DEPARTMENT OF MATHEMATICS

MATHS 255 Assignment 6 Solutions Due: 12 September, 2001

1. Prove that any natural number n is congruent modulo 9 to the sum of its decimal digits. [We say that $a_m a_{m-1} \cdots a_0$ is the decimal expansion of n if

$$\forall i,\ a_i \in \mathbf{Z},\ \ 0 \le a_i \le 9\ ;\ \ a_m \ne 0 \quad \text{and } n = \sum_{i=0}^{m} a_i (10)^i .$$

You may assume the existence and uniqueness of such an expansion for each $n \in \mathbf{N}$.]

We need to show that if $n = \sum_{i=0}^{m} a_i (10)^i$, then $n \equiv \sum_{i=0}^{m} a_i \bmod 9$.

$$10 \equiv 1 \bmod 9 \ \Rightarrow\ \forall i,\ 10^i \equiv 1 \bmod 9 \ \Rightarrow\ a_i (10)^i \equiv a_i \bmod 9 \ \Rightarrow\ \sum_{i=0}^{m} a_i (10)^i \equiv \sum_{i=0}^{m} a_i \bmod 9$$

$\Rightarrow \quad n \equiv \sum_{i=0}^{m} a_i \bmod 9$, as required.

2. Find all invertible elements of $\mathbf{Z}_{40}$, and find the inverse of each of them. [Use a calculator or computer if you wish, but explain your methods.]

The invertible elements are of the form $\bar{n}$ where $\gcd(n, 40) = 1$. These are
$\bar{1},\ \bar{3},\ \bar{7},\ \bar{9},\ \overline{11},\ \overline{13},\ \overline{17},\ \overline{19},\ \overline{21},\ \overline{23},\ \overline{27},\ \overline{29},\ \overline{31},\ \overline{33},\ \overline{37},\ \overline{39},$
A few observations that simplify finding the inverses are that if $\bar{a}\bar{b} = \bar{1}$, then $(-\bar{a})(-\bar{b}) = \bar{1}$, so that $(\overline{40} - \bar{a})(\overline{40} - \bar{b}) = \bar{1}$. Also, if $ab = -1$ then $(-a)b = a(-b) = 1$. $81 = 9 \cdot 9 = 3 \cdot 27$, $121 = 11 \cdot 11$, also, $39 = 13 \cdot 3$, and $119 = 17 \cdot 7$ From these clues, we get the inverses of 1, 3, 7, 9, 11, 13, 17, 23, 27, 29, 31, 33, 37, 39 to be 1, 27, 23, 9, 11, 37, 33, 7, 3, 29, 31, 17, 13, 39 respectively. (The overbars should be there, but you get the idea.) By using the euclidean algorithm to find gcd(21,40) or by observing that 21x21=441, we get that the inverse of 21 is 21 so that the inverse of 19 is 19.

Thus the invertible elements and their inverses are, respectively,
$\bar{1},\ \bar{3},\ \bar{7},\ \bar{9},\ \overline{11},\ \overline{13},\ \overline{17},\ \overline{19},\ \overline{21},\ \overline{23},\ \overline{27},\ \overline{29},\ \overline{31},\ \overline{33},\ \overline{37},\ \overline{39},$

$\bar{1},\ \overline{27},\ \overline{23},\ \bar{9},\ \overline{11},\ \overline{37},\ \overline{33},\ \overline{19},\ \overline{21},\ \bar{7},\ \bar{3},\ \overline{29},\ \overline{31},\ \overline{17},\ \overline{13},\ \overline{39},$

[It is interesting to note that there are four numbers which are their own inverse, i.e. four solutions in $\mathbf{Z}_{40}$ to the quadratic equation $x^2 - \bar{1} = \bar{0}$.]

3. Find the quotient and remainder when $a(x)$ is divided by $b(x)$ where

$$a(x) = x^7 + x^5 - x^4 + x^3 + x^2 - x \ + \bar{1} \quad \text{and} \quad b(x) = x^3 - x + \bar{1},$$

(a) assuming $a(x)$, $b(x)$ are in $\mathbf{Z}_2[x]$.

Quotient: $x^4 + \bar{1}$. Remainder: x^2.

(b) assuming $a(x)$, $b(x)$ are in $\mathbf{Z}_3[x]$.

Quotient: $x^4 + \bar{2}x^2 - \bar{2}x\ (= x^4 + \bar{2}x^2 + x)$. Remainder: $x + \bar{1}$.

4. Write down <u>all</u> polynomials of degree ≤ 3 in $\mathbf{Z}_2[x]$, and indicate those which are irreducible. Also write down all <u>irreducible</u> polynomials of degree 4 in $\mathbf{Z}_2[x]$. Explain your answers.

Thepolynomials of degree ≤ 3 are of the form $ax^3 + bx^2 + cx + d$ where $a,b,c,d \in \{\bar{0},\bar{1}\}$,,That means 16 possibilities.

$1, 0$

$x+1,\ x$

$x^2 + x + 1,\ x^2 + x,\ x^2 + 1,\ x^2$

$x^3 + x^2 + x + 1,\ x^3 + x^2 + x,\ x^3 + x^2 + 1,\ x^3 + x^2,\ x^3 + x + 1, x^3 + x, x^3 + 1,\ x^3$

The irreducible ones are those of degree 1 plus those that have no factor of degree 1, i.e. no roots in $\mathbf{Z}_2$, which is easily checked, giving only five:

$x,\ x+1,\ x^2 + x + 1,\ x^3 + x^2 + 1,\ x^3 + x + 1$.

The irreducibles of degree 4 are those of the form $x^4 + ax^3 + bx^2 + cx + d$ which are not multiples of x or $x+1$, (i.e. have no roots in $\mathbf{Z}_2$) and which are not a product of two irreducibles of degree 2, that is, not = $x^4 + x^2 + 1\ = (x^2 + x + 1)^2$. This means that they are of the form $x^4 + ax^3 + bx^2 + cx + 1$ with $a + b + c = 1$ but not = $x^4 + x^2 + 1\ = (x^2 + x + 1)^2$ This leaves exactly $(a,b,c) = (0,0,1), (1,0,0), (1,1,1)$. So the irreducible polynomials of degree 4 are $x^4 + x + 1,\ x^4 + x^3 + 1,\ x^4 + x^3\ + x^2 + x + 1$.