CS/MATH 111 Winter 2013
Final Test

- The test is 2 hours and 30 minutes long, starting at **7PM** and ending at **9:30PM**
- There are **8** problems on the test. Each problem is worth 10 points.
- Write legibly. What can't be read won't be credited.
- **Before** you start:
  - Make sure that your final has all 8 problems
  - Put your name and SID on the front page below and on top of *each* page

Name	SID

problem	1	2	3	4	5	6	7	8	total
score									

NAME: SID:

Problem 1: (a) For each pseudo-code below, give the *exact formula* for the number of words printed if the input is n (where $n \geq 1$), and then give its asymptotic value (using the Θ-notation.)

Pseudo-code	Formula	Asympt. value
procedure Ahem(n) **for** $j \leftarrow 1$ **to** $n+1$ **for** $i \leftarrow 1$ **to** j **do** print("ahem")	$T(n) = \sum_{=1}^{n+1} j = (n+1)(n+2)/2$	$\Theta(n^2)$

procedure Geez(n)
if $n = 1$ **then**
print("geez geez")
else
for $i \leftarrow 1$ **to** 3 **do**
Geez($n-1$)
	$T(1) = 2$ and $T(n) = 3T(n-1)$. So $T(n) = 2 \cdot 3^n$.	$\Theta(3^n)$

(b) For each pseudo-code below, give a recurrence for the asymptotic value for the number of words printed if the input is n (where $n \geq 1$) and then its solution (using the Θ-notation.)

Pseudo-code	Recurrence	Solution
procedure Oops(n) **if** $n > 2$ **then** print("oops") Oops($n/3$) Oops($n/3$)	$T(n) = 2T(n/3) + 1$	$\Theta(n^{\log_3 2})$
procedure Eeek(n) **if** $n > 2$ **then** **for** $j \leftarrow 1$ **to** n **do** print("eeek") **for** $k \leftarrow 1$ **to** 4 **do** Eeek($n/2$)	$T(n) = 4T(n/2) + n$	$\Theta(n^2)$
procedure Whew(n) **if** $n > 1$ **then** **for** $j \leftarrow 1$ **to** n^2 **do** print("whew") **for** $k \leftarrow 1$ **to** 5 **do** Whew($n/2$)	$T(n) = 5T(n/2) + n^2$	$\Theta(n^{\log 5})$

NAME: SID:

Problem 2: (a) Explain how the RSA cryptosystem works.

Initialization:	Choose two different primes p and q, and let $n = pq$. Let $\phi(n) = (p-1)(q-1)$. Choose an integer e relatively prime to $\phi(n)$. Let $d = e^{-1} \pmod{\phi(n)}$. Public key is $P = (n, e)$. Secret key is $S = d$.
Encryption:	If M is the message then its encryption is $E(M) = M^e \,\mathrm{rem}\, n$
Decryption:	If C is the ciphertext then its decrypted as $D(C) = C^d \,\mathrm{rem}\, n$

(b) Below you are given five choices of parameters p, q, e, d of RSA. For each choice tell whether these parameters are correct[1] (write YES/NO). If not, give a brief justification (at most 10 words).

p	q	e	d	correct?	justify if not correct
23	51	18	89	NO	51 is not prime
23	11	33	103	NO	33 is not relatively prime to $\phi(n) = 220$
3	7	5	5	YES	
17	17	3	171	NO	p and q should be different
11	7	13	37	YES	

[1] For correctness it is only required that the decryption function is the inverse of the encryption function.

NAME: SID:

Problem 3: (a) Give a complete statement of the principle of inclusion-exclusion.

Let $S_1, ..., S_k$ be finite sets. Then the cardinality of their union is

$$\left|\bigcup_{j=1}^{k} S_j\right| = \sum_{j=1}^{k}(-1)^{j+1} \sum_{\ell_1<\ell_2<...<\ell_j} \left|\bigcap_{i=1}^{j} S_{\ell_i}\right|$$

(b) We have three sets A, B, C that satisfy

- $|A| = |B| = 14$ and $|C| = 19$,
- $|A \cap B| = |A \cap C| = \frac{3}{14}|A \cup B \cup C|$ and $|B \cap C| = 8$,
- $|A \cap B \cap C| = 1$.

