Exploring Equivalence Relations v 1.0

Dr. Chuck Rocca

Contents

1 Introduction and Directions

In this packet you will review/explore the concepts of equivalence relations and classes. In particular you will see how, using equivalence classes, we can create new structures from old ones. You will also spend time practicing some hopefully familiar skills including modular arithmetic, polynomial arithmetic, proof reading, and proof writing.

You should *write* answer to the questions for this packet directly in the space provided. Your work must be neat and legible, so, if you need to, complete it on scrap paper first, and then write it in the packet. The material in the first two sections should be somewhat familiar. The third section is very new but will help you to see how well you understand the concept of equivalence relations and classes.

2 Integers Modulo n

Some Definitions

Definition 1 (Divisibility)**.** We say that an integer **b *divides an integer* a**, written $b|a$, if and only if there exists a unique integer q, called the quotient, such that $a = qb$.

Exercises 1. For each pair decide if b divides a, $b|a$, or b doesn't divide a, $b\not| \, a$:

1. $5|60$ since $60 = 12(5)$ ✓
2. $5 \not| \, 63$ since $12(5) < 63 < 13(5)$ ✗
3. 4 ____ 7 since ________________
4. 4 ____ 16 since ________________
5. -3 ____ 24 since ________________
6. 5 ____ -17 since ________________
7. 12 ____ 4 since ________________
8. -2 ____ 20 since ________________

Definition 2 (Integers Mod n)**.** Given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$ we say that **a *is equivalent to* b *modulo* n**, written $a \equiv b \pmod{n}$, if and only if $n|(a - b)$.

Exercises 2. For the given $a, b, n \in \mathbb{Z}$ decide if $a \equiv b \pmod{n}$:

1. $12 \equiv 33 \pmod{7}$ since $7|(12 - 33)$ ✓
2. $45 \not\equiv 13 \pmod{7}$ since $7 \not| \, (45 - 13)$ ✗
3. 4 ____ $7 \pmod{5}$ since ________________
4. 4 ____ $7 \pmod{3}$ since ________________
5. 4 ____ $19 \pmod{5}$ since ________________
6. 73 ____ $25 \pmod{12}$ since ________________
7. 17 ____ $54 \pmod{7}$ since ________________
8. 75 ____ $9 \pmod{6}$ since ________________

For this packet, we will take the following theorem (the ***Division Algorithm***) and its immediate corollary as given. These give a way of talking more generally about what happens when one integer divides another.

Theorem 1 (Division Algorithm)**.** *Given $a, b \in \mathbb{Z}$ with $b \neq 0$ there exists unique integers q and r, called the quotient and remainder, such that $a = qb + r$ and $0 \leq r < |b|$.*

Corollary. *Given $a, n \in \mathbb{Z}$ with $n > 0$, we can write $a - r = qn$ or $a \equiv r \pmod{n}$ for a unique $0 \leq r < n$.*

Exercises 3. For the given $a, n \in \mathbb{Z}$, $n > 0$, find r such that $a \equiv r \pmod{n}$ and $0 \leq r < n$:

1. Given $a = 27$ and $n = 11$,

   $r = 5 = 27 - 2(11)$ ✓

2. Given $a = -13$ and $n = 11$,

   $r = 8 = -13 + 2(11)$ ✓

3. Given $a = 47$ and $n = 5$,

   ____

4. Given $a = 33$ and $n = 9$,

   ____

5. Given $a = 14$ and $n = 3$,

   ____

6. Given $a = -37$ and $n = 13$,

   ____

7. Given $a = -2$ and $n = 7$,

   ____

8. Given $a = 24$ and $n = 5$,

   ____

Reflexive

Definition 3 (Reflexive)**.** A relation between a set and its self, $A \sim A$, is ***reflexive*** if and only if for all $a \in A$, $a \sim a$.

Lemma 2. *The modular congruence from definition 2 is a reflexive relation.*

Proof. Let $a, n \in \mathbb{Z}$ and assume that $n > 0$. Note that

$$n(0) = 0 = a - a$$

so that $n | a - a$. **(1)** Therefore, $a \equiv a \pmod{n}$**(2)** and modular congruence is reflexive. □

Justify each of the labeled details in the above proof.

(1)

(2)

Symmetric

Definition 4 (Symmetric)**.** A relation between a set and its self, $A \sim A$, is ***symmetric*** if and only if for all $a, b \in A$, $a \sim b$ implies $b \sim a$.

