Math 55: Final Exam, Dec 18, 1996

Problem 1: Show all steps in the following calculations.
(a) Use the Euclidean algorithm to compute gcd(21, 13).
(b) Use your work from (a) to find integers s and t such that $\gcd(21,13) = s \cdot 21 + t \cdot 13$.
(c) Use the procedure of the Chinese Remainder Theorem to find an integer x with $0 \le x < 21 \cdot 13 = 273$ such that

$$x \bmod 21 = 5$$

$$x \bmod 13 = 3$$

Solution 1: **(a)** The Euclidean algorithm goes as follows:

$$\begin{array}{lll}
 & x = 21 & y = 13 \\
r = 21 \bmod 13 = 8 & x = 13 & y = 8 \\
r = 5 & x = 8 & y = 5 \\
r = 3 & x = 5 & y = 3 \\
r = 2 & x = 3 & y = 2 \\
r = 1 & x = 2 & y = 1 \\
r = 0 & x = 1 = \gcd(21,13) & y = 0
\end{array}$$

(b) Working backwards, we find

$$\begin{aligned}
1 &= 3 - 2 = 3 - (5 - 3) \\
&= -1 \cdot 5 + 2 \cdot 3 = -1 \cdot 5 + 2 \cdot (8 - 5) \\
&= 2 \cdot 8 - 3 \cdot 5 = 2 \cdot 8 - 3 \cdot (13 - 8) \\
&= -3 \cdot 13 + 5 \cdot 8 = -3 \cdot 13 + 5 \cdot (21 - 13) \\
&= 5 \cdot 21 - 8 \cdot 13.
\end{aligned}$$

Thus $s = 5$ and $t = -8$.
(c) Since $M = 21 \cdot 13 = 273$ and the moduli 13 and 21 are relatively prime, a unique solution to the problem exists by the Chinese Remainder Theorem. To find it, we put $M_1 = 13$, $M_2 = 21$ and seek x in the form $x = x_1 M_1 + x_2 M_2$. Then the equations separate and we have to solve

$$x_1 M_1 \bmod 21 = 13 x_1 \bmod 21 = 5$$

and

$$x_2 M_2 \bmod 13 = 21 x_2 \bmod 13 = 3.$$

Thus we can solve these two equations independently by finding the inverses of 13 mod 21 and 21 mod 13 and multiplying. From **(b)**, we have $1 = 5 \cdot 21 - 8 \cdot 13$, so $5 \cdot 21 \bmod 13 = 1$ and $-8 \cdot 13 \bmod 21 = 13 \cdot 13 \bmod 21 = 1$. Multiplying through, we find

$$13 \cdot 13 x_1 \bmod 21 = x_1 \bmod 21 = 13 \cdot 5 \bmod 21 = 2$$

and

$$5 \cdot 21 x_2 \bmod 13 = x_2 \bmod 13 = 5 \cdot 3 \bmod 13 = 2.$$

Thus $x_1 = x_2 = 2$ and $x = 2 \cdot 13 + 2 \cdot 21 \bmod 273 = 68$. Checking, we note that $x \bmod 21 = 5$ and $x \bmod 13 = 3$.

Problem 2: A computer network consists of $n \geq 10$ computers, each one directly connected to 2 or more of the others.
(a) Prove or give a counterexample: There are at least two computers in the network that are directly connected to the same number of other computers.
(b) Suppose we want to study the network traffic level by sending a packet from computer to computer through the network so that the packet passes through each connection exactly once (in any direction) and returns to its starting point. State a simple condition on the number of connections to each computer which is necessary and sufficient for this test to be possible.

Solution 2: (a) For $j = 1, \ldots, n$ let c_j be the number of connections from computer j to the others. We are given that each c_j is one of the $n-1$ integers between 2 and n; since there are n of the c_j's, two must be identical by the pigeonhole principle. The corresponding computers are connected to the same number of other computers.
(b) Consider the network as a graph with the vertices being computers and the edges being the connections between computers. Then the test we want to do amounts to finding an Euler circuit, which can be done iff every vertex has even degree. Thus the test can be done iff each computer has connections to an even number of other computers.

