CSC165H1: Problem Set 1 Sample Solutions

Due October 2 before 4 p.m.

Note: solutions are incomplete, and meant to be used as guidelines only. We encourage you to ask follow-up questions on the course forum or during office hours.

1. **[6 marks] Truth tables and formulas.** Consider the following formula:

$$\neg r \Rightarrow (\neg p \Rightarrow q)$$

(a) **[2 marks]** Write the truth table for the formula. (No need to show your calculations).

Solution

p	q	r	$\neg r \Rightarrow (\neg p \Rightarrow q)$
T	T	T	T
T	T	F	T
T	F	T	T
T	F	F	T
F	T	T	T
F	T	F	T
F	F	T	T
F	F	F	F

(b) **[2 marks]** Write a logically equivalent formula that doesn't use $\Rightarrow$ or $\Leftrightarrow$, in other words it uses only $\wedge, \vee$, or $\neg$. Show how you derived the result.

Solution

$$\begin{aligned}
\neg r \Rightarrow (\neg p \Rightarrow q) &\equiv r \vee (\neg p \Rightarrow q) && \text{\# material implication} \\
&\equiv r \vee (p \vee q) && \text{\# material implication again} \\
&\equiv r \vee p \vee q && \text{\# } \vee \text{ is associative}
\end{aligned}$$

(c) **[2 marks]** Write formula that is logically equivalent to the **converse** of the given formula, and that doesn't use $\Rightarrow$ or $\Leftrightarrow$, in other words it uses only $\wedge, \vee$, or $\neg$. Show how you derived the result.

Solution

$$\begin{aligned}
(\neg p \Rightarrow q) \Rightarrow \neg r &\equiv \neg(\neg p \Rightarrow q) \vee \neg r && \text{\# material implication} \\
&\equiv (\neg p \wedge \neg q) \vee \neg r && \text{\#De Morgan's}
\end{aligned}$$

2. **[6 marks] one-to-one and onto**

Use the following definitions in the questions below.

Onto(f): $\forall n \in \mathbb{N}, \exists m \in \mathbb{N}, f(m) = n$, for $f : \mathbb{N} \to \mathbb{N}$.

OneToOne(f): $\forall m, n \in \mathbb{N}, m \neq n \Rightarrow f(m) \neq f(n)$, for $f : \mathbb{N} \to \mathbb{N}$.

(a) **[1 mark]** Suppose $\neg$**Onto(g)**. Write this in predicate logic **without** using the predicate name **Onto**.

> **Solution**
>
> I simply negate the definition of **Onto(g)**:
>
> $$\exists n \in \mathbb{N}, \forall m \in \mathbb{N}, g(m) \neq n$$

(b) **[1 mark]** Suppose $\neg$**OneToOne(h)**. Write this in predicate logic **without** using the predicate name **OneToOne**.

> **Solution**
>
> Again, I negate the definition of **OneToOne(h)**:
>
> $$\exists m, n \in \mathbb{N}, m \neq n \wedge h(m) = h(n)$$

(c) **[1 mark]** Give an example of a function $f : \mathbb{N} \to \mathbb{N}$ where **Onto(f)** and **OneToOne(f)**.

> **Solution**
>
> This function always sends different inputs to different outputs (themselves!), and any element of the codomain is output from itself in the domain:
>
> $$f(n) = n$$

(d) **[1 mark]** Give an example of a function $f : \mathbb{N} \to \mathbb{N}$ where $\neg$**Onto(f)** and **OneToOne(f)**.

> **Solution**
>
> Every input produces output twice itself, so different inputs get sent to different outputs, but there are no inputs that produce any odd natural number as output:
>
> $$f(n) = 2n$$

(e) **[1 mark]** Give an example of a function $f : \mathbb{N} \to \mathbb{N}$ where **Onto(f)** and $\neg$**OneToOne(f)**.

