SOLUTIONS TO PROBLEM SET 2

MAT 108

Abstract. These are the solutions to Problem Set 1 for MAT 108 in the Fall Quarter 2020. The problems were posted online on Sunday Oct 4 and due Friday Oct 16.

Proofs by Contradiction

Problem 1. Show that there do not exist two integers $n, m \in \mathbb{Z}$ such that $n^4 - 4m = 2$.

Hint: Proof by contradiction, i.e. assume that there exist two integers $n, m \in \mathbb{Z}$ such that $n^4 - 4m = 2$ and reach a contradiction.

Solution. Suppose there exist integers $n, m \in \mathbb{Z}$ satisfying $n^4 - 4m = 2$. If n is odd, then n^4 is odd, so $n^4 - 4m$ is odd, which contradicts $n^4 - 4m = 2$. If n is even, then $n = 2k$ for some integer $k \in \mathbb{Z}$, and consequently $n^4 = 16k^2$. Then

$$n^4 - 4m = 16k^2 - 4m = 4(4k^2 - m),$$

which is divisible by 4. But our assumption is that thhis quantity is equal to 2, which is not divisible by 2. Therefore, we have a contradiction whether n is odd or even, so we conclude that no such integers exist.

Problem 2. A natural number $n \in \mathbb{N}$ which is only divisible by 1 and n is said to be a *prime* number. Prove that there are infinitely many prime numbers.

Hint: Proof by contradiction, i.e. assume that there exist finitely many primes $\{p_1, p_2, \ldots p_N\}$, and then try to reach a contradiction. (Clue: Consider the number $P = p_1 \cdot p_2 \cdot \ldots \cdot p_N + 1$. Is this a prime ?)

Solution. First we prove a Lemma: *every natural number greater than* 1 *has a prime factor greater than* 1. To prove the lemma, we start with a natural number $n \in \mathbb{N}$ and find a prime number $p > 1$ such that $n = ap$ for some integer a. If n is prime, then we are done. Otherwise, n is divisible by a natural number r_1 satisfying $1 < r_1 < p$ and $n = k_1 r_1$ for some k_1. If r_1 is prime, then we are done.

Continue along this process: for each number r_i constructed, stop if r_i is prime. Otherwise, r_i is divisible by a natural number r_{i+1} satisfying $1 < r_{i+1} < r_i$ and $r_i = k_{i+1} r_{i+1}$. Notice that at each step, we decrease the factor. That is, we have a chain of inequalities

$$1 < \cdots < r_3 < r_2 < r_1 < n.$$

This process must stop with at most n steps, so we arrive at a prime number r_m (for some final step m) satisfying

$$n = k_1 r_1 = k_1(k_2 r_2) = k_1(k_2(k_3 r_3)) = \cdots = (k_1 k_2 \cdots k_m) r_m.$$

Therefore, r_m is a prime factor of n, satisfying $n = ap$ for $a = k_1 k_2 \cdots k_m$. Finally, since each r_i was greater than 1 by construction, we have $r_m > 1$, proving the lemma. In fact, if we apply the lemma to the natural number $\frac{n}{r_m} <$ (which is less than n), we find another prime factor of n. Continuing in this until we reach a quotient of 1, we find an even stronger result: *every natural number greater than* 1 *is equal to a product of primes, each greater than* 1.

We proceed with the main proof by contradiction. Assume the result is false, that there are *not* infinitely many primes. Then there are only finitely many primes, say N of them, and we can arrange the primes into a set $\{p_1, p_2, \ldots, p_N\}$. Form the product

$$Q = p_1 p_2 \cdots p_N,$$

and define the number $P = Q + 1$. By the lemma above, P has a prime factor $r > 1$ satisfying $P = ar$ for some integer a.

Since r is prime, it must be in our list, so $r = p_i$ for some $i \in \{1, 2, \ldots, N\}$. Therefore,

$$Q = p_1 p_2 \cdots p_{i-1} p_i p_{i+1} \ldots p_N = (p_1 p_2 \cdots p_{i-1} p_{i+1} \ldots p_N) p_i = br.$$

Where we define $b = p_1 p_2 \cdots p_{i-1} p_{i+1} \ldots p_N$. Recalling the definition of P, $P = Q + 1$, we now have the two equations

$$Q + 1 = ar$$
$$Q = br.$$

Subtracting these two equations, we find $1 = (a - b)r$, so 1 is divisible by r. But $r > 1$, and 1 is not divisible by any number greater than 1, so we arrive at a contradiction. Therefore, we conclude that our original assumption was not true, and there *are* infinitely many primes.

