UNIVERSITY OF TORONTO
MATH ACADEMY 2019

DAY 2: DIOPHANTINE EQUATIONS

1. Part I: Problems

Problem 1, Preparations: Solving Diophantine Equations in complicated and many ingenious techniques are required to solve them. It is a fact that there is no general method to solve them, and that ideas that work very well for some cases are not suitable at all for other. In this problem we will review and learn some facts that will be useful in what follows.

(1) Many Diophantine equations reduce to algebraic manipulations and factorizations. Some of them are very original and probably you already know some. Factor the following expressions:
   - $x^2 - y^2$,
   - $4x^2 + 4x + 1$,
   - $x^n - y^n$
   - $x^4 + 4y^4$, the factorization of this is called Sophie Germain Identity.
   - $x^3 + y^3 + z^3 - 3xyz$.
   - $x^4 + y^4 + (x+y)^4$, the factorization of this is used to study sums of fourth powers, just as we studied sums of squares.

(2) Many Diophantine equations rely on divisibility properties of certain type of numbers. Solve the following excercises:
   - What are the possible remindes of a sum of two squares when you divide it by 4? By 8?
   - Recall that

$$(x+y)^2 = x^2 + 2xy + y^2,$$
$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3,$$
$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4.$$

     Realize that for $p = 2$ and $p = 3$ all the coefficients of the middle terms (i.e. not of x^p, y^p) are multiples of p, whereas for 4 this is not the case as 6 is not a multiple of 4. Prove this always happens: *let p be a prime number, then all the middle coefficients of $(x+y)^p$ are multiples of p.*
   - A classical results in number theory is due to Fermat and states: *if p is a prime number and n is any integer, then $n^p - n$ is always divisible by p.* It is called *Fermat's Little Theorem.* Prove this using the previous question or otherwise.

(3) An useful tool goes by the name of *Vieta Jumping*. The idea is to construct a solution to an equation if we already know the previous ones. To understand this, prove the following:
- Consider the quadratic equation $AX^2+BX+C=0$, with $A \neq 0$, and let r_1 and r_2 be the solutions. Prove $r_1 + r_2 = -\frac{B}{A}$ and $r_1 r_2 = \frac{C}{A}$.
- Suppose for the quadratic equation we know a solution r_1. Justify that $-\frac{B}{A} - r_1$ is the other solution. This way of constructing a new solution from the coefficients and the known roots is what is called Vieta Jumping. It seems very simple, but it is quite useful.
- How should this look for the case of a higher degree equation?

Problem 2, Particular Diophantine Equations:: In this problem we will solve some particular Diophantine equations. You should find all the solutions to the given equations in integers or prove there are no solutions.

(1) Find all integer solutions to $a^2 + b^2 - 8c = 6$.
(2) Find all integer solutions to $x^4 - 6x^2 + 1 = 7 * 2^y$.
(3) Find all integer solutions to $(xy - 7)^2 = x^2 + y^2$.
(4) Find all natural numbers n for which $n^4 + 4^n$ is a prime number.
(5) Find all right triangles with integer side lengths such that their areas and perimeters are equal
(6) Find all integers n for which $n! + 7$ is an square.

Problem 3, Fermat's Descent: Many Diophantine equations actually have no solutions but to prove such a thing is extremely challenging. Fermat developed a method to achieve this which is based in the following idea: *every set of positive integers has a smaller element.*

The idea then is to *suppose* there exists a solution to a given Diophantine equation and construct a new one that is smaller according to some way of comparing solutions. In order to explain this idea better do the following problem (try it by yourself first): Prove that the equation

$$x^2 + y^2 + z^2 = 2xyz,$$

has as unique integer solution $x = 0$, $y = 0$ and $z = 0$.

