Diophantine Equations (Number Theory)

Written By

James Bang

Baulkham Hills High School

Thursday 7th February, 2019.

1 | Introduction

Diophantine equations, named after Diophantus of Alexandria, are essentially equations which hold for integers, or some subset of the integers (such as the primes). They usually appear in a rather simple form in a competition paper (kinda like functional equations if you were in math club in 2018), however they may range from very easy to ridiculously difficult in nature. Some of the most difficult olympiad questions were Diophantine equations, and some (such as Fermat's Last Theorem) took mathematicians a full 358 years of progress to be solved.

In this handout, I will be demonstrating various elementary techniques in solving Diophantine equations. Some of them are very challenging, so I promise none of you will be bored. Have fun!

How to use this document: I believe there are not as many technicalities in understanding this topic, unlike the previous one. However, I still strongly recommend listening carefully in class as it is probably a lot quicker to have someone explain the concepts instead of trying to figure them out for yourself. At home, you should be attempting as many questions as possible (this is how you improve); if you're stuck, read over the section again to look for new techniques to use. If you are stuck for some time, just find me somewhere and I'll give some extra hints.

2 | Basic Definitions & Notations

A Diophantine question usually has the following structure/appearance:

Find all positive integers x, y, n such that the following equation holds:

$$(n^2+2)^x = (2n-1)^y.$$

So, as quite clear from the statement, we want to find **all** (ordered) triples of positive integers (x, y, n) such that if we plug them into the above equation, equality will hold. For example, if I let $n = 5$ and $x = 2$, $y = 3$ then I get $(27)^2 = (9)^3$, which is clearly true; this means $(x, y, n) = (2, 3, 5)$ is a **solution** to the above equation.

Notice that I have found one solution to the equation, namely $(2, 3, 5)$. **We haven't solved the question yet!!** The question is asking us to find **all** solutions to the equation, so we actually need to find as many as we can and **prove** that no other solution exists. (We won't solve this question now, but you will probably be able to by the end of this handout.)

- Often, instead of "Find all positive integers x, y, n", the alternative phrase "Find all $x, y, z \in \mathbb{N}$ (or $\mathbb{Z}^+$)" is used instead. These two statements mean the exact same thing: $\mathbb{N}$ and $\mathbb{Z}$ respectively mean the natural numbers (**NOT INCLUDING 0**) and all integers, and so $\mathbb{Z}^+$ means the positive integers (the exact same as $\mathbb{N}$). Similarly, the other "big sets" can be defined: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ represent the sets of rational, real and complex numbers respectively. Also $\in$ just means "is an element of".

- Sometimes, a Diophantine equation may be present in other forms, such as "Prove that there exists infinitely many (x, y) such that (equation)", or "Find all pairs of integers (x, y) such that (something) divides (something)". They're essentially just variations of Diophantine equations, and the same theory from this handout applies.

That's about it for definitions. Let's solve some questions! (Don't worry, it'll get harder.)

Problem 2.0.1: An example

Find all pairs of integers (m, n) such that $mn = m + n$.

Note that we want to find all integer solutions, so that includes negatives as well. What solutions are there? Trivially, $(0, 0)$ seems to work; upon further inspection, $(2, 2)$ also seems to work. Are there any more solutions?

Let's rewrite the equation in the form $mn - m - n + 1 = 1$. Now, notice that the left side factors, so

$$mn - m - n + 1 = (m - 1)(n - 1) = 1.$$

It looks like a pretty good step, because now we have two integers $m-1$ and $n-1$ that multiply to get 1. This means $m-1$ and $n-1$ are both either 1 or -1, which gives rise to the two solutions $(m, n) = (0, 0)$ and $(2, 2)$. $\square$

The above example demonstrates what is required to fully solve a Diophantine equation: first you must provide all solutions to the equation, and then come up with a reasoning/proof to show *why* those are the only solutions. However, **don't forget to plug in and test your solutions!** It may take only a few seconds, but it's always good to make sure that your "solutions" are actually indeed solutions.

3 | Techniques to solve Diophantines

Now that we (hopefully) understand the concept of a Diophantine equation, we will explore some approaches to solving such equations.

3.1 Modular Arithmetic (or "Mods")

We say that $a \equiv b \pmod{n}$ if and only if $n \mid a - b$. To **take something modulo** n is essentially taking the remainder of that number when divided by n.

It turns out that the congruence sign $\equiv$ behaves very similarly to the classical $=$ sign. It is straightforward to verify the following properties by definition:

- If $a \equiv b \pmod{n}$, then $ka \equiv kb \pmod{n}$ whenever $k \in \mathbb{Z}$
- If $a \equiv b \pmod{n}$, then $a + k \equiv b + k \pmod{n}$ whenever $k \in \mathbb{Z}$
- If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ whenever $k \in \mathbb{Z}^+$
- If $ak \equiv bk \pmod{n}$, then $a \equiv b \pmod{n/[\gcd(k, n)]}$ whenever $k \in \mathbb{Z}^+$.
- If $\gcd(a, n) = 1$, then a has a *unique inverse modulo* n: that is, there exists an integer b such that $ab \equiv 1$ or $b^{-1} \equiv a \pmod{n}$, and if b, b' are both inverses of a then $b \equiv b' \pmod{n}$.
- If $a \equiv b \pmod{n}$, then you also have $a \equiv b \pmod{d}$ for any divisor $d \mid n$.

