Great Theoretical Ideas In Computer Science

Steven Rudich

CS 15-251

Spring 2004

Lecture 6

Jan 29, 2004

Carnegie Mellon University

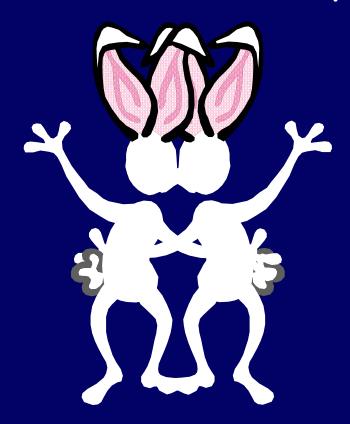
Rabbits, Continued Fractions, The Golden Ratio, and Euclid's GCD

$$\frac{3+\sqrt{13}}{2} = 3 + \frac{1}{3+\frac$$

4

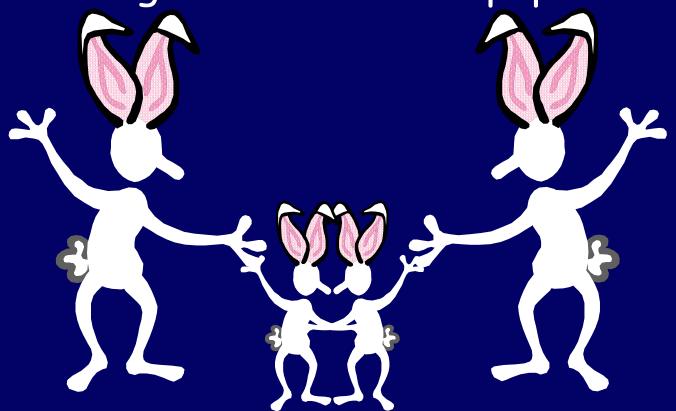
Leonardo Fibonacci

In 1202, Fibonacci proposed a problem about the growth of rabbit populations.



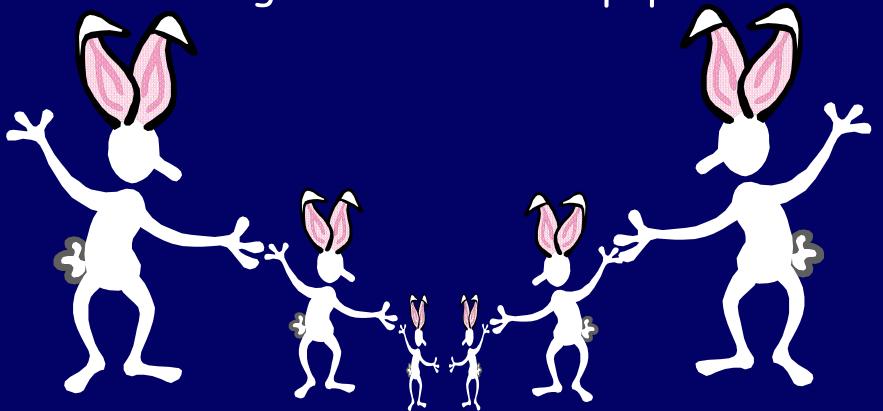
Leonardo Fibonacci

In 1202, Fibonacci proposed a problem about the growth of rabbit populations.



Leonardo Fibonacci

In 1202, Fibonacci proposed a problem about the growth of rabbit populations.



- · A rabbit lives forever
- ·The population starts as a single newborn pair
- •Every month, each productive pair begets a new pair which will become productive after 2 months old

 F_n = # of rabbit pairs at the beginning of the n^{th} month

month	1	2	3	4	5	6	7
rabbits							

- · A rabbit lives forever
- ·The population starts as a single newborn pair
- •Every month, each productive pair begets a new pair which will become productive after 2 months old

 F_n = # of rabbit pairs at the beginning of the n^{th} month

month	1	2	3	4	5	6	7
rabbits	1						

- · A rabbit lives forever
- ·The population starts as a single newborn pair
- •Every month, each productive pair begets a new pair which will become productive after 2 months old

month	1	2	3	4	5	6	7
rabbits	1	1					

- · A rabbit lives forever
- ·The population starts as a single newborn pair
- •Every month, each productive pair begets a new pair which will become productive after 2 months old

month	1	2	3	4	5	6	7
rabbits	1	1	2				

- · A rabbit lives forever
- ·The population starts as a single newborn pair
- •Every month, each productive pair begets a new pair which will become productive after 2 months old

month	1	2	3	4	5	6	7
rabbits	1	1	2	3			

- · A rabbit lives forever
- ·The population starts as a single newborn pair
- •Every month, each productive pair begets a new pair which will become productive after 2 months old

 F_n = # of rabbit pairs at the beginning of the n^{th} month

month	1	2	3	4	5	6	7
rabbits	1	1	2	3	5		

- · A rabbit lives forever
- ·The population starts as a single newborn pair
- •Every month, each productive pair begets a new pair which will become productive after 2 months old

month	1	2	3	4	5	6	7
rabbits	1	1	2	3	5	8	13



Inductive Definition or Recurrence Relation for the Fibonacci Numbers

Stage 0, Initial Condition, or Base Case: Fib(1) = 1; Fib (2) = 1

Inductive Rule For n>3, Fib(n) = Fib(n-1) + Fib(n-2)

n	0	1	2	3	4	5	6	7
Fib(n)	%	1	1	2	3	5	8	13



Inductive Definition or Recurrence Relation for the Fibonacci Numbers

Stage 0, Initial Condition, or Base Case: Fib(0) = 0; Fib (1) = 1

Inductive Rule For n>1, Fib(n) = Fib(n-1) + Fib(n-2)

n	0	1	2	3	4	5	6	7
Fib(n)	0	1	1	2	3	5	8	13

A (Simple) Continued Fraction Is Any Expression Of The Form:

$$a + \frac{1}{b + \frac{1}{c + \frac{1}{d + \frac{1}{e + \frac{1}{g + \frac{1}{i + \frac{1}{j + \dots}}}}}}}$$

where a, b, c, ... are whole numbers.

