MATEMATIK
Chalmers tekniska högskola

Tentamen i DISKRET MATEMATIK (TMA965)
23 oktober 2006, kl 8.30–12.30

Hjälpmedel: inga. No books, notes or calculators.
Telefonvakt: Jan Stevens, 0709-322268

OBS! Linje och inskrivningsår samt namn och personnummer skall anges.

---

1. Consider the RSA public-key crypto system with public key $(e, n) = (3, 33)$. Use $A = 1$, $\ldots$, $Z = 26$, @ $= 27$, & $= 28$, \$ $= 29$, ␣ (space) $= 30$, % $= 31$, ! $= 32$ and . $= 0$.
a) Encrypt CHALMERS.
b) Determine the decryption key d and decrypt the message 'MII%FLU@K!'. (10 p)

2. a) Give a combinatorial proof for the equality

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

when $0 < k < n$.
b) Give a combinatorial proof for the equality

$$3^n = \sum_{k=0}^{n} \binom{n}{k} 2^k .$$

3. Show that for any graph G holds

$$\chi(G) \leq \frac{1}{2} + \sqrt{2|E| + \frac{1}{4}} .$$

4. What is the last digit in the number 7^{2006}?

5. Consider a group with 91 elements. Prove that there exists an element whose order is 7.

6. a) Construct a linear code with 3×6 check matrix, which corrects one error.
b) Correct, if necessary, the words 111011 and 100111.

Good luck! Jan Stevens