(1) Justify that for any solution (x, y, z) all its entries are even numbers. (A way to do this is to check the possible residues when dividing by 4.)
(2) Now that you know all entries are even, write $x = 2u, y = 2v, z = 2w$. Prove that (u, v, w) is now a solution of $X^2 + Y^2 + Z^2 = 4XYZ$.
(3) Repeat the process to prove that any solution of $X^2+Y^2+Z^2 = 4XYZ$ must have X, Y, Z even and get now a solution, with their halves, of $X^2 + Y^2 + Z^2 = 8XYZ$.
(4) Justify why this process can continue forever, that is, starting with one solution (x, y, z), you can deduce every one of its entries is divisible by every power of 2.
(5) Conclude from the previous parts that $X = Y = Z = 0$.

Another method to solve this equation is based in a very famous inequality called **Arithmetic - Geometric Mean inequality**.

(1) Prove that for any positive numbers x and y we have
$$\frac{x+y}{2} \geq \sqrt{xy},$$
with equality only if $x = y$. The left hand side is called the *arithmetic mean* of x, y whereas the left hand side is called the *geometric mean*, which explains the name of the inequality.

(2) This inequality is general: for positive numbers $x_1, ..., x_n$ we have
$$\frac{x_1 + ... + x_n}{n} \geq \sqrt[n]{x_1 ... x_n}.$$
With equality if and only if all numbers are equal. In particular, the case of three numbers of the arithmetic - geometric mean inequality is
$$\frac{X+Y+Z}{3} \geq \sqrt[3]{XYZ}.$$
Prove this.

(3) We will use this for the Diophantine equation $x^2 + y^2 + z^2 = 2xyz$. Suppose you have a solution (x, y, z). Justify you can suppose all its entries are nonnegative.

(4) Use the inequality for three variables to prove that any solution (x, y, z) to the Diophantine euqation satifies
$$x^2y^2z^2 \leq \frac{8}{27}xyz.$$

(5) Prove there is a finite number of positive integers N such that
$$27N^2 \leq 8N$$
and from this that the value xyz of a solution only has a finite number of possibilities.

(6) Conclude from the previous parts that $(0, 0, 0)$ is the only solution to the equation.

If you are interested in proving the general Arithmetic Geometric mean inequality a very clever way to prove it is due to the mathematician Augustin Louis Cauchy and follows the following steps:

- First prove that if you know the inequality for the case of n, then you know it for the case of $2n$.
- Now prove that if you know the inequality for the case of n, then you know it for the case of $n - 1$.
- Since you already know it for $n = 2$, this two steps prove it for all n. Verify this.

Finally, to have another example, use infinite descent, or otherwise, to prove that $x^3 + 2y^3 + 4z^3 = 0$ has no other solution in integers than $(0, 0, 0)$. This equation is due to Euler.

Problem 4, On the sum of Squares: We have seen in the course several ways to study the sum of four squares. In here we will study the case of two squares. We will answer the question: *Which positive integers n are a sum of 2 squares, i.e. for which integers n there exist integers x, y such that*
$$n = x^2 + y^2.$$

There are several known proofs. Here we sill study Euler's proof of the theorem: *a number n is a sum of two squares if and only if every prime $q|n$ with $q = 4k + 3$ appears an even number of times.*

It is quite convoluted at some parts so make sure to have some examples at hand to do not get lost and do not get deterred by the intricacies of the questions. If you get stuck at one step, assume it and go to the next part!

