Lecture 3: Primes and Chinese Remainder Theorem

Lecture 3

Objectives

By the end of this lecture you should be able to understand

1. Primes and Composites
2. Fundamental Theorem of Arithmetic
3. Unique Factorization and its implications
4. Chinese Remainder Theorem

Outline

Primes and Composites

Definition

A positive integer $p > 1$ is called a prime number p if its only positive divisors are 1 and p, i.e., $d \mid p$ implies that either $d = 1$ or $d = p$. Any integer greater than 1 that is not a prime is called a composite number.

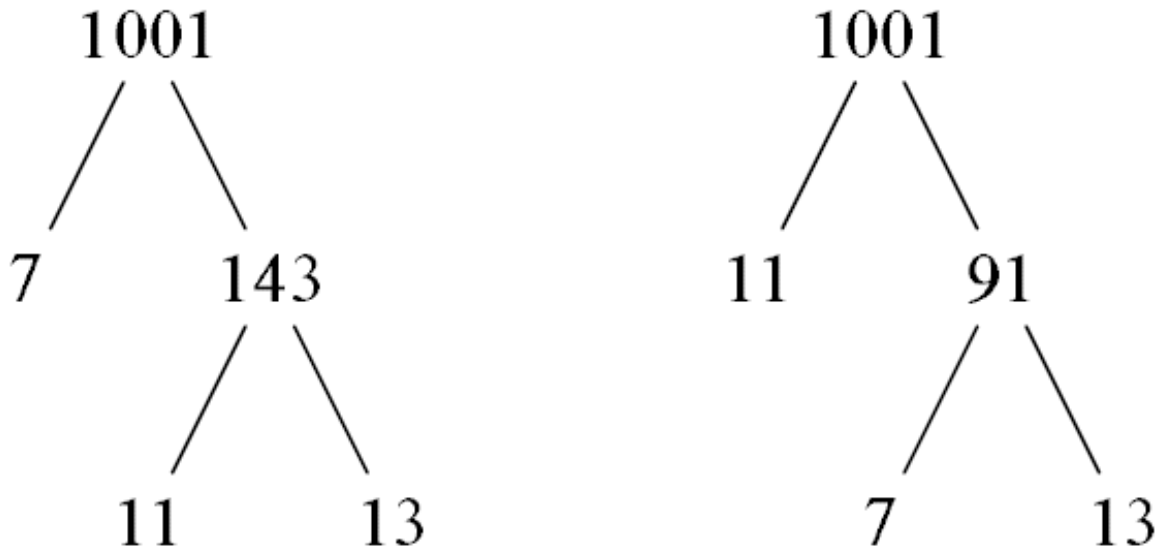
- Integer 0 is neither a prime nor composite.
- Integer 1 is neither a prime nor composite.
- Integer 2 is the only even prime.
- Primes are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots$
- Composites are $4 = 2 \times 2$, $6 = 2 \times 3$, $8 = 2 \times 4$, $10 = 2 \times 5$, $12 = 2 \times 6$, $14 = 2 \times 7$, $15 = 3 \times 5$, $\ldots$

Integer Factorization

- By definition, a composite number can be factorized into a product of two smaller integers
$$1001 = 7 \times 143$$
- If one of the factors is not prime, we factorize it into a product of two even smaller integers
$$1001 = 7 \times 143 = 7 \times 11 \times 13$$
- We repeat this process until the number is factorized into prime factors. This process is called *Integer Factorization*.
- Factorization sequence is not unique, we could have done
$$1001 = 11 \times 91 = 11 \times 7 \times 3$$
- *But* the final factorization form is unique.

Integer Factorization as a Binary Tree

- We can represent each way of factorization as a binary tree



- Integers in the leaves give a representation of 1001 as a product of primes.
- Notice that the two final representations differ only by the order of these primes.

Is the Representation Unique?

Consider this example

$$78227 \times 244999 = 19165536773 = 99599 \times 192427$$

Does it prove that there can be two different representations of the same integer as a product of primes?

