## CSE 311: Foundations of Computing

## Lecture 16: Recursion \& Strong Induction Applications: Fibonacci \& Euclid



## Last time: recursive definitions of functions

- $F(0)=0 ; F(n+1)=F(n)+1$ for all $n \geq 0$.
- $G(0)=1 ; \quad G(n+1)=2 \cdot G(n)$ for all $n \geq 0$.
- $0!=1 ;(n+1)!=(n+1) \cdot n!$ for all $n \geq 0$.
- $H(0)=1 ; H(n+1)=2^{H(n)}$ for all $n \geq 0$.


## More Recursive Definitions

Suppose that $h: \mathbb{N} \rightarrow \mathbb{R}$.
Then we have familiar summation notation:
$\sum_{i=0}^{0} h(i)=h(0)$
$\sum_{i=0}^{n+1} h(i)=h(n+1)+\sum_{i=0}^{n} h(i)$ for $n \geq 0$

There is also product notation:
$\prod_{i=0}^{0} h(i)=h(0)$
$\prod_{i=0}^{n+1} h(i)=h(n+1) \cdot \prod_{i=0}^{n} h(i)$ for $n \geq 0$

Fibonacci Numbers

$$
\begin{aligned}
& f_{0}=0 \\
& f_{1}=1 \\
& f_{n}=f_{n-1}+f_{n-2} \text { for all } n \geq 2
\end{aligned}
$$



## Strong Inductive Proofs In 5 Easy Steps

1. "Let $P(n)$ be... . We will show that $P(n)$ is true for all integers $n \geq b$ by strong induction."
2. "Base Case:" Prove $P(b)$
3. "Inductive Hypothesis:

Assume that for some arbitrary integer $k \geq b$,
$P(j)$ is true for every integer $j$ from $b$ to $k "$
4. "Inductive Step:" Prove that $P(k+1)$ is true:

Use the goal to figure out what you need.
Make sure you are using I.H. (that $P(b), \ldots, P(k)$ are true) and point out where you are using it.
(Don't assume $P(k+1)$ !!)
5. "Conclusion: $P(n)$ is true for all integers $n \geq b$ "

## Bounding Fibonacci I: $f_{n}<2^{n}$ for all $n \geq 0$

$$
\begin{aligned}
& \boldsymbol{f}_{0}=\mathbf{0} \quad \boldsymbol{f}_{1}=\mathbf{1} \\
& \boldsymbol{f}_{n}=\boldsymbol{f}_{n-1}+\boldsymbol{f}_{n-2} \text { for all } n \geq \mathbf{2} \\
& \hline
\end{aligned}
$$

## Bounding Fibonacci I: $f_{n}<2^{n}$ for all $n \geq 0$

1. Let $P(n)$ be " $f_{n}<2^{n}$ ". We prove that $P(n)$ is true for all integers $\mathrm{n} \geq 0$ by strong induction.

$$
\begin{aligned}
& \boldsymbol{f}_{0}=\mathbf{0} \quad \boldsymbol{f}_{1}=\mathbf{1} \\
& \boldsymbol{f}_{n}=\boldsymbol{f}_{n-1}+\boldsymbol{f}_{n-2} \text { for all } n \geq \mathbf{2}
\end{aligned}
$$

## Bounding Fibonacci I: $f_{n}<2^{n}$ for all $n \geq 0$

1. Let $P(n)$ be " $f_{n}<2^{n}$ ". We prove that $P(n)$ is true for all integers $\mathrm{n} \geq 0$ by strong induction.
2. Base Case: $f_{0}=0<1=2^{0}$ so $P(0)$ is true.

$$
\begin{aligned}
& \boldsymbol{f}_{0}=\mathbf{0} \quad \boldsymbol{f}_{1}=\mathbf{1} \\
& \boldsymbol{f}_{n}=\boldsymbol{f}_{n-1}+\boldsymbol{f}_{n-2} \text { for all } n \geq \mathbf{2}
\end{aligned}
$$

