

**Math 55: Sample Final Exam, 9 December 2009**

- 1:** (a) Compute  $1155^{55} \bmod 17$ .  
(b) Find the smallest positive inverse of  $10 \bmod 17$ .  
(c) State the Chinese Remainder Theorem.  
(d) Use the procedure of the Chinese Remainder Theorem to compute  $1155^{55} \bmod 170$ .  
(e) State Fermat's little Theorem.  
(f) Use Fermat's little Theorem to find the smallest odd prime number which divides  $1155^{55} - 1$ .

- 2:** Choose a *positive* integer solution ( $x_1 > 0, x_2 > 0, x_3 > 0$ ) of

$$x_1 + x_2 + x_3 = 42$$

at random, where each solution has equal probability.

- (a) What is the probability of selecting  $(14, 14, 14)$ ?  
(b) What is the probability that at least one of the  $x$ 's is exactly equal to 20?  
(c) What is the probability that  $x_1 = 10$ , given that  $x_2 = 14$ ?

- 3:** (a) Let  $B$  be the set of finite bit strings

$$B = \{x \mid \exists n \geq 0 (x = b_0b_1b_2 \dots b_n \text{ where } b_i = 0 \text{ or } 1)\}.$$

Is  $B$  finite, countable or uncountable? Why?

- (b) Let  $F$  be the set of all Boolean-valued functions  $f : \mathbf{N} \rightarrow \{0, 1\}$  of a nonnegative integer variable. Is  $F$  finite, countable or uncountable? Why?  
(c) Given any Boolean-valued function  $f$  of a nonnegative integer variable  $n$ , can we always find a C program which accepts input  $n$  and outputs  $f(n)$ ? Why or why not?

- 4:** The cycle  $C_n$  is the simple graph on vertices  $V = \{1, 2, 3, \dots, n\}$  with edges  $E = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \dots, \{n-1, n\}, \{n, 1\}\}$ . The *cocycle*  $\bar{C}_n$  is its complement, with vertices  $\bar{V}$  and edges  $\bar{E}$ . Justify your answer to each of the following questions.

- (a) Determine the cardinality of  $\bar{E}$ .
- (b) For which  $n$  are  $C_n$  and  $\bar{C}_n$  isomorphic?
- (c) For which  $n$  does  $\bar{C}_n$  have an Euler circuit?

5: Define the divisibility relation  $R$  on  $\mathbf{Z}_n = \{1, 2, 3, 4, \dots, n\}$  by  $aRb \leftrightarrow a|b$ .

- (a) Define a partial order and prove or disprove that  $R$  is one.
- (b) Let  $M$  be the matrix of  $R$ . Show that the number  $d(j)$  of divisors of any integer  $j \in \mathbf{Z}_n$  is given by the sum of the entries in column  $j$  of  $M$ :

$$d(j) = \sum_{i=1}^n M_{ij}.$$

- (c) Evaluate  $d(p)$  for any prime  $p \in \mathbf{Z}_n$  and  $d(2^k)$  for any  $2^k \in \mathbf{Z}_n$ .
- (d) Consider the experiment of selecting an integer  $j$  from  $\mathbf{Z}_n$  at random, with equal probabilities. Show that

$$E(d) \leq \sum_{k=1}^n \frac{1}{k}.$$

6: Consider the following algorithm:

```

procedure  $S(a, b : \text{positive integers})$ 
 $c := 1$ 
while  $a \neq b$ 
    if  $a \bmod 2 = b \bmod 2 = 0$ 
         $a := a/2$ 
         $b := b/2$ 
         $c := 2c$ 
    else if  $a \bmod 2 = 0 \wedge b \bmod 2 = 1$ 
         $a := a/2$ 
    else if  $a \bmod 2 = 1 \wedge b \bmod 2 = 0$ 
         $b := b/2$ 
    else
         $d := |a - b|$ 
         $b := \min(a, b)$ 
         $a := d$ 
    end if

```

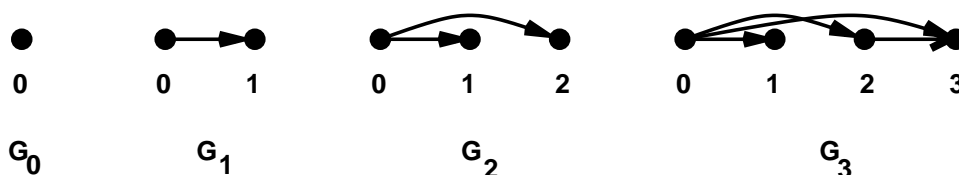
```

end while
return ac
end

```

- (a) What does  $S(38, 14)$  return?
- (b) What function of  $(a, b)$  does  $S$  compute? Justify your answer.
- (c) What is the worst-case complexity of  $S$  in terms of  $a$  and  $b$ ? Justify your answer.