A Continued Fraction can have a finite or infinite number of terms.

$$a + \frac{1}{b + \frac{1}{c + \frac{1}{d + \frac{1}{e + \frac{1}{g + \frac{1}{i + \frac{1}{j + \dots}}}}}}}$$

We also denote this fraction by [a,b,c,d,e,f..]

A Finite Continued Fraction

$$2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{2}}}$$

Also denoted [2.3.4.2.0,0,0,0,0,...]

A Infinite Continued Fraction

$$\begin{array}{c}
1 + \frac{1}{2 + \dots}}}}}}} \\
2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \dots}}}} \\
Also denoted [1,2,2,2,\dots]$$

Recursively Defined Form For CF

CF = whole number, or

= whole number
$$+\frac{1}{CF}$$

$$\frac{67}{29} = 2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{2}}}$$

$$\frac{5}{3} = 1 + \frac{1}{1 + \frac{1}{2}}$$

$$\frac{5}{3} = 1 + \frac{1}{1 + \frac{1}{1}}$$

$$1 + \frac{1}{1 + \frac{1}{1}}$$

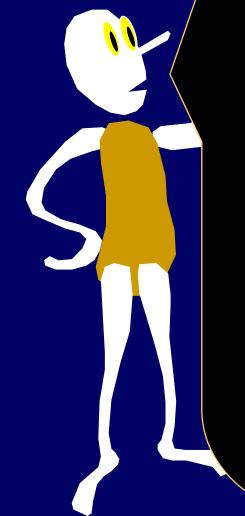
$$= [1,1,1,1,0,0,0,...]$$

$$? = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}}$$

$$\frac{8}{5} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}$$

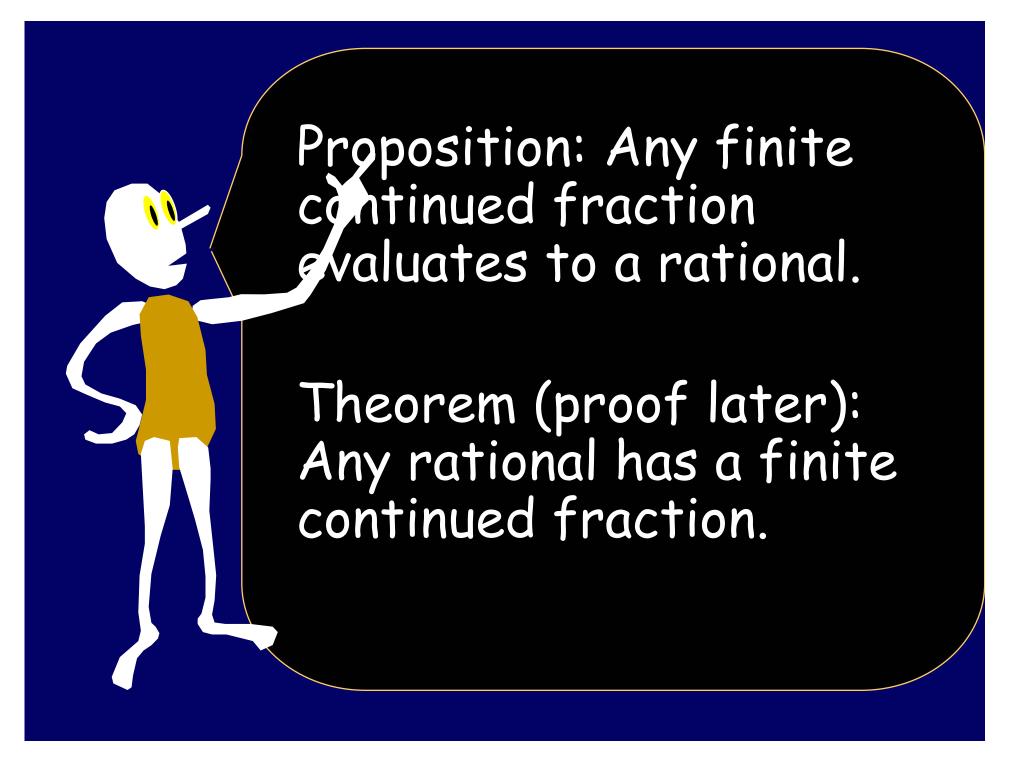
$$1 + \frac{1}{1 + \frac{1}{1}}$$

$$\frac{13}{8} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}}$$



Let $r_1 = [1,0,0,0...]$ $r_2 = [1,1,0,0,0...]$ $r_3 = [1,1,1,0,0...]$ and so on.

> Theorem: $r_n = Fib(n+1)/Fib(n)$



Continued Fraction Representation

$$\sqrt{2} = 1 + \frac{1}{2 + \dots}}}}}}}$$

Quadratic Equations

$$X^2 - 3x - 1 = 0$$

$$X = \frac{3 + \sqrt{13}}{2}$$

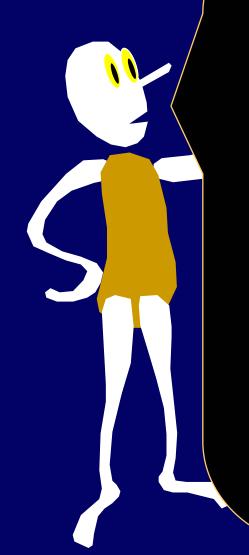
$$X^2 = 3X + 1$$

 $X = 3 + 1/X$

$$X = 3 + 1/X = 3 + 1/[3 + 1/X] = ...$$

Continued Fraction Representation

$$\frac{3+\sqrt{13}}{2} = 3 + \frac{1}{3+\frac{1}{3+\frac{1}{3+\frac{1}{3+\frac{1}{3+\frac{1}{3+\frac{1}{3+\dots}}}}}}}$$



Conclusion: Any quadratic solution has a periodic continued fraction.

