10. Selected Topic: "sophisticated runtime-computation" for Euklid's alg. based on Fibonacci numbers

Euklids algorithm for computing greatest common divisor of 2 number $a, b \in \mathbb{Z}$.

```
EUKLID (a,b)          // a,b ∈ N
| IF (b = 0)
|       return a
| ELSE return EUKLID(b, a mod b)
```

$a \bmod b = a - k \cdot b$ for $k = \left\lfloor \frac{a}{b} \right\rfloor$

__Lemma 10.1__ EUKLID correctly computes $gcd(a,b)$.

__proof__: remains to show that for all $a, b \in \mathbb{N}$ it holds that $gcd(a,b) = gcd(b, a \bmod b)$

$x \mid y \;\&\; y \mid x \iff x = y, \; y > 0$

show $gcd(a,b) \mid gcd(b, a \bmod b)$
& $gcd(b, a \bmod b) \mid gcd(a,b)$

Put $d := gcd(a,b)$
$\Rightarrow d \mid a \;\&\; d \mid b$

Claim: $d \mid (ax+by) \quad \forall x,y \in \mathbb{Z}$

proof claim: $\begin{matrix} d \mid a \\ d \mid b \end{matrix} \Rightarrow \begin{matrix} a = k \cdot d \\ b = k' \cdot d \end{matrix} \xrightarrow{\forall x,y \in \mathbb{Z}} \begin{matrix} ax = kxd \\ by = k'yd \end{matrix}$

$$\Rightarrow ax+by = kxd + k'yd$$
$$= (kx + k'y)d$$
$$= \tilde{k} \cdot d$$

$$\Rightarrow k \mid (ax+by)$$

$/\!\diamond$

$\Rightarrow d \mid (ax+by) \quad \forall x,y \in \mathbb{Z}$

$\left.\begin{matrix} x = 1 \\ y = -q \\ \text{with } q = \lfloor \frac{a}{b} \rfloor \end{matrix}\right\} \Rightarrow d \mid (\underbrace{a - qb}_{= a \bmod b}) \Rightarrow d \mid a \bmod b$

Since $d \mid b$ & $d \mid (a \bmod b) \Rightarrow d \mid \gcd(b, a \bmod b)$

$\boxed{I}$

Now put $d = \gcd(b, a \bmod b)$

Since $d \mid b$ & $d \mid (a \bmod b)$

Now, a can be written as $a = q \cdot b + a - q \cdot b$, $q = \lfloor \frac{a}{b} \rfloor$

$$\overset{\text{Def}}{=} q \cdot b + a \bmod b$$

$\Rightarrow$ a is a linear kombination of b & a mod b by claim above: $d \mid$ every lin. comb. of b & $a \bmod b$

& a is lin. combin of b & $a \bmod b$

$\Rightarrow d \mid a$

$\Rightarrow d \mid a$ & $d \mid b \Rightarrow d \mid \gcd(a,b)$ II

I + II + III $\Rightarrow \gcd(a,b) = \gcd(b, a \bmod a)$ $\square$

Runtime? $\longrightarrow$ Fib. nr.

Fib.nr.: 1, 1, 2, 3, 5, 8, 13, 21, ...

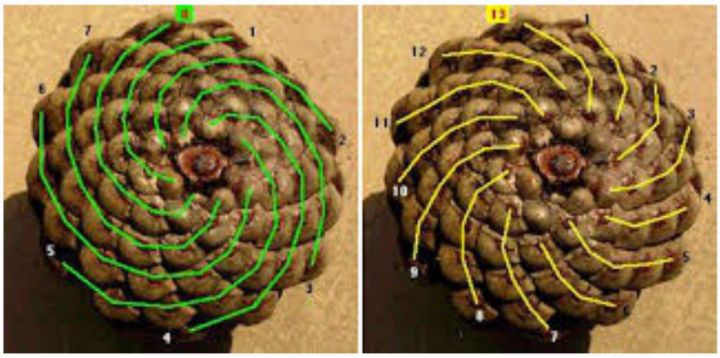
$$F(1)=F(2)=1, \quad F(n)=F(n-1)+F(n-2) \quad \forall n>2$$

