Survey Located At:
http://www.surveymonkey.com/s.asp?u=665323704735
Due **Wednesday** April 25th.
Homework #3

- Due date now on Wednesday at 4:00pm
- 31 questions total
- Covers six sections total
  - 2.3: Functions
  - 2.4: Sequences and Summations
  - 3.4: Integers and Division
  - 3.5: Primes and Greatest Common Divisors
  - 3.6: Integers and Algorithms
  - 3.7: Applications of Number Theory
Show versus Prove

Show:
- Informal
- Explanation
- Diagrams

Prove:
- Formal
- Based on “facts”
- Uses rules of inference
- Many methods:
  - By Construction
  - By Contraposition
  - By Contradiction
  - By Counterexample
Section 2.3 hints and examples.
Function Notation

- $f: A \rightarrow B$
  - Function $f$ has:
    - domain $A$
    - codomain $B$
  - For $f(a) = b$:
    - input $a \in A$
    - output $b \in B$
  - One input variable

- $f: A \times B \rightarrow C$
  - Function $f$ has:
    - domain $A \times B$
    - codomain $C$
  - For $f(a, b) = c$:
    - input $a \in A$
    - input $b \in B$
    - output $c \in C$
  - Two input variables
Function Notation

\[ f( m, n ) = m + n \]

- Let \( m \in \mathbb{N} \) and \( n \in \mathbb{N} \):
  - \( f( 1, 2 ) = 1 + 2 = 3 \)
  - \( f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \)
- Let \( m \in \mathbb{Z} \) and \( n \in \mathbb{N} \):
  - \( f( -4, 1 ) = -4 + 1 = -3 \)
  - \( f: \mathbb{Z} \times \mathbb{N} \rightarrow \mathbb{Z} \)
- Let \( m \in \mathbb{Z} \) and \( n \in \mathbb{R} \):
  - \( f( 2, 0.15 ) = 2 + 0.15 = 2.15 \)
  - \( f: \mathbb{Z} \times \mathbb{R} \rightarrow \mathbb{R} \)
A function $f: A \rightarrow B$ is onto iff:

- For every $b \in B$ there is an $a \in A$ with $f(a) = b$
- $\forall b \ \exists a \ (f(a) = b)$
- The codomain is equal to the range
Determine if the function $f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ is onto:

- $f(m, n) = m + n$
  - Onto!
  - For every $p \in \mathbb{Z}$ can we find a pair $(m, n)$ such that $m + n = p$?
    - Let $m = 1$, $n = p - 1$.

- $f(m, n) = m^2 + n^2$
  - Not onto
  - There is no pair $(m, n)$ such that $m^2 + n^2 = -1$. 
Homework #3

Section 2.4 hints and examples.
Summation

- **Notation:** \( \sum_{j=m}^{n} a_j = a_m + a_{m+1} + \cdots + a_n \)

- **Examples:**

\[
\sum_{k=1}^{5} (k + 1) = (1+1) + (2+1) + (3+1) + (4+1) + (5+1)
\]

\[
= (2) + (3) + (4) + (5) + (6)
\]

\[
= 20
\]

\[
S = \{2,4,6,8\}
\]

\[
\sum_{j \in S} j = 2 + 4 + 6 + 8 = 20
\]

(work out on board)
Double Summation

Example:

\[
\sum_{i=1}^{2} \sum_{j=1}^{3} i + j = \sum_{i=1}^{2} \left( \sum_{j=1}^{3} i + j \right)
\]

\[
= \sum_{i=1}^{2} \left( (i + 1) + (i + 2) + (i + 3) \right)
\]

\[
= \sum_{i=1}^{2} (3i + 6)
\]

\[
= (3 \cdot 1 + 6) + (3 \cdot 2 + 6)
\]

\[
= 3 + 6 + 6 + 6
\]

\[
= 21
\]

(work out on board)
Products

- **Notation:** \[ \prod_{j=m}^{n} a_j = a_m \times a_{m+1} \times \cdots \times a_n \]

- **Examples:**
  \[ \prod_{i=0}^{10} i = 0 \times 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \]
  \[= 0 \]

  \[ \prod_{i=1}^{100} (-1)^i = (-1)^1 \times (-1)^2 \times \cdots \times (-1)^{99} \times (-1)^{100} \]
  \[= -1 \times 1 \times \cdots \times -1 \times 1 \]
  \[= 1 \]

(work out on board)
Section 3.4 hints and examples.
Number Theory Motivation

- What does it deal with?
  - Studies properties and relationships of specific classes of numbers
  - Most commonly studied classes of numbers:
    - Positive Integers
    - Primes

- What is this stuff good for?
  - Number theory used in cryptography
    - Basis for RSA public-key system
  - Integers often used in programming
    - Array indices
Proofs with Integer Division

- If $a, b \in \mathbb{Z}$ with $a \neq 0$:
  - $a \mid b$ if there exists a $k$ such that $a \cdot k = b$.

