

15-251: F09

Practice Test 2 Solutions

Repeat After Me.

This part is to test your ability to regurgitate basic facts. You should either have these facts memorized or be able to re-derive them on the spot.

1. [5 points] \mathbb{I} is the set of irrational numbers. Which properties does the set $\mathbb{I} \cup \{0\}$ have under addition?

Associativity	Closure	Identity	Inverse	Commutativity
Yes	No	Yes	Yes	Yes

2. [5 points] Take a *red* die and a *blue* die. Each die can come up either 1, 2, 3, 4, 5, or 6. How many ways are there to get

an even number on the red die **AND** an odd number on the blue die?

There are 3 ways of choosing an even number on the red die, and 3 ways of choosing an odd number on the blue die, giving the answer 9.

Some of you calculated the *probability* of the event above, and while we gave full credit for these solutions, we'd urge you to read the problems more carefully.

3. [5 points] How many numbers in \mathbb{Z}_{35} have multiplicative inverses? (You **don't** have to list them.)

The numbers in \mathbb{Z}_{35} that have multiplicative inverses are precisely those in \mathbb{Z}_{35}^* (i.e., those x such that $\gcd(x, 35) = 1$). And there are $\phi(35) = \phi(5)\phi(7) = 4 \cdot 6 = 24$ of them.

4. [5 points] Compute

$$39^{26} \pmod{35}$$

Give an integer answer in the range 0 to 34.

The answer is 16. Note that $39 \equiv_{35} 4$ is in \mathbb{Z}_{35}^* , and hence we can use Euler's theorem. So,

$$\begin{aligned} 39^{26} &\equiv_{35} 4^{26} \\ &\equiv_{35} 4^{26 \bmod \phi(35)} \\ &\equiv_{35} 4^2 = 16. \end{aligned}$$

5. [5 points] Let G be a group of prime order. Write down all the possible subgroups of G .

The two possible subgroups are the trivial group consisting only of the identity element, and G itself. Why? By Lagrange's theorem, we know that if H is a subgroup of G , then $|H| \mid |G|$. But G has prime order, and the only numbers that divide a prime are 1 and the prime itself.

6. [5 points] Let X be the random variable denoting the outcome of one roll of a standard 6-sided die. What is $\mathbb{E}[2X + 3]$?

10. Note that $\mathbb{E}[X] = \frac{1+2+3+4+5+6}{6} = 3.5$. By linearity of expectations, $\mathbb{E}[2X + 3] = 2\mathbb{E}[X] + \mathbb{E}[3] = 2 \cdot 3.5 + 3 = 10$.

7. [10 points] In the first 3 parts, let X be a random variable; We assume **nothing** else about it. Mark the following statements as **True** or **False**. (Provide explanations if you must.)

- F $\mathbb{E}[X \times X] = \mathbb{E}[X] \times \mathbb{E}[X]$.
- F $\Pr(X \geq \mathbb{E}[X]) = \frac{1}{2}$.
- T $\Pr(X \geq 2\mathbb{E}[X]) \leq \frac{1}{2}$.
- F $\Pr(X = \mathbb{E}[X]) > 0$.
- T If A and B are independent events, then \bar{A} and \bar{B} are also independent events.

Basic Techniques.

This part will test your ability to apply techniques that we have explicitly identified in lecture. You need to have practiced each technique enough to be able to handle small variations in the problems.

8. [15 points] A *biased* coin, which comes up heads with probability p , is tossed until we see either a **total** of 2 heads or a **total** of 2 tails. Answer the following questions.

- (5 pts) What is the sample space? (List all possible outcomes)

The sample space is $\{HH, HTH, THH, TT, THT, HTT\}$.

- (5 pts) In this experiment, what is the probability that we get consecutive heads?

The probability we get consecutive heads is the sum of the probabilities we get HH and THH , which are p^2 and $(1-p)p^2$ respectively, so the probability is $p^2(2-p)$.

