**LUNDS TEKNISKA HÖGSKOLA** **LÖSNINGAR**
**MATEMATIK** **DISKRET MATEMATIK FMAA25/MATB13**
**2017–08–14**

**1.** Using inclusion/exclusion with condition $c_i$=is divisible by $i$ we get that $S_0 - S_1 + S_2 - S_3$ numbers are not divisible by any the three numbers. Therefore $S_1 - S_2 + S_3$ numbers are satisfying at least one condition. Using $S_1 = N(c_3) + N(c_7) + N(c_{10}) = \lfloor \frac{100}{3} \rfloor + \lfloor \frac{100}{7} \rfloor + \lfloor \frac{100}{10} \rfloor = 57$, $S_2 = N(c_3c_7) + N(c_3c_{10}) + N(c_7c_{10}) = \lfloor \frac{100}{21} \rfloor + \lfloor \frac{100}{30} \rfloor + \lfloor \frac{100}{70} \rfloor = 8$ and $S_3 = N(c_3c_7c_{10}) = 0$ we find that $S_1 - S_2 + S_3 = 49$

**2.** Let $p(x) = x^3 + 2x^2 + 2x + 2$.

**a)** Dividing $x^5$ by $p(x)$ we find that $x^5 = (x^2 - 2x + 2)p(x) + (-2x^2 + 1)$. (The computation is in $\mathbb{Z}_5[x]$ so coefficients are reduced modulo 5.) This shows that $[x^2][x^3] = [-2x^2 + 1]$.

**b)** Using the Euclidean algorithm on $q(x) = x^2 + 2x$ and $p(x)$ and backsubstituting we find that $1 = (-2x - 2)p(x) + (2x^2 + 2x - 1)q(x)$. This shows that $[2x^2 + 2x - 1]$ is an inverse of $q(x)$.

**c)** $R$ is a field if and only if $p(x)$ is irreducible. Since $p(x)$ is of degree three it is reducible if and only if it has a first degree factor. By the factor theorem this happens exactly when $p(x)$ has a zero. We can easily check that $p(x)$ has no zero and therefore $R$ must be a field.

**3.** **a)** The system has a unique solution modulo $3 \cdot 5 \cdot 11 = 165$ by the Chinese remainder theorem. We find the solution by solving subsystems and adding their solutions. First solve

$$\begin{cases} x_1 \equiv 2 \pmod 3 \\ x_1 \equiv 0 \pmod 5 \\ x_1 \equiv 0 \pmod{11}. \end{cases}$$

By the last two equations $x_1 = 55s$ and the first equations then says that $x_1 \equiv 55s \equiv s \equiv 2 \pmod 3$. This shows we can choose $s = 2$ to get $x_1 = 110$. Proceeding in the same way for the other two subsystems we get $x_2 = 2 \cdot 33 = 66$ and $x_3 = 0 \cdot 15 = 0$. The resulting solutions is $x = x_1 + x_2 + x_3 = 176 \equiv 11 \pmod{165}$. All solutions are $x = 11 + 165k$ where $k$ is any integer.

**b)** Here the Chinese remainder theorem does not apply since 6 and 10 have a common factor. By the first equation $x$ must be even and by the second equation $x$ must be odd. Therefore the system has no solutions.

**4.** **a)** $\frac{19!}{(3!)^2(2!)^5}$

**b)** Use the exponential generating function $f(x) = (1 + x)^{10}$ (each of the ten letters can be included or not) and compute the coefficient of $\frac{x^7}{7!}$ which is $7!\binom{10}{7} = \frac{10!}{3!}$

c) Here the generating function is $f(x) = (1+x)^8(1+x+\frac{x^3}{3!})$ since the letters $E$ and $T$ may occur three times. Expanding the square and summing all coefficients of degree five we get $\binom{8}{5} + 2\binom{8}{4} + \binom{8}{3} + \frac{1}{3}\binom{8}{2} + \frac{1}{3}\binom{8}{1} = 264$ so the answer is $5!264 = 31680$

**5.** a) That the separation is two can be seen by checking the weight of all 8 code words or looking at the columns of the control matrix $H = (1111)$. ()The control matrix can be obtained from the normal form of $G$, but since it has only one row it is easy to find it by knowing its row is perpendicular to each row of $G$.)

b) Using $H$ we find that $w_1$ and $w_3$ are in $C$.

c) Using theorem 4.6 in the lecture notes by Andersson where $C_1$ is the code in **a)** and $C_2 = \{(0000), (1111)\}$ we get a code of separation 4 with generating matrix. (This is exactly the construction of a Reed-Muller code from example 4.7.)

$$G' = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

**6.** Let $a_n$ be the number of words of length $n$ in the letters $A, B, C$ not containing the substring $CC$.

a) It is easy to see that $a_1 = 3$, $a_2 = 9 - 1 = 8$. For $a_3$ and $a_4$ one can use inclusion/exclusion to keep track of the forbidden strings. For example, to find $a_3$, $c_i$ is the condition that the string starts with $CC$, $c_2$ the condition that we have $CC$ at the end. Then we get $27 - (3+3) + 1 = 22$ permitted strings. Likewise, for $a_4$ we get $81 - (9+9+9) + (3+1+3) - 1 = 60$ permitted strings.

b) Let $a_n = b_n + c_n$ where $b_n$ counts those words that end with $C$ and $c_n$ those not ending with $C$. Then $b_n = c_{n-1}$ since all permitted words ending with $C$ are obtained by adding a $C$ at the end of a word *not* ending with $C$. Also $c_n = 2(b_{n-1} + c_{n-1})$ since words not ending with $C$ are obtained by adding $A$ or $B$ at the end of any permitted word of length $n-1$. Substituting the second recurrence into the first we get $c_n = 2c_{n-2} + 2c_{n-1}$. Noting that $c_0 = 1$ and $c_1 = 2$ we can solve for $c_n$ by the usual method for linear recurrences and find that $c_n = \frac{1}{2\sqrt{3}}(1+\sqrt{3})^{n+1} - \frac{1}{2\sqrt{3}}(1-\sqrt{3})^{n+1}$. From $a_n = b_n + c_n = c_{n-1} + c_n$ we now, after some simplification, get $a_n = \frac{1}{6}((2\sqrt{3}+3)(1+\sqrt{3})^n + (3-2\sqrt{3})(1-\sqrt{3})^n)$