Homework 8: Question 1: N and Parity

Let Ω = {zero, one, ×, +}.

N is an Ω-algebra with the set of natural numbers ù ={0, 1, 2, 3, …} as carrier, and with + and × defined as usual.

Parity is an Ω-algebra with the carrier {odd, even}. The operations are defined as follows in **Parity**:

zero = even

one = odd

+	**Even**	**Odd**
Even	Even	Odd
Odd	Odd	Even

´	**Even**	**Odd**
Even	Even	Even
Odd	Even	Odd

Let *f*: **N** → **Parity** be the homomorphism between these two algebras. Then *f*: ù → {odd, even}, the mapping between their respective carriers, can be defined as follows:

Then *f* = {*x* ∈ ù | *x* = even if *x* is divisible by two without a remainder, and *x* = odd otherwise}= {<0, even>, <1, odd>, <2, even>, <3, odd>, …}

(a) **ker** *f* = f^{-1}Bf (by definition of **ker**)

= {<even, 0>, <odd, 1>, <even, 2>, <odd, 3> …} B {<0, even>, <1, odd>, <2, even>, <3, odd>, …}

From this it becomes clear what **ker** *f* will do. It will map 0 onto all even numbers, 1 onto all odd numbers, 2 onto all even numbers, 3 onto all odd numbers, etc. Thus, **ker** *f* is an equivalence relation on ù that will partition ù into the following equivalence classes:

{*x* ∈ ù | *x* is divisible by two without a remainder} = {0, 2, 4, 6, …}

{*x* ∈ ù | *x* is not divisible by two without a remainder} = {1, 3, 5, 7, …}

(b) The quotient set of ù by the equivalence relation **ker** *f*, ù/**ker** *f* = {{0, 2, 4, 6, …}, {1, 3, 5, 7, …}}

The operations of the quotient algebra **N/ker** *f* are defined as follows:

+({0, 2, 4, …}, {0, 2, 4, …}) = {0,2,4, …}

+({0, 2, 4, …}, {1, 3, 5, …}) = {1, 3, 5, …}

+({1, 3, 5, …}, {1, 3, 5, …}) = {0, 2, 4, …}

+({1, 3, 5, …}, {0, 2, 4, …}) = {1, 3, 5, …}

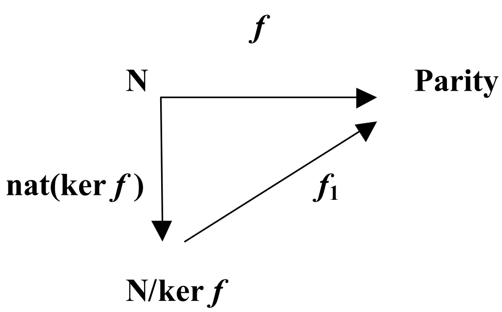
×({0, 2, 4, …}, {0, 2, 4, …}) = {0, 2, 4, …}

×({0, 2, 4, …}, {1, 3, 5, …}) = {0, 2, 4, …}

×({1, 3, 5, …}, {1, 3, 5, …}) = {1, 3, 5, …}

×({1, 3, 5, …}, {0, 2, 4, …}) = {0, 2, 4, …}

(c)



Homework 8.2: Question 1: Congruences on Nat

The equivalence relation Q_{Mod4} will partition the carrier of **Nat**, ù, into four equivalence classes. The quotient set that corresponds to this equivalence relation is shown below:

ù/Q_{Mod4} = {{0, 4, 8, 12, …}, {1, 5, 9, 13, …}, {2, 6, 10, 14,…}, {3, 7, 11, 15,…}}

We can restate the set ù/Q_{Mod4} as follows:

ù/Q_{Mod4} = {{$y\in$ ù | $x\in$ ù, $y = 4x$}, {$y\in$ ù | $x\in$ ù, $y = 4x + 1$}, {$y\in$ ù | $x\in$ ù, $y = 4x + 2$}, {$y\in$ ù | $x\in$ ù, $y = 4x + 3$}}

It is now easy to show that Q_{Mod4} agrees with all the operations from Ω_{Numb} = {**zero**, **one**, +, ×}.

For the operations **zero** and **one** this is obviously true.

There are four equivalence classes. The operations + and × are binary. There are therefore $4^2 = 16$ possible ways in which these four equivalence classes can combine with each of these two operations. However, since both + and $\times$ are commutative, we don't actually have to consider all 16 possible combinations. If we have considered ($x + y$), by commutativity we have also considered ($y + x$) – and similarly for $\times$. We therefore have to consider only 10 possible combinations.

