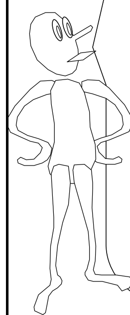
Great Theoretical Ideas In Computer Science

Steven Rudich — CS 15-251 — Spring 2005

Lecture 12 — Feb 17, 2005 — Carnegie Mellon University

Ancient Wisdom: Primes, Continued Fractions, The Golden Ratio, and Euclid's GCD

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



Definition: A number > 1 is prime if it has no other factors, besides 1 and itself.

Each number can be factored into primes in a unique way. [Euclid]

Theorem: Each natural has a unique factorization into primes written in non-decreasing order.

Definition: A number > 1 is prime if it has no other factors, besides 1 and itself.

Primes: 2, 3, 5, 7, 11, 13, 17, …

Factorizations:
- 42 = 2 * 3 * 7
- 84 = 2 * 2 * 3 * 7
- 13 = 13

Theorem: Each natural has a unique factorization into primes written in non-decreasing order.

Let n be the least counter-example.

Hence, n has at least two ways of being written as a product of primes:

$n = p_1\, p_2 \,..\, p_k = q_1\, q_2 \dots q_t$

The p's must be totally different primes than the q's or else we could divide both sides by one of a common prime and get a smaller counter-example.

Without loss of generality, assume $p_1 > q_1$.

Theorem: Each natural has a unique factorization into primes written in non-decreasing order.

Let n be the least counter-example.

$n = p_1\, p_2 \,..\, p_k = q_1\, q_2 \dots q_t$ [with $p_1 > q_1$]

$n \geq p_1 p_1 > p_1\, q_1 + 1$ [since $p_1 > q_1$]

$m = n - p_1 q_1$ [hence $1 < m < n$]

Theorem: Each natural has a unique factorization into primes written in non-decreasing order.

Let n be the least counter-example.

$n = p_1\, p_2 \,..\, p_k = q_1\, q_2 \dots q_t$ [with $p_1 > q_1$]

$n \geq p_1 p_1 > p_1\, q_1 + 1$ [since $p_1 > q_1$]

$m = n - p_1 q_1$ [hence $1 < m < n$]

Notice: $m = p_1(p_2 \,..\, p_k - q_1) = q_1(q_2 \dots q_t - p_1)$

Thus, $p_1 | m$ and $q_1 | m$

Theorem: Each natural has a unique factorization into primes written in non-decreasing order.

Let n be the least counter-example.

$n = p_1 p_2 .. p_k = q_1 q_2 \dots q_t$ [with $p_1 > q_1$]

$n \geq p_1p_1 > p_1 q_1 + 1$ [since $p_1 > q_1$]

$m = n - p_1q_1$ [hence $1 < m < n$]

Notice: $m = p_1(p_2 .. p_k - q_1) = q_1(q_2 \dots q_t - p_1)$

Thus, $p_1|m$ and $q_1|m$

By unique factorization of m, $p_1q_1|m$. Thus $m = p_1q_1z$

We have: $m = n - p_1q_1 = p_1(p_2 .. p_k - q_1) = p_1q_1z$

Theorem: Each natural has a unique factorization into primes written in non-decreasing order.

Let n be the least counter-example.

$n = p_1 p_2 .. p_k = q_1 q_2 \dots q_t$ [with $p_1 > q_1$]

$n \geq p_1p_1 > p_1 q_1 + 1$ [since $p_1 > q_1$]

$m = n - p_1q_1$ [hence $1 < m < n$]

Notice: $m = p_1(p_2 .. p_k - q_1) = q_1(q_2 \dots q_t - p_1)$

Thus, $p_1|m$ and $q_1|m$

By unique factorization of m, $p_1q_1|m$. Thus $m = p_1q_1z$

We have: $m = n - p_1q_1 = p_1(p_2 .. p_k - q_1) = p_1q_1z$

Dividing by p_1 we obtain: $(p_2 .. p_k - q_1) = q_1z$

$p_2 .. p_k = q_1z + q_1 = q_1(z+1) \Rightarrow q_1|p_2 \dots p_k$

Theorem: Each natural has a unique factorization into primes written in non-decreasing order.

Let n be the least counter-example.

