Staff Solutions to Midterm Exam April 7

Problem 1 (Modular arithmetic) (20 points).
In this problem, we will construct a simple test for divisibility by 11.

(a) Explain why
\[
\text{rem}(10^n, 11) = \begin{cases} 
1 & \text{if } n \text{ is even,} \\
\text{rem}(-1, 11) & \text{if } n \text{ is odd,}
\end{cases}
\]
for all nonnegative integers \(n\).

**Solution.**
\[10^n \equiv -1 \pmod{11}\] and since congruence is preserved under product, \[10^n \equiv (-1)^n \pmod{11}\]. Hence \(\text{rem}(10^n, 11) = \text{rem}((-1)^n, 11)\).

(b) Take a big number, such as 47262938151. Sum the digits, where every other digit is negated:
\[4 + (-7) + 2 + (-6) + 2 + (-9) + 3 + (-8) + 1 + (-5) + 1 = -22.\]
Explain why the original number is a multiple of 11 if and only if this sum is a multiple of 11. For example, this number 47262938151 is divisible by 11 since -22 is divisible by 11.

**Solution.** A number in decimal has the form:
\[d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0\]
By part (a),
\[d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0\]
\[\equiv d_k \cdot 1 + d_{k-1} \cdot (-1) + \ldots + d_1 \cdot (-1) + d_0 \cdot 1 \pmod{11}\]
\[= d_k - d_{k-1} + \ldots - d_1 + d_0\]
when \(k\) is even. The case where \(k\) is odd is the same with the signs reversed.
So the procedure given in the problem computes \pm\ this alternating sum of digits. In particular, the original number is congruent to zero mod 11 iff the alternating sum is congruent to zero mod 11, which is the same as being divisible by 11.

Problem 2 (Number theory and RSA) (20 points).
Indicate whether the following statements are true or false by circling T or F. Provide a brief argument justifying your choice for each statement.

(a) Let \(n\) and \(a\) be positive integers. If \(n\) and \(a\) are relatively prime, then
\[a^{\phi(n)^2} \equiv 1 \pmod{n}.\]

T  F

---

2014, Eric Lehman, F Tom Leighton, Albert R Meyer. This work is available under the terms of the Creative Commons Attribution-ShareAlike 3.0 license.
Solution. True. Euler’s Theorem states that if \( n \) and \( a \) are relatively prime, then \( a^{\phi(n)} \equiv 1 \pmod{n} \). Raising both sides to the \( \phi(n)^{\text{th}} \) power, we get that
\[
a^{(\phi(n))^2} = \left(a^{\phi(n)}\right)^{\phi(n)} \equiv 1^{\phi(n)} = 1 \pmod{n}.
\]

(b) If \( n \) is a product of two distinct primes, then \( \phi(n) \) is even. T F

Solution. True. Let \( n = pq \) for primes \( p, q \). Then, \( \phi(n) = \phi(p)\phi(q) = (p-1)(q-1) \). Since 2 is the only even prime, at least one of \( p \) and \( q \) must be odd, so at least one of \( p-1 \) and \( q-1 \) must be even. Therefore, \( (p-1)(q-1) \) must be even.

(c) Suppose \( a, b, c, d \) are any four positive integers and \( ac \equiv bc \pmod{d} \). Then
\[
a \equiv b \pmod{d}.
\]
T F

Solution. False. To cancel \( c \), we require that \( c \) is relatively prime to \( d \). A counter-example is \( a = 1, b = 2, d = 3, \) and \( c = 6 \).

(d) An efficient algorithm for FACTORING would render RSA insecure. T F

Solution. True. An eavesdropper could find the private key from the factorization of \( n \) in the public key in the same way that the RSA Receiver does. Namely, an eavesdropper could use the efficient factoring algorithm as follows: from the public key \((n, d)\), calculate the prime factors \( p \) and \( q \) of \( n \), and compute the inverse of \( d \) modulo \( (p-1)(q-1) \) to get the private key \( e \), after which the eavesdropper can decrypt any message transmitted by a sender.