Problem 3. (20 pts) Prove that there are infinitely many prime numbers that have residue 3 when divided by 4. Equivalently, prove that there are infinitely many prime numbers p of the form $p = 4k - 1$ for some natural number $k \in \mathbb{N}$.

For instance, $p = 2$ or $p = 5$ are prime numbers but they are not of the form $p = 4k - 1$ for any $k \in \mathbb{N}$. So not *every* prime number is of the form $p = 4k - 1$, this problem asks you to show that there are infinitely many of them.

Hint: Adapt your proof by contradiction in Problem 2 to this case.

Solution. We again start with a Lemma: *For any integers $k_1, k_2, \ldots, k_m$, the product $(4k_1 - 3)(4k_2 - 3)\cdots(4k_m - 3)$ has residue (meaning, remainder) 1 modulo 4.* We induct on the natural number $m \geq 1$. The base case $m = 1$ is clear, because $4k_1 - 3$ has residue 1. Now, suppose the result is true for a given value m. This means that

$$(4k_1 - 3)(4k_2 - 3)\cdots(4k_m - 3) = 4K - 3$$

for some integer K. To test the case $m + 1$, we calculate

$$\begin{aligned}(4k_1 - 3)(4k_2 - 3)\cdots(4k_m - 3)(4k_{m+1} - 3) &= (4K - 3)(4k_{m+1} - 3)\\ &= 16 \cdot K \cdot k_{m+1} - 12(K + k_{m+1}) + 9\\ &= 4(4 \cdot K \cdot k_{m+1} - 3(K + k_{m+1})) + 9\\ &= 4(4 \cdot K \cdot k_{m+1} - 3(K + k_{m+1}) + 3) - 3,\end{aligned}$$

which is the form we want, so the claim is proved.

For the main proof, we again proceed by contradiction. Assume the result is false, that there are *not* infinitely many primes of the form $4k - 1$. Then there are only finitely many primes of this form, say N of them, and we can arrange them into the set $\{p_1, p_2, \ldots, p_N\}$. As before, form the product

$$Q = p_1 p_2 \cdots p_N.$$

Now define the number $P = 4Q - 1$. In Problem 2, we showed that every number greater than 1 can be written as a product of primes. Note that $P > 3$ (because $3 = 4 \cdot 1 - 1$ is definitely in our list of primes), so we can use this result.

Since P is odd, it is not divisible by 2, so our result tells us that P is a product of odd primes. All odd numbers are of the form $4k - 1$ or $4k - 3$ for some integer k, and we now want to show that P is divisible by at least one prime of the form $4k - 1$ (i.e., a prime in our set $\{p_1, p_2, \ldots, p_N\}$). Suppose for the sake of contradiction that P can be written as a product of primes all of the form $4k - 3$. Then we have

$$4Q - 1 = P = (4k_1 - 3)(4k_2 - 3)\cdots(4k_m - 3) \tag{0.1}$$

for some integers $k_1, k_2, \ldots, k_m$ (here the factors $4k_1 - 3, 4k_2 - 3$ etc. are the supposed prime factors of P). By our lemma, the right-hand side of Equation (0.1) has residue 1 modulo 4. But the left-hand side clearly has residue 3, so we have a contradiction. Therefore, we conclude that P must have some prime factor r of the form $r = 4k - 1$.

The rest of the proof is the same as the proof of Problem 2. Since our prime r has residue 3 modulo 4, it must be in our set $\{p_1, p_2, \ldots, p_N\}$. Therefore, r divides Q, meaning r also divides $4Q$. Since r divides $4Q$ and P, r must divide their difference: $4Q - P = 1$. But r is an odd prime number, so $r > 1$, which means r cannot be a factor of 1. Therefore, as in Problem 2, we reach a contradiction. We conclude that the original statement was not true, so there *are* infinitely many primes of the form $4k - 1$.

Proofs by Induction

Problem 4. (20=5+5+10 pts) (Proposition 2.18 in Textbook) Prove the following three statements:

(i) For all $k \in \mathbb{N}$, $k^3 + 2k$ is divisible by 3.

(ii) For all $k \in \mathbb{N}$, $k^4 - 6k^3 + 11k^2 - 6k$ is divisible by 4.

