# Week 4 Part B highlights

- Modular arithmetic and applications
- Proof by contradiction
- Strong induction
- Use insights from proofs to develop new algorithms
- Distinguish between and use as appropriate each of structural induction, mathematical induction, and strong induction

# Tuesday

**Modular Arithmetic, zybook 7.1**: It's the arithmetic used on the clock.

"How many minutes past the hour are we at?" *Model with* **x mod** 60

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Time:** | 12:00pm | 12:15pm | 12:30pm | 12:45pm | 1:00pm | 1:15pm | 1:30pm | 1:45pm |
| **Minutes past noon:** | 0 | 15 | 30 | 45 | 60 | 75 | 90 | 105 |
| **Minutes past the hour:** | 0 | 15 | 30 | 45 | 0 | 15 | 30 | 45 |

**More generally,** given an integer $m > 1$, we can define a **ring** to be the set $\mathbb{Z}_m = \{0, 1, 2, ..., m - 1\}$. The operation **mod m** can then be seen as a function $f_m : \mathbb{Z} \to \mathbb{Z}_m$ that takes an integer $x$ as input and outputs **x mod m**.

We can define arithmetic operations (like addition, subtraction, multiplication, etc) on the elements in this set $\mathbb{Z}_m$ in the usual way, except that the mod $m$ function is applied afterwards to ensure that the result will again be in $\mathbb{Z}_m$.

**Why is modular arithmetic useful?**

**Observation:** For any integers $a, j$ and positive integer $m$, $(a + j \cdot m)$ **mod** $m = a$ **mod** $m$

**Definition:** Let $m$ be an integer greater than 1. Let $a$ and $b$ be any two integers. Then $a$ is congruent to $b$ (**mod** m), denoted as $a \equiv b \pmod{m}$ if and only if ____________________

**Practice using the notation for congruence**

(i) Write examples of numbers that are congruent to each other (**mod** 60):

(ii) Restate the observation $(a + j \cdot m) \textbf{ mod } m = a \textbf{ mod } m$:

(iii) Compute without a calculator:

$(365 + 657) \textbf{ mod } 60 =$ ____________________________________

$(365 \cdot 657) \textbf{ mod } 60 =$ ____________________________________

**Theorem 1:** For $a, b, c \in \mathbb{Z}$ and positive integer $m$

(i) $a \equiv a \pmod{m}$

(ii) $a \equiv b \pmod{m}$ iff $b \equiv a \pmod{m}$

(iii) if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$

**Informally**: congruence is like equality.

**Theorem 2:** For $a, b, a', b' \in \mathbb{Z}$ and positive integer $m$, if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then:

(i) $(a + b) \equiv (a' + b') \pmod{m}$

(ii) $(a - b) \equiv (a' - b') \pmod{m}$

(iii) $(a \cdot b) \equiv (a' \cdot b') \pmod{m}$

**Informally**: can bring mod "inside" and do it first, for addition and for multiplication.

**Some very neat applications of the congruence theorems**[1]

What is $8^{1759} \ \mathbf{mod}\ \mathbf{7}$?

Is the 8000th Fibonacci number divisible by 3?

Prove some of the tricks you learned in high school to check divisibility by 3 and 11

[1] credits: Prof. Daniel Lokshtanov's Winter 22 offering of CS40.

**Proof of some of the congruence theorems**

**Finding multiplicative inverse of a number mod m** : A key step in RSA crypto algorithm

**Definition (zybook 6.5.1):** A multiplicative inverse mod m (or just inverse mod m) of an integer $x$, is an integer $s \in \{1, 2, \ldots, m-1\}$ such that $sx$ **mod** $m = 1$.

**The multiplicative inverse of x (mod m) only exists when:** ____________________

**Theorem (zybook 6.5.2)**: Let x and y be integers, then there are integers $s$ and $t$ such that $gcd(x, y) = sx + ty$

Constructive proof based on Euclid's algorithm, known as extended Euclid's algorithm

**Find the inverse of 3 mod 7**

**Prove** or **disprove** the following claims:

| | |
|---|---|
| Claim: There is a greatest integer. | Claim: There is a least integer. |
| Claim: There is a greatest prime number. | Claim: There is a least prime number. |

**New! Proof by Contradiction** (Rosen 1.7 p86, zybook 7.2)
To prove that a statement $p$ is true, pick another statement $r$ and once we show that $\neg p \to (r \wedge \neg r)$ then we can conclude that $p$ is true.

*Extra examples*: Prove or disprove that $\mathbb{N}$, $\mathbb{Q}$ each have a least and a greatest element.

The **set of rational numbers**, $\mathbb{Q}$ is defined as

$$\left\{ \frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z} \text{ and } q \neq 0 \right\} \qquad \text{or, equivalently,} \qquad \{x \in \mathbb{R} \mid \exists p \in \mathbb{Z} \exists q \in \mathbb{Z}^+ (p = x \cdot q)\}$$

*Extra practice*: Use the definition of set equality to prove that the definitions above give the same set.

**Goal**: The square root of 2 is not a rational number. In other words: $\neg \exists x \in \mathbb{Q}(x^2 - 2 = 0)$

**Attempted proof**: The definition of the set of rational numbers is the collection of fractions $p/q$ where $p$ is an integer and $q$ is a nonzero integer. Looking for a **witness** $p$ and $q$, we can write the square root of 2 as the fraction $\sqrt{2}/1$, where 1 is a nonzero integer. Since the numerator is not in the domain, this witness is not allowed, and we have shown that the square root of 2 is not a fraction of integers (with nonzero denominator). Thus, the square root of 2 is not rational.