## Bounding Fibonacci I: $f_{n}<2^{n}$ for all $n \geq 0$

1. Let $P(n)$ be " $f_{n}<2^{n "}$. We prove that $P(n)$ is true for all integers $\mathrm{n} \geq 0$ by strong induction.
2. Base Case: $f_{0}=0<1=2^{0}$ so $P(0)$ is true.
3. Inductive Hypothesis: Assume that for some arbitrary integer $k \geq 0$, we have $f_{j}<2^{j}$ for every integer $j$ from 0 to $k$.

$$
\begin{aligned}
& \boldsymbol{f}_{0}=\mathbf{0} \quad \boldsymbol{f}_{1}=\mathbf{1} \\
& \boldsymbol{f}_{n}=\boldsymbol{f}_{n-1}+\boldsymbol{f}_{n-2} \text { for all } n \geq \mathbf{2}
\end{aligned}
$$

## Bounding Fibonacci I: $f_{n}<2^{n}$ for all $n \geq 0$

1. Let $P(n)$ be " $f_{n}<2^{n "}$. We prove that $P(n)$ is true for all integers $\mathrm{n} \geq 0$ by strong induction.
2. Base Case: $f_{0}=0<1=2^{0}$ so $P(0)$ is true.
3. Inductive Hypothesis: Assume that for some arbitrary integer $k \geq 0$, we have $f_{j}<2^{j}$ for every integer j from 0 to $k$.
4. Inductive Step: Goal: Show $P(k+1)$; that is, $f_{k+1}<2^{k+1}$

$$
\begin{aligned}
& f_{0}=0 \quad f_{1}=1 \\
& f_{n}=f_{n-1}+f_{n-2} \text { for all } n \geq 2
\end{aligned}
$$

## Bounding Fibonacci I: $f_{n}<2^{n}$ for all $n \geq 0$

1. Let $P(n)$ be " $f_{n}<2^{n "}$. We prove that $P(n)$ is true for all integers $\mathrm{n} \geq 0$ by strong induction.
2. Base Case: $f_{0}=0<1=2^{0}$ so $P(0)$ is true.
3. Inductive Hypothesis: Assume that for some arbitrary integer $k \geq 0$, we have $f_{j}<2^{j}$ for every integer $j$ from 0 to $k$.
4. Inductive Step: Goal: Show $P(k+1)$; that is, $f_{k+1}<2^{k+1}$

Case $k+1=1$ :
Case $k+1 \geq 2$ :

$$
\begin{aligned}
& f_{0}=\mathbf{0} \quad f_{1}=1 \\
& f_{n}=f_{n-1}+f_{n-2} \quad \text { for all } n \geq 2
\end{aligned}
$$

## Bounding Fibonacci I: $f_{n}<2^{n}$ for all $n \geq 0$

1. Let $P(n)$ be " $f_{n}<2^{n "}$. We prove that $P(n)$ is true for all integers $\mathrm{n} \geq 0$ by strong induction.
2. Base Case: $f_{0}=0<1=2^{0}$ so $P(0)$ is true.
3. Inductive Hypothesis: Assume that for some arbitrary integer $k \geq 0$, we have $f_{j}<2^{j}$ for every integer $j$ from 0 to $k$.
4. Inductive Step: Goal: Show $P(k+1)$; that is, $f_{k+1}<2^{k+1}$

Case $k+1=1$ : Then $f_{1}=1<2=2^{1}$ so $P(k+1)$ is true here.
Case $k+1 \geq 2$ :

$$
\begin{aligned}
& \boldsymbol{f}_{0}=\mathbf{0} \quad \boldsymbol{f}_{1}=\mathbf{1} \\
& \boldsymbol{f}_{n}=\boldsymbol{f}_{n-1}+\boldsymbol{f}_{n-2} \text { for all } n \geq \mathbf{2} \\
& \hline
\end{aligned}
$$

## Bounding Fibonacci I: $f_{n}<2^{n}$ for all $n \geq 0$

1. Let $\mathrm{P}(\mathrm{n})$ be " $\mathrm{f}_{\mathrm{n}}<2^{\mathrm{n}}$ ". We prove that $\mathrm{P}(\mathrm{n})$ is true for all integers $\mathrm{n} \geq 0$ by strong induction.
2. Base Case: $f_{0}=0<1=2^{0}$ so $P(0)$ is true.
3. Inductive Hypothesis: Assume that for some arbitrary integer $\mathrm{k} \geq 0$, we have $\mathrm{f}_{\mathrm{j}}<2^{j}$ for every integer j from 0 to k .
4. Inductive Step: Goal: Show $\mathrm{P}(\mathrm{k}+1)$; that is, $\mathrm{f}_{\mathrm{k}+1}<2^{k+1}$

