Great Theoretical Ideas In Computer Science

Steven Rudich

CS 15-251 Spring 2004

Lecture 6 Jan 29, 2004

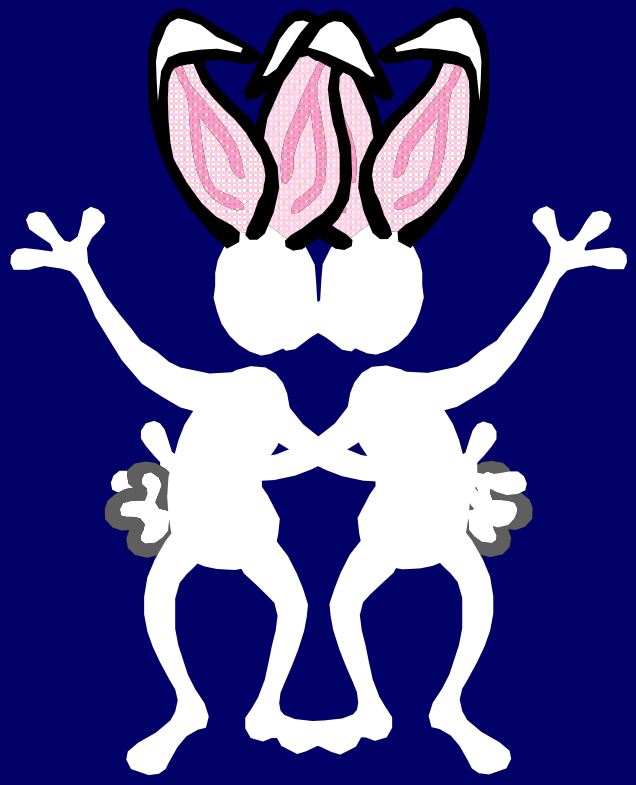
Carnegie Mellon University

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

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

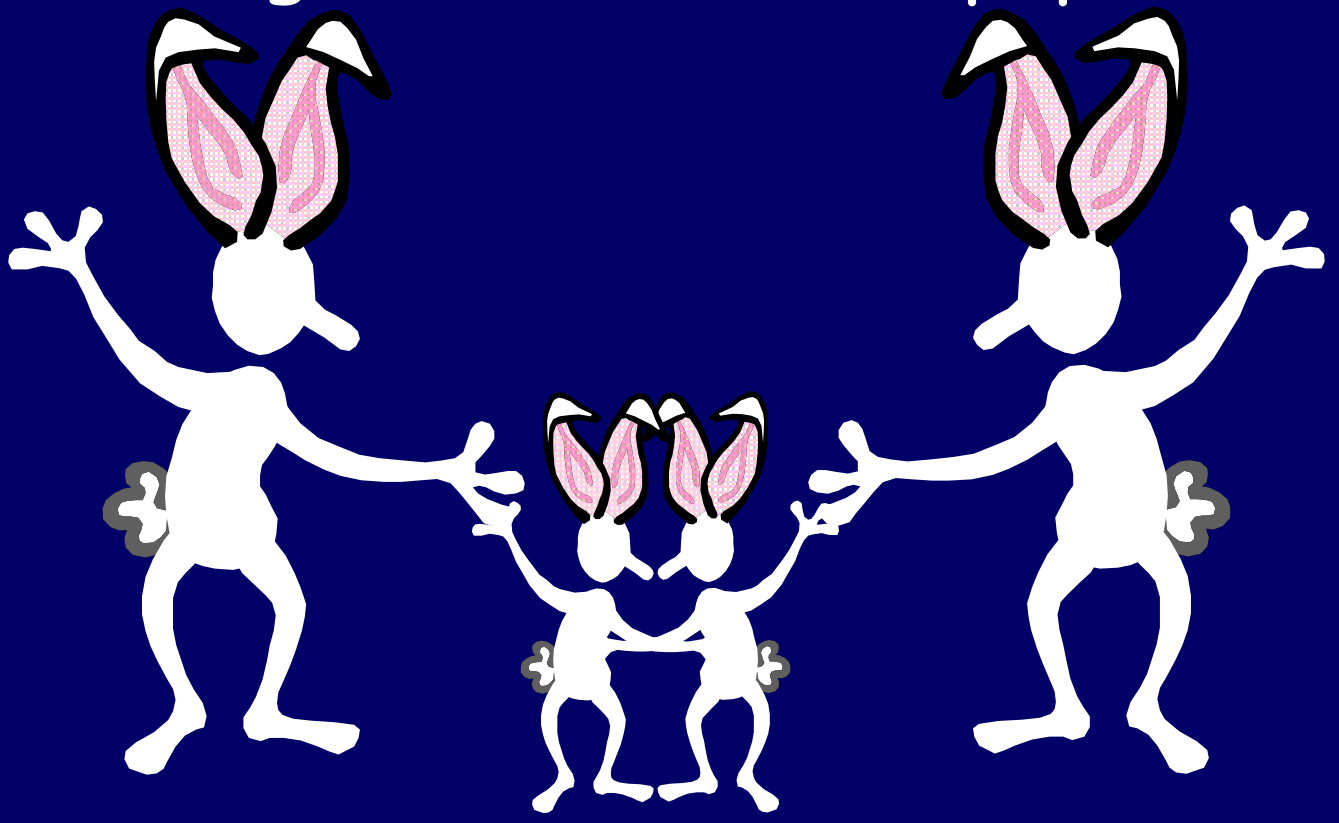
Leonardo Fibonacci

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



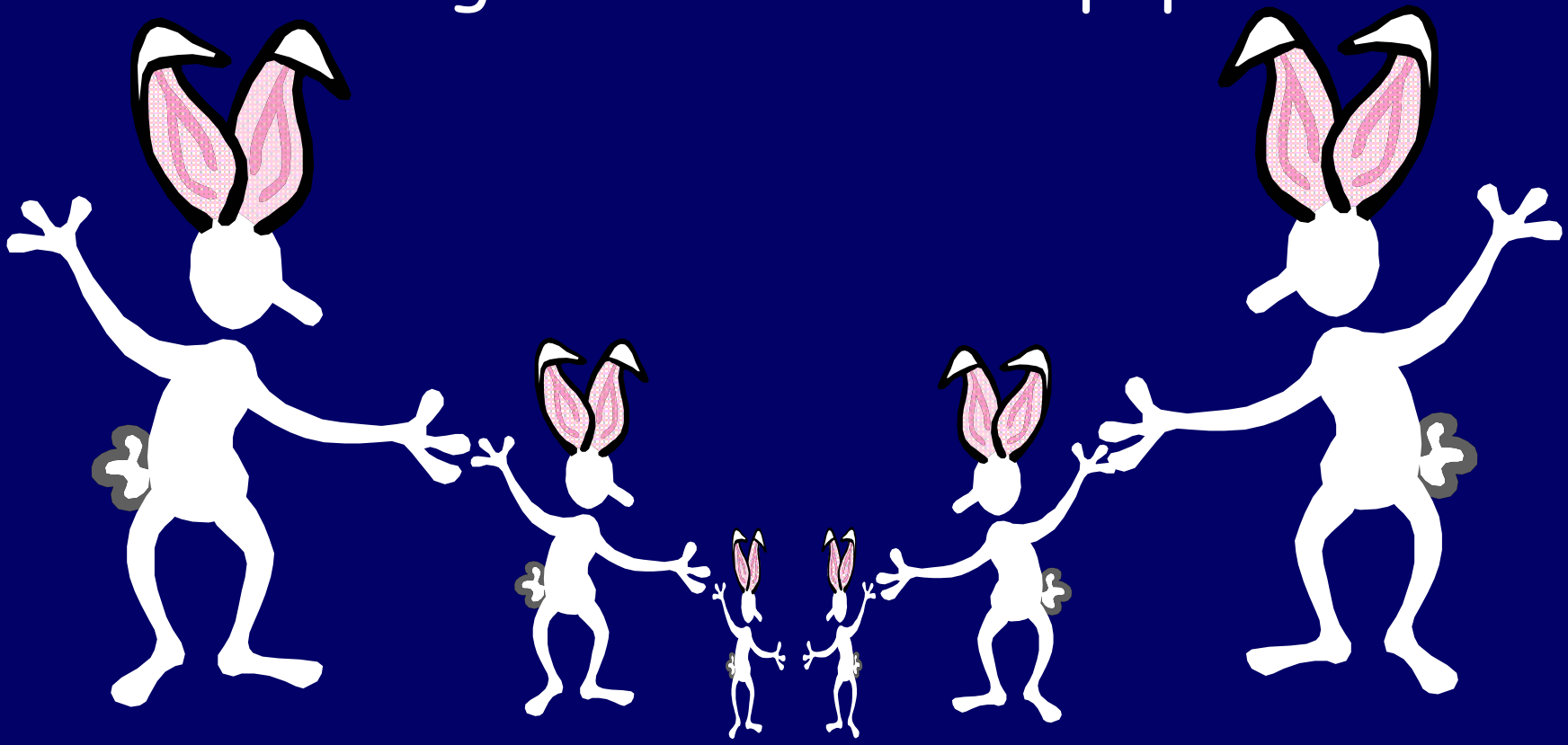
Leonardo Fibonacci

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.



