HKUST – Department of Computer Science and Engineering
COMP 2711: Discrete Math Tools for CS – Spring 2013

Serial #

Final Examination

Date: Tuesday, 28 May 2013 Time: 4:30pm–7:30pm

Name: ______________________ Student ID: ____________________
Email: ______________________ Lecture and Tutorial: __________
Program (circle one): COMP CPEG BBA+COMP BBA+CPEG others

Instructions

- This is a closed book exam. It consists of 17 pages and 10 questions.
- Please write your name, student ID, email, lecture section and tutorial on this page.
- For each subsequent page, please write your student ID at the top of the page in the space provided.
- Please sign the honor code statement on page 2.
- Answer all the questions within the space provided on the examination paper. You may use the back of the pages for your rough work. The last three pages are scrap paper and may also be used for rough work. Each question is on a separate page. This is for clarity and is not meant to imply that each question requires a full page answer. Many can be answered using only a few lines.
- **Unless otherwise specified you *must* always explain how you derived your answer. A number without an explanation will be considered an incorrect answer.**

Questions	1	2	3	4	5	6	7	8	9	10	Total
Score											

Student ID: ______________

As part of HKUST's introduction of an honor code, the HKUST Senate has recommended that all students be asked to sign a brief declaration printed on examination answer books that their answers are their own work, and that they are aware of the regulations relating to academic integrity. Following this, please read and sign the declaration below.

```
I declare that the answers submitted for
this examination are my own work.

I understand that sanctions will be
imposed, if I am found to have violated the
University regulations governing academic
integrity.

Student's Name:      ______________________

Student's Signature: ______________________
```

Problem 1: [10 points]

(a) Let m and n be two positive integers such that m divides n, i.e., $n = sm$ for some other integer s. Show that, for any integer x,

$$(x \bmod n) \bmod m = x \bmod m.$$

(b) For each number in Z_8, state if it has a multiplicative inverse mod 8, and if it has, state its inverse. There is no need to explain your answer.

Answer: (a) Let $x \bmod n = r_1$. Then $x = q_1 n + r_1$ for some integer q_1. Further let $r_1 \bmod m = r_2$. Then $r_1 = q_2 m + r_2$ for some integer q_2. Hence,

$$x = q_1 n + q_2 m + r_2 = q_1 s m + q_2 m + r_2 = (q_1 s + q_2)m + r_2,$$

where $0 \leq r_2 < m$. Consequently,

$$x \bmod m = r_2 = (x \bmod n) \bmod m.$$

(b) 0 has no inverse; 1's inverse is 1; 2 has no inverse; 3's inverse is 3; 4 has no inverse; 5's inverse is 5; 6 has no inverse; 7's inverse is 7.

Problem 2: [12 points]
Suppose for applying RSA, $p = 11$, $q = 19$, and $e = 7$.

(a) What is the public key (e, n)?

(b) Calculate the private (secret) key d. Show the computational steps.

(c) Encrypt the message 100 using repeated squaring. Show the computational steps.

[WORKSPACE FOR THIS PROBLEM INCLUDES THIS AND THE NEXT PAGE]

Answer: (a) The public key is the pair: (e, n) where $e = 7$ and $n = p * q = 209$.

(b) The private key is given by

$$d = e^{-1} \bmod (p-1)(q-1) = 7^{-1} \bmod 180.$$

To find the multiplicative inverse of 7 in Z_{180}, we run the extended GCD algorithm:

$180 = 7 \times 25 + 5$, thus $gcd(7, 180) = gcd(5, 7)$,
$7 = 5 \times 1 + 2$, thus $gcd(5, 7) = gcd(2, 5)$,
$5 = 2 \times 2 + 1$, thus $gcd(2, 5) = gcd(1, 2) = 1$.
$2 = 1 \times 2 + 0$, thus $gcd(1, 2) = 1$.

Now working backward, we get:

$$\begin{aligned} 1 &= 1 \times 1 + 2 \times 0 \\ &= 5 - 2 \times 2 \\ &= 5 - 2 \times (7 - 5 \times 1) = 3 \times 5 - 2 \times 7 \\ &= 3 \times (180 - 25 \times 7) - 2 \times 7 = 3 \times 180 - 77 \times 7. \end{aligned}$$

Thus $d = -77 \bmod 180 = 103$.