Case $k+1=1$ : Then $f_{1}=1<2=2^{1}$ so $P(k+1)$ is true here.
Case $k+1 \geq 2$ : Then $f_{k+1}=f_{k}+f_{k-1}$ by definition

$$
\begin{aligned}
& <2^{k}+2^{k-1} \text { by the IH since } k-1 \geq 0 \\
& <2^{k}+2^{k}=2 \cdot 2^{k}=2^{k+1}
\end{aligned}
$$

so $P(k+1)$ is true in this case.
These are the only cases so $P(k+1)$ follows.

$$
\begin{aligned}
& f_{0}=0 \quad f_{1}=1 \\
& f_{n}=f_{n-1}+f_{n-2} \text { for all } n \geq 2
\end{aligned}
$$

## Bounding Fibonacci I: $f_{n}<2^{n}$ for all $n \geq 0$

1. Let $\mathrm{P}(\mathrm{n})$ be " $\mathrm{f}_{\mathrm{n}}<2^{n}$ ". We prove that $\mathrm{P}(\mathrm{n})$ is true for all integers $\mathrm{n} \geq 0$ by strong induction.
2. Base Case: $f_{0}=0<1=2^{0}$ so $P(0)$ is true.
3. Inductive Hypothesis: Assume that for some arbitrary integer $\mathrm{k} \geq 0$, we have $\mathrm{f}_{\mathrm{j}}<2^{j}$ for every integer j from 0 to k .
4. Inductive Step: Goal: Show $\mathrm{P}(\mathrm{k}+1)$; that is, $\mathrm{f}_{\mathrm{k}+1}<2^{k+1}$

Case $k+1=1$ : Then $f_{1}=1<2=2^{1}$ so $P(k+1)$ is true here.
Case $k+1 \geq 2$ : Then $f_{k+1}=f_{k}+f_{k-1}$ by definition

$$
\begin{aligned}
& <2^{k}+2^{k-1} \text { by the IH since } k-1 \geq 0 \\
& <2^{k}+2^{k}=2 \cdot 2^{k}=2^{k+1}
\end{aligned}
$$

so $P(k+1)$ is true in this case.
These are the only cases so $P(k+1)$ follows.
5. Therefore by strong induction, $f_{n}<2^{n}$ for all integers $n \geq 0$.

$$
\begin{aligned}
& \boldsymbol{f}_{0}=0 \quad f_{1}=1 \\
& f_{n}=f_{n-1}+f_{n-2} \text { for all } n \geq 2
\end{aligned}
$$

## Bounding Fibonacci II: $f_{n} \geq 2^{n / 2-1}$ for all $n \geq 2$

$$
\begin{aligned}
& f_{0}=\mathbf{0} \quad \boldsymbol{f}_{1}=\mathbf{1} \\
& \boldsymbol{f}_{n}=\boldsymbol{f}_{n-1}+\boldsymbol{f}_{n-2} \text { for all } n \geq \mathbf{2}
\end{aligned}
$$

Bounding Fibonacci II: $f_{n} \geq 2^{n / 2-1}$ for all $n \geq 2$

1. Let $P(n)$ be " $f_{n} \geq 2^{n / 2-1}$ ". We prove that $P(n)$ is true for all integers $\mathrm{n} \geq 2$ by strong induction.

$$
\begin{aligned}
& f_{0}=\mathbf{0} \quad \boldsymbol{f}_{1}=\mathbf{1} \\
& \boldsymbol{f}_{n}=\boldsymbol{f}_{n-1}+\boldsymbol{f}_{n-2} \text { for all } n \geq \mathbf{2}
\end{aligned}
$$