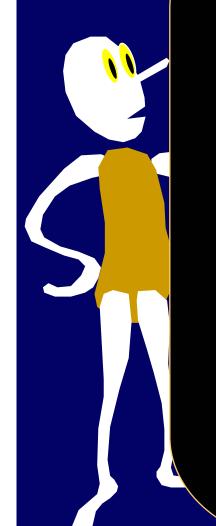
Converse (homework):
Any periodic continued
fraction is the solution
of a quadratic equation.

Continued Fraction Representation

$$e-1=1+\frac{1}{1+\frac{1}{2+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\dots}}}}}}}$$

Continued Fraction Representation

$$\pi = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}}}}}$$

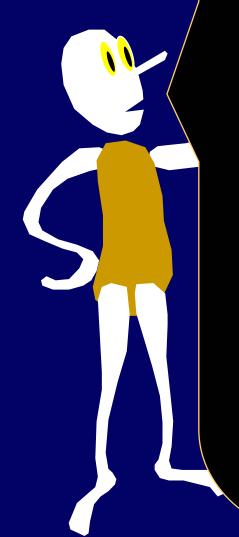


What a cool representation!

Finite CF = Rationals

Periodic CF = Quadratic Roots

And some numbers reveal hidden regularity.

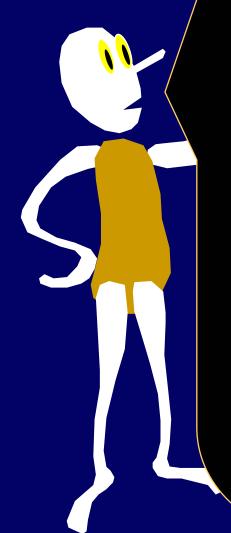


And there is more! Let $\alpha =$ $[a_1, a_2, a_3, ...]$ be a CF.

Define $C_1 = [a_1,0,0,0,0,0...]$ Define $C_2 = [a_1,a_2,0,0,0...]$ Define $C_3 = [a_1,a_2,a_3,0...]$ and so on. Let $\alpha = [a_1, a_2, a_3, ...]$ be a CF.

 C_k is called the k^{th} convergent of α

where α is the limit of the sequence C_1 , C_2 , C_3 ...



Define a rational p/q to be a "best approximator" to a real α , if no rational number of smaller denominator comes closer.