Lemma 3. *The modular congruence from definition 2 is a symmetric relation.*

Proof. Let $a, b, n \in \mathbb{Z}$, assume that $n > 0$ and $a \equiv b \pmod{n}$. We know then that $n|(a-b)$, **(3)** $a - b = qn$,**(4)** and $b - a = -qn$. **(5)** Therefore, $b \equiv a \pmod{n}$**(6)** and, thus, modular congruence is symmetric. □

Justify each of the labeled details in the above proof.

(3)

(4)

(5)

(6)

Transitive

Definition 5 (Transitive)**.** A relation between a set and its self, $A \sim A$, is ***transitive*** if and only if for all $a, b, c \in A$, $a \sim b$ and $b \sim c$ implies $a \sim c$.

Lemma 4. *The modular congruence from definition 2 is a transitive relation.*

Proof. Let $a, b, c, n \in \mathbb{Z}$, assume that $n > 0$, $a \equiv b \pmod{n}$, and $b \equiv c \pmod{n}$. Then we may write

$$\begin{aligned} a - c &= (a - b) + (b - c)^{(7)} \\ &= q_0 n + q_1 n^{(8)} \\ &= (q_0 + q_1)n \end{aligned}$$

for some unique q_0 and q_1. This means $n|(a - c)^{(9)}$ and $a \equiv c \pmod{n}$. **(10)** Therefore we have that modular congruence is transitive. □

Justify each of the labeled details in the above proof.

(7)

(8)

(9)

(10)

Equivalence Relations and Classes

Definition 6 (Equivalence Relation)**.** A relation between a set and its self, $A \sim A$, is an ***equivalence relation*** if and only if it is reflexive, symmetric, and transitive.

From the lemmas 2, 3, & 4 we conclude that ***modular congruence is an equivalence relation***.

Definition 7 (Equivalence Classes)**.** Given an equivalence relation between a set and its self, $A \sim A$, and given $a \in A$, the ***equivalnce class of a*** is the set

$$[a] = \{x \in A | x \sim a\}.$$

Theorem 1 together with corollary 2 ensures that given a positive integer n every integer a is equivalent to a unique remainder $0 \leq r < n$. These remainders will be our ***equivalence class representatives***, i.e. for all $a \in \mathbb{Z}$ we have $a \in [r]$ for some remainder r.

Exercises 4. For each pair a and n give the appropriate equivalence class representative r for $a \pmod{n}$.

1. Given $a = 18$ and $n = 7$

   $r = 4 = 18 - 2(7)$”

2. Given $a = 37$ and $n = 5$

   $r = 2 = 37 - 7(5)$”

3. Given $a = -10$ and $n = 13$

   $r =$ ________________

4. Given $a = -17$ and $n = 10$

   $r =$ ________________

5. Given $a = 32$ and $n = 3$

   $r =$ ________________

6. Given $a = -42$ and $n = 42$

   $r =$ ________________

7. Given $a = 11$ and $n = 9$

   $r =$ ________________

8. Given $a = -8$ and $n = 11$

   $r =$ ________________

Operations

Definition 8 (Closed & Binary Operation)**.** A set A is said to be ***closed*** under a ***binary operation*** $*$ if and only if $*$ is a function from $A \times A$ to A. Normally we would write this as

$$\forall a, b \in A : a * b \in A.$$

Exercises 5. For each set and each function decide if we have a closed binary operation.

1. Set $A = \mathbb{Z}$ and operation $(a, b) \mapsto a + b$:

   The sum of two integers is an integer; this is a closed binary operation. ✓

2. Set $A = \mathbb{Z}$ and operation $a \mapsto 2a$:

   This is not a binary operation; there is only one input. ✗

3. Set $A = \mathbb{N}$ and operation $(a, b) \mapsto a - b$:

   Since $1 - 2 = -1 \notin \mathbb{N}$, this is not closed. ✗

4. Set $A = \mathbb{Z}$ and operation $(a, b) \mapsto a \times b$:

   The product of two integers is an integer; this is a closed binary operation. ✓

5. Set $A = \mathbb{Z}$ and operation $(a, b) \mapsto a \div b$:

6. Set $A = \mathbb{Z}$ and operation $(a, b) \mapsto a^b$:

7. Set $A = \mathbb{N}$ and operation $(a, b) \mapsto a^b$:

8. Set $A = \mathbb{Q}$ and operation $(a, b) \mapsto a/(b^2 + 1)$:

Definition 9 (Operation Respecting)**.** We say that a relation, $\sim$, ***respects a binary operation***, $*$, if and only if $(a \sim b)$ and $(c \sim d)$ implies $(a * c \sim b * d)$.

