CS 113
DISCRETE STRUCTURES

Chapter 3: Algorithms

HOMEWORK

- **All homework is from the Exercises**
  - **No problems are from the Review Exercises**
- **Section 3.2 (p. 127): 19, 21**
- **Section 3.3 (p. 131): 1-5 (all), 13, 22-24 (all)**
- **Section 3.4 (p. 137): 8, 9, 12, 27, 28**
- **Section 3.5 (p. 149): 1-12 (all), 17, 19**
- **Section 3.7 (p. 160): 1-9 (all)**

MODULAR ARITHMETIC

- **We will look at numbers “% 5”**
  - **I will call this “mod 5 math”**
  - **The 5 here is not important**
    - **You could have chosen any number**
- **One way to understand mod 5 math is to do arithmetic ”on a clock”**
- **Our clock will have the numbers 0, 1, 2, 3, and 4**
  - **We stop at the number one less than 5, which is 4**
- **First we try to understand these numbers by counting**

MODULAR ARITHMETIC-COUNTING

- **Now we will live "on the clock"**
- **You are counting the Cheerios as they roll out of the box into a bowl**
  - **Cheerios are a type of breakfast cereal, and you decide to have Cheerios for breakfast**
- **Remember, you are living on the clock**
- **You look at your empty bowl and say, "0"**
- **One Cheerio rolls out of the box and you say, "1"**
- **You continue, "2", "3", "4"**

MODULAR ARITHMETIC-MORE COUNTING

- **One more Cheerio rolls out of the box**
- **What do you do?**
- **You say the next number on the clock**
- **This means that, instead of 5, you say "0"**
- **Your new way of counting is this**
  - **In the table below, the top row is our usual idea of numbers**
  - **The bottom row is our new idea of numbers**

Usual	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
New	0	1	2	3	4	0	1	2	3	4	0

MODULAR ARITHMETIC-JUST NUMBERS

- **Let's check this**
  - **I say "1." You say, "Of course. You mean 1."**
  - **I say "2." You say, "Come on. It's 2."**
    - **You are starting to get bored.**
  - **I say "8." You say, "Aha! Though you would catch me. It's 3."**
    - **You are moving around the clock**
    - **This is the same as doing mod 5 math**

MODULAR ARITHMETIC-MODULAR IDEAS

- **Moving around the clock is the same as taking the remainder "%5"**
  - **The number of times you move around the clock is the quotient**
  - **The number you end on is the remainder**
  - **For example, to find 17**
    - **You circle the clock 3 full times. (Start at 1)**
    - **You end on 2**

MODULAR ARITHMETIC-NOTATION

- **Remember, the only numbers we work with are 0, 1, 2, 3, 4**
  - **All numbers in our normal world must be seen as one of these**
- **We only write the numbers 0-4 on the right side of an equal sign**
  - **We don't even use an equal sign!**
    - **We use the congruence symbol from geometry**
    - **We even call it "congruent"!**
- **Some examples are on the next slide**

MODULAR ARITHMETIC-MORE NOTATION

- **Here are some examples**
  - **2 (mod 5) ≡ 2 (mod 5)**
  - **7 (mod 5) ≡ 2 (mod 5)**
  - **24 (mod 5) ≡ 4 (mod 5)**
- **And again, what these mean is this**
  - **Take the example of 24 (mod 5) ≡ 4 (mod 5)**
  - **It means that if you start at 1 and count to 24, you will end on 4**
  - **It also mean, of course, that 24 % 5 = 5**

MODULAR ARITHMETIC-NEGATIVE NUMBERS

- **How about -3?**
  - **You start at 0 and go backward 3 numbers.**
  - **You end at 2.**
- **So, we write -3 (mod 5) ≡ 2 (mod 5)**
- **A few slides back I mentioned "mod 5 math"**
- **Let's see if we can add, subtract, and multiply these numbers**
  - **We could divide, but that could be painful**

MODULAR ARITHMETIC- ADDITION

- **$2 + 1 = 3$ (Usual number ideas)**
- **Also, $(2 + 1) \pmod 5 \equiv 3 \pmod 5$**
- **Why is this?**
  - **Start at 2 on the clock**
  - **Move1 more number around**
  - **You arrive at 3**

MODULAR ARITHMETIC-MORE ADDITION

- How about (6+7) mod 5?
  - Start at 6
    - To find this, start at 1
    - Count to 6
    - You are back at 1 again
  - Then move 7 more numbers around the clock
  - You arrive at 3
- So then
  - $(6+7) \pmod 5 \equiv 3 \pmod 5$