- #7. Show that if $a, b,$ and $c$ are integers with $c \neq 0$, such that $ac \mid bc$, then $a \mid b$.
  - If $ac \mid bc$, then there is an integer $k$ such that:
    $$ack = bc$$
    $$\frac{1}{c} (ack = bc)$$
    $$ak = b$$
  - Therefore, we can state that $a \mid b$. 
#21. Show that if:

- \( n \mid m \), where \( n, m \) are positive integers \( > 1 \), and
- \( a \equiv b \pmod{m} \), where \( a \) and \( b \) are integers

Then:

- \( a \equiv b \pmod{n} \)

Since \( n \mid m \), we know there exists an integer \( i \) such that \( n \ i = m \) (by definition 1).
Proofs with Integer Division

#21. Show that if:
- \( n \mid m \), where \( n, m \) are positive integers \( > 1 \), and
- \( a \equiv b \pmod{m} \), where \( a \) and \( b \) are integers

Then:
- \( a \equiv b \pmod{n} \)

Since \( a \equiv b \pmod{m} \), we know that there exists an integer \( a = b + jm \) (by theorem 1).
Proofs with Integer Division

#21. Show that if:

- $n \mid m$, where $n, m$ are positive integers $> 1$, and
- $a \equiv b \pmod{m}$, where $a$ and $b$ are integers

Then:

- $n \ i = m$
- $a = b + jm$

\[ a = b + jm = b + jni = b + (ji)n = b + kn = b \pmod{n} \]
Section 3.5 hints and examples.
Euler $\phi$-function

$\phi(n) = \# \text{ of positive integers } \leq n \text{ that are relatively prime to } n$

- $\phi(4)
  - \text{gcd}(4, 4) = 4$
  - $\text{gcd}(3, 4) = 1$
  - $\text{gcd}(2, 4) = 2$
  - $\text{gcd}(1, 4) = 1$
  - $\phi(4) = 2$

- $\phi(10)
  - \text{gcd}(1, 10) = 1$
  - \text{gcd}(3, 10) = 1$
  - \text{gcd}(7, 10) = 1$
  - \text{gcd}(9, 10) = 1$
  - $\phi(10) = 4$
Section 3.6 hints and examples.
Number Conversion Motivation

- **Binary:**
  - Low-level language of computers
  - Easy to represent in electrical systems ("on" versus "off")
  - Can implement Boolean logic

- **Octal:**
  - File permissions in Unix often use an octal representation

- **Decimal:**
  - Number representation used in most modern languages

- **Hexadecimal:**
  - Used by HTML/CSS to represent colors
  - Character codes often represented in hexadecimal
Decimal Expansion

\[
(0101\ 1111)_2 =
\]

\[
0 \times 2^7 + 1 \times 2^6 + 0 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0
\]

digit
Decimal Expansion

\( (0101\ 1111)_2 = \)

\[
0 \times 2^7 + 1 \times 2^6 + 0 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0
\]

"base"
binary = base 2
Decimal Expansion

\[
(0101\ 1111)_{2} =
\]

\[
\begin{array}{cccccccc}
0 & 1 & 0 & 1 & 1 & 1 & 1 & 1\\
7 & 6 & 5 & 4 & 3 & 2 & 1 & 0\\
0 \times 2^{7} + 1 \times 2^{6} + 0 \times 2^{5} + 1 \times 2^{4} + 1 \times 2^{3} + 1 \times 2^{2} + 1 \times 2^{1} + 1 \times 2^{0}\\
\end{array}
\]
Decimal Expansion

\[ (0101\ 1111)_{2} = \]

\[
0 \times 2^{7} + 1 \times 2^{6} + 0 \times 2^{5} + 1 \times 2^{4} + 1 \times 2^{3} + 1 \times 2^{2} + 1 \times 2^{1} + 1 \times 2^{0}
\]

\[
2^{6} + 2^{4} + 2^{3} + 2^{2} + 2^{1} + 2^{0} = 64 + 16 + 8 + 4 + 2 + 1 = 95
\]
Hexadecimal Expansion

\[ 177130 = ( \ ? )_{16} \]

\[ 177130 \div 16 = 11070.625 \]

\[ 177130 = 16 \times 11070 + 10 \]

\[ 11070 = 16 \times 691 + 14 \]
Hexadecimal Expansion

177130 = ( ? )_{16}

177130 = 16 \times 11070 + 10
11070 = 16 \times 691 + 14
691 = 16 \times 43 + 3
43 = 16 \times 2 + 11
2 = 16 \times 0 + 2

2 B 3 E A
Hexadecimal Expansion

\[ 177130 = (\ ? \ )_{16} \]

\[
\begin{align*}
177130 &= 16 \times 11070 + 10 \\
11070 &= 16 \times 691 + 14 \\
691 &= 16 \times 43 + 3 \\
43 &= 16 \times 2 + 11 \\
2 &= 16 \times 0 + 2
\end{align*}
\]

\[(2B3EA)_{16}\]
Section 3.7 hints and examples.
Examples

- See PDF example for:
  - Euclidean Algorithm
  - Greatest Common Divisor
  - Modular Inverses
Fermat’s Little Theorem

Show that $2^{340} \equiv 1 \pmod{11}$:

- By Fermat’s Little Theorem: $a^{10} \equiv 1 \pmod{11}$
- We can rewrite $2^{340} = (2^{10})^{34}$
- Therefore we get:

$$2^{340} = (2^{10})^{34}$$

$$\equiv (1)^{34} \pmod{11}$$

$$\equiv 1 \pmod{11}$$