> **Solution**
>
> Inputs 0 and 1 both produce output 0, and for every output n there is corresponding input $2n$:
>
> $$f(n) = \lfloor n/2 \rfloor$$

(f) **[1 mark]** Give an example of a function $f : \mathbb{N} \to \mathbb{N}$ where $\neg$**Onto(f)** and $\neg$**OneToOne(f)**.

> **Solution**
>
> Inputs 0 and 1 both produce output 5, and there is no input that produces output 6:
>
> $$f(n) = 5$$

3. **[7 marks] modular arithmetic**

(a) **[2 marks]** Prove Example 2.19(1) from the course notes.

Solution

translation: Example 2.19(1) states:

$$\forall a, b, c, d, n \in \mathbb{Z}, n \neq 0 \Rightarrow (a \equiv c \bmod n \wedge b \equiv d \bmod n \Rightarrow a + b \equiv c + d \bmod n)$$

discussion: Unpacking the definition of congruence modulo n tells us that $n \mid (a-c)$ and $n \mid b-d$. It looks as though adding $(a-c)$ and $(b-d)$ gives us what we want.

header: Let $a, b, c, d \in \mathbb{Z}$. Let $n \in \mathbb{Z}^+$. Assume $a \equiv c \bmod n$ and $b \equiv d \bmod n$, in other words $n \mid (a-c)$ and $n \mid (b-d)$. WTS $n \mid ((a+b)-(c+d))$.

body:

$$\begin{aligned} n \mid (a-c) \wedge n \mid (b-d) \quad \Rightarrow \quad & n \mid (1 \cdot (a-c) + 1 \cdot (b-d)) \\ & \text{\# by divisibility of linear combinations, proved in lecture} \\ & n \mid ((a+b)-(c+d)) \quad \blacksquare \end{aligned}$$

(b) **[2 marks]** Prove Example 2.19(3) from the course notes.

Solution

translation: Example 2.19(3) states:

$$\forall a, b, c, d, n \in \mathbb{Z}, n \neq 0 \Rightarrow (a \equiv c \bmod n \wedge b \equiv d \bmod n \Rightarrow ab \equiv cd \bmod n)$$

discussion: Unpacking the definition of congruence modulo n and using linear combination worked so well last time that I will try it again. Since I need to end up with an ab term, I multiply $(a-c)$ by b, but then I need to multiply $(b-d)$ by something to undo the damage... Multiplying by c seems to work!

header: Let $a, b, c, d, n \in \mathbb{Z}$. Assume $n \neq 0$ and $a \equiv c \bmod n$ and $b \equiv d \bmod n$, in other words $n \mid (a-c)$ and $n \mid (b-d)$. WTS $n \mid (ab - cd)$.

body:

$$\begin{aligned} n \mid (a-c) \wedge n \mid (b-d) \quad \Rightarrow \quad & n \mid b \cdot (a-c) + c \cdot (b-d)) \\ & \text{\# by divisibility of linear combinations, proved in lecture} \\ & n \mid (ab - cd) \quad \blacksquare \end{aligned}$$

(c) **[3 marks]** Use Example 2.19(3) to find the units digit of 257^{256}. Use Example 2.19(3) to prove your result — we will not accept the argument that you used a calculator or programming language to compute this with brute force.

Solution

translation:

$$257^{256} \equiv 1 \bmod 10$$

description: The translation says, in other words, $\exists k \in \mathbb{Z}, 257^{256} = 10k + 1$, or the units digit of 257^{256} is 1. I show by repeatedly multiplying pairs of numbers equivalent to each other modulo 10.

I will use a small lemma in the process:*

claim:

$$\forall a, b, c, n \in , n \neq 0 \Rightarrow (a \equiv b \bmod n \wedge b \equiv c \bmod n \Rightarrow a \equiv c \bmod n)$$

header: Let $a, b, c, n \in \mathbb{Z}$. Assume $n \neq 0 \wedge a \equiv b \bmod n \wedge b \equiv c \bmod n$. WTS $a \equiv c \bmod n$.

body:

$n \mid (a - b) \wedge n \mid (b - c)$ # definition of congruence

$n \mid 1 \cdot (a - b) + 1 \cdot (b - c)$ # by divisibility of linear combinations

