CS1231 TUTORIAL 8

1. Consider the RSA cryptosystem with $p = 29$, $q = 53$, so that $n = pq = 1537$ and with $e = 47$. Thus the enciphering key is $(1537, 47)$.

(i) Encrypt the message HELP using 01 for A, 02 for B, etc..

(ii) Decrypt the message obtained in (i).

2. Let a and b be positive integers and d be the smallest positive integer that can be written in the form $as + bt$, where $t, s \in \mathbb{Z}$. Prove that $d = \gcd(a, b)$.

3. Prove the following by mathematical induction.

(a) $\sum_{i=1}^{n+1} i2^i = n2^{n+2} + 2 \ \forall n \in \mathbb{Z}^*$.

(b) $6 \mid 7^n - 1 \ \forall n \in \mathbb{Z}^*$.

(c) $1 + nx \leq (1 + x)^n$ for each integer $n \geq 2$ and for all real numbers $x > -1$.

4. Suppose that $h_0, h_1, \ldots$ is a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_2 = 3 \qquad \text{and} \qquad h_k = h_{k-1} + h_{k-2} + h_{k-3} \quad \text{for} \quad k \geq 3$$

Prove that $h_n \leq 3^n$ for all $n \geq 0$.

5. What's wrong with the following proof that $2^n = 1$ for all $n \in \mathbb{Z}^*$?

Basis step: $2^0 = 1$.

Inductive step: Assume that $2^j = 1$ for $j = 0, 1 \ldots, k$. Then

$$2^{k+1} = \frac{2^k \cdot 2^k}{2^{k-1}} = \frac{1 \cdot 1}{1} = 1.$$

6. For which positive integer is the following true? Make an educated guess.

$$2^n > n^2 + n$$

Next give a proof using mathematical induction.