## Bounding Fibonacci II: $f_{n} \geq 2^{n / 2-1}$ for all $n \geq 2$

1. Let $P(n)$ be " $f_{n} \geq 2^{n / 2-1}$ ". We prove that $P(n)$ is true for all integers $n \geq 2$ by strong induction.
2. Base Case: $f_{2}=f_{1}+f_{0}=1$ and $2^{2 / 2-1}=2^{0}=1$ so $P(2)$ is true.

$$
\begin{aligned}
& \boldsymbol{f}_{0}=\mathbf{0} \quad \boldsymbol{f}_{1}=\mathbf{1} \\
& \boldsymbol{f}_{n}=\boldsymbol{f}_{n-1}+\boldsymbol{f}_{n-2} \text { for all } n \geq \mathbf{2}
\end{aligned}
$$

Bounding Fibonacci II: $f_{n} \geq 2^{n / 2-1}$ for all $n \geq 2$

1. Let $P(n)$ be " $f_{n} \geq 2^{n / 2-1}$ ". We prove that $P(n)$ is true for all integers $\mathrm{n} \geq 2$ by strong induction.
2. Base Case: $f_{2}=f_{1}+f_{0}=1$ and $2^{2 / 2-1}=2^{0}=1$ so $P(2)$ is true.
3. Inductive Hypothesis: Assume that for some arbitrary integer $\mathrm{k} \geq 2, \mathrm{P}(\mathrm{j})$ is true for every integer j from 2 to k .

$$
\begin{aligned}
& f_{0}=\mathbf{0} \quad f_{1}=\mathbf{1} \\
& f_{n}=f_{n-1}+f_{n-2} \text { for all } n \geq 2
\end{aligned}
$$

## Bounding Fibonacci II: $f_{n} \geq 2^{n / 2-1}$ for all $n \geq 2$

1. Let $P(n)$ be " $f_{n} \geq 2^{n / 2-1}$ ". We prove that $P(n)$ is true for all integers $\mathrm{n} \geq 2$ by strong induction.
2. Base Case: $f_{2}=f_{1}+f_{0}=1$ and $2^{2 / 2-1}=2^{0}=1$ so $P(2)$ is true.
3. Inductive Hypothesis: Assume that for some arbitrary integer $\mathrm{k} \geq 2, \mathrm{P}(\mathrm{j})$ is true for every integer j from 2 to k .
4. Inductive Step: Goal: Show $P(k+1)$; that is, $f_{k+1} \geq 2^{(k+1) / 2-1}$

$$
\begin{aligned}
& f_{0}=\mathbf{0} \quad f_{1}=\mathbf{1} \\
& \boldsymbol{f}_{n}=\boldsymbol{f}_{n-1}+\boldsymbol{f}_{n-2} \text { for all } n \geq \mathbf{2}
\end{aligned}
$$

## Bounding Fibonacci II: $f_{n} \geq 2^{n / 2-1}$ for all $n \geq 2$

1. Let $P(n)$ be " $f_{n} \geq 2^{n / 2-1}$ ". We prove that $P(n)$ is true for all integers $\mathrm{n} \geq 2$ by strong induction.
2. Base Case: $f_{2}=f_{1}+f_{0}=1$ and $2^{2 / 2-1}=2^{0}=1$ so $P(2)$ is true.
3. Inductive Hypothesis: Assume that for some arbitrary integer $\mathrm{k} \geq 2, \mathrm{P}(\mathrm{j})$ is true for every integer j from 2 to k .
4. Inductive Step: Goal: Show $P(k+1)$; that is, $f_{k+1} \geq 2^{(k+1) / 2-1}$

No need for cases for the definition here:

$$
f_{k+1}=f_{k}+f_{k-1} \text { since } k+1 \geq 2
$$

Now just want to apply the IH to get $\mathrm{P}(\mathrm{k})$ and $\mathrm{P}(\mathrm{k}-1)$
Problem: Though we can get $P(k)$ since $k \geq 2$,
$\mathrm{k}-1$ may only be 1 so we can't conclude $\mathrm{P}(\mathrm{k}-1)$
Solution: Separate cases for when $k-1=1$ (or $k+1=3$ ).