**7:** Define a directed graph  $G_n = (V_n, E_n)$  for nonnegative integers  $n$  as follows.  $G_0$  has one vertex named 0 and no edges. Given  $G_n = (V_n, E_n)$ , we form  $V_{n+1}$  by adding one more vertex  $n + 1$ . The edge set  $E_{n+1}$  is  $E_n$  plus edges  $(j, n + 1)$  for all *even*  $j \in V_n$ . The first few look like this:



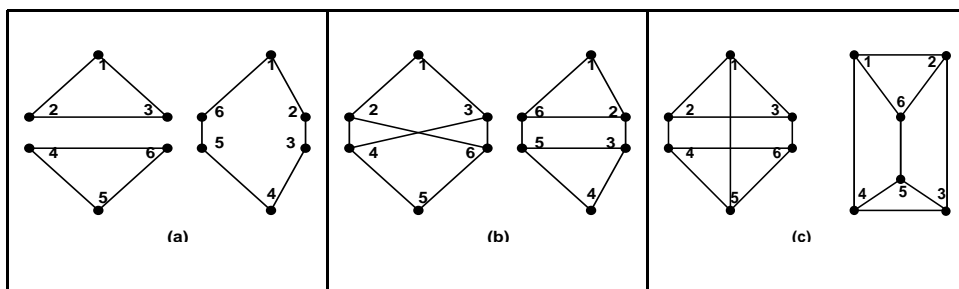
- (a) Find the smallest partial order  $\preceq$  on  $V_n$  whose directed graph contains  $G_n$  and describe it concretely:  $i \preceq j$  iff ...
- (b) Draw the Hasse diagram for  $\preceq$  when  $n = 4$ .
- (c) Define maximal elements of a poset and determine all maximal elements of the poset  $(V_n, \preceq)$ .
- (d) Derive a first-order recurrence for the number  $e_n$  of edges in  $G_n$ .
- (e) Derive a second-order recurrence for the number  $e_n$  of edges in  $G_n$ .
- (f) Solve your second-order recurrence and check the results for  $n \leq 3$ .
- (g) Use the recurrence relation to find an explicit formula with no  $\sum$  or ... for the generating function

$$G(x) = \sum_{n=0}^{\infty} e_n x^n.$$

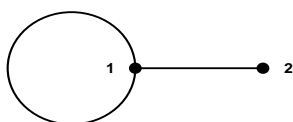
**8:** Define a relation  $R$  on simple graphs  $G = (V, E)$  by the requirement that  $G_1 R G_2$  iff  $|V_1| = |V_2|$ ,  $|E_1| = |E_2|$ , and there is a bijection  $f : V_1 \rightarrow V_2$  such that for every  $v \in V_1$ ,  $\deg(f(v)) = \deg(v)$ .

- (a) State the definition of an equivalence relation and prove that  $R$  is an equivalence relation.
- (b) Define isomorphism of simple graphs and prove that if  $G_1$  is isomorphic to  $G_2$  then  $G_1RG_2$ .
- (c) Find two nonisomorphic simple graphs  $G_1$  and  $G_2$  such that  $G_1RG_2$ .
- (d) Draw one representative of each equivalence class  $C$  of  $R$ , for simple graphs with  $n = 4$  vertices and  $e = 0$  to 4 edges.
- (e) Fix  $n = 4$  vertices and consider the experiment of selecting an equivalence class  $C$  at random with equal probabilities. Let  $f(C)$  be the random variable which is 1 if every graph in  $C$  contains an Euler circuit and 0 otherwise. State general formulas for the expectation  $E(f)$  and variance  $V(f)$  of  $f$ . Compute  $E(f)$  and  $V(f)$ .

**9:** For each of the following pairs of graphs, either specify an isomorphism between the left and the right graph, or state why there cannot be one.



