**MAN 240 (2003) : Inlämningsuppgift 1**

**1 (2.6.12 in old Biggs)** A *lattice point* in 3-dimensional space is a point all of whose coordinates are integers. Show that if we are given nine lattice points then there is at least one pair for which the midpoint of the line segment joining them is also a lattice point.

**2.** How many different 'words' can you make from the letters of the word 'inlämningsuppgift' ?

**3.** How many poker hands give
**(i)** nothing
**(ii)** a pair
**(iii)** two pairs
**(iv)** three of a kind
**(v)** a straight
**(vi)** a flush
**(vii)** a full house
**(viii)** four of a kind
**(ix)** a straight flush
**(x)** a royal flush ?

**4.** You are faced with a class of 20 screaming children, so to shut them up you give them some candy. Say you have 70 pieces of candy and you want to make sure each child gets at least 2 pieces (since you're a sadist, you let them fight over the rest !!). How many ways can the candy be divided up ?

**5.** Simplify as much as possible the expression

$$\sum_{k=0}^{n} k \cdot \binom{n}{k}.$$

(N.B.: For full points, you will avoid all use of the formula for binomial coefficients).

**6.** Prove the following identities 'combinatorially' (i.e.: by showing that both sides count the same thing in two different ways and thereby avoiding use of the formula for binomial coefficients) :

$$\binom{n}{k} \cdot \binom{k}{i} = \binom{n}{i} \cdot \binom{n-i}{k-i},$$
$$n \cdot \binom{2n}{n} = (n+1) \cdot \binom{2n}{n+1}.$$

(In the first identity, $n \geq k \geq i$ are non-negative integers).

**7.** Find and prove a formula for the sum of the first $n$ odd positive integers, without using induction on $n$.

**8.** A collection $\mathcal{C}$ of subsets of $\{1, ..., n\}$ is said to be intersecting if

$$A \cap B \neq \phi$$

for each pair of subsets from $\mathcal{C}$. Find (with proof) the maximum possible number of subsets in such a collection (as a function of $n$).

**9.** Let $k \leq l \leq n$ be positive integers. Let $A, B$ be subsets of $\{1, ..., n\}$ of size $k, l$ respectively. $A$ is said to *cover* $B$ if $A \subseteq B$.

Find (with proof) the smallest possible size of a collection of 2-element subsets of $\{1, ..., n\}$ which covers all 3-element subsets of $\{1, ..., n\}$.

* **10.** Consider the map $\pi : \mathbf{N} \rightarrow \mathbf{N}$ defined inductively as follows :

(i) $\pi(1) = 1,\ \pi(2) = 2$,

(ii) for each $k \geq 3$, $\pi(k)$ is the smallest number which does not appear among $\pi(1), ..., \pi(k-1)$ such that, for no $1 \leq i \leq k/2$ is it the case that

$$\pi(k) - \pi(k-i) = \pi(k-i) - \pi(k-2i).$$

(Note : For obvious reasons, the map $\pi$ is said to 'avoid arithmetic progressions'. The first few terms in the sequence $(\pi(n))$ are 1,2,4,3,5,6,8,7,10,9,13,...).

**(i)** Show that $\pi$ is a bijection from $\mathbf{N}$ to $\mathbf{N}$.

(By definition, $\pi$ is injective. The hard part is to show it is surjective).

**(ii)** Show that, in fact, for all positive integers $n$,

$$\frac{1}{4} \leq \frac{\pi(n)}{n} \leq \frac{3}{2}.$$

[Note : I have a conjecture that

$$\lim_{n \to \infty} \frac{\pi(n)}{n}$$

exists and equals 1. If you can either prove or disprove this conjecture, then I will give you VG on the course without doing any more work !!].

**11.** Let $n$ be a positive integer which is a product of two distinct, unknown primes $p$ and $q$. Assuming you know both $n$ and $\phi(n)$, explain how you would find $p$ and $q$.

(Remark : The point of this exercise is to illustrate how knowledge of $\phi(n)$ is the key to breaking an RSA cryptosystem).

***** denotes an exercise which I consider somewhat more difficult than the others.