LUNDS TEKNISKA HÖGSKOLA	**SOLUTIONS**
MATEMATIK	**DISKRET MATEMATIK**
	2018–08–25

1. From the characteristic equation $r^2 + 5r + 6 = 0$ we find that all solutions to the corresponding homogenous equation are $a_n^{(H)} = A(-2)^n + B(-3)^n$.

To find a particular solution we make the ansatz $a_n^{(P)} = Cn(-2)^n$. (The factor n is needed since we would otherwise get a solution to the homogenous equation.)

Substitution of $a_n^{(P)}$ into the recurrence results in the equation $C(-2)^n(-2) = 4(-2)^n$. Hence $C = -2$ and $a_n = a_n^{(H)} + a_n^{(P)} = (A - 2n)(-2)^n + B(-3)^n$ From the inital conditions we get $B = 0$ and $A = 6$ resulting in the solution $a_n = (6 - 2n)(-2)^n$.

2. We note that $3, 4$ and 7 are pairwise relatively prime, so by the Chinese remainder theorem there is a unique solution modulo $3 \cdot 4 \cdot 7 = 84$.

Solving the corresponding system with RHS replaces by $1, 0, 0$ we have solutions $x_1 = 28t$ whenever $x_1 \equiv t$ is congruent to 1 modulo 3. Thus $x_1 = 28$ works.

In the same way we can find that $x_2 = 21$ and $x_3 = 36$ are solutions of the systems with RHS equal to $0, 1, 0$ and $0, 0, 1$ respectively. It follows that $x = 3x_1 + 1x_2 + 3x_3 = 185$ solves the original system, and that all solutions are given by $x = 185 + 84k$ where k is any integer. (Or equivalently $x = 17 + 84k$, where k is any integer.)

3. **a)** For each marble we select one of the four boxes independently. This can be done in 4^7 ways.

b) This is the same thing as counting all strings of length seven in say A,B,C,D with every letter occurring at least once. We can use the exponential generating function $f(x) = (x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots)^4 = (e^x-1)^4 = e^{4x}-4e^{3x}+6e^{2x}-4e^x+1$. Our answer equals 7! times the coefficient of x^7. By Taylor expansion we get $7!(\frac{4^7}{7!}) - 4\frac{3^7}{7!} + 6\frac{2^7}{7!} - 4\frac{1}{7!} = 8400$.

c) By the definition of Stirling numbers the answer is $S(7, 4) = 350$.

d) The number of solutions using four boxes plus the number of solutions using three boxes is $S(7, 4) + S(7, 3) = 350 + 301 = 651$

4. A sequence is determined once we decide how many instances of each number we will include as there is exactly one way to arrange then nondecreasingly. In other words we are after the number of solution of $a+b+c = n$ with a even. The generating function of the number of solutions is

$$g(x) = \frac{1}{(1-x)^2}\frac{1}{1-x^2} = \frac{1}{(1+x)}\frac{1}{(1-x)^3}$$

Using decomposition into partial fractions and the generalized binomial expansion we get

$$g(x) = \frac{1}{8}(\frac{1}{1+x} + \frac{7-4x+x^2}{(1-x)^3}) =$$

$$= \frac{1}{8}(\sum_{k=0}^{\infty}(-x)^k + (7-4x+x^2)\sum_{j=0}^{\infty}\binom{-3}{j}(-x)^j)$$

Using the fact that $\binom{-3}{j} = \binom{j+2}{j}(-1)^j = \frac{(j+2)(j+1)}{2}(-1)^j$ we find that the coefficient of x^n equals

$$\frac{1}{8}((-1)^n + 7\frac{(n+2)(n+1)}{2} - 4\frac{(n+1)n}{2} + \frac{n(n-1)}{2}) = \frac{1}{8}(2n^2+8n+7+(-1)^n)$$

5. **a)** The dimension is the dimension of the space of sequences minus the dimension of the orthogonal code= number of columns in H minus number of rows in H=6-2=4.

b) As the code is linear we can get the separation as the smallest number of columns in H that are linearly dependent. It is easy to verify that no two columns of H are dependent. On the other hand any three are since the vectors are in a two-dimensional space. This shows that the separation is three.

c) We compute the symdromes w_iH^t. For w_2 we have $w_2H^t = (0,0)$ which shows that w_2 is a code word. Concerning w_1 we find that $w_1H^t = (2,3) = 2(1,5)$, a multiple of the fifth column of H. This tells us that w_1 has one error and can be corrected to (2 0 3 0 2 0). Finally w_3 has syndrome $(-1,0)$, which is not a multiple of any column in H. Thus w_3 contains more than one error and cannot be corrected since the code has separation three.

6. **a)** As 43 is a prime $\mathbb{Z}_{43}$ is a field and by lemma 5.5 in Andersson combined with Fermat's little theorem every element has order that divides 42. The possible orders are then $1, 2, 3, 6, 7, 14, 21$ and 42.

b) We know, by theorem 5.9 in Andersson, that $\mathbb{Z}_{43}$ has a primitive element. Let us call this element a.

Now think of k as fixed. Then $o(a^k) = l \Leftrightarrow a^{kl} = 1$ but $a^{kt} = 1$ does not hold for any $0 < t < l \Leftrightarrow l$ is the smallest positive number t with $42|kt$. The number l must then be $\frac{42}{(42,k)}$. To sum up $o(a^k) = \frac{42}{(42,k)}$.

Now for given order d we want to count the $k \in [0,42]$ such that $d = o(a^k) = \frac{42}{(42,k)}$. Any such k must be of the form $\frac{42}{d}s$ with $s \in [0, d-1]$ and equality occurs exactly when $(d,s) = 1$. The number of such s is $\varphi(d)$ (by the definition of Eulers φ-function). Knowing that there are $\varphi(d)$ elements of order d we can create the table below

d	42	21	14	7	6	3	2	1
$\varphi(d)$	12	12	6	6	2	2	1	1