

PRINT Your Name: _____,
(Last) (First)

READ AND SIGN The Honor Code:

As a member of the UC Berkeley community, I act with honesty, integrity, and respect for others.

Signed: _____

PRINT Your Student ID: _____

WRITE your exam room: _____

WRITE the name of the person sitting to your left: _____

WRITE the name of the person sitting to your right: _____

PLEASE READ THE FOLLOWING INSTRUCTIONS CAREFULLY

- After the exam starts, please *write your student ID on every page*. **You will not be allowed to write anything once the exam ends.**
- We will not grade anything outside of the space provided for a problem unless we are clearly told in the space provided for the question to look elsewhere. We will not grade scratch paper, all work must be on exam.
- The questions vary in difficulty. If you get stuck on any one, it helps to leave it and try another one.
- In general, no justification on short answer/true false questions is required unless otherwise indicated. Write your answers in boxes where provided.
- Calculators are not allowed. **You do NOT need to simplify any probability related answers to a decimal fraction**, but your answer must be in the simplest form (no summations or integrals).
- You may consult only *3 sheets of notes*. Apart from that, you are not allowed to look at books, notes, etc. Any electronic devices such as phones and computers are NOT permitted.
- Regrades will be due quickly so watch piazza.
- There are **19** double sided pages on the exam. Notify a proctor immediately if a page is missing.
- You have **180** minutes: there are **6** sections with a total of **68** parts on this exam worth a total of **243** points.

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

1. Discrete Math: True/False (12 parts: 3 points each.)

1. $(\forall x, \forall y) \neg P(x, y) \equiv \neg \exists y, \exists x, P(x, y)$

↳ not + ple satisfies

True

False

2. $(P \implies Q) \equiv (Q \implies P)$

↳ converse

True

False

3. Any simple graph with n vertices can be colored with $n-1$ colors.

↳ n max $K_n \rightarrow \text{deg}(v) = n-1 + 1$

True

False

4. The set of all finite undirected graphs is countable.

↳ $|V|=n \rightarrow \# = K_n$
 ↳ binary strings

True

False

5. The function $f(x) = ax \pmod N$ is a bijection from and to $\{0, \dots, N-1\}$ if and only if $\text{gcd}(a, N) = 1$.

$f^{-1}(y) = a^{-1}y = x$

True

False

6. For a prime p , the function $f(x) = x^d \pmod p$ is a bijection from and to $\{0, \dots, p-1\}$ when $\text{gcd}(d, p-1) = 1$.

$f^{-1}(y) = x^{d^{-1}} \rightarrow 1 \equiv \text{mod } p-1$
 $d \equiv d^{-1} \pmod{p-1}$
 $x^{d \cdot d^{-1}} = x \pmod p$

True

False

7. A male optimal pairing cannot be female optimal.

True

False

8. For any undirected graph, the number of odd-degree vertices is odd.

$\sum \text{deg}(v) = 2e$ (even)

True

False

9. For every real number x , there is a program that given k , will print out the k th digit of x .

True

False

10. There is a program that, given another program P , will determine if P halts when given no input.

True

False

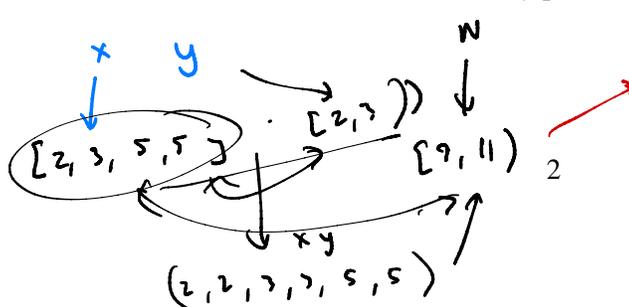
11. Any connected simple graph with n vertices and exactly n edges is planar.