$n = p_1 p_2 .. p_k = q_1 q_2 \dots q_t$ [with $p_1 > q_1$]

$n \geq p_1p_1 > p_1 q_1 + 1$ [since $p_1 > q_1$]

$m = n - p_1q_1$ [hence $1 < m < n$]

Notice: $m = p_1(p_2 .. p_k - q_1) = q_1(q_2 \dots q_t - p_1)$

Thus, $p_1|m$ and $q_1|m$

By unique factorization of m, $p_1q_1|m$. Thus $m = p_1q_1z$

We have: $m = n - p_1q_1 = p_1(p_2 .. p_k - q_1) = p_1q_1z$

Dividing by p_1 we obtain: $(p_2 .. p_k - q_1) = q_1z$

$p_2 .. p_k = q_1z + q_1 = q_1(z+1) \Rightarrow q_1|p_2 \dots p_k$

Now by unique factorization of $p_2 \dots p_k$, q_1 must be one of $p_2, \dots, p_k$.
But this contradicts the fact that the p's and q's are disjoint.

Multiplication might just be a "one-way" function

Multiplication is fast to compute

Reverse multiplication is apparently slow

We have a feasible method to multiply 1000 bit numbers [Egyptian multiplication]

Factoring the product of two random 1000 bit primes has no known feasible approach.

Grade School GCD algorithm

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?

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

Common factors: 2^1 and 3^1

Answer: 6

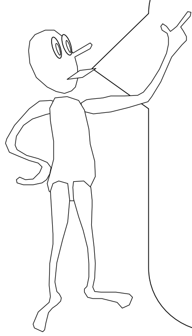
How to find GCD(A,B)?

A Naïve method:

Factor A into prime powers.

Factor B into prime powers.

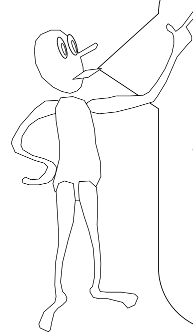
Create GCD by multiplying together each common prime raised to the highest power that goes into both A and B.



Hang on!

This requires factoring A and B.

No one knows a particularly fast way to factor numbers in general.



EUCLID had a <u>much better</u> 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)
```

A small example

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

Note: GCD(67, 29) = 1

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	

But is it correct?

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

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

$d|A$ and $d|B \Leftrightarrow d|(A - kB)$

The set of common divisors of A, B equals the set of common divisors of B, A-kB.

Does the algorithm stop?

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

Claim: A mod B < $\frac{1}{2}$ A

Proof:

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

If B < $\frac{1}{2}$ A then <u>any</u> X Mod B < B < $\frac{1}{2}$ A

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

Does the algorithm stop?

```
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)

Less than $\frac{1}{2}$ of 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)

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)

Less than $\frac{1}{2}$ of A

Euclid's GCD Termination

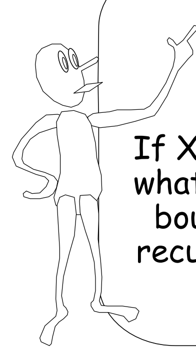
```
Euclid(A,B)          // requires A≥B≥0
If B=0 then return A
       else return Euclid(B, A mod B)
```

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

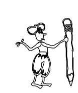
Euclid's GCD Termination

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

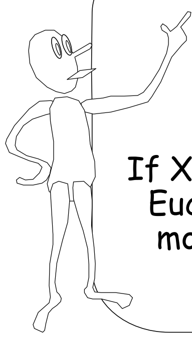
Theorem:
If two input numbers have an n bit binary representation, Euclid Algorithm will not take more than 2n calls to terminate.



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=<-3,7> – 2*<13,-30>	0=<-29,67>

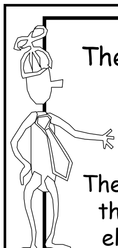
Euclid(1,0) outputs 1 = 13*67 – 30*29

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	0=<-29,67>

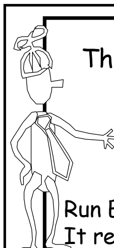
Euclid(1,0) outputs 1 = 13*67 – 30*29



The multiplicative inverse of $x \in Z_n^*$ is the unique $y \in Z_n^*$ such that $x *_n y \equiv_n 1$.

The unique inverse of a must exist because the x row contains a permutation of the elements and hence contains a unique 1.