The last few in the list point out it's usually very annoying to deal with composite mods. In fact, if $a^2 \equiv b^2 \pmod{n}$, then in general you cannot assume $a \equiv \pm b \pmod{n}$ unless n is prime. Therefore, we restrict ourselves to prime modulus p (or, at the very least, prime powers p^k); in this way, a lot of this gcd stuff can be removed, resulting in cleaner expressions to deal with.[1]

Well, what relevance does this have to Diophantines? It turns out that if an integer equation has a solution in $\mathbb{Z}$, then it must also have a solution when both sides are taken modulo n for any positive integer n. It seems kinda obvious, but if we select the right n, we may find certain properties on the integers that we are after.

Problem 3.1.1

Find all integer solutions (x, y) to the equation $x^2 = 3y^2 + 2$.

Testing some values, we can't seem to find a solution to the equation at all, making modular arithmetic a good candidate for solving this question, and so we start testing some mods. Taking mod 2 gives $x^2 \equiv y^2 \pmod{2}$, which really isn't that useful because there exist integer solutions to this (for example $(x, y) = (0, 0)$, although this isn't a solution to the original equation). What about mod 3? Then we get

$$x^2 \equiv 2 \pmod{3}.$$

But then we test out $x^2 \pmod{3} \equiv 0, 1, 1, 0, 1, 1, \ldots$, which means x^2 can never be $2 \pmod{3}$. Thus there are no solutions to the equation in modulo 3, and so no solutions over the integers. $\square$

The above example is one in which certain arithmetic functions, such as squares, leave a small (or "nice") set of residues in mod p for some prime p ($p = 3$ in the above case). There are other functions which leave nice residues mod n for certain values n (usually $n = p$ is prime), and some are in the table below.

Function $f(x)$	"Good" values of n	Residue of $f \pmod{n}$
$f(x) = x^2$	4 Essentially any prime $p \geq 3$	$0, 1$ Exactly $\frac{p+1}{2}$ residues
$f(x) = x^3$	7 13 $3 \mid p - 1$	$0, 1, -1$ $0, 1, -1, 8, -8$ Exactly $\frac{p+2}{3}$ residues
$f(x) = x^k$	$k \mid p - 1$	Exactly $\frac{p-1}{k} + 1$ residues
$f(x) = x!$	All n	$x! \equiv 0 \pmod{n}$ for all large x
$f(x) = a^x$	$n \mid a \pm 1$	$1, -1$

This is far from an exhaustive list, but most of the time you don't need to memorize such table; you can just test out the function modulo your chosen n and find its residues as in the problem above.

Problem 3.1.2

Prove that the equation $x^5 - y^2 = 4$ has no solutions (x, y) over the integers.

Since we want to show that the equation has no solutions, it may be a good idea to try showing that the equation has no solutions modulo n, for a well-chosen n. Which one could work?

[1] In fact, taking a number modulo n is equivalent to taking the number modulo $p^\alpha \mid n$ for each prime power p^α fully dividing n (i.e. $p^{\alpha+1} \nmid n$); this is known as the **Chinese Remainder Theorem**.

Well, in our equation we have an x^5 and y^2 term. Looking at our table, we know that x^k leaves a nice residue set modulo p (for a prime p) when $k \mid p-1$. So we want to find a prime p such that $5 \mid p-1$ and $2 \mid p-1$. How about try $p = 11$?

Notice $y^2 \equiv 0, 1, 3, 4, 5, 9 \pmod{11}$ and $x^5 \equiv 0, 1, -1 \pmod{11}$. So after subtraction modulo 11, we get

$$x^5 - y^2 \equiv 0, 1, 2, 3, 5, 6, 7, 8, 9, 10 \pmod{11},$$

and we are fortunate in this case since none of them are $4 \pmod{11}$. Hence there are no solutions. □

Problem 3.1.3. Find all integer solutions (x, y) to the equation $x^3 + y^4 = 7$.

Problem 3.1.4. Solve the equation $x^2 + y^2 = 2019$ over the positive integers.

Problem 3.1.5. Find all positive integer solutions (x, y) to the equation $x^2 - y! = 2001$.

Problem 3.1.6. Find all positive integers n such that $2^n + 7^n$ is a perfect square.

3.1.1 Fermat's Little Theorem

If I asked you to compute $17^{2016} \pmod{2017}$, then what would you do? It is technically possible to expand out 17^{2016} and long divide it to get the remainder, but that's impractical and also kinda stupid in some way, especially if there exists a faster way to do it.

