

**Problem 1:** Please prove that the sets  $E = \{\text{even integers}\}$ ,  $\mathbb{N}$ , and  $\mathbb{Z}$  are infinite sets and that they have the same cardinality.

*Claim 1:* The sets  $E$ ,  $\mathbb{N}$ , and  $\mathbb{Z}$  are infinite sets that have the same cardinality.

*Proof 1:* The claim is composed of several atomic statements: The first three claim that  $E$ ,  $\mathbb{N}$ , and  $\mathbb{Z}$  are infinite sets and the fourth claims that they have the same cardinality. These statements will be verified independently.

*Subclaim 1-1a:* The set  $E$  is an infinite set.

*Subproof 1-1a:* The set  $E$  is an infinite set if there exists a bijection from a proper subset of  $E$  to  $E$ . Let the set  $B$  be a subset of  $E$  such that  $B = \{b \in E : 4 \mid b\}$ . Additionally, let  $f : E \rightarrow B$  such that  $f(e) = 2 \cdot e \forall e \in E$ . In this proof, we will show that the function  $f$  is a bijection between  $E$  and  $B$ , and thus that  $E$  is infinite.

For a function to be bijective, it must be both surjective and injective. For the function  $f$  to be surjective,  $\forall b \in B, \exists e \in E \ni f(e) = b$ . If  $b \in B$ , then we know that  $b$  is divisible by 4 such that  $\exists c \in \mathbb{Z} \ni 4 \cdot c = b$  but 4 is also divisible by 2, implying that  $2(2 \cdot c) = b$ . Note that  $2 \cdot c \in E$ , which implies that  $\exists e \in E \ni 2 \cdot e = b$ , and hence that  $\exists e \in E \ni f(e) = b$ , making  $f$  surjective.

For a function to be injective,  $f(a) = f(b)$  must imply that  $a = b$ . Let  $e_1, e_2 \in E$ . This implies that  $f(e_1) = f(e_2) \Rightarrow 2e_1 = 2e_2$  and consequently that  $2e_1 - 2e_2 = 0$  and  $2(e_1 - e_2) = 0$ . But then  $-e_2$  must be the additive inverse of  $e_1$ , making  $e_1 = e_2$ . Therefore,  $f(a) = f(b) \Rightarrow a = b$ , making  $f$  injective. Because  $f$  is both injective and surjective, it is also bijective. Therefore, because  $B$  is a proper subset of  $E$  and  $f$  a bijection between  $B$  and  $E$  the cardinality of set  $E$  is infinite.

*Subclaim 1-1b:* The set  $\mathbb{N}$  is an infinite set.

*Subproof 1-1b:* The set  $\mathbb{N}$  is an infinite set if there exists a bijection from a proper subset of  $\mathbb{N}$  to  $\mathbb{N}$ . Let the set  $B$  be a subset of  $\mathbb{N}$  such that  $B = \{b \in \mathbb{N} : 2 \mid b\}$ . Additionally, let  $f : \mathbb{N} \rightarrow B$  such that  $f(n) = 2 \cdot n \forall n \in \mathbb{N}$ . In this proof, we will show that the function  $f$  is a bijection between  $\mathbb{N}$  and  $B$ , and thus that the cardinality of  $\mathbb{N}$  is infinite.

For a function to be bijective, it must be both surjective and injective. For the function  $f$  to be surjective,  $\forall b \in B, \exists n \in \mathbb{N} \ni f(n) = b$ . If  $b \in B$ , then we know that  $b$  is divisible by 2 such that  $\exists c \in \mathbb{Z} \ni 2 \cdot c = b$ . Note that  $c \in \mathbb{N}$ , implying that  $\exists n \in \mathbb{N} \ni 2 \cdot n = b$ , and hence that  $\exists n \in \mathbb{N} \ni f(n) = b$ , making  $f$  surjective.

For a function to be injective,  $f(a) = f(b)$  must imply that  $a = b$ . Let  $n_1, n_2 \in \mathbb{N}$ . This implies that  $f(n_1) = f(n_2) \Rightarrow 2n_1 = 2n_2$  and consequently that  $2n_1 - 2n_2 = 0$  and  $2(n_1 - n_2) = 0$ . But then  $-n_2$  must be the additive inverse of  $n_1$ , making  $n_1 = n_2$ . Therefore,  $f(a) = f(b) \Rightarrow a = b$ , making  $f$  injective. Because  $f$  is both injective and surjective, it is also bijective. Therefore, because  $B$  is a proper subset of  $\mathbb{N}$  and  $f$  is a bijection between  $B$  and  $\mathbb{N}$ , the cardinality of  $\mathbb{N}$  is infinite.

