ALGEBRAIC SYSTEMS

Exam 2
October 29, 2007

The point value of each problem is given in the margin. Total = 80 points.

(8) 1. Find the quotient and remainder when \( x^4 - x^3 + x^2 \) is divided by \( 2x^2 + x + 1 \) in \( \mathbb{Z}_3[x] \).

Then state the relationship between the four polynomials (as given in the division algorithm).

\[
\begin{array}{c|cc|cc|cc|cc|cc}
2x^2 + x + 1 & 2x^4 & -x^3 & +x^2 \\
\hline
2x^2(2x^2 + x + 1) & 2x^4 & +2x^3 & +2x^2 \\
\hline
0 & 0 & -x^2 \\
-2(2x^2 + x + 1) & 0 & 0 & 0 \\
\hline
\end{array}
\]

Thus \( x^4 - x^3 + x^2 = (2x^2 - 2)(2x^2 + x + 1) + (2x + 2) \)

or \( x^4 - x^3 + x^2 = (2x^2 + 1)(2x^2 + x + 1) + (2x + 2) \)

(8) 2. a) Find the set of units \( U_9 \) in \( \mathbb{Z}_9 \).

\[ U_9 = \{1, 2, 4, 5, 7, 8\} \]

all elements \( a \) with \( \gcd(a, 9) = 1 \)

b) Find all zero divisors in \( \mathbb{Z}_9 \) and show explicitly why each is a zero divisor. (Remember 0 is not called a zero divisor.)

\[
\begin{align*}
3 & \not\mid 3, 6 \\
\gcd(a, 9) & > 1 \\
\end{align*}
\]

\[ 3 \cdot 3 \equiv 0 \pmod{9} \]

\[ 6 \cdot 3 \equiv 0 \pmod{9} \]

(4) 3. Find \( \phi(600) \), the number of integers from 1 to 600 that are relatively prime to 600.

\[ 600 = 6 \cdot 100 = 2^3 \cdot 3 \cdot 5^2 \]

\[ \phi(600) = \phi(2^3) \phi(3) \phi(5^2) = 4 \cdot 2 \cdot (5^2 - 5) = 160 \]

(2) 4. Find the set of units in \( \mathbb{Z}_3[x] \).

\[ \{1, 2\} \quad \text{must be a nonzero constant polynomial.} \]
5. a) State Fermat’s Little Theorem. (Dealing with modular exponentiation.)

Let \( p \) be a prime and \( a \) an integer with \( p \) not divide \( a \). Then

\[
a^{p-1} \equiv 1 \pmod{p}.
\]

b) Use Euler's Theorem to evaluate \( 17^{241} \pmod{35} \)

\[
\phi(35) = \phi(7, 5) = 6 \cdot 4 = 24.
\]

Since \( \gcd(17, 35) = 1 \) we have \( 17^{24} \equiv 1 \pmod{35} \), by Euler's Theorem.

\[
17^{241} = 17^{24 \cdot 10 + 1} = (17^{24})^{10} \cdot 17 \equiv 1 \cdot 17 \equiv 17 \pmod{35}
\]

(8) 5. Let \( z = -1 + i \in \mathbb{C} \).

a) Find \( |z| \) and the polar form (or exponential polar form) of \( z \).

\[
|z| = \sqrt{(-1)^2 + 1^2} = \sqrt{2}, \quad \theta = \text{polar angle} = \frac{3}{4} \pi.
\]

\[
z = r \, e^{i \theta} = \sqrt{2} \, e^{\frac{3}{4} \pi \, i}
\]

or \( z = \sqrt{2} \left( \cos \left( \frac{3}{4} \pi \right) + i \sin \left( \frac{3}{4} \pi \right) \right) \)

b) Find \( z^{10} \). Express your final answer in the form \( a + bi \).

\[
z^{10} = (\sqrt{2})^{10} \left( e^{\frac{3}{4} \pi \, i} \right)^{10} = 2^5 \cdot 10 \, e^{\frac{30}{4} \pi \, i} = 2^5 \, e^{\frac{15}{2} \pi \, i}
\]

Now \( \frac{15}{2} \pi \) is equivalent to the angle \( \frac{3}{2} \pi \), so

\[
z^{10} = 2^5 \, e^{\frac{3}{2} \pi \, i} = 2^5 (-i) = -32 \, i
\]

(5) 6. Find all cube roots of \( i \) in \( \mathbb{C} \). Express your answers in polar form or exponential form.

\[
i = e^{\frac{\pi}{2} \, i} = e^{\left( \frac{\pi}{2} + 2\pi k \right) \, i}, \quad k = 0, 1, 2
\]

\[
i^{\frac{1}{3}} = e^{\left( \frac{\pi}{2} + 2\pi k \right) \, i \cdot \frac{1}{3}} = e^{\left( \frac{\pi}{6} + \frac{2\pi}{3} k \right) \, i}, \quad k = 0, 1, 2
\]
(8) 7. Give examples of the following.
   a) A noncommutative ring. \( M_{2,2}(\mathbb{R}) \), \( \mathbb{R} = \text{any ring} \)
   b) Two different rings with 16 elements. (Hint: Think about a matrix ring for one example.)
      \( \mathbb{Z}_{16} \) \( \mathbb{M}_{2,2}(\mathbb{Z}_2) \), since \( 2^4 = 16 \).
   c) An integral domain that is not a field.
      \( \mathbb{Z} \), \( \mathbb{Z}[x] \), etc.
   d) A ring with infinitely many elements that has zero divisors.
      \( M_{2,2}(\mathbb{R}) \), \( \mathbb{Z}_6[x] \), etc.