Theorem 5 (Modular Arithmetic)**.** *The modular congruence relation from definition 2 respects the operations of addition, subtraction, and multiplication, i.e. given* $a, b, c, d, n \in \mathbb{Z}$ *with* $n > 0$ *if* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$*, then*

- $a + c \equiv b + d \pmod{n}$
- $a - c \equiv b - d \pmod{n}$
- $a \times c \equiv b \times d \pmod{n}$

Proof. Fill in the details in the following two-column proof.

Claim	Justification
$a, b, c, d, n \in \mathbb{Z},\ n > 0$	
$a \equiv b \pmod{n},\ c \equiv d \pmod{n}$	
$a - b = q_0 n,\ c - d = q_1 n$	
$(a \pm c) - (b \pm d) = (a - b) \pm (c - d)$	
$(a - b) \pm (c - d) = q_0 n \pm q_1 n = (q_0 \pm q_1)n$	
$\therefore (a \pm c) \equiv (b \pm d) \pmod{n}$	
$(ac) - (bd) = (ac - bc + bc - bd)$	
$(ac - bc + bc - bd) = c(a - b) + b(c - d)$	
$c(a - b) + b(c - d) = Qn$	
$\therefore (a \times c) \equiv (b \times d) \pmod{n}$	

□

Rewrite the proof as a paragraph proof using proper conventions for English and for mathematical writing.

(Take Two). Assume that $a, b, c, d, n \in \mathbb{Z}$, $n > 0$, $a \equiv b \pmod{n}$, and $c \equiv d \pmod{n}$.

□

Therefore modular congruence (definition 2) is an equivalence relation (lemmas 2, 3, and 4) and respects the usual binary operations under which integers are closed (theorem 5).

3 Division and Polynomials

Familiar But New Definitions

Definition 10 (Polynomials over the Rationals)**.** A ***polynomial over the rationals*** is an expression of the form

$$\sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_i x^i + \cdots + a_n x^n$$

where x is an arbitrary symbol, $rx = xr$ for all $r \in \mathbb{Q}$, and for all i, $i \in \mathbb{N}$ and $a_i \in \mathbb{Q}$. The set of all such polynomials is denoted $\mathbb{Q}[x]$.

Definition 11 (Degree of a Polynomial)**.** Given a polynomial $f(x) \in \mathbb{Q}[x]$, the ***degree of the polynomial*** is the highest power of x in $f(x)$ when $f(x)$ is non-zero. If $f(x) = a_0 \in \mathbb{Q}$ we say the degree is 0 and if $f(x) = 0$, then we say $f(x)$ has no degree. The degree of a polynomial is written $deg(f)$.

Note that for a given polynomial $f(x) \in \mathbb{Q}[x]$

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_i x^i + \cdots + a_n x^n$$

the the a_i are ***coefficients***, a_n, when $deg(f) = n$, is the ***leading coefficient***, and a_0 is the ***constant term***.

Exercises 6. For each polynomial, identify if it is in $\mathbb{Q}[x]$ and if it is find its constant term, degree, and leading coefficient.

Polynomial	In $\mathbb{Q}[x]$?	a_0	$deg(f)$	a_n
$17x^2 + 3x + 9$	✓	9	2	17
$\pi x^5 - 3x^{17} - 32$	✗	N/A	N/A	N/A
$-25x^5 - x^4 - 13x - 2$				
$17x^{-3} + x^5 + 5x$				
$5x^5 - x^{42} + \sqrt{2}x^2 - 4$				
$13 + x - 12x^2 - 47x^9$				
$5x^5 - x^{42} + 17x^2 - 4$				
$72 - 3x + 12x^{-3} - 5x^7$				

As with integers we can define concepts of ***divisibility*** and ***division*** for polynomials.

Definition 12 (Divisibility)**.** We say that a polynomial **b(x)** ***divides a polynomial*** **a(x)**, written $b(x)|a(x)$, if and only if there exists a unique polynomial $q(x)$, called the quotient, such that $a(x) = q(x)b(x)$.

