

# MA/CSSE 473

## Day 06

**Modular  
Exponentiation**

**Mathematical Induction**



# MA/CSSE 473 Day 06

- HW 3 will be available later today.
- I'll send an email
- **Student Questions**
  - These took 25 minutes
- Modular Exponentiation Algorithm/Analysis
- Mathematical induction review



# Modular Exponentiation

- In some cryptosystems, we need to compute  $x^y$  modulo  $N$ , where all three numbers are several hundred bits long. Can it be done quickly?
- Can we simply take  $x^y$  and then figure out the remainder modulo  $N$ ?
- Suppose  $x$  and  $y$  are only 20 bits long.
  - $x^y$  is at least  $(2^{19})^{(2^{19})}$ , which is about 10 million bits long.
  - Imagine how big it will be if  $y$  is a 500-bit number!
- To save space, we could repeatedly multiply by  $x$ , taking the remainder modulo  $N$  each time.
  - If  $y$  is 500 bits, then there would be  $2^{500}$  multiplications.
  - This algorithm is exponential in the length of  $y$ .
  - Ouch!



# Modular Exponentiation Algorithm

```
def modexp(x, y, N):  
    if y==0:  
        return 1  
    z = modexp(x, y/2, N)  
    if y%2 == 0:  
        return (z*z) % N  
    return (x*z*z) % N
```

- Let  $n$  be the maximum number of bits in  $x$ ,  $y$ , or  $N$
- The algorithm requires at most \_\_\_ recursive calls
- Each call is  $\Theta(\quad)$
- So the overall algorithm is  $\Theta(\quad)$



# Modular Exponentiation Algorithm

```
def modexp(x, y, N):  
    if y==0:  
        return 1  
    z = modexp(x, y/2, N)  
    if y%2 == 0:  
        return (z*z) % N  
    return (x*z*z) % N
```

- Let  $n$  be the maximum number of bits in  $x$ ,  $y$ , or  $N$
- The algorithm requires at most  $n$  recursive calls
- Each call is  $\Theta(n^2)$
- So the overall algorithm is  $\Theta(n^3)$



# Induction Review

- To show that property  $P(n)$  is true for all integers  $n \geq n_0$ , it suffices to show:
  - **Ordinary Induction**
    - $P(n_0)$  is true
    - For all  $k \geq n_0$ , if  $P(k)$  is true, then  $P(k+1)$  is also true.

or

- **Strong Induction**
  - $P(n_0)$  is true
  - For all  $k > n_0$ , if  $P(j)$  is true for all  $j$  with  $n_0 \leq j < k$ , then  $P(k)$  is also true.



# Induction examples

- For all  $N \geq 0$ , 
$$\sum_{i=1}^N i \cdot 2^i = 2^{N+1}(N-1) + 2$$
  - This is formula 7 on P 470, and is useful in one of the HW2 problems
- Show that any postage amount of 24 cents or more can be achieved using only 5-cent stamps and 7-cent stamps

