CS 70 Discrete Mathematics and Probability Theory
Fall 2023 Rao and Tal

Midterm Solutions

PRINT Your Name: Oski Bear

SIGN Your Name: *OSKI*

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

1. Pledge.

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

In particular, I acknowledge that:

- I alone am taking this exam. Other than with the instructor and GSI, I will not have any verbal, written, or electronic communication about the exam with anyone else while I am taking the exam or while others are taking the exam.
- I will not refer to any books, notes, or online sources of information while taking the exam, other than what the instructor has allowed.
- I will not take screenshots, photos, or otherwise make copies of exam questions to share with others.

SIGN Your Name: _____

2. Warmup

(1 point) What is the greatest common divisor of **all** finite natural number student answers to this question?

Answer: 1. In fact, no matter what the actual greatest common divisor is, answering 1 will make the GCD of all numerical answers equal to 1.

3. Propositional Logic (and other stuff.)

1. Let P, Q and R be propositions.
   (a) $P \implies Q$ is equivalent to $\neg P \implies \neg Q$.
   Answer: False. This is the converse, not contrapositive. Let P be False and Q be True.
   (b) $(P \wedge Q) \implies R$ is equivalent to $\neg R \implies$ _____.
   Answer: $\neg P \vee \neg Q$ or $\neg(P \wedge Q)$
2. For predicates $P(x)$ and $Q(x)$,
   $$\neg(\exists x \in \mathbb{Z})(P(x) \vee Q(x)) \equiv (\forall x \in \mathbb{Z})(\neg P(x) \wedge \neg Q(x)).$$
   Answer: True. This is just an application of DeMorgan's laws.
3. For predicates $P(x)$ and $Q(x,y)$,
   $$\neg(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(P(x) \wedge Q(x,y)) \equiv (\exists x \in \mathbb{N})(\forall y \in \mathbb{N})(\neg P(x) \wedge \neg Q(x,y)).$$
   Answer: False. The $\wedge$ on the RHS must be a $\vee$, due to DeMorgan's laws.
4. $(\forall a,b \in \mathbb{N})(\frac{a}{b} \neq \sqrt{2})$.
   Answer: True. $\sqrt{2}$ is not rational.
5. $(\forall n \in \mathbb{N})\left[(\exists i \in \mathbb{N})(i^2 = n) \vee (\forall a,b \in \mathbb{N})(\frac{a}{b} \neq \sqrt{n})\right]$.
   Answer: True. $\sqrt{n}$ is not rational unless n is a perfect square. The proof: assume $(a/b)^2 = n$. Since n is not a perfect square, it must have a prime factorization with some odd powers, but $b^2 = na^2$ implies that the prime factorization of na^2 has even powers. But size n must have a prime in its factorization with an odd power, and a^2 can only have an even power of that prime, the expression must contain an odd prime power in its factorization.

4. Short proofs.

First, say whether each statement is true or false, and then prove or give a counterexample. The proof or counterexample should be brief.

1. (5 points) If $a \mid b$ and $a \mid c$, then $a \mid (b+5c)$.
   Answer: True. $b = ka$, and $c = \ell a$, thus $(b+5c) = ka+5\ell a = a(k+5\ell)$ which implies $a|(b+5c)$.
2. (5 points) If $b^2 = n$, then $n \mid b$.
   Answer: False. Consider $b = 2$, and $n = 4$.
3. (5 points) If n is not a perfect square, and its prime factorization is $p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$, then at least one k_i must be odd.
   Answer: True. We prove the contrapositive. Assume that all k_i are even, and thus $k_i = 2\ell_i$ for some ℓ_i. Let $k = p_1^{\ell_1} \cdots p_m^{\ell_m}$. Then,

$$n = p_1^{k_1} \cdots p_m^{k_m} = p_1^{2\ell_1} \cdots p_m^{2\ell_m} = \left(p_1^{\ell_1} \cdots p_m^{\ell_m}\right)^2 = k^2.$$

   This means n is a perfect square.

