Name SOLUTIONS

PID _____

Exam 1

MTH 310, Thursday June 7, 2018

Instructions: This exam is closed notes, closed books, no calculators and no electronic devices of any kind. There are four problems worth 25 points each and one extrac credit worth 15 points. 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	E	Total

Problem 1.

a. (15 points) Compute the remainder of 310^{2018} when divided by 3.

Notice that $310 = 3(103)+1$. It follows that $[310]_3 = [1]_3$. Thus, $[310]_3^{2018} = [1]_3^{2018} = [1]_3$.

b. (10 points) Find the multiplicative inverse of $[8]_{31}$ in $\mathbb{Z}_{31}$.

We can use the Euclidean algorithm to see that

$$31 = 8 \cdot 3 + 7$$
$$8 = 7 + 1.$$

Thus, $1 = 8 - 7 = 8 - (31 - 8 \cdot 3) = 8 \cdot 4 - 31$. It follows that $[8]_{31}[4]_{31} = [32]_{31} = [1]_{31}$. Thus, $[4]_{31} = [8]_{31}^{-1}$.

Problem 2.

a. (15 pts) Let $a, b \in \mathbb{Z}$ not both zero and let gcd of $(a, b) = d$. Prove that if $a = dm$ and $b = dn$ for some $m, n \in \mathbb{Z}$ then the gcd of $(m, n) = 1$.

Since the gcd of $(a, b) = d$ there exists $u, v \in \mathbb{Z}$ such that $au + bv = d$. By substitution,

$$\begin{aligned} d &= (dm)u + (dn)v \\ &= dmu + dmv \\ &= d(mu + nv). \end{aligned}$$

Cancellation implies that $1 = mu + nv$ is the smallest positive linear combination of m and n. Therefore, the gcd of $(m, n) = 1$.

b. (10 pts) Let $r = \dfrac{a}{b}$ for some $a, b \in \mathbb{Z} \setminus \{0\}$. Use part a. to show that $r = \dfrac{m}{n}$ for some $m, n \in \mathbb{Z}$ with gcd of $(m, n) = 1$.

Let gcd of $(a, b) = d$. Then, part a. we can write $a = dm$ and $a = bn$ where $m, n \in \mathbb{Z}$ and the gcd of $(m, n) = 1$. It follows that

$$r = \frac{a}{b} = \frac{dm}{dn} = \frac{m}{n} \qquad \text{where} \quad (m, n) = 1.$$

Problem 3. Let R and S be rings and $f : R \to S$ be a homomorphism of rings. Define the *kernel* of f as a subset of R by

$$\ker f := \{a \in R : f(a) = 0_S\} \subset R.$$

a. (10 pts) Prove that $\ker f$ is a subring of R.

Let $a, b \in \ker f$, so that $f(a) = 0_S$ and $f(b) = 0_S$. Since f is a homomorphism it respects addition and multiplication. It follows that

$$\begin{aligned} f(a+b) &= f(a) + f(b) \\ &= 0_S + 0_s = 0_s; \end{aligned}$$

and

$$\begin{aligned} f(a \cdot b) &= f(a) \cdot f(b) \\ &= 0_S \cdot 0_S = 0_S. \end{aligned}$$

Therefore, $a + b \in \ker f$ and $a \cdot b \in \ker f$, that is, f is closed under addition and multiplication.

From the basic ring homomorphism properties we know that $f(0_R) = 0_S$. Thus, $0_R \in \ker f$.

Consider $-a \in R$ the additive inverse of $a \in \ker f$. From the basic ring homomorphism properties we know that, $f(-a) = -f(a) = -0_S = 0_S$. Thus, $-a \in \ker f$.

By the subring theorem, we have shown that $\ker f$ is a subring of R.

b. (15 pts) Prove that f is an isomorphism if and only if f is surjective and $\ker f = \{0_R\}$.

($\implies$) Let f be an isomorphism. Then, f is a bijective homomorphism. Thus, f is surjective. From the basic ring homomorphism properties we know that $f(0_R) = 0_S$. Thus, $0_R \in \ker f$.

If $a \in \ker f$, then $f(a) = 0_S$. Thus, $f(a) = f(0_R)$. By injectivity, $a = 0_R$. Therefore, $\ker f = \{0_R\}$.

