CS 70 Discrete Mathematics and Probability Theory
Fall 2013 Week 3 Discussion

Modular Arithmetic

1. In class you learned how to compute $\gcd(a,b)$ using Euclid's algorithm. Now prove that for every number d such that $d|a$ and $d|b$, we must have $d|\gcd(a,b)$. Try to provide a mathematically rigorous proof.

2. Find out whether the equation $51x = 1 \pmod{113}$ has a solution, and find one if it does. What about the equation $85x = 119 \pmod{221}$?

3. Prove that if $x = y \pmod 3$ and $x = y \pmod 5$ then $x = y \pmod{15}$.

4. Prove the following:

   - If $x = y \pmod n$ and $z = w \pmod n$ then $xz = yw \pmod n$.
   - If x has two modular inverses y and z mod n, then $y = z \pmod n$.

5. Prove that Fibonacci numbers mod n become periodic. Find an upper-bound on the length of the period as a function of n. Next, prove that if $a|b$ then $F_a|F_b$. **Challenge:** first prove that $\gcd(F_a, F_b) = \gcd(F_{(b \bmod a)}, F_a)$, and then prove that $\gcd(F_a, F_b) = F_{\gcd(a,b)}$.