For ease of reference, I will give each of the equivalence classes names:

[+0] = {$y \in$ ù | $x \in$ ù, $y = 4x$}

[+1] = {$y \in$ ù | $x \in$ ù, $y = 4x + 1$}

[+2] = {$y \in$ ù | $x \in$ ù, $y = 4x + 2$}

[+3] = {$y \in$ ù | $x \in$ ù, $y = 4x + 3$}

To show that Q_{Mod4} agrees with +:

$x, y \in$ ù.

Class [+0] + Class [+0] = $4x + 4y = 4(x + y)$

Therefore, the result of applying + to any two members from Class [+0], will always result in an answer from Class [+0].

Class [+0] + Class [+1] = $4x + (4y + 1) = 4(x + y) + 1$

Therefore, the result of applying + to any member from Class [+0] and any member from Class [+1], will always result in an answer from Class [+1].

Class [+0] + Class [+2] = $4x + (4y + 2) = 4(x + y) + 2$

Therefore, the result of applying + to any member from Class [+0] and any member from Class [+2], will always result in an answer from Class [+2].

Class [+0] + Class [+3] = $4x + (4y + 3) = 4(x + y) + 3$

Therefore, the result of applying + to any member from Class [+0] and any member from Class [+3], will always result in an answer from Class [+3].

Class [+1] + Class [+1] = $(4x + 1) + (4y + 1) = 4(x + y) + 2$

Therefore, the result of applying + to any two members from Class [+1], will always result in an answer from Class [+2].

Class [+1] + Class [+2] = (4*x* + 1) + (4*y* + 2) = 4(*x* + *y*) + 3

Therefore, the result of applying + to any member from Class [+1] and any member from Class [+2], will always result in an answer from Class [+3].

Class [+1] + Class [+3] = (4*x* + 1) + (4*y* + 3) = 4(*x* + *y* + 1)

The result here is therefore 4 times an integer, and therefore a member of Class [+0]. Therefore, the result of applying + to any member from Class [+1] and any member from Class [+3], will always result in an answer from Class [+0].

Class [+2] + Class [+2] = (4*x* + 2) + (4*y* + 2) = 4(*x* + *y* + 1)

The result here is therefore 4 times an integer, and therefore a member of Class [+0]. Therefore, the result of applying + to any two members from Class [+2], will always result in an answer from Class [+0].

Class [+2] + Class [+3] = (4*x* + 2) + (4*y* + 3) = 4(*x* + *y* + 1) + 1

The result here is therefore (4 times an integer) + 1, and therefore a member of Class [+1]. Therefore, the result of applying + to any member from Class [+2] and any member from Class [+3], will always result in an answer from Class [+1].

Class [+3] + Class [+3] = (4*x* + 3) + (4*y* + 3) = 4(*x* + *y* + 1) + 2

The result here is therefore (4 times an integer) + 2, and therefore a member of Class [+2]. Therefore, the result of applying + to any two members from Class [+3], will always result in an answer from Class [+2].

To show that Q_{Mod4} agrees with ´ :

$x, y \in$ ù.

Class [+0] × Class [+0] = 4*x* × 4*y* = 16*xy* = 4(4*xy*)

This is 4 × an integer, and therefore a member of Class [+0]. Therefore, the result of applying × to any two members from Class [+0], will always result in an answer from Class [+0].

Class [+0] × Class [+1] = 4*x* × (4*y* + 1) = 16*xy* + 4*x* = 4(4*xy* + *x*)

This is 4 × an integer, and therefore a member of Class [+0]. Therefore, the result of applying × to any member from Class [+0] and any member from Class [+1], will always result in an answer from Class [+0].

Class [+0] $\times$ Class [+2] = $4x \times (4y + 2) = 16xy + 8x = 4(4xy + 2x)$

This is 4 $\times$ an integer, and therefore a member of Class [+0]. Therefore, the result of applying $\times$ to any member from Class [+0] and any member from Class [+2], will always result in an answer from Class [+0].

Class [+0] $\times$ Class [+3] = $4x \times (4y + 3) = 16xy + 12x = 4(4xy + 3x)$

This is 4 $\times$ an integer, and therefore a member of Class [+0]. Therefore, the result of applying $\times$ to any member from Class [+0] and any member from Class [+3], will always result in an answer from Class [+0].

