Bounding Arguments

Written by Andy Tran for the MaPS Correspondence Program

15 February 2021

1 Introduction

Bounding arguments are an extremely useful tool in number theory and algebra, as it can significantly reduce the number of potential solutions to a particular problem. There is a wide variety of types of bounding arguments which we will explore in these lecture notes.

2 Dominating Terms

For large values of n and some constant c, notice that $n! > c^n > n^c > n$. If we see expressions like this, we can deduce that once the variables are sufficiently large, one side of an equation will be greater than the other side, so there will be no solutions. However, you will need to prove each step rigorously.

Example 2.1 *Find all positive integers n such that $2^n = n^2$*

Solution: For a question like this, where we are given an equation, it is usually a wise idea to try substituting a few numbers and seeing the behaviour of both sides! Indeed, the first few values of n give us:

n	2^n	n^2
1	2	1
2	4	4
3	8	9
4	16	16
5	32	25
6	64	36

Excellent, this already gives us two values for n where $2^n = n^2$, so we know that $n = 2$ and 4 are solutions! You will also notice that from here on, 2^n grows much more quickly than n^2, so you might want to prove that $2^n > n^2$ for $n \geq 5$ to show that there are no more solutions. Indeed, we can prove this by induction.

Lemma: $2^n > n^2$ for $n \geq 5$

In the base case, when $n = 5$ we have that $2^n = 32$ and $n^2 = 25$ so that $2^n > n^2$.

Now suppose that for some integer k, $2^k > k^2$. It suffices to show that $2^{k+1} > (k+1)^2$.

We have that

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &> 2 \cdot k^2 \quad \text{(inductive assumption)} \\ &= k^2 + k^2 \\ &> k^2 + 2k + 1 \quad (\text{as } k > 5) \\ &= (k+1)^2 \end{aligned}$$

This concludes the induction, so there are no solutions to $2^n > n^2$ for $n \geq 5$. This means that the only solutions to $2^n = n^2$ are $n = 2, 4$. $\square$

Exercise 2.2 *Find all positive integers n such that $2^n = n! + n$*

3 Factorisation and Divisibility

An important property of the integers (which makes number theory so distinguishable from algebra) is divisibility. The Fundamental Theorem of Arithmetic tells us that each positive integer can be factorised uniquely into primes, and so if we can factorise sides of an equation, we can greatly reduce the possible solutions to an equation. However, you may need to do some algebraic manipulation before you can factorise one side of an equation.

Example 3.1 *Find all integers m and n such that $mn = m + n$*

Solution: to aim for a factorisation, we can notice that the terms looks similar to $(m-1)(n-1) = mn - m - n + 1$. So lets try move things around and factorise!

$$mn = m + n$$

$$mn - m - n = 0$$

$$mn - m - n + 1 = 1$$

$$(m-1)(n-1) = 1$$

Since $m - 1$ and $n - 1$ are integers that multiply to 1, they must both be -1 or 1! This gives us the only solutions $(m, n) = (0, 0)$ or $(2, 2)$. $\square$

Exercise 3.2 *Find all integers m and n such that $\frac{1}{m} + \frac{1}{n} = \frac{1}{10}$.*

Factorisation and divisibility ties in quite nicely with the next section!

4 WLOG - Without Loss Of Generality

4.1 Symmetric Expressions

An expression is defined as **symmetric** if you can swap any two variables and the expression remains the same. For example if we swap x and y around in $x^2 + xy + y^2$, we obtain $y^2 + yx + x^2$ which is the same expression, so we may call it **symmetric**.

In a symmetric equation, we may assume that the variables follow an increasing or decreasing sequence (since we can just swap any pair of variables to arrange them in this way). ie. in the previous example, any possible values of x and y would have to satisfy $x \geq y$ or $y \geq x$. But we deduced that we could swap x and y around and the expression would remain the same. Hence, we may assume that $x \geq y$ and that if we have any pairs of values $(x, y) = (a, b)$ then by swapping the values $(x, y) = (b, a)$, we can accommodate for the case when $y \geq x$.

Hence, make sure you remember to account for permutations of solutions if you WLOG something during your proof.

4.2 Cyclic Expressions

Consider the following case: if we swap a and b around in the expression $a^2b + b^2c + c^2a$, we obtain $b^2a + a^2c + c^2b$ which is different, so this expression is not symmetric. However, if we **cycle** the variables $a \to b, b \to c, c \to a$ then we obtain $b^2c + c^2a + a^2b$ which is indeed the same as the original expression. We call such an expression **cyclic**, and notice how all symmetric expressions are cyclic but not all cyclic expressions are symmetric.

In a cyclic equation, we may assume that **one** of the variables is the smallest or largest (since we can cycle through the variables, until the our desired variable is the largest or smallest). For example, in the above example, we may assume that $a \leq b$ and $a \leq c$, but notice that we cannot assume that $a \leq b \leq c$.

Also, remember to account for cycles of your solutions if you WLOG this during your proof.

