EECS 70 Discrete Mathematics and Probability Theory
Spring 2013 Anant Sahai MT 1

PRINT your student ID: 3033084 0xx

PRINT AND SIGN your name: _____, _____ _____
(last) (first) (signature)

PRINT your Unix account login: cs70-_____
PRINT your discussion section and GSI: _____

Mark Here	Section	Time	Location	GSI
	1	9-10am	6 Evans	Ramtin
	2	10-11am	71 Evans	Ramtin
	3	11-12pm	71 Evans	Nima
	4	12-1pm	2 Evans	Nima
	5	1-2pm	87 Evans	Sridhar
	6	2-3pm	2070 VLSB	Sridhar
	7	3-4pm	85 Evans	Chung-Wei
	8	4-5pm	9 Evans	Chung-Wei
	9	5-6pm	9 Evans	Richard
	10	1-2pm	3105 Etch.	Chenyu
	11	2-3pm	151 Barr.	Kate
	12	4-5pm	B51 Hilde.	Richard
	13	6-7pm	70 Evans	Sibi
	14	12-1pm	101 Wheel.	Chenyu
	15	4-5pm	156 Dwin.	Sibi

Prob. 1	
Prob. 2	
Prob. 3	
Total	

Names of the people sitting next to you: _____

You may consult your one handwritten note sheet. **(You must turn it in with your exam.)** Phones, calculators, tablets, and computers are not permitted. No collaboration is allowed at all and you are not allowed to look at another's work.

Please write your answers in the spaces provided in the test; in particular, we will not grade anything on the back of an exam page unless we are clearly told on the front of the page to look there.

You have 120 minutes. There are 3 questions, of varying numbers of points. The questions are of varying difficulty, so avoid spending too long on any one question.

Do not turn this page until your instructor tells you to do so.

PRINT your name and student ID: _____

Problem 1. Stable Marriage (20 points)

a. (5 points) Assume that there are three men 1, 2, and 3 and three women A, B, and C. Their preference lists are given below.

Man	Preference List
1	$A > C > B$
2	$A > B > C$
3	$C > A > B$

Woman	Preference List
A	$3 > 1 > 2$
B	$2 > 3 > 1$
C	$1 > 2 > 3$

Is the pairing $\{(1,C),(2,A),(3,B)\}$ stable? Why?

Not stable.

(1, A) forms a rouge couple

b. (5 points) **Run the traditional propose and reject algorithm on the example above and write down the pairing that is produced.** Show your work (i.e. the intermediate steps of the algorithm).

	A	B	C
D1	1, ~~2~~		3
D2	1	2	3

2 days

(1, A) (2, B) (C, 3)

PRINT your name and student ID: _____

c. (10 points) Karl and Emma are having a disagreement regarding the traditional propose-and-reject algorithm. They both agree that it favors men over women. But they disagree about what, if anything, can be done without changing the ritual form of men proposing, women rejecting, and people getting married when there are no more rejections.

Karl mansplains: "It's hopeless. Men are obviously going to propose in the order of their preferences. It's male optimal so why would they do anything else? As far as the women are concerned, given that they face a specific choice of proposals at any given time, they are obviously going to select the suitor they like the most. So unless we smash the system entirely, it is going to keep all women down."

Emma says: "People are more perceptive and forward-looking that you think. Women talk to each other and know each other's preferences regarding men. They can also figure out the preferences of the men they might be interested in. A smart and confident woman should be able to do better for herself in the long run by not trying to cling to the best man she can get at the moment. By rejecting more strategically, she can simultaneously help out both herself and her friends."

Is Emma ever right? If it is impossible, prove it.

If it is possible, **construct and analyze an example (a complete set of people and their preference lists) in which a particular woman acting on her own (within the traditional ritual form of men proposing and women rejecting) can get a better match for herself while not hurting any other woman.** Show how she can do so. The resulting pairing should also be stable.

Emma is right

Example.

1	A	C	B
2	B	A	C
3	A	B	C

A	2	3	1
B	3	2	1
C	2	3	1

Emma's strategy.