The rabbit reproduction model

- 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							

The rabbit reproduction model

- 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						

The rabbit reproduction model

- 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					

The rabbit reproduction model

- 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				

The rabbit reproduction model

- 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			

The rabbit reproduction model

- 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		

The rabbit reproduction model

- 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	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)

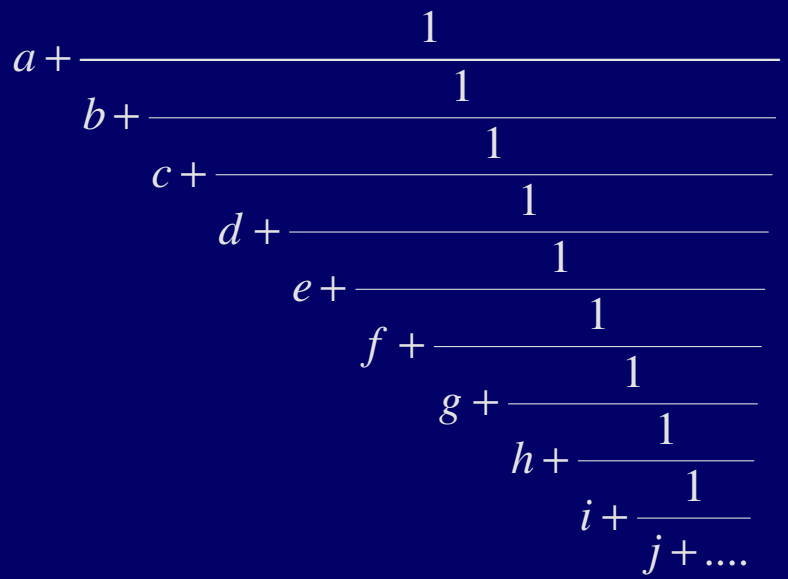
n	0	1	2	3	4	5	6	7
Fib(n)	0	1	1	2	3	5	8	13

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

$$a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{d + \cfrac{1}{e + \cfrac{1}{f + \cfrac{1}{g + \cfrac{1}{h + \cfrac{1}{i + \cfrac{1}{j + \ldots.}}}}}}}}}$$

where a, b, c, … are whole numbers.

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



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

A Finite Continued Fraction

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

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

A Infinite Continued Fraction

Also denoted [1,2,2,2,....

Recursively Defined Form For CF

$$\text{CF} = \text{whole number, or}$$

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

Ancient Greek Representation: Continued Fraction Representation

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

Ancient Greek Representation: Continued Fraction Representation

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

Ancient Greek Representation: Continued Fraction Representation

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

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

Ancient Greek Representation: Continued Fraction Representation

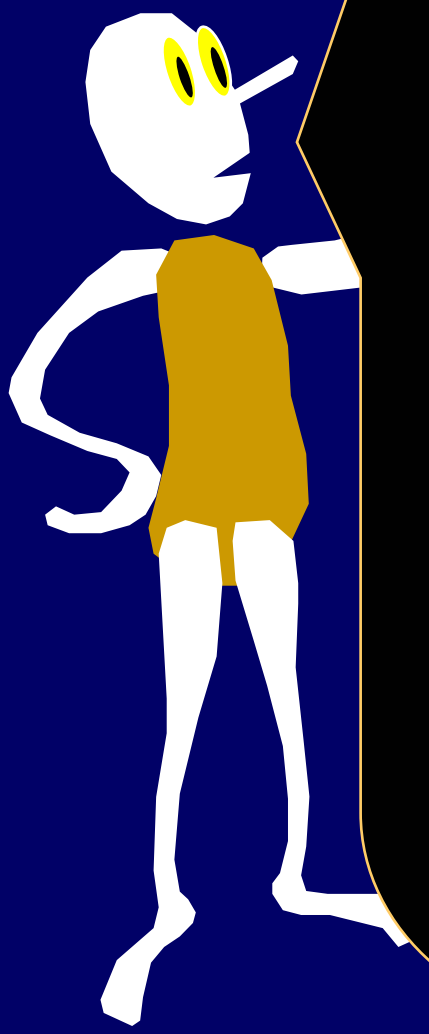
$$? = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}$$

Ancient Greek Representation: Continued Fraction Representation

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

Ancient Greek Representation: Continued Fraction Representation

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



Let r_1 = [1,0,0,0..]

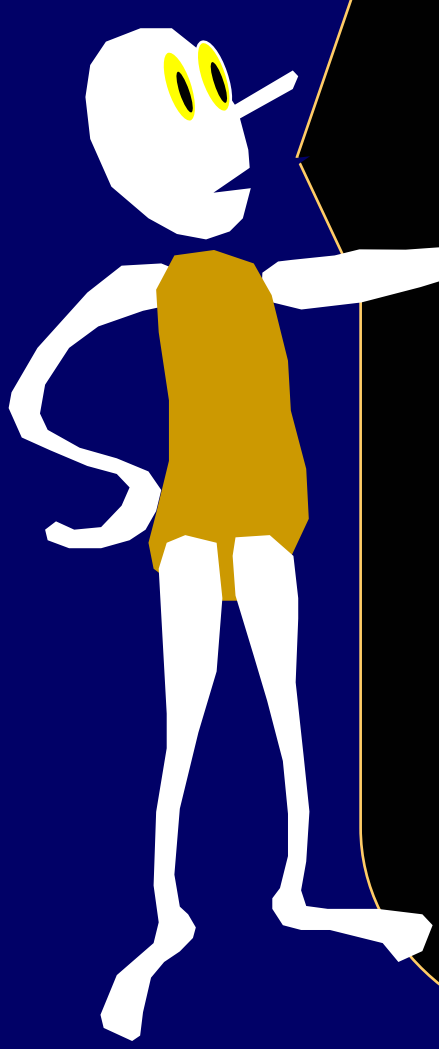
r_2 = [1,1,0,0,0....

r_3 = [1,1,1,0,0...

and so on.

Theorem:

r_n = Fib(n+1)/Fib(n)



Proposition: Any finite continued fraction evaluates to a rational.

Theorem (proof later): Any rational has a finite continued fraction.

Continued Fraction Representation

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}}}}}}}}$$

Quadratic Equations

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

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

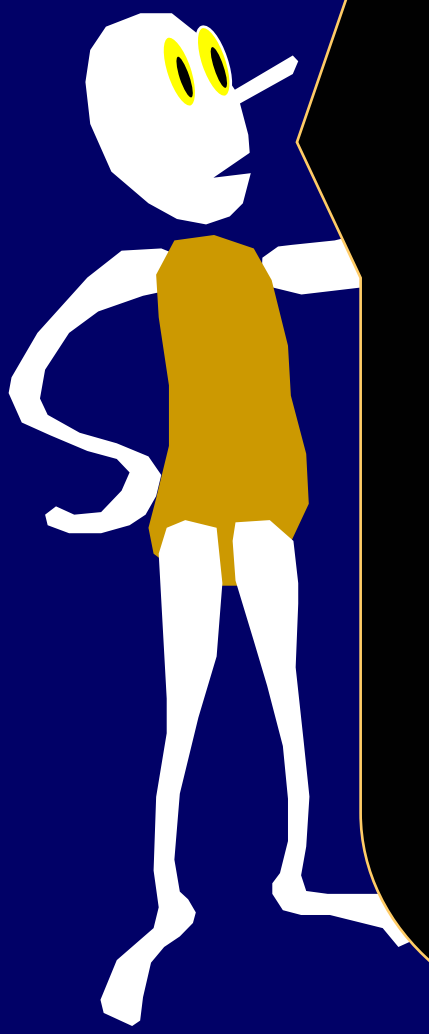
$X^2 = 3X + 1$

$X = 3 + 1/X$

$X = 3 + 1/X = 3 + 1/[3 + 1/X] = \ldots$

Continued Fraction Representation

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



Conclusion: Any quadratic solution has a periodic continued fraction.

