Practice Problems

Modern Algebra II, Dave Bayer, September 29, 2009

Name: ______________________________

[1] (6 pts)	[2] (6 pts)	[3] (6 pts)	[4] (6 pts)	[5] (6 pts)	TOTAL

Please work only one problem per page, starting with the pages provided. Clearly label your answer. If a problem continues on a new page, clearly state this fact on both the old and the new pages.

(Note that there are more than five practice problems here. The actual exam will consist of five problems.)

[**1**] Find a pair of inverse ring isomorphisms between $\mathbb{Z}/91\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$. Show that your maps are in fact inverse to each other. Using these maps, compute 5^{26} mod 91.

[2] Find a pair of inverse ring isomorphisms between $\mathbb{Z}/187\mathbb{Z}$ and $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$. Show that your maps are in fact inverse to each other. Using these maps, compute 3^{32} mod 187.

[**3**] Find a pair of inverse ring isomorphisms between $\mathbb{Z}/144\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$. Show that your maps are in fact inverse to each other. Using these maps, compute 5^{25} mod 144.

[**4**] A message is represented as an integer $a \mod 55$. You receive the encrypted message $a^7 \equiv 13 \mod 55$. What is a?

[5] A message is represented as an integer $a \mod 91$. You receive the encrypted message $a^{17} \equiv 61 \mod 91$. What is a?

[**6**] A message is represented as an integer $a \mod 187$. You receive the encrypted message $a^9 \equiv 60 \mod 187$. What is a?

[7] Let A be an $n \times n$ matrix with entries in $\mathbb{R}$, satisfying the polynomial relation

$$(x-2)(x-3) \;=\; 0$$

Find a formula for e^{At} as a polynomial expression in A. Give an example of a matrix A for which this is the minimal polynomial relation, and check your formula using this matrix.

[**8**] Let A be an $n \times n$ matrix with entries in $\mathbb{R}$, satisfying the polynomial relation

$$(x-2)^2 \;=\; 0$$

Find a formula for e^{At} as a polynomial expression in A. Give an example of a matrix A for which this is the minimal polynomial relation, and check your formula using this matrix.

[**9**] Let A be an $n \times n$ matrix with entries in $\mathbb{R}$, satisfying the polynomial relation

$$(x-2)^2(x-3) \;=\; 0$$

Find a formula for e^{At} as a polynomial expression in A. Give an example of a matrix A for which this is the minimal polynomial relation, and check your formula using this matrix.

[**10**] Construct the finite field $\mathbb{F}_4$ as an extension of $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, by finding an irreducible polynomial of degree 2 with coefficients in $\mathbb{F}_2$. What are the two roots of your irreducible polynomial?

[**11**] Construct the finite field $\mathbb{F}_8$ as an extension of $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, by finding an irreducible polynomial of degree 3 with coefficients in $\mathbb{F}_2$. What are the three roots of your irreducible polynomial?

[12] Construct the finite field $\mathbb{F}_9$ as an extension of $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$, by finding an irreducible polynomial of degree 2 with coefficients in $\mathbb{F}_3$. What are the two roots of your irreducible polynomial?

[13] Construct the finite field $\mathbb{F}_{16}$ as an extension of $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, by finding an irreducible polynomial of degree 4 with coefficients in $\mathbb{F}_2$. What are the four roots of your irreducible polynomial?

[**14**] Construct the finite field $\mathbb{F}_{25}$ as an extension of $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$, by finding an irreducible polynomial of degree 2 with coefficients in $\mathbb{F}_5$. What are the two roots of your irreducible polynomial?

[15] Construct the finite field $\mathbb{F}_{27}$ as an extension of $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$, by finding an irreducible polynomial of degree 3 with coefficients in $\mathbb{F}_3$. What are the three roots of your irreducible polynomial?

[16] Let $\mathbb{Z}[x]$ be the ring of polynomials in x with coeficients in $\mathbb{Z}$. Give an example of a maximal ideal $I \subset \mathbb{Z}[x]$. Give an example of an ideal I which is prime but not maximal. Are there any ideals I such that the quotient $\mathbb{Z}[x]$ is a field not of the form $\mathbb{Z}/p\mathbb{Z}$ for a prime p?