5. Long proofs.

1. (6 points) Consider the recursive sequence defined by

$$x_1 = 1 \text{ and } x_n = \sqrt{1+x_{n-1}} \text{ for all } n \geq 2.$$

   Prove that $x_n < 2$ for all $n \geq 1$.
   Answer: We proceed by induction.

   Base Case: For $n = 1$ we see $x_1 = 1 < 2$.

   Inductive Hypothesis: Suppose $x_k < 2$ for some arbitrary integer $k \geq 1$.
   Inductive Step: We observe

$$\begin{aligned} x_{k+1} &= \sqrt{1+x_k} \\ &< \sqrt{1+2} \\ &= \sqrt{3} \\ &< 2 \end{aligned}$$

   which shows $x_{k+1} < 2$.

   Remark: You can actually show an even tighter bound of $x_n < \frac{1+\sqrt{5}}{2}$ by arguing that $x_n \nearrow \frac{1+\sqrt{5}}{2}$ as $n \to \infty$ by Monotone Convergence Theorem from real analysis which is not in scope for this course.
2. (10 points) Prove that $2^{n+2} + 3^{2n+1}$ is divisible by 7 for all $n \geq 1$.
   Answer: We proceed by induction.
   Base case: For $n = 1$, we have that $2^{1+2} + 3^{2\cdot 1+1} = 8 + 27 = 35$, and 35 is divisible by 7.
   Inductive Hypothesis: For some $n = k \geq 1$, suppose that $2^{k+2} + 3^{2k+1} = 7m$ for some m.

Inductive Step: For the case of $n = k+1$,

$$\begin{aligned} 2^{k+3} + 3^{2k+3} &= 2 \cdot 2^{k+2} + 9 \cdot 3^{2k+1} \\ &= 2\left(2^{k+2} + 3^{2k+1}\right) + 7 \cdot 3^{2k+1} \\ &= 2 \cdot 7m + 7 \cdot 3^{2k+1} && \text{(I.H.)} \\ &= 7\left(2m + 3^{2k+1}\right) \end{aligned}$$

which proves that $7 \mid 2^{k+3} + 3^{2k+3}$, completing our induction.

Alternate Solution: We can solve this problem purely with modular arithmetic. We claim

$$\begin{aligned} 2^{n+2} + 3^{2n+1} &\equiv 2^n \cdot 4 + 9^n \cdot 3 \\ &\equiv 2^n \cdot 4 + 2^n \cdot 3 \\ &\equiv 2^n (4+3) \\ &\equiv 0 \pmod 7 \end{aligned}$$

as desired.

6. Stability in Matchings.

We consider instances of the stable matching problem below.

1. In an instance, if a job and candidate are paired in both the job propose and candidate propose matching algorithms, they are partners in all stable pairings.

   Answer: True. If not, due to optimality properties of the proper group, each would prefer in each in any other stable pairing and thus would be a rogue couple and contradict that the pairing is stable.

2. In an instance, if some job and candidate are paired in both the job and candidate optimal pairings, then there is only one possible stable pairing for this instance.

   Answer: False. Take an any instance where there are different stable pairings, and add a job and candidate who are each other's favorite. The last pair will be paired in every stable pairing, but there are at least two different stable pairings.

3. For an $n = 2$ instance, a stable pairing is always job optimal or candidate optimal (or both).

   Answer: True. There are at most two possible pairings. There is a job optimal stable pairing and a candidate optimal stable pairing. If they are the same, the other pairing is not stable since each job and candidate would prefer to be with the other entity due to the optimality of the other pairing for both.

4. There are instances where a candidate can reject the wrong job and do better (i.e. end up with a more preferable partner).

   Answer: True. For the $n = 2$ instance with different optimal pairings. If the candidate can reject a job, they can switch to the optimal pairing for candidates. But one has to have a job on the string to reject. Thus, we add an a third job who asks the first two in sequence. Thus allows them to reject their first proposers and obtain their optimal job in the 2 by 2 instance.

7. Graphs

You may assume all graphs in this section are simple (as defined in the notes) unless otherwise specified. Also a graph can't have zero vertices.

