# Final Review

# Problem 1 - Predicates and Quantifiers

---

Diff(x): x has 2 different shoes  on

Smart(x): x is smart

Friends(x,y): x is friends with than y

1. Everyone with 2 different shoes on is smart
2. Only smart people have 2 different shoes on
3. At least one person with 2 different shoes on is dumb
4. Everyone that is smart is friends with someone with 2 different shoes on
5. No one with different shoes on is friends with any smart person

# Problem 1 - Solution

1. $\forall x$: Diff(x) -> Smart(x) -if diff shoes then smart
2. $\forall x$: Diff(x) -> Smart(x) -to be smart, must have different shoes on
3. $\exists x$: Diff(x) $\land$ $\neg$Smart(x) -there is someone that is not smart and has 2 diff shoes
4. $\forall x \exists y$: Smart(x) -> (Friends(x,y) $\land$ Diff(y)) -for every smart person there exists someone with diff shoes and they are friends
5. $\forall x \forall y$: Diff(x)-> (Smart(y) $\land$ $\neg$Friends(x,y)) -for every person with different shoes on they are not friends with all smart people

Remember De Morgan's Law - push negation through so there are different ways to write these: $\neg\forall x \exists y P(x,y) = \exists x \forall y \neg P(x,y)$

# Problem 2 - Induction

---

Prove that $5^{2n+1} + 2^{2n+1}$ is divisible by 7, for all $n \geq 0$

# Problem 2 - Solution

Base Case: $n=0 \rightarrow 5^{2(0)+1} + 2^{2(0)+1} = 5^1+2^1 = 7 \rightarrow 7$ divides 7 HOLDS

Inductive Hypothesis: $\exists K \geq 0$: $5^{2k+1} + 2^{2k+1}$ is divisible by 7.

Inductive Step: show $5^{2(k+1)+1} + 2^{2(k+1)+1}$ is divisible by 7

1. $5^{2k+2+1} + 2^{2k+2+1} = 5^{2k+3} + 2^{2k+3} = 5^2*5^{2k+1} + 2^2*2^{2k+1}$
2. $25*5^{2k+1} + 4*2^{2k+1}$
3. $25*5^{2k+1} + 25*2^{2k+1} - 21*2^{2k+1}$
4. $25(5^{2k+1} + 2^{2k+1})- 21*2^{2k+1}$
   By the IH we know that the value in the parenthesis is divisible by 7. Also -21 is divisible by 7 (-3*7). Thus the combination of the 2 terms is also divisible by 7. We have finished the proof.

# Problem 3 - Graph Proof

---

Prove that every Full binary tree with N leaves has exactly 2N-1 vertices. (use induction)

# Problem 3 - Solution

Base Case: h=0 just the root so 1 leaf. N=1 2*1-1 = 1 HOLDS

Inductive Hypothesis: ∃K ≥ 0: Every full binary tree with k leaves has exactly 2K-1 vertices

Inductive Step:
Full binary tree with K+1 leaves.
We know there must be a pair of two leaves that are siblings (hw problem). If we remove that pair, its parents become a leaf and we are left with a tree of (k+1(-2+1)) = k leaves.
By the IH, this new tree must have 2k-1 vertices. When we add back in the two vertices that we removed, our tree then must have 2k-1+2 = 2k+1 vertices

# Problem 4 - Modular Inverse

a) Find the inverse of 13mod57

b) Find the inverse of 13mod63

# Problem 4 - Solution

Inverse of 13mod57

```
57 = 13(4)+5
13 = 5(2)+3
5 = 3(1)+2
3 = 2(1)+1
stop here gcd(13,57) = 1
```

```
1 = 3-2(1)                     take last equation
1 = 3-(5-3(1))1                substitute 2 for 5-3(1)
1 = 3 - 5(1) + 3(1)            distribute
1 = 3(2) - 5(1)                simplify
1 = (13-5(2))(2) - 5(1)        sub 3 for 13-5(3)
1 = 13(2) - 5(4) - 5(1)        distribute
1 = 13(2) - 5(5)               simplify
1 = 13(2) - (57-13(4))(5)      sub 5 for 57-13(4)
1 = 13(2) - 57(5) - 13(20)     distribute
1 = 13(22) - 57(5)             simplify
```

The inverse is 22 since it is the coefficient of 13 in the linear combination

$$13^{-1} \equiv 22 \bmod 57$$

# Problem 4 - Solution

Inverse of 13mod63

63 = 13(4)+11
13 = 11(1)+2
11 = 2(5)+1
stop here gcd(13,63) = 1

| | |
|---|---|
| 1 = 11 - 2(5) | |
| 1 = 11 - (13-11(1))(5) | sub 2 with 13-11(1) |
| 1 = 11 - 13(5) - 11(5) | distribute the 5 |
| 1 = 11(6) - 13(5) | simplify |
| 1 = (63 - 13(4))(6) - 13(5) | sub 11 with 63-13(4) |
| 1 = 63(6) - 13(24) - 13(5) | distribute the 6 |
| 1 = 63(6) - 13(29) | simplify |

The inverse is -29 since it is the coefficient of 13. But we want our value to be between 0 and 62 so we will add 63 to -29 = 34. So 34mod63 is the inverse.

$$13^{-1} \equiv -29 \bmod 63 \equiv 34 \bmod 63$$

# Problem 5 - CRT

“Engineering. Business. CAL. CS. Long ago, the four majors lived together in harmony … then everything changed when the Business Majors attacked. Only Sandeep, master of all four departments, could stop them, but when Stevens needed him most, he vanished. No one had heard of him for over 100 semesters, until the CS 135 TAs uncovered a prophecy that he will return, but it was encrypted using modular arithmetic. Help the CS 135 TAs uncover the secret of Sandeep’s return to save Stevens and inductively, the world.”

