

Group number: 4

Group Name: Monica Tandel, Niranjan Pawar, Vasanthi Lingamdinne

ASSIGNMENT 1

Show that for any integer $k \geq 1$, if $a > b \geq 1$ and $b < F_{k+1}$ (where F_i is the i -th Fibonacci number), then Euclid's algorithm on a, b takes fewer than k iterations of the while loop. (Ignore swaps or use $2k$ instead.)

Pre condition:- $k \geq 1, a > b \geq 1, b < F_{k+1}$

Basis Case:- $\gcd(a, b) = \gcd(b, r)$, where $r = \text{rem}(a, b)$
We can say that the value of r independent of a will always lie between $0 \leq r < b$, as b is the quotient.

$$\gcd(b, r) = \gcd(r, r_1) \quad \text{where } r_1 = \text{rem}(b, r)$$

So we check the possible values of r_1 for all possible values of r .

If $b > r \geq F_k$ then $r_1 < F_{k-1}$,

If $0 < r < b/2$ then $r_1 < F_{k-1}$,

If $b/2 \leq r < F_k$ then $r_1 > F_{k-1}$ but $r_2 < F_{k-2}$

Because in division, for a value of r as the r_1 become large the value of r_2 gets smaller.

Termination:- This process keeps on going until when the $F_{(k=2)} = 1$ and r_n must be smaller than F_2 which is 0. I.e the \gcd process will terminate at or before F_2 .

Correctness- We prove that it requires less than k steps of the Fibonacci series to complete $\gcd(a, b)$.

Mathematical Example

The value of a does not matter.

Let $K=12$, so $F_{k+1=13}=233$,

As $b < F_{k+1}$, we take upper bound for b which is $F_{k+1}-1=232$, so $b=232$,

Now r can be in the following range $0 \leq r < b$,

If $b > r > F_k$ i.e $232 > r > 144$ then $r_1 < 89$

If $0 < r < b/2$ i.e $0 < r < 116$ then $r_1 < 89$,

If $b/2 < r < F_k$ i.e $116 \leq r < 144$ then $r_1 > 89$ but $r_2 < 55$

Following with that process, $r_n < F_2=1$, or $r_n=0$, thus $r_n=0$ at $k=2$, thus gcd is calculated before k steps.