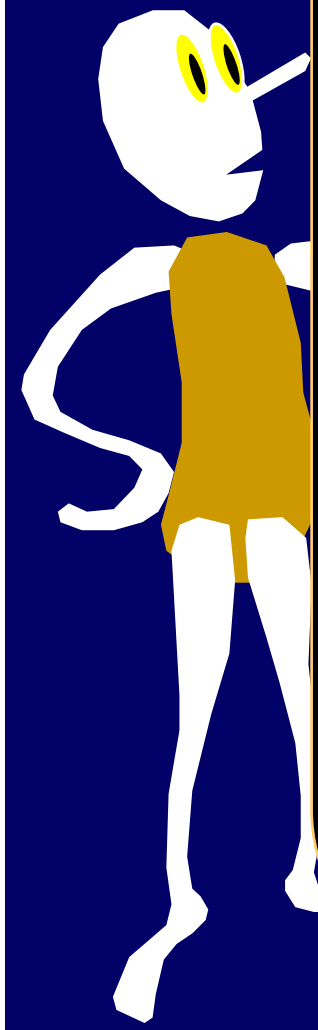
Converse (homework): Any periodic continued fraction is the solution of a quadratic equation.

Continued Fraction Representation

$$e-1=1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6+\cfrac{1}{1+\ldots}}}}}}}}}$$

Continued Fraction Representation

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \ldots}}}}}}}}}$$

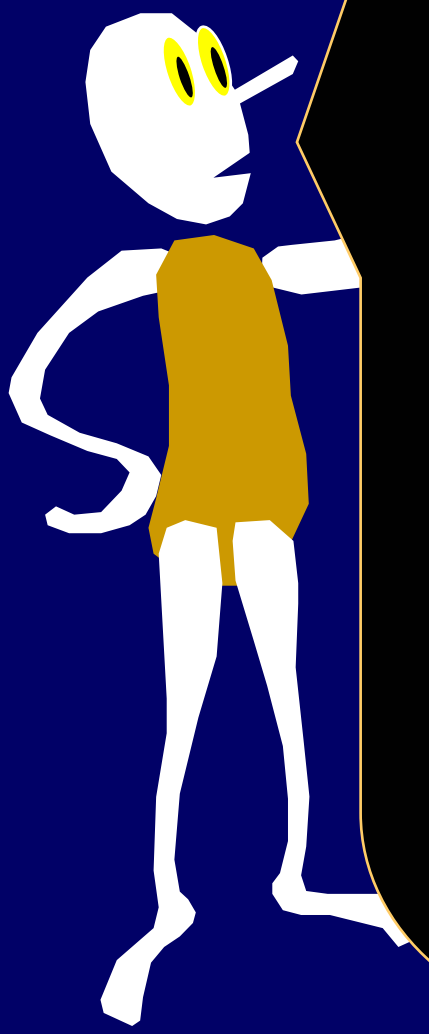


What a cool representation!

Finite CF = Rationals

Periodic CF = Quadratic Roots

And some numbers reveal hidden regularity.

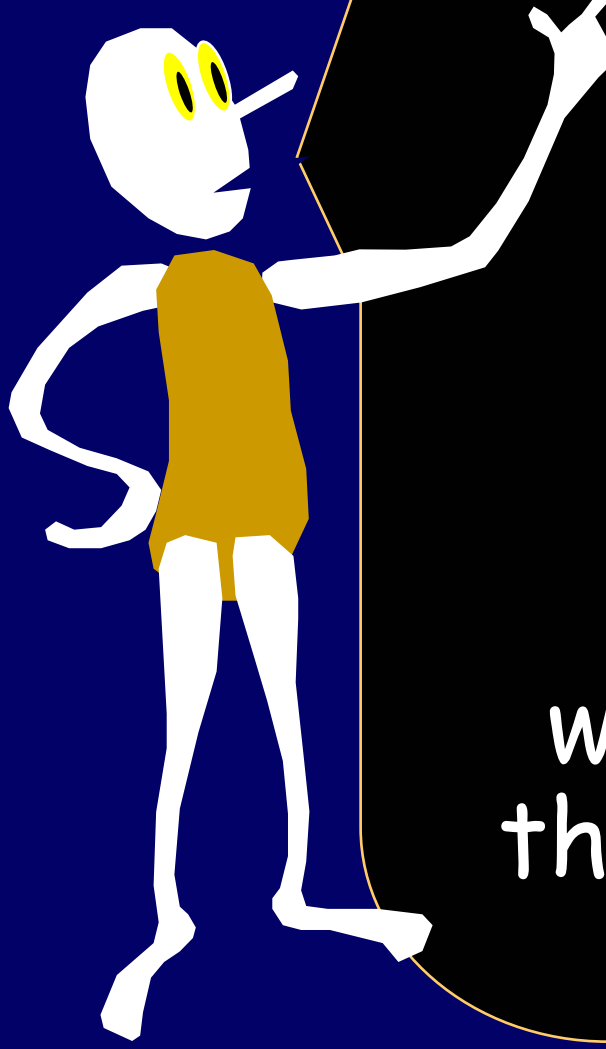


And there is more!

Let α =
$[a_1, a_2, a_3, ..]$ be a CF.

Define $C_1 = [a_1,0,0,0,0..]$
Define $C_2 = [a_1,a_2,0,0,0..]$
Define $C_3 = [a_1,a_2,a_3,0..]$

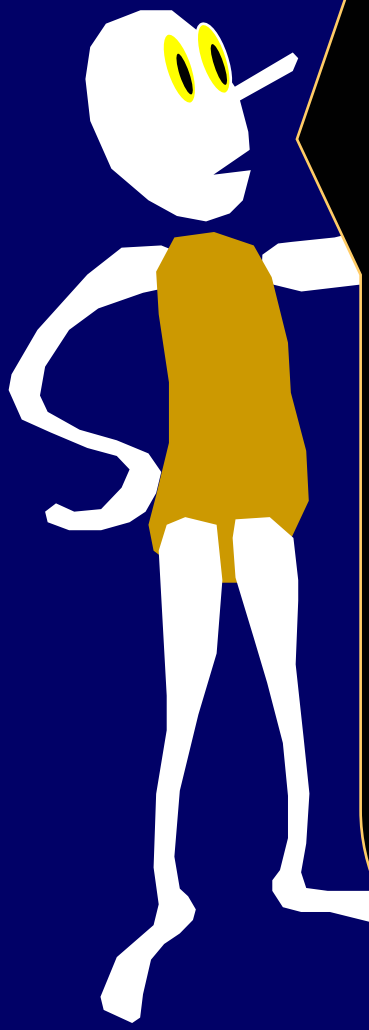
and so on.



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.

For any CF representation of α, each convergent of the CF is a "best approximator" for α !

