MAT 3343, APPLIED ALGEBRA, FALL 2003

Answers to the Final Exam

Problem 1. Suppose d and k are integers such that $d > 0$, $d|(11k+4)$, and $d|(10k+3)$. Show that $d = 1$ or $d = 7$.

Answer: Under the given hypotheses, we know that $d|10(11k+4) + (-11)(10k+3)$.. Therefore $d|110k + 40 - 110k - 33$, hence $d|7$. Since 7 is prime, we have $d = 1$ or $d = 7$.

Problem 2. (a) Show that no integer of the form $k^2 + 1$ is a multiple of 7.

Answer: The equation $7|(k^2+1)$ is equivalent to $\bar{k}^2 + 1 \equiv 0 (\bmod 7)$, or $\bar{k}^2 \equiv -1 (\bmod 7)$. The squares in $\mathbb{Z}_7$ are $0^2 = 0$, $1^2 = (-1)^2 = 1$, $2^2 = (-2)^2 = 4$, $3^2 = (-3)^2 = 9 = 2$. Hence no square in $\mathbb{Z}_7$ is equal to -1.

(b) Find all integers k such that $k^2 + 1$ is a multiple of 13.

Answer: As in part (a), this is equivalent to finding all k such that $\bar{k}^2 \equiv -1 (\bmod 13)$. We examine all squares in $\mathbb{Z}_{13}$: $0^2 = 0, 1^2 = (-1)^2 = 1, 2^2 = (-2)^2 = 4, 3^2 = (-3)^2 = 9, 4^2 = (-4)^2 = 16 = 3, 5^2 = (-5)^2 = 25 = -1$. We may stop here, as we have found two solutions $\bar{k} = \pm 5$, and $\mathbb{Z}_{13}$ is a field and therefore a quadratic equation has no more than 2 solutions. Thus, the general solution is $\bar{k} \equiv \pm 5 (\bmod 13)$. This means, the general integer solution is $k \in \{5 + 13a, -5 + 13a \mid a \in \mathbb{Z}\}$, or $k \in \{\ldots, -8, -5, 5, 8, 18, 21, \ldots\}$.

Problem 3. Consider the following set of real 2×2-matrices:

$$R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

(a) Show that R is a commutative ring, with the usual operations of addition and multiplication of matrices. (You may assume common properties of matrices without proof).

Answer: We already know that the set of all 2×2-matrices forms a (non-commutative) ring. Thus, it suffices to check that R is a subring, and that R is commutative. To check that it is a subring, we must check that it contains 0 and 1, and is closed under addition, multiplication, and negation. We note that $0 \in R$ and $1 \in R$. Further, if $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$, then

$$A + B = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \in R$$

$$-A = \begin{pmatrix} -a & -b \\ b & -a \end{pmatrix} \in R$$

$$AB = \begin{pmatrix} ac - bd & ad + bc \\ -(ad+bc) & ac - bd \end{pmatrix} \in R$$

Finally we check commutativity:

$$BA = \begin{pmatrix} ac - bd & ad + bc \\ -(ad+bc) & ac - bd \end{pmatrix} = AB.$$

(b) Is R a field? Prove or give a counterexample.

Answer: Each matrix in R has determinant $a^2 + b^2$, and thus it is invertible unless $a = b = 0$. It remains to check that the inverse is indeed in R. But we have

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

hence, the inverse is in R (if $(a, b) \neq (0, 0)$). Thus, R is a field. (Note: R is indeed isomorphic to the field of complex numbers $\mathbb{C}$, via the isomorphism $a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$).

Problem 4. Recall that the factorial of n is defined as $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$.

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 $\mathbb{Z}_p$).

Answer: Consider the units $1, 2, \ldots, p-1$ in $\mathbb{Z}_p$. Since the equation $x^2 = 1$ has at most two roots, there are at most two elements which are their own inverse: these elements are 1 and -1. The set of remaining units can be divided into pairs of numbers that are mutually inverse. Now consider the product of all units. The mutually inverse pairs cancel out to 1, so the product of all units is equal to $1 \cdot -1 = -1$.

Problem 5. My RSA public key is given by $(N, e) = (55, 27)$.

(a) What is my secret decryption key d?

Answer: We have $N = pq = 5 \cdot 11$. The encryption and decryption keys satisfy the relation $ed \equiv 1 (\operatorname{mod} \varphi(N))$, where $\varphi(N) = (p-1)(q-1) = 4 \cdot 10 = 40$. Thus $27d \equiv 1 (\operatorname{mod} 40)$. We use Euclid's algorithm to solve this, and we find

$$\begin{array}{rcrcl} 40 & = & 1 \cdot 27 & + & 13 \\ 27 & = & 2 \cdot 13 & + & 1 \end{array}$$

Thus, $1 = 27 - 2 \cdot 13 = 27 - 2 \cdot (40 - 27) = 3 \cdot 27 - 2 \cdot 40$. It follows that $27 \cdot 3 \equiv 1 (\operatorname{mod} 40)$, thus $d = 3$.

