Harvard University
Computer Science 20

Problem Set 2

PROBLEM 1

Consider the following mathematical statement: "For any integers x and y, if there is some integer $d > 1$ such that $d \mid x$ and $d \mid y$, then x and y are *not* relatively prime."

(A) Translate the sentence into propositional logic. Stress test it with some test cases of different values for x, y, and d. You may use the predicates $\mathrm{RelPrime}(x, y)$ and $\mathrm{Divisor}(d, x, y)$. You do not need to include the domains for the variables in your logical formula.
(B) Put the formula into Prenex Normal Form. Show your full derivation with the justification for each step.
(C) State the contrapositive of the original claim both in English (with some math) and in logic.

Solution.
(A)
$\forall x, y \in \mathbb{Z}.[\exists d \in \mathbb{Z}.(d > 1) \wedge (d \mid x) \wedge (d \mid y)] \rightarrow [\neg RelPrime(x, y)]$
(B)
1. $\forall x, y \in \mathbb{Z}.\neg[\exists d \in \mathbb{Z}.(d > 1) \wedge (d \mid x) \wedge (d \mid y)] \vee [\neg RelPrime(x, y)]$: removing implication
2. $\forall x, y \in \mathbb{Z}.\forall d \in \mathbb{Z}.\neg[(d > 1) \wedge (d \mid x) \wedge (d \mid y)] \vee [\neg RelPrime(x, y)]$: shift-in negations in-order to make quantifiers global

(C)
For any integers x and y, if x and y are co-prime, then there does not exist some integer $d > 1$ such that $d|x$ and $d|y$

$\forall x, y \in \mathbb{Z}.[RelPrime(x, y] \rightarrow \neg[\exists d \in \mathbb{Z}(d > 1) \wedge (d|x) \wedge (d|y))]$

PROBLEM 2

The domain of discourse is the natural numbers. Let $\Pi(x, y, z)$ = "z is the product of x and y". Define each of the following in terms of Π. You may also use $=$ in your formula to compare numbers for equality.

(A) Write a formula that means "there exists an x that is the multiplicative identity". Recall that a multiplicative identity is a number that leaves unchanged any number by which it is multiplied.

(B) Let n be some (fixed) positive integer. Write a formula that means "n is a prime number". Note that n should not be quantified in your formula because it is already a fixed value. (Added challenge: use your multiplicative identity formula). Recall that a prime number is a natural number greater than 1 cannot be evenly divided by any natural numbers other than 1 and itself.

(C) Write a formula that symbolizes the commutative property for the multiplication of integers (i.e. $x \times y = y \times x$).

(D) Write a formula that symbolizes the associative law for the multiplication of integers (i.e. $x \times (y \times z) = (x \times y) \times z$).

Solution.
(A)
$\forall(y \in \mathbb{N})\exists(x \in \mathbb{N}).\Pi(x, y, x)$
(B)
$\forall(a \in \mathbb{N})\nexists(b \in \mathbb{N}).(b > 1) \wedge \Pi(a, b, n)$
(C)
$\forall(x, y \in \mathbb{N}).[x * y == y * x]$ note. not sure if '==' is a valid expression to check equality, so alternative expression below
$\forall(x, y \in \mathbb{N})\exists(d \in \mathbb{N}).\Pi(x, y, d) \wedge \Pi(y, x, d)$
(D)
$\forall(x, y, z) \in \mathbb{N}).[(x * y) * z == x * (y * z)]$ note. not sure if '==' is a valid expression to check equality, so alternative expression below
$\forall(x, y, z) \in \mathbb{N})\exists(d \in \mathbb{N}).\Pi((x * y), z, d) \wedge \Pi(x, (y * z), d)$

PROBLEM 3

For any real numbers x and y, let's define the operation $\oslash$ by the equation $x \oslash y = 2(x + y)$

Disprove the following claim: For any real numbers x,y, and z, $(x \oslash y) \oslash z = x \oslash (y \oslash z)$

Solution.
Proof by contradiction: For any real numbers x,y, and z, $(x \oslash y) \oslash z = x \oslash (y \oslash z)$. Find numbers such that theorem doesn't hold.

Assume that $(x \oslash y) \oslash z = x \oslash (y \oslash z)$ is true, then find contradiction.

1. Inline '$\oslash$' operator definition: $2(2(x + y) + z) = 2(x + 2(y + z))$
2. Simplify: $4x + 4y + 2z + 2x + 4y + 4z$
2. Simplify: $2x + 2y + z = x + 2y + 2z$

When $x \neq z$ and $y \in \mathbb{Z}$, the equation is invalid eg. $x := 3, y := 4, z := 5$
Replacing vars w/ literals: $(3 \oslash 4) \oslash 5 = 3 \oslash (4 \oslash 5)$
Simplified: $6 + 8 + 5 = 3 + 8 + 10$
Simplified: $11 = 13$ (false/invalid statement)

As shown above, when you plugin any two integers (not equal to each other) for x and y (eg, $x := 3, y := 4, z := 5$; the equation simplifies to (11 = 13), which is false and a contradiction, proving the claim to false.

PROBLEM 4

If x and y are integers and $x^2 + y^2$ is even, prove that $x + y$ is even.

Note: You may use without proof the fact that the product of two integers is even unless both integers are odd. You may use without proof the closure properties of the integers.

