MAT 3343, APPLIED ALGEBRA, FALL 2002

Prof. P. Selinger

Problem 1 (10 points). For any integer $a \in \mathbb{Z}$, define $a\mathbb{Z} = \{ax | x \in \mathbb{Z}\}$. Prove: for all $a, b \in \mathbb{Z}$, $b|a$ if and only if $a\mathbb{Z} \subseteq b\mathbb{Z}$.

Problem 2. (a) **(5 points)** Find all solutions of $30x = 15$ in $\mathbb{Z}_{55}$. How many different solutions are there?

(b) **(10 points)** For given integers $a, b, n \in \mathbb{Z}$, prove that the equation $ax = b$ has a solution in $\mathbb{Z}_n$ if and only if $\gcd(a, n)|b$.

Problem 3 (10 points). Find the general solution of the following system of equations in $\mathbb{Z}_7$:

$$\left(\begin{array}{l} 2x + 3y + 4z = 5 \\ 3x + 4y + 6z = 0 \end{array} \right)$$

Problem 4 (10 points). Let R be a Euclidean ring. Suppose $a, b, c \in R$ and $\gcd(a, b) = 1$. Prove that $a|bc$ implies $a|c$.

Problem 5 (10 points). Find the greatest common divisor of the following two polynomials in $\mathbb{Z}_3[x]$:

$$\begin{array}{rcl} p(x) & = & x^5 + x^4 + 2x^3 + 2 \\ q(x) & = & x^5 + x^3 + x^2 + x + 2 \end{array}$$

Problem 6 (10 points). Consider the $(7, 4)$-Hamming code with the following generator matrix G and parity check matrix H:

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

(a) Encode the message 0011, 1101, 1111 using this code.

(b) Decode the message 1101010, 0110111, 0111101, correcting all single-bit errors.

Problem 7 (10 points). Recall that the factorial of n is defined as $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1)$.

Show that if p is prime, then $(p-1)! \equiv -1 (\operatorname{mod} p)$. (Hint: $(p-1)!$ is the product of all the units in $\mathbb{Z}_p$).

Problem 8. Let R be a Euclidean ring, and let $a \in R$ be an element. On R, define a relation $\sim$ by $x \sim y \iff a|(x-y)$.

(a) **(5 points)** Prove that $\sim$ is an equivalence relation.

(b) **(5 points)** Prove that addition and multiplication are well-defined on $R/{\sim}$ by $[x]_\sim + [y]_\sim = [x+y]_\sim$ and $[x]_\sim [y]_\sim = [xy]_\sim$.

(c) **(5 points)** Prove that if a is irreducible, then $R/{\sim}$ is a field.