(1) Prove $(x^2 + y^2)(z^2 + w^2) = (xz + wy)^2 + (xw - yz)^2$. We will use this identity in many tricky ways below.
(2) Prove that the set of numbers that is representable as a sum of two squares is closed under multiplication, that is, if a and b are representable as sum of two squares, so is ab.
(3) Suppose p is a prime number that is the sum of two squares and n is a sum of two squares such that $p|n$. Prove that n/p is also the sum of two squares. To do this write $p = x^2 + y^2$ and $n = a^2 + b^2$ and explore the quantity $(xa)^2 - (yb)^2 = (xa + yb)(xa - yb)$.
(4) Suppose that q is a prime number that is NOT the sum of two squares and n is a sum of two squares such that $q|n$. Prove that n/q has in its prime factorization a prime that is not the sum of two squares.
(5) Now let $n = a^2 + b^2$ be a sum of two squares, with a and b relatively prime, and d one of its divisors. Define x and y to be the integers such that $|a - xd|$ is minimal and $|b - yd|$ is minimal (make sure you understand what this means). Prove that $|a - xd| < d/2$ and $|b - yd| < d/2$.
(6) Suppose d is not a sum of two squares. Deduce there exists a number $q|d$, $q < d/2$ that is not a sum of two squares.
(7) Repeat the process, but now with q instead of d to obtain an infinite descent $d > q > ...$ of numbers, which are not sum of squares, that divide n. Conclude this is a contradiction.
(8) Verify that we have proved that if n is a sum of two relatively prime squares then all of its factors are sum of two squares.
(9) Prove that a prime p of the form $4k + 3$ is NOT a sum of two squares.
(10) Using Fermat Little Theorem for a prime $p = 4k + 1$, deduce that p divides $(1)^{4k} - 1, ..., (4k)^{4k} - 4k$. Consider the consecutive differences

$$(1)^{4k} - 2^{4k}, ..., (4k - 1)^{4k} - (4k)^{4k}.$$

Notice that each of them is of the form $a^{4k} - b^{4k} = (a^{2k} + b^{2k})(a^{2k} - b^{2k})$ and it is a multiple of p (make sure you agree with this). Since p is a prime it divides, for each difference, one of the factors. Prove that if it divides $a^{2k} + b^{2k}$ for some a and b, then it is a sum of two squares.
(11) Suppose you write, for some integer m, the sequence $1^m, 2^m, 3^m, ...$ in a row and below wrote the consecutive differences, and so forth. Let's see the case $m = 2$:

$$1, 4, 9, 16, 25, 36, 49, ...$$
$$3, 5, 7, 9, 11, 13, ...$$
$$2, 2, 2, 2, 2, ...$$

It evetually becomes constant. Let's see the case for $m = 3$:

$$1, 8, 27, 64, 125, ...$$
$$7, 19, 37, 61, ...$$
$$12, 18, 24, ...$$
$$6, 6, 6, ...$$

It again becomes constant. Prove that this is always the case and that the constant value is $m!$.

(12) Using the previous result, show that it can't be that p divides $(a^{2s}-b^{2s})$ for all consecutive differences, since it would divide $(4k)!$.

(13) From all your work so far conclude the theorem: a number n is a sum of two squares if and only if every prime $q|n$ with $q = 4k + 3$ appears an even number of times in its prime factorization.

Problem 5, Fermat's Last Theorem: Probably the most famous Diophantine Equation is Fermat's Last Theorem which says that for any integer $n > 2$ the only solutions to the Diohpantine Equation

$$x^n + y^n = z^n,$$

are the trivial ones, that is, $(x, y, z) = (0, 0, 0)$ and $(0, \pm 1, \pm 1)$ with the right choice of signs, and its permutations. This was conjectured by Fermat in 1637 and was a driving force for Number Theory until its final resolution by Andrew Wiles in 1994, using very sophisticated methods relating to modular forms!

Many instances of this equation, that is, for particular values of n, were solved by previous mathematicians by very clever arguments and the first real proof that holds for an infinite number of cases (but not all of course) is due to Sophie Germain. Here we explore some particular cases. Prove that it is enough to prove the theorem only for the case in which n is prime or a power of 2.

In here we will prove the case, due to Fermat, of $n = 4$. Other cases were known as $n = 3$, $n = 5$ and $n = 7$, these last two turned out to be extremely tricky!

(1) Prove that it is enough to prove the theorem only for the case in which n is prime or a power of 2.

(2) In order to prove the case $n = 4$, we need to study the case $n = 2$ for which there are infinite number of solutions. This equation is $X^2+Y^2 = Z^2$ and its integer solutions are called Pythagorean Triples, for obvious reasons! Prove that for any integers m and n, $(m^2 - nr, 2mn, m^2 + n^2)$ is a Pythagorean Triple.