	A	B	C
D1	1, ~~3~~	2	
D2	1	~~2~~, 3	
D3	~~1~~, 2	3	
D4	2	3	1

TMA

	A	B	C
D1	~~1~~, 3	2	
D2	3	2, ~~1~~	
D3	3	2	1.

TMA : (1, C). (2, B) (3, A)

Emma : (1, C) (3, B) (2, A). stable. harms no one

A, B get their favorite men.

Some thoughts: since between woman pessimal. man optimal. there might be several stable pairings. Using a god's view. woman can achieve their target.

PRINT your name and student ID: _____

Problem 2. [True or false] (48 points)

Circle TRUE or FALSE.

Prove all statements that you think are true and disprove (e.g. by showing a counterexample) all statements that you think are false.

Reminder: $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ represents the set of non-negative integers.

(a) TRUE or FALSE: Suppose that P, Q are propositions, $(\neg(P \Rightarrow Q))$ is logically equivalent to $(Q \Rightarrow P)$.

False.

$P \Rightarrow Q \equiv \neg P \vee Q \equiv$

$\neg(P \Rightarrow Q) \equiv \neg(\neg P \vee Q)$

$\equiv P \wedge \neg Q$

$Q \Rightarrow P \equiv \neg Q \vee P$

not equivalent.

P	Q	$P \Rightarrow Q$	$\neg(P \Rightarrow Q)$	$Q \Rightarrow P$
T	T	T	F	T
T	F	F	T	T
F	T	T	F	F
F	F	T	F	T.

(b) TRUE or FALSE: Consider the Fibonacci numbers

$$F(n) = \begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ F(n-1) + F(n-2) & \text{if } n \geq 2 \end{cases}$$

$F(n)$ is even if and only if n is a multiple of 3.

Induction.

1	2	3	4	5	6	7	8	9
1	1	2	3	5	8	13	21	34

BC: $k = 0$ ✓

IH: $k \in N$. $\wedge$ $n = 3k$. $F(3k) = 2d$. $d \in N$.

IS: $n = 3(k+1) = 3k+3$

$F(3k+3) = F(3k+2) + F(3k+1)$

$= F(3k+1) + F(3k) + F(3k+1)$

$= 2F(3k+1) + F(3k)$ (By IH)

$= 2(F(3k+1) + d)$ $F(3k+1) \in N$.

So $F(3k+3)$ is even.

PRINT your name and student ID: _____

(c) TRUE or FALSE: If $a \in \mathbb{N}$ and $m \in \mathbb{N}$ are such that $0 < a < m$ and $\gcd(a,m) = 1$, then $a^{m-1} = 1 \mod m$.

False. Fermat's Little Theorem. m is prime

$S = \{1, 2, \cdots, m-1\}$ $S' = \{a, 2a, \cdots, (m-1)a\}$

S. S' are same set. otherwise $(j-k) \cdot a \equiv 0 \mod m$

$(j-k)a = dm$.

not possible since

$j-k < m$. $\wedge$ $a < m$.

Multiply elements in S. S'

$(m-1)! \mod m$ $a^{m-1}(m-1)! \mod m$

However $\exists i \in \{1, 2, \cdots, m-1\}$ $\gcd(i, m) \neq 1$.

so multiplicative inverse does not exist. cannot cancel out.

So $a^{m-1} \not\equiv 1 \mod m$. e.g. $m = 4$ $a = 3$

$3^{4-1} = 27 \mod 4 = 3 \mod 4$.

(d) TRUE or FALSE: If n is an integer and $n^3 + 5$ is odd then n is even.

True. $(n \in \mathbb{Z} \wedge (n^3+5 = 2d+1 . d \in \mathbb{Z})) \Rightarrow n \in 2k. k \in \mathbb{Z}$.

5 is odd. even + odd = odd

odd + odd = ~~odd~~ even

So n^3 is ~~odd~~ even

To prove n^3 ~~odd~~ even $\Rightarrow$ n ~~od~~ even

proof by contraposition

n odd $\Rightarrow$ n^3 odd.

$n = 2k+1$ odd

$n^3 = 8k^3 + 12k^2 + 6k + 1$

$= 2(4k^3 + 6k^2 + 3k) + 1$ odd.