*Subclaim 1-1c:* The set  $\mathbb{Z}$  is an infinite set.

*Subproof 1-1c:* The set  $\mathbb{Z}$  is an infinite set if there exists a bijection from a proper subset of  $\mathbb{Z}$  to  $\mathbb{Z}$ . Let the set  $B$  be a subset of  $\mathbb{Z}$  such that  $B = \{b \in \mathbb{Z} : 2 \mid b\}$ . Additionally, let  $f : \mathbb{Z} \rightarrow B$  such that  $f(z) = 2 \cdot z \forall z \in \mathbb{Z}$ . In this proof, we will show that the function  $f$  is a bijection between  $\mathbb{Z}$  and  $B$ , and thus that  $\mathbb{Z}$  is infinite.

For a function to be bijective, it must be both surjective and injective. For the function  $f$  to be surjective,  $\forall b \in B, \exists z \in \mathbb{Z} \ni f(z) = b$ . If  $b \in B$ , then we know that  $b$  is divisible by 2 such that  $\exists c \in \mathbb{Z} \ni 2 \cdot c = b$ , implying that  $\exists n \in \mathbb{N} \ni f(n) = b$ , making  $f$  surjective.

For a function to be injective,  $f(a) = f(b)$  must imply that  $a = b$ . Let  $z_1, z_2 \in \mathbb{Z}$ . This implies that  $f(z_1) = f(z_2) \Rightarrow 2z_1 = 2z_2$  and consequently that  $2z_1 - 2z_2 = 0$  and  $2(z_1 - z_2) = 0$ . But then  $-z_2$  must be the additive inverse of  $z_1$ , making  $z_1 = z_2$ . Therefore,  $f(a) = f(b) \Rightarrow a = b$ , making  $f$  injective. Because  $f$  is both injective and surjective, it is also bijective. Therefore, because  $B$  is a subset of  $\mathbb{Z}$ , and  $f$  is a bijection between  $B$  and  $\mathbb{Z}$ , the cardinality of  $\mathbb{Z}$  is infinite.

*Lemma 1-2:* Let  $A, B, C \in \{\text{Sets}\}$ . Before we can prove that the sets  $E$ ,  $\mathbb{N}$ , and  $\mathbb{Z}$  have the same cardinality, we must first prove that if the cardinality of set  $A$  is equal to the cardinality of  $B$ , and the cardinality of  $B$  is equal to the cardinality of  $C$ , then the cardinality of  $A$  is equal to the cardinality of  $C$ .

Because the cardinality of  $A$  is equal to the cardinality of  $B$ , there is a bijection between  $A$  and  $B$  such that

$f : A \xrightarrow[\text{onto}]{1:1} B$ . By the same logic, there is also a bijection between  $B$  and  $C$  such that  $g : B \xrightarrow[\text{onto}]{1:1} C$ . Define a separate function  $h : A \rightarrow C$  where  $h(a) = g(f(a))$ . We will show that  $h$  is a bijection from  $A$  to  $C$  and in doing so, that the cardinality of  $A$  and the cardinality of  $C$  are equal.

First, we show that  $h$  is surjective, or that  $\forall a \in A, \exists c \in C \ni h(a) = c$ . We know that  $\forall b \in B, \exists a \in A \ni f(a) = b$  because  $f$  is a bijection between  $A$  and  $B$ . We also know that  $\forall c \in C, \exists b \in B \ni g(b) = c$ . Therefore,  $\forall c \in C, \exists a \in A \ni g(f(a)) = c$ , implying that  $\forall c \in C, \exists a \in A \ni h(a) = c$  and making  $h$  surjective.

Next we show that  $h$  is injective, or that  $h(a_1) = h(a_2) \Rightarrow a_1 = a_2 \forall a_1, a_2 \in A$  or, by its contrapositive, that  $a_1 \neq a_2 \Rightarrow h(a_1) \neq h(a_2)$ . Let  $a_1 \neq a_2$ , which implies that  $f(a_1) \neq f(a_2)$  and finally that  $g(f(a_1)) \neq g(f(a_2))$ . The function  $h$  is defined as  $h(a) = g(f(a))$ , and therefore,  $a_1 \neq a_2 \Rightarrow h(a_1) \neq h(a_2)$ , making  $h$  injective. We have shown that  $h$  is both injective and surjective and therefore is bijective. The function  $h$  is a bijection between  $A$  and  $C$  which implies that the cardinality of  $A$  is the equal to the cardinality of  $C$ .