Problem 3 (DAGs and Partial Orders) (20 points).
Let \( G \) be an arbitrary directed acyclic graph with 100 vertices.

(a) What is the size of the largest chain that \( G \) could possibly have? Justify your reasoning.

Solution. 100.
Let \( G \) be a linear order. This gives a chain of size 100.

(b) What is the size of the largest antichain that \( G \) could possibly have? Justify your reasoning.

Solution. 100.
Let \( G \) be the empty graph with 100 vertices (and no edges). This gives an antichain of size 100.

(c) Argue that for any such \( G \), either there is a chain or there is an antichain containing at least 10 vertices.

Solution. Dilworth’s Lemma states that any DAG with \( n \) vertices must have either a chain of size at least \( t \), or an antichain of size at least \( n/t \). Substitute \( n = 100 \) and \( t = 10 \) to obtain the result.

(d) Give an example of \( G \) where the maximum-size chain and the maximum-size antichain both have size 10.
Solution. Partition the vertices $V$ into 10 blocks of 10 vertices each. Linearly order vertices within each block, and leave different blocks disconnected.

The set of all vertices from any one block forms a chain of 10 vertices. Any vertex from another block is incomparable with the vertices we have chosen, and therefore no chain of bigger size is possible.

On the other hand, the length of the maximum-size antichain is also 10. We can construct a set consisting of exactly one vertex from each of the 10 blocks, forming an antichain of 10 vertices. Any set of 11 vertices would have to contain 2 vertices from the same chain, and so would not be an antichain, so no antichain of size bigger than 10 is possible.

Problem 4 (Degree sequences) (20 points).

The degree sequence of a simple graph $G$ with $n$ vertices is the length-$n$ sequence of the degrees of the vertices listed in weakly increasing order. For example, if $G$ is a 4-vertex tree, then its degree sequence is either $(1,1,1,3)$ or $(1,1,2,2)$.

Briefly explain why each of the following sequences is not a degree sequence of any connected simple graph.

(a) $(1,2,3,4,5,6,7)$

Solution. There are only 7 vertices, so the degree of any vertex is at most 6.

(b) $(0,2,2,2,2)$

Solution. There is a vertex with degree 0, and there is more than one vertex, so the graph is not connected.

(c) $(1,3,3,4,4,4)$

Solution. By the Handshaking Lemma, the sum of degrees in any simple graph must be even, which is not true in this case since $1 + 3 + 3 + 4 + 4 + 4 = 19$.

(d) A sequence of $n$ integers whose sum is less than $2n - 2$.

Solution. There are too few edges. The sum of the degrees is twice the number of edges by the Handshaking Lemma 11.2.1. However, the number of edges in any $n$-vertex connected graph is at least $n - 1$ (Corollary 11.9.8). Therefore, the sum of the degrees must be at least $2n - 2$.

Problem 5 (Coloring & Induction) (30 points).

A simple graph, $G$, is said to have width $w$ iff there is a way to list all its vertices so that each vertex is adjacent to at most $w$ vertices that appear earlier in the list. For example, if the degree of every vertex is at most $w$, then the graph obviously has width at most $w$—just list the vertices in any order.

This problem will show that every graph with width $w$ is $(w + 1)$-colorable using induction on the number of vertices in the graph.

(a) Clearly state the Induction Hypothesis, $P(n)$.

Solution. $P(n)$ is the proposition that for all $w \in \mathbb{N}$ and all $n$-vertex graphs $G$ with width $w$, the graph $G$ is $(w + 1)$-colorable.
(b) Prove the base case for $n = 1$.

Solution. Every graph with 1 vertex has width 0 and is $0 + 1 = 1$ colorable. Therefore, $P(1)$ is true. ■

(c) Prove the induction step.

Hint: Remove the last vertex.

Solution. Proof. Assume that $P(n)$ is true for some $n \geq 1$ and let $G$ be an $(n + 1)$-vertex graph with width $w$. We need only show that $G$ is $(w + 1)$-colorable.

