How to find $\gcd(f_{n+1}, f_{n+2})$ by using Euclidean algorithm for the Fibonacci numbers whenever $n > 1$?

Find $\gcd(f_{n+1}, f_{n+2})$ by using Euclidean algorithm for the Fibonacci numbers whenever $n > 1$. How many division algorithms are needed? (Recall that the Fibonacci sequence (f_n) is defined by setting $f_1 = f_2 = 1$ and $f_{n+2} = f_{n+1} + f_n$ for all $n \in \mathbb{N}^*$, and look here to get information about Euclidean algorithm)

(elementary-number-theory)

edited Sep 9 '11 at 12:57
J. M. isn't a mathematician
55.1k 5 126 261

asked Sep 9 '11 at 9:47
alvoutila
1,386 3 18 43

7 $\gcd(F_{n+1}, F_{n+2}) = \gcd(F_{n+1}, F_{n+2} - F_{n+1}) = \gcd(F_{n+1}, F_n)$, and then use induction... – anon Sep 9 '11 at 9:54

4 @anon: You could consider fleshing that out to a full answer? Given that the OP doesn't seem to be in the business of accepting answers it may not be worth your while? – Jyrki Lahtonen ♦ Sep 9 '11 at 10:56

1 Are Fibonacci numbers the "worst case" as far as efficiency of Euclid's algorithm is concerned? – Michael Hardy Sep 9 '11 at 13:46

1 @Michael: Yes. At each step, you can only subtract F_i once from F_{i+1}, so the number of iterations needed is maximal, given the size of the two initial numbers. – TMM Sep 9 '11 at 14:24

1 @Michael: I think that the proof of that (sometime in the early 1800s, I believe) was one of the first analyses of an algorithm as well as one of the first practical applications of the Fibonacci numbers. – Mike Spivey Sep 9 '11 at 15:26

1 Answer

anon's answer:

$$\gcd(F_{n+1}, F_{n+2}) = \gcd(F_{n+1}, F_{n+2} - F_{n+1}) = \gcd(F_{n+1}, F_n).$$

Therefore

$$\gcd(F_{n+1}, F_n) = \gcd(F_2, F_1) = \gcd(1, 1) = 1.$$

In other words, any two adjacent Fibonacci numbers are relatively prime.

Since

$$\gcd(F_n, F_{n+2}) = \gcd(F_n, F_{n+1} + F_n) = \gcd(F_n, F_{n+1}),$$

this is also true for any two Fibonacci numbers of distance 2. Since $(F_3, F_6) = (2, 8) = 2$, the pattern ends here - or so you might think...

It is not difficult to prove that

$$F_{n+k+1} = F_{k+1}F_{n+1} + F_kF_n.$$

Therefore

$$\gcd(F_{n+k+1}, F_{n+1}) = \gcd(F_kF_n, F_{n+1}) = \gcd(F_k, F_{n+1}).$$

Considering what happened, we deduce

$$(F_a, F_b) = F_{(a,b)}.$$

answered Sep 9 '11 at 12:31
Yuval Filmus
45.1k 3 61 131

1 Here's the complete proof and then some. Note that you don't need to first prove $(F_{n+1}, F_n) = 1$ since it is a special case. – Bill Dubuque Sep 9 '11 at 19:51

@anon: How do you get that gcd(F_{n+1}, F_{n+2})=gcd($F_{n+1}, F_{n+2} - F_{n+1}$)=gcd($F_n, F_{n+1}$)? I know that $F_{n+2} = F_{n+1} + F_n$, but how you get that $F_{n+2} = F_{n+2} - F_{n+1} = F_{n+1}$ – alvoutila Sep 10 '11 at 15:05

1 @alvoutilla: I'm not saying $F_{n+2} = F_n$, I'm using the well-known fact that $\gcd(a, b) = \gcd(a, b - a)$. If you're having trouble realizing why this works, consider thinking of a and b in terms of their prime factorizations (and use $\gcd(cn, cm) = c \cdot \gcd(n, m)$). – anon Sep 10 '11 at 22:48

@anon: But a and b are primes in this case(because they have not prime factorization except trivial one(a and b itself)? Where I use gcd(cn, cm) = c*gcd(n,m) and how I use it? like this gcd(ca,cb)=c gcd(a,b)= ...? – alvoutila Sep 12 '11 at 15:12

1 @alvoutila: You really shouldn't analyze the Euclidean algorithm without being fully familiar with basic gcd properties first. :) The identity I gave is independent of whether or not a, b are primes. First let's prove it holds when a, b are coprime. Suppose that $\gcd(a, b) = 1$ so that they are coprime and let

$d = \gcd(a, b-a)$. Since $d|a$ and $d|(b-a)$, d must also divide their sum $a+(b-a)=b$ (the sum of two multiples of a number d must also be a multiple of the number). But $d|a, d|b \implies d=1$ because they're coprime! (continued) – anon Sep 12 '11 at 19:10