(12) 8. Indicate whether the following sets are closed under addition (C.A.), closed under multiplication (C.M.), Rings (Ring), Commutative rings (C.Ring), Rings with Unity (R.U.), Integral Domains (Domain), Fields (Field). Circle all correct answers on each problem.

   a) \( \mathbb{Z}_{10} \)
      \( \text{C.A.} \) \( \text{C.M.} \) \( \text{Ring} \) \( \text{C.Ring} \) \( \text{R.U.} \) \( \text{Domain} \) \( \text{Field} \)

   b) \( \mathbb{Z}_5 \)
      \( \text{C.A.} \) \( \text{C.M.} \) \( \text{Ring} \) \( \text{C.Ring} \) \( \text{R.U} \) \( \text{Domain} \) \( \text{Field} \)

   c) \( \mathbb{Z}_5[x] \)
      \( \text{C.A.} \) \( \text{C.M.} \) \( \text{Ring} \) \( \text{C.Ring} \) \( \text{R.U.} \) \( \text{Domain} \) \( \text{Field} \)

   d) \( \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{Z} \right\} \)
      \( \text{C.A.} \) \( \text{C.M.} \) \( \text{Ring} \) \( \text{C.Ring} \) \( \text{R.U.} \) \( \text{Domain} \) \( \text{Field} \)
      \( \begin{bmatrix} a \circ c & 0 \\ 0 & b \circ d \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \)

   e) \( \{[0], [3], [6]\} \) in \( \mathbb{Z}_7 \)
      \( \text{C.A.} \) \( \text{C.M.} \) \( \text{Ring} \) \( \text{C.Ring} \) \( \text{R.U.} \) \( \text{Domain} \) \( \text{Field} \)

   f) \( E = \{2n : n \in \mathbb{Z}\} \)
      \( \text{C.A.} \) \( \text{C.M.} \) \( \text{Ring} \) \( \text{C.Ring} \) \( \text{R.U.} \) \( \text{Domain} \) \( \text{Field} \)

(6) 9. Prove that if \( p \) is a prime then \( \mathbb{Z}_p \) is a field. (You may assume an appropriate theorem on when a number has a multiplicative inverse \( \text{(mod} \ m) \).)

We may assume \( \mathbb{Z}_p \) is a commutative ring. The unity element in \( \mathbb{Z}_p \) is \( 1 = [1]_p \). Let \( a \) be a nonzero element of \( \mathbb{Z}_p \). Then \( p \) divides \( a \) and so \( \gcd(p, a) = 1 \), since \( p \) is a prime. Thus \( a \) has a multiplicative inverse \( \text{(mod} \ p) \), that is, \( a^{-1} \) exists in \( \mathbb{Z}_p \). Therefore \( \mathbb{Z}_p \) is a field.
10. Prove that for any complex numbers \( z = a + bi \) and \( w = c + di \) that \( \overline{zw} = \overline{z} \overline{w} \).

\[
\overline{zw} = \overline{(a+bi)(c+di)} = (ac - bd) + (bc + ad)i = \overline{(ac - bd)} - (bc + ad)i
\]

\[
\overline{z} \cdot \overline{w} = (a - bi)(c - di) = ac + bd - bc - adi = (ac - bd) - (bc + ad)i
\]

Thus \( \overline{zw} = \overline{z} \overline{w} \).

11. Find all numbers of the form 23ab4a6 divisible by 99.

Must be divisible by 11 and 9.

Test 11: \( 2 - 3 + a - b + 4 - a + b = 9 - b = 0 \), \( b = -1 \), \( 1111111111 \) etc.

Since \( b \in \{0, 1, 2, \ldots, 9\} \) we must have \( b = 9 \).

Test 9: \( 2 + 3 + a + b + 4 + a + 6 = 15 + 2a + b = 24 + 2a = 9, 18, 27, 36, 45 \)

Since \( a \in \{0, 1, 2, \ldots, 9\} \) we must have \( 24 + 2a = 36 \)

\[ \Rightarrow 2a = 12 \]
\[ \Rightarrow a = 6 \]

Thus only 2369466 is divisible by 99.

Extra Credit:

1. Prove that for any real number \( \theta \), \( e^{i\theta} = \cos(\theta) + i\sin(\theta) \). (You may assume convergence properties of series.)

\[
e^{i\theta} = 1 + i\theta + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} + \frac{(i\theta)^5}{5!} + \cdots
\]

\[= 1 + i\theta - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \frac{\theta^4}{4!} + i\frac{\theta^5}{5!} + \cdots
\]

\[= (1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \cdots) + i \left( \theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \cdots \right)
\]

\[= \cos \theta + i \sin \theta
\]

2. Let \( R \) be a ring with unity, and \( x \) be an element of \( R \) such that \( x^2 = 0 \). Prove that \( x + 1 \) is a unit in \( R \) by explicitly finding its multiplicative inverse.

Note: \( (1+x)(1-x) = 1 + x - x - x^2 = 1 - x^2 = 1 \)

and \( (1-x)(1+x) = 1 - x^2 = 1 \)

Thus \( (1-x) \) is the multiplicative inverse of \( 1+x \).