CSCI 0220 Discrete Structures and Probability C. Klivans

Recitation 3

Date: March 8, 2015

Problem 3.1

In public key cryptography, each individual has a public key and a secret key. The public key is used to encrypt messages, and the secret key is used to decrypt messages. The public key is known by everyone, so that anyone can encrypt a message and send it to the individual. The secret key is known only by the individual, so that only they can decrypt the messages sent to them.

A common example of public key cryptography uses the product of two large distinct primes $n = pq$ as a public key and the factorization (p, q) as a secret key. In this problem, we will explore one tactic for discovering someone's secret key.

Let $n = pq$ be a public key. Suppose you have found two integers x and y such that $x^2 \equiv y^2 \mod n$, but $x \not\equiv \pm y \mod n$. Explain how you can find (p, q).

Problem 3.2

Goal: Prove that if p is prime, then $(p-1)! \equiv$ -1 (mod p)

a) Show that if x∈{2,3,...,p-2}, there exists a y such that xy ≡ 1 (mod p)

b) Show that y ≠ 1, x, or p-1

c) Conclude the proof of the theorem.

d) Apply the theorem to find the remainder of 97! when divided by 101.

Problem 3.3

Use induction to prove the following generalization of one of De Morgan's laws:

$$\neg(p_1 \vee p_2 \vee p_3 \vee ... \vee p_n) = \neg p_1 \wedge \neg p_2 \wedge ... \wedge \neg p_n$$

for $n \in \mathbb{Z}^+, n \geq 2$.

Problem 3.4

Find the value of the missing literal "x" in each of the following logical equations:

(a) $x \wedge (x \vee 1) = 0$

(b) $(x \vee 1) \wedge (x \vee 0) = 1$

(c) $1 \rightarrow ((1 \rightarrow \neg x) \wedge (x \rightarrow 1)) = 0$

(d) $(x \rightarrow (x \rightarrow (x \wedge \neg x))) = x$