Staff Solutions to Conflict Midterm Exam April 5

Problem 1 (GCD) (12 points).
Use the Euclidean Algorithm to prove that
\[ \gcd(13a + 8b, 5a + 3b) = \gcd(a, b). \]

Solution.
\[
\begin{align*}
gcd(13a + 8b, 5a + 3b) &= gcd(5a + 3b, 3a + 2b) \\
&= gcd(3a + 2b, 2a + b) \\
&= gcd(2a + b, a + b) \\
&= gcd(a, a + b) \\
&= gcd(a, b) \\
&= gcd(1a, 1) \\
&= gcd(a, b)
\end{align*}
\]

Problem 2 (Congruence) (15 points).
Assume that
\[ a \equiv b \pmod{n}, \]
where \( n > 1 \) and \( a \) and \( b \) are integers.

STAFF NOTE: 5 points for each part.

(a) For what positive integer value(s) of \( k \) does \( 2a \equiv 2b \pmod{kn} \) hold?

Solution. Only for \( k = 1, 2 \) are the only values that work for all \( a, b, n \).

(b) For what positive integer value(s) of \( k \) does \( a^k \equiv b^k \pmod{n} \) hold? For what values are the two statements equivalent (remember that for the two statements to be equivalent both directions of implications must hold)?

Solution. The statement holds for all positive integer \( k \), but the two statements are equivalent only in the trivial case where \( k = 1 \).
(e) Is this equivalent to saying that \( \gcd(a, n) = \gcd(b, n) \)? Either show the equivalence or give a counterexample.

**Solution. Not equivalent.**

There is a one-way implication: if \( a \equiv b \pmod{n} \), then the \( \gcd \)'s are equal, but the converse fails. For example,

\[
gcd(3, 11) = gcd(7, 11) = 1 \quad \text{but} \quad 3 \not\equiv 7 \pmod{11}.
\]

---

**Problem 3** (Congruence) (13 points).

The sum of the digits of the base 10 representation of an integer is congruent modulo 9 to that integer. For example,

\[
763 \equiv 7 + 6 + 3 \pmod{9}.
\]

We can say that “9 is a good modulus for base 10.”

More generally, we’ll say “\( k \) is a good modulus for base \( b \)” when, for any nonnegative integer \( n \), the sum of the digits of the base \( b \) representation of \( n \) is congruent to \( n \) modulo \( k \). So 2 is not a good modulus for base 10 because

\[
763 \not\equiv 7 + 6 + 3 \pmod{2}.
\]

**STAFF NOTE:** parts a,b,c,d worth 2,3,5,3 points.

(a) What integers \( k > 1 \) are good moduli for base 10?

**Solution.** 3 and 9.

(b) Show that if \( b \equiv 1 \pmod{k} \), then \( k \) is good for base \( b \).

**Solution.**

\[
d_m \cdot b^m + d_{m-1} \cdot b^{m-1} + \cdots + d_1 \cdot b^1 + d_0 \cdot b^0 \\
\equiv d_m \cdot 1^m + d_{m-1} \cdot 1^{m-1} + \cdots + d_1 \cdot 1^1 + d_0 \cdot 1^0 \pmod{k} \\
= d_m + d_{m-1} + \cdots + d_1 + d_0.
\]

(c) Prove conversely, that if \( k \) is good for some base \( b \geq 2 \), then \( b \equiv 1 \pmod{k} \).

**Hint:** Try \( n = b \).

**Solution.** For \( n = b \), the base \( b \) representation of \( n \) is \( 10 \) so if \( k \) is a good modulus for base \( b \) we have

\[
n \equiv 1 + 0 \pmod{k},
\]

that is,

\[
b \equiv 1 \pmod{k}.
\]
(d) Exactly which integers $k > 1$ are good moduli for base 85?

Solution. 2,3,4,6,7,12,14,21,28,42,84

Problem 4 (Scheduling) (18 points).
A tennis tournament among a set of players consists of a series of two-player matches. Usually the objective is to determine a single best player. The organizers of the Math for Computer Science tournament want to do more: they want to find a linear ranking of all the players. To avoid controversy, they want to avoid the awkward situation of having a sequence of players each of whom beats the next player in the sequence and then having last player beat the first. So the organizers will keep a running record of who beat whom during the tournament, and they never allow simultaneous matches whose outcomes could lead to an awkward situation.

Knowledge of binary relations can help the organizers in arranging the tournament. Namely, at any stage of the tournament, the organizers have a record of who lost to whom. Mathematically, we can say that there is a binary relation, $L$, on players where $p \mathrel{L} q$ means that player $p$ lost a match to player $q$. No awkward situations means that the positive length walk relation, $L^+$, is a strict partial order. Indicate which of the following partial order concepts correspond to the properties (a)–(j) of the partial order $L^+$.

<table>
<thead>
<tr>
<th>Partial Order Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>comparable</td>
</tr>
<tr>
<td>incomparable</td>
</tr>
<tr>
<td>maximum</td>
</tr>
<tr>
<td>maximal</td>
</tr>
<tr>
<td>minimum</td>
</tr>
<tr>
<td>minimal</td>
</tr>
<tr>
<td>a chain</td>
</tr>
<tr>
<td>an antichain</td>
</tr>
<tr>
<td>reflexive</td>
</tr>
<tr>
<td>irreflexive</td>
</tr>
<tr>
<td>asymmetric</td>
</tr>
<tr>
<td>a topological sort</td>
</tr>
<tr>
<td>a linear order</td>
</tr>
</tbody>
</table>

STAFF NOTE: -2pts for each wrong answer.

(a) An unbeaten player so far is a **maximal** element.

(b) A player who has lost every match he was in is a **minimal** element.

(c) A player who is sure to rank first at the end of the tournament is a **maximum** element.