Continued Fraction Representation

$C_1 = 3$

$C_2 = 22/7$

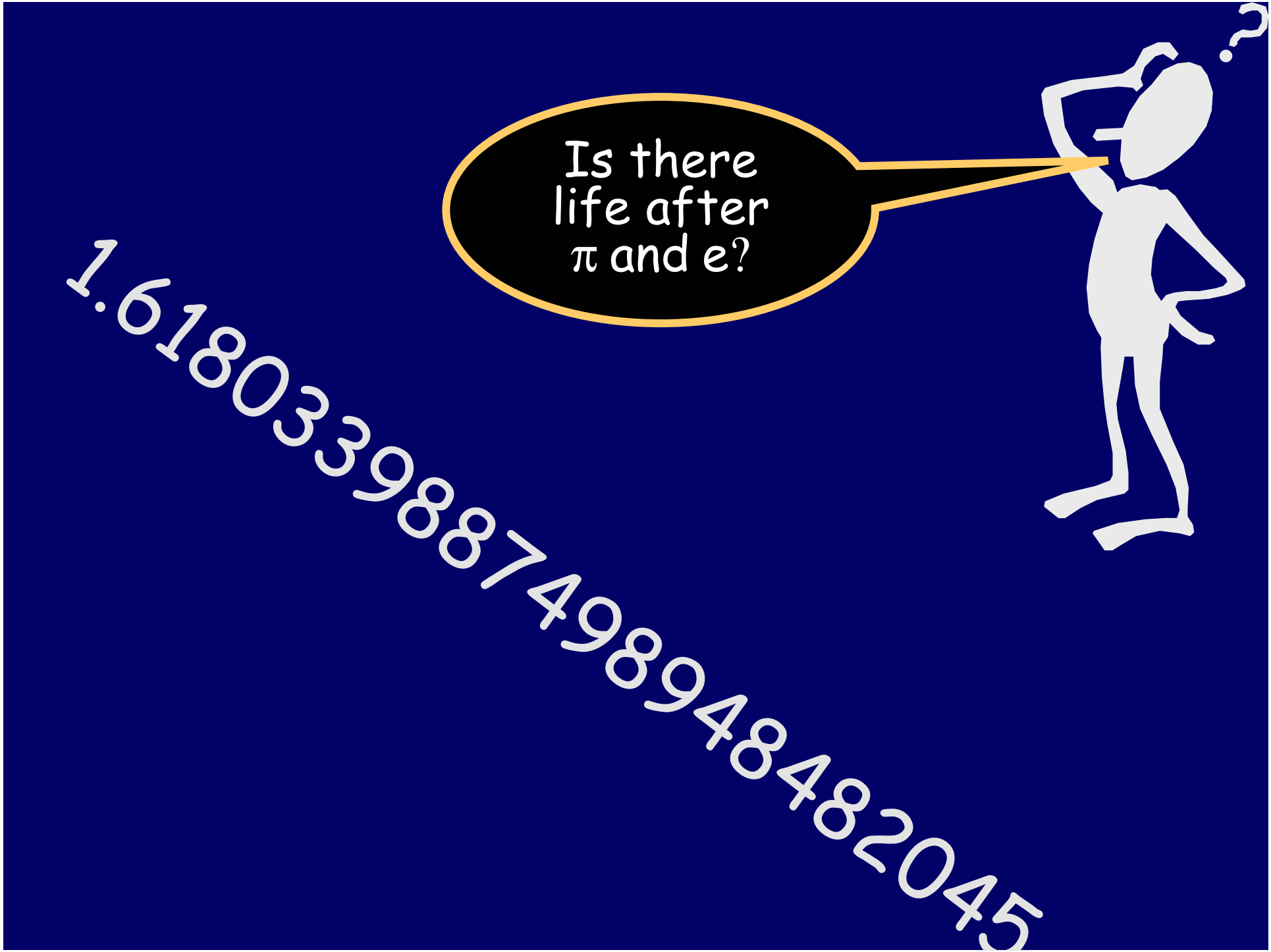
$C_3 = 333/106$

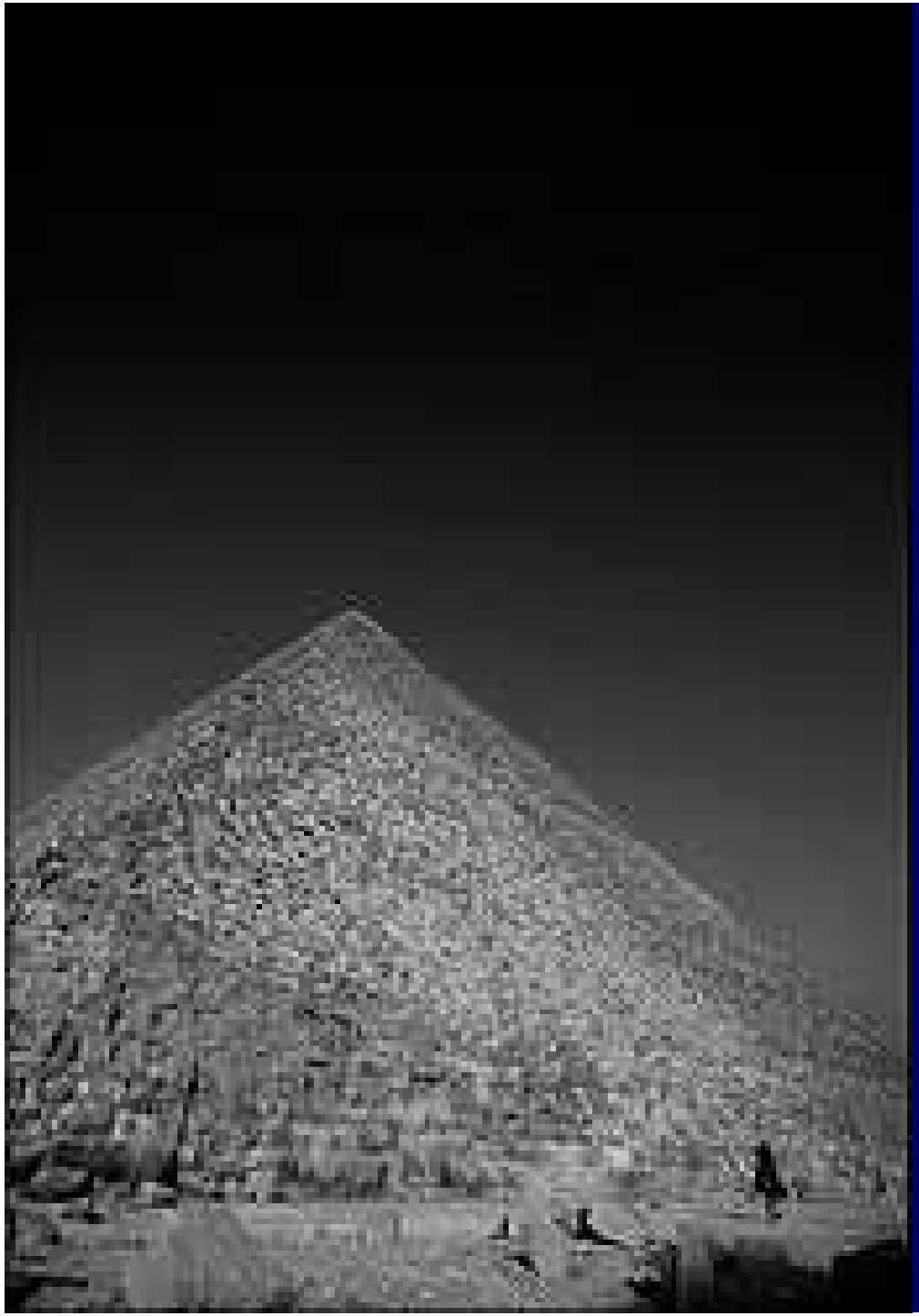
$C_4 = 355/113$

$C_5 = 103993/33102$

$C_6 = 104348/33215$