↳ tree + 1 $\rightarrow e \leq 3v - 6$
 $3 \leq 4 - 6 \rightarrow 3$

True

False

12. Given two numbers, x and y , that are relatively prime to N , the product xy is relatively prime to N .



True

False

2. Discrete Math: Short Answer (10 parts: 4 points each)

1. If $\gcd(x, y) = d$, what is the least common multiple of x and y (smallest natural number n where both $x|n$ and $y|n$)? [Leave your answer in terms of x, y, d]

Handwritten notes for Q1: $\exists \frac{x}{d} = i$, $\exists \frac{y}{d} = j$. lcm $\begin{matrix} n|i & x \\ n|j & y \end{matrix}$. $i \cdot j \cdot d$. $\frac{x}{d} \cdot \frac{y}{d} \cdot d \rightarrow \frac{xy}{d}$. $\frac{xy}{d}$

2. Consider the graph with vertices $\{0, \dots, N-1\}$ and edges $(i, i+a) \pmod N$ for some $a \not\equiv 0 \pmod N$. Let $d = \gcd(a, N)$. What is the length of the longest cycle in this graph in terms of some subset of N, a , and d ?

Handwritten notes for Q2: $i, i+a$. $i + k \cdot a \equiv x \pmod N$. $N_j d \rightarrow \frac{N}{d} \cdot d \rightarrow N_j$. $k \cdot a \equiv 0 \pmod N$. $k = \frac{N}{d}$. $\frac{N}{d}$

3. What is the minimum number of women who get their favorite partner (first in their preference list) in a female optimal stable pairing? (Note that the minimum is over any instance.)

4. What is the number of ways to split 7 dollars among Alice, Bob and Eve? (Each person should get an whole number of dollars.)

Handwritten notes for Q4: stars and bars. $\binom{7+2}{2} = \binom{9}{2}$.

5. What is $6^{24} \pmod{35}$?

Handwritten notes for Q5: $a \equiv b \pmod{m}$. $6^4 \equiv 1 \pmod{35}$. 57 .

6. If one has three distinct degree at most d polynomials, $P(x), Q(x), R(x)$, what is the maximum number of intersections across all pairs of polynomials?

Recall that we define intersections to be two polynomials having the same value at a point. (That is if $P(1) = Q(1)$, and $P(2) = R(2)$ and $R(3) = Q(3)$, that is three intersections. If they all meet at a point $P(1) = Q(1) = R(1)$, that is three intersections.)

Handwritten notes for Q6: $d+1$. $3d$. $P(x) \rightarrow d+1$. $Q(x) \rightarrow d+1$. $R(x) \rightarrow d+1$. $(3,2), (2,4), (1,5)$. $(3,2), (2,4), (1,6)$.

7. Working modulo a prime $p > d$, given a degree exactly d polynomial $P(x)$, how many polynomials $Q(x)$ of degree at most d are there such that $P(x)$ and $Q(x)$ intersect at exactly d points?

$$\binom{p}{d} (p-1)$$

8. Recall that the vertices in a d -dimensional hypercube correspond to $0-1$ strings of length d . We call the number of 1's in this representation the **weight** of a vertex.

- (a) How many vertices in a d -dimensional hypercube have weight k ?

weight $k \rightarrow k$ out bits

$$\binom{d}{k}$$

- (b) How many edges are between vertices with weight at most k and vertices with weight greater than k ?

$\binom{d}{k} (d-k)$

k is out of d $(d-k)$

d is 1

9. How many elements of $\{0, \dots, p^k - 1\}$ are relatively prime to p ?

$p^k - p^{k-1}$

$\rightarrow \lfloor N/a \rfloor$

$p^k - p^{k-1}$

3. Some proofs. (3 parts. 5/5/8 points.)

1. Recall for x, y , with $\gcd(x, y) = d$, that there are $a, b \in \mathbb{Z}$ where $ax + by = d$. Prove that $\gcd(a, b) = 1$.

$X = \text{Max}(X_1, X_2)$ → cont → iid
↳ order

$$P(X \leq x) = [P(X_1 \leq x) \cdot P(X_2 \leq x)]$$
↳
(X₁) (X₂) → iid ↳ V = min(X₁, X₂)
↳ X₁ or X₂

$$\text{cov}(X_1, X_2) = |X_1 - X_2| = \text{max}(X_1, X_2) - \text{min}(X_1, X_2)$$

2. You have n coins. The probability of the i th coin being heads is $1/(i+1)$ (i.e., the biases of the coins are $\frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{n+1}$). You flip all the coins. What is the probability that you see an even number of heads? Prove it. (Hint: the answer is quite simple.)