(b) Decrypt the message $[1; 4; 10]$.

Answer: We must compute 1^3, 4^3, and 11^3 $(\operatorname{mod} 55)$. Clearly $1^3 = 1$, and $4^3 = 64 \equiv 9 (\operatorname{mod} 55)$. Also, $10^3 = 1000 \equiv 10 (\operatorname{mod} 55)$. So the decrypted message is $[1; 9; 10]$.

Problem 6. Find all integers x which satisfy the following two equations simultaneously:

$$x^2 \equiv 4 (\operatorname{mod} 7)$$
$$x^3 \equiv x (\operatorname{mod} 5)$$

Justify your answer.

Answer: The first equation is equivalent to $x^2 - 4 \equiv 0 (\operatorname{mod} 7)$, or $(x+2)(x-2) \equiv 0 (\operatorname{mod} 7)$, therefore $x \equiv \pm 2 (\operatorname{mod} 7)$. The second equation is equivalent to $x^3 - x \equiv 0 (\operatorname{mod} 5)$, hence $x(x^2 - 1) \equiv 0 (\operatorname{mod} 5)$, hence $x(x+1)(x-1) \equiv 0 (\operatorname{mod} 5)$, hence $x \in \{0, -1, 1\} (\operatorname{mod} 5)$. By the

Chinese Remainder Theorem, each combination gives exactly one solution in $\mathbb{Z}_{35}$, hence there is a total of 6 solutions:

$$\begin{array}{lll}
x \equiv 2(\bmod 7), & x \equiv 0(\bmod 5) & \iff x \equiv -5(\bmod 35) \\
x \equiv 2(\bmod 7), & x \equiv 1(\bmod 5) & \iff x \equiv 16(\bmod 35) \\
x \equiv 2(\bmod 7), & x \equiv -1(\bmod 5) & \iff x \equiv 9(\bmod 35) \\
x \equiv -2(\bmod 7), & x \equiv 0(\bmod 5) & \iff x \equiv 5(\bmod 35) \\
x \equiv -2(\bmod 7), & x \equiv -1(\bmod 5) & \iff x \equiv -16(\bmod 35) \\
x \equiv -2(\bmod 7), & x \equiv 1(\bmod 5) & \iff x \equiv -9(\bmod 35)
\end{array}$$

Thus, the general solution set is $\{-16, -9, -5, 5, 9, 16\} + 35\mathbb{Z}$.

Problem 7. Which of the following polynomials are irreducible in $\mathbb{Q}[x]$? Give reasons.

(a) $x^5 + x^3 + x^2 + 1$.

Answer: Not irreducible, because $x^5 + x^3 + x^2 + 1 = (x^3 + 1)(x^2 + 1)$. Also, because -1 is a root.

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

Answer: Irreducible by Eisenstein's criterion with $p = 2$. Note that $p = 2$ divides all coefficients but the highest one, and $p^2 = 4$ does not divide the lowest coefficient (-6).

(c) $x^3 + x^2 - 7$.

Answer: Irreducible. By the rational root theorem, the only possible rational roots for this polynomial are $\pm 1, \pm 7$. It is quickly checked that these are not in fact roots. Hence, $x^3 + x^2 - 7$ has no linear factors in $\mathbb{Q}[x]$, and therefore it must be irreducible.

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

Answer: Irreducible by Eisenstein's criterion with $p = 3$. Note that Eisenstein's criterion with $p = 2$ does *not apply*, because $2^2 = 4$ divides the lowest coefficient, $a_0 = 12$.

Problem 8. Consider the polynomial $(8, 4)$-code with generating polynomial $p(x) = x^4 + x^3 + x^2 + 1$.

(a) Find the generating matrix for this code (make sure that your generating matrix generates a *systematic* code).