- (5 pts) Now, *given that* the process went on for 3 flips, what is the (conditional) probability of getting consecutive heads?

The probability that we get consecutive heads given it took 3 flips is $(1-p)p^2$, since we must have gotten THH . The probability it took 3 flips is $1-p^2-(1-p)^2=2p(1-p)$, since he must have avoided HH and TT . Thus, the answer is:

$$\frac{(1-p)p^2}{2p(1-p)} = \frac{p}{2}$$

9. [15 points] Recall that $\phi(n)$ is the Euler phi function. Given three distinct primes p, q, r , give an expression for $\phi(pqr)$.

$$(p-1)(q-1)(r-1)$$

There are pqr elements in $[0, pqr-1]$; of these, qr are divisible by p , pr are divisible by q , pq are divisible by r . Additionally, r are divisible by pq , q are divisible by pr , p are divisible by qr , and one is divisible by pqr . We combine all of these to avoid over/undercounting to get:

$$\phi(pqr) = pqr - qr - pr - pq + r + q + p - 1 = (p-1)(q-1)(r-1)$$

Note that we are using Inclusion/Exclusion here.

(10 pts) Give and prove an expression for $\phi(p^2)$, where p is prime.

$$p(p-1)$$

Consider all the p^2 elements in the set $\{0, 1, \dots, p^2-1\}$. Out of these, the p elements $\{0, p, 2p, \dots, (p-1)p\}$ —which are the p multiples of p —have a GCD greater than 1. All other elements have a GCD of 1, because they do not have any factor of p , and p^2 only has p as a factor. Hence, $\phi(p^2) = p^2 - p = p(p-1)$.

A Moment's Thought!

This section tests your ability to think a bit more insightfully. You must give complete explanations of your answers.

10. [20 points] Professor Gupta and Professor Lafferty each independently and uniformly at random pick a subset of n problems from a set of n^2 problems to put on this test. What is the probability a given problem is picked by *both professors*? What is the expected number of problems picked by *both professors*? (Please give clear reasons.)

Let G_i be the indicator variable for the event that the i -th problem is picked by Professor Gupta, and L_i be the indicator variable for the event that the i -th problem is picked by Professor Lafferty. Hence, if B_i is the indicator variable for the event that the i -th problem is picked by both, then $B_i = L_i \times G_i$. Since G_i and L_i are independent random variables,

$$E[B_i] = E[L_i \times G_i] = E[L_i] \times E[G_i].$$

Now, if the i -th problem is picked by Prof Gupta, then the number of ways for him to pick the other $k - 1$ problems is $\binom{k^2-1}{k-1}$. Since the total number of ways to pick k problems out of k^2 is $\binom{k^2}{k}$, and each set of k problems is equally likely,

$$E[G_i] = \Pr[i\text{-th problem is picked by Gupta}] = \frac{\binom{k^2-1}{k-1}}{\binom{k^2}{k}} = \frac{1}{k}.$$

Similarly, $E[L_i] = \frac{1}{k}$, giving us that $E[B_i] = E[G_i] \times E[L_i] = \frac{1}{k^2}$. Now the probability of the event that the i -th problem is picked by both is equal to the expectation of the indicator variable for that event, which is $E[B_i] = \frac{1}{k^2}$.

Finally, if the random variable B denotes the number of problems picked by both, then $B = \sum_{i=1}^{k^2} B_i$, and by the linearity of expectation

$$E[B] = \sum_{i=1}^{k^2} E[B_i] = k^2 \times \frac{1}{k^2} = 1.$$

Common Mistakes: You must explain why $E[G_i]$ or $E[B_i]$ are $1/k$ — just saying that it is k/k^2 is not enough.

While we don't always expect you to write quite as detailed solutions as the one above in an exam, we do want you to tell us when you are using linearity of expectations; in that case, you must make also clear what the random variables are. Also, you cannot talk about $\Pr[X]$ if X is an r.v., just as you cannot talk about $E[A]$ if A is an event.