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

PRINT your student ID: _____

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?**

**Solution:** No. There exists a rogue couple $(1,A)$. Man 1 prefers $A$ than his current partner $C$, and woman $A$ prefers man 1 than her current partner 2. Similarly $(3,A)$ also form a rogue 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).

**Solution:**

| Day | 1 | 2 |
|---|---|---|
| $A$ | (1), 2 | (1) |
| $B$ | | (2) |
| $C$ | (3) | (3) |

The produced pairing from Traditional Propose & Reject Algorithm is $\{(1,A),(2,B),(3,C)\}$.

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.

**Solution:** Emma is right. Here is an example of six people, three men $(1,2,3)$ and three women $(A,B,C)$, together with their respective preference lists. We're using the same one in the parts before.

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

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

We know what happens when we run the Traditional Propose & Reject Algorithm with these preference lists. We get the pairing $\{(1,A),(2,B),(3,C)\}$. But here, we can see that both $A$ and $C$ can do better.

Now, woman $A$ looks at the preference lists of all the men and women and notices something. If she doesn't cling to the best she can get at the moment, she can end up with someone better! Further, she can do so without hurting $B$ and $C$. Let's see how this plays out.

On day 1 of the Traditional Algorithm, we have the following proposals. The only change here is that $A$ now rejects 1 instead of 2 even though she likes 1 more among them.

| Day | 1 |
|---|---|
| $A$ | 1, (2) |
| $B$ | |
| $C$ | (3) |

Now, we continue from as normal, using the Traditional Propose & Reject Algorithm. Here are the remaining days.

| Day | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $A$ | 1, (2) | (2) | 2, (3) | (3) |
| $B$ | | | | (2) |
| $C$ | (3) | (1), 3 | (1) | (1) |

The pairing produced from the run above is $\{(3,A),(2,B),(1,C)\}$. We see that woman $A$ acting on her own on day one changed the face of the game for the women.

Is this pairing stable? Well, of course it is! Each woman ends up with the man she likes the most.

In conclusion, we can say with conviction that Emma was indeed right! A forward-think woman can potentially improve the ostensibly bleak outcome of the Traditional Propose & Reject Algorithm by strategically rejecting in the early stages.

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: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ 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 $(Q \Rightarrow P)$.

**Solution:** Consider the truth values of both statements:

| $P$ | $Q$ | $P \Rightarrow Q$ | $\neg(P \Rightarrow Q)$ | $Q \Rightarrow P$ |
|---|---|---|---|---|
| $T$ | $T$ | $T$ | $F$ | $T$ |
| $T$ | $F$ | $F$ | $T$ | $T$ |
| $F$ | $T$ | $T$ | $F$ | $F$ |
| $F$ | $F$ | $T$ | $F$ | $T$ |

(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.

**Solution:**

If we look at the Fibonacci numbers starting from index 0, we can see a repetitive pattern of "even, odd, odd, even, odd, odd..."

So first, let's establish this pattern with a proof.

We want to show by (strong) induction that $F(n)$ is even if $n$ is a multiple of 3 and is odd otherwise.

**Base Cases:**
$k = 0$. Then $F(0) = 0$ is even.
$k = 1$. Then $F(1) = 1$ is odd.
$k = 2$. Then $F(2) = 1$ is odd.
Thus, the statement holds for these base cases.

**Inductive Hypothesis:** Assume the statement is true for all $0 \leq j \leq k$, i.e. $F(j)$ is even if $j$ is a multiple of 3 and is odd otherwise.

**Inductive Step:** We want to show that $F(k+1)$ is even if $k+1$ is a multiple of 3 and is odd otherwise. Consider the following cases:

(a) Case $k+1 = 3t$ for some $t$: Then $F(k+1) = F(3t) = F(3t-1) + F(3t-2)$
Since both $F(3t-1)$ and $F(3t-2)$ are odd, their sum is even. So, $F(k+1) = F(3t)$ is even.

(b) Case $k+1 = 3t+1$ for some $t$: Then $F(k+1) = F(3t+1) = F(3t) + F(3t-1)$
Since $F(3t)$ is even and $F(3t-1)$ is odd, their sum is odd. So, $F(k+1) = F(3t+1)$ is odd.

(c) Case $k+1 = 3t+2$ for some $t$: Then $F(k+1) = F(3t+2) = F(3t+1) + F(3t)$
Since $F(3t)$ is even and $F(3t+1)$ is odd, their sum is odd. So, $F(k+1) = F(3t+2)$ is odd.

Thus, we have shown that the pattern we described above indeed holds. Now, we can go about proving the statement in the question. We must prove two directions:

If $n$ is a multiple of 3, then $F(n)$ is even.
This is just what we showed above.

If $F(n)$ is even, then $n$ is a multiple of 3. Instead of proving this statement, let's look at its contrapositive. If $n$ is not a multiple of 3, then $F(n)$ is not even. Again, this is exactly what we showed above.

Thus, we have proved that $F(n)$ is even if and only if $n$ is a multiple of 3.

(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 $a^{m-1} = 1 \mod m$.

**Solution:** Choose $a = 3$ and $m = 8$. We see that the two numbers satisfy the constraints as they are both positive integers, coprime, and $a < m$. Using repeated squaring, one can calculate $3^7 \mod 8$ to be:

$$3^2 = 9 \mod 8 = 1$$
$$3^4 = (3^2)^2 \mod 8 = 1$$
$$3^7 = 3^{4+2+1} = 3^4 \cdot 3^2 \cdot 3^1 = 1 \cdot 1 \cdot 3 = 3 \neq 1 \mod 8$$

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

**Solution:** Proof by contrapositive. Suppose $n$ is an odd integer. We want to show that $n^3 + 5$ is even. Since $n$ is odd, we can express it as $n = 2k + 1$ for some integer $k$. It's easy to see that the product of odd integers are odd, or in this case, we can show arithmetically that $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1$, which is odd. The sum of $n^3$, an odd number, and 5, another odd number, is even, which is what we set out to prove.