(c) 100 is encrypted to $100^7 \bmod n$, where $n = 11 \times 19 = 209$.

$100^7 \bmod 209 = 100^{4+2+1} \bmod 209 = 100 \times 100^2 \times 100^4 \bmod 209$.

$100 \bmod 209 = 100$.
$100^2 \bmod 209 = 10000 \bmod 209 = 177$.
$100^4 \bmod 209 = 177 * 177 \bmod 209 = 188$.

Thus $100^7 \bmod 209 = (100 \times 177 \times 188) \bmod 209 = 111$.

[WORKSPACE FOR PROBLEM 2]

Problem 3: [10 points]

Let p and q be two different prime numbers. Let $a \in Z_p$ and $b \in Z_q$. Consider the following two modular equations:

$$\begin{aligned} x \bmod p &= a, \\ x \bmod q &= b. \end{aligned}$$

We have learned in class that there exists $x \in Z_{pq}$ that satisfies the two equations. Give a **contrapositive proof** for the following statement:

There is **only one** $x \in Z_{pq}$ that satisfies the two equations.

Note that this is the uniqueness part of the Chinese Reminder Theorem.

Proof: Let s denote the statement. The premise is always true. So, the statement is $T \to s$. By contrapositive rule, we prove $\neg s \to F$. This means that we assume $\neg s$ and then derive some contradiction.

Assume there are two **different** numbers x_1 and x_2 from Z_{pq} that satisfy the equations.

Without losing generality, assume $x_1 > x_2$. Then $0 < (x_1 - x_2) < pq - 1$. Hence $(x_1 - x_2)$ is not divisible by pq.

Because both x_1 and x_2 satisfy the equations, we have

$$\begin{aligned} x_1 \bmod p &= a, \qquad x_1 \bmod q = b. \\ x_2 \bmod p &= a, \qquad x_2 \bmod q = b. \end{aligned}$$

By subtracting the second line from the first, we

$$x_1 \bmod p - x_2 \bmod p = 0, \qquad x_1 \bmod q - x_2 \bmod q = 0,$$

which imply:

$$(x_1 - x_2) \bmod p = 0, \qquad (x_1 - x_2) \bmod q = 0.$$

These two equations mean that $(x_1 - x_2)$ is divisible by p and q. Because p and q are different prime numbers, this implies that $(x_1 - x_2)$ is divisible by pq, which contradicts our earlier conclusion that $(x_1 - x_2)$ is not divisible by pq.

The statement is therefore proved. Q.E.D

Problem 4: [10 points]
Prove the following equality **without** using repeated squaring:

$$46^{120} \bmod 77 = 1.$$

[Hint: Make use of the fact that $77 = 11 \cdot 7$ and try to use Fermat's Little Theorem and the Chinese Reminder Theorem.]

Answer: Let $r = 46^{120} \bmod 77$. Using Problem 1 (a), we get

$$r \bmod 7 = 46^{120} \bmod 7, r \bmod 11 = 46^{120} \bmod 11.$$

By Fermat's Little Theorem, we have

$$\begin{aligned}
&46^{120} \bmod 7 = (4^6)^{20} \bmod 7 = (4^6 \bmod 7)^{20} \bmod 7 = 1, \\
&46^{120} \bmod 11 = (4^{10})^{12} \bmod 11 = (4^{10} \bmod 11)^{12} \bmod 11 = 1.
\end{aligned}$$

So, we have

$$r \bmod 7 = 1, r \bmod 11 = 1.$$

Obviously, we also have

$$1 \bmod 7 = 1, 1 \bmod 11 = 1.$$

It follows from the Chinese Reminder Theorem that $r = 1$. The proof is completed.

Student ID: ____________

Problem 5: [6 points]
For each of the following pairs of logic statements, either prove that the two statements are logically equivalent, or give a counterexample. In your proof, you may use either a truth table or logic laws. A counterexample should consist of a truth setting of the variables and the truth values of the statements under the setting.