Fermat's Little Theorem: *Suppose p is a prime number and a is any integer not divisible by p. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

To prove this, rewrite the above as $a^p \equiv a \pmod{p}$ (this version actually holds for $p \mid a$ as well, since both a^p and a are then divisible by p), and we use a tool called **mathematical induction**. For $a = 1$ we trivially have $1^a \equiv 1 \pmod{p}$. Suppose we have $k^p \equiv k \pmod{p}$ for some $k \geq 1$; we want $(k+1)^p \equiv k+1 \pmod{p}$ by the inductive hypothesis. Expanding[2] the bracket on the left gives

$$(k+1)^p - (k+1) = \sum_{j=0}^{p} \binom{p}{j} k^j - (k+1) \equiv \binom{p}{0} + \binom{p}{p} k^p - (k+1) \equiv k^p - k \equiv 0 \pmod{p},$$

where we have used $p \mid \binom{p}{k} = \frac{p!}{k!(p-k)!}$ for each $1 \leq k \leq p-1$, and $p \mid k^p - k$ by the inductive step. □

Now don't worry if this sounds super complicated, because we will resort to only applications of the theorem (at least for now, until perhaps section 3.5).

Problem 3.1.3

Do there exist 2018 integers $x_1, x_2, \ldots, x_{2018}$ such that both equations

$$x_1 + x_2 + \cdots + x_{2018} \equiv 1234 \pmod{2017},$$

$$x_1^{2017} + x_2^{2017} + \cdots + x_{2018}^{2017} \equiv 5678 \pmod{2017}$$

are satisfied?

It looks impossible at the start, but if you know Fermat's Little Theorem, it's not too hard; you have $x_i^{2017} \equiv x_i \pmod{2017}$ since 2017 is prime, so you have

$$1234 \equiv x_1 + x_2 + \cdots + x_{2018} \equiv x_1^{2017} + x_2^{2017} + \cdots + x_{2018}^{2017} \equiv 5678 \pmod{2017}$$

or so $2017 \mid 5678 - 1234 = 4444$, which obviously is not true. Hence there are no solutions. □

[2] If you really want to try understanding this proof, then look up Newton's Binomial Formula. Also see the footnote on the bottom of page 8, where I have detailed the formula for use in that section.

3.2 Bounding Arguments

Can the number $\sqrt{x^2+x+1}$ be an integer for a positive integer x? We could try supposing there exists some positive integer y such that $x^2+x+1=y^2$, which is equivalent to $(2x+1)^2+3=(2y)^2$ or $(2y+(2x+1))(2y-(2x+1))=3$, which finds no solutions for $x \geqslant 1$ since $2y+2x+1 \geq 2+2+1=5>3$, and $|2y-(2x+1)| \neq 0$ as it is odd. It works, but it doesn't seem like the neatest way to solve the question. (At least we hope for a slightly better way!)

An alternative way to solve this question would be to argue the following: Suppose $x \geqslant 1$, then we have

$$x^2 < x^2+x+1 < (x+1)^2 \implies x < \sqrt{x^2+x+1} < x+1.$$

Then if $\sqrt{x^2+x+1}$ is an integer, then it has to be strictly between two consecutive integers x and $x+1$, which is a contradiction and thus no x exists. □ (That's better!)

This technique is known as **Square Bunching**, and exists within a broader category of **Bounding Arguments**. Essentially, as the same suggests, we use a bit of algebra and inequalities to show that equality cannot hold; most of the time, it's used when you make the observation that one side has to grow so much faster than the other side that equality cannot hold for sufficiently large values. An example is as follows.

Problem 3.2.1

Find all positive integers x, y, z such that the number $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}$ is also a positive integer.

So the observation with this question is how if x, y, z are all super large, then each fraction has to be rather small, and their sum will be eventually less than 1 (and so can't be an integer). How do we formalise this notion?

What we do is as follows: Let's assume $x \geqslant y \geqslant z$ by re-ordering $\{x, y, z\}$. Then since the sum of the fractions is a positive integer, it must be at least 1, and so we have

$$1 \leq \frac{1}{x}+\frac{1}{y}+\frac{1}{z} \leq \frac{1}{z}+\frac{1}{z}+\frac{1}{z}=\frac{3}{z},$$

giving $z \leq 3$. This is pretty good, since we only need to check the cases $z=1,2,3$. For $z=3$ we easily get $x=y=3$, since z is the smallest of the three. For the other two cases, we have either $1/x+1/y$ or $1/x+1/y+1/2$ are integers; we can then use the idea above to bound both x and y separately.

Exercise: Finish off the problem using the hints given as above. □

Bounding arguments are usually very useful in problems in which using mods don't seem to simplify the problem much. There are other situations in which bounding arguments may be handy; for instance, if you have $a \mid b$ but $a \neq b$, not only do you have $b \geqslant a+1$, you actually have $b \geqslant 2a$.

Problem 3.2.2. Find all positive integer solutions (x, y) to $1+x+x^2+x^3+x^4=y^2$.