Fib.nr frequently occur in nature & reason mainly "evol. optim" properties & fact that Fib-nr are closely related to the golden ratio

Examples

pineapple

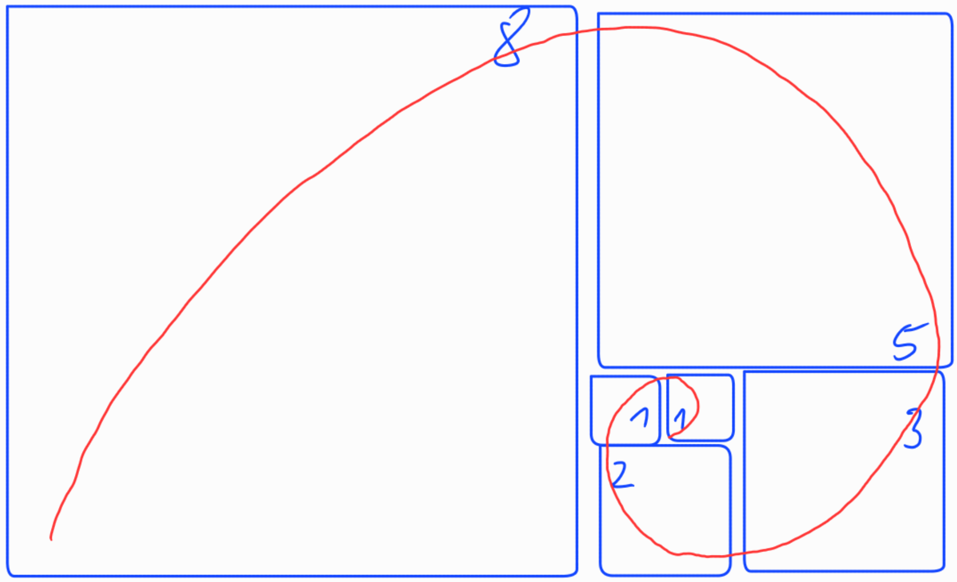
pine cone

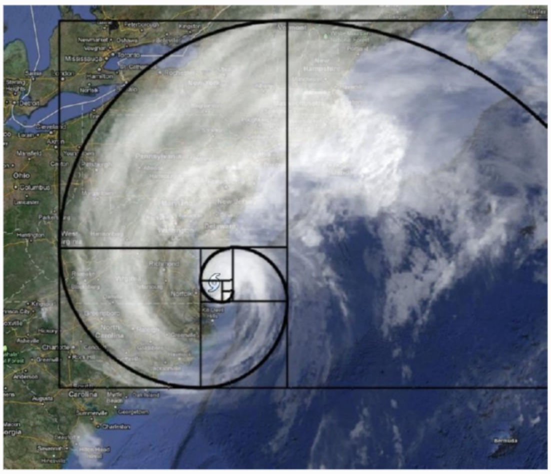


count spirals $\underbrace{8, 13, 21}_{\text{consecutive Fib nr}}$

$\underbrace{8, 13}_{\text{consecutive Fib nr.}}$

Typical Pattern





Hurricane

Snail shell

# of petals : mayflower #petals 5
marigold #petals 13
daisy #petals $\in \{34, 55, 89\}$

Lilies 3 petals

Buttercup 5 petals

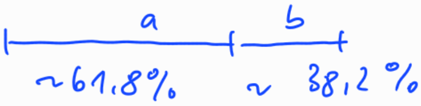
Cosmos 8 petals

Asters 13 petals

Fib-nr are closely related to golden ratio.

golden ratio = ratio of number a, b

st $\quad \dfrac{a}{b} = \dfrac{a+b}{a} = \phi$



$$\phi = \frac{a+b}{a} = \frac{a}{b} \iff \frac{a}{b} - 1 - \frac{b}{a} = 0$$

$$\iff \phi - 1 - \frac{1}{\phi} = 0$$

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

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

$$\hat{\phi} = \frac{1-\sqrt{5}}{2}$$

$\phi \approx \underline{1{,}618\,033\,9}8875\ldots$

i	1	2	3	4	5	6	7	8	...
F_i	1	1	2	3	5	8	13	21	...
$\frac{F_{i+1}}{F_i}$	1	2	1,5	$1{,}\bar{6}$	1,6	1,625	1,615	...	

