COMP 2711H Discrete Mathematical Tools for Computer Science
2021 Fall Semester
Homework 2: Number Theory and Cryptography
Handed out: Sep 29
Due: Oct 13

Problem 1. In class, we defined modulo m multiplication ($\cdot_m$) and modulo m addition ($+_m$) over the set of integers $Z_m = \{0, 1, \ldots, m-1\}$. State and prove the distributive law for $\cdot_m$ over $+_m$.

Problem 2. Recall that if a prime number divides a product of two integers, then it divides one of these two integers.

(a) Use this to show that as b runs through the integers from 0 to $p-1$, with p prime, the products $a \cdot_p b$ are all different (for each fixed choice of a between 1 and $p-1$).

(b) Explain why (a) implies that every integer greater than 0 and less than p has a unique multiplicative inverse in Z_p if p is prime.

Problem 3. Prove that if an element of Z_n has a multiplicative inverse, then it has a unique inverse in Z_n.

Problem 4. Consider the recursive implementation of Euclid's GCD algorithm. Given inputs x and y, roughly how many times does this program make a recursive call to itself. Try to relate this to the total number of digits in x and y.

Problem 5. Recall that the sequence of Fibonacci numbers are defined as follows: $F_0 = 0, F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. Show that any two successive Fibonacci numbers are relatively prime.

Problem 6. Consider the following modular equation:

$$16 \cdot_{55} x = 15.$$

Does it have any solution $x \in Z_{55}$? If yes, show how to obtain the solution(s). If not, explain why not.

Problem 7. How many solutions with x between 0 and 34 are there to the system of equations

$$\begin{aligned} x \mod 5 &= 4 \\ x \mod 7 &= 5\ ? \end{aligned}$$

What are these solutions? Present two different ways for solving this problem, one of which uses the method based on the proof of the Chinese Remainder Theorem.

Problem 8. Prove that $n^7 - n$ is divisible by 42. (*Hint:* Apply Fermat's little theorem to show that $n^7 \equiv n \pmod{p}$, for $p = 2, 3$ and 7.)

Problem 9. We implement the RSA cryptosystem by choosing two prime numbers $p = 23$ and $q = 37$. (In practice the prime numbers used should be very large.) We further choose a number $e = 17$ which is relatively prime to $(p-1)(q-1) = 22 \cdot 36 = 792$.

(a) What is the value of the secret key d? You should show all the calculations and further verify that it satisfies the requirement of a secret key.

(b) Suppose the message is 100. Show how to use the RSA cryptosystem to encrypt the message and then decrypt the resulting message. Show all your calculations.

Problem 10. Prove that p divides

$$(p-1)!\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots \frac{1}{p-1}\right)$$

if $p \geq 3$ is a prime number.