- 78227 is not a prime! $78227 = 137 \times 571$
- 99599 is not a prime! $99599 = 137 \times 727$
- 244999 is not a prime! $244999 = 337 \times 727$
- 192427 is not a prime! $192427 = 337 \times 571$

$19165536773 = 137 \times 337 \times 571 \times 727$ is the correct prime factorization of 19165536773

Another form of Euclid's Lemma

Lemma

If p is a prime number, and p divides ab, then p divides either a or b.

Proof.

- Assume $p \nmid a$
- $\gcd(a,p) \mid p$ implies either $\gcd(a,p) = 1$ or $\gcd(a,p) = p$
- But $p \nmid a$, then $\gcd(a,p) = 1$
- Then multiplication by a is invertible: $xa \equiv 1 \pmod{p}$ for some $x \in \{1, 2, \ldots, p-1\}$
- $p \mid ab \longrightarrow ab \equiv 0 \longrightarrow xab \equiv 0 \longrightarrow b \equiv 0 \pmod{p} \longrightarrow p \mid b$

Generalization to multiple factors

Corollary (1)

If p is a prime, and $p \mid a_1 a_2 \dots a_n$, then $p \mid a_k$ for $1 \leq k \leq n$.

Corollary (2)

If $p, q_1, q_2, \dots, q_n$ are all primes, and $p \mid q_1 q_2 \dots q_n$, then $p = q_k$ for $1 \leq k \leq n$.

Proof.

(1) Do it by yourself using induction
(2) From Corollary (1), we know $p \mid q_k$ for $1 \leq k \leq n$. But since q_k is prime, its only factors are 1 and q_k itself. Because p is prime, then $p > 1$, then we conclude that $p = q_k$ □

Fundamental Theorem of Arithmetic

Theorem

Every integer $n > 1$ can be represented as a product of one or more prime numbers. Any two such representations of the same integer n can differ only by the order of factors.

Proof of Uniqueness

Proof.

- Assume two different representations

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$$

- Assume the two representations have common factors
  $\Longrightarrow$ Cancel them until there are no more common factors.

- Assume the two representations do not have common factors.
  Since $p_1 | q_1 q_2 \dots q_l$, then p_1 divides one of $q_1, q_2, \dots, q_l$.
  Then $p_1 \mid q_i,\ 1 \leq i \leq l$, But since q_i is prime, then $p_1 = q_i$
  $\Longrightarrow$ Contradiction.

Canonical Factorization

For any representation of n as a product of primes, we can sort the factors in ascending order and group all the equal primes together. Then we will get the canonical representation:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

where $p_1 < p_2 < \ldots < p_k$ are primes, and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers.

It follows from the unique factorization theorem that the canonical representation of any $n > 1$ is unique

Other Representations

- Assume a set of primes $p_1 = 2, p_2 = 3, \ldots p_m$ such that all prime divisors of n are in this set, then we can represent

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}$$

- In this case, n is represented as a sequence

$$(\alpha_1, \alpha_2, \ldots, \alpha_m), \text{ where } \alpha_i \begin{cases} = 0, & \text{if } p_i \nmid n \\ \neq 0, & \text{if } p_i \mid n \end{cases}$$

- For the set of all primes $\{p_1, p_2, p_3, \ldots\}$, any positive integer n is represented by the infinite sequence $(\alpha_1, \alpha_2, \alpha_3, \ldots)$
- In this representation, we can easily multiply 2 numbers by adding their power sequences, but there is no simple way to sum two numbers.

Divisibility Criterion

When does m divides n?