Answer: We need to find the codewords corresponding to the four basis plaintext words $(1, 0, 0, 0)$, $(0, 1, 0, 0)$, and so forth. Thus, we need to represent each plaintext as a polynomial, multiply by x^4, and add the remainder of the division by $p(x)$. We get:

$$\begin{array}{ll}
(1000) \to x^3 \to x^7 = (x^4 + x^3 + x^2 + 1)(x^3 + x^2 + 1) + 1 & \to (10000001) \\
(0100) \to x^2 \to x^6 = (x^4 + x^3 + x^2 + 1)(x^2 + x) + x^3 + x^2 + x & \to (01001110) \\
(0010) \to x^1 \to x^5 = (x^4 + x^3 + x^2 + 1)(x + 1) + x^2 + x + 1 & \to (00100111) \\
(0001) \to x^0 \to x^4 = (x^4 + x^3 + x^2 + 1)(1) + x^3 + x^2 + 1 & \to (00011101)
\end{array}$$

Thus, the generator matrix is

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

(b) For $i = 1, \ldots, 8$, let $r_i(x)$ be the remainder of the division of x^{8-i} by $p(x)$. Let H be the matrix whose ith row is $r_i(x)$, represented as a vector in $\mathbb{Z}_2^4$. Find H, and prove that it is a parity check matrix for the code from (a).

Answer: The respective remainders are: $r_1(x) = 1$, $r_2(x) = x^3 + x^2 + x$, $r_3(x) = x^2 + x + 1$, $r_4(x) = x^3 + x^2 + 1$ (these were calculated in part (a)), and $r_5(x) = x^3$, $r_6(x) = x^2$, $r_7(x) = x$, $r_8(x) = 1$. These remainders are simply the syndromes for each possible single-bit error, and thus they form the rows of a parity check matrix. We get

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

(c) What is the minimum Hamming weight of this code? Thus how many errors does it correct/detect?

Answer: It is easy to see that each codeword has even weight. Moreover, there is a codeword of weight 2, so the minimum Hamming weight is 2. The code detects 1 errors and corrects 0.

Problem 9. Consider the linear code with generator matrix

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

Find the coset of the received word $(0, 0, 1, 0, 1)$. What is the coset leader? What is therefore the most likely corrected codeword?

Answer: Let $w = (00101)$. The coset is

$$\{vG + w | v \in \mathbb{R}^3\} = \{00101, 10110, 01100, 11110, 00011, 10000, 01010, 11000\}.$$

The natural coset leader is (10000), since it has the smallest Hamming weight (and thus is the most likely error, assuming that errors occur independently in each bit). Therefore, the most likely corrected codeword is $(00101) + (10000) = (10101) = (101)G$.

Problem 10. Find the greatest common divisor of $x^4+x^3+2x^2+x+1$ and $x^4+2x^3+3x^2+2x+2$ in $\mathbb{R}[x]$.

Answer: We use Euclid's algorithm.

$$\begin{array}{rcl}
(x^4+2x^3+3x^2+2x+2) &=& (x^4+x^3+2x^2+x+1)(1) \quad + \quad (x^3+x^2+x+1) \\
(x^4+x^3+2x^2+x+1) &=& (x^3+x^2+x+1)(x) \quad + \quad (x^2+1) \\
(x^3+x^2+x+1) &=& (x^2+1)(x+1) \quad + \quad 0
\end{array}$$

Therefore, the greatest common divisor is x^2+1.

Problem 11. Consider the Galois Field $\mathrm{GF}(9)$, and let α be an element with $\alpha^2+2\alpha+2=0$.

(a) Is α a primitive element?

Answer: We first make a representation of the Galois Field $\mathrm{GF}(9)$.

α^0	$= 1$	01
α^1	$= \alpha$	10
α^2	$= \alpha+1$	11
α^3	$= 2\alpha+1$	21
α^4	$= 2$	02
α^5	$= 2\alpha$	20
α^6	$= 2\alpha+2$	22
α^7	$= \alpha+2$	12
α^8	$= 1$	01

We find that α is indeed a primitive element.

(b) Find all primitive elements in $\mathrm{GF}(9)$.

Answer: Since α is primitive and of order 8, it follows that the primitive elements are of the form α^i, where $\gcd(i,8)=1$, so α^3, α^5, and α^7.

(c) Find an irreducible polynomial which has $\alpha+1$ as a root.

Answer: Let $x=\alpha+1=\alpha^2$. Then $x^0=1$, $x^1=\alpha^2=\alpha+1$, $x^2=\alpha^4=2$. We get a linear dependency, namely $x^2+1=0$. So x^2+1 has $\alpha+1$ as a root. Since it is the smallest degree polynomial with this property, it is irreducible.

Problem 12. Find the generator polynomial of a 4-error correcting $(31,k)$ BCH code. Note that a representation of $\mathrm{GF}(32)$ can be found on the attached sheet (page 6). What is the plaintext length k of this code?