Problem 3.2.3. Find all positive integer solutions (x, y) to $y^2=x^2+xy^3-1$

Problem 3.2.4. Find all nonnegative integer solutions (x, y) to the equation $x^3+8x^2-6x+8=y^3$.

Problem 3.2.5. Find all triples of positive integers (x, y, z) such that

$$\left(1+\frac{1}{x}\right)\left(1+\frac{1}{y}\right)\left(1+\frac{1}{z}\right)=2.$$

Problem 3.2.6. Find all integer solutions (x, y) to the equation $y^2+y=x^4+x^3+x^2+x$.

Problem 3.2.7 (Extension to Problem 3.2.1). A positive integer n is given. Show that there are at least one, but only finitely many, n-tuples of positive integers $(x_1, \ldots, x_n)$ such that

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} \in \mathbb{Z}^+.$$

3.3 Infinite Descent

Infinite Descent is a method of forming a contradiction in a certain group of Diophantine equations, where the existence of a solution implies the existence of a "smaller" solution (in some sense). Since we are dealing with positive integers, they cannot decrease forever, which is a contradiction. This is demonstrated through the example below.

Problem 3.3.1: Irrationality of $\sqrt{2}$

Show that the equation $x^2 = 2y^2$ has no solution in **positive** integers x, y.

The idea of infinite descent occurs as follows. Suppose we have a solution (x, y). Then since a solution exists, a *smallest solution* (x_0, y_0) must exist (we can define it as the solution (x, y) such that $x + y$ takes the smallest value, and if there are many then randomly choose one), for which $x_0^2 = 2 \cdot y_0^2$.

Since $2 \mid x_0^2$, x_0 is even, and so there exists an integer $N \geqslant 1$ such that $x_0 = 2N$. Then substituting back into the equation gives

$$2y_0^2 = x_0^2 = (2N)^2 = 4N^2 \implies 2N^2 = y_0^2$$

and thus (y_0, N) is also a solution to the original equation. However, we have

$$N + y_0 = \frac{x_0}{2} + y_0 < x_0 + y_0,$$

contradicting the assumption that (x_0, y_0) is the minimal solution. Thus, since there is no minimal solution, there cannot be a solution at all. □

In fact, this is exactly how you prove that $\sqrt{2}$ is an irrational number; to see this, just notice that the equation is equivalent to $\sqrt{2} = x/y$, where the existence of such x, y lead to a contradiction as above. In a very similar way, you can show that any number of the form $\sqrt[b]{a}$, where a, b are positive integers, must be either an integer or is irrational. Try this!

Problem 3.3.2. Solve the equation $x^3 + 3y^3 + 9z^3 = 3xyz$ over the integers.

Problem 3.3.3. Find all positive integers x, y, z such that $x^2 + y^2 = 7z^2$.

Problem 3.3.4 (IMO 1988 Q6).[3] Let a, b be positive integers, for which $ab + 1 \mid a^2 + b^2$. Show that $\frac{a^2+b^2}{ab+1}$ is a perfect square.

Problem 3.3.5 (Fermat's Last Theorem, $n = 4$, generalised). Show that the equation $x^4 + y^4 = z^2$ does not have a solution in positive integers x, y, z.

3.4 Pell's Equation

Pell's equation is essentially an equation of the form $x^2 - Ny^2 = 1$, where N is a positive integer which is **not** a perfect square. It is known that for each such N, there exists a nontrivial solution (as in $(x, y) \neq (1, 0)$), however the proof of this fact is quite difficult and I won't include it here.

[3] This question is quite difficult. **Hint**: Turn it into $x^2 + b^2 = k(xb + 1)$, where $x = a$. Suppose you have the solution $a < b$ such that $|a + b|$ is minimal. You have a quadratic in x with a root a, so consider the other root b_1 of the equation, so that (a, b_1) is another solution. Is this solution "smaller" than (a, b)?

Problem 3.4.1

Are there infinitely many positive integers $n > k$ such that $1+2+\cdots+k = (k+1)+(k+2)+\cdots+n$?

Well in the current form the question doesn't look much appealing at all, and so let's try re-writing the equation. We can add the expression on the left side to both sides to get

$$2(1+2+\cdots+k) = 1+2+\cdots+n,$$

and since $1+2+\cdots+n = n(n+1)/2$ and $1+2+\cdots+k = k(k+1)/2$ we have

$$2k(k+1)/2 = n(n+1)/2 \implies 2((2k+1)^2-1) = (2n+1)^2-1$$

and upon letting $x = 2n+1$ and $y = 2k+1$ (with the condition that x, y are both odd) we arrive at

$$x^2-2y^2 = -1.$$

It's not quite a Pell's equation (we call equations of the form $x^2 - Ny^2 = a$ a "Pell-type equation"), but it really doesn't matter for our current purpose.