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \ldots}}}}}}}}}}$$


Is there life after π and e?
1.6180339887498948482045

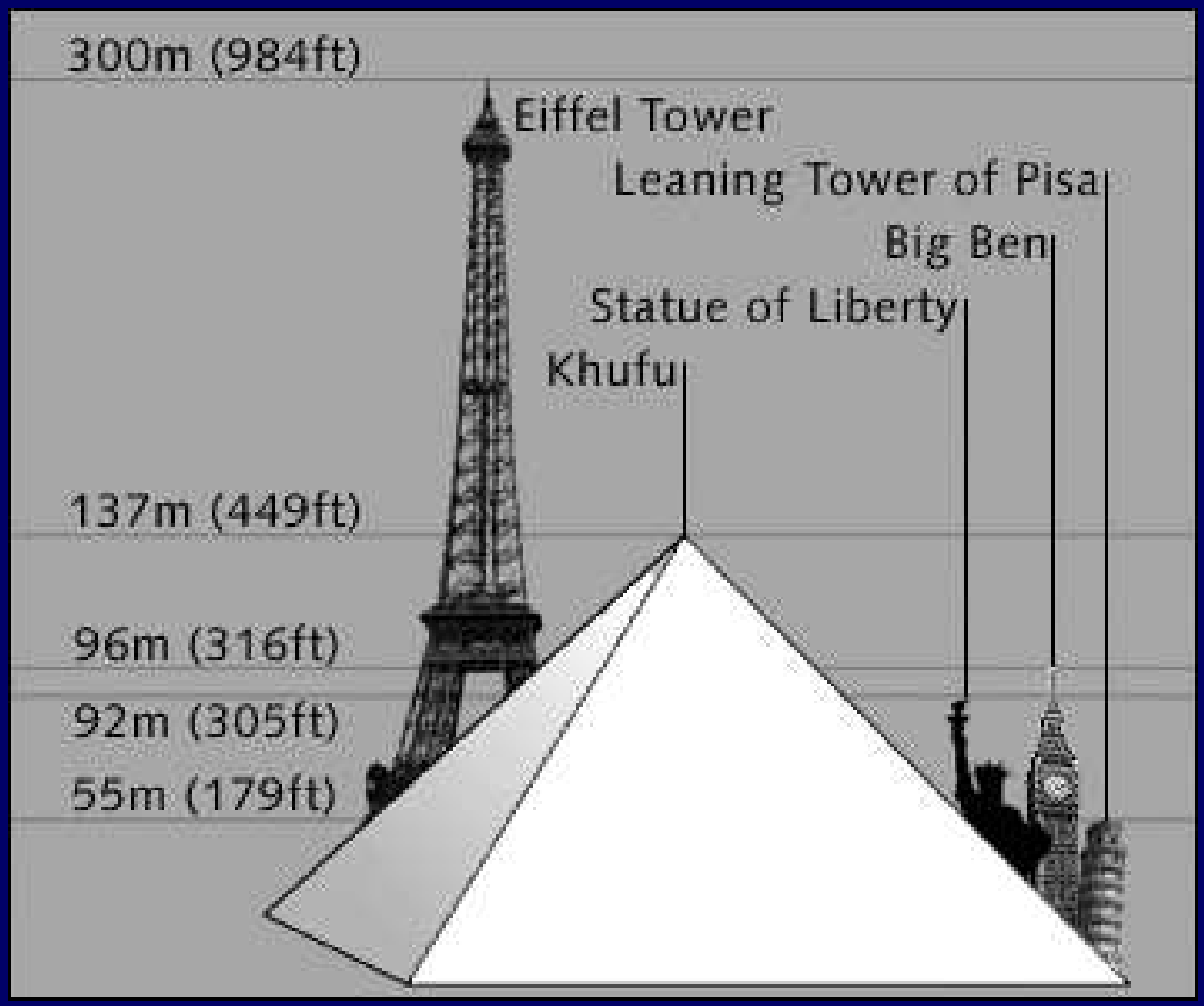


Khufu

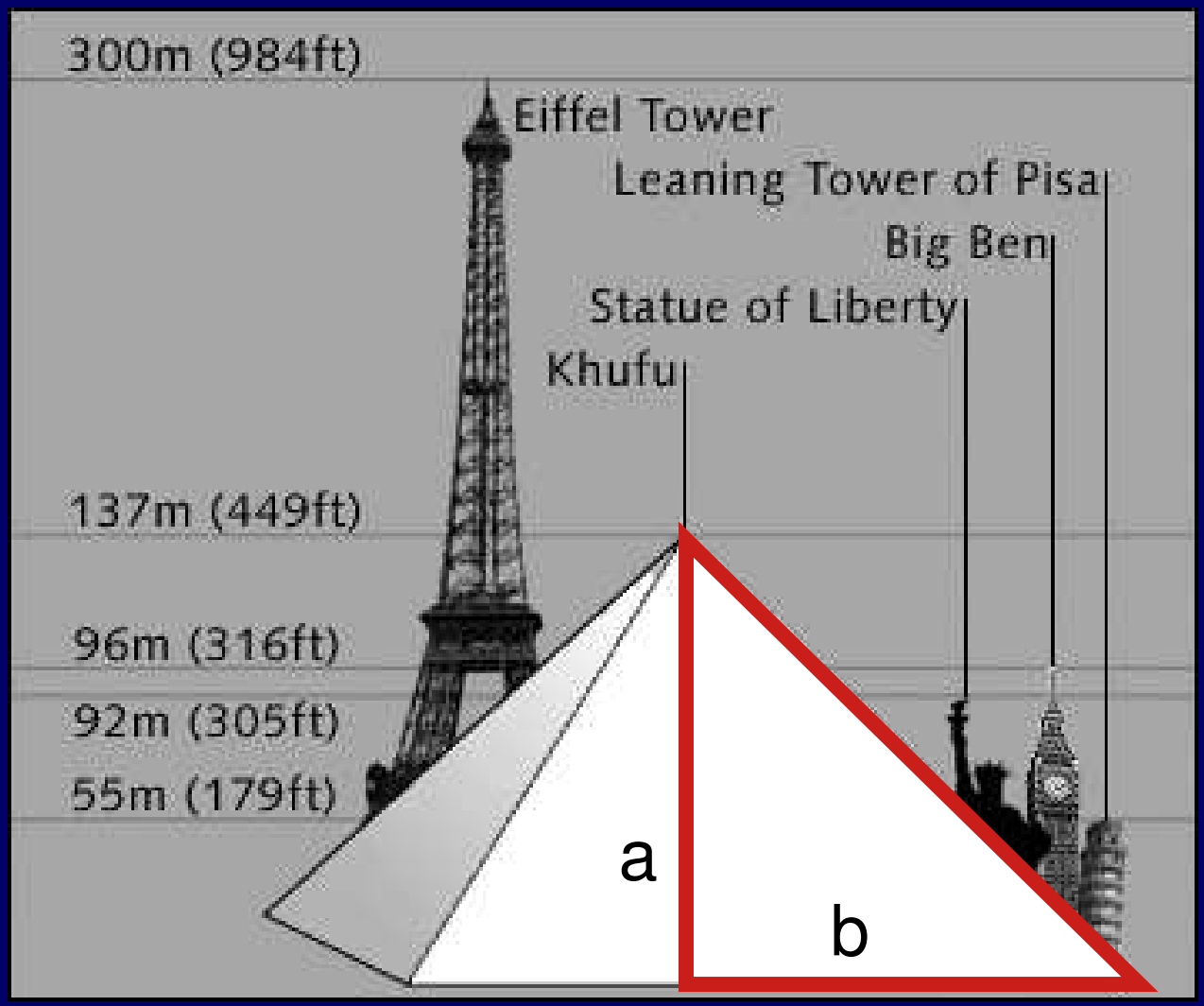
- 2589-2566 B.C.
- 2,300,000 blocks averaging 2.5 tons each

