Final Examination

Your name:_____

- This exam is **closed book** except for a seven side crib sheet (3.5 2-sided pages). Total time is 3 hours.
- Write your solutions in the space provided with your name on every page. If you need more space, write on the back of the sheet containing the problem. Please keep your entire answer to a problem on that problem's page.
- GOOD LUCK!

DO NOT WRITE BELOW THIS LINE

Problem	Points	Grade	Grader
1	15		
2	15		
3	10		
4	10		
5	8		
6	8		
7	6		
8	10		
9	12		
10	6		
11	14		
12	15		
13	24		
14	15		
15	12		
16	20		
Total	200		

Short Answer Questions

Problem 1 (**Number Theory**) (**15 points**).

Circle true or false for the statements below, and *provide counterexamples* for those that are false. Variables, a, b, c, m, n range over the integers and $m, n > 1$.

(a) $\gcd(1 + a, 1 + b) = 1 + \gcd(a, b)$. **true** **false**

(b) If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$. **true** **false**

(c) $\gcd(a^n, b^n) = (\gcd(a, b))^n$ **true** **false**

(d) If $\gcd(a, b) \neq 1$ and $\gcd(b, c) \neq 1$, then $\gcd(a, c) \neq 1$. **true** **false**

(e) If an integer linear combination of a and b equals 1, then so does some integer linear combination of a^2 and b^2. **true** **false**

(f) If an integer linear combination of a and b equals 2, then so does some integer linear combination of a^2 and b^2. **true** **false**

(g) If $ac \equiv bc \pmod{n}$ and n does not divide c, then $a \equiv b \pmod{n}$. **true** **false**

(h) If $a \equiv b \pmod{\phi(n)}$ for $a, b > 0$, then $c^a \equiv c^b \pmod{n}$. **true** **false**

(i) If $a \equiv b \pmod{nm}$, then $a \equiv b \pmod{n}$. **true** **false**

(j) If $\gcd(m, n) = 1$, then $[a \equiv b \pmod{m}$ AND $a \equiv b \pmod{n}]$ iff $[a \equiv b \pmod{mn}]$ **true** **false**

(k) if $\gcd(a, n) = 1$, then $a^{n-1} \equiv b \pmod{n}$ **true** **false**

(l) a has a multiplicative inverse modulo b iff b has a multiplicative inverse modulo a. **true** **false**

Problem 2 (Graphs) (15 points).

(a) Circle all the properties below that are preserved under graph isomorphism.

- There is a simple cycle that includes all the vertices.
- Two edges are of equal length.
- The graph remains connected if any two edges are removed.
- There exists an edge that is an edge of every spanning tree.
- The negation of a property that is preserved under isomorphism.

(b) For the following statements about trees, circle **true** or **false**, and *provide counterexamples* for those that are **false**.

- Any connected subgraph is a tree. **true** **false**

- Adding an edge between two vertices creates a cycle. **true** **false**

- The number of vertices is one less than twice the number of leaves. **true** **false**

- The number of vertices is one less than the number of edges. **true** **false**

- For every finite graph, there is one (a tree) that spans it. **true** **false**

(c) What is the minimum number of vertices possible in a nonplanar graph? _____

(d) What is the minimum number of edges possible in a nonplanar graph that is 2-colorable? _____

(e) A *sink* in a digraph is a vertex with no edges leaving it. Circle whichever of the following assertions are true of stable distributions on finite digraphs with exactly two sinks:

- there may not be any
- there may be a unique one

- there are exacty two
- there may be a countably infinite number
- there may be a uncountable number
- there always is an uncountable number

Problem 3 (Partial orders) (10 points).
For each of the relations below, indicate whether it is

a *weak partial order* (**WPO**), a *strict partial order* (**SPO**),
and if so, whether it is *path-total* (**Tot**)

If it is neither (**WPO**) nor (**SPO**), indicate whether it is

transitive (**Tr**), *symmetric* (**Sym**), *asymmetric* (**Asym**)

(a) The relation $a = b + 1$ between integers, a, b, _____

(b) The superset relation, $\supseteq$ on the power set of the integers. _____

(c) The relation $\text{Ex}[R] < \text{Ex}[S]$ between real-valued random variables R, S. _____

(d) The empty relation on the set of rationals. _____

(e) the divides relation on the positive powers of 4. _____

For the next three parts, let f, g be nonnegative functions from the integers to the real numbers.

(f) the "Big Oh" relation, $f = O(g)$, _____

(g) the "Little Oh" relation, $f = o(g)$, _____

(h) the "asymptotically equal" relation, $f \sim g$. _____

Problem 4 (Big Oh) (10 points).
Recall that if f and g are positive real-valued functions on $\mathbb{N}^+$, then $f = O(g)$ iff there exist $c, n_0 \in \mathbb{Z}^+$ such that

$$\forall n \geq n_o.\ f(n) \leq cg(n).$$

For each pair of functions f and g below, indicate the **smallest** $c \in \mathbb{Z}^+$, and for that smallest c, the **smallest corresponding** $n_0 \in \mathbb{Z}^+$, that would establish $f = O(g)$ by the definition given above. If there is no such c, write ∞.