(3) It turns out that **all** Pythagorean triples are constructed this way. Prove this.

(4) Now, for the proof of the case $n = 4$, we will study first the equation $X^4 + Y^4 = Z^2$. Prove that if this equation has no nontrivial solution then the case $n = 4$ of Fermat Last theorem is true.

(5) Prove that any solution to $X^4 + Y^4 = Z^2$ satisfies that any two of them are relatively prime, that is, share no common divisor.

(6) Once you know this, prove that one of X and Y is even and the other is odd. Suppose from now on X is odd. Prove that Z is even.

(7) For any nontrivial solution of $X^4 + Y^4 = Z^2$ we have (X^2, Y^2, Z) is a pythagorean triple. Hence, you have $X^2 = m^2 - n^2, Y^2 = 2mn, Z = m^2 + n^2$.
(8) Deduce the existence of relatively prime integers a and b such that $X = a^2 - b^2$, $n = 2ab$ and $m = a^2 + b^2$.
(9) Prove that $Y^2 = 4(a^2 + b^2)ab$. From this equation deduce that $a^2 + b^2$, a and b are each one a square.
(10) Form the previous point deduce the existence of a new solution (A, B, C) to $A^4 + B^4 = C^2$ with $|C| < |Z|$.
(11) Deduce that the last inequality leads to a contradiction and from this conclude the only solutions to $X^4 + Y^4 = Z^2$ is $0, 0, 0$.

Problem 6, Markov's Equation: A very interesting Diophantine Equation is

$$x^2 + y^2 + z^2 = 3xyz.$$

Notice we studied a similar equation in a previous problem, with the 3 substituted by 2, and saw that it had no solutions besides $(0, 0, 0)$. Things are very different here!

(1) Find all solutions to this equation with positive entries smaller than 50.
(2) Recall the Fibonacci Numbers given by $F_{n+2} = F_{n+1} + F_n$ and $F_1 = F_2 = 1$. Prove that the triple $(1, F_{2n-1}, F_{2n+1})$ is a solution to Markov's Equation. Conclude that this Diophantine equation has an infinite number of solutions!

Now that we know there is an infinite number of solutions, we ask if we can give them structure of some sort. The amazing answer to this is *yes* and the structure they have is called the *Markov tree*. In order to understand this structure we will use Vieta Jumping as follows: suppose (x, y, z) is a solution to the equation and consider the quadratic equation

$$T^2 - 3yzT + (y^2 + z^2) = 0.$$

(1) Justify that x is a solution to this quadratic equation. Since this is a quadratic equation, it has another solution besides x. Use Vieta Jumping to write this solution in terms of x, y, z.
(2) Using the previous step, conclude that given (x, y, z) we can construct another solution $(3yz - x, y, z)$.
(3) Use this method to construct solutions starting from $(1, 1, 1)$ via Vieta Jumping.
(4) To get rid of multiplicities we will now consider only solutions with $x \geq y \geq z$. For each solution, draw a node in the plane (i.e. your paper) and connect two nodes if you can construct one solution from the other via Vieta Jumping.
(5) The drawing you get is a tree! To prove this justify that every node, besides $(1, 1, 1)$ has exactly three neighbors (according to which element you apply Vieta jumping to). Explain why this implies this drawing is a tree.
(6) Now prove EVERY solution appears in the tree.

Problem 7, $y^2 = x^3 + 17$**:** A very important class of Diophantine Equations are called *Elliptic Curves*. They are extremely interesting because the structure of the rational solution, that is, solutions in rational numbers, not necessarily integers, have great structure. The theory is way more complicated that what we can explain here (it is hard!) but we can give a glimpse of where the ideas begin. The basic idea is to use analytic geometry:

