CS1231 TUTORIAL 8

1. Translate the message into an integer:

$$08 \;\; 051 \;\; 216$$

Encrypt each block using $C = M^e$ **Mod** 2537:

$$8^{47} \textbf{ Mod } 1537 = 814, \quad 51^{47} \textbf{ Mod } 1537 = 419, \quad 216^{47} \textbf{ Mod } 1537 = 1456$$

The encripted message is

$$814 \;\; 419 \;\; 1456.$$

(b) We need to find the inverse d of $e = 47 \bmod (p-1)(q-1) = 1456$. Using the Euclidean algorithm, we have

$$\begin{aligned} 1456 &= 47 \cdot 30 + 46 \qquad & 1 &= 47 - 46 \cdot 1 \\ 47 &= 46 \cdot 1 + 1 & &= 47 - (1456 - 47 \cdot 30) \cdot 1 = 47 \cdot 31 - 1456 \cdot 1 \end{aligned}$$

Thus $d = 31$. The decryption formula is thus $M = C^{31}$ **Mod** 1537.

$$814^{31} \textbf{ Mod } 1537 = 8 \quad 419^{31} \textbf{ Mod } 1537 = 051 \quad 1456^{31} \textbf{ Mod } 1537 = 216$$

The message is 8051216 which translates back to HELP.

Note: All the congruences are calculated using modular exponentiation.

2. Let $d = au + bv$. We first prove that $d \mid a$. Dividing a by d, we have $a = qd + r$ where $q \in \mathbb{Z}^+$ and $0 \le r < d$. Then, replacing d by $au + bv$ and simplifying, we have $r = a(1 - uq) + b(-vq)$. Thus r can also be written in the form $as + bt$. But $r < d$. Thus $r > 0$ will lead to a contradiction. So $r = 0$ and we conclude that $d \mid a$. Similarly $d \mid b$.

Now if e is a common divisor of a and b, then, using $d = au + bv$, we conclude that $e \mid d$. Thus $e \le d$.

So all common divisors are $\le d$ and whence $d = \gcd(a, b)$.

3. (a) Basis step: It's easily checked that it's true for $n = 0$.

Inductive step: Assume that it's true for $0, 1, \ldots, k$. Now for the case $k + 1$:

$$\begin{aligned} \sum_{i=1}^{k+2} i2^i = (k+2)2^{k+2} + \sum_{i=1}^{k+1} i2^i &= (k+2)2^{k+2} + (k)2^{k+2} + 2 \\ &= (2k+2)2^{k+2} + 2 = (k+1)2^{k+3} + 2 \end{aligned}$$

Thus the result holds for $k+1$ and the proof is complete.

(b) Basis step: True for $n = 0$ (check this)

Inductive step: Assume that the result holds for some $0, 1, \ldots, k$. Thus $6 \mid 7^k - 1$, or $7^k - 1 = 6q$ for some $q \in \mathbb{Z}$. Now consider the case $k+1$.

Then $7^{k+1} - 1 = 7(7^k) - 1 = 7(6q+1) - 1 = 6(7q+1)$. Thus $6 \mid 7^{k+1}$. The proof is now complete by M.I.

(c) Basis step: When $n = 2$, we have $(1+x)^2 = 1 + 2x + x^2 \geq 1 + 2x$ (since $x^2 \geq 0$). Thus the result is true for $n = 2$.

Inductive step: Assume that the result holds for $2, 3, \ldots, k$. Thus $1 + kx \leq (1+x)^k$. Now consider the case $k+1$. Thus

$$(1+x)^{k+1} = (1+x)(1+x)^k \geq (1+x)(1+kx) = 1 + (k+1)x + kx^2 \geq 1 + (k+1)x$$

The last two inequalities are true because $1 + x \geq 0$ and $kx^2 \geq 0$. Hence the result holds for $k+1$ as well. The proof is now complete by M.I.

4.

Basis step: Note that $h_n \leq 3^n$ for $n = 0, 1, 2$.

Inductive step: Now assume that it's true for all $n = 0, 1, 2, \ldots k$, where $k \geq 2$. Then

$$h_{k+1} = h_k + h_{k-1} + h_{k-2} \leq 3^k + 3^{k-1} + 3^{k-2} = 13.3^{k-2} \leq 27.3^{k-2} = 3^{k+1}.$$

Hence the result holds for $n = k+1$ and the proof is complete.

5. The inductive step is not valid for $k = 0$ because the denominator becomes $2^{k-1} = 2^{-1}$ and this is not covered by the induction hypothesis.

6. $n = 1, 2, 3, 4$: False. True when $n = 5, 6$. Thus should be true for $n \geq 5$.

Base case: $n = 5$, already checked.

Inductive step: Suppose the inequality holds for $n = 5, \ldots, k$ for some integer $k \geq 5$. Now

$$\begin{aligned}
2^{k+1} &= 2 \cdot 2^k > 2(k^2 + k) \\
&= [(k+1)^2 + (k+1)] - [(k+1)^2 + (k+1)] + 2k^2 + 2k \\
&= [(k+1)^2 + (k+1)] - k^2 - 2k - 1 - k - 1 + 2k^2 + 2k \\
&= [(k+1)^2 + (k+1)] + k^2 - k - 2 \\
&> (k+1)^2 + (k+1)
\end{aligned}$$

since $k^2 - k - 2 = k(k-1) - 2 > 0$ for $k \geq 5$.

Alternatively, you can also work from $(k+1)^2 + (k+1)$. For $k \geq 5$,

$$(k+1)^2 + (k+1) = k^2 + 3k + 2 < k^2 + 4k < k^2 + k^2 = 2k^2 < 2(k^2 + k) < 2 \cdot 2^k = 2^{k+1}.$$