Discrete Math, 375 (Spring 2015): Mid-term 2.

Do all of the problems below. Please write your name and your class (the class time of 1030 or 1200) on blank cover sheet (the backside should be blank as well). Write neatly and be clear. Remember that you're amazing.

Problem 1. [A cookie for you: 10 points] State the definition for the following:

(a) A probability distribution P on a countable set S.

(b) For a pair of positive integers a,n, define the residue class $\overline{a}$ of a modulo n.

Solution.

First, I strongly recommend that you all give precisely the definition I give. I will always give full credit for such answers. For those of you that attend the lecture Tuesday before class when I gave those definitions, it seems you all did. For those you that don't attend lectures always (that's fine, you are free to do what you wish), you could have guessed which two definitions would be on the exam from the review sheet. If you are in doubt about the "official" definition, ask me. I have no sympathy for people that cannot get two definitions that you were told in advance to know.

For (a): A **probability distribution** on a countable set S is a function

$$P\colon S \longrightarrow [0,1]$$

such that

$$\sum_{s\in S} P(s) = 1.$$

Remark. If you didn't say P was a function, you got no credit. That was a common mistake. I gave no credit for "fluffy" answers like it gives a way of measuring probabilities of things. That is a concept that is loose and not a rigorous definition.

For (b): The **residue class** of a modulo n is the set

$$\overline{a} = \{m \in \mathbf{Z} \;:\; n \mid (a-m)\}.$$

Remark. For the most part, people gave the above. If you gave a definition of what a general residue class was, I gave little/no credit.

Problem 2. [Red or Blue: 10 points] State whether or not the following is true or false. You do not need to justify your answer.

(a) Given positive integers a,b,n, if $ab = 0 \mod n$, then either $a = 0 \mod n$ or $b = 0 \mod n$.

(b) For two random variables X, Y on a probability space S, we have

$$E(XY) = E(X)E(Y).$$

(c) $\mathbf{Z}/17\mathbf{Z}$ is a field.

(d) There are infinitely many primes of the form $2k+1$ where $k \in \mathbf{N}$.

Solution.

(a) False. Take $a = 2$, $b = 3$, $n = 6$. This is directly from the homework. This was also mentioned in lecture.

(b) False. This is only true if the random variables are independent.

(c). True. This is directly from the homework. This was also mentioned in lecture.

(d) True. There are infinitely many odd primes as there can only be one even one!

Problem 3. [Can you count beyond the atom?: 10 points]

(a) Find an integer $0 \leq a \leq 1008$ such that

$$5^{1011} = a \mod 1009.$$

(b) Find an integer $2 \leq a \leq 16$ such that

$$5^a = 1 \mod 17.$$

(c) Compute $\phi(18), \phi(19)$ where ϕ is the Euler ϕ–function.

Solution

(a). Since 1009 is prime and $\text{GCD}(5, 1009) = 1$, by Fermat, we have

$$5^{1008} = 1 \mod 1009$$

and so

$$5^{1011} = 5^{1008} \cdot 5^3 = 1 \cdot 5^3 = 125 \mod 1009.$$

Thus $a = 125$.

(b). Since 17 is prime and $\text{GCD}(5, 17) = 1$, by Fermat, we have

$$5^{16} = 1 \mod 17.$$

So $a = 16$.

(c). $18 = 2 \cdot 3^2$. Thus

$$\phi(18) = \phi(2)\phi(9) = 2\left(1 - \frac{1}{2}\right) 9 \left(1 - \frac{1}{3}\right) = 6.$$

Since 19 is prime, $\phi(19) = 18$.

Remark. I told the class on Tuesday about these problems (modulo slightly misinforming the class about problem (b)). There were some simple mistakes on (a) that I largely ignored. On (b), in class I said the problem would be of the form: find $0 < a < 16$ such that

$$5a = 1 \quad \text{mod } 17.$$

Sorry about that. The problem that was actually on the exam is easier. To solve $5a = 1$ mod 17, you can still use Fermat. Specifically, by Fermat, we have

$$5^{16} = 1 \quad \text{mod } 17$$

and so

$$a = 5^{15} \quad \text{mod } 17$$

would work. I didn't want you to have to do much in the way of computation here and so I replaced the problem with the easier one of find a such that $5^a = 1 \quad \text{mod } 17$. On (c), most of you got $\phi(19)$ but there were various mistakes on $\phi(18)$.