Continued Fraction Representation

$$C_1 = 3$$

$$C_2 = 22/7$$

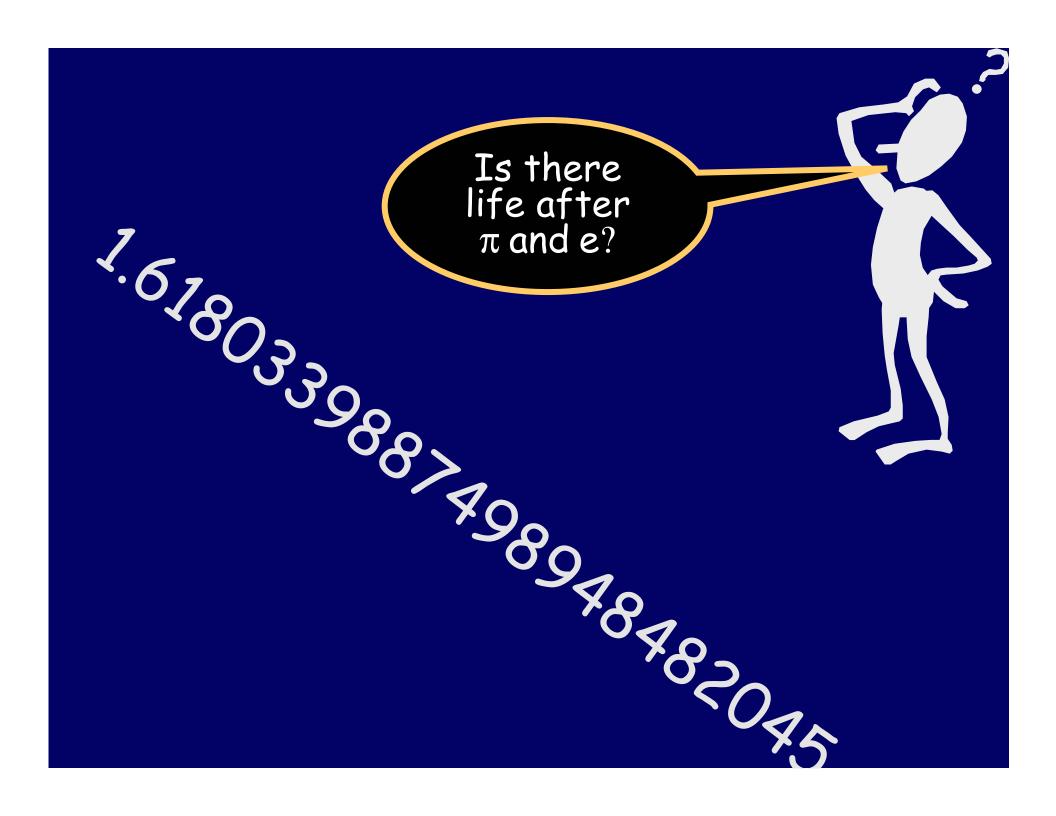
$$C_3 = 333/106$$

$$C_4 = 355/113$$

$$C_5$$
= 103993/33102

$$C_6 = 104348/33215$$

$$\pi = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \frac$$





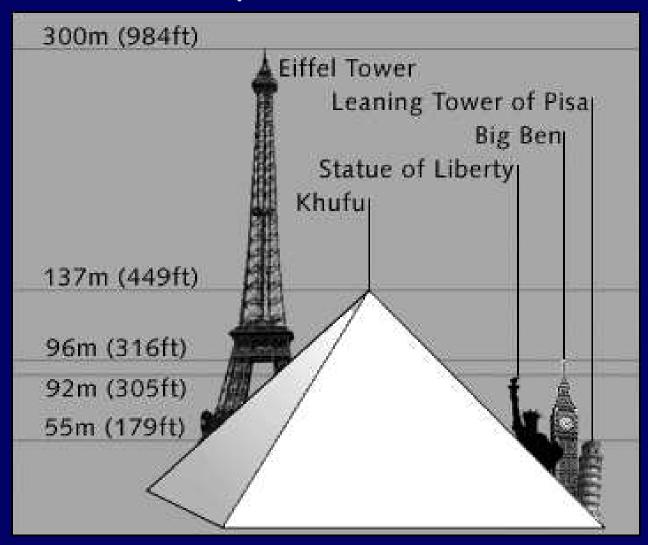
Khufu

·2589-2566 B.C.

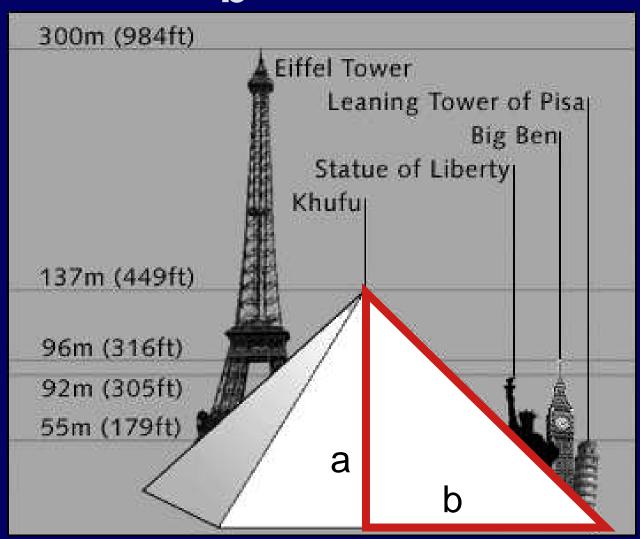
2,300,000 blocksaveraging 2.5 tons each



Great Pyramid at Gizeh



$$\frac{a}{b} = 1.618$$



The ratio of the altitude of a face to half the base

Golden Ratio Divine Proportion

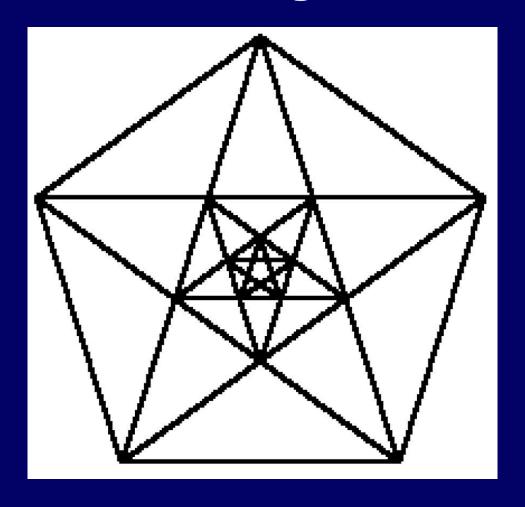
 ϕ = 1.6180339887498948482045...

"Phi" is named after the Greek sculptor <u>Phi</u>dias

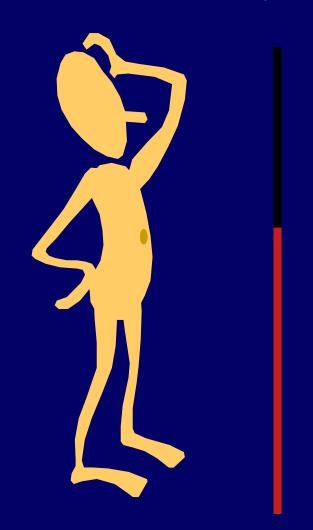
Parthenon, Athens (400 B.C.)



Pentagon



Ratio of height of the person to the height of a person's navel



Definition of ϕ (Euclid)

Ratio obtained when you divide a line segment into two unequal parts such that the ratio of the whole to the larger part is the same as the ratio of the larger to the smaller.

$$\phi = \frac{AC}{AB} = \frac{AB}{BC}$$

$$\phi^2 = \frac{AC}{BC}$$

$$\phi^2 - \phi = \frac{AC}{BC} - \frac{AB}{BC} = \frac{BC}{BC} = 1$$

$$\phi^2 - \phi - 1 = 0$$

Definition of ϕ (Euclid)

Ratio obtained when you divide a line segment into two unequal parts such that the ratio of the whole to the larger part is the same as the ratio of the larger to the smaller.

$$\phi^2 - \phi - 1 = 0$$

$$\phi = \frac{\sqrt{5} + 1}{2}$$

The Divine Quadratic

$$\phi^2 - \phi - 1 = 0$$

$$\phi = \frac{\sqrt{5} + 1}{2}$$

$$\phi = 1 + 1/\phi$$

Expanding Recursively

$$\phi = 1 + \frac{1}{\phi}$$

Expanding Recursively

$$\phi = 1 + \frac{1}{\phi}$$

$$= 1 + \frac{1}{1 + \frac{1}{\phi}}$$

Expanding Recursively

$$\phi = 1 + \frac{1}{\phi}$$

$$= 1 + \frac{1}{1 + \frac{1}{\phi}}$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\phi}}}$$

$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\phi}}}$$

Continued Fraction Representation

$$\phi = 1 + \frac{1}{1 + \dots}}}}}}}$$

Continued Fraction Representation

$$\frac{1+\sqrt{5}}{2} = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\dots}}}}}}}$$