Package

Great Pyramid at Gizeh



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



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

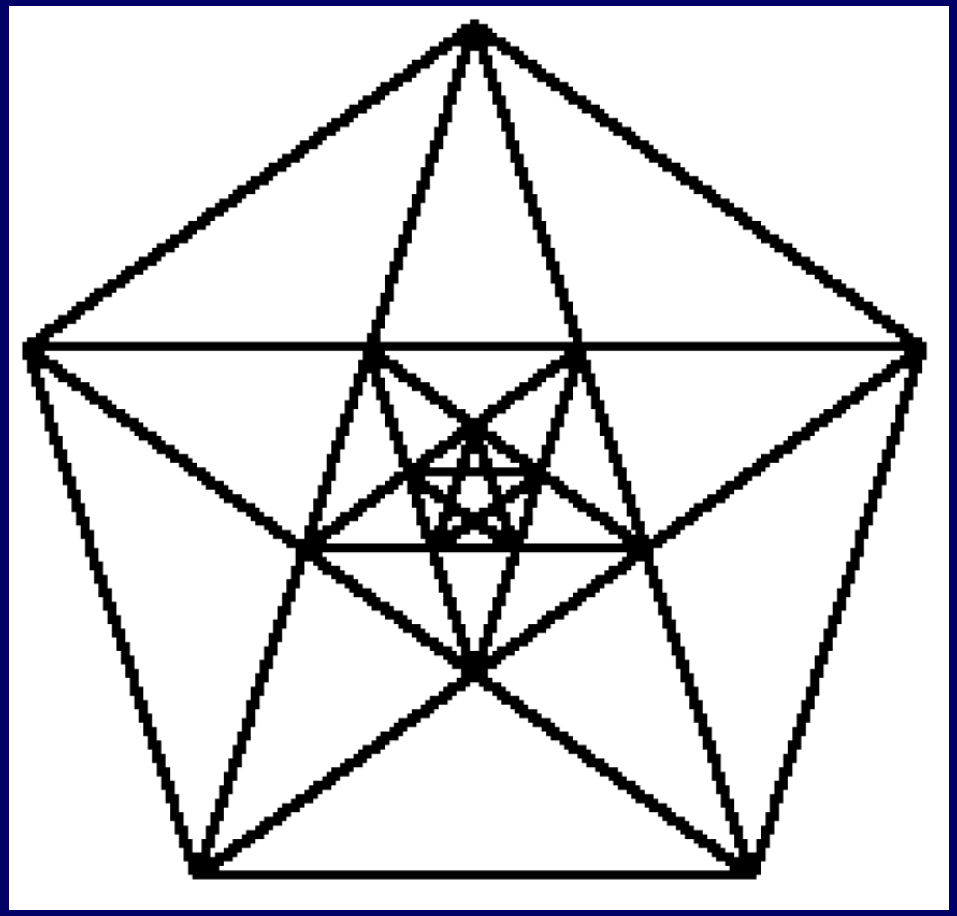
Golden Ratio
Divine Proportion

ϕ = 1.61803398874989948482045…

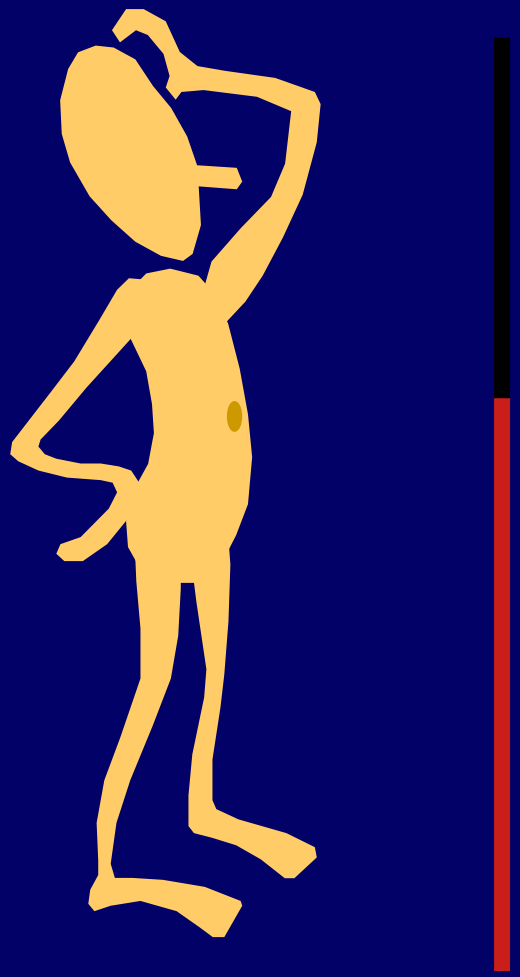
"Phi" is named after the Greek sculptor Phidias

Parthenon, Athens (400 B.C.)

Pentagon



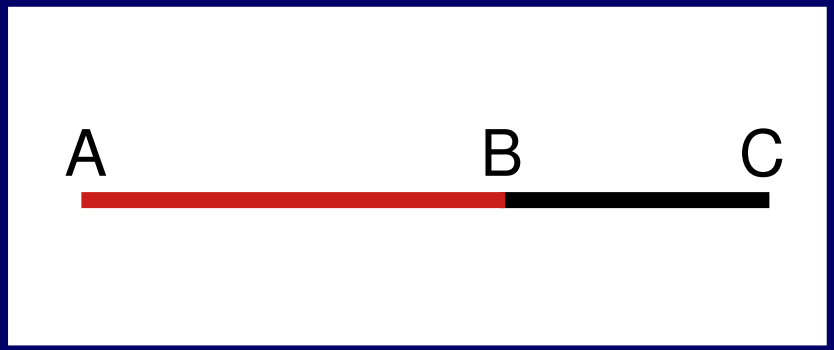
Ratio of height of the person to the height of a person's navel



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.

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



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

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

$$\boxed{\phi^2 - \phi - 1 = 0}$$

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

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

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

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

Continued Fraction Representation

$$\phi = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}}}}}}}}}$$

Continued Fraction Representation

$$\frac{1+\sqrt{5}}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}}}}}}}}}$$

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

$$\frac{1+\sqrt{5}}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}}}}}}}}}$$

Continued Fraction Representation

$$\frac{1+\sqrt{5}}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}}}}}}}}}$$

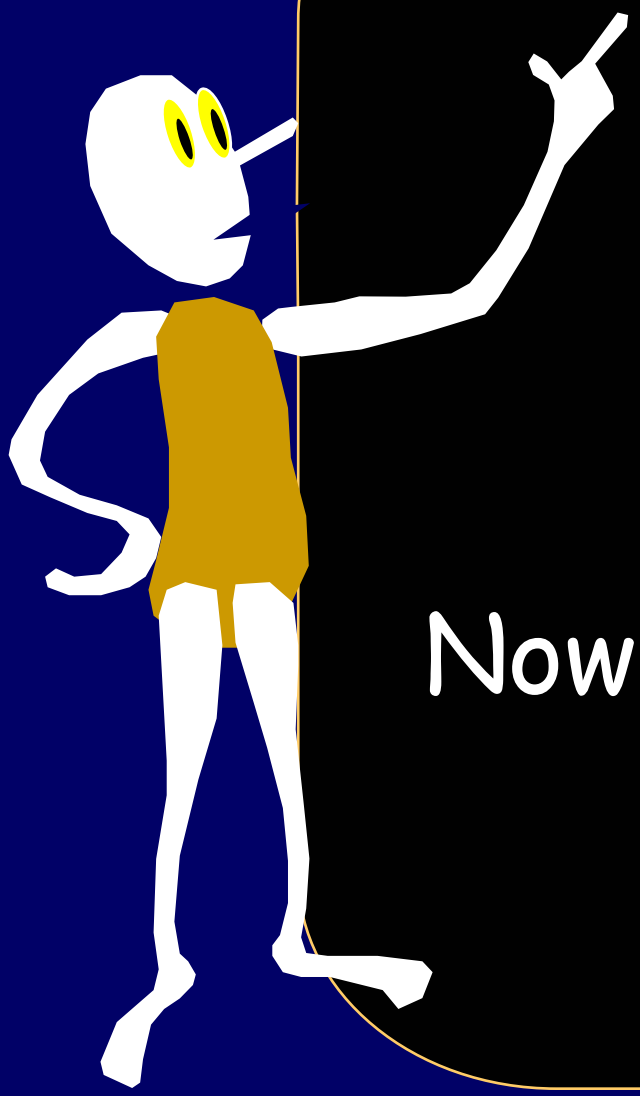
$$\lim_{n\to\infty} \frac{F_n}{F_{n-1}} = \phi = \frac{1+\sqrt{5}}{2}$$

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 = 1.618033988749894848482045

Now back to grad school!



I mean…

Now back to grade school.

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?