↳ for even number of heads ↳ 1 tails but even
↳ 1 head
↳ odd number ↳ 1 heads but odd
↳ 1 tails
 $\Omega \rightarrow (1/2)$ even

$$P(X=i \cap X=j) = 0$$
↳
{0, 1, 2}

$$\pi(0) = \pi(1) + \pi(2)$$
 $P(1,0) \quad P(2,0)$

$$\pi(i) = \pi(0) \cdot P(0,1)$$

SID:

3. Consider a game with two players alternating turns. The game begins with $N > 0$ flags. On each turn, each player can remove 1, 2, 3, or 4 flags. A player wins if they remove the last flag (even if they removed several in that turn).

Show that if both players play optimally, player 2 wins if N is a multiple of 5, and player 1 wins otherwise.

4. Probability: True/False. (7 parts, 3 points each.)

1. For a random variable X , the event " $X = 3$ " is independent of the event " $X = 4$ ".
 True
 False
2. Let X, Y be Normal with mean μ and variance σ^2 , independent of each other. Let $Z = 2X + 3Y$. Then, $LLSE[Z | X] = MMSE[Z | X]$.
 True
 False
3. Any irreducible Markov chain where one state has a self loop is aperiodic.
 True
 False
4. Given a Markov Chain, let the random variables X_1, X_2, X_3, \dots , where X_t = the state visited at time t in the Markov Chain. Then $E[X_t | X_{t-1} = x] = E[X_t | X_{t-1} = x \cap X_{t-2} = x']$.
 True
 False
5. Given an expected value μ , a variance $\sigma^2 \geq 0$, and a probability p , it is always possible to choose a and b such that a discrete random variable X which is a with probability p and b with probability $1 - p$ will have the specified expected value and variance.
 True
 False
6. Consider two random variables, X and Y , with joint density function $f(x, y) = 4xy$ when $x, y \in [0, 1]$ and 0 elsewhere. X and Y are independent.
 True
 False
7. Suppose every state in a Markov chain has exactly one outgoing transition. There is one state, s , whose outgoing transition is a self-loop. All other states' outgoing transitions are not self-loops. If a unique stationary distribution exists, it must have probability 1 on s and 0 everywhere else.
 True
 False

5. Probability: Short Answer. (17 parts, 4 points each.)

1. Consider $X \sim G(p)$, a geometric random variable X with parameter p . What is $Pr[X > i | X > j]$ for $i \geq j$?

2. Suppose we have a random variable, X , with pdf

$$f(x) = \begin{cases} cx^2, & \text{if } 0 \leq x \leq 1 \\ 0, & \text{otherwise} \end{cases}$$

What is c ?

3. Given a binomial random variable X with parameters n and p , ($X \sim B(n, p)$) what is $Pr[X = E[X]]$? (You should assume pn is an integer.)

4. $Pr[A|B] = 1/2$, and $Pr[B] = 1/2$, and A and B are independent events. What is $Pr[A]$?

5. Aaron is teaching section and has 6 problems on the worksheet. The time it takes for him to finish covering each question are i.i.d. random variables that follow the exponential distribution with parameter $\lambda = 1/20$. Additionally, for each question, Aaron may choose to skip it entirely with probability $p = 1/3$. What is the expected time of section?

6. Let X be a uniformly distributed variable on the interval $[3, 6]$. What is $\text{Var}(X)$?

Answer

↳ 1)

Short Answer T/F

↳ 1) T → if all F_{xy} tuples $\rightarrow P(x,y)$
then there cannot exist K_y tuple $\rightarrow P(x,y)$

2) F

3) max graph K_n n vertices
 $K_n \rightarrow \begin{cases} \text{deg}(v) = n-1 \\ \text{+1 color for } v \Rightarrow n \text{ colors} \end{cases}$
 ↳ F