# Problem 5 - CRT

The prophecy states that Sandeep will return in the year these three events occur:

Favardin's dog, Martini, howls at the Moon

Attila takes a ride on Favardin's yacht

Tuition rises

Here's what we know:

1) Martini howls at the moon every 8 years, and the last known year he howled was 2021
2) Attila takes a ride on Favardin's yacht every 11 years, and the last known year they took a ride is 2016
3) Tuition rises every 15 years (lol yeah right), and the last known year it rose was 2021

# Problem 5 - Solution

Step 1:

Simplify

$x \equiv 2021 \bmod 8 \equiv 5 \bmod 8$

$x \equiv 2016 \bmod 11 \equiv 3 \bmod 11$

$x \equiv 2021 \bmod 15 \equiv 11 \bmod 15$

Step 2:

Find #'s

$m = 8 \cdot 11 \cdot 15 = 1320$

$m_1 = 11 \cdot 15 = 165$

$m_2 = 8 \cdot 15 = 120$

$m_3 = 8 \cdot 11 = 88$

# Problem 5 - Solution

**Step 3:**

Pulverizer

1) Find $165 \cdot y \equiv 1 \bmod 8$

$$
\begin{aligned}
&\gcd(165, 8) \rightarrow 165 - 20 \cdot 8 = 5 \\
&= \gcd(8, 5) \rightarrow 8 - 5 = 3 \\
&= \gcd(5, 3) \rightarrow 5 - 3 = 2 \\
&= \gcd(3, 2) \rightarrow 3 - 2 = 1 \\
&= \gcd(2, 1)
\end{aligned}
$$

$\cancel{1}, \cancel{2}, \cancel{3}, \cancel{5}, 8, 165$

$$
\begin{aligned}
&3 - 2 = 1 \\
&3 - (5 - 3) = 1 \\
&2 \cdot 3 - 5 = 1 \\
&2 \cdot (8 - 5) - 5 = 1 \\
&2 \cdot 8 - 3 \cdot 5 = 1 \\
&2 \cdot 8 - 3(165 - 20 \cdot 8) = 1 \\
&62 \cdot \underline{8} - 3 \cdot \underline{165} = 1
\end{aligned}
$$

Thus $y = -3 \equiv 5$

Check $-3 \cdot 165 \bmod 8 \equiv -3 \cdot 165 + 8 \cdot 165 \bmod 8$

$\equiv 5 \cdot 165 \bmod 8 \equiv 5 \cdot 5 \bmod 8 \equiv 1 \bmod 8$

# Problem 5 - Solution

-

2) Find $120 \cdot y_2 \equiv 1 \bmod 11$

$\gcd(120, 11) \rightarrow 120 - 10 \cdot 11 = 10$

$= \gcd(11, 10) \rightarrow 11 - 10 = 1$

$= \gcd(10, 1)$

$r_i$ 10, 11, 120

$11 - 10 = 1$

$11 - (120 - 10 \cdot 11) = 1$

$11 \cdot 11 - 120 = 1$

$y_2 = -1 \equiv 10$

Check $-1 \cdot 120 \bmod 11 \equiv -1 \cdot 120 + 11 \cdot 120 \bmod 11$

$\equiv 120 \cdot 10 \bmod 11 \equiv 1 \bmod 11$

# Problem 5 - Solution

3) Find $88 y_3 \equiv 1 \bmod 15$

$\gcd(88, 15) \rightarrow 88 - 5 \cdot 15 = 13$

$= \gcd(15, 13) \rightarrow 15 - 13 = 2$

$= \gcd(13, 2) \rightarrow 13 - 2 \cdot 6 = 1$

$= \gcd(2, 1)$

$1, \cancel{2}, \cancel{13}, 15, 88$

$13 - 2 \cdot 5 = 1$

$13 - (15 - 13) \cdot 6 = 1$

$7 \cdot 13 - 6 \cdot 15 = 1$

$7 \cdot (88 - 5 \cdot 15) - 6 \cdot 15) = 1$

$y_3 = 7$

$7 \cdot 88 - 35 \cdot 15 = 1$

<u>Check</u>: $7 \cdot 88 \bmod 15 \equiv 528 \bmod 15$

$\equiv 1 \bmod 15$

# Problem 5 - Solution

Step 4

Solution

$$x \equiv (a_1 y_1 m_1 + a_2 y_2 m_2 + a_3 y_3 m_3) \bmod m$$

$$\equiv (5 \cdot 5 \cdot 165 + 3 \cdot 10 \cdot 120 + 11 \cdot 7 \cdot 88) \bmod 1320$$

$$\equiv (14051) \bmod 1320$$

$$\equiv \boxed{1301}$$

# Problem 5 - Solution

We've shown that every 1301 years, all three of these events occur at the same time!

Since we're living in 2022, the next time they will occur is the year (1301) + 1320 = **2621!**

*2023 😳

# What to study

- Zybooks!
- Lab slides (midterm review slides)
- Problem Set questions
- Logic
  - Predicates, tree method, quantifiers
- Induction
  - Format for the proof (apply IH in IS!)
- Relations, Functions
  - know definitions (injective/bijective, closures, equivalence relations, etc)
- Number Theory
  - Pulverizer, mod inverse, CRT
- Graphs
  - PROOFS!!!, know definitions (cycles, walks, etc)