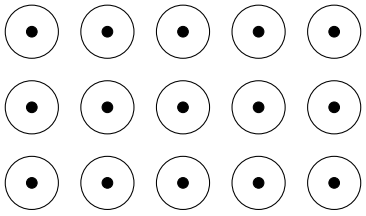
- Consider the points $P = (-2, 3)$ and $Q = (2, 5)$. Prove that they satisfy the equation.
- Find the equation of the line that goes through P and Q. This line, when graphed in the $XY-$plane intersects the curve $y^2 = x^3 + 17$ one more time. Find this intersection and call it R.
- Repeat the process now with P and R, and with Q and R.
- Justify why, if we keep doing this, every time we will find a new point whose coordinates are rational.
- Keep doing this, in an orderly way to do not get lost in your computations, until you have found 7 different solutions with *integer* entries.
- It turns out there is an extra one with integer entries, but to get to it doing this you will require some time. Using a computer find this point.

The idea of elliptic curves is that with this process, starting with some fixed points, in this case P and Q, and creating the line through them and finding the intersection, we get a set with a lot of structure. It is called *group structure*, in simple terms, is one in which we can *add* and *substract* and the main result is that there is a finite set of initial points such that repeating this process (which in the group language is called adding) generates all rational solutions!

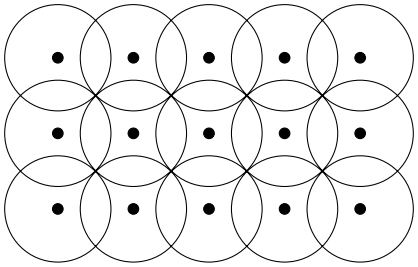
2. Part II: As seen in a book.

We have talked in the course about the four square theorem and in the excercises about the two square theorem. In both of them we have seen that it is important to solve the particular case of primes, that is, which primes are represented by the particular form. For the four squares every prime can be written in that form, and for the two squares only those of the form $4k + 1$. Hermann Minkoswki came up with a very ingenious argument to prove these results, giving birth to an area of number theory called *The Geometry of Numbers*.

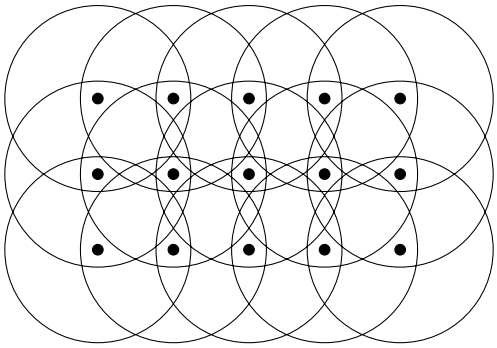
The idea of the concept that he introduced is about packings: that is, place a figure around the origin of the plane, and translate it to every integer point. For example, for circles of small radius it would look like this (the middle point is the origin):



But if we increase the radius the circles will intersect! But still, each circle has inside only one lattice point (that is, a point with integer coordinates) at its centre.



Eventually, if we make the radius huge, each translate will have other lattice point besides its center.



Minkowski's theorem states that this is not an accident and that it only depends on the form of the figure and its volume. A figure is *centrally symmetric* if reflecting it with respect to the origin does not change the figure. It is *convex* if the line joining two of its points is inside the figure. We present now a proof and a statement of Minkowski's theorem. Read it and think how would you explain it with your own words. You might have to find by yourself what is a lattice, this is an easy concept, but it is a good exercise to read the definition by yourself. If this confuses you, please ask!

One of the important observations of Minkowski, which we referred to in the beginning of this chapter, is the following.

Theorem 1.7 (Minkowski, 1896). *Let $C \subseteq \mathbb{R}^d$ be a convex body, centrally symmetric about the origin, and let Λ be a unit lattice. If $\operatorname{Vol} C > 2^d$, then C contains at least one lattice point different from $\mathbf{0}$.*

Proof. Consider the bodies $\frac{1}{2}C + u = \{\frac{1}{2}c + u \mid c \in C\}$, where $u \in \Lambda$. If two of them (say, $\frac{1}{2}C + u$ and $\frac{1}{2}C + v$) have a point p in common, then $p - u, p - v \in \frac{1}{2}C$. But then, $v - p \in \frac{1}{2}C$; thus $\mathbf{0} \neq v - u = (v - p) + (p - u) \in \frac{1}{2}C + \frac{1}{2}C = C$ and $v - u \in \Lambda$.