Determine the cardinality of $A \cup B \cup C$.

Let $x = |A \cup B \cup C|$. Then, using the inclusion-exclusion formula, we get

$$x = 14 + 14 + 19 - \frac{3}{14}x - \frac{3}{14}x - 8 + 1$$

so $x = 28$.

NAME: SID:

Problem 4: (a) Give a complete statement of Fermat's Little Theorem.

If p is a prime number and $a \in \{1, 2, ..., p-1\}$ then $a^{p-1} = 1 \pmod{p}$.

(b) Use Fermat's Little Theorem to compute the following values:

$78^{112} \pmod{113} = 1$

$3^{39635} \pmod{31} =$

Computing modulo 31, we get $3^{39635} = 3^{39630} \cdot 3^5 = 3^5 = 243 = 26$

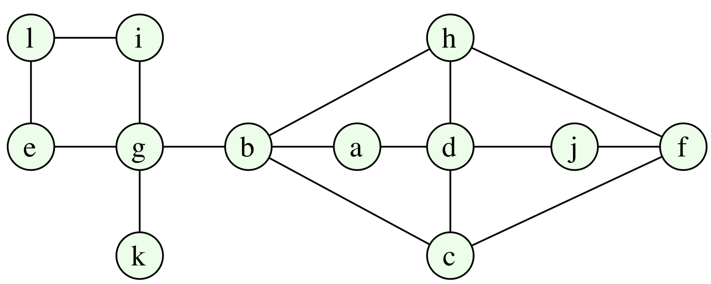
Problem 5: (a) Give a complete definition of a perfect matching in a bipartite graph.

A set M of edges is called a matching if any two edges in M have different endpoints. A matching M is called perfect if it covers every vertex, that is every vertex is an endpoint of an edge in M.

(b) State Hall's Theorem.

A bipartite graph $G = (U, V, E)$ with $|U| = |V|$ has a perfect matching if and only if for any set $X \subseteq U$ we have $|N(X)| \geq |X|$, where $N(X)$ denotes the set of all neighbors of vertices in X.

(c) Determine whether the graph below is bipartite and if it is, whether it has a perfect matching. You must give a complete justification for your answer.

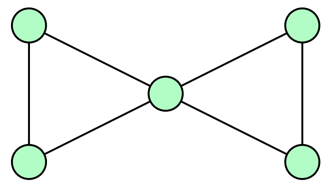


Bipartite partition: $U = \{a, c, h, j, g, l\}$, $V = \{b, d, f, e, i, k\}$.

This graph does not have a perfect matching. To see why, let $X = \{a, c, j, h\}$. Then $N(X) = \{b, d, f\}$. So $|N(X)| < |X|$, violating Hall's Theorem.

Problem 6: (a) Prove or disprove the following statement: "If a graph G has an Euler tour then G also has a Hamiltonian cycle".

This is false. One example is a bow-tie graph.



This graph has an Euler tour (because all degrees are even) but it does not have a Hamiltonian cycle, because any cycle that visits all vertices must traverse the middle vertex twice.

(b) Prove or disprove the following statement: "If a bipartite graph G has a Hamiltonian cycle then G has a perfect matching".

This is true. For the proof, suppose that G has a Hamiltonian cycle $H = v_1 v_2 ... v_n v_1$. Let M consist of edges (v_1, v_2), (v_3, v_4), (v_5, v_6), ..., (v_{n-1}, v_n), that is every second edge from H. Then every vertex is covered by M and no two edges in M share an endpoint, so M is a perfect matching.

Problem 7: Using mathematical induction prove that

$$\sum_{i=0}^{n} 5^i \;=\; \tfrac{1}{4}(5^{n+1} - 1).$$

(Only proofs by induction will be accepted.)

We first check the base case. For $n = 0$, the left-hand side is $\sum_{i=0}^{0} 5^i = 5^0 = 1$ and the right-hand side is $\frac{1}{4}(5^{0+1} - 1) = 1$, so the equality holds.

