Proof of Problem 7 in Chapter 7
15 November 2010
Corrected

In this proof I include proofs of the assertions in the hint to Problem 6. I decided that you didn't have to prove those assertions since they're suggested in the previous hint, but I think I ought to.

You'll notice that I don't use the Euclidean algorithm as the hint suggests.

Theorem 1. *For any integers $m, n > 0$, let $d = \gcd(m, n)$. Then $\gcd(f_m, f_n) = f_d$.*

I will use three lemmas in the proof. So, first I state and prove the lemmas.

Lemma 2. *The gcd function has the additive properties*

$$\gcd(a, b + ka) = \gcd(a, b)$$

for any integer k.

Proof. This is a fundamental property in number theory. A more basic property, proved from the unique factorization property of natural numbers (but I won't prove it), is that if $c|a$ and $c|b$, then $c|\gcd(a, b)$.

First we prove that $\gcd(a, b)$ divides $\gcd(a, b + ka)$. Define $d = \gcd(a, b)$. Since $d|a$ and $d|b$, we can write $a = d\alpha$ and $b = d\beta$. Then $b + ka = d(\beta + k\alpha)$, so $d|b + ka$. It follows that $d|\gcd(a, b + ka)$.

Now we prove that $d' = \gcd(a, b + ka)$ divides $\gcd(a, b)$. But this is implied by the first part. Let $a' = a$ and $b' = b + ka$; then $d'|b' - ka'$ by the first part with $-k$ instead of k, so $d'|b$. Therefore, $d'|\gcd(a, b) = d$. Since $d'|d$ and (as we showed previously) $d|d'$, $d = d'$. □

Lemma 3. *If a, c are relatively prime, then $\gcd(a, bc) = \gcd(a, b)$.*

Proof. Let $d = \gcd(a, b)$. Since $d|a$ and $d|b$ (so $d|bc$), d is a factor of $\gcd(a, bc)$. Now, suppose $\gcd(a, bc)/d \neq 1$; then $\gcd(a, bc)/d$ has a prime factor p. Thus, $pd|\gcd(a, bc)$.

It follows that $pd|a$ and $pd|bc$. However, $pd \nmid b$ because if it did, then $pd|a, b$ so $\gcd(a, b)$ would be a multiple of pd, while we know it is d, and $d < pd$. Since $pd \nmid b$, we deduce that $p \nmid (b/d)$. Also, $pd \nmid c$ because a, c are relatively prime and $p|a$. Because $(b/d)c$ has a unique prime factorization, any prime that divides it must divide either b/d or c. We have shown that $p \nmid b/d$ and $p \nmid c$. Therefore, $p \nmid (b/d)c$, so $pd \nmid bc$, contrary to the hypothesis about pd.

This contradiction proves that $\gcd(a, bc)/d = 1$, i.e., $\gcd(a, bc) = d = \gcd(a, b)$. □

Lemma 4. *For $n > m > 0$ we have the general recurrence formulas*

$$f_n = f_{m+1} f_{n-m} + f_m f_{n-m-1} = f_m f_{n-m+1} + f_{m-1} f_{n-m}.$$

Proof. We prove this by induction on m. The induction hypothesis $H(m)$ is:

$$f_n = f_{m+1} f_{n-m} + f_m f_{n-m-1} \text{ for all } n > m. \tag{1}$$

(Please note that the "for all $n > m$" is an essential part of the induction hypothesis. If you leave it out, your can't give a complete proof.)

For $m = 1$ the general formula says $f_n = f_2 f_{n-1} + f_1 f_{n-2}$. Since $f_1 = f_2 = 1$, this last is just the basic Fibonacci recurrence $f_n = f_{n-1} + f_{n-2}$, valid for $n \geq 2$. As $n > m = 1$, it is true that $n \geq 2$, so $H(1)$ is proved.

