Math 55

PROFESSOR KENNETH A. RIBET

Final Examination

May 11, 2015

11:30AM–2:30PM, 100 Lewis Hall

Please put away all books, calculators, cell phones and other devices. You may consult a single two-sided sheet of notes. Please write carefully and clearly in *complete sentences*. Be sure to explain what you are doing: the paper you hand in will be your only representative when your work is graded. Do not worry about simplifying or evaluating expressions with decimal numbers, factorials, binomial coefficients and the like.

At the conclusion of the exam, hand your paper in to your GSI.

The point values for the ten questions were respectively: 5, 4, 5, 5, 4, 5, 5, 4, 4, 5. The maximum possible score was 46.

1a. Show that $\binom{-n}{10} = \binom{n+9}{10}$ when n is a positive integer.

This was intended to be straightforward. See Example 8 on page 540 of the book for an explanation of the identity $\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}$. In this case, $r = 10$ is even, so the term $(-1)^r$ is just 1.

b. Prove that $3^{32} - 2^{32}$ is divisible by 13

An equivalent statement is that 3^{32} and 2^{32} coincide mod 13. Now $3^2 = 9$ and $2^2 = 4$. Since these are negatives of each other mod 13, their squares are equal mod 13: $3^4 \equiv 2^4 \pmod{13}$. Since 32 is a multiple of 4, the 32nd powers agree mod 13 as well.

2. Let S be the set of 5-card poker hands with the uniform probability distribution. Let $X : S \to \{0, 1, 2, 3, 4\}$ be the random variable that assigns to each hand the number of aces

in that hand. What is the expected value of X? (Once again: you need to explain your answer; writing down a number is not sufficient.)

Pretty much by definition, $E(X) = 0 \cdot a_0 + 1 \cdot a_1 + 2 \cdot a_2 + 3 \cdot a_3 + 4 \cdot a_4$, where a_i is the probability that a hand has i aces. If you write down the a_i correctly, you get an expression involving binominal coefficients that one can calculate to be 5/13. (By my rules, you could write everthing down in terms of binomial coefficients, walk away and get full credit.)

A more thoughtful way of proceeding is to imagine that poker hands are ordered so that there is a first card, second card and so on in the hand. There's actually a standard order to a deck of cards; this is the order in which cards are arranged when you open up a brand new deck. Hence there's an unambiguous way of arranging the hand. You can let X_j ($j = 1, \cdots, 5$) be the random variable whose value is 1 if the jth card is an ace and 0 otherwise. Then clearly $X = X_1 + X_2 + \cdots + X_5$, so that $E(X) = \sum E(X_j)$. Since the probability that the jth card is an ace should be $\frac{1}{13}$, we should get $E(X) = \frac{5}{13}$. If you write an explanation like this, you get full credit as well.

3. Let G be the simple graph whose vertices are the bit strings of length 4, two bit strings being connected by an edge if and only if they differ in exactly one place.

This problem appears as question #9 on the spring, 2013 final exam. Check the course web site for the solution that I wrote two years ago.

a. Show that G is bipartite and that G has no circuits of length three.

b. Is G planar?

4. Ivet has a bag of 12 biased coins. Six of these come up heads 3/5 of the time, while the other six come up tails 2/3 of the time. Ivet reaches into the bag, pulls out a coin at random and tosses it. The coin comes up tails. What is the probability that she pulled out a coin that is biased toward tails?

This is more or less the biased coin problem on the second midterm, but I changed the numbers and the wording a bit. Let E be the event that Ivet pulled out a tail-biased coin, so that $\overline{E}$ is the event that she pulled out a head-biased coin. Let F be the event that she pulls out a coin, flips it and gets "tails." We seek to calculate $p(E|F)$. The formula that we should apply is $p(E|F) = \frac{p(F|E)p(E)}{p(F)}$. Now $p(F) = p(F \cap E) + p(F \cap \overline{E}) = p(F|E)p(E) + p(F|\overline{E})p(\overline{E})$. We can plug in this formula for $p(F)$ and get

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

But $p(E) = p(\overline{E}) = 1/2$, so we can simplify a bit:

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

Now $p(F|E) = 2/3$ and $p(F|\overline{E}) = 2/5$. Thus my answer is $5/8$. Your mileage may vary.

