EECS 70 Discrete Math and Probability
Spring 2020 UC Berkeley

Midterm 1

Exam location: Wheeler Auditorium

PRINT your student ID: ____

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

PRINT your discussion section and GSI (the one you attend): ____

Row Number (front row is 1): __________ Seat Number (left most is 1): __________

Name and SID of the person to your left: ____

Name and SID of the person to your right: ____

Name and SID of the person in front of you: ____

Name and SID of the person behind you: ____

Section 0: Pre-exam questions (3 points)

1. **What other courses are you taking this term? (1 pt)**

2. **Think back to remember a moment where something in some course really clicked for you. Describe it. How did you feel? (2 pts)**

Do not turn this page until the proctor tells you to do so. You can work on Section 0 above before time starts.

PRINT your name and student ID: ____

[Extra page. If you want the work on this page to be graded, make sure you tell us on the problem's main page.]

PRINT your name and student ID: ______________________________

3. **Short Answer (8 pts)**

These are all short answer questions. Write your final answers inside the appropriate boxes. You don't need to justify your answer, just show whatever work that you actually had to do outside the box.

(a) (2 pts) **Fill in the truth-table for** $\neg Q \implies P$:

P	Q	$\neg Q \implies P$
T	T	
T	F	
F	T	
F	F	

(b) (1 pt) **Find the multiplicative inverse of 18 mod 73.** Your answer should be an integer in $\{0,1,2,\ldots,72\}$. To spare you some calculations, note that: $73 - 4 * 18 = 1$

(c) (3 pts) **Find** 42^{1601} mod 17. Your answer should be an integer in $\{0,1,2,\ldots,16\}$.

(d) (2 pts) For distinct primes p and q, **how many numbers in the set** $\{0,1,\ldots,pq-1\}$ **do not have a multiplicative inverse modulo** pq**?**

PRINT your name and student ID: ____

4. A proof (6 pts)

Suppose x, y are integers. **Prove that if xy and $x+y$ are both even, then both x and y must be even.**

PRINT your name and student ID: ______________________________

5. Multi-GCD (8 pts)

In this problem we quickly explore a generalization of the GCD and EGCD algorithms to more than two numbers at a time. For natural numbers $n_1, n_2, \ldots, n_k \in \mathbb{N}$, let $\text{GCD}(n_1, n_2, \ldots, n_k)$ denote the largest natural number which divides each of $n_1, n_2, \ldots, n_k$.

One thing that we observe is that $\text{GCD}(a,b,c) = \text{GCD}(a, \text{GCD}(b,c))$.

This fact also allows us to naturally extend the EGCD algorithm to more than two integers. **Find** $a,b,c \in \mathbb{Z}$ **such that** $21a + 15b + 35c = 1$**.**

Here are some calculations that might be helpful: $35 - 2*15 = 5$ and $21 - 4*5 = 1$.

$a =$

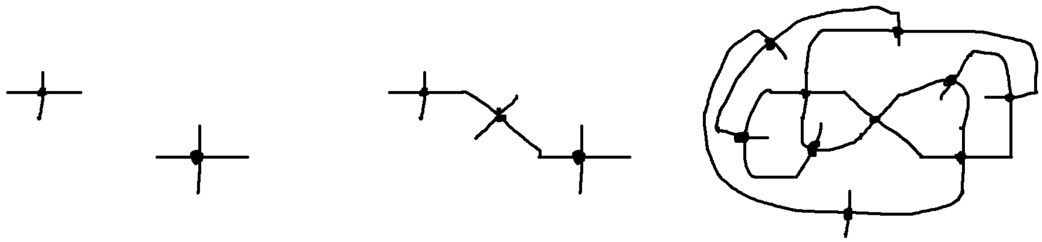
$b =$

$c =$

6. Graph Game (21 pts)

Alice and Bob are playing a game where they take turns drawing on a piece of paper. Alice goes first and Bob goes second. The rules of the game are as follows:

- We start off with n crosses, i.e. spots with four free ends.
- During their turn, a player must connect any two free ends with a curve, provided the curve does not intersect any existing curves or crosses, and then add a stroke across the curve to create two more free ends.
- If any player cannot move, they lose the game.



