CSC165H1: Problem Set 1 Sample Solutions

Due October 4 before 10 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. **[4 marks] Truth tables and formulas.** Consider the following formula:

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

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

Solution

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

(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

$$\begin{aligned} (p \vee q) \Rightarrow r &\equiv \neg(p \vee q) \vee r && \text{(equivalence from class)} \\ &\equiv (\neg p \wedge \neg q) \vee r && \text{(DeMorgan's Law)} \end{aligned}$$

2. **[10 marks] congruence**

Find a natural number m congruent to 5 (mod 7), and another natural number n congruent to 2 (mod 7). Find what the product mn is congruent to (mod 7), and then make a statement about the congruence of the product of any pairs of natural numbers that have the same congruences as the m and n you found, (mod 7).

(a) **[5 marks]** Write a predicate formula that expresses your statement in the form of a universally quantified implication. If you believe the statement, prove it true. If you disbelieve the statement, prove it false.

Solution

This statement is true:

$$\forall m, n \in \mathbb{N}, [m \equiv 5 \pmod 7 \wedge n \equiv 2 \pmod 7] \Rightarrow mn \equiv 3 \pmod 7$$

Proof: Let $m, n \in \mathbb{N}$. Assume $m \equiv 5 \pmod 7$ and $n \equiv 2 \pmod 7$, in other words there are $k_1, k_2 \in \mathbb{Z}$ such that $7k_1 = m - 5$ and $7k_2 = n - 2$. Let k_1 and k_2 be such values. Let $k_3 = 7k_1k_2 + 2k_1 + 5k_2 + 1$. I need to show that $7 \mid (mn - 3)$, which I'll do by showing that $7k_3 + 3 = mn$:

$$\begin{aligned} 7k_3 + 3 &= 49k_1k_2 + 14k_1 + 35k_2 + 10 \\ &= (7k_1 + 5)(7k_2 + 2) = mn \quad \blacksquare \end{aligned}$$

Another statement, taking into account that m and n might change rôles, is

$$\forall m, n \in \mathbb{N}, [m \equiv 5 \pmod 7 \wedge n \equiv 2 \pmod 7] \vee [n \equiv 5 \pmod 7 \wedge m \equiv 2 \pmod 7] \Rightarrow mn \equiv 3 \pmod 7$$

(b) **[5 marks]** Write the converse of your formula from the previous part. If you believe the converse, prove it true. If you disbelieve the converse, prove it false.

Solution

The converse is false:

$$\forall m, n \in \mathbb{N}, mn \equiv 3 \pmod 7 \Rightarrow [m \equiv 5 \pmod 7 \wedge n \equiv 2 \pmod 7]$$

I prove that the negation is true:

$$\exists m, n \in \mathbb{N}, mn \equiv 3 \pmod 7 \wedge [m \not\equiv 5 \pmod 7 \vee n \not\equiv 2 \pmod 7]$$

Proof: Let $m = 1$ and $n = 3$. Then $7 \times 0 = mn - 3$, so $mn \equiv 3 \pmod 7$. However $7 \nmid m - 5$, so $m \not\equiv 5 \pmod 7$ $\blacksquare$.

3. **[4 marks] one-to-one pigeonholes**

The **pigeonhole principle** says, informally, that if n pigeons roost in fewer than n pigeonholes, at least one pigeonhole will be crowded with more than 1 pigeon.

To make this precise, we first formalize the notion of un-crowded for $f : D \mapsto R$:

OneToOne(f): $\forall x, y \in D, x \neq y \Rightarrow f(x) \neq f(y)$, where $f : D \mapsto R$, $|D|, |R| \in \mathbb{N}^+$.

Let $F = \{f \mid f : D \mapsto R \wedge |D| > 0 \wedge |R| > 0\}$ The pigeonhole principle says that:

$$\forall f \in F, \text{OneToOne}(f) \Rightarrow |D| \leq |R|$$

(a) **[4 marks]** Use the pigeonhole principle to prove that if $n \geq 2$ people go to the same party, there are at least 2 people who shake hands with the same number of other people. **Hint**: Take the set of people at the party as your domain, define a function that evaluates how many people each person shook hands with.

Solution

I'll use the contrapositive of the pigeonhole principle, since it seems convenient:

$$\forall f \in F, |R| < |D| \Rightarrow \neg \text{OneToOne}(f)$$

Proof: Let D be the set of people at a party, let $f(d)$ be the number of other people $d \in D$ shakes hands with, and let $R = \{f(d) \mid d \in D\}$. Assume $|D| \geq 2$. I need to show that $|R| < |D|$ There are two extreme cases to consider:

Case 1, where at least one person shakes hands with nobody: Since $|D| \geq 2$, having one person refuse to shake hands reduces each person's possible handshake partners from $|D| - 1$ to $|D| - 2$. Thus the values in R range from a minimum of 0 to no more than $|D| - 2$, and $|R| \leq |D| - 1 < |D|$. This means that, by the pigeonhold principle, f is not 1–1 so there must be a pair of people who shake hands with the same number of other people.