Answer: First, we find irreducible polynomials $p_i(x)$ for $p_i(\alpha^i)=0$, for $i=1,3,5,7$. We have $p_1(x)=x^5+x^2+1$. For $p_3(x)$, let $x=\alpha^3$, and calculate x^n for various n:

$$\begin{array}{ll}
x^0=\alpha^0=1 & (00001) \\
x^1=\alpha^3 & (01000) \\
x^2=\alpha^6=\alpha^3+\alpha & (01010) \\
x^3=\alpha^9=\alpha^4+\alpha^3+\alpha & (11010) \\
x^4=\alpha^{12}=\alpha^3+\alpha^2+\alpha & (01110) \\
x^5=\alpha^{15}=\alpha^4+\alpha^3+\alpha^2+\alpha+1 & (11111)
\end{array}$$

We find a linear dependency between these 6 vectors: $x^5 + x^4 + x^3 + x^2 + 1 = 0$ has α^3 as a root. Since $x^0, \ldots, x^4$ are linearly independent, no smaller-degree polynomial has α^3 as a root, and thus $p_3(x) = x^5 + x^4 + x^3 + x^2 + 1$ is irreducible.

For $p_5(x)$, let $x = \alpha^5$, and calculate:

$$\begin{array}{ll} x^0 = \alpha^0 = 1 & (00001) \\ x^1 = \alpha^5 & (00101) \\ x^2 = \alpha^{10} & (10001) \\ x^3 = \alpha^{15} & (11111) \\ x^4 = \alpha^{20} & (01100) \\ x^5 = \alpha^{25} & (11001) \end{array}$$

We find a linear dependency between these 6 vectors, which is $p_5(x) = x^5 + x^4 + x^2 + x + 1$.

For $p_7(x)$, let $x = \alpha^7$, and calculate:

$$\begin{array}{ll} x^0 = \alpha^0 = 1 & (00001) \\ x^1 = \alpha^7 & (10100) \\ x^2 = \alpha^{14} & (11101) \\ x^3 = \alpha^{21} & (11000) \\ x^4 = \alpha^{28} & (10110) \\ x^5 = \alpha^{35} & (10000) \end{array}$$

We find a linear dependency between these 6 vectors, which is $p_7(x) = x^5 + x^3 + x^2 + x + 1$.

Therefore, the generator polynomial is

$$\begin{array}{rcl} p(x) & = & \gcd(p_1(x), p_3(x), p_5(x), p_7(x)) \\ & = & (x^5 + x^2 + 1)(x^5 + x^4 + x^3 + x^2 + 1)(x^5 + x^4 + x^2 + x + 1)(x^5 + x^3 + x^2 + x + 1). \end{array}$$

which is of degree 20, thus the plaintext length is 11.

Attachment: Representation of $GF(32)$ with $\alpha^5 = \alpha^2 + 1$

$\alpha^0 = 1$	00001
$\alpha^1 = \alpha$	00010
$\alpha^2 = \alpha^2$	00100
$\alpha^3 = \alpha^3$	01000
$\alpha^4 = \alpha^4$	10000
$\alpha^5 = \alpha^2 + 1$	00101
$\alpha^6 = \alpha^3 + \alpha$	01010
$\alpha^7 = \alpha^4 + \alpha^2$	10100
$\alpha^8 = \alpha^3 + \alpha^2 + 1$	01101
$\alpha^9 = \alpha^4 + \alpha^3 + \alpha$	11010
$\alpha^{10} = \alpha^4 + 1$	10001
$\alpha^{11} = \alpha^2 + \alpha + 1$	00111
$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha$	01110
$\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2$	11100
$\alpha^{14} = \alpha^4 + \alpha^3 + \alpha^2 + 1$	11101
$\alpha^{15} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	11111

$\alpha^{16} = \alpha^4 + \alpha^3 + \alpha + 1$	11011
$\alpha^{17} = \alpha^4 + \alpha + 1$	10011
$\alpha^{18} = \alpha + 1$	00011
$\alpha^{19} = \alpha^2 + \alpha$	00110
$\alpha^{20} = \alpha^3 + \alpha^2$	01100
$\alpha^{21} = \alpha^4 + \alpha^3$	11000
$\alpha^{22} = \alpha^4 + \alpha^2 + 1$	10101
$\alpha^{23} = \alpha^3 + \alpha^2 + \alpha + 1$	01111
$\alpha^{24} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	11110
$\alpha^{25} = \alpha^4 + \alpha^3 + 1$	11001
$\alpha^{26} = \alpha^4 + \alpha^2 + \alpha + 1$	10111
$\alpha^{27} = \alpha^3 + \alpha + 1$	01011
$\alpha^{28} = \alpha^4 + \alpha^2 + \alpha$	10110
$\alpha^{29} = \alpha^3 + 1$	01001
$\alpha^{30} = \alpha^4 + \alpha$	10010
$\alpha^{31} = 1$	00001