Name SOLUTIONS

PID ______________________

Final

MTH 310, Thursday June 28, 2018

Instructions: This exam is closed notes, closed books, no calculators and no electronic devices of any kind. There are five problems worth 20 points each. If a problem has multiple parts, it may be possible to solve a later part without solving the previous parts. Solutions should be written neatly and in a logically organized manner. Partial credit will be given if the student demonstrates an understanding of the problem and presents some steps leading to the solution. Correct answers with *no work* will be given *no credit*. The back sheets may be used as scratch paper but will not be graded for credit.

1	2	3	4	5	Total

Problem 1.

a. (10 points) Compute the remainder of 2^{310} when divided by 5. (*Hint*: $2^{310} = (2^2)^{155}$)

Following the hint we have that $2^{310} = 4^{155}$. Thus, $[2^{310}]_5 = [4]_5^{155} = [-1]_5^{155} = [-1]_5 = [4]_5$. By comparing congruence classes we have determined that the remainder is 4.

b. (10 points) Let $f : \mathbb{Z}_6 \to \mathbb{Z}_4$ be a homomorphism of rings with $f([1]_6) = [2]_4$. Compute $f([4]_6)$.

$$\begin{aligned} f([4]_6) &= f([1]_6 + [1]_6 + [1]_6 + [1]_6) \\ &= f([1]_6) + f([1]_6) + f([1]_6) + f([1]_6) \qquad \text{(f respects addition)} \\ &= [2]_4 + [2]_4 + [2]_4 + [2]_4 \\ &= [8]_4 = [0]_4. \end{aligned}$$

Problem 2. Let $p(x) = x^3 + 2x + 1$ in $\mathbb{Z}_3[x]$.

a. (6 pts) Show that $p(x)$ is irreducible in $\mathbb{Z}_3[x]$.

We have that

$$\begin{aligned} p(0) &= 0^3 + 2(0) + 1 = 1 \\ p(1) &= 1^3 + 2(1) + 1 = 1 \\ p(2) &= 2^3 + 2(2) + 1 = 1. \end{aligned}$$

Thus $p(x)$ has no roots in $\mathbb{Z}_3$. By the Factor Theorem, $p(x)$ has no linear factor. Since $p(x)$ is degree 3 and has no linear factor we conclude that $p(x)$ is irreducible.

b. (7 pts) Find the inverse of $[x^2 + 1]$ in $\mathbb{Z}_3[x]/\langle p \rangle$.

Following the Euclidean Algorithm we find that

$$\begin{aligned} x^3 + 2x + 1 &= (x^2 + 1)(x) + (x + 1) \\ x^2 + 1 &= (x + 1)(x + 2) + 2 \end{aligned}$$

where the first equality can be seen by long division, and the second can just be check by hand:

Therefore,

$$\begin{aligned} 2 &= (x^2 + 1) - (x + 1)(x + 2) \\ &= (x^2 + 1) - ((x^3 + 2x + 1) - (x^2 + 1)(x))(x + 2) \\ &= (x^2 + 1)(1 + x(x + 2)) + (x^3 + 2x + 1)(-1)(x + 2) \\ &= (x^2 + 1)(x^2 + 2x + 1) + (x^3 + 2x + 1)(2x + 1) \end{aligned}$$

Multiplying by 2 we have

$$1 = (x^2 + 1)(2x^2 + x + 2) + (x^3 + 2x + 1)(x + 2).$$

Therefore, $[2x^2 + x + 2] = [x^2 + 1]^{-1}$.

c. (7 pts) How many elements are in the quotient ring $\mathbb{Z}_3[x]/\langle p \rangle$? Is $\mathbb{Z}_3[x]/\langle p \rangle$ a field?

Since each congruence class has a representative of degree less then 3, we have that $\mathbb{Z}_3[x]/\langle p \rangle = \{ax^2 + bx + c : a, b, c \in \mathbb{Z}_3\}$. Therefore, $\mathbb{Z}_3[x]/\langle p \rangle$ has $3^3 = 27$ elements.

Yes, the quotient ring $\mathbb{Z}_3[x]/\langle p \rangle$ is a field since p is irreducible, as we proved in a.

Problem 3.

a. (6 pts) Show that $x^2 + 1$ has no roots in $\mathbb{Z}_7$.