(iii) For all $k \in \mathbb{N}$, $k^3 + 5k$ is divisible by 6.

Hint: In the induction step you might want to use the binomial formulas:

$$(n+1)^2 = (n+1)(n+1) = n^2 + 2n + 1,$$
$$(n+1)^3 = (n+1)(n+1)(n+1) = n^3 + 3n^2 + 3n + 1,$$
$$(n+1)^4 = (n+1)(n+1)(n+1)(n+1) = n^4 + 4n^3 + 6n^2 + 4n + 1.$$

Solution.

(i) For the base case, we check if the statement holds for $k = 1$. We get $1^3 + 2(1) = 3$, which is divisible by 3. Now assume $n^3 + 2n$ is divisible by 3 and we see if this still holds for $(n+1)^3 + 2(n+1)$. Indeed, we get

$$\begin{aligned}(n+1)^3 + 2(n+1) &= n^3 + 3n^2 + 5n + 3 \\ &= (n^3 + 2n) + (3n^2 + 3n + 3)\end{aligned}$$

where the first part in the parenthesis is divisible by 3 by our induction hypothesis. The sum of two numbers, each of which is divisible by 3, is also divisible by 3, so we are done.

(ii) We have $1^4 - 6(1)^3 + 11(1)^2 - 6(1) = 0$, which is divisible by 4. Assume $n^4 - 6n^3 + 11n^2 - 6n$ is divisible by 4. Then,

$$\begin{aligned}(n+1)^4 - 6(n+1)^3 + 11(n+1)^2 - 6(n+1) &= n^4 - 2n^3 - n^2 + 2n \\ &= (n^4 - 6n^3 + 11n^2 - 6n) + (4n^3 - 12n^2 + 4n)\end{aligned}$$

where the first part in the parenthesis is divisible by 4 by our induction hypothesis. The result then follows by a similar reasoning as part (i).

(iii) For $k = 1$, we get $1^3 + 5(1) = 6$ is divisible by 6, which is true. Now assume $n^3 + 5n$ is divisible by 6. Then,

$$\begin{aligned}(n+1)^3 + 5(n+1) &= n^3 + 3n^2 + 8n + 6 \\ &= (n^3 + 5n) + (3n^2 + 3n + 6) \\ &= (n^3 + 5n) + 3n(n+1) + 6\end{aligned}$$

where the first part in the parenthesis is divisible by 6 by our induction hypothesis. To finish this problem, we show $3n(n+1)$ is divisible by 6. First, notice that $n(n+1)$ will always be divisible by 2 because this product consists of one odd number and one even number. Then, multiplying this product by 3 tells $3n(n+1)$ must be divisible by 6.

Problem 5. (20=10+10 pts) Prove by induction the following two formulas:

(i) For all $k \in \mathbb{N}$, we have
$$1+2+3+4+\ldots+(k-1)+k = \frac{k(k+1)}{2}.$$
The left hand side is the sum of all the natural numbers less equal than k, i.e. from 1 to k, the latter included.

(ii) For all $k \in \mathbb{N}$, we have
$$1^2+2^2+3^2+4^2+\ldots+(k-1)^2+k^2 = \frac{k(k+1)(2k+1)}{6}.$$
The left hand side is the sum of *the squares* of all the natural numbers less equal than k, i.e. from 1^2 to k^2, the latter included.

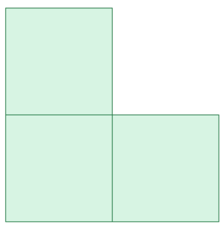
Solution.

(i) If $k=1$, then $1 = \frac{1(1+1)}{2}$, which is true. Now suppose
$$1+2+\cdots+(n-1)+n = \frac{n(n+1)}{2}.$$
Then,
$$\begin{aligned} 1+2+\cdots+(n-1)+n+(n+1) &= \frac{n(n+1)}{2}+(n+1) \\ &= \frac{n^2+n+2n+2}{2} \\ &= \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)((n+1)+1)}{2} \end{aligned}$$
where the first equality follows from our induction hypothesis.