Remark. Precisely 5 students gave the following answer to (a):

$$\begin{aligned}
&5^{1009} = 1 \quad \text{mod } 1009 \qquad \text{(this is not correct)}\\
&5^{1011} = 1 \cdot 19 \cdot 19 \quad \text{mod } 1009 \qquad \text{(I have no clue where 19 came from)}\\
&5^{1011} = 361 \quad \text{mod } 1009.
\end{aligned}$$

When n exams are identical (most telling with weird, wrong answers), I presume that n people collaborated on the exam. I encourage collaboration on the problem sets for sure. I never actually forbid collaboration on exams but I do have a general rule when it comes to collaboration. If you collaborate in the real world, you are a team, for better or worse. Success and failure is shared equally. As such, if n people collaborate on the exam, each individual gets $1/n$ of the total value of their individual exam score. You can collaborate as a class on the exam if you wish. However, as each class has at least 30 people and the exam is worth 60 points, the maximum value obtainable would be 2. Given that I gave you the two definitions in advance and told you that there were two true and two false in Problem 2, each student is ensured (in theory) a score of at least 15 if they work solo. I'd suggest working solo. Our team of 5 was ensured no better than 12 for each individual. You can see that you'd not want a team bigger than 4 but really 2-3. A 2 person team doesn't seem that bad if you don't think you can score above 30. Finally, if you collaborate but were not aware that you collaborated, you should be more careful about who can see your exam. That is not my problem.

Problem 4. [Uniformize my distribution: 10 points] Let $S = \{1, \ldots, 120\}$ and let P be a uniform probability distribution.

(a) Determine the probability that $x \in S$ satisfies $x = 0 \mod 4$.

(b) Determine the probability that $x \in S$ satisfies $x = 0 \mod a$ and $x \neq 0 \mod 4$ where $a \in \{2, 3\}$.

Solution.

(a). The probability that an integer is divisible by 4 is $1/4$. You can enumerate the list of such elements in the set $S = \{1, \ldots, 120\}$. Specifically,

$$E = \{4k \; : \; k = 1, \ldots, 30\}.$$

In particular, there are 30 such numbers and so the probability P that a given number is divisible by 4 is

$$P = \frac{|E|}{|S|} = \frac{30}{120} = \frac{1}{4}.$$

(b). The probability that an integer is divisible by $2, 3$ is $1/6$. As in part (a), we can enumerate the set $E_{2,3}$ of numbers that are divisible by by 2 and 3. In fact, being divisible by 2 and 3 is equivalent to being divisible by 6. Thus,

$$E_{2,3} = \{6k \; : \; k = 1, \ldots, 20\}.$$

Now, we can write out this list

$$E_{2,3} = \{6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120\}.$$

The elements that are divisible by 4 are nothing more than the numbers in S that are divisible by 12:

$$E_{2,3,4} = \{12, 24, 26, 48, 60, 72, 84, 96, 108, 120\}.$$

Therefore, the event of interest for us is given by

$$E = E_{2,3} - E_{2,3,4} = \{6, 18, 30, 42, 54, 66, 78, 90, 102, 114\}.$$

The probability of the event E is then

$$P = \frac{|E|}{|S|} = \frac{10}{120} = \frac{1}{12}.$$

Remark. For those of you that said the probability of the event was larger than $1/6$ should have actually thought about this problem more. Most of you got (a) and so you should have know that if the numbers are divisible by both 2 and 3, the probability of the event E could certainly be no bigger than $1/6$. Two popular answers were $5/12$ and $7/12$, both of which are clearly wrong via this simple analysis.

Remark. I graded both (a) and (b) as all or nothing. If you got the right answer, you got full credit. If you didn't get the right answer, you got no credit.

Problem 5. [Dr. Mer: 10 points]

(a) Let a, b be positive integers. Prove that

$$\mathrm{GCD}(2^a - 1, 2^b - 1) = 2^{\mathrm{GCD}(a,b)} - 1.$$

(b) Let $p > 2$ be a prime. Prove that if ℓ is a prime that divides $2^p - 1$, then $\ell = 2kp + 1$ for some positive integer k.