Hence, we may assume that the sets $\frac{1}{2}C + u (u \in \Lambda)$ are all disjoint, which easily implies that $\operatorname{Vol}(\frac{1}{2}C) = (1/2^d)\operatorname{Vol} C \leq 1$. □

FIGURE 1. Minkowski's Theorem

We also present a proof of the four and the two square theorem using this result. We have not introduced all the notation needed, but the only notation that you need to know how to codify is the following: we say that $a \equiv b \pmod{c}$ if c divides $a-b$. That is, if a and b leave the same reminder when divided by c. This symbol is called a *congruence* and was introduced by Gauss. It is a spectacular symbol that makes many things easier to handle. It is also called modular arithmetic. When reading this proof and you find the symbol translate it back to divisibility and do drawings! If you get confused with the notation, ask! This is a challenging task, but you can do it! Do particular examples!

After you have done this, you can go further and see the proof of the four square theorem. Now that you have read this, explain it with your own words and examples. Which proof do you like more of this theorem?

(The proofs are at the end of the document!)

3. Part III: Exploration

15 theorem: We have talked in the course about the four square theorem. A way to restate this theorem is as follows: we consider now a *function*

$$Q(x, y, z, w) = x^2 + y^2 + z^2 + w^2,$$

that we can evaluate at integer entries. For example,

$$Q(1, 2, 3, 2) = 1 + 4 + 9 + 4 = 18.$$

Using this quadratic form we can restate the theorem as: *the function Q takes all integer values when evaluated at integer points.* This type of function is called a quadratic form and they are very important object of study in mathematics and it has always been of interest to number theory to understand which integers can be represented by certain quadratic forms. A general quadratic form, without constant term, in n variables has the form

$$P(X) = A_1x_1^2 + ... + A_nx_n^2 + A_{12}x_1x_2 + ... + A_{ij}x_ix_j + ... + A_{n-1,n}x_{n-1}x_n.$$

An important distinction, that comes from the time of Gauss and his studies with these objects, is between forms in which each coefficient is an integer and those in which each coefficient is an integer and, moreover, the ones of mixed terms are even. The first ones are called integer-matrix forms, and the second ones are called integer-valued forms. We will focus on integer-matrix forms, for example, Q as above, or $R(x, y, z) = x^2 + y^2 + z^2 + 2yz$. There is a further restriction to be made, called positive definite, quadratic forms that asks that the form is always positive, except when it is evaluated at 0.

We have seen that Q represents every integer, but this could be asked of any other positive-definite integer-matrix quadratic form, and not every one satisfies this. For example x^2+y^2 does not represent every integer, as it doesn't represent the number 3. The same could be said about $x^2+y^2+z^2$ which fails to represent some integers. Those forms that do represent all integers are called **universal** and the 15 theorem is an spectacular criterion to decide when one of these forms is universal. It goes as follows:

The 15 **Theorem:** *If a positive-definite integer-matrix quadratic form represents every integer from* 1 *to* 15*, inclusively, then it is universal.*

This result, and related issues, have a long history but the final simple proof is due to Manjul Bhargava. (Some instances of this were known to Ramanujan, which proved this for quadratic forms of 4 variables.)

The Unicity Conjecture: We have studied the Markov Equation

$$x^2 + y^2 + z^2 = 3xyz.$$

A number that appears in a solution to this equation is called a Markov Number. An interesting exercise is to prove that every Markov Number appears in some solution as the biggest number of x, y, z. The unicity conjecture, which has a long history, and several proofs have been provided but they have been flawed, goes as follows: Every markov Number is the biggest number a *unique* time.

4. Images of the proofs of two and four square theorem.

All the images in this handout are taken from the book *Combinatorial Geometry* by Janos Pach and Pankaj K. Agarwal, chapter I.