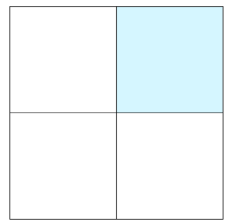
(ii) If $k=1$, then $1^2 = \frac{1(1+1)(2(1)+1)}{6}$, which is true. Now suppose
$$1^2+2^2+3^2+4^2+\ldots+(n-1)^2+n^2 = \frac{n(n+1)(2n+1)}{6}.$$
Then,
$$\begin{aligned} 1^2+2^2+3^2+4^2+\ldots+(n-1)^2+n^2+(n+1)^2 &= \frac{n(n+1)(2n+1)}{6}+(n+1)^2 \\ &= \frac{n(n+1)(2n+1)+6(n+1)^2}{6} \\ &= \frac{(n+1)(n(2n+1)+6(n+1))}{6} \\ &= \frac{(n+1)(2n^2+7n+6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \\ &= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6} \end{aligned}$$
where the first equality follows from our induction hypothesis.

Problem 6. (20 pts) Let $k \in \mathbb{N}$ be a natural number. Consider a $2^k \times 2^k$ square board divided into equal square tiles of 1×1 size, like a chess board. (So the $2^k \times 2^k$ board is covered by 2^{2k} tiles.) Remove one tile from the $2^k \times 2^k$ board. Prove **by induction** that the remaining part of the board can be covered with *triomino* pieces, i.e. pieces made of three unit tiles with an L-shape.

I have depicted in Figure 1 the triomino pieces (Left) and an example of the case $k = 1$ (Right), where you can see a board of size $2^1 \times 2^1$ with one tile (the blue one) removed. It is clear in this case, that the board with one tile removed can be covered with triomino pieces, in this case, exactly one triomino piece (covering the three white tiles).



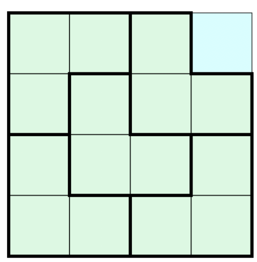
(A) A triomino piece.



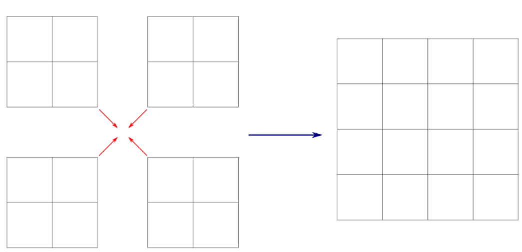
(B) The $2^k \times 2^k$ board with one tile removed in the case $k = 1$, where the board is 2×2.

FIGURE 1. The art of tiling a board with a missing tile with triominos, as presented in Problem 6. The goal is to prove that you can always tile with triominos if a tile is missing in a $2^k \times 2^k$ board.

Solution. The case $k = 1$ is covered above. To help us visualize this problem even more, let's consider the case $k = 2$ before our inductive step. If we remove one tile from a 4×4 board, then we see that we can cover the rest of the board with five triomino pieces.



Now assume a $2^n \times 2^n$ square board with one tile removed can be covered with triomino pieces. Consider a $2^{n+1} \times 2^{n+1}$ board, which we can think of as four $2^n \times 2^n$ boards. An example for $n = 1$ is shown below.



Let the tile we remove be on the top right. Then, by our induction hypothesis, the top right $2^n \times 2^n$ board can be covered by triomino pieces. To show the remaining three $2^n \times 2^n$ boards can be covered by triomino pieces, draw one triomino piece so that it occupies one space on each board (i.e. draw the piece near the center of the $2^{n+1} \times 2^{n+1}$ board). Then, we can apply our induction hypothesis to each board and we are done.

Problem 7. (20 pts) Let $k \in \mathbb{N}$ be a natural number. Consider k distinct straight lines in the plane. These are infinitely long straight lines, and we assume that no two such lines are parallel and no three such lines every intersect at a single point. Prove that k such lines divide the plane into $(k^2 + k + 2)/2$ regions.