MODULAR ARITHMETIC-SHORCUT MATH

- **You might notice that 6 (mod 5) is the same as 1 (mod 5)**
    - **To find this, start at 1**
    - **Count to 6**
    - **You are back at 1 again**
- **Similarly, 7 (mod 5) is the same as 2 (mod 5)**
- **So then**
    - **$(6+7) \pmod 5 \equiv (1+2) \pmod 5 = 3 \pmod 5$**

MODULAR ARITHMETIC-EXPONENTS

- **You can use these shortcuts along with the normal algebraic ideas**
- **Example 1: What is (23)(47) (mod 9)?**
  - **This is 23 (mod 9) * 47 (mod 9), which is 5 (mod 9) * 2 (mod 9)**
  - **And, 5 (mod 9) * 2 (mod 9) = 10 (mod 9) ≡ 1 (mod 9)**
  - **In summary, then, 23 (mod 9) * 47 (mod 9) ≡ 1 (mod 9)**

MODULAR ARITHMETIC-ONCE AGAIN

- **Using these shortcuts yet one more time**
- **Example 2: $4^8 \pmod 5$?**
- **$4^2 \pmod 5 \equiv 4*4 \pmod 5 \equiv 16 \pmod 5 \equiv 1 \pmod 5$**
- **So, $4^8 \pmod 5 \equiv (4^2)^4 \pmod 5 \equiv 1^4 \pmod 5$, which is**
  $1 \pmod 5$
- **In summary, $4^8 \pmod 5 \equiv 1 \pmod 5$**

MODULAR ARITHMETIC- A BRIEF WORD ABOUT DIVISION

- **Division can be painful, even impossible**
- **For example**
  - **1/3 (mod 5) ≡ 2 (mod 5)**
  - **This is because (multiplying both sides by 3)**
    - **1 (mod 5) ≡ (3*2) (mod 5)**
- **In the same way, ¾ (mod 5) ≡ 2 (mod 5)**
  - **This is because multiplying both sides by 4 gives**
    - **3 (mod 5) ≡ 8 (mod 5), which is true**
- **However, there is no such thing as 1/3 (mod 9) or 1/6 (mod 9)**
  - **You can verify this by trying 0, 1, 2, 3, 4, 5, 6, 7, 8**

MODULAR ARITHMETIC- A BRIEF WORD ABOUT DIVISION

- **Division can be painful, even impossible**
- **For example**
  - **1/3 (mod 5) ≡ 2 (mod 5)**
  - **This is because (multiplying both sides by 3)**
    - **1 (mod 5) ≡ (3*2) (mod 5)**
- **In the same way, ¾ (mod 5) ≡ 2 (mod 5)**
  - **This is because multiplying both sides by 4 gives**
    - **3 (mod 5) ≡ 8 (mod 5), which is true**

MODULAR ARITHMETIC- MORE ABOUT DIVISION

- **However, there is no such thing as 1/3 (mod 9) or 1/6 (mod 9)**
  - **You can verify this by trying 0, 1, 2, 3, 4, 5, 6, 7, 8**
- **Therefore, we are skipping division**

- **Also, people don't usually write fractions in modular arithmetic**
- **Everything is whole numbers**

MODULAR ARITHMETIC-SOLVING EQUATIONS

- **Suppose we try to solve 3x = 4 (mod 11)**
- **We can try 1, 2, 3, etc., for x and see which works**
  - **We call this "trial and error"**
- **Here is the start of the process**
- **x=1: 3x = 3, which is not = 7 (mod 11)**
- **x=2: 3x = 6, which is not = 7 (mod 11)**
- **x=3: 3x = 9, which is not = 7 (mod 11)**
- **x=4: 3x = 12 = 1 (mod 11), which is not = 7 (mod 11)**
- **x=5: 3x = 15 = 4 (mod 11), which is not = 7 (mod 11)**

MODULAR ARITHMETIC- SOLVING EQUATIONS

- Here is another way to solve an equation
- Suppose we try to solve 3x = 7 (mod 11)
- This means 3x = 11 + 7, 3x = 2*11 + 7, 3x = 3*11 + 7, etc.
- We can write that as 3x = 11k + 7 for some integer k
- Solving for x gives x = (11k + 7)/3
- You can try values of k until you find a value of 11k + 7 that is divisible by 3
- This is a little easier than just trial and error

QUESTIONS

- Any questions?