Theorem 6 (Division Algorithm)**.** *Given* $a(x), b(x) \in \mathbb{Q}[x]$ *with* $b(x) \neq 0$ *there exists unique polynomials* $q(x)$ *and* $r(x)$*, called the quotient and remainder, such that* $a(x) = q(x)b(x) + r(x)$ *and* $r(x) = 0$ *or* $0 \leq deg(r) < deg(b)$*.*

Exercises 7. For each pair $a(x), b(x) \in \mathbb{Q}[x]$ identify $q(x)$ and $r(x)$ as in theorem 6 such that

$$a(x) = q(x)b(x) + r(x)$$

and indicate if $b(x)|a(x)$ as in definition 12.

1. Given $a(x) = x^2 + 3x + 2$ and $b(x) = x - 1$

$$a(x) = (x + 4)b(x) + 6$$

and $b(x) \not| \, a(x)$.

2. Given $a(x) = x^2 + 3x + 2$ and $b(x) = x + 1$

$$a(x) = (x + 2)b(x) + 0$$

and $b(x)|a(x)$.

3. Given $a(x) = 25x^2 + 2x + 5$ and $b(x) = 5x + 1$

4. Given $a(x) = x^2 - 5x + 7$ and $b(x) = x^2 + 1$

5. Given $a(x) = x^3 - 7x + 6$ and $b(x) = 2x + 1$

6. Given $a(x) = x^3 - 4x^2 + 5x - 2$ and $b(x) = x - 2$

Corollary (Remainder Theorem)**.** *Given $f(x) \in \mathbb{Q}[x]$ and $a \in \mathbb{Q}$, if $f(x) = (x-a)q(x) + r$, then $f(a) = r \in \mathbb{Q}$.*

Corollary (Factor Theorem)**.** *Given $f(x) \in \mathbb{Q}[x]$ and $a \in \mathbb{Q}$, $f(a) = 0$ if and only if $f(x) = (x-a)g(x)$ and $g(x) \in \mathbb{Q}[x]$.*

An Equivalence Relation

Definition 13 (Polynomials Mod $n(x)$)**.** Given $a(x), b(x), n(x) \in \mathbb{Q}[x]$ with $deg(n) \geq 0$, we say that **a(x)** ***is equivalent to*** **b(x)** ***modulo*** **n(x)**, written $a(x) \equiv b(x) \pmod{n(x)}$, if and only if $n(x)|(a(x) - b(x))$.

Theorem 7. *Polynomial modular equivalence is an equivalence relation.*

Proof. Let $a(x), b(x), c(x), n(x) \in \mathbb{Q}[x]$ with $deg(n) \geq 0$. Since

$$(n(x))0 = 0 = a(x) - a(x),$$

the relation is reflexive. **(11)** Next, assuming $a(x) \equiv b(x) \pmod{n(x)}$,

$$a(x) - b(x) = q(x)n(x)$$

and

$$b(x) - a(x) = -q(x)n(x)$$

for some $q(x) \in \mathbb{Q}[x]$, therefore the relation is symmetric. **(12)** Finally, if we additionally assume $b(x) \equiv c(x) \pmod{n(x)}$, then

$$a(x) - c(x) = a(x) - b(x) + b(x) - c(x) = \overline{q}(x)n(x)$$

for some $\overline{q}(x) \in \mathbb{Q}[x]$**(13)** and $a(x) \equiv c(x) \pmod{n(x)}$; the relation is transitive. **(14)** □

Exercises 8. Fill in justifications for each of the numbered items in the previous proof.

(11)

(12)

(13)

(14)

As with integers, we can define a standard set of equivalence class representatives by using the remainders defined by the ***Division Algorithm for Polynomials*** (theorem 6).

Exercises 9. Find the equivalence class representative for each $a(x)$ below using $n(x) = x^2 + 1$.

1. Given $a(x) = x^3 + 2$ we find that $r(x) = 2 - x$. ✔

2. Given $a(x) = x^3 - x^2 + x + 6$ we find that $r(x) = 7$. ✔

3. Given $a(x) = x^2 + x - 8$ we find that $r(x) = x - 9$. ✔

4. Given $a(x) = x^4 + 2x^2$ we find that $r(x) =$

5. Given $a(x) = x^5 - 7$ we find that $r(x) =$

6. Given $a(x) = x^2 + 2$ we find that $r(x) =$

7. Given $a(x) = x^4 + 3x^2 + 2$ we find that $r(x) =$

Operations

Theorem 8 (Arithmetic Mod $n(x)$)**.** *Polynomial modular equivalence (definition 13) respects the operations of polynomial addition, subtraction, and multiplication.*

Following theorem 5, write a two-column proof of theorem 8, then translate it to a paragraph proof.

