GCD of Fibonacci Numbers

Saksham Sethi

Let F_n represent the n^{th} Fibonacci number.

1 Statement

$$\gcd(F_m, F_n) = F_{\gcd(m,n)}.$$

2 Proof

2.1 Lemma 1

2.1.1 Statement of Lemma 1

$$F_{m+n} = F_{m-1}F_n + F_m F_{n+1}.$$

2.1.2 Proof of Lemma 1

We will fix n arbitrarily and use induction on m.

Base Case: $m = 1$: The statement now becomes $F_{n+1} = F_0 F_n + F_1 F_{n+1}$. We know that $F_0 = 0$ and $F_1 = 1$, so the equation is now $F_{n+1} = (0)(1) + (1)(F_{n+1}) = F_{n+1}$, which is obviously true.

Inductive step: Assume that the statement holds true for some m. Therefore,

$$F_{(m+1)+n} = F_{m+(n+1)} = F_{m+n} + F_{m+(n-1)}$$
$$= \mathrm{F}_{m-1}F_n + F_m F_{n+1} + F_{m-1}F_{n-1} + F_m F_n$$
$$= (\mathrm{F}_m)(F_n + F_{n+1}) + (F_{m-1})(F_n + F_{n-1}) = (F_m)(F_{n+2}) + (F_{m-1})(F_{n+1})$$
or

$$F_{m+(n+1)} = (F_m)(F_{n+2}) + (F_{m-1})(F_{n+1}),$$

which completes our induction.

2.2 Lemma 2

2.2.1 Statement of Lemma 2

$$F_{mn} \text{ is divisible by } F_m$$

2.2.2 Proof of Lemma 2

Base Case: $n = 1$: This just gives F_m is divisible by F_m, which is of course true.

Inductive step on n: Assume that F_{mn} is divisible by F_m. Therefore,

$$F_{m(n+1)} = F_{mn+m} = F_{mn-1}F_m + F_{mn}F_{m+1},$$

where the last simplification was using Lemma 1.

Since we know by the assumption that F_{mn} is divisible by F_m and F_m is divisible by F_m, we know that the above expression is divisible by F_m as well, since both it's terms are separately. □

2.3 Proving the original statement

We will assign $n = qm + r$ for some integers q and r, and we will use Lemma 1 and Lemma 2 in our proof.

We know that

$$\gcd(F_m, F_n) = \gcd(F_m, F_{qm+r}) = \gcd(F_m, F_{qm-1}F_r + F_{qm}F_{r+1}),$$

where the last simplification is by Lemma 1. Also,

$$\gcd(F_m, F_{qm-1}F_r + F_{qm}F_{r+1}) = \gcd(F_m, F_{qm-1}F_r)$$

since $F_{qm}F_{r+1}$ is divisible by F_m by Lemma 2. Thus finally, we have

$$\gcd(F_m, F_n) = \gcd(F_m, F_{qm-1}F_r).$$

But we know that

$$\gcd(F_{qm}, F_{qm-1}) = \gcd(F_m, F_{qm-1}) = 1,$$

so we deduce that

$$\gcd(F_m, F_n) = \gcd(F_m, F_{qm-1}F_r) = \gcd(F_m, F_r).$$

or

$$\boxed{\gcd(F_m, F_n) = \gcd(F_m, F_r).}$$

If we recall, r was the remainder when n is divided by m. Aha! This looks like the Euclidean Algorithm! And we also know that

$$\gcd(m, n) = \gcd(m, \mathrm{rem}(n, m)) = \gcd(m, r)$$

or

$$\boxed{\gcd(m,n) = \gcd(m,r).}$$

Our two boxed statements reveal something important: that using the Euclidean Algorithm on F_m and F_n goes in exactly the same way as with using it on it's subscripts, and the other way around as well.

Therefore, when we finally get to

$$\gcd(m,n) = \gcd(\gcd(m,n), 0)$$

by repeatedly using the Euclidean Algorithm on the second boxed statement, we can say using our revelation that

$$\gcd(F_m, F_n) = \gcd(F_{\gcd(m,n)}, 0) = F_{\gcd(m,n)}$$

or

$$\boxed{\gcd(F_m, F_n) = F_{\gcd(m,n)}},$$

as desired. □

3 Remarks

3.1 General

The original statement is really fascinating! Trying some examples, we find the two other lemmas, and it turns out that they help proving the original proposition.

3.2 Thought Process

1. Take examples and see if it works

2. Explore Fibonacci numbers more, even if it is unrelated to the proposition.

3. Discovered Lemma 2

4. Attempt proving Lemma 2

5. Needed to have a simplification of F_{x+y} to prove it

6. Discovered Lemma 1

7. Proved Lemma 1

8. Used Lemma 1 to prove Lemma 2

9. Came back to the original statement

10. Simplified it using both Lemma 1 and 2

11. Noticing that Euclidean Algorithm revelation

12. Finishing it up

The main guideline I used in this problem is basically just alternating between experimenting and proving. And not only in this problem, this guideline extends to all proving problems.