Now let $m > 1$ and assume $H(m-1)$ is true. That is, we're assuming

$$f_n = f_m f_{n-m+1} + f_{m-1} f_{n-m} \text{ for all } n \geq m. \tag{2}$$

We want to prove $H(m)$, that is, we want to prove

$$f_n = f_{m+1} f_{n-m} + f_m f_{n-m-1} \text{ for all } n > m. \tag{3}$$

Since $n > m$, Equation (2) applies, therefore

$$\begin{aligned} f_n &= f_m f_{n-m+1} + f_{m-1} f_{n-m} \\ &= f_m (f_{n-m} + f_{n-m-1}) + f_{m-1} f_{n-m} \\ &= f_m f_{n-m-1} + (f_{m-1} + f_m) f_{n-m} \\ &= f_m f_{n-m-1} + f_{m+1} f_{n-m}. \end{aligned} \tag{4}$$

This is $H(m)$, so we have deduced $H(m)$ from $H(m-1)$. By the Principle of Mathematical Induction, $H(m)$ is true for all $m \geq 1$.

To conclude the proof, note that in Equation (4) we showed that the last expression equals the middle expression in Lemma 4. □

Lemma 5. $\gcd(f_r, f_{r+1}) = 1$ *for all* $r \geq 0$.

Proof. Using Lemma 2, we see that

$$\gcd(f_r, f_{r+1}) = \gcd(f_r, f_r + f_{r-1}) = \gcd(f_r, f_{r-1}) = \gcd(f_{r'}, f_{r'+1})$$

where $r' = r - 1$. Thus, $\gcd(f_r, f_{r+1})$ is a constant, independent of the particular value of r. For instance, it equals $\gcd(f_1, f_2) = \gcd(1, 1) = 1$. □

Proof of Theorem 1. The proof is by strong induction on $\max(m, n)$, which (by choice of variable names) I may assume is n. The induction hypothesis is $H_{\text{Fib}}(n)$, stated as "If $m \in \{1, 2, \ldots, n\}$ and $d = \gcd(m, n)$, then $f_d = \gcd(f_m, f_n)$."

The base case is $n = 1$. Then $m = 1$, so $d = \gcd(m, n) = 1$. Moreover, $f_m = f_n = 1$ and $\gcd(f_m, f_n) = 1$. Since $f_1 = 1$, the induction assumption $H_{\text{Fib}}(1)$ is proved.

Now suppose $n > 1$ and assume $H_{\text{Fib}}(n')$ is true for all n' such that $0 < n' < n$. (This is the Strong Form of induction.) We want to prove $H_{\text{Fib}}(n)$. Thus, let $0 < m \leq n$. For convenience, define $k = m - n$.

There are two cases: $k = 0$ and $k > 0$.

If $k = 0$, then $m = n$ so $f_m = f_n$. Then $\gcd(m, n) = n$ and $\gcd(f_m, f_n) = f_n$, so the induction hypothesis is true.

Now assume $k > 0$. By Lemma 4,

$$f_n = f_{m+1} f_k + f_m f_{k-1}.$$

Since $d = \gcd(m, n)$, we have $d = \gcd(m, n - m) = \gcd(m, k)$ by Lemma 2. Therefore, by induction, $f_d = \gcd(f_m, f_k)$.

Now we evaluate

$$\gcd(f_m, f_n) = \gcd(f_m, f_{m+1} f_{n-m} + f_m f_{n-m-1}) = \gcd(f_m, f_{m+1} f_{n-m})$$

by Lemma 2. As f_m and f_{m+1} are relatively prime by Lemma 5,

$$\gcd(f_m, f_{m+1} f_{n-m}) = \gcd(f_m, f_{n-m})$$

by Lemma 3.

Now, $\gcd(m, n-m) = \gcd(m, n) = d$ by Lemma 2, and $\max(m, n-m) < n$, so by the induction hypothesis, $\gcd(f_m, f_{n-m}) = f_d$. Therefore, $\gcd(f_m, f_n) = f_d$. That proves $H_{\mathrm{Fib}}(n)$ assuming $H_{\mathrm{Fib}}(n')$ for all n' with $0 < n' < n$. By the Strong Form of the Principle of Mathematical Induction, $H_{\mathrm{Fib}}(n)$ is true for all $n > 0$. $\square$