*Subclaim 1-2:* The sets  $E$ ,  $\mathbb{N}$ , and  $\mathbb{Z}$  have the same cardinality

*Subproof 1-2:* Two sets are said to have the same cardinality if there exists a bijection from one set to the other. We proved in Subproof 1-1c that there exists a bijection from  $E$  to  $\mathbb{Z}$ , which implies that the cardinality of  $E$  is equal to the cardinality of  $\mathbb{Z}$ . We will now prove that there exists a bijection from  $\mathbb{N}$  to  $\mathbb{Z}$  and in doing so show that the cardinality of  $\mathbb{Z}$  is equal to the cardinality of  $\mathbb{N}$ .

Let the function  $f : \mathbb{Z} \rightarrow \mathbb{N}$  be a piecewise function where

$$f(z) = \begin{cases} 2 \cdot z & z \geq 0 \\ -2 \cdot z - 1 & z < 0 \end{cases}.$$

The function  $f$  maps the negative integers from  $\mathbb{Z}$  to the odd integers in  $\mathbb{N}$ , and the non-negative integers from  $\mathbb{Z}$  to the even integers in  $\mathbb{N}$  although we will show that the function  $f$  is bijective more rigorously by showing that  $f$  is both surjective and injective.

For  $f$  to be surjective, we just show that  $\forall n \in \mathbb{N}, \exists z \in \mathbb{Z} \ni f(z) = n$ . When  $2 \nmid n$ , then  $f(z) = 2z$  and because  $2 \nmid n$ , then we know that there exists an element in  $\mathbb{Z}$  such that  $2z = n$ . Furthermore, because the product of two positive values must be positive, then  $z$  must be greater than zero, satisfying the piecewise constraints in  $f$ . If  $n$  is odd, then  $\exists k \in \mathbb{N} \ni 2k - 1 = n$ , implying that there also  $\exists k_- \in \mathbb{Z} \ni k_- = -k$ . Therefore,  $\exists k \in \mathbb{N} \ni 2k - 1 = n \Rightarrow \exists k_- \in \mathbb{Z} \ni -2k_- = n$  and hence, that  $f(k_-) = n$ . Therefore,  $f$  is surjective.

To show that  $f$  is injective, we show that  $f(a) = f(b) \Rightarrow a = b$ . If  $2 \nmid f(a)$ , then  $f(a) = 2 \cdot a$  and  $f(b) = 2 \cdot b$  which implies that  $2 \cdot a - 2 \cdot b = 0$  and consequently that  $2(a - b) = 0$ , which implies that  $a = b$ . If  $2 \nmid f(a)$ , then  $f(a) = -2 \cdot a - 1$  and  $f(b) = -2 \cdot b - 1$  which implies that  $-2 \cdot a - 1 - (-2 \cdot b - 1) = 0$  and consequently that  $-2 \cdot a - 1 + 2 \cdot b + 1 = 0$  which is equivalent to  $-2(a - b) = 0$ , and implies that  $a = b$  which in turn implies that  $f$  is injective.

We have shown that the cardinality of  $\mathbb{Z}$  is equal to the cardinality of  $E$  and that the cardinality of  $\mathbb{Z}$  is also equal to the cardinality of  $\mathbb{N}$ . By lemma 1-2, we also know that the cardinality of  $E$  is equal to the cardinality of  $\mathbb{N}$ , implying that  $\mathbb{Z}$ ,  $\mathbb{N}$ , and  $E$  all have the same cardinality.

**Problem 2:** Please prove that the set  $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$  is infinite, but does not have the same cardinality as  $\mathbb{N}$  (and hence not the same as  $E$  and  $\mathbb{Z}$ )

*Claim 2:* The set  $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$  is infinite but does not have the same cardinality as  $\mathbb{N}$

*Proof 2:* The claim is composed of two atomic statements: The first claims that the set  $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$  is infinite and the second claims that the same set does not have the same cardinality as  $\mathbb{N}$ . The two statements will be verified independently.