Case 2, every person shakes hands with at least one other person: $|D| \geq 2$, so each person takes part in at least one handshake. In this case the values in R range from a minimum of 1 to no more than $|D| - 1$, so again $|R| \leq |D| - 1 < |D|$. Thus, by the pigeonhole principle f is not 1–1 so there must be a pair of people who shake hands with the same number of people.

In both cases our claim is verified. ■

You may also use the pigeonhole principle in subsequent questions in this assignment.

4. **[21 marks] modular arithmetic with primes**

Let a, p be natural numbers with p prime and $\gcd(a, p) = 1$. Let $T = \{1, \ldots, p - 1\}$, the positive integers less than p.

Define $r_p(x)$ as the remainder after division of x by p.

Prove each of the following claims. You may use the result of an earlier claim to help prove a later claim, for example Claim (e) might help prove Claim (f). You may even use an earlier claim you haven't proven to help prove a later claim.

(a) **[3 marks] Claim:** $\{r_p(an) \mid n \in T\} \subseteq T$. **Hint:** Consider the material in *Characterizations* in the course notes.

Solution

Proof: Let a, p, and T be as defined above, and assume $\gcd(a, p) = 1$. Let n be an arbitrary, fixed element of T. By the Quotient-Remainder Theorem $r_p(an)$ is a natural number less than p. It is enough for me to show that $r_p(an) \neq 0$ to establish that $r_p(an) \in T$.
By the definition of remainder in the Quotient-Remainder Theorem, $p \mid (an - r_p(an))$. Since $\gcd(a, p) = 1$, $p \nmid a$, and since $1 \leq n < p$, $p \nmid n$. Together $p \nmid a \wedge p \nmid n$ imply, by Example 2.14, $p \nmid an$, and so $r_p(an) \neq 0$. ■

(b) **[3 marks] Claim:** If n_1 and n_2 are distinct numbers in T, then $r_p(an_1) \neq r_p(an_2)$. **Hint:** Consider the material in *Characterizations* in the course notes.

Solution

Proof: Let a, p, and T be as defined above, and assume $\gcd(a,p) = 1$. Let $n_1, n_2 \in T$, and assume $n_1 > n_2$. I must show that $r_p(an_1) \neq r_p(an_2)$.
By Example 2.14, $an_1 \equiv r_p(an_1) \pmod p$ and $an_2 \equiv r_p(an_2) \pmod p$, so $(an_1 - an_2) \equiv (n_1 - n_2) \pmod p$. Then

$$\begin{aligned} p \nmid a \wedge p \nmid (n_1 - n_2) &\Rightarrow p \nmid a(n_1 - n_2) \\ &\qquad \text{(Example 2.14, since } \gcd(a,p) = 1 \text{ and } p > n_1 - n_2 > 0) \\ &\Rightarrow a(n_1 - n_2) \not\equiv 0 \pmod p \\ &\Rightarrow an_1 - an_2 \not\equiv 0 \pmod p \\ &\Rightarrow r_p(an_1) - r_p(an_2) \not\equiv 0 \pmod p \\ &\Rightarrow r_p(an_1) \neq r_p(an_2) \quad \blacksquare \end{aligned}$$

(c) **[3 marks] Claim:** $|\{r_p(an) \mid n \in T\}| = |T|$.

Solution

Proof: Let a, p and T be as defined above, and assume $\gcd(a,p) = 1$. Let $T' = \{r_p(an) \mid n \in T\}$, and $f : T \mapsto T'$ be defined by $f(n) = r_p(an)$.
By part (b), f is 1–1, so by the pigeonhole principle $|T| \leq |T'|$. In part (a) we showed $T' \subseteq T$, so $|T'| \leq |T|$. Taken together $|T| \leq |T'| \wedge |T'| \leq |T| \Rightarrow |T| = |T'|$. $\blacksquare$

(d) **[3 marks] Claim:** $\{r_p(an) \mid n \in T\} = T$. **Hint:** For finite sets A and B if $A \subseteq B$ then $|B| = |B \setminus A| + |A|$.

Solution

Proof: Let a, p, T, and T' be as defined above.
In part (c) we showed that $|T| = |T'|$ and in part (a) we showed that $T' \subseteq T$. Also, $|T| = p - 1$, so T is finite.
That means that $|T \setminus T'| = |T| - |T'| = 0$. Since T is a superset of T' and has no elements other than those in T', $T = T'$. $\blacksquare$

(e) **[3 marks] Claim:** $\Pi_{i=1}^{i=p-1} r_p(ai) = \Pi_{i=1}^{i=p-1} i$.

Solution

Proof: Let a, p, T, and T' be as defined above.
Then $\Pi_{i=1}^{i=p-1} r_p(ai)$ is the product of all elements in T' and $\Pi_{i=1}^{i=p-1} i$ is the product of all elements in T. By part (d) $T = T'$, so the products are the same.

