CISS362: Introduction to Automata Theory, Languages, and Computation
Assignment 3

The following are some properties of integers. In the following x, y, z, w are integers. First we have the basic rules for addition:

A1. $x + y$ is an integer.

A2. $(x + y) + z$ can be rewritten as $x + (y + z)$.

A3. $x + (y + z)$ can be rewritten as $(x + y) + z$.

A4. $x + (-x)$ can be rewritten as 0.

A5. 0 can be rewritten as $x + (-x)$.

A6. $0 + x$ can be rewritten as x.

A7. x can be rewritten as $0 + x$.

A8. $x + 0$ can be rewritten as x.

A9. x can be rewritten as $x + 0$.

A10. $x + y$ can be rewritten as $y + x$.

(A = addition.) Now for the multiplication rules:

M1. xy is an integer.

M2. $(xy)z$ can be rewritten as $x(yz)$.

M3. $x(yz)$ can be rewritten as $(xy)z$.

M4. $1x$ can be rewritten as x.

M5. x can be rewritten as $1x$.

M6. $x1$ can be rewritten as x.

M7. x can be rewritten as $x1$.

M8. xy can be rewritten as yx.

(M = multiplication.) Here are the rules involving both addition and multiplication

AM1. $x(y+z)$ can be rewritten as $xy+xz$

AM2. $xy+xz$ can be rewritten as $x(y+z)$

(AM = addition and multiplication,) Here are some facts that you may assume. There are facts that can be derived from the above rules

F1. If $x=y$, then $xz=yz$.

F3. If $x=y$, then $x+z=y+z$.

F3. $0x$ can be replaced by 0.

F4. $x0$ can be replaced by 0.

F5. If $x=y$ and $z=w$, then $x+z=y+w$.

(F = facts.) We want to prove some basic facts divisibility. Given two integer a, b we say that a divides b, and we write $a \mid b$ is there is an integer c such that $ac=b$. This of course means that

D1 "$a \mid b$" can be replaced by "$ac=b$ for some integer c".

D2 "$ac=b$ for some integer c" can be replaced by "$a \mid b$".

(D = definition.)

Several proofs are already provided. make sure you study them to see how I want you to write the proofs. I'v simplified the proofs to make it easier to understand so that we're not overly caught up with formal logic.

Q1. Let a be an integer. Prove that $1 \mid a$.

SOLUTION.

$$\begin{aligned} & 1a = a && \text{by M4} \\ \therefore\ & 1c = a \text{ for some integer } c(= a) \\ \therefore\ & 1 \mid a && \text{by D2} \end{aligned}$$

Note. The above shows you how to take a fact and produce another that involves "for some ....". Basically if you have a propositional formula $P(x)$ where x is a variable, then if $P(v)$ is true where v is a value, then "$P(x)$ is true for some value for x" must also be true (duh). It's pretty obvious right?

It's the same as saying if

"I have a pebble in my pocket"

then of course

"I have an x in my pocket for some x.

Right? This is an "axiom" or rule in logic meaning to say that this way of deducing a new fact is allowed because it models the way human beings think. Because this axiom produces a new fact, it's also called an **inference rule**.

Note that the "opposite" of that is not true! Just because I can say that "I have an x in my pocket for some x", it does not mean that "I have a pebble in my pocket" because what I have in my pocket might very well be my pet lizard.

This is basically what you see in your discrete math class as an axiom in logic:

$$\begin{aligned} & P(a) \\ \therefore\ & \exists x(P(x)) \end{aligned}$$

This inference rule is called existential generalization. From now on we'll call it EG. So you should write the proof like this:

$$\begin{aligned} & 1a = a && \text{by M4} \\ \therefore\ & 1c = a \text{ for some integer } c(= a) && \text{by EG} \\ \therefore\ & 1 \mid a && \text{by D2} \end{aligned}$$

Note. Note that the only reason why proofs at an undergraduate level are written so tediously is because you have to learn how to think and argue logically and precisely. The above format allows you to check the correctness of your logic. Papers written even in research journals are actually *not* written in the above format. For instance in a paper one would write:

> *Since* $1a = a$*, we have* $1c = a$ *for some integer* c *and hence by definition* $1 \mid a$*, i.e.* 1 *divides* a*.*

or even

> *Since* $1a = a$*, by definition* 1 *divides* a*.*

Note. The application of "rule" D1 or D2 is not a deduction (or inference). It's just a linguistic translation of notation and definition.

Q2. Let a be an integer. Prove that $a \mid a$.

SOLUTION.

	$a = a$	
$\therefore$	$1a = a$	by M5
$\therefore$	$ca = a$ for some integer $c(= 1)$	by F1
$\therefore$	$ac = a$ for some integer c	by M8
$\therefore$	$a \mid a$	by D2

Q3. Let a, b, c be integers. Prove that if $a \mid b$, then $a \mid (bc)$.

SOLUTION.

$a \mid b$	
$\therefore\ ax = b$ for some integer x	by D1
$\therefore\ (ax)c = bc$ for some integer x	by F1
$\therefore\ a(xc) = bc$ for some integer x	by M2
$\therefore\ a(xc) = bc$ for some integer xc	by M1
$\therefore\ ay = bc$ for some integer $y(= xc)$	by EG
$\therefore\ a \mid bc$	by D2

Q4. Let a, b, c be integers. Prove that if $a \mid b$ and $b \mid c$, then $a \mid c$.

SOLUTION. From $a \mid b$ we have:

$$\begin{array}{lll} & a \mid b & \\ \therefore & ax = b \text{ for some integer } x & \text{by D1} \end{array} \quad \text{(A)}$$

From $b \mid c$ we have:

$$\begin{array}{lll} & b \mid c & \\ \therefore & by = c \text{ for some integer } y & \text{by D1} \end{array} \quad \text{(B)}$$

From (A) and (B) (rewriting b as ax (A) in (B)) we have:

$$\begin{array}{lll} & (ax)y = c \text{ for some integers } x, y & \\ \therefore & a(xy) = c \text{ for some integers } x, y & \text{by M2} \\ \therefore & a(xy) = c \text{ for some integer } xy & \text{by M1} \\ \therefore & az = c \text{ for some integers } z(= xy) & \text{by F1} \\ \therefore & a \mid c & \text{by D2} \end{array}$$

Q5. Let a, b, c be integers. Prove that if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

SOLUTION. From $a \mid b$ we have:

$$\begin{aligned} & a \mid b \\ \therefore\ & ax = b \text{ for some integer } x && \text{by D1} && \text{(A)} \end{aligned}$$

From $a \mid c$ we have:

$$\begin{aligned} & a \mid c \\ \therefore\ & ay = c \text{ for some integer } y && \text{by D1} && \text{(B)} \end{aligned}$$

From (A) and (B) we have:

$$\begin{aligned} & ax + ay = b + c \text{ for some integers } x, y \\ \therefore\ & a(x + y) = b + c \text{ for some integers } x, y && \text{by AM2} \\ \therefore\ & a(x + y) = b + c \text{ for some integer } x + y && \text{by A1} \\ \therefore\ & az = b + c \text{ for some integers } z(= x + y) && \text{by F1} \\ \therefore\ & a \mid (b + c) && \text{by D2} \end{aligned}$$