Notice that $(x, y) = (3, 2)$ is a solution to the equation $x^2-2y^2 = 1$, and further notice that $(x, y) = (7, 5)$ is a solution to the equation $x^2 - 2y^2 = -1$. Then we use the so-called **Brahmagupta's Identity**:

$$(a^2+Nb^2)(c^2+Nd^2) = (ac-Nbd)^2+N(ad+bc)^2.$$

If we have a solution (x, y) to $x^2 - 2y^2 = -1$ (for instance $(x, y) = (7, 5)$), then the identity gives

$$-1 = (x^2-2y^2)(3^2-2(2^2)) = (3x+4y)^2-2(2x+3y)^2$$

and so $(3x + 4y, 2x + 3y)$ is also a solution to the equation. This solution is clearly larger (in that $3x + 4y > x$ and $2x + 3y > y$), and furthermore both $3x + 4y$ and $2x + 3y$ are odd. This generates infinitely many solutions to the original equation, and so there are indeed infinitely many solutions. □

In general, for each Pell equation $x^2 - Ny^2 = 1$, there exists a solution (x_0, y_0) called the **fundamental solution** which minimises the value of x (in (x, y)). Then every other solution (x_k, y_k) is in the form

$$x_k + y_k\sqrt{N} = \left(x_0 + y_0\sqrt{N}\right)^k.$$

Problem 3.4.2. Show that the equation

$$\binom{n}{k-1} = 2\binom{n}{k} + \binom{n}{k+1}$$

holds for infinitely many pairs (n, k) of positive integers with $n > k$.[4]

Problem 3.4.3. Show that the equation $x^2 + y^2 - 1 = 4xy$ has infinitely many solutions in x, y.

Problem 3.4.4. Show that if $n \geqslant 1$ is such that $3n+1$ and $4n+1$ are both perfect squares, then $56 \mid n$.

Problem 3.4.5. Show that if $m = 2 + 2\sqrt{28n^2 + 1}$ is an integer, then m must be a perfect square.

Problem 3.4.6. Prove that if the difference of two consecutive cubes is n^2 for some positive integer n, then $2n - 1$ must be a perfect square.

3.5 "Lifting the Exponent" Lemma

In this section we will consider the following problem.

[4] The symbol $\binom{n}{k}$ is the **binomial coefficient** and is defined as $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Problem 3.5.1

Suppose a, b are **distinct** integers and p is a prime such that $p \mid a-b$. Show that $p^2 \mid a^p - b^p$.

So we have a p in the exponent which seems kinda random, and direct modular arithmetic doesn't really seem to do anything in this case. So, let's try some algebra!

Recall the formula $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$ (to prove it, just expand the brackets on the right and cancel terms). Therefore, since $p \mid a-b$, we may be interested in try showing

$$a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} \equiv 0 \pmod{p}.$$

If a, b are both divisible by p, then the problem is rather trivial since all the terms on the left are divisible by p. If $p \nmid a, b$, then we know $a \equiv b \pmod{p}$, and so

$$a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} \equiv \underbrace{a^{p-1} + a^{p-1} + \cdots + a^{p-1}}_{p \text{ terms}} \equiv p \cdot a^{p-1} \equiv 0 \pmod{p}.$$

So yay, we have proven the problem statement! □

After we have solved this question, we start asking ourselves, well exactly how many times can p divide the number $a^{p-1} + a^{p-2}b + \cdots + b^{p-1}$? It turns out the previous divisibility is rather tight:

Problem 3.5.2

Suppose a, b are integers and $p \geqslant 3$ is prime such that $p \nmid a, b$ and $p \mid a-b$. Then $p \mid \frac{a^p - b^p}{a-b}$, but

$$p^2 \nmid \frac{a^p - b^p}{a-b} \quad (= a^{p-1} + a^{p-2}b + \cdots + b^{p-1}).$$

We have already shown the first part of the problem in **Problem 3.5.1**. How on earth are we going to show the second part?

Let $b = a + pk$ for an integer k (since $p \mid a-b$). Then we try plugging into the equation, and we want to try showing

$$p^2 \nmid a^{p-1} + a^{p-2}(a+pk) + \cdots + a(a+pk)^{p-2} + (a+pk)^{p-1}.$$

It turns out we have to expand these brackets, but it's not as bad as you might expect:

Lemma: $(a+pk)^N \equiv a^N + Na^{N-1}pk \pmod{p^2}$, whenever $N \geqslant 1$.

Proof: By the Binomial Formula[5], we get that $(a+pk)^N = a^N + \binom{N}{1}a^{N-1}pk + \binom{N}{2}a^{N-2}(pk)^2 + \cdots$. Notice that each term of the form $\binom{N}{\ell}a^{N-\ell}(pk)^\ell$ is divisible by p^2 for each $\ell \geqslant 2$, so every term vanishes except for the first two, in mod p^2. Since $\binom{N}{1} = N$, the Lemma is done. □

