Proof Techniques Problem Set 2 Solutions

Mathcamp 2003, Week 1

due Thursday

I've tried to make these solutions both clear and satisfying. Ideally, this will provide a template for you to use in writing proofs.

1. Every odd number (and thus prime number) can be written in the form $4k+1$ or $4k+3$ (this means that its remainder, when divided by 4, is either 1 or 3). We're going to work up to some variations on the infinitude of primes.

   (a) What kind of number do you get when multiplying two numbers of the form $4k+1$? What about $4k+3$? What about multiplying the two together?

   We do three calculations. $(4k_1+1)\cdot(4k_2+1) = 16k_1k_2+4k_1+4k_2+1 = 4(4k_1k_2+k_1+k_2)+1$ is a number of type $4k+1$.

   $(4k_1+3)\cdot(4k_2+3) = 16k_1k_2+12k_1+12k_2+9 = 4(4k_1k_2+3k_1+3k_2+2)+1$ is a number of type $4k+1$.

   $(4k_1+1)\cdot(4k_2+3) = 16k_1k_2+12k_1+4k_2+3 = 4(4k_1k_2+3k_1+k_2)+3$ is a number of type $4k+3$.

   (b) Prove that there are infinitely many primes of the form $4k+3$ (hint: suppose there were a finite list with $p_1 = 3$, $p_2 = 7$, $p_3 = 11$, etc. Consider $4p_2p_3p_4\dots p_n+3$. Why do we omit p_1?).

   Suppose for contradiction that there were a finite number of primes of the form $4k+3$. List them out in the form $p_1 = 3, p_2 = 7, p_3 = 11, \dots, p_n$. Consider the quantity $n = 4p_2p_3p_4\dots p_n+3$. This value is not divisible by $p_1 = 3$ because it is a sum of two numbers one of which is not divisible by 3 and one of which is. Additionally, n is not divisible by any of p_2 through p_n because it is again a sum of two numbers, one of which is divisible by each p_i and one of which is not (in fact, any division will have remainder 3).

   n must have a prime factorization. Additionally, one prime that divides it must be of the form $4k+3$; multiplying just numbers of the form $4k+1$ yields again another number of that type, so this cannot be a product of only primes of the form $4k+1$. This prime that divides it, of the form $4k+3$, cannot be any of p_1 through p_n by the above argument. Thus, the list of primes we compiled was not complete; this is a contradiction, so that list cannot exist and there are infinitely many primes of the form $4k + 3$.

(c) Can you do the same thing for primes of the form $4k + 1$?

It is true that there are infinitely many primes of the form $4k+1$, but the proof is more involved and this method does not work. The problem is in the last step: when we compile the number $4p_1p_2 \dots p_n + 1$, we cannot guarantee that any of its prime factors are actually of the form $4k + 1$, because primes of the form $4k + 3$ can multiply to produce a number of the form $4k + 1$.

For a proof that does work, see, for example, *Proofs from the Book* in the section on what numbers can be represented as the sum of two squares (a very cool proof as well!).

2. Suppose you are given 25 points in the plane such that, among any three of them, two are at distance less than one unit from each other. Prove that there is a circle of radius 1 that contains 13 of the points.

   Choose any point A. If all points are within distance 1 from A, then we are done because all points are in a circle of radius 1 about A. Otherwise, there is some point B at distance greater than 1 from A. Each of the other 23 points must lie in a circle of radius 1 about A or else a circle of radius 1 about B (or it violates the given condition). Then, by the pigeonhole principle, one of these circles contains at least 13 of the points.

3. We showed in class that, if you choose 55 numbers between 1 and 100, there are two that differ by 9. Prove that there are also two that differ by 10, 12, and 13. Is it also true for 11? Why or why not?

   I will use a different method than that from class: the method from class fails, for example, for 12. Thanks to Jeremy for pointing this out.

   We'll just do 12; the rest can be done in the same way.

   We construct the following sets: $\{1, \dots, 24\}, \{25, \dots, 48\}, \{49, \dots, 72\}, \{73, \dots, 96\}$, and $\{97, \dots, 100\}$. By the pigeonhole principle, if we choose any 13 points from any of the first four sets, then two of the chosen numbers will have the same remainder when divided by 12. This means that those numbers will differ by 12.