4) undirected graph \rightarrow binary string finite

↳ \Rightarrow countable

not $N=6 \quad a=3$

$f(x) = 3x \pmod 6$

1	\rightarrow	3	\rightarrow	only cover 3 groups
2	\rightarrow	0		
3	\rightarrow	3		9-6
4	\rightarrow	0		12
5	\rightarrow	3		15-12
0	\rightarrow	0		

inverse functions

5) $f(x) = ax \pmod N$ bijection only if $f^{-1}(x)$ exist \Rightarrow bijection \rightarrow true

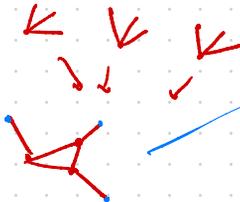
6) cond that allows inverse to exist
 ↳ $f^{-1}(x) = x^e \pmod p$ st $e = d^{-1} \pmod{p-1}$

$$\begin{aligned} & x^{de} \pmod p \\ & \downarrow x^{(p-1)+1} \rightarrow \text{FLT} \\ & \downarrow x \pmod p \end{aligned}$$

7) Not slope

8) $\sum \text{deg}(v) = 2E$
 if \exists odd $\text{deg}(v)$ is odd \rightarrow not $2E$ contra

↳



nothing other side

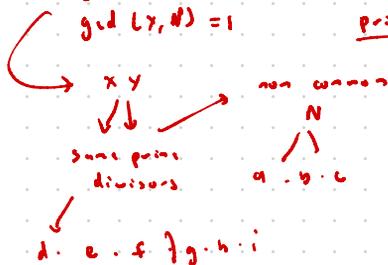
11) n vertex exactly n edges tree always planar 1 face
 ↳ tree \rightarrow

$$\begin{aligned} n &\leq 3n - 6 \\ 2 &\leq 4 - 6 \rightarrow \underline{3 \leq 3} \quad \checkmark \end{aligned}$$



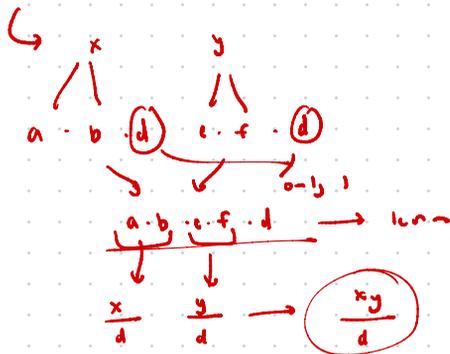
11) xy coprime to N

$\Rightarrow \text{gcd}(x, N) = 1 \rightarrow$ no common prime divisors
 $\text{gcd}(y, N) = 1$



2) short answer discrete

1) $\text{gcd}(x, y) = d$ $\text{lcm}(x, y)$



2) steps needed to get back to i

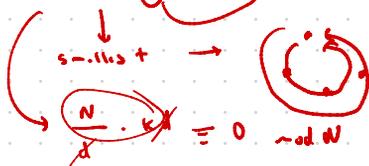
$i + ja \equiv i \pmod{N}$

steps $d = \text{gcd}(a, N)$

$ja \equiv 0 \pmod{N}$

$j \cdot kd \equiv 0 \pmod{N}$

$N \cdot kd \equiv 0$ times around



3) St. bin. Multibig

4) 7 stars 2 bins $\rightarrow 3-1$
 $\hookrightarrow \binom{9}{2}$

5) $a^{24} \pmod{35}$ \rightarrow $\begin{matrix} 7 \cdot 5 \\ 6 \cdot 4 \end{matrix}$
 $\hookrightarrow 1 \rightarrow a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$
 $\rightarrow a^{24} \equiv 1 \pmod{35} \Rightarrow$

6) all distinct \rightarrow $PL(x) \rightarrow \left[\begin{matrix} d+1 \\ \text{points} \end{matrix} \right]$
 \rightarrow must differ from each by at least 1 point
 $\Rightarrow 3d \rightarrow (d+1) \cdot 3$
 \uparrow
for each