$$
\begin{aligned}
& f_{0}=0 \quad f_{1}=1 \\
& f_{n}=f_{n-1}+f_{n-2} \text { for all } n \geq 2
\end{aligned}
$$

## Bounding Fibonacci II: $f_{n} \geq 2^{n / 2-1}$ for all $n \geq 2$

1. Let $P(n)$ be " $f_{n} \geq 2^{n / 2-1}$ ". We prove that $P(n)$ is true for all integers $\mathrm{n} \geq 2$ by strong induction.
2. Base Case: $f_{2}=f_{1}+f_{0}=1$ and $2^{2 / 2-1}=2^{0}=1$ so $P(2)$ is true.
3. Inductive Hypothesis: Assume that for some arbitrary integer $\mathrm{k} \geq 2, \mathrm{P}(\mathrm{j})$ is true for every integer j from 2 to k .
4. Inductive Step: Goal: Show $P(k+1)$; that is, $f_{k+1} \geq 2^{(k+1) / 2-1}$

Case $\mathrm{k}=2$ :
Case $\mathrm{k} \geq 3$ :

$$
\begin{aligned}
& f_{0}=\mathbf{0} \quad \boldsymbol{f}_{1}=\mathbf{1} \\
& \boldsymbol{f}_{n}=\boldsymbol{f}_{n-1}+\boldsymbol{f}_{n-2} \text { for all } n \geq \mathbf{2}
\end{aligned}
$$

## Bounding Fibonacci II: $f_{n} \geq 2^{n / 2-1}$ for all $n \geq 2$

1. Let $P(n)$ be " $f_{n} \geq 2^{n / 2-1}$ ". We prove that $P(n)$ is true for all integers $\mathrm{n} \geq 2$ by strong induction.
2. Base Case: $f_{2}=f_{1}+f_{0}=1$ and $2^{2 / 2-1}=2^{0}=1$ so $P(2)$ is true.
3. Inductive Hypothesis: Assume that for some arbitrary integer $\mathrm{k} \geq 2, \mathrm{P}(\mathrm{j})$ is true for every integer j from 2 to k .
4. Inductive Step: Goal: Show $P(k+1)$; that is, $f_{k+1} \geq 2^{(k+1) / 2-1}$

Case $k=2$ : Then $f_{k+1}=f_{3}=f_{2}+f_{1}=2 \geq 2^{1 / 2}=2^{3 / 2-1}=2^{(k+1) / 2-1}$
Case $k \geq 3$ :

$$
\begin{aligned}
& f_{0}=\mathbf{0} \quad \boldsymbol{f}_{1}=\mathbf{1} \\
& \boldsymbol{f}_{n}=\boldsymbol{f}_{n-1}+\boldsymbol{f}_{n-2} \text { for all } n \geq \mathbf{2} \\
& \hline
\end{aligned}
$$

## Bounding Fibonacci II: $f_{n} \geq 2^{n / 2-1}$ for all $n \geq 2$

1. Let $P(n)$ be " $f_{n} \geq 2^{n / 2-1}$ ". We prove that $P(n)$ is true for all integers $\mathrm{n} \geq 2$ by strong induction.
2. Base Case: $f_{2}=f_{1}+f_{0}=1$ and $2^{2 / 2-1}=2^{0}=1$ so $P(2)$ is true.
3. Inductive Hypothesis: Assume that for some arbitrary integer $\mathrm{k} \geq 2, \mathrm{P}(\mathrm{j})$ is true for every integer j from 2 to k .
4. Inductive Step: Goal: Show $P(k+1)$; that is, $f_{k+1} \geq 2^{(k+1) / 2-1}$

Case $\mathrm{k}=2$ : Then $\mathrm{f}_{\mathrm{k}+1}=\mathrm{f}_{3}=\mathrm{f}_{2}+\mathrm{f}_{1}=2 \geq 2^{1 / 2}=2^{3 / 2-1}=2^{(k+1) / 2-1}$
Case $k \geq 3: \quad f_{k+1}=f_{k}+f_{k-1}$ by definition

$$
\begin{aligned}
& \geq 2^{k / 2-1}+2^{(k-1) / 2-1} \text { by the IH since } k-1 \geq 2 \\
& \geq 2^{(k-1) / 2-1}+2^{(k-1) / 2-1}=2^{(k-1) / 2}=2^{(k+1) / 2-1}
\end{aligned}
$$