Problem 3: Find a formula for the number of triples (x, y, z) of nonnegative integers satisfying

$$x + y + z = 16$$

(a) and no other restrictions,
(b) subject to

$$x \geq 4 \ \wedge \ y \geq 4 \ \wedge \ z \geq 4,$$

(c) subject to

$$x \leq 6 \ \wedge \ y \leq 6 \ \wedge \ z \leq 6.$$

Solution 3: (a) This is the number of ways to choose 16 objects of three kinds with repetition: By stars and bars, this is

$$\binom{18}{2} = 153.$$

(b) The restriction that we must have at least four of each kind is dealt with by taking four of each kind to begin with, leaving four objects to be chosen from three kinds: By stars and bars, this is

$$\binom{6}{2} = 15.$$

(c) Let A be the set of solutions found in **(a)**, and let

$$A_1 = \{(x,y,z) \in A | x \geq 7\}, A_2 = \{(x,y,z) \in A | y \geq 7\}, A_3 = \{(x,y,z) \in A | z \geq 7\}.$$

Thus we want to compute

$$|A - A_1 \cap A_2 \cap A_3| = |A| - |A_1 \cap A_2 \cap A_3| = |A| - |A_1| - |A_2| - |A_3| + |A_1 \cap A_2| + |A_2 \cap A_3| + |A_3 \cap A_1| - |A_1 \cap A_2 \cap A_3|$$

by inclusion-exclusion. By the approach of **(b)**, we have (using symmetry)

$$|A_1| = |A_2| = |A_3| = \binom{11}{2},$$

$$|A_1 \cap A_2| = |A_2 \cap A_3| = |A_3 \cap A_1| = \binom{4}{2}$$

and

$$|A_1 \cap A_2 \cap A_3| = 0$$

since the equation cannot be satisfied if x, y and z are all at least 7. Thus the answer is

$$\binom{18}{2} - 3 \cdot \binom{11}{2} + 3 \cdot \binom{4}{2} = 6.$$

Problem 4: Let F_n be the nth Fibonacci number defined by $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$ for $n \geq 1$. (They are 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, etc.)
(a) Use induction to prove that $\gcd(F_{n+1}, F_n) = 1$ for $n \geq 1$.
(b) For $n \geq 1$, let $E(n)$ be the number of "$x \bmod y$" calculations required by the Euclidean algorithm to compute $\gcd(F_{n+1}, F_n)$. Use induction to prove that $E(n) = O(n)$.

Solution 4: **(a)** First, we have $\gcd(F_2, F_1) = \gcd(1,1) = 1$ for $n = 1$, establishing the base. Now assume $\gcd(F_{n+1}, F_n) = 1$. Then

$$\gcd(F_{n+2}, F_{n+1}) = \gcd(F_{n+1} + F_n, F_{n+1}) = \gcd(F_{n+1}, F_n) = 1,$$

completing the inductive step. Note that $\gcd(a, a+b) = \gcd(a, b)$ since any divisor of a and b is a divisor of a and $a+b$ and vice versa.
(b) Let $P(n)$ be the statement "$E(n) \leq n$." The base case $P(1)$ is clearly true since $\gcd(1,1) = 1$ requires one 1 mod 1 calculation. For the inductive step, we fix $n > 2$ and assume $P(n-1)$ is true. Then the first step of the Euclidean algorithm for $\gcd(F_{n+1}, F_n)$ reads

$$\begin{array}{rll} & x = F_{n+1} & y = F_n \\ r = F_{n+1} \bmod F_n = F_{n-1} & x = F_n & y = F_{n-1} \end{array}$$

since $F_{n+1} = F_n + F_{n-1}$ and $F_{n-1} < F_n$ imply that $F_{n+1} \bmod F_n = F_{n-1}$. Hence taking the first step, at a cost of one $x \bmod y$ calculation, reduces $\gcd(F_{n+1}, F_n)$ to $\gcd(F_n, F_{n-1})$. The cost of the latter is $E(n-1)$ so we have $E(n) = 1 + E(n-1)$. By the inductive assumption, $E(n-1) \leq n-1$ so this proves $E(n) \leq n = O(n)$.

Problem 5: Let $X = \{a, b, c\}$ and let S be the set of all equivalence relations on S. Consider S as a sample space with uniform probability distribution. Let g (respectively f) be the random variable which assigns to an equivalence relation R the cardinality of its smallest (respectively largest) equivalence class. For example, if R is equality = then $g(R) = f(R) = 1$.
(a) Calculate the cardinality of S.
(b) Calculate $E(f)$ and $V(f)$.
(c) Use Chebyshev's inequality to show that there is a 60% probability that the largest equivalence class of a randomly chosen equivalence relation on X has exactly 2 elements.
(d) Prove or disprove: f and g are independent random variables.