7) $\binom{p}{d}$

bits

8) a) $\binom{d}{k} \rightarrow$ where ones are

b) $\binom{d}{k} (d-k)$

\hookrightarrow where zeros

\rightarrow turn into 1

that weight here is weight $k+1$



9) $a \in \mathbb{Z}_0 \dots p^k - 1$ | $\text{gcd}(a, p) = 1$

\hookrightarrow # relatively prime p

$\rightarrow p^k$ bits $\rightarrow p^{k-1} = \frac{p^{k-1}(p-1)}{p-1}$

$\hookrightarrow \frac{p^k}{p} = p^{k-1}$

\hookrightarrow every $e \exists \text{gcd} \neq 1$

3) 1) $\text{gcd}(a, b) = 1$

$$\begin{aligned} \left. \begin{array}{l} x, y \\ \downarrow \quad \downarrow \\ i \cdot d \quad j \cdot d \end{array} \right\} & \rightarrow a(i \cdot d) + b(j \cdot d) = d \\ & a i + b j = 1 \\ & \Rightarrow \text{gcd}(a, b) = 1 \end{aligned}$$

↳ using groups of a & b
can reach 1 which means
can't be common groups

2) inductively calculate

$$\left\{ \begin{array}{l} P(E_1) = 1/2 \end{array} \right. \rightarrow \begin{array}{l} \text{even heads for} \\ i \text{ coins} \end{array}$$

$$P(E_2) = P(\overset{\text{odd}}{E_1} \text{ and tails on } 2) \text{ or } P(\overset{\text{even}}{E_1} \text{ and tails on } 2)$$

$$\left\{ \begin{array}{l} 1/2 \cdot (1/2) + 1/2 \cdot (1 - 1/2) = \frac{1}{2} \end{array} \right.$$

↳ initial flip matters

↳ \forall group of coins \rightarrow an opposite $\frac{1}{2}$ likely odd arrangement

↳ change 1st coin $\rightarrow \frac{1}{2}$

3) Induct

↳ BL of NE $\{1, 2, 3, 4\}$

↳ remove all wins

Induction

↳ N not multiple of 5

↳ P_1 remove $\{1, 2, 3, 4\}$ to make multiple of 5

P_2 must remove $\{1, 2, 3, 4\}$ to make not multiple of 5

↳ indat still BL and left with and P_1 turn

$\{1, 2, 3, 4\} \rightarrow$ win P_1

4 Prob)

T/F

1. False mutually exclusive

$$P(X=3 \cap X=4) = 0$$

2. Out of scope linear least squares estimator

3. True self loop reach back 1 step

4. True marker prop

5. True system
 $\begin{cases} u= \\ v= \end{cases}$

6. True $f(x) \int_0^1 f(x,y) dy = 2x \downarrow 2x$

$f(y) \int_0^1 f(x,y) dx = 2y \downarrow 2y$

$2x \cdot 2y = 4xy$

7) $\begin{cases} \text{st. dist} \\ E[\# \text{ of returns}] \end{cases} \rightarrow \text{prop. of steps in state}$

$\hookrightarrow \text{when } n \rightarrow \infty$

True always stays in state in

5

1) $X \sim b(p)$ memoryless

\hookrightarrow starts over after j $P(X > i-j)$

$P(X) = (1-p)^{i-j} \rightarrow$

2) $f(x) = \begin{cases} cx^2 & 0 < x < 1 \\ 0 & \text{elsewhere} \end{cases}$

$$\int_0^1 cx^2 = \frac{cx^3}{3} \Big|_0^1 = c/3 = 1$$

$\hookrightarrow 3$

3) $np = E[X]$

$$P(X = np) = \binom{n}{np} p^{np} (1-p)^{n-np}$$

$$4) \quad P(A|B) = P(A) = \frac{1}{2}$$

if A, B i.i.d

5)

$$X = X_1 + \dots + X_6$$

$$E[X_i] = E[X_i | \text{prob}] \cdot P(\text{prob}) + E[X_i | \text{no prob}] \cdot P(\text{no})$$

$$0 \cdot \frac{1}{3} + \frac{1}{\lambda} \cdot (1 - \frac{1}{3}) = 20 \cdot \frac{2}{3}$$

$$E[X] = 6 \cdot E[X_i] = 6 \cdot 20 \cdot \frac{2}{3} = 80$$

6)

$$X \sim \text{Unif}(3, 6)$$

$$\hookrightarrow X = 3, 4, 4.5, 5, 6$$

$$\text{Var}(X) = \text{Var}(X_i)$$