Class[+1]$\times$Class[+1] = $(4x+1) \times (4y+1) = 16xy + 4x + 4y + 1 = 4(4xy + x + y) + 1$

This is (4 $\times$ an integer) + 1, and therefore a member of Class [+1]. Therefore, the result of applying $\times$ to any two members from Class [+1], will always result in an answer from Class [+1].

Class[+1]$\times$Class[+2]=$(4x+1) \times (4y+2) = 16xy + 8x + 4y + 2 = 4(4xy + 2x + y) + 2$

This is (4 $\times$ an integer) + 2, and therefore a member of Class [+2]. Therefore, the result of applying $\times$ to any member from Class [+1] and any member from Class [+2], will always result in an answer from Class [+2].

Class[+1]$\times$Class[+3]=$(4x+1) \times (4y+3) = 16xy + 12x + 4y + 3 = 4(4xy + 3x + y) +3$

The result here is therefore (4 times an integer) + 3, and therefore a member of Class [+3]. Therefore, the result of applying $\times$ to any member from Class [+1] and any member from Class [+3], will always result in an answer from Class [+3].

Class[+2]$\times$Class[+2]=$(4x+2)\times(4y+2) = 16xy + 8x + 8y + 4 = 4(4xy + 2x + 2y + 1)$

The result here is therefore 4 times an integer, and therefore a member of Class [+0]. Therefore, the result of applying $\times$ to any two members from Class [+2], will always result in an answer from Class [+0].

Class[+2]$\times$Class[+3]=$(4x+2)\times(4y+3)=16xy + 12x + 8y + 6 = 4(4xy+3x+2y+1) + 2$

The result here is therefore (4 times an integer) + 2, and therefore a member of Class [+2]. Therefore, the result of applying $\times$ to any member from Class [+2] and any member from Class [+3], will always result in an answer from Class [+2].

Class[+3]×Class[+3]=(4x+3)×(4y+3)=16xy+12x+12y+9 = 4(4xy+3x+3y+2) + 1

The result here is therefore (4 times an integer) + 1, and therefore a member of Class [+1]. Therefore, the result of applying × to any two members from Class [+3], will always result in an answer from Class [+1].

We have therefore shown that Q_{Mod4} on ù agrees with all operations in Ω_{Numb}. From this it follows that Q_{Mod4} is a congruence on **Nat**.

Homework 8.2: Question 2: More congruences on Nat

The equivalence relation $Q_{Mod\,n}$ = {<x, y> | $x =_{Mod\,n} y$} on ù will agree with every operation in Ω_{Numb} for all values of $n > 1$, $n \in$ ù. $Q_{Mod\,n}$ therefore is a congruence on **Nat** for every n.

The general formula for the quotient set of $Q_{Mod\,n}$ on ù, is:

ù/$Q_{Mod\,n}$ = {{$y\in$ ù | $x\in$ ù, $y = xn$}, {$y\in$ ù | $x\in$ ù, $y = xn + 1$}, {$y\in$ ù | $x\in$ ù, $y = xn + 2$}, …, {$y\in$ ù | $x\in$ ù, $y = xn + (n-1)$}}

Again, the agreement of $Q_{Mod\,n}$ = with **zero** and **one** is obvious.

For a specific value of n, any member of ù can be expressed in terms of one and only one of the formulas that define the different equivalence classes that correspond to that specific value of n.[1]

Also, for a specific value of n, the result of adding any two of the formulas that define the different equivalence classes that correspond to that specific value of n, or of multiplying any two of these formulas, can always be expressed by one and only of these formulas.[2]

It therefore follows that applying + to any two operands that are members from two[3] specific equivalence classes, will always yield a result in the same equivalence class, no matter which specific members of the equivalence classes are chosen as operands. The same is true of ×.

$Q_{Mod\,n}$ is therefore a congruence on **Nat** for every n.

---

1 This is provable, but seems obvious enough that I won't actually prove it. The claim is that, for instance, 18_{Mod4} can be expressed by only one the formulas that correspond to the equivalence classes of Mod4, namely 4x + 2. That is 18_{Mod4} = 4(4) + 2. There is no other way possible of expressing 18 in terms of the formulas corresponding to the equivalence classes of Mod4. Obviously, 4(4) + … will not work – this yields to large a number. Also, 4(3) + … will not do. Then we need to add 6, and there is no of the formulas in Mod4 that adds more than 3.

2 This is intended to express the fact that, in Mod8 for instance, the result of (z8 +3) + (y8 + 4), can be expressed as (z+y)8 + 7, which corresponds to one and only of the formulas that define the equivalence classes of Q_{Mod8}.

3 (not necessarily distinct)