Math 55 final exam, May 16, 2019

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

Problem	1	2	3	4	5	6	7	8	9	Total
Points	8	6	7	8	8	8	8	8	8	69

1a. Use the equation $1 = 121 \cdot 18 - 7 \cdot 311$ to find an integer x that satisfies the congruence $18x \equiv 7 \bmod 311$. (There's no need to simplify your answer.)

The equation shows that $121 \cdot 18 \equiv 1 \bmod 311$. It follows that $7 \cdot 121 \cdot 18 \equiv 7 \bmod 311$. Hence we may take $x = 7 \cdot 121 = 847$.

b. How many solutions are there to this congruence if solutions are counted as the same if and only if they are congruent mod 311?

There is only one solution. If $18x \equiv 7 \bmod 311$, then $121 \cdot 18x \equiv 121 \cdot 7 \bmod 311$. Because $121 \cdot 18 \equiv 1 \bmod 311$, we get that $x \equiv 121 \cdot 7 \bmod 311$.

2. Let $\{a_n\}$ be the sequence defined by $a_0 = 0$, $a_1 = 1$,

$$a_{n+2} = 3a_{n+1} - a_n \text{ for } n \geq 0.$$

Show that a_n is the Fibonacci number f_{2n} for all $n \geq 0$.

Since $f_0 = 0$ and $f_2 = 1$, the statement to be proved is true for $n = 0, 1$. The statement can be proved for all n by (strong) induction if we know that the numbers f_{2n} satisfy the same recurrence formula that is given for the a_n. In other words, we need to show

$$f_{2n+4} \overset{?}{=} 3f_{2n+2} - f_{2n}$$

for $n \geq 0$. Using the recurrence formula for the Fibonacci numbers twice, we obtain

$$f_{2n+4} = f_{2n+3} + f_{2n+2} = 2f_{2n+2} + f_{2n+1}.$$

On the other hand, a single application of the recurrence formula yields

$$3f_{2n+2} = 2f_{2n+2} + f_{2n+2} = 2f_{2n+2} + f_{2n+1} + f_{2n}.$$

Subtraction then gives

$$f_{2n+4} - 3f_{2n+2} = f_{2n},$$

which is visibly equivalent to the desired formula.

A different way to proceed is to use the technique of §8.2. There's a formula for f_n in Example 4 of this section. Replacing n by $2n$, one gets a formula for f_{2n}. Now "solve" the recurrence relation for the sequence $\{a_n\}$ by the techniques of this section. The result is

$$a_n = \frac{1}{\sqrt{5}}\left(\left(\frac{3+\sqrt{5}}{2}\right)^n - \left(\frac{3-\sqrt{5}}{2}\right)^n\right).$$

To compare the formulas for a_n and for f_{2n}, one needs to observe that

$$\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{3+\sqrt{5}}{2}.$$

3. A die is rolled repeatedly until two different faces have come up. Explain why the expected number of rolls is $1 + \frac{6}{5}$.

We roll the die once and get some number, say 4. Then we have to roll the die repeatedly until we get something other than 4. The probability of getting a non-4 is $\frac{5}{6}$. By our Bernoulli trial calculations (recalled in the review session on May 9), the expected number rolls needed to get a non-4 is the reciprocal of $\frac{5}{6}$, i.e., $\frac{6}{5}$. You add 1 to this fraction to account for the initial roll (of 4, or whatever).

4. What is the probability that a 5-card poker hand has at least two face cards? (The face cards are the jacks, queens and kings. Thus there are 12 face cards in a standard 52-card deck.)

We can calculate: (a) the number of poker hands in total, (b) the number of poker hands with no face cards at all, and (c) the number of poker hands with exactly one face card. The answer will be (a) − (b) − (c), divided by (a). The number of poker hands is $\binom{52}{5}$; similarly, the number of poker hands that avoid the 12 face cards is $\binom{40}{5}$. The number of hands that have exactly one face card is $12 \cdot \binom{40}{4}$. (You choose a face card and then choose four non-face cards.) Thus the number of hands with at least two face cards is

$$\binom{52}{5} - \binom{40}{5} - 12 \cdot \binom{40}{4} = 844272.$$

Divide this by $\binom{52}{5}$ to get the answer.

5. Before going on vacation for a week, you ask an unreliable friend to water your ailing plant. Without water, the plant has a 90 percent chance of dying. With water, it has a 20 percent chance of dying. The probability that your friend will forget to water it is 30 percent.

