15-151 Math Foundations CS – EXCEL

Topic: **Number Theory, Modular Arithmetic, Functions**
Session Date: **Thu Oct 11**

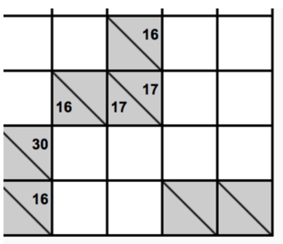
EXCEL Leader: Sam Yong
Email: myong@andrew.cmu.edu
Academic Development
Cyert Hall B5 | 412-268-6878

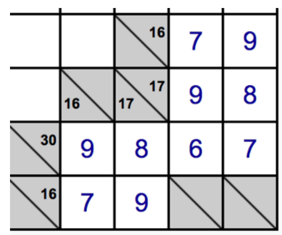
Services available: Supplemental Instruction (SI), Academic Counseling in Study Skills, Individual & Walk-in Tutoring

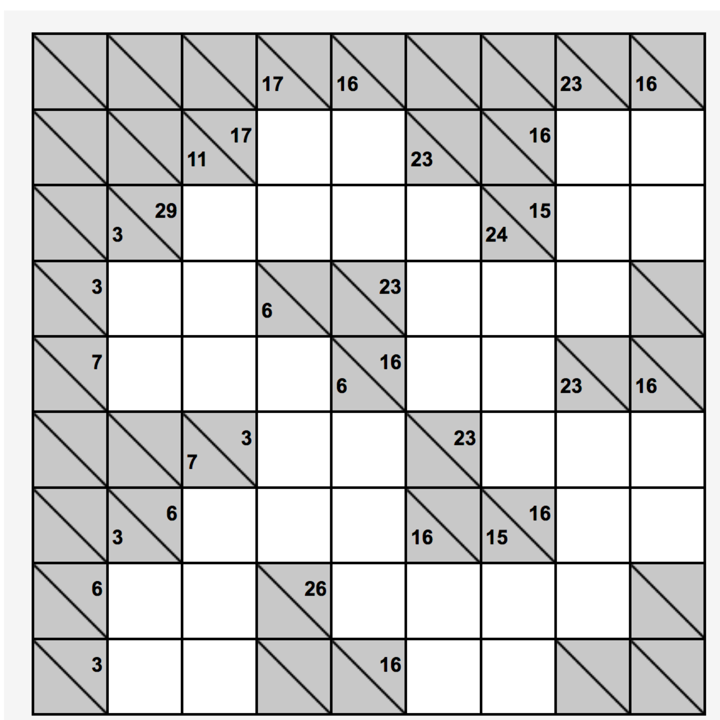
"If you can't solve a problem, then there is an easier problem you can solve: find it."

– **George Pólya**

Puzzle 001. **Kakuro** is like a crossword puzzle with numbers. Each "word" must add up to the number provided in the clue above it or to the left. Words can only use the numbers 1 through 9, and a given number can only be used once in a word. Every kakuro puzzle has one and only solution, and can be solved through logic alone.







1. **Fun**ctions **Fun**damentals
    - Let X and Y be sets. A **function** f from X to Y is a mathematical object which assigns to each element of X exactly one element of Y. Given $x \in X$, the element of Y associated with x by f is denoted __________, and is called the value of f at x. We write ____________________ to denote that f is a function from X to Y. We say X is the __________ of f and Y is the __________ of f.
    - **Totality**: A value $f(x)$ should be ______________________________.
    - **Existence**: For each __________, the specified value ____.
    - **Uniqueness**: For each __________, the specified value ______________________________. That is, if $x = x' \in X$ then we should have ____________________.
    - Given functions $f: X \to Y$ and $g: Y \to Z$, their **composition** $g \circ f$ is the function ____. Intuitively, $g \circ f$ is the function resulting from first applying __________, then applying __________.
    - A function $f: X \to Y$ is **injective** (or **one-to-one**) if ______________________________ for all $x, x' \in X$. An injective function is said to be an injection. By contrapositive, $f: X \to Y$ being injective is equivalent to saying that if $x, x' \in X$ and $x \neq x'$, then ____________________.
    - A function $f: X \to Y$ is **surjective** (or **onto**) if $\forall$__________, $\exists$__________, __________. A surjective function is said to be a surjection.
    - A function is **bijective** if it is __________ and __________. A bijective function is said to be a bijection.

Puzzle 002. Do you remember the four numbers game last week? Again, use only $+ - \times \div$ to make 24.