**10:** Consider the following undirected pseudograph  $G$ :

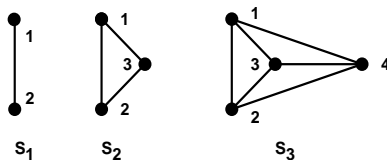


- (a) Write down the adjacency matrix  $A$  of  $G$ .
- (b) Find all paths of length 3 from 1 to 2; for example, one is  $(1, 1, 1, 2)$ , where the path loops twice at 1 then goes from 1 to 2.
- (c) Use the adjacency matrix  $A$  to express the number of paths from 1 to 2 of any specified length  $n \geq 1$  in terms of the Fibonacci numbers (defined by  $f_0 = 0$ ,  $f_1 = 1$ ,  $f_{n+1} = f_n + f_{n-1}$  for  $n \geq 1$ ).

- 11:** Let  $S$  be the set of permutations of  $n \geq 100$  objects.
- (a) How many elements of  $S$  leave the third object fixed?
  - (b) Consider the experiment of choosing an element of  $S$  randomly with equal probabilities. Let  $f$  be the random variable defined by  $f(\sigma) = |\{j : \sigma(j) = j\}|$ , so  $f(\sigma)$  is the number of fixed points of  $\sigma$ . Compute the expectation of  $f$ .
  - (c) Compute the variance  $V(f)$  and standard deviation  $\sigma(f)$  of  $f$ .
  - (d) Show that a randomly chosen permutation of  $n \geq 100$  objects is 99% certain to leave less than 11 objects fixed.

- 12:** Find the remainder of  $2^{326}$
- (a) mod 2,
  - (b) mod 5.
  - (c) State Fermat's little Theorem.
  - (d) Find  $2^{326} \bmod 47$ .
  - (e) State the Chinese Remainder Theorem for three moduli.
  - (f) Use the preceding results (a), (b), (d) and (e) to compute  $2^{326} \bmod 470$ .

**13:** The *simplex graph*  $S_n = (V_n, E_n)$  in  $n$  dimensions is defined recursively as follows.  $S_0$  has one vertex and no edges. Given  $S_n = (V_n, E_n)$ , we form  $V_{n+1}$  by adding one more vertex  $v$ . The edge set  $E_{n+1}$  is  $E_n$  plus edges connecting  $v$  to every vertex in  $V_n$ . The first few look like this:



- (a) Find the number  $v_n$  of vertices in  $S_n$ .
- (b) Find the degree  $d$  of each vertex in  $S_n$ .
- (c) Use the Handshaking Theorem to find the number  $e_n$  of edges in  $S_n$ .
- (d) Derive a first-order inhomogeneous recurrence relation for the number  $e_n$  of edges in  $S_n$ .
- (e) Derive the generating function for  $e_n$  from the recurrence relation.
- (f) Taylor-expand the generating function to derive a closed formula for  $e_n$  and check against (c).

**14:** Define the divisibility relation  $R$  on the set  $\mathbf{Z} = \{1, 2, 3, 4, \dots\}$  of positive integers by  $aRb \leftrightarrow a|b$ .

(a) Define a partial order and prove or disprove that  $R$  is one.

(b) Let  $M$  be the matrix of  $R$ . Show that the number  $d(j)$  of divisors of any integer  $j \in \mathbf{Z}$  is given by the sum of the entries in column  $j$  of  $M$ :

$$d(j) = \sum_{i=1}^j M_{ij} = \sum_{i=1}^{\infty} M_{ij}.$$

Note that  $M_{ij} = 0$  for  $i > j$ .

(c) Evaluate  $d(p^m q^n)$  for any distinct primes  $p$  and  $q$  and any positive integers  $m$  and  $n$ .

(d) Consider the experiment of selecting an integer  $j$  from  $\mathbf{Z}$  at random, where  $j$  is selected with probability  $p(j) = K/j^4$ . The constant  $K$  is chosen to make the probabilities sum to 1, and its exact value is known but irrelevant. Evaluate  $E(d)$ . You may find the following formula helpful:

$$\sum_{i=1}^{\infty} \sum_{j=1}^i = \sum_{j=1}^{\infty} \sum_{i=j}^{\infty} = \sum_{1 \leq j \leq i < \infty} .$$

(e) Let  $f(j) = j^2$  be another random variable in this experiment. Should  $f$  and  $d$  be independent? Why or why not? Justify your opinion with a proof.