Solution:

Part (a):

Set

$$m = \mathrm{GCD}(2^a - 1, 2^b - 1), \quad n = \mathrm{GCD}(a, b).$$

We first show that m divides $2^n - 1$. We know that there exist integers s, t such that

$$as + bt = n.$$

Now

$$2^a = 2^b = 1 \mod m.$$

Thus,

$$2^{as} 2^{bt} = 1^s \cdot 1^t = 1 \mod m.$$

Hence m divides $2^{as+bt} - 1 = 2^n - 1$. For the second part, we will show that $2^n - 1$ divides both $2^a - 1, 2^b - 1$. If that is true, then $2^n - 1$ is a common divisor of both $2^a - 1, 2^b - 1$. We must then have that $2^n - 1 \leq m$ since m is the greatest common divisor. In particular, $2^n - 1 = m$ since $m \mid 2^n - 1$. To see that $2^n - 1$ divides $2^a - 1, 2^b - 1$, we first write $a = q_a n$ and $b = q_b n$ for a pair of positive integers q_a, q_b. Now, we see that

$$\frac{2^{q_a n} - 1}{2^n - 1} = 2^{(q_a - 1)n} + 2^{(q_a - 2)n} + \cdots + 2^{2n} + 2^n + 1.$$

Similarly,

$$\frac{2^{q_b n} - 1}{2^n - 1} = 2^{(q_b - 1)n} + 2^{(q_b - 2)n} + \cdots + 2^{2n} + 2^n + 1.$$

Remark: How did I compute the above fractions? Well, I used something called polynomial division that you learned in basic algebra. Set

$$f_a(x) = x^{q_a n} - 1, \quad f_b(x) = x^{q_b n} - 1, \quad g(x) = x^n - 1.$$

Then

$$\frac{f_a(x)}{g(x)} = \sum_{j=1}^{q_a} x^{(q_a - j)n}$$

and

$$\frac{f_b(x)}{g(x)} = \sum_{j=1}^{q_b} x^{(q_b - j)n}.$$

As an example, take $q_a = 3$ and $n = 2$. So we have $f_a(x) = x^6 - 1$ and $g(x) = x^2 - 1$. To compute

$$\frac{x^6 - 1}{x^2 - 1}$$

we perform polynomial division. We see that we need to multiply x^2 by x^4 to get an x^6 term and so in the first step, we have

$$\frac{x^6 - 1}{x^2 - 1} = x^4 + \frac{x^4 - 1}{x^2 - 1}.$$

At the next step, we need to multiple x^2 by x^2 to get x^4 and so

$$\frac{x^4 - 1}{x^2 - 1} = x^2 + \frac{x^2 - 1}{x^2 - 1} = x^2 + 1.$$

Thus

$$\frac{x^6 - 1}{x^2 - 1} = x^4 + x^2 + 1.$$

Now evaluate this formula for $x = 2$.

Part (b):

Let ℓ be a prime divisor of $2^p - 1$. By Fermat, we have

$$2^{\ell - 1} = 1 \mod \ell$$

and since ℓ divides $2^p - 1$, we have

$$2^p = 1 \mod \ell.$$

It follows that p divides $(\ell - 1)/2$ (this also uses that p is prime and that $p > 2$) and so

$$\frac{\ell - 1}{2} = kp$$

or

$$\ell = 2kp + 1.$$

Remark. The assertion ”it follows that p divides $(\ell-1)/2$” is not entirely obvious. Let k be the smallest positive integer such that

$$2^k = 1 \mod \ell.$$

Since the group of units of $\mathbf{Z}/\ell\mathbf{Z}$ has order $\phi(\ell) = \ell - 1$, we know that k divides $\ell - 1$. We also know that k divides p. Since p is an odd prime, k must be odd and so k must divide $(\ell-1)/2$. Note that $\ell - 1$ is even since ℓ is odd as ℓ divides the odd number $2^p - 1$. So we can write

