# CSE 15
# Discrete Mathematics

## Lecture 17 – Applications of Congruences & Mathematical Induction

# Announcement

- HW #8
  - Due **5pm** 11/21 (Wed) with 1 extra day of re-submission.

- Reading assignment
  - Ch. 5.1 – 5.4 of textbook

# Applications of Congruences (Ch. 4.5)

- Hashing Functions
- Check Digits

# Hashing Functions

- **Definition**: A *hashing function* $\boldsymbol{h}$ assigns memory location $\boldsymbol{h(k)}$ to the record that has $\boldsymbol{k}$ as its key.
  - A common hashing function is $h(k) = k \textbf{ mod } m$, where $m$ is the number of memory locations.
  - Because this hashing function is onto, all memory locations are possible.

**Example**: Let $h(k) = k \textbf{ mod } 111$. This hashing function assigns the records of customers with social security numbers as keys to memory locations in the following manner:

$h(064212848) = 064212848 \textbf{ mod } 111 = 14$

$h(037149212) = 037149212 \textbf{ mod } 111 = 65$

$h(107405723) = 107405723 \textbf{ mod } 111 = 14$, but since location 14 is already occupied, the record is assigned to the next available position, which is 15. (Linear Probing)

# Hashing Functions

- The hashing function is not one-to-one as there are many more possible keys than memory locations.
- When more than one record is assigned to the same location, a *collision* occurs.
- Here a collision has been resolved by assigning the record to the first free location.
- There are many other methods of handling with collisions.

# Check Digits: UPCs

- A common method of detecting errors in strings of digits is to add an extra digit at the end, which is evaluated using a function. If the final digit is not correct, then the string is assumed not to be correct.

  **Example**: Retail products are identified by their *Universal Product Codes* (*UPC*s). Usually these have 12 decimal digits, the last one being the check digit.

  The check digit is determined by the congruence:

  $3x_1+x_2+3x_3+x_4+3x_5+x_6+3x_7+x_8+3x_9+x_{10}+3x_{11}+x_{12} \equiv 0 \pmod{10}$.

# Check Digits: UPCs

$3x_1+x_2+3x_3+x_4+3x_5+x_6+3x_7+x_8+3x_9+x_{10}+3x_{11}+x_{12} \equiv 0 \pmod{10}$.

**Problem:**

Suppose that the first 11 digits of the UPC are 79357343104. What is the check digit?

**Solution:**

$3\cdot7+9+3\cdot3+5+3\cdot7+3+3\cdot4+3+3\cdot1+0+3\cdot4+ x_{12} \equiv 0 \pmod{10}$

$21 + 9 + 9 + 5 + 21 + 3 + 12+ 3 + 3 + 0 + 12 + x_{12} \equiv 0 \pmod{10}$

$98 + x_{12} \equiv 0 \pmod{10}$

So, the check digit is 2.

# Check Digits: UPCs

$3x_1+x_2+3x_3+x_4+3x_5+x_6+3x_7+x_8+3x_9+x_{10}+3x_{11}+x_{12} \equiv 0$ (mod 10).

**Problem:**

Is 041331021641 a valid UPC?

**Solution:**

$$3\cdot0+4+3\cdot1+3+3\cdot3+1+3\cdot0+2+3\cdot1+6+3\cdot4+1 \overset{?}{\equiv} 0 \pmod{10}$$

$$0+4+3+3+9+1+0+2+3+6+12+1 = 44 \equiv 4 \not\equiv 0 \pmod{10}$$

Hence, 041331021641 is not a valid UPC.

# Check Digits: ISBNs

- Books are identified by an *International Standard Book Number* (ISBN-10), a 10 digit code.
  - The first 9 digits identify the language, the publisher, and the book.
  - The tenth digit is a check digit, which is determined by the following congruence
$$x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}.$$
- The validity of an ISBN-10 number can be evaluated with the equivalent
$$\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}.$$
- A *single error* is an error in one digit of an identification number and a *transposition error* is the accidental interchanging of two digits. Both of these kinds of errors can be detected by the check digit for ISBN-10.

# Check Digits: ISBNs

$$x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}. \quad \sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}.$$

**Problem:**

Suppose that the first 9 digits of the ISBN-10 are 007288008.

What is the check digit?