**15:** (a) List all partitions of  $Z_3 = \{1, 2, 3\}$  into disjoint nonempty subsets.

(b) Let  $E$  be the set of equivalence relations  $\{1, 2, 3\}$ . List the matrices  $M$  of all elements of  $E$ , and show how they correspond to the partitions you found in (a).

(c) Let the partial order  $\preceq$  on  $E$  be defined by

$$\forall R \in E \forall S \in E ( R \preceq S \iff \forall a \in Z_3 \forall b \in Z_3 ( aRb \rightarrow aSb ) ).$$

Draw the digraph and the Hasse diagram of the relation  $\preceq$ .

(d) List  $E$  in a topologically sorted order.

**16:** Define the divisibility relation  $R$  on  $\mathbf{Z}_n = \{1, 2, 3, 4, \dots, n\}$  by  $aRb \leftrightarrow a|b$ .

(a) Define a partial order and prove or disprove that  $R$  is one.

(b) Let  $M$  be the matrix of  $R$ . Show that the number  $d(j)$  of divisors of any integer  $j \in \mathbf{Z}_n$  is given by the sum of the entries in column  $j$  of  $M$ :

$$d(j) = \sum_{i=1}^n M_{ij}.$$

- (c) Evaluate  $d(pq)$  for any primes  $p$  and  $q$  such that  $pq \in \mathbf{Z}_n$ .  
 (d) Consider the experiment of selecting an integer  $j$  from  $\mathbf{Z}_n$  at random, with equal probabilities. Show that

$$E(d) \leq \sum_{k=1}^n \frac{1}{k}.$$

- (e) Prove by induction that  $E(d) = O(\log n)$ .

**17:** Suppose that the correct answer to a randomly chosen true-false exam question is **T** with probability  $2/5$ , **F** with probability  $2/5$  and **C** with probability  $1/5$ . Consider two exams 1 and 2 with two questions each. Let  $A_1$  be the event that test 1 has at least one question whose correct answer is **T**, and  $A_2$  the event that the correct answer to the *first* question on test 2 is **T**. For  $i = 1, 2$  let  $C_i$  be the event that all the correct answers for test number  $i$  are **T**.

- (a) What is the sample space? What is the probability of each point  $x \in S$ ? What is the total expected number of correct answers which are **T** on both exams?  
 (b) Calculate the probabilities  $P(A_1)$  and  $P(A_2)$ .  
 (c) Calculate the conditional probabilities  $P(C_1|A_1)$  and  $P(C_2|A_2)$ .  
 (d) Define independence of two events  $A$  and  $B$ .  
 (e) For which  $i$  and  $j$  are  $A_i$  and  $C_j$  independent?

**18:** (a) Let  $B$  be the set of finite bit strings

$$B = \{x \mid \exists n \geq 0 (x = b_0b_1b_2 \dots b_n \text{ where } b_i = 0 \text{ or } 1) \}.$$

Is  $B$  finite, countable or uncountable? Why?

- (b) Let  $F$  be the set of all Boolean-valued functions  $f : \mathbf{N} \rightarrow \{0, 1\}$  of a nonnegative integer variable. Is  $F$  finite, countable or uncountable? Why?  
 (c) Given any Boolean-valued function  $f$  of a nonnegative integer variable  $n$ , can we always find a C program which accepts input  $n$  and outputs  $f(n)$ ? Why or why not?

**19:** Let  $S$  be the set of bit strings of length less than or equal to 3:

$$S = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 100, 011, 101, 110, 111\}.$$

- (a) Define a relation  $R$  on  $S$  by letting  $aRb$  whenever  $a$  and  $b$  have the same number of 1's. Prove from the definition of an equivalence relation that  $R$  is an equivalence relation.
- (b) Write down the partition of  $S$  which corresponds to the equivalence relation  $R$ .
- (c) Define another relation  $\preceq$  on  $S$  by letting  $a \preceq b$  whenever  $a$  is a substring of  $b$ . (Precise definition:  $a$  is a substring of  $b$  iff  $b$  is obtained from  $a$  by prefixing and postfixing  $a$  with some nonnegative number of 0 and 1 bits.) Prove from the definition of a partial order that  $\preceq$  is a partial order on  $S$ .
- (d) Draw the Hasse diagram for  $\preceq$  on  $S$  and use it to list  $S$  in a topologically sorted order.