ALGEBRAIC SYSTEMS
Exam 2
November 6, 2009

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

(6)  1. Define the addition law for $\mathbb{Z}_m$ and prove that it is well defined.
(You may assume properties of congruences.)
For any $[a]_m, [b]_m \in \mathbb{Z}_m$, $[a]_m + [b]_m = [a + b]_m$.

Suppose $[a]_m = [a']_m$, $[b]_m = [b']_m$. Then $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$.
Thus, by property of congruences $a + b \equiv a' + b' \pmod{m}$. This implies that $[a + b]_m = [a' + b']_m$.

(3)  2. a) Let $R$ be a ring with unity. Define what it means for an element $a \in R$ to be a unit.
$\text{a is a unit if there exists a } b \in R \text{ such that } ab = 1 \text{ and } ba = 1$.

b) Let $U_{150}$ be the group of units in $\mathbb{Z}_{150}$. Find $|U_{150}|$, the number of elements in $U_{150}$.

\[
|U_{150}| = \phi(150) = \phi(2 \cdot 3 \cdot 5^2) = \phi(2) \phi(3) \phi(5^2) = 1 \cdot 2 \cdot (5^2 - 5) = 1 \cdot 2 \cdot 20 = 40
\]

(2)  c) Find a zero divisor in $\mathbb{Z}_{15}$ and show why it satisfies the definition of a zero divisor.
$3$ is a zero divisor since $3 \cdot 0 \equiv 5 \cdot 0$ and $3 \cdot 5 \equiv 0$.

(2)  d) Find all zero divisors in $\mathbb{Z}_{15}$. (No justification required.)
$\{3, 5, 6, 9, 10, 12\}$
Note: 0 is not called a zero divisor.
3. a) State Euler's Theorem. (Dealing with modular exponentiation \((\text{mod } m)\).) Let \(m \in \mathbb{N}, a \in \mathbb{Z} \text{ with } \gcd(a, m) = 1\). Then
\[
\phi(m) a^{\phi(m)} \equiv 1 \pmod{m}
\]
b) Use Fermat’s Little Theorem or Euler’s Theorem to evaluate \(23^{93} \pmod{47}\)

Since \(47\) is a prime and \(\gcd(23, 47) = 1\), we have by FLT
\[
23^{46} \equiv 1 \pmod{47}
\]
Thus \(23^{93} \equiv 23^{46 \cdot 2 + 1} \equiv (23^{46})^2 \cdot 23 \equiv 1^2 \cdot 23 \equiv 23 \pmod{47}\).

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

a) Find \(|z|\) and the exponential polar form of \(z\).
\[
|z| = \sqrt{(-1)^2 + 1^2} = \sqrt{2}
\]
\[
z = r e^{i \theta} = \sqrt{2} e^{\frac{3}{4} \pi i}
\]

b) Find \(z^6\). Express your final answer in standard form \(a + bi\) with no trig functions.
\[
z^6 = \left(\sqrt{2} e^{\frac{3}{4} \pi i}\right)^6 = 2^3 e^{\frac{3}{4} \cdot 6 \pi i} = 8 e^{\frac{3}{2} \pi i} = 8 e^{\frac{3}{2} \pi i}
\]
\[
\frac{3}{2} \pi \approx \pi / 2
\]

5. Find all cube roots of \(i\) in \(\mathbb{C}\). Express your answers in polar form or exponential polar form and plot the points on the unit circle.

