Solutions exam TMA965 discrete mathematics 23 October 2006

1. We compute $r^3 \bmod 33$. This can be done by first computing modulo 3 (note that $r^3 \equiv r \pmod 3$) and modulo 11. We have $(\pm 2)^3 \equiv \pm 8 \pmod 11$, $(\pm 3)^3 \equiv \pm 5 \pmod{11}$, $(\pm 4)^3 \equiv \pm 9 \pmod{11}$ and $(\pm 5)^3 \equiv \pm 4 \pmod{11}$. We find from CHALMERS = 3 8 1 12 13 5 18 19 the sequence 27 17 1 12 19 26 24 28 or @QALSZX&.
Because $\varphi(33) = 2 \cdot 10$ and $3 \cdot 7 \equiv 1 \pmod{20}$ is $d = 7$. We have $r^7 \equiv r \pmod 3$ and $(\pm 2)^7 \equiv \pm 7 \pmod{11}$, $(\pm 3)^7 \equiv \pm 9 \pmod{11}$, $(\pm 4)^7 \equiv \pm 5 \pmod{11}$ and $(\pm 5)^7 \equiv \pm 3 \pmod{11}$. From MII%FLU@K! = 13 9 9 31 6 12 21 27 11 32 we get 7 15 15 4 30 12 21 3 11 32 = GOOD LUCK!.

2. a) Divide the k-element subsets of $\{1, \ldots, n\}$ into two classes, those not containing 1 and those containing 1. There are $\binom{n-1}{k}$ of the first type and $\binom{n-1}{k-1}$ of the second type.
b) The left hand side counts the number of words of length n in the alphabet 1, 2, 3. For each $0 \leq k \leq n$ the number of words with exactly $n-k$ 1's is $\binom{n}{k}2^k$ since we first choose $n-k$ places for the 1's, or equivalently k places for the 2's and 3's, and then put on the k places a word of length 2 in the alphabet 2, 3. Summing over all k gives all words, thereby proving the formula combinatorially.

3. We show that $|E| \geq \frac{1}{2}\chi(\chi - 1)$. Solving for χ gives then the required formula. Let the graph be coloured with the minimal number of colours. Consider two colours. Between the vertices with the first colour and those of the second colour there is at least one edge, for otherwise all the vertices considered could be given the same colour. Therefore there are at least as many edges as there are pairs of colours, namely $\binom{\chi}{2}$.

4. We compute modulo 10. As $\varphi(10) = 4$ and $\gcd(7, 10) = 1$ we have that $7^4 \equiv 1 \bmod 10$ by Euler's theorem. As $2006 = 4 \cdot 501 + 2$ we get $7^{2006} \equiv 1^{501} \cdot 7^2 \equiv 9 \bmod 10$. Hence the last digit is 9.

5. The order of an element can be 1, 7, 13 or 91. If x has order 91, then x^{13} has order 7. Assume there is no element of order 7. Then every $x \neq 1$ has order 13. Each such element generates a cyclic subgroup of order 13. Two such subgroups intersect in a subgroup whose order is a divisor of 13, so they coincide or have only the identity in common. Therefore the complement of the identity is partitioned into disjoint sets with 12 elements each. But $91 - 1 = 90$ is not divisible by 12. This contradiction shows that the assumption made, that there is no element of order 7, is not correct.

6. a) The matrix

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

has no column containing only zeroes and all columns are distinct, so the code with check matrix H corrects one error.
b) The error syndrome for 111011 is $(0, 1, 1)^t$ and for 100111 $(1, 1, 0)^t$. The first word has one error at position 3, the second at position 6. They are corrected to 110011 and 100110.