Since $G$ has width $w$, the vertices of $G$ can be listed with each vertex adjacent to at most $w$ earlier in the list. Let $v$ be the last vertex in the list, and Let $G'$ be the graph obtained by removing, $v$, and all edges incident to $v$, from $G$.

Now $G'$ has $n$ vertices and still has width $w$ since the sequence $S$ with its last vertex removed is a sequence consisting of all the vertices of $G'$ with each vertex adjacent to exactly the same previous vertices. Therefore, by the Induction Hypothesis, $G'$ is $(w + 1)$-colorable.

We can define a $(w + 1)$-coloring of $G$ as follows: color all the vertices of $G$ besides $v$ using the $(w + 1)$-coloring of $G'$. Since there are at most $w$ colors among the $w$ vertices adjacent to $v$, there will always be one of the $w + 1$ colors that differs from these $w$ colors. So assigning this color to $v$ yields the required $(w + 1)$-coloring of $G$.

This proves $P(n + 1)$ and completes the induction step. ■

Problem 6 (Matching) (20 points). (a) Prove that the bipartite graph $G$ in Figure 1 has no perfect matching by exhibiting a bottleneck in it.

Solution. It is not possible because $\{a, b, c, e\}$ is a bottleneck: $|G(\{a, b, c, e\})| = |\{v, x, y\}| = 3 < 4 = |\{a, b, c, e\}|$. (It is easy to see that there are no bottlenecks with exactly 1, 2, 3, or 5 vertices from $L(G)$.)

Another way to identify a bottleneck is to observe that the $L(G)$ and $R(G)$ are the same size, and so there is a bottleneck on the right iff there is one on the left. So an alternative answer is to observe that $\{w, z\}$ is a bottleneck in the other direction: $|G^{-1}(\{w, z\})| = |\{d\}| = 1 < 2 = |\{w, z\}|$. ■
(b) The bipartite graph $H$ in Figure 2 has an easily verified property that implies it has a matching that covers $L(H)$. Exactly what is the property?

![Figure 2](image-url)

**Figure 2** $H$.

**Solution.** The graph is degree-constrained, and so Theorem 11.5.6 ensure that a matching exists. In particular, each vertex in $L(H)$ has degree at least 3, while each vertex in $R(H)$ has degree at most 3.

One matching, for example, is:

$\langle a-z \rangle, \langle b-w \rangle, \langle c-v \rangle, \langle d-x \rangle$.

Problem 7 (Convergent Series) (20 points).

There is a number $a$ such that

$$\sum_{i=1}^{\infty} i^p$$

converges to a finite value iff $p < a$.

(a) What is the value of $a$?

**Solution.** $-1$.

(b) Circle all of the following that would be good approaches as part of a proof that this value of $a$ is correct.

i. Find a closed form for

$$\int_{1}^{\infty} x^p \, dx.$$ 

ii. Find a closed form for

$$\int_{1}^{\infty} i^p \, dp.$$ 

iii. Induction on $p$.

iv. Induction on $n$ using the following sum

$$\sum_{i=1}^{n} i^p.$$
v. Compare the series term-by-term with the Harmonic series.

Solution. (1) and (5).

(1) is correct because $x^p$ is decreasing in $x$ if $p < 0$ and increasing if $p \geq 0$. So by Theorem 13.3.2, the sum can be approximated by the integral

$$\int_1^\infty x^p \, dx = \begin{cases} \frac{-1}{p+1} & \text{if } p < -1, \\ \infty & \text{if } p \geq -1. \end{cases}$$

So if $p < -1$, Theorem 13.3.2 implies that the sum is bounded above by one plus the integral. Since the sum is increasing, this implies has a finite limit, that is, it converges.

Likewise, the sum is bounded below by the integral, and so diverges if $p \geq -1$.

(5) is correct because for $p = -1$, the sum is the harmonic series which we know diverges. But for $p \geq -1$, the value of $i^p$ increases with $p$, the sum will be larger, and hence also diverge for $p > -1$.

Induction on $n$ is not a plausible approach because ideas from the other approaches would be needed to handle the induction step anyway, at which point the induction would be moot. ■