Name: ________________________________

ID number: ____________________________

There are 2 questions for a total of 10 points.

---

1. (2 points) Recall the `Euclid-GCD` algorithm discussed in class for finding the gcd of positive integers $a \geq b > 0$. The algorithm makes a sequence of recursive calls until the second input becomes 0. For example, the sequence of recursive calls for finding the gcd of 2 and 1 are:

$$\texttt{Euclid-GCD}(2, 1) \rightarrow \texttt{Euclid-GCD}(1, 0)$$

Write down the sequence of recursive calls made when the algorithms is used for finding the gcd of 53 and 991.

Solution: $\texttt{Euclid-GCD}(991, 53) \rightarrow \texttt{Euclid-GCD}(53, 37) \rightarrow \texttt{Euclid-GCD}(37, 16) \rightarrow \texttt{Euclid-GCD}(16, 5) \rightarrow \texttt{Euclid-GCD}(5, 1) \rightarrow \texttt{Euclid-GCD}(1, 0)$.

2. (8 points) Recall the Euclid-GCD(a, b) algorithm discussed in the lectures for finding the gcd of two integers a and b. Prove the following theorem:

Theorem 1 (Lame's theorem)**.** *For any integer $k \geq 1$, if $a > b \geq 1$ and $b < F_{k+1}$, then the call Euclid-GCD(a, b) makes fewer than k recursive calls.*

Here F_k denotes the k^{th} number in the Fibonacci sequence $(0, 1, 1, 2, 3, 5, 8, 13, ...)$
(*Note that since this question was part of the tutorial sheet, special emphasis will be given to the clarity of your proof while grading.*)

Solution: We will prove the statement using strong induction. Consider the following propositional function:
$P(b)$: The number of recursive calls made by the Euclid-GCD algorithm when run with inputs $a \geq b$ with $b < F_{k+1}$ is $< k$.

Basis step: Here we will show that $P(1)$ and $P(2)$ are true.

For any $a > 0$, the number of recursive calls is 1 when $b = 1$. Furthermore, $b = 1 < F_{k+1}$ only if $k \geq 2$, and for all such k the number of recursive calls is $< k$. So, $P(1)$ holds.

For any $a > 0$, the number of recursive calls is ≤ 2 when $b = 2$. This is because in the next recursive call the smaller number will either be 0 or 1 in which case there can be at most 1 more recursive call. Furthermore, $b = 2 < F_{k+1}$ only if $k \geq 3$, and for all such k the number of recursive calls is $< k$. So, $P(2)$ holds.

Inductive step: We will assume that $P(1), ..., P(b-1)$ holds for an arbitrary integer $b \geq 3$ and then show that $P(b)$ holds.

Suppose k is the smallest integer such that $b < F_{k+1}$. This means that $b \geq F_k$. We break the analysis into the following two parts:

- $a\ (mod\ b) < F_k$: In this case, after the first recursive call, the pair of numbers that is used for further recursive calls is $(b, a\ (mod\ b))$. Now since in this case, $a\ (mod\ b) < b$ and $a\ (mod\ b) < F_k$, using the induction hypothesis, we get that the number of further recursive calls is $< (k-1)$ and hence the total number of recursive calls is $< (k-1)+1 = k$.

- $a\ (mod\ b) \geq F_k$: In this case, the pair of numbers after the first recursive call is $(b, a\ (mod\ b))$. Let the pair after the second recursive call be $(a\ (mod\ b), d)$. Then, since $a\ (mod\ b) \geq F_k$ and $b < F_{k+1}$, we have $d < b + 1 - a\ (mod\ b) \leq F_{k+1} - F_k = F_{k-1}$. Moreover, since $d < b$, we can apply the inductive hypothesis to conclude that the total number of recursive calls is $< (k-2)+2 = k$.

The above two cases shows that $P(b)$ is true. So, using the principle of strong induction, we conclude that $P(n)$ holds for all values of $n \geq 1$. This concludes the proof of Lame's Theorem.