Fall 2013

18.310 Homework 9 Solutions

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 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 $gcd(f_{2012}, f_{2013}) = s \cdot f_{2012} + t \cdot f_{2013}$.

   Solution: Note that

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

   Applying this formula inductively we get

$$\gcd(f_{2012}, f_{2013}) = \gcd(f_1, f_0) = 1.$$

   By the extended Euclidean algorithm, there are a_n, b_n integers such that

$$a_n f_n + b_n f_{n+1} = \gcd(f_n, f_{n+1}) = 1.$$

   For example

$$f_2 - f_1 = 1,$$

   and since $f_3 = f_2 + f_1$, we get

$$2f_2 - f_3 = 1,$$

   similarly since $f_4 = f_3 + f_2$,

$$2f_4 - 3f_3 = 1.$$

   By inspection, we guess that a solution to this problem is

$$(-1)^n (f_n f_n - f_{n-1} f_{n+1}) = 1.$$

   This is certainly true for $n = 1$, and

$$(-1)^n (f_n f_n - f_{n-1} f_{n+1}) = (-1)^{n-1} (f_{n-1} f_{n-1} - f_n (f_n - f_{n-1})) = (-1)^{n-1} (f_{n-1} f_{n-1} - f_n f_{n-2}) = 1.$$

   by induction.

3. Find all integer solutions to

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

Solution: Since 15 and 16 are coprime, by the Chinese remainder theorem, there will be precisely one residue class modulo 240 as the solution to the first two equations. Using the first two equations we get that

$$x = 10 + 15k \equiv 5 \pmod{16}$$

implies

$$16k - k \equiv -k \equiv -5 \pmod{16}$$

so that $k \equiv 5 \pmod{16}$ and

$$x = 85 + 240\ell.$$

Since 240 and 77 are also coprime there will be precisely one solution modulo 18480. Using the last equation we get

$$x = 85 + 240k \equiv 8 + 9k \equiv 7 \pmod{77}.$$

This implies $9k \equiv -1 \pmod{77}$, and since $9^{-1} \equiv -17 \pmod{77}$, we get

$$k \equiv 17 \pmod{77},$$

and then

$$x \equiv 85 + 240 * 17 = 4165 \pmod{18480}$$

is the solution to this system.

4. Calculate (showing your steps) $13^{(23^{33})} \pmod{17}$. Note that by Fermat's little theorem (since 17 is prime), $13^{16} \equiv 1 \pmod{17}$. So write

$$13^{(23^{33})} = 13^{(16k+(23^{33}) \mod 16)} \equiv 13^{((23^{33}) \mod 16)} \pmod{17}.$$

Let's calculate then

$$23^{33} \equiv 7^{33} = (7^2)^{16}7 \equiv 1^{16}7 = 7 \pmod{16}.$$

Finally we get

$$13^{(23^{33})} \equiv 13^7 = (169)^3 13 \equiv (-1)^3 13 = -13 \equiv 4 \pmod{17}.$$

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 $a * a^{k-1}$.

Solution: Since G is finite there are some $i < j$ such that $a^i = a^j$. Equivalently, there is a positive integer k such that $a^k = 1$. Note that if $k = 1$, we get $a = 1$, and then $a^{-1} = a = a^1$. On the other hand, if $k > 1$, $1 = a^k = aa^{k-1}$, and then $a^{-1} = a^{k-1}$.

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.

Solution: Julie knows that $N_A = p_A q_A$, and $N_B = p_A q_B$. Calculating $\gcd(N_A, N_B) = p_A$ she can get the first prime, and then dividing get the second one for both.

18.310 Principles of Discrete Applied Mathematics
Fall 2013