$$p = ak, \quad \frac{\ell-1}{2} = bk.$$

Note that $k > 1$ since $2 < \ell$ and so $2 \neq 1 \mod \ell$. Since p is prime and a, k are positive integers, it must be that $a = 1$. Thus

$$p = k$$

and so

$$\frac{\ell-1}{2} = bp.$$

Solving for ℓ, we have

$$\ell = 2bp - 1.$$

Remark. You do not need to know any group theory to do the above problem either. We again start with the smallest positive integer $k > 1$ such that

$$2^k = 1 \mod \ell.$$

If m is a positive integer such that

$$2^m = 1 \mod \ell,$$

then $k \leq m$. Assume that k does not divide m. Then

$$m = ck + r$$

where

$$0 < r < k.$$

Now, we have

$$1 = 2^m = 2^{ck+r} = 2^{ck}2^r = 2^r \mod \ell.$$

Thus,

$$2^r = 1 \mod \ell.$$

That is a contradiction though since $0 < r < k$. Specifically, r is a smallest positive integer than k and also satisfies

$$2^r = 1 \mod \ell.$$

However, we chose k to be the smallest positive integer with this property. From that elementary argument, we see that if k must divide p and $\ell - 1$. We then argue as before to see that $k = p$. Finally, since p is odd and $\ell - 1$ is even, we see that p divides $(\ell - 1)/2$.

Remark. The grading on (a),(b) was fairly strict in that I gave little/no partial credit. Whether you got partial credit for crap was largely how much I trusted you after reading Problems 1-4. If, for instance, you clearly didn't know how to do Problems 1 or 3, I tended to give no credit whereas I may have given 1-2 points (likely 1) for crap.

Remark. I appreciate that Problem 5 wasn't easy. That said, it didn't use any mathematics that is beyond your skill set. Basic algebra. Basic results from our class. Only 3 students got 5 points or better on Problem 5. You can read more about some related material via the link: `http://en.wikipedia.org/wiki/Mersenne_prime`.

Problem 6. [Dr. Zsig: 10 points]

(a) Let $b > 6$ be a positive a positive integer. Prove that if $k > 1$, there exists a prime ℓ that divides $b^k - 1$ but does not divide $b^j - 1$ for any $1 \leq j < k$.

(b) Let $b > 6$ be a positive integer. Prove that for $k \geq 1$, there exists a prime ℓ that divides $b^k + 1$ but does not divide $b^j + 1$ or $b^{2j} - 1$ for any $1 \leq j < k$.

Solution.

(a). This result is due to Bang and Zsigmondy's theorem. It isn't that hard in the sense that it uses fairly elementary things but is surely well beyond what you can do in class on an exam. It looks so simple too! I learned of this result after producing, over a few months, various special cases of it that I needed in a paper. In my applications, b was an odd prime. You can find a discuss of how to prove it via the link to below: `http://math.stackexchange.com/questions/660585/elementary-proof-of-zsigmondys-theorem`. You can also find more at the wiki page: `http://en.wikipedia.org/wiki/Zsigmondy%27s_theorem`.

No one really made much progress on (a). As such, it is as if the problem never existed. In fact, "Joke Bonus" has a much greater effect than this part of problem 6.

(b). The solution to (b) can also be found via the above link. However, it is quite simple. Consider $b^{2k} - 1$ where $b > 6$ and $k > 1$. By (a), there is a prime that divides $b^{2k} - 1$ but does not divide $2^j - 1$ for all $1 \leq j < 2k$. Now,

$$b^{2k} - 1 = (b^k - 1)(b^k + 1).$$

Since ℓ divides $b^{2k}-1$ but not b^k-1, it must be that ℓ divides b^k+1. For any $j<k$, we have

$$b^{2j}-1=(b^j-1)(b^j+1).$$

In particular, since ℓ does not divide $b^{2j}-1$, it must be that ℓ does not divide b^j+1 also.

Remark. If your (a) didn't have any content, I tended to give 0 points. A few attempts garnered more than 0. In fact, 5 out of roughly 80 students got more than 0 points with 4 of them getting 1 points and 1 person getting 2 points. On (b), if you at any point factored $b^{2k}-1=(b^k-1)(b^k+1)$, I gave nearly full credit. If you didn't factor then you likely got very little credit.