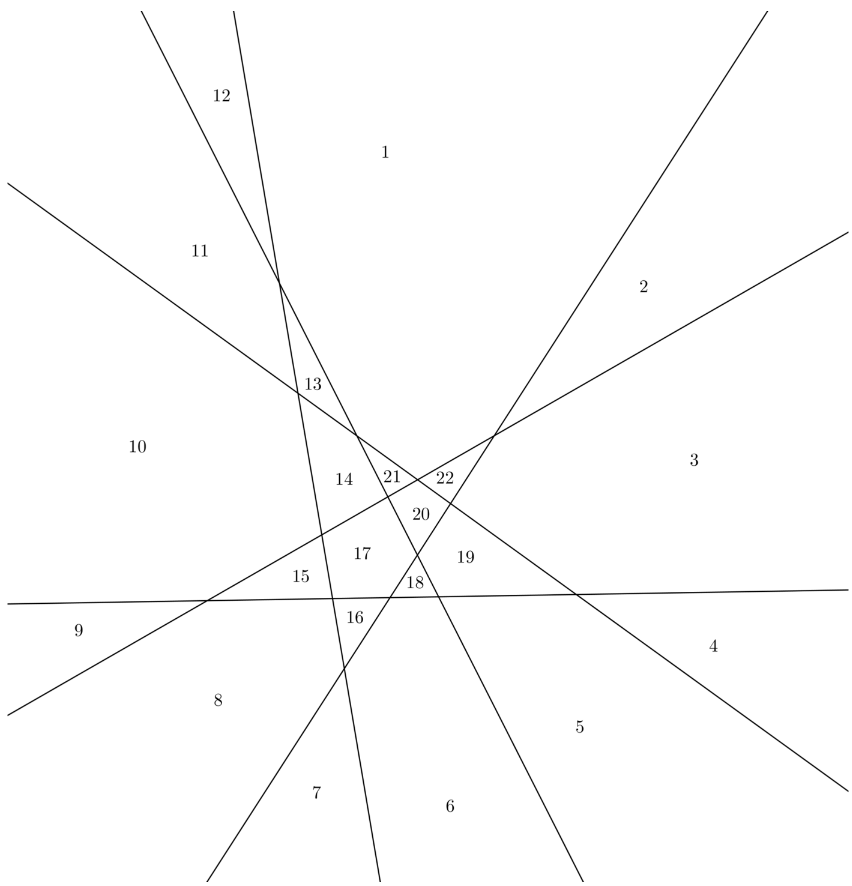
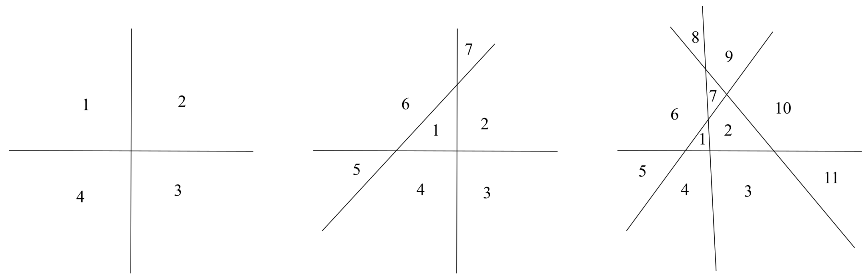


FIGURE 2. Six lines dividing the plane in 22 regions. This is the case $k = 6$ in Problem 7.

Hint: This can be proven by induction, but it is crucial in this problem that you play and experiment with this formula first. It will give you an intuition on how to prove the general case, by adding one line at a time and seeing how new regions appear.

For instance, for one line we have $k = 1$ and one line divides the plane into $(1^2 + 1 + 2)/2 = 2$ regions. By hand, try at least the formula for $k = 2, 3$ and $k = 4$. I have depicted the case $k = 6$ in Figure 2, where the plane is divided into $(k^2 + k + 2)/2 = (6^2 + 6 + 2)/2 = 22$ regions.

Solution. The case for $k = 1$ is covered above. The cases $k = 2, 3, 4$ are depicted below.



We have $(2^2 + 2 + 2)/2 = 4$, $(3^2 + 3 + 2)/2 = 7$, and $(4^2 + 4 + 2)/2 = 11$. We now prove the problem. The base cases were handled so we move on to the inductive step. Assume n lines satisfying our conditions divide the plane into $(n^2 + n + 2)/2$ regions. We look at what happens when we add one more line. Since this new line cannot be parallel to the other n lines and no three lines intersect at a single point, we conclude this line adds n intersection points. In other words, this new line is divided into $n+1$ segments so we have $n + 1$ additional regions. Thus, we have that $n + 1$ lines divide the plane into

$$\frac{n^2+n+2}{2}+(n+1) = \frac{n^2+3n+4}{2} = \frac{(n^2+2n+1)+(n+1)+2}{2} = \frac{(n+1)^2+(n+1)+2}{2}$$

regions.