- Consider canonical representations:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$
$$n = q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}$$

- Then $m \mid n$ when:
  1. $p_i \in \{q_1, q_2, \dots, q_l\}\ \forall i \in \{1, 2, \dots, k\}$
  2. If $p_i = q_j$, then $\alpha_i \leq \beta_j$

Coprime Numbers

When numbers m and n are coprime? when $\gcd(m,n) = 1$

- Consider canonical representations:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$
$$n = q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}$$

- Then $\gcd(m,n) = 1$ when
  1. $p_i \notin \{q_1, q_2, \dots, q_l\}\ \forall i \in \{1, 2, \dots, k\}$
  2. $q_j \notin \{p_1, p_2, \dots, q_k\}\ \forall j \in \{1, 2, \dots, l\}$

Computing GCD and LCM

- Let $p_1, p_2, \ldots, p_k$ be all prime divisors of m and n
- Then

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$
$$n = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$$
$$\gcd(m,n) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \ldots p_k^{\min(\alpha_k,\beta_k)}$$
$$\operatorname{lcm}(m,n) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \ldots p_k^{\max(\alpha_k,\beta_k)}$$

- Some α_i and β_j can be zero in this case.
- For any α and β: $\min(\alpha,\beta) + \max(\alpha,\beta) = \alpha + \beta$
- Then $\gcd(m,n) \times \operatorname{lcm}(m,n) = mn$

Exercise

Lemma

If $a \mid n$, $b \mid n$ *and* $\gcd(a, b) = 1$, *then* $ab \mid n$

Proof.

Prove it by yourself using the canonical representation of a, b and n.

□

GCD vs. Prime Factorization

Note that computing GCD is much easier than prime factorization. The former can be done with Euclid's algorithm, and no efficient algorithm is known for the latter.

Historical Example

- Imagine you are a general, and you want count your troop while keeping your troop count N secret from enemy [1].
- In a morning drill you ask your soldiers to line up in rows of $5 \rightarrow$ you note that 3 soldiers are left in the last row.
- Then, you divide them into rows of $8 \rightarrow 7$ are left in the last row.
- Then, you divide them into rows of $9 \rightarrow 2$ are left in the last row.
- Assuming that $N < 350$, then the troops count $N = 263$.

[1] www.quantamagazine.org/how-ancient-war-trickery-is-alive-in-math-today-20210914

In a Mathematical Notation

- Our goal is to find an integer x that satisfies the following system of congruence

$$x \equiv 3 \pmod 5 \tag{1}$$
$$x \equiv 7 \pmod 8 \tag{2}$$
$$x \equiv 2 \pmod 9 \tag{3}$$

- 1st congruence tells that $x \in R_5 = \{3, 8, 13, 18, 23, \ldots\}$
- 2nd congruence refine our choices by limiting them to $x \in R_5 \cap R_8$, where $R_8 = \{7, 15, 23, 31, \ldots\}$
- 3rd congruence further refine our choices by limiting them to $x \in R_5 \cap R_8 \cap R_9$, where $R_9 = \{2, 11, 20, \ldots\}$

Chinese Remainder Theorem (CRT)

Theorem

Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1 \; \forall \, i \neq j$. Then the system of linear congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a solution $x \equiv a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r \pmod{n}$, where $n = n_1 n_2 \ldots n_r$, $N_i = n/n_i$, and x_i is the solution of $N_i x_i \equiv 1 \pmod{n_i}$

Direct Application of CRT

To find a simultaneous solution of the system of linear congruence

$$x \equiv 3 \pmod 5$$
$$x \equiv 7 \pmod 8$$
$$x \equiv 2 \pmod 9$$

- Construct $n = 5 \times 8 \times 9 = 360 \rightarrow N_1 = 72, N_2 = 45, N_3 = 40$
- Solve $72x_1 \equiv 1 \pmod 5$ to get $x_1 \equiv 3 \pmod 5$
- Solve $45x_2 \equiv 1 \pmod 8$ to get $x_2 \equiv 5 \pmod 8$
- Solve $40x_3 \equiv 1 \pmod 9$ to get $x_3 \equiv 7 \pmod 9$
- $\hat{x} \equiv 3N_1x_1 + 7N_2x_2 + 2N_rx_r \equiv 2783 \equiv 263 \pmod n$

Proof of Existence

Proof.

