DM549 and DS820

Lecture 14: Solving Congruences

Kevin Aguyar Brix
Email: kabrix@imada.sdu.dk

University of Southern Denmark

30 October, 2024

Last Time: Primes, gcd, lcm

Definition (Definition 4.3.1)

Let $n \in \mathbb{Z}$ with $n \geq 2$. We call n a *prime number* (primtal) if the only positive factors of n are 1 and n. If n is not prime, n is called *composite* (sammensat).

The Fundamental Theorem of Arithmetic (no proof, Theorem 4.3.1)

Let $n \in \mathbb{Z}$ with $n \geq 2$. One can write n as a product of prime numbers in exactly one way (up to rearranging factors).

Definition (Definition 4.3.2)

Let $a, b \in \mathbb{Z} \setminus \{0\}$. Then $\gcd(a, b) = \max\left\{d \;\middle|\; d \mid a \wedge d \mid b\right\}$ is called the *greatest common divisor* (største fælles divisor) of a and b.

Definition (Definition 4.3.2)

Let $a, b \in \mathbb{Z}^+$. Then $\operatorname{lcm}(a, b) = \min\left\{m \;\middle|\; a \mid m \wedge b \mid m\right\}$ is called the *least common multiple* (mindst fælles multiplum) of a and b.

Last Time: The Euclidean Algorithm

Euclidean Algorithm: To compute $\gcd(a, b)$ assuming $a > b$,

- Start with $x = a$ and $y = b$.
- As long as $y \neq 0$:
  - Replace (x, y) with $(y, x \bmod y)$.
- Return x.

Theorem (Theorem 4.3.6)

Let $a, b \in \mathbb{Z}^+$. Then there exist $s, t \in \mathbb{Z}$ with $\gcd(a, b) = sa + tb$.

A Quiz

Go to `pollev.com/kevs`

When Division of Congruences *is* Possible

Theorem (Theorem 4.3.7)

Let $a, b \in \mathbb{Z}$, $c \in \mathbb{Z} \setminus \{0\}$ and $m \in \mathbb{Z}^+$. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

In the proof, we use the following lemma:

Lemma (Lemma 4.3.2)

Let $a, b, c \in \mathbb{Z}^+$ with $\gcd(a, b) = 1$ and $a \mid bc$. Then $a \mid c$.

This lemma, in turn, follows by the previous theorem. Recall:

Theorem (Theorem 4.3.6)

Let $a, b \in \mathbb{Z}^+$. Then there exist $s, t \in \mathbb{Z}$ with $\gcd(a, b) = sa + tb$.

Remark: Lemma 4.3.2 can also be used to show the uniqueness part of the fundamental theorem of arithmetic.

Linear Congruences and Multiplicative Inverses

Definition

Let $a, b, m \in \mathbb{Z}$ with $m \geq 2$, and let $x \in \mathbb{Z}$ be variable. Then

$$a \cdot x \equiv b \pmod{m}$$

is called a *linear congruence* (linear congruence).

Remark:

- It is possible that no solution exists.
- If $x = n$ is a solution, then $x = n + k \cdot m$ is also a solution for any $k \in \mathbb{Z}$!

Multiplicative Inverse

Theorem (Theorem 4.4.1 for the first part)

Let $a, m \in \mathbb{Z}$ with $m \geq 2$. If $\gcd(a, m) = 1$, there exists precisely one $\bar{a} \in \mathbb{Z}_m$ with

$$\bar{a} \cdot a \equiv 1 \pmod{m}.$$

We call $\bar{a}$ the *multiplicative inverse* (multiplicativ invers) of a modulo m. If $\gcd(a, m) \neq 1$, there does not exist such an inverse.

Recall: $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$.

Solving linear congruences when $\gcd(a, m) = 1$**:**

- Compute multiplicative inverse $\bar{a}$ of a modulo m.
  - The constructive proof shows how!
- Multiply both sides of the congruence with $\bar{a}$.

Existence of Solutions and Inverses: Overview

Multiplicative inverses of a modulo m:

- If $\gcd(a, m) = 1$, there exists a unique multiplicative inverse in $\mathbb{Z}_m$.
- If $\gcd(a, m) \neq 1$, there does not exist a multiplicative inverse.

Solutions of the congruence $a \cdot x \equiv b \pmod{m}$:

- If $\gcd(a, m) = 1$, there exists a unique solution in $\mathbb{Z}_m$.
- If $\gcd(a, m) \neq 1$, there may exist a solution.
  - One can derive conditions under which a solution exists, but we will not elaborate further.

A Quiz

Go to `pollev.com/kevs`

A Motivating Example

Assume:

- Your favorite band puts out an album next year, and from then on every four years.
- Your second favorite band puts out an album in three years, and from then on every six years.

In which year will there be an album from both bands?

Congruence Systems

Definition

Let $a_1, \ldots, a_n, m_1, \ldots, m_n \in \mathbb{Z}$ with $m_1, \ldots, m_n \geq 2$, and let $x \in \mathbb{Z}$ be variable. Then

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\ldots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

is called a *congruence system* (kongruenssystem)

Remark:

- If $x = n$ is a solution, then $x = n + k \cdot m$ is also a solution for any $k \in \mathbb{Z}$, where m is the least common multiple of $m_1, m_2, \ldots, m_n$.
- The following are equivalent:
  - (i) There exists a solution.
  - (ii) There exists a solution in $\mathbb{Z}_m$.
  - (iii) There exists precisely one solution in $\mathbb{Z}_m$.

Repetition: The Chinese Remainder Theorem

The Chinese Remainder Theorem (Theorem 4.4.2)

Let $a_1, \ldots, a_n \in \mathbb{Z}$, and let $m_1, \ldots, m_n \geq 2$ be integers that are pairwise relatively prime. Then the congruence system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\ldots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution $x \in \mathbb{Z}_m$ where $m = m_1 \cdot m_2 \cdot \cdots \cdot m_n$.

Note on the name: Name is due to Chinese heritage of problems involving systems of linear congruences.

Solving Congruence Systems with Pairwise Coprime Moduli

The previous constructive proof yields the following algorithm for solving congruence systems with pairwise coprime moduli.

Algorithm:

- Let $m = m_1 \cdot m_2 \cdot \cdots \cdot m_n$.
- For $k \in \{1, \ldots, n\}$:
  - Let $M_k = \frac{m}{m_k}$.
  - Find the multiplicative inverse y_k of M_k modulo m_k (e.g., using the Euclidean Algorithm).
- Return $x = \sum_{k=1}^{n} M_k y_k a_k$.

Remark: If $m_1, \ldots, m_n$ are not pairwise prime, a solution to the congruence system *may* exist, but it cannot be computed with the above method! (Why?)