$$\frac{F_{22}}{F_{21}} = \frac{17711}{10946} = \underline{1{,}6180339}8502\ldots$$

$$\text{“} \frac{F_{i+1}}{F_i} \xrightarrow{i\to\infty} \phi \text{”}$$

Eg honeybees: ratio of $\frac{\text{female bees}}{\text{male bees}} \approx \phi$

ratio of $\frac{\text{length shoulder to fingertip}}{\text{length elbow to fingertip}} \approx \phi$

L. 10.2 $\quad F_i = \frac{\phi^i - \hat{\phi}^i}{\sqrt{5}}$

proof: (1) $1+\phi = 1 + \frac{1+\sqrt{5}}{2}$

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

$= \frac{6+2\sqrt{5}}{4}$

(2) $\phi^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+2\sqrt{5}+5}{4}$

$= \frac{6+2\sqrt{5}}{4}$

(1)+(2) $\Rightarrow$ $1+\phi = \phi^2$ (analogously for $\hat{\phi}$)

$\Rightarrow \forall i: \quad \phi^{i-1} + \phi^{i-2} = \phi^{i-2}(\phi+1)$

$= \phi^{i-2} \cdot \phi^2 = \phi^i$

(*)

by induction show: $F_i = \dfrac{\phi^i - \hat{\phi}^i}{\sqrt{5}}$

$i = 1$

$$1 = F_1 \overset{?}{=} \frac{\phi^1 - \hat{\phi}^1}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}}$$

$$= \frac{\sqrt{5}}{\sqrt{5}} = 1 \checkmark$$

$i = 2$

$$1 = F_2 \overset{?}{=} \frac{\phi^2 - \hat{\phi}^2}{\sqrt{5}} = \frac{\frac{1+2\sqrt{5}+5}{4} - \frac{1-2\sqrt{5}+5}{4}}{\sqrt{5}}$$

$$= \frac{4\sqrt{5}}{4\sqrt{5}} = 1 \checkmark$$

Assume Indhyp holds for all $k \in \{1, 2, \dots, i-1\}$, $i > 2$

$$F_i = F_{i-1} + F_{i-2} \overset{\text{Ind Hyp}}{=} \frac{\phi^{i-1} - \hat{\phi}^{i-1}}{\sqrt{5}} + \frac{\phi^{i-2} - \hat{\phi}^{i-2}}{\sqrt{5}}$$

$$= \frac{(\phi^{i-1} + \phi^{i-2})}{\sqrt{5}} - \frac{(\hat{\phi}^{i-1} + \hat{\phi}^{i-2})}{\sqrt{5}}$$

$$\overset{(*)}{=} \frac{\phi^i - \hat{\phi}^i}{\sqrt{5}} \checkmark$$

$\square$

Asymptotic behavior of F_i ?

$$\phi \approx 1{,}618 \qquad \hat{\phi} \approx -0{,}618 \quad \Rightarrow \quad \phi^i \xrightarrow{i \to \infty} \text{expon. grows} \qquad \hat{\phi}^i \xrightarrow{i \to \infty} 0$$

$$F_i = \frac{\phi^i - \hat{\phi}^i}{\sqrt{5}} \quad \underset{i}{\overset{\text{large}}{\rightsquigarrow}} \quad F_i \sim \frac{\phi^i}{\sqrt{5}}$$

"expon. growth".

$F_n \in O(\phi^n)$

by induction $F_1 = 1 \leq c_1 \phi \in O(\phi)$

$F_2 = 1 \leq c_2 \phi^2 \in O(\phi^2)$

true for $F_1 \ldots F_{n-1}$

now, $F_n = F_{n-1} + F_{n-2} \leq c\, \phi^{n-1} + c\, \phi^{n-2}$ for some large const c