So by contrapositive: If $n$ is an integer and $n^3 + 5$ is odd then $n$ is even.

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

**Solution:** We proved this by induction on $x$ as followed:

**Base Case:** $x = 1$. Then $a \equiv b \mod m$ as given. Thus, the base case for $x = 1$ is true. By definition of congruent modulo, we also know that $b = a + km$ for some integer $k$.

**Inductive Hypothesis:** Assume the statement is true for $x = n$, i.e. $a^n \equiv b^n \mod m$. By definition of congruent modulo, we also know that $b^n = a^n + lm$ for some integer $l$.

**Inductive Step:** We want to show that for $x = n+1$, $a^{n+1} \equiv b^{n+1} \mod m$. Expanding the right side, we have:

$$\begin{aligned} b^{n+1} &= b^n \cdot b \mod m \\ &= (a^n + lm)(a + km) \mod m \quad \text{(By the Inductive Hypothesis and Base Case)} \\ &= a^{n+1} + m(ka^n + la + lmk) \mod m \\ &\equiv a^{n+1} \mod m \end{aligned}$$

By induction, we have shown that $a \equiv b \mod m \implies a^x \equiv b^x \mod m$.

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

**Solution:** Find a counterexample. One that would work in this case is, $a = 1$, $b = 4$, $m = 3$, and $x = 2$. One can easily see that $1 \equiv 4 \mod 3 = 1$. However, $2^1 = 2 \mod 3 = 2$, whereas $2^4 = 16 \mod 3 = 1$. Thus, the original claim is false.

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.**

**Solution:** To encrypt the message 2, we want to compute the value $E(x) = x^e \mod N = 2^5 \mod 105 = 32$.

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

**Solution:** Similarly, to encrypt the message 3, we want to compute the value $E(x) = x^e \mod N = 3^5 \mod 105 = 243 \mod 105 = 33$.

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.

$d =$ **29**

**Solution:** Let the three primes number be $p, q, r$ respectively. In this problem, $p = 3, q = 5, r = 7$. Hence, $(p-1)(q-1)(r-1) = 2 \cdot 4 \cdot 6 = 48$. We want to calculate the number $d$ such that $d$ is the inverse of $e$ mod $(p-1)(q-1)(r-1)$, or 5 mod 48. We can apply the Extended Euclid's algorithm `extended-gcd(48, 5)`:

| Function Calls | $(x, y)$ | $x$ div $y$ | $x$ mod $y$ |
|---|---|---|---|
| #1 | $(48, 5)$ | 9 | 3 |
| #2 | $(5, 3)$ | 1 | 2 |
| #3 | $(3, 2)$ | 1 | 1 |
| #4 | $(2, 1)$ | 2 | 0 |
| #5 | $(1, 0)$ | __ | __ |

The returned values of all recursive calls are:

| Function Calls | $(d, a, b)$ | Returned Values |
|---|---|---|
| #5 | __ | $(1, 1, 0)$ |
| #4 | $(1, 1, 0)$ | $(1, 0, 1)$ |
| #3 | $(1, 0, 1)$ | $(1, 1, -1)$ |
| #2 | $(1, 1, -1)$ | $(1, -1, 2)$ |
| #1 | $(1, -1, 2)$ | $(1, 2, -19)$ |

Therefore, we get $-19 \cdot 5 + 2 \cdot 48 = 1$. A valid, positive value of $d$ would be $-19 + 48 = 29$.

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. $\forall x, (0 \leq x < N) \Rightarrow (D(E(x)) = x)$.)

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

**Solution:** As seen in lecture, we need to show that $(x^e)^d = x \mod N$. We first consider the exponent $ed$. By definition of $d$, we know that $ed = 1 \mod (p-1)(q-1)(r-1)$; hence we can write $ed = 1 + k(p-1)(q-1)(r-1)$ for some integer $k$, and therefore $x^{ed} - x = x^{1+k(p-1)(q-1)(r-1)} - x = x(x^{1+k(p-1)(q-1)(r-1)} - 1)$

Our goal is to show that this last expression is equal to $0 \mod N$ for every $x$. To do so, we claim that it is divisible by $p$, of which there are two cases:

**Case 1**: *$x$ is not a multiple of $p$.* In this case, $x \neq 0 \mod p$, we can use Fermat's Little Theorem to deduce that $x^{p-1} = 1 \mod p$, and hence $x^{1+k(p-1)(q-1)(r-1)} - 1 = 0 \mod p$, as required.

**Case 2**: *$x$ is a multiple of $p$.* In that case, the expression $x(x^{1+k(p-1)(q-1)(r-1)} - 1)$ clearly has a factor of $x$, so it is divisible by $p$.

By an entirely symmetrical argument, $x(x^{1+k(p-1)(q-1)(r-1)} - 1)$ is also divisible by $q$ and $r$. Therefore, it is divisible by all three numbers, all of which are prime; thus, it must be divisible by their product, $pqr = N$. But this implies that the expression is equal to $0 \mod N$, which is exactly what we want to prove.

PRINT your name and student ID: _____

[Extra Page.]