Fall 2013

18.310 Homework 9

Due Thursday November 14th at 6PM

Instructions: Remember to submit a separate PDF for each question. Do not forget to include a list of your collaborators or to state that you worked on your own.

1. The complete article (see homework 6) is due on Thursday Nov 14th. Some of you have not received yet feedback on their first, incomplete draft, but we hope everyone will have feedback within a day or so. In any case, you should try to improve your article as much as possible, and not limit yourself to addressing the comments the staff raised. In addition to uploading the article on online, you will also be asked to email it to 2 other students (to be chosen by us); additional instructions will follow next Wednesday.

   This version of your article will be peer-reviewed by two other 18.310 students, and these peer reviews will be due on Wed Nov 20th. The final version will be due on Wednesday December 11th.

2. Let $(f_n)_{n\geq 0}$ be the Fibonacci numbers: $f_0 = f_1 = 1$ and $f_i = f_{i-1} + f_{i-2}$ for $i \geq 2$. Calculate $gcd(f_{2012}, f_{2013})$. Also, find integers s and t such that $gcd(f_{2012}, f_{2013}) = s \cdot f_{2012} + t \cdot f_{2013}$.

3. Find all integer solutions to

$$x \equiv 10 \pmod{15}$$
$$x \equiv 5 \pmod{16}$$
$$x \equiv 7 \pmod{77}$$

4. Calculate (showing your steps) $13^{(23^{33})} \pmod{17}$.

5. Let $(G, *)$ be a finite group (i.e. $|G|$ is finite), and a be any element of G. Show that the inverse of a, denoted by a^{-1}, belongs to $\{a^1, a^2, a^3, \cdots, a^k, \cdots\}$, where a^1 is defined as a and a^k for $k > 1$ is defined as $a * a^{k-1}$.

6. Suppose Alice and Bob each generate public-private key pairs (N_A, z_A) and (N_A, y_A) for Alice and (N_B, z_B) and (N_B, y_B) for Bob, to be used for the RSA algorithm. But unfortunately, one of the primes that Bob used to construct his keys is the same as one of the primes that Alice used. Explain how Julie knowing this fact could find the private keys of both Alice and Bob.

18.310 Principles of Discrete Applied Mathematics
Fall 2013