Now let $k > 0$ and assume that the equation holds for $n = k$, that is

$$\sum_{i=0}^{k} 5^i \;=\; \tfrac{1}{4}(5^{k+1} - 1).$$

We claim that it also holds for $n = k + 1$, that is

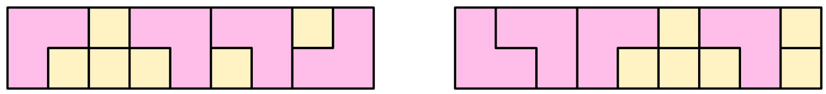
$$\sum_{i=0}^{k+1} 5^i \;=\; \tfrac{1}{4}(5^{k+2} - 1).$$

We derive this equation as follows:

$$\begin{aligned}
\sum_{i=0}^{k+1} 5^i &= \sum_{i=0}^{k} 5^i + 5^{k+1} \\
&= \tfrac{1}{4}(5^{k+1} - 1) + 5^{k+1} \\
&= \tfrac{1}{4} \cdot 5^{k+1} - \tfrac{1}{4} + 5^{k+1} \\
&= (\tfrac{1}{4} + 1) \cdot 5^{k+1} - \tfrac{1}{4} \\
&= \tfrac{5}{4} \cdot 5^{k+1} - \tfrac{1}{4} \\
&= \tfrac{1}{4} \cdot 5^{k+2} - \tfrac{1}{4} \\
&= \tfrac{1}{4}(5^{k+2} - 1),
\end{aligned}$$

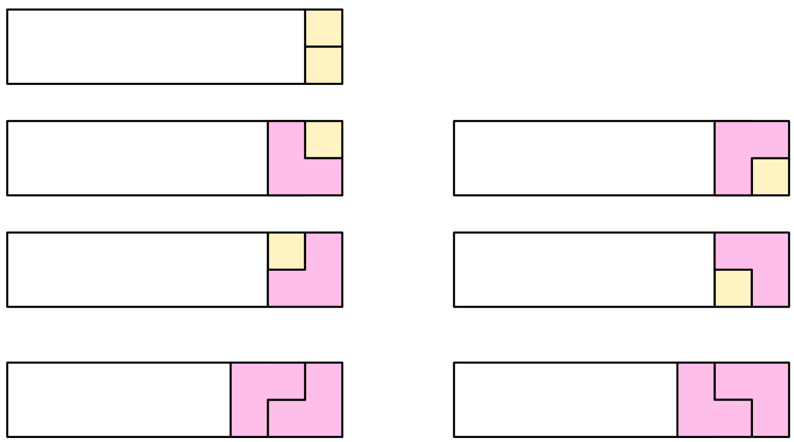
where in the second step we used the inductive assumption, and the remaining steps are just algebra.

Problem 8: We want to tile a $2 \times n$ strip with 1×1 tiles and L-shaped tiles of width and height 2. Here are two examples of such a tiling of a 2×9 strip:



Let $A(n)$ be the number of such tilings. (a) Give a recurrence relation for $A(n)$ and justify it. (b) Solve the recurrence to compute $A(n)$.

Here are possible endings:



This gives us recurrence

$$A(n) = A(n-1) + 4A(n-2) + 2A(n-3)$$

with $A(0) = 1$, $A(1) = 1$, and $A(2) = 5$.

The characteristic equation is $x^3 - x^2 - 4x - 2 = 0$ and its roots are -1, $1-\sqrt{3}$, and $1+\sqrt{3}$. So the general form of the solution is

$$A(n) = \alpha_1(-1)^n + \alpha_2(1-\sqrt{3})^n + \alpha_3(1+\sqrt{3})^n.$$

The initial conditions give us

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 1 \\ \alpha_1(-1) + \alpha_2(1-\sqrt{3}) + \alpha_3(1+\sqrt{3}) &= 1 \\ \alpha_1 + \alpha_2(4-2\sqrt{3}) + \alpha_3(4+2\sqrt{3}) &= 5 \end{aligned}$$

Solving, we get $\alpha_1 = 1$, $\alpha_2 = -1/\sqrt{3}$ and $\alpha_3 = 1/\sqrt{3}$. So

$$A(n) = (-1)^n - \frac{1}{\sqrt{3}}(1-\sqrt{3})^n + \frac{1}{\sqrt{3}}(1+\sqrt{3})^n.$$