$n \mid (a - c)$

$a \equiv c \bmod n$ # definition of congruence ■

main header: WTS $257^{256} \equiv 1 \bmod 10$.

main body:

$$\begin{aligned}
257 &\equiv 7 \bmod 10 && \text{\# since } 10 \mid 257 - 7 \\
257^2 &\equiv 7^2 \bmod 10 && \text{\# by 2.19(3)} \\
7^2 &\equiv 9 \bmod 10 && \text{\# since } 10 \mid 49 - 9 \\
257^2 &\equiv 9 \bmod 10 && \text{\# by lemma} \\
257^4 &\equiv 9^2 \bmod 10 && \text{\# by 2.19(3)} \\
9^2 &\equiv 1 \bmod 10 && \text{\# since } 10 \mid 81 - 1 \\
257^4 &\equiv 1 \bmod 10 && \text{\# by lemma} \\
257^8 &\equiv 1^2 \bmod 10 && \text{\# by 2.19(3)} \\
257^{16} &\equiv 1^4 \bmod 10 && \text{\# by 2.19(3)} \\
257^{32} &\equiv 1^8 \bmod 10 && \text{\# by 2.19(3)} \\
257^{64} &\equiv 1^{16} \bmod 10 && \text{\# by 2.19(3)} \\
257^{128} &\equiv 1^{32} \bmod 10 && \text{\# by 2.19(3)} \\
257^{256} &\equiv 1^{64} \bmod 10 && \text{\# by 2.19(3)} \\
257^{256} &\equiv 1 \bmod 10 && \text{\# } 1^{64} = 1 \quad ■
\end{aligned}$$

*Fairly obvious, so we won't require this for full marks.

4. **[7 marks] remainders**

(a) **[1 mark]** Prove:

$$\exists x \in [0, 34], x \equiv 3 \bmod 5 \wedge x \equiv 5 \bmod 7$$

Solution

discussion: I can just check the 35 integers 0, ..., 34 and find one that works.

header: Let $x = 33$. WTS $x \equiv 3 \bmod 5 \wedge x \equiv 5 \bmod 7$.

body:

$$\begin{aligned} & 5 \mid (33-3) \wedge 7 \mid (33-5) \\ & 33 \equiv 3 \bmod 5 \wedge 33 \equiv 5 \bmod 7 \# \text{ definition of congruence} \\ & x \equiv 3 \bmod 5 \wedge x \equiv 5 \bmod 7 \quad \blacksquare \end{aligned}$$

(b) **[1 mark]** Prove:

$$\exists m_1, m_2 \in \mathbb{Z}, (m_1 \times 7) + (m_2 \times 11) = 1$$

... by finding suitable values for m_1 and m_2.

Solution

discussion: I experiment with multiples of 7 and 11 to find a pair that are within 1 of each other: 21 and 22 will do!

header: Let $m_1 = -3$ and let $m_2 = 2$. WTS $m_1 7 + m_2 11 = 1$.

body:

$$m_1 7 + m_2 11 \;=\; (-3)7 + (2)11 = -21 + 22 = 1 \quad \blacksquare$$

(c) **[2 marks]** Assume that m_1, m_2 are integers such that $(m_1 \times 7) + (m_2 \times 11) = 1$. Prove:

$$\forall a_1, a_2 \in \mathbb{Z}, (a_2 \times m_1 \times 7) + (a_1 \times m_2 \times 11) \equiv a_2 \bmod 11$$

Solution

translation:

$$\forall m_1, m_2 \in \mathbb{Z}, m_1 7 + m_2 11 = 1 \Rightarrow \forall a_1, a_2 \in \mathbb{Z}, a_2 m_1 7 + a_1 m_2 11 \equiv a_2 \bmod 11$$

discussion: Since the first term has a factor $m_1 7$, I will try to add and then subtract $m_2 11$, based on the assumed linear combination, to see if I can isolate a_2.