Now we plug back into the equation above. We have

$$\begin{aligned}
&a^{p-1} + a^{p-2}(a+pk) + a^{p-3}(a+pk)^2 + \cdots + a(a+pk)^{p-2} + (a+pk)^{p-1} \\
&\equiv a^{p-1} + a^{p-2}(a+pk) + a^{p-3}(a^2 + 2apk) + \cdots + a(a^{p-2} + (p-2)a^{p-3}pk) + (a^{p-1} + (p-1)a^{p-2}pk) \\
&\equiv pa^{p-1} + pka^{p-2}(1 + 2 + \cdots + (p-1)) \pmod{p^2} \\
&\equiv pa^{p-1} + pka^{p-2} \cdot \frac{p(p-1)}{2} \pmod{p^2},
\end{aligned}$$

[5] The Newton's Binomial Formula is $(a+b)^N = \binom{N}{0}a^N + \binom{N}{1}a^{N-1}b + \binom{N}{2}a^{N-2}b^2 + \cdots + \binom{N}{N-1}ab^{N-1} + \binom{N}{N}b^N$, where $\binom{N}{k} = \frac{N!}{k!(N-k)!}$ and in particular $\binom{N}{N} = \binom{N}{0} = 1$ and $\binom{N}{1} = \binom{N}{N-1} = N$.

where we have used $1+2+\cdots+(p-1)=p(p-1)/2$. Now we recall $p\neq 2$ from earlier and so p^2 divides the latter term in the above. Furthermore $p\nmid a$, so we finally have

$$\frac{a^p-b^p}{a-b}=a^{p-1}+a^{p-2}b+\cdots+ab^{p-2}+b^{p-1}\equiv p\cdot a^{p-1}\not\equiv 0 \pmod{p^2}. \square$$

This proof may seem a bit brutal, but it is quite important to know this method of proving divisibilities.

Exercise: Check that the entire proof above still works when p is replaced by kp, where k is any positive integer not divisible by p; in other words,

$$p \mid \frac{a^{kp}-b^{kp}}{a-b}, \quad \text{but} \quad p^2\nmid \frac{a^{kp}-b^{kp}}{a-b}.$$

In fact, these problems are actually a special case of a well-established lemma, which is stated as follows.

Definition (ν_p): *For a prime p, we define the function $\nu_p(n)$ for an integer n as the number of times p divides n; in other words,*

$$\nu_p(n)=\begin{cases}\alpha & \text{if } \alpha \text{ is the integer such that } p^\alpha\mid n,\ p^{\alpha+1}\nmid n,\\ \infty & \text{if } n=0.\end{cases}$$

For example we have $\nu_3(81)=\nu_3(3^4)=4$ and $\nu_3(4)=0$. Also note the following properties:

- We have $a\mid b$ if and only if $\nu_p(a)\leq\nu_p(b)$ for all primes p. As a corollary, if $\nu_p(a)=\nu_p(b)$ for all primes p, then $a=b$. (If every prime divides a and b the same number of times, then $a=b$.)
- The function $\nu_p(n)$ is **log-additive**, i.e. $\nu_p(a)+\nu_p(b)=\nu_p(ab)$ holds for any integers a,b.
- We have $\nu_p(n)\leq\log_p(n)$. This is because $p^{\nu_p(n)}\mid n$ by definition, so $p^{\nu_p(n)}\leq n$ and take $\log_p$ of both sides to get the result. This property is useful for bounding arguments.
- If $\nu_p(a)\neq\nu_p(b)$, then $\nu_p(ka+\ell b)=\min\{\nu_p(a),\nu_p(b)\}$ whenever k,ℓ are integers not divisible by p.

With these properties stated out, we are ready to state the Lemma:

Lifting The Exponent Lemma: *Suppose $p\geqslant 3$ is a prime number, and a,b are distinct integers (not necessarily positive) such that $p\mid a-b$ but $p\nmid a,b$. Then for any positive integer n, we have*

$$\nu_p(a^n-b^n)=\nu_p(a-b)+\nu_p(n).$$

For the case $p=2$, if a,b both odd and $2\mid n$, then you have

$$\nu_2(a^n-b^n)=\nu_2(a^2-b^2)+\nu_2(n)-1.$$

In the case where $p=2$ and a,b,n odd, we have $\nu_2(a^n-b^n)=\nu_2(a-b)$.

It turns out that our methods in solving Problems 3.5.1 and 3.5.2 essentially generalise to give the above Lemma for the primes $p\geq 3$. You can try proving it if you want, but we will not go through it here; instead, we shall see some applications.

Problem 3.5.3

Let k be a given positive integer. Find all positive integers n such that $3^k\mid 2^n-1$.

Well, we currently cannot use Lifting the Exponent (LTE) Lemma because 3 does not divide $2 - 1$. However, we notice that 3 divides $4 - 1 = 2^2 - 1$, so we may be interested to try showing n even.

Suppose n is odd. Then by taking modulo 3, since $k \geqslant 1$ we have $2^n - 1 \equiv (-1)^n - 1 \equiv -2 \not\equiv 0 \pmod 3$, since n is odd which gives $(-1)^n = -1$. This is a contradiction, so n is even.