1. A hypercube of dimension n has an even number of edges for $n \geq$ ____. (Give a tight bound.)
   Answer: 2. It has $n2^{n-1}$ edges. So for $n \geq 2$, this has a factor of 2.
2. A complete graph, K_n, has an even number of edges for any $n > 3$.
   Answer: False. The number of edges is $n(n-1)/2$. If $n = 2k+1$, we have $(2k+1)(2k)/2 = (2k+1)k$, thus if k is odd, this is odd.
3. Recall a cut in a graph $G = (V,E)$ is a subset $S \subseteq V$. We define the *edges in the cut* S to be the edges with one endpoint in S and the other endpoint in $V \setminus S$.
   (a) In a complete graph on n vertices, given a cut of size k, how many edges are in this cut?
   Answer: $k \times (n-k)$. All the edges are present, and for each of the k vertices in S, the edge to each of the $n-k$ vertices is present.
   (b) For an n-vertex tree, what is the least number of edges in any cut? (Note $|S| \geq 1$ and $|V \setminus S| \geq 1$.)
   Answer: 1. Since it is connected.
   (c) For an n-vertex tree, what is the maximum number of edges in any cut?
   Answer: $n-1$. It is bipartite, so all edges are in the cut that splits the vertices into two sets.
4. Adding an edge e to a graph either reduces the number of connected components or creates (at least) one cycle that uses edge e.
   Answer: True. Either the edge is between two vertices in the same connected component in which case there is a path between its endpoints which forms a cycle when the edge is included.
5. What is the minimum number of connected components for any graph with n vertices and e edges?
   Answer: $\max(n-e, 1)$. Beginning with zero edges, the least number of components is n, adding an edge can reduce the number of connect components by at most 1. You can't have less than one connected components.
6. An n vertex graph with ___ edges must have a cycle. (Recall graphs are simple unless otherwise stated. Give a tight bound.)
   Answer: n. Again, adding edges can reduce the number of components by 1 or adds an edge in a connected component creating a cycle. Thus, after adding $n-1$ there is a single component and the nth edge must create a cycle.

8. Graph: proofs

1. Recall that an edge coloring of a graph $G = (V,E)$ is a coloring of edges such that no pair of edges sharing a common vertex have the same color.
   (a) A dimension n hypercube can be edge colored with n colors.
   Answer: True. Color each dimension differently.
   (b) Any graph with maximum degree d can be edge colored with d colors.
   Answer: False. A triangle, K_3, needs 3 colors and has degree 2.
   (c) Any bipartite graph can be edge colored with 2 colors.
   Answer: False. The minimum number of edge colors must be the maximum degree. A bipartite graph can have arbitrary degree, see, for example the hypercube.
   (d) Consider an $n > 2$ vertex bipartite graph where every vertex has degree d, and where the edges can be decomposed into Hamiltonian cycles. That is, there is a set S of Hamiltonian cycles in G where each edge appears in exactly one Hamiltonian cycle. Recall a Hamiltonian cycle is a simple cycle in the graph that contains every vertex.
      i. What is the number of edges in this graph?
      Answer: $nd/2$. The sum of the degrees is twice the number of edges.

ii. How many Hamiltonian cycles are in S?
Answer: $d/2$. Each Hamiltonian cycle uses degree 2 from each vertex.

iii. (5 points) Prove that any such graph can be edge colored with d colors.
Answer: For $d = 2$, the Hamiltonian cycle can be 2-colored. Otherwise, one can remove a Hamiltonian cycle and the degree of each vertex drops by 2 and is covered by the remaining Hamiltonian cycles. One can color the Hamiltonian cycle with 2 colors and the remaining graph with $d-2$ colors by induction.

2. (6 points) Recall a bipartite graph $G = (L, R, E)$ has vertices $V = L \cup R$, and edges $(u, v) \in E$ such that $u \in L$ and $v \in R$.
A *Hall set* is a set $S \subseteq L$, where $|N(S)| < |S|$, and $N(S)$ is the set of neighbors of vertices in S. That is,

$$N(S) = \{v \mid (\exists u \in S)((u, v) \in E)\}.$$

Argue that if every vertex has degree exactly $d > 0$, there is no Hall Set. (Hint: think about the sum of the degrees in S.)
Answer: The number of edges incident to S is $d|S|$, and thus their neighbors must also have sum of degrees of at least $d|S|$, since the maximum degree is d, $d|N(S)| \geq d|S|$ which implies $|N(S)| \geq |S|$.