Solution 5: **(a)** Since every equivalence relation on X corresponds to a unique partition of X into equivalence classes, we can count equivalence relations most easily by counting the partitions of X (into disjoint nonempty subsets). They are (with values of g and f listed to the right)

R	$g(R)$	$f(R)$
$\{\{a\},\{b\},\{c\}\}$	1	1
$\{\{a\},\{b,c\}\}$	1	2
$\{\{b\},\{c,a\}\}$	1	2
$\{\{c\},\{a,b\}\}$	1	2
$\{\{a,b,c\}\}$	3	3

so $|S| = 5$.

(b) From the table above,

$$E(f) = \frac{1}{5}(1+2+2+2+3) = 2$$

and

$$V(f) = E(f^2) - E(f)^2 = \frac{1}{5}(1+4+4+4+9) - 2^2 = \frac{2}{5}.$$

(c) Put $r = 1/\sigma(f)$ in Chebyshev's inequality

$$P(|f - E(f)| \geq r\sigma(f)) \leq \frac{1}{r^2}$$

to get

$$P(|f - E(f)| \geq 1) \leq \sigma(f)^2 = V(f) = \frac{2}{5}.$$

Thus there is a 60% probability that the largest equivalence class of a randomly chosen equivalence relation has cardinality *strictly* between $E(f) - 1 = 1$ and $E(f) + 1 = 3$. But this cardinality is an integer, so if it lies strictly between 1 and 3 then it must be exactly 2. Note that this is obvious from the list of partitions in **(a)** since 3 of the 5 have $f(R) = 2$.

(d) Intuitively, f and g should not be independent because knowing f completely determines g. Proof:

$$P(f = 3 \wedge g = 3) = \frac{1}{5} \neq \frac{1}{5} \cdot \frac{1}{5} = P(f = 3)P(g = 3).$$

Problem 6: Consider the following pseudocode:

```
function F (n, A = (a1, ..., an), m, B = (b1, ..., bm), f: A --> B) do i := 1, m
    s := 0
    do j := 1, n
        if(f(aj) = bi) s := s + 1
    end do
    if(s != 1) return F := False
end do
return F := True
```

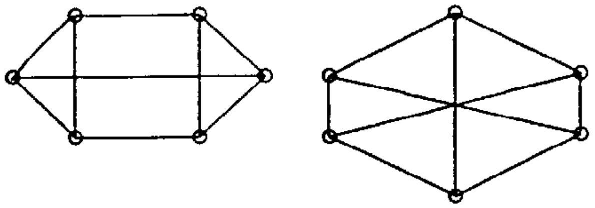
(a) What does it compute?

(b) What is its worst-case complexity in terms of `m` and `n` in big-O notation?

Solution 6: **(a)** It returns `True` iff the input function f is a bijection (a one-to-one correspondence) between A and B.

(b) The worst case is when `s` is always equal to 1 in the inner loop, so the outer loop does not terminate early. Then `F` requires `mn` evaluations of `f`, so the worst-case complexity is $O(\texttt{mn})$.

Problem 7: Prove or disprove: the following graphs are isomorphic.



Solution 7: The two graphs are not isomorphic: the left one contains a subgraph isomorphic to K_3 (either of the left or right triangles will do) while the right one does not. More directly, the left graph contains three mutually adjacent vertices while the right does not. Note that the two graphs have the same number of vertices and edges and the vertices all have degree 3, so the obvious tests will not rule out isomorphism.

Problem 8: Suppose that a randomly chosen child is male with probability 1/2 and female with probability 1/2. Consider two families 1 and 2 with two children each. Let A_1 be the event that family 1 has at least one male child and A_2 be the event that the *oldest* child in family 2 is male. For $i = 1, 2$ let C_i be the event that family number i has two male children.
(a) What is the sample space S? What is the probability $P(x)$ of each point $x \in S$? What is the total expected number of male children in both families?
(b) Calculate the probabilities $P(A_1)$ and $P(A_2)$.
(c) Calculate the conditional probabilities $P(C_1|A_1)$ and $P(C_2|A_2)$. Given that A_1 and A_2 take place, which is more likely: C_1 or C_2?
(d) Define what it means for two events A and B to be independent.
(e) For which i and j are A_i and C_j independent?