5. Suppose that $f : A \to \mathcal{P}(A)$ is a function from a set to its power set. Let

$$B = \{\, b \in A \,|\, b \notin f(b) \,\},$$

and let c be an element of A. Show that $f(c) \neq B$ by deriving a contradiction from the assumption $f(c) = B$.

This problem was #4 on the first midterm. See the course web site for my solution to the problem. (Watson Ladd discussed this problem in the Tuesday review session last week as well.)

6a. Suppose that n is a positive integer. Prove that there are two different elements of the sequence

$$0!, 1!, 2!, \ldots, n!$$

that leave the same remainder when divided by n.

This is a clear application of the pigeonhole principle.

Whoops, it would have been, except for the fact that $0! = 1!$. Anyone who notices this and applies this equality to parts (a) and (b) gets five free points. Sometimes the best-laid plans. . . .

You have $n + 1$ numbers and we are discussing their residues mod n. There are only n possible residues mod n, so two of the numbers will have the same residue. Having the same residue is a synonym for leaving the same remainder on division by n.

b. Show that there are integers i and j with $0 \leq i < j \leq n$ such that $j! - i!$ is a multiple of n.

Two numbers have the same residue mod n is and only if their difference is a multiple of n.

7. Find the number of surjective (onto) functions from the set $\{\, 1, 2, 3, 4, 5, 6 \,\}$ to the set $\{\, a, b, c \,\}$.

This is an annoying inclusion–exclusion problem. I more or less did it on the board at the review session last Thursday. (When I did it, the source set had five elements instead of six, but that's no biggie.)

Let S be the set of *all* functions $\{\, 1, 2, 3, 4, 5, 6 \,\} \longrightarrow \{\, a, b, c \,\}$. Then S has 3^6 elements because there are three choices for the images of each element of the source set. Let A be the set of functions whose images do not contain a. Similarly define B and C. Then the set $A \cup B \cup C$ is the set of non-surjective functions from the source set to the target

set. Accordingly, the number that we seek is $|S| - |A \cup B \cup C|$. Thus we need to calculate $|A \cup B \cup C|$, which we can do by inclusion exclusion:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

As I explained on Thursday, $A \cap B \cap C$ is the null set because it's the set of functions from $\{1, 2, 3, 4, 5, 6\}$ to $\{a, b, c\}$ whose images contain none of a, b, c. The sets A, B and C each have 2^6 elements, while the three double intersections each have $1^6 = 1$ element. Thus the answer is apparently

$$3^6 - 3 \cdot 2^6 + 3 \cdot 1^6 = 540.$$

Of course, there's no need to calculate the final answer as 540.

8. Bob is learning about RSA encryption. To try a numerical example, Bob chooses the small prime numbers $p = 15213907$ and $q = 98804683$, and the encryption exponent $e = 461442496988431$. Running the extended Euclidean algorithm, he finds the equation

$$1 = 1234567e - 378978(p-1)(q-1).$$

Bob now wishes to find a decryption exponent, a positive integer d such that

$$(M^e)^d \equiv M \pmod{pq}$$

for all integers M such that $\gcd(M, pq) = 1$.

Help Bob by supplying him with the sought-after integer d and write a paragraph that explains to him why this d will work.

The decryption exponent is the inverse of the encryption exponent, modulo $(p-1)(q-1)$. Mod this product, we have (from the displayed Euclidean equation) $1 \equiv 1234567e$, so that the inverse of the encryption exponent e is 1234567. We take $d = 1234567$. You should tell Bob that $(M^e)^d \equiv 1 \bmod p$ by Fermat's Little Theorem; similarly $(M^e)^d \equiv 1 \bmod q$. Hence $(M^e)^d - 1$ is divisible by p and by q. Since these two divsors are relatively prime, $(M^e)^d - 1$ is divisible by their product, pq. Thus we have the displayed congruence that you were to justify to Bob.