7	9	9	13
4	5	7	12
3	4	6	6

2. What is a **modular arithmetic** application we look at many times every day?
    - Fix $n \in \mathbb{Z}$. Given integers $a, b \in \mathbb{Z}$, we say a is **congruent** to b **modulo** n, and write ____________________ if ____________________. If a is not congruent to b modulo n, write ____________________. The number n is called ____________________.
    - True or False?
        a) $11 \equiv 5 \; mod \; 2$ __________
        b) $11 \equiv 5 \; mod \; 3$ __________
        c) $11 \equiv 5 \; mod \; 4$ __________
        d) $12 \equiv 18 \; mod \; 6$ __________
        e) $-1 \equiv 23 \; mod \; 4$ __________
        f) $-1 \equiv 13 \; mod \; 4$ __________
    - Prove **Theorem** 3.3.6: Let $a, b, c \in \mathbb{Z}$ and let n be a modulus. Then
        a) $a \equiv a \; mod \; n$
        b) If $a \equiv b \; mod \; n$, then $b \equiv a \; mod \; n$
        c) If $a \equiv b \; mod \; n$ and $b \equiv c \; mod \; n$, then $a \equiv c \; mod \; n$

3. Prove **Proposition** 3.3.7: Fix a modulus n and let $a, b \in \mathbb{Z}$. The following are equivalent,
    a) a and b leave the same remainder when divided by n
    b) $a = b + kn$ for some $k \in \mathbb{Z}$
    c) $a \equiv b \; mod \; n$

[Step 1: How do we prove three statements equivalent?]

Puzzle 003. Prove the following **visually**. (Hint: squares, area of a rectangle)

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

---

4. Prove **Theorem** 3.3.9: Fix a modulus *n*, and let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ such that

$$a_1 \equiv b_1 \; mod \; n \wedge a_2 \equiv b_2 \; mod \; n$$

Then,

a) $a_1 + a_2 \equiv b_1 + b_2 \; mod \; n$
b) $a_1 a_2 \equiv b_1 b_2 \; mod \; n$
c) $a_1 - a_2 \equiv b_1 - b_2 \; mod \; n$

5. Find all integers *x* such that $2x + 9 \equiv 3x + 7 \; mod \; 5$.

[Show your steps formally. Reference theorems and propositions above when necessary.]

6. Fix a modulus n. Prove or disprove: $\forall a, b, q \in \mathbb{Z}$ with $q \not\equiv 0 \; mod \; n$,

$$qa \equiv qb \; mod \; n \;\; \Rightarrow a \equiv b \; mod \; n$$

---

7. **Definition** 3.3.15. Fix a modulus *n*. Given $a \in \mathbb{Z}$, a **multiplicative inverse** for *a* modulo *n* is an integer *u* such that ____________________.

8. Prove **Proposition** 3.3.19: Let $a \in \mathbb{Z}$ and let *n* be a modulus. Then *a* has a multiplicative inverse modulo *n* if and only if ____________________.

9. Find all integers x such that $25x - 4 \equiv 4x + 3 \; mod \; 13$.

---

10. Big Little Theorems

- **Fermat's little theorem**: Let $a, p \in \mathbb{Z}$ with p a positive prime. Then ____________________ mod p. Corollary: If $p \nmid a$, then ____________________.
- Review **totient** and **Euler's Theorem** on your own.
- **Wilson's theorem**: Let $n > 1$ be a modulus. Then n is prime if and only if ____________________.
- **Chinese remainder theorem**: Let m, n be moduli and let $a, b \in \mathbb{Z}$. If m and n are coprime, then there exists an integer solution x to the simultaneous congruence

  $$x \equiv a \; mod \; m \wedge x \equiv b \; mod \; n$$

  Moreover, if $x, y \in \mathbb{Z}$ are two such solutions, then $x \equiv y \; mod \; mn$.
- Review the generalized version of Chinese remainder theorem on your own.

11. Find the remainder of 3^{10601} when divided by 13.

12. Find the remainder of $3^{45} \cdot 44!$ when divided by 47.

13. Prove that gaps between consecutive primes can be made arbitrarily large. That is, prove that for all natural numbers *n*, there exists an integer *a* such that the follow numbers are all composite.

$$a, a+1, a+2, \dots, a+n$$

14. **R**eal **S**ecret **A**pplication of number theory (seriously, Rivest-Shamir-Aldeman)

- Step 1: Let p and q be distinct ____________________, and let $n = pq$. Then $\varphi(n) =$ ____________________.
- Step 2: Choose integer e with ____________________ and $e \perp$ __________. The pair (n, e) is called the ____________________.
- Step 3: Choose integer d with ____________________. The pair (n, d) is called the ____________________.
- Step 4: To encrypt a message M (which is encoded as an integer), compute $K \in [n]$ such that ____________________. Then __________ is the encrypted message.
- Step 5: The original message M can be recovered since ____________________.

Puzzle 004. How would two entities on an open unsafe network channel establish a pair of public-secret keys in the first place?

---

15. For each of the following functions: is it injective? Surjective? Bijective? Prove your claims.

- $f\colon \mathbb{R} \to \mathbb{R}$ via $f(x) = 2x + 1$
- $g\colon \mathbb{R} \to \mathbb{R}$ via $g(x) = x^2$
- $g'\colon \mathbb{R} \to \mathbb{R}^+$ via $g'(x) = x^2$
- $h\colon \mathbb{R} \to \mathbb{R}^+$ via $h(x) = e^x$