Above, we have an example of states of a game with $n = 2$ at the start, after one move, and after the game has concluded.

(a) (6 pts) Note that the graph formed by the curves is always planar. Assume that the center of each cross is a vertex and any intersection of a curve with a stroke is also a vertex. The curves connecting two vertices are edges. *Note that each move in the game therefore is adding two edges even though it is described as drawing a single curve.*

After m moves have been made, how many vertices, edges, and free ends are there on the paper? Recall that at $m = 0$, we start with $v(0) = n$ vertices, $e(0) = 0$ edges, and $f_e(0) = 4n$ free ends.

$v(m) =$

$e(m) =$

$f_e(m) =$

(b) (3 pts) When the game concludes, the graph must be connected and planar. A planar graph subdivides the plane into faces. **How many free ends can be in a face of this concluding planar graph?** *(HINT: Remember, no more moves can be made when the game is over.)*

PRINT your name and student ID: ______________________________

(c) (12 pts) Since Alice goes first and Bob and Alice alternate turns, Alice plays odd numbered moves and Bob plays even numbered ones. **For which n does Alice win and for which n does Bob win?** Justify your answer.

(HINT: Euler's formula says that $v + f = e + 2$ for connected planar graphs. The answers from the previous parts can help here.)

PRINT your name and student ID: ____

7. Toy Stability (38 pts)

Edward is babysitting n kids. He has n toys and wants to distribute them to the kids so that every kid gets a toy. Every kid has a preference list towards the n toys. Edward's goal is to reach a **stable pairing**, which is defined to be a pairing in which *there doesn't exist a rogue group of kids who can exchange their toys among each other with everyone in the group getting a more preferred toy.*

Note: in this problem, toys are inanimate and so have no preferences of their own.

(a) (6 pts) Let $n = 3$ and let the preference list of the 3 kids (1, 2, 3) towards 3 toys (A, B, C) be as follows:

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

Determine whether each of the following is a stable pairing. Fill in the appropriate bubble.

i. (1, A), (2, B), (3, C) ○ **Stable** ○ **Not Stable**

ii. (1, A), (2, C), (3, B) ○ **Stable** ○ **Not Stable**

iii. (1, B), (2, C), (3, A) ○ **Stable** ○ **Not Stable**

(b) (10 pts) Edward comes up with an algorithm to distribute the toys via a game. It proceeds in the following steps:

i. Start the epoch counter, a global variable for this algorithm, at 1.

ii. Initially pair each kid with a toy randomly, ask them to hold their tentative toy, and place all kids (holding their tentative toy) in the center of the room. All these kids and toys in the center of the room are considered to be in the game.

iii. Ask each kid still in the game to point to the person in the game who holds their most preferred toy among all the toys **that are still in the game**. Treat this as a directed graph in which the kids in the game are vertices and the edges represent who they are pointing to.

iv. If there is a directed cycle in the graph (including potentially a cycle of length 1 where a person is just pointing to themselves), then arbitrarily pick such a cycle. This is called a “trading cycle.”

v. For every kid in the picked trading cycle, assign them the toy that they are pointing to. In addition, give each of these kids a card that says the current epoch number. Send these kids outside the room, thereby removing them and their assigned toys from the game. All the kids still in the game cross off the removed toys from their preference lists.

vi. If there are still kids in the game, increment the epoch number by one and repeat from step iii. Otherwise, the game has concluded and every kid has been assigned a toy.

Execute the algorithm for the following preference list for $n = 6$ starting from the initial pairing $(1,A),(2,B),(3,C),(4,D),(5,E),(6,F)$**.** You only need to provide the final pairing in the box.

Kid	Preference List
1	$C > B > D > A > F > E$
2	$C > E > F > A > D > B$
3	$C > A > D > E > F > B$
4	$B > E > F > D > A > C$
5	$A > C > B > D > E > F$
6	$B > D > E > F > A > C$

(1,   ), (2,   ), (3,   ), (4,   ), (5,   ), (6,   )

PRINT your name and student ID: ____

(c) (8 pts) For the general algorithm given, **prove that if there are still kids in the game, there must be at least one trading cycle (including possibly a cycle of length 1).**

(HINT: Remember, the kids are vertices and the directed edges represent which kid/toy they are pointing at. What must happen as we walk along these edges?)