9. Modular Arithmetic.

1. What is $7^{50} \pmod{35}$?
Answer: 14. By RSA, we know that $a^{(p-1)(q-1)} = 1 \pmod{pq}$. Here, $p = 5$ and $q = 7$, so we know that $7^{(5-1)(7-1)} \equiv 7^{24} \equiv 1 \pmod{35}$. Further, $(7^{24})^2 = 7^{48} \equiv 1 \pmod{35}$, so $7^{50} \equiv 7^2 \cdot 7^{48} \equiv 49 \equiv 14 \pmod{35}$.
2. Suppose q is prime and $N = q^2$.
   (a) How many elements in the set $S = \{0, 1, \ldots, N-1\}$ are relatively prime to N?
   Answer: $q^2 - q = q(q-1)$. There are q numbers in the range that are divisible by q.
   (b) If a has $\gcd(q, a) = 1$, then a has an inverse modulo N.
   Answer: True. This condition implies $\gcd(a, N) = 1$ which means the inverse exists by extended euclidean algorithm.
   (c) $a^x \equiv a \pmod{N}$ for $x = 1$ or $x =$ _____ if $gcd(a, N) = 1$. (Answer is an expression possibly involving N, q or S. Hint: what is the function $f(x) = ax \pmod{N}$ on the set S?)
   Answer: $k|S| + 1$ or $kq(q-1) + 1$ for any integer k (the natural solution is for $k = 1$). The proof is that $f(x)$ in the hint is a bijection as a has an inverse. Thus the image of $f(x)$, $\{y | ax \text{ for } x \in S\}$, is simply S. Multiplying the set together with and without the multiple of a, gives a factor of $a^{|S|}$, which implies $a^{|S|} = 1 \pmod{N}$ and $a^{|S|+1} = a \pmod{N}$
3. If $ab \equiv 0 \pmod{n}$ then either $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$.
Answer: False. Consider $n = 8, a = 2, b = 4$.
4. An integer a is an integer linear combination of x and y if $a = ix + jy$ for some integers i, j.
Consider two linear combinations of x and y: $m = ax + by$ and $n = cx + dy$.
   (a) Any integer linear combination of m and n is an integer linear combination of x and y.
   Answer: True. Consider $ax + by$ and $cx + dy$ then $i(ax + by) + j(cx + dy) = (ia + jc)x + (iab + jd)y$ and is thus an integer combination of x and y.
   (b) The smallest positive number that is an integer linear combination of x and y is $\min(x, y)$.
   Answer: False. If $x = 6$ and $y = 4$, $x - y = 2$ is an integer combination of 4 and 6 and less than $\min(x, y)$

(c) The smallest positive number that is an integer linear combination of x and y is $\gcd(x,y)$.
Answer: True. At a high level, this is just the Extended Euclid equation. Given any two integer combinations of x and y, m and n, one can observe that $m-n$ has the same divisors as m and n. Thus, $gcd(m,m-n) = gcd(m,n)$, then one can find the smallest integer combination of m and $m-n$ which is the $gcd(m,m-n)$ by induction. The base results from either being zero, in which case the gcd is the other number. If one starts with $m = x$ and $n = y$ one obtains the result.
Alternate Solution: $gcd(x,y)$ is a linear combination of x and y by Extended Euclid. Furthermore, $gcd(x,y)$ must divide any linear combination of x and y (since it divides both x and y), and hence any positive number which is a linear combination of x and y cannot be smaller than $gcd(x,y)$.

5. If $x \equiv a \pmod{m}$ and $x \equiv a \pmod{n}$, where $\gcd(n,m) = 1$, then $x \equiv a \pmod{mn}$.
Answer: True. This is a solution, and by CRT it is unique.

