Mathematics 366	Midterm 1 (100 points)	9/30/09

Points (leave blank)					
1	2	3	4	5	Σ

Name: SAMPLE
(clearly, please)

You can work on the problems in any order you like. Show your work! All problems carry the same weight.
Calculation steps and explanation for statements made are a crucial part of a solution. Partial credit will be given sparingly – rather complete one problem than start two only partially.

1) Find an integer solution x for the equation

$$23x \bmod 89 = 4$$

gcd(23, 89):

$89 = 3 \cdot 23 + 20 \Rightarrow 20 = 89 - 3 \cdot 23$

$23 = 1 \cdot 20 + 3 \qquad 3 = 23 - 20$

$20 = 6 \cdot 3 + 2 \qquad 2 = 20 - 6 \cdot 3$

$3 = 1 \cdot 2 + 1 \Rightarrow 1 = 3 - 2$

$\Rightarrow 1 = 3 - 2 = 3 - 20 + 6 \cdot 3 = 7 \cdot (23 - 20) - 20 = 7 \cdot 23 - 8(89 - 3 \cdot 23)$

$= -8(89) + 31 \cdot 23 \Rightarrow 23^{-1} \equiv 31 \pmod{89}$

$\Rightarrow x \equiv 4 \cdot 31 \equiv 124 \equiv 35 \pmod{89}$

2) Determine (with explanation) the units and zero divisors in the ring $\mathbb{Z}_{10}$.

As $\gcd(10,1) = \gcd(10,3) = \gcd(10,7) = \gcd(10,9) = 1$

$\{1, 3, 7, 9\}$ are units

As $2 \cdot 5 \equiv 4 \cdot 5 \equiv 6\,5 \equiv 8\,5 \equiv 0 \pmod{10}$

$\{2, 4, 5, 6, 8\}$ are zero divisors.

As units cannot be zero divisors and we exhausted $\mathbb{Z}_{10} - \{0\}$, these are all

3) Construct the multiplication table for the field with 4 elements by using polynomial arithmetic modulo 2 and modulo $x^2 + x + 1$.

In this field, calculate $\frac{a}{a+1}$, where a is the element represented by the polynomial x.

Elements = possible remainders = $\{0, 1, x, x+1\}$

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

$x^2 \equiv -x+1 \pmod{x^2+x+1}$

$\equiv x+1 \pmod 2$

$x(x+1) = x^2+x \equiv -1(x^2+x+1)$

$\equiv 1 \ (2)$

To calculate $\frac{a}{a+1}$, note that $x \cdot (x+1) = 1 \Rightarrow \frac{1}{x+1} = x$

$\Rightarrow \frac{a}{a+1} = \frac{x}{x+1} = x \cdot \frac{1}{x+1} = x \cdot x = x^2 \underset{\text{Table}}{\equiv} x+1 \pmod{x^2+x+1}$ $\pmod 2$

Thus $\frac{a}{a+1} = a+1 = x+1$

4) Let $R = \mathbb{Q}[x]$ and let $A = \{f \in R \mid f(1) = 0\}$.
a) Show that A is a subring of R.
b) Show that A is an ideal in R.
c) Let $B = \{f \in R \mid f(1) = 1\}$. Show that B is not a subring of R.

a) ~~Let~~ Clearly $f(x) = 0$ is an element of $A \Rightarrow A \neq \emptyset$

Let $f, g \in A$ Then $(f+g)(1) = f(1) + g(1) = 0 + 0 = 0$

$\Rightarrow f+g \in A$

Similarly $(-f)(1) = -f(1) = -0 = 0 \Rightarrow -f \in A$.

and $(fg)(1) = f(1)\, g(1) = 0\, 0 = 0$.

Thus $A \leq R$.

b) Let $f \in A$, $g \in R$ Then $(fg)(1) = f(1)\, g(1)$

sufficient, as R is commutative

$= 0\, g(1) = 0$ $\Rightarrow fg \in A$ Thus (as $A \leq R$) also $A \trianglelefteq R$.

c) Let $f(x) = x$. Then $f(x) \in B$

But $(f+f)(1) = f(1) + f(1) = 1 + 1 = 2 \neq 1$

Thus ~~f(1)~~ $f+f \notin B$, and therefore $B \not\leq R$

5) Let R be a commutative ring with one, in which R and $\{0\}$ are the only ideals. For $0 \neq x \in R$ consider the ideal generated by x, which is $A = \langle x \rangle_R = \{rx \mid r \in R\} \triangleleft R$. Show that $A \neq \{0\}$ and thus $A = R$. Conclude that x must have an inverse and therefore conclude that R is a field.
Your proof should consists of full sentences. (It is not sufficient to simply point to lecture or homework.)

Let $0 \neq x \in R$ and let $A = \langle x \rangle_R$ Then $A \neq \{0\}$,

thus (by assumption) $A = R$ But thus $1_R \in A = \langle x \rangle_R$

exists, as it does.

Thus there exists $r \in R$ s.t.

$1_R = x \cdot r$ Thus (R commutative) x is a unit

R therefore is a commutative ring with 1 in which every nonzero elt. is a unit Thus it is a field.