We already know that the convergents of this CF have the form Fib(n+1)/Fib(n)

$$\frac{1+\sqrt{5}}{2} = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\dots}}}}}}}$$

Continued Fraction Representation

$$\frac{1+\sqrt{5}}{2} = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\dots}}}}}}} = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\dots}}}$$

$$\lim_{n o\infty}rac{F_{\mathrm{n}}}{F_{\mathrm{n-1}}}=\varphi=rac{1+\sqrt{5}}{2}$$

1,1,2,3,5,8,13,21,34,55,....

```
2/1 = 2

3/2 = 1.5

5/3 = 1.666...

8/5 = 1.6

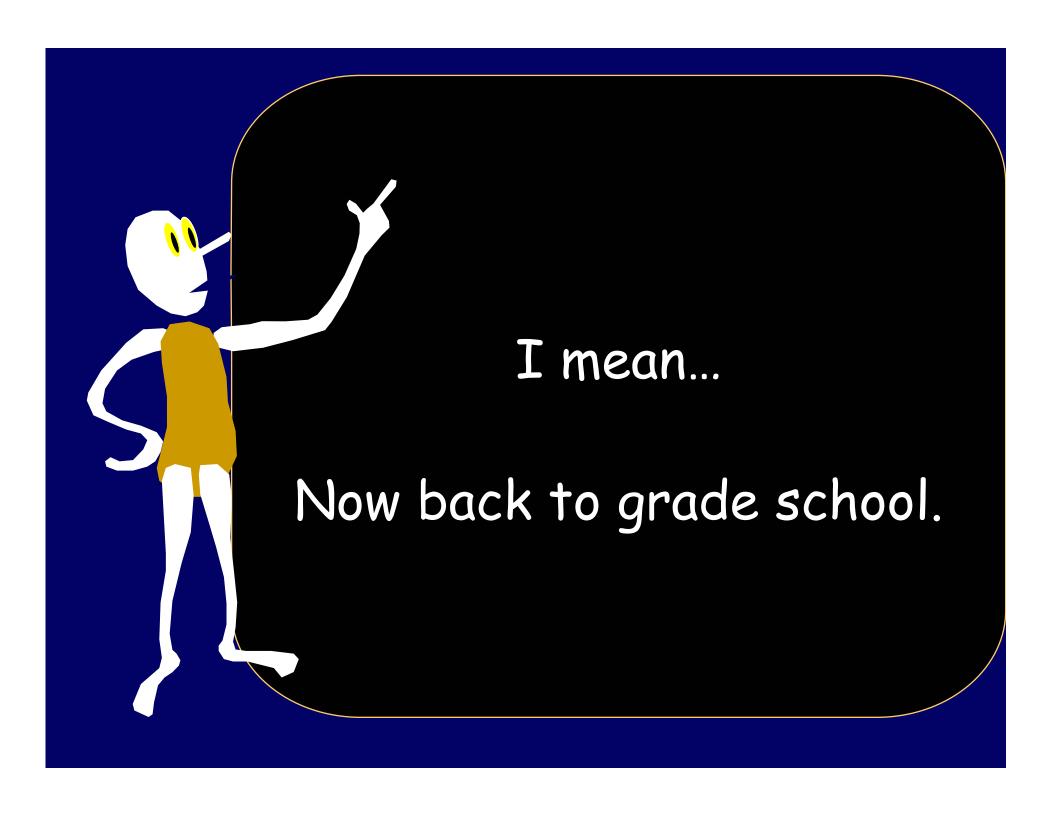
13/8 = 1.625

21/13= 1.6153846...

34/21= 1.61904...
```

 ϕ = 1.6180339887498948482045





Grade School GCD algorithm

Definition: GCD(A,B) is the greatest common divisor. I.e., the largest number that goes evenly into both A and B.,