Example 4.1 *How many triples of integers* (a, b, c) *are there such that*

$$abc + ab + bc + ca + a + b + c = 104.$$

Solution: A starting point here would probably be to add 1 to both sides of the equation so it can be factorised!

$$abc + ab + bc + ca + a + b + c = 104$$

$$abc + ab + bc + ca + a + b + c + 1 = 105$$

$$(a + 1)(b + 1)(c + 1) = 105$$

Note that since a, b, c can be any integer and $105 = 3 \cdot 5 \cdot 105$, we have a lot of cases to consider! However, the equation is symmetric in a, b, c so we can WLOG assume that $a \leq b \leq c$, and consider unique factorisations of 105. This gives us the possible factorisations and the corresponding number of arrangements (n) accounting for symmetry:

$a+1$	$b+1$	$c+1$	n
3	5	7	6
1	7	15	6
1	5	21	6
1	3	35	6
1	1	105	3
-7	-5	-3	6
-15	-7	-1	6
-21	-5	-1	6
-35	-3	-1	6
-105	-1	-1	3

In total, we can see that there are 54 triples of integers (a, b, c) that satisfy the given equaiton. $\square$

Exercise 4.2 *Find all positive integers a, b, c such that $abc = ab + bc + ca$.*

5 Modular Arithmetic

Modular Arithmetic is a powerful tool in restricting the possible solutions to an equation because if an equation is to be true, it must also be true when the equation is taken to any modulus. This is particularly useful if we consider quadratic residues (in mod 4 or prime mods), cubic residues (in mod 7) and so on. Furthermore, it can be useful if we see factorials as they have many factors and so when they are sufficiently large, they will be congruent to 0 in any mod. Note that it often takes some trial and error to find which modulus to use.

Example 5.1 *Find all positive integers m and n such that $m^2 = n! + 5$*

Solution: Again, it might be a wise starting point to test some values to see if we can see any solutions and observe patterns. We'll test different values for n, and try to see if they are a square number (which means there is a solution for m)!

n	$n!+5$	square
1	6	no
2	9	yes
3	11	no
4	29	no
5	125	no
6	725	no

We have found one solution! And you may think that there might not be any more solutions... To do this, we can consider both sides in mod 7 for $n \geq 7$.

Note that if $n \geq 7$, we have that $7|n!$ so

$$n! + 5 \equiv 5 \ (mod\ 7).$$

But considering quadratic residues in mod 7, we have:

m	m^2 (mod 7)
0	0
1	1
2	4
3	2
4	2
5	4
6	1

This means that for all integers m, we have

$$m^2 \equiv 0, 1, 2, 4 \ (mod\ 7).$$

Since the left and right sides of the equation leave a different remainder when divided by 7, they cannot be equal for $n \geq 7$. Hence, the only solution is $(m, n) = (3, 2)$. □

Remark: Notice that we are actually using the contrapositive here! We are using the fact that:

an integer solution to the equation exists $\implies$ an integer solution exists in mod 7

is equivalent to

an integer solution does **not** exist in mod 7 $\implies$ **no** integer solution to the equation exists

Exercise 5.2 *Find all integers a and b such that $a^2 = b^5 + 7$*

6 The Discrete Inequality and Bunching

Another important property of the integers is that of discreteness, so this means that between two consecutive integers, there are no other integers. This leads to the **discrete inequality** which states that if m and n are integers such that $m > n$, then $m \geq n + 1$.

As obvious as this may be, it has some very powerful implications. For example, between any two consecutive squares, there are no other square numbers, and similarly for cubes and so on. Furthermore, if a and b are positive integers such that $a|b$, then we can deduce that $b \geq a$, but if we know that $b > a$, the discrete inequality tells us that $b \geq 2a$.

Example 6.1 *Find all positive integers n such that $n^2 + n + 1$ is a perfect square.*

Solution: To solve this question, you might notice that the expression $n^2 + n + 1$ looks a little bit similar to $n^2 + 2n + 1 = (n + 1)^2$ which is a perfect square! In fact, you know that it will be strictly less than $(n + 1)^2$. But also notice that since n is a positive integer, $n^2 + n + 1 > n^2$, another perfect square! Combining this, we can write:

$$n^2 < n^2 + n + 1 < n^2 + 2n + 1 = (n + 1)^2.$$

This means that $n^2 + n + 1$ is always between two consecutive squares, so it can never be a square itself! This means that there are no positive integers n such that $n^2 + n + 1$ is a perfect square. □

Exercise 6.2 *Find all integers a and b such that $a^2 + 4b$ and $b^2 + 4a$ are both squares.*

7 The Quadratic Discriminant

Another technique which can be used is with **quadratic discriminants** if we have a diophantine equation which is quadratic in one of the variables. From the quadratic formula, we then know that the discrimant must be a perfect square which can give us a simpler equation to deal with to look for solutions.

Example 7.1 *Find all integers m and n such that*

$$m^2 + 2mn - n = 1$$

Solution: This equation can seem quite scary at first and you should probably try to throw some of the earlier tricks at it. But one way to approach it is to rearrange it into a quadratic in m:

$$m^2 + 2mn - n - 1 = 0.$$

Now, if we look at the discriminant of this quadratic, we have

$$\Delta = (2n)^2 - 4(1)(-n-1)$$

$$\Delta = 4n^2 + 4n + 4$$
$$\Delta = 4(n^2 + n + 1)$$

In order for there to be an integer solution, we must have that Δ is a perfect square, and so $n^2 + n + 1$ must be a perfect square. But we have shown in example 6.1 that $n^2 + n + 1$ is not a square for any positive n.

However, $n^2 + n + 1$ is a square for $n = 0, -1$, but for $n < -1$, we have that

$$(n+1)^2 = n^2 + 2n + 1 < n^2 + n + 1 < n^2.$$

So that the only solutions can occur when $n = 0, 1$. Substituting in $n = 0$ gives the solutions $m = 1, -1$ and substituting in $n = -1$ gives the solutions $m = 0, 2$. Hence, all the solutions are $(m, n) = (-1, 0), (0, -1), (1, 0), (2, -1)$. □

Exercise 7.2 *Find all integers a and b such that*

$$2a^4 - ab + b^2 + 2 = 0.$$