(a) $(p \wedge q) \Rightarrow r$ and $\neg p \vee \neg q \vee r$

(b) $(p \wedge q) \Rightarrow r$ and $\neg r \Rightarrow (p \Rightarrow \neg q)$

(c) $(p \Rightarrow r) \wedge (q \Rightarrow r)$ and $(p \wedge q) \Rightarrow r$

Answer: (a) Equivalent.

$$\begin{aligned}(p \wedge q) \Rightarrow r &\equiv \neg(p \wedge q) \vee r \quad (s \Rightarrow t \equiv \neg s \vee t)\\ &\equiv \neg p \vee \neg q \vee r \quad \text{(by DeMorgan's law)}\end{aligned}$$

(b) Equivalent.

$$\begin{aligned}\neg r \Rightarrow (p \Rightarrow \neg q) &\equiv r \vee (\neg p \vee \neg q) \quad (\ s \Rightarrow t \equiv \neg s \vee t)\\ &\equiv (p \wedge q) \Rightarrow r \quad \text{(by part (a))}\end{aligned}$$

(c) Not equivalent. Counter example: $p = T$, $q = F$, $r = F$. The first statement is false, while the second statement is true.

Problem 6: [9 points]
Consider the following three statements:

(i) All rich people have famous-brand products and don't have part-time jobs.

(ii) Some students with part-time jobs have famous-brand products.

(iii) All students with part-time jobs are not rich.

Let U be the universe of all people and define the following predicates:

$$\begin{aligned} R(x) &: \text{ x is a rich person} \\ F(x) &: \text{ x has famous-brand products} \\ S(x) &: \text{ x is a student} \\ J(x) &: \text{ x has part-time jobs.} \end{aligned}$$

(a) Write down the logic statements for the three statements above.

(b) Does (i) logically imply (iii)? If yes, give a proof. Clearly state the logic inference rule that you use at each step. If no, explain why not.

Answer: (a) (i) $\forall x \in U(R(x) \Rightarrow (F(x) \wedge \neg J(x)))$
(ii) $\exists x \in U(S(x) \wedge J(x) \wedge F(x))$
(iii) $\forall x \in U(S(x) \wedge J(x) \Rightarrow \neg R(x))$

(b) Yes, (i) does imply (iii).
Proof: Statement (i) can be broken up into the following two statements:

$$\forall x \in U(R(x) \Rightarrow F(x))$$
$$\forall x \in U(R(x) \Rightarrow \neg J(x))$$

The contrapositive of the second rule is:

$$\forall x \in U(J(x) \Rightarrow \neg R(x))$$

Let x be a generic element in U. We have

$$\begin{aligned} S(x) \wedge J(x) &\Rightarrow J(x) \\ J(x) &\Rightarrow \neg R(x) \end{aligned}$$

By transitivity of logic implication, we get:

$$S(x) \wedge J(x) \Rightarrow \neg R(x)$$

By the rule of Universal Generalization, we obtain:

$$\forall x \in U(S(x) \wedge J(x) \Rightarrow \neg R(x)).$$

Q.E.D

Problem 7: [10 points]
Use induction to prove that, for any integer $n \geq 1$,

$$5^n + 2 \cdot 11^n \text{ is divisible by } 3.$$

Proof: Base case: When $n = 1$, we have

$$5^1 + 2 \times 11^1 = 27,$$

which is divisible by 3. So, the statement is true for $n = 1$.

Induction hypothesis: Now let $n > 1$. Assume the statement is true for $n - 1$, i.e.,

$$5^{n-1} + 2 \cdot 11^{n-1} \text{ is divisible by } 3.$$

Induction step: Consider the case of n:

$$\begin{aligned}
5^n + 2 \cdot 11^n &= 5^{n-1} + 4 \cdot 5^{n-1} + 2 \cdot 11^{n-1} + 20 \cdot 11^{n-1} \\
&= 5^{n-1} + 2 \cdot 11^{n-1} + 4(5^{n-1} + 5 \cdot 11^{n-1}) \\
&= 5^{n-1} + 2 \cdot 11^{n-1} + 4(5^{n-1} + 2 \cdot 11^{n-1} + 3 \cdot 11^{n-1}) \\
&= 3y + 4(3y + 3 \cdot 11^{n-1}) \\
&= 3(5y + 4 \cdot 11^{n-1}),
\end{aligned}$$

which is divisible by 3.

By the principle of Mathematical Induction, we conclude that the statement is true for all integer $n \geq 1$. Q.E.D

Student ID: ____________

Problem 8: [10 points]
Consider a function $T(n)$ defined on integers n that are powers of 2. Suppose

$$T(1) = 1, \quad T(n) = 3T(n/2) + n^2.$$

Iterate the recurrence or use a recursion tree to find a closed-form expression for $T(n)$. Simplify the closed-form expression using the big Θ notation.