(d) A set of players whose rankings relative to each other are unique is a **chain**.

(e) Two players can be matched in the next stage of the tournament only if they are **incomparable** elements.

(f) The final ranking at the end of the tournament will be a **topological sort**.

(g) No more matches are possible if and only if $L^+$ is a **linear order**.

(h) A set of players any two of whom could be paired up to play the next match is an **antichain**.

(i) The fact that no player loses to himself corresponds to $L^+$ being **irreflexive**.

(j) If there are 256 players, what is the smallest number of matches that could possibly have been played in a completed tournament?

Solution. **255**.
Problem 5 (Partial Orders/Scheduling) (16 points).
Answer the following questions about the powerset, \( \text{pow}(\{1, 2, 3, 4\}) \), partially ordered by the strict subset relation \( \subset \).

STAFF NOTE: parts a,b,c,d worth 3,4,4,5 points

(a) Give an example of a maximum length chain.

Solution.

\[ \emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}, \{1, 2, 3, 4\}. \]

(b) Give an example of an antichain of size 6.

Solution.

\[ \{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 3\}, \{2, 4\}, \{1, 4\}. \]

(c) Describe an example of a topological sort of \( \text{pow}(\{1, 2, 3, 4\}) \).

Solution. The empty set, followed by the four 1-element sets in any order, followed by the six 2-element sets in any order, followed by the four 3-element sets in any order followed by \( \{1, 2, 3, 4\} \).

(d) Suppose the partial order describes scheduling constraints on 16 tasks. That is, if

\[ A \subset B \subseteq \{1, 2, 3, 4\}, \]

then \( A \) has to be completed before \( B \) starts.\(^1\) What is the length of a minimum time 3-processor schedule?

Solution. 7. For example, a length-7 3-processor schedule is:

\[ \emptyset \]

\[ 1, 2, 3 \]

\[ 4, 12, 23 \]

\[ 34, 14, 24 \]

\[ 13, 124, 234 \]

\[ 123, 134 \]

\[ 1234. \]

Moreover, no shorter schedule is possible: there is a unique minimum task, \( \emptyset \), which must come first and a unique maximum task, \( \{1, 2, 3, 4\} \), which must come last; this leaves 14 tasks which require at least 

\[ \left\lceil 14/3 \right\rceil = 5 \]

more parallel steps.

Problem 6 (Simple Graphs) (10 points).
Among connected simple graphs whose sum of vertex degrees is 26:

\(^1\) As usual, we assume each task requires one time unit to complete.
STAFF NOTE: a,b worth 5 points each.
  part a answer “13” gets −4.

(a) what is the largest possible number of vertices?

Solution. 14.
With total degree 26 there are 13 edges. The largest number of vertices in a connected graph with 13 edges
is a tree with 14 vertices.

(b) what is the smallest possible number of vertices?

Solution. 6.
A complete graph has the largest possible number of edges for a given number of vertices. The complete
graph $K_6$ has 15 edges, so by deleting two edges one can get a connected graph with 13 edges.
The complete graph $K_5$ has 10 edges, which is too small.

Problem 7 (Partial Orders/Chains) (16 points).
Let $R$ be a weak partial order on a set, $A$. Suppose $C$ is a finite chain.\(^2\)

(a) Prove that $C$ has a maximum element. Hint: Induction on the size of $C$.

Solution. As hinted, we give a proof by induction on the size of $C$.

Proof. The induction hypothesis is:

$$P(n) := \text{If } C \text{ is a chain of size } n, \text{ then } C \text{ has a maximum element.}$$

Base case: ($n = 1$). The one element is $C$ is the maximum (and also minimum) element, by definition
of maximum.

Induction step: To prove $P(n + 1)$ for $n \geq 1$, let $C_{n+1}$ be a chain of size $n + 1$ and let $x$ be an arbitrary
element in $C_{n+1}$. Then $C_{n+1} \setminus \{x\}$ is a chain of size $n$, so it has a maximum element $m$ by induction
hypothesis. Now compare $x$ and $m$. If $x R m$, then $m$ is the3 maximum element in $C_{n+1}$. On the other
hand, $m R x$, then (by transitivity of $R$), $x$ is a maximum element of $C_{n+1}$. In any case, $C_{n+1}$ has a
maximum element, which proves $P(n + 1)$.

(b) Conclude that there is a unique sequence of all the elements of $C$ that is strictly increasing.
Hint: Induction on the size of $C$, using part (a).

Solution. As hinted, we give a proof by induction on the size of $C$.

Proof. The induction hypothesis is:

$$Q(n) := \text{If } C \text{ is a chain of size } n, \text{ then there is a unique sequence of all the elements of } C \text{ that is}
\text{strictly increasing.}$$

\(^2\)A set $C$ is a chain when it is nonempty, and all elements $c, d \in C$ are comparable. Elements $c$ and $d$ are comparable iff $[c R d \text{ or } d R c]$.\(^3\)
**Base case:** $(n = 1)$. Immediate.

**Induction step:** To prove $Q(n + 1)$ for $n \geq 1$, let $C_{n+1}$ be a chain of size $n + 1$. By part (a), $C_{n+1}$ has a maximum element, $m$. Then $C_{n+1} - \{m\}$ is a chain of size $n$, so there is a unique strictly increasing sequence, $C_{n+1} - \{m\}$, of all the elements of $C_{n+1} - \{m\}$. Then $C_{n+1} - \{m\}$ followed by $m$ is a strictly increasing sequence of the elements of $C_{n+1}$. Moreover, this sequence is unique, because any strictly increasing sequence elements in $C_{n+1}$ can only consist of a strictly sequence of elements in $C_{n+1} - \{m\}$, which is unique by hypothesis, followed by $m$. ■