LUNDS TEKNISKA HÖGSKOLA LÖSNINGAR
MATEMATIK DISKRET MATEMATIK FMAA25/MATB13
2017–05–30

1. Using the characteristic polynomial we find that the homogenous equation has solutions $x_n^H = A \cdot 3^n + b \cdot 2^n$. For the particular solution we try $x_n^P = C \cdot n \cdot 2^n$ (We include the factor n because we otherwise would get a solution of the homogenous equation.) Substituting into the equation we find that $C = -\frac{5}{2}$ and initial conditions then imply that $A = 2$ and $B = 3$. **Answer:**$x_n = 2 \cdot 3^n + 3 \cdot 2^n - \frac{5}{2} n \cdot 2^n$

2. Let $h(x) = x^3 + 2x^2 + 2x + 2$.

a) $[x^2] \cdot [x^3] = [x^5] = [(x^2 + 3x + 2)h(x) + 3x^2 + 1] = [3x^2 + 1]$

b) The Euclidean algorithm on $f(x) = x^2 + 2x$ and $h(x)$ show that they have no common factors and backsubstitution in the computations give $1 = h(x)(3x + 3) + f(x)(2x^2 + 2x + 4)$. Hence $[f(x)]$ is invertible with inverse $[2x^2 + 2x + 4]$

c) R is a field if and only if $h(x)$ is irreducible. As h is of degree three it is reducible if and only if it has a factor of degree one. By the factor theorem the latter is equivalent to h having a zero. Now $h(0) = 2, h(1) = 2$ and $h(2) = 1$, so we conclude that $h(x)$ is irreducible and hence that R is a field.

3. **a)** This is most easily done using the recursion $S(n+1, k) = S(n, k) + kS(n, k)$. to produce Stirling's triangle.

	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$
$n=1$	1				
$n=2$	1	1			
$n=3$	1	3	1		
$n=4$	1	7	6	1	
$n=5$	1	15	25	10	1

b) The answer is $S(5, 3)$ by the definition of Stirling numbers and $S(5, 3) = 25$ by the table in **a**.

c) The number of surjective functions from a set of size n to a set of size k is $k!S(n, k)$ so in this case we get $3!S(5, 3) = 6 \cdot 25 = 150$ such functions.

4. **a)** The number of words is $3^3 = 27$ since any word can be represented by three (=dimension of the code) coefficients in $\mathbb{Z}_3$.

b) After eliminating G to normal form we find that

$$H = \begin{pmatrix} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 2 & 1 & 0 & 0 & 1 \end{pmatrix}$$

is a control matrix.

c) Any pair of columns of H are linearly independent but there are dependent triples, for example $H_2 = H_5 + 2H_6$. This shows that the separation is three. (Alternatively one can list the 27 code words and find the smallest weight among them.)

d) The word $w1$ has syndrome (110). This cannot be corrected since to is not a multiple of a column in H and can be written in more than one way as a linear combination of two columns of H. Two examples of such combinations are $H_3 - H_1$ and $H_4 + H_5$. Therefore $w1$ has no unique closest code word and is therefore not correctable. For w_2 the syndrome is (202) which is $2H_1$. Therefore the corrected word is (020012), obtained by subtracting the coset leader (200000) from w_2. Finally w_3 has syndrome (000) so it is in the code.

5. We can solve this using (ordinary) generating functions. Let

$$f(x) = (x^5 + x^{11})^3(1 + x + x^2 + x^3 + \cdots)(1 + x^2 + x^4 + x^6 + \cdots) =$$

$$= x^{15}(1 + x^6)^3 \cdot \frac{1}{1-x} \cdot \frac{1}{1-x^2}.$$

After partial fraction decomposition of the last two factors we get

$$x^{15}(1+x^6)^3(\frac{1}{2}\frac{1}{(1-x)^2}+\frac{1}{4}\frac{1}{1-x}+\frac{1}{4}\frac{1}{1+x}) = x^{15}(1+x^6)^3\sum_{j=0}^{\infty}(\frac{1}{2}\binom{-2}{j}(-x)^j+\frac{1}{4}x^j+\frac{1}{4}(-x)^j),$$

where the last step is from the generalised binomial expansion. Now let

$$c_j = \frac{1}{2}\binom{-2}{j}(-1)^j + \frac{1}{4} + \frac{1}{4}(-1)^j = \frac{j+1}{2} + \frac{1}{4} + \frac{1}{4}(-1)^j$$

be the coefficent of x^j in the series.

a) Using the fact that $x^{15}(1 + x^6)^3 = x^{15}(1 + 3x^6 + 3x^{12} + x^{18})$ we see that only two terms contribute to the coefficient of x^{24} and that the coefficient is $c_9 + 3c_3 = 5 + 3 \cdot 2 = 11$

b) As above we find that three terms contribute to the coefficient of x^{30} and that the coefficient is $c_{15} + 3c_9 + 3c_3 = 8 + 3 \cdot 5 + 3 \cdot 2 = 29$

c) Here all four terms contribute and we get the coefficient $c_{k-15} + 3c_{k-21} + 3c_{k-27} + c_{k-33} = \frac{k-14}{2} + 3\frac{k-20}{2} + 3\frac{k-26}{2} + \frac{k-32}{2} = 4k - 92$ for even k and for odd k we should add $\frac{1}{2}(1 + 3 + 3 + 1) = 4$ so that we get $4k - 88$.

6. Assume that p and q are different primes. Look at the ring $\mathbb{Z}_{p^2q}$ and the subset $\mathbb{Z}^*_{p^2q}$ consisting of its invertible elements.

a) The invertible elements are those $[a]$ $1 \leq a \leq n$ with $(a, n) = 1$. By the definition of Euler's ϕ function the number of such a is $\phi(p^2q)$ and we have derived a formula saying that $\phi(p^2q) = p^2q(1-1/p)(1-1/q) = p(p-1)(q-1)$. (If you do not remember this formula you can use inclusion exclusion with $c_1 =$ divisible by p and $c_2 =$ divisible by q.)

b) Yes, if $[a]$ and $[b]$ have inverses then $[a][b] = [ab]$ has inverse $[b^{-1}a^{-1}]$

c) No, it is not closed under addition. For example $[1], [p-1] \in \mathbb{Z}^*_{p^2q}$, but $[1] + [p-1] = [p] = [0]$ is not invertible and hence not in $\mathbb{Z}^*_{p^2q}$. (The fact that $[0]$ in not in the set also proves that it is not a subring.)

d) If $\phi(x) = \phi(y)$ then $ax = ay$. Multiplying by $[a^{-1}]$ we get that $x = y$. This shows that ϕ is injective.

e) $\Rightarrow$) If $x^{p(p-1)(q-1)} = 1$ then $x^{p(p-1)(q-1)-1}$ is an inverse of x. $\Leftarrow$) Use the mapping in **d)** with a replaced by x. ϕ is an injective map from a finite set to itself, and therefore it must be bijective. Let $j = p(p-1)(q-1)$ and let $x_1, x_2, \ldots, x_j$ be a list of the elements of $\mathbb{Z}^*_{p^2q}$. Then, ϕ being bijective, $\phi(x_1), \phi(x_2), \ldots, \phi(x_j) = x \cdot x_1, x \cdot x_2, \ldots x \cdot x_j$ lists exactly the same elements but in a different order. Multiplying all elements in each list we find that $x_1 x_2 \cdots x_j = x^j x_1 x_2 \cdots x_j$ Multiplying by the inverse of $x_1 x_2 \cdots x_j$ we now see that $1 = x^j = x^{p(p-1)(q-1)}$.