**Solution**:

$X_{10} \equiv 1{\cdot}0+2{\cdot}0+3{\cdot}7+4{\cdot}2+5{\cdot}8+6{\cdot}8+7{\cdot}0+8{\cdot}0+9{\cdot}8 \pmod{11}.$

$X_{10} \equiv 0+0+21+8+40+48+0+0+72 \pmod{11}.$

$X_{10} \equiv 189 \equiv 2 \pmod{11}.$

Hence, $X_{10} = 2.$

# Check Digits: ISBNs

$$x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}. \qquad \sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}.$$

**Problem:**

Is 084930149X a valid ISBN10?

X is used for the digit 10.

**Solution**:

$1{\cdot}0+2{\cdot}8+3{\cdot}4+4{\cdot}9+5{\cdot}3+6{\cdot}0+7{\cdot}1+8{\cdot}4+9{\cdot}9+10{\cdot}10 =$

$0 + 16 + 12 + 36 + 15 + 0 + 7 + 32 + 81 + 100 =$

$299 \equiv 2 \not\equiv 0 \pmod{11}$

Hence, 084930149X is not a valid ISBN-10.

# Mathematical Induction (Ch. 5.1)

- Mathematical Induction
- Examples of Proof by Mathematical Induction
- Mistaken Proofs by Mathematical Induction
- Guidelines for Proofs by Mathematical Induction

# Principle of Mathematical Induction

- ***Principle of Mathematical Induction***: To prove that $P(n)$ is true for all positive integers $n$, we complete these steps:
  - ***Basis Step***: Show that $P(1)$ is true.
  - ***Inductive Step***: Show that $P(k) \rightarrow P(k + 1)$ is true for all positive integers $k$.
- To complete the inductive step, assuming the *inductive hypothesis* that $P(k)$ holds for an arbitrary integer $k$, show that $P(k + 1)$ must be true.
- Proofs by mathematical induction do not always start at the integer 1. In such a case, the basis step begins at a starting point $b$ where $b$ is an integer.
- Works when you know the result.

# Proving a Summation Formula by Mathematical Induction

**Example**: Show that: $$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

**Solution**:

- BASIS STEP: $P(1)$ is true since $1(1 + 1)/2 = 1$.
- INDUCTIVE STEP: Assume true for $P(k)$.

  The inductive hypothesis is $$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

  Under this assumption,

$$\begin{aligned}
1 + 2 + \ldots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

# Conjecturing and Proving Correct a Summation Formula

**Example**: Conjecture and prove correct a formula for the sum of the first *n* positive odd integers. Then prove your conjecture.

**Solution**: We have:

$$1=1,\ 1+3 = 4,\ 1+3+5 = 9,\ 1+3+5+7 = 16,\ 1+3+5+7+9 = 25.$$

- We can conjecture that the sum of the first *n* positive odd integers is $n^2$,

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

- We prove the conjecture is proved correct with mathematical induction.
- BASIS STEP: $P(1)$ is true since $1^2 = 1$.
- INDUCTIVE STEP: $P(k) \rightarrow P(k + 1)$ for every positive integer $k$.

*continued* →

# Conjecturing and Proving Correct a Summation Formula

Assume the inductive hypothesis holds and then show that $P(k+1)$ holds has well.

**Inductive Hypothesis**: $1+3+5+\cdots+(2k-1)=k^2$

- So, assuming $P(k)$, it follows that:

$$\begin{aligned}1+3+\cdots+(2k-1)+(2k+1) &= [1+3+\cdots+(2k-1)]+(2k+1)\\ &= k^2+(2k+1)\ (\textit{by the inductive hypo.})\\ &= k^2+2k+1\\ &= (k+1)^2\end{aligned}$$

- Hence, we have shown that $P(k+1)$ follows from $P(k)$.
- Therefore the sum of the first $n$ positive odd integers is $n^2$.