Now the problem is a direct application of the LTE Lemma, because we have $3^k \mid 4^{n/2} - 1$, and so we can obtain

$$k = \nu_3(3^k) \leq \nu_3(4^{n/2} - 1) = \nu_3(4 - 1) + \nu_3(n/2) = 1 + \nu_3(n)$$

which gives $\nu_3(n) \geqslant k - 1$. Since we had n even, it turns out that all such integers n is in the form $n = 2 \cdot 3^{k-1}N$ for a positive integer N. □

Problem 3.5.4. Show that the number $a^{a-1} - 1$ is never square-free[6] whenever $a \geqslant 3$.

Problem 3.5.5. Find the largest number k for which 2017^k divides the number

$$2016^{2017^{2018}} + 2018^{2017^{2016}}.$$

Problem 3.5.6. Let p be a prime number, and a, n are positive integers. Show that if $2^p + 3^p = a^n$, then $n = 1$.

Problem 3.5.7. Find all solutions to the equation $a^p - 1 = p^k$ where p is prime and a, k are integers.

Problem 3.5.8. For some integer n, the number $3^n - 2^n$ is the perfect power of a prime. Show that n is also prime.

Problem 3.5.9. Let r, s be two positive rational numbers such that for infinitely many $n \geqslant 1$, the number $r^n - s^n$ is an integer. Show that both r, s are integers.

Problem 3.5.10. Find all nonnegative integer solutions to the equation $x^5 + y^4 = 2013^z$.

3.6 Other useful lemmas and theorems (Not going over these in class)

- A **Pythagorean triple** $\left(x, y, \sqrt{x^2 + y^2}\right)$, $\gcd(x, y) = 1$, can be written as $(2mn, m^2 - n^2, m^2 + n^2)$.
- **Zsigmondy's Theorem:** Apart from a handful of exceptions, given positive integers $a > b > 0$ and $n \geqslant 1$, there exists a prime p (called the **primitive prime divisor**) such that $p \mid a^n - b^n$, but $p \nmid a^k - b^k$ for each $k < n$. Exceptions are $(a, b, n) = (2, 1, 6), (a, 2^k - a, 2)$ and $(a, a - 1, 1)$.
- **Cyclotomic Polynomials:** Let's suppose you factor $x^k - 1$ for $k = 1, 2, \ldots, n$. Each time you do so, you receive a "new" polynomial $\Phi_n(X)$: for instance $\Phi_1(X) = X - 1$, $\Phi_4(X) = X^2 + 1$, and in general

  $$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ \gcd(n,k)=1}} \left(X - e^{2i\pi k/n}\right).$$

  Then if $p \mid \Phi_n(x)$ for some integers n, x, then you have either $p \equiv 1 \pmod n$ or $p \mid n$. As a special case, if $p \mid x^2 + 1 = \Phi_4(x)$ for some integer x then $p = 2$ or $p \equiv 1 \pmod 4$.

4 | Problem Section

The problems in this section use one or more of the techniques I have described above. Some of them, especially the ones at the back, may be quite hard and may approach the level of the hardest questions

[6] A number n is **square-free** if and only if it can be represented in the form $n = p_1 p_2 \ldots p_k$ for distinct primes p_i (i.e. any $p \mid n$ has $\nu_p(n) = 1$).

ever proposed for the IMO. Stars indicate relative difficulty (with perhaps a bit of exaggeration at the end), and questions after 4.30 are rather difficult. As always, good luck!

Problem 4.1. Find all integer solutions (x, y) to the equation $x^2 = 65y - 1$.

Problem 4.2. Prove that there are no integer solutions to the equation $x^2 - 10y^2 = 3$.

Problem 4.3. Prove that there are no integer solutions to the equation $x^2 - 2y^2 = 10$.

Problem 4.4. Find all right angled Pythagorean triangles with their areas and perimeters equal.

Problem 4.5. Find all integers x such that $x^3 + 15x + 11$ is a perfect cube.

Problem 4.6. Find all triples (a, b, c) of positive integers a, b, c such that $ab + bc + ca = 2 + abc$.

Problem 4.7. Does there exist an integer n such that both $n + 3$ and $n^2 + 3$ are both perfect cubes?

Problem 4.8. Prove that if a prime number is of the form $a^b - 1$ $(b \geq 2)$, then $a = 2$ and b is a prime.

Problem 4.9. Prove that if a prime number is of the form $2^n + 1$, then n is a power of 2.

Problem 4.10. Find all pairs of positive integers (m, n) such hat $mn + 5m = 3n + 17$.

***Problem 4.11.** Find all integer solutions (m, n) to the equation $1 + 5 \cdot 2^m = n^2$.

***Problem 4.12.** Does the equation $x^n + y^n = z^{n+1}$ have infinitely many integer solutions (x, y, z)?

***Problem 4.13.** Find all positive integer solutions (x, y) to the equation $x^y = y^x$.

***Problem 4.14.** Let m, n be positive integers. Show that $m^{n+2} + m^{n+1} + m^n$ is **not** a perfect square.

***Problem 4.15.** Determine all triples of prime numbers (p, q, r) such that $p(q - r) = q + r$.

***Problem 4.16.** Determine all triples (x, y, p) of integers such that $x^4 + 4y^4 = p$ and p is prime.

***Problem 4.17.** Determine all pairs (x, y) of positive integers such that $x^2 + 24 = y!$.

***Problem 4.18.** Determine the largest $n \geqslant 1$ for which $4^n + 2^{2018} + 1$ is a perfect square.

***Problem 4.19.** Suppose a, b, c are positive integers. Show out of the three numbers a^2+b+c, b^2+c+a and $c^2 + a + b$, at least one of them is not a perfect square.