(Two-column proof).

Claim Justification

□

(Paragraph Proof). Assume $a, b, c, d, n \in \mathbb{Q}[x]$, $deg(n) \geq 0$, $a(x) \equiv b(x) \pmod{n(x)}$, and $c(x) \equiv d(x) \pmod{n}$.

□

4 A Trick with Natural Numbers

A New Relation

Definition 14. Given $(a,b),(c,d) \in \mathbb{N} \times \mathbb{N}$ we will say that $(a,b) \sim (c,d)$ if and only if $a + d = c + b$ in $\mathbb{N}$.

Example 1. Consider the following examples:

1. $(2,3) \sim (5,6)$ since $2 + 6 = 5 + 3$ ✓
2. $(17,10) \sim (8,1)$ since $17 + 1 = 8 + 10$ ✓
3. $(5,5) \sim (1,1)$ since $5 + 1 = 1 + 5$ ✓
4. $(7,4) \not\sim (4,7)$ since $7 + 7 \neq 4 + 4$ ✗
5. $(7,2) \sim (12,7)$ since $7 + 7 = 12 + 2$ ✓
6. $(3,2) \not\sim (9,10)$ since $3 + 10 \neq 9 + 1$ ✗

Exercises 10. Identify which pairs relate, $(a,b) \sim (c,d)$, and which do not, $(a,b) \not\sim (c,d)$:

1. $(4,5)$ ____ $(17,18)$ since ________________
2. $(7,3)$ ____ $(12,16)$ since ________________
3. $(7,1)$ ____ $(9,3)$ since ________________
4. $(2,7)$ ____ $(1,6)$ since ________________
5. $(3,4)$ ____ $(9,8)$ since ________________
6. $(3,3)$ ____ $(7,7)$ since ________________

Remark (Comment on Subtraction). Given $(a,b),(c,d) \in \mathbb{N} \times \mathbb{N}$ if $(a,b) \sim (c,d)$, then by definition 14

$$a + d = c + d,$$

but this is equivalent to

$$a - b = c - d, \tag{1}$$

however we don't usually use this because ***subtraction isn't well defined for*** $\mathbb{N}$. (15) In what follows it will sometimes be helpful to use equation 1 even though it is not well defined in $\mathbb{N}$. Whenever possible you should seek to avoid this. (Note: Theorem 11 is really the only place this is needed.)

Exercises 11. Why is it the case that "subtraction isn't well defined for $\mathbb{N}$," as stated in the previous remark?

Lemma 9. *Given $n, k \in \mathbb{N}$ the following pairs are always related:*

1. $(n + k, n) \sim (k + 1, 1)$,
2. $(n, n + k) \sim (1, k + 1)$, *and*
3. $(n, n) \sim (1, 1)$.

Proof. Let $n, k \in \mathbb{N}$ be arbitrary. Then

□

An Equivalence Relation

Theorem 10. *The relation defined on $\mathbb{N} \times \mathbb{N}$ in definition 14 is an equivalence relation.*

Proof. We can show that the theorem is true by showing the relation is reflexive, symmetric and transitive.

- ***Reflexive:***

- ***Symmetric:***

- ***Transitive:***

□

Definition 15. Using the relation defined in definition 14, let

$$(\mathbb{N} \times \mathbb{N}) / \sim = \{[(a, b)] | (a, b) \in \mathbb{N} \times \mathbb{N}\}$$

be the set of all equivalence classes of ordered pairs; i.e.

$$[(a, b)] = \{(c, d) | (c, d) \sim (a, b)\}.$$

Operations

Definition 16 (Addition)**.** Given $(a,b),(c,d)\in\mathbb{N}\times\mathbb{N}$ define addition by

$$(a,b)+(c,d)=(a+c,b+d).$$

Exercises 12. Sum the pairs using the rule $(a,b)+(c,d)=(a+c,b+d)$ and then reduce them to the form $(1,n)$, $(n,1)$, or $(1,1)$ (see lemma 9 above):

