COP 3502 1/24/22

TO DO

Video Lectures - Redo link (watch)

✓ Post P1 to Webcourses

✓ Post RP1 to Webcourses

Make Groups

Quizzes → TA

Post Quiz Stats

TODAY - Recursion

✓ Towers of Hanoi

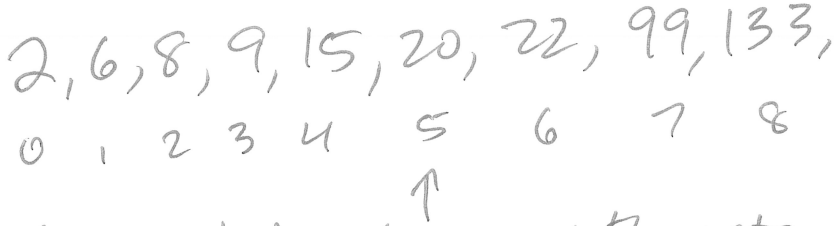
Binary Search

Fast Modular Expo

```
Towers(int start, int end, int n) {
    if (n > 0) {
        1. Towers(start, mid, n-1)
        2. Move disk n from start to end.
        3. Towers(mid, end, n-1)
    }
```

Binary Search

Input: Sorted array, value I'm looking for
Output: Is the value in the array? (Y/N)



Iteratively - while loop with ints low, high

```
int binsearch(int* array, int length, int value);
```

Recursive

```
int binsearchrec(int *array, int low, int high, int value)
    if (low > high) return 0;
    int mid = ((low + high)/2;
    if (value < array[mid])
        return binsearchrec(array, low, mid-1, value);
    else if (value > array[mid])
        return binsearchrec(array, mid+1, high, value);
    else
        return 1;
}
```

Fast Modular Exponentiation

Calculate $a^b \bmod c$ for ints a, b and c. (In code $a^b \% c$)

```
int res = 1;
for (int i = 0; i < b; i++)
    res = (res * a) % c;
```

} # steps = b.

$a^{1,000,000} \% c$

$= \left(\left(a^{500,000} \right) \% c \right)^2 \% c$

Calc $a^{500,000}$ (halfway)

Save ans.

SQUARE IT!

$(a^n)^2 = a^{2n}$

$a^n = a^{n-1} \times a$

```
long long fastModExpo(long long base, long long exp, long long mod) {
    if (exp == 0) return 1 % mod;
    if (exp % 2 == 0) {
        long long tmp = fastModExpo(base, exp/2, mod);
        return (tmp * tmp) % mod;
    }
    return (base * fastModExpo(base, exp-1, mod)) % mod;
}
```

exp divides by 2 every 2 recursive calls

$\frac{exp}{2^k} = 1$; $k = \log_2 exp$

$exp = 2^k$