*Subclaim 2-1:* The set  $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$  is infinite

*Subproof 2-1:* To show that the set  $(0, 1)$  is infinite, we show that the function  $f : (0, 1) \rightarrow (0, \frac{1}{2})$  is bijective where  $f$  is defined as  $f(a) = \frac{a}{2}$ . To show that  $f$  is bijective, we first show that  $f$  is surjective, that is  $\forall b \in (0, \frac{1}{2}), \exists a \in (0, 1) \ni f(a) = b$ . From the definition of  $f$ , we know that  $f(a) = b \Rightarrow \frac{a}{2} = b$ , which also im-

plies that  $2b = a$  and thus (dumbass reader) there does exist an  $a$  such that  $f(a) = b$  and  $f$  is surjective.

We next show that  $f$  is injective, that is  $f(a) = f(b) \Rightarrow a = b \forall a \in (0, 1), b \in (0, \frac{1}{2})$ . From the definition of  $f$ ,  $f(a) = f(b) \Rightarrow \frac{a}{2} = \frac{b}{2}$ , which implies that  $\frac{a}{2} \cdot 2 = \frac{b}{2} \cdot 2$  and finally that  $a = b$ . Therefore, if  $f(a) = f(b)$ , then  $a = b$  and  $f$  is injective.

Because  $f$  is both surjective and injective,  $f$  is also bijective, implying that there exists a bijection between  $(0, \frac{1}{2})$  and  $(0, 1)$ . Furthermore, because  $(0, \frac{1}{2})$  is a proper subset of  $(0, 1)$ , the set  $(0, 1)$  is infinite.

*Subclaim 2-2:* The set  $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$  does not have the same cardinality as  $\mathbb{N}$ .

*Subproof 2-2:* To show that the set  $(0, 1)$  does not have the same cardinality as  $\mathbb{N}$ , we must show that there cannot exist a bijection between the two sets. In doing so, it is sufficient to show that there cannot exist a surjection between the two sets. Suppose there exists a surjection  $f : \mathbb{N} \rightarrow (0, 1)$  where the values in the domain and codomain are organized into a table such that

$x$ (Domain)	$f(x)$ (codomain)
1	$f(1)$
2	$f(2)$
3	$f(3)$
4	$f(4)$
$\vdots$	$\vdots$

Because each element in the codomain of  $f$  is in the set  $(0, 1)$ , each value can be expressed in decimal form, where each decimal place contains a value from zero to nine such that  $f(i) = 0.x_{i,1}x_{i,2}x_{i,3}x_{i,4} \cdots x_{i,n}$ , where  $n$  represents the number of values in the decimal representation and can be any arbitrary value in the set of all positive integers. Let  $x_{i,j}$  be the value of the  $j^{\text{th}}$  decimal place for  $f(i) \forall i \in \mathbb{N}$ . The table representing the domain and codomain of  $f$  can be rewritten where

$x$ (Domain)	$f(x)$ (codomain)
1	$0.x_{1,1}x_{1,2}x_{1,3}x_{1,4} \cdots x_{1,n_1}$
2	$0.x_{2,1}x_{2,2}x_{2,3}x_{2,4} \cdots x_{2,n_2}$
3	$0.x_{3,1}x_{3,2}x_{3,3}x_{3,4} \cdots x_{3,n_3}$
4	$0.x_{4,1}x_{4,2}x_{4,3}x_{4,4} \cdots x_{4,n_4}$
$\vdots$	$\vdots$

Let  $\Phi(i, j)$  map  $(i, j)$  to one if  $x_{i,j} = 0$ , and zero otherwise such that

$$\Phi(i, j) = \begin{cases} 1 & x_{i,j} = 0 \\ 0 & x_{i,j} \neq 0 \end{cases}.$$

Let  $a \in (0, 1)$  which is constructed using the diagonal elements from the codomain of  $f$  as shown in Table 1 so that  $a = 0.\Phi(1, 1)\Phi(2, 2)\Phi(3, 3) \cdots \Phi(n, n)$ . The element  $a$  cannot be equal to  $f(1)$ . If the first entry of  $f(1)$  is equal to