(a) $f(n) = \frac{1}{2}\ln n^2, g(n) = n.$ $c =$ _____, $n_0 =$ _____

(b) $f(n) = n, g(n) = n \ln n.$ $c =$ _____, $n_0 =$ _____

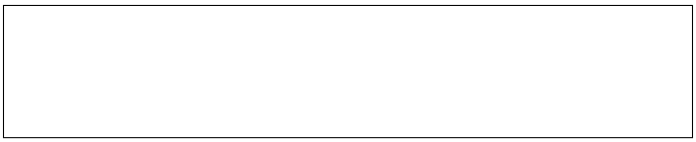
(c) $f(n) = 2^n, g(n) = n^4 \ln n$ $c =$ _____, $n_0 =$ _____

(d) $f(n) = 3\sin\left(\frac{\pi(n-1)}{100}\right) + 2, g(n) = 0.2.$ $c =$ _____, $n_0 =$ _____

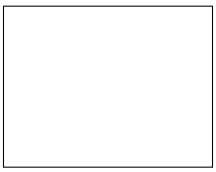
Problem 5 (Preserved Invariant) (8 points).
We describe a state machine for multiplying a real number, x, by a nonnegative integer, y, using only addition, and multiplication and division by 3. The states are triples of numbers (r, s, a) where $s \in \mathbb{N}$. The initial state is $(x, y, 0)$. The transitions are given by the rule that for $s > 0$:

$$(r, s, a) \to \begin{cases} (3r, s/3, a) & \text{if } 3 \mid s \\ (3r, (s-1)/3, a + r) & \text{if } 3 \mid (s-1) \\ (3r, (s-2)/3, a + 2r) & \text{otherwise.} \end{cases}$$

State a preserved invariant that leads to a simple proof that the algorithm is partially correct —that is, if $s = 0$, then $a = xy$.



Problem 6 (Exponential mod n) (8 points).
What is the remainder of 63^{9601} divided by 220?



Problem 7 (Matching) (6 points).
A researcher analyzing data on heterosexual sexual behavior in a group of m males and f females found that within the group, the male average number of female partners was 10% larger that the female average number of male partners.

Circle all of the assertions below that are implied by the above information on average numbers of partners:

- males exaggerate their number of female partners
- $m = (9/10)\, f$
- $m = (10/11)\, f$
- $m = (11/10)\, f$
- there cannot be a perfect matching with each male matched to one of his female partners
- there cannot be a perfect matching with each female matched to one of her male partners

Problem 8 (Counting passwords) (10 points).
A certain company wants to have security for their computer systems. So they have given everyone a password. A length 10 word containing each of the characters:

a, d, e, f, i, l, o, p, r, s,

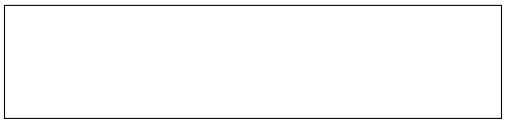
is called a *cword*. A password will be a cword which does not contain any of the subwords "fails", "failed", or "drop".

For example, the following two words are passwords: adefiloprs, srpolifeda,
but the following three cwords are not: a**drop**eflis, **failedrop**s, **drop**e**fails**.

(a) How many cwords contain the subword "drop"? _____

(b) How many cwords contain both "drop" and "fails"? _____

(c) Use the Inclusion-Exclusion Principle to find a simple arithmetic formula involving factorials for the number of passwords.



Problem 9 (Counting relations) (12 points).

How many binary relations are there on the set $\{0, 1\}$? _____

How many are there that are:

transitive? _____

asymmetric? _____

reflexive? _____

irreflexive? _____

strict partial orders? _____

weak partial orders? _____

Problem 10 (Quantifiers & Law of Large Numbers) (6 points).
Let $G_1, G_2, G_3, \ldots$, be an infinite sequence of pairwise independent random variables with the same expectation, μ, and the same finite variance. Let

$$f(n,\epsilon) ::= \Pr\left[\left|\frac{\sum_{i=1}^{n} G_i}{n} - \mu\right| \leq \epsilon\right].$$

The Weak Law of Large Numbers can be expressed as a logical formula of the form:

$$\forall \epsilon > 0\, Q_1\, Q_2 \ldots\, [f(n,\epsilon) \geq 1 - \delta]$$

where $Q_1 Q_2 \ldots$ is a sequence of quantifiers from among:

$$\begin{array}{cccccc} \forall n & \exists n & \forall n_0 & \exists n_0 & \forall n \geq n_0 & \exists n \geq n_0 \\ & \forall \delta > 0 & \exists \delta > 0 & \forall \delta \geq 0 & \exists \delta \geq 0 & \end{array}$$

Here the n and n_0 range over natural numbers, and δ and ϵ range over real numbers.