Answer: Iterating the recurrence, we get:

$$\begin{aligned}
T(n) &= T(2^j) \\
&= 3T(2^{j-1}) + 2^{2j} \\
&= 3(3T(2^{j-2}) + 2^{2(j-1)}) + 2^{2j} \\
&= 3^2T(2^{j-2}) + \frac{3}{4}2^{2j} + 2^{2j} \\
&= 3^2(3T(2^{j-3}) + 2^{2(j-2)}) + \frac{3}{4}2^{2j} + 2^{2j} \\
&= 3^3T(2^{j-3}) + (\frac{3}{4})^2 2^{2j} + \frac{3}{4}2^{2j} + 2^{2j} \\
&\vdots \\
&= 3^jT(1) + (\frac{3}{4})^{j-1}2^{2j} + \ldots + \frac{3}{4}2^{2j} + 2^{2j} \\
&= 3^j + 2^{2j}\frac{1-(3/4)^j}{1-3/4} \\
&= 3^j + 4 \cdot 2^{2j} - 4 \cdot 3^j = 4 \cdot 2^{2j} - 3 \cdot 3^j \\
&= 4n^2 - 3n^{log_2 3} \\
&= \Theta(n^2).
\end{aligned}$$

Problem 9: [11 points]
Consider a function $T(n)$ defined on integers n that are powers of 3. Suppose

$$T(1) = 1, \quad T(n) \leq 9T(\frac{n}{3}) + 4n^2 + 100n \ \forall n > 1.$$

Use **advanced induction** to prove that

$$T(n) = O(n^2 \log n).$$

Proof 1: It suffices to show that there exist n_0 and c such that

$$T(n) \leq cn^2 \log n \qquad \forall n = 3^i, n > n_0.$$

- Base case: Pick $n_0 = 1$. Then the base case is when $n = 3^1 = 3$:

$$T(3) \leq 9T(1) + 43^2 + 100 \times 3 = 345.$$

We want the right hand side to be no greater than $c3^2 \log 3$. To satisfy the condition, we need $c \geq \frac{115}{3 \log 3}$.

- Induction Hypothesis: Suppose

$$T(m) \leq cm^2 \log m \qquad \forall m = 3^i, m < n.$$

- Induction Step:

$$\begin{aligned} T(n) &\leq 9T(\frac{n}{3}) + 4n^2 + 100n \\ &\leq 9c(\frac{n}{3})^2 \log \frac{n}{3} + 4n^2 + 100n \\ &= cn^2 \log n - cn^2 \log 3 + 4n^2 + 100n \\ &= cn^2 \log n \quad \text{if } c > 104/\log 3 \end{aligned}$$

So, the proof follows through if we choose $n_0 = 1$ and $c = \max\{\frac{115}{3 \log 3}, 104/\log 3\} = 104/\log 3$. The proof is completed.

Proof 2: It suffices to show there exist positive constants c_1, c_2 and n_0 such that

$$T(n) \le c_1 n^2 \log_3 n - c_2 n, \ \forall n > n_0. \qquad (*)$$

Base case: Let $n_0 = 1$. Remember n is a power of 3. The smallest such integer such that $n > 1$ is 3. So, the base case is $n = 3$. For this case, we have

$$T(3) \le 9T(1) + 4 \times 3^2 + 100 \times 3 = 345 \le 9c_1 - 3c_2.$$

This is true when $c_1 \ge \frac{3c_2+345}{9} = \frac{c_2+115}{3}$.

Induction hypothesis: Now let $n > 3$. Assume that, for any m such that $1 \le m < n$ and m is power of 3, the following is true:

$$T(m) \le c_1 m^2 \log_3 m - c_2 m.$$

Induction step: Now consider the case of n:

$$\begin{aligned}
T(n) &\le 9T(\frac{n}{3}) + 4n^2 + 100n \\
&\le 9(c_1(\frac{n}{3})^2 \log_3 \frac{n}{3} - c_2\frac{n}{3}) + 4n^2 + 100n \\
&= c_1 n^2 \log_3 n - c_1 n^2 - 3c_2 n + 4n^2 + 100n \\
&= c_1 n^2 \log_3 n - c_2 n + (4 - c_1)n^2 + (100 - 2c_2)n \\
&\le c_1 n^2 \log_3 n - c_2 n + (4 - c_1)n^2 + (100 - 2c_2)n^2 \\
&= c_1 n^2 \log_3 n - c_2 n + (104 - c_1 - 8c_2)n^2 \\
&\le c_1 n^2 \log_3 n - c_2 n, \quad \text{when } (104 - c_1 - 2c_2)n^2 \le 0
\end{aligned}$$