$x$ (Domain)	$f(x)$ (codomain)
1	$0.\textcolor{red}{x}_{1,1}x_{1,2}x_{1,3}x_{1,4} \cdots x_{1,n_1}$
2	$0.x_{2,1}\textcolor{red}{x}_{2,2}x_{2,3}x_{2,4} \cdots x_{2,n_2}$
3	$0.x_{3,1}x_{3,2}\textcolor{red}{x}_{3,3}x_{3,4} \cdots x_{3,n_3}$
4	$0.x_{4,1}x_{4,2}x_{4,3}\textcolor{red}{x}_{4,4} \cdots x_{4,n_4}$
$\vdots$	$\vdots$

Table 1: Diagonal elements

0, then the first value of  $a$  is equal to 1. If the first value of  $f(1)$  is not equal to 0, then the first decimal entry of  $a$  is equal zero, so that  $f(1) \neq a$ . The same logic applies for any  $f(i)$ ,  $i \in \mathbb{N}$ , implying that  $a$  has no preimage despite being an element in  $(0, 1)$ . Therefore,  $f$  is not a surjection, which contradicts the original assumption that  $f$  was surjective between  $\mathbb{N}$  and  $(0, 1)$ . Therefore, there cannot exist any surjection (and by extension, any bijection)

between  $\mathbb{N}$  and  $(0, 1)$  which also means that the cardinality of  $\mathbb{N}$  is not equal to the cardinality of  $(0, 1)$ .

**Problem 3:** Recall  $\implies, \vee, \wedge$ , and  $\nabla$  are binary logical operations on  $\mathcal{M}$  we've studied. Recall  $\neg$  is a (the only) logical *operator* (or *unary operation*) on  $\mathcal{M}$  we've studied. Please determine, with justification, the number of different binary logical operations on  $\mathcal{M}$  there can be. Also, determine the number of logical operators there can be.

*Claim 3-1:* There are 16 possible binary operations on  $\mathcal{M}$

*Proof 3-1:* A binary operation is essentially a mapping  $f : (\{\text{True}, \text{False}\} \times \{\text{True}, \text{False}\}) \rightarrow \{\text{True}, \text{False}\}$ , where the domain of  $f$  has four elements:  $(\text{True}, \text{True}), (\text{True}, \text{False}), (\text{False}, \text{True})$  and  $(\text{False}, \text{False})$ . The image of each element in the domain can be either True, or False such that

P	Q	$f(P, Q)$
True	True	{True, False}
True	False	{True, False}
False	True	{True, False}
False	False	{True, False}

Let the set  $\mathcal{S}$  include all possible combinations of the set  $\{(P, Q) \times f(P, Q)\}$ . Note that for each row in the table, the number of elements in  $\mathcal{S}$  doubles, implying that there are  $2^4 = 16$  modes of behavior for a binary operation in  $\mathcal{M}$ . Each mode of behavior can be represented by at most one binary operation and so, there can be at most 16 binary operations on  $\mathcal{M}$ .

*Claim 3-2:* There can exist up to four binary operators on  $\mathcal{M}$

*Proof 3-2:* A binary operator on  $\mathcal{M}$  is defined as a function  $f : \mathcal{M} \rightarrow \mathcal{M}$ . A truth table for such a function could be written as

P	$f(P)$
True	{True, False}
False	{True, False}

Note that there are two rows in the truth table for a binary operator on  $\mathcal{M}$ . By the same logic as Proof 3-1, this implies that the number of combinations of  $(P, f(P))$  is equal to  $2^2 = 4$  and because a binary operator on  $\mathcal{M}$  can only represent one combination, there are four possible binary operators on  $\mathcal{M}$ .

**Problem 4:** Turn the logical system  $(\mathcal{M}, \Phi, \wedge, \vee, \implies, \impliedby, \iff, \neg)$  into a purely algebraic system over  $(\mathbb{Z}_2, +, \cdot)$  with, for  $x \in \mathcal{M}$ ,  $\Phi(x) = 0$  if  $x$  is true and  $\Phi(x) = 1$  if  $x$  is false. Use the logical system to show that any statement of the form  $[\neg P \wedge ((\text{neg} P \implies Q) \wedge \neg Q)] \implies P$  is a tautology.

The logical system  $(\mathcal{M}, \Phi, \wedge, \vee, \implies, \impliedby, \iff, \neg)$  can be expressed as an algebraic system over  $(\mathbb{Z}_2, +, \cdot)$  by expressing  $\Phi, \wedge, \vee, \implies, \impliedby, \iff$ , and  $\neg$  in term of  $+$  and  $\cdot$  in  $\mathbb{Z}_2$ .