So true.

PRINT your name and student ID: _____

(e) TRUE or FALSE: $a \equiv b \mod m \Longrightarrow a^x \equiv b^x \mod m$ (assume that a, b, m, and x are all positive integers)

True.

Theorem: $a \equiv b \pmod m$. $c \equiv d \pmod m$

$a \cdot c \equiv b \cdot d \pmod m$

here $a \equiv b \pmod m$ ~~take~~ take $a \equiv c$. $b \equiv d$.

then $a \cdot a \equiv b \cdot b \mod m$.

and apparently. you can keep multiplying. it holds true for $a^x \equiv b^x \pmod m$

(f) TRUE or FALSE: $a \equiv b \mod m \Longrightarrow x^a \equiv x^b \mod m$ (assume that a, b, m, and x are all positive integers)

False

$x = 2$. $a = 3$. $b = 4$. $m = 3$.

$x^a = 2^3$

$x^b = 2^4$

$2^3 \bmod 3 = 2 \not\equiv 2^4 \bmod 3 = 1. \pmod 3$

$\pmod 3$

PRINT your name and student ID: _____

Problem 3. RSA. (45 points)

Rather than doing traditional RSA based on two prime numbers, suppose that your friend suggests using three prime numbers. She decides to use $N = 105 = 3 \cdot 5 \cdot 7$ and selects $e = 5$ so that the public key is $(N, e) = (105, 5)$.

a. (4 points) **Encrypt the message 2 using this public key.**

$E(m) = m^e \bmod N$

$E(2) = 2^5 \bmod 105$

$= 32 \bmod 105$

b. (6 points) **Encrypt the message 3 using this public key.**

$E(3) = 3^5 \bmod 105$

$= 33 \bmod 105.$

PRINT your name and student ID: _____

c. (15 points) **What property should the secret key d satisfy? Calculate what you think the secret key d should be for this public key** $(N = 105, e = 5)$. Explain your reasoning and show your work.

It is alright if you don't prove that this is the right property, proofs are required in the next part. No proofs needed in part c.

d = $e^{-1} \cancel{\text{mod}}$ 29 mod 48.

$e^{-1} \bmod (3-1)(5-1)(7-1)$

$= 5^{-1} \bmod 48$

$d = e^{-1} \bmod (p-1)(q-1)(r-1)$

$48a + 5b = 1$

$a = 2 \quad b = -19.$

inverse = 29 mod 48

PRINT your name and student ID: _____

d. (20 points) **Prove that the encryption function $E(x) = x^e \bmod N$ and the decryption function $D(y) = y^d \bmod N$ above are inverses.** (i.e. $\forall x, (0 \le x < N) \Rightarrow (D(E(x)) = x)$.)

(HINT: Follow the RSA proof from class and just adapt it for when there are three primes involved.)

prove

$x^{ed} \equiv x \bmod N$ for every $x \in \{0, 1, \dots, N-1\}$

$x^{ed} - x \equiv 0 \bmod N$

$x(x^{ed-1} - 1) \equiv 0 \bmod N$

case 1. x is multiple of N. done.

case 2. x not multiple of N.

$ed \equiv 1 \bmod (p-1)(q-1)(r-1)$

~~$\equiv 1 \bmod$~~

$ed = 1 + k(p-1)(q-1)(r-1)$.

$x(x^{ed-1} - 1) \equiv x(x^{k(p-1)(q-1)(r-1)} - 1)$ prove divisible by p

~~① $x^{p-1} \bmod p$~~

① since $x \not\equiv 0 \bmod p$. Fermat's Little Theorem. $x^{p-1} \equiv 1 \bmod p$

p is prime.

~~$x^{p-1} \equiv 1 \bmod p$~~

so $x(x^{k(p-1)(q-1)(r-1)} \equiv 1 \bmod p$ ~~so $x^{ed} - x \equiv 0 \bmod N$~~

②. prove divisible by q.

③. prove divisible by r.

so $x^{ed} - x \equiv 0 \bmod pqr$

$\equiv 0 \bmod N$.

$p = 3$. $q = 5$ $r = 7$.