(f) **[3 marks] Claim:** $r_p(a^{p-1}) = 1$. **Hint:** You may assume, as a consequence of Example 2.18, that if for $i \in \{1, 2, \ldots, k\}$ $a_i \equiv b_i \pmod p$, then $\Pi_1^k a_i \equiv \Pi_1^k b_i \pmod p$. You may also assume, as an extension of Example 2.14, that for any $k > 1$, if prime $p \nmid b_1 \wedge p \nmid b_2 \wedge \cdots \wedge p \nmid b_k$, then $p \nmid (b_1 \times b_2 \times \cdots \times b_k)$.

Solution

Proof: Let a, p, T, and T' be as defined above. I need to show that $a^{p-1} \equiv 1 \pmod{p}$, in other words that $p \mid (a^{p-1} - 1)$.
By the Quotient-Remainder Theorem $r_p(ai) \equiv ai \pmod{p}$, so as a consequence of Example 2.18

$$\begin{aligned}
\Pi_{i=1}^{p-1} i &\equiv \Pi_{i=1}^{p-1} r_p(ai) \pmod{p} && \text{(shown equal in part (e))} \\
&\equiv \Pi_{i=1}^{p-1} ai \pmod{p} && \text{(consequence of 2.18)} \\
&\equiv a^{p-1} \Pi_{i=1}^{p-1} i \pmod{p} && \text{(factor out } a\text{)} \\
\Pi_{i=1}^{p-1} i &\equiv a^{p-1} \Pi_{i=1}^{p-1} i \pmod{p} \\
&\Rightarrow p \mid (a^{p-1} \Pi_{i=1}^{p-1} i - \Pi_{i=1}^{p-1} i) \\
&\Rightarrow p \mid (a^{p-1} - 1) \Pi_{i=1}^{p-1} i \\
p \nmid \Pi_{i=1}^{p-1} i &\Rightarrow p \mid (a^{p-1} - 1) \\
&\quad \text{(Generalization of Example 2.14 to more than 2 factors)} \quad \blacksquare
\end{aligned}$$

(g) **[3 marks] Claim:** If a is an arbitrary natural number that isn't divisible by 5, then $r_5(a^{100}) = 1$.

Solution

Proof: Let a be as defined above. I must show that $a^{100} \equiv 1 \pmod{5}$.
By part (f) $a^4 \equiv 1 \pmod{5}$. As a consequence of Example 2.18 $a^{100} \equiv (a^4)^{25} \equiv 1^{25} \equiv 1 \pmod{5}$. $\blacksquare$

5. **[6 marks] primes**

Since, as shown in the course notes, there are infinitely many primes, it is not possible for a consecutive sequence of composite (non-prime) natural numbers to stretch on forever. However, arbitrarily long prime-free sequences exist. On the other hand, for any natural number we can always set an upper bound on how far away the next prime can be.

Prove each of the following statements. You may use the Prime predicate.

(a) **[3 marks] Claim:** For any $k \in \mathbb{N}$ there is some $n \in \mathbb{N}$ such that $n, n+1, \ldots, n+k$ are composite. **Hint:** Think about $(k+2)!$.

Solution

Proof: Let $k \in \mathbb{N}$. Let $n = (k+2)! + 2$ and let $i \in \mathbb{N}, i \leq k$. I must show that $n + i$ is composite, that is it has a divisor different from themself and 1.
By construction $i + 2$ is one of the factors of $(k+2)!$, so $(i+2) \mid (k+2)!$, and thus (by linear combinations of multiples) $(i+2) \mid [(k+2)! + (i+2)]$ and $(k+2)! + (i+2) = n + i$.

Also by construction:

$$\begin{aligned} 0 &\leq i \\ 2 &\leq i+2 \\ 1 &< i+2 \\ i &\leq k \\ i+2 &\leq (k+2) \leq (k+2)! \qquad (\text{Since } k+1 \geq 1) \\ i+2 &< (k+2)!+2 = n \end{aligned}$$

This shows that $n+i$ has divisor $i+2$ and $1 < i+2 < n$. ■

(b) **[3 marks] Claim:** For any positive natural number n there exists a prime p with $n < p < n!+2$. **Hint:** Think about $n!$, and the proof of Theorem 2.3, that there are infinitely many primes.

Solution

Proof: Let $n \in \mathbb{N}^+$. Since $n!+1 > 1$, there must be some prime $p \mid n!+1$* Let p be such a prime.

Then $p \nmid n!$, since otherwise we'd have $p \mid (n!+1-n!)$, and the only divisor of 1 is itself.

Since $p \nmid n!$ $p \notin \{1, \ldots, n\}$ and $p > n$. Since $p \mid n!+1$, $p \leq n!+1$. Thus $n < p < n!+2$.

■

*Every integer greater than 1 has at least one prime factor.