COMP 2711H Discrete Mathematical Tools for Computer Science
2014 Fall Semester
Homework 4
Handed out: Nov 10
Due: Nov 19

Problem 1. Recall the standard divisibility rule for 3: an integer is divisible by 3 if and only if the sum of its digits is divisible by 3. State and prove divisibility rules for $4, 9$, and 11.

Problem 2. 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 3. Prove that $n^{13} - n$ is divisible by 2730.

Problem 4. 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 5. Recall that Z_n represents the set of integers $\{0, 1, \cdots, n-1\}$ and $\cdot_n$ represents the multiplication operator modulo n. Consider the set of numbers $\{5 \cdot_8 1, 5 \cdot_8 2, \ldots, 5 \cdot_8 7\}$. Do these numbers form a permutation of the nonzero elements of the set Z_8? Would you get a permutation if you used another nonzero member of Z_8 in place of 5? What general principle explains these observations? State the general principle and give a proof of it.

Problem 6. Compute the fourth power mod 10 of each element of Z_{10}. What do you observe? In particular, when is the result 1 and when is it not 1? What famous theorem explains your observations? State the theorem (extend it if necessary to explain your observations) and give a proof of it.

Problem 7. Show that any prime $p > 5$ divides infinitely many integers in the sequence $9, 99, 999, 9999, \ldots$.

Problem 8. Let p be a prime number. Prove that if $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.

Problem 9. Consider the system of congruences $x \equiv 4 \pmod{6}$ and $x \equiv 13 \pmod{15}$. Find all solutions to this system of congruences using two different methods: (a) the method of back substitution and (b) the method suggested by the construction used in the proof of the Chinese remainder theorem. (*Hint:* It may be convenient to first transform the congruences to equivalent congruences modulo suitable prime numbers.)

Problem 10. 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 11. Prove that an integer $n > 1$ is prime if and only if the following holds: $(n-1)! \equiv -1 \pmod{n}$. (This is known as Wilson's theorem.)

Problem 12. 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.