Math 55 midterm exam, April 4, 2019

Problem	1	2	3	4	5	6	Total
Points	6	5	6	5	6	6	34

You all acted with honesty, integrity, and respect for others.

1a. For $n \geq 0$, determine the number of bit strings of length n that do not contain the string `01`.

The condition about not containing `01` means that all the `0`'s need to be to the right of all the `1`'s. You can plunk down any number `0`'s from 0 of them to n of them. These get justified to the right, and then `1`'s get filled in to the left of the `0`'s. Conclusion: there are $n + 1$ possible bit strings that satisfy the condition.

b. Let b_n be the number of bit strings of length n that do not contain `000`. Show that $b_0 = 1$, $b_1 = 2$, $b_2 = 4$ and

$$b_{n+3} = b_{n+2} + b_{n+1} + b_n$$

for $n \geq 0$.

Think of bit strings of length $n + 3$, working from the left to the right. If the first character is a `1`, then the string of length $n + 2$ to the right of the leftmost `1` can be any string that avoids `000`. This explains the term b_{n+2} in the sum. Suppose now that the string of length $n + 3$ begins `01`. Then the remaining piece of length $n + 1$ can be any string of that length that avoids `000`. This explains the term b_{n+1} in the sum. Finally, suppose that the string begins `00`. To avoid `000`, it had better begin `001`. The remaining n places can be chosen to constitute any string of length n that avoids `000`. This explains the third and final term in the sum.

What about the initial values? Strings of length 0, 1 and 2 cannot contain `000`. Therefore, b_0, b_1 and b_2 are equal to the number of strings of the relevant length. There's one string of length 0 (the empty string), two of length 1 and 4 of length 2. As a check, note that the recursive formula

for b_{n+3} states that there are seven strings of length 3 that do not contain 000. That's correct: there are eight strings altogether, including the string 000.

2. Math 55 students Alice and Bob announce their RSA public keys as $(n, 13)$ and $(n, 40)$; because they are good friends, they use the same modulus n. After learning that Charlie employed RSA to send the same message to Alice and Bob, Eve succeeds at retrieving the encrypted texts that Charlie sent to the two recipients. How can Eve recover Charlie's plain text from the two encrypted texts?

This problem is based on a question in the text. The main point is that the two exponents need to be relatively prime. I chose 40 and 13 because it's clear how to write 1 as a linear combination of these two relatively prime integers: $1 = 40 - 3 \times 13$. Unfortunately, 40 is not a good choice for Bob's "e" because e needs to be relatively prime to $(p-1)(q-1)$, so e had better be odd! At least one student picked up on this issue and asked about it. My apologies for including an inadmissible number as part of the problem.

If Charlie's plain text is m mod n, then Charlie sends m^{13} to Alice and m^{40} to Bob. (All quantities are computed mod n.) Eve can recover m as $m^{40} \cdot (m^{13})^{-3}$. To compute $(m^{13})^{-3}$ mod n, Eve can cube m^{13} and then compute the mod n inverse of the cube; she could also invert m^{13} and cube the inverse. Note that the inverse of a mod n is obtained via the Euclidean algorithm, as we learned in class.

3a. How many ways are there to distribute six red hats, six blue hats and six gold hats to a group of 18 students if each student receives one hat? [The hats are identical except for their colors.]

First distribute the six red hats; there are $\binom{18}{6}$ ways to do that. Then give out the blue hats; there are now $\binom{12}{6}$ ways to do that. Finally, give out the remaining six hats to the remaining six students—there's no longer any choice. The answer is thus $\binom{18}{6} \cdot \binom{12}{6}$.

b. How many ways are there to carry out the task in part (a) if the two identical twins in the class are to receive the same color hat?

First, decide what color hats the twins will wear; there are 3 ways to do that. Give the twins their hats. Then distribute the remaining four hats of that color to 4 of the remaining students; there are $\binom{16}{4}$ ways to do that. Then continue as before; the choices number $\binom{12}{6}$ and 1 for the remaining two colors. The answer is thus

$$3 \cdot \binom{16}{4} \cdot \binom{12}{6}.$$

The ratio between the answers in the two parts of the question is the probability that the twins will receive the same color hat if the hats are distributed randomly. This ratio is seen to be 5/17 by the following argument: Begin by giving hats to the two twins, starting with one of the twins—whom we'll call the "first twin." After the first twin gets a hat, there are 17 hats left, of which 5 have the color of the hat now worn by the first twin. The second twin has a 5 in 17 chance of getting the same color hat as her sister. As an exercise, check that 5/17 is indeed the ratio of the two answers.