(d) (4 pts) **Prove that the algorithm must terminate if started with a finite number n of kids and toys.** Feel free to assume the previous part, even if you didn't get the proof.

PRINT your name and student ID: ____

(e) (10 pts) **Show that the algorithm produces a stable pairing.**
(HINT: The kids' epoch numbers and the well-ordering principle might be helpful.)

PRINT your name and student ID: ____________________

8. RSA with three primes, two exponents, and a glitch (15 pts)

Suppose you have three distinct primes p, q, r and positive natural numbers e_1 and e_2 that are both coprime with $p-1, q-1$, and $r-1$.

Suppose further that x is a natural number from $1, 2, \ldots, pqr-1$. Let $y_1 = x^{e_1} \bmod pqr$ and $y_2 = x^{e_2} \bmod pqr$ be two different encryptions of x.

There was a glitch and you lose both y_1 and y_2. Suppose you only have access to $y_p = y_1 \bmod p$ and $y_q = y_1 \bmod q$ from the first encryption, and $y_r = y_2 \bmod r$ from the second encryption.

Give an explicit way to recover x from these three numbers y_p, y_q, y_r, given knowledge of p, q, r, e_1, e_2. Describe all computations that you would have to do. You may invoke egcd as a subroutine freely, as well as standard mod operations of addition, multiplication, and exponentiation.

(HINT: You might want to recover x_p, x_q, x_r first.)

PRINT your name and student ID: ________________________________

[Extra page. If you want the work on this page to be graded, make sure you tell us on the problem's main page.]

PRINT your name and student ID: ____

9. Secret Sharing (30 pts)

There is a 100 bit-long secret s that we want to distribute among ten people so that if any two of them get together, they can reconstruct the secret but any one of them on their own learns essentially nothing about the secret. We number the ten people $0, 1, \ldots, 9$.

Instead of using the exact scheme described in lecture and homework, this problem asks you to investigate some variant schemes.

(a) (10 pts) We pick a prime number q that is 101 bits long. We use this q to work within $GF(q)$. We roll a q-sided die to get a number f from $0, 1, \ldots, q-1$. We use Lagrange interpolation to construct a degree 1 polynomial $P(x)$ with coefficients from $GF(q)$ so that $P(x)$ passes through the points $P(10) = s$ and $P(11) = f$. To person i, we distribute the secret share $y_i = P(i)$.

Describe exactly how you would recover the secret from any two people getting together. Everyone knows the scheme that is being used, and in particular, knows their own number, the prime number q, and the fact that $P(x)$ must be a degree 1 polynomial.

(b) (8 pts) For the scheme described in the previous part, **explain why any one person on their own has learned essentially nothing about the secret that they didn't already know before they got their secret share.**

(HINT: You need to show that based on what they know, they cannot rule out any possible value for the secret s.)

PRINT your name and student ID: ____

(c) (12 pts) Here is an alternative scheme. We pick a collection of twelve prime numbers $q_0, q_1, \ldots, q_{11}$ that are each 101 bits long (they are all actually bigger than 2^{100}) and arranged in decreasing order $q_0 > q_1 > \cdots > q_{11}$. We roll a q_{11} sided die to get a number f from $0, \ldots, q_{11} - 1$. We then compute the number $p = (sv_{10} + fv_{11}) \bmod q_{10}q_{11}$ where v_{10} is the smallest natural number such that $v_{10} \bmod q_{10} = 1$ and $v_{10} \bmod q_{11} = 0$, and similarly v_{11} is the smallest natural number such that $v_{11} \bmod q_{10} = 0$ and $v_{11} \bmod q_{11} = 1$.

To person i, we distribute the secret share $y_i = p \bmod q_i$. Note that each share is at most 101 bits long.

Describe exactly how you would recover the secret from any two people getting together. You can assume that everyone knows all the primes q_i — this list of primes isn't secret.

(HINT: What is p mod q_{10}?)

PRINT your name and student ID: ________________________________

[Doodle page! Draw us something if you want or give us suggestions or complaints. You can also use this page to report anything suspicious that you might have noticed.]