$12 = 2^2 * 3$ $\quad\quad$ $18 = 2*3^2$

Common factors: 2^1 and 3^1

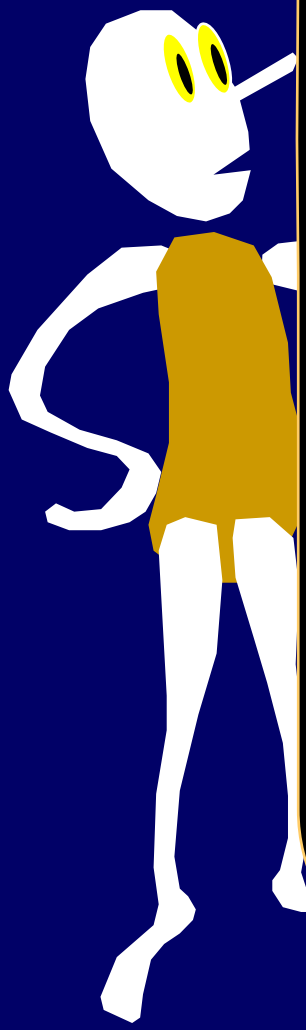
Answer: 6

Grade School GCD algorithm

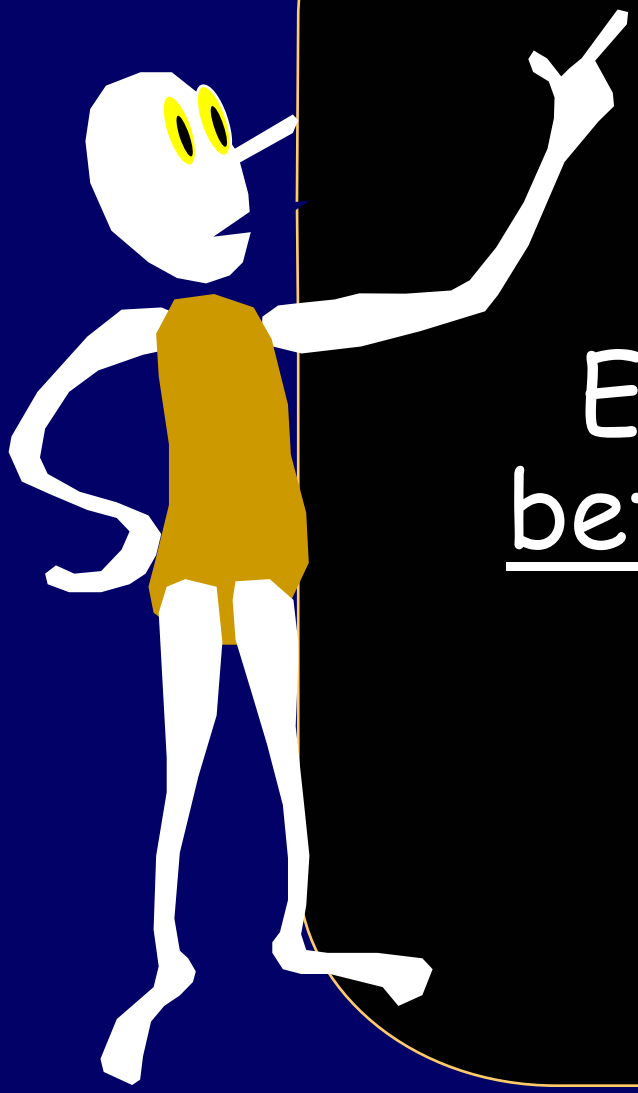
Definition: GCD(A,B) is the greatest common divisor. I.e., the largest number that goes evenly into both A and B.,

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.



EUCLID had a much better way to compute GCD!

Ancient Recursion
Euclid's GCD algorithm

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

GCD(67,29) = 1

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

GCD(A,B) = GCD(B, A mod B)

d|A and

admin/: Permission denied.

←→ d|B and d| (A - kB)

The set of common divisors of A, B equals

Euclid's GCD Termination

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

$A \bmod B < \frac{1}{2} A$

Proof:

If $B > \frac{1}{2} A$ then $A \bmod B = A - B < \frac{1}{2} A$

If $B < \frac{1}{2} A$ then ANY X Mod B $< \frac{1}{2} A$

If $B = \frac{1}{2} A$ then $A \bmod B = 0$

Euclid's GCD Termination

```
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, A mod B)

Euclid's GCD Termination

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

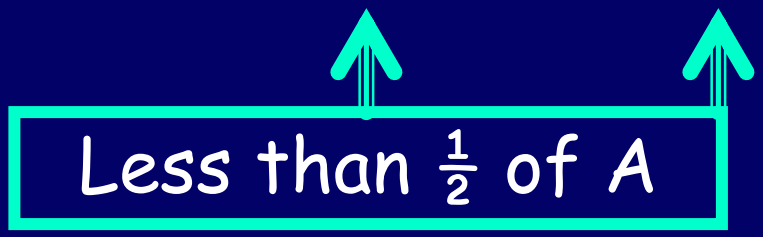
GCD(A,B) calls GCD(B, $< \frac{1}{2} A$)

Euclid's GCD Termination

```
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, $<\frac{1}{2}A$)

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



Euclid's GCD Termination

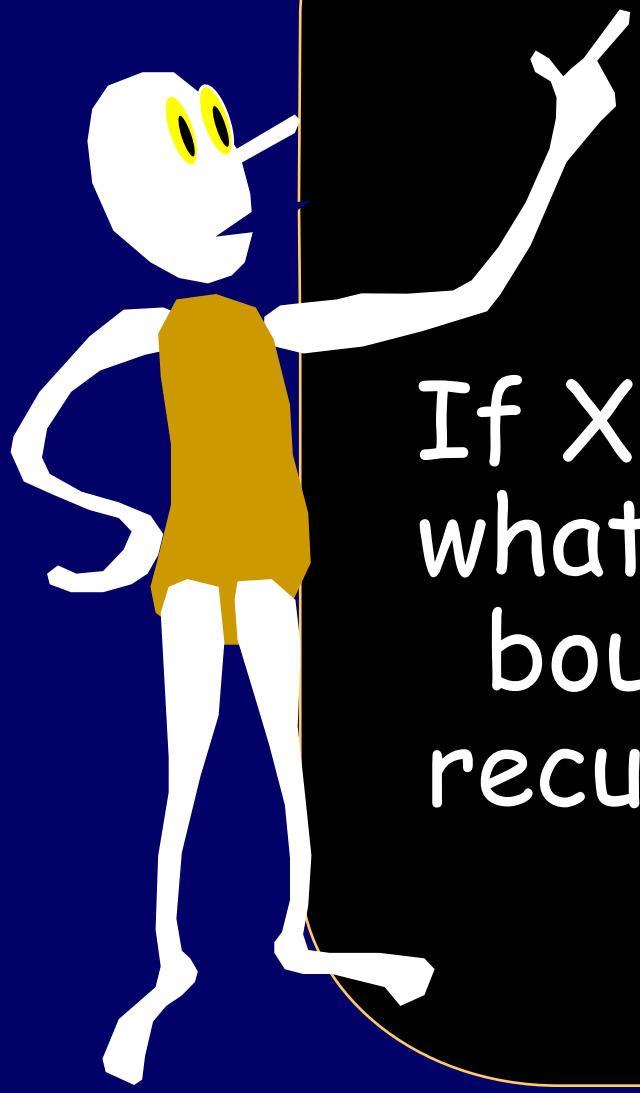
```
EUCLID(A,B)          // requires A≥B≥0
If B=0 then   Return A
       else   Return Euclid(B, A mod B)
```

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

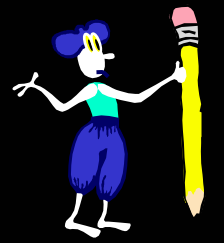
Euclid's GCD Termination

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

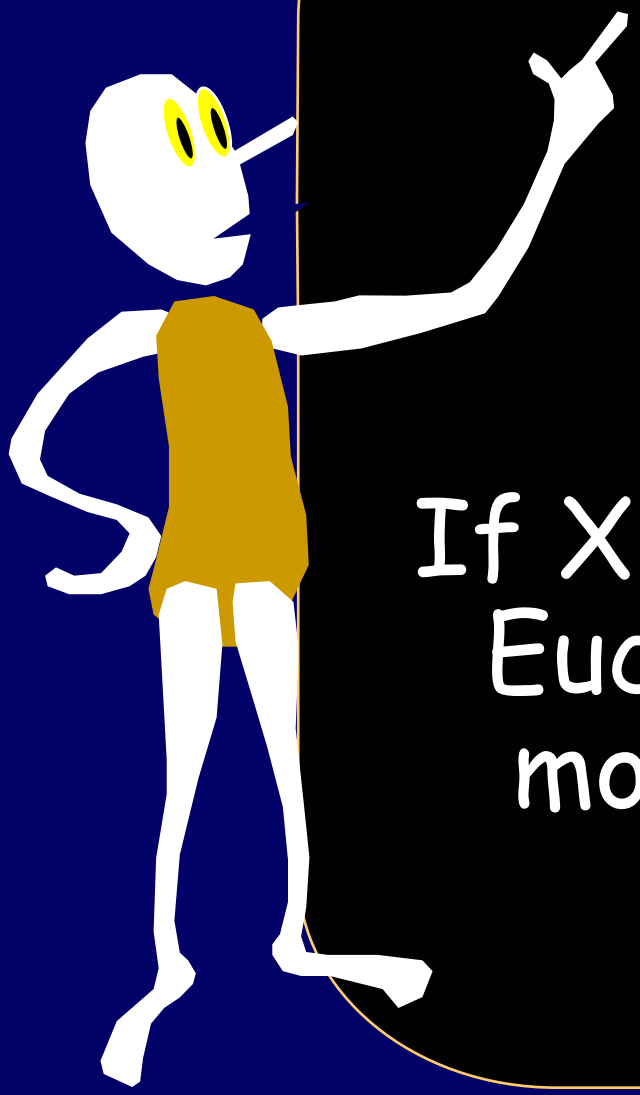
Theorem:
If two input numbers have an n bit binary representation, Euclid Algorithm will not take more than 2n calls to terminate.