Solution 8: **(a)** Let child number j in family i be represented by a Boolean variable $c_{ij} = 0$ if female and 1 if male. The sample space is then the set of 4-bit strings $S = \{c_{11}c_{12}c_{21}c_{22} | c_{ij} = 0, 1\}$. Since the sample space has $2^4 = 16$ equally likely points, $P(x) = 1/16$ for any $x \in S$. The total expected number of male children is 1/2.
(b) Since A_1 contains $3 \cdot 4 = 12$ and A_2 contains $4 \cdot 2 = 8$ points, we have $P(A_1) = 12/16 = 3/4$ and $P(A_2) = 8/16 = 1/2$.
(c) First, we observe that $P(C_1) = P(C_2) = 1/4$. Since $A_i \subseteq C_i$ for $i = 1, 2$, we have $P(C_i \cap A_i) = 1/4$ for $i = 1, 2$ as well. By definition of conditional probability, then,

$$P(C_1|A_1) = \frac{P(C_1 \cap A_1)}{P(A_1)} = 1/3$$

and

$$P(C_2|A_2) = \frac{P(C_2 \cap A_2)}{P(A_2)} = 1/2.$$

Thus given A_1 and A_2, C_2 is more likely than C_1.
(d) Two events A and B are independent iff $P(A \cap B) = P(A)P(B)$.
(e) Since $P(C_i|A_i) \neq P(C_i)$ for $i = 1, 2$, C_i is *not* independent of A_i. We expect that C_1 should be independent of A_2 and C_2 independent of A_1 because they are events concerned with different families. To verify this, we need only calculate

$$P(C_1 \cap A_2) = P(\{1110, 1111\}) = 2/16 = (1/4) \cdot (1/2) = P(C_1)P(A_2)$$

and

$$P(C_2 \cap A_1) = P(\{1011, 0111, 1111\}) = 3/16 = (1/4) \cdot (3/4) = P(C_2)P(A_1).$$

Problem 9: Let p and q be propositional variables. Let X be the following set of propositions in the variables p and q:

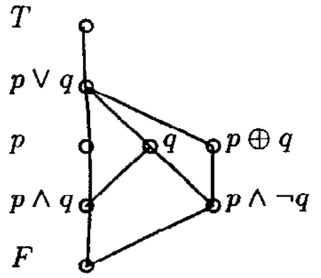
$$X = \{T, F, p, q, p \wedge q, p \wedge \neg q, p \vee q, p \oplus q\}.$$

Define a relation R on X by $\alpha R \beta$ iff $\alpha \to \beta$ is a tautology.
(a) Construct a truth table showing the values of all elements of X (except T and F).
(b) Check that R is a partial order on X.
(c) Construct the Hasse diagram for the poset $P = (X, R)$.
(d) List P in a topologically sorted order.

Solution 9: **(a)** The truth table reads:

p	q	$p \wedge q$	$p \vee q$	$p \wedge \neg q$	$p \oplus q$
T	T	T	T	F	F
F	T	F	T	F	T
T	F	F	T	T	T
F	F	F	F	F	F

(b) We need to check reflexivity, antisymmetry and transitivity. First, R is reflexive because for any proposition r, the implication $r \to r$ is a tautology: either r is F or T and $r \to r$ is T in either case. For antisymmetry, we observe that there are no two distinct elements a and b of X such that $a \to b$ and $b \to a$ are both tautologies; thus R is antisymmetric. Transitivity is equivalent to the statement that $(p \to q \wedge q \to r) \to (p \to r)$ is a tautology, which is transitivity of implication. To prove it, suppose $p \to r$ is F. Then p is T and r is F. If q is T then $q \to r$ is F, while if q is F then $p \to q$ is F; in either case, we are done.
(c) The Hasse diagram looks like:



(d) Topologically sorted orders for P are found by pulling off a minimal element at each step. They include

$$F, p \wedge \neg q, p \oplus q, p \wedge q, p, q, p \vee q, T$$
$$F, p \wedge q, p, q, p \wedge \neg q, p \oplus q, p \vee q, T$$
$$F, p \wedge q, p \wedge \neg q, p, q, p \oplus q, p \vee q, T$$

and many others.