Homework 2 Solutions

Math 318, Spring 2016

Problem 1.

Part (a)

Proposition. *If m and n are positive integers, then* $\gcd\big(2^m - 1, 2^n - 1\big) = 2^{\gcd(m,n)} - 1$.

Proof. We proceed by induction on $m + n$. The base case is $m + n = 2$, in which case $m = n = 1$ and the given statement clearly holds. For $m + n > 2$, we can assume without loss of generality that $m \leq n$. Then

$$\begin{aligned}\gcd\big(2^m - 1, 2^n - 1\big) \;&=\; \gcd\big(2^m - 1, (2^n - 1) - (2^m - 1)\big) \;=\; \gcd\big(2^m - 1, 2^n - 2^m\big) \\ &=\; \gcd\big(2^m - 1, 2^m(2^{n-m} - 1)\big) \;=\; \gcd\big(2^m - 1, 2^{n-m} - 1\big),\end{aligned}$$

where the equality follows from the fact that $2^m - 1$ and 2^m are relatively prime. Since $m + (n - m) < m + n$, our induction hypothesis tells us that

$$\gcd\big(2^m - 1, 2^{n-m} - 1\big) \;=\; 2^{\gcd(m,n-m)} - 1 \;=\; 2^{\gcd(m,n)} - 1$$

and hence $\gcd\big(2^m - 1, 2^n - 1\big) = 2^{\gcd(m,n)} - 1$. □

Part (b)

Proposition. *If n is composite then $2^n - 1$ is composite.*

Proof. Suppose n is composite, and let d be a positive divisor of n other than 1 or n. Then

$$\gcd\big(2^d - 1, 2^n - 1\big) \;=\; 2^{\gcd(d,n)} - 1 \;=\; 2^d - 1.$$

Thus $2^d - 1$ divides $2^n - 1$, and since $1 < 2^d - 1 < 2^n - 1$ is follows that $2^n - 1$ is composite. □

Problem 2.

The **Fibonacci sequence** $F_1, F_2, F_3, \ldots$ is defined by $F_1 = 1$, $F_2 = 1$, and

$$F_n \;=\; F_{n-1} + F_{n-2}$$

for all $n \geq 3$.

Part (a)

Proposition. *If $n \geq 2$ then F_{n-1} and F_n are relatively prime.*

Proof. We proceed by induction on n. For $n = 2$, we have $F_{n-1} = F_n = 1$, so F_{n-1} and F_n are relatively prime. For $n > 2$, we have

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

By our induction hypothesis, F_{n-1} and F_{n-2} are relatively prime, so F_{n-1} and F_n must be relatively prime as well. □

Part (b)

Proposition. *We have* $F_{m+n} = F_m F_{n+1} + F_{m-1} F_n$ *for all* $m \geq 2$ *and* $n \geq 1$.

Proof. We proceed by induction on n. For $n = 1$, the given equation is simply

$$F_{m+1} = F_m + F_{m-1},$$

which is the recurrence relation for the Fibonacci numbers. For $n > 1$, we change $m + n$ to $(m + 1) + (n - 1)$ and apply our induction hypothesis:

$$\begin{aligned} F_{m+n} \;&=\; F_{(m+1)+(n-1)} \;=\; F_{m+1}F_n + F_m F_{n-1} \\ &=\; (F_m + F_{m-1})F_n + F_m F_{n-1} \;=\; F_m(F_n + F_{n-1}) + F_{m-1}F_n \\ &=\; F_m F_{n+1} + F_{m-1} F_n. \end{aligned}$$

□

Part (c)

Proposition. *If* $m, n \geq 1$, *then* $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

Proof. We proceed by induction on $m + n$. The base case is $m + n = 2$, for which $m = n = 1$ and the given statement clearly holds. For $m + n > 2$, we can assume without loss of generality that $m \leq n$. If $m = 1$ or $m = n$ then clearly the statement holds, so we may assume that $m \geq 2$ and $n - m \geq 1$. Then it follows from part (b) that

$$F_n \;=\; F_{m+(n-m)} \;=\; F_m F_{n-m+1} + F_{m-1} F_{n-m}$$

so

$$\begin{aligned} \gcd(F_m, F_n) \;&=\; \gcd(F_m, F_m F_{n-m+1} + F_{m-1} F_{n-m}) \\ &=\; \gcd(F_m, F_{m-1} F_{n-m}) \;=\; \gcd(F_m, F_{n-m}), \end{aligned}$$

where the last equality follows from the fact that F_m and F_{m-1} are relatively prime. Since $m + (n - m) < m + n$, our induction hypothesis tells us that

$$\gcd(F_m, F_{n-m}) \;=\; F_{\gcd(m,n-m)} \;=\; F_{\gcd(m,n)}$$

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