India Based on Sanskrit Literature – Rationalistic Age (1,000 BC – 242 BC)”

Sulva Sutra (8-th Century B.C.)

“The square of the diagonal of an oblong is equal to the square of both its sides.”

Sulva Sutra (8-th Century B.C.)

- How to find the value of a diagonal in relation to the side of the square?
- “Increase the measure by its third part, and this third by its own fourth, less the thirty-fourth part of that fourth.”

$$1 + \frac{1}{3} + \frac{1}{3 \cdot 4} - \frac{1}{3 \cdot 4 \cdot 34} = 1.4142156$$

Sulva Sutra (8-th Century B.C.)

$$\sqrt{2} = 1.414214$$

$$1 + \frac{1}{3} + \frac{1}{3 \cdot 4} - \frac{1}{3 \cdot 4 \cdot 34} = 1.4142156$$

Well-Ordering Principle

Each non - empty subset of N has a smallest number.

The set of natural numbers is well - ordered.

Lemma 1

For any natural number $A > 1$, there exists a prime number p such that p/A .

Proof 1

1. Assume there is a set K of natural numbers greater than 1 that do not have any prime divisors. By the well-ordering principle, K has a smallest element $k > 1$.
2. k cannot be a prime, because if it were, it would have itself as a prime divisor.
3. Then k is a composite number. Thus,
 $k = ab, a < k$ and $b < k$.
4. Since k is the smallest natural number that does not have a prime divisor and $a < k$ and $b < k$, a and b both have prime divisors.

Proof 1

5. But then k must have the same prime divisors as a and b .

Bezout's Identity

If a and b are integers whose greatest common divisor is d , then there are integers x and y such that

$$ax + by = d.$$

Bezout's Identity: Example

$$\gcd(12, 42) = 6$$

$$12x + 42y = 6$$

$$x = 4, y = -1$$

$$12 \cdot 4 + 42 \cdot (-1) = 6$$

$$x = -3, y = 1$$

$$(-3) \cdot 12 + 1 \cdot 42 = 6$$

Euclid's 1st Theorem (Book VII of Euclid's Elements)

- 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 $p|b$.

Euclid's 1st Theorem: Proof

If $p \mid ab$, p is prime, then $p \mid a$ or $p \mid b$.

Assume that $p \mid ab$, p is prime, $\neg(p \mid a)$.

Then $\gcd(p, a) = 1$. By Bezout's Identity,
there are integers x and y such that $px + ay = 1$.

Since $p \mid ab$, $rp = ab$, for some integer r .

$$\begin{aligned} b &= b(px + ay) = bpx + bay \\ &= bpx + rpy = p(bx + ry). \end{aligned}$$

So p is a factor of b .

Euclid's 2nd Theorem (Proposition IX.20 in Euclid's Elements)

The number of primes is infinite.

Euclid's 2nd Theorem

2,3,5,7,11,13,17,...

Let p_i be the i -th prime.

$$N = 2 \cdot 3 \cdot 5 \cdot \dots \cdot p_i + 1.$$

N is the i -th Euclid number.

Euclid's 2nd Theorem Reformulated

Given a finite sequence of primes
 $2, 3, 5, \dots, p_i$, $N = 2 \cdot 3 \cdot 5 \cdot \dots \cdot p_i + 1$ is
either a new prime or a product of
primes.

Euclid's 2nd Theorem: Proof

1. Let there be a finite number of primes.
2. Let these primes be $2, 3, 5, \dots, p_i$.
3. Consider the number $E = 2 \cdot 3 \cdot 5 \cdot \dots \cdot p_i + 1$.
4. E is not divisible by any primes $2, 3, 5, \dots, p_i$.
5. E is either a prime or a composite number.
6. If E is a prime, we are done.
7. By Lemma 1, if E is a composite, E must have a prime divisor.
8. But from 4, it follows that the prime divisor must be greater than p_i .

Euclid's 2nd Theorem: Another Formulation

Let p_i be the i -th prime. So that $p_0 = 0$,

$$p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \dots$$

Consider $E = p_n! + 1$. Then E is either a prime or is divisible by a prime $> p_n$.

Euclid's 2nd Theorem: Proof

Assume that E is not a prime. Then E is composite. Then there must be a prime divisor of E . That prime divisor must be greater than p_n .

Equation 7.1 (Ch. 3)

$$P_{n+1} \leq P_n! + 1.$$

Equation 7.1: Proof

1. Consider $E = p_n! + 1$.
2. By Euclid's 2nd Theorem, E is either a prime or has a prime divisor $> p_n$.
3. Either way, $p_{n+1} \leq p_n! + 1$.

Examples

$$p_0 = 0$$

$$p_1 = 2$$

$$p_2 = 3$$

$$p_3 = 5 \leq p_2! + 1 = 3 \cdot 2 \cdot 1 + 1 = 7$$

$$p_4 = 7 \leq p_3! + 1 = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 + 1 = 121$$

Example 1

Show that p_n is primitive recursive.

Example

1. $p_0 = 0$.

2. $p_{n+1} = \min_{t \leq p_n! + 1} [\text{Prime}(t) \& t > p_n]$.

Example 1

$$h(y, z) = \min_{t \leq z} [\text{Prime}(t) \& t > y].$$

$$k(x) = h(x, x!+1).$$

Example 1

1. $p_0 = 0.$

2. $p_{n+1} = k(p_n).$

Fundamental Theorem of Arithmetic

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)

Suggested Reading

- Section 3.7.