

Greatest Common Divisor

Gcd. Find largest integer that evenly divides into p and q.

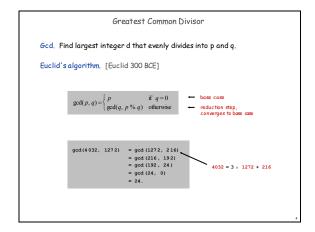
Ex. gcd(4032, 1272) = 24.

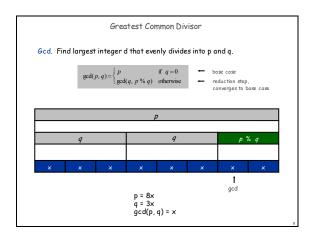
4032 = 26 × 32 × 71
1272 = 23 × 31 × 531
gcd = 23 × 31 = 24

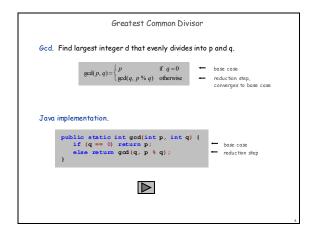
Applications.

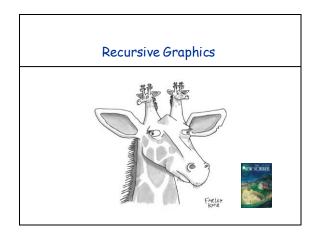
Simplify fractions: 1272/4032 = 53/168.

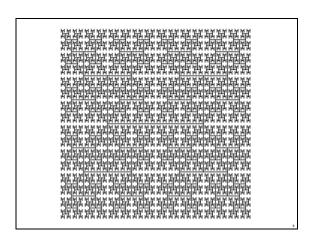
RSA cryptosystem.

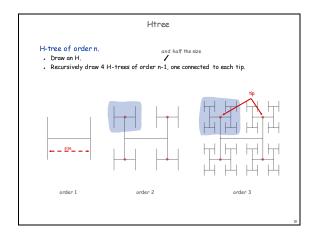


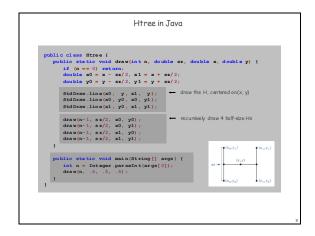


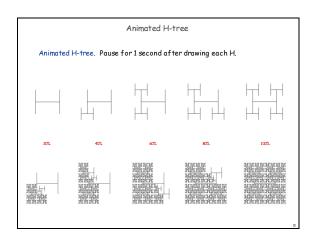




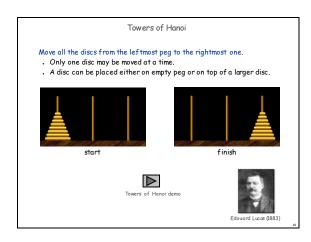


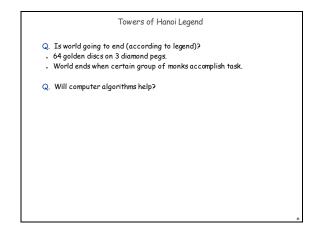


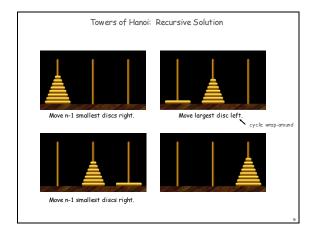


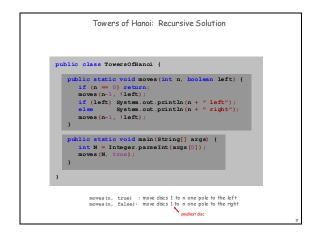


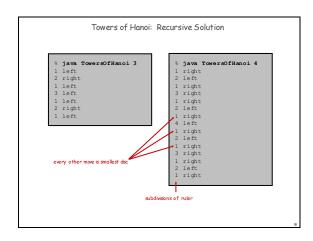


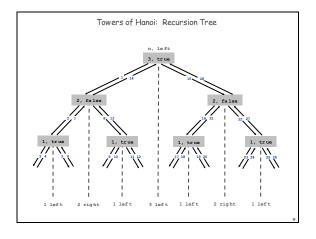












Remarkable properties of recursive solution.

Takes 2" - 1 moves to solve n disc problem.

Sequence of discs is same as subdivisions of ruler.

Every other move involves smallest disc.

Recursive algorithm yields non-recursive solution!

Alternate between two moves:

- move smallest disc to right if n is even

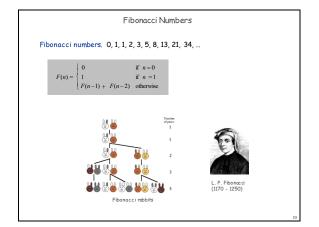
- make only legal move not involving smallest disc

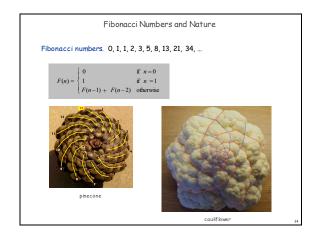
Recursive algorithm may reveal fate of world.

Takes 585 billion years for n = 64 (at rate of 1 disc per second).

Reassuring fact: any solution takes at least this long!

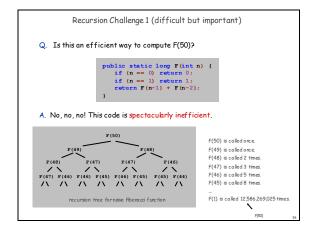
Fibonacci Numbers





A Possible Pitfall With Recursion

Fibonacci numbers. 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, ... $F(n) = \begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ F(n-1) + F(n-2) & \text{otherwise} \end{cases}$ A natural for recursion? $public static long F(int n) \{ if (n = -0) return 0; if (n = -1) return 1; return 1; return 1; return 1; return F(n-1) + F(n-2); \}$



How to write simple recursive programs? Base case, reduction step. Trace the execution of a recursive program. Use pictures. Why learn recursion? New mode of thinking. Powerful programming tool.

Extra Slides