6. Consider an integer x such that $x \equiv a \pmod{m}$ and $x = a + kn$ for integers k and n, where $\gcd(m,n) = q$.

(a) If x is non-zero, what is the smallest *strictly positive* value for k where x satisfies the properties?
Answer: m/q. $a + mn/q = a \pmod{m}$. $kn = 0 \pmod{m}$ if and only if $kn/q = 0 \pmod{m}/q$, and thus $k = 0 \pmod{m}$, since n/q has no common factors with m/q. Thus, the smallest positive value is m/q.

(b) How many values of $x \in \{0,\ldots,mn-1\}$ are solutions?
Answer: q. Any $x = a + ikn$ is a solution. There are q such x's in the range.

10. Modular Arithmetic: generator?

Consider a prime $p > 2$ such that $(p-1) = q_1 \cdot q_2 \cdots q_k$ for distinct primes $q_1,\ldots,q_k$.

1. (3 points) Prove that there is a nonzero element x such that $x^n - 1 \not\equiv 0 \pmod{p}$, where $n < p-1$.
Answer: Since $x^n - 1$ is a degree n polynomial, it has at most n roots. Since $n < p-1$, and there are $p-1$ nonzero congruent classes mod p, by the pigeonhole principle, there must exist some nonzero x such that $x^n - 1 \not\equiv 0 \pmod{p}$, as desired.

2. (6 points) Prove that there is a nonzero element $a \not\equiv 1 \pmod{p}$ such that $a^{q_i} \equiv 1 \pmod{p}$ for any $i \in \{1,\ldots,k\}$.
Answer: For any $b \not\equiv 0 \pmod{p}$, $b^{(p-1)} \equiv 1 \pmod{p}$. But this means, $(b^{(p-1)/q_i})^{q_i} \equiv 1 \pmod{p}$. Thus, $a = b^{(p-1)/q_i}$ suffices. However, we still need to show that there is a choice for b such that $a = b^{(p-1)/q_i} \not\equiv 1 \pmod{p}$. Using the previous part, we know that $x^{(p-1)/q_i} - 1$ is of degree $(p-1)/q_i$, and thus must have at most $(p-1)/q_i$ zeroes, i.e., there are at most $(p-1)/q_i < p-1$ possible values of nonzero b that make $b^{(p-1)/q_i} \equiv 1 \pmod{p}$, so there must still exist some nonzero b that makes $a \equiv b^{(p-1)/q_i} \not\equiv 1 \pmod{p}$ but $a^{q_i} \equiv b^{p-1} \equiv 1 \pmod{p}$.

3. (6 points) Let the *order* of x be the smallest positive integer k such that $x^k \equiv 1 \pmod{p}$. Prove that if $x^q \equiv 1 \pmod{p}$ and d is the order of x, then $d \mid q$.
Answer: Divide q by d with remainder: $q = d \cdot m + r$, where $0 \le r \le d-1$. Suppose by contradiction that $r \neq 0$. We have $1 \equiv x^q \equiv x^{dm+r} \equiv (x^d)^m \cdot x^r \equiv x^r \pmod{p}$. This means that r is a positive number smaller than d such that $x^r \equiv 1 \pmod{p}$, a contradiction to the minimality of d.

Remark: During the exam, the problem statement originally said $x^q \equiv 1 \pmod{n}$ instead of $\pmod{p}$. As a result, this problem was not graded, but the problem statement has now been fixed for students who use this exam to practice in the future.

11. Swiper, no swiping!

(6 points) Suppose Dora and Boots are exchanging a message via RSA with $N = 15$ (where $p = 3$ and $q = 5$). Swiper spies the encrypted message $E(x) \equiv 10 \pmod{15}$. If the original message x is less than 15, explain how Swiper can recover x and provide an explicit value for x without knowing the encryption key e.

Answer: Denote the decryption key as d (which is unknown). Then, $x \equiv 10^d \pmod{15}$. Individually, $x \equiv 10^d \equiv 0 \pmod{5}$ and $x \equiv 10^d \equiv 1^d \equiv 1 \pmod{3}$. From Chinese Remainder Theorem, we uniquely construct $x \equiv 10 \pmod{15}$ and since $x < 15$ we have $x = 10$.

