Math 342 Problem set 1 (due 13/9/11)

Linear algebra over $\mathbb{F}_2$

1. Solve the system of equations
$$\begin{cases} x+y &= 1 \\ x+y+z &= 0 \\ y+z &= 0 \end{cases}$$
over $\mathbb{F}_2$ (that is, with $x, y, z \in \{0, 1\}$ and subject to the rules of addition and multiplication we obtained in class).

2. Can the bit vector $(0,1,1,1,0) \in \mathbb{F}_2^5$ be represented as a linear combination of the vectors $\{(1,0,0,0,0), (0,1,0,0,0), (1,0,1,0,1)\}$?
Hint: the coefficients in the combination must also come from $\mathbb{F}_2$.

Induction

3. Use induction to show that among every three consecutive positive integers there is one that is divisible by 3.

4. Show that for every $n \geq 0$, $x - y$ divides $x^n - y^n$ as polynomials.

5. §2A.E23.

6. (Bernoulli's inequality) Show that $(1+x)^n \geq 1 + nx$ for any natural number n and real $x > -1$.

Divisibility

An integer a is said to *divide* the integer b if there is a third integer c such that $ac = b$. For example, 2 divides 6 since $2 \cdot 3 = 6$, but 5 does not divide 6.

7. For each integer $n \in \{6, 12, 17\}$:
   (a) List the positive integers which divide n.
   (b) Find the sum of the divisors of n which are different from n (that is, for each n add all the numbers you got in part (a) except for n itself).
   (c) Is n *abundant* (the sum is bigger than n), *deficient* (the sum is less than n) or *perfect* (the sum is equal to n)?
8. Using the lists of divisors from the previous problem:
   (a) What is the largest number that divides both 6 and 12?
   (b) What is the largest number that divides both 12 and 17?

REMARK. (Aside) Perfect numbers are rare and only finitely many are known. It is believed that there are infinitely many even perfect numbers, but this is not known. It is not known if there exist any odd perfect numbers.

Problem set 0

1. Let $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \in M_3(\mathbb{F}_2)$. Let $\underline{v} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \in \mathbb{F}_2^3$.
   (a) Calculate $A\underline{v}$.
   (b) Is A invertible? If so, find A^{-1}.
2. (§2A.E5) Show that $\frac{1-x^{n+1}}{1-x} = 1 + x + \cdots + x^n = \sum_{k=0}^{n} x^k$.

Solution examples

1.
   (a) $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 + 0\cdot 1 + 1\cdot 0 \\ 0\cdot 1 + 0\cdot 1 + 1\cdot 0 \\ 1\cdot 1 + 1\cdot 1 + 1\cdot 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$
   (b) Expanding in the first row, $\det A = 1 \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} - 1 \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = 1 \neq 0$, so A is invertible.
   We already know that $A \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ and that $A \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ (this is the second column of A) so $A^{-1} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ and $A^{-1} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$. Finally, since the first and last columns of A add to $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ we have $A \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ so $A^{-1} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ and the matrix of A^{-1} is $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.
2. For $n = 0$ we need to show $\frac{1-x}{1-x} = \sum_{k=0}^{0} x^k$ and indeed both sides equal 1. We continue by induction. Assuming the truth of the claim for some n, we have

$$
\begin{aligned}
\sum_{k=0}^{n+1} x^k &= \sum_{k=0}^{n} x^k + x^{n+1} \\
&= \frac{1-x^{n+1}}{1-x} + x^{n+1} && \text{by the induction hypothesis} \\
&= \frac{1-x^{n+1}+x^{n+1}-x^{n+2}}{1-x} \\
&= \frac{1-x^{(n+1)+1}}{1-x}.
\end{aligned}
$$