What is the GCD of 12 and 18? $12 = 2^2 * 3$ $18 = 2*3^2$

Common factors: 21 and 31

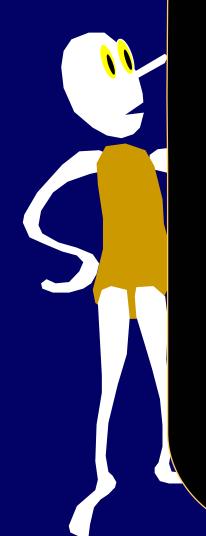
Answer: 6

Grade School GCD algorithm

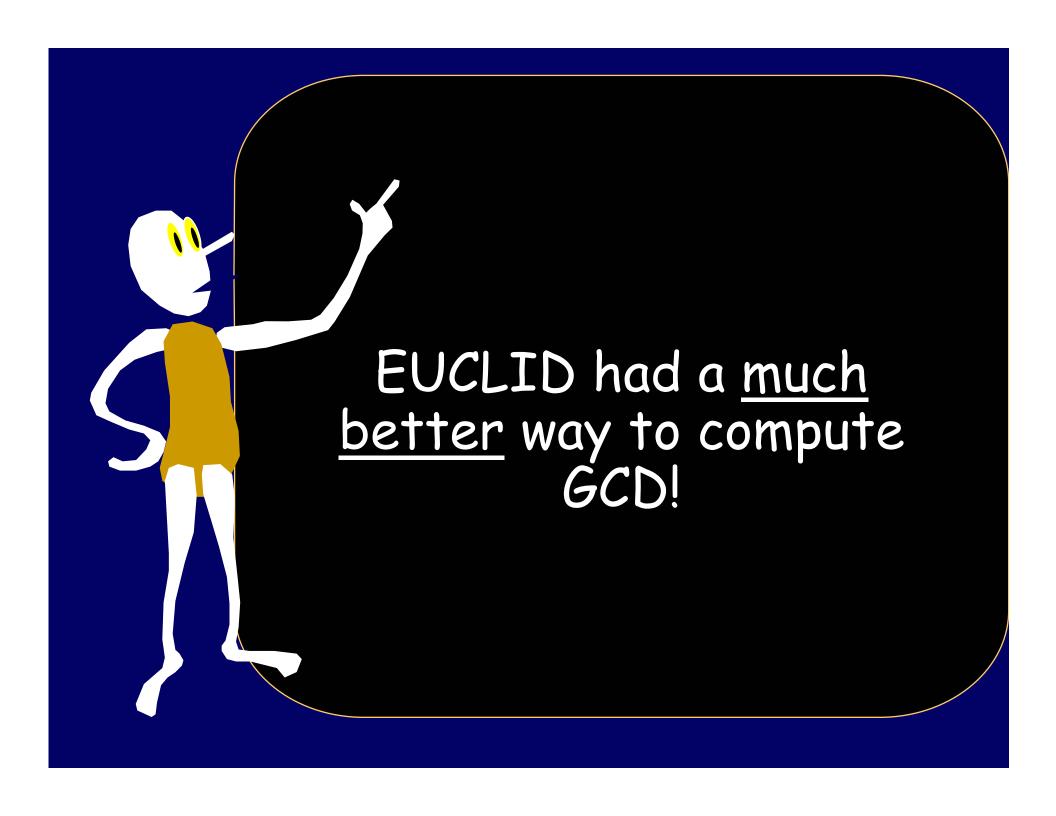
Definition: GCD(A,B) is the greatest common divisor. I.e., the largest number that goes evenly into both A and B.,

Factor A into prime powers. Factor B into prime powers.

Create GCD by multiplying together each common prime raised to the highest power that goes into both A and B.



The problem with the grade school method is that it requires factoring A and B. No one knows a particularly fast way to factor a number into parts.



Ancient Recursion Euclid's GCD algorithm

EUCLID(A,B) // requires $A \ge B \ge 0$ If B=0 then Return A else Return Euclid(B, A mod B)

GCD(67,29) = 1

```
EUCLID(A,B) // requires A \ge B \ge 0
If B=0 then Return A
else Return Euclid(B, A mod B)
```

```
Euclid(67,29) 67 mod 29 = 9

Euclid(29,9) 29 mod 9 = 2

Euclid(9,2) 9 mod 2 = 1

Euclid(2,1) 2 mod 1 = 0

Euclid(1,0) outputs 1
```

Euclid's GCD Correctness

```
EUCLID(A,B) // requires A \ge B \ge 0
If B=0 then Return A
else Return Euclid(B, A mod B)
GCD(A,B) = GCD(B, A \text{ mod B})
```

d|A and admin/: Permission denied. $\leftarrow \rightarrow$ d|B and d| (A - kB)

The set of common divisors of A, B equals

```
EUCLID(A,B)
                        // requires A≥B≥0
If B=0 then Return A
                  Return Euclid (B, A mod B)
         else
  A mod B < \frac{1}{2} A
  Proof:
  If B > \frac{1}{2} A then A mod B = A - B
                                              \langle \frac{1}{2} A
                                              \langle \frac{1}{2} A
  If B < \frac{1}{2} A then ANY X Mod B
  If B = \frac{1}{2} A then A mod B = 0
```

```
EUCLID(A,B) // requires A \ge B \ge 0
If B=0 then Return A
else Return Euclid(B, A mod B)
```

GCD(A,B) calls GCD(B, A mod B)



```
EUCLID(A,B) // requires A≥B≥0

If B=0 then Return A

else Return Euclid(B, A mod B)
```

GCD(A,B) calls $GCD(B, \langle \frac{1}{2}A)$

```
EUCLID(A,B) // requires A \ge B \ge 0
If B=0 then Return A
else Return Euclid(B, A mod B)
```

GCD(A,B) calls $GCD(B, \langle \frac{1}{2}A)$

which calls $GCD(\langle \frac{1}{2}A, B \mod \langle \frac{1}{2}A \rangle)$



```
EUCLID(A,B) // requires A≥B≥0

If B=0 then Return A

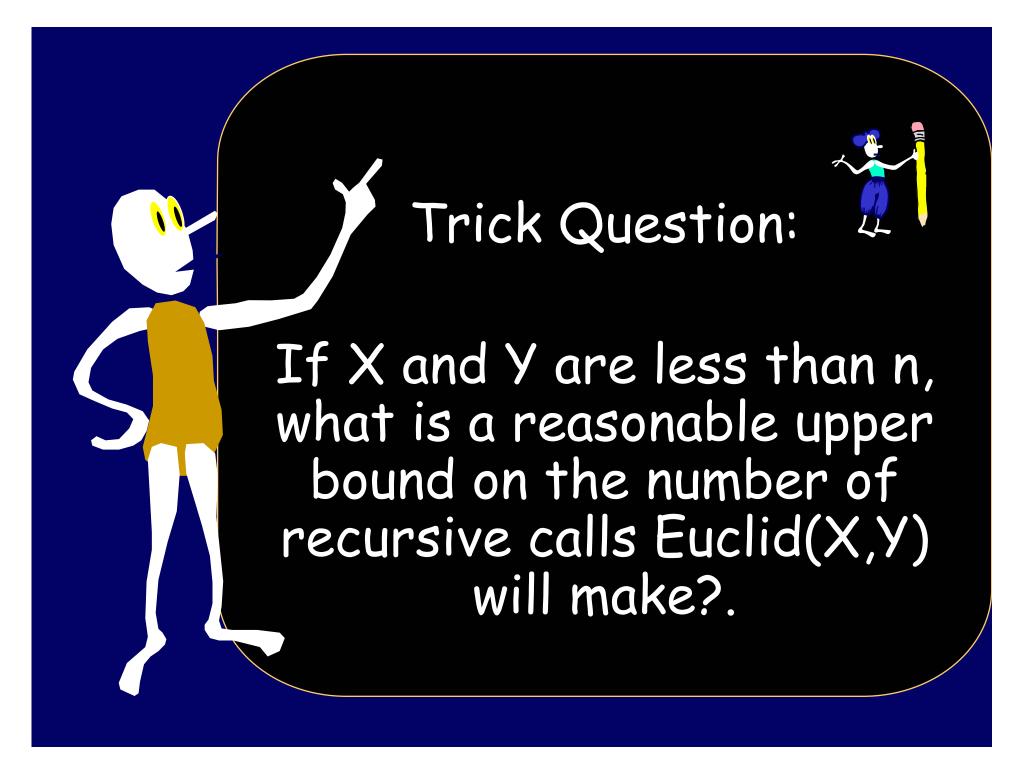
else Return Euclid(B, A mod B)
```