So $P(k+1)$ is true in both cases.
5. Therefore by strong induction, $f_{n} \geq 2^{n / 2-1}$ for all integers $n \geq 0$.

$$
\begin{aligned}
& f_{0}=0 \quad f_{1}=1 \\
& f_{n}=f_{n-1}+f_{n-2} \text { for all } n \geq 2
\end{aligned}
$$

## Running time of Euclid's algorithm

Theorem: Suppose that Euclid's Algorithm takes $n$ steps for $\operatorname{gcd}(a, b)$ with $a \geq b>0$. Then, $a \geq f_{n+1}$.

## Running time of Euclid's algorithm

Theorem: Suppose that Euclid's Algorithm takes $n$ steps for $\operatorname{gcd}(a, b)$ with $a \geq b>0$. Then, $a \geq f_{n+1}$.

An informal way to get the idea: Consider an $n$ step gcd calculation starting with $r_{n+1}=a$ and $r_{n}=b$ :

$$
\begin{aligned}
r_{n+1} & =q_{n} r_{n}+r_{n-1} \\
r_{n} & =q_{n-1} r_{n-1}+r_{n-2} \\
& \cdots \\
r_{3} & =q_{2} r_{2}+r_{1} \\
r_{2} & =q_{1} r_{1}
\end{aligned}
$$

For all $k \geq 2, r_{k-1}=r_{k+1} \bmod r_{k}$

Now $r_{1} \geq 1$ and each $q_{k}$ must be $\geq 1$. If we replace all the $q_{k}$ 's by 1 and replace $r_{1}$ by 1 , we can only reduce the $r_{k}$ 's. After that reduction, $r_{k}=f_{k}$ for every $k$.

## Running time of Euclid's algorithm

Theorem: Suppose that Euclid's Algorithm takes $n$ steps for $\operatorname{gcd}(a, b)$ with $a \geq b>0$. Then, $a \geq f_{n+1}$.

We go by strong induction on $n$.
Let $P(n)$ be " $g c d(a, b)$ with $a \geq b>0$ takes $n$ steps $\rightarrow a \geq f_{n+1}$ " for all $n \geq 1$.
Base Case: $n=1$ Suppose Euclid's Algorithm with $a \geq b>0$ takes 1 step. By assumption, $a \geq b \geq 1=f_{2}$ so $P(1)$ holds.

Induction Hypothesis: Suppose that for some integer $\mathrm{k} \geq 1, \mathrm{P}(\mathrm{j})$ is true for all integers j s.t. $1 \leq \mathrm{j} \leq \mathrm{k}$

## Running time of Euclid's algorithm

Theorem: Suppose that Euclid's Algorithm takes $n$ steps for $\operatorname{gcd}(a, b)$ with $a \geq b>0$. Then, $a \geq f_{n+1}$.

We go by strong induction on $n$.
Let $P(n)$ be " $\operatorname{gcd}(a, b)$ with $a \geq b>0$ takes $n$ steps $\rightarrow a \geq f_{n+1}$ " for all $n \geq 1$.
Base Case: $n=1$ Suppose Euclid's Algorithm with $a \geq b>0$ takes 1 step. By assumption, $a \geq b \geq 1=f_{2}$ so $P(1)$ holds.

Induction Hypothesis: Suppose that for some integer $\mathrm{k} \geq 1, \mathrm{P}(\mathrm{j})$ is true for all integers j s.t. $1 \leq \mathrm{j} \leq \mathrm{k}$

Inductive Step: We want to show: if $\operatorname{gcd}(\mathrm{a}, \mathrm{b})$ with $\mathrm{a} \geq \mathrm{b}>0$ takes $\mathrm{k}+1$ steps, then $a \geq f_{k+2}$.