Write out the proper sequence $Q_1 Q_2 \ldots$

Derivation & Proof Questions

Problem 11 (Combinatorial proof) (14 points).
Let S be the set of all length-n sequences of letters a, b, and exactly one c.

(a) Show that the cardinality of S is equal to $n2^{n-1}$.

(b) Show that the cardinality of S is equal to

$$\sum_{k=1}^{n} k\binom{n}{k}.$$

(c) What combinatorial identity now follows?

Problem 12 (Conditional probability) (15 points).
There is a rare and serious disease called Beaver Fever which afflicts about 1 person in 1000. Victims of this disease start telling math jokes in social settings, believing other people will think they're funny.

Doctor Meyer has some fairly reliable tests for this disease. In particular:

- If a person has Beaver Fever, the probability that Meyer diagnoses the person as having the disease is 0.99.
- If a person doesn't have it, the probability that Meyer diagnoses that person as not having Beaver Fever is 0.97.

Let B be the event that a randomly chosen person has Beaver Fever, and Y be the event that Meyer's diagnosis is "Yes, that person has Beaver Fever," with $\overline{B}$ and $\overline{Y}$ the complements of these events.

(a) The description above explicitly gives the values of the following quantities. What are their values?

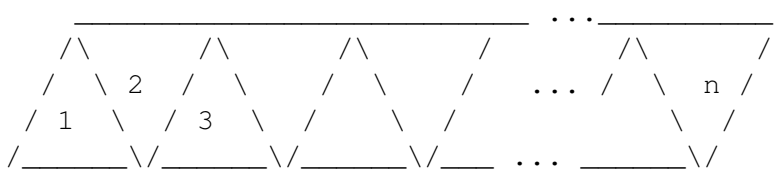
$\Pr[B]$ _____ $\Pr\left[Y \mid B\right]$ _____ $\Pr\left[\overline{Y} \mid \overline{B}\right]$ _____

(b) Write formulas for $\Pr[\overline{B}]$ and $\Pr\left[Y \mid \overline{B}\right]$ solely in terms of the explicitly given expressions. Literally use the expressions, not their numeric values.

(c) Write a formula for the probability that Doctor Meyer says a person has the disease solely in terms of $\Pr[B]$, $\Pr[\overline{B}]$, $\Pr\left[Y \mid B\right]$ and $\Pr\left[Y \mid \overline{B}\right]$.

(d) Write a formula solely in terms of the explicitly given quantities for the probability that a person has Beaver Fever given that Doctor Meyer says the person has it.

Problem 13 (Variance) (24 points).
Let T_n be the graph consisting of n consecutive triangles arranged as follows:



(a) Each edge in T_n is colored red with probability r and blue with probability $b ::= 1 - r$ mutually independently. A triangle is *monochromatic* if its edges are all blue or all red. What is the probability, m, that a particular triangle is monochromatic?

(b) Let I_T be an indicator random variable for the event that a given triangle, T, is monochromatic.

What is $\text{Ex}[I_T]$? What is $\text{Var}[I_T]$?

You may state your answer in terms of the probability, m, from the previous problem part.

(c) Let T and T' be any two different triangles. If the triangles don't share an edge, then the random variables I_T and $I_{T'}$ are obviously independent. Suppose that $r = 1/2$ and T and T' do share an edge. Show that I_T and $I_{T'}$ remain independent in this case.

(d) Let M be the random variable equal to the total number of monochromatic triangles in the graph. If $r = 1/2$, what is $\text{Var}[M]$?

(e) Prove that

$$\lim_{n\to\infty} \Pr[|M - \mathrm{Ex}[M]| \geq n/1000] = 0.$$

Problem 14 (Expectation) (15 points).
You have a process for generating a positive integer, K. The behavior of your process each time you use it is (mutually) independent of all its other uses. You use your process to generate a random integer, and then use your procedure repeatedly until you generate an integer as big as your first one. Let R be the number of additional integers you have to generate.

(a) State and briefly explain a simple formula for $\mathrm{Ex}[R \mid K = k]$ in terms of $\Pr[K \geq k]$.

Suppose $\Pr[K = k] = \Theta(k^{-4})$.

(b) Show that $\Pr[K \geq k] = \Theta(k^{-3})$.

(c) Show that $\mathrm{Ex}[R]$ is infinite.

Problem 15 (Induction) (12 points).
Use strong induction to prove that $n \leq 3^{n/3}$ for every integer $n \geq 0$.

Problem 16 (Structural Induction) (20 points).
The Arithmetic Trig Functions (*Atrig*'s) are the set of functions of one real variable defined recursively as follows:

Base cases:

- The identity function, $\mathrm{id}(x) ::= x$ is an *Atrig*,
- any constant function is an *Atrig*,
- the sine function is an *Atrig*,

Constructor cases:
If f, g are *Atrig*'s, then so are

1. $f + g$
2. $f \cdot g$
3. the composition $f \circ g$.

Prove by Structural Induction on this definition that if $f(x)$ is an *Atrig*, then so is $f' ::= df/dx$.