***Problem 4.20.** Find all pairs (m, n) of nonnegative integers such that $6^m + 2^n + 2$ is a perfect square.

***Problem 4.21.** Let p be a given odd prime. Determine all pairs (m, n) of positive integers that satisfy

$$(p - 1)(p^m + 1) = 4m(m + 1).$$

****Problem 4.22.** Prove that there are no pair of integers (x, y) other than $(0, 0)$ and $(0, -1)$ for which the equation $y(y + 1) = x(x^2 + x + 1)$ holds.

****Problem 4.23.** Determine all triples of positive integers (x, y, z) such that $7x^x + 13y^y = 20z^z$.

****Problem 4.24.** Find all pairs (x, y) of positive integers such that $x^{2012} = y^x$.

****Problem 4.25.** Let x, y, z be positive integers that satisfy

$$\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}.$$

Show that $20 \mid xy$.

****Problem 4.26.** Find all solutions in positive integers to the equation $21^x + 4^y = z^2$.

****Problem 4.27.** Let m be a positive integer and $p > m$ is a prime. Prove that the number of positive integers n for which $m^2 + n^2 + p^2 - 2(mn + np + mp)$ is a perfect square is independent of the prime p.

*****Problem 4.28.** Determine all pairs (a, b) of positive integers such that $ab^2 + b + 7 \mid a^2b + a + b$.

*****Problem 4.29.** Can we find an integer $N \geqslant 1$ divisible by exactly 2019 different primes, and also satisfies $N \mid 2^N + 1$? (N is allowed to be divisible by a prime power, as long as that prime is counted once.)

*****Problem 4.30.** Determine all ordered pairs (m, n) of positive integers such that $mn - 1 \mid n^3 + 1$.

*****Problem 4.31.** Let a, b, c, d be odd integers such that $0 < a < b < c < d$ and $ad = bc$. Suppose further that $a + d = 2^k$ and $b + c = 2^\ell$ for some positive integers k, ℓ. Show that $a = 1$.

*****Problem 4.32.** Determine all integers $n \geqslant 1$ such that $n^2 \mid 2^n + 1$.

*****Problem 4.33.** Let a, b, c, d be integers with $a > b > c > d > 0$. Suppose further that

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Show that $ad + bc$ is not prime.

*****Problem 4.34.** Let n, m, k, ℓ be positive integers with $n \geqslant 2$ such that $n^k + mn^\ell + 1$ divides $n^{k+\ell} - 1$. Prove that one of the following two properties hold:

- $m = 1$ and $\ell = 2k$;
- $\ell \mid k$ and $m = (n^{k-\ell} - 1)/(n^\ell - 1)$.

******Problem 4.35.** Find all pairs of prime numbers (p, q) for which $p > q$ and

$$\frac{(p+q)^{p+q}(p-q)^{p-q} - 1}{(p+q)^{p-q}(p-q)^{p+q} - 1}$$

is an integer.

**********Problem 4.36.** Let x and y be positive integers. If $x^{2^n} - 1$ is divisible by $2^n y + 1$ for every positive integer n, prove that $x = 1$.

***************Problem 4.37.** Find all positive integers $m, n \geqslant 2$ such that $q = m + 1 \equiv 3 \pmod 4$ is a prime number, and for some prime p and nonnegative integer a, the following equation holds:

$$\frac{m^{2^n - 1} - 1}{m - 1} = m^n + p^a.$$

********************Problem 4.38.** Find the smallest positive integer n for which there exists infinitely many n-tuples of distinct positive rational numbers $(r_1, r_2, \ldots, r_n)$ for which both

$$r_1 + r_2 + \cdots +_n, \quad \frac{1}{r_1} + \frac{1}{r_2} + \cdots + \frac{1}{r_n}$$

are integers.

****************************Problem 4.39.** Find all positive integers n for which there exist non-negative integers $a_1, a_2, \ldots, a_n$ such that

$$\frac{1}{2^{a_1}} + \frac{1}{2^{a_2}} + \cdots + \frac{1}{2^{a_n}} = \frac{1}{3^{a_1}} + \frac{2}{3^{a_2}} + \cdots + \frac{n}{3^{a_n}} = 1.$$

************************************Problem 4.40.** Let k be a positive integer. A sequence $a_0, a_1, a_2, \ldots$ of integers satisfy

$$a_n = \frac{a_{n-1} + n^k}{n}$$

for all integers $n \geqslant 1$. Show that $k - 2$ is divisible by 3.