So, we have shown that inequality (*) is true when

$$n_0 = 1, c_2 > 0, c_1 \ge \max\{\frac{c_2 + 115}{3}, 104 - 2c_2\}.$$

Consequently, $T(n) = O(n^2 \log n)$. Q.E.D

Problem 10: [12 points]
Box A contains 3 white balls and 1 red ball, while Box B contains 4 white balls. One ball is randomly drawn from each box and the two balls are then randomly put back into the boxes so that each box still contains four balls. This process is repeated again and again. Let p_n be the probability that the red ball is in Box A after the process is repeated n times.

(a) What is p_1?

(b) For $n > 2$, express p_n in terms of p_{n-1}?

(c) Solve the recurrence from (b) to find a closed-form expression for p_n in terms of n.

Show your derivations.

[WORKSPACE FOR PROBLEM 10 INCLUDES THIS AND THE NEXT PAGE]

Answer: Let us first define some events:

- $E_{red-in-A}$: Red ball in A.
- $E_{red-from-A}$: Red ball drawn from box A.
- $E_{white-from-A}$: White ball drawn from box A.
- $E_{red-to-A}$: Red ball put back to box A.
- $E_{red-from-B}$: Red ball drawn from box B.

Let $P_n(E)$ of the probability of an event E after the process is repeated n times. Note that we want is $p_n = P_n(E_{red-in-A})$

(a) We have:

$$\begin{aligned} p_1 &= P_1(E_{red-in-A}) \\ &= P_0(E_{white-from-A}) + P_0(E_{red-from-A}) \times P_0(E_{red-to-A}) \\ &= \frac{3}{4} + \frac{1}{4} \times \frac{1}{2} = \frac{7}{8} \end{aligned}$$

[WORKSPACE FOR PROBLEM 10]

(b) After the process is repeated $n-1$ times, the red ball is in box A with probability p_{n-1} and it is in box B with probability $1-p_{n-1}$.

* If the red ball is in box A after $n-1$ times, then $P_n(E_{red-in-A}) = \frac{7}{8}$, as shown in (a).
* If the red ball is in box B after $n-1$ times, then

$$\begin{aligned} P_n(E_{red-in-A}) &= P_{n-1}(E_{red-from-B}) \times P_{n-1}(E_{red-to-A}|) \\ &= \frac{1}{4} \times \frac{1}{2} = \frac{1}{8} \end{aligned}$$

Putting those two cases together, we have

$$p_n = p_{n-1}\frac{7}{8} + (1-p_{n-1})\frac{1}{8} = \frac{3}{4}p_{n-1} + \frac{1}{8}$$

(c) Iterating the recurrence, we get:

$$\begin{aligned} p_n &= \frac{3}{4}p_{n-1} + \frac{1}{8} \\ &= \frac{3}{4}(\frac{3}{4}p_{n-2} + \frac{1}{8}) + \frac{1}{8} \\ &= (\frac{3}{4})^2 p_{n-2} + \frac{1}{8}(\frac{3}{4} + 1) \\ &= (\frac{3}{4})^2(\frac{3}{4}p_{n-3} + \frac{1}{8}) + (\frac{3}{4} + 1)\frac{1}{8} \\ &= (\frac{3}{4})^3 p_{n-3} + \frac{1}{8}((\frac{3}{4})^2 + \frac{3}{4} + 1) \\ &= \ldots \\ &= (\frac{3}{4})^n p_0 + \frac{1}{8}((\frac{3}{4})^{n-1} + \ldots + \frac{3}{4} + 1) \\ &= (\frac{3}{4})^n + \frac{1}{8}\frac{1-(\frac{3}{4})^n}{1-\frac{3}{4}} \\ &= \frac{1}{2} + \frac{1}{2}(\frac{3}{4})^n \end{aligned}$$

Student ID: ______________

Scrap Paper 1

Student ID: ______________

Scrap Paper 2

Student ID: ______________

Scrap Paper 3