   We're going to apply pigeonhole again, this time using the sets we constructed as our holes. Indeed, we have five holes, but the fifth can hold at most four of the chosen 55 numbers. Thus we will need to distribute at least 51 numbers between the remaining four holes.

   By the generalized pigeonhole principle, there is a hole that holds at least $51/4 > 12$ numbers, that is, at least 13 numbers. By our earlier statement, this means that there are two numbers that differ by 12.

4. Prove that it is impossible to color the plane with two colors (say, red and blue) such that each pair of points one unit apart has a different color.

Assume for contradiction that such a coloring was possible. Consider any equilateral triangle with side length 1. If any two vertices are the same color, then we have found a pair of points one unit apart that are the same color. But we have two colors and three points; the pigeonhole principle (for example) requires that two vertices have the same color.

5. Suppose that each point in the plane is colored either red or blue (without the conditions from the previous problem). Show that there is some rectangle all of whose vertices are the same color (hint: the trick with the pigeonhole principle is to figure out where to put your holes; once you get that, the rest falls into place nicely).

   This one's tough! It should have had at least one (*).

   Consider a 3×9 grid of points (that is, 3 vertices vertically and 9 vertices horizontally).

   For any three vertices, there are 8 different possible color combinations for the vertices. We have 9 vertical sets of three vertices, so some two of them (by pigeonhole) must have the same coloring. Consider these two; each of them has (the same) two vertices either red or blue. Draw a rectangle using those vertices, and we are done.

6. A point in the plane is a *lattice point* if both of its coordinates are integers (for example, $(0, 1), (4, 5), (-5, 18)$ are all lattice points; $(\frac{1}{2}, 8)$ is not).

   (a) Prove that, if one chooses five lattice points in the plane, the midpoint of some two of them is a lattice point.

   Consider the parity of each of the various lattice points: you can have (even, even), (even, odd), (odd, even), or (odd, odd). If you have two vertices with the same parity, then their midpoint will be a lattice point (because adding two even integers or two odd integers yields an even integer).

   We have four different parities, but five points, so some two have the same parity by the pigeonhole principle; then the midpoint of those two points is a lattice point.

   (b) Do the same for nine lattice points in 3-dimensional space.

   The parity argument functions in the same way as before; if we have two points with the same parity in all their coordinates, their midpoint is a lattice point. There are eight possible parities, and nine points, so two have the same parity; we are done.

7. (a) (*) Suppose we choose five integers $a_1, \ldots, a_5$. Prove that either one of the a_i's is divisible by 5, or the sum of several numbers in a row is divisible by 5.

   Consider the five sums $a_1, a_1 + a_2, \ldots, a_1 + \ldots + a_5$. If any of them has remainder zero when dividing by five, then we're done. Otherwise, we have four possible remainders and five sums; some two of the sums have the same remainder when divided by 5.

Subtract one from the other; we get a sum of consecutive a_i's which is evenly divisible by 5. For example, subtracting $a_1 + a_2$ from $a_1 + a_2 + a_3 + a_4$ gives us the sum $a_3 + a_4$, which has consecutive entries.

(b) Prove the same result for arbitrary n: that is, given n integers $a_1, \ldots, a_n$, some sum of consecutive a_i's is divisible by n.

We consider the n sums $a_1, a_1 + a_2, \ldots, a_1 + \ldots + a_n$. If any of these have remainder 0 when dividing by n, we're done, so assume none of them do. Then some two of them have the same remainder when dividing by n (because there are $n - 1$ remaining remainders). Subtract one from the other; this new sum is a sum of consecutive a_i's, and has remainder 0 when divided by n.

8. (*) Prove that, for any n, there is a number composed entirely of 1's and 0's that is divisible by n (hint: use a result we had from class).

   Consider all numbers of the form $11\ldots1$. There are some two of these that both have the same remainder when divided by n (we saw this result in class). Subtract one from the other; you get a number of the form $11\ldots100\ldots0$ which is divisible by n.

Additional questions

These are, in general, not so challenging, so I'll leave them to you. They're fun enough, though.

1. Given 37 numbers, show that you can choose seven of them such that their sum is divisible by 7 (this is different from previous problems because you must choose exactly seven numbers). Can you generalize?
2. Prove that, out of any set of 27 odd numbers all less than 100, some pair sum to 102.
3. Let x be any real number. Show that, among the numbers $x, 2x, 3x, \ldots, (n-1)x$, there is one that differs from an integer by at most $\frac{1}{n}$.