*Claim 4-1:* The operator  $\neg$  can be expressed in terms of  $+$  and  $\cdot$  from  $\mathbb{Z}_2$ .

*Proof 4-1:* Recall how the multiplication table for  $\mathbb{Z}_2$  is

$+$	0	1
0	0	1
1	1	0

and that the column corresponding to 1 can be written in a truth table format as

$P$	$P + 1$
0	1
1	0

where 0 denotes 'True' and 1 denotes 'False'. Note how the truth table for  $P$  and  $P + 1$  is the same as the truth table for  $\neg$ , implying that  $\neg$  can be expressed algebraically such that  $\neg P \equiv P + 1$  in  $\mathbb{Z}_2$ .

*Claim 4-2:* The operation  $\vee$  can be expressed in terms of  $+$  and  $\cdot$  from  $\mathbb{Z}_2$ .

*Proof 4-2:* The truth table for the operation  $\vee$  is

$P$	$\Phi(P)$	$Q$	$\Phi(Q)$	$P \vee Q$	$\Phi(P \vee Q)$
True	0	True	0	True	0
False	1	True	0	True	0
True	0	False	1	True	0
False	1	False	1	False	1

Note how the table for multiplication in  $\mathbb{Z}_2$  is

$+$	0	1
0	0	0
1	0	1

which can be expressed in terms of  $\Phi(\cdot)$  and reorganized as a truth table such that

$\Phi(P)$	$\Phi(Q)$	$\Phi(P) \cdot \Phi(Q)$
0	0	0
1	0	0
0	1	0
1	1	1

which is equivalent to the truth table for  $\vee$ , therefore  $\vee$  can be expressed algebraically in terms of  $(\mathbb{Z}_2, +, \cdot)$ .

*Claim 4-3:* The operation  $\wedge$  can be expressed in terms of  $+$  and  $\cdot$  from  $\mathbb{Z}_2$ .

*Proof 4-3:* De Morgan's Theorem states that  $\neg(P \wedge Q) \iff \neg P \vee \neg Q$ , implying that  $P \wedge Q \iff \neg(\neg P \vee \neg Q)$ . Note that the expression  $P \wedge Q$  is equivalent to another expression which contains only the  $\neg$  operator and the  $\vee$  operation which we have shown can be expressed algebraically in  $(\mathbb{Z}_2, +, \cdot)$  which implies that  $\wedge$  can also be expressed as such.

*Claim 4-4:* The operation  $\implies$  can be expressed in terms of  $+$  and  $\cdot$  from  $\mathbb{Z}_2$ .

*Proof 4-4:* From homework 2, recall that  $P \implies Q$  can be expressed in terms of the logical statement  $P \vee \neg Q$ . Because the operator  $\vee$  and the operation  $\neg$  can be expressed algebraically, then  $P \vee \neg Q$  can also be expressed as such, implying that  $P \implies Q$  can be written in terms of the algebraic system  $(\mathbb{Z}_2, \cdot, +)$ .

*Claim 4-5:* The operation  $\iff$  can be expressed in terms of  $+$  and  $\cdot$  from  $\mathbb{Z}_2$ .

*Proof 4-5:* The truth table for the operator  $P \iff Q$  is given as

$P$	$Q$	$P \iff Q$
True	True	True
True	False	False
False	True	False
False	False	True

and can be expressed as a logical statement  $Q \vee \neg P$  as shown by their truth tables

$P$	$Q$	$P \iff Q$	$Q \vee \neg P$
True	True	True	True
True	False	False	False
False	True	False	True
False	False	True	True

The logical operator  $\vee$  and the operation  $\neg$  have already been shown to be expressible in the algebraic system  $(\mathbb{Z}_2, +, \cdot)$  which implies that  $\iff$  can as well because  $\iff$  can be expressed in terms of  $\vee$  and  $\neg$ .

*Claim 4-6:* The operation  $\iff$  can be expressed in terms of  $+$  and  $\cdot$  from  $\mathbb{Z}_2$ .