$= c\, \phi^n$

$\Rightarrow F_n \in O(\phi^n)$

$1 + \phi = \phi^2 \overset{\cdot c \phi^{n-2}}{\Longrightarrow} c\phi^{n-2} + c\phi^{n-1} = c\, \phi^n$

shown above

$F_n \in \Omega(\phi^n)$ show $F_n \geq c \cdot \phi^n \quad \forall n \geq n_0$

choose $c = \frac{1}{\phi^2} \rightarrow$ to show $F_n \geq \phi^{n-2}$

Induction $F_1 = 1 \geq \phi^{-1}$

$F_2 = 1 \geq \phi^0$

Assume correct for $F_1, F_2 \ldots F_{n-1}$

Consider $F_n = F_{n-2} + F_{n-1} \underset{\text{Ind Hyp}}{\geq} \phi^{n-4} + \phi^{n-3}$

$$= \phi^{n-4}(1+\phi)$$

$$= \phi^{n-4}\phi^2 = \phi^{n-2}$$

$\Rightarrow F_n \in \Omega(\phi^n)$

$\Rightarrow F_n \in \Theta(\phi^n)$

Back to runtime.

```
EUKLID (a,b)
    IF (b=0)
        return a
    ELSE return EUKLID(b, a mod b)
```

Wlog $a > b$, why? IF $b > a \geq 0$ → Euklid makes recursive call Euklid$(b, \underbrace{a \bmod b}_{=a})$

IF $b = a$ → $a \bmod b = 0$ stops after 1st recursive call.

Lemma 10.3

Let $a > b \geq 0$ integers. Assume EUKLID(a,b) has $k \geq 1$ recursive calls

$\Rightarrow a \geq F_{k+2}$ & $b \geq F_{k+1}$

proof by induction on k.

$k = 1 \Rightarrow$ we have 1 recursive call.

$\Rightarrow b \geq 1 = F_2$

Since $a > b \Rightarrow a > 1$

$\Rightarrow a \geq 2 = F_3$ ✓

Assume Indhyp hold for $\leq k-1$ recursive calls

Consider now case: "k calls"

Since $k > 0 \Rightarrow b > 0$

& EUKLID(a,b) calls

EUKLID$(b, a \bmod b)$

in here (after this call) we have $k-1$ further recursive calls can apply Ind hyp : $\boxed{b \geq F_{k+1}}$ ✓

$a \bmod b \geq F_k$

it remains to show that $a \geq F_{k+2}$

Observe: $a > b > 0$

& $$b + (a \bmod b) \overset{\text{Def}}{=} b + \left(a - b\left\lfloor \frac{a}{b} \right\rfloor\right)$$
$$= a - \underbrace{\Big(b\underbrace{\left\lfloor \tfrac{a}{b} \right\rfloor}_{\geq 1 \text{ since } a>b} - b\Big)}_{\geq 0} \leq a$$

$$\Rightarrow a \geq b + (a \bmod b)$$
$$\geq F_{k+1} + F_k = F_{k+2}$$

$\square$

Thm. 10.4 (Lamé)

$\forall$ integer $k \geq 1$: if $a > b \geq 1$ & $b < F_{k+1}$
EUCLID(a,b) has less than k recursive calls.

Proof: Contraposition of L. 10.3

$\square$

REMARK: This boundary is the best possible one since for $a = F_{k+1}$ & $b = F_k < F_{k+1}$ we have precisely k calls [Exercise] what is now k for a, b?

Assume: $F_k \in \Theta(\phi^k)$

$F_k \leq b < F_{k+1}$

in particular we showed in proof for "$F_k \in \Theta(\phi^k)$"

that $F_k \geq c \cdot \phi^k$ for $c = \frac{1}{\phi^2}$

$\Rightarrow b \geq F_k \geq \phi^{k-2} \quad \Rightarrow \log_\phi(b) \geq \log_\phi(\phi^{k-2}) = k-2$

Now, $\log_2(\phi) \approx 0{,}69 > \frac{1}{2}$

$\Rightarrow \frac{1}{2} \cdot (k-2) < \log_2(\phi) \cdot \log_\phi(b) = \log_2(b)$

log rules

$\Rightarrow k-2 < 2\log_2(b)$

$k < 2\log_2(b) + 2$

$\Rightarrow k \in O(\log_2(b))$

this is extremely fast!

eg. even if $b = 2^n$ large nr

$\Rightarrow \log_2(b) = n$!