First Exam

Modern Algebra II, Dave Bayer, October 5, 2010

Name: solutions

[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.

[1] Define a maximal ideal, and give an example of a maximal ideal. Define a prime ideal, and give an example of a prime ideal. Give an example of three prime ideals $I \subset J \subset K$, each strictly contained in the next.

I maximal $\Leftrightarrow$ no J so $I \subsetneq J \subsetneq (1)$

$\Leftrightarrow$ R/I field

(p) maximal in $\mathbb{Z}$, $\mathbb{Z}/(p) \cong \mathbb{F}_p$ field

---

I prime $\Leftrightarrow$ $ab \in I \Rightarrow a \in I$ or $b \in I$

$\Leftrightarrow$ R/I integral domain

(p) prime in $\mathbb{Z}$, $\mathbb{Z}/(p) \cong \mathbb{F}_p$ also integral domain

---

in $R = \mathbb{Z}[x]$

ideals: $(0) \subsetneq (2) \subsetneq (2, x^2+x+1)$

quotients: $\mathbb{Z}[x]$ $\quad \mathbb{Z}/2\mathbb{Z}[x] \cong \mathbb{F}_2[x]$ $\quad \mathbb{F}_4 \cong \mathbb{F}_2[x]/(x^2+x+1)$

(all quotients are integral domains)

$77 = 7 \cdot 11$

[2] Compute 5^{32} mod 77.

$$(\mathbb{Z}/77\mathbb{Z})^* \cong (\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/11\mathbb{Z})^*$$

$$\cong \quad C_6 \times C_{10}$$

so for any invertible a, $a^{30} = 1$

thus $\boxed{5^{32} \equiv 5^2 \equiv 25 \bmod 77}$

[3] A message is represented as an integer a mod 57. You receive the encrypted message $a^{11} \equiv 2 \mod 57$. What is a?

$$57 = 3 \cdot 19$$

$$(\mathbb{Z}/57\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/19\mathbb{Z})^*$$

$$\cong \quad C_2 \quad \times \quad C_{18}$$

so for any invertible a, $a^{18} = 1$

---

want e so $(a^{11})^e = a \mod 57$

exponents work mod 18

want e so $11e \equiv 1 \mod 18$

11 22 33 44 55

18 36 54

ha!

$5 \cdot 11 = 55 \equiv 1 \mod 18$

so if $a^{11} = 2$, then $a = (a^{11})^5 = 2^5 = \boxed{32}$

---

check $32^{11} = 2$?

mod 3, $32^{11} = (-1)^{11} = -1 = 2$ ☑

mod 19, $32 = -6$

$32^2 = 36 = -2$

$32^{10} = (32^2)^5 = (-2)^5 = -32 = 6$

$\Rightarrow 32^{11} = -6 \cdot 6 = -36 = 2$ ☑

[4] Let A be a 2×2 matrix with entries in $\mathbb{R}$, satisfying the polynomial relation

$$(x-1)(x-3) = 0$$

Find a formula for A^n as a polynomial expression in A. What is $\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}^n$?

$$\mathbb{R}[x]/_{(x-1)(x-3)} \cong \mathbb{R}[x]/_{(x-1)} \times \mathbb{R}[x]/_{(x-3)}$$

$$1 = \tfrac{1}{2}(x-1) - \tfrac{1}{2}(x-3) \quad \text{so}$$

$$\boxed{-\tfrac{4}{2}(x-3) + \tfrac{2}{2}(x-1) \longleftarrow (4, 2)}$$

$$\begin{array}{ccc} -\tfrac{1}{2}(x-3) & & (1, 0) \\ \tfrac{1}{2}(x-1) & & (0, 1) \\ \hline 1 & \longleftarrow & (1, 1) \end{array}$$

$$x^n = (1, 3^n) \bmod (x-1, x-3)$$

$$\mapsto -\tfrac{1}{2}(x-3) + \tfrac{3^n}{2}(x-1)$$

$$\boxed{A^n = -\tfrac{1}{2}(A-3I) + \tfrac{3^n}{2}(A-I)}$$

$$\boxed{\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}^n = -\tfrac{1}{2}\begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} + \tfrac{3^n}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}}$$

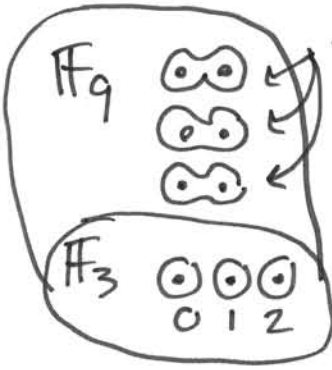
check

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \checkmark$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}^1 = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \checkmark$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}^2 = -\tfrac{1}{2}\begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} + \tfrac{9}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 5 & 4 \\ 4 & 5 \end{bmatrix} \checkmark$$

[5] 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 $\mathbb{F}_3$. Find a generator of the multiplicative group $\mathbb{F}_9^*$ of nonzero elements of $\mathbb{F}_9$. Demonstrate that your choice is indeed a generator.



3 irred polys monic, deg $2/\mathbb{F}_3$

irreducible $\Leftrightarrow$ no root 0,1,2

x^2	x	1	$x=1$	$x=2$	
1	0	1	2	2	x^2+1
~~1~~	~~0~~	~~2~~	~~0~~		
~~1~~	~~1~~	~~1~~	~~0~~		
1	1	2	1	2	x^2+x+2
~~1~~	~~2~~	~~1~~	~~1~~	~~0~~	
1	2	2	2	1	x^2+2x+2

pick simplest

so $\mathbb{F}_9 \cong \mathbb{F}_3[\alpha]/(\alpha^2+1)$

$(\mathbb{F}_9)^* \cong C_8$ For $a \in \mathbb{F}_9^*$, either a generates C_8 or $a^4 = 1$

α generates $\mathbb{F}_9^*$?

$\alpha^1 = \alpha$, $\alpha^2 = \alpha^2$ $\quad \dfrac{2\alpha^2+2}{2}$ $\quad \alpha^3 = 2\alpha$, $\alpha^4 = 1$ guess not!

$C_4 = \{1, 2, \alpha, 2\alpha\} \subset C_8$

$C_8 \setminus C_4 = \{\alpha+1, \alpha+2, 2\alpha+1, 2\alpha+2\}$ any must work

$(\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha$ $\quad \dfrac{2\alpha^2 \quad +2}{2\alpha}$ $\quad$ so $(\alpha+1)^4 = (2\alpha)^2 = \alpha^2 = 2 \neq 1$

$\Rightarrow$ $\boxed{\alpha+1 \text{ generates } \mathbb{F}_9^*}$