Office hours tomorrow only 2-3 p.m. (excuse: lots of marking...)
Outline

power

notes

annotations
Master Theorem
(for divide-and-conquer recurrences)

If $f$ from the previous slide has $f \in \theta(n^d)$, then

$$T(n) = \begin{cases} 
\theta(n^d) & \text{if } a < b^d \\
\theta(n^d \log n) & \text{if } a = b^d \\
\theta(n^{\log_b a}) & \text{if } a > b^d 
\end{cases}$$
```python
def pow(b, n, mod):
    if n == 0:
        return 1
    r = b if n % b == 1 else 1
    half_pow = pow(b, n//b, mod)
    return (half_pow * half_pow * r) % mod

def pow2(b, n, mod):
    if n == 0:
        return 1
    r = b if n % b == 1 else 1
    return (pow2(b, n//b, mod) * pow2(b, n//b, mod) * r) % mod

def pow3(b, n, mod):
    return b**n % mod

(see power.py)
```
iterative power...

```python
def power(x, y):
    z = 1
    m = 0
    while m < y:
        z = z * x
        m = m + 1
    return z
```

- precondition? \( y \in \mathbb{N}, x \in \mathbb{R} \)
- postcondition? returns \( x^y = z \)
- notation for mutation call \( z_i, m_i \) values of \( z \) and \( m \) (respectively) after the \( i \)th iteration
Partial correctness

Precondition + execution + termination imply postcondition

A loop invariant helps get us closer

\( P(i) \) if there is an \( i \)th iteration of the

loop then \( m_i \leq y \land z_i = x^m_i \)

Claim: \( \forall i \in \mathbb{N}, \text{if precond satisfied, then } P(i) \)

Base case: If \( i = 0 \), then \( m_i = 0 \) and \( z_i = 1 \)

(Inspect code), and \( m_i = 0 \leq 1 = z_i \) also

\( z_i = 1 = x^0 = x^m_i \checkmark \) so \( P(0) \) holds.

Induction: Assume \( i \in \mathbb{N} \), assume \( P(i) \) and assume

there is an \( (i+1) \)th iteration

Then \( m_i < y \), since otherwise no \( (i+1) \)th
iteration. Thus \( m_{i+1} \leq y \) (since natural number

differ by at least \( 1 \) (\( m_i \) starts natural, and adds

1 each iter). By \( 1H \), \( z_{i+1} = x^{m_{i+1}} \), and line 4

means \( z_{i+1} = \varnothing z_{i} \times x = x^{m_i} \times x = x^{m_{i+1}} \)
partial correctness

precondition+execution+termination imply postcondition

a loop invariant helps get us closer

Assume $I$ (loop invariant) and termination.

Then, call last iteration iteration $k$.

So $L1$ says $m_k \leq y \land z_k = x^{m_k}$

$\land$ loop terminates, so $m_k \geq y \Rightarrow m_k = y$

$\Rightarrow m_k = y$, so postcondition follows $z_k = z = x^{m_k} = x^y$
prove partial correctness
prove termination show progress towards exiting loop.

associate a decreasing sequence in \( \mathbb{N} \) with loop iterations it helps to add claims to the loop invariant

if \( n \) is a \( \downarrow \) sequence in \( \mathbb{N} \), it must have smallest value (Well Ordering), hence a lost iteration.

how about \( <y - m_i> \in \text{natural?} \)

Claim: \( y - m_i \in \mathbb{N} \) and (if there is an \((i+1)\)th iteration then \( y - m_i > y - m_{i+1} \). By 21 iteration \( m_i \leq y \), so \( y - m_i \geq 0 \) and \( y \in \mathbb{N}, m_i \in \mathbb{N} \). 

\( m_i \leq y \), so \( y - m_i \geq 0 \) and \( y \in \mathbb{N}, m_i \in \mathbb{N} \). 

so \( y - m_i \in \mathbb{Z} \to \mathbb{N} \).

So \( y - m_i \in \mathbb{Z} \to \mathbb{N} \).

If there is an \((i+1)\)th iteration, then \( m_{i+1} = m_i + 1 \) (line 5), so

\( y - m_i > y - m_{i+1} = y - (m_i + 1) = y - m_{i+1} \)

So \( <y - m_i> \) is a decreasing sequence in \( \mathbb{N} \) +

so well termination
put it together — correctness
correctness by design

draw pictures of before, during, after
pre: A sorted, comparable with x
post: $0 \leq p \leq n$ and $A[0..p-1] < x \leq A[p .. n-1]$

“derive” conditions from pictures
do we have termination?