## Running time of Euclid's algorithm

Induction Hypothesis: Suppose that for some integer $\mathrm{k} \geq 1, \mathrm{P}(\mathrm{j})$ is true for all integers j s.t. $1 \leq \mathrm{j} \leq \mathrm{k}$
Inductive Step: Goal: if $\operatorname{gcd}(a, b)$ with $a \geq b>0$ takes $k+1$ steps, then $a \geq f_{k+2}$.

Now if $k+1=2$, then Euclid's algorithm on $a$ and $b$ can be written as

$$
\begin{aligned}
a & =q_{2} b+r_{1} \\
b & =q_{1} r_{1} \\
\text { and } r_{1} & >0 .
\end{aligned}
$$

Also, since $a \geq b>0$ we must have $q_{2} \geq 1$ and $b \geq 1$.
So $a=q_{2} b+r_{1} \geq b+r_{1} \geq 1+1=2=f_{3}=f_{k+2}$ as required.

## Running time of Euclid's algorithm

Induction Hypothesis: Suppose that for some integer $\mathrm{k} \geq 1, \mathrm{P}(\mathrm{j})$ is true for all integers j s.t. $1 \leq \mathrm{j} \leq \mathrm{k}$
Inductive Step: Goal: if $\operatorname{gcd}(a, b)$ with $a \geq b>0$ takes $k+1$ steps, then $a \geq f_{k+2}$.

Next suppose that $k+1 \geq 3$ so for the first 3 steps of Euclid's algorithm on $a$ and $b$ we have

$$
\begin{aligned}
& a=q_{k+1} b+r_{k} \\
& b=q_{k} r_{k}+r_{k-1} \\
& r_{k}=q_{k-1} r_{k-1}+r_{k-2}
\end{aligned}
$$

and there are $k-2$ more steps after this.

## Running time of Euclid's algorithm

Induction Hypothesis: Suppose that for some integer $\mathrm{k} \geq 1, \mathrm{P}(\mathrm{j})$ is true for all integers j s.t. $1 \leq \mathrm{j} \leq \mathrm{k}$
Inductive Step: Goal: if $\operatorname{gcd}(a, b)$ with $a \geq b>0$ takes $k+1$ steps, then $a \geq f_{k+2}$.

Next suppose that $k+1 \geq 3$ so for the first 3 steps of Euclid's algorithm on $a$ and $b$ we have

$$
\begin{aligned}
& a=q_{k+1} b+r_{k} \\
& b=q_{k} r_{k}+r_{k-1} \\
& r_{k}=q_{k-1} r_{k-1}+r_{k-2}
\end{aligned}
$$

and there are $k-2$ more steps after this. Note that this means that the $\operatorname{gcd}\left(b, r_{k}\right)$ takes $k$ steps and $\operatorname{gcd}\left(r_{k}, r_{k-1}\right)$ takes $k-1$ steps.

So since $k, k-1 \geq 1$ by the IH we have $b \geq f_{k+1}$ and $r_{k} \geq f_{k}$.

## Running time of Euclid's algorithm

Induction Hypothesis: Suppose that for some integer $\mathrm{k} \geq 1, \mathrm{P}(\mathrm{j})$ is true for all integers j s.t. $1 \leq \mathrm{j} \leq \mathrm{k}$
Inductive Step: Goal: if $\operatorname{gcd}(a, b)$ with $a \geq b>0$ takes $k+1$ steps, then $a \geq f_{k+2}$.

Next suppose that $k+1 \geq 3$ so for the first 3 steps of Euclid's algorithm on $a$ and $b$ we have

$$
\begin{aligned}
& a=q_{k+1} b+r_{k} \\
& b=q_{k} r_{k}+r_{k-1} \\
& r_{k}=q_{k-1} r_{k-1}+r_{k-2}
\end{aligned}
$$

and there are $k-2$ more steps after this. Note that this means that the $\operatorname{gcd}\left(b, r_{k}\right)$ takes $k$ steps and $\operatorname{gcd}\left(r_{k}, r_{k-1}\right)$ takes $k-1$ steps.

So since $k, k-1 \geq 1$ by the IH we have $b \geq f_{k+1}$ and $r_{k} \geq f_{k}$.
Also, since $a \geq b$ we must have $q_{k+1} \geq 1$.
So $a=q_{k+1} b+r_{k} \geq b+r_{k} \geq f_{k+1}+f_{k}=f_{k+2}$ as required.

