

# MC215: MATHEMATICAL REASONING AND DISCRETE STRUCTURES

---

## □ Wednesday, 11/19/08

### ■ From last time:

- Recursive functions and algorithms

### ■ Today:

- Return, go over Exam #2
- More on recursion
- Euclidean Algorithm

- **READING:**  
5.3 "lite"

- **EXERCISES:**  
pp. 258-259:  
1-4, 16, 17

# Designing a recursive procedure for the Tower of Hanoi Puzzle

---

- **Input needed for procedure:**
  - $n$  = the number of disks,
  - *start* = the name of the source tower,
  - *finish* = the name of the destination tower, and
  - *extra* = the name of the *extra* tower.
- **Output of the procedure:** A printed list of instructions saying how to move the disks.
- **Example:** If  $n = 2$ , *start* = 'A', *finish* = 'C', and *extra* = 'B', then the output might be:
  - Move a disk from A to B.
  - Move a disk from A to C.
  - Move a disk from B to C.

# Algorithm for Tower of Hanoi

---

- **Input:** *n, start, finish, extra*
- **Output:** Instructions to move n disks from start to finish, using extra
- **Hanoi (n, start, finish, extra) {**
  - If ( $n > 0$ ) {
    - Hanoi (n-1, start, extra, finish)
    - Print ["Move a disk from ", start, " to ", finish]
    - Hanoi (n-1, extra, finish, start)
  - }
- }

# Some comments on the solution

- How many disks must we move to solve the game of size  $n$ ?
  - By our observations, *twice* the number for  $n-1$ , plus 1 for moving the bottom disk. So...

Number of disks	Number of disk moves		
0		0 =	$2^0 - 1$
1	$2*0 + 1 =$	1 =	$2^1 - 1$
2	$2*1 + 1 =$	3 =	$2^2 - 1$
3	$2*3 + 1 =$	7 =	$2^3 - 1$
4	$2*7 + 1 =$	15 =	$2^4 - 1$
5	$2*15 + 1 =$	31 =	$2^5 - 1$
<b>20</b>		<b>1,048,575 =</b>	<b><math>2^{20} - 1</math></b>

# More comments

---

- In general, to solve the game with  $n$  disks requires  $2^n - 1$  moves!!
- Since this grows exponentially in  $n$ , the problem quickly becomes too big for any computer to handle!
- This is true even if we write the algorithm non-recursively!

# Euclidean Algorithm: Finding a GCD

---

- Famous algorithm for finding the **greatest common divisor of any two integers**.
- Appears in **Euclid's Elements, c. 300 BC**, but probably known up to a century earlier.
- **Definition:** If  $m$  and  $n$  are two integers, not both zero, then  **$\text{GCD}(m, n)$**  = greatest positive integer that is a divisor of both  $m$  and  $n$ .
  - Note: If  $m > 0$ , then  **$\text{GCD}(m, 0) = m$** .
  - Sometimes we also define  **$\text{GCD}(0, 0) = 0$**

# Examples

---

- $\text{GCD}(24, 18)$
- $\text{GCD}(18, 24)$
- $\text{GCD}(-24, 18)$
- $\text{GCD}(33, 0)$
- If  $a \mid b$  (means  $a$  is a divisor of  $b$ ), then what is  $\text{GCD}(a, b)$ ?
- If  $p$  is a prime number, and  $q < p$ , what is  $\text{GCD}(p, q)$ ?

# Theorem underlying Euclidean Algorithm

---

□ **Theorem.** If  $a$  and  $b$  are integers, with  $b > 0$  and  $r = a \bmod b$ , then

$$\begin{aligned}\text{GCD}(a, b) &= \text{GCD}(b, r) \\ &= \text{GCD}(b, a \bmod b).\end{aligned}$$

□ **Proof.** Show that  $d$  is a divisor of  **$a$  and  $b$**  IFF  $d$  is a divisor of  **$b$  and  $r$** . Thus  $a$  and  $b$  have same gcd as  $b$  and  $r$ .

■  $\exists q, r, 0 \leq r < b$ , such that  $a = b q + r$ .

■  $d \mid (b \text{ and } r) \rightarrow d \mid b q + r = a$

■  $d \mid (a \text{ and } b) \rightarrow d \mid a - b q = r$

# Recursive Euclidean Algorithm

---

1. **GCD(a, b) {**
2.     **If (b = 0) return a**
3.     **Else return GCD(b, a mod b)**
4. **}**

□ **Try it on:**

- 0, 0            5, 0            0,5
- 10, 5           5, 10           25, 15
- 15, 25