4. Let $\alpha = (1 + \sqrt{5})/2$. Prove that the nth Fibonacci number is less than α^{n-1} for all $n \geq 2$.

On February 28, we proved a **Lemma** to the effect that the nth Fibonacci number is greater than α^{n-2}. The problem can be done in the same way, using strong induction. The base cases are statements for $n = 2$ and $n = 3$. The second Fibonacci number f_2 is 1; it's less than $\alpha = \alpha^1$, which is around 1.618. The third Fibonacci number is 2; it's less than α^2, which is $1 + \alpha$.

5. Alice buys a bag of 12 coins. Four of these are biased coins that come up heads 3/4 of the time; the other eight are fair coins. Sylvia reaches into the bag, pulls out a coin at random and tosses it. Sylvia's coin comes up heads! What is the probability that she pulled out a top-heavy coin?

The phrase "top-heavy" was borrowed from the Spring, 2015 Math 55 final, where there was a problem that began: "Alice buys a bag of 12 biased coins. Six of these are top-heavy coins that come up heads 2/3 of the time, while the other six are bottom-heavy coins that come up tails 2/3 of the time. . . ." In the midterm exam room, we agreed that "top-heavy" would mean "heads-favoring" (as it did in 2015).

To do the problem, we use the formula

$$p(F|E) = \frac{p(E|F)p(F)}{p(E|F)p(F) + p(E|\overline{F})p(\overline{F})}$$

that Rosen calls "Bayes' Theorem." We let F be the event that Sylvia pulls out a top-heavy coin and E the event that the coin toss yields a `H`. Then $p(F) = \frac{1}{3}$, $p(\overline{F}) = \frac{2}{3}$, $p(E|F) = \frac{3}{4}$, $p(E|\overline{F}) = \frac{1}{2}$. Put these numbers into the formula and you'll emerge with $\frac{3}{7}$ as the answer.

6a. Given that a poker hand contains at least three of the four aces in a deck of cards, what is the probability that it contains all four of the aces?

People asked for the number of cards in a poker hand, and we reminded them that the number is 5. We also supplied the additional information that a standard deck of cards has 52 cards in it.

The word "Given" telegraphs conditional probability. Here the answer will be A/B, where B is the number of poker hands with 3 or more aces and B is the number of poker hands with all four aces. Clearly, $B = 48$ because a hand with four aces needs only one more card to fill up the hand; there are 48 non-aces. For B, it might be easiest to compute the number of poker hands with exactly three aces. To select such a hand, we need to choose the ace that will be missing; there are four possibilities. Then we have to choose the two remaining cards from the non-aces; there are $\binom{48}{2}$ choices. Hence $B = 48 + 4 \cdot \binom{48}{2} = 4560$ and the answer is $48/4560 = 1/95$.

b. An urn contains 20 red balls, 20 green balls and 20 blue balls. Three of the 60 balls are removed at random. What is the expected number of green balls that have been removed from the urn?

This question is based on the "60 Balls" slide from our March 14 class meeting. A mechanical way to do the problem is to write the answer as 0 times the probability that no green balls have been removed, plus 1 times the probability that one green ball was removed, plus.... This leads to the numerical formula

$$\frac{1}{\binom{60}{3}}\left\{0\cdot\binom{40}{3}\binom{20}{0}+1\cdot\binom{40}{2}\binom{20}{1}+2\cdot\binom{40}{1}\binom{20}{2}+3\cdot\binom{40}{0}\binom{20}{3}\right\}.$$

That's a fine answer, and you'll get full credit if you submitted it. However, you can compute this expression, once you've left the exam, and you'll see that the answer simplifies to 1. How is this possible? Let X_R, X_G and X_B be the random variables that count the numbers of red, green and blue balls (respectively). The sum $X_R + X_G + X_B$ is the constant random variable 3. Hence $E(X_R) + E(X_G) + E(X_B) = 3$. On the other hand, the three random variables play symmetrical roles and therefore have a common expected value. That expected value is therefore 1.