Mat – 1.128   **Elements of Discrete Mathematics** (3 cp)

2nd partial examination   6.5.2003

Write first clearly on each sheet of paper

– Mat–1.128   EDM,   2nd part. exam.   6.5.2003

– Student identification number, family name, given names, faculty, signature

Scientific (non-programmable) calculators allowed.

1.   *a)*   Find the inverse 52^{-1} (mod 650),   if it exists.

b)   Solve the congruence problem $52\,x \equiv 338$ (mod 650).

2.   We know that the integer $n = pq = 137\,591$ is a product of two prime numbers, and that $\varphi(n) = 136\,752$.   Find the primes p and q.

3.   *a)*   Construct the Galois field $GF(25)$.

b)   Find all values for $\sqrt{\sqrt{2}} \in GF(25)$.

4.   A Hamming   (7, 4) – code has the parity check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

a)   Encode the message words   1101   and   1010.

b)   Decode the received words   1111000   and   0110011.

c)   A symmetric binary channel is used for data transmission. The error probability in transmission of a single bit is $p = 0.8\,\%$.   What is the probability for an erroneous decoding of the two–word message in part   *a)* ?