($\impliedby$) Let f be a surjective and assume $\ker f = \{0_R\}$. By assumption f is a surjective homomorphism, so we are left to show f is injective. Suppose $f(a) = f(b)$. Then by cancellation,

$$\begin{aligned} f(a) &= 0_S + f(b) \\ f(a) - f(b) &= 0_S \\ f(a-b) &= 0_S. \end{aligned}$$

Therefore, $a - b \in \ker f$. By assumption $\ker f = \{0_R\}$ is the set of just the zero element, thus $a - b = 0_R$ which implies $a = 0_R + b = b$. Therefore, f is injective.

Problem 4. Let $f : \mathbb{Z}_3 \to \mathbb{Z}_8$ be a ring homomorphism.

a. (5 pts) Let $[a]_8 \in \mathbb{Z}_8$. Show that if $[a]_8 + [a]_8 + [a]_8 = [0]_8$ then $[a]_8 = [0]_8$.

From the assumptions it follows that

$$\begin{aligned}[0]_8 &= [a]_8 + [a]_8 + [a]_8 \\ &= [a + a + a]_8 \\ &= [3a]_8 \\ &= [3]_8[a]_8.\end{aligned}$$

Since the gcd of $(3, 8) = 1$ this implie sthat $[3]_8$ is a unit in $\mathbb{Z}_8$. Multiplying by $[3]_8^{-1}$ we get

$$\begin{aligned}[3]_8^{-1}[0]_8 &= [3]_8^{-1}[3]_8[a]_8 \\ [0]_8 &= [1]_8[a]_8 \\ &= [a]_8.\end{aligned}$$

We conclude that $[a]_8 = [0]_8$.

b. (10 pts) Use part a. to prove that $f([1]_3) = [0]_8$.

Let $[a]_8 = f([1]_3) \in \mathbb{Z}_8$. Since $[1]_3 + [1]_3 + [1]_3 = [3]_3 = [0]_3$ and since f respects addition, it follows that

$$\begin{aligned}[0]_8 &= f([0]_3) \qquad (\text{ ring homomorphism property}) \\ &= f([1]_3 + [1]_3 + [1]_3) \\ &= f([1]_3) + f([1]_3) + f([1]_3) \\ &= [a]_8 + [a]_8 + [a]_8.\end{aligned}$$

Applying part a. we conclude that $[0]_8 = [a]_8 = f([1]_3)$.

c. (10 pts) Use part b. to conclude that f must be the zero homomorphism, that is,

$$f(\ [b]_3\ ) = [0]_8 \qquad \text{for all} \quad [b] \in \mathbb{Z}_3.$$

(*Hint:* Write $[b]_3 = [b \cdot 1]_3 = [b]_3 \cdot [1]_3$.)

Let $[b]_3 \in \mathbb{Z}_3$. Applying the hint and part b. we have that

$$\begin{aligned}f([b]_3) &= f([b]_3[1]_3) \\ &= f([b]_3)f([1]_3) \\ &= f([b]_3)[0]_8 \\ &= [0]_8,\end{aligned}$$

where in the second equality we used that f respects multiplication. Therefore, $f([b]_3) = [0]_8$ for all $[b]_3 \in \mathbb{Z}_3$. We conclude that f is the zero homomorphism.

Extra Credit. (15 pts) Let p be prime and consider $\mathbb{Z}_p$. Define the set

$$S := \{(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p : a^2 = b^2 + 1 \text{ in } \mathbb{Z}_p\}.$$

Find the cardinality of the set S.

First consider the case $p > 2$. If $a^2 = b^2 + 1$ then $a^2 - b^2 = 1$ and thus $(a+b)(a-b) = 1$. Consider the change of variables $x = a + b$ and $y = a - b$. This change of variables is indeed bijective since it can be implemented as the linear transformation $T : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_p$ where $T = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a+b \\ a-b \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}.$$

If $p > 2$ then $\det T = -2 \neq 0$ in $\mathbb{Z}_p$ and we conclude that T is invertible and therefore bijective.

Thus, we count the number of solutions to $xy = 1$ in $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is a field every nonzero element x is a unit. By uniqueness of inverses, the pairs (x, x^{-1}) for $x \neq 0$ are the only solutions. Thus, there are exactly $p - 1$ solutions. We conclude that $|S| = p - 1$.

If $p = 2$ then $\mathbb{Z}_2 \times \mathbb{Z}_2$ has four elements. We can check each one by one to see if they are in S. In this case, we have that $S = \{(0, 1), (1, 0)\}$.