9. Establish the congruence

$$f_n \equiv 3 \cdot 8^n - 3 \cdot 4^n \pmod{11}$$

for $n \geq 0$. Here, f_n is the nth Fibonacci number.

This problem was intended to be a straightforward proof by (strong) induction. For $n = 0$, the right-hand side and the left hand side are both 0. For $n = 1$, the right-hand side is $3(8 - 4) = 12 \equiv 1$ and the left-hand side is 1 as well. These are our two base cases. For $n \geq 0$, we have

$$f_{n+2} = f_{n+1} + f_n \equiv 3(8^{n+1} + 8^n) - 3(4^{n+1} + 4^n)$$

mod 11. Thus it suffices to establish the two congruences (mod 11)

$$8^{n+2} \equiv 8^{n+1} + 8^n, \qquad 4^{n+2} \equiv 4^{n+1} + 4^n.$$

Because all terms in the left-hand congruence contain a factor 8^n, the left-hand congruence will follow if we can show that $8^2 \equiv 8 + 1 \pmod{11}$; similarly, the right-hand congruence will

follow from $4^2 \equiv 4+1 \pmod{11}$. Both of these latter congruences can be checked easily: 11 divides $64 - 9 = 55$ and $16 - 5 = 11$.

10a. In how many different ways can 20 identical cookies be distributed among six distinct children if each child receives at least two cookies?

Give each child two cookies. Then 12 have been given away and 8 remain to be distributed to the six children. This is a full bore bagel (= stars and bars) problem; the answer is $\binom{8+5}{5}$. It's also a fully boring problem—sorry.

PS: The phrase "distinct children" was lifted from Example 11 on page 543 of the book. It's certainly not very appealing.

b. In how many different ways can 20 distinguishable cookies be placed into three indistinguishable boxes?

You might sidle up to the problem this way. Suppose that the boxes are labeled (say "A," "B," "C"). Then there are three ways to place the first cookie in a box, three ways to place the second cookie in a box, and so on. The number of ways to place the 20 cookies into three labeled boxes is 3^{20}. Now you might say that there are $3! = 6$ ways to label the boxes, so we should divide by 6 and get $3^{20}/6$ as our answer. That's a pretty good answer, but it's not a whole number, so something is amiss!

To see what's wrong, think what happens if you label one of the boxes, say "A," and throw all 20 cookies into box A. Then you can label the other two (empty) boxes "B" and "C" or "C" and "B," and both choices lead to the same way of placing the 20 cookies into labeled boxes. However, this problem arises only when two of the three boxes are empty. If at least two of the boxes receive cookies, then the six ways of labeling the boxes lead to six different ways of assigning cookies to labeled boxes. It seems to me that we should separate out the three ways of throwing all cookies into a single labeled box; these three ways lead to a single way of placing the cookies into indistinguishable boxes. The other $3^{20} - 3$ ways to putting cookies into labeled boxes can be converted into ways of putting cookies into indistinguishable boxes by the division that we contemplated in the paragraph above. My answer is thus

$$\frac{3^{20} - 3}{6} + 1 = \frac{3^{19} + 1}{2} = 581130734.$$

You can compare this problem with Example 10 on page 430 of the book: "How many ways are there to put four different employees into three indistinguishable offices, when each office can contain any number of employees?" It's the same as my problem, but with 20 replaced by 4. My answer $\dfrac{3^{19}+1}{2}$ then gets replaced by $\dfrac{3^3+1}{2} = 14$, which is the same as Rosen's answer. However, the book doesn't try to discuss the problem conceptually; instead, it just lists the 14 possibilities: "Counting all the possibilities, we find that there are 14 ways to put four different employees into three indistinguishable offices." I think that the author

could have done better. (Note: there's no need for you to calculate the fraction $\frac{3^{19}+1}{2}$ as 581130734.)