As you read this problem, you'll quite possibly recall Bayes' theorem

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

Part (b) makes one think that we should let E be the event that the plant is dead when you return and F is the event that your friend forgot to water it.

a. What is the probability that your plant will be dead at the end of the week?

We are looking for $p(E)$, which is the denominator

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

in the second fraction above. The two summands in this expression correspond to these two situations: your friend forgot to water it and it died, and your friend remembered to water it and it died. Now $p(E|F) = 0.9$, $p(E|\overline{F}) = 0.2$, $p(F) = 0.3$, $p(\overline{F}) = 0.7$. Thus

$$p(E) = 0.9 \cdot 0.3 + 0.2 \cdot 0.7 = 0.41.$$

b. If the plant is dead when you return, what is the probability that your friend forgot to water it?

This is $p(E|F) = \dfrac{0.9 \cdot 0.3}{0.41} = 27/41$. Numerically, the probability is about 66%.

6. The expansion of $(x+y+z)^3$ contains ten terms after like terms are collected:

$$(x+y+z)^3 = x^3 + 3x^2y + 3xy^2 + y^3 + 3x^2z + 6xyz + 3y^2z + 3xz^2 + 3yz^2 + z^3.$$

After like terms are collected, how many terms are there in the expansion of $(x+y+z+w)^{100}$?

We need to find the number of expressions $x^a y^b z^c w^d$ with $a+b+c+d = 100$, i.e., the number of solutions to the equation

$$a+b+c+d = 100$$

in non-negative integers. This is a bagel problem; you're buying 100 bagels and there are four kinds of bagels. The answer is thus $\dbinom{103}{3}$, or 176851 if you're calculating at home.

7. Suppose that A is a finite set with at least two elements and that R is an equivalence relation on A. Show that there are two distinct elements of A whose equivalence classes under R have the same size.

Each equivalence class has at least one element because $[a]_R$ contains a. An equivalence class can be all of A. (Think of the relation in which all elements of A are related to each other.) Thus the possible sizes of the equivalence classes are 1, 2, 3,…, n if $n = |A|$. Because there are n elements of A, it does not look as if the pigeonhole principle will be useful: think of the pigeons as the elements of A and pigeonholes as the possible sizes of equivalence classes. However, there's an extra piece of information—and note that the same theme occurred in a homework problem: if there is an equivalence class of size 1, there is no equivalence class of size n. (If $[a]_R$ has size 1, then a is related only to itself; if $[b]_R$ has size n, then b is related to everything, including a.) Hence there are always at most $n-1$ sizes of equivalence classes. Since there are n elements of A, the pigeonhole principle implies that there are two elements whose equivalence classes have the same size.

8. Math 55 students Alice and Bob announce their RSA public keys as (n, a) and (n, b); because they are good friends, they use the same modulus n. Their exponents a and b are relatively prime. 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 was on the second midterm more or less verbatim, except that the exponents 13 and 40 of the midterm have been replaced by unknown numbers a and b. Both of these exponents are relatively prime to $\phi(n)$ (because we're in the world of RSA) and they are relatively prime to each other (according to the statement of the problem). If Charlie's plain text is m, Charlie sends the encrypted texts m^a and m^b (mod n) to Alice and Bob, respectively. Eve uses the Euclidean algorithm to write $1 = ra + sb$ and computes $(m^a)^r(m^b)^s = m^1 = m$ modulo n. The only wrinkle is that one of the numbers r and s is negative. Say r is negative. Then we compute $(m^a)^r$ by computing the inverse of m^a mod n and raising that inverse to the $-r$ power.

9a. For which values of n does the complete graph on n vertices have an Euler circuit?

"A connected multigraph with at least two vertices has an Euler circuit if and only if each of its vertices has even degree." In K_n, each vertex is connected (once) to the $n-1$ other vertices and thus has degree $n-1$. Thus the condition is that n be odd. You might want to consider what happens when $n = 1$ and the graph has no edges.

b. If A, B and C are sets such that $A \cap C = B \cap C$ and $A \cup C = B \cup C$, does it follow that $A = B$? (Give a proof or a counterexample.)

It does follow that $A = B$. This was explained by Max during the review session of May 9. To show $A = B$, you have to show that $x \in A \longrightarrow x \in B$ and vice versa. However, A and B play symmetrical roles, so the "vice versa" is automatic: you just change all occurrences of "A" to "B" and vice versa. Let

$x \in A$. If x is in C, x is in $A \cap C = B \cap C$, and thus is in B. Assume now that x is in A but *not* in C. Then x is in $A \cup C = B \cup C$ but not in C. Therefore it must be in B.