*The problem in the above attempted proof is that* ____________________________________

**Proof**:

**Lemma 1:** For every two integers $p$ and $q$, not both zero, $gcd\left(\frac{p}{gcd(p,q)}, \frac{q}{gcd(p,q)}\right) = 1$.

**Lemma 2:** For every two integers $a$ and $b$, not both zero, with $gcd(a, b) = 1$, it is not the case that both $a$ is even and $b$ is even.

**Lemma 3:** For every integer $x$, $x$ is even if and only if $x^2$ is even.

**Greatest common divisor** (Rosen 4.3 p265) Let $a$ and $b$ be integers, not both zero. The largest integer $d$ such that $d$ is a factor of $a$ and $d$ is a factor of $b$ is called the greatest common divisor of $a$ and $b$ and is denoted by $gcd(a, b)$.

**Definition** (Rosen p257): An integer $p$ greater than 1 is called **prime** if the only positive factors of $p$ are 1 and $p$. A positive integer that is greater than 1 and is not prime is called composite.

**Theorem** (Rosen p336): Every positive integer *greater than 1* is a product of (one or more) primes.

**Proof by strong induction**, with $b = 2$ and $j = 0$.

**Basis step**: WTS property is true about 2.

**Inductive step**: Consider an arbitrary integer $n \geq 2$. Assume (as the IH) that the property is true about each of $2, \ldots, n$. WTS that the property is true about $n + 1$.

**Case 1**:

**Case 2**:

**New! Proof by Strong Induction** (Rosen 5.2 p337, zybook 7.1)
To prove that a universal quantification over the set of all integers greater than or equal to some base integer $b$ holds, pick a fixed nonnegative integer $j$ and then:

| | |
|---|---|
| Basis Step: | Show the statement holds for $b$, $b + 1$, $\ldots$, $b + j$. |
| Recursive Step: | Consider an arbitrary integer $n$ greater than or equal to $b + j$, assume (as the **strong induction hypothesis**) that the property holds for **each of** $b$, $b + 1$, $\ldots$, $n$, and use this and other facts to prove that the property holds for $n + 1$. |

For which non-negative integers $n$ can we make change for $n$ with coins of value 5 cents and 3 cents?

Restating: We can make change for __________, we cannot make change for _______________, and

______________________________________ $\star$

**Proof of $\star$ by mathematical induction** ($b = 8$)

**Basis step**: WTS property is true about 8

**Inductive step**: Consider an arbitrary $n \geq 8$. Assume (as the IH) that there are nonnegative integers $x, y$ such that $n = 5x + 3y$. WTS that there are nonnegative integers $x', y'$ such that $n + 1 = 5x' + 3y'$. We consider two cases, depending on whether any 5 cent coins are used for $n$.

*Case 1*: Assume .
Define $x' =$
and $y' =$
(both in $\mathbb{N}$ by case assumption).
Calculating:

$$5x' + 3y' \overset{\text{by def}}{=}$$
$$\overset{\text{rearranging}}{=}$$
$$\overset{\text{IH}}{=}$$

*Case 2*: Assume .
Therefore $n = 3y$ and $n \geq 8$, by case assumption. Therefore, $y \geq 3$ Define $x' = 2$ and $y' = y - 3$ (both in $\mathbb{N}$ by case assumption). Calculating:

$$\begin{aligned} 5x' + 3y' &\overset{\text{by def}}{=} 5(2) + 3(y - 3) = 10 + 3y - 9 \\ &\overset{\text{rearranging}}{=} 3y + 10 - 9 \\ &\overset{\text{IH and case}}{=} n + 10 - 9 = n + 1 \end{aligned}$$

**Proof of $\star$ by strong induction** ($b = 8$ and $j = 2$)

**Basis step**: WTS property is true about $8, 9, 10$

**Inductive step**: Consider an arbitrary $n \geq 10$. Assume (as the IH) that the property is true about each of $8, 9, 10, \ldots, n$. WTS that there are nonnegative integers $x', y'$ such that $n + 1 = 5x' + 3y'$.

### Algorithms for making change

Change making (greedy) algorithm in pseudocode

```
procedure change(c_1, c_2, ..., c_r: values of denominations of coins, where c_1 > c_2 > ... > c_r; n: a positive integer)

for i := 1 to r
  d_i := 0 {d_i counts the number of coin of denomination c_i used}
  while n ≥ c_i
    d_i := d_i + 1 {Add a coin of denomination c_i}
    n := n − c_i

return d_1, d_2, ..., d_r {d_i the number of coins of denomination c_i in the change for i=1, 2, ..., r}
```

The greedy approach doesn't work with 5¢ and 3¢ coins even for large values of n. However, we can write two new algorithms inspired by the proofs that we completed using mathematical induction and strong induction.

### Recursive algorithms for making change

One recursive algo for making change using 5¢ and 3¢ coins

```
procedure change1(n: a positive integer)
if n = 8
  (d_1, d_2) := (1, 1)
(x, y) := change1(n-1)
if x ≥ 1
  (d_1, d_2) := (x − 1, y + 2)
else
  (d_1, d_2) := (2, y − 3)

return (d_1, d_2) {d_1, d_2 are the number of 5¢ and 3¢ coins respectively }
```

Another recursive algo for making change using 5¢ and 3¢ coins

```
procedure change2(n: a positive integer)
if n = 8
  (d_1, d_2) := (1, 1)
if n = 9
  (d_1, d_2) := (0, 3)
if n = 10
  (d_1, d_2) := (2, 0)

(x, y) := change1(n-3)
(d_1, d_2) := (x, y + 1)

return (d_1, d_2) {d_1, d_2 are the number of 5¢ and 3¢ coins respectively }
```