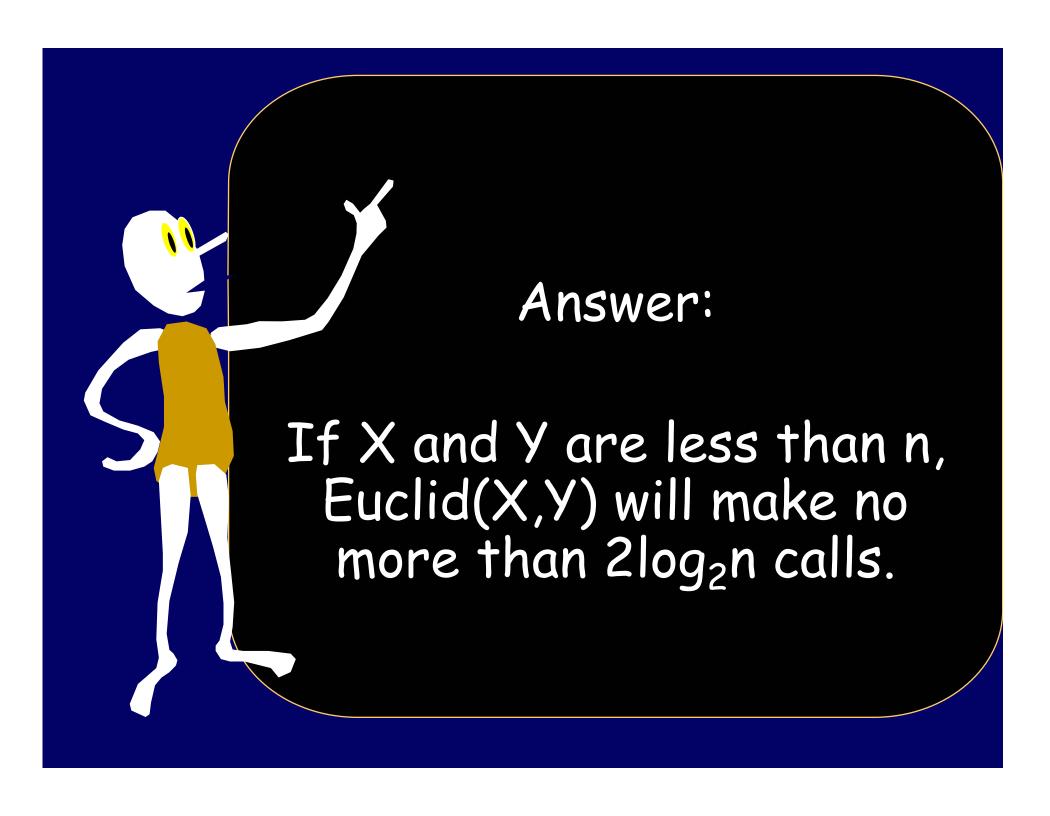
Every two recursive calls, the input numbers drop by half.

EUCLID(A,B) // requires $A \ge B \ge 0$ If B=0 then Return A else Return Euclid(B, A mod B)

Theorem:

If two input numbers have an n bit binary representation, Euclid Algorithm will not take more than 2n calls to terminate.





EUCLID(A,B) // requires $A \ge B \ge 0$ If B=0 then Return A else Return Euclid(B, A mod B)

```
Euclid(67,29) 67 - 2*29 = 67 mod 29 = 9

Euclid(29,9) 29 - 3*9 = 29 mod 9 = 2

Euclid(9,2) 9 - 4*2 = 9 mod 2 = 1

Euclid(2,1) 2 - 2*1 = 2 mod 1 = 0

Euclid(1,0) outputs 1
```

Let <r,s> denote the number r*67 + s*29. Calculate all intermediate values in this representation.

```
67=<1,0> 29=<0,1>
Euclid(67,29) 9=<1,0> - 2*<0,1> 9 =<1,-2>
Euclid(29,9) 2=<0,1> - 3*<1,-2> 2=<-3,7>
Euclid(9,2) 1=<1,-2> - 4*<-3,7> 1=<13,-30>
Euclid(2,1) 0=2 - 2*1 2=<-3,7>
```

1 = 13*67 - 30*29

Euclid(1,0) outputs

Euclid's Extended GCD algorithm

Input: X,Y

Output: r,s,d such that rX+sY = d = GCD(X,Y)

67=<1,0> 29=<0,1> Euclid(67,29) 9=67 - 2*29 9=<1,-2> Euclid(29,9) 2=29 - 3*9 2=<-3,7> Euclid(9,2) 1=9 - 4*2 1=<13,-30> Euclid(2,1) 0=2 - 2*1 2=<-3,7>

Euclid(1,0) outputs 1 = 13*67 - 30*29

Euclid's GCD algorithm

EUCLID(A,B)

// requires A≥B≥0

If B=0 then

Return A

else

Return Euclid(B, A mod B)