*Proof 4-6:* The truth table for  $\iff$  is given as

$P$	$Q$	$P \iff Q$
True	True	True
False	True	False
True	False	False
False	False	True

which implies that

$\Phi(P)$	$\Phi(Q)$	$\Phi(P \iff Q)$
0	0	0
1	0	1
0	1	1
1	1	0

and can be expressed logically as  $(P \wedge Q) \vee (\neg P \wedge \neg Q)$ . The logical expression for  $\iff$  is built upon the operators/operations  $\wedge, \vee$  and  $\neg$  which can be expressed algebraically in  $(\mathbb{Z}_2, +, \cdot)$ . Therefore,  $\iff$  can also be expressed algebraically in  $(\mathbb{Z}_2, +, \cdot)$ .

*Claim 4-7:* The statement  $[\neg P \wedge ((\neg P \implies Q) \wedge \neg Q)] \implies P$  is a tautology.

*Proof 4-7:* Begin by defining the following expressions

$$\neg P \equiv P + 1 \quad (1)$$

$$P \implies Q \equiv Q(P + 1) \quad (2)$$

$$P \wedge Q \equiv (P + 1)(Q + 1) + 1 \quad (3)$$

$$1 + 1 \equiv 0 \text{ in } \mathbb{Z}_2 \quad (4)$$

$$PP \equiv P \quad (5)$$

. Next, begin replacing all  $\neg$  operations such that

$$[\neg P \wedge ((\neg P \implies Q) \wedge \neg Q)] \implies P \equiv [(P + 1) \wedge (((P + 1) \implies Q) \wedge (Q + 1))] \implies P$$

Next, we replace the first use of the implies operation with it's mathematical definition from (2), yielding

$$[\neg P \wedge ((\neg P \implies Q) \wedge \neg Q)] \implies P \equiv [(P + 1) \wedge (((P + (1 + 1))Q) \wedge (Q + 1))] \implies P$$

But because  $1 + 1 = 0$  in  $\mathbb{Z}_2$ , we can also say that

$$[\neg P \wedge ((\neg P \implies Q) \wedge \neg Q)] \implies P \equiv [(P + 1) \wedge ((PQ) \wedge (Q + 1))] \implies P.$$

The next step is to substitute the algebraic definition for  $\wedge$  for the second  $\wedge$  operation such that

$$[\neg P \wedge ((\neg P \implies Q) \wedge \neg Q)] \implies P \equiv [(P + 1) \wedge ((PQ + 1)(Q + 1 + 1))] \implies P.$$

which reduces to

$$[\neg P \wedge ((\neg P \implies Q) \wedge \neg Q)] \implies P \equiv [(P + 1) \wedge (PQQ + Q)] \implies P.$$

Note, that  $QQ \equiv Q$  because when  $Q = 1, QQ = 1$  and when  $Q = 0, QQ = 0$ , therefore the previous expression can be simplified again as

$$[\neg P \wedge ((\neg P \implies Q) \wedge \neg Q)] \implies P \equiv [(P + 1) \wedge (PQ + Q)] \implies P.$$

Next, we substitute the last remaining  $\wedge$  operation for its algebraic definition to obtain

$$[\neg P \wedge ((\neg P \implies Q) \wedge \neg Q)] \implies P \equiv [(P + 1 + 1)(PQ + Q + 1)] \implies P.$$

which simplifies to

$$[\neg P \wedge ((\neg P \implies Q) \wedge \neg Q)] \implies P \equiv [(PPQ + PQ + P)] \implies P$$

and alternatively as

$$[\neg P \wedge ((\neg P \implies Q) \wedge \neg Q)] \implies P \equiv [(PQ + PQ + P)] \implies P.$$

Note that when  $PQ = 1, PQ + PQ = 0$ , and when  $PQ = 0, PQ + PQ = 0$ , therefore,  $PQ + PQ = 0$  can be applied to the previous expression as

$$[\neg P \wedge ((\neg P \implies Q) \wedge \neg Q)] \implies P \equiv P \implies P$$

and finally, the algebraic definition of  $\implies$  is used to show that

$$[\neg P \wedge ((\neg P \implies Q) \wedge \neg Q)] \implies P \equiv P(P + 1).$$

Because the expression  $P(P+1) = 0$  when  $P = 1$ , and  $P(P+1) = 0$  when  $P = 0$ , we can say that

$$[\neg P \wedge ((\neg P \implies Q) \wedge \neg Q)] \implies P \equiv 0.$$

which implies that the statement  $[\neg P \wedge ((\neg P \implies Q) \wedge \neg Q)] \implies P$  is a tautology as the statement is always true.