In polar form \(i = 1 e^{\frac{\pi}{2} i} = e^{\frac{\pi}{2} i} = e^{\left(\frac{\pi}{2} + 2\pi k\right) i}\)

\[
i^{1/3} = \left(e^{\left(\frac{\pi}{2} + 2\pi k\right) i}\right)^{\frac{1}{3}} = e^{\left(\frac{\pi}{6} + \frac{2\pi}{3} k\right) i}, \quad k = 0, 1, 2
\]

\[
e^{\frac{\pi}{6} i} \quad e^{\frac{\pi}{2} i} = -i
\]
6. Short answer.
   a) Give an example of a noncommutative ring. \( \mathbb{M}_{2,2}(\mathbb{Z}) \) (Any matrix ring) .

   b) Give an example of a finite field. \( \mathbb{Z}_p \), where \( p \) is any prime .

   c) Give an example of an integral domain that is not a field but has infinitely many units. \( \mathbb{R}[x] \)

   d) Give an example of three distinct integral domains \( A, B, C \) with \( A \subset B \subset C \).

\[ \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \quad , \quad \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \quad , \quad \text{etc.} \quad \mathbb{Z} \subset \mathbb{Q}[x] \subset \mathbb{R}[x] \]

7. 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) \( \mathbb{Z}_9 \) (C.A) (C.M) (Ring) (C.Ring) (R.U) Domain Field

   b) \( M_{2,2}(\mathbb{Z}) \) (C.A) (C.M) (Ring) (C.Ring) (R.U) Domain Field

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

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

   e) \( \{0, 1, 4, 8\} \) in \( \mathbb{Z}_{12} \) (C.A) (C.M) (Ring) (C.Ring) (R.U) Domain Field

6. Prove the cancellation law for \( \mathbb{Z}_m \).
If \( \gcd(a, m) = 1 \) and \( ax \equiv ay \pmod{m} \), then \( x \equiv y \pmod{m} \).
(You may assume appropriate lemmas.)

Since \( \gcd(a, m) = 1 \) we know \( a \) has an inverse \( a^{-1} \in \mathbb{Z}_m \). Thus

\[ ax \equiv ay \pmod{m} \]

\[ \Rightarrow a^{-1}(ax) \equiv a^{-1}(ay) \pmod{m} \]

\[ \Rightarrow (a^{-1})x \equiv (a^{-1})y \pmod{m} \]

\[ \Rightarrow 1 \times x \equiv 1 \times y \pmod{m} \]

\[ \Rightarrow x \equiv y \pmod{m} . \]
(8) 9. a) Let \( z \in \mathbb{C} \) with polar angle \( \theta \) and \( |z| = r \).
Prove (geometrically) that \( z = r(\cos(\theta) + i\sin(\theta)) \).

Say \( z = x + iy \).

By def of trig functions
\[ x = r \cos \theta \]
\[ y = r \sin \theta \]
Thus \( z = r \cos \theta + i(r \sin \theta) \).

\[
\frac{z \cdot \overline{z}}{|z|^2} = \frac{z \cdot \overline{z}}{|z|^2} = \frac{|z|^2}{|z|^2} = 1
\]
Thus \( \frac{z}{|z|^2} \) satisfies the def. of mult. inverse.
Also note \( \frac{z}{|z|^2} \in \mathbb{C} \) since \( z \) is nonzero, so \( |z| \neq 0 \).

b) Let \( z \) be a nonzero complex number. Prove that \( z^{-1} = \frac{z}{|z|^2} \).

(6) 10. Find the quotient and remainder when \( x^3 + x^2 \) is divided by \( 2x^2 - 1 \) in \( \mathbb{Z}_3[x] \). Then state the relationship between the four polynomials (as given in the division algorithm).

\[
\begin{align*}
2x^2 - 1 & \overline{=} \frac{2x + 2}{x^3 + x^2} \\
2x(2x^2 - 1) & \overline{=} \frac{x^3 - 2x}{x^2 + 2x} \\
2(2x - 1) & \overline{=} \frac{x^2 - 2}{2x + 2}
\end{align*}
\]

Quotient = \( 2x + 2 \)
Remainder = \( 2x + 2 \)

\( f(x) = q(x) \cdot g(x) + r(x) \)
\[ x^3 + x^2 = (2x + 2)(2x^2 - 1) + (2x + 2) \].