1. $(4,5)+(7,8) = \mathbf{(11,13)\sim(1,3)}$
2. $(3,3)+(11,9) = \mathbf{(14,12)\sim(3,1)}$
3. $(7,1)+(5,5)$ ________
4. $(9,9)+(3,1)$ ________
5. $(10,5)+(5,10)$ ________
6. $(1,6)+(6,1)$ ________
7. $(3,1)+(9,10)$ ________
8. $(8,8)+(10,9)$ ________

Definition 17 (Multiplication)**.** Given $(a,b),(c,d)\in\mathbb{N}\times\mathbb{N}$ define multiplication by

$$(a,b)\times(c,d)=(ac+bd,ad+bc).$$

Exercises 13. Multiply the pairs using the rule $(a,b)\times(c,d)=(ac+bd,ad+bc)$ and then reduce them to the form $(1,n)$, $(n,1)$, or $(1,1)$ (see lemma 9 above):

1. $(1,2)\times(3,7) = \mathbf{(17,13)\sim(5,1)}$
2. $(2,1)\times(4,2) = \mathbf{(10,8)\sim(3,1)}$
3. $(1,1)\times(1,8)$ ________
4. $(5,4)\times(4,5)$ ________
5. $(7,1)\times(5,6)$ ________
6. $(7,1)\times(6,5)$ ________
7. $(3,1)\times(3,1)$ ________
8. $(5,7)\times(5,7)$ ________

Theorem 11 (Respecting Operations)**.** *Let* $(a,b),(c,d),(a_1,b_1),(c_1,d_1)\in\mathbb{N}\times\mathbb{N}$ *and assume*

$$(a,b)\sim(a_1,b_1) \textit{ and } (c,d)\sim(c_1,d_1),$$

then with addition and multiplication defined as in definitions 16 and 17,

$$(a,b)+(c,d)\sim(a_1,b_1)+(c_1,d_1)$$

and

$$(a,b)\times(c,d)\sim(a_1,b_1)\times(c_1,d_1).$$

Proof. Let $(a,b),(c,d),(a_1,b_1),(c_1,d_1)\in\mathbb{N}\times\mathbb{N}$ and assume

$$(a,b)\sim(a_1,b_1) \textit{ and } (c,d)\sim(c_1,d_1).$$

This means that

□

Lemma 12. *Using the relation in definition 14 and the operations from definitions 16 and 17, for all $a, b \in \mathbb{N}$ we have that*

1. $((a,b)+(1,1)) \sim (a,b)$, *(Additive Identity)*
2. $((a,b)+(b,a)) \sim (1,1)$, *(Additive Inverse)*
3. $((a,b)\times(1,1)) \sim (1,1)$, *(Zero)*
4. $((a,b)\times(2,1)) \sim (a,b)$, *(Multiplicative Identity) and*
5. $((a,b)\times(1,2)) \sim (b,a)$. *(Negatives)*

Proof. Let $a, b, n \in \mathbb{N}$.

1. Simplifying $(a,b)+(n,n)$ we get

   and so (n,n) is the additive identity.
2. Simplifying $(a,b)+(b,a)$ we get

   and so (a,b) and (b,a) additive inverses.
3. Simplifying $(a,b)\times(n,n)$ we get

   and so (n,n) acts like zero.
4. Simplifying $(a,b)\times(n+1,n)$ we get

   and so $(n+1,1)$ is the multiplicative identity.
5. Simplifying $(a,b)\times(n,n+1)$ we get

   and so $(1,n+1)$ acts like negative one.

□

Corollary. *The set $\mathbb{N} \times \mathbb{N}$ together with the relation in definition 14 and the operations from definitions 16 and 17 is equivalent to the ring of integers, $\mathbb{Z}$.*

Define a map

$$\phi : (\mathbb{N} \times \mathbb{N}) / \sim \longrightarrow \mathbb{Z} :$$

in order to justify corollary 4. You will want to look carefully at the results in Lemma 12 to help decide how to define ϕ.

- $\phi((1,1)) =$__________________

- $\phi((2,1)) =$__________________

- $\phi((1,2)) =$__________________

- $\phi((7,3)) =$__________________

- $\phi((n,n)) =$__________________

- $\phi((n,1)) =$__________________

- $\phi((1,n)) =$__________________

- $\phi((m,n)) =$__________________