header: Let $m_1, m_2 \in \mathbb{Z}$. Assume $m_1 7 + m_2 11 = 1$. Let $a_1, a_2 \in \mathbb{Z}$. WTS $a_2 m_1 7 + a_1 m_2 11 \equiv a_2 \bmod 11$.

body:

$$\begin{aligned}
a_2 m_1 7 + a_1 m_2 11 &= a_2(m_1 7 + m_2 11 - m_2 11) + a_1 m_2 11 \\
&\qquad \text{\# by assumption } m_1 7 + m_2 11 = 1 \\
&= a_2 - a_2 m_2 11 + a_1 m_2 11 \\
&= a_2 + (a_1 - a_2) m_2 11 \\
a_2 m_1 7 + a_1 m_2 11 - a_2 &= (a_1 - a_2) m_2 11 \\
& \quad 11 \mid (a_2 m_1 7 + a_1 m_2 11 - a_2) \\
&\qquad \text{\# definition of divides} \\
a_2 m_1 7 + a_1 m_2 11 &\equiv a_2 \bmod 11 \quad \blacksquare
\end{aligned}$$

(d) **[3 marks]** Prove that if p_1, p_2 are any two distinct primes and a_1, a_2 are any two integers, then there is some integer x such that $x \equiv a_1 \bmod p_1$ and $x \equiv a_2 \bmod p_2$. **Hint:** Note that $\gcd(p_1, p_2) = 1$, read the material on gcd in the course notes, and read the previous part of this question.

Solution

translation:

$$\forall p_1, p_2, a_1, a_2 \in \mathbb{Z}, Prime(p_1) \wedge Prime(p_2) \wedge p_1 \neq p_2 \Rightarrow \exists x \in \mathbb{Z}, x \equiv a_1 \bmod p_1 \wedge x \equiv a_2 \bmod p_2$$

discussion: The structure is identical to the previous question if I substitute p_1 for 7 and p_2 for 11.

I also know that, since $\gcd(p_1, p_2) = 1$ there are integers m_1 and m_2 so that $m_1 p_1 + m_2 p_2 = 1$.

header: Let $p_1, p_2, a_1, a_2 \in \mathbb{Z}$. Assume $Prime(p_1) \wedge Prime(p_2) \wedge p_1 \neq p_2$. WTS:

$$\exists x \in \mathbb{Z}, x \equiv a_1 \bmod p_1 \wedge x \equiv a_2 \bmod p_2$$

body:

$$\begin{aligned}
p_1 > 1 \wedge p_2 > 1 &\qquad \text{\# definition of } Prime(p_1), Prime(p_2) \\
p_1 \nmid p_2 \wedge p_2 \nmid p_1 &\qquad \text{\# } p_1 \neq 1 \neq p_2 \wedge p_1 \neq p_2 \\
&\qquad\quad \wedge \text{ definition of } Prime(p_1), Prime(p_2) \\
\gcd(p_1, p_2) = 1 &\qquad \text{\# only possible divisor left} \\
\exists m_1, m_2 \in \mathbb{Z}, m_1 p_1 + m_2 p_2 = 1 &\qquad \text{\# Course Notes, p. 56} \\
\text{Let } x = a_2 m_1 p_1 + a_1 m_2 p_2 &
\end{aligned}$$

$$\begin{aligned}
x - a_2 &= a_2(m_1 p_1 + m_2 p_2 - m_2 p_2) + a_1 m_2 p_2 - a_2 \\
&= a_2 - a_2 m_2 p_2 + a_1 m_2 p_2 - a_2 \qquad \text{\# } m_1 p_1 + m_2 p_2 = 1 \\
x - a_2 &= (a_1 - a_2) m_2 p_2 \\
& \quad p_2 \mid x - a_2 \qquad \text{\# there's a factor of } p_2 \\
& \quad x \equiv a_2 \bmod p_2 \qquad \text{\# definition of congruence} \\
x \equiv a_1 \bmod p_1 & \qquad \text{\# swap roles of } a_1, p_1 \text{ with } a_2, p_2 \text{ in algebra above} \\
& \quad \blacksquare
\end{aligned}$$