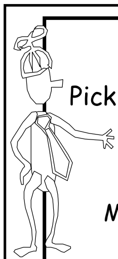
*	1	y	3	4
1	1	2	3	4
2	2	4	1	3
x	3	1	4	2
4	4	3	2	1



The multiplicative inverse of $x \in Z_n^*$ is the unique $y \in Z_n^*$ such that $x *_n y \equiv_n 1$.

TO QUICKLY COMPUTE Y FROM X:

Run Extended_Euclid(x,n).
It returns a,b, and d such that ax+bn = d
But d = GCD(x,n) = 1, so ax + bn = 1
Hence MODULO n: ax = 1 (mod n)
Thus, a is the multiplicative inverse of x.



The RSA story:

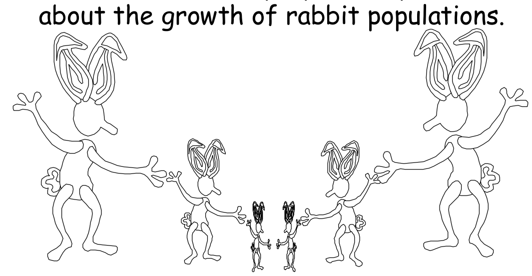
Pick 2 distinct. random 1000 bit primes, p and q.

Multiply them to get: n
Multiply (p-1) and (q-1) to compute $\phi(n)$
Randomly pick an e s.t. GCD(e,n) = 1.
Publish n and e
Compute the multiplicative inverse of e mod $\phi(n)$ to get a secret number d.

$(M^e)^d = m^{ed} = m^1 \pmod n$

Leonardo Fibonacci

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



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.

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

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

A Finite Continued Fraction

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

Denoted by [2,3,4,2,0,0,0,…]

An Infinite Continued Fraction

$$1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\ldots}}}}}}}}}$$

Denoted by [1,2,2,2,...]

Recursively Defined Form For CF

$$\begin{aligned}\mathrm{CF} &= \text{whole number, or}\\ &= \text{whole number} + \frac{1}{\mathrm{CF}}\end{aligned}$$

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

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

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

Ancient Greek Representation:
Continued Fraction Representation

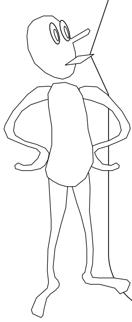
$$\frac{13}{8} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}}$$

= [1,1,1,1,1,0,0,0,…]

A Pattern?

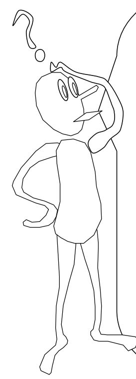
Let r_1 = [1,0,0,0,…] = 1
r_2 = [1,1,0,0,0,…] = 2/1
r_3 = [1,1,1,0,0,0…] = 3/2
r_4 = [1,1,1,1,0,0,0…] = 5/3
and so on.

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



Proposition: Any finite continued fraction evaluates to a rational.

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



Hmm.

Finite CFs = Rationals.

Then what do infinite continued fractions represent?

An infinite continued fraction

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

Quadratic Equations

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

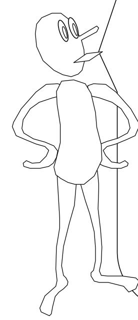
$$X = \frac{3+\sqrt{13}}{2}$$

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

X = 3 + 1/X = 3 + 1/[3 + 1/X] = …

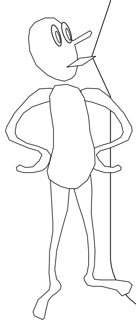
A Periodic CF

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



Theorem: Any quadratic solution has a periodic continued fraction.

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



So they express even more ….

What about those non-recurring continued fractions?

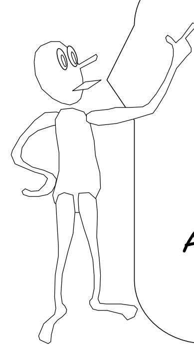
Non-periodic CFs

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

What is the pattern?

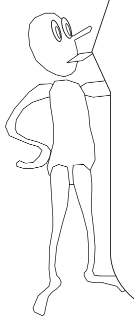
$$\pi=3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{292+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+....}}}}}}}}}$$

No one knows!



What a cool representation!

Finite CF: Rationals
Periodic CF: Quadratic roots
And some numbers reveal hidden regularity.



More good news…

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.