Trick Question:



If X and Y are less than n, what is a reasonable upper bound on the number of recursive calls Euclid(X,Y) will make?.



Answer:

If X and Y are less than n, Euclid(X,Y) will make no more than $2\log_2 n$ calls.

EUCLID(A,B) // requires A≥B≥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>

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

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 $T(m) \leq 2\log_2 m$

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

```
EUCLID(A,B)                    // requires A≥B≥0

If B=0 then          Return A

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

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

Lemma:
Euclid(F_{k+1},F_k) makes k recursive calls

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 $T(F_k) \geq k$

Lemma: Euclid(F_{k+1},F_k) makes k recursive calls

Corollary: $T(F_k) \geq k$

Lemma: Euclid(F_{k+1},F_k) makes k recursive calls

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

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

We prove $T(F_k) \leq k$ it by proving that:

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

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

Lemma: Euclid(F_{k+1},F_k) makes k recursive calls

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

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

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

$\forall\ k \geq 2$, 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.

$B \geq 1$ and $A \geq 2$

$B \geq F_2$ $\quad$ $A \geq F_3$

$\forall\ k \geq 2$, 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: $B \geq F_k$ and A mod $B \geq F_{k-1}$

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

By induction: $B \geq F_k$ and $A \bmod B \geq F_{k-1}$

$B + (A \bmod B) \geq F_k + F_{k-1} \geq F_{k+1}$

$A \geq B + (A \bmod B)$

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

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

Corollary:
If $T(m) \geq k$ then $m \geq F_k$

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

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

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

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

Euclid(67,29)
Euclid(29,9)
Euclid(9,2)
Euclid(2,1)
Euclid(1,0)

67 div 29 = 2
29 div 9 = 3
9 div 2 = 4
2 div 1 = 2

Euclid's GCD = Continued Fractions

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

Euclid(A,B) = Euclid(B, A mod B)

Stop when B=0

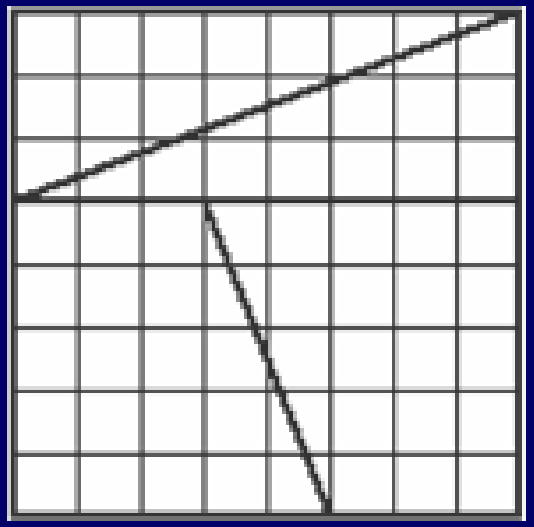
Theorem: All fractions have finite continuous fraction expansions

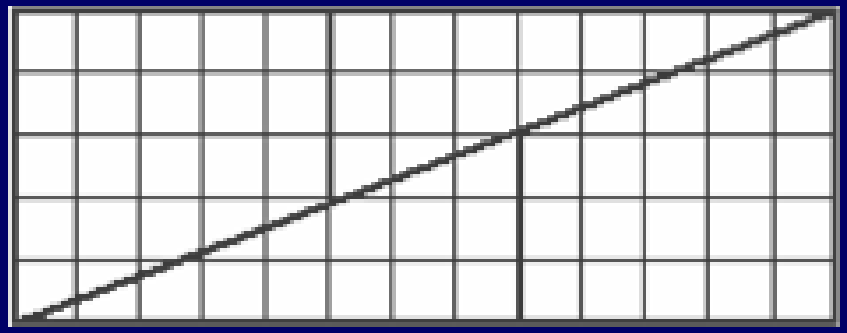
$$\frac{A}{B} = \left\lfloor \frac{A}{B} \right\rfloor + \frac{1}{\frac{B}{A \bmod B}}$$

Euclid(A,B) = Euclid(B, A mod B)

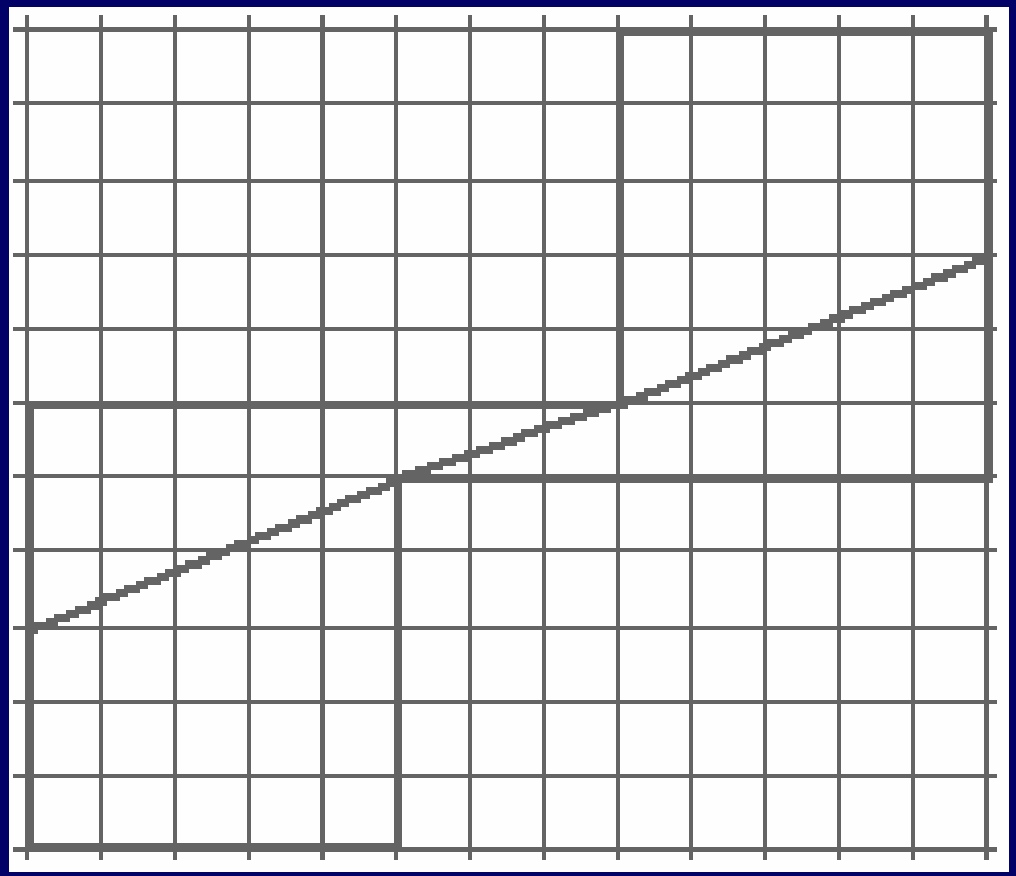
Stop when B=0

Fibonacci Magic Trick





Another Trick!



REFERENCES

Continued Fractions, C. D. Olds

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