We can simply check by hand that $f(x) = x^2 + 1$ has no roots in $\mathbb{Z}_7$.

$$\begin{aligned} f(0) &= 0^2 + 1 = 1 \\ f(1) &= 1^2 + 1 = 2 \\ f(2) &= 2^2 + 1 = 5 \\ f(3) &= 3^2 + 1 = 3 \\ f(4) &= 4^2 + 1 = 3 \\ f(5) &= 5^2 + 1 = 5 \\ f(6) &= 6^2 + 1 = 2. \end{aligned}$$

Therefore $f(x)$ has no roots in $\mathbb{Z}_7$.

b. (7 pts) Show that if $a \neq 0$ or $b \neq 0$ in $\mathbb{Z}_7$ then $a^2 + b^2 \neq 0$ in $\mathbb{Z}_7$.

(*Hint:* First, show that if $b \neq 0$ then $a^2 + b^2 = b^2((b^{-1}a)^2 + 1)$. Then, use part a.)

If $b \neq 0$ then b is a unit since $\mathbb{Z}_7$ is a field and $b^2 = b \cdot b \neq 0$ since $\mathbb{Z}_7$ is an integral domain.

If $a = 0$, then $a^2 + b^2 = b^2 \neq 0$.

Suppose $a \neq 0$. Following the hint we have

$$a^2 + b^2 = b^2(c) \qquad \text{where} \qquad c = (b^{-1}a)^2 + 1.$$

By a. we know that $c = f(b^{-1}a) = (b^{-1}a)^2 + 1 \neq 0$ since $b^{-1}a \neq 0$. Since $a^2 + b^2$ is a product of two non-zero elements and $\mathbb{Z}_7$ is an integral domain, we conclude that $a^2 + b^2 \neq 0$.

c. (7 pts) Consider the ring $\mathbb{Z}_7[i] := \{a + ib : a, b \in \mathbb{Z}_7\}$. Recall that $i^2 = -1$ and

$$\begin{aligned} (a + ib) + (c + id) &= (a + c) + i(b + d), \\ (a + ib)(c + id) &= (ac - bd) + i(ad + bc). \end{aligned}$$

Prove that $\mathbb{Z}_7[i]$ is an integral domain. Is $\mathbb{Z}_7[i]$ a field?

Let $a + ib, c + id \in \mathbb{Z}_7[i]$ and suppose $(a + ib)(c + id) = 0$. It follows that

$$\begin{aligned} 0 &= (a + ib)(a - ib)(c + id)(c - id) \\ &= (a^2 + b^2)(c^2 + d^2). \end{aligned}$$

Since $\mathbb{Z}_7$ is a integral domain, either $a^2 + b^2 = 0$ or $c^2 + d^2 = 0$. By the contrapositive of what we showed in b., if $a^2 + b^2 = 0$ then $a = 0$ and $b = 0$. Therefore, $a + ib = 0$. Similarly, if $c^2 + d^2 = 0$ then $c + id = 0$. We conclude that $\mathbb{Z}_7[x]$ is an integral domain.

$\mathbb{Z}_7[i]$ has $7^2 = 49$ elements. We know that every finite integral domain is a field, therefore $\mathbb{Z}_7[i]$ is a field.

Problem 4. Let $f : R \to S$ be a homomorphism of rings and $J \subset S$ be an ideal. Define the set

$$I = \{a \in R : f(a) \in J\} \subset R.$$

a. (6 pts) Show that $\ker f \subset I$.

Let $a \in \ker f$, that is, $f(a) = 0_S$. Since J is an ideal, its a subring and contains $0_S \in J$. Thus $f(a) \in J$ which implies that $a \in I$. Therefore, $\ker f \subset I$.

b. (7 pts) Prove that I is a subring of R.

Let $a, b \in I$, that is, $f(a) \in J$ and $f(b) \in J$. Since J is an ideal it is closed under addition and multiplication, therefore, $f(a) + f(b) \in J$ and $f(a)f(b) \in J$. Since f is a homomorphism

$$f(a + b) = f(a) + f(b) \in J$$
$$f(ab) = f(a)f(b) \in J.$$

Therefore $a + b \in J$ and $ab \in J$.

By a basic ring homomorphism property we know that $f(0_R) = O_S \in J$ which implies $0_R \in I$ and $f(-a) = -f(a) \in J$. By the subring theorem we conclude that I is a subring of R.

c. (7 pts) Prove that I is an ideal in R.

