MAT 3343, APPLIED ALGEBRA, FALL 2002

Final Exam, December 17, 2002

Prof. P. Selinger

Problem 1. 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. Find all solutions of $28x = 35$ in $\mathbb{Z}_{77}$. How many different solutions are there?

Problem 3. True or false? For each of the following statements, give a proof or a counterexample. Here, $a, b, c, d, e, f \in \mathbb{Z}$.

(a) If $\gcd(a, b) = 1$ and $c|a$, then $\gcd(c, b) = 1$.

(b) If $\gcd(a, b) = c$ and $\gcd(d, e) = f$, then $\gcd(ad, be) = cf$.

(c) If $\gcd(a, b) = c$, then $\gcd(a^2, b^2) = c^2$.

Problem 4. Find all solutions (x, y, z) of the following system of linear equations in $\mathbb{Z}_7$.

$$\begin{array}{ccccccc} 1x & + & 3y & + & 5z & = & 0 \\ 1x & + & 2y & + & 3z & = & 4 \\ 2x & + & 3y & + & 4z & = & 5 \end{array}$$

Problem 5. What is the greatest common divisor of the following two polynomials in $\mathbb{Z}_2$:

$$p(x) = x^5 + x^4 + x^3 + x^2 + x + 1, \quad q(x) = x^4 + x^2 + x + 1.$$

Problem 6. Which of the following polynomials are irreducible in $\mathbb{Q}[x]$? Give reasons.

(a) $x^3 + x^2 + x + 1$.

(b) $x^4 + 3x^2 - 6$.

(c) $x^3 + x^2 - 5$.

(d) $x^5 + 12x^4 + 18x^3 + 30x + 12$.

Problem 7. Find all rational roots of $2x^3 + x^2 + x - 1$. How do you know you have all of them?

Problem 8. Consider the $(7, 3)$-code with generating polynomial $x^4 + x^2 + x + 1$ over $\mathbb{Z}_2$.

(a) Make a list of the 8 valid codewords of this code.

(b) Encode the message 001, 110, 101.

(c) What is the minimum Hamming distance of this code? How many errors does this code detect, and how many does it correct?

(d) Decode 1011011, 0111011, 1101110.

Problem 9. Ziggy Hamming, a distant but much less well-known relative of the famous R.W. Hamming, proposes an error-correcting (8,4)-code with generator matrix

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

(a) What is the minimum Hamming distance of this code? How many errors does this code detect / correct? The minimum weight of any non-zero codeword, and thus the minimum Hamming distance of the code, is 4. Thus the code detects 3 errors and corrects 1.

(b) Find a parity check matrix for this code.

Problem 10. Let α be a primitive element in $GF(16)$, where $\alpha^4 = \alpha + 1$.

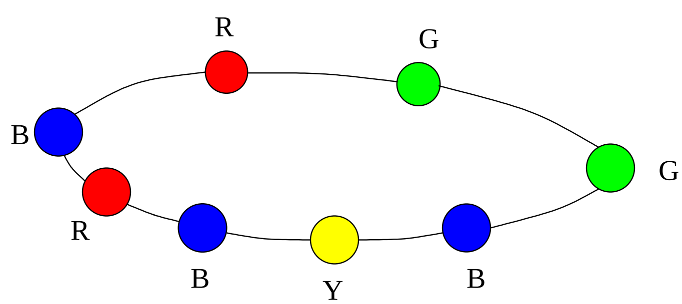
(a) Find an irreducible polynomial $p(x) \in \mathbb{Z}_2[x]$ such that $p(\alpha^3) = 0$. What are the other roots of $p(x)$ in $GF(16)$?

Let $y = \alpha^3$. Then we read from the table: $y^0 = \alpha^0 = 0001$, $y^1 = \alpha^3 = 1000$, $y^2 = \alpha^6 = 1100$, $y^3 = \alpha^9 = 1010$, $y^4 = \alpha^{12} = 1111$. These five elements are linearly dependent, and we find that $y^4 + y^3 + y^2 + y + 1 = 0$. Thus, $p(x) = x^4 + x^3 + x^2 + x + 1$ is the smallest degree polynomial which has $y = \alpha^3$ as a root (hence $p(x)$ is also irreducible).

To find the other roots of $p(x)$, recall that $p(x^2) = p(x)^2$, and hence, whenever x is a root, then so is x^2. Thus, $p(x)$ has roots α^3, α^6, α^{12}, $\alpha^{24} = \alpha^9$. As a polynomial of degree 4, $p(x)$ can have at most four distinct roots, so these are all of them.

(b) Find the generator polynomial of the two-error-correcting BCH code of length 15, starting with the primitive element α.

Problem 11. How many different necklaces consisting of 8 beads can be formed if there are 4 bead colors available? Regard two necklaces as identical if one can be obtained from the other by rotations only.



Problem 12. Recall that the order of a modulo q is the smallest n such that $a^n \equiv 1 (\bmod q)$. Prove that if $q > 2$ is odd and the order of 2 modulo q is $q - 1$, then q is prime. Is the converse true?