T(m) = the largest number of recursive calls that Euclid makes on any input pair with B=m

Euclid's GCD algorithm

EUCLID(A,B)

// requires A≥B≥0

If B=0 then

Return A

else

Return Euclid(B, A mod B)

We already know that $T(m) \le 2\log_2 m$

Lame: $T(F_k) = k$ [1845]

EUCLID(A,B) // requires $A \ge B \ge 0$

If B=0 then Return A

else Return Euclid(B, A mod B)

First we show that $T(F_k) \ge k$

```
Euclid(F_{k+1},F_k) will call ...
Euclid(F_k,F_{k-1}) will call ...
Euclid(F_{k-1},F_{k-2}) will call ...
```

Euclid(F_2,F_1) will call ... Euclid(F_1,F_0) Hence $T(F_k) \ge k$

Corollary: $T(F_k) \ge k$

We have: $T(F_k) \ge k$

We now want to show: $T(F_k) \leq k$

We prove $T(F_k) \le k$ it by proving that: Euclid(A,B) makes k calls \Rightarrow $A \ge F_{k+1}$ and $B \ge F_k$

We proceed by induction on k, starting at k=2.

Euclid(A,B) makes k calls
$$\Rightarrow$$

 $A \ge F_{k+1}$ and $B \ge F_k$

$$\forall$$
 k \geq 2, Euclid(A,B) makes k calls \Rightarrow A \geq F_{k+1} and B \geq F_k

Base: k=2

B > 0 since EUCLID doesn't halt right away.

$$B \ge 1$$
 and $A \ge 2$
 $B \ge F_2$ $A \ge F_3$

\forall k \geq 2, Euclid(A,B) makes k calls \Rightarrow A \geq F_{k+1} and B \geq F_k

Assume we have proved the hypothesis up to k-1

K>2 means EUCLID(A, B) will call

EUCLID(B, A mod B) which will make k-1 recursive calls

By induction: $B \ge F_k$ and A mod $B \ge F_{k-1}$

\forall k \geq 2, Euclid(A,B) makes k calls \Rightarrow A \geq F_{k+1} and B \geq F_k

By induction: $B \ge F_k$ and A mod $B \ge F_{k-1}$

$$B + (A \mod B) \ge F_k + F_{k-1} \ge F_{k+1}$$

$$A \ge B + (A \mod B)$$

Thus:
$$A \ge F_{k+1}$$

\forall k \geq 2, Euclid(A,B) makes k calls \Rightarrow A \geq F_{k+1} and B \geq F_k

Corollary:

If $T(m) \ge k$ then $m \ge F_k$

Hence, $T(F_k) = K$ for all k.

And a worst case input for requiring k steps in the pair F_{k+1} and F_{k} .

Continued fraction representation of a standard fraction

$$\frac{67}{29} = 2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{2}}}$$

$$67/29 = 2$$
 with remainder $9/29 = 2 + 1/(29/9)$

$$\frac{67}{29} = 2 + \frac{1}{\frac{29}{9}} = 2 + \frac{1}{3 + \frac{2}{9}} = + \frac{1}{3 + \frac{1}{4 + \frac{1}{2}}}$$

A Representational Correspondence

$$\frac{67}{29} = 2 + \frac{1}{\frac{29}{9}} = 2 + \frac{1}{3 + \frac{2}{9}} 2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{2}}}$$

Euclid(67,29) 67 div 29 = 2 Euclid(29,9) 29 div 9 = 3 Euclid(9,2) 9 div 2 = 4 Euclid(2,1) 2 div 1 = 2 Euclid(1,0)

Euclid's GCD = Continued Fractions

$$\frac{A}{B} = \left\lfloor \frac{A}{B} \right\rfloor + \frac{1}{B}$$

$$A \mod B$$

Euclid(A,B) = Euclid($B,A \mod B$) Stop when B=0

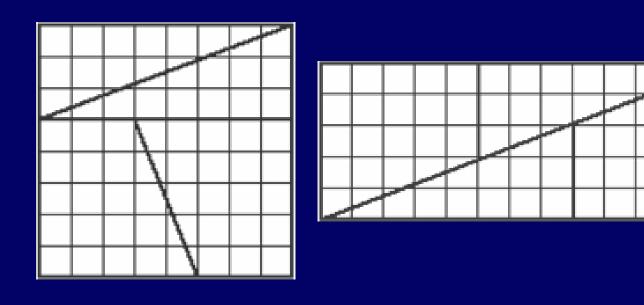
Theorem: All fractions have finite continuous fraction expansions

$$\frac{A}{B} = \left\lfloor \frac{A}{B} \right\rfloor + \frac{1}{B}$$

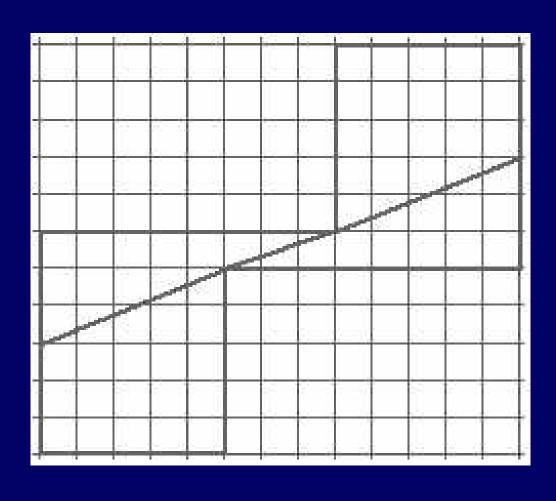
$$A \mod B$$

Euclid(A,B) = Euclid($B,A \mod B$) Stop when B=0

Fibonacci Magic Trick



Another Trick!



REFERENCES

Continued Fractions, C. D. Olds

The Art Of Computer Programming, Vol 2, by Donald Knuth