12. Polynomial and Applications.

1. If a secret is encoded at $x = 0$ into a line that goes through the points $(1,1)$ and $(2,3)$ in arithmetic modulo 5, then what is the secret? (Answer should be in $\{0,\ldots,4\}$.)

   Answer: 4. The line has slope 2. Thus the value is is $-1 \pmod{4}$ at $x = 0$.

2. Consider two polynomials $P(x)$ and $Q(x)$, both with degrees exactly d_P and d_Q, respectively.

   (a) What is the degree of $P(x)Q(x)$?
   Answer: $d_P + d_Q$. This is the power of the leading term.

   (b) Suppose we perform polynomial division to compute $P(x)/Q(x)$, resulting in the equation $P(x) = D(x)Q(x) + R(x)$ for some other polynomials $D(x)$ and $R(x)$.

   i. What is the degree of $D(x)$, possibly in terms of d_P and d_Q?
   Answer: $d_P - d_Q$. Suppose the leading term of P and Q are x^{d_P} and x^{d_Q}, respectively. When dividing, the leading term of D is $(x^{d_P})/(x^{d_Q}) = x^{d_P - d_Q}$.

   ii. What is the maximum degree of $R(x)$, possibly in terms of d_P and d_Q?
   Answer: $d_Q - 1$. $R(x)$ is constructed as the remainder and so if $R(x)$ were to hypothetically have a degree larger than $d_Q - 1$ then we could further divide $R(x)$ by $Q(x)$.

   iii. If $R(x) = 0$, then all the roots of $Q(x)$ are roots of $P(x)$.
   Answer: True. We have $P(x) = D(x)Q(x)$ and so if $Q(x) = 0$, then $P(x) = D(x)Q(x) = D(x) \cdot 0 = 0$.

   iv. If $R(x) = 0$, then all the roots of $D(x)$ are roots of $P(x)$.
   Answer: True. Same solution as above but use $D(x) = 0$ instead of $Q(x) = 0$.

3. Suppose we want to send a message of size 1, protecting against 1 general error, where the received packets are $R(1) = 2$, $R(2) = 1$, $R(3) = 2$ working modulo 5. Consider the Berlekamp–Welch scheme in the following.

   (a) What is the error polynomial $E(x)$?
   Answer: $x - 2 \pmod{5}$ or $x + 3 \pmod{5}$. A message of size 1 corresponds to a constant polynomial, and thus the message was 2 and the error was at point 2.

   (b) What is $Q(x)$?
   Answer: $2x + 1 \pmod{5}$. $Q(x) = P(x)E(x) = 2(x+3) \pmod{5}$.

13. Blank Space[s]

1. (1 point each) We will walk through a proof for the following identity:

$$\sum_{i=0}^{n} \binom{n}{i} \sum_{j=0}^{n-i} \binom{n-i}{j} = 3^n.$$

   Fill in the blanks below.

Suppose we have three bins labeled A, B, and C, and n balls labeled 1 through n.

On the RHS, we go one ball at a time. Each ball can go into 3 possible bins, so the total number of ways to distribute the n balls is __(a)__.

On the LHS, we go one bin at a time. From the n balls we start with, there are __(b)__ ways to put some arbitrary number of __(c)__ balls into bin A. Then, from the remaining __(d)__ balls, there are __(e)__ ways to put some arbitrary number of __(f)__ balls into bin B. Then, we put all the remaining __(g)__ balls into bin C, which happens in __(h)__ way(s).

(a) **Answer:** 3^n
(b) **Answer:** $\binom{n}{i}$
(c) **Answer:** i
(d) **Answer:** $n-i$
(e) **Answer:** $\binom{n-i}{j}$
(f) **Answer:** j
(g) **Answer:** $n-i-j$
(h) **Answer:** 1

2. (1 point each) The password to unlock the CS70 Fall 2023 Midterm Solutions document can be opened with a secret code. The solutions should only be released when **both of these two conditions** are met.
   - Condition 1: Either all 14 TAs must agree, OR 10 TAs and Alec Li must agree
   - Condition 2: 20 Readers must agree

   Fill in the blanks to complete the following secret sharing scheme that satisfies these conditions.

