CS 70 Fall 2016 — Discrete Mathematics and Probability Theory — Seshia and Walrand — HW 5

1. **Sundry**

   Before you start your homework, write down your team. Who else did you work with on this homework? List names and email addresses. (In case of hw party, you can also just describe the group.) How did you work on this homework? Working in groups of 3-5 will earn credit for your "Sundry" grade.

   Please copy the following statement and sign next to it:

   I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up.

2. **Amaze Your Friends**

   (a) You want to trick your friends into thinking you can perform mental arithmetic with very large numbers What are the last digits of the following numbers?

   i. 11^{2014}

   ii. 9^{10001}

   iii. $3^{987654321}$

   (b) You know that you can quickly tell a number n is divisible by 9 if and only if the sum of the digits of n is divisible by 9. Prove that you can use this trick to quickly calculate if a number is divisible by 9.

3. **Short Answer: Modular Arithmetic**

   (a) What is the multiplicative inverse of $3 \pmod 7$?

   (b) What is the multiplicative inverse of $n-1$ modulo n? (An expression that may involve n. Simplicity matters.)

   (c) What is the solution to the equation $3x = 6 \pmod{17}$? (A number in $\{0,\dots,16\}$ or "No solution".)

   (d) Let $R_0 = 0; R_1 = 2; R_n = 4R_{n-1} - 3R_{n-2}$ for $n \geq 2$. Is $R_n = 2 \pmod 3$ for $n \geq 1$? (True or False)

   (e) Given that $extended-gcd(53,m) = (1,7,-1)$, that is $(7)(53)+(-1)m = 1$, what is the solution to $53x+3 = 10 \pmod m$? (Answer should be an expression that is interpreted $(\bmod\ m)$, and shouldn't consists of fractions.)

4. (a) Compute the inverse of 37 modulo 64 using Euclid's extended GCD algorithm.

(b) Prove that $gcd(F_n, F_{n-1}) = 1$, where $F_0 = 0$ and $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$.

5. **Tweaking RSA**

   (This problem will not be graded, the solution will be posted on the problem thread on piazza.)

   (a) You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and p is prime. Similar to the original method, for any message $x \in \{0, 1, \dots, N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$. Show how you choose e and d in the encryption and decryption function, respectively. Prove that the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

   (b) Can Eve now compute d in the decryption function? If so, by what algorithm?

   (c) Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where p, q, r are all prime). Explain how you can do so.

6. **Using RSA** Kevin and Bob decide to apply the RSA cryptography so that Kevin can send a secret message to Bob.

   (a) Assuming $p = 3$, $q = 11$, and $e = 7$, what is d? Calculate the exact value.

   (b) Following Part (a), what is the original message if Bob receives 4? Calculate the exact value.

7. **(Breaking RSA)**

   (a) Eve is not convinced she needs to factor $N = pq$ in order to break RSA. She argues: "All I need to know is $(p-1)(q-1)$... then I can find d as the inverse of e mod $(p-1)(q-1)$. This should be easier than factoring N". Prove Eve wrong, by showing that if she knows $(p-1)(q-1)$, she can easily factor N (thus showing finding $(p-1)(q-1)$ is at least as hard as factoring N).. Assume Eve has a friend Wolfram, who can easily return the roots of polynomials over $\mathbb{R}$ (this is, in fact, easy).

   (b) When working with RSA, it is not uncommon to use $e = 3$ in the public key. Suppose that Alice has sent Bob, Carol, and Dorothy the same message indicating the time she is having her birthday party. Eve, who is not invited, wants to decrypt the message and show up to the party. Bob, Carol, and Dorothy have public keys $(N_1, e_1), (N_2, e_2), (N_3, e_3)$ respectively, where $e_1 = e_2 = e_3 = 3$. Furthermore assume that N_1, N_2, N_3 are all different. Alice has chosen a number $0 \leq x < \min\{N_1, N_2, N_3\}$ which indicates the time her party starts and has encoded it via the three public keys and sent it to her three friends. Eve has been able to obtain the three encoded messages. Prove that Eve can figure out x. First solve the problem when two of N_1, N_2, N_3 have a common factor. Then solve it when no two of them have a common factor. Again, assume Eve is friends with Wolfram as above.

Hint: The concept behind this problem is the Chinese Remainder Theorem: Suppose $n_1, ..., n_k$ are positive integers, that are pairwise co-prime. Then, for any given sequence of integers $a_1, ..., a_k$, there exists an integer x solving the following system of simultaneous congruences: $\begin{cases} x \equiv a_1 (\bmod n_1) \\ x \equiv a_2 (\bmod n_2) \\ ... \\ x \equiv a_k (\bmod n_k) \end{cases}$

Furthermore, all solutions x of the system are congruent modulo the product, $N = n_1 ... n_k$. Hence: $x \equiv y (\bmod n_i) for 1 \leq i \leq k \Leftrightarrow x \equiv y (\bmod N)$