# Proving Inequalities

**Example**: Use mathematical induction to prove that $n < 2^n$ for all positive integers $n$.

**Solution**: Let $P(n)$ be the proposition that $n < 2^n$.

- BASIS STEP: $P(1)$ is true since $1 < 2^1 = 2$.
- INDUCTIVE STEP: Assume $P(k)$ holds, i.e., $k < 2^k$, for an arbitrary positive integer $k$.
- Must show that $P(k + 1)$ holds.
- Since by the inductive hypothesis, $k < 2^k$, it follows that: $k + 1 < 2^k + 1 \leq 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$

Therefore $n < 2^n$ holds for all positive integers $n$. ◀

# Proving Inequalities

**Example**: Use mathematical induction to prove that $2^n < n!$ for every integer $n \geq 4$. //remember the base not 1//

**Solution**: Let $P(n)$ be the proposition that $2^n < n!$.

- BASIS STEP: $P(4)$ is true since $2^4 = 16 < 4! = 24$.
- INDUCTIVE STEP: Assume $P(k)$ holds, i.e., $2^k < k!$ for an arbitrary integer $k \geq 4$. To show that $P(k + 1)$ holds:

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &< 2 \cdot k! \qquad \textit{(by the inductive hypothesis)} \\ &< (k+1)k! \\ &= (k+1)! \end{aligned}$$

Therefore, $2^n < n!$ holds, for every integer $n \geq 4$. ◀

Note here the basis step is $P(4)$, since $P(0)$, $P(1)$, $P(2)$, and $P(3)$ are all false

# Proving Divisibility Results

**Example**: Use mathematical induction to prove that $n^3 - n$ is divisible by 3, for every positive integer $n$.

**Solution**: Let $P(n)$ be the proposition that $n^3 - n$ is divisible by 3.

- BASIS STEP: $P(1)$ is true since $1^3 - 1 = 0$, which is divisible by 3.
- INDUCTIVE STEP: Assume $P(k)$ holds, i.e., $k^3 - k$ is divisible by 3, for an arbitrary positive integer $k$. To show that $P(k + 1)$ follows:

$$\begin{aligned}(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1) \\ &= (k^3 - k) + 3(k^2 + k)\end{aligned}$$

By the inductive hypothesis, the first term $(k^3 - k)$ is divisible by 3 and the second term is divisible by 3 since it is an integer multiplied by 3. So $(k + 1)^3 - (k + 1)$ is divisible by 3.

Thus, $n^3 - n$ is divisible by 3, for every integer positive integer $n$. ◀

# Number of Subsets of a Finite Set

**Example**: Use mathematical induction to show that if $S$ is a finite set with n elements, where $n$ is a nonnegative integer, then $S$ has $2^n$ subsets.

**Solution**: Let $P(n)$ be the proposition that a set with $n$ elements has $2^n$ subsets.

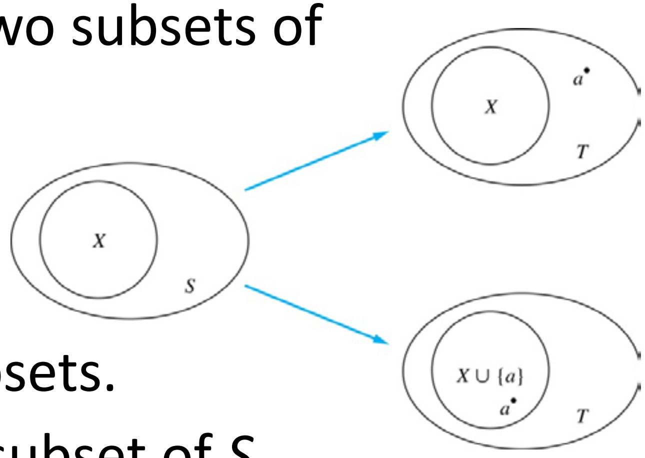
- Basis Step: $P(0)$ is true, because the empty set has only itself as a subset and $2^0 = 1$.
- Inductive Step: Assume $P(k)$ is true for an arbitrary nonnegative integer $k$.

*continued* →

# Number of Subsets of a Finite Set

**Inductive Hypothesis**: For an arbitrary nonnegative integer $k$, every set with $k$ elements has $2^k$ subsets.

- Let $T$ be a set with $k + 1$ elements. Then $T = S \cup \{a\}$, where $a \in T$ and $S = T - \{a\}$. Hence $|S| = k$.
- For each subset $X$ of $S$, there are exactly two subsets of $T$, i.e., $X$ and $X \cup \{a\}$.




- By the inductive hypothesis $S$ has $2^k$ subsets.
- Since there are two subsets of $T$ for each subset of $S$, the number of subsets of $T$ is $2 \cdot 2^k = 2^{k+1}$ .