Convergents

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

Define: $C_1 = [a_1,0,0,0,0..]$
$C_2 = [a_1,a_2,0,0,0,...]$
$C_3 = [a_1,a_2,a_3,0,0,...]$ and so on.

C_k is called the k-th convergent of α

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

Best Approximator Theorem

A rational p/q is the <u>best approximator</u> to a real α if no rational number of denominator smaller than q comes closer to α.

BEST APPROXIMATOR THEOREM:
Given any CF representation of α, each convergent of the CF is a best approximator for α !

Best Approximators of π

$C_1 = 3$

$C_2 = 22/7$

$C_3 = 333/106$

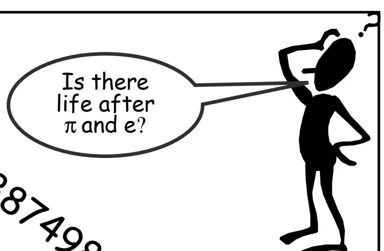
$C_4 = 355/113$

$C_5 = 103993/33102$

$C_6 = 104348/33215$

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

1.61803398874989484820458....



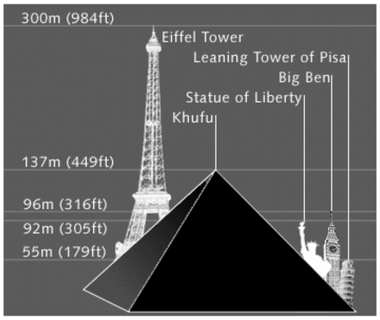
Khufu

•2589-2566 B.C.

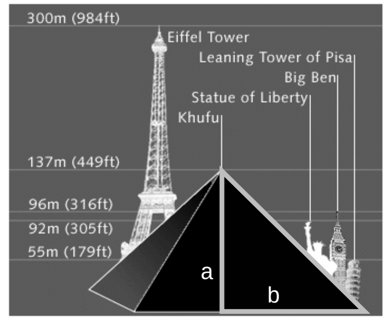
•2,300,000 blocks averaging 2.5 tons each

Package

Great Pyramid at Gizeh



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



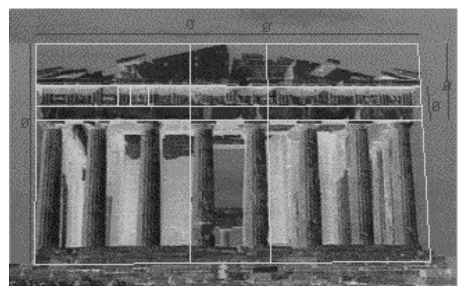
The ratio of the altitude of a face to half the base

Golden Ratio: the divine proportion

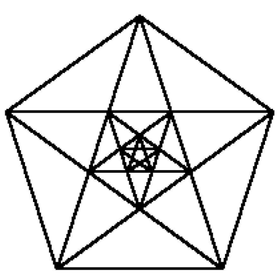
ϕ = 1.6180339887498948482045…

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

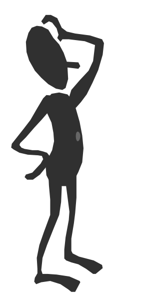
Parthenon, Athens (400 B.C.)



Pentagon



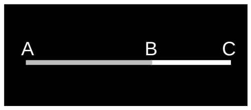
Ratio of height of the person to the height of a person’s navel



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.

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



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

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

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

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

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

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

Expanding Recursively

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

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

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

Continued Fraction Representation

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

Continued Fraction Representation

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

Remember?

We already saw the convergents of this CF

[1,1,1,1,1,1,1,1,1,1,1,...]

are of the form

Fib(n+1)/Fib(n)

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

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 = 1.6180339887498948482045

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)

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

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)	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

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

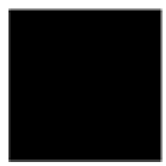
Euclid(A,B) = Euclid(B, A mod B)
Stop when B=0

Theorem: All fractions have finite continuous fraction expansions

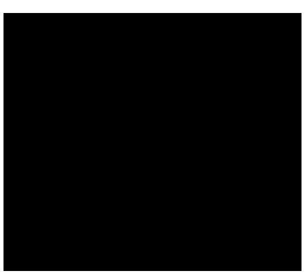
$$\frac{A}{B} = \left\lfloor \frac{A}{B} \right\rfloor + \frac{1}{\frac{B}{A \bmod B}}$$

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