$$f_n = \begin{cases} 0 \dots\dots & \text{if } n=0 \\ 1 \dots\dots & \text{if } n=1 \\ f_{n-1}+f_{n-2} \dots & \text{if } n \geq 2. \end{cases}$$

$$f_n = \frac{\varphi^n - \psi^n}{\sqrt{5}} < \frac{\varphi^n + 1}{\sqrt{5}}$$

$\varphi = \frac{1+\sqrt{5}}{2}$ $\quad \psi = \frac{1-\sqrt{5}}{2}.$

$\varphi \approx 1.618$ $\quad \cancel{\psi \approx 0.618}$

-0.618

n	f_n
0	0
1	1
2	1
3	2
4	3
5	5
6	8
7	13
8	21
9	34
10	55
11	89
12	144
13	233
14	377
15	610
16	987
17	1917
18	2584
19	4161

F_n = the number of ways of writing n as a sum of 1's and 2's.

$$F_n = \begin{cases} 1 & \text{if } n=0 \\ 1 & \text{if } n=1. \\ F_{n-1}+F_{n-2} & \text{if } n \geq 2. \end{cases}$$

$F_0 = 1$

$F_1 = 1$ $\qquad 1 = 1.$

$F_2 = 2$ $\qquad 2 = 1+1$, $2 = 2.$

$F_3 = 3$ $\qquad 3 = 1+1+1 = 2+1 = 1+2.$

Theorem: $F_n = f_{n+1}.$

$7 = \cancel{1/2 +}$

$n = 1 + \underbrace{\bigcirc}$ ← a sum of 1's & 2's that add up to $n-1$. (F_{n-1} ways).

OR.

$= 2 + \underbrace{\bigcirc}$ ← a sum of 1's & 2's that add up to $n-2$. (F_{n-2} ways).

Greatest Common Divisor.

Eg. $\gcd(20,15) = 5.$ $\quad \frac{20}{5} = 4$ ✓ $\quad \frac{15}{5} = 3$ ✓

For two positive integers a and b, $\gcd(a,b)$ is the largest integer that divides both a and b.

[Maximum d such that $\frac{a}{d}$ and $\frac{b}{d}$ are integers].

$\underset{\text{int.}}{\uparrow}$

$a = 20$
$b = 6.$

$$\overset{a}{20} = \overset{q}{3} \cdot \overset{b}{6} + \overset{r}{2}$$

$a \bmod b = r.$

$20 \bmod 6 = 2.$

$\overset{a}{17} \bmod \overset{b}{12} = 5.$

$17 = \overset{q}{1} \cdot 12 + \overset{r}{5}.$

$23 \bmod 1 = 0.$

$\underset{a}{23} = \underset{q}{23} \cdot \underset{b}{1} + \underset{r}{0}$

$45 \bmod 15 = 0.$

$45 = 3 \cdot 15 + 0$

Euclid's GCD Algorithm.

Uses the mod (remainder) operation. — For any integers a and b, there exists integers q and r such that $a = q \cdot b + r$

Lemma: If $a \bmod b = 0$ then $\gcd(a,b) = b.$

Proof: $a \bmod b = 0 \Rightarrow a = q \cdot b + 0 \Rightarrow \frac{a}{b} = \underset{\text{int.}}{q} \quad \frac{b}{b} = \underset{\text{int}}{1}$

Lemma: If $a \bmod b = r \neq 0$ then $\gcd(a,b) = \gcd(b,r)$

Let d be any common divisor of a and b.

Proof: $a \bmod b = r \Rightarrow a = \overset{\text{int.}}{q} \cdot b + r, \Leftrightarrow \underset{\text{int.}}{\frac{a}{d}} = \underset{\text{int.}}{\frac{q \cdot b}{d}} + \underset{\text{int.}}{\frac{r}{d}}$

d is a divisor of b and r.

$\gcd(a,b) = \gcd(b,r)$

Euclid(a, b) // $a > b \geq 1$.

→ $r = a \bmod b$.

→ if $r = 0$ return b

return Euclid(b, r)

$a > b$. $\gcd(a, b) \to \gcd(b, r)$.

$a>b$. smaller $\leq b-1$.

$r = a \bmod b \in \{0, \dots, b-1\}$.

Algorith terminates.

Euclid(75, 45)	$75 = 1 \cdot 45 + \overset{r}{30}$.
Euclid(45, 30)	$45 = 1 \cdot 30 + 15$
Euclid(30, 15)	$30 = 2 \cdot 15 + 0$
return 15.	

Euclid(34, 21)	$34 = 1 \cdot 21 + 13$.
Euclid(21, 13)	$21 = 1 \cdot 13 + 8$
Euclid(13, 8)	$13 = 1 \cdot 8 + 5$
Euclid(8, 5)	$8 = 1 \cdot 5 + 3$
Euclid(5, 3)	$5 = 1 \cdot 3 + 2$
Euclid(3, 2)	$3 = 1 \cdot 2 + 1$
Euclid(2, 1)	$2 = 2 \cdot 1 + 0$
return 1.	

Let $M(a,b)$ = the number of mod operations performed when running Euclid(a,b).

Claim: ~~If~~ Let $a>b\geq 1$ and let $m=M(a,b)$. Then $a\geq f_{m+2}$ and $b\geq f_{m+1}$.

Proof by induction on m. Base case $m=1$.

$b\geq 1 = f_2$ $\quad a\geq 2 = f_3 = f_{m+2}$.

$= f_{m+1}$.

· Now assume the claim is true for $K\in\{1,2,\dots,m-1\}$ and prove it for $m\geq 2$.

• ~~If~~ Since $m\geq 2$ $\quad r = a \bmod b \neq 0$.

$$m = M(a,b) = 1 + M(b,r) \iff M(b,r) = m-1$$

By the inductive hypothesis.

$$b\geq f_{m-1+2} = f_{m+1} \quad \text{and} \quad r \geq f_{m-1+1} = f_m.$$

$$a \bmod b = r \iff a = q\cdot b + r$$
$$\geq b + r$$
$$\geq f_{m+1} + f_m = f_{m+2}$$

$m = \#$ mod operations.

make up for missing ψ

$$a \geq f_{m+2} \geq \frac{\varphi^{m+2} - 1}{\sqrt{5}}$$

$$a\sqrt{5} + 1 \geq \varphi^{m+2}.$$

$$\log(a\sqrt{5}+1) \geq (m+2) \cdot \log \varphi$$

$$\frac{\log(a\sqrt{5}+1)}{\log \varphi} - 2 \geq m \leftarrow$$

$$m = \Theta(\log a).$$