Let $a \in I$ and $r \in R$. It follows that $f(a) \in J$ and $f(r) \in S$. Since J is an ideal it has the ideal property, thus $f(a)f(r) = f(ar) \in J$ and $f(r)f(a) = f(ra) \in J$ Therefore, $ar \in I$ and $ra \in I$.

Problem 5. Let $\phi : \mathbb{Z}[x] \to \mathbb{Z}_3$ be defined by

$$\phi(a_0 + a_1 x + \cdots + a_n x^n) = [a_0]_3.$$

a. (10 pts) Prove that ϕ is a surjective ring homomorphism

Let $[a] \in \mathbb{Z}_3$. Then, for the constant polynomial $a \in \mathbb{Z}[x]$ we have that $\phi(a) = [a]_3$. Thus, ϕ is surjective. Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ and $g(x) = b_0 + b_1 x + \cdots b_n x^n$ be in $\mathbb{Z}[x]$. We can assume without loss of generality that $m = n$ by adding terms with 0 coefficient Then,

$$\begin{aligned}
\phi(f(x) + g(x)) &= \phi((a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n \\
&= [a_0] + [b_0] \\
&= \phi(f(x)) + \phi(g(x)) \\
\phi(f(x)g(x)) &= \phi\left(\sum_{k=0}^{n+n} c_k x^k\right) \qquad\qquad \text{where} \qquad c_k = \sum_{i=0}^{k} a_i b_{k-i} \\
&= [c_0] \\
&= [a_0 b_0] \\
&= [a_0][b_0] \\
&= \phi(f(x))\phi(g(x)).
\end{aligned}$$

Thus ϕ respects $+$ and $\cdot$. We conclude that ϕ is a surjective homomorphism.

b. (10 pts) Show that $\ker \phi = \langle 3, x \rangle$ is the ideal generated by 3 and x.

(Thus, by the First Isomorphism Theorem we have that $\mathbb{Z}[x]/\langle 3, x \rangle \cong \mathbb{Z}_3$.)

Recall that $\langle 3, x \rangle = \{3f(x) + xg(x) : f(x), g(x) \in \mathbb{Z}[x]\}$.

Let $f(x) \in \ker \phi$ and write $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Then, $\phi(f(x)) = [a_0] = [0]$. Thus, $3 | a_0$ and there exists $k \in \mathbb{Z}$ such that $a_0 = 3k$. It follows that

$$\begin{aligned}
f(x) &= a_0 + a_1 x + \cdots + a_n x^n \\
&= 3k + x(a_1 + a_2 x + \cdots + a_n x^{n-1}).
\end{aligned}$$

Thus, $f(x) \in \langle 3, x \rangle$.

Let $h(x) \in \langle 3, x \rangle$ and write $h(x) = 3f(x) + xg(x)$ for some $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ and $g(x) = b_0 + b_1 x + \cdots b_n x^n$ be in $\mathbb{Z}[x]$. It follows that

$$\begin{aligned}
\phi(h(x)) &= \phi(3f(x) + xg(x)) \\
&= \phi(3)\phi(f(x)) + \phi(x)\phi(g(x)) \\
&= [0]\phi(f(x)) + [0]\phi(g(x)) \\
&= [0],
\end{aligned}$$

where we use that $\phi(3) = [3] = [0]$ and $\phi(x) = [0]$. Therefore $h(x) = 3f(x) + xg(x) \in \ker \phi$.

We conclude that $\ker f = \langle 3, x \rangle$.

Extra Credit. (10 pts)

Let $n, p \in \mathbb{Z}$ be a positive, p be prime and $\langle p \rangle \subset \mathbb{Z}[x]$ denote the principal ideal generated by p. Suppose for $f(x), g(x), h(x), r(x), s(x) \in \mathbb{Z}[x]$ we have that

$$(f(x)r(x) + g(x)s(x)) + \langle p \rangle = 1 + \langle p \rangle$$

and

$$(f(x)g(x)) + \langle p \rangle = h(x) + \langle p \rangle.$$

Prove that there exist $F(x), G(x) \in \mathbb{Z}[x]$ such that the following hold

i. $F(x) + \langle p \rangle = f(x) + \langle p \rangle$,

ii. $G(x) + \langle p \rangle = g(x) + \langle p \rangle$,

iii. $F(x)G(x) + \langle p^n \rangle = h(x) + \langle p^n \rangle$.