Solution.
Proof by contraposative: I will prove the contraposative of the claim by showing that both $x + y$ and $x^2 + y^2$ are odd
Definition: Even(x) is true if $x \in 2k; k \in \mathbb{Z}$
Definition : Odd(x) is true if $x = 2k + 1; k \in \mathbb{Z}$
$Lemma_1$: Odd + Even = Odd $\because k_1, k_2, k_3 \in \mathbb{Z}; 2k_1 + (2k_2 + 1) = 2k_3 + 1$
$Lemma_2$: Odd - Even = Odd $\because$ let $k, k_1, k_2, k_3 \in \mathbb{Z}$; Even := $2k$; Odd:= $2k + 1$; $(2k_1 + 1) - 2k_1 = 2(k_1 - k_2) + 1 = 2k_3 + 1$ (Odd)

Claim: $\forall(x, y \in \mathbb{Z}).Even(x^2 + y^2) \rightarrow Even(x + y)$
Contraposative: $\forall(x, y \in \mathbb{Z}).Odd(x + y) \rightarrow Odd(x^2 + y^2)$

let k_1, k_2, x, y be integers
$x + y = 2k_1 + 1$
$(x + y)^2 = (2k_1 + 1)^2$
$x^2 + 2xy + y^2 = 4k_1^2 + 4k_1 + 1$
$x^2 + 2xy + y^2 = 2(2k_1^2 + 2k_1) + 1$
integers are closed addition and multiplication.$\therefore 2k_1k_1 + 2k_1 \in \mathbb{Z}$
let $k_2 := 2k_1^2 + 2k_1$
$x^2 + 2xy + y^2 = 2k_2 + 1 \therefore x^2 + 2xy + y^2$ is odd

$2xy$ must be even $\because$ it is the product of an even integer "2" and another (arbitrary) integer xy.

Since $x^2 + 2xy + y^2$ is odd and $2xy$ is even, and the difference between an odd and even number must be odd ($Lemma_2$), therefore $(x^2 + 2xy + y^2) - (2xy)$ or $(x^2 + y^2)$ must be odd.

PROBLEM 5

Extend the proof of the Division Algorithm to the case of negative integers. (Note that the proof of uniqueness for non-negative numbers given in class did not depend on $a \geq 0$, so you only have to establish existence.)
Hint: Suppose $-a$ is a negative number (so a is positive). From the Division Algorithm for positive integers, we already know that there are unique q' and r such that $a = q'd + r'$ and $0 \leq r' < d$. We need to find q and r such that $-a = qd + r$. Consider two cases, when $r' = 0$ and when $r' > 0$. These examples may help:

$$25 = 2 \cdot 9 + 7 \qquad -25 = (-3) \cdot 9 + 2 \tag{1}$$

$$49 = 5 \cdot 9 + 4 \qquad -49 = (-6) \cdot 9 + 5 \tag{2}$$

Solution.

Proof. We can will extend the proof of the Division Algorithm to the case of negative integers by showing that for any integer a and any positive integer d, there exists unique integers q and r: $a = qd + r$ and $0 \leq r < d$.
Given the existing definition for the division algorithm for a positive integer a such that $a = q'd + r'$. We can rewrite the algorithm for a negative integer $-a$ as: $-a = -(q'd + r')$ or $-a = -q'd - r'$

Case 1: $r' = 0$
$a = q'd + r$
$-a = -q'd - r$
if $r' = 0$ then $-a = -q'd$ and r satisfies $0 \leq r < d \because r = 0$
and then if we let $q = -q'$ (this being a valid definition because both variables are positive/negative integers), then $-a = qd + r$.
By algebraically manipulating our original proof into something which represented negative inputs, we were able to demonstrate that q and r exists which satisfy the conditions.

Case 2: $r' > 0$
$-a = -q'd - r'$
$-a = -q'd - d + d - r'$
$-a = (-q(-q' + 1)d + (d - r')$
let q := -(q' + 1) and let r := (d - r') : We are able to define q and r as such because integers are closed under addition (and subtraction) and all variables involved are integers.
Our definition of r satisfies $0 \leq r < d$ because $0 \leq (d - r') < d$ and $0 < r' < d$ causes the difference between d and r' to be greater than or equal to zero and less than r.

Once we populate our original division algorithm with our new definitions we get $-a = qd + r$ showing that there exist integers q and d that satisfy the algorithm (and as a result of our definitions q', r' and their conditions).

In conclusion, the proof of Division algorithm can be extended to all negative numbers by showing that the algorithm holds true for cases when r' (the remainder is equal to or when the remainder is greater than 0)

PROBLEM 6

The integers a and b are *relatively prime* if $\mathrm{GCD}(a, b) = 1$. Consider the following claim:

Prove: If, for some $x \in \mathbb{Z}$, $ax \equiv 1 \pmod{b}$, then a and b are relatively prime.

Note: You may find it useful to refer to the logical formulation of a very similar claim you saw in an earlier problem.

Solution.
Proof. I will prove that for some $x \in \mathbb{Z}$, $ax \equiv 1 \pmod{b}$, then a and b are relatively prime.

$(x \in \mathbb{Z}; ax \equiv_b 1) \rightarrow (a \perp b)$

Assume a and b are not co-prime. GCD(a,b) = d where d is an integer greater than 1. $ax \equiv 1 \mod b$ means that there exists an integer k: $ax = 1 + kb$

Since $(d|a)$ and $(d|b)$ we can define $a := d * a'$ and $b := d * b'$ for integers a' and b'.
$da'x = 1 + kdb'$
$da'x - kdb' = 1$
$d(a'x - kb') = 1$
The left hand side $(d(a'x - kb'))$ is divisible by d, which means it is multiple of d.
However, the right-hand side is 1, which is not divisible by d ($\because d > 1$), creating a contradiction because we cannot get 1 as a product of two integers where at least one is greater than 1.