Algorithm Design and Analysis

Not Strong Enough

March 7, 2020

1 Bit Complexity of Euclid Algorithm

1.0.1: Exersise 6.

Remember the "period" algorithm for computing $F'_n := (F_n \mod k)$ discussed in class: (1) find some i, j between 0 and k^2 for which $F'_i = F'_j$ and $F'_{i+1} = F'_{j+1}$. Then for $d := j - i$ the sequence F'_n will repeat every d steps, as there will be a cycle. This cycle can either be a "true cycle" or a "lasso". Show that a lasso cannot happen. That is, show that the smallest i for which this happens is 0.

Proof. We prove it by contradiction.

Let $i_0 > 0$ be the smallest i for which this happen, i.e, for some $j > 0$ we have: for $\forall p \geqslant i_0 > 0, F'_{p+j} = F'_p$. Since for $p \geqslant 1$, the fibonacci numbers are defined as $F_{p+1} = F_p + F_{p-1}$, we have $F'_{p+1} = (F'_p + F'_{p-1}) \mod k$. It follows that $F'_{p-1} = (F'_{p+1} - F'_p + k) \mod k$.

Because $F'_{i_0} = F'_{i_0+j}, F'_{i_0+1} = F'_{i_0+1+j}$, we have

$$\begin{aligned} F'_{i_0-1} &= (F'_{i_0+1} - F'_{i_0} + k) \mod k \\ &= (F'_{i_0+1+j} - F'_{i_0+j} + k) \mod k \\ &= F'_{i_0-1+j} \end{aligned}$$

, which is contradict with out hypothesis.

Thus, i_0 isn't the smallest i, and we can conclude that the smallest i is 0. □