- We look at the solution x in modulo n_i

$$x \equiv a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r \pmod{n_i}$$

- $N_i = n/n_i = n_0 n_1 \ldots n_{i-1} n_{i+1} \ldots n_r$ has all moduli except n_i
- N_j a multiple of n_i $\forall j \neq i \implies N_j \equiv 0 \pmod{n_i}$ $\forall\, j \neq i$
- Then we have $x \equiv a_i N_i x_i \pmod{n_i}$ (all other terms are cancelled)
- But $\gcd(N_i, n_i) = 1$ because all moduli are co-primes
- Hence, the congruence $N_i x_i \equiv 1 \pmod{n_i}$ has a unique solution
- Then $x \equiv a_i N_i x_i \equiv a_i \pmod{n_i}$

Proof of Uniqueness

Proof.

- Assume y is any other solution for the system of congruence

$$x \equiv a_i \equiv y \pmod{n_i} \quad \forall i \in \{1, 2, \ldots, r\}$$

- Then $n_i \mid x - y \quad \forall i \in \{1, 2, \ldots, r\}$
- But all moduli are co-primes, $\gcd(n_i, n_j) = 1$
- Then their product also divides $x - y \implies n_1 n_2 \ldots n_r \mid x - y$
- This means $n \mid x - y$ or $x \equiv y \pmod{n}$
- Therefore, the 2 solution must be congruent in module n

System of Linear Congruences in Two Unknowns

Theorem

The system of linear congruences

$$ax + by \equiv r \pmod{n}$$
$$cx + dy \equiv s \pmod{n}$$

has a unique solution modulo n whenever $\gcd(ad - bc, n) = 1$

Proof.

- Using method of elimination

$$(ad - bc)x = dr - bs \pmod{n},\ (ad - bc)y = as - cr \pmod{n}$$

- $ad - bc$ has a unique inverse modulo n iff $\gcd(ad - bc, n) = 1$

□

Chinese Remainder Map

Theorem

Let $n_1, n_2, \ldots, n_r$ *be positive integers such that* $\gcd(n_i, n_j) = 1 \, \forall \, i \neq j$, $n = n_1 n_2 \ldots n_r$, *and* $x \equiv a_i \pmod{n_i} \, \forall i = 1, \ldots, r$. *Define the map*

$$\theta : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \mathbb{Z}_{n_r},$$

where

$$\theta(x) = (a_1, a_2, \ldots, a_r).$$

This map is unique in modulo n

Properties of Chinese Remainder Map

For all $\alpha, \beta \in \mathbb{Z}_n$, if $\theta(\alpha) = (\alpha_1, \ldots, \alpha_r)$ and $\theta(\beta) = (\beta_1, \ldots, \beta_r)$ [2]

- Addition: $\theta(\alpha + \beta) = (\alpha_1 + \beta_1, \ldots, \alpha_r + \beta_r)$
- Negative: $\theta(-\alpha) = (-\alpha_1, \ldots, -\alpha_r)$
- Multiplication: $\theta(\alpha\beta) = (\alpha_1\beta_1, \ldots, \alpha_r\beta_r)$
- Inverse: If the multiplicative inverses of α, α_1, ..., α_r exist in modulo n, n_1, ..., n_r, then $\theta(\alpha^{-1}) = \left(\alpha_1^{-1}, \ldots, \alpha_r^{-1}\right)$

This mapping can be used to split a very large number (in modulo n) into its remainders in modulo $(n_1, \ldots, n_r)$ such that $n_1 n_2 \ldots n_r = n$. This number splitting is used to accelerate computations by parallel processing of the remainders α_i on multiple threads/blocks in GPUs or multiple processes in mutli-core CPUs. It can be also used to speed up regular algorithms on integer numbers (section 4.4 in Shoup book)

[2] A Computational Introduction to Number Theory and Algebra, Victor Shoup, version 2, Theorem 2.8