   Because there are 2 conditions, we encode the secret code to the solutions document as $P(0)$ in a degree __(a)__ polynomial $P(x)$.

   We will encode 1 point from $P(x)$ as the secret to another polynomial $Q(x)$ corresponding to Condition 1. $Q(x)$ will have degree __(b)__, and __(c)__ point(s) will given to each TA. Alec Li specifically will receive __(d)__ point(s). All points given are distinct.

   To satisfy Condition 2, we encode another point from $P(x)$ as the secret to another polynomial $R(x)$. $R(x)$ will be a degree __(e)__ polynomial and each Reader will be given __(f)__ point(s).

(a) **Answer:** 1
(b) **Answer:** 13
(c) **Answer:** 1
(d) **Answer:** 4
(e) **Answer:** 19
(f) **Answer:** 1

14. Two dice or not two dice

Shreyas is rolling a fair six-sided die 3 times. He writes down the resulting three numbers as a sequence. One possible sequence is 4,2,1. You may leave your answer in terms of exponents and binomial coefficients without simplifying.

1. Compute the total number of possible outcomes for the sequence.
   Answer: 216. Each roll has 6 possible outcomes. By the first rule of counting, the total is $6 \cdot 6 \cdot 6 = 6^3 = 216$.
2. Compute the total number of sequences such that the rolls are strictly increasing.

Answer: $\binom{6}{3} = 20$. Recall that there are $\binom{6}{3} = 20$ ways to sample without replacement 3 numbers from 1 through 6 such that the order does not matter. For each of these 3 chosen numbers, there's only 1 way we can arrange them such that they form an increasing sequence. Hence, the answer is $1 \cdot \binom{6}{3} = 20$.

3. Compute the total number of sequences such that the rolls are nondecreasing.

   Answer: $\binom{8}{5} = \binom{8}{3} = 56$.We can reduce this problem to stars and bars. Suppose we had 6 bins labeled 1 through 6 and 3 balls representing our three rolls. We can drop our 3 balls randomly across the three bins and simply generate a non decreasing sequence by reading from left to right. We inadvertently handle the cases of repetition: suppose bin 2 has 2 balls and bin 5 has the remaining ball; then our sequence is 2,2,5. The number of ways to distribute 3 balls across 6 bins is $\binom{3+6-1}{6-1} = \binom{8}{5} = 56$.

4. Compute the total number of ways such that 1 does not appear in any of the rolls.

   Answer: 125. This means that each roll was some number from 2 to 6, inclusive, which happen in 5 ways. Hence, by the first rule of counting, there are $5^3 = 125$ ways in which this can happen.

5. Compute the total number of sequences where at least one of the first two rolls is the number 1.

   Answer: 66. We use inclusion-exclusion. Denote A_1 as the set of outcomes where the first roll is a 1 and A_2 as the set of outcomes where the second roll is a 1. We see that $|A_1| = |A_2| = 1 \cdot 6 \cdot 6 = 36$ and $|A_1 \cap A_2| = 1 \cdot 1 \cdot 6 = 6$. Hence,

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = 36 + 36 - 6 = 66.$$

6. Compute the total number of sequences where the product of all the rolls is even.

   Answer: $6^3 - 3^3 = 189$. We instead compute the number of sequences whose product is odd. For the product of three numbers to be odd, all three numbers must be odd. For each roll, there are 3 outcomes $(1,3,5)$ which are odd. Hence, there are $3^3 = 27$ ways for all three rolls to be odd. Since there are 216 possible outcomes in total from part A, this means the number of outcomes where the product is even is $6^3 - 3^3 = 189$.

15. Proof: Countability

(6 points) Prove that the set of irrational numbers ($\mathbb{R} \setminus \mathbb{Q}$) is uncountable.

Answer: The set of real numbers is the union of the set of rational numbers and the set of irrational numbers; that is, $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$.

Suppose for contradiction that $\mathbb{R} \setminus \mathbb{Q}$ is countable. Then, the union $\mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$ is a union of countable sets, and is thus countable. However, we know that this union is the set of real numbers, which we know is uncountable, giving us a contradiction. This means that the set of irrationals must be uncountable.