Theorem 1.12 (Euler, Fermat). *Every prime p of the form $4m + 1$ can be expressed as the sum of the squares of two integers.*

Proof. If p is a prime of the form $4m + 1$ then, by Corollary 1.11, there is an integer $0 \neq z < p$ such that $z^2 \equiv -1 \pmod{p}$. It is easily seen that

$$\Lambda = \{(x, y) \in \mathbb{Z}^2 | y \equiv xz \pmod{p}\}$$

is a lattice in the plane with $\det \Lambda = p$ (see Exercises 1.7 and 1.8).

Let C be a disc of radius $r = \sqrt{3p/2}$ centered at the origin. Then

$$\text{Vol}\, C = r^2\pi = \frac{3\pi p}{2} > 4p = 2^2 \det \Lambda.$$

So by Theorem 1.7 there exists a point $(x, y) \in \Lambda$, different from the origin, for which

$$0 \neq x^2 + y^2 \equiv x^2 + x^2z^2 \equiv 0 \pmod{p}.$$

Since $x^2 + y^2$ is a multiple of p strictly between 0 and $2p$, $x^2 + y^2$ must be equal to p. □

Figure 2. Two Square Theorem

Theorem 1.13 (Fermat, Lagrange). *Every positive integer can be expressed as the sum of the squares of four integers.*

Proof. First observe that it is sufficient to show that every prime can be written as the sum of four squares. Indeed, if $n = n_1 n_2$ and

$$n_1 = x_1^2 + y_1^2 + v_1^2 + z_1^2, \qquad n_2 = x_2^2 + y_2^2 + v_2^2 + z_2^2,$$

then

FIGURE 3. Four Square Theorem, Page 1

$$\begin{aligned} n &= (x_1^2 + y_1^2 + v_1^2 + z_1^2)(x_2^2 + y_2^2 + v_2^2 + z_2^2) \\ &= (x_1x_2 - y_1y_2 - v_1v_2 - z_1z_2)^2 + (x_1y_2 + y_1x_2 + v_1z_2 - z_1v_2)^2 \\ &\quad + (x_1v_2 - y_1z_2 + v_1x_2 + z_1y_2)^2 + (x_1z_2 + y_1v_2 - v_1y_2 + z_1x_2)^2. \end{aligned}$$

Since $2 = 1^2 + 1^2 + 0^2 + 0^2$, we have to prove the assertion only for odd primes p. Notice that a^2 (as well as $-b^2 - 1$) takes exactly $(p+1)/2$ distinct values as a (resp. b) varies over the elements of $\mathbb{Z}_p$. Thus, we can choose $a, b \in \mathbb{Z}$ such that $a^2 \equiv -b^2 - 1$, i.e.,

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

Let us consider the lattice

$$\Lambda = \{(x, y, v, z) \in \mathbb{Z}^4 | v \equiv ax + by, z \equiv bx - ay \pmod{p}\}$$

in $\mathbb{R}^4$. It is easy to see that $\det \Lambda = p^2$. Denoting by C the four-dimensional ball of radius $r = \sqrt{1.9p}$, we obtain

$$\operatorname{Vol} C = \frac{r^4\pi^2}{2} = \frac{(1.9)^2\pi^2}{2}p^2 > 2^4 \det \Lambda.$$

Hence, by Theorem 1.7, there exists a point $(x, y, v, z) \in \Lambda$ satisfying

$$0 \neq x^2 + y^2 + v^2 + z^2 \leq r^2 < 2p.$$

On the other hand, modulo p we have

$$\begin{aligned} x^2 + y^2 + v^2 + z^2 &\equiv x^2 + y^2 + (ax + by)^2 + (bx - ay)^2 \\ &\equiv (x^2 + y^2)(a^2 + b^2 + 1) \equiv 0. \end{aligned}$$

Hence, $x^2 + y^2 + v^2 + z^2 = p$, completing the proof. □

FIGURE 4. Four Square Theorem, Page 2