## Running time of Euclid's algorithm

Theorem: Suppose that Euclid's Algorithm takes $n$ steps for $\operatorname{gcd}(a, b)$ with $a \geq b>0$. Then, $a \geq f_{n+1}$.

Why does this help us bound the running time of Euclid's Algorithm?

We already proved that $f_{n} \geq 2^{n / 2-1}$ so $f_{n+1} \geq 2^{(n-1) / 2}$
Therefore: if Euclid's Algorithm takes $n$ steps
for $\operatorname{gcd}(a, b)$ with $a \geq b>0$
then $a \geq 2^{(n-1) / 2}$
so $(n-1) / 2 \leq \log _{2} a$ or $n \leq 1+2 \log _{2} a$
i.e., \# of steps $\leq 1+$ twice the \# of bits in $a$.

## Recursive Definition of Sets

## Recursive Definition

- Basis Step: $0 \in S$
- Recursive Step: If $x \in S$, then $x+2 \in S$
- Exclusion Rule: Every element in $S$ follows from basis steps and a finite number of recursive steps.


## Recursive Definitions of Sets

Natural numbers
Basis: $\quad 0 \in S$
Recursive: If $x \in S$, then $x+1 \in S$
Even numbers
Basis: $\quad 0 \in S$
Recursive: If $x \in S$, then $x+2 \in S$

Powers of 3:
Basis: $1 \in S$
Recursive: If $x \in S$, then $3 x \in S$.
Basis: $\quad[0,0] \in S,[1,1] \in S$
Recursive: If $[n-1, x] \in S$ and $[n, y] \in S$, then $[n+1, x+y] \in S$.

## Recursive Definitions of Sets

Natural numbers
Basis: $\quad 0 \in S$
Recursive: If $x \in S$, then $x+1 \in S$

Even numbers
Basis: $\quad 0 \in S$
Recursive: If $x \in S$, then $x+2 \in S$

Powers of 3:
Basis: $1 \in S$
Recursive: If $x \in S$, then $3 x \in S$.
Basis: $\quad[0,0] \in S,[1,1] \in S$
Recursive: If $[n-1, x] \in S$ and $[n, y] \in S$,
Fibonacci numbers then $[n+1, x+y] \in S$.

## Recursive Definitions of Sets: General Form

## Recursive definition

- Basis step: Some specific elements are in $S$
- Recursive step: Given some existing named elements in $S$ some new objects constructed from these named elements are also in $S$.
- Exclusion rule: Every element in $S$ follows from basis steps and a finite number of recursive steps


## Strings

- An alphabet $\Sigma$ is any finite set of characters
- The set $\Sigma^{*}$ of strings over the alphabet $\Sigma$ is defined by
- Basis: $\varepsilon \in \Sigma$ ( $\varepsilon$ is the empty string)
- Recursive: if $w \in \Sigma^{*}, a \in \Sigma$, then $w a \in \Sigma^{*}$


## Palindromes

Palindromes are strings that are the same backwards and forwards

## Basis:

$\varepsilon$ is a palindrome and any $a \in \Sigma$ is a palindrome

Recursive step:
If $p$ is a palindrome then apa is a palindrome for every $a \in \Sigma$

## All Binary Strings with no 1's before 0's

Basis:
$\varepsilon \in S$
Recursive:
If $x \in S$, then $0 x \in S$
If $x \in S$, then $x 1 \in S$

## Function Definitions on Recursively Defined Sets

Length:

$$
\operatorname{len}(E)=0
$$

$$
\operatorname{len}(w a)=1+\operatorname{len}(w) \text { for } w \in \Sigma^{*}, a \in \Sigma
$$

Reversal:

$$
\begin{aligned}
& \varepsilon^{R}=\varepsilon \\
& (w a)^{R}=a w^{R} \text { for } w \in \Sigma^{*}, a \in \Sigma
\end{aligned}
$$

Concatenation:
$x \bullet E=x$ for $x \in